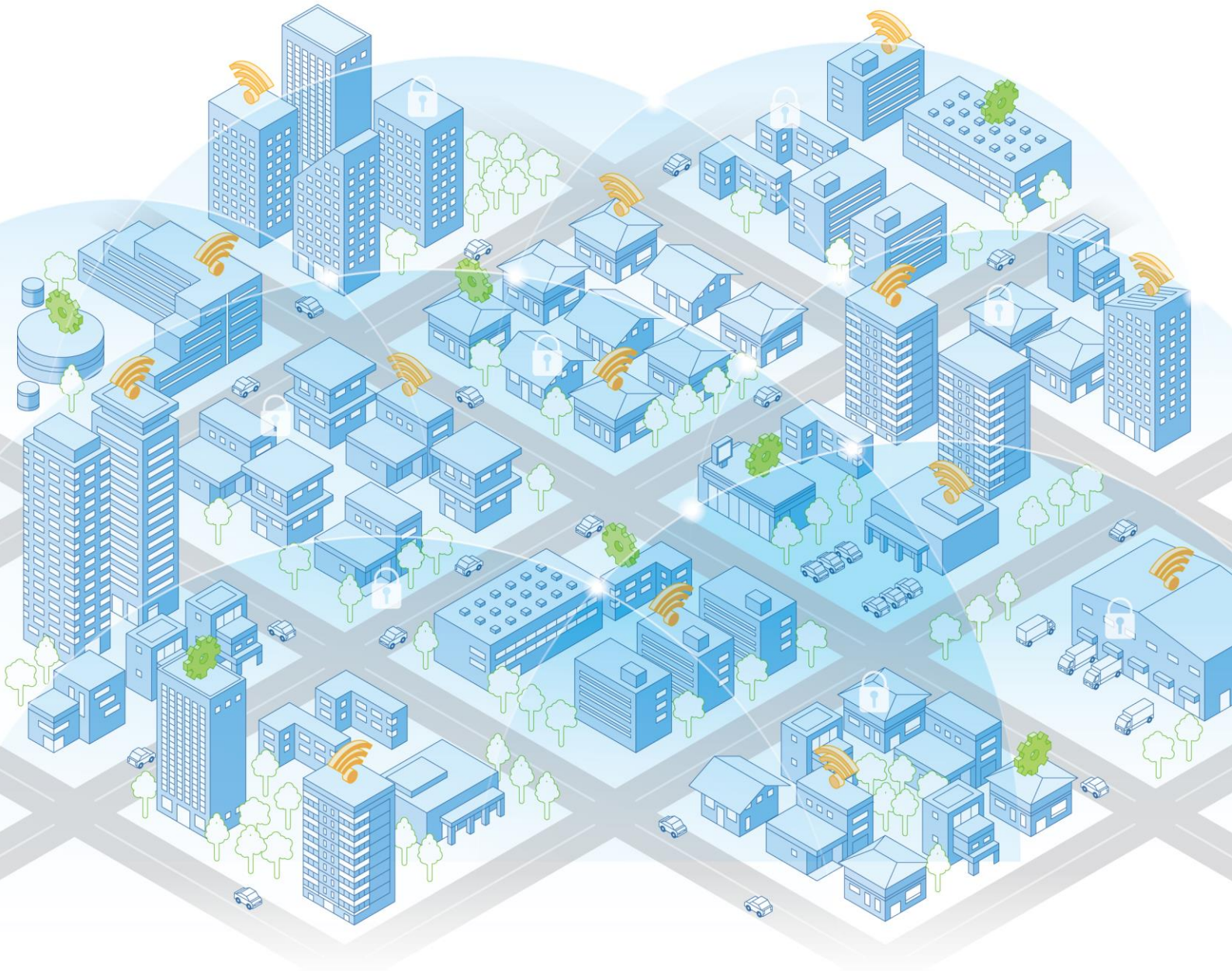
IoT 機器を開発する中小企業向け
製品セキュリティ対策ガイド

サイバー攻撃から大切な製品を守るための第一歩

※中小企業の皆様を主な対象としていますが、これからセキュリティ対策に取り組む
IoT 機器等を開発する皆様にご活用いただけます。



経済産業省　商務情報政策局
サイバーセキュリティ課

目次

経営者の皆様へ

IoT 製品のセキュリティ対策の不備により、お客様に被害が及ぶおそれや、メーカに多大な不利益が生じる可能性があります！

IoT 機器等に対するサイバー攻撃は急増しています[1]。IoT 機器等メーカが、製造する IoT 機器等に十分なセキュリティ対策を行わなかった場合、悪意ある攻撃者によって脆弱性をついた不正な操作がなされるなど、お客様に被害が及ぶおそれがあります。また、メーカについても、リコール対応が必要になった事例や、訴訟に発展した事例もあるなど、経営に対して多大な不利益が生じる可能性もあります。中小企業だからといって IoT 機器等に対するセキュリティ対策がおろそかでよいということは決してなく、企業規模によらず、必要なセキュリティ機能を IoT 機器等に搭載させるための対策を行うことが必要です。

（参考）メーカに生じる不利益の例

❶ 経済損失

製品の販売中止による機会損失だけでなく、顧客等への説明や製品の回収等、膨大な対応コストがかかるほか、顧客からの損害賠償請求や株価の下落を招く可能性があります。

❷ 信頼損失

セキュリティ対策や発生したインシデントへの対応に不備があった場合、製品や企業の評価の低下に繋がります。製品がサイバー攻撃の踏み台となり、他社や広く一般に被害が及ぶと、社会からの信頼を失いかねません。それに付随し、従業員の意欲低下を招くおそれもあります。

【事例】 脆弱な家庭用ネットワークカメラの開発企業に対する訴訟

家庭用ネットワークカメラに対して、脆弱性を悪用した不正アクセスが行われ、嫌がらせや身代金の要求等の被害を受けた複数のユーザにより、製品開発企業に対して 500 万ドルを求める集団訴訟が起こされました。

本ガイドでは、IoT 機器等にセキュリティ対策を行う第一歩として取り組んでいただきたいことを示しています！

本ガイドは、IoT 機器等を開発する中小企業の皆様に、IoT 機器等にセキュリティ対策を施すこと、特に設計や開発段階からセキュリティを考慮することの重要性について認識いただくために、機器のライフサイクルフェーズを通じた対策を整理し、セキュリティ対策を進める際、最初に取り組む事項を示しています。

IoT 製品のセキュリティを確認するためにセキュリティ検証が有効ですが、出荷前の検証だ

[1] 国立研究開発法人情報通信研究機構が運用する大規模サイバー攻撃観測網（NICTER）の観測レポートでは、「IoT 機器を狙った通信が依然として最も多い」とされている。（令和 4 年版情報通信白書）

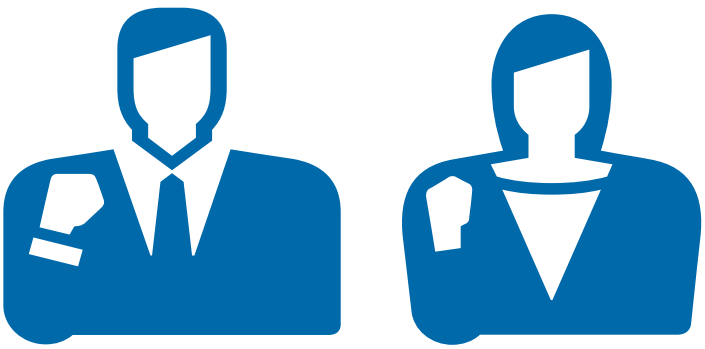
けでは、脆弱性が発見された場合、製品の販売やセキュリティ自体の確保に支障が出たり、製品が悪用されたりすることでお客様に迷惑をかける可能性もあります。そのため、セキュリティ対策を「自分ごと」として捉え、設計や開発段階からセキュリティを考慮すること（セキュリティ・バイ・デザイン）がとても重要です。

しかし、IoTのセキュリティに関しては国内外に複数のガイドラインや規格等が提示されており、何から始めてよいかがわかりにくい場合もあります。本ガイドでは、IoT 機器等のセキュリティ対策を行おうとする企業が、対策の第一歩として取り組んでいただきたいことを示しており、また付録には効果的な対策を行う中小企業の事例も載せています。

対策1～6のそれぞれを実施することが理想的ですが、企業によっては対策全てを網羅的に実施することは難しい場合もあると考えられます。そのような企業においては、企業の経営方針、成長ステージ、人員の状況や体制、予算、製品の特性、顧客との関係など、自社を取り巻く様々な環境を考慮しつつ、優先順位をつけて、まずできるところから対策を進めることが重要です。もちろん、リソース不足の解消やコスト低減のために外部の専門家を活用することも有効ですが、自社製品の特徴を深く理解し、責任を持ってセキュリティ対策を推進するためには、セキュリティ専門家を目指す社内人材を見いだし、適切な役割と権限を付与するとともに、長期的なキャリアパスも見据えて育成することも検討しましょう。

経営者が率先して、セキュリティ対策を推進しましょう！

セキュリティ対策は上記の不利益を被らないために必要であるとともに、対策の実施によってセキュリティに関するリスクを許容できる水準に下げることは、企業として果たすべき社会的責任であり、経営者は責任を持って実践しなければなりません。本ガイドをもとに、経営者が率先して IoT 機器等のセキュリティ対策を推進し、開発者に対策を指示するとともに、企業としての対策方針の検討、予算や人材の割当を行いましょう。また、部品の調達先や保守の委託先を含めた対策を進めるとともに、インシデントが発生した際に円滑に対応できるよう、平時から社内外の関係者とコミュニケーションを図り信頼関係を築きましょう。



本ガイドの概要

基本的な考え方

サイバー攻撃の脅威が増している中、IoT 機器等のセキュリティを確保することは極めて重要です。企業規模によらず、IoT 機器等に必要なセキュリティ機能を搭載させる対策を実施しましょう。

IoT 製品にセキュリティが実装されていることを確認するためには、セキュリティ検証を行うことが有効です。しかし、出荷前の検証だけでは、その時点で問題が発見された際に、製品リリースが遅くなる、改修に新たなコストがかかる、本来の機能を制限してリリースせざるを得なくなるといった製品の販売に影響が出ることも考えられるほか、発見された問題に対して必要な機能が実装できないなど製品のセキュリティ自体に支障が出てしまう可能性もあります。その結果、情報の漏えいや製品の悪用など、お客様が迷惑を被る事象が発生する可能性もあります。

こうした事態を回避するためには、まずは経営者からセキュリティ担当者や開発担当者といった実務者まで、IoT 機器等のセキュリティを確保することを「自分ごと」として捉えることが重要であり、実際の取組としては、設計や開発段階からセキュリティを考慮すること（セキュリティ・バイ・デザイン）がとても重要です。IoT 機器等のセキュリティ対策を自社で「自分ごと」として捉えることができれば、製品に必要なセキュリティ対策に関する判断ができるようになり、製品のセキュリティ対策費用の低減や差別化にも繋がります。

こうした取組を、中小企業をはじめとした IoT 機器メーカに手軽に行っていただきたいですが、IoT のセキュリティに関しては国内外に複数のガイドラインや規格等が提示されており、セキュリティ対策に取り組もうとする企業にとっては、何から始めてよいかがわかりにくい場合もあります。本ガイドでは、IoT 機器等のセキュリティ対策を行おうとする中小企業をはじめとした企業が、対策の第一歩として取り組んでいただきたいことを示しています。また、本ガイドの付録として、リソースに限りがありながらも、セキュリティ対策を効果的に進める中小企業の事例集も作成していますので、ぜひ参考にしてください。

