消費者向け IoT 製品のセキュリティに関する行動規範

タイトル

消費者向け IoT 製品のセキュリティに関する行動規範

日付

2018 年 10 月

概要

私たちの身のまわりには、インターネットに接続するデバイスが増加しています。それに伴い、これまでオフラインで利用していた製品や家電の「モノのインターネット（IoT）」化も進んでいます。

IoTは、新しい時代の象徴です。テクノロジが人々の暮らしの一部となり、より便利でより楽しい生活を実現します。多くの個人データがオンライン上のデバイスやサービスに保存されている今、こうした製品に対するサイバーセキュリティ対策は、自宅の防犯強化と同じくらい重要なものになっています。

本行動規範は、消費者向け IoT 製品の設計段階で安全性が確保されるように、またユーザーがデジタルの世界を安心して楽しめるようにガイドラインを設けることで、こうした製品の開発、製造、販売に携わる利害関係者を支援することを目的として作成されています。

本行動規範は、IoT のセキュリティにおけるベストプラクティスを、成果に焦点を当てた 13 項目のガイドラインにまとめたものです。本行動規範は、デジタル・文化・メディア・スポーツ省（DCMS）が、国家サイバーセキュリティセンター（NCSC）と協力し、産業界、消費者団体、学界とも連携して作成しました。本行動規範の草案は、2018 年 3 月に、Secure by Design 報告書の中で発表されました。[1]

はじめに

モノのインターネット（IoT）は、人々に大きなチャンスをもたらします。しかし、市場に出回っているデバイスのほとんどについて、基本的なセキュリティ対策が施されているとはいえない状況です。インターネット接続を利

[1] DCMS、2018 年、「Secure by Design: Improving the cyber security of consumer Internet of Things: Report（セキュリティバイデザイン：消費者向け IoT 製品のサイバーセキュリティの強化）」 https://www.gov.uk/government/publications/secure-by-design

用したテクノロジーのメリットを安全に享受できるよう、十分なセキュリティ対策とプライバシー対策で、オンラインの活動を保護する必要があります。

本行動規範では、IoT 製品のメーカーやその他の利害関係者を対象に、消費者向け IoT 製品と関連サービスのセキュリティ強化に向けた実践的な対策をまとめています。この 13 項目を実践することは、消費者のプライバシーと安全を守ると共に、IoT 製品を消費者がより簡単に安心して使えるようにすることにも貢献します。また、セキュリティ対策が不足している IoT デバイスやサービスを悪用する DDoS 攻撃（分散型サービス妨害）の脅威も低減できます。

本ガイドラインは、IoT セキュリティにおけるベストプラクティスをまとめたものです。これらのガイドラインは規範的なものではなく、成果に重点を置いており、各事業者が自社の製品に合ったセキュリティ対策を新たに考案し実践できるよう、柔軟性も持たせてあります。

本行動規範は、セキュリティに関するあらゆる問題を解決できる特効薬ではありません。安全な IoT を実現するためには、各企業がセキュリティを中心に据えた考え方に切り替え、安全な開発ライフサイクルに投資することが不可欠です。製品やサービスは、製品開発の段階からライフサイクル全般を通して、セキュリティを考慮して設計する必要があります。さらに、自社の製品やサービスに関連するサイバーセキュリティのリスクを定期的に評価し、適切な対策を取らなくてはなりません。

IoT 製品のサプライチェーンは、複数のコンポーネントメーカーやサービス提供事業者などが含まれることが多いため、世界規模の複雑な構造になりがちです。本行動規範を提供するねらいは、こうしたサプライチェーン全体において、セキュリティに関する変革を積極的に推し進められるようにすることです。

さまざまな業界団体や国際フォーラムが、IoT セキュリティの推奨事項や標準を策定しています。[2]本行動規範は、こうした取り組みや関連するサイバーセキュリティ標準を補完、支援することを目的としています。消費者向け IoT 製品に関連する今後の保証制度や信頼性評価認定制度に本行動規範が反映されるよう、産業界と直接連携しながら策定を進めました。

本行動規範の実施は、既存のデータ保護法を遵守することにつながる場合もあります。例えば、個人データの安全な取り扱いを定めた EU 一般データ保護規則（GDPR）などです。[3]

---

[2] PETRAS、2018 年、「Summary literature review of industry recommendations and international developments on IoT security（IoT セキュリティに関する業界推奨と国際的な開発動向の文献要約）」 https://www.gov.uk/government/publications/secure-by-design

