経済産業省「電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン」について

背景と経緯

今日、インターネットが広く普及し、我が国においてもSociety5.0を目指す中、家電製品、ガス製品なども、既に、インターネット接続により便利に活用され始めています。例えば、スマートスピーカーの音声アシスタント機能を通じ家電製品が遠隔操作されるなど、使用者に新たな便益が提供され始めています。

一方で、家電製品などがインターネット環境で使われることで想定されるリスクに対し、安全が確実に確保されるよう対策を取ることが必要になっています。

そこで、家電製品、ガス製品などのIoT化等による安全確保を推進し、消費者の安全を守る視点から、海外の規格（※）を参照しつつ、経済産業省は、令和３年4月28日に「電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン」（以後、「IoT製品安全ガイドライン」）を策定し、公表しました。

IoT製品安全ガイドラインは、経済産業省のWebサイトで公開しています。

https://www.meti.go.jp/product_safety/consumer/system/iot.html

※IEC 60335-1(2020)(Household and similar electrical appliances - Safety - Part 1 : General requirements) 等

IoT製品安全ガイドライン作成の意義

IoT製品安全ガイドラインは、業界・企業による自主的な製品安全確保の取組で積極的に活用されることを期待して作成されました。

IoT製品安全ガイドライン作成の背景

社会環境の変化

家電製品、ガス製品のIoT化の進展

使用者の便益

- （製品の）インターネット接続により便利に活用されることが見込まれている
- 製品安全４法※対象製品も新たなサービスと連携し、使用者に新たな便益が提供されていくことが想定される

IT・ネットワーク技術の急速な進化

IT・ネットワーク技術の適用が生み出す新しいリスク

新しいリスク低減のための対策の必要性

- 一般家庭にある製品の脆弱性へのサイバー攻撃の懸念
- 家電製品等がインターネット環境で使われることで想定されるリスクについて、誤操作のみならず、通信遮断やサイバー攻撃を含めた場合であっても、安全が確実に確保されるよう対策を取ることが必要

※消費生活用製品安全法、電気用品安全法、液化石油ガスの保安の確保及び取引の適正化に関する法律、ガス事業法

目指すべき方向性

IoT製品安全ガイドラインでは、目指すべき方向性として、製造メーカーが新しい対策の適用に取り組むことを期待しています。安全機能と通信回線の分離、予防安全機能、ソフトウェアのアップデート時の安全確保対策等がこれにあたります。

IoT製品安全ガイドラインにおける考え方

①**安全機能と通信回線との分離**を要求。

⇒**通信回線に不具合が生じても安全機能が維持される**ことを要請

②新たに『**予防安全機能**』という考え方を取り入れ、可能な範囲でこれを要求。

⇒『予防安全機能』とは、安全機能ではないが、**遠隔操作によるリスク低減に効果が見込まれ、製品事故や機器の近くにいる者の危険を未然に防ぐ機能**

IoT製品安全ガイドラインを踏まえた対策

遠隔操作機構を有する機器は、**通信回線を利用したソフトウェアのダウンロードやアップデート等が行われる場合**が考えられる。

ソフトウェアアップデートの安全確保

「７．（３）不正アクセスへの対応について」

機器の機能安全に影響がないことを確認することが必要

「８．（１）製品の修理、メンテナンス時」

機能安全に係る保護電子回路のソフトウェアを変更する場合、・・・**インストール中又はインストール後であっても規格の安全要求事項への適合性を損なってはならない**　等

「８．（２）ソフトウェア等のアップデート時」

機能安全を保護電子回路に依存する場合、・・・**機能安全に係る機器内のデバイスの真正性や完全性※を確保**する必要がある　等

「８．（３）ii）ソフトウェアのアップデートについて」

機能安全を担う保護電子回路のソフトウェアのアップデートを行う場合、
・・・**アップデート中に機器の運転が停止した場合、遠隔操作者及び使用者にその旨、通知する手段を確保**すること　等

※真正性は主としてなりすましがないこと・本物であること等、完全性は主として改ざんや欠損がないことを示す。

安全確保の考え方：スリーステップメソッドの拡張

遠隔操作する機器の安全は、製造メーカーの安全設計（ステップ1、ステップ2相当）によって守られていますが、ステップ3相当の対策として、遠隔操作者／使用者が遠隔操作を過信せず、異常発生時等に能動的に行動するように注意喚起することで、より一層の安全を期待できます。