対策1～6のそれぞれを実施することが理想的ですが、中小企業においては、予算や人員が限られるケースもあるなど、本ガイドで示している対策全てを網羅的に実施することは難しい場合もあると考えられます。このような場合には、企業の経営方針、成長ステージ、人員の状況や体制、予算、製品の特性、顧客との関係など、自社を取り巻く様々な環境を考慮しつつ、優先順位をつけて、まずできるところから対策を進めることが重要です。

ガイドの主な対象

- **IoT 機器等を開発する中小企業の経営者**
- **IoT 機器等を開発する中小企業のセキュリティ担当者・開発担当者・品質管理者**

※ 中小企業[2]は、様々な経営課題の中でセキュリティ対策に取り組む優先順位が低くなる場合や、セキュリティ担当者が別の業務を兼務している場合が多いことから、実施事項をわかりやすく示した本ガイドは、主に中小企業を対象としています。ただし、本ガイドに記載している事項は中小企業以外の企業にとっても参照されるべき事項であるため、セキュリティ対策に取り組もうしている IoT 機器等を開発する皆様にご活用いただけます。

ガイドの構成

本ガイドでは、機器開発のライフサイクルフェーズを

① 「方針・体制構築」
② 「設計・開発」
③ 「検証」
④ 「運用・保守」

の 4 つに大別しています。

「各フェーズで求められる対策」の章には、各ライフサイクルフェーズにおいて、セキュリティ対策に取り組もうとする企業が最初に検討すべき対策を示しています。

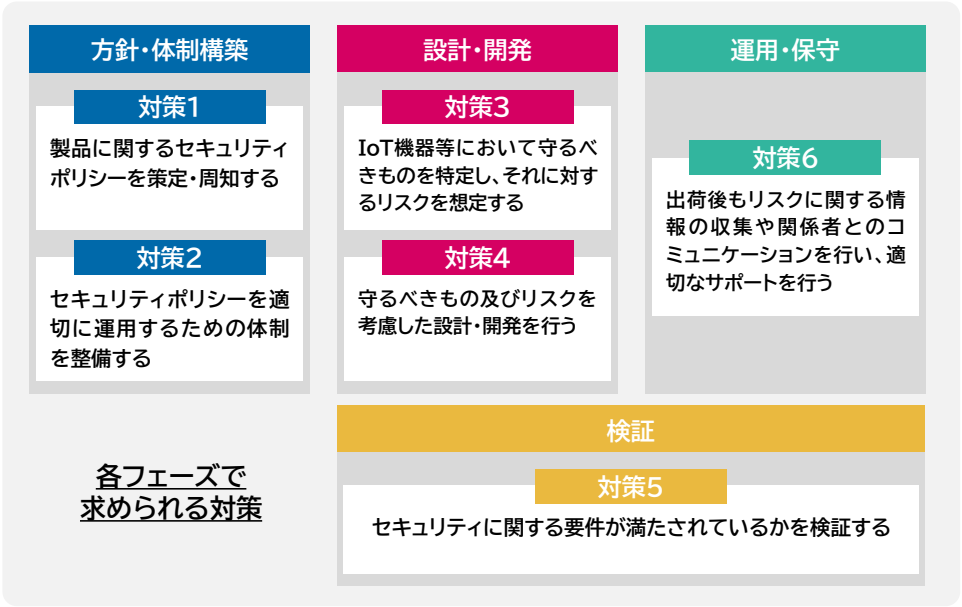
「設計・開発フェーズで検討すべき主な技術的対策」の章には、特に設計・開発の段階において、セキュリティ対策に取り組もうとする企業が最初に検討すべき主な技術的対策について、IoT 機器等の特徴別に示しています。

「IoT 機器等を開発する中小企業の対策事例集」の章には、中小企業による実際の対策事例を示しており、それぞれの企業の状況に応じてどのような対策を実施すれば良いかについての参考情報を提供しています。

[2] 中小企業基本法では中小企業者の範囲と小規模企業者の定義を次の表のように規定しています。
https://www.chusho.meti.go.jp/faq/faq/faq01_teigi.htm#q1

業 種	中小企業者（下記のいずれかを満たすこと）		小規模企業者
	資本金の額又は出資の総額	常時使用する従業員の数	常時使用する従業員の数
①製造業、建設業、運輸業 その他の業種（②～④を除く）	3億円以下	300人以下	20人以下
②卸売業	1億円以下	100人以下	5人以下
③サービス業	5,000万円以下	100人以下	5人以下
④小売業	5,000万円以下	50人以下	5人以下

本ガイドで示した対策の全体像



設計・開発フェーズで検討すべき主な技術的対策

IoT機器で提供する機能と対応する主な技術的対策

(1) 通信機能を提供するIoT機器等	(2) データの送信・保存機能を有するIoT機器等	(3) 高い可用性が求められるIoT機器等
A 認証・認可機能の提供 B アップデート機能の提供 C ログの保存機能の提供	A データの暗号化・保護機能の提供 B データの削除機能の提供	A システムの復旧の提供 B 異常検知機能の提供

(参考)本ガイドと「IoT セキュリティガイドライン[3]」との対応関係

本ガイドの対策	IoT セキュリティガイドラインの項目
【対策1】製品に関するセキュリティポリシーを策定・周知する	要点 1
【対策2】セキュリティポリシーを適切に運用するための体制を整備する	要点 1
【対策3】IoT 機器等において守るべきものを特定し、それに対するリスクを想定する	要点 2, 3, 4, 5, 6, 7, 20
【対策4】守るべきもの及びリスクを考慮した設計・開発を行う	要点 8
【対策5】セキュリティに関する要件が満たされているかを検証する	-
【対策6】出荷後もリスクに関する情報の収集や関係者とのコミュニケーションを行い、適切なサポートを行う	要点 17, 18, 19, 21
設計・開発フェーズで検討すべき主な技術的対策	要点 9, 11, 13, 14, 15, 16, 17

[3] IoT セキュリティガイドライン ver 1.0(IoT 推進コンソーシアム・総務省・経済産業省)
https://www.soumu.go.jp/main_content/000428393.pdf

ガイドの活用方法

「各フェーズで求められる対策」には、「方針・体制構築フェーズで求められる対策」、「設計・開発フェーズで求められる対策」、「検証フェーズで求められる対策」、「運用・保守フェーズで求められる対策」の4つの節があり、6 つの必要な対策を示しています。それぞれの対策は、「対策を実施しない場合に考えられるリスク」、「最初に取り組む主な対策」、「参考資料」、「コラム」から構成されています。対策 1～6 のそれぞれを実施することが理想的ですが、難しい場合には自社を取り巻く様々な環境を考慮しつつ、優先順位をつけて、できるところから対策を進めることが重要です。

各フェーズで求められる対策の活用方法

項目	活用方法
対策を実施しない場合に考えられるリスク	リスクが自社に与える影響を考慮した上で、対策の実施を検討するために、ご覧ください。
最初に取り組む主な対策	最初に取り組む主な対策を把握するために、ご覧ください。
参考資料	対策を実施する上で参考となる資料を示しています。より詳しい情報を知りたい場合に、ご覧ください。
コラム	対策に関する追加情報を記載しています。対策を実施する上での参考にしてください。

「設計・開発フェーズで検討すべき主な技術的対策」は、「対策内容」、「対策理由」、「考慮すべきポイント」、「機器検証サービス事業者からのアドバイス」、「国内外のガイドラインや指針との対応表」から構成されています。

設計・開発フェーズで検討すべき主な技術的対策

項目	活用方法
対策内容	最初に検討すべき主な技術的対策を把握するために、ご覧ください。
対策理由	対策の実施を検討する際に、ご覧ください。
考慮すべきポイント	対策を実施する上で考慮すべきポイントを把握するために、ご覧ください。
機器検証サービス事業者からのアドバイス	検証でよく見られる脆弱性を踏まえ、留意すべきポイントをアドバイスとして記載しています。対策を実施する上での参考にしてください。
国内外のガイドラインや指針との対応表	国内外のガイドラインや指針の項目と各技術的対策との対応表を示しています。より詳しい情報を知りたい場合に、ご覧ください。

「IoT 機器等を開発する中小企業の対策事例集」では、中小企業 5 社の対策事例を紹介しており、「基本情報」、「対策のポイント」、「対策内容」、「対策に力を入れたことによるメリット」から構成されています。

IoT 機器等を開発する中小企業の対策事例集

項目	活用方法
基本情報 （製品種、消費者/産業向け、従業員数、資本金）	事例企業の基礎情報を把握するためにご覧ください。
対策のポイント	事例企業による対策のポイントを記載しています。各企業の背景や対策への考え方等を把握するためにご覧ください。
対策内容	各ライフサイクルフェーズにおける実際の対策内容を示しています。それぞれの企業の状況に応じてどのような対策を実施すれば良いかについて検討する上での参考にしてください。
対策に力を入れたことによるメリット	対策の実施を検討する際に、ご覧ください。

方針・体制構築フェーズで求められる対策

対策 1　製品に関するセキュリティポリシーを策定・周知する

対策を実施しない場合に考えられるリスク

- セキュリティに対する社内の意識が高まらず、製品への対策が統一的に実施されないことにより、自社の製品がサイバー攻撃を受ける可能性が高まる。
- 自社の製品に脆弱性が発見されたり、サイバー攻撃を受けたりしたときの対応が遅れ、自社や顧客に被害が拡大する。
- 製品がサイバー攻撃を受け、顧客に被害が出た場合に、損害賠償やリコール対応等の対応が必要になる。

最初に取り組む主な対策

- **経営者が率先して、製品に関するセキュリティポリシーを策定し、広報や教育によって社内に浸透させましょう。**
- **実施状況や社会的な要求事項の変化を踏まえ、ポリシーの見直しを行いましょう。**

セキュリティポリシーの項目例

■ **技術的な対策方針**

検証の実施やアップデートに関する取り組み、サポート期間の設定といった脆弱性への対応方針のほか、設計・開発に関わる文書の管理について記載しましょう。

■ **情報提供に関する方針**

サポート終了後の対応も含めた製品の適切な利用方法に関するアナウンスやセキュリティに関する注意喚起等、ユーザに対する情報提供方針について記載しましょう。

参考資料

- 製品セキュリティポリシーの具体例を確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[4]』の「1 製品セキュリティポリシーの策定」をご覧ください。以下のような、製品セキュリティポリシーの策定に関して、レベル毎の実施内容と開示例が記載されています。「実施することが理想的な事項」はレベル 3 ですが、その実施が困難な場合はレベル 2、それも難しい場合はレベル 1 の記載事項を参照します。

[4] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

レベル毎の実施内容

レベル	実施内容
1	製品セキュリティに関する方針・考え方を、製品セキュリティポリシーとして策定します。
2	製品セキュリティに関する方針・考え方を、製品セキュリティポリシーとして策定し、外部に開示します。
3	製品セキュリティに関する方針・考え方に加え、実施事項を含めて製品セキュリティポリシーとして策定し、外部に開示します。

製品セキュリティポリシーの開示例

【開示例（レベル 3）】

製品セキュリティポリシー

当社は、製品セキュリティレベル維持及び改善を含めた活動を継続的に実施し、お客様に安全性の高い製品を提供します。

(1)組織的対策
当社では、全社的な方針の下、製品セキュリティを確保する体制を整備し、セキュリティ対策を実施します。また、国内外のガイド等に基づいた製品セキュリティ対策基準を策定し、これに基づいた製品のセキュリティ設計・開発を行います。

(2)技術的対策
当社では、製品の出荷前に脆弱性検査を実施し、製品に脆弱性が含まれないように努めます。また、出荷後も、自社製品の脆弱性に関する情報を収集し、発見された脆弱性が、お客様への被害や製品性能に影響を及ぼす可能性があると判断した場合には、アップデートや対策ソフトウェアの提供等、当社が必要と判断した対応策等、適切な情報を提供します。

