IoT開発における
セキュリティ設計の手引き

2018 年 4 月

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目 次

図 目 次

表 目 次

公開にあたって

近年、IoT（Internet of Things）が多くの注目を集めている。IoT によってネットワークに接続される機器は、一部には IoT のために全く新しく開発されたものも存在するが、その多くは従来から存在するネットワークに接続されていなかった機器を改良したものである。

これまでの機器は、スタンドアロンで動作することが前提で、ハードウェアによる制御や機器内に閉じた回線を通した制御を行うものが多かった。これに対して、IoT に対応する機器では、インターネットを含む様々なネットワークと接続して動作すること、クラウドを活用すること、ソフトウェアで制御すること、個人情報などの機微な情報を含む様々な情報を取り扱うことを前提とし、セキュリティ設計を見直す必要がある。

情報システムではセキュリティの問題に対し、システムの脅威分析結果に基づいたセキュリティ設計と実装を行うと共に、そのシステムの運用時点において新たに発覚した脆弱性（セキュリティ上の弱点）の対策を含めて、対応を行っている。IoT においても、脅威分析結果に基づくセキュリティ設計・実装と、従来の情報システムで得られた脆弱性対策の知見を組み合わせた形で、対応していく事が重要である。しかしながら、IoT においては、その単体のシステムに閉じず、繋がることを前提とするネットワークや他システムやサービスとの接続面でのセキュリティや、その責任分界点など、様々な課題が存在している。

本書は、IoT 開発においてセキュリティ設計を担当する開発者に向けた手引きである。IoT のセキュリティ設計において行う、脅威分析・対策検討・脆弱性への対応方法を解説する。セキュリティを検討する上で参考となる、IoT 関連のセキュリティガイドを紹介する。また、いくつかの例題をもとに、IoT システムにおける脅威分析と対策検討の実施例を示す。

本手引きを活用することで、IoT に関わる各業界がセキュアな製品を、ユーザに提供できるようになることを期待する。

2016 年 5 月 12 日

独立行政法人　情報処理推進機構	辻　宏郷
独立行政法人　情報処理推進機構	岡下　博子
独立行政法人　情報処理推進機構	工藤　誠也
独立行政法人　情報処理推進機構	桑名　利幸
独立行政法人　情報処理推進機構	金野　千里

1. はじめに

1.1.IoT のセキュリティの現状と課題

IoTを情報の流れと構成からみると、「モノ」(Things:デバイス(機器)やシステム等)がネットワークと接続し、それを介して情報のやり取りをし、「モノ」に対しては情報やサービスが提供されるが、情報交換の相手は「モノ」同士であったり、他のシステムであったりする。また、「モノ」が所有している情報がネットワークを介してバックエンドにあるシステムやクラウドサービスに収集されてビッグデータとなり、様々な利用がなされたり、それにより新たに生成された情報が再び「モノ」にフィードバックされたりする。

これは、例えば「モノ」を PC に置き換えてみれば、一般的なインターネットシステムと構造的には何ら変わらない。従って、IoT に対する脅威としては、パソコンと同様のことを想定することになり、これまで情報セキュリティで培われてきた技術を活用して対策することになる。ただ、IoT の描く世界では、以下のような固有の様々な課題が存在しており、それらが対応を困難にしている。

(1) ネットに繋がる脅威をこれまで考慮してなかった分野の機器の接続が想定される
(2) 生命に関わる機器やシステムが繋がることが想定される
(3) 「モノ」同士が、無線等で自律的に繋がることが想定される
(4) 「モノ」のコストの観点から、セキュリティ対策が省かれることが想定される
(5) ネットを介して収集される情報の用途は、「モノ」側では制御が困難であり、バックエンドにあるシステムやクラウドサービス側での管理範囲となる
(6) つながる世界を拡げていくためには、「モノ」同士の技術的(通信プロトコル、暗号、認証等)、およびビジネス的な約束事が不可欠となってくる

この内、課題(1)(2)(3)(4)については、「モノ」におけるセキュリティ対策を「モノ」の開発者が考えることになるが、課題(5)(6)に対しては、様々な分野の事業者の連携や業界基準、あるいは個人情報やプライバシー情報の取り扱いなどにおいては制度や規制が必要になってくるものと考えられる。IoT の世界におけるセキュリティは、「モノ」単体やその製造者による管理に止まらず、「モノ」と接続して情報をやり取りするサービス側のセキュリティ(特に収集情報の取り扱い範囲と管理等)も絡んでくるため、問題を困難としている[11]。

1.2.本書のねらい

本書では、IoT のセキュリティ設計を担当する開発者に向けた手引きとして、参考となる情報をまとめたものである。

最初に、本書が対象とする IoT を明確化するために、IoT の全体像をモデル化し、各々の構成要素を定義する。

☞ **2. 本書における IoT の定義**

次に、IoT のセキュリティ設計において行うべき、脅威分析・対策検討・脆弱性への対応について解説する。

☞ **3. IoT のセキュリティ設計**

また、セキュリティを検討する上で参考となる、IoT 関連のセキュリティガイドを紹介する。

☞ **4. IoT 関連のセキュリティガイド**

そして、いくつかの例題をもとに、IoT システムにおける脅威分析と対策検討の実施例を示す。

☞ **5. IoT システムにおける脅威分析と対策検討の実施例**

最後に、IoT システムのセキュリティを実現する上で根幹となる暗号技術の重要性を説明し、実装した暗号技術の安全性を客観的に評価するためのチェックリストを添付する。

☞ **6. IoT セキュリティの根幹を支える暗号技術**

これらの情報が、IoT 開発におけるセキュリティ設計を進める上で、具体的な参考となることを目的としている。

IoT のセキュリティ設計においては、分野毎、システム毎に脅威分析や対策検討を行い、明確化することが重要である。本書に示す IoT のセキュリティ設計、典型的な分野における脅威分析と対策検討の実施例、参考となるガイド等を参考に、各々の IoT 開発におけるセキュリティ設計を行い、セキュアな製品開発の参考になることを期待している。

IPA ではこれまでに組込みセキュリティ[1][3]、情報家電セキュリティ[2]、自動車セキュリティ[4][6][7]、制御システム[5][17][19]、医療機器のセキュリティ[8]に関する調査報告や取り組みガイドを公表している。IoT 機器の内、該当する業界の方は、それらの資料も参照されることを推奨する。

なお、本手引きは、IPA が先行して公開している「つながる世界の開発方針」[12]の 17 指針における分析、設計、保守、運用の開発ライフサイクルの各指針（ただしセーフティに関する指針項目は本書の検討範囲外）を個別の IoT システム分野で実装していく際の、想定される脅威とセキュリティ対策の具体的な分析事例に相当する位置づけである。巻末の**付録 D.**に開発方針と本書の各記載項目との対応を示す。

2. 本書における IoT の定義

IoT を検討するために、様々な団体で IoT の全体像や構成要素のモデル化が行われている[23][24]。本書においては、IoT のセキュリティを検討するために、先行事例を参考にしながら、IoT の全体像をモデル化した(**図 2-1**)。

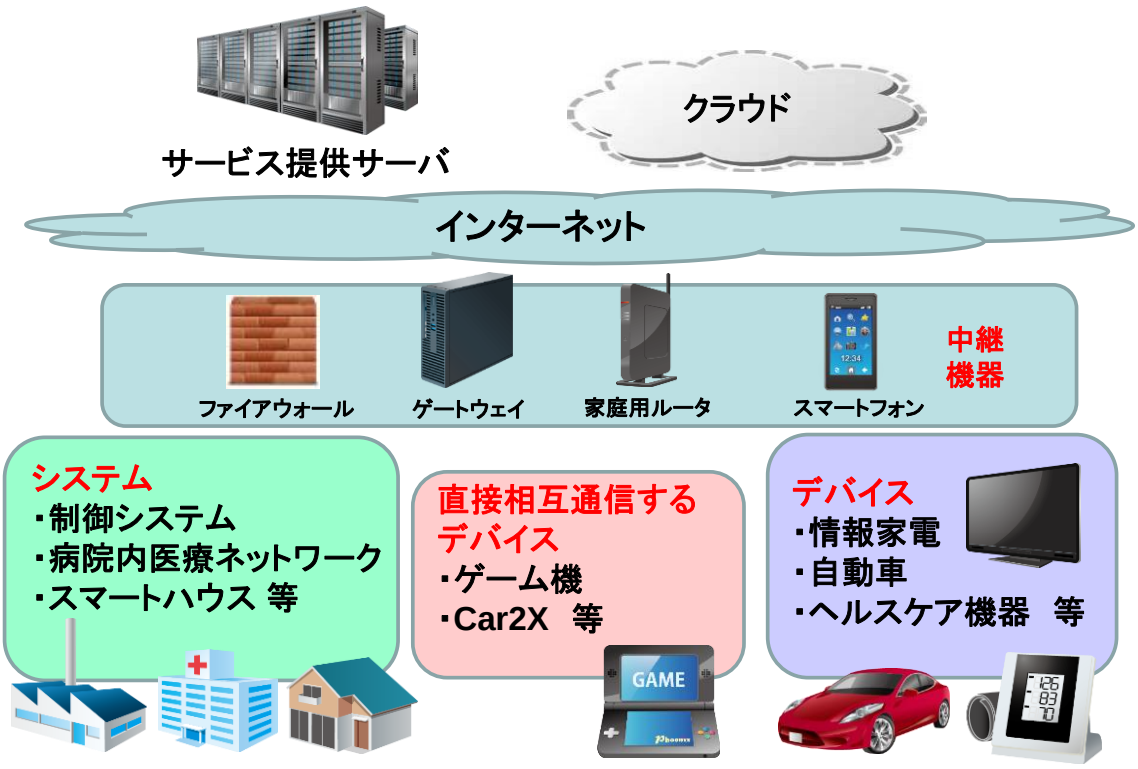


図 2-1　本書における IoT の全体像

以下に IoT の構成要素を定義する。本書では、以下の構成要素からなる IoT 全体像(IoT システム)のセキュリティを検討対象とする。

2.1.サービス提供サーバ・クラウド

第一の構成要素は、ネットワークに接続され、IoT に対応するサービスを提供するサーバやクラウドサービスである。IoT 対応以前からネットワークを介してサービスを提供している場合、脅威に対する対策を実施済みであろうと考えられる。

しかしながら、IoT によってこれまでにない様々な価値の高い情報が収集されることが想定され、攻撃者にとって従来以上に魅力的な攻撃対象となることから、運営事業者は既存の対策を強化していく必要がある。例えば、確実な脆弱性対策や認証・ログイン方法の見直しが重要である。

IoT を対象として新たにサーバやクラウドサービスを構築する場合は、従来から確立されてきたセキュリティ対策を実装すると共に、これらの点を考慮することが望まれる。

2.2. 中継機器

第二の構成要素は、IoT 機器やシステムをネットワークに接続する中継機器である。

従来から存在する据え置き型のファイアウォール、ゲートウェイ、ルータに加えて、容易に持ち運べるスマートフォンが中継機器としての重要な役割を担うようになってきている。

IoT におけるデバイスは、その種類によっては大きさや性能上の制限から充分なセキュリティ対策を実装出来ないことがある。この場合、中継機器において不正通信をブロックしてデバイスと通信させない等、デバイスのセキュリティ対策を補完する役割を担うことが期待される。

2.3. システム

第三の構成要素は、システムである。ここでは、単一の機器ではなく、複数の機器で構成されるシステムが、広義の IoT 機器として中継機器経由でネットワークに接続されるケースを想定している。システムの例として、制御システム、病院内の医療ネットワークシステム、スマートハウス（スマートホーム）等が考えられる。

システムによっては、長時間利用する機器や停止が許されない機器が存在し、脆弱性が発見されて更新ソフトウェアやパッチが提供されたとしても、それらを適用出来ないことがあり得る。また、元々はネットワークに接続されることを前提として設計されていないため、サポートの終了した OS やミドルウェア、アプリケーションを利用している場合もある。この様に、システム内部には充分なセキュリティが実装できない機器も存在するため、システム全体としてのセキュリティ対策が困難な場合もあり得る。

2.4. デバイス

第四の構成要素は、デバイス、即ち IoT によってネットワークに接続される機器（IoT 機器）である。情報家電、ヘルスケア機器等、様々な機器が存在する。自動車も一つの IoT 機器と考えることが出来る。

前述の通り、デバイス上に充分なセキュリティ対策を実装できない場合、対策の一部を中継機器

に代行してもらう可能性が考えらえる。

また、モバイル通信機能の低コスト化に伴い、今後は、中継機器を介さずにインターネットへの接続機能を有するデバイスが増加することが考えられる。この場合は、中継機器としての一部機能を内蔵する高機能なデバイスとして、中継機器とデバイスの二つの面からセキュリティを考慮する必要がある。

2.5.直接相互通信するデバイス

第五の構成要素は、直接相互通信するデバイスである。中継機器を通してネットワークに接続するだけでなく、デバイス自身が他のデバイスと直接通信する機能をもったものを、この分類としている。機器同士の通信機能を有するポータブルゲーム機や、車々間通信 Car2X に対応した自動車などが該当する。

この分類に属するデバイスは他のデバイスと直接通信を行うため、中継機器で不正通信を完全にブロックすることが出来ない。不正に改変・改造されたデバイスと接続した場合の対策を、デバイス上において実装する必要がある。

直接相互通信するデバイスも一つの IoT 機器であるが、直接相互通信しないデバイスとは異なる考慮が必要なことから、別の分類としている。

3. IoT のセキュリティ設計

一般的に、IoT 製品やサービスのセキュリティ設計を行う場合は、以下の手順で実施する。

Step1: 対象とする IoT 製品やサービスのシステム全体構成を明確化する。
Step2: システムにおいて、保護すべき情報・機能・資産を明確化する。
【脅威分析】
Step3: 保護すべき情報・機能・資産に対して、想定される脅威を明確化する。
【対策検討】
Step4: 脅威に対抗する対策の候補(ベストプラクティス)を明確化する。
Step5: どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して
選定する。

本章では、IoT のセキュリティ設計における脅威分析と対策検討、セキュリティ対策の一つとして必要不可欠な脆弱性への対応について解説する。

3.1. 脅威分析

IoT 製品やサービスに対してセキュリティ対策を検討するためには、脅威分析を実施し、保護すべき情報・機能・資産に対して想定される脅威を明確化することが必要である。

脅威分析には、様々なアプローチがある。一般的によく用いられるのは、対象となるシステム全体や構成要素に対して、想定される脅威を明確化し、脅威に対する脆弱性（攻撃を受け入れてしまうシステム上の弱点）、脅威に起因するシステムに対する被害（リスク）を評価する。そのリスク評価結果に基づき、リスクの高い箇所に脅威に対抗するためのセキュリティ対策を実装して脆弱性の低減を図ることになる。このアプローチによる典型的ないくつかの事例を、5 章で解説する。

一方、リスク脅威分析の他の手法として、システムやサービスに対して回避したい被害をまず列挙し、それぞれの被害を生じさせる脅威と脆弱性を考慮した「攻撃手順」（攻撃ツリー）を明確化し、各手順を抑止するための対策を選定するアプローチもある。IoT システム自体は、様々なシステムやサービスが絡んでくる広範なシステムも含まれてくることから、システムによっては、このアプローチも有効であるものと考えられる。以下ではこのアプローチの適用例を解説することにする。

最初に、回避しなければならない「被害」を列挙する。次に、その被害を発生させるいくつかの「攻撃シナリオ」に分類する。攻撃シナリオによっては、さらに細分化した「ケース」に分類することもある。最後に、その攻撃シナリオまたはケースを達成する「攻撃手順」（攻撃ツリー）へ分解していく。攻撃手順によっては、さらに複数の攻撃手順のシーケンス（AND 条件）や複数の選択肢（OR 条件）に細分化可能な場合もある。

この様に脅威分析を行った結果の表示例を**表 3-1** に示す。シーケンス（AND 条件）を連続する行、複数の選択肢（OR 条件）を空白行の挿入で表現している。この例では、**表 3-2** に示す攻撃シナリオ・攻撃手順により**「被害１」**が発生し得ることを示している。

表 3-1　脅威分析結果の表示例

被害1			
	攻撃シナリオ（1）		
		ケース（a）	
			攻撃手順1－1
			攻撃手順1－2
		ケース（b）	
			攻撃手順2
		ケース（c）	
			攻撃手順3
			攻撃手順4
	攻撃シナリオ（2）		
		攻撃手順5－1	
		攻撃手順5－2	

表 3-2　被害1に至る攻撃シナリオ・攻撃手順

#	攻撃シナリオ		攻撃手順シーケンス
1	攻撃シナリオ（1）	ケース（a）	攻撃手順1－1　→　攻撃手順1－2
2		ケース（b）	攻撃手順2
3		ケース（c）	攻撃手順3
4			攻撃手順4
5	攻撃シナリオ（2）		攻撃手順5－1　→　攻撃手順5－2

ここでは、例題として、個人の住宅や事業所に設置したカメラを用いて、遠隔（PC やスマートフォン、タブレット端末）から監視対象区域の静止画像等を監視する「ネットワークカメラ」システム（**図 3-1**）に対する、攻撃ツリーによる脅威分析の実施例を示す。

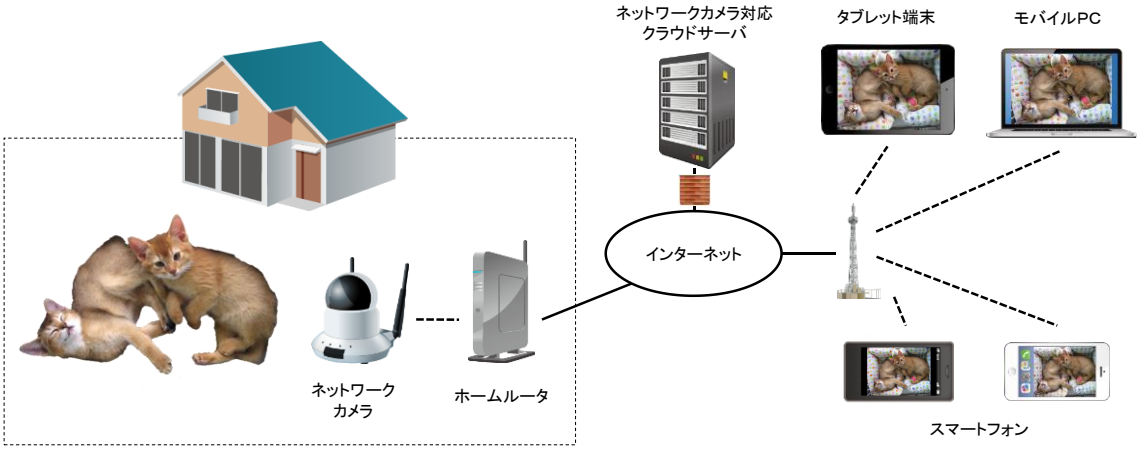


図 3-1　ネットワークカメラのシステム構成

最初に、以下の三項目をネットワークカメラとして回避すべき被害と設定し、上記被害を生じる脅威（攻撃シナリオやケース）を洗い出し、攻撃手順へと段階的に詳細化することによって、対策を検討するための材料とする。

- ネットワークカメラの画像を盗み見される。（**表 3-3**）
- ネットワークカメラからの画像が改ざんされる。（**表 3-4**）
- ネットワークカメラの画像が閲覧不能とされる。（**表 3-5**）

なお、ネットワークカメラの脆弱性を突いて侵入した後、ネットワークカメラとしての機能は正常動作させつつ、その裏で攻撃者が用意した不正プログラム（ウイルス）をネットワークカメラ上で動作させる攻撃も考えらえる。ネットワークカメラのユーザに直接的な被害は生じないが、DDoS 攻撃の踏み台に悪用された場合、「悪意のない加害者」として攻撃者（＝「悪意のある加害者」）に加担することとなり、結果として第三者に多大な被害を生じる恐れがある[16]。脅威分析においては、この様な攻撃も「脅威の一つ」として捉え、セキュリティ対策を検討する必要がある。

また、ネットワークカメラを用いるためには、家庭内またはオフィスにルータを設置し、インターネットに接続する必要がある。ルータを介して家庭内またはオフィス内のコンピュータや情報家電等に対する攻撃も想定されるため、実際には IoT 中継機器であるルータに対するセキュリティも考慮する必要があるが、本節における例示では省略している。

表 3-3　攻撃ツリーを用いたネットワークカメラに対する脅威分析の例（1/3）

1．ネットワークカメラの画像を盗み見される。			
	（1）正規のユーザに成りすましてカメラにアクセスして、画像を不正閲覧する。		
		（a）パスワードが設定されていないカメラの画像を不正閲覧する。	
			画像閲覧アプリ等を使用して、カメラにアクセスする。
		（b）パスワードがデフォルト値のままのカメラの画像を不正閲覧する。	
			画像閲覧アプリ等を使用して、デフォルト値のパスワードを入力し、カメラにアクセスする。
		（c）不正入手・判明したパスワードを利用して、カメラの画像を不正閲覧する。	
			画像閲覧アプリ等を使用して、パスワードリスト攻撃で不正ログインを試み、カメラにアクセスする。
			画像閲覧アプリ等を使用して、パスワード辞書攻撃で不正ログインを試み、カメラにアクセスする。
	（2）正規ユーザが閲覧中のカメラ画像データを、ネットワーク上で盗聴する。		
		ネットワーク上のパケットをキャプチャし、画像データ部分を抽出する。	
	（3）脆弱性を悪用してネットワークカメラ内部に侵入し、画像データを窃取する。		
		脆弱性を突いて、カメラ内部に不正アクセスする。	
		カメラ内部の画像データを抽出し、カメラの外へ持ち出す。	

表 3-4　攻撃ツリーを用いたネットワークカメラに対する脅威分析の例（2/3）

2. ネットワークカメラからの画像が改ざんされる。
（1）正規ユーザが閲覧中のカメラ画像データを、ネットワーク上で改ざんする。
ネットワーク上のパケットをキャプチャし、画像データ部分を改ざんする。
（2）脆弱性を悪用してネットワークカメラ内部に侵入し、画像データを改ざんする。
脆弱性を突いて、カメラ内部に不正アクセスする。
カメラ内部の画像データを抽出し、改ざんする。