[3] GDPR 第 5 条（1）（f）は、個人データの「完全性と機密性」について定めています。

本行動規範の実施

本行動規範には、その各ガイドラインと主な業界標準、推奨事項、指針との関連性を示す補足資料が用意されています。[4]この資料では 13 項目のガイドラインの背景説明も提供されており、各項目を実施する際に役立ちます。さらに、本行動規範と多くのグローバル企業が取り入れている IoT セキュリティ対策との関係性も確認できます。

優先項目と本書の構成

初期設定パスワード、脆弱性に関する情報の公開、セキュリティアップデートに関する対策を取り入れると、セキュリティ上、特に大きな効果が短期間で期待できるため、最初の 3 項目に高い優先度が設定されています。

補足説明では各項目の実施理由と詳細を解説しています。また、本書末尾にある注記では、よくある質問と回答を紹介しています。

対象読者

各項目では、主な実施担当者となる利害関係者を示しています。利害関係者の定義は、下表を参考にしてください。

デバイスメーカー	組立が完了したインターネット接続型の最終製品を製造する企業。完成品には、さまざまな他社製品が含まれる場合がある。
IoT サービス提供事業者	IoT ソリューションの一部として、ネットワークやクラウドストレージ、データ移管などのサービスを提供する企業。インターネット接続型デバイスの提供が、サービスに含まれることがある。

[4] DCMS、2018 年、「Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security（IoT セキュリティの推奨事項、方針、標準と消費者向け IoT 製品のセキュリティに関する行動規範との関連性）」https://www.gov.uk/government/publications/secure-by-design

モバイルアプリケーション開発事業者	モバイルデバイスで動作するアプリケーションの開発、提供を行う企業。こうしたアプリケーションは、デバイスとの通信手段として、IoT ソリューションに含まれることが多い。
小売業者	インターネット接続型の製品や関連サービスを消費者に販売する業者。

用語に関する留意点

「セキュリティ上重要なデータ」という用語は、GDPR で定義されている特定カテゴリのデータ（正式には「重要な個人データ」と呼ばれるもの）など、他の機密データと区別するために使用します。セキュリティ上重要なデータには、暗号化された初期化ベクトルなどがあります。

本書では「消費者」という表現に統一していますが、ここで「消費者」とは、IoT 製品やサービスのエンドユーザー一般を指しています。

本行動規範の適用範囲

本行動規範は、インターネットやホームネットワーク（両方またはその一方）と関連サービスに接続する消費者向け IoT 製品に適用されます。以下がその例です（これらに限定されるものではありません）。

- インターネット接続型の玩具やベビーモニター
- 煙感知器やドアロックなど、インターネット接続型の防犯/防災関連製品
- スマートカメラ、スマートテレビ、スマートスピーカー
- ウェアラブル健康管理製品
- インターネット接続型のホームオートメーションシステムや警報システム
- インターネット接続型の家電（洗濯機や冷蔵庫など）
- スマートホームアシスタント

本書では、IoT デバイスに接続しているデジタルサービスをまとめて関連サービスと呼びます。モバイルアプリケーション、クラウドコンピューティング/ストレージ、メッセージサービス向けサードパーティ製 API などがこれに該当します。

レビュー

デジタル・文化・メディア・スポーツ省は、少なくとも 2 年おきに本行動規範を見直し、最新版を公開します。最新の情報については、securebydesign@culture.gov.uk にお問い合わせください。

ガイドライン

1) 初期パスワードを設定しない

IoT デバイスにはすべて個別のパスワードを設定します。また、工場出荷時の汎用的な初期値にリセットできないようにします。

IoT デバイスの多くは、汎用的なユーザー名とパスワード（「admin、admin」など）が初期設定された状態で販売されており、消費者が設定を変更することになっています。しかし、IoT 製品ではこうした設定がセキュリティ関連の問題の温床になっているため、その使用を廃止する必要があります。パスワードやその他の認証方法に関するベストプラクティスに従ってください。[5]

主な実施担当者：デバイスメーカー

2) 脆弱性に関する情報の公開方針を導入する

インターネットに接続するデバイスやサービスを提供する企業は、脆弱性情報の公開方針の一環として、セキュリティ調査官などが問題を報告するための連絡窓口を提示するものとします。公開された脆弱性に対して速やかに対策を取るようにしてください。

