IPA Better Life with IT

「つながる世界の開発指針」 Part2: １７指針の解説

SECセミナー

2016年6月27日

独立行政法人情報処理推進機構（IPA)
技術本部ソフトウェア高信頼化センター（SEC)
研究員　小崎 光義

開発指針一覧

IoT機器/システムの開発者が安全/安心の確保のために最低限検討して欲しい事項を、開発ライフサイクルに沿って17の指針として整理。

「つながる世界の開発指針」の内容

目次：
- 第一章 つながる世界と開発指針の目的
- 第二章 開発指針の対象
- 第三章 つながる世界のリスク想定
- 第四章 つながる世界の開発指針（17指針）
- 第五章 今後必要となる対策技術例

※各指針毎にポイント・解説・対策例を記載

http://www.ipa.go.jp/files/000051411.pdf

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針1 安全安心の基本方針を策定する
		指針2 安全安心のための体制・人材を見直す
		指針3 内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する
		指針5 つながることによるリスクを想定する
		指針6 つながりで波及するリスクを想定する
		指針7 物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする
		指針9 つながる相手に迷惑をかけない設計をする
		指針10 安全安心を実現する設計の整合性をとる
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける
		指針14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針17 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

開発企業における開発指針の使い方

SEC Software Reliability Enhancement Center

◆ 開発指針の利活用方針

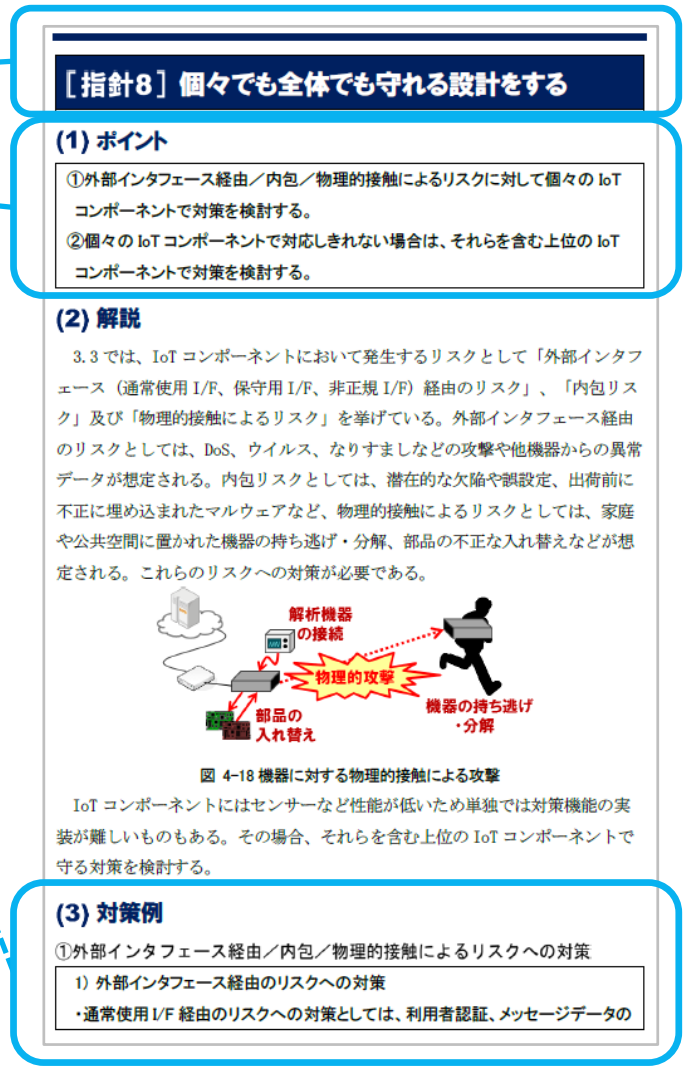
開発指針

各指針のポイントは必ず検討すべき内容

対策の実施は当事者の判断とする。実施する場合は各指針の対策例が参考となる

◆ 開発指針の利活用方法

- IoT製品やシステムの開発時のチェックリストとして利用する。
- 指針で記述している事項は、検討時に企業や団体、業界の実情に合わせてカスタマイズして利用する。
- 内部での開発のみならず受発注の要件確認にも活用する。
- チェック結果を取組みのエビデンスとして活用する。



［指針8］個々でも全体でも守れる設計をする

(1) ポイント

①外部インタフェース経由／内包／物理的接触によるリスクに対して個々の IoT コンポーネントで対策を検討する。
②個々の IoT コンポーネントで対応しきれない場合は、それらを含む上位の IoT コンポーネントで対策を検討する。

(2) 解説

3.3 では、IoT コンポーネントにおいて発生するリスクとして「外部インタフェース（通常使用 I/F、保守用 I/F、非正規 I/F）経由のリスク」、「内包リスク」及び「物理的接触によるリスク」を挙げている。外部インタフェース経由のリスクとしては、DoS、ウイルス、なりすましなどの攻撃や他機器からの異常データが想定される。内包リスクとしては、潜在的な欠陥や誤設定、出荷前に不正に埋め込まれたマルウェアなど、物理的接触によるリスクとしては、家庭や公共空間に置かれた機器の持ち逃げ・分解、部品の不正な入れ替えなどが想定される。これらのリスクへの対策が必要である。