これまでの製品安全の考え方

■これまで、製品安全の考え方は、製造事業者等が、製品が使用される状況の中で起こりうるハザードを想定し、製品自体が人体への危害や物件への損傷を与えぬよう、設計等において、物理的に安全を確保し、事故が起きてもその危害、傷害の程度が小さくなるよう設計している（物理的安全）。また、ある一定の温度や電圧など危険な閾値を超えると、製品が物理的に止まるなどの電気・電子的な制御機構による安全防護策（機能安全）が講じられる。

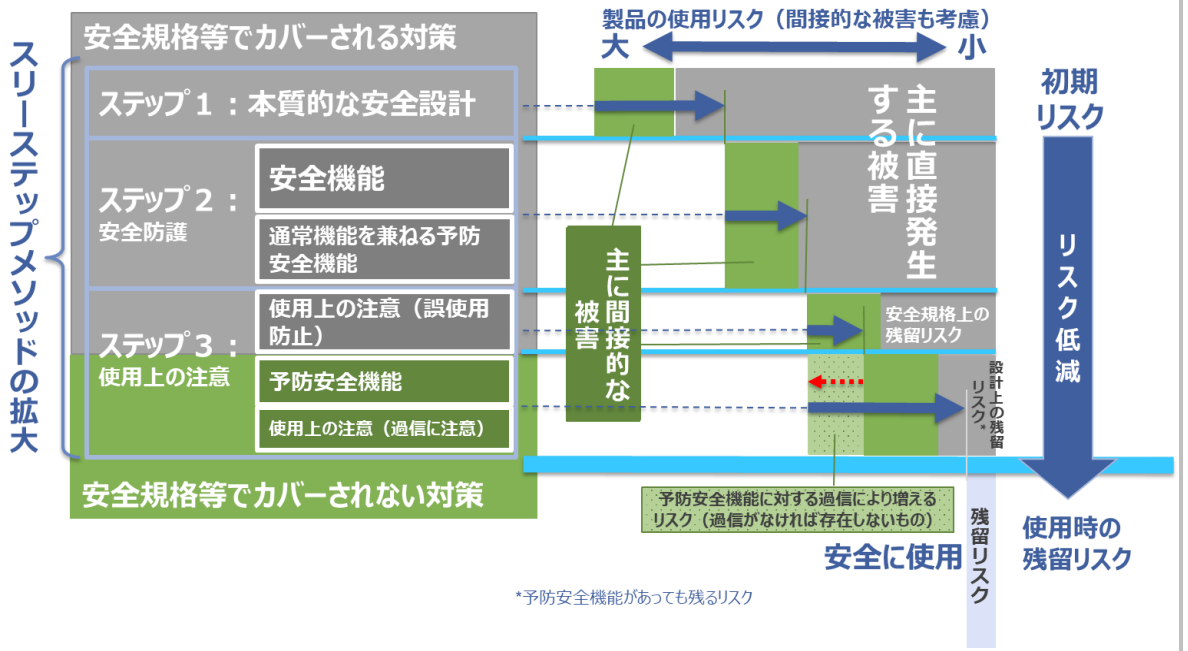
■製品開発や設計においては、スリーステップメソッドと呼ばれる①本質的な安全設計（危険事象の基になることを除去、危害の程度や発生頻度を低減）、②安全防護（安全装置などの保護手段）、③使用上の注意（残留リスクを知らせ、安全な行動を促す(警告表示等)）の３つのステップでリスクを低減することが、安全を確保する共通概念とされている。

