制御システムセキュリティカンファレンス 2021

JPCERT Coordination Center

NTT DATA
Trusted Global Innovator

急激な進化を続けるスマート家電の遠隔操作の現状から見えてきた課題
ー IEC60335-1第６版の公開と予防安全機能によってこれからの製品安全設計はどう変わる？

2021年2月12日

株式会社NTTデータ経営研究所
エグゼクティブスペシャリスト　三笠　武則

1. 電気用品等のスマート化に関する現状

2. 遠隔操作される電気用品等の安全とセキュリティ

3. 人に危害を及ぼす遠隔操作への対策の現状

4. IEC60335-1第６版が求めるソフトウェアと遠隔操作に対する要求事項

5. 遠隔操作による間接被害への対応の在り方

電気用品等のスマート化に関する現状

スマートホームは市場拡大中だが・・・

スマートホーム市場は、2030年に向けて有望な成長市場であると注目を集めており、市場レポートも多数公表されているところ。

【IDCの最新の市場予測】

- 市場全体で2024年のスマートデバイスは14億4170万台に到達する予想。2020年から2024年のCAGRは14.0%

- 出荷台数ベースでこの動きを牽引するのは、ビデオエンターテインメント用デバイス（スマートテレビ、デジタルメディアアダプター等）、ホームモニタリング・セキュリティデバイス、スマートスピーカー

- 特に、ホームモニタリング・セキュリティデバイスの成長が顕著

出典：https://www.idc.com/getdoc.jsp?containerId=prUS46891320

電気用品等のスマート化は？　確かにスマート化の範囲は広がっている！

殆どの家電製品がスマート化されてきている。特に、洗濯機・衣類乾燥機、冷蔵庫、冷凍庫、掃除機、エアコン、空気清浄機・除湿器・加湿器等はIoT化が進んでいる。

国内外企業（日、米、欧、中、韓）が提供するスマートホームPF

スマートスピーカー等を軸にしたIT企業によるPF

電機メーカーによる自社製品が相互に接続されたPF

経産省「商業動態統計」における家電製品分類

プラットフォームで展開されている
家電製品を調査の上、「商業動態統計」
の分類項目に対してマッピング

商品分類表

商品分類等	内容例示
AV家電	テレビ・プロジェクタ（CRT、液晶、PDP）、ビデオディスク、BD・DVD（再生専用、録画再生機）、BS・CS 機器、ステレオ、スピーカ、AV 編集機器、ラジオ・ポータブルオーディオ、GPS ナビゲーション、ヘッドホン、マイクロホン、AV 接続機器、電子楽器、VTR、携帯オーディオ機器、ホームオーディオ機器、メディアクリーナ等
情報家電	パソコン・パソコン周辺機器（デスクトップ型・ノート型パソコン、タブレット端末、モニタ、プリンタ等）、ゲーム関連機器、電子手帳・辞書、コピー・シュレッダー等
通信家電	移動体通信機器（携帯電話機、パーソナル無線、データ通信カード・端末）、電話機・FAX 等
カメラ類	ビデオカメラ・デッキ、デジタルスチルカメラ（コンパクト型、一眼レフ）、カメラアクセサリ、交換レンズ等
生活家電	家事・調理家電（洗濯機・衣類乾燥機、ふとん乾燥機、冷蔵庫・冷凍庫、炊飯器、電子レンジ、オーブンレンジ、食器洗い機・乾燥機、電磁調理器、クッキングヒーター、ホームベーカリー、トースター、電子炊飯ジャー、ジャーポット、電気ケトル、コンロ・ガステーブル、電気プレート・鍋、ジューサー・ミキサー類、コーヒーメーカー、もちつき機、精米機、家庭用ゴミ処理機、浄水器・カートリッジ、アイロン・ズボンプレッサ、クリーナ、スチーム・高圧洗浄クリーナ、掃除機等）
	理美容・健康関連（シェーバー、ドライヤー・ヘアアイロン、フェイスケア器具、ボディケア器具、散髪器具、電動歯ブラシ、電気測定器具（電子血圧計、電子体温計、電子歩数計等）、フィットネス機器、電気マッサージ器具・治療器、吸入器等）
	空調・季節家電（エアコン、冷風機・冷風扇、扇風機、換気扇、空気清浄機・除湿機・加湿器、石油暖房器具、温水ルームヒータ、電気温風機・電気ストーブ、家具調こたつ、電気カーペット、電気掛・敷毛布等）
その他	温水洗浄便座、24時間風呂、モニタ付ドアホン、火災警報器、照明器具、電池、管球、配線器具、自然冷媒ヒートポンプ給湯器等