図 4-18 機器に対する物理的接触による攻撃

IoT コンポーネントにはセンサーなど性能が低いため単独では対策機能の実装が難しいものもある。その場合、それらを含む上位の IoT コンポーネントで守る対策を検討する。

(3) 対策例

①外部インタフェース経由／内包／物理的接触によるリスクへの対策

1) 外部インタフェース経由のリスクへの対策
・通常使用 I/F 経由のリスクへの対策としては、利用者認証、メッセージデータの

［指針1］安全安心の基本方針を策定する

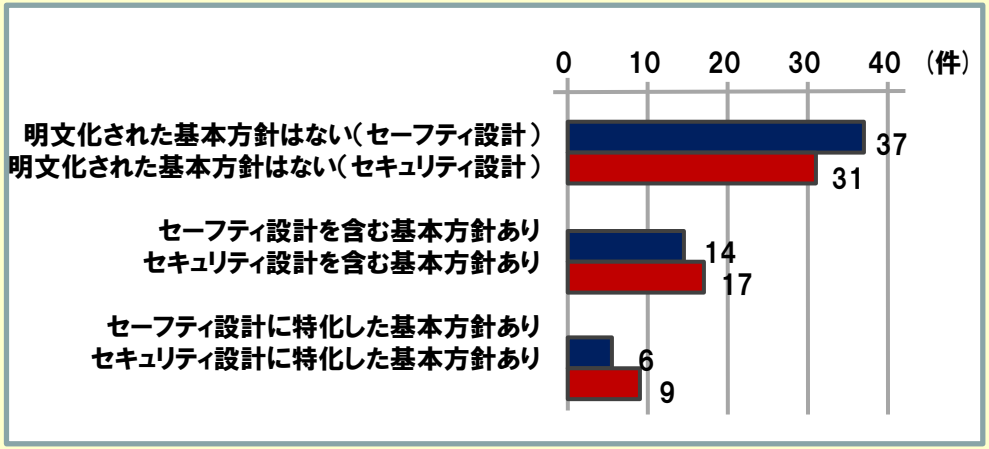
SEC Software Reliability Enhancement Center

ポイント

①経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。

解説

・現状、セーフティとセキュリティ設計の基本方針を策定している企業は少ない。



・両基本方針の策定、企業内への周知、遵守状況の把握及び見直しが必要。

対策例

1)企業が考慮すべき項目例

・安全安心な管理体制の確立および関連規程の整備・遵守など

2) つながる世界で必要となる事項

・企画・設計段階からの安全安心への取組み（Safety & Security by Design）、
・つながる世界の安全安心対策の検証・評価の方針
・つながる世界の事故やインシデントへの迅速な対応方針
・継続的な実現状況の把握と見直し　など

[指針2] 安全安心のための体制・人材を見直す

SEC Software Reliability Enhancement Center

ポイント

①つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。
②そのための人材（開発担当者や保守担当者など）を確保・育成する。

解説

つながる世界では、想定外の問題が発生したり、影響が広域に波及するため、
・緊急対応や抜本的対策を行う体制が必要

・知識や技術を活用して対応に当たる人材の確保・育成が必要

対策例

1)安全安心に関する体制や環境の例
- 製品安全に関する事業者ハンドブック
- CSIRT（シーサート）
- リスク対策効果の検証環境　など

2)人材育成に有用な情報源の例
- つながる世界のセーフティ＆セキュリティ設計入門
- 組込みシステムのセキュリティへの取組みガイド　など

［指針3］内部不正やミスに備える

SEC Software Reliability Enhancement Center

ポイント

①つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。
②関係者のミスを防ぐとともに、ミスがあっても安全安心を守る対策を検討する。

解説

・事例が増えているIoTサービスにおける内部不正への対策が必要。
・また、標的型攻撃メールなどにより機器やシステムの設計情報が漏えいしないよう、ミスへの対策も必要。

対策例

1) 内部不正への対策例

企業内の問題の把握及び是正（教育など）

表　内部不正の基本 5 原則

基本5原則	概要
犯行を難しくする(やりにくくする)	対策を強化することで犯罪行為を難しくする
捕まるリスクを高める（やると見つかる）	管理や監視を強化することで捕まるリスクを高める
犯行の見返りを減らす（割に合わない）	標的を隠す/排除する、利益をなくすことで犯行を防ぐ
犯行の誘因を減らす（その気にさせない）	犯罪を行う気持ちにさせないことで犯行を抑止する
犯罪の弁明をさせない（言い訳させない）	犯行者による自らの行為の正当化理由を排除する