IoT製品安全ガイドラインにおける安全確保の考え方

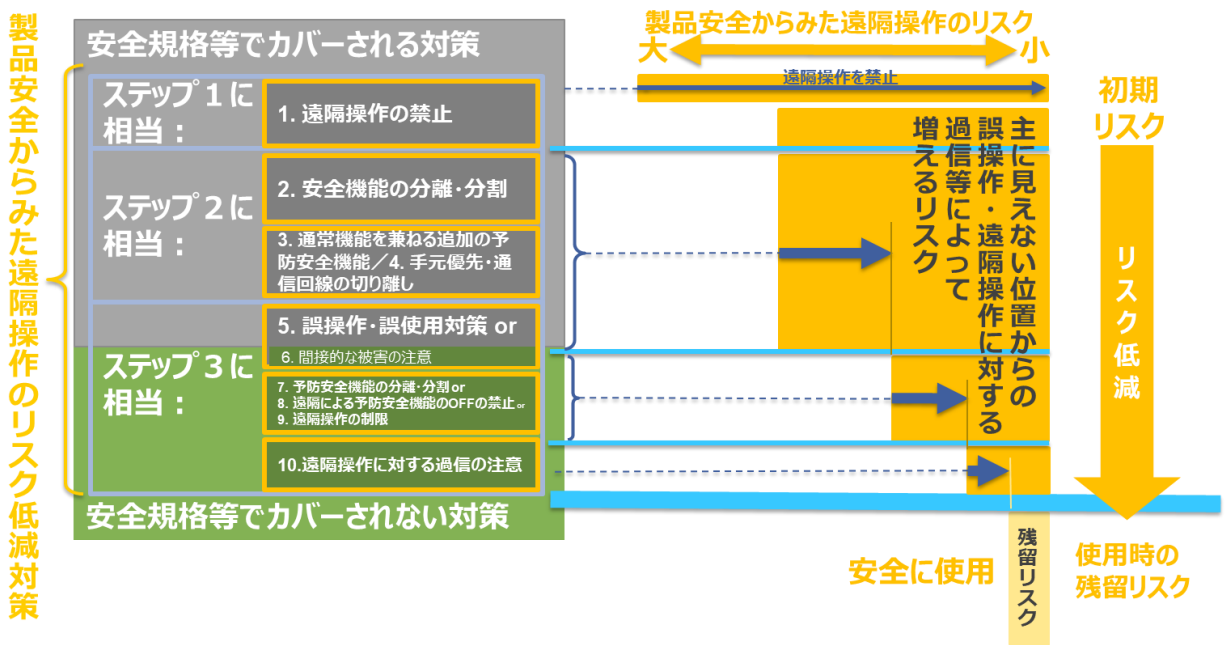
■通信遮断やサイバー攻撃を含めた新たなリスク（間接的な被害等によるリスク及び遠隔操作によるリスク）に対応するため、スリーステップメソッドの考え方を拡大した。（IoT製品安全ガイドラインでは、概略図と対策の用語の解釈を提示）

【参考】スリーステップメソッドの拡張イメージ

間接被害等に対するリスク低減対策



遠隔操作に対するリスク低減対策



リスク評価の考え方：間接的な被害の考慮

遠隔操作を行おうとする製品に対しては、製品の近傍、周辺に与えうる「間接的な被害」も考慮することが大切です。

IoT製品安全ガイドラインにおける「間接的な被害」は、機器の操作者が遠隔操作することにより機器の近くにいる使用者や周辺において直接発生する被害及び機器が運転、停止し続けることによる被害をいう。被害の範囲については、既に遠隔操作機構を有している機器や今後遠隔操作が考えられる対象製品を選定し、想定されうる被害のユースケース及びリスクシナリオ※1を踏まえ検討した。

【間接的な被害：具体的な被害とは※2】

- 熱中症
- 子供の溺れ
- 間接的に生じる火災や火傷
- 間接的に生じる健康被害（めまい、吐き気、一酸化炭素中毒等）

【間接的な被害の例：リスクシナリオ例より】

製品	ユースケース	リスクシナリオ
温風暖房機（床置き） （注）壁や天井設置の浴室用・脱衣室用の暖房換気乾燥機は対象外	温風暖房機の上部に洗濯物を干した状態で外出した。 帰宅時に部屋が暖かくなっているように、帰宅前に遠隔操作で温風暖房機をOFF→ONした。	温風暖房機が生み出した上昇気流で洗濯物が浮き上がり、温風暖房機の上に落下して炎上し、火事が発生した。

※1 ユースケース／リスクシナリオ及び対策例については、「令和２年度産業保安等技術基準策定研究開発等事業（電気用品等製品のIoT化等による安全確保の在り方に関する動向調査）」（以下、「調査報告書」という）の図表2-38を参照してください。
※2 現時点で想定されうる蓋然性が高い被害のみ対象としたが、今後の社会情勢の変化や製品事故の動向などにより変化していくものであることに留意が必要

予防安全機能の適用

IoT製品安全ガイドラインでは、遠隔操作することによって増大するリスクを低減するため、予防安全機能を組み込むことが推奨されています。これには、異常発生時等に遠隔操作者／使用者の能動的な行動を促すための異常通知／取るべき対応の伝達も含まれています。