出典：令和元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）報告書

電気用品等のスマート化は？　確かにスマート化の範囲は広がっている！

遠隔から操作できる機能も多種多様。

IoT化により現在可能となっている家電の遠隔操作の例

	洗濯機・衣類乾燥機	冷蔵庫・冷凍庫	電子レンジ	エアコン	空気清浄機・除湿器・加湿器
ON/OFF	外から運転・予約	－	－	生活パターンに応じたタイマー設定 屋外からの運転ON/OFF	タイマーセット 屋外からの運転ON/OFF
機器の操作（設定変更）	洗濯モード切替（洗濯前）	庫内の温度設定の変更	音声操作（加熱秒数変更等）	• 運転モード変更 • 温度設定変更 • 掃除等変更	• 運転履歴から自動で運転切り替え • 季節状況や天気状況から自動で運転設定変更
使用者への情報提供（リコメンド機能）	ステータス通知（運転終了時刻が近づいたとき、柔軟剤や洗剤が無くなった時にプッシュ通知）	• 食材の経過日数の管理 • ドアの閉め忘れお知らせ機能 • 献立提案	• レシピ登録 • 献立提案	－	－
その他		• 高齢者見守り機能（ドア開閉から安否を通知） • 伝言機能			

出典：令和元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）報告書

皆さん、スマート家電を実感していますか？

スマート家電のビジネスモデルにはお国柄がある。
我が国、米国、欧州、中国ではそれぞれ訴求ポイントが異なるのが実状。

我が国

多機能・
＆高性能

欧州

単価の高い市場特化

米国

パーツを自由に組み上げ

中国

類似品、
１億人の長者向け

家電製品の世界市場は事業買収によって中国がリード

中国の家電大手は、我が国、米国等の家電事業を買収し、世界シェアを大幅に伸ばした。

ハイアール

（買収：三洋電機白物家電事業、GE家電）

美的集団

（買収：東芝白物家電事業）

格力電気

ハイセンス

（買収：東芝映像事業）

家電をクラウドに繋ぐ動きは、中国メーカーが牽引？

中国メーカーにおいては、エアコン、洗濯機、空気清浄機・除湿器・加湿器、ロボット掃除機、IHこんろ／ガスこんろを始めとして、幅広い家電がIoT化されている。
例えば、コンロは、電気／ガスを問わず、我が国では遠隔操作は禁止との認識。扇風機の遠隔操作は子供には危険かも。国によって考え方に相違がある。

製品	社数	中国の主要家電メーカー				
		Midea Group 美的集団	Xiaomi 小米科技	Gree Electric 珠海格力電器	Haier 海尔集团	Hisense 海信集团
エアコン	5社	○	○ （IoT化されたエアコンではなく、エアコンをIoT化するプラグを販売）	○	○	○
洗濯機	4社	○	○	×	○	○
空気清浄機・除湿器・加湿器		○ （空気清浄機）	○ （空気清浄機）	○ （加湿器）	○ （空気清浄機）	×
ロボット掃除機	3社	○	○	×	○	×
IHコンロ/ガスコンロ		○ （IH）	○ （IH）	×	○ （ガス）	×

製品	社数	中国の主要家電メーカー				
		Midea Group 美的集团	Xiaomi 小米科技	Gree Electric 珠海格力電器	Haier 海尔集团	Hisense 海信集团
炊飯器	2社	○	○	×	×	×
オーブン		○	×	×	○	×
給湯器		×	○ （電気ケトル）	×	○ （電気・ガス）	×
冷蔵庫		×	×	×	○	○
扇風機	1社	×	○	×	×	×
電気ヒーター		×	○	×	×	×
スマートプラグ		×	○	×	×	×
電気スタンド		×	○ (スマート電球)	×	×	×
浄水器		×	×	×	○	×
食洗器		×	×	×	○	×
換気扇		×	×	×	○	×
温風暖房機（ガス・石油）	0社	×	×	×	×	×

（注）2020年秋の弊社調査結果に基づき作成

クラウドにはどんな機能が実装されるのか？

例えば、

1. IPアドレス解決のための機能
2. ユーザーが遠隔操作する際の認証情報管理・適用
3. ユーザーのスマートフォンに向けて、他者による操作や機器の停止などがあったことをプッシュ機能で通知
4. スマートフォンアプリ・家電製品用のファームウェアの配信用のサーバ
5. 家電製品とインターネットの接続状態の監視のための定期通信
6. ユーザーの家電製品の操作履歴、故障履歴、運転データの収集
7. ユーザがアプリ上でカスタマイズした設定情報のバックアップ　等