出典：IPA「組織における内部不正防止ガイドライン」より

2) 社員のミスや違反への対策例

・標的型攻撃への対応など

[指針4] 守るべきものを特定する

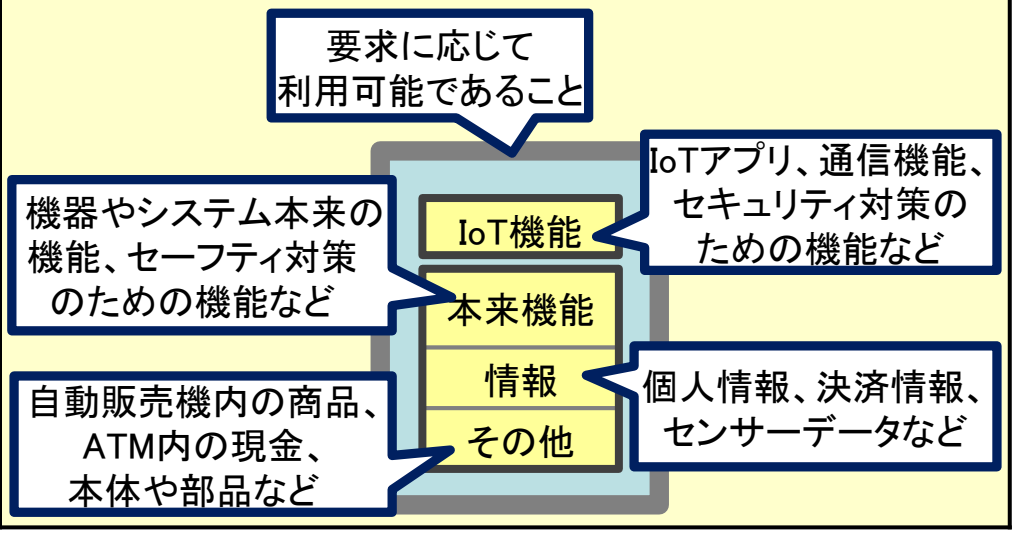
SEC Software Reliability Enhancement Center

ポイント

①つながる世界の安全安心の観点で、守るべき本来機能や情報などを特定する。
②つなげるための機能（IoT機能）についても、本来機能や情報の安全安心のために、守るべきものとして特定する。

解説

つながる世界において、IoTコンポーネントの守るべきものを特定。



対策例

・守るべきIoT機能、本来機能、情報、その他の洗い出し

表　守るべき情報の例

情報資産	説明
コンテンツ	音声、画像、動画、コンテンツ利用履歴等
ユーザ情報	ユーザの個人情報、ユーザ認証情報、利用・操作履歴等
機器情報	情報家電そのものに関する情報、機器認証情報等
ソフトウェアの状態情報	各ソフトウェアに固有の状態情報
ソフトウェアの設定情報	各ソフトウェアに固有の設定情報
ソフトウェア	OS、ミドルウェア、アプリケーション等
設計情報、内部ロジック	仕様・設計等の設計情報

出典：IPA「組込みシステムのセキュリティへの取組みガイド」を基に作成

[指針5] つながることによるリスクを想定する

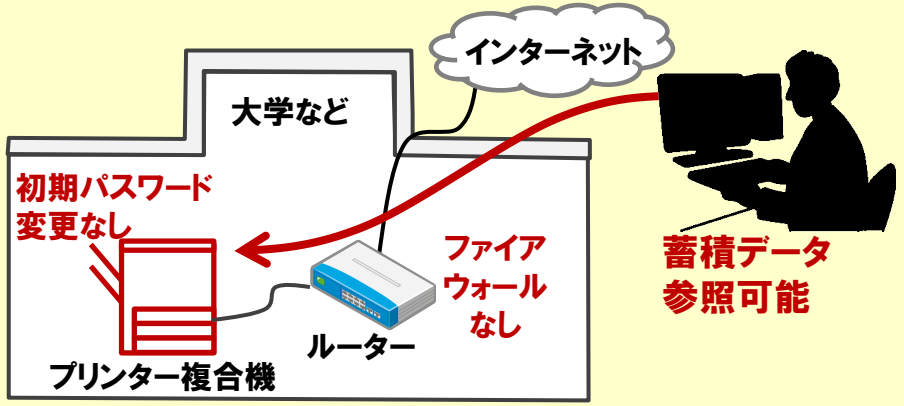
SEC Software Reliability Enhancement Center

ポイント

①クローズドなネットワーク向けの機器やシステムであっても、IoTコンポーネントとして使われる前提でリスクを想定する。
②保守時のリスク、保守用ツールの悪用によるリスクも想定する。

解説

・ファイアウォールなどで守られたり、インターネットから隔離して利用する想定の機器にセキュリティ上の問題が発生。



・保守用ツールを改造して攻撃される事例も発生。

対策例

指針4の守るべきものに対するリスクを想定
・IoTコンポーネントとしてのリスクの想定
1) クローズドなネットワーク向けでもIoTコンポーネントとしてのリスクを想定
2) 想定外の状況への対応

・保守時のリスク、保守用ツールの悪用によるリスクの想定
1) 保守時の攻撃リスクの想定
2) 保守用ツールの悪用リスクの想定

[指針6] つながりで波及するリスクを想定する

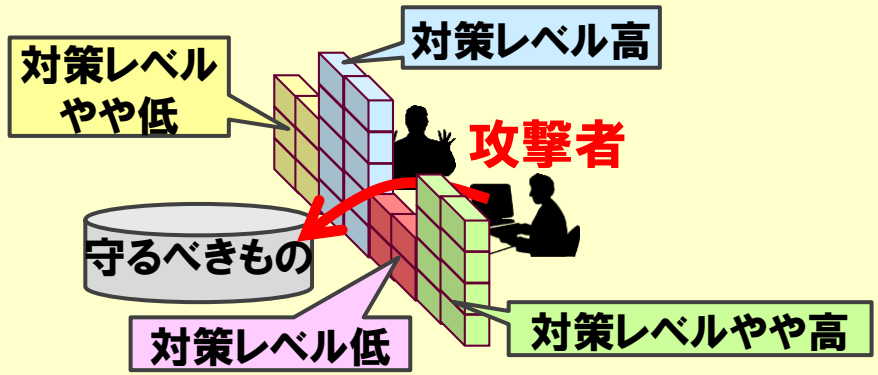
SEC Software Reliability Enhancement Center