表 3-5　攻撃ツリーを用いたネットワークカメラに対する脅威分析の例（3/3）

3. ネットワークカメラの画像が閲覧不能とされる。
（1）ネットワークカメラを DoS 攻撃して、応答不能状態または停止状態にさせる。
ネットワークカメラの IP アドレスおよびポート番号を割り出す。
ネットワークカメラに対して、大量のパケットを送信する。
（2）正規ユーザのカメラへのアクセスを妨害する。
（a）ホームルータを DoS 攻撃して、応答不能状態または停止状態にさせる。
ホームルータの IP アドレスおよびポート番号を割り出す。
ホームルータに対して、大量のパケットを送信する。
（b）クラウド経由のアクセスの場合、 クラウドサーバを DoS 攻撃して、応答不能状態または停止状態にさせる。
クラウドサーバの IP アドレスおよびポート番号を割り出す。
クラウドサーバに対して、大量のパケットを送信する。
（3）脆弱性を悪用してネットワークカメラ内部に侵入し、画像データを削除する。
脆弱性を突いて、カメラ内部に不正アクセスする。
カメラ内部の画像データを抽出し、削除する。

3.2.セキュリティ対策の検討

前節で述べた脅威分析の結果に基づき、必要となるセキュリティ対策を検討する。脅威および攻撃手法に依存するが、単一の対策によって攻撃を100%防御することは困難であり、複数の対策を組み合わせた多層防御が望ましい。

しかしながら、全ての対策を実装することは困難であるため、実装対象のリソース（CPU の処理能力やメモリ容量等）、投入可能なコスト、インシデント発生時の影響度等を考慮して、対策を選定する必要がある。

表 3-6～**表 3-7** に、主なセキュリティ対策候補の一覧を示す[1]。

表 3-8 に、前節で実施した脅威分析の一部（**表 3-3**）に対して、対策候補を洗い出した例を示す。

IoT の脅威対策において、暗号技術を用いた認証、電子署名、暗号化を導入することが考えられる。しかしながら、導入した暗号技術の利用方法に不備が存在した場合、それらによって生じる脆弱性を攻撃して暗号技術の効果を無効化する攻撃が成立する。採用した暗号技術の安全性を確認するチェックリストを**付録 C.**に添付したので、活用して頂きたい。

[1] 検討対象の IoT システムによっては、表中に記載したセキュリティ対策以外の対策や、表中に記載した対策を細分化・詳細化した対策が候補となる場合が考えられる。文献[19]では、全 47 項目の技術的対策／物理的対策／運用面での対策を紹介している。

表 3-6　対策候補一覧（1/2）

対策名	機能・目的	対応する脅威の例
脆弱性対策	開発段階での脆弱性混入を防止する。運用段階で検出された脆弱性を解消する。 （ソフトウェア更新の配布・適用やパッチ適用などを含む。詳細は、3.3 節を参照。）	ウイルス感染、不正アクセス
セキュア開発	実装時にセキュアプログラミングを実施する。また、セキュリティテストを実施したことを確認の上で出荷する。	ウイルス感染
サーバセキュリティ	サーバのセキュリティ（設定情報を含む）を定期的に確認し、問題があれば修正する。	不正アクセス
FW 機能	接続先を IP アドレス・ポート番号で制限する。	不正アクセス、DoS 攻撃
サーバ認証	クライアントがサーバを認証することにより、サーバへの成りすましを防止する。	成りすまし、情報漏えい
フィルタリング	信頼できないウェブサイトへのアクセスを禁止する。また、信頼できないアドレスからのメール受信を拒否する。	ウイルス感染、SPAM メール
IDS/IPS	入出力データを監視し、不正アクセスの検知、抑止を行う。	不正アクセス、DoS 攻撃
DoS 対策	DoS 攻撃（DDoS 攻撃を含む）を遮断するための対策を実施する。	DoS 攻撃
アンチウイルス	ウイルスを検知・除去して、ウイルス感染を防止する。	ウイルス感染
仮想パッチ	ソフトウェア更新等が実施できず、脆弱性を完全に除去できない場合、脆弱性を突いた攻撃を前段にてブロックする。	ウイルス感染
ユーザ認証	利用者を認証することにより、利用者の成りすましによる脅威を防止する。可能であれば、複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。	不正利用、不正アクセス、情報漏えい
メッセージ認証	通信相手から送信されたメッセージを認証することにより、通信相手への成りすましによる偽メッセージ送信や、メッセージの改ざんを防止する。	成りすまし、データ改ざん、不正コマンド

表 3-7　対策候補一覧（2/2）

対策名	機能・目的	対応する脅威の例
通信路暗号化	データの通信路を暗号化し、通信路上のデータが漏えいしたとしても、無価値化する（攻撃者にとって無意味なものとする）。また、通信路上でのデータの改ざんを検知する。	盗聴・改ざん
データ暗号化	データ自体を暗号化し、仮に蓄積時または通信時のデータが漏えいしたとしても、無価値化する（攻撃者にとって無意味なものとする）。	情報漏えい
データ二次利用禁止	データの目的外利用を禁止し、二次利用先からの漏えいを防止する。	情報漏えい
ホワイトリスト制御	予め許可したプログラム以外の動作を禁止し、ウイルス感染を防止する。	ウイルス感染
ソフトウェア署名	署名されたソフトウェアの動作のみ許可し、ウイルス感染したソフトウェアや不正改造されたソフトウェアの動作を防止する。	ウイルス感染、不正改造
出荷時状態リセット	IoT 機器を出荷時状態にリセットして、データや出荷後の設定を全て削除する。	情報漏えい
セキュア消去	記録していた場所から復元不可能な様にした上で、データを消去する。	情報漏えい
耐タンパーH/W	筐体開封を検知して内部情報を自動消去する等、ハードウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。	情報漏えい、不正改造
耐タンパーS/W	プログラムやデータ構造の難読化等、ソフトウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。	情報漏えい、不正改造
遠隔ロック	遠隔操作により IoT 機器の機能をロックし、第三者による不正利用を防止する。	不正利用
遠隔消去	遠隔操作により IoT 機器内のデータを消去し、情報漏えいを防止する。	情報漏えい
ログ分析	各種ログを分析することで、不正アクセスを検知し、何が行われたかを突き止める。	不正アクセス
説明書周知徹底	使用上の注意事項を説明書に明記し、使用開始前の利用者の一読を周知徹底する。	（設定誤り・操作誤りに起因する各種脅威）

表 3-8　脅威分析に対する対策検討の例

脅威	対策候補（ベストプラクティス）	
	対策名	備考
1．ネットワークカメラの画像を盗み見される。		
（1）正規のユーザに成りすましてカメラにアクセスして、画像を…		
（a）パスワードが設定されていないカメラの画像を不正閲覧…		
画像閲覧アプリ等を使用して、カメラにアクセスする。	ユーザ認証	パスワード未設定を許容しない。
	説明書周知徹底	パスワード設定の必要性を説明書にて注意喚起。
（b）パスワードがデフォルト値のままのカメラの画像を不正…		
画像閲覧アプリ等を使用して、デフォルト値のパスワードを入力し、カメラにアクセスする。	ユーザ認証	デフォルト値のままのパスワードを許容しない。
	説明書周知徹底	パスワード変更の必要性を説明書にて注意喚起。
（c）不正入手した・判明したパスワードを利用して、カメラの…		
画像閲覧アプリ等を使用して、パスワードリスト攻撃で不正ログインを試み、カメラにアクセスする。	ユーザ認証	一定回数以上のログイン失敗でロックアウト。
	説明書周知徹底	パスワードの使いまわしを説明書にて注意喚起。
画像閲覧アプリ等を使用して、パスワード辞書攻撃で不正ログインを試み、カメラにアクセスする。	ユーザ認証	一定回数以上のログイン失敗でロックアウト。
	説明書周知徹底	安易なパスワード利用を説明書にて注意喚起。
（2）正規ユーザが閲覧中のカメラ画像データを、ネットワーク上で…		
ネットワーク上のパケットをキャプチャし、画像データ部分を…	通信路暗号化	ネットワーク上転送データの暗号化。
（3）脆弱性を悪用してネットワークカメラ内部に侵入し、画像データを…		
脆弱性を突いて、カメラ内部に不正アクセスする。	脆弱性対策	脆弱性発生時の早期パッチ提供等。
カメラ内部の画像データを抽出し、カメラの外へ持ち出す。	データ暗号化	カメラ内部保存データの暗号化。

3.3.脆弱性への対応

IoT に脆弱性が存在すると、攻撃者にとって絶好の標的となり得る。従って、脆弱性への対応（脆弱性対策）は必要不可欠なセキュリティ対策であり、脆弱性を持った製品を出荷しないこと、脆弱性が発見された場合は速やかに解消することが重要である。本節では、開発段階および運用段階における脆弱性への対応の留意点を示す。また、IPA が提供する脆弱性対応に活用可能なコンテンツを紹介する。

3.3.1. 開発段階での対応

脆弱性を持った製品を出荷しないため、IoT の開発段階において、以下を実施すべきである。

(1) 新たに脆弱性を作り込まないこと

ソフトウェア（ファームウェア）開発において、セキュアプログラミング技術の適用やコーディング規約[10]の利用によって、新たな脆弱性を作り込まない様にする。ハードウェアに生じる脆弱性の対策（例えば、物理的な攻撃への対策）も考慮する。

(2) 既知の脆弱性を解消すること

ソフトウェア（ファームウェア）開発において、外部のソフトウェア部品（オープンソース等のフリーウェアを含む）を利用する場合、既知の脆弱性が存在しないか確認する。後述する脆弱性対策情報データベース JVN-iPedia が活用可能である。

なお、オープンソースを利用する場合、ソースコードが公開されているため、脆弱性の問題箇所が特定されやすく、脆弱性対策を怠った場合に、攻撃者によって攻撃手段として悪用されやすい点に留意すべきである。また、公開されているサンプルコードに脆弱性が存在し、そのままコピー＆ペーストで流用して開発した製品に脆弱性が混入した事例もあるため、サンプルコードは脆弱性が存在しないことを確認した上で利用すべきである。

(3) 残留している脆弱性を検出・解消すること

製品出荷前の脆弱性検査として、各種のテスト（既知の脆弱性検査、ソースコード検査、ファジング[9]による未知の脆弱性検出）を実施し、残留している脆弱性を検出・出荷までに解消する。

(4) 製品出荷後の脆弱性の新たな発見に備えること。

開発段階で脆弱性をゼロにすることは、容易ではない。製品出荷の時点では脆弱性でなかったものの、技術の進展に伴い脆弱性とみなされる場合（例えば、暗号アルゴリズムや鍵長の危殆化）もあり得る。従って、製品出荷後の脆弱性の発見に備えて、ソフトウェア（ファームウェア）の更新機能を実装すべきである。

3.3.2. 運用段階での対応

製品出荷後の脆弱性の検出や新規発見に備えて、また検出・新規発見が生じた際の対応として、IoT の運用段階にて以下を実施すべきである。製品出荷前に特別な断り書きをしていない限り、製品の動作保証をしているサポート期間中は、以下の対応を継続的に実施することが望まれる。

(1) 継続的な脆弱性対策情報の収集

出荷した製品自体、製品開発に利用した外部のソフトウェア部品において、新たな脆弱性が検出・発見されていないか、継続的な脆弱性対策情報の収集が必要である。

(2) 脆弱性対策情報（更新ソフトウェアを含む）の作成

新たな脆弱性が検出・発見された場合、脆弱性対策情報（脆弱性の概要、深刻度、影響を受ける範囲、想定される影響、対策等）を作成する。

ソフトウェア（ファームウェア）上の脆弱性の場合、通常の対策は、脆弱性を解消した更新ソフトウェア（アップデート）を提供し、利用者に適用してもらうことである。更新ソフトウェアの提供までに時間を要する場合や利用者がすぐに更新を適用できないと考えられる場合は、他の回避策（例えば、製品の特定の機能をオフにして脆弱性の影響を受けない様に抑止する）を準備する。

(3) 脆弱性対策情報の利用者への通知

脆弱性対策情報が作成できたら、速やかに、確実に利用者に通知することが望まれる。また、脆弱性情報が公知になった際に、悪用される危険性が高まるため、一斉に伝えられるようにしておくことが望まれる。周知を図る手段の一つとして、次節で述べる脆弱性届出制度の活用を検討して頂きたい。

(4) 更新ソフトウェアの製品への適用

更新ソフトウェアを提供した場合、速やかに、利用者に確実に適用してもらうことが重要である。

IT 技術に不慣れな利用者が使用する可能性がある製品や、利用者における更新ソフトウェアの適用が容易でない製品の場合、通信路や放送電波等による遠隔操作によって自動的に更新ソフトウェアを適用する方法が考えられる。この場合、製品出荷時の時点において、製品が自動更新機能を有していることを、取扱い説明書への分かり易い記載で利用者に適切に告知しておくことが望まれる。また、更新によって製品の持つ機能が変更される場合は、自動更新を避けて、利用者の了承を得る確認プロセスの後、更新を適用する様に実施することが望まれる。

なお、利用者における更新ソフトウェアの適用が困難な製品の場合やハードウェアの脆弱性の場合、IoT の製品分野によっては、リコールを実施し、製品を一旦回収してアップデート・改修作業を実施する可能性について考慮しておくことが必要であろう。

3.3.3. IPA が提供するコンテンツの活用

脆弱性への対応支援として、IPA では、脆弱性対策情報を提供するデータベース、脆弱性関連情報の適切な流通等により、被害発生を抑止するための制度等を運用している[11][13]。

(1) 脆弱性対策情報データベース:JVN iPedia[15]

IPA では、これまで報告された脆弱性対策情報をデータベースとその利用機能(例えば製品名やバージョンで該当する脆弱性を全て検索する機能等)を合わせて、脆弱性対策情報データベース「JVN iPedia」として一般公開している(**図 3-2**)。2018 年 3 月の時点において、約 80,000 件の国内外のソフトウェアの脆弱性対策情報が蓄積されている。従って、本データベースを、開発段階の対応(2)における業務に活用することや、運用段階の対応(1)における新規登録された脆弱性の有無確認や対策情報の収集に活用することが可能である。

(2) 脆弱性届出制度[14]

IPA では、ソフトウェア製品やウェブサイトで発見された脆弱性の届出を受付けている。受付けられた脆弱性は、ソフトウェア製品であれば、JPCERT/CC が開発者(提供者)に脆弱性対策対応を依頼し、対策情報が用意されたら、その情報を広く周知する役割を果たしている。これが、「早期警戒パートナーシップ」制度である。対策情報の用意された脆弱性は、(1)のデータベースにも登録される。本制度においては、毎年、多数の脆弱性情報が届出られており、家電やホームルータ等の

IoT 機器も含まれている。今後、IoT に関わる製品の届出がさらに増加すると推測される。

(3) IoT 製品・サービス脆弱性対応ガイド[21]

IPA では、IoT 製品や IoT サービスを開発・提供している企業の経営者や管理者を対象として、IoT 製品・サービスの提供における、セキュリティ対応に対する企業の責任の考え方や脆弱性対策が必要な理由を解説する「IoT 製品・サービス脆弱性対応ガイド」を公開した(**図 3-3**)。

上記以外の脆弱性対応支援については、「IPA 脆弱性対策コンテンツリファレンス」[13]を参照。

図 3-2　脆弱性情報データベース「JVN iPedia」

図 3-3　IoT 製品・サービス脆弱性対応ガイド

4. IoT 関連のセキュリティガイド

本章では、IoT のセキュリティを検討する上で参考となる、IoT 関連のセキュリティガイドを紹介する。本書の最初の版の公開（2016 年 5 月）を前後として、国内外において様々な機関・団体から IoT のセキュリティに関するガイドライン等が公開されている。**表 4-1** に IPA が公開した IoT 関連の主なガイドライン等、**表 4-2** に国内で公開された IoT 関連の主なガイドライン等、**表 4-3** に海外で公開された IoT 関連の主なガイドライン等を示す。

本書では、海外で公開された（英語で執筆された）セキュリティガイドの内、

- OWASP（Open Web Application Security Project）
- OTA（Online Trust Alliance）
- GSMA（GSM Association）

の活動とそれらの団体が無償で公開しているガイドについて紹介する。

表 4-1　IPA が公開した IoT 関連の主なガイドライン等

公開資料名	対象読者と主な内容	公開年月
つながる世界の開発指針[12]	・経営者、開発者、保守者 ・考慮すべき事項、指針	2016 年 3 月（第 1 版） 2017 年 6 月（第 2 版）
IoT 開発におけるセキュリティ設計の手引き	・開発者 ・具体的な設計手法	2016 年 5 月
「つながる世界の開発指針」の実践に向けた手引き　IoT 高信頼化機能編[18]	・開発者 ・設計時に考慮すべき高信頼化要件・機能	2017 年 5 月
ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト[20]	・調達者（利用者、運用者） ・機能要件、対策要件、対策方法	2017 年 12 月
IoT 製品・サービス脆弱性対応ガイド[21]	・IoT 製品・サービスの開発・提供企業の経営者・管理者 ・脆弱性対策の必要性の解説	2018 年 3 月

表 4-2　国内で公開された IoT 関連の主なガイドライン等

公開機関・団体	公開資料名	対象読者と主な内容	公開年月
経済産業省・総務省・IoT 推進コンソーシアム	IoT セキュリティガイドライン ver1.0[25]	・供給者、利用者 ・具体的なセキュリティ要件	2016 年 7 月
内閣官房サイバーセキュリティセンター（NISC）	安全な IoT システムのためのセキュリティ に関する一般的枠組[26]	・設計者、構築者、運営者 ・基本的なセキュリティ要件	2016 年 8 月
日本クラウドセキュリティアライアンス[27] （CSAJC）	IoT 早期導入者のためのセキュリティガイダンス （2015 年 4 月公開英語版の翻訳）	・実装者 ・具体的な管理手法	2016 年 2 月
	IoT における ID/アクセス管理　要点ガイダンス （2015 年 9 月公開英語版の翻訳）	・ID 管理の運用者 ・具体的な推奨要件	2016 年 4 月
	Internet of Things（IoT）インシデントの影響評価 に関する考察	・事業者（構築者・運営者） ・リスク評価手法	2016 年 4 月（v1.0） 2016 年 5 月（v1.1）
	「つながる世界」を破綻させないための セキュアな IoT 製品開発　13 のステップ （2016 年 11 月公開英語版の翻訳）	・IoT 機器の開発者 ・具体的な設計・開発手法	2017 年 5 月（v1.0） 2017 年 6 月（v1.1）
重要生活機器連携セキュリティ協議会[28] （CCDS）	製品分野別セキュリティガイドライン　車載器編	・特定の IoT 機器の設計に 関わる会社の経営者、 設計者、開発者 ・システムインテグレータ、利用 者（金融端末（ATM）編のみ） ・特定の製品分野において考慮 すべき設計・開発手法	2016 年 6 月（v1.0） 2017 年 5 月（v2.0）
	製品分野別セキュリティガイドライン　IoT-GW 編		
	製品分野別セキュリティガイドライン　金融端末（ATM）編		
	製品分野別セキュリティガイドライン　オープン POS 編		
	IoT セキュリティ評価検証ガイドライン	・設計者、開発者、評価検証 エンジニア、管理責任者 ・セキュリティ評価検証 プロセス、リスク評価手法	2017 年 6 月
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[29]	・コンシューマ向け IoT 機器の 開発者、サービス提供者 ・考慮・検討すべき事項	2016 年 6 月
日本防犯設備協会	防犯カメラシステムネットワーク構築ガイドⅡ －インターネットとの接続に係る脅威と対策－[30]	・システム設計／構築／運営者 ・設計時・運営時の留意点	2017 年 5 月

表 4-3　海外で公開された IoT 関連の主なガイドライン等

公開機関・団体	公開資料名	対象読者と主な内容	公開年月
OWASP （The Open Web Application Security Project）	Top 10 IoT Vulnerabilities from 2014	・製造者、開発者、利用者 ・具体的なセキュリティ要件	2014 年
	IoT Vulnerabilities	・製造者、開発者、利用者 ・脆弱性と攻撃対象の概要	2017 年 8 月
FTC （Federal Trade Commission：連邦取引委員会）	Internet of Things: Privacy and Security in a Connected World[31]	・コンシューマ向け IoT 機器の開発者 ・利点とリスク	2015 年 1 月
GSMA（GSM Association）	GSMA IoT Security Guidelines	・設計者、開発者、サービス提供者、通信事業者 ・設計・実装方法、運用方法	2016 年 2 月（v1.0） 2017 年 10 月（v2.0）
	GSMA IoT Security Assessment	・開発者、サービス提供者 ・セキュリティ評価チェックリスト	2017 年 10 月
OTA（Online Trust Alliance）	OTA IoT Trust Framework	・開発者、利用者 ・戦略的な原則	2016 年 3 月（v1.0） 2017 年 6 月（v2.5）
NIST （National Institute of Standards and Technology：米国国立標準技術研究所）	NIST Special Publication 800-183: Networks of ‘Things’[32]	・計算機科学者、IT 管理者、ネットワーク専門家、ソフトウェア技術者 ・モデル化、原理・原則	2016 年 7 月
IIC（Industrial Internet Consortium）	Industrial Internet of Things Volume G4: Security Framework[33]	・産業向け IoT（IIoT）の所有者、運用者、システムインテグレータ、ビジネス上の意思決定者等 ・セキュリティアーキテクチャ、設計・運用方法	2016 年 9 月
U.S. Department of Homeland Security （米国国土安全保障省）	Strategic Principles for Securing the Internet of Things[34]	・開発者、製造者、サービス提供者、利用者 ・戦略的な原則	2016 年 11 月
IoT Security Foundation	IoT Security Compliance Framework[35]	・開発者 ・基本的な原則	2016 年 12 月
ENISA（European Union Agency for Network and Information Security）	Baseline Security Recommendations for IoT[36]	・製造者、開発者、運用者、利用者 ・基本的な推奨要件	2017 年 11 月

4.1.OWASP Internet of Things Project

OWASP（Open Web Application Security Project）は、組織による信頼可能なアプリケーションの考案・開発・獲得・操作・維持を可能とするために活動している、国際的なオープンなコミュニティである。OWASP の運営母体である OWASP Foundation は、2001 年 12 月に設立され、2004 年 4 月にアメリカ合衆国政府認定 NPO となっている。

OWASP Internet of Things Project[37][45]は、OWASP 内のプロジェクトの一つであり、製造業者・開発者・消費者の IoT に関わるセキュリティ上の問題の理解向上を支援すること、IoT 技術の構築・展開・評価に際して利用者のセキュリティ上の検討を支援することを目的とした活動を行っている。このプロジェクトの成果は、Creative Commons Attribution-ShareAlike 3.0 License で公開されている。このプロジェクトでは、製造業者・開発者・消費者（利用者）の三つの観点からセキュリティを検討している。2017 年 8 月末の時点では、

- IoT Attack Surface Areas Project[38]
- IoT Testing Guides Project [41]
- IoT Vulnerabilities Project[39]