（注）2020年秋の弊社調査結果に基づき作成

どのような電気用品が安全に遠隔操作できるのか？

安全に遠隔操作できる電気用品とは、人の注意が行き届かないところで使うことを前提に設計された機器である。

人の注意が行き届かないところで使うことを前提に設計された機器

機器が単独（自己完結）で安全を確保しなければならず、より安全に配慮した設計が求められる

機器が単独（自己完結）で安全を確保できるので、遠隔操作が可能

遠隔操作の定義とは？

遠隔操作とは、機器が見えない位置からの操作のことである。
本日の講演の中では、公衆ネットワークを介しての遠隔操作を対象として話を進める。

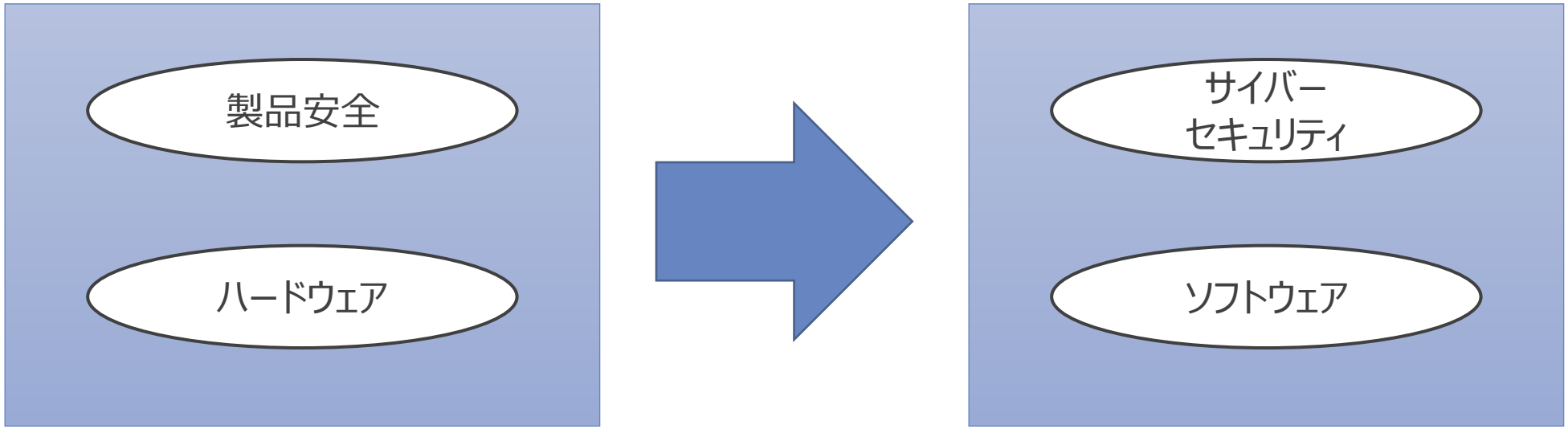
1. 遠隔操作とは、機器が見えない位置からの操作のこと。機器をOFF→ONする操作、ON→OFFする操作、機器の性能を調整する操作が対象となる。

2. 見えない位置とは、機器を直接見通すことができない位置のこと。別の部屋からの操作、共有管理室からの操作、外部（宅外）からの操作に分類される。

遠隔操作される電気用品等の安全とセキュリティ

今までは、安全とセキュリティは別物で順次

製品安全設計は、伝統的にハードウェア設計。一方で、ソフトウェア開発は別物で、担当する組織も異なるのが一般。製品開発の手順は、安全／ハードウェアの後に、サイバーセキュリティ／ソフトウェアというのが一般的な流れであり、別々の技術者が担当してきた。



従って、基本的には、製品安全規格とサイバーセキュリティ対策指針は別物で独立

安全／ハードウェアとサイバーセキュリティ／ソフトウェアは別物であるが故に、対応する製品安全規格とサイバーセキュリティ対策指針は別物で独立してきた。製品出荷後のソフトウェアアップデートの扱いがこの状況を変えつつある。

