経済産業省

IoT機器等を開発する中小企業向け
製品セキュリティ対策ガイド
概要版

経済産業省　商務情報政策局
サイバーセキュリティ課

経営者の皆様へ　～　IoT機器等の開発時のセキュリティ向上に向けて

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。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、経営に対して多大な不利益が生じる可能性もあります。

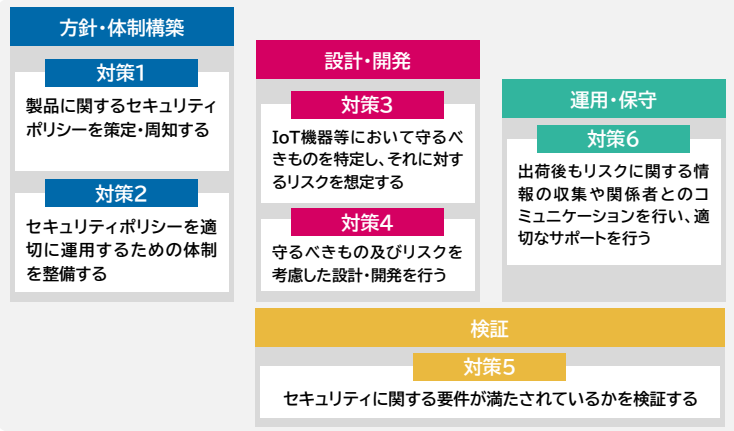
【事例】 脆弱な家庭用ネットワークカメラの開発企業に対する訴訟

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！

- 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、セキュリティ検証が有効です。しかし、出荷前の検証で問題が発見された場合、製品の販売に影響が出るほか、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る可能性もあります。そのため、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、対策に取り組もうとする企業には、何から始めてよいかがわかりにくい場合があります。 → 対策を進める際、最初に取り組む事項
  - 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。 → 対策を効果的に進める中小企業の事例集



- 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！

- 対策によってセキュリティ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。

経営者が率先して推進すべきセキュリティ対策

- ✓ 開発者への対策指示、企業の対策方針の検討、予算や人材の割当
- ✓ 部品の調達先や保守の委託先を含めた対策
- ✓ インシデントに備えた、平時からの社内外関係者との信頼関係構築

「IoT機器等を開発する中小企業向け製品セキュリティ対策ガイド」全体概要

ガイドの基本的な考え方

- 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、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、セキュリティ検証が有効です。しかし、**出荷前の検証で問題が発見**された場合には、**製品の販売に影響が出る**ことも考えられるほか、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。そのため、**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、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**場合があります。
  → **IoT機器等のセキュリティ対策を行おうとする企業が第一歩として取り組む対策を提示**

- 本ガイドに示した対策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など、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。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。
  → **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を掲載**

ガイドの想定読者の方

- 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。

各フェーズで求められる対策

方針・体制構築

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

設計・開発

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4
守るべきもの及びリスクを考慮した設計・開発を行う

運用・保守

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

検証

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

設計・開発フェーズで検討すべき主な技術的対策

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	(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

「各フェーズで求められる対策」

- **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**を示している。

節	項目	最初に取り組む主な対策
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	• 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。
	【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	• 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。
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	• 想定されるユーザ及びユースケースを定めましょう。 • 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。 • 守るべきものに対する多様なリスクを想定しましょう。
	【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。 • 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。
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	• 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。
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	• 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。 • 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。

「設計・開発フェーズで検討すべき主な技術的対策」

- **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機器等で提供する機能毎**に示している。

機能等の特徴	主な技術的対策	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	• 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。
	B) アップデート機能の提供	• 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。
	C) ログの保存機能の提供	• IoT機器等の重要な操作や通信のログを保存する。
(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	• 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。
	B) データの削除機能の提供	• 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。
(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	• 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。
	B) 異常検知機能の提供	• IoT機器等の動作異常を検知できる機能を提供する。

「IoT機器を開発する中小企業の対策事例集」

- セキュリティ対策を効果的に進める中小企業による実際の対策事例を示すことで、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する。
- 企業や製品の基本情報のほか、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を記載している。

事例集に掲載している中小企業

	製品種	消費者/産業向け	従業員数	資本金	対策のポイント
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	• 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。
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	• 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。 • 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。
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	• 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。 • 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。
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	• 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、セキュリティ対策を実施。 • 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、契約において責任範囲を設定。 • 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。 • 最新製品ではソフトウェアアップデートをOTA（Over-the-Air：無線通信経由）で毎月実施。
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	• 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を選定。 • 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。