(3)情報の提供
セキュリティレベルの維持は、適切なセキュリティ対策を行った当社製品をお客様が適切に利用することで実現できます。当社は、セキュリティに関する注意喚起やセキュリティを確保した上で製品を利用するための情報等を提供します。

【開示例（レベル 2 の場合の例）】

製品セキュリティに関する方針

当社では、以下の方針の下、製品セキュリティの確保に取り組みます。

1. 製品セキュリティを確保するための体制を整備します。
2. セキュリティを考慮した設計・開発を行い、製品出荷前は、脆弱性検査により脆弱性の解消に努めます。
3. 製品出荷後も脆弱性情報を広く収集し、リスクがあると判断した場合は迅速に対応を行います。
4. セキュリティに関する情報や対策方法を利用者の皆様に提供します。

出所）IPA『脆弱性対処に向けた製品開発者向けガイド』

対策 2　セキュリティポリシーを適切に運用するための体制を整備する

対策を実施しない場合に考えられるリスク

- 策定したセキュリティポリシーが体制・人員不足により実行されず、適切な対策が実施されないことで、サイバー攻撃を受ける可能性が高まる。
- セキュリティポリシーの更新を行わず、古いセキュリティポリシーに基づく対策が実施されることで適切な対策が実施されず、サイバー攻撃を受ける可能性が高まる。
- 自社の製品に脆弱性が発見されたり、サイバー攻撃を受けたりしたときの対応が遅れ、自社や顧客に被害が拡大する。

最初に取り組む主な対策

- **セキュリティポリシーを適切に運用するために必要な関係者や組織の洗い出しを行い、それぞれの役割や責任を明確化しましょう。**
  - 必要であれば、部署を跨いだ連携や新しい組織の立ち上げを検討するほか、自社で実施が難しい項目は外部に委託するなどして、外部の専門家を含めた体制を構築することも検討しましょう。また、自社社員に不足する知識を教育し、育成することも検討しましょう。

セキュリティポリシーを適切に運用するために求められる役割例

■ **攻撃事例や脆弱性情報を収集する役割**

製品に関連する攻撃事例や脆弱性情報を収集する役割。

■ **製品にセキュリティ対策を施す役割**

製品に対してセキュリティ対策を施す役割。検証等を通じて脆弱性が見つかった場合は、セキュリティパッチの適用といった対応を行いましょう。

■ **製品にセキュリティ対策が適切に施されているかを確認する役割**

セキュリティに関する要件が満たされているかについて、検証等を通じて確認する役割。外部の機器検証サービス事業者へ依頼を行う場合は、事業者の選定・依頼を行いましょう。詳細は、対策 5 をご覧ください。

■ **製品出荷後に生じたインシデントに対応する役割**

インシデントが発生した際、各部門や外部組織と連携しながら、対応する役割。

■ **ユーザとコミュニケーションを取る役割**

ユーザからの問い合わせを受け付け、ユーザに対するアナウンスを行う役割。

■ **セキュリティに関する情報提供を行う役割**

法務や広報の観点を踏まえ、脆弱性やセキュリティに関する情報を対外的に公表する役割。所管官庁等への報告も行いましょう。

参考資料

- セキュリティ対策を行う上で連携が必要となる関係者とその役割を確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[5]』の「附属：主要な関係者・役割表」をご覧ください。以下のように、連携する社内外の関係者と関与が整理されており、本文では具体的な役割も示されています。

主要な関係者と関与

		方針・組織	設計・開発	製品出荷後	
				平時	緊急時
自組織の関連部門	経営層	○		△	○
	法務部門	○			△
	広報部門	○		○	○
	リスクマネジメント部門	○		△	○
	製品管理部門	○	○	○	○
	調達部門		○	△	△
	設計/開発部門		○	○	○
	品質検査部門		○	○	○
	情報収集部門			○	○
	製品サポート窓口			○	○
	脆弱性受付窓口				○
外部関係者	製品サプライヤ		○	○	○
	セキュリティベンダ		△	△	△
	情報共有組織				
	脆弱性情報の報告者				○
	代理店	△		○	○
	一般消費者				○

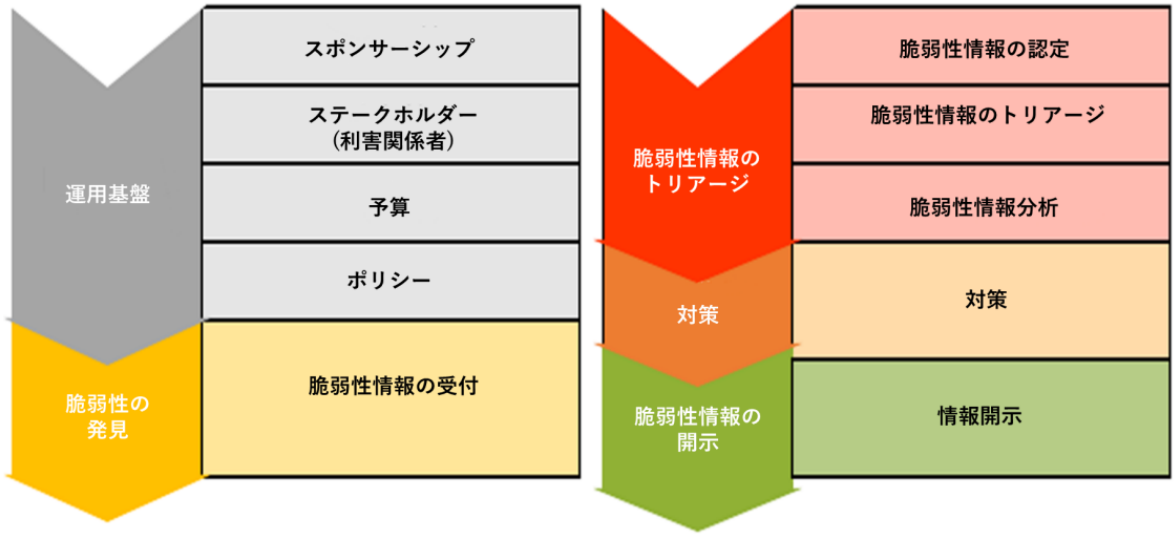
凡例：○ 当該部門/関係者の関与が必須、△ 当該部門/関係者の関与が状況次第

出所）IPA『脆弱性対処に向けた製品開発者向けガイド』を元に作成

[5] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

- インシデントに対応する役割の詳細を確認したい場合は、FIRST『製品セキュリティインシデント対応チーム（PSIRT）成熟度ドキュメント[6]』の「成熟度レベル 1」をご覧ください。以下のように、基本レベルである成熟度レベル 1 において望まれるインシデント対応チームのサービスが記載されています。

成熟度レベル 1 の望ましいインシデント対応チームのサービス



出所）FIRST『製品セキュリティインシデント対応チーム（PSIRT）成熟度ドキュメント』

- サイバーセキュリティに関する体制構築や人材確保におけるポイントを確認したい場合は、経済産業省・IPA『サイバーセキュリティ体制構築・人材確保の手引き（第 2.0 版）[7]』をご覧ください。

[6] https://www.jpcert.or.jp/tips/2022/wr222901.html
[7] https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html

設計・開発フェーズで求められる対策

対策３　IoT 機器等において守るべきものを特定し、それに対するリスクを想定する

対策を実施しない場合に考えられるリスク

- 守るべきものを正しく特定できていないことにより、製品に適切なセキュリティ対策が実装されず、脆弱性が残存してしまい、サイバー攻撃を受ける可能性が高まる。

最初に取り組む主な対策

- **想定されるユーザ及びユースケースを定めましょう。**
  - IoT 機器等に想定されるリスクは、誰がどのように使うかでも異なります。IoT 機器のリスクを適切に想定するために、設計の早い段階から IoT 機器の利用事例であるユースケースを定め、ユーザにおける IoT 機器の利用目的や要求事項、関係者を明らかにしましょう。ユースケースを定める際は、使用される地域や環境、状況や期間、販売経路等を考慮しましょう。

  ユースケースの例

  家電の遠隔操作、ドローンを用いた写真撮影、物流倉庫の無人輸送　等

- **ユーザのセキュリティニーズについて検討し、守るべきものを特定しましょう。**
  - セキュリティニーズについて検討する際は、
    - ユーザの使用目的
    - IoT 機器等が他の製品やシステムに与える影響
    - 扱うデータの性質
    - 既存のセキュリティ要件

    等について考慮しましょう。
  - IoT 機器等が有する機能及びデータのそれぞれに対して、セキュリティニーズを踏まえて守るべきものの洗い出しを行いましょう。このとき、IoT 機器等に接続される他の機器やシステム、クラウドも洗い出しの対象に含めましょう。

- **守るべきものに対する多様なリスクを想定しましょう。**
  - IoT 機器等が安全であるという前提を疑い、様々な脅威を考慮しましょう。
  - 自社での実施が難しい場合は、外部の機器検証サービス事業者等の専門家にリスク分析の依頼を行いましょう。

リスク分析の手順

① 守るべきものに対する攻撃ポイントを洗い出しましょう。攻撃ポイントの例として、入出力インターフェースや通信経路等が挙げられます。物理的な攻撃も想定します。
② 脅威分析モデルを参考に、各攻撃ポイントに想定される脅威例を検討しましょう。本検討を行う上では、対象機器と類似する機器における過去の脆弱性報告事例を参考にしましょう。
③ 仕様に沿った正規の使い方と脅威となる使い方を同一のユースケース図に表現したミスユースケース例を検討するなどして、脆弱性や危険な操作の可能性を明らかにしましょう。
④ 想定した脅威例や脆弱性からリスクの発生頻度や想定被害を考慮して、守るべきものに対するリスクを分析し、対応すべきリスクの優先度を決定しましょう。過去の攻撃や対策事例も参考に、ネットワークに繋がることによるリスクや、繋がりにより波及するリスクの想定を行いましょう。

参考資料

- ユーザ及びユースケースの特定やセキュリティニーズの検討について詳細な解説を確認したい場合は、NIST『NISTIR 8259[8]』の「Activity 1:想定される顧客を特定し、想定されるユースケースを定義する」「Activity 2:顧客のサイバーセキュリティのニーズと目標を調査する」をご覧ください。「Activity 1」では、ユースケース定義のための質問事項、「Activity 2」では、顧客のニーズと目標に関する情報収集のための質問事項が示されています。

【ユースケース定義のための質問事項】
- どのように利用されるか。
  （例:単一目的か複数目的か、別の機器に組み込まれるかそうでないか、単一ユーザか複数ユーザか、個人利用か商業利用か　等）
- 地理的にどこで利用されるか。
  （例:国内、法的規制がある国　等）
- どのような物理環境で利用されるか。
  （例:屋内か屋外か、静止か移動か、公的か私的か、可動か不動か　等）
- 使用期間はどれぐらいか。
  （例:数時間、数年、二十数年　等）
- 他のシステムにどのような依存関係を持つ可能性があるか。
  （例:特定のハブを使用する、クラウドに接続する　等）
- 攻撃者はどのように IoT 機器等を悪用し、侵害する可能性があるか。
  （例:DDoS 攻撃、他の機器等への攻撃の踏み台　等）
- IoT 機器等の利用に際し、セキュリティリスクに関連する他の要素はあるか。
  （例:安全性、プライバシ　等）

[8] https://csrc.nist.gov/publications/detail/nistir/8259/final

【顧客のニーズと目標に関する情報収集のための質問事項】
- IoT 機器は物理的な世界とどのように相互作用するか。
- IoT 機器は、許可された人、プロセス、および他のデバイスによって、どのようにアクセス管理、および監視される必要があるか。
- IoT 機器の既知のサイバーセキュリティ要件は何か。
- IoT 機器のサイバーセキュリティ能力の利用が、IoT 機器の運用特性や環境特性によってどのように妨げられる可能性があるか。
- IoT 機器のデータの性質はどのようなものになるか。
- 顧客が必要とする可能性のある IoT 機器の信頼度はどの程度か。
- IoT 機器が他の機器、システム、環境と相互作用することで、どのような複雑性がもたらされるか。