セキュリティ上の脆弱性を把握することで、各企業の対応が可能になります。また企業は、製品のセキュリティライフサイクルの一環として、自社の製品やサービスに潜むセキュリティ上の脆弱性を継続的に監視し、脆弱性を発見、是正する必要があります。脆弱性については、第一に、影響を受ける利害関係者に直接報告しなければなりません。利害関係者に直接報告できない場合は、その問題を政府機関に報告することが可能です。[6]状況に応じたアプローチについては、末尾の注記で詳細を確認してください。企業は、管轄権を有する業界団体に情報を共有するようにしてください。[7]

---

[5] 次の指針を参考にしてください。NCSC、2016 年、「Password Guidance: Simplifying Your Approach（パスワードに関する指針：アプローチの簡略化）」https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approachNIST、2017 年、「NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management（NIST 特別刊行 800-63B：デジタル ID に関する指針 - 認証とライフサイクル管理）」https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

[6] 英国では、脆弱性に関する報告をこちらに送ることができます：https://www.ncsc.gov.uk/contact

[7] 管轄権を有する業界団体には、GSMA や IoT セキュリティ財団などがあります。脆弱性情報の公開に関する ISO/IEC 29147 標準を参考に作成された「Guidance on Coordinated Vulnerability Disclosure（協調的な

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

3) ソフトウェアを定期的に更新する

インターネット接続型デバイスのソフトウェアコンポーネントは、安全な方法で更新できなければなりません。更新は適切なタイミングで行うものとし、デバイスの機能に影響を及ぼさないようにします。エンドポイントのデバイスについて製品寿命に関する方針を公開するものとします。デバイスのソフトウェアにアップデートを提供する最短の期間と、サポート期間の設定理由を明示してください。更新が必要な場合はその都度、消費者に明確に通知すると共に、消費者が簡単に更新できるようにします。制約があり、物理的に更新できないデバイスについては、製品を分離可能および交換可能にする必要があります。

セキュリティパッチの提供元の安全性も保証する必要があります。配信は安全なチャネルを通じて行います。更新中も、可能な限りデバイスの基本機能を使えるようにしてください。例えば、時計であれば時間を表示し、サーモスタットであれば温度の自動調節を継続し、鍵であれば開閉できる状態が続くようにします。こうした対策は設計段階において考慮すべき点ですが、適切な検討や管理がなされていない場合、デバイスやシステムの種類によっては重大な安全上の問題を引き起こすものもあります。

ソフトウェアアップデートは、デバイス販売後に提供するものとし、デバイスごとに適切なタイミングで配信します。ソフトウェアアップデートのサポート期間は、製品購入時に消費者に明確に提示するものとします。小売業者およびメーカー、またはそのいずれかが、更新の必要性を消費者に通知する必要があります。制約があり、ソフトウェアの更新ができないデバイスについては、交換サポートの適用条件と対象期間を明確に提示してください。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

4) 認証情報とセキュリティ上重要なデータを安全に保存する

認証情報はすべて、サービスやデバイス内に安全な形で保存するものとします。デバイスのソフトウェアに認証情報をハードコード化することは認められません。

脆弱性の公開に関する指針）」は、IoT セキュリティ財団から取得できます。GSMA による業界別の「協調的な脆弱性の公開」プログラムはこちらを参照してください：https://www.gsma.com/cvd

ソフトウェアにハードコード化されたユーザー名やパスワードなどの認証情報は、デバイスやアプリケーションのリバースエンジニアリングを通して簡単に発見できます。ハードコード化された情報を、単純な手法で難読化したり暗号化したりしたものも、容易に解読されます。安全に保存すべきセキュリティ上重要なデータとは、暗号鍵、デバイスの識別情報、初期化ベクトルなどを指します。TEE（Trusted Execution Environment）や関連ストレージが提供する、安全性と信頼性に優れたストレージ構造を活用してください。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

5) 安全に通信する

リモート管理やリモート制御を含め、セキュリティ上重要なデータは、テクノロジやその使用方法の属性に応じて暗号化して転送する必要があります。鍵はすべて安全に管理する必要があります。

同業者によるレビューが受けられるオープンなインターネット規格を採用することが強く推奨されます。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