等の複数のサブプロジェクトに分割されており、それぞれの成果として、

- IoT Attack Surface Areas[38]
- IoT Vulnerabilities[39]
- Top 10 IoT Vulnerabilities from 2014[40][47]
- Firmware Analysis
  (Security Testing Guidance for IoT Attack Surface “Device Firmware”)
- IoT Testing Guides[41][46]
- IoT Security Guidance[42]
- Principles of IoT Security[43]
- IoT Framework Assessment[44]

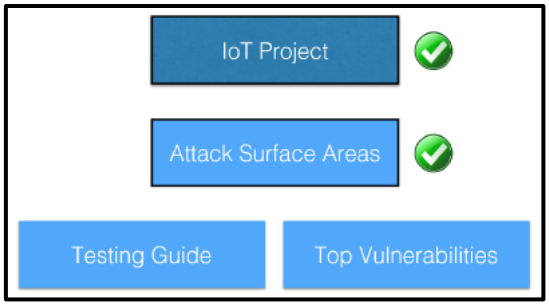
等を公開している。

2014 年にまとめられた Top 10 IoT Vulnerabilities from 2014 では、IoT において脆弱性を生じやすい 10 のポイントを整理し、攻撃者、攻撃手法、セキュリティ上の弱点、技術的な影響、ビジネスへの影響が具体的にどういうものか詳しく定義し、脆弱性の例、攻撃例、問題を回避するための手引きが述べられており、参考となる。また、IoT Security Guidance では、上記の 10 種類

の脆弱性に対して、製造業者、開発者、消費者のそれぞれの視点で、何をしなければならないか、具体的な注意事項を示している。さらに、IoT Testing Guides は、上記 10 種類の脆弱性を生じさせないため、試験実施者が考慮すべき注意事項を示している。

現在も更新を続けている IoT Vulnerabilities では、2017 年 8 月の時点で IoT における 17 種類の脆弱性とその概要、攻撃対象（脆弱性発生箇所）の関係を整理している。

2017 年 8 月時点での OWASP Internet of Things Project のプロジェクトーサブプロジェクト編成は、以下の様になっている（OWASP のウェブサイト[37]から引用）。



各サブプロジェクトとその成果を**表 4-4** に示す。

OWASP Internet of Things Project の主な成果である OWASP Top 10 IoT Vulnerabilities from 2014、IoT Security Guidance、IoT Testing Guides、IoT Vulnerabilities の概要は、巻末の**付録 A.**にて紹介する。

表 4-4　OWASP Internet of Things Project の編成と成果

OWASP Internet of Things Project	
IoT Attack Surface Areas Project *(DRAFT)*	攻撃対象領域：攻撃対象と脆弱性の関係を整理
IoT Vulnerabilities Project	17 種類の脆弱性とその概要、攻撃対象（脆弱性発生箇所）の関係を整理
Top 10 IoT Vulnerabilities from 2014	2014 年に選定した IoT の 10 大脆弱性について、以下の点を整理 攻撃者、攻撃手法、セキュリティ上の弱点、技術的影響、ビジネスへの影響、 脆弱性の確認方法、攻撃シナリオ例、脆弱性の解消方法
Medical Attack Surfaces (sub) Project	医療機器を出荷する前に評価すべき、基本的な攻撃対象領域の考慮点
Firmware Analysis Project	攻撃対象「機器のファームウェア」に対するセキュリティ試験ガイドとして、 ファームウェア解析に関する情報を提供
IoT Firmware Analysis Primer	ファームウェア解析入門
IoT Security Logging (sub) Project *(working draft)*	IoT 関連システムにおいてログを記録すべき最低限のイベントの一覧
ICS/SCADA Software Weaknesses Project	ICS/SCADA における 10 大ソフトウェア脆弱性
IoT Security Policy Project	（開発中）
Community Information	他団体、ポッドキャスト、カンファレンスの情報を掲載
IoT Testing Guides *(DRAFT)*	IoT の 10 大脆弱性(2014)に対する試験実施時のセキュリティ上の考慮事項
IoT Security Guidance *(DRAFT)*	IoT の 10 大脆弱性(2014)に対する製造者・開発者・消費者のセキュリティ上の考慮事項
Principles of IoT Security	IoT セキュリティに関する 16 項目の原則
IoT Framework Assessment	各構成要素に対するセキュアな IoT フレームワークとしての考慮事項

出典：OWASP Internet of Things Project[37] を基に作成

4.2.OTA IoT Trust Framework

Online Trust Alliance（OTA）[48]は、オンラインの信頼性を強化して、ユーザに公的な権限を与えることをミッションに、インターネットの技術革新や活力促進を支援する、アメリカ合衆国内国歳入法第 501 条 C 項 3 号に基づく非営利団体である。2005 年、業界内の非公式な作業グループとして結成され、ユーザのセキュリティやプライバシー、アイデンティティの保護を強化するためのベストプラクティスやツールを開発・改良することで、企業、政策立案者、ステークホルダーへの啓発支援を目的としている。OTA はアメリカ合衆国ワシントン州シアトル近郊のベルビューに本拠地を置き、Symantec・Verisign・Diginet・Microsoft・Twitter・GAP 等、100 以上の組織が加盟している。

IoT Trustworthy Working Group（ITWG）は、2015 年 1 月に OTA の中に設立された作業グループで、ベンダーに中立な複数のステークホルダーで構成されている。ITWG は、IoT におけるプライバシー、セキュリティ、持続可能性の問題に対するベストプラクティスにフォーカスしたフレームワークとして、 OTA IoT Trust Framework[49]を開発・公開した。

OTA の IoT Trust Framework は、先ずは、（1）ホームオートメーションとコネクテッドホーム製品、（2）ヘルスケア＆フィットネス分野向けウェアラブル技術に焦点をおいた検討を実施し、2016 年 3 月 3 日、30 個の必須・推奨項目を規定した正式版の最初の版（Released 3/2/2016）を公開した。また、2016 年 4 月 8 日、30 項目の補足説明を行う IoT Trust Framework - Resource Guide[50]のドラフト（Updated 4/8/2016）が公開した。

その後、IoT Trust Framework は繰り返し更新作業を実施し、2017 年 11 月時点での最新版（v2.5、updated 10/14/17）では、全 40 個の必須・推奨項目の規定となった。また、IoT Trust Framework - Resource Guide の最新版（Updated January 5, 2017）は、2017 年 1 月公開の IoT Trust Framework（v2.0, Released Jan 5, 2017）[51]に対応した版が公開されている。

OTA IoT Trust Framework の更新履歴を、**表 4-5** に示す。また、2017 年 11 月時点での OTA IoT Trust Framework の最新版の概要を、巻末の**付録 B.**にて紹介する。

表 4-5　OTA IoT Trust Framework の主な更新履歴

日付	更新履歴
2016/03/03	OTA IoT Trust Framework - Released 3/2/2016 の公開 ・全 30 項目の必須・推奨項目を規定。正式版として公開。
2016/04/08	IoT Trust Framework - Resource Guide, Updated 4/8/2016 の公開 ・30 項目の補足説明を行うガイド。ドラフト版として公開。
2016/07/12	OTA IoT Trust Framework - Updated July 12, 2016 の更新 ・国際的規制要件への対応を必須項目として追加し、 全 31 個の必須・推奨項目の規定となった。
2016/09/01	IoT Trust Framework - Resource Guide, Updated 9/1/2016 の更新 ・IoT Trust Framework の Updated 7/12/2016 に対応した修正を行い、 31 項目の補足説明を行うガイドとなった（ドラフト版の扱いのまま）。
2016/09/21	OTA IoT Trust Framework - Updated September 21, 2016 の更新 ・いくつかの規定を見直すと共に、コネクテッドホームおよびウェアラブル技術 に対して差異の無くなった「必須」「推奨」規定を統一。
2016/09/28	IoT Trust Framework - Resource Guide, Updated 9/28/2016 の更新 ・IoT Trust Framework の Updated 9/21/2016 に対応した修正 （ドラフト版の扱いのまま）。
2017/01/05	IoT Trust Framework v2.0 - Released Jan 5, 2017 の公開 ・必須・推奨項目を四種類の大分類「セキュリティ」「ユーザ・アクセスと資格情報」「プライバシー、透明性と開示」「通知と関連ベストプラクティス」に分類すると共に、見直し・追加を行い、全 37 項目の規定となった。 IoT Trust Framework - Resource Guide, Updated January 5, 2017 の公開 ・同時公開の v2.0 に対応した修正。正式版として公開。
2017/05/04	IoT Security & Privacy Trust Framework v2.0 の更新 ・v2.0 以前との相違点を示すマーカーの削除、v2.0 の最初の版の公開時に 削除されていた「用語、定義、明確化」の復活。
2017/06/22	IoT Security & Privacy Trust Framework v2.5 の公開 ・項目の見直し・追加・分割を行い、全 40 項目の必須・推奨項目の規定となった。2017 年 11 月時点での最新版。

4.3.GSMA IoT Security Guidelines & Assessment

GSMA（GSM Association）は、1995 年に設立された移動体通信事業者の業界団体であり、約 800 社の通信事業者と 250 社以上の関連事業者（携帯電話端末および機器製造業者、ソフトウェア会社、インターネット会社等）から構成されている。

GSMA は、2016 年 2 月、新しい IoT 製品やサービスを開発しているサービス提供者向けに、複数の分冊から成る GSMA IoT Security Guidelines Version 1.0 を公開した後、2016 年 11 月に Version 1.1 を、2017 年 10 月に Version 2.0 を公開している[52][53]。

主な想定読者は、

- IoT サービス提供者：
  新たに革新的な「繋がる製品やサービス」を開発しようとしている企業または組織
- IoT 機器製造業者：
  IoT サービス提供者向けに IoT サービス対応の IoT 機器を提供する製造業者
- IoT 開発者：
  IoT サービス提供者向けに IoT サービスの開発を代行する開発者
- ネットワーク通信事業者：
  IoT サービス提供者向けにネットワーク通信サービスを提供する事業者

としている。

GSMA IoT Security Guidelines は、IoT 産業界が IoT のセキュリティ問題に関する共通理解を確立することを手助けすることを意図している。IoT サービスのライフサイクルを通してセキュリティのベストプラクティスが実装されることを確実にするために、セキュアな IoT サービスを開発するための方法論を示している。これらの文書は、IoT サービスにおける一般的なセキュリティ脅威と脆弱性を軽減する方法に関して、推奨要件を提供している。

文書のスコープは、IoT サービスおよびネットワーク要素の設計と実装に関する推奨に限定している。これらの文書は、新たな IoT 仕様や標準の作成を牽引することを意図しておらず、現時点で利用可能なソリューション、標準、ベストプラクティスを参照している。

現在の GSMA IoT Security Guidelines は、以下に示す五部構成となっている。

- CLP.11: IoT Security Guidelines Overview Document[54]
  IoT 技術またはサービスの実装者に対して、セキュアな製品を開発するための設計ガイドを提供する文書セットの導入部として、実装者に関連する技術またはサービスの側面を理解

するための全体的なモデルを示す。これらの側面または構成要素を特定することで、実装者が各々の構成要素に関連するリスクを評価し、補償するための方法を決定出来ることを期待している。
想定読者は、IoT サービスに関わる全ての関係者、即ち、IoT サービス提供者、IoT 機器製造業者、IoT 開発者、ネットワーク通信サービス事業者である。
CLP.11 のみ、日本語訳が公開されている。

- CLP.12: IoT Security Guidelines for IoT Service Ecosystem[55]
  サービスエコシステムの観点から IoT 製品またはサービスの全ての構成要素を評価するためのガイド。サービスエコシステムには、IoT インフラの中心を占める全ての構成要素（例えば、サービス、サーバ、データベース・クラスタ、ネットワーク要素、製品やサービスの内部構成要素に至る他の技術）を含む。
  想定読者は、IoT サービスに関わる全ての関係者、即ち、IoT サービス提供者、IoT 機器製造業者、IoT 開発者、ネットワーク通信サービス事業者である。

- CLP.13: IoT Security Guidelines for IoT Endpoint Ecosystem[56]
  IoT エンドポイント機器の観点から IoT サービスの構成要素を評価するためのガイド。エンドポイントとは、インターネットに接続した製品またはサービスの一部としての機能またはタスクを実行する物理的なコンピューティング機器（例えば、ウェアラブルなフィットネス機器、産業制御システム、自動車のテレマティクス・ユニット、個人用ドローン・ユニット）である。
  想定読者は、IoT サービスに関わる全ての関係者、即ち、IoT サービス提供者、IoT 機器製造業者、IoT 開発者、ネットワーク通信サービス事業者である。

- CLP.14: IoT Security Guidelines for Network Operators[57]
  IoT サービス提供者向けにネットワーク通信サービスを提供するネットワーク通信事業者のために、システムのセキュリティやデータのプライバシーを確実にするためのセキュリティガイド。
  想定読者は、ネットワーク通信事業者および IoT サービス提供者である。

- CLP.17: GSMA IoT Security Assessment[58]
  IoT 製品、サービスおよびコンポーネントが GSMA IoT Security Guidelines を順守しているか否かを自己評価するためのセキュリティ評価チェックリスト。
  Version 1.1 以降で追加された。

5. IoT システムにおける脅威分析と対策検討の実施例

本章では、いくつかの例題をもとに、IoT システムにおける脅威分析と対策検討の具体的な実施例を示す。3 章で示したセキュリティ設計の手順に従い、(1)デジタルテレビ、(2)ヘルスケア機器とクラウドサービス、(3)スマートハウス、(4)コネクテッドカーを題材とした IoT システムに対して以下を行った。

- 対象 IoT システム／サービスの全体構成図の作成
- 保護すべき情報・機能・資産の明確化
- 想定される脅威の明確化
- 対策候補（ベストプラクティス）の明確化

これらの題材に対する脅威分析・対策検討の実施結果を、対象分野の概要・動向・特徴と共に示している。

なお、対策の一部は、4 章で示した OWASP Top 10 IoT Vulnerabilities from 2014 および OTA IoT Trust Framework の推奨要件が参考になると考えられるため、対応する要件番号を記載した。OWASP1～OWASP10 は、付録 A.の**表 A-1** の 2014-I1～I10 に対応する。また、OTA1～OTA40 は、付録 B.の**表 B-1**～**表 B-6** の 1.～40.に対応する。[2]

これらの例にならって、それぞれの分野の IoT システムにおいて脅威分析と対策検討が実施されて、セキュアな IoT 製品開発に繋がることを期待する。

[2] 但し、OTA1, OTA7, OTA8, OTA18, OTA19, OTA21, OTA22, OTA24, OTA25, OTA28～OTA31, OTA38, OTA39 は、本章における対応要件には該当しないため、表中には記載が存在しない。

5.1.デジタルテレビ

本節では、情報家電（ネットワーク接続機能を有する情報通信機器および家庭電化製品）の一つであるデジタルテレビにおける脅威と対策の検討例を示す。ここではデジタルテレビを題材としているが、ネットワーク接続機能を備えた情報家電一般（DVD/BD/HDD レコーダー、冷蔵庫、エアコン等）に対しても、同様の脅威と対策が考えられる。

【対象分野の概要】

デジタルテレビ（DTV）とは、デジタル変調技術とデジタル圧縮技術を使用したテレビ放送（2000 年 12 月から開始された BS デジタル放送および 2013 年 12 月から開始された地上デジタル放送）に対応した受信機である。デジタルテレビには、それ以前のテレビと比較して、外部メディアの利用、内蔵ハードディスクディスクドライブ、LAN 接続、インターネット接続等、様々な情報利用機能が付加されており、IoT 機器の先駆けとも言える存在である。

【動向】

情報家電の設定不備や脆弱性が攻撃者によって悪用され、第三者への攻撃に用いられた事例が報告されている。2004 年、初期設定状態（ユーザ名・パスワードなしでアクセス可能）のままの DVD/HD レコーダーが外部からプロキシサーバーとしてアクセス可能となっており、スパムコメントの送信（踏み台）に悪用された事件が発生した。[3]また、近年、脆弱性を有するホームルータが乗っ取られ、DDoS 攻撃の踏み台に悪用される事件が相次いでいる。[4] 2016 年、マルウェア Mirai に感染した IoT 機器で構成されたボットネットによる大規模 DDoS 攻撃が世界中に影響を与えたが、これらの機器の中には多くの情報家電が含まれていたことが報告されている[16]。

情報家電の脆弱性が利用者自身に損害を与える事例も報告されている。2015 年 DEF CON において、インターネット接続機能を有する冷蔵庫に SSL サーバ証明書の検証処理に不備があり、冷蔵庫の扉に搭載された液晶パネルと Google Calendar の通信時、中間者攻撃によって Google サービスへのログイン情報が窃取される危険性が指摘された。[5]

---

[3] JVN iPedia: JVNDB-2004-000589 東芝製 HDD&DVD ビデオレコーダーへ認証なしでアクセス可能
http://jvndb.jvn.jp/ja/contents/2004/JVNDB-2004-000589.html

[4] 警察庁: 日本国内のオープン・リゾルバを踏み台とした DDoS 攻撃発生に起因すると考えられるパケットの増加について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140723.pdf

[5] PEN TEST PARTNERS: Hacking DefCon 23's IoT Village Samsung fridge
https://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

【分野の特徴】

IT システム（PC 等）と比較して、デジタルテレビの様な情報家電は製品寿命が長く、10 年以上使い続けられる可能性が高いため、継続的なサポート（同等レベルの対策提供の継続、周辺状況に応じた対策の強化）が求められる。

【全体構成図の解説】

2010 年度、IPA では家電業界各社と経済産業省の参画の下、情報家電におけるセキュリティ対策についての勉強会を実施した。勉強会の活動において、商品化が先行しているデジタルテレビを対象に、デジタルテレビにおけるネットワーク接続を含む情報利用機能、それらの機能の利用で想定されるセキュリティ上の脅威、脅威群に対するセキュリティ対策を明確化した[2]。

ここでは、当時整理したデジタルテレビに対する脅威と対策をベースとして見直しを行い、IoT における「デバイス」である「デジタルテレビ」本体と、「サービス提供サーバ」であるインターネット上の各サイト（メーカーサイト、TV 局サイト、一般サイト）における脅威と対策の全体像を、**図 5-1** に示す。

このシステムでは、以下に示す脅威が想定される。

- デジタルテレビに接続可能な媒体からのウイルス感染
- ユーザ操作に起因する脅威（設定不良、操作ミス、テレビ内部の情報の漏えい）
- 宅内における脅威（正規利用者以外による不正利用、不正設定）
- ネット経由・ネット接続時の脅威（ウイルス感染、盗聴、不正アクセス、DoS 等）
- インターネット上の各サイト（ポータルサイト）における脅威

【セキュリティ対策の留意事項】

製品寿命が長いことから、攻撃者の技術の進歩に追従して、防御力を強化していく必要がある。すなわち、製品出荷後にセキュリティ機能を強化できる様に、予めソフトウェア更新機能等を実装しておくべきである。

【脅威と対策表の構成と特徴】

先に示した脅威に対して、例えば以下に示す対策が有効であると考えられる。

- 脆弱性対策
- ファイアウォール機能（接続先を IP アドレス・ポート番号にて制限等）
- アンチウイルス
- 通信路暗号化

これらの脅威と対策を**図 5-1** の上にマッピングしている。また、脅威と対策、および IoT 関連のセキュリティガイド（OWASP Internet of Things Project、OTA IoT Trust Framework）の関係を整理した一覧を、**表 5-1**～**表 5-2** に示す。

デジタルテレビに対する脅威と対策の詳細については、2011 年 2 月に IPA から公開した「2010 年度版 情報家電におけるセキュリティ対策 検討報告書」[2]を参照のこと。

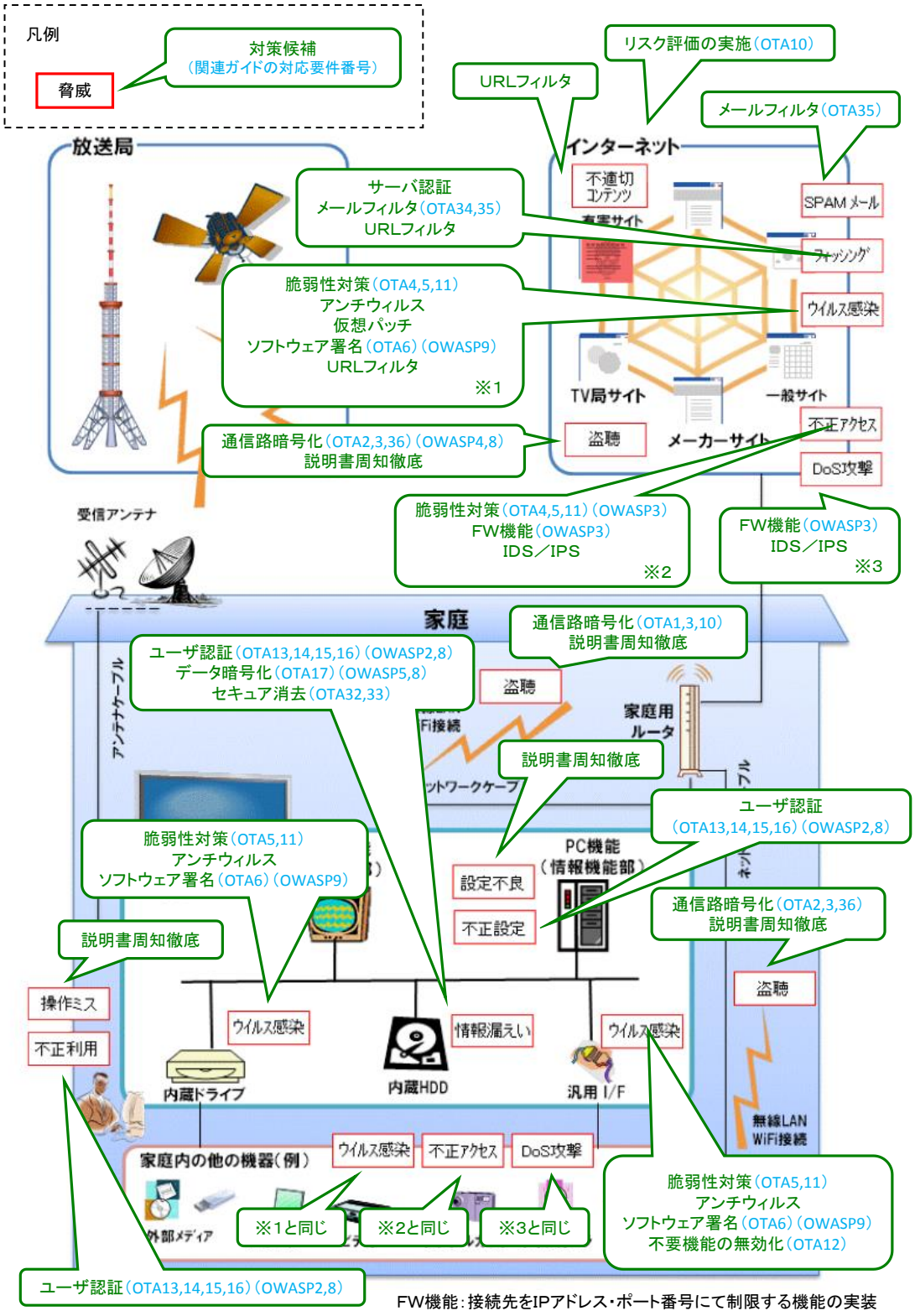


図 5-1　デジタルテレビの脅威と対策の検討例

表 5-1　デジタルテレビの脅威と対策表（1/2）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
デジタルテレビ	基本機能	操作ミス	説明書周知徹底		
		不正利用	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
	PC 機能 （情報機能部）	設定不良	説明書周知徹底		
		不正設定	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
	内蔵ドライブ → 基本機能 または PC 機能	ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
	汎用 I/F → 基本機能 または PC 機能	ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			不要機能の無効化	OTA12	
	内蔵 HDD	情報漏えい	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			データ暗号化	OTA17	OWASP5, OWASP8
			セキュア消去	OTA32, OTA33	
家庭内 LAN	Wi-Fi 通信 （無線 LAN）	盗聴	通信路暗号化	OTA2, OTA3, OTA36	
			説明書周知徹底		

