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。

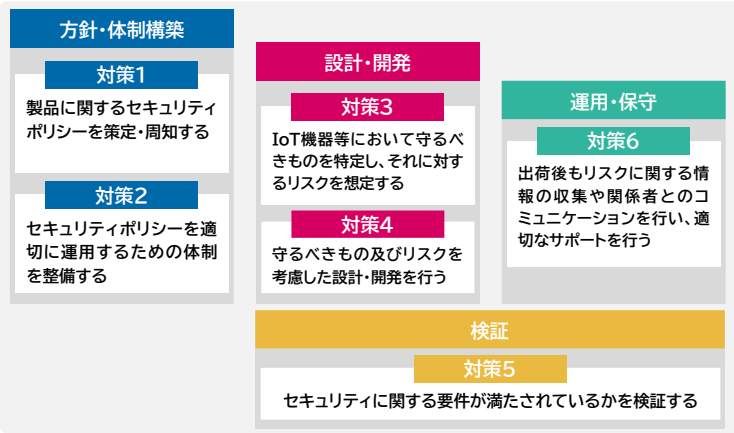
本ガイドでは、IoT機器等にセキュリティ対策を行う第一歩として取り組んでいただきたいことを示しています！

- 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。
  - 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。
  - より高いレベルのセキュリティ対策を目指す場合、**「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」※のラベル取得を目指すことが一つの指標**となります。

対策を進める際、最初に取り組む事項

対策を効果的に進める中小企業の事例集

JC-STARのラベル取得に向けた参考情報



- 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

※ IPA, セキュリティ要件適合評価及びラベリング制度（JC-STAR）https://www.ipa.go.jp/security/jc-star/index.html