6) 攻撃対象になる場所を最小限に抑える

すべてのデバイスとサービスは、「最小権限の原則」に則って運用します。未使用のポートは閉じ、ハードウェアへの不要なアクセスを認めず、サービスが利用されていない場合は提供をやめ、サービス運用に必要な機能に絞り込んでコードを作成するようにしてください。ソフトウェアは、セキュリティと機能の両方を考慮し、適切な権限だけを提供して運用します。

最小権限の原則は、優れたセキュリティエンジニアリングの基本原理であり、他のアプリケーションと同様、IoT にも適用できます。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者

7) ソフトウェアの整合性を確認する

IoT デバイスのソフトウェアは、安全な起動メカニズムで検証する必要があります。未承認の変更が検出された場合は、デバイスから消費者/管理者に対して問題を知らせる警告を発するようにし、警告の発信に必要なネットワーク以外には接続しないようにしてください。

こうした状況から遠隔操作で復旧するには、たとえば、既知の正常なバージョンをローカルに保存し、安全な復旧とデバイスの更新に備えるなど、既知の正常な状態を確保しておく必要があります。こうすることで、サービス妨害、コストのかかるリコール、出張メンテナンスを回避しながら、攻撃者がデバイスを乗っ取って更新やその他のネットワーク通信機構を破壊するリスクを管理できます。

主な実施担当者：デバイスメーカー

8）個人データの保護を徹底する

デバイスまたはサービスの一方または両方で個人データを処理する場合、一般データ保護規則（GDPR）やデータ保護法（2018 年）など、該当するデータ保護法に従って処理しなければなりません。デバイスメーカーと IoT サービスプロバイダは、それぞれのデバイスやサービスにおいて、消費者のデータを誰が、どのように、何の目的で使用するかという明確かつ透明性の高い情報を消費者に提供する必要があります。これは、関与する可能性のある第三者にも適用されます（広告主を含む）。消費者の同意に基づいて個人データを処理する場合、その個人データは正当かつ合法的に取得し、消費者はいつでもその情報の使用を中止できるものとします。

このガイドラインでは、次のような行動が求められます。
i）IoT メーカー、サービスプロバイダ、アプリケーション開発会社は、製品やサービスの開発および提供時に、データ保護の義務に従う必要があります。
ii）個人データはデータ保護法に従って処理する必要があります。
iii）ユーザーは、指定した内容で製品のデータ処理作業が確実に実施され、機能していることを確認できるものとします。
iv）ユーザーには、デバイスやサービスの機能を適切に構成することでプライバシーを保護できる手段を与えるものとします。

主な実施担当者：デバイスメーカー、IoT サービスプロバイダ、モバイルアプリケーション開発会社、小売業者

9）機能停止時のシステムの復旧性を確保する

製品やサービスの用途または依存するその他のシステムで必要とされる場合には、データネットワークの停止や停電の可能性を考慮した復旧性を IoT デバイスやサービスに組み込む必要があります。可能であれば、ネットワークが停止しても、IoT サービスは動作を継続してローカルで機能し続けるべきであり、停電から回復

した場合は、スムーズに復旧するものとします。デバイスをネットワークに復旧させる際は、膨大な数が一度に再接続するのではなく、秩序を保って合理的な形で復旧させる必要があります。

消費者が使用する IoT システムおよびデバイスは、安全性や生命に影響を及ぼす重要な場面で運用される機会が増えています。ネットワーク停止時にローカルでサービスを継続することは、復旧性を高める手法の 1 つです。他にも、サービスに冗長性を組み込んだり、DDoS 攻撃を緩和したりするといった対策があります。必要な復旧性のレベルは、用途の重要度に合わせて設定し、その内容に従って決定します。ただし、システム、サービス、デバイスに依存している他の要素が想定より広範囲に影響を及ぼす可能性があるため、そうした要素も考慮する必要があります。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者

10）システムの遠隔データを監視する

IoT デバイスやサービスから使用状況や測定データなどの遠隔データを収集する場合、セキュリティ異常の有無を監視する必要があります。

ログデータなどの遠隔情報の監視はセキュリティ評価に役立ちます。異常な状況をいち早く確認して対処することが可能になるため、セキュリティリスクを最小限に抑え、問題を迅速に緩和できます。ただし、ガイドライン 8 に従い、個人データの処理は最小限に抑え、収集するデータとその理由に関する情報を消費者に提示することが推奨されます。