表 5-2　デジタルテレビの脅威と対策表（2/2）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
インターネット	メーカーサイト TV 局サイト 一般サイト および 各サイトと デジタルテレビ との 間の通信	全脅威共通	リスク評価の実施	OTA10	
		ウイルス感染	脆弱性対策	OTA4, OTA5, OTA11	
			アンチウイルス		
			仮想パッチ		
			ソフトウェア署名	OTA6	OWASP9
			URL フィルタ		
		盗聴	通信路暗号化	OTA2, OTA3, OTA36	OWASP4, OWASP8
			説明書周知徹底		
		不正アクセス	脆弱性対策	OTA4, OTA5, OTA11	OWASP3
			FW 機能		OWASP3
			IDS/IPS		
		DoS 攻撃	FW 機能		OWASP3
			IDS/IPS		
		SPAM メール	メールフィルタ	OTA35	
		フィッシング	サーバ認証		
			メールフィルタ	OTA34, OTA35	
			URL フィルタ		
		不適切コンテンツ	URL フィルタ		

5.2.ヘルスケア機器とクラウドサービス

本節では、ネットワーク対応ヘルスケア機器とクラウドサービスの連携によって、個人のヘルスケアデータを一元管理する IoT システムにおける脅威と対策の検討例を示す。

【対象分野の概要】

「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」（旧称「薬事法」）では、「人若しくは動物の疾病の診断、治療若しくは予防に使用されること、又は人若しくは動物の身体の構造若しくは機能に影響を及ぼすことが目的とされている機械器具等（再生医療等製品を除く。）であつて、政令で定めるもの」を「医療機器」と定義している。医療機器は、さらに、以下の三種類に分類されている。

- 「一般医療機器」（クラスⅠ）
  副作用又は機能の障害が生じた場合においても、人の生命及び健康に影響を与えるおそれがほとんどない医療機器。
- 「管理医療機器」（クラスⅡ）
  副作用又は機能の障害が生じた場合において人の生命及び健康に影響を与えるおそれがあることからその適切な管理が必要な医療機器。
- 「高度管理医療機器」（クラスⅢ、クラスⅣ）
  副作用又は機能の障害が生じた場合において人の生命及び健康に重大な影響を与えるおそれがあることからその適切な管理が必要な医療機器。

IPA が 2013 年度に実施した医療機器における情報セキュリティに関する調査[8]では、「使用することにより健康の増進や体型の維持向上が期待できるとされている器具」を「ヘルスケア機器」と定義した。ヘルスケア機器は、以下のいずれかであり、今後ネットワークへの接続が拡大していくと考えられる。

- 「医療機器」の内、不具合が生じた場合でも人体への影響が軽微である「管理医療機器（クラスⅡ）」に該当し、かつ一般人により主として利用される、電子体温計や携帯型電子式血圧計、携帯型心電計、電気治療器等の機器
- 「医療機器」でない、エアロバイク、活動量計、睡眠計、体組成計等の機器

また、本節の検討においては対象としていないが、「高度管理医療機器」の中にもネットワークへの接続機能を有する医療機器が増加すると共に、脅威・インシデント事例が報告されている。

【動向】

医療機器に対する脅威・インシデント事例としては、2011 年 Black Hat で Jerome Radcliffe 氏が報告したインスリンポンプへのハッキング[6]、2012 年 Breakpoint Security Conference 2012 で Barnaby Jack 氏が発表した心臓ペースメーカーへのハッキング[7]、2015 年 Billy Rios 氏が発表した薬剤ライブラリや輸液ポンプの設定等を管理するサーバソフトウェアの脆弱性[8]、2016 年に公開されたインスリンポンプの脆弱性(治療情報や機器データの漏洩や機器の不正操作の恐れ)[9]、2017 年に公開された心臓ペースメーカーの脆弱性(不正な遠隔操作によりバッテリの枯渇や不適切な心拍管理の恐れ)[10] [11]等が報告されている。

【分野の特徴】

研究者による医療機器へのハッキングの研究は、医療機器に対して患者の人命にかかわる攻撃が可能であることを示した。また、医療機器によって収集された患者のヘルスケアデータは、取扱いに注意を要する機微な情報である。各機器がネットワークにつながることによって、長期間におけるデータの保管や専門的な分析など、高付加価値のあるサービスの提供が期待される反面、データの取り扱いや管理が重要な分野である。

【全体構成図の解説】

近年、歩数・活動量計、体重体組成計、血圧計等のヘルスケア機器のネットワーク対応モデルが利用可能となり、インターネットに接続された PC やスマートフォン等を中継機器としてクラウド上のサーバ(ヘルスケア対応のクラウドサービス)と通信することによって、個人のヘルスケアデータを一元管理するサービスが提供されている[67][68]。その全体像のイメージを**図 5-2** に示す。各々のヘルスケア機器からクラウドサービスへの接続は、様々な選択肢が存在する。外出先においては、スマートフォンやモバイルルータを中継機器として、モバイル通信(LTE 等)を用いた携帯電話通信事業者網とインターネット経由でクラウドサービスに接続する。自宅においては、スマートフォンや

---

[6] J. Radcliffe: Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System, Black Hat USA 2011
https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf
[7] B. Jack: Hacking Humans. Breakpoint Security Conference 2012
[8] WIRED: DRUG PUMP'S SECURITY FLAW LETS HACKERS RAISE ROSE LIMITS,
https://www.wired.com/2015/04/drug-pumps-security-flaw-lets-hackers-raise-dose-limits/
[9] JVNVU#95089754: Animas OneTouch Ping に複数の脆弱性 http://jvn.jp/vu/JVNVU95089754/
[10] FDA: Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication
https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm
[11] Abbott: Abbott Issues New Updates for Implanted Cardiac Devices
http://abbott.mediaroom.com/2017-08-29-Abbott-issues-new-updates-for-implanted-cardiac-devices

PC、ホームルータを多段の中継機器として、インターネット経由でクラウドサービスに接続する。ヘルスケア機器と中継機器の間の通信は、機器の仕様に応じて、Bluetooth・NFC といった無線通信や USB 接続の有線通信およびそれらの組合せが選択可能である。また、中継機器同士の通信は、機器の仕様に応じて、無線通信（Wi-Fi）および有線通信（LAN）が選択可能である。

図において、ネットワーク対応のヘルスケア機器によって計測された個人のヘルスケアデータは、スマートフォン・PC・ホームルータ等の中継機器を通して、インターネット上のクラウドサービスに送信・登録される。また、クラウドサービスに保管されたヘルスケアデータは、スマートフォンや PC から参照可能である。ネットワーク対応ヘルスケア機器の種類が増えることによって、収集・一元管理するヘルスケアデータの項目が充実し、よりきめ細かい健康管理が可能となる。

このシステムでは、以下に示す脅威が想定される。

- ネットワーク対応ヘルスケア機器に保存されたヘルスケアデータの漏えい
- 通信路上のヘルスケアデータの盗聴・改ざん
- クラウドサービスやホームルータへの不正アクセス・DoS 攻撃
- PC・スマートフォン上に一時保存されたヘルスケアデータの漏えい
- クラウドサービス上に収集・一元管理されたヘルスケアデータの一括漏えい

【セキュリティ対策の留意事項】

このシステムにおいては、個人のヘルスケアデータという機微な情報を取り扱うため、特に情報の漏えい・盗聴・改ざんに対する対策の実装が望まれる。また、クラウドサービスのログイン情報（アカウント、パスワード）を窃取し、正規利用者に成りすましてクラウドサービス上のヘルスケアデータを取得する不正アクセスの脅威が考えられるため、クラウドサービスのログイン情報の厳重な管理が望まれる。また、クラウドサービスへの不正アクセスや DoS 攻撃、内部不正等に備える必要がある。

【脅威と対策表の構成と特徴】

先に示した脅威に対して、例えば以下に示す対策が有効であると考えられる。

- ヘルスケア機器、PC・スマートフォン、クラウドサービス上のデータ暗号化
- ヘルスケア機器、スマートフォンの分解対策（耐タンパー）
- ヘルスケア機器、PC・スマートフォン上のデータのセキュアな消去
- スマートフォンの紛失・盗難対策（遠隔管理、遠隔データ消去）

- スマートフォンの不正利用対策（認証、端末ロック）
- PC・スマートフォンのウイルス感染対策
- 通信路の暗号化
- クラウドサービス、ホームルータの不正アクセス対策、DoS 対策

これらの脅威と対策を**図 5-2** の上にマッピングしている。また、脅威と対策、および IoT 関連のセキュリティガイド（OWASP Internet of Things Project、OTA IoT Trust Framework）の関係を整理した一覧を**表 5-3**～**表 5-6** に示す。

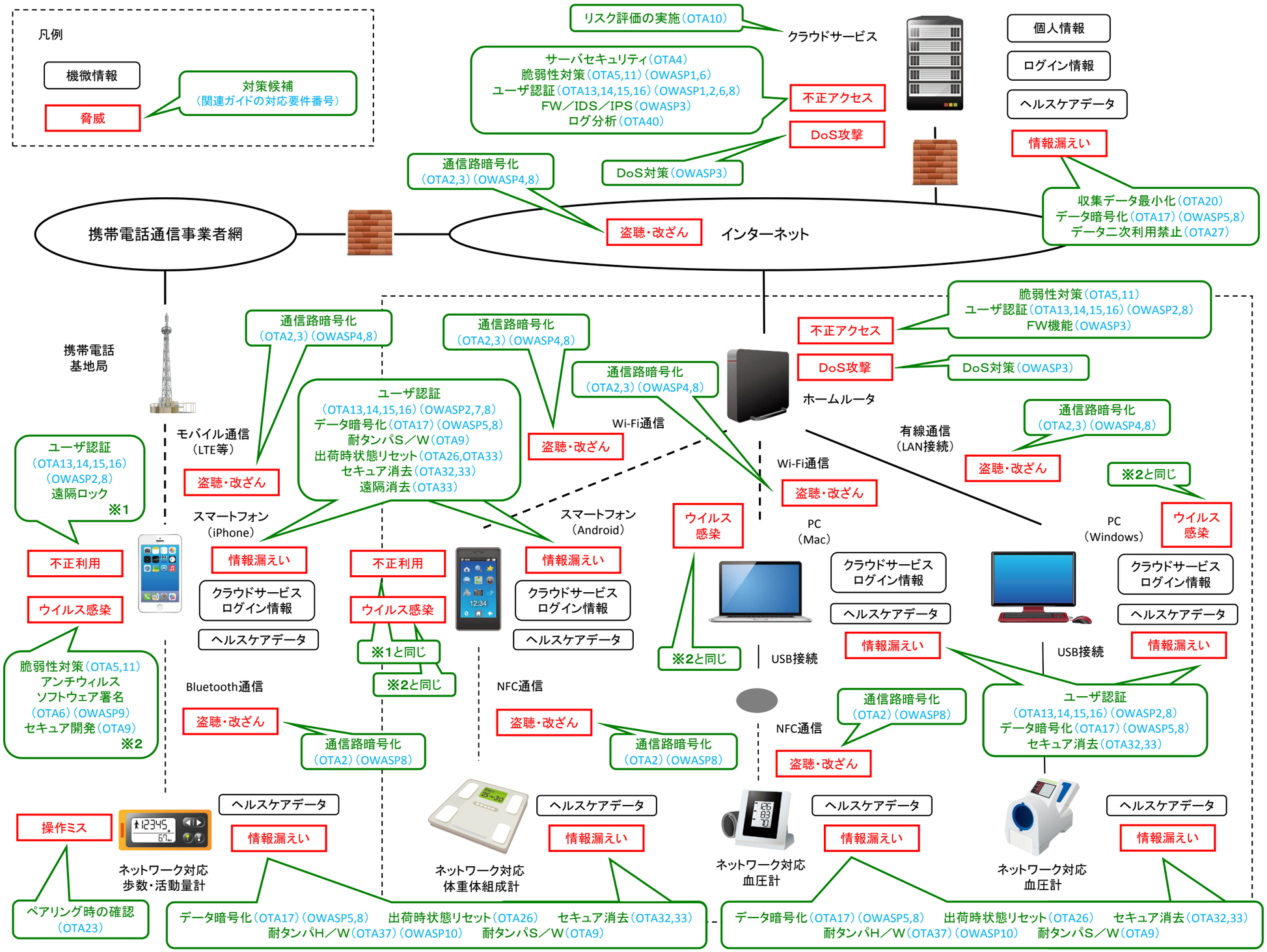


図 5-2　ヘルスケア機器とクラウドサービスの脅威と対策の検討例

このページは空白です。

表 5-3　ヘルスケア機器とクラウドサービスの脅威と対策表（1/4）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
ヘルスケア機器	ネットワーク対応歩数・活動量計	操作ミス	ペアリング時の確認	OTA23	
		情報漏えい	データ暗号化	OTA17	OWASP5, OWASP8
			出荷時状態リセット	OTA26	
			セキュア消去	OTA32, OTA33	
			耐タンパーH/W	OTA37	OWASP10
			耐タンパーS/W	OTA9	
	ネットワーク対応体重体組成計	情報漏えい	データ暗号化	OTA17	OWASP5, OWASP8
			出荷時状態リセット	OTA26	
			セキュア消去	OTA32, OTA33	
			耐タンパーH/W	OTA37	OWASP10
			耐タンパーS/W	OTA9	
	ネットワーク対応血圧計	情報漏えい	データ暗号化	OTA17	OWASP5, OWASP8
			出荷時状態リセット	OTA26	
			セキュア消去	OTA32, OTA33	
			耐タンパーH/W	OTA37	OWASP10
			耐タンパーS/W	OTA9	

表 5-4　ヘルスケア機器とクラウドサービスの脅威と対策表（2/4）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
機器・スマホ/PC 間の無線通信	Bluetooth 通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
	NFC 通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
屋内外での中継機器	スマートフォン	不正利用	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			遠隔ロック		
		ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA9	
		情報漏えい	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP7, OWASP8
			データ暗号化	OTA17	OWASP5, OWASP8
			耐タンパーS/W	OTA9	
			出荷時状態リセット	OTA26, OTA33	
			セキュア消去	OTA32, OTA33	
			遠隔消去	OTA33	
スマホ・基地局間の無線通信	モバイル通信（LTE 等）	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8

表 5-5　ヘルスケア機器とクラウドサービスの脅威と対策表（3/4）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
屋内での中継機器	PC	ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA9	
		情報漏えい	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			データ暗号化	OTA17	OWASP5, OWASP8
			セキュア消去	OTA30, OTA31	
PC・ルータ間の通信	Wi-Fi 通信	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8
	有線通信	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8
屋内での中継機器	ホームルータ	不正アクセス	脆弱性対策	OTA5, OTA11	
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			FW 機能		OWASP3
		DoS 攻撃	DoS 対策		OWASP3

表 5-6　ヘルスケア機器とクラウドサービスの脅威と対策表（4/4）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
ヘルスケア対応クラウドサービス	クラウドサービス	全脅威共通	リスク評価の実施	OTA10	
		不正アクセス	サーバセキュリティ	OTA4	
			脆弱性対策	OTA5, OTA11	OWASP1, OWASP6
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP1, OWASP2, OWASP6, OWASP8
			FW／IDS／IPS		OWASP3
			ログ分析	OTA40	
		DoS 攻撃	DoS 対策		OWASP3
		情報漏えい	収集データ最小化	OTA20	
			データ暗号化	OTA17	OWASP5, OWASP8
			データ二次利用禁止	OTA27	
クラウドサービスとの通信	インターネット	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8

5.3.スマートハウス

本節では、家庭内機器を一元管理することによって省エネルギーを実現する IoT システムである、スマートハウスにおける脅威と対策の検討例を示す。

【対象分野の概要】

スマートハウスとは、家庭内エネルギー利用を最適に制御する住宅である。家庭の電力需給（発電、蓄電、消費）を制御する HEMS（Home Energy Management System）を中心に、対応する機器を一元管理することによって、省エネルギーを実現する[69][70]。

【動向】

2015 年 5 月、朝日新聞より、スマートハウスにおいて情報を一元管理する HEMS がインターネットに接続されている場合、外部の第三者から不正アクセスされる可能性について報告があった。[12]当該 HEMS はホームルータを介してインターネットに接続することを前提としていたが、30 世帯以上でインターネットに直結していたため、HEMS のモニター画面が見える状態になっており、第三者に情報を見られたり、家庭内機器を遠隔操作されたりする恐れがあった。また、2016 年 3 月、ガス給湯器やガス床暖房等を携帯電話等により遠隔操作するサービスにおいて、機器の利用者（契約者）が替わった際のパスワード未発行または前契約者と同一パスワード発行のため、前契約者による機器の遠隔操作や顧客情報の閲覧が可能となっていた。[13]

【分野の特徴】

スマートハウスにおける各機器の情報を不正に取得された場合、個人のプライベートデータの漏えいという脅威に加えて、取得したデータ（消費電力や施錠状況）を悪用して、不在と分かった場合に遠隔操作で施錠解除し、家屋に浸入される恐れがある。さらに、家庭内機器を不正に遠隔操作されると、電気やガスの無駄使いといった金銭的被害や、最悪の場合、火災や宅内冠水といった物理的な被害を生じる危険性がある。従って、データの保護に加えて、許可なき遠隔操作につながる不正アクセスを防止することが重要な分野である。

---

12 朝日新聞デジタル：鍵開け・のぞき見…スマートハウスご注意　他人操作恐れ
http://digital.asahi.com/articles/ASH525J2JH52PTIL00H.html

13 東京ガス：住宅機器の遠隔操作サービス「リモートプラス」ならびにガスの消し忘れ確認サービス「確かめ～る」における不適切なパスワードの発行について
http://www.tokyo-gas.co.jp/important/20160325-06.pdf

【全体構成図の解説】

図 5-3 は、スマートハウスの一例をモデル化したものである。HEMS コントローラを中心に接続された HEMS 対応機器やそれ以外のネットワーク対応機器がホームルータを介してインターネットに接続されており、外出先からスマートフォンを用いてクラウドサービス経由で家庭内の機器にアクセスすることによって、家庭内の機器の様子を監視したり、遠隔操作したりすることが可能となる。

このシステムでは、以下に示す脅威が想定される。

- スマートハウス内に設置された機器に保存されたデータの漏えい
- 通信路上のデータの盗聴・改ざん
- クラウドサービスやホームルータへの不正アクセス
  （不正ログイン、その後の不正コマンド発行による許可なき遠隔操作）
- クラウドサービスやホームルータへの DoS 攻撃
- クラウドサービス上に保存されたデータの漏えい

【セキュリティ対策の留意事項】

スマートハウスにおいては、情報漏えい対策に加えて、適切に遠隔操作が行われるための対策の実装が重要である。即ち、第三者による家庭内機器の許可なき遠隔操作を防止するための対策（不正アクセス対策）や、正規の利用者による正当な遠隔操作の妨害を受けないための対策（DoS 対策）の実装が望まれる。

【脅威と対策表の構成と特徴】

先に示した脅威に対して、例えば以下に示す対策が有効であると考えられる。

- 機器内部に保存されたデータ、クラウドサービス上のデータ暗号化
- 屋外に設置する機器の分解対策（耐タンパー）、データのセキュアな消去
- 通信路の暗号化
- クラウドサービスやホームルータにおける不正アクセス対策（脆弱性対策、認証強化等）
- クラウドサービスやホームルータにおける DoS 対策

これらの脅威と対策を**図 5-3** の上にマッピングしている。また、脅威と対策、および IoT 関連のセキュリティガイド（OWASP Internet of Things Project、OTA IoT Trust Framework）の関係を整理した一覧を**表 5-7**～**表 5-9** に示す。