予防安全機能とは

定義	「遠隔操作機構の操作者の過信や誤操作によって生じる被害や遠隔操作された機器の近くにいる使用者に及ぼす危害に対して、防止又は低減できる機能」
推奨事項	対象製品の遠隔操作に際しては、機器の近くにいる人や機器の周辺への危害を回避するべく、可能な範囲で、設計段階から、予防安全機能を組み込むこと。

予防安全機能の主な例

■ **遠隔操作のリスク低減**

➢ 遠隔操作者の過信／誤操作／誤使用によって生じる直接被害／間接被害や、遠隔操作が使用者（機器の近くにいる人）に及ぼす不意の危害を、防止または低減できる機能

■ **能動的な行動を促すための異常通知等**

➢ 遠隔操作者中であることの表示や機器の周辺等の安全を確認するシステムが、使用者（機器の近くにいる人）に対する警報も含めて、操作者及び使用者に対応を依頼して遠隔操作時のリスクを低減する機能

予防安全機能と通常機能・安全機能の比較

	動作	使用者との関係	安全動作確認試験	基本設計
通常機能	通常状態で働く	使用者が設定してもよい。	平常温度試験、漏洩電流試験、定格消費電力試験	壊れても安全
予防安全機能	異常状態になる前に働く。	使用者が設定できるものもある。	予防安全機能が義務づけされる製品では、動作確認試験がある場合もある。	壊れても安全又は使用者の過信に注意。
安全機能	異常状態で動く。（通常状態で動作してはならない）	使用者は設定できない。	異常運転試験（合理的に予見可能な誤使用等）、電子部品の故障試験	信頼性評価

予防安全機能の適用例

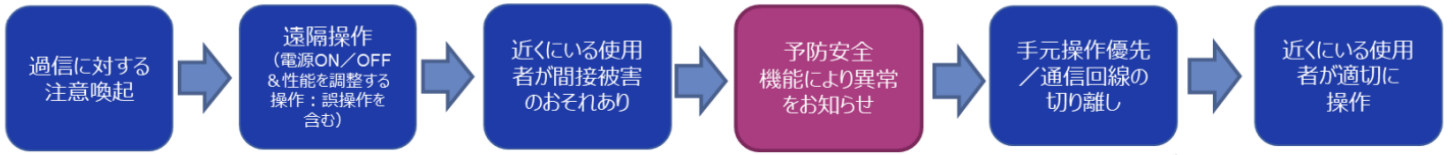
予防安全機能は間接的な被害のリスクを低減する役割を担いますが、必ず動作する保証はないので、最後はヒューズ等の物理的手段（安全機能）で安全を確保することが推奨されます。これが難しい場合は、人の手元操作で安全を回復するべく、異常を伝えて能動的な行動を促します。

予防安全機能の適用例

【遠隔操作による機器の電源OFFを過信】

- ■ 遠隔操作の過信に対する注意喚起
- ■ 予防安全機能は、条件により動作しない可能性があるため、過信してはならないことを使用者に注意喚起
- ■ 通信障害等
- ■ 消し忘れ防止機能等
- ■ 予防安全機能の故障

【通常機能の遠隔操作】



- ■ 予防安全機能は、条件により動作しない可能性があるため、過信してはならないことを使用者に注意喚起
- ■ 熱中症など
- ■ 近くにいる使用者に能動的に対応を要求
  ※やけどの場合、通常機能で温度をコントロール
- ■ 予防安全機能が故障したときの最終手段
- ※やけどの場合、使用者が逃げられるので、便座等を除き、多重防護の考えがない（最終手段がない）

※「調査報告書の図表2-27、2-29を参照。

事例による予防安全機能の選択

予防安全機能をどのように活用するかの参考とするため、ユースケース・リスクシナリオと対策例の例示を集約・整理することにも取り組んでいます。事例からスタートできるので、設計がしやすくなります。