電気用品等では、これらをブリッジする技術規格は定められていない。
しかし、製品出荷後のソフトウェアアップデートが、この溝を埋め始めている。

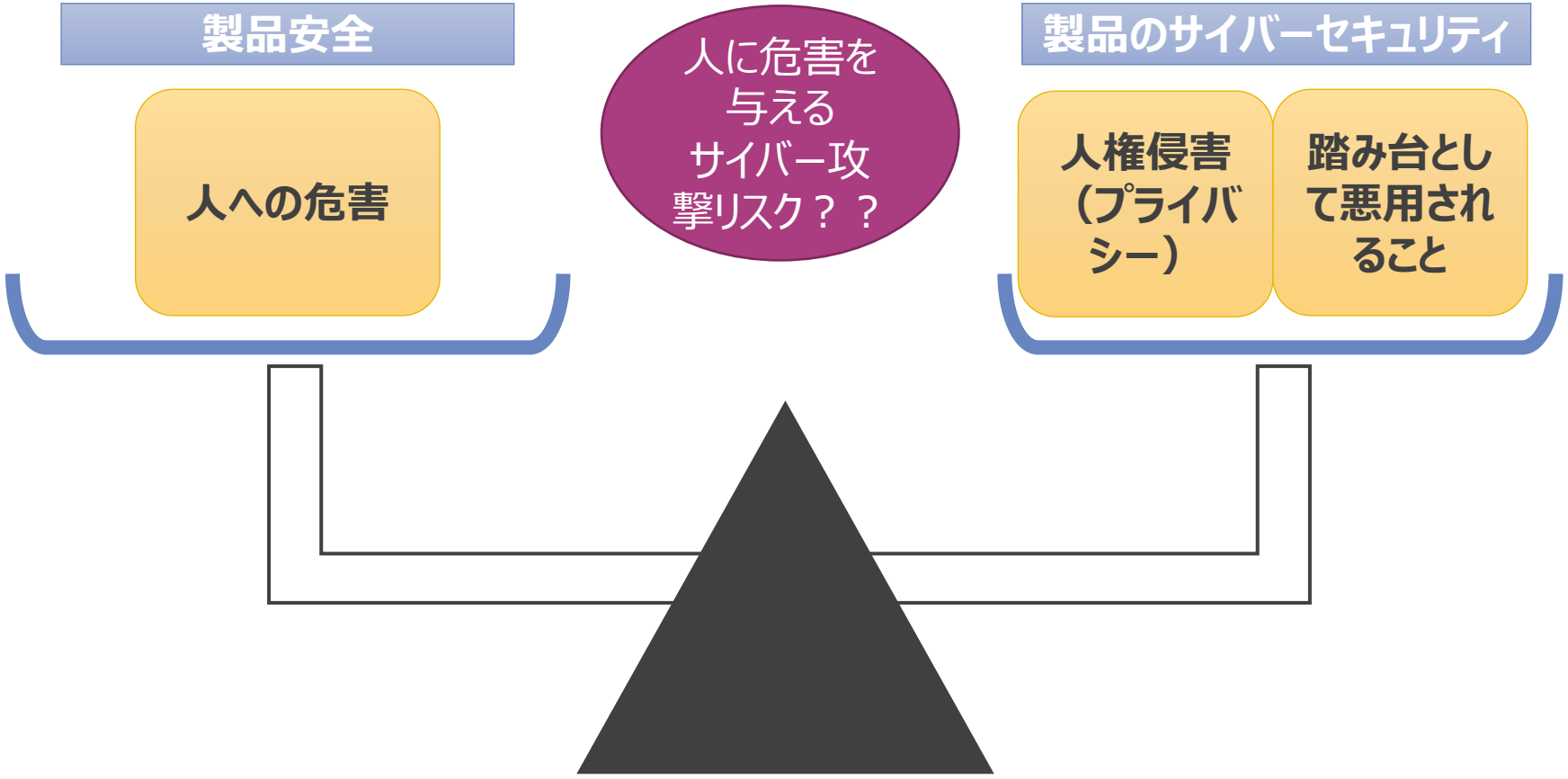
	製品安全規格・法制度	サイバーセキュリティ対策基準
国内	電気用品安全法等	サイバーフィジカルセキュリティ対策フレームワーク（経済産業省） CCDS　IoT分野共通セキュリティ要件ガイドライン　等
国際標準	IEC60335 Part 1／Part 2	英国の行動規範（DCMS）、欧州標準（ETSI）、EUサイバーセキュリティ認証フレームワーク（ENISA）、米国民間（UL）、米国の複数の州等多数

ASTMの製品安全規格

一般に、消費者IoT製品が対象であり、電気用品等のウェイトは必ずしも高くない

重視されるサイバーセキュリティリスクとは何か？

どちらが重く、どちらが軽いということはない。しかし、現状ではこれらは別々の枠組みで取り扱われている。
IoT化と遠隔操作は、人に危害を与えるサイバー攻撃リスクを生み出すことになる。これをどの程度重視すべきかについては、少なくとも、現行の法制度／技術規格や対策基準は答えを与えてくれない。



人に危害を与えるサイバー攻撃リスクの論点　－電気用品の場合

製品安全設計において、人に危害を与えるサイバー攻撃リスクを考える際には、法制度上の位置付け、生じる結果の同等性、完全性重視などに注意が必要。