ポイント

①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。
②特に、安全安心対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。

解説

・つながりを通じて影響が広範囲に伝播。
・安全安心対策のレベルが異なるIoTコンポーネントがつながることで全体的な安全安心対策のレベルが低下。



対策例

・つながりにより波及するリスクの想定
1) 異常がつながりにより波及するリスクの想定
2) 共同利用の機器やシステムを介して波及するリスクの想定

・安全安心対策のレベルが低い機器やシステムがつながったことにより影響が波及するリスクが高まることの想定

［指針7］物理的なリスクを認識する

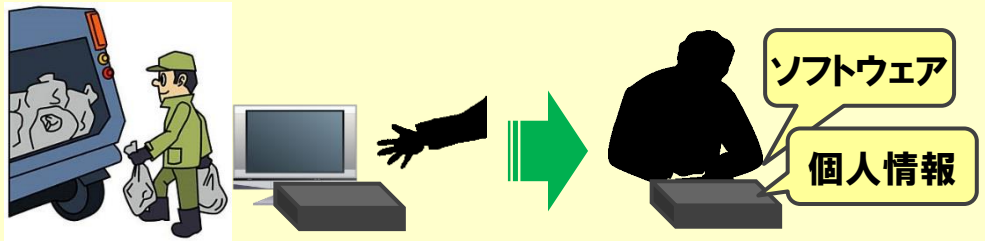
SEC Software Reliability Enhancement Center

ポイント

①盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。
②中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。

解説

・紛失した機器が不正操作されたり、駐車場や公共空間に設置した機器が第三者によって物理的に攻撃される危険性。
・廃棄した機器から情報が漏えいしたり、不正なソフトウェアを組み込んだ機器が中古販売される可能性。



対策例

・物理的リスクの想定例
1) 盗まれたり紛失したIoTコンポーネントに起因するリスクの想定
2) 管理者のいない場所で物理的に攻撃されるリスクの想定
・不正な読み出しや書き換えの想定例
1) 廃棄されたIoTコンポーネントから守るべきものを読み出されるリスクの想定
2) IoTコンポーネントに不正な仕組みを埋め込み、中古販売されるリスクの想定

[指針8] 個々でも全体でも守れる設計をする

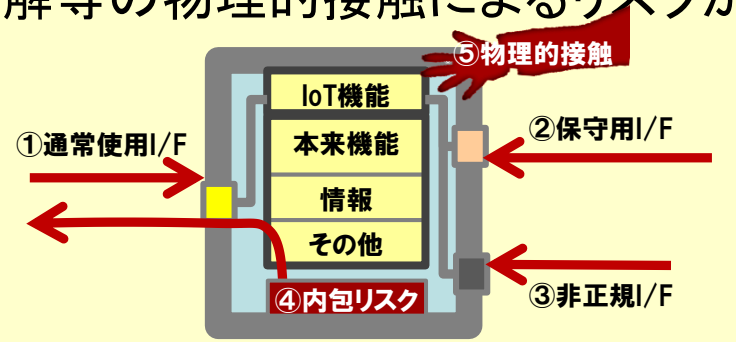
SEC Software Reliability Enhancement Center

ポイント

①外部インタフェース経由／内包／物理的接触によるリスクに対して個々のIoTコンポーネントで対策を検討する。
②個々のIoTコンポーネントで対応しきれない場合は、それらを含む上位のIoTコンポーネントで対策を検討する。

解説

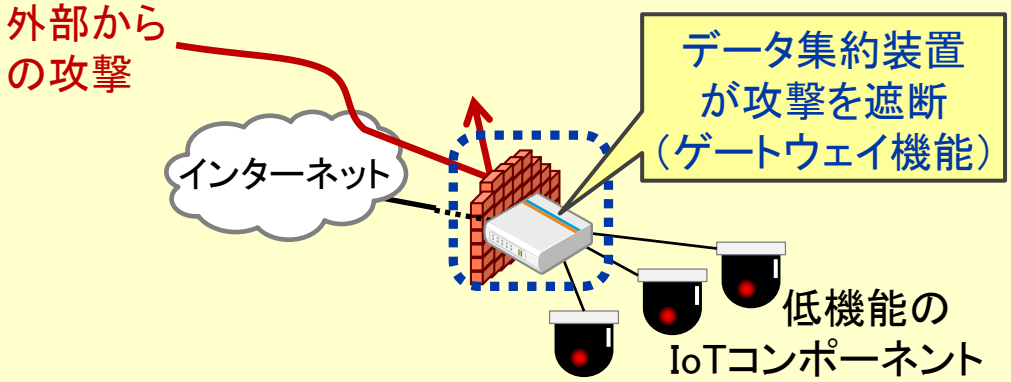
・外部インタフェース経由のリスク、潜在的な欠陥等の内包リスク、機器の持ち逃げ・分解等の物理的接触によるリスクが課題。