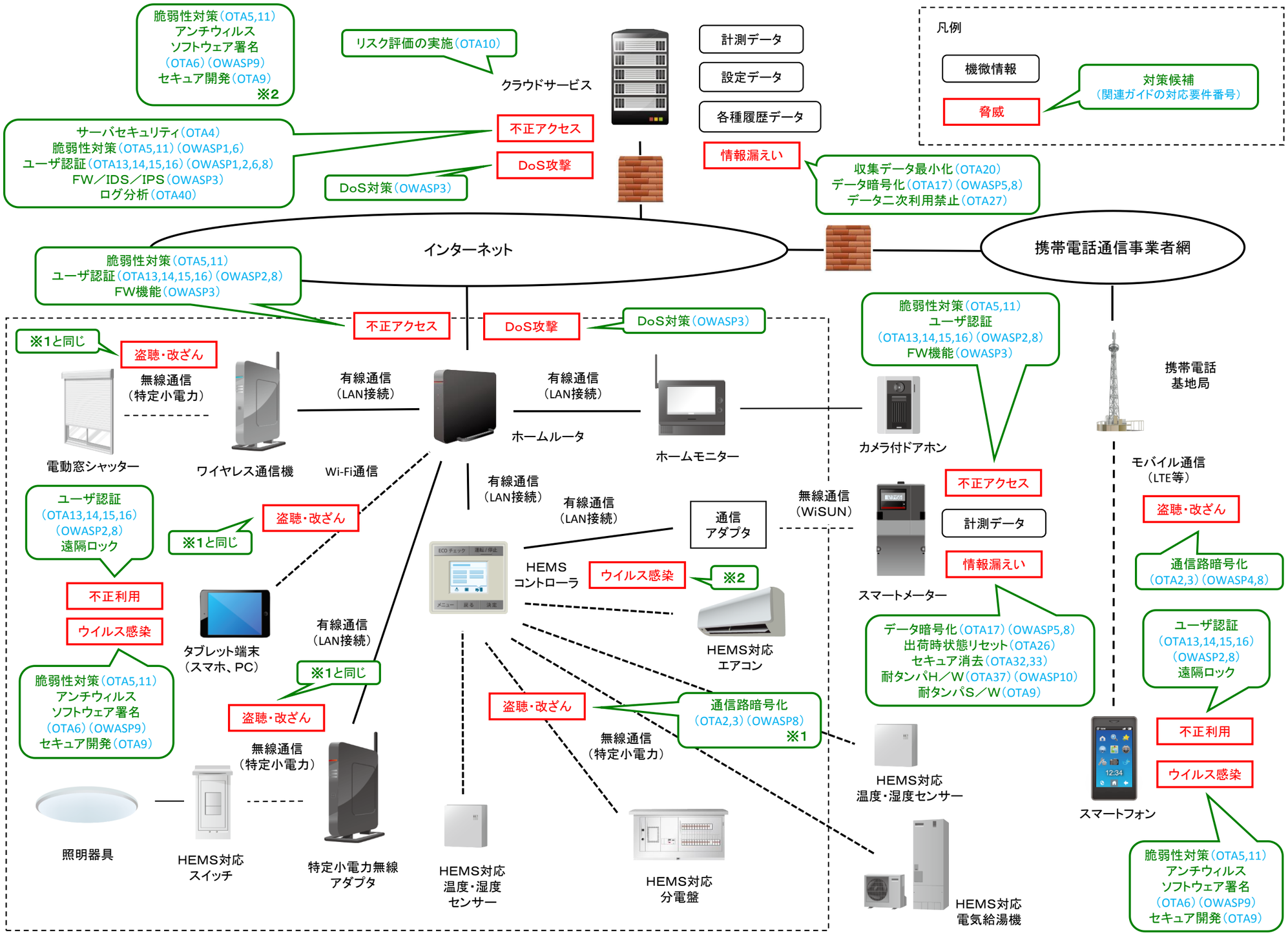


図 5-3　スマートハウスの脅威と対策の検討例

このページは空白です。

表 5-7　スマートハウスの脅威と対策表（1/3）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
スマートハウス（屋内）	HEMS コントローラ	ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA9	
	ホームルータ	不正アクセス	脆弱性対策	OTA5, OTA11	
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			FW 機能		OWASP3
		DoS 攻撃	DoS 対策		OWASP3
	無線通信（特定小電力、WiSUN、Wi-Fi）	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP8
	タブレット端末	不正利用	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			遠隔ロック		
		ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA9	

表 5-8　スマートハウスの脅威と対策表（2/3）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
スマートハウス（屋外）	スマートメーター	不正アクセス	脆弱性対策	OTA5, OTA11	
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			FW 機能		OWASP3
		情報漏えい	データ暗号化	OTA17	OWASP5, OWASP8
			出荷時状態リセット	OTA24	
			セキュア消去	OTA32, OTA33	
			耐タンパーH/W	OTA37	OWASP10
			耐タンパーS/W	OTA9	
ユーザ（外出先）	スマートフォン	不正利用	ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			遠隔ロック		
		ウイルス感染	脆弱性対策	OTA5, OTA11	
			アンチウイルス		
			ソフトウェア署名	OTA6	OWASP9
			セキュア開発	OTA9	
スマートフォン・基地局間の無線通信	モバイル通信（LTE 等）	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8

表 5-9　スマートハウスの脅威と対策表（3/3）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
スマートハウス対応クラウドサービス	クラウドサービス	全脅威共通	リスク評価の実施	OTA10	
		不正アクセス	サーバセキュリティ	OTA4	
			脆弱性対策	OTA5, OTA11	OWASP1, OWASP6
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP1, OWASP2, OWASP6, OWASP8
			FW／IDS／IPS		OWASP3
			ログ分析	OTA40	
		DoS 攻撃	DoS 対策		OWASP3
		情報漏えい	収集データ最小化	OTA20	
			データ暗号化	OTA17	OWASP5, OWASP8
			データ二次利用禁止	OTA27	

5.4.コネクテッドカー

本節では、コネクテッドカーにおける脅威と対策の検討例を示す。

【対象分野の概要】

コネクテッドカーとは、ICT 端末としての機能を有する自動車で、車両の状態や周囲の道路状況等の様々なデータをセンサーにより取得し、ネットワークを介して集積・分析することで、新たな価値を生み出すことが期待されている[71]。

【動向】

従来の自動車の情報セキュリティに関するインシデント事例としては、主にセキュリティ研究者によって、以下に示す様な攻撃成功例が公開されている。

- CAN（Controller Area Network）に対する攻撃の研究[14]
- CAN（Controller Area Network）：OBD-Ⅱや直接接続による攻撃例[15]
- ファームウェアの改ざんによるブレーキ、ステアリング。エアコン等への干渉攻撃[16]
- 脆弱性を攻撃したエンジンスタートや扉の開閉操作[17]
- TPMS（Tire Pressure Monitoring System）への攻撃の研究[18]
- イモビライザー（電子キーを利用した自動車盗難防止機能）の遠隔操作

コネクテッドカーでは、従来の自動車以上にネットワークへの接続性が強化されるため、より脅威が高まることが想定される。

---

[14] Karl Koscher 他: Experimental Security Analysis of a Modern Automobile, 2010 IEEE Symposium on Security and Privacy
http://www.autosec.org/pubs/cars-oakland2010.pdf
[15] Chris Valasek 他: Adventures in Automotive Networks and Control Units, DEF CON 21
http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
[16] Charlie Miller 他: , Remote Exploitation of an Unaltered Passenger Vehicle, Black Hat USA 2015
http://illmatics.com/Remote%20Car%20Hacking.pdf
[17] Kevin Mahaffey 他: How to Hack a Tesla Model S, DEF CON 23
https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/
[18] Ishtiaq Rouf 他: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, 19th USENIX Security Symposium
https://www.usenix.org/legacy/events/sec10/tech/full_papers/Rouf.pdf

【分野の特徴】

運転中の自動車に対する攻撃（遠隔操作）によって、運転者の意図しない運転操作が行われた場合、重大な事故が発生して運転者や同乗者の人命にかかわる恐れがある。

また、コネクテッドカーが収集するデータ（ハンドル、アクセル、ブレーク操作等）は、一つ一つは些細な情報であるが、他の情報（GPS 等）と組み合わせた上、個人（運転者）を特定することが出来た場合、個人の詳細な行動履歴を把握する情報源となるため、守秘すべきプライバシー情報になると考えられる。

【全体構成図の解説】

IPA が 2012 年度に第 1 版を公開した「自動車の情報セキュリティへの取組みガイド」[7]では、IPA において自動車の各機能を整理した自動車の機能モデル（IPA カー）を仮定し、各機能が持つ情報やそれを利用するサービスについて検討した上で、各機能に想定される脅威を洗い出し、その対策を列挙した。自動車は、自動車製造業者や価格帯（グレード）によって構造・機能等に違いがあるため、業界共通的な自動車のモデルを定義することは困難であることから、「IPA カー」では車載 LAN を最大限に抽象化して一本のバスに全ての機能が接続されるものと仮定した。

近年の自動車の車載ネットワークは、必要とされる伝送速度・信頼性等それぞれの制御対象に応じて最適なネットワークを選択する傾向があり、車種によって違いはあるものの、「パワートレイン系」「シャーシ系」「安全系」「ボディ系」「車載情報系」「故障診断系」等から構成されている[72][73][74]。ここでは、複数のサブネットワークがセントラルゲートウェイを介して接続される形態をモデル化した全体像を、**図 5-4** に示す。

このシステムでは、以下に示す脅威が想定される。

- 車載機器内部に保存されたデータの漏えい
- 車載機器のウイルス感染、機器への不正アクセス
- 車載機器間の通信データの盗聴・改ざん
- 自動車と外部機器やインターネット上のサーバとの間の通信データの盗聴・改ざん
- （主に使用者自身による）車載機器の不正改造
- OBD-Ⅱポートに対する不正アクセス、不正コマンド送信、DoS 攻撃
- コネクテッドカーと通信するインターネット上のサーバに対する各種攻撃

【セキュリティ対策の留意事項】

コネクテッドカーにおいては、正常な運転操作を妨げる遠隔操作に対する防御策の実装が重要である。また、正常な運転操作に必要となる通信への妨害（通信データの改ざん、DoS）に対しても、防御策の実装が不可欠である。さらに、コネクテッドカーが収集するデータを、個人情報につながる機微な情報の一部として捉えて、その漏えい防止策を実装することが望まれる。

【脅威と対策表の構成と特徴】

先に示した脅威に対して、例えば以下に示す対策が有効であると考えられる。

- 機器内部のデータ暗号化
- 不正プログラムの動作防止（ホワイトリスト制御、ソフトウェア署名）
- 機器の分解対策（耐タンパー）、データのセキュアな消去
- 通信路の暗号化
- OBD-Ⅱポートにおける脆弱性対策、認証の強化、DoS 対策
- インターネット上のサーバにおけるデータ暗号化、脆弱性対策、認証の強化

これらの脅威と対策を**図 5-4** の上にマッピングしている。また脅威と対策、および IoT 関連のセキュリティガイド（OWASP Internet of Things Project、OTA IoT Trust Framework）の関係を整理した一覧を**表 5-10**～**表 5-12** に示す。

なお、車載ネットワーク構成はメーカー・車種によって異なるため、必ずしも検討の構成と同一ではない。構成要素（ECU: Electronic Control Unit やカーナビ、ITS 車載器等）の種類によって、守るべき情報資産、脅威、対策は異なり、本書の分析はその一例を示したに過ぎない。

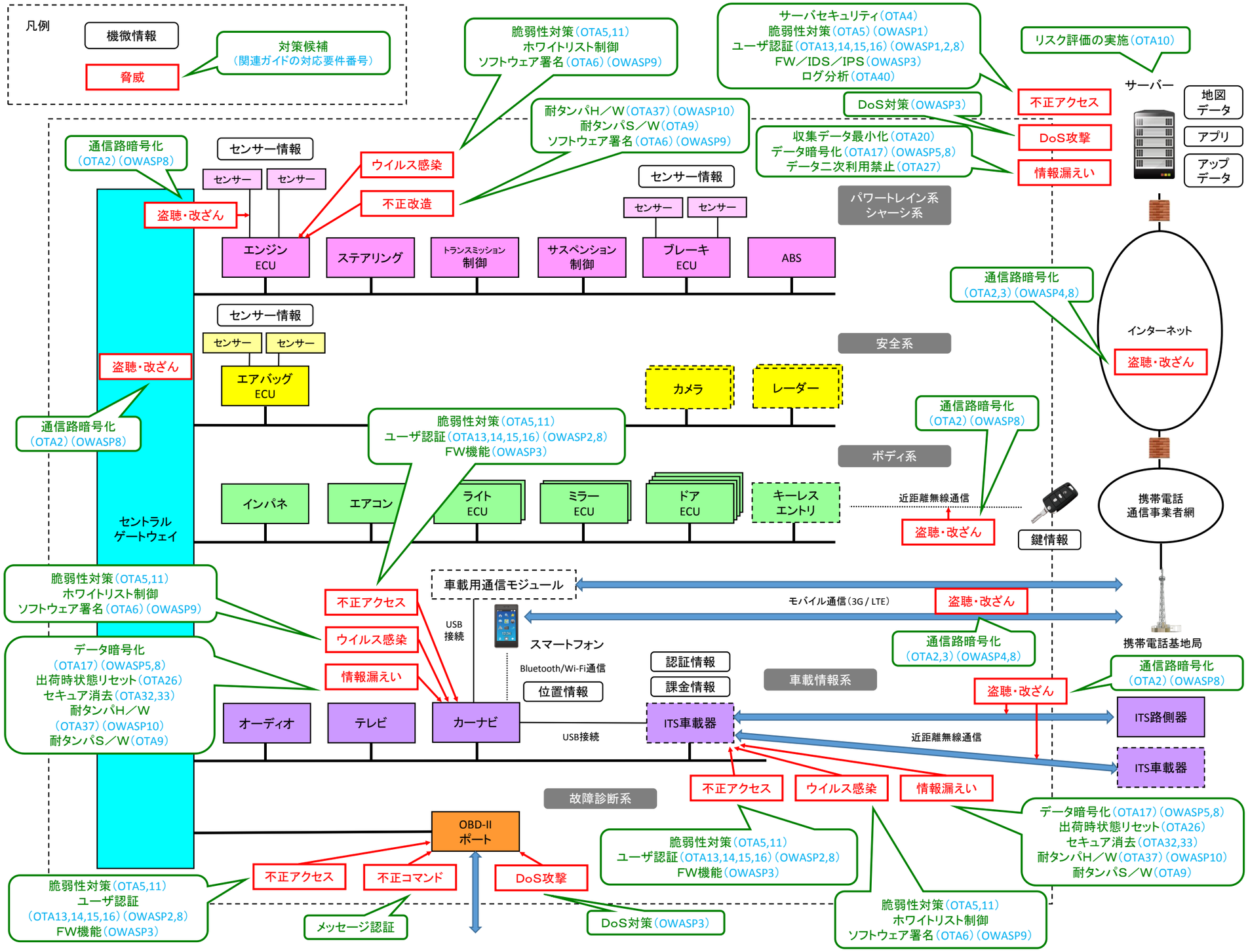


図 5-4　コネクテッドカーの脅威と対策の検討例

このページは空白です。

表 5-10　コネクテッドカーの脅威と対策表（1/3）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
コネクテッドカー	ECU	ウイルス感染	脆弱性対策	OTA5, OTA11	
			ホワイトリスト制御		
			ソフトウェア署名	OTA6,	OWASP9
		不正改造	耐タンパーH/W	OTA37	OWASP10
			耐タンパーS/W	OTA9	
			ソフトウェア署名	OTA6	OWASP9
	ECU・センサー間通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
	車載ネットワーク内（ECU・ECU 間等）通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
	OBD-II ポート	不正アクセス	脆弱性対策	OTA5, OTA11	
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			FW 機能		OWASP3
		不正コマンド	メッセージ認証		
		DoS 攻撃	DoS 対策		OWASP3

表 5-11　コネクテッドカーの脅威と対策表（2/3）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
コネクテッドカー	カーナビ	不正アクセス	脆弱性対策	OTA5, OTA11	
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8
			FW 機能		OWASP3
		ウイルス感染	脆弱性対策	OTA5, OTA11	
			ホワイトリスト制御		
			ソフトウェア署名	OTA6	OWASP9
		情報漏えい	データ暗号化	OTA17	OWASP5, OWASP8
			出荷時状態リセット	OTA26	
			セキュア消去	OTA32, OTA33	
			耐タンパーH/W	OTA37	OWASP10
			耐タンパーS/W	OTA9	
	ITS 車載器	不正アクセス	カーナビの脅威対策と同じ		
		ウイルス感染			
		情報漏えい			
キーレスエントリ・電子鍵間通信	近距離無線通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8

表 5-12　コネクテッドカーの脅威と対策表（3/3）

脅威			対策候補		
発生箇所		脅威名	対策名	他のガイドとの関係	
				OTA	OWASP
カーナビ・サーバ間の通信	モバイル通信（3G／LTE）	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8
	インターネット	盗聴・改ざん	通信路暗号化	OTA2, OTA3	OWASP4, OWASP8
サーバ	カーナビ製造業者または第三者	全脅威共通	リスク評価の実施	OTA10	
		不正アクセス	サーバセキュリティ	OTA4	
			脆弱性対策	OTA5	OWASP1, OWASP6
			ユーザ認証	OTA13, OTA14, OTA15, OTA16	OWASP1, OWASP2, OWASP6, OWASP8
			FW／IDS／IPS		OWASP3
			ログ分析	OTA40	
		DoS 攻撃	DoS 対策		OWASP3
		情報漏えい	収集データ最小化	OTA20	
			データ暗号化	OTA17	OWASP5, OWASP8
			データ二次利用禁止	OTA27	
ITS 車載器・ITS 路側器間の通信	近距離無線通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
ITS 車載器間の通信	近距離無線通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8

6. IoT セキュリティの根幹を支える暗号技術

IoT においては、保護すべき情報に対する不正アクセス、盗聴、改ざん・偽造、成りすましといった脅威への対策として、暗号技術を用いた認証、暗号化、電子署名を導入することが考えられる。すなわち、暗号技術は IoT セキュリティの根幹を支える重要な技術の一つである。

しかしながら、暗号技術を導入しても、暗号アルゴリズムの鍵長の選択、暗号鍵の管理(鍵の生成・配布・保管・用途・廃棄、鍵の一意性)、鍵関連情報(パラメータ)の取り扱いに不備が存在した場合、それらの脆弱性を攻撃して認証、暗号化、電子署名の効果を無効化する攻撃が成立する。

例えば、2014 年の Black Hat Europe 2014 において、Alberto Garcia Illera 氏と Javier Vazquez Vidal 氏が、スペインの電力会社で採用されているスマートメーターの脆弱性について報告した。[19]このシステムでは、共通鍵暗号アルゴリズムとして、鍵長 128 ビットの AES という、安全と考えられている暗号技術を採用していたが、全てのスマートメーターが同一の暗号鍵となっており、起動時または製造時にインストールされたものをそのまま使用していた。このため、一台のメーターを入手・分解して鍵を取得し、ファームウェアを書き換えることによって、電力の遮断を含む全てのコマンドを成りすまして送信可能であった。

また、2010 年にはインターネット接続機能を有する家庭用ゲーム機において、正当なプログラムのみ動作可能とするために導入されていた公開鍵暗号アルゴリズム ECDSA の秘密鍵(システム全体のセキュリティの根幹となる存在であり、「ルートキー」と呼ばれていた)が漏えいした。[20]これは、秘密鍵を生成する際に使用するランダムであるはずの値が常に同じ値であったため、秘密鍵を推測可能であったと報告されている。

すなわち、安全であると考えられる暗号アルゴリズムを用いた認証・暗号化・電子署名を導入しても、設計上の不備・誤りが存在したり、運用方法が不適切であったりする場合は、その脆弱性を突いて攻撃が成立する恐れがある。

IoT セキュリティにおいて採用した暗号技術の利用・運用方針を明確化し、安全性の評価を支援するチェックリストを**付録 C.**に添付したので、活用して頂きたい。

---

[19] Black Hat Europe 2014: LIGHTS OFF! THE DARKNESS OF THE SMART METERS
https://www.blackhat.com/eu-14/briefings.html#lights-off-the-darkness-of-the-smart-meters

[20] exophase: Hackers Describe PS3 Security As Epic Fail, Gain Unrestricted Access
https://www.exophase.com/20540/hackers-describe-ps3-security-as-epic-fail-gain-unrestricted-access/

【コラム】

WPA2 の脆弱性（KRACKs 攻撃）における暗号技術の利用誤り

2017 年 10 月 16 日（米国時間）、無線 LAN の暗号化通信手段として、広く利用されているセキュリティプロトコル WPA2 の脆弱性が公開され、世界中を騒ぎに巻き込んだ。KRACKs（Key Reinstallation AttaCKs）[21]と名付けられたこの攻撃は、WPA2 仕様の脆弱性（プロトコル設計上の曖昧性や誤り）、クライアントおよびアクセスポイントの脆弱性（実装上の誤り）を悪用し、暗号技術の不適切な使い方をさせることで、その効果を無効化し、暗号化されたパケットの復号や通信パケットの改ざんを可能とする攻撃であった[22]。

WPA2 の脆弱性報告 JVN（JVNVU#90609033）[23]には、以下の概要が記述されている。

> Wi-Fi Protected Access II（WPA2）には、ハンドシェイク中に Nonce およびセッション鍵の再利用を許容してしまう問題があります

この「Nonce およびセッション鍵の再利用」とは、WPA2 における暗号技術の利用において、

- 暗号化方式 CCMP（暗号アルゴリズム AES）を利用している場合、
  AES の CCM モードで、同一の暗号鍵で、同一の Nonce を使用すること
- 暗号化方式 GCMP（暗号アルゴリズム AES）を利用している場合、
  AES の GCM モードで、同一の暗号鍵で、同一の初期化ベクタを使用すること

に相当している。これは、暗号技術チェックリストにおける、

項番 22：【ブロック暗号の CCM モードを使用している場合】
◎同一の共通鍵で使用される全ての Nonce が互いに異なること
（同一の共通鍵で同じ Nonce を再使用しないこと）。
項番 23：【ブロック暗号の…GCM モード…を使用している場合】
◎初期化ベクタ（IV）は、一意の（互いに異なる）値を使用すること。

の要件を満たさないプロトコル設計や実装となっていることを意味する。

セキュリティ設計時に本チェックリストを活用することによって、この様な暗号技術の利用誤りを見つけることが出来る。

---

21 https://www.krackattacks.com/
22 https://papers.mathyvanhoef.com/ccs2017.pdf
23 https://jvn.jp/vu/JVNVU90609033/index.html

参考文献

【IPA 報告書類】

[1] 組込みシステムのセキュリティへの取組みガイド, IPA, 2009/7/6
https://www.ipa.go.jp/security/fy20/reports/emb_app/index.html

[2] 「情報家電におけるセキュリティ対策　検討報告書」, IPA, 2011/2/1
https://www.ipa.go.jp/security/fy22/reports/electronic/index.html

[3] 「組込みシステムのセキュリティへの取組みガイド(2010 年度改訂版)」, IPA, 2011/2/22
https://www.ipa.go.jp/security/fy22/reports/emb_app2010/index.html

[4] 「2010 年度　自動車の情報セキュリティ動向に関する調査」報告書の公開, IPA, 2011/4/26
https://www.ipa.go.jp/security/fy22/reports/emb_car/index.html

[5] 「2010　年度　制御システムの情報セキュリティ動向に関する調査」報告書の公開, IPA, 2011/5/9
https://www.ipa.go.jp/security/fy22/reports/ics_sec/index.html

[6] 「2011 年度　自動車の情報セキュリティ動向に関する調査」報告書の公開, IPA, 2012/5/31
https://www.ipa.go.jp/security/fy23/reports/emb_car/index.html

[7] 「自動車の情報セキュリティへの取組みガイド」第 2 版を公開　～製品のライフサイクル(製造工程、配送を含む)をカバーするセキュリティへの対応～, IPA, 2017/3/23
https://www.ipa.go.jp/security/iot/emb_car2.html

[8] 医療機器における情報セキュリティに関する調査(2013 年度), IPA, 2014/4/16
https://www.ipa.go.jp/security/fy25/reports/medi_sec/index.html