【予防安全機能を含む複数の対策を組み合わせて間接的な被害のリスクを低減する例】

調査報告書　図表2-38より引用

製品	ユースケース	リスクシナリオ	3ステップメソッドによる方策・対策の一例（案）
ロボット掃除機	家の中にいる使用者が、電気ストーブを床に置いて使っていた。別の家族が電気ストーブの近くの床に、買い物から帰宅したらたたむつもりの洗濯物の山を置いていた。 この家族が、買い物の間に掃除をすませようと、ロボット掃除機を遠隔操作でOFF→ONしたが、家の中にいた使用者はたまたまロボット掃除機が見えない位置にいた。	買い物に出た家族が、家の中で電気ストーブを使っていた使用者が見えない位置からロボット掃除機を操作し、電気ストーブのコードを巻き込んで、電気ストーブが床の洗濯物の山に入り込み、洗濯物が焦げる又は火災に至る。	<ステップ２：手元優先・通信回線の切り離し> ロボット掃除機が意図せず動く可能性を考慮して機械式等の主電源スイッチ又は通信回線切り離し用のスイッチを用意する。 a. AND <ステップ３：予防安全機能> 障害物回避機能を予防安全機能として設計する。 b. AND <ステップ３：使用上の注意（誤使用防止）> 使用者に対する注意として、掃除する前に床の整理整頓を実施するよう取扱説明書にて記載する。 AND c. <ステップ３：間接的な被害の注意> 家の中にいる使用者が電気ストーブなどを使用するときは、必ず主電源スイッチ又は通信回線の切り離し用のスイッチをOFFにすることを本体に表示又は取説に記載する。

間接被害を生じる遠隔操作のユースケースを例示

遠隔操作で生じる間接被害の発生シナリオを例示

スリーステップメソッドによる対策例の組合せ

この例示では、a.b.c.の３つを同時に適用することで、遠隔操作のリスクを低減。
このうち b. は予防安全機能の組込である。

遠隔操作を行う機器の分類の考え方

IoT製品安全ガイドラインでは、機器を「遠隔操作に不向きな機器」と「遠隔操作を許容する機器」に大別し※、後者について、製造事業者の参考となるよう、ユースケース／リスクシナリオ例に基づいて対策例を示しています。

※機器の分類表については、調査報告書の図表2-35（電気用品）及び図表2-36（ガス用品）を参照してください。なお、これらの分類結果は2021年4月時点での整理であり、今後の社会情勢の変化等により変化していくものであることに留意が必要です。

人の注意が行き届く状態で動作する機器 ⇒遠隔操作に不向きな機器

- 操作する者が自ら手を触れ機器を動作させることで、その機器の機能、役割を果たす（すなわち、操作者の存在を前提に安全設計されている）機器
- 機器の表面に触れると火傷する、可動部に触れると傷害を受けるなど可動時に危険な部分が露出する機器
- その他遠隔操作することで危険のリスクが著しく増す機器

例：電気用品では、アイロン、ミシン、ヘアケア用機器、ほとんどの調理用機器など

人の注意が行き届かない状態で動作する機器 ⇒遠隔操作を許容する機器

- 「人の注意が行き届く状態で動作する機器」以外の機器
- ガス用品の技術上の基準等に関する省令及び液化石油ガス器具等の技術上の基準等に関する省令で遠隔操作が認められている機器