出所)NIST『NISTIR 8259』

- 脅威分析の手法について詳細な解説を確認したい場合は、経済産業省『機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き[9] 別冊 1』の「3 対象機器の脅威分析」や IPA『IoT 開発におけるセキュリティ設計の手引き[10]』の「3.1 脅威分析」をご覧ください。『機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き 別冊 1』では、脅威分析の手順例として、以下が挙げられています。

  1. 脅威分析の対象の決定と守るべき資産の洗い出し
  2. データフローの可視化
  3. 脅威の洗い出し
  4. 脅威を実現する攻撃手法の調査
  5. 脅威が実現した場合のリスクの評価

  脅威分析と対策検討の具体的な実施例を確認したい場合は、IPA『IoT 開発におけるセキュリティ設計の手引き』の「5. IoT システムにおける脅威分析と対策検討の実施例」をご覧ください。デジタルテレビ、ヘルスケア機器とクラウドサービス、スマートハウス、コネクテッドカーを題材とした IoT システムに対しての例が示されています。

- リスク形態及びリスクに対応するセキュリティ・セーフティ対策の類型化の手法を確認したい場合は、経済産業省『IoT セキュリティ・セーフティ・フレームワーク[11]』をご覧ください。このフレームワークでは、影響を受ける様々な事象を「発生したインシデントの影響の回復困難性の度合い」及び「発生したインシデントの経済的影響の度合い」の 2 軸で整理しています。

[9] https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html
[10] https://www.ipa.go.jp/security/iot/iotguide.html
[11] https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

セキュリティ・セーフティ要求の観点のイメージ

出所）経済産業省『IoT セキュリティ・セーフティ・フレームワーク』

コラム

消費者向け IoT 機器等と産業向け IoT 機器等との考え方の違い

消費者向け IoT 機器等の場合は、一般的なユースケースを基に、広く様々なユーザ等関係者や利用環境等を想定して必要なセキュリティ機能を検討する必要がありますが、産業向け IoT 機器等の場合、ユーザから仕様について要望が出る場合があります。ユースケースについてユーザに確認する際、セキュリティニーズについても把握し、ユーザが安心して IoT 機器等を使えるよう設計を行いましょう。

コラム

サプライチェーンにおける IoT 機器等の位置づけ

IoT 機器等が、電力・ガス・化学プラント等の重要インフラサービスや、脆弱性が悪用された場合に人命や経済に大きな影響を与える製品の一部を構成する場合があります。自社の IoT 機器等のサプライチェーンにおける位置づけを把握した上で、セキュリティニーズを検討しましょう。

対策 4　守るべきもの及びリスクを考慮した設計・開発を行う

対策を実施しない場合に考えられるリスク

- 設計・開発後に脆弱性が確認されると、再度設計・開発から見直さざるをえなくなり、製品のリリースが遅れる。
- 設計・開発の不備により、脆弱性が残存してしまい、サイバー攻撃を受ける可能性が高まる。
- 構成要素の脆弱性を認識できない、または構成要素に脆弱性が発見された場合もパッチ適用などの対応ができず、自社の製品がサイバー攻撃を受ける可能性が高まる。

最初に取り組む主な対策

- **対策 3 で想定したリスクをもとに、設計・開発の段階からリスクへの対策を IoT 機器等に施しましょう。**
  - 本書 P30 に記載の「設計・開発フェーズで検討すべき主な技術的対策」を参考に、必要な対策を選定しましょう。
  - 対策を選定し、設計を行う段階では、設計書のレビューも実施しましょう。
- **自社での実施が難しい場合は、機器検証サービス事業者等の専門家に設計・開発段階におけるセキュリティ対策の考慮事項について助言を受けることも有効です。**

設計・開発全般の留意事項

- **IoT 機器等の全ての構成要素（ライブラリやモジュール等）に関して構成管理を実施し、脆弱性情報の監視を行いましょう。**

  構成管理で記録すべき情報

  - 製品・ライブラリ・モジュール名
  - 製品・ライブラリ・モジュール開発者名
  - バージョン情報
- **攻撃対象となる場所を最小限に抑えましょう。**
  - 未使用のポートを閉じましょう。
  - 物理インターフェースを通じたハードウェアへの不要なアクセスを防ぎましょう。
  - 不必要な機能は搭載しないようにしましょう。

- **施設や環境のセキュリティ確保に努めましょう。**
  - 開発に使用する施設や設備は、自組織で使う一般的な情報システムと物理的にも（入退室管理等）、論理的にも（アクセス制限等）、分離しましょう。
  - 開発に使用する端末では、業務目的での日常的なメールやブラウザの使用を制限することを検討しましょう。
- **製品の標準的な利用期間を考慮した上で、ハードウェアのスペックや搭載するセキュリティ機能を検討しましょう。構成要素を含め、製品のサポート期間を定めましょう。**
- **想定したリスクへの対策を全て実施することが難しい場合、残存するリスクを許容できるか否かを判断し、許容できない場合はリスク移転としてサイバー保険への加入等を検討しましょう。**
- **設計・開発段階から、いつどの段階でどのような検証を行うかの計画を立て、実行しましょう。**
  - 検証についての詳細は、対策 5 をご覧ください。

参考資料

- IoT 機器等の開発者が開発時に考慮すべき点を把握するため、IPA『つながる世界の開発指針[12]』をご覧ください。本ガイドで示した対策の詳細や発展的な対策について解説されています。
- セキュリティニーズへの対応方法について詳細な解説を確認したい場合は、NIST『NISTIR 8259[13]』の「Activity 3：顧客のニーズと目標に対処する方法を決定する」「Activity 4：顧客のニーズと目標を十分にサポートするための計画を立てる」をご覧ください。「Activity 3」では、ニーズと目標への対処のための質問事項、「Activity 4」では、顧客のニーズと問題を特定するための質問事項が示されています。
- 構成管理を行う際に留意すべき点について確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[14]』の「6 既知の脆弱性解消」をご覧ください。構成管理を行う上でのポイントとしては以下の点が挙げられています。

  ・ 委託開発したソフトウェアについては、そのソフトウェアの構成要素の情報を納品物に含むよう契約に明記する。
  ・ 設計・開発工程（要件定義、設計、テスト）で製品に組み込む製品（コンポーネント）に変更が生じた場合は、随時記録する。また、製品リリース時に最新情報を運用部門へ展開できるようにする。

- セキュリティに配慮したコーディングについて確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[14]』の「7 セキュアコーディング」をご覧ください。
- 開発環境のセキュリティ確保について詳細を確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[14]』の「8 開発環境のセキュリティ確保」をご覧ください。開発に使う施設・設備、開発中の製品のソースコードや仕様書等、開発に使用するソフトウェア製品それぞれについて、セキュリティを確保するための実施手順について記載されています。

12 https://www.ipa.go.jp/sec/publish/tn16-002.html
13 https://csrc.nist.gov/publications/detail/nistir/8259/final
14 https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

コラム

脆弱性データベースを用いた対応の検討

JVN iPedia は、JPCERT/CC と情報処理推進機構（IPA）が共同で運営する脆弱性情報データベースです。キーワードやベンダ名、製品名等で検索を行い、自社の IoT 機器等で用いる構成要素の脆弱性を調べ、対応を検討しましょう。また、米国国立標準技術研究所（NIST）が運営する脆弱性情報データベース National Vulnerability Database（NVD）も必要性があれば、ご活用ください。
JVN iPedia ホームページ: https://jvndb.jvn.jp/
NVD ホームページ: https://nvd.nist.gov/vuln/search

コラム

外部委託や調達の管理

外部から調達を行う場合には、必要なセキュリティ対策が実施されていない、納品後に脆弱性が発見された場合に対応してもらえないといったトラブルが起きることもあります。機器やモジュールの製造を外部に委託したり、構成要素の調達を行ったりする場合、セキュリティニーズについて取引先に伝えるとともに、納入された機器やモジュールに対して対策がきちんと行われているかを確認する必要があります。また、納品後に脆弱性が検出されたり、インシデントが発生したりした場合の責任や対応方針について、契約項目に含めるようにしましょう。

調達の際に確認すべきポイント

- 製品セキュリティポリシーが策定・開示されているか
- 製品セキュリティサポート方針が明示されているか
- 製品セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか
- 製品セキュリティを確保するための機能（アップデート機能、初期化機能等）があるか
- 基準に則ったセキュリティチェックや検証が行われているか
- 製品及び構成要素の脆弱性情報が収集されているか
- 製品のセキュリティ機能や設定に関する情報が公表されているか

コラム

ソフトウェア管理手法

ソフトウェアの脆弱性管理のために、Software Bill of Materials（SBOM（エスボム）：ソフトウェア部品表）を用いる手法があります。SBOM とは、オープンソフトウェアや商用ソフトウェアを構成するコンポーネントやライセンス、互いの依存関係等をリスト化したものです。サプライチェーンで構成管理ができることから、高いセキュリティが求められる製品分野では活用される動きもあります。

検証フェーズで求められる対策

対策 5　セキュリティに関する要件が満たされているかを検証する

対策を実施しない場合に考えられるリスク

- 出荷後に脆弱性を発見した場合、製品回収等の対応が必要となる。
- 製品に脆弱性が残存し、ユーザに製品が渡った後、ユーザがサイバー攻撃を受ける可能性が高まる。製品が悪用され、ユーザに被害が出た場合には、損害賠償やリコール対応等の対応が必要になる。

最初に取り組む主な対策

- **設計・開発段階から検証計画を立て、セキュリティに関する要件が満たされているか検証し、その結果を踏まえて改善を行いましょう。**
  - 出荷前だけでなく、各段階で必要な検証を行いましょう。
    - 設計・開発フェーズで必要な検証：文書レビュー
    - 検証フェーズで必要な検証：ソフトウェア検証、システム検証
  - 内部での検証が難しい IoT 機器等やインシデントが発生した際の影響が大きい IoT 機器等の検証は、外部の機器検証サービス事業者へ依頼しましょう。第三者による検証を実施することで、想定できていなかったリスクを明らかにできる可能性があります。

インシデントが発生した際の影響が大きい IoT 機器等の例

- **ユーザに財務上の損失や事業継続への影響を生じさせる可能性がある IoT 機器等**
  （例：通信機器、スマートメーターなど電力関連機器、決済端末など金融関係機器　等）
- **ユーザの人命や安全に影響を及ぼす可能性がある IoT 機器等**
  （例：自動車、医療機器、防犯関連機器　等）
- **開発者に多大な賠償責任や法的責任を生じさせる可能性がある IoT 機器等**
  （例：上記の他、個人情報を扱う生活家電、サイバー攻撃により乗っ取られると広範囲に影響を及ぼすネットワークカメラ　等）

外部の機器検証サービス事業者へ依頼する際に留意すべき点

- **検証機器の取扱いや機密保持、検証内容について事前に擦り合わせ及び取り決めを行いましょう。**
- **外部の機器検証サービス事業者による検証を受けたからといって、サイバー攻撃のリスクがゼロになるわけではありません。出荷後も脆弱性への対応を行い、リスク低下に向けた取り組みを定期的かつ継続的に実施しましょう。**

参考資料

- セキュリティ検証の具体的な実施手順を確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[15]』の「9 開発時の脆弱性検査」をご覧ください。以下のように、脆弱性検査の手法について概要や特徴が示されています。