主な実施担当者：IoT サービス提供事業者

11）消費者が個人データを容易に削除できるように配慮する

デバイスとサービスは、所有権が移動した場合や、消費者が削除を求める場合、あるいは消費者がデバイスの廃棄を求める場合に、個人データを容易に削除できるように構成する必要があります。消費者には、個人データの削除方法を明確に提示します。

IoT デバイスは譲渡される可能性があり、また最終的にリサイクルまたは廃棄されることも考えられます。そのため、消費者がサービス、デバイス、アプリケーションの個人データを管理および削除できる仕組みを用意する必要があります。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

12）デバイスを容易に設置してメンテナンスできるように配慮する

IoT デバイスの設置とメンテナンスは最小限の手順で完了すべきであり、セキュリティのベストプラクティスに従って使いやすさを確保する必要があります。消費者には、デバイスを安全にセットアップするためのガイダンスも提示します。

消費者の誤解や構成ミスで発生するセキュリティ問題は、複雑で使いにくいユーザーインターフェイスのデザインを改善することで減少、または完全に解消できる場合があります。デバイスの安全な構成方法をガイダンスとしてユーザーに明確に伝えることで、脅威に直面する機会を削減できます。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

13）入力データを検証する

サービスおよびデバイスにおいて、ユーザーインターフェイス経由でのデータ入力と、アプリケーションプログラミングインターフェイス（API）経由またはネットワーク間でのデータ転送は、検証の対象となります。

正しくフォーマットされていないデータや、コードが異なるタイプのインターフェイス間で転送されると、システムが破壊される可能性があります。多くの場合、攻撃者は自動ツールを使用し、データ検証を怠ったことで発生する隙間や弱点を狙って攻撃をしかけます。たとえば、以下のようなデータが標的になります。
i）予期しないタイプのデータ（ユーザーが入力したテキストではなく、実行可能なコードなど）。
ii）範囲外のデータ（センサーの温度範囲を超える温度値など）。

主な実施担当者：デバイスメーカー、IoT サービス提供事業者、モバイルアプリケーション開発事業者

その他の補足事項

*ガイドライン 1 - 初期パスワードを設定しない：*ユーザーやシステムを認証する際に、パスワードに頼らず代替の認証方法を導入する動きが進んでいますが、一部の IoT 製品は、ユーザーインターフェイスからネットワークプロトコルまで、いまだにデフォルトのユーザー名とパスワードを設定した状態で販売されています。こうした慣習は直ちに排除すべきです。他者による変更が不可能な一意の識別子を与えることで、デバイスのセキュリティはさらに強化できます。

*ガイドライン 2 - 協調的な脆弱性の公開（CVD）：*CVD は、国際標準化機構（ISO）で標準化されており、簡単に導入でき、世界中の複数の大手ソフトウェア会社でその効果が実証されています。[8]しかし、CVD は、IoT 業界では未だに確立されていません。セキュリティ研究者との連携に躊躇している企業もあります。CVD により、セキュリティ研究者は企業と連絡を取り、悪意のある不正利用の脅威にさらされる前にセキュリティ問題を通知できます。その結果、企業は脆弱性を公開する前に解決できる可能性があります。

インターネット接続デバイスやサービスを提供する企業は、CVD プログラムの不備により被害を受ける可能性がある第三者に対する注意義務があります。さらに、業界団体を通じてこの情報を共有することで、同じ問題に対処する他の企業を支援できます。

状況に応じて、公開には異なるアプローチが必要になる場合があります。
単一の製品やサービスに関連する脆弱性は、影響を受ける関係者（デバイスメーカー、IoT サービスプロバイダ、モバイルアプリケーション開発会社など）に直接報告する必要があります。こうした報告では、セキュリティ研究者や業界の同業者が情報の提供元になります。デバイスメーカーや影響を受ける他の関係者と連絡を取った後で、当事者によるタイムリーな対処が見られない場合は、NCSC に直接問題を報告できます。

システムの脆弱性：デバイスメーカーなどの関係者が、システムに関わる問題を発見する場合もあります。デバイスメーカー自身の製品でその問題を解決することも重要ですが、その情報を共有することで、業界と消費者にも大きなメリットをもたらすことができます。同様にセキュリティ研究者も、こうしたシステム関連の脆弱性を報告する場合があります。この場合は、関連するしかるべき業界団体が、より広範囲に対処できるように調整します。NCSC は、調整された対処方法を確立するために、助言とガイダンスをしかるべき業界団体に提供します。