[9] 脆弱性対策:ファジング, IPA, 2017/3/3
https://www.ipa.go.jp/security/vuln/fuzzing.html

[10] SEC BOOKS: ESCR Ver.2.0:【改訂版】組込みソフトウェア開発向けコーディング作法ガイド [C 言語版] Ver.2.0, IPA, 2015/4/10
https://www.ipa.go.jp/sec/publish/tn13-001.html

[11] つながる世界における脅威と脆弱性検討のポイント, SEC journal No.43, IPA, 2015/12/1
https://www.ipa.go.jp/files/000049573.pdf

[12] 利用時の品質の観点を盛り込んだ「つながる世界の開発指針(第 2 版)」を発行, IPA, 2017/6/30
https://www.ipa.go.jp/sec/reports/20170630.html

[13] IPA 脆弱性対策コンテンツリファレンス, IPA, 2017/3
https://www.ipa.go.jp/files/000051352.pdf

[14] 情報セキュリティ早期警戒パートナーシップガイドライン, IPA, 2017/5/30
https://www.ipa.go.jp/security/ciadr/partnership_guide.html

[15] JVN iPedia 脆弱性対策情報データベース, IPA
https://jvndb.jvn.jp/

[16] 情報セキュリティ 10 大脅威 2017, IPA, 2017/3/30
https://www.ipa.go.jp/security/vuln/10threats2017.html

[17] 制御システム利用者のための脆弱性対応ガイド 第 3 版, IPA, 2017/3/30
https://www.ipa.go.jp/files/000058489.pdf

[18]「つながる世界の開発指針」の実践に向けた手引き IoT 高信頼化機能編, IPA, 2017/5/8
https://www.ipa.go.jp/sec/reports/20170508.html

[19] 制御システムのセキュリティリスク分析ガイド～セキュリティ対策におけるリスク分析実施のススメ～, IPA, 2017/10/2
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

[20] ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト, IPA, 2017/12/7
https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/index.html

[21] IoT 製品・サービス脆弱性対応ガイド, IPA, 2018/3/22
https://www.ipa.go.jp/security/fy29/reports/vuln_handling/index.html#L3

[22] 情報セキュリティ 10 大脅威 2018, IPA, 2018/3/30
https://www.ipa.go.jp/security/vuln/10threats2018.html

【IoT モデル化】

[23] IoT のセキュリティ脅威と今後の動向, 兜森清忠（株式会社シマンテック／IoT セキュリティ WG リーダー）, JNSA Network Security Forum 2015, 日本ネットワークセキュリティ協会, 2015/1/20
http://www.jnsa.org/seminar/nsf/2015/data/A1_kabuomori.pdf

[24] 拡大する IoT とそのセキュリティについて, 松岡正人（株式会社カスペルスキー／IoT セキュリティ WG リーダー）, JNSA 2014 年度活動報告会, 日本ネットワークセキュリティ協会, 2015/6/9
http://www.jnsa.org/seminar/2015/0609/data/A7_iot.pdf

【IoT 関連のセキュリティガイド（OWASP, OTA, GSMA 以外）】

[25] IoT セキュリティガイドライン ver 1.0, 経済産業省・総務省・IoT 推進コンソーシアム, 2016/7/5
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

[26] 安全な IoT システムのためのセキュリティに関する一般的枠組, 内閣官房サイバーセキュリティセンター（NISC）, 2016/8/26
https://www.nisc.go.jp/active/kihon/res_iot_fw2016.html

[27] IoT クラウドサービスワーキンググループ，日本クラウドセキュリティアライアンス（CSAJC）
https://www.cloudsecurityalliance.jp/IoT_WG.html

[28] 協議会・研究会公開資料，重要生活機器連携セキュリティ協議会（CCDS）
https://www.ccds.or.jp/public_document/index.html

[29] コンシューマ向け IoT セキュリティガイド（IoT セキュリティワーキンググループ），日本ネットワークセキュリティ協会（JNSA），2016/6/24
http://www.jnsa.org/result/iot/

[30] 防犯カメラシステムネットワーク構築ガイドⅡ　ーインターネットとの接続に係る脅威と対策ー，日本防犯設備協会，2017/5/22
http://www.ssaj.or.jp/guidebook/pdf/421.pdf

[31] Internet of Things: Privacy and Security in a Connected World，FTC，2015/1/27
https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[32] NIST Special Publication 800-183 - Networks of 'Things'，NIST，2016/7
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

[33] Industrial Internet of Things Volume G4: Security Framework，IIC，2016/9/19
https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[34] Strategic Principles for Securing the Internet of Things，U.S. Department of Homeland Security，2016/11/15
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

[35] IoT Security Compliance Framework，IoT Security Foundation，2016/12
https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

[36] Baseline Security Recommendations for IoT，ENISA，2017/11/20
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

【OWASP Internet of Things Project】

[37] OWASP Internet of Things Project，OWASP，2017/8/19
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[38] IoT Attack Surface Areas Project，OWASP Internet of Things Project，2017/8/19
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Attack_Surface_Areas

[39] IoT Vulnerabilities Project，OWASP Internet of Things Project，2017/8/19
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Vulnerabilities

[40] Top IoT Vulnerabilities, OWASP IoT Vulnerabilities Project, 2016/5/18
https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

[41] IoT Testing Guides, OWASP Internet of Things Project, 2016/5/14
https://www.owasp.org/index.php/IoT_Testing_Guides

[42] IoT Security Guidance, OWASP Internet of Things Project, 2017/2/14
https://www.owasp.org/index.php/IoT_Security_Guidance

[43] Principles of IoT Security, OWASP Internet of Things Project, 2016/5/14
https://www.owasp.org/index.php/Principles_of_IoT_Security

[44] IoT Framework Assessment, OWASP Internet of Things Project, 2016/5/14
https://www.owasp.org/index.php/IoT_Framework_Assessment

[45] IoT 時代において重要性が増すデバイスのセキュリティ(OWASP でビルドインセキュリティ第5回), 坪 和樹(OWASP Japan), CodeZine, 2016/2/12
http://codezine.jp/article/detail/9232

[46] OWASP IoT Testing Guidance のガイダンス, 虎塚(クラスメソッド株式会社), Developers.IO, 2015/11/6
http://dev.classmethod.jp/security/owasp-iot-testing-guidanece/

[47] IoT のセキュリティリスク Top10 とそれらへの対応方法, 牧田延大, F5 Networks DevCentral, 2015/9/1
https://devcentral.f5.com/articles/iot-top-10

【OTA IoT Trust Framework】

[48] Internet of Things, Online Trust Alliance(OTA)
https://otalliance.org/IoT

[49] OTA IoT Trust Framework - Updated July 12, 2016, Online Trust Alliance(OTA), 2016/7/12
https://otalliance.org/IoT

[50] IoT Trust Framework - Resource Guide Updated 4/8/2016, Online Trust Alliance (OTA), 2016/4/8
https://otalliance.org/IoT

[51] IoT のリスクマネジメントガイド役「IoT Trust Framework」の最新版が公開, THE ZERO/ONE, 2017/01/18
https://the01.jp/p0004112/

【GSMA IoT Security Guidelines】

[52] GSMA IoT Security Guidelines & Assessment, GSMA
https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

[53] GSMA IoT Security Guidelines - complete document set, GSMA, 2017/10/31
https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/

[54] CLP.11 - IoT Security Guidelines Overview Document, GSMA, 2017/10/31
https://www.gsma.com/iot/iot-security-guidelines-overview-document/

[55] CLP.12 - IoT Security Guidelines for Service Ecosystems, GSMA, 2017/10/31
https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/

[56] CLP.13 - IoT Security Guidelines for Endpoint Ecosystems, GSMA, 2017/10/31
https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/

[57] CLP.14 - IoT Security Guidelines for Network Operators, GSMA, 2017/10/31
https://www.gsma.com/iot/iot-security-guidelines-for-network-operators/

[58] CLP.17 - GSMA IoT Security Assessment, GSMA, 2017/10/31
https://www.gsma.com/iot/iot-security-assessment/

【暗号技術関連】

[59] NIST Special Publication 800-38A 2001 Edition - Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST, 2001/12/1
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[60] NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, NIST, 2007/7/20
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

[61] NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST, 2007/11/28
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[62] NIST Special Publication 800-57 Part 1 Revision 4 - Recommendation for Key Management Part 1: General, NIST, 2016/1/28
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[63] NIST Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST, 2015/6/24
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

[64] NIST Special Publication 800-131A Revision 1 - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Length , NIST , 2015/11/6
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

[65] NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity , NIST , 2014/9/25
http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[66] 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト），CRYPTREC，2017/3/30
http://www.cryptrec.go.jp/list/cryptrec-ls-0001-2016.pdf

【ヘルスケア】

[67] OMRON connect，オムロン ヘルスケア株式会社
https://www.omronconnect.com/jp/ja_def/

[68] 健康管理サービス HealthPlanet，株式会社タニタヘルスリンク
https://www.healthplanet.jp/

【スマートハウス】

[69] スマートコミュニティ・アライアンス（JSCA: Japan Smart Community Alliance）
https://www.smart-japan.org/

[70] HEMS - 住まいの設備と建材，パナソニック株式会社
http://sumai.panasonic.jp/hems/

【コネクテッドカー】

[71] コネクテッドカー・オートノマスカー，平成 27 年版 情報通信白書，総務省，2015/7/28
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc241210.html

[72]「自動車と IoT（Internet of Things）」 自動車の情報化（テレマティクス）化から始まる IoT の世界，EY 総研インサイト Vol.2 Autumn 2014，EY 総合研究所，2014/10/6
http://eyi.eyjapan.jp/knowledge/insight/pdf/2014-10-vol02-all.pdf

[73] 情報化する自動車と車載ネットワークの動向 ～安全と利便性の追求に伴う高速通信への対応～，今月のトピックス No.207，日本政策投資銀行，2014/3/24
http://www.dbj.jp/pdf/investigate/mo_report/0000015497_file3.pdf

[74] 車載通信ネットワークの標準化の動向 －FlexRay と MOST を中心に－，後藤正博・徳田昭雄・立本博文，社会システム研究 第 23 号，立命館大学，2011/9
http://www.ritsumei.ac.jp/acd/re/ssrc/result/memoirs/kiyou23/23-07.pdf

付録 A.　OWASP Internet of Things Project の成果概要

OWASP Internet of Things Project の主な成果の概要を示す。プロジェクトの成果は随時更新されているため、詳細および最新情報については、OWASP のウェブサイト[37]を参照のこと。

現在、OWASP Internet of Things Project では、IoT に関する脆弱性を 17 種類に分類し、その概要、攻撃対象（脆弱性発生箇所）との関係を整理している。また、2014 年に公開した Top 10 IoT Vulnerabilities from 2014 では、IoT に関わる 10 大脆弱性に関して、

- 脅威となる人（Threat Agents）
- 攻撃手法（Attack Vectors）
  - 悪用難易度（Exploitability）
- セキュリティ上の弱点（Security Weakness）
  - 普及度（Prevalence）
  - 検出難易度（Detectability）
- 技術的影響（Technical Impacts）
- ビジネスへの影響（Business Impacts）
- 当該脆弱性の有無の確認方法
- 攻撃シナリオの例（Example Attack Scenarios）
- 脆弱性を解消する方法
- 参照（References）

を示している。**表 A-1** に 10 大脆弱性の概要を、**表 A-2** に脆弱性の記載例（抜粋）を示す。

また、OWASP Internet of Things Project の成果である、IoT Security Guidance および IoT Testing Guides（現時点では共にドラフト段階）では、各脆弱性に関して、

- 製造業者（Manufacturer）が考慮すべきセキュリティ
- 開発者（Developer）が考慮すべきセキュリティ
- 消費者（Consumer）が考慮すべきセキュリティ
- 試験実施者（Tester）が考慮すべきセキュリティ

を具体的に示している。**表 A-3** に記載例（抜粋）を示す。

IoT Vulnerabilities に示された 17 種類の脆弱性の概要を、**表 A-4** および**表 A-5** に示す。

表 A-1　OWASP Top 10 IoT Vulnerabilities from 2014 の概要

脆弱性	攻撃者	攻撃手法	セキュリティ上の弱点		技術的影響	ビジネスへの影響
		悪用難易度	普及度	検出難易度		
2014-I1: 安全でない Web インタフェース	アプリ依存	容易	中	容易	深刻	アプリ／ビジネス依存
2014-I2: 不十分な認証／認可	アプリ依存	普通	中	容易	深刻	アプリ／ビジネス依存
2014-I3: 安全でないネットワークサービス	アプリ依存	普通	低	普通	中程度	アプリ／ビジネス依存
2014-I4: トランスポート暗号化の欠如	アプリ依存	普通	中	容易	深刻	アプリ／ビジネス依存
2014-I5: プライバシーの懸念	アプリ依存	普通	中	容易	深刻	アプリ／ビジネス依存
2014-I6: 安全でないクラウドインタフェース	アプリ依存	普通	中	容易	深刻	アプリ／ビジネス依存
2014-I7: 安全でないモバイルインタフェース	アプリ依存	普通	中	容易	深刻	アプリ／ビジネス依存
2014-I8: 不十分なセキュリティ設定	アプリ依存	普通	中	容易	中程度	アプリ／ビジネス依存
2014-I9: 安全でないソフトウェア／ファームウェア	アプリ依存	困難	中	容易	深刻	アプリ／ビジネス依存
2014-I10: 貧弱な物理セキュリティ	アプリ依存	普通	中	普通	深刻	アプリ／ビジネス依存

出典：OWASP Internet of Things Project, Top IoT Vulnerabilities[37][40] を基に作成

表 A-2　OWASP Top 10 IoT Vulnerabilities from 2014 における記載例（抜粋）

2014-I1: 安全でない Web インタフェース					
脅威となる人	攻撃手法	セキュリティ上の弱点		技術的影響	ビジネスへの影響
	悪用難易度	普及度	検出難易度		
アプリ依存	容易	中	容易	深刻	アプリ／ビジネス依存
内部ユーザおよび外部ユーザを含む、Web インタフェースにアクセスする全ての人。	攻撃者は弱い資格情報の利用、平文の資格情報の捕獲、Web インタフェース用アカウントの列挙を用いて攻撃する。 攻撃は、外部ユーザあるいは内部ユーザから行われる可能性がある。	アカウント列挙、アカウントロックアウトの欠如、弱い資格情報といった問題が存在する時、Web インタフェースが安全でない可能性がある。 Web インタフェースを内部ネットワークのみに公開する意図であったとしても、内部ユーザからの脅威は外部ユーザからの脅威と同様に重要であるため、安全でない Web インタフェースが蔓延している。 …		安全でない Web インタフェースは、結果としてデータの消失やセキュリティ破壊、責任追跡性の欠如、アクセス拒否を生じて、機器の完全な乗っ取りに繋がる可能性がある。	安全でない Web インタフェースは、機器の破損に加えて、消費者を傷付けることに繋がることを熟考せよ。 あなたの顧客が傷付いてもよいのですか？ あなたの商標が傷付いてもよいのですか？

脆弱性の確認方法	・製品の初期設定中に既定のユーザ名とパスワードを変更することが可能であるか否か確認する。 ・3～5 回ログインの試みに失敗した後、特定のアカウントがロックアウトされるか否か確認する。 …
攻撃シナリオの例	シナリオ #1: Web インタフェースは、無効なアカウント入力に対して、そのアカウントが存在しないことを攻撃者に通知する「Forgot Password」機能を提供する。アカウントが有効であることを識別すると、アカウントロックアウト制御が存在しない場合、無期限のパスワード推測攻撃が可能となる。 …
脆弱性の解消方法	1. 既定のパスワードと、理想的には既定のユーザ名を、初期設定中に変更すること。 2. パスワード回復機構は強固で、攻撃者に正規のアカウントを示唆する情報を与えないこと。 …

出典：OWASP Internet of Things Project, Top IoT Vulnerabilities[37][40] を基に作成

表 A-3　OWASP IoT Security Guidance, IoT Testing Guides における記載例（抜粋）

2014-I1: 安全でない Web インタフェース	
製造者の 考慮事項	・全ての Web インタフェースにおいて、弱いパスワードを禁止すること。 ・全ての Web インタフェースにおいて、アカウントロックアウト機構を備えていること。 ・全ての Web インタフェースにおいて、XSS、SQLi および CSRF の脆弱性に対して試験していること。 ・全ての Web インタフェースにおいて、伝送する情報を保護するために HTTPS を用いる能力を備えていること。 …
開発者の 考慮事項	・全ての Web インタフェースのコーディングにおいて、弱いパスワードの使用を防止する様に書かれていること。 ・全ての Web インタフェースのコーディングにおいて、アカウントロックアウト機構を含む様に書かれていること。 ・全ての Web インタフェースのコーディングにおいて、XSS、SQLi 及び CSRF の脆弱性に対して試験していること。 ・全ての Web インタフェースにおいて、伝送する情報を保護するために HTTPS を用いる能力を備えていること。 …
消費者の 考慮事項	・システムが HTTPS を使用するオプションを有しているならば、有効化すること。 ・システムが二要素認証オプションを有しているならば、有効化すること。 ・システムが Web アプリケーションファイアウォールオプションを有しているならば、有効化すること。 ・システムがローカルな、あるいはクラウドベースの Web アプリケーションを有しているならば、既定のパスワードを強固なものに変更し、さらに、可能であれば既定のユーザ名も変更すること。 …

2014-I1: 安全でない Web インタフェース	
試験実施者の 考慮事項	・弱いパスワードが許されているか否か決定するために、全ての Web インタフェースを評価すること。 ・アカウントロックアウト機構を評価すること。 ・XSS、SQLi 及び CSRF の脆弱性やその他の Web アプリケーション脆弱性に対して、Web インタフェースを評価すること。 ・転送する情報を保護するための HTTPS の使用を評価すること。 …

出典：OWASP Internet of Things Project, IoT Security Guidance, IoT Testing Guides[37][41][42] を基に作成

表 A-4　IoT Vulnerabilities の概要（1/2）

	脆弱性	攻撃箇所	要約
1	ユーザ名列挙	・管理インタフェース ・デバイス Web インタフェース ・クラウドインタフェース ・モバイルアプリケーション	・認証機構とやり取りすることによって、有効なユーザ名の集合を収集することが可能
2	弱いパスワード	・管理インタフェース ・デバイス Web インタフェース ・クラウドインタフェース ・モバイルアプリケーション	・例えば、アカウントのパスワードとして”1234”や”123456”を設定可能 ・予めプログラムされたデフォルトパスワードの利用
3	アカウントの凍結	・管理インタフェース ・デバイス Web インタフェース ・クラウドインタフェース ・モバイルアプリケーション	・3～5 回のログイン失敗後、認証の試みの継続送信が可能
4	暗号化されていないサービス	・デバイスネットワークサービス	・ネットワークサービスは、攻撃者による盗聴・改ざんを防止するための適切な暗号化が未実施
5	二要素認証の欠如	・管理インタフェース ・クラウド Web インタフェース ・モバイルアプリケーション	・セキュリティトークンや指紋認証装置等の二要素認証機構の欠如
6	不十分な暗号化の実装	・デバイスネットワークサービス	・暗号化は実装されているが、設定不十分または更新不十分（例えば、SSL v2 の利用）
7	暗号化せずに配布される更新	・更新機構	・ネットワーク経由での更新配布時、TLS 未使用または更新ファイルの暗号化未実施
8	書き換え可能な更新記憶領域	・更新機構	・更新ファイルの記憶領域は誰でも書き換え可能なため、改ざんされたファームウェアが全ユーザに配布される恐れがある
9	DoS（Denial of Service）	・デバイスネットワークサービス	・サービスまたは全ての機器に対する DoS 攻撃が可能

出典：OWASP Internet of Things Project, IoT Vulnerabilities[37][39] を基に作成

表 A-5　IoT Vulnerabilities の概要（2/2）

	脆弱性	攻撃箇所	要約
10	記憶媒体の取り外し	・デバイス物理インタフェース	・機器からの記憶媒体の物理的取り外し可能
11	手動更新機構の欠如	・更新機構	・手動による機器の更新確認の強制不可能
12	更新機構の欠落	・更新機構	・機器の更新の不可能
13	ファームウェアバージョンと 最終更新日の表示	・デバイスファームウェア	・現在のファームウェアのバージョンの非表示、 最終更新日の非表示
14	ファームウェア及び記憶装置 （IC チップ）の抜き取り	・JTAG/SWD インタフェース ・In-Situ dumping ・OTA アップデートの横取り ・製造業者の Web サイトからの ダウンロード ・eMMC tapping ・SPI Flash / eMMC チップの 半田付け取り外しとアダプタ経由 での内容読出	・ファームウェアには、ソースコード、実行するサービスのバイナリ コード、初期設定パスワード、SSH 鍵等、多くの有用な情報が 含まれている
15	デバイスのコード実行フロー 処理	・JTAG/SWD インタフェース ・サイドチャネル攻撃	・JTAG アダプタ経由の gdb 利用による、ファームウェア改ざんと ソフトウェアベースのセキュリティ制御の回避 ・サイトチャネル攻撃は、実行フローの書き換えやデバイス内の情報 の窃取に利用可能
16	コンソールへのアクセス取得	・シリアルインタフェース （SPI/UART）	・シリアルインタフェース経由の接続による、デバイスのコンソールの フルアクセス取得 ・カスタマイズされたブートローダー等のセキュリティ機能は、攻撃者 によるシングルユーザモードへの侵入を防止するが、バイパスする ことも可能
17	セキュアでない第三者部品	ソフトウェア	・旧バージョンの busybox、openssl、ssh、Web サーバ等

出典：OWASP Internet of Things Project, IoT Vulnerabilities[37][39] を基に作成

付録 B.　OTA IoT Trust Framework の概要

OTA IoT Trust Framework® v2.5 で規定された 40 項目の概要と「必須」「推奨」の規定（仮訳）を、**表 B-1～表 B-7** に示す。

【訳注】原文では、ユーザ（user）、エンドユーザ（end-user）、消費者（consumer）の単語が使い分けられているが、仮訳では全て「ユーザ」としている。

各項目には、「必須」「推奨」の種別が示されている。

以前公開されていたドラフト版においては、適用分野として、(1)コネクテッドホーム、(2)ウェアラブル技術を対象とし、分野別で異なる種別が規定されていた。正式版の最初の版（Released 3/2/2016）では両者の相違点は無くなり、現在の最新版には、適用分野の欄は存在しない。