脆弱性検査の手法

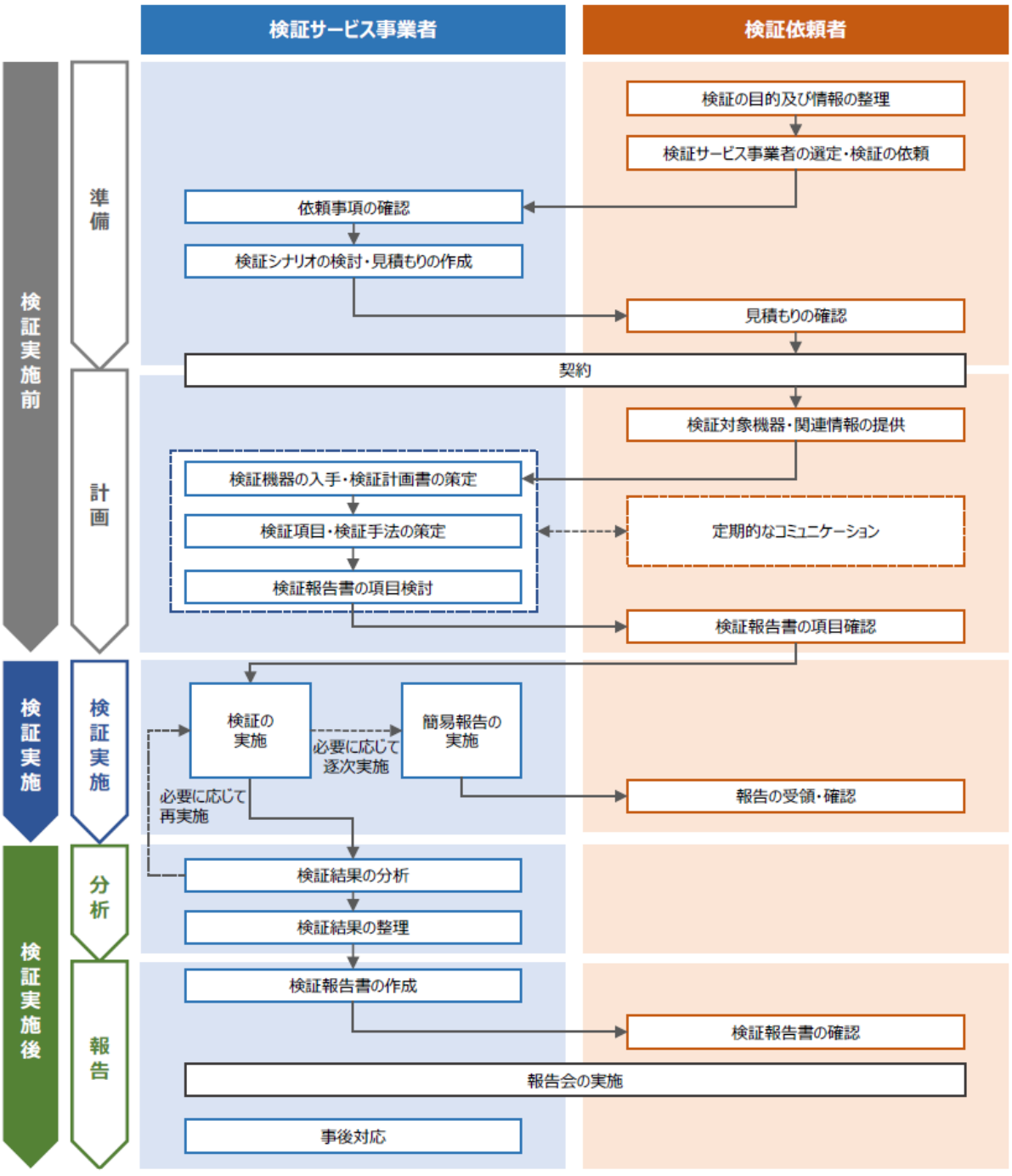
検査名	概要	特徴
ソースコードセキュリティ検査	・ソースコードに作り込んでしまった脆弱性を検出する検査。 ・ソースコードの中の脆弱性を引き起こしやすい関数を見つけたり、構文解析を実施したりします。	・実装の段階で生じる脆弱性を対象に検査することが主です。よって、設計で入り込んでしまう脆弱性や未知の脆弱性は検証できません。
ウェブアプリケーションセキュリティ検査	・文字列を送付したり、ページの遷移を確認したりして、ウェブアプリケーションに特化した脆弱性の存在を検出する検査。	・深刻な被害をもたらすSQLインジェクション等の脆弱性を見つけることができる。 ・実装の段階で作り込まれる脆弱性の発見に向いている。
システムセキュリティ検査	・組み込み構成要素（コンポーネント）等に脆弱性がないか確認するためのリクエストや、バージョンを確認するためのリクエストを送付し、既知の脆弱性が残っていないか、セキュティ上問題のある設定が行われていないか等を検出する検査。	・基本的に既知の脆弱性を見つけることを目的としている。
ファジングによる検査	・脆弱性を発現させやすいデータやファイルを送り込み、脆弱性を検出する検査。	・他の検査では見つけづらい脆弱性が見つけられる。
ペネトレーションテスト	・攻撃者が実際に侵入できるかどうかという点に着目した検査。	・攻撃者がどこまで侵入できるのか、何をされてしまうのか、の検証に着目していることが特徴。 ・ソフトウェアの脆弱性だけではなく、ネットワーク上の不適切な運用についても見つけることができる。

出所）IPA『脆弱性対処に向けた製品開発者向けガイド』

[15] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

- より良い検証サービスを受けるために必要な検証依頼者が実施すべき事項や持つべき知識、並びに検証サービス事業者・検証依頼者間の適切なコミュニケーションのために二者間で共有すべき情報や留意すべき事項について確認したい場合は、経済産業省『機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き[16]』をご覧ください。機器検証の実施手順が以下のように示されており、検証を進める際の各段階において、検証依頼者が実施すべき事項が整理されています。

機器検証の実施手順



出所）経済産業省『機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き

[16] https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

- IoT 特有のリスクに対する品質確認の際にチェックすべき項目について確認したい場合は、IPA『つながる世界の品質確保に向けた手引き[17]』の「中小規模向け IoT 品質確認チェックリスト」をご覧ください。以下で示している 24 項目のチェックリストを活用することで、考慮や対策に漏れがないか自己診断できます。

自己診断チェックリスト

自己診断チェックリスト

対策済／一部対策済／検討中／未着手／対象外

	No.	チェック内容	チェック欄
検証・評価計画	(1)	IoT機器・システムとしての特徴や産業分野の規則など守らなければならない事項などの観点から検証・評価方針を策定していますか？	
	(2)	つながる範囲を明確化して、リスクとコストを意識しながら、検証・評価計画を策定していますか？	
	(3)	検証・評価の結果として残すべき記録（テストの実施環境、実施項目、テスト結果、実行ログなど）が明確になっていますか？	
	(4)	検証・評価計画書やテスト設計書、テストの合否判定の結果に対する合意方法や、トラブルシューティングに関する協力について、関係者間で決めていますか？	
要求仕様レビュー	(5)	IoT特有の機能、性能、将来の拡張を考慮して、要求仕様の妥当性をレビューしていますか？	
	(6)	利用者や利用環境を網羅的に考慮して、要求仕様の妥当性をレビューしていますか？	
	(7)	IoT機器の障害や劣化による影響、セキュリティ対策など、安全安心を考慮して、要求仕様の妥当性をレビューしていますか？	
	(8)	IoT機器・システムを長期的に安定して稼働させるための保守・運用を考慮して、要求仕様の妥当性をレビューしていますか？	
テスト設計	(9)	接続する機器の最大接続数やデータの最大量を考慮したテストや、性能テストを設計していますか？	
	(10)	メーカやバージョンが異なる機器と接続するときの機能の互換性や、システム連携の情報の互換性を考慮したテストを設計していますか？	
	(11)	利用者の特性・スキル、利用場所、利用シーンなどを想定したテストを設計していますか？	
	(12)	機器の故障やシステム障害の発生を想定したテストを設計していますか？	
	(13)	つながることによるセキュリティの脅威やそれがセーフティに及ぼす影響を考慮したテストを設計していますか？	
	(14)	障害解析に必要なログの収集や転送を行う機能、アップデートに関する機能（セキュアな転送、失敗時の回復、負荷・性能など）のテストを設計していますか？	
テスト実施	(15)	テスト設計で抽出したテストを確実に実施するために必要なテスト環境は準備できていますか？	
	(16)	テスト設計で抽出したテストを効率化するための手段を検討していますか？	
	(17)	テストの実行順序や組み合わせを考慮してテストをしていますか？	
	(18)	合否判断の根拠となるエビデンスを残し、テスト実施結果を開発チームと確認していますか？	
	(19)	IoTの機能が当初の目的や目標を満足しているか総合評価し、評価結果を関係者と合意していますか？	
運用計画	(20)	運用中に起こり得るシステムの機能や性能を劣化させる事項を予測し、それらの発生を把握するような監視方法と発生時の対応プロセスを決めていますか？	
	(21)	機能や性能が利用者の視点で目標を達成できているか評価し、評価結果を関係者と共有し、開発にフィードバックするプロセスを決めていますか？	
運用実施	(22)	リリース後の利用環境の変化や最新の技術情報を把握し、対応していますか？	
	(23)	利用者が利用する機能と安全安心に関する機能が正常に維持できていることを、確認していますか？	
	(24)	ソフトウェアの更新時は、接続先システムに影響を与えないことを確認していますか？	

出所）IPA『つながる世界の品質確保に向けた手引き』

[17] https://www.ipa.go.jp/sec/publish/tn18-001.html

運用・保守フェーズで求められる対策

対策 6　出荷後もリスクに関する情報の収集や関係者とのコミュニケーションを行い、適切なサポートを行う

対策を実施しない場合に考えられるリスク

- 製品の脆弱性により、ユーザがサイバー攻撃を受ける可能性が高まる。製品が悪用され、ユーザに被害が出た場合には、損害賠償やリコール対応等の対応が必要になる。
- ユーザに対して適切な情報提供が行われないことにより、新たな脅威に対応することができなかったり、誤った機器の取り扱いやセキュリティ対策が機能しなかったりすることで、ユーザがサイバー攻撃を受ける可能性が高まる。
- インシデントが生じた際のコミュニケーションがうまくできないことにより、対応が遅れ、自社及びユーザの被害が拡大する。

最初に取り組む主な対策

- **世の中で発生している事故やインシデント、脆弱性情報を収集しましょう。自社製品または構成要素に脆弱性が存在する場合、脆弱性によって生じる被害の発生可能性や影響を検討し、リスクに応じた対応を検討します。自社製品に関する問題が見つかった場合は、適切に情報提供を行うほか、セキュリティパッチによる対応を行いましょう。**
  - 商流や販売経路を踏まえ、問題が生じた際の報告先や報告手段を検討しておきましょう。
  - セキュリティパッチでの対応が難しい場合は、代替策を検討し、その旨を報告しましょう。
  - 公表される脆弱性の深刻度は、必ずしも自社製品への影響の大きさを示す訳ではありません。一方、構成要素の脆弱性が潜在的に自社製品に影響することもあります。脆弱性に対しては、製品の開発状況や特性を踏まえ、コストダウンや差別化も意識した上で、自社としての対応方針を定めましょう。
- **製品を選ぶ際に参考となる情報の提供や正しい利用の促進のため、セキュリティに関する機能や利用する際の注意点（サポート期間や廃棄に関する点を含む）について、パッケージや取扱説明書、製品情報を掲載している Web サイト等にわかりやすく記載しましょう。**
- **外注先やユーザと適切なコミュニケーションを実施するための窓口や、JPCERT/CC と脆弱性やインシデントに関する情報のやり取りを行うための窓口を設置しましょう。**

