

参考：サイバーセキュリティ対策について

I o T製品のサイバーセキュリティを確保するためにセキュリティ検証が有効ですが、製品の出荷前の検証だけでは、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、そのことで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。以下に、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ます。

【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。

【対策3】 I o T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

- 想定されるユーザー及びユースケースを定めましょう。
- ユーザー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I o T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ましょう。
- I o T機器等のすべての構成要素（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。
- 攻撃対象となる場所を最小限に抑えましょう。
- ミスユースケースを想定しましょう。
- 施設や環境のセキュリティ確保に努めましょう。
- 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すべ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。

【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。

【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サイト等に分かりやすく記載しましょう。
- 外注先やユーザー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。

詳細は、以下URLをご参照ください。

<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>

(<https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide.pdf>)

また、サイバーセキュリティ対策については、以下URLもご参照ください。

<サイバーセキュリティ経営ガイドライン>

(https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf)

<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（経産省公表）>

(https://www.meti.go.jp/policy/netsecurity/wg3/akakenshou_tebiki_202205kaitei.pdf)

<EC サイト構築・運用セキュリティガイドライン（IPA公表）>

(<https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html>)