遠隔から機器をON する行為

遠隔から機器をOFF する行為

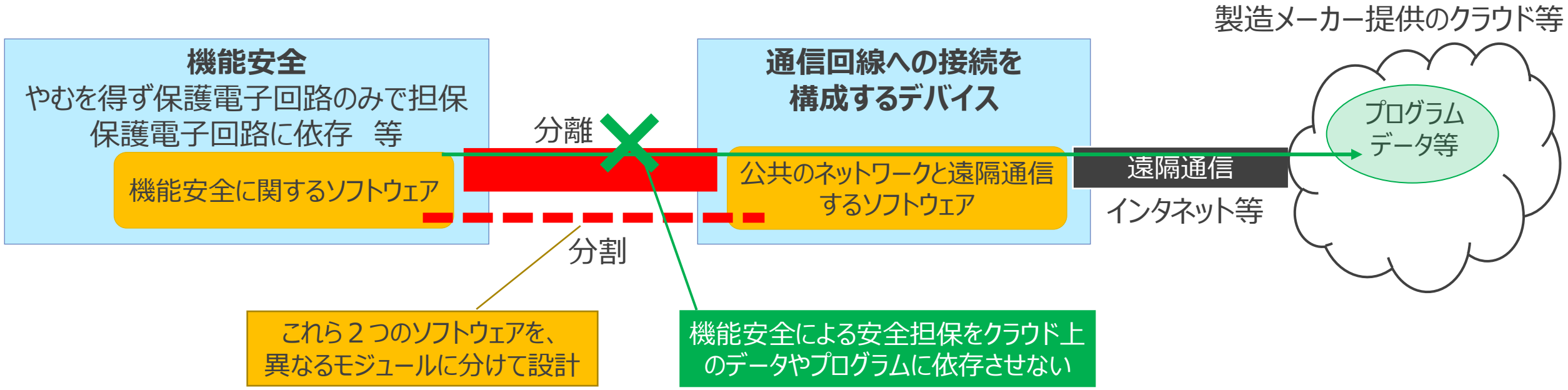
機器の設定を調節する行為

→ **ケーススタディを実施**

安全機能の分離・分割

IoT製品安全ガイドラインでは、遠隔操作を悪意のある攻撃から守り、ソフトウェアアップデートを安全に適用できるように、安全防護と情報セキュリティを中心とした対策の重要性を示しています。ここでまず重要になるのが、異常発生時の安全機能（機能安全）と通信回線の分離・分割です。

【安全機能（機能安全）と通信回線の分離・分割の実現イメージ】



安全機能の分離・分割

安全機能（機能安全）と通信回線の分離・分割は、製品設計において配慮すべきとされていることに加えて、製品の修理・メンテナンス時（特に、機能安全に係る保護電子回路のソフトウェアを変更する場合）や機能安全のソフトウェアアップデート時にもこれが維持されることが望ましいとされています。

機能安全を確実に働かせるための設計

基本＝保護電子回路＋ヒューズ等の物理的な保護装置

↓ 物理的な手段で分離できない場合

通信回線と機能安全の分離

↓ やむを得ず、通信回線と機能安全を分離できない場合

機器の安全を遠隔通信に依存させないことを推奨

「安全機能（機能安全を含む）に関するソフトウェア」と「公共のネットワークと遠隔通信するソフトウェア」を分割

安全機能の分離・分割

【安全機能と通信回線との分離・分割：実現方法】

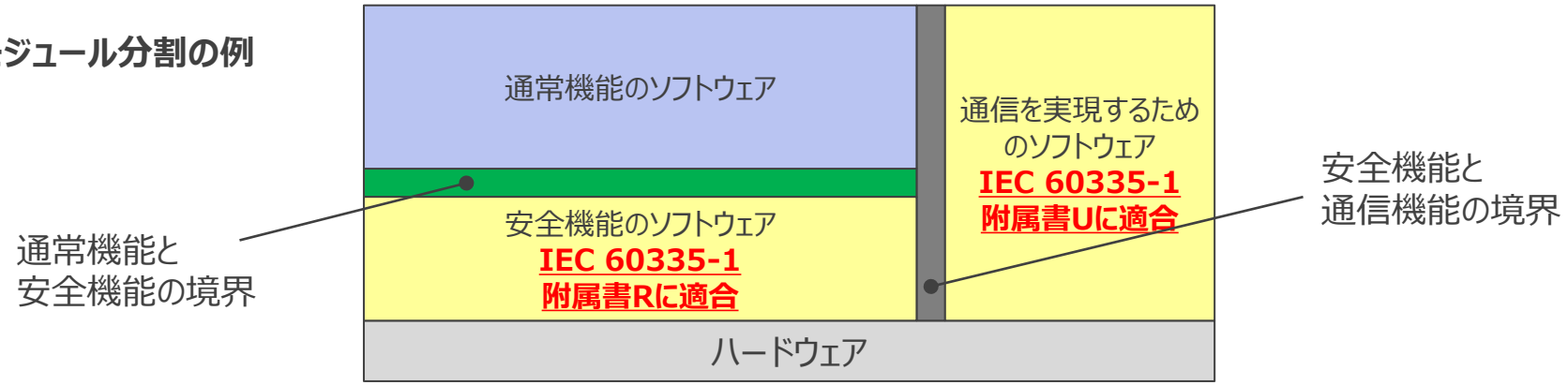
分離(separation)と分割(partitioning)

分離：あらかじめ定義されたデータインタフェースを介して、相互作用する可能性のある、異なったソフトウエア間の機能間の分割。分離は物理的または仮想的に適切な分割を実現することで行うことができる。