リスクに関する情報の収集先の例

- **IPA ホームページ「重要なセキュリティ情報一覧」**
  https://www.ipa.go.jp/security/announce/alert.html
- **JVN iPedia ホームページ**
  https://jvndb.jvn.jp/
- **JPCERT/CC メーリングリスト**
  https://www.jpcert.or.jp/announce.html

参考資料

- 関係者に対する情報提供のポイントを確認したい場合は、IoT 推進コンソーシアム・総務省・経済産業省『IoT セキュリティガイドライン ver 1.0[18]』の「要点 18：出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える」「要点 19：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」をご覧ください。
- 脆弱性に対する対策情報の公表例を確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[19]』の「11 脆弱性報告の受付・対策情報の公表」をご覧ください。以下のように、公表例が示されています。

対策情報の公表例

☆☆☆☆株式会社 ＞ セキュリティ脆弱性情報 ＞ ○○○○製品

緊急

○○○○製品における××××の脆弱性

公開日 20XX 年 12 月 4 日
最終更新日 20XX 年 12 月 9 日

■概要
○○○○のバージョン△△以前に××××の脆弱性が存在することが判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、○○○○が動作しているコンピュータ上で□□□□が実行されてしまう危険性があります。
この問題の影響を受ける○○○○のバージョンを以下に示しますので、以下の修正プログラムを適用してください。
該当製品をご利用の場合、今後被害が拡大するおそれがあるため、至急、修正プログラムをインストールしてください。

■該当製品の確認方法
影響を受ける製品は以下の製品です。

製品名称　○○○○
該当バージョン
1.5.4 (Windows 版)　以前の全てのバージョン
1.5.4 (Linux 版)　以前の全てのバージョン

使用しているバージョン番号の確認方法は以下の通りです。
1. ○○○○を起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している○○○○のバージョン番号です。

バージョン表示ウィンドウの図 （省略）

■脆弱性の説明
○○○○製品は、ファイルの■■■■のために▽▽▽▽の機能を搭載しています。◎◎◎◎データの一部として提供され▲▲▲▲で配布された▽▽▽▽の機能に、××××の脆弱性が存在するため、外部の第三者からインターネット越しに□□□□を実行される脆弱性が存在します。
※その他の設定および条件

[18] https://www.soumu.go.jp/main_content/000428393.pdf
[19] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

▽▽▽▽の機能が搭載されていないバージョン 1.5.4 以前（Windows 版） を利用している場合、または、この機能が無効化されている場合には、外部の第三者からインターネット越しに□□□□を実行されることはありません。
・CWE-20　不適切な入力確認

■脆弱性がもたらす脅威
システム管理者権限でログインして本ソフトウエアを利用している場合、攻撃が成功すると、悪意のある第三者によってコンピュータを完全に制御されてしまう可能性があります。これにより、悪意のある第三者は、不正プログラムのインストール、データの変更や削除など、システム管理者の権限でコンピュータを任意に操作する可能性があります。
・CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/BS9.8　緊急
・○○製品における技術詳細情報

■対策方法
バージョン 1.5.4.より前の製品を利用されているお客様は、一度製品をアンインストールしてから対策版製品をインストールしてください。バージョン 1.1 以降の製品を利用されているお客様は、修正プログラムをインストールしてください。
各プログラムのインストール方法に関しては同梱の readme.txt を参照してください。

対象製品名称　○○○○
修正プログラムのダウンロード
1.5.5 patch.zip (Windows 版) 20XX.12.4
1.5.5 patch.tgz (Linux 版) 20XX.12.4

・修正プログラムによって置き換えられる設定ファイル
xxxxx.cfg、yyyyy.dif

■回避策
この脆弱性は、次の手順で影響を緩和できる場合があります。
○○○○で使用する管理用ポート番号宛ての通信を、信頼できる IP アドレスのみに限定するよう、ルータ等にてフィルタリング設定を行うことで、攻撃元の範囲を限定することができます。

■関連情報
CVE-20XX-12345678
JVN#12345678 ○○○○製品における××××の脆弱性

■謝辞
□□□の□□□氏よりこの問題をご報告いただき（略）

■更新履歴
20XX.12.4　この脆弱性情報ページを公開しました。
20XX.12.9　脆弱性がもたらす脅威に、システム管理者の権限でコンピュータを任意に操作する際の技術詳細情報を追加しました。

■連絡先
本件に関するお問い合わせはこちら
脆弱性連絡窓口
電話　：03-xxxxx-xxxx (平日 10:00 – 17:00)
メール：example@example.co.jp

出所）IPA『脆弱性対処に向けた製品開発者向けガイド』

- 脆弱性情報の取扱いに関する詳細な解説を確認したい場合は、JPCERT/CC『脆弱性関連情報取扱いガイドライン[20]』をご覧ください。
- 一般消費者に提供すべき情報について確認したい場合は、IPA『脆弱性対処に向けた製品開発者向けガイド[21]』の「12 一般消費者の製品利用時における実施事項の明示」「IV. 一般消費者に向けて実施すべきこと」をご覧ください。「12 一般消費者の製品利用時における実施事項の明示」には、以下のように、利用者の実施事項が示されています。

20 https://www.jpcert.or.jp/vh/vul-guideline2019.pdf
21 https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

利用者の実施事項

利用者の実施事項
■ **利用開始前に実施することの明示** ➢ パスワード設定・ネットワーク接続設定等の初期設定を正しく実施すること ➢ 利用開始時に工場出荷時の製品共通のアカウント・パスワードを変更すること ■ **利用中に実施することの明示** ➢ 製品のアップデート情報や脆弱性対策情報を確認し、必要な対策を実施すること ➢ 製品が提供するセキュリティ機能を利用すること ➢ バックアップや設定内容の記録を行うこと ➢ セキュリティサポートが終了した製品の利用は中止するか、サポート対応中の製品に変更すること ■ **利用終了時に実施することの明示** ➢ 製品を利用しない場合は、ネットワークから切り離すこと ➢ 製品を廃棄する際に保存されているデータを消去すること（初期化等）

出所）IPA『脆弱性対処に向けた製品開発者向けガイド』

- ユーザのセキュリティニーズに対するリスクやサポートに関するユーザとのコミュニケーションについての詳細を確認したい場合は NIST『NISTIR 8259[22]』の「Activity 5：顧客とのコミュニケーション方法の明確化」「Activity 6：顧客に何を伝え、どのように伝えるかを決める」をご覧ください。「Activity 5」では、コミュニケーションアプローチを定義するための質問事項が示されています。

【質問事項】
- 顧客が理解できる専門用語は何か。
- 顧客はどの程度の情報を必要とするか。
- 情報はどこで、どのように提供されるのか。
- 情報の完全性はどのようにして確認されるのか。
- 顧客はメーカである自社とコミュニケーションをとる必要があるか。

コラム

脆弱性関連情報への対応

脆弱性が検出された場合、IPA に脆弱性関連情報を届け出、JPCERT/CC がその公表に関する調整を行うことが推奨されていますが、そのようなプロセスを経ずに脆弱性関連情報が公開されてしまうことがあります。過去の事例では、脆弱性を検出したユーザからの連絡に対して期日までに返答を行わなかったために、SNS で広く脆弱性関連情報を公開されてしまったケースがありました。このようなケースにも対応できるよう、脆弱性関連情報への対応体制を平時から整えておきましょう。

[22] https://csrc.nist.gov/publications/detail/nistir/8259/final

設計・開発フェーズで検討すべき主な技術的対策

現在の IoT 機器等は、位置・温度・動作等の取得やデータ化及び他の機器の制御等いろいろな機能があり、様々な分野で利用が広がっています。一方で、IoT 機器等のこれらの機能を使い重要なデータを扱ったり重要な処理を行ったりするためには、セキュリティ対策が必要になります。そのため、本章では、IoT 機器等で提供する機能と対応する主な技術的対策をまとめました。本ガイドの対策 3 で想定したセキュリティニーズとリスクの検討結果をもとに、以下のセキュリティ対策を参考に、対策を選定し、IoT 機器等への実装を検討してください。

IoT 機器等で提供する機能と対応する主な技術的対策

（1）	通信機能を提供する IoT 機器等	A	認証・認可機能の提供
		B	アップデート機能の提供
		C	ログの保存機能の提供
（2）	データの送信・保存機能を有する IoT 機器等	A	データの暗号化・保護機能の提供
		B	データの削除機能の提供
（3）	高い可用性が求められる IoT 機器等	A	システムの復旧の提供
		B	異常検知機能の提供

機器検証サービス事業者からのアドバイス

本章の内容に関連した対策で、機器検証サービス事業者から IoT 機器等の開発者に向けたアドバイスとして特に注意すべき事項を記載しています。セキュリティ対策の検討のため、活用してください。

国内外のガイドラインや指針との対応関係

本章に記載したセキュリティ対策と国内外のガイドラインや指針との対応関係を示しています。セキュリティ対策に関する詳細な情報が必要な場合は、これらのガイドラインや指針をご覧ください。

なお、本章で示した具体的なセキュリティ対策は、一律に実施を求めるものではなく、本ガイドの対策 3 で示した守るべきものやリスクへの対応に応じて適切なセキュリティ対策を検討するための参考情報として活用してください。

(1) 通信機能を提供する IoT 機器等

A 認証・認可機能の提供

対策
- IoT 機器等のユーザの認証・認可機能を提供する。
- IoT 機器等の通信先認証の機能を提供する。

理由
- IoT 機器等の不正な利用を防ぐ。
- IoT 機器等の通信でユーザの重要なデータの漏えいを防ぐ。

機能の提供には以下を考慮しましょう。
- ユーザ認証の初期パスワードを設定しない。
- クラウドサービスの利用については、認証機能とは別の認可機能を提供する。
- ユーザが接続先(Bluetooth デバイス等)に応じた接続方法を設定でき、設定内容を確認できるようにする。
- 実装する通信プロトコルは、独自のプロトコルを利用せず、標準規格等のオープンな規格を利用する。

B アップデート機能の提供

対策
- 出荷後に新たな脆弱性が検出されることを想定し、ソフトウェアやファームウェアをアップデートできるようにする。

理由
- 新たに検出された脆弱性に対応できず、IoT 機器等を利用できなくなるといった事態を防ぐ。

機能の提供には以下を考慮しましょう。
- ソフトウェアやファームウェアのアップデートに加え、新たなソフトウェアやファームウェアの構成変更ができるようにする。

C ログの保存機能の提供

対策
- IoT 機器等の重要な操作や通信のログを保存する。

理由
- 不正防止や異常検知、インシデント発生時の調査にログを活用できる。

機能の提供には以下を考慮しましょう。
- 意図した接続先と設定通りの通信をしているのかの確認にあたって、後述の「異常検知機能の提供」も検討する。

(2) データの送信・保存機能を有する IoT 機器等

A　データの暗号化・保護機能の提供

対策
- ユーザの個人データや設定データ及びプライバシに関するデータを暗号化して保存・送信できるようにする。

理由
- IoT 機器等に保存しているユーザの重要なデータの漏えいを防ぐ。
- IoT 機器等の通信によるユーザの重要なデータの漏えいを防ぐ。

機能の提供には以下を考慮しましょう。

- 送信データの暗号には、TLS 等のセキュリティプロトコルを利用する。
- 保存データの暗号化にあたって、暗号化アルゴリズムや鍵長を検討し、鍵のハードコードを避ける。
- データの完全性が求められる場合、改ざん防止機能の提供も検討する。