詳細については、OTA のウェブサイトからダウンロード可能な各文書を参照のこと。

表 B-1　OTA IoT Trust Framework（1/7）

IoT Trust Framework　● 必須　○ 推奨	
セキュリティ ー 機器、アプリケーション、クラウドサービス	
1. 機器がセキュリティに関連する更新を受信する機能を有するか否かを、開示すること。機能を有する場合は、機器がセキュリティ更新を自動的に受信可能であるか否か、機器が正しく適切な方法で更新されたことを保証するためにどの様なユーザ操作が要求されるか、開示すること。	●
2. 機器および関連アプリケーションは、現在の一般に認められたセキュリティプロトコル、暗号プロトコル、ベストプラクティスに対応していること。全ての個人情報は、送信や保管の際、現在の一般に認められたセキュリティ標準を用いて暗号化されなければならない。伝送路には有線接続、Wi-Fi および Bluetooth 接続を含むが、これらに限定するものではない。	●
3. IoT をサポートする全ての Web サイトは、機器からバックエンドサービスまでのユーザセッションを完全に暗号化しなければならない。現在のベストプラクティスには、HTTPS または HTTP Strict Transport Security（HSTS）を既定とすること等があり、AOSSL または Always On SSL として知られている。機器は、バックエンドサービスやサポートするアプリケーションを確実に認証するための仕組みを有することが望ましい。[1]	●
4. IoT をサポートするサイトは、脆弱性の影響を許容範囲内に低減するために、サイトのセキュリティとサーバ設定の定期的なモニタリングと継続的な改善を実装しなければならない。少なくとも半年毎に、ペネトレーションテストを実施すること。[2]	●
5. 外部の第三者（顧客、消費者、学術界、研究コミュニティを含むが、これらに限定しない）からの脆弱性報告を受付、管理し、速やかに対応するためのプロセスとシステムを含む、協調的な脆弱性の開示を確立・維持すること。製品発売後、設計上の脆弱性や脅威を、リモートでの更新と、実施可能な詳細対策情報を含むアドバイザリ（ユーザへの通知）の提供の両方またはいずれか、あるいはその他の効果的な仕組みを通して、社会的に責任ある方法で修正すること。開発者は、脆弱性の検出を促進するために、「脆弱性報奨金」制度やクラウドソーシング方式を検討することが望ましい。	●
6. ソフトウェアおよびファームウェアの更新、パッチ、改版を、自動化された安全かつセキュアな方法で提供する仕組みが確保されていること。その様な更新は、署名がされており、署名生成と完全性の検証あるいはその他の方法により、信頼のおける配信元から配信されたものであることが立証されなければならない。もしくは、そのいずれかが為されなければならない。	●

出典：OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

表 B-2　OTA IoT Trust Framework（2/7）

IoT Trust Framework　● 必須　○ 推奨	
セキュリティー ー 機器、アプリケーション、クラウドサービス （続き）	
7. 更新およびパッチは、ユーザに通知することなく、ユーザが設定したユーザ固有の設定、セキュリティ設定およびプライバシー設定を変更してはならない。機器のファームウェアやソフトウェアを上書きする場合は、最初の利用時に、ユーザがプライバシー設定を確認・選択できる様にしなければならない。	●
8. セキュリティ更新プロセスが半自動更新の場合、その旨を開示しなければならない。半自動更新は、ユーザに更新を承認、認可または拒否する選択肢が提供される。データの消費や接続（モバイルキャリアまたは ISP）等によっては、ユーザは更新をいつ、どの様に行うのか自分で決定したいと望む場合がある。一方、自動更新は、ユーザによる介入なしでシームレスに機器宛てに配信され、ユーザへの通知が行われる場合とそうでない場合がある。	●
9. 全ての IoT 機器および関連するソフトウェアについて、利用している第三者ソフトウェア／オープンソースソフトウェアやコンポーネントのインベントリを管理すると共に、単体テスト、システムテスト、受け入れテスト、リグレッションテストおよび脅威モデリングを含む、厳格で、標準化されたソフトウェア開発ライフサイクルテストに従うこと。また、機器、アプリケーションおよびクラウドサービス間の情報漏えいの防止を含む、一連の典型的なユースケースにおいて、一般に認められたコードおよびシステムの堅牢化技術を利用すること。セキュアなソフトウェア開発には、プロジェクトの発端から実装、試験、利用段階を通じて、セキュリティを考慮することが必要である。機器は、最新のソフトウェアで出荷し、既知のクリティカルな脆弱性に対応するため、最初の起動時に自動更新を行うことが望ましい。	●
10. 全てのサービスおよびクラウド提供者に対して、セキュリティおよびコンプライアンス上のリスク評価を実施すること。 IoT resource guide https://otalliance.org/IoT を参照。	●
11. ソフトウェア、ファームウェア、ハードウェア、第三者ソフトウェアライブラリ（オープンソースのモジュールやプラグインを含む）を含む「構成要素の一覧」を作成、管理すること。報告された脆弱性を速やかに修正するため、機器、モバイル、クラウドサービスに対して行うこと。	○
12. 運用に必要な最小限の要件で、機器を設計すること。例えば、運用や保守に必要となる場合にのみ、USB ポートやメモリカードスロットを含めることが望ましい。また、未使用のポートやサービスは無効化することが望ましい。	●

出典：OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

表 B-3　OTA IoT Trust Framework（3/7）

IoT Trust Framework　● 必須　○ 推奨	
ユーザ・アクセスと資格情報	
13. システムが一意に生成したパスワード、ワンタイム・パスワードの提供、あるいは、別のセキュアな証明書（認証情報）の利用を含む、強固な認証方法を既定として含むこと。必要に応じて、管理者権限でのアクセスには別途一意のパスワードを要求し、機器とサービス、工場出荷時状態へのリセット時の各々への影響について明確に記述すること。	●
14. 一般に認められたパスワード回復機能を IoT アプリケーションに提供すること。回復には、パスワードと、パスワードがない場合には多要素での確認・認証方法（電子メールや電話等）を用いた認証情報をリセットする仕組みの両方、またはいずれかをサポートすること。	●
15. 無効なログインの試行がある程度の回数続いた場合、ユーザアカウントやサポート用アカウントのロックや無効化を行い、「総当り攻撃（ブルートフォース攻撃）」や他の不正なログインの試み（自動ログインボット等）を防止すること。	●
16. パスワードのリセットまたは変更にあたっては、セキュアな認証の実施と、ユーザへの通常と異なる方法（out-of-band）での通知の両方またはいずれかを行うこと。	●
17. 認証情報（ユーザパスワードを含むが、これに限定しない）は、ソルトを用い、ハッシュ化と暗号化の両方またはいずれかを行わなければならない。これは、不正アクセスやブルートフォース攻撃を防止するために、全ての認証情報を保存する際に適用すること。	●

出典：OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

表 B-4　OTA IoT Trust Framework（4/7）

IoT Trust Framework　● 必須　○ 推奨	
プライバシー、透明性と開示	
18. ユーザが購入、起動、ダウンロード、利用者登録を行う前に確認できるように、プライバシーポリシー、セキュリティポリシー、サポートポリシーは簡単に見つけられ、明確で、かつ容易に入手できるようにすること。製品パッケージ上や Web サイトに目立つ様に配置することに加えて、QR コードやユーザフレンドリーな短縮 URL、店頭での他の同様な方法を活用することが推奨される。	●
19.（製品保証の範囲を超えた）セキュリティおよびパッチサポートの実施期間および終了時期を開示すること。サポートは、例えば 2025 年 1 月 1 日など、定められた期日（sunset date）に終了してもよいし、あるいは、伝統的な保証の様に、購入日から一定期間経過後に終了してもよい。理想的には、開示するサポート実施期間や終了時期は機器の想定寿命と合わせるべきであり、購入前にユーザに通知されることが望ましい。（*IoT 機器は、無期限にセキュアに保つ、あるいはパッチを適用することはできないと考えられる。使用可能期間を超えて機器と使用するリスクとその影響、および警告が無視されたり機器の使用を中止しなかったりした場合の他者への影響について、ユーザに伝えることを検討すること。*）ユーザがサポート費用を支払わなければならない場合や年間サポート契約に加入しなければならない場合は、購入前に開示することが望ましい。	●
20. 情報の収集は提供する機器やサービスの機能性や情報を収集する目的に合理的に有用なものに限定し、収集する全ての個人情報と機微な情報の種類および属性情報、その利用方法、収集目的を目立つ様に開示すること。それ以外の目的のための収集に関しては、目的を開示し、ユーザに選択権（オプトイン）を提供すること。	●
21. ネットワークへの接続やバックエンドのサービスが利用不能または停止となった場合、どの機能がどの様に作動しなくなるのか（人・物に対する物理的なセキュリティへの潜在的な影響を含むが、それらに限定しない）について、開示すること。開示する情報には、機器がセキュリティ更新を受信しなくなった場合やユーザが機器のアップデートを怠った場合に、何が起こるのかを含むこと。（*潜在的な脅威を低減するため、機器の使用形態や安全性に応じて、製品の主要機能を維持しつつ、ネットワーク接続性やポートを無効化する機能を組み込むことを検討すること。*）	●
22. データ保有ポリシーおよび個人情報の保管期間を開示すること。	●
23. IoT 機器は、他の機器、プラットホーム、サービスとの間で初めてペアリング、無線接続、有線接続を行う際、ユーザに通知と承認要求の両方またはいずれかを行わなければならない。	●

出典：OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

表 B-5　OTA IoT Trust Framework（5/7）

IoT Trust Framework　● 必須　○ 推奨	
プライバシー、透明性と開示 （続き）	
24. IoT 機器／製品／サービスの所有権およびデータの移譲が可能か、移譲する場合どうすればよいかを、開示すること（例えば、スマートハウスの新しい所有者への売却や、フィットネス・トラッカーの売却など）。	●
25. 製品機能またはサービス運用に必要で、そのためだけに使用する場合を除き、第三者との個人情報の共有はユーザの積極的な同意が得られた場合のみとすること。第三者であるサービス提供者に対しても、共有したデータの機密保持、データの紛失／漏えいインシデントや不正アクセス発生時の通知要件を含め、同じポリシーの遵守を要求すること。	●
26.「工場出荷時の既定値」にリセットする機能を含めて、ユーザが IoT 機器のプライバシー設定を確認・編集できる機能とマニュアルの両方またはいずれかを提供すること。	●
27. データを収集した事業の売却または清算によるものでない限り、個人を特定可能なユーザ情報を売却または譲渡しないことを誓約すること。売却や精算の場合でも、当該事業を取得した相手のプライバシーポリシーが実質的に変わらないこと。もし変わる場合にはユーザに通知し、同意を得なければならない。	●
28. プライバシー保護に関する情報が購入前に明確に開示されていない場合、製品の利用にあたり提示されたプライバシー保護情報を確認した後で、ユーザが無料で返品できるようにすること。返品期間（日数）は、小売業者の現在の一般的な交換ポリシーと一致しているか、そうでなければ事前に提示しなければならない。	●
29. ポリシーを拒否またはオプトアウトする選択肢を提供する場合は常に、製品の機能や機能性への影響を含め、拒否またはオプトアウトの影響を明瞭かつ客観的に説明しなければならない。ユーザに対して、オプトインやデータを共有することによるユーザにとっての有用性を伝えることが推奨される。	●
30. 適用対象となる規制（COPPA: Children's Online Privacy Protection Act を含むがそれに限定しない）および国際的プライバシー、セキュリティ、データ転送に関する規制要件を満たすこと。[3] [4]	●
31. 最低でも過去 2 年間分のプライバシー通知に関する変更履歴を公開すること。ベストプラクティスとして、履歴には日付（タイムスタンプ）、変更点の朱書きによる明確化、変更による影響の概要を含めること等が挙げられる。	●

出典: OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

表 B-6　OTA IoT Trust Framework（6/7）

IoT Trust Framework　● 必須　○ 推奨	
通知と関連ベストプラクティス	
32. 機器の利用中止、紛失、売却に際して、ユーザまたは代理人が企業のサーバに保管された（購入履歴以外の）個人情報や機微な情報を削除または匿名化できる機能を提供すること。	○
33. 譲渡、レンタル、紛失または売却の際、ユーザデータを消去する機能を含め、機器およびアプリケーションを工場出荷時の状態にリセットする機能を提供すること。	○
34. エンドユーザによる通信（電子メールや SMS を含むが、これらに限定しない）は、スピアフィッシングや成りすましを防止するため、認証プロトコルを採用しなければならない。ドメインは、全てのセキュリティおよびプライバシーに関わる通信や通知について、SPF、DKIM、DMARC を実装することが望ましい。パークドメイン（parked domains）や電子メールを送信しないドメインについて、通知することが望ましい。[5]	●
35. 電子メール通信は、DMARC ポリシーの公開 180 日以内に、受信拒否または検疫ポリシーを履行すること。そうすることが、ISP や受信ネットワークが認証の検証に失敗した電子メールを拒否するのに役立つ。[6]	○
36. 電子メール通信を使用している IoT ベンダーは、通信の安全やメッセージのプライバシーおよび完全性の強化を支援するため、一般に認められたセキュリティ技術の利用を含め、トランスポートレベルでセキュリティ（機密性）を行うことが望ましい。（「SMTP における STARTTLS（Opportunistic TLS for email）」とも呼ばれる）[7]	○
37. 機器への物理的な細工の防止または検知に役立つ対策を実装すること。この様な対策は、設置後の機器の悪意の目的での筐体開封や改造、またはセキュリティが侵害された状態で販売店に返却されることを防止する助けとなる。	○
38. 視覚、聴覚、運動能力に障害のあるユーザに関するアクセシビリティをどう提供するか検討し、全てのユーザが最大のアクセシビリティを享受できる様にすること。	○
39. 潜在的なセキュリティやプライバシーに関する問題、サポート終了に関する通知、製品のリコールに関してユーザへ最大限周知するため、アプリケーション内での（アプリケーションを通した）通知を含め、ユーザへの通知手段を整備すること。通知内容は、一般的なユーザの読解力で最大限理解できる様に記述することが望ましい。ユーザにとって英語が「第 2 言語」であるかも知れないことを考慮し、多国語での通知を検討すること（セキュリティおよびメッセージの完全性に関しては、関連する原則を参照のこと）。	●

出典：OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

表 B-7　OTA IoT Trust Framework（7/7）

IoT Trust Framework　● 必須　○ 推奨	
通知と関連ベストプラクティス	
40. セキュリティ侵害が発生した場合の対応計画、およびユーザへの通知に関する計画について、少なくとも年 1 回、もしくは内部システム・技術・運用に重要な変更があった場合の両方またはいずれかにおいて、再評価・テスト（演習）・更新を行うこと。	●

用語、定義、明確化

1. スコープ　－「ウェアラブル技術を含む、家庭および企業において使用される消費者向け機器およびサービス」に重点を置く。自動運転車を含むスマートカー、医療機器および HIPPA（医療保険の相互運用性と説明責任に関する法律）法におけるデータ[8]は、本フレームワークの対象外である。しかしながら、大部分の要件は適用可能と考えられる。対象外としたものは、それぞれ米国家道路交通安全局（NHTSA）と米食品医薬品局（FDA）の規制対象に該当する。[9]

2. 機器メーカー、ベンダー、アプリケーション開発者、サービス提供者、プラットホーム・オペレータは、全て「企業」という言葉で表わしている。

【訳注】本注意書きは、フレームワーク全体に関わるものであり、上記に引用した表では「ベンダー」「サービス提供者」等の用語がそのまま使用されているケースもある。

3. 企業は、警察・司法機関と情報共有を行った場合はその旨を公表し、（法に抵触しない範囲で）適切な透明性に関するレポート（transparency report）へのリンクを含めることが期待される。

4. スマート機器とは、ネットワークに接続された機器（およびセンサー）を指し、一方向の通信のみを行うものも含む。

出典：OTA IoT Trust Framework® v2.5 - Updated 10/14/17[49] を基に作成

[1] https://otalliance.org/resources/always-ssl-aossl

[2] https://otalliance.org/blog/responsible-coordinated-ethical-vulnerability-disclosures

[3] 企業、製品およびサービスは、個人情報および機微な情報の収集・取扱いに関する当該法域の全ての法および規則（EU-US Privacy Shield Framework www.commerce.gov/privacyshield や EU General Data Protection Regulation (GDPR) www.eugdpr.org の厳守を含むが、これらに限定しない）に従わなければならない。従わない場合は本フレームワークに不準拠となる。

[4] COPPA https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[5] Email Authentication - https://otalliance.org/eauth

[6] DMARC - https://otalliance.org/resources/dmarc

[7] TLS for Email - https://otalliance.org/best-practices/transport-layered-security-tls-email

[8] 米国保険福祉省、ヘルスケア情報のプライバシー http://www.hhs.gov/hipaa/index.html

[9] http://www.nhtsa.gov/Vehicle+Safety および http://www.fda.gov/MedicalDevices/default.htm

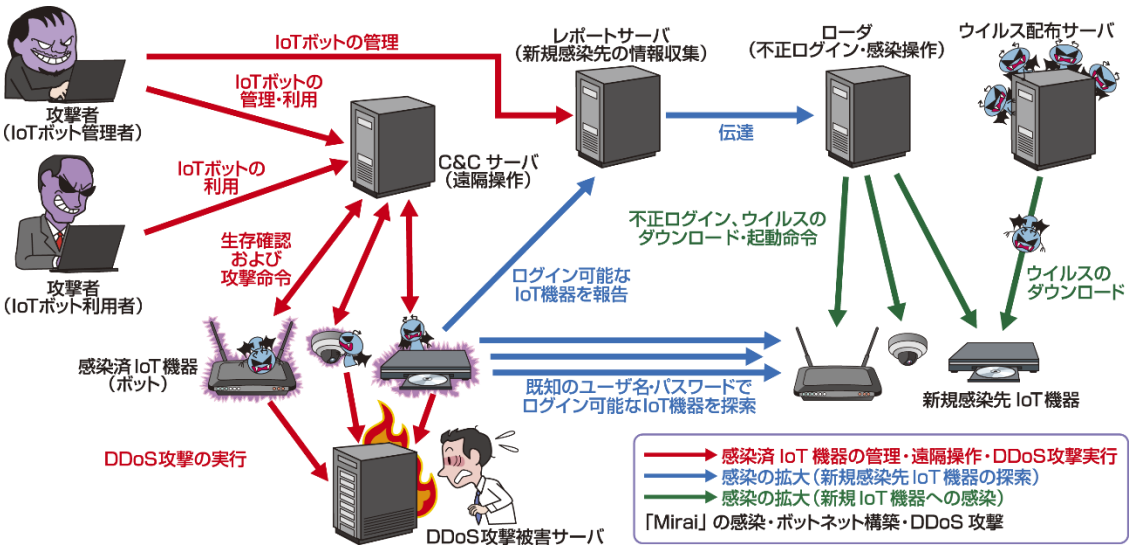
【コラム】

顕在化・多様化する IoT のセキュリティ脅威

本書の最初の版を公開した後、2016 年 9 月、ウイルス「Mirai」に感染した IoT 機器を踏み台とした大規模 DDoS 攻撃が発生し、セキュリティ設定・対策が不十分なままネットワークに接続された多数の IoT 機器の存在やセキュリティ対策の重要性を再認識することとなった。10 月には DNS サービス提供会社 Dyn に対して DDoS 攻撃が行われ、同社のサービスを利用する Twitter 等のサービスが一時利用不能となる等、第三者に多大な被害を与えることを示した。「Mirai」の脅威と対策の詳細に関しては、「情報セキュリティ 10 大脅威 2017」[16]を参照されたい。

2016 年 10 月には、「Mirai」が感染時に悪用する脆弱性（telnet の動作や初期値のままのパスワード等）と同様の脆弱性を攻撃して IoT 機器に感染するが、DDoS 攻撃に悪用せず、侵入口となるポートを遮断して他のウイルス感染を防ぐ「Hajime」が出現した。2017 年に入ると、感染した IoT 機器の設定変更、インターネット接続妨害、動作速度低下、機器上のファイル消去等の致命的な改変を行い、最終的に使用不能にする「BrickerBot」が出現し、セキュリティ設定・対策が不十分な IoT 機器のユーザ自身に被害が及ぶこととなった。「Mirai」や「Hajime」は IoT 機器の電源断によって消滅するが、脆弱性を放置した機器は、再起動後に同種または別のウイルスに感染するため、「Mirai」とその亜種（脆弱性を悪用してパスワードを初期値から変更した機器にも感染）、「Hajime」、「BrickerBot」による脆弱な IoT 機器を狙った陣取り合戦の様相を示している。

2016 年報告された事例では、ウイルスに感染する IoT 機器の大半は海外にあり、DDoS 攻撃の対象となるサーバも海外であったが、最近では、国内の IoT 機器への感染拡大や Mirai の亜種が狙う脆弱性を有する機器の国内流通が報告される等、対岸の火事ではなくなってきている。国内の対策だけでは解決しない問題ではあるが、IoT 機器のセキュリティ対策強化が強く望まれる。



付録 C.　IoT における暗号技術利用チェックリスト

IoT で採用した暗号技術の利用・運用方針を明確化し、安全性の評価を支援するチェックリストを示す。このチェックリストは、いくつかに分類された複数の評価項目から成る。各評価項目には、「必須」または「推奨」のセキュリティ要件を設定し、要件のもととなった国際標準・業界標準等の関連箇所を参照として記載した。また、各々の IoT における対応状況（各評価項目に対する判定とその根拠）を記入することで暗号技術に関する設計・運用状況を明確化し、第三者によって適切であるか否かを判定する際に利用することが出来る。

評価項目の設定に当たっては、米国政府機関である NIST（National Institute of Standards and Technology、アメリカ国立標準技術研究所）が定めた暗号鍵のガイドライン（NIST Special Publication 800-57, Recommendation for Key Management）[62]、スマートグリッドのセキュリティガイドライン（NISTIR 7628, Guidelines for Smart Grid Cybersecurity）[65]、CRYPTREC（Cryptography Research and Evaluation Committees）で定めた電子政府推奨暗号リスト[66]などの規定を参考に評価項目を設定した。

なお、IoT では小型機器において IT システムと同様の暗号を実装することが困難な場合を考慮し、IT システムに対して求められる要件よりは緩やかな目標を設定している。例えば、一般の IT システムであれば、CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された鍵長 128 ビット以上の共通鍵暗号を採用することが「必須」とされるべきである。本チェックリストでは、鍵長 128 ビット以上のみを「必須」とし、「電子政府推奨暗号リスト」に掲載されたアルゴリズムの採用は「推奨」に留め、達成条件を緩和している。可能であるならば、本チェックリストに示した「必須」のみならず、「推奨」を含む全ての要件を満たすことが望ましい。