・対策機能の実装が難しい低性能のIoTコンポーネントも課題。

対策例

・外部インタフェース経由／内包／物理的接触によるリスクへの対策
・対策が不十分なIoTコンポーネントを上位のIoTコンポーネントで守る対策



[指針9] つながる相手に迷惑をかけない設計をする

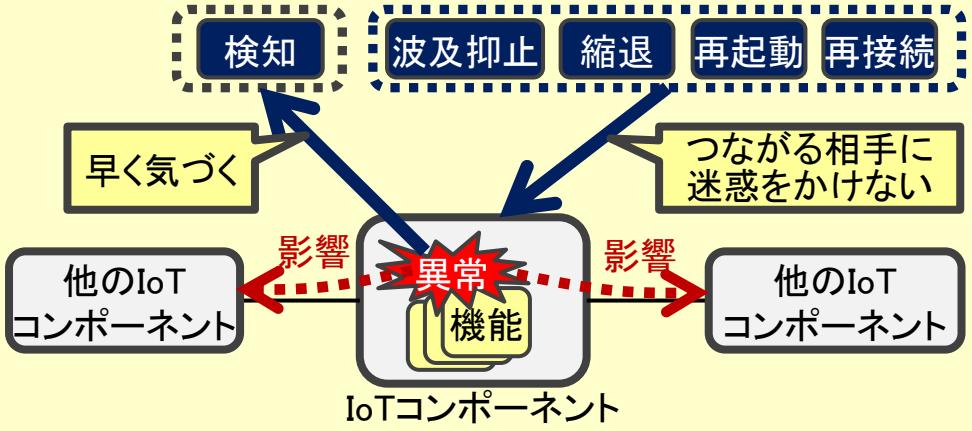
SEC Software Reliability Enhancement Center

ポイント

①IoTコンポーネントの異常を検知できる設計を検討する。
②異常を検知したときの適切な振る舞いを検討する。

解説

・異常な動作が発生した場合、影響の波及を防ぐために、早急に検知することが必要。
・異常な状態が検知された場合、内容に応じてネットワークから切り離すことが必要。



・状況に応じて早期に復旧することが必要。

対策例

・異常状態の検知
1) 連携した複数のIoTコンポーネントの監視
2) IoTコンポーネントの監視による負荷の増加の抑制

・異常発生時の波及抑止や復旧
1) 異常状態の影響の波及抑止
2) 異常が発生した機能の縮退
3) IoTコンポーネントの再起動・再接続
4) IoTコンポーネントの復旧

［指針10］安全安心を実現する設計の整合性をとる

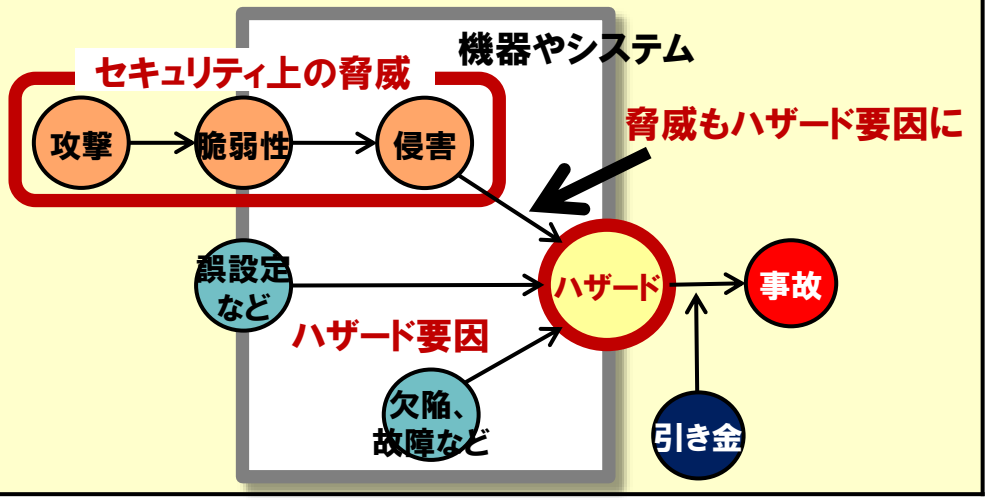
SEC Software Reliability Enhancement Center