B　データの削除機能の提供

対策
- ユーザが IoT 機器等の利用を終了し、廃棄、返却等する際に、個人データ、設定データ及びプライバシに関するデータを削除できるようにする。

理由
- 利用を終了した IoT 機器等に保存しているユーザの重要なデータの漏えいを防ぐ。

機能の導入には以下を考慮しましょう。

- 個人データ、設定データ及びプライバシに関するデータの範囲や定義を定め、マニュアル等でユーザに示す。

(3) 高い可用性が求められる IoT 機器等

A　システムの復旧の提供

対策
- 高い可用性が求められる機能については、機能停止時の復旧方法を提供する。

理由
- 高い可用性を求められる IoT 機器等の機能停止によるリスクを最小化する。

機能の導入には以下を考慮しましょう。
- システムの復旧だけではなく、異常検知や異常時のアラート等の代替案も考慮する。
- 死活監視する機器やシステムを別途構築することをユーザに推奨する。

B　異常検知機能の提供

対策
- IoT 機器等の動作異常を検知できる機能を提供する。

理由
- 悪意のある第三者による意図しない IoT 機器等の変更や動作の異常が分からないまま使い続けることを防ぐ。

機能の導入には以下を考慮しましょう。
- 検知すべき異常の定義や検知可能な範囲を定め、マニュアル等でユーザに示す。

機器検証サービス事業者からのアドバイス

機器検証サービス事業者からの IoT 機器等の開発者に向けたアドバイスとして、特に注意すべき事項を記載しています。市場にある IoT 機器等の具体的な事例やケースと、対策の例示を参考に検討してください。

なお、現在の IoT 製品には、モバイルアプリを付随する場合も多く、モバイルアプリのバグや API の脆弱性によってインシデントが発生するケースも考えられます。そのため、以下のアドバイスを参考にモバイルアプリの対策も検討してください。

関連項目	具体的なアドバイス
（1）通信機能を提供する IoT 機器等	
A）認証・認可機能の提供	● **パスワード設定** パスワード設定にあたって、推測されやすいパスワードを設定可能なケース、初期パスワードを変更しないで IoT 機器等を利用できるケース、初期パスワードに再変更できるケース等があります。パスワードが推測されにくいよう、機器共通ではない初期パスワードの設定を検討しましょう。また、初期パスワードの変更及び推測されにくいパスワードへの変更をユーザに強制することを検討しましょう。 ● **アクセス権限** 多くの機能を搭載している IoT 機器等において、あらゆるデータや設定にユーザが全てアクセス可能になっているケースがあります。必要に応じて、特定のデータや設定内容のアクセス権限を管理者のみに設定する等の対策を検討しましょう。 ● **管理画面** IoT 機器等が提供する Web 管理画面の入力値検証の不備が見つかることがあります。また、Web アプリで、クロスサイトスクリプティング（XSS）や OS コマンド・インジェクション等の初歩的な脆弱性が検出されるケースもあります。IPA の『安全なウェブサイトの作り方[23]』を参考に、安全な Web 管理画面・アプリの作成に努めましょう。
B）アップデート機能の提供	● **アップデート実施・自動更新** ソフトウェアやファームウェアのアップデート頻度が低いケースが見られます。また、自動更新機能が提供されておらず、適切なアップデートが実施できないケースがあります。適時アップデートを実施するとともに、自動更新機能の提供を検討しましょう。

[23] https://www.ipa.go.jp/security/vuln/websecurity.html

（2）データの送信・保存機能を有する IoT 機器等	
A）データの暗号化・保護機能の提供	● **平文通信・不要なポート** データ送信等の通信に関するセキュリティについて、平文通信しかできないケースや不要なポートを開放しているケースがあります。重要なデータの送信では、通信を暗号化するとともに、不要なポートを開放しないことを検討しましょう。 ● **デバッグポート** デバッグポートの悪用が可能になっているケースがあります。出荷・量産品では、デバックポートを残さないよう検討しましょう。また、デバッグポートを残さざるを得ない場合は、デバッグポートの悪用を防ぐ対策を施すことを検討しましょう。

国内外のガイドラインや指針との対応

本章に記載したセキュリティ対策と国内外のガイドラインや指針との対応関係を示します。セキュリティ対策に関する詳細な情報が必要な場合は、国内外のガイドラインや指針をご覧ください。

ガイドラインや指針 / セキュリティ対策	IoT セキュリティガイドライン[24]/つながる世界の開発指針[25]	脆弱性対処に向けた製品開発者向けガイド[26]	米国 NISTIR 8259A[27]	英国 消費者向け IoT 製品のセキュリティに関する行動規範[28]
（1）通信機能を提供する IoT 機器等				
A）認証・認可機能の提供	要点 11, 14, 15, 16/指針 11, 14, 16	-	No.4	No.1, 5
B）アップデート機能の提供	要点 17/指針 14	No.5	No.2, 5	No.3, 7
C）ログの保存機能の提供	要点 13/指針 13	No.4	No.6	-
（2）データの送信・保存機能を有する IoT 機器等				
A）データの暗号化・保護機能の提供	要点 13, 14, 15/指針 13, 14	No.4	No.3	No.4, 5, 8
B）データの削除機能の提供	（一般利用者ルール 4）	-	-	No.11
（3）高い可用性が求められる IoT 機器等				
A）システムの復旧の提供	要点 9/指針 9	-	-	No.9
B）異常検知機能の提供	要点 9/指針 9	No.4	-	No.7, 10

[24] https://www.soumu.go.jp/main_content/000428393.pdf
[25] https://www.ipa.go.jp/sec/publish/tn16-002.html
[26] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html
[27] https://csrc.nist.gov/publications/detail/nistir/8259a/final
[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973920/054718_DCMS_IoT_Code_of_Practice_JAPANESE_V2.pdf

IoT 機器等を開発する中小企業の対策事例集

本事例集では、中小企業 5 社による実際の対策事例を示しています。それぞれの企業の状況に応じて、どのような対策を実施すれば良いかについての参考としてください。

事例掲載企業一覧

企業名	製品種	消費者向け 産業向け	従業員数	資本金
株式会社 SYNCHRO	アプライアンス製品	産業向け	10～19 人	1～3 億円未満
GROOVE X 株式会社	ロボット	消費者向け	100～199 人	5 千万～ 1 億円未満
ソナス 株式会社	無線モジュール・ センサー	産業向け	30～49 人	1～3 億円未満
A 社	CPU ボード・ ゲートウェイ	産業向け	50～99 人	1～3 億円未満
B 社	モバイルルーター	消費者向け	10～19 人	5 百～1 千万円 未満

<table>
<tr><th colspan="4">株式会社 SYNCHRO のセキュリティ対策事例</th></tr>
<tr><td>製品種</td><td>アプライアンス製品</td><td>消費者/産業向け</td><td>産業向け</td></tr>
<tr><td>従業員数</td><td>10～19 名</td><td>資本金</td><td>1～3 億円未満</td></tr>
<tr><td>対策のポイント</td><td colspan="3">● 社内開発のほか、開発パートナーに製品開発を委託している部分もあり、パートナーやエンドユーザと相談しながらセキュリティ対策を実施している。</td></tr>
<tr><td>対策内容</td><td colspan="3">方針・体制構築フェーズの対策
● 必要なセキュリティ対策を社内で検討し、そのセキュリティ対策に対応可能な開発パートナーを選定している。
● 情報の授受は、メールではなく、全てオンプレミスのビジネスチャットシステムで行っている。
 
設計・開発フェーズの対策
● デザインレビューを行い、セキュリティ対策について検討している。可能な場合は、社外の方にも協力いただき、コストや期間といった観点を含めたレビューを実施している。
● ファジングを考慮した設計仕様書及び試験仕様書を設計段階で作成している。
● 対策にかかるコストを考慮した上で、セキュリティ対策の範囲と実施可否についての検討を行っている。
検証フェーズの対策
● まずインターナルテストを社内で実施し、次にパートナーやエンドユーザも交えてシステムテストを実施している。システムテストは NG 項目がなくなるまで行う。
運用・保守フェーズの対策
● 搭載 OS や使用している OSS のアップデート状況をチェックし、重大な脆弱性がある場合はアップデートの実施または推奨を行っている。
● 運用を止めてはいけないケースが多いため、安定稼働とのバランスを考え、稼働に影響するおそれがある場合は、パートナーやエンドユーザと相談し、回避策やリスク緩和策を講じた上で、アップデートの実施を見送る場合もある。</td></tr>
<tr><td>対策に力を入れたことによるメリット</td><td colspan="3">● 検討したセキュリティ対策に対応可能な開発パートナーを選定することで、開発プロジェクト全体でのセキュリティ対策を強化できた。
● オンプレミスのビジネスチャットシステムを活用することで、ソースコードの授受も可能な高いセキュリティ性能の確保と、暗号化不要で機密情報の授受が可能という利便性の両立が可能となった。
● 設計段階で試験仕様を立案することで、設計精度の向上と試験項目の漏れ防止が可能となった。</td></tr>
</table>

<table>
<tr><th colspan="4">GROOVE X 株式会社のセキュリティ対策事例</th></tr>
<tr><td>製品種</td><td>ロボット</td><td>消費者/産業向け</td><td>消費者向け</td></tr>
<tr><td>従業員数</td><td>100～199 名</td><td>資本金</td><td>1 千万～1 億円未満</td></tr>
<tr><td>対策のポイント</td><td colspan="3">● 開発リソースが限られているスタートアップ企業であったが、開発当初からセキュリティに対する高い意識をもって対策を進めていた。
● セキュリティコンサルタントと共に脅威分析を実施し、ユーザの個人情報の保護とアップデート対応できない機能を最優先に対策を実施した。</td></tr>
<tr><td>対策内容</td><td colspan="3">方針・体制構築フェーズの対策
● 開発初期に、セキュリティ検討チームを立ち上げた。
● 個人情報に関するデータ（画像や音声等）を扱うため、データ収集方針としてユーザの信頼を第一に定めた。
● 収集したデータの管理体制として、システムのセキュリティポリシーを定めた社内セキュリティガイドラインを作成し、システム毎に管理者を定義して、セキュリティ対策の更新やアクセス権限の管理を実施している。
 
設計・開発フェーズの対策
● セキュリティ検討チームで、ユーザストーリーから懸念の洗い出しを行った。また IPA 等のガイドラインの勉強を行い、OS・認証・通信・コーディングにおけるセキュリティ要件定義を実施した。
● より網羅的に検討するため、セキュリティコンサルタントに依頼して脅威分析を行った。コンサルタントと共に対策すべき全体量を洗い出し、個人情報やアップデートで対応できない箇所等、優先順位を決めて対策を実施した。
● データ収集方針のもと、暗号化保存やユーザで収集をオフにできる仕組み等、個人情報を安易に収集・閲覧できない仕組みを構築した。
検証フェーズの対策
● メジャーアップデート配信毎に、社内で規定した検証項目を実施している。
運用・保守フェーズの対策
● ユーザから個人情報や通信の安全性に関する質問が多数寄せられたため、セキュリティ対策を図解でわかりやすく説明できる資料を準備した。
● 社内セキュリティガイドラインに則り、個人情報を管理しているシステムのアクセス権限を定期的に見直している。
● 「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[29]」に基づき、脆弱性発見時の対応について JPCERT/CC に相談できるようにしている。</td></tr>
<tr><td>対策に力を入れたことによるメリット</td><td colspan="3">● 個人情報の漏洩防止はもちろん、ユーザへの情報開示を積極的に行うことで問い合わせへもスムーズに回答でき、安心して利用いただいている。</td></tr>
</table>

[29] 経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」を踏まえ、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたもの。