注：物理的とは、別CPUにするなど、ハードウェアを分けること。
仮想的とは、ソフトウェア上のモジュール分割のこと。

分割：ソフトウェアを異なる機能を持つモジュールに分割し、モジュール間のインタフェースを定義することでソフトウェアを構成する、高信頼設計手法の一つ。

モジュール分割の例



※モジュールとは、ソフトウェア全体を構成するための、基本となる独立したソフトウェアの構成要素のことを言う。（日本大百科全書(ニッポニカ)参照）

安全機能の分離・分割

【分離・分割のまとめ】

1. 保護電子回路だけに頼らず、**物理的な保護装置**を組み込むことが望ましい。
2. 物理的な保護装置を組み込まない場合、安全機能と通信回線を物理的に分離すること。この措置を取れない場合は、保護電子回路・外部の通信回線との通信に使うソフトウェアはモジュールを適切に分割すること。
3. CPUを物理的に分けることは必須ではない。モジュール間のデータの繋がりが少なく、かつモジュール間インタフェースが明確になるように分割すれば良い。
4. **外部の通信回線は不確実**という前提に立つので、安全機能・予防安全機能は外部側に依存しないこと。
5. 上記②③④の設計は、該当部分の設計資料上で明確にしておく。
認証時は設計資料を用いて説明。

遠隔操作のリスク低減対策の限界と使う人の役割

遠隔操作によりトラブルが発生する場合、遠隔操作を行う人自身ではなく、遠隔操作される製品の近く（遠隔操作者からは見通すことができない場所）で物損（火災）や人への間接的な被害が生じる可能性があります。
製造メーカーは予防安全機能※を組み合わせてリスクの低減に努めるだけではなく、使用する人がその機能を過信あるいは誤操作・誤使用し、機器の近くにいる使用者などに不意に危害を与えないよう、使用条件、使用上のリスク・注意点、異常通知があった場合に取るべき対応(手元操作の優先、近くにいる使用者による通信回線切り離し)等、能動的に安全な使い方ができるよう注意喚起をすることが大切です。

※予防安全機能とは、安全機能とは別に、遠隔操作機構の操作者の過信や誤操作によって生じる被害や、遠隔操作された機器の近くにいる使用者に及ぼす危害を防止又は低減できる機能のこと

予防安全機能は万能ではないため、

① 予防安全機能を過信しないように使用者に説明することが大切

② 使用者に、安全に使用することにご協力いただくことが重要

- どのように使ってほしいか（意図する使用）、どのような使い方をしてほしくないか（予見可能な誤使用）をきちんと使用者に伝えることが重要
- 異常通知があった場合に取るべき対応を予め確認し、いざという時に能動的に行動して危険を回避してもらうことが大切

どのような機器に対して事例が収集・公表されているのか

現在のユースケース／リスクシナリオの例示は、14機器／24シナリオです。事例をさらに収集・整理することで、間接的な被害を生じるリスクの発生シナリオとこれに対する対策例の例示は、さらに参考にしやすいものになります。

■ ユースケース／リスクシナリオが例示されている製品

【空調等】
- エアコン
- ファンヒーター
- 換気扇

【給湯器】
- 電気温水器
- ガス給湯器

【暖房機】
- 温風暖房機（床置き）
- FF暖房機
- FE暖房機

【ドラム式洗濯機・乾燥機】
- ドラム式電気洗濯機・乾燥機
- ドラム式ガス乾燥機

【掃除機】
- ロボット掃除機

【炊飯器・ポット】
- 電気炊飯器
- ポット

【照明】
- 電気スタンド（ランプが露出している場合に限る）

ユースケース／リスクシナリオに対応した対策例の活用イメージ

今後、IoT家電等の普及が更に加速することが想定される中、IoT製品の安全確保に向けて機能が充実されることが期待されます。そのためにも例えば、「事業者の安全活動に資するユースケース・リスクシナリオ」をさらに収集し、製造事業者自らが安全向上に取り組む環境を整えることが効果的と考えています。

収集・整理された「ユースケース／リスクシナリオとその対策例」を活用することのメリット例

1. リスク評価を行う必要がある「間接的な被害の発生シナリオ」を容易に特定・選択できる

2. リスク評価の対象とする間接的な被害の発生シナリオに対し、例示された対策ノウハウを有効に活用することで、効果的な対策の特定・選択が容易になる。

最後に、

IoT製品安全ガイドラインの適用にあたり、必要に応じ、必要な時に、必要な箇所を選択して使うことが期待されています。

例えば、予防安全機能等の基本的な考え方を理解するために活用できるほか、製品出荷後のソフトウェアアップデート時に配慮すべき事項の特定にも役立てることができます。