ポイント

①安全安心を実現するための設計を見える化する。
②安全安心を実現するための設計の相互の影響を確認する。

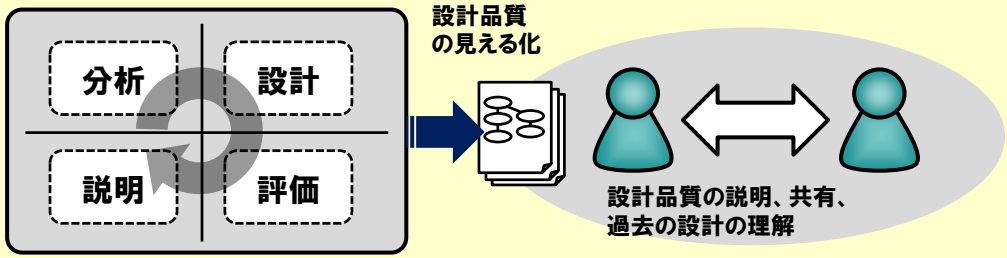
解説

・セキュリティ上の脅威がセーフティのハザード要因となったり、セキュリティ機能の実装がセーフティ機能や本来機能に影響を与えないか確認が必要。



対策例

・安全安心の設計の見える化



・セーフティとセキュリティの相互の影響の確認

1)セーフティ機能を含む守るべきものを特定、脅威とリスクを分析
2)セキュリティ対策を行い、リスクを再評価

［指針11］不特定の相手とつなげられても安全安心を確保できる設計をする

SEC Software Reliability Enhancement Center

ポイント

① IoTコンポーネントがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。

解説

・メーカが意識していない不特定の機器がつなげられ、情報が漏えいしたり、誤動作が発生するリスクの想定が必要。

製品出荷、システム提供　→　インテグレータがつなげる　→　先進ユーザがつなげる

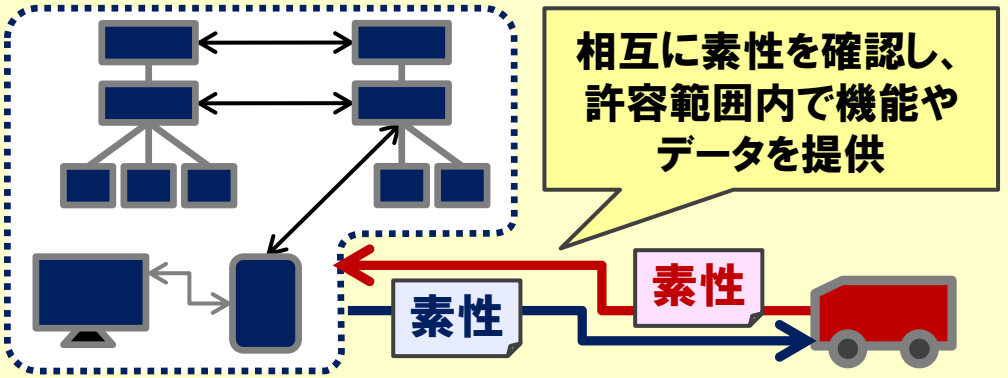
・同じメーカ同士の製品でも、後から出荷された型式やバージョンで同様のリスクの想定が必要。

対策例

・つながる相手やつながる状況を確認しその内容に応じてつながり方を判断する設計

1)相手のメーカ、年式、準拠規格といった素性に関する情報を交換、確認

2) 相手の素性や状況に応じて、接続可否、提供機能や情報の範囲を変更



［指針12］安全安心を実現する設計の検証・評価を行う

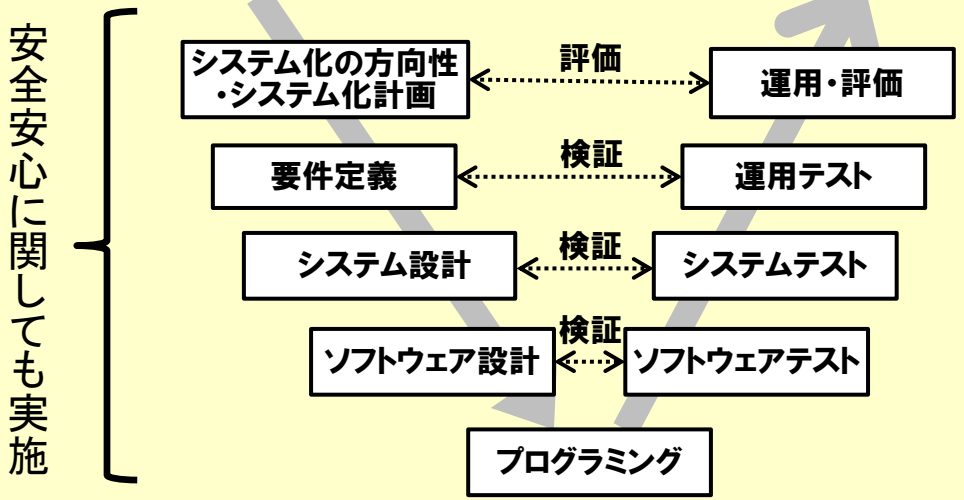
SEC Software Reliability Enhancement Center

ポイント

①つながる機器やシステムは、IoTならではのリスクも考慮して安全安心の設計の検証・評価を行う。

解説

・安全安心の要件や設計が満たされているかの「検証」が必要。
・安全安心の設計がつながる世界において妥当であるかの「評価」が必要。



対策例

・各指針の反映
17の指針を検討し、検証・評価に反映

・機器やシステムの安全安心対策のレベルに応じた検証・評価
1)セーフティに関する国際規格
2)コモンクライテリア（ISO/IEC 15408）
3)EDSA(Embedded Device Security Assurance)認証　など