脆弱性への対処の「タイムリー性」は案件ごとに大きく異なりますが、脆弱性プロセスの事実上の目安となるのは 90 日以内での完了です。ハードウェアの修正に要する時間は、ソフトウェアの修正より大幅に長くなる可能性があります。さらに、修正をデバイス単位で展開しなければならない場合は、サーバーソフトウェアの修正より時間がかかることがあります。

*ガイドライン 3 - ソフトウェアを定期的に更新する：*ソフトウェアセキュリティの更新は、ユーザーや幅広い技術エコシステムを守るために企業が行うべき最も重要な作業の 1 つです。多くの場合、脆弱性は、セキュリティとの関連を想定していないソフトウェアコンポーネントが主因となります。このため、一般的な原則として、すべ

[8] 国際標準化機構、2014 年、「ISO/IEC 29147 - Vulnerability Disclosure（脆弱性の公開）」、https://www.iso.org/standard/45170.html。

てのソフトウェアを常に最新の状態に保ち、確実にメンテナンスする必要があります。通常、修正は自動更新の一部として予防的にデバイスに適用し、悪用される前にセキュリティの脆弱性を解消します。ただし、クラウド更新、デバイス更新、その他のサービス更新が含まれる場合、こうした修正の管理は複雑になります。消費者に対して更新サポートの現状を分かりやすく伝えるには、明確な管理と展開の計画が不可欠です。

多くの場合、ソフトウェア更新を公開する場合は、サブコンポーネントのメーカーなど、他の組織に対する複数の依存関係が発生します。しかし、それが更新を控える理由にはなりません。本行動規範の目的は、ソフトウェアサプライチェーン全体にプラスとなるセキュリティ変更を促進することです。デバイスに修正パッチを適用できない状況は他にもいくつかあります。非常に制約の多いデバイスもその 1 つです。この場合、入れ替えに関する計画を作成し、消費者に明確に伝える必要があります。計画では、テクノロジを入れ替えるスケジュールを明らかにし、可能であれば、ハードウェアとソフトウェアのサポートが終了するタイミングを示します。

消費者にとっては、デバイスが継続的に機能することが重要です。このため、更新を適用する場合は、できるだけ「デバイスの機能に影響しない」ように配慮する必要があります。特に、安全関連の機能を担うデバイスは、更新中も完全に停止するべきではありません。暖房装置や盗難警報器の動作を維持するなど、最小限のシステム機能を維持する必要があります。このタイプのデバイスを製造するメーカーは、より復旧性の高いアーキテクチャへの移行も検討すべきです。

ソフトウェア更新の仕組みは攻撃の標的になりやすいため、その仕組みの安全性を確保することが重要です。

*ガイドライン 5 - 安全に通信する：*セキュリティ制御と暗号化の使用が妥当かどうかの判断は、使用状況など、多くの要素により左右されます。[9]セキュリティは絶えず進化しているため、暗号化対策に関する絶対的な助言は困難です。そうした助言は早々に過去のものになり、無意味になる可能性があります。開発会社は、暗号化に対する攻撃への耐性を保ちながら、ユーザーのニーズを満たすように製品を開発する必要があります。

*ガイドライン 7 - ソフトウェアの整合性を確認する：*IoT デバイスがソフトウェアの異常を検出した場合、適切な人物に通知する機能が必要です。デバイスによっては、管理モードでその機能を提供する場合もあります。たとえば、部屋の温度を調整するサーモスタットで、他の設定を変更できないユーザーモードを設定します。この場合、管理者へのアラートがあれば、そのアラートに対して対処することができます。

---

[9] ガイダンスをダウンロードできます。たとえば、NCSC によるガイダンスは https://www.ncsc.gov.uk/guidance/tls-external-facing-services で入手可能です。

*ガイドライン 9 - 機能停止時のシステムの復旧性を確保する：*このガイドラインの目的は、IoT サービスの動作を維持することです。IoT デバイスは、個人の安全確保に関連する機能も含めて、消費者の生活のあらゆる部分で導入が進んでいます。たとえば、コネクテッドドアへのインターネット接続が失われると誰かが閉め出されるなど、人々の生活に対する影響が拡大しています。また、クラウドサービスに対する DDoS 攻撃により、家庭の暖房システムが停止する可能性もあります。他の安全関連の規制への配慮も不可欠ですが、機能停止がそうした問題の引き金にならないように構成することも重要です。