<table>
<tr><th colspan="4">ソナス株式会社のセキュリティ対策事例</th></tr>
<tr><td>製品種</td><td>無線モジュール・センサー</td><td>消費者/産業向け</td><td>産業向け</td></tr>
<tr><td>従業員数</td><td>30～49 名</td><td>資本金</td><td>1～3 億円未満</td></tr>
<tr><td>対策のポイント</td><td colspan="3">● スタートアップで技術の商品化に取り組んでおり、社内体制が整備できている段階ではないが、顧客からセキュリティの確保を求められていることもあり、エンジニアの意識やスキルが高く、連携しながら、積極的にセキュリティ対策を実施している。
● 社長に直接報告や相談をしやすい環境であり、セキュリティに関して課題があれば、社内でスピード感を持って対応することが可能である。</td></tr>
<tr><td>対策内容</td><td colspan="3">方針・体制構築フェーズの対策
● エンジニアの個々のスキルに立脚しつつも、相互に補完し合いながらセキュリティ対策を実施している。
設計・開発フェーズの対策
● 議論ベースで脅威分析や設計の確認を行っている。
● 暗号化、認証、メモリ管理といった開発時の一般的なセキュリティ対策を実施している。
● GitHub や Jira といったツールを用いて構成管理を実施している。
● 開発環境のネットワークと業務ネットワークを分離している。
 
検証フェーズの対策
● 社内の品質管理担当者が、典型的な攻撃の可否や開発者が提示したテスト項目について、製品出荷前に確認している。
運用・保守フェーズの対策
● JPCERT/CC のメーリングリストや JVN 脆弱性レポート、SNS 等から脆弱性情報を入手している。
● 製品のサポート期間を納入仕様書に記載している。
● 製品に問題が発生した際の電話とメールのサポート窓口を一本化している。</td></tr>
<tr><td>対策に力を入れたことによるメリット</td><td colspan="3">● セキュリティ対策が実施できていることが当たり前のこととして顧客から捉えられている。対策の不備により生じうる負の影響が発生しないことがメリットと認識している。</td></tr>
</table>

A 社のセキュリティ対策事例			
製品種	CPU ボード・ゲートウェイ	消費者/産業向け	産業向け
従業員数	50～99 人	資本金	1～3 億円未満
対策のポイント	● **開発部門のセキュリティ意識や技術力が高く**、国内外の規格を元にした独自のセキュリティポリシーに基づき、セキュリティ対策の実施を行っている。 ● 半完成品を扱っているため、ハードウェアセキュリティは自社の責任とする一方、OSS をベースとした**ソフトウェアのソースコードと仕様は全て公開し、ソフトウェアに関する対策責任は顧客として、契約で責任範囲を定めている**。 ● 出荷後も顧客と頻繁にコミュニケーションを取り、**顧客のリクエストに応じて、セキュリティに関するアドバイスを実施**している。 ● **最新製品ではソフトウェアアップデートを OTA[30]で毎月実施**している。		
対策内容	**方針・体制構築フェーズの対策** ● 電気通信事業法のセキュリティ対策基準に基づく JATE（一般財団法人電気通信端末機器審査協会）の認証基準をベースとして、**独自のセキュリティポリシーを作成**し、自社の IoT 製品全てに適用している。本ポリシーは**社内 Wiki に掲載しており、開発時やレビュー時に参照**している。 **設計・開発フェーズの対策** ● **IPA の『つながる世界の開発指針[31]』等のガイドラインの記載内容に基づき、製品のセキュリティニーズについて検討**している。 ● ETSI EN 303 645[32]の要件のもと、リスク分析を行っている。 ● セキュアコーディングが実現できているか、自動化テストで確認している。 **検証フェーズの対策** ● 製品のセキュリティ対策に関して、**開発の開始時点及び出荷前の時点でレビュー**を行っている。 **運用・保守フェーズの対策** ● 開発部門の大半が **JPCERT/CC や Debian のメーリングリストに登録**し、脆弱性情報の収集を行っている。 ● ソフトウェアアップデートに併せて**セキュリティに関するニュースを配信**している。 ● **脆弱性情報の受付フォームを設置**している。		
対策に力を入れたことによるメリット	● OTA 機能の実装についてアピールを行ったところ、**セキュリティに関心がある顧客にも訴求ができるようになり、売り上げの幅が広がった**。 ● 製品に搭載している SoC[33]のセキュリティ機能を使いこなしているため、**SoC ベンダからのサポート**を受けやすくなった。		

[30] Over-the-Air、無線通信経由によるソフトウェアアップデート
[31] https://www.ipa.go.jp/sec/publish/tn16-002.html
[32] 欧州電気通信標準化機構（ETSI）が定める消費者向け IoT 機器におけるセキュリティ規格
[33] System on a chip、システムの機能を1つの半導体チップで実現するデバイス

<table>
<tr><th colspan="4">B 社のセキュリティ対策事例</th></tr>
<tr><td>製品種</td><td>モバイルルーター</td><td>消費者/産業向け</td><td>消費者向け</td></tr>
<tr><td>従業員数</td><td>10～19 名</td><td>資本金</td><td>5 百～1 千万円未満</td></tr>
<tr><td>対策のポイント</td><td colspan="3">● 開発メンバーの議論を基に、利便性やコストとのバランスを踏まえ、社長が製品に実装するセキュリティ対策の選定を行っている。
● 第三者による検証を活用し、実施したセキュリティ対策に不備がないかを確認している。</td></tr>
<tr><td>対策内容</td><td colspan="3">方針・体制構築フェーズの対策
● 小規模な組織であるため、セキュリティ対策に関するポリシーは文書化していないが、各開発メンバーの最新の知識を基にセキュリティ対策を実施している。
 
設計・開発フェーズの対策
● どのようなユースケースが想定されるかを開発メンバーで議論した上で、実施するセキュリティ対策について検討し、最終的には社長が判断を行っている。特に、利用者による設定のカスタマイズ性、コスト、セキュリティとのバランスを意識した開発を行っている。
● 機器に対するポートスキャンを実施しているほか、クロスサイトスクリプティングのような代表的な脆弱性について留意したコーディングを行っている。また、Git を用いた構成管理も実施している。
検証フェーズの対策
● 脆弱性の検出を目的として、製品出荷前または製品出荷後に、セキュリティ検証事業者に検証を依頼している。基本的な検証については、数百万円程度を想定している。
運用・保守フェーズの対策
● 遠隔でファームウェアのアップデートができる仕組みを整えている。</td></tr>
<tr><td>対策に力を入れたことによるメリット</td><td colspan="3">● 利用者からのセキュリティに対する要望が高い状況になく、目に見えるメリットは感じにくいが、製品を安心して使用いただくための取り組みとしてセキュリティ対策を実施している。</td></tr>
</table>

付録 1 用語集

■ **IoT(Internet of Things)**

既存又は開発中の相互運用可能な情報通信技術により、物理的又は仮想的なモノをネットワーク接続した、高度なサービスを実現するグローバルインフラ。[IoT セキュリティガイドライン ver 1.0]

■ **IoT 機器等**

ネットワークに常時接続される機器及び機器に使用される部品等。

■ **JPCERT/CC(コーディネーションセンター)**

日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う民間の非営利団体。

■ **TLS(Transport Layer Security)**

インターネット上で暗号化したデータを送受信するためのプロトコルである SSL(Secure Sockets Layer)をもとに開発された後継規格。

■ **鍵長**

データの暗号化や復号に用いられる暗号鍵の長さ。

■ **可用性**

機器やシステムが継続して稼働できる能力。

■ **脅威**

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。[JIS Q 27000:2014]

■ **脅威分析**

機器やソフトウェア、システム等に対する脅威を抽出し、その影響を評価すること。

■ **脅威分析モデル**

脅威分析において、脅威を洗い出すために使われるモデル。例えば、STRIDE モデルでは、攻撃側の視点で脅威を Spoofing(偽造)、Tampering(改竄)、Repudiation(否認)、Information Disclosure(情報漏洩)、Denial of service (サービス拒否)、Elevation of privilege(権限昇格)の 6 つに分類する。

■ **機器検証サービス事業者**

機器に対してセキュリティ検証をサービスとして提供している事業者。

■ **クロスサイトスクリプティング（XSS）**

管理画面等の Web ページへの出力処理に問題があることで、その Web ページにスクリプト等を埋め込まれてしまう脆弱性。

■ **構成管理**

システムを構成する要素の管理を行うこと。

■ **OS コマンド・インジェクション**

外部からの攻撃により、Web サーバの OS コマンドを不正に実行されてしまう脆弱性。

■ **サイバー攻撃**

資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000:2014]

■ **サイバーセキュリティ**

電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。

■ **死活監視**

機器やシステムが稼働しているかどうかを外部から継続的に監視すること。

■ **脆弱性**

一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q 27000:2014]

■ **脆弱性検証**

脆弱性の存在を確認するアクティブなセキュリティ検証手法。[NIST SP 800-115]

■ **PSIRT（Product Security Incident Response Team）**

製品セキュリティインシデント対応チームのことで、自社製品のセキュリティの向上を担い、インシデントが発生した際に対応する組織。

■ **セキュアコーディング**

サイバー攻撃に耐え得る堅牢なプログラミングを行うこと。

■ **セキュリティ検証**

機器、システム、組織における脅威に対するセキュリティ対策の妥当性や脆弱性の有無を確認する手法。

■ **セキュリティパッチ**

セキュリティ上の問題が発覚したときに配布される修正プログラム。

■ **入力値検証**

入力値が期待している形式かどうかを確かめる処理。

■ **認証**

エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000:2014]

■ **認可**

アクセス権限に基づいたアクセス機能の提供を含む権限の付与 [ISO 7498-2:1989]

■ **ハードコード**

ソースコード中で動作環境や利用条件に応じて変えるべき変数を、定数や文字列等の形式で書き込むこと。

■ **平文**

暗号化されていないデータ。

■ **ユースケース図**

ソフトウェアやコンピュータシステムの開発段階で作成する、利用者の要求や利用目的を明確に定義したユースケースを図示したもの。

■ **ライフサイクル**

ある製品が開発され、市場に出てから売れ、最終的に廃棄されるまでの一連の過程。

■ **リスク**

目的に対する不確かさの影響。[JIS Q 27000:2014]

付録 2 参考文書

- 脆弱性対処に向けた製品開発者向けガイド（IPA）
  https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

- 製品セキュリティインシデント対応チーム（PSIRT）成熟度ドキュメント（FIRST）
  https://www.jpcert.or.jp/tips/2022/wr222901.html

- サイバーセキュリティ体制構築・人材確保の手引き（第 2.0 版）（経済産業省・IPA）
  https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html

- NISTIR 8259（NIST）
  https://csrc.nist.gov/publications/detail/nistir/8259/final

- NISTIR 8259A（NIST）
  https://csrc.nist.gov/publications/detail/nistir/8259a/final

- 機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き（経済産業省）
  https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

- IoT 開発におけるセキュリティ設計の手引き（IPA）
  https://www.ipa.go.jp/security/iot/iotguide.html

- IoT セキュリティ・セーフティ・フレームワーク（経済産業省）
  https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

- つながる世界の開発指針（IPA）
  https://www.ipa.go.jp/sec/publish/tn16-002.html

- つながる世界の品質確保に向けた手引き（IPA）
  https://www.ipa.go.jp/sec/publish/tn18-001.html

- IoT セキュリティガイドライン ver 1.0（IoT 推進コンソーシアム・総務省・経済産業省）
  https://www.soumu.go.jp/main_content/000428393.pdf

- 脆弱性関連情報取扱いガイドライン Ver 6.1（JPCERT/CC）
  https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

- 安全なウェブサイトの作り方（IPA）
  https://www.ipa.go.jp/security/vuln/websecurity.html

- 消費者向け IoT 製品のセキュリティに関する行動規範（英国 デジタル・文化・メディア・スポーツ省）
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973920/054718_DCMS_IoT_Code_of_Practice_JAPANESE_V2.pdf

- Secure Software Development Framework（NIST）
  https://csrc.nist.gov/publications/detail/sp/800-218/final