・最新のハザードや脅威の情報を入手し、検証・評価に反映

［指針13］自身がどのような状態かを把握し、記録する機能を設ける

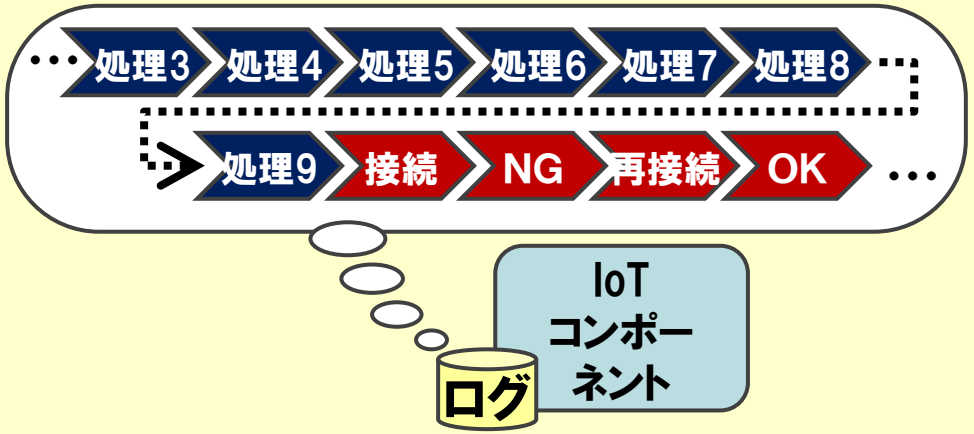
SEC Software Reliability Enhancement Center

ポイント

①自身の状態や他機器との通信状況を把握して記録する機能を検討する。
②記録を不正に消去・改ざんされないようにする機能を検討する。

解説

・個々のIoTコンポーネントがそれぞれの状態や他機器との通信状態を把握して収集することが必要。
・その内容を不正に消去・改ざんされることのないよう記録・保管することが必要。



対策例

・自身の状態や他機器との通信状態を把握して記録
1)保管方針を策定
2)各IoTコンポーネントで動作を記録
3)IoTコンポーネント間でログの時刻を同期

・記録の不正な消去、改ざんの防止
1)アクセス権限の設定、暗号化
2)収集データの保管装置への定期的な送信
3)追記のみ可能な仕組みの採用　など

［指針14］時間が経っても安全安心を維持する機能を設ける

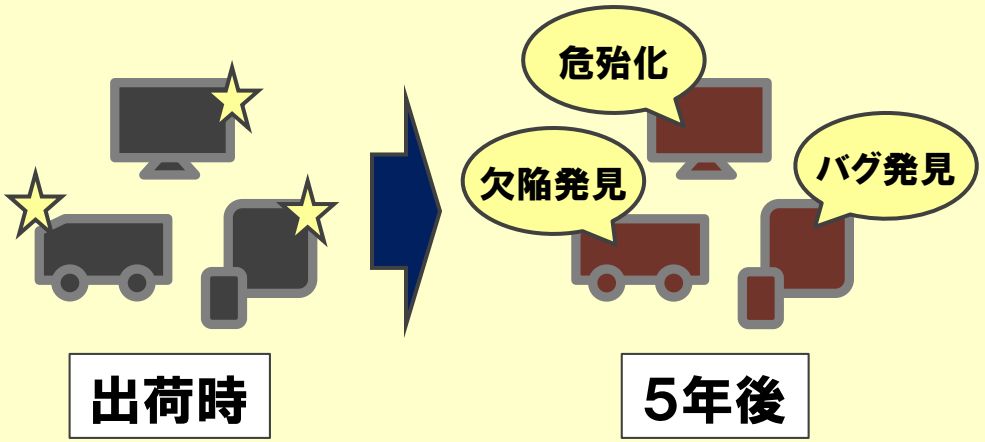
SEC Software Reliability Enhancement Center

ポイント

①経年で増大するリスクに対し、アップデートなどで安全安心を維持する機能を検討する。

解説

・自動車や家電などは10年以上利用するケースも多い
・経年で増大するリスクに対し、アップデート安全安心を維持することが必要。



対策例

・アップデートなどで安全安心を維持する機能
手動・遠隔アップデートなどの機能追加

・アップデートなどによる影響の低減
1)遠隔アップデートにおける回線負荷の分散
2)自動アップデート後に動作しなくなった場合のリカバリー
3)アップデート時のウイルス混入防止

・IoTコンポーネントの利用場所の把握
深刻な不具合が発見された場合のIoTコンポーネントの特定や停止など

［指針15］出荷後もIoTリスクを把握し、情報発信する

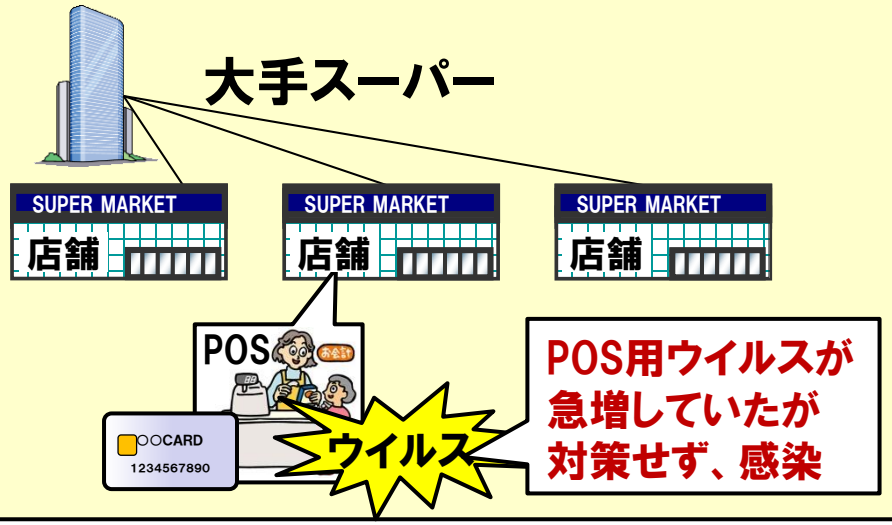
SEC Software Reliability Enhancement Center

ポイント

①欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する。
②必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する。

解説

・急増しているリスクを把握し、予防を実施。
・そのために関係者と協力し継続的に情報収集・分析、情報発信することが必要。



対策例

・事故やインシデントの情報収集・分析
1)世の中で発生している事故やインシデントの情報を収集・分析
2)JPCERT/CCやISACとの連携　など

・つながるリスクの情報発信
1)組織内へのCSIRTの設置
2)JPCERT/CCやISACへの情報提供　など

［指針16］出荷後の関係事業者に守ってもらいたいことを伝える

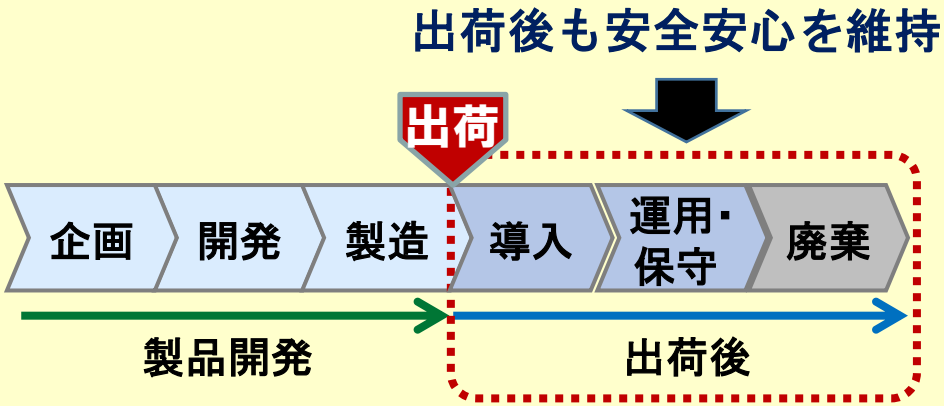
SEC Software Reliability Enhancement Center

ポイント

①導入、運用、保守、廃棄で守ってもらいたいことを直接それらの業務に関わっている担当者や外部の事業者に伝える。

解説

・急増しているリスクを把握し、予防を実施。
・そのために関係者と協力し継続的に情報収集・分析、情報発信することが必要。



対策例

・導入時の対策（以下は避ける）
1)ファイアウォールの無い環境への設置
2)ログイン用パスワードの未設定　など
・運用・保守時の対策
1)IoTコンポーネントのセキュリティ機能の劣化や新たな脆弱性への対応
2)他者が推定しにくいパスワード設定やソフトウェアアップデート未実施への対応
3)復旧機能では回復が困難な障害への対応
・リユース・廃棄時の対策
内包する個人情報・秘密情報の消去　など

［指針17］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

SEC Software Reliability Enhancement Center

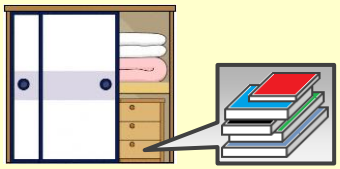
ポイント

①不用意なつなぎ方や不正な使い方をすると、自分だけでなく、他人に被害を与えたり、環境に悪影響を与えたりするリスクがあることを一般利用者に伝える。
②安全安心を維持していくために一般利用者に守ってもらいたいことを伝える。

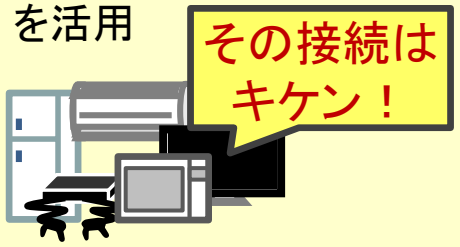
解説

・つながる世界は便利ではあるがリスクもあることを一般利用者に周知。
・IoTコンポーネントの不具合・脆弱性対策の必要性を理解、協力いただく。

取扱説明書に書いても忘れられる可能性あり



機器等のインタフェースを活用



対策例

・不用意なつなぎ方によるリスク周知
- オープニングの操作画面での表示
- マニュアル、保証書、Webサイトでの掲載

・一般利用者に実施していただきたいことの周知
- アップデート実施の推奨
- 無線LANのセキュリティの設定
- リユース・廃棄時の個人情報や秘密情報消去プログラム　など

ご清聴ありがとうございました。