IoT における暗号技術チェックリスト（1/5）

		暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照[59][61][62][63][64][65][66]	チェックリスト回答欄	
				判定	根拠（任意記入欄）
暗号アルゴリズムと鍵長					
	1	【暗号化アルゴリズム（共通鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された共通鍵暗号を採用することが望ましい。 〇共通鍵暗号としてブロック暗号を採用する場合、 CRYPTREC 暗号リストに掲載された暗号利用モードを採用することが望ましい。 ◎鍵長 128 ビット以上の暗号鍵を選択すること。	・NIST SP800-57 Part 1: 4.2.2, 5.6 ・NIST SP800-131A: 2 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	2	【電子署名アルゴリズム（公開鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された公開鍵暗号を採用することが望ましい。 ◎有限体上の離散対数問題または素因数分解問題に基づく公開鍵暗号の場合、鍵長 2048 ビット以上（西暦 2030 年まで） または鍵長 3072 ビット以上（西暦 2031 年以降）の暗号鍵を選択すること。 ◎楕円曲線上の離散対数問題に基づく公開鍵暗号の場合、鍵長 256 ビット以上の暗号鍵を選択すること。	・NIST SP800-57 Part 1: 4.2.4, 5.6 ・NIST SP800-131A: 3 ・NISTIR 7628: 4.1.2.2, 4.1.2.5, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	3	【鍵共有／鍵配送アルゴリズム（公開鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された公開鍵暗号を採用することが望ましい。 ◎有限体上の離散対数問題または素因数分解問題に基づく公開鍵暗号の場合、鍵長 2048 ビット以上（西暦 2030 年まで） または鍵長 3072 ビット以上（西暦 2031 年以降）の暗号鍵を選択すること。 ◎楕円曲線上の離散対数問題に基づく公開鍵暗号の場合、鍵長 256 ビット以上の暗号鍵を選択すること。	・NIST SP800-57 Part 1: 4.2.5, 5.6 ・NIST SP800-131A: 5, 6 ・NISTIR 7628: 4.1.2.2, 4.1.2.5, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	4	【鍵ラッピングアルゴリズム（共通鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された共通鍵暗号を採用することが望ましい。 ◎鍵長 128 ビット以上の暗号鍵を選択すること。	・NIST SP800-57 Part 1: 4.2.5.4, 5.6 ・NIST SP800-131A: 7 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	5	【鍵生成（導出）アルゴリズムを使用している場合】 ◎安全なアルゴリズムを選択すること。 〇内部で他のアルゴリズムを使用している場合、 CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたアルゴリズムを採用することが望ましい。 ◎共通鍵暗号ベースの場合、鍵長 128 ビット以上の暗号鍵を選択すること。	・NIST SP800-131A: 8 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	6	【ハッシュアルゴリズムを使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたハッシュ関数を採用することが望ましい。	・NIST SP800-57 Part 1: 4.2.1 ・NIST SP800-131A: 9 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	7	【メッセージ認証アルゴリズム（メッセージ認証コード）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたメッセージ認証コードを採用することが望ましい。 ◎鍵付きハッシュベースの場合、セキュリティ強度（共通鍵換算の鍵長）128 ビット以上の暗号鍵を選択すること。 ◎共通鍵暗号ベースの場合、鍵長 128 ビット以上の暗号鍵を選択すること。	・NIST SP800-57 Part 1: 4.2.3, 5.6 ・NIST SP800-131A: 10 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・CRYPTREC 暗号リスト		
	8	【乱数生成アルゴリズムを使用している場合】 ◎安全なアルゴリズムを選択すること。 〇内部で他のアルゴリズムを使用している場合、 CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたアルゴリズムを採用することが望ましい。	・NIST SP800-57 Part 1: 4.2.7 ・NIST SP800-90A ・NIST SP800-131A: 4 ・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.4, 4.2.1.7 ・CRYPTREC 暗号リスト		

IoT における暗号技術チェックリスト（2/5）

		暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照[59][61][62][63][64][65][66]	チェックリスト回答欄	
				判定	根拠（任意記入欄）
鍵の生成					
	9	【共通鍵暗号（共通鍵）を使用している場合】 ◎安全な方法を用いて、鍵を生成すること。 〇共通鍵は、以下のいずれかの方法で生成することが望ましい。 （1） ローカル（鍵を使用する機器内）で、以下のいずれかの方法で生成する。 ・機器配布前に疑似乱数生成アルゴリズムに初期 seed を設定し、稼働中の不確定要素を用いて seed を更新して鍵生成する。 ・機器内に事前設定済みの長期鍵から、鍵生成関数（KDF: Key Derivation Function）を用いて鍵生成する。 （2） リモート（同一の鍵を使用する他の機器や信頼できる第三者（例：鍵サーバ））において生成した鍵を受け取る。 〇共通鍵は、過去に生成した鍵と重複しないことを確認した上で生成することが望ましい。	・NISTIR 7628: 4.2.1.2, 4.2.2.3		
	10	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎安全な方法を用いて、鍵ペアを生成すること。 〇耐タンパー性を有する H/W（例：HSM、暗号専用回路を持つ IC）の内部にて鍵ペアを生成することが望ましい。	・NISTIR 7628: 4.1.2.4.2		
鍵の配布					
	11	【共通鍵暗号（共通鍵）を使用している場合】 ◎共通鍵は、完全性および機密性を満たす条件の下で配布すること。 〇鍵の配布に用いるメカニズム（例：暗号アルゴリズム）は、少なくとも鍵と同等の強度を持っていることが望ましい。	・NIST SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.2.2.3, 4.3.3.3		
	12	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎公開鍵は完全性を、秘密鍵は完全性および機密性を満たす条件の下で配布すること。 〇鍵の配布に用いるメカニズム（例：暗号アルゴリズム）は、少なくとも鍵と同等の強度を持っていることが望ましい。	・NIST SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.3.3.3		
鍵の保管					
	13	【共通鍵暗号（共通鍵）を使用している場合】 ◎共通鍵は、完全性および機密性を満たす条件の下で保管すること。 〇永続的に利用する共通鍵は、耐タンパー性を有する H/W（例：暗号専用回路を持つ IC）の内部で保管することが望ましい。	・NIST SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.2.2.3, 4.3.3.3		
	14	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎公開鍵は完全性を、秘密鍵は完全性および機密性を満たす条件の下で保管すること。 〇秘密鍵は、耐タンパー性を有する H/W（例：HSM、暗号専用回路を持つ IC）の内部で保管することが望ましい。	・NIST SP800-57 Part 1: 6.1.1 ・NISTIR 7628: 4.1.2.4.2, 4.3.3.3		
鍵の用途					
	15	〇一つの鍵は、単一の用途（例：暗号化、認証、鍵ラッピング、乱数生成、電子署名）で利用することが望ましい。 ・単一の暗号鍵の暗号処理が同時に複数の機能を実現する場合（例：署名と認証、暗号化と認証）を除く。 ・鍵共有／鍵配送用途の公開鍵／秘密鍵ペアに対する公開鍵証明書発行要求のための電子署名を除く。	・NIST SP800-57 Part1: 5.2		
鍵の一意性					
	16	【共通鍵暗号（共通鍵）を使用している場合】 ◎同報通信に利用する場合を除き、暗号化通信する一対の機器毎に一意の共通鍵を使用すること（三台以上の機器で共通鍵を共用しないこと）。	・NISTIR 7628: 4.1.3, 4.3.3.3		
	17	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎機器毎に一意の公開鍵ペアを使用すること（二台以上の機器で秘密鍵を共用しないこと）。	・NISTIR 7628: 4.1.3, 4.3.3.3		

IoT における暗号技術チェックリスト（3/5）

暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）		参照[59][60][61][62][63][64][65][66]	チェックリスト回答欄	
			判定	根拠（任意記入欄）
鍵関連情報（パラメータ）				
18	【楕円曲線暗号アルゴリズムを使用している場合】 ◎安全なドメインパラメータを使用すること。 ◎ドメインパラメータは、完全性を満たす条件の下で配布・保管すること。	・NIST SP800-57 Part 1: 6.1.2 ・NISTIR 7628: 4.1.2.5		
19	【ブロック暗号を使用している場合】 ◎ブロック暗号は、適切な利用モード（CBC モード、CTR モード等）を選択した上で利用すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された利用モードを採用することが望ましい。	・NIST SP800-57 Part1: 4.1.2.2, 4.2.2.3 ・CRYPTREC 暗号リスト		
20	【ブロック暗号の CBC モード、CFB モード、OFB モードを使用している場合】 ◎CBC モード、CFB モードにおける初期化ベクタ（IV）は、予測不能性を満たすこと。 ◎OFB モードにおける初期化ベクタ（IV）は、一意の（互いに異なる）値を使用すること。 ◎初期化ベクタ（IV）は、完全性を満たす条件の下で配布・保管すること。	・NIST SP800-57 Part 1: 6.1.2 ・NIST SP800-38A: 5.3, Appendix C		
21	【ブロック暗号の CTR モードを使用している場合】 ◎同一の共通鍵で使用される全てのカウンタが互いに異なること（同一の共通鍵で同じカウンタを再使用しないこと）。	・NIST SP800-38A: 6.5, Appendix B		
22	【ブロック暗号の CCM モードを使用している場合】 ◎同一の共通鍵で使用される全ての Nonce が互いに異なること（同一の共通鍵で同じ Nonce を再使用しないこと）。	・NIST SP800-38C: 5.3		
23	【ブロック暗号の GCM モード、GMAC モードを使用している場合】 ◎初期化ベクタ（IV）は、一意の（互いに異なる）値を使用すること。 ◎初期化ベクタ（IV）は、完全性を満たす条件の下で配布・保管すること。	・NIST SP800-57 Part 1: 6.1.2 ・NIST SP800-38D: 5.2.1.1, 8.2, 9, Appendix A		
24	【共有秘密情報（Shared Secrets）を使用している場合】 ◎共有秘密情報は、完全性および機密性を満たす条件の下で配布・保管すること。 ◎使用の終了した共有秘密情報は、速やかに廃棄すること。	・NIST SP800-57 Part 1: 6.1.2		
25	【乱数生成用 seed を使用している場合】 ◎乱数生成用 seed は、十分なエントロピーを持った値を使用すること。 ◎乱数生成用 seed は、完全性および機密性を満たす条件の下で配布・保管すること。 ◎一回使用した乱数生成用 seed は、速やかに廃棄すること。	・NIST SP800-57 Part 1: 6.1.2 ・NISTIR 7628: 4.1.2.1, 4.2.1.2, 4.2.1.4		

IoT における暗号技術チェックリスト（4/5）

	暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照[59][60][61][62][63][64][65][66]	チェックリスト回答欄	
			判定	根拠（任意記入欄）
鍵の更新				
26	【データ暗号化用途の共通鍵（共通鍵暗号）を使用している場合】 ◎データ暗号化用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇データ暗号化用途の共通鍵は、高頻度に利用する場合、1 日～1 週間以内に更新することが望ましい。 〇データ暗号化用途の共通鍵は、中頻度に利用する場合、1 ヶ月以内に更新することが望ましい。 〇データ暗号化用途の共通鍵は、低頻度に利用する場合、2 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.2.2.3, 4.3.3.3		
27	【認証用途の共通鍵（共通鍵暗号）を使用している場合】 ◎認証用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇認証用途の共通鍵は、2 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
28	【鍵ラッピング用途の共通鍵（共通鍵暗号）を使用している場合】 ◎鍵ラッピング用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇鍵ラッピング用途の共通鍵は、高頻度に利用する場合、1 日～1 週間以内に更新することが望ましい。 〇鍵ラッピング用途の共通鍵は、中頻度に利用する場合、1 ヶ月以内に更新することが望ましい。 〇鍵ラッピング用途の共通鍵は、低頻度に利用する場合、2 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
29	【マスター鍵用途の共通鍵（共通鍵暗号）を使用している場合】 ◎マスター鍵用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇マスター鍵用途の共通鍵は、少なくとも 1 年毎に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
30	【乱数生成用途の共通鍵（共通鍵暗号）または公開鍵／秘密鍵ペア（公開鍵暗号）を使用している場合】 ◎乱数生成用途の共通鍵・公開鍵／秘密鍵ペアは、適切な利用期間を経過した後、鍵ペアを更新すること。 〇乱数生成アルゴリズムが鍵の更新について規定している場合は、それに従うことが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
31	【電子署名用途の公開鍵／秘密鍵ペア（公開鍵暗号）を使用している場合】 ◎電子署名用途の公開鍵／秘密鍵ペアは、適切な利用期間を経過した後、鍵ペアを更新すること。 〇電子署名用途の公開鍵／秘密鍵ペアは、1 年～3 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
32	【認証用途の公開鍵／秘密鍵ペア（公開鍵暗号）を使用している場合】 ◎認証用途の公開鍵／秘密鍵ペアは、適切な利用期間を経過した後、鍵ペアを更新すること。 〇認証用途の公開鍵／秘密鍵ペアは、1 年～2 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
33	【鍵共有用途の静的（永続的）な秘密鍵／公開鍵ペア（公開鍵暗号）を使用している場合】 ◎鍵共有用途の静的な秘密鍵／公開鍵は、適切な利用期間を経過した後、鍵ペアを更新すること。 〇鍵共有用途の静的な秘密鍵／公開鍵は、1 年～2 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
34	【鍵共有用途の一時的な秘密鍵／公開鍵ペア（公開鍵暗号）を使用している場合】 ◎鍵共有用途の一時的な秘密鍵／公開鍵は、一回利用する度に、鍵ペアを更新すること。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
35	【鍵配送用途の秘密鍵／公開鍵ペア（公開鍵暗号）を使用している場合】 ◎鍵配送用途の秘密鍵／公開鍵は、適切な利用期間を経過した後、鍵ペアを更新すること。 〇鍵配送用途の秘密鍵／公開鍵は、2 年以内に更新することが望ましい。	・NIST SP800-57 Part1: 5.3 ・NISTIR 7628: 4.3.3.3		
36	◎鍵の漏えいが発覚した場合、速やかに鍵を更新すること。	・NIST SP800-57 Part1: 8.2.3		
37	〇同一の共通鍵を用いて暗号化を行う回数には、制限を設けることが望ましい。 〇適切な利用回数を経過した後、鍵を更新することが望ましい。	・NIST SP800-57 Part1: 8.2.3 ・NISTIR 7628: 4.2.2.3		
38	◎鍵の更新は、以下のいずれかの方法を用いて、安全に行うこと。 ・古い鍵には依存しない形で新しい鍵を生成する（Re-keying）。 ・古い鍵に依存する形で新しい鍵を生成する（Key Update）。この場合、新しい鍵から古い鍵を類推不可能なこと。	・NIST SP800-57 Part1: 8.2.3		

IoT における暗号技術チェックリスト（5/5）

暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照[59][60][61][62][63][64][65][66]	チェックリスト回答欄	
				判定	根拠（任意記入欄）
鍵の廃棄					
	39	◎不要となった鍵は、安全に廃棄すること。 〇不要となった鍵（共通鍵暗号の共通鍵、公開鍵暗号の秘密鍵）は、その時点で速やかに削除することが望ましい。	・NIST SP800-57 Part1: 8.4 ・NISTIR 7628: 4.3.3.3		
	40	◎運用期間中に継続使用する鍵について、運用終了後の安全な廃棄計画を立てておくこと。 〇運用期間中に継続使用する鍵は、運用期間終了後、速やかに削除することが望ましい。	・NIST SP800-57 Part1: 8.4		
危殆化対策					
	41	暗号アルゴリズムや鍵長の危殆化（想定を上回る安全性の低下）に備えて、 ◎暗号アルゴリズムの入れ替えや鍵長の延長を考慮しておくこと。 〇予備の暗号アルゴリズムを実装しておくことが望ましい。	・NISTIR 7628: 4.2.1.3		

【注】 参照において、「CRYPTREC 推奨暗号リスト」とは、CRYPTREC が公開する「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（平成 29 年 3 月 30 日版）を指す。
http://www.cryptrec.go.jp/images/cryptrec-ls-0001-2016.pdf
今後、同リストが改定された場合、推奨される暗号アルゴリズムやモードは変更される可能性を考慮する必要がある。
例えば、設計・開発時に採用した暗号がリストから削除された場合は、別の推奨暗号へ移行することが望ましい。
このため、暗号アルゴリズムの入れ替えや鍵長の延長を考慮しておくことが必須要件である（項番 41 参照）。

付録 D.　「つながる世界の開発指針」と本書の対応

IPA が先行して公開している「つながる世界の開発方針」[12]の 17 指針における分析、設計、保守、運用の開発ライフサイクルの各指針（指針 4～指針 17）と本書における具体的な分析事例での各記載項目との対応を示す。

表 D-1　「つながる世界の開発指針」との対応表

「つながる世界の開発指針」			本書（「IoT 開発におけるセキュリティ設計の手引き」）の対応箇所	
分析	指針 4	守るべきものを特定する	5.1.～5.4.	実施例として、システム構成を整理し、図 5-1～図 5-4 にて各構成要素や機微な情報の所在を明確化。
	指針 5	つながることによるリスクを想定する	3.1.	実施方法の例として、接続があると判明した箇所に対する脅威分析を説明。
			3.2.	実施方法の例として、接続点において発生すると考えられる脅威に対する対策検討を説明。
			5.1.～5.4.	実施例として、システム構成を整理し、図 5-1～図 5-4 にて接続の有無を明確化。
			5.1.～5.4.	実施例として、図 5-1～5-4、表 5-1～表 5-12 にて接続点において発生する脅威と対策を明確化。
	指針 6	つながりで波及するリスクを想定する	（同上）	指針 5 と同一（接続する機器が攻撃の入口・脅威の糸口となるか否か、分析・検討する）。
	指針 7	物理的なリスクを認識する	3.1.	脅威分析において、物理的なリスクも検討対象とする。但し、3.1.では物理的リスクに該当する例はない。
			3.2.	物理的リスクによって生じると考えらえる脅威に対して、対策を検討する。
			5.1.～5.4.	実施例として、図 5-1～5-4、表 5-1～表 5-12 にて物理的リスクに起因する脅威と対策を明確化。
設計	指針 8	個々でも全体でも守れる設計をする	2.	IoT 構成要素の定義・説明（2.5.）にて、機器によっては他の機器と連携して防御する可能性について示唆。
			3.2.	実施方法の例として、①外部インタフェース経由および③物理的接触によるリスクによって生じる脅威に対する対策検討を説明。
			3.3.	実施方法の例として、②内包リスクによって生じる脅威に対する対策検討（脆弱性対策）を説明。
			5.1.～5.4.	実施例として、図 5-1～5-4、表 5-1～表 5-12 にて各リスクに起因する脅威と対策を明確化。
			付録 C.	セキュリティ対策の根幹となる暗号技術の安全性を確認するチェックリストを提供。
	指針 9	つながる相手に迷惑をかけない設計をする	-	異常発生が攻撃に起因する場合は、他の脅威同様に扱う。不十分な安全性に起因する場合は、本書の対象外。
	指針 10	安全安心を実現する設計の整合性をとる	n/a	セキュリティ上の脅威がセーフティに与える影響については、本書の対象外。
	指針 11	不特定の相手とつなげられても安全安心を確保できる設計をする	3.1.	脅威分析において、想定外の相手と接続するリスクも検討対象とする。
			3.2.	想定外の相手と接続するリスクによって生じると考えらえる脅威に対して、対策を検討する。
			5.1.～5.4.	実施例として、図 5-1～5-4、表 5-1～表 5-12 にて想定外接続リスクに起因する脅威と対策を明確化。
			付録 C.	接続相手を確認する際の認証において用いる暗号技術の安全性を確認するチェックリストを提供。
	指針 12	安全安心を実現する設計の検証・評価を行う	n/a	セキュリティ対策の検証・認証については、本書の対象外。
保守	指針 13	自身がどのような状態かを把握し、記録する機能を設ける	n/a	本書で例とした小型機器では、ログ記録・分析は困難と思われるため、対策例として示していない。
	指針 14	時間が経っても安全安心を維持する機能を設ける	3.2.	実施方法の例として、更新ソフトウェアに対する署名（改ざん防止）等について説明。
			3.3.	実施方法の例として、脆弱性対策（ソフトウェア更新機能の実装と更新の提供等）について説明。
			5.1.～5.4.	実施例として、図 5-1～5-4、表 5-1～表 5-12 にて更新ソフトウェア配布に対する脅威と対策を明確化。
			付録 C.	暗号技術の利用チェックリストにおいて、暗号技術の危殆化に関する対策の事前実装有無を確認。
運用	指針 15	出荷後も IoT リスクを把握し、情報発信する	3.3.2.	運用段階における脆弱性対策（脆弱性対策情報の公開、更新ソフトウェアの提供等）について説明。
	指針 16	出荷後の関係事業者に守ってもらいたいことを伝える	3.2	実施方法の例として、出荷後の対策について説明。関係者への周知徹底は、本書の対象外。
			5.1.～5.4.	実施例として、図 5-1～5-4、表 5-1～表 5-12 にて脅威と対策を明確化。
	指針 17	つながることによるリスクを一般利用者に知ってもらう	3.2.	実施方法の例として、表 3-7 にて対策「説明書周知徹底」を記載。
			5.1.	実施例として、図 5-1・表 5-1～5-2 にて対策「説明書周知徹底」を記載。

更新履歴

2016 年 5 月 12 日	初版
2016 年 6 月 6 日	CRYPTREC 暗号リストの更新（2016 年 5 月 16 日）に伴う同リストへの参照更新、その他の誤字修正
2016 年 8 月 1 日	OTA IoT Trust Framework の更新（2016 年 7 月 12 日）の反映、その他の誤字修正
2016 年 12 月 28 日	IoT 構成要素の定義修正、セキュリティ設計手順の記載箇所移動、脅威分析と対策検討の実施例における主要脅威・対策の記述修正、OWASP Internet of Things Project のプロジェクト構成変更（2016 年 8 月 10 日）の反映、OTA IoT Trust Framework の更新（2016 年 9 月 21 日）の反映、その他の誤字修正
2017 年 12 月 15 日	国内外で公開された IoT 関連のセキュリティガイドライン等の表追加、OWASP Internet of Things Project のプロジェクト構成変更（2017 年 8 月 19 日）の反映と IoT Vulnerabilities の追加、OTA IoT Trust Framework の更新（2017 年 10 月 14 日）の反映、GSMA Security Guidelines の更新（2017 年 10 月 31 日）の反映、コラムの追加、参考文献の追加・修正、その他の誤字修正
2018 年 4 月 2 日	IPA が提供する脆弱性対策コンテンツの更新、国内外で公開された IoT 関連のセキュリティガイドライン等の表の更新、暗号技術利用チェックリストの更新、コラムの修正

本手引きは、以下の URL からダウンロード可能です。
https://www.ipa.go.jp/security/iot/iotguide.html

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート センターオフィス
TEL: 03-5978-7527　FAX: 03-5978-7552
https://www.ipa.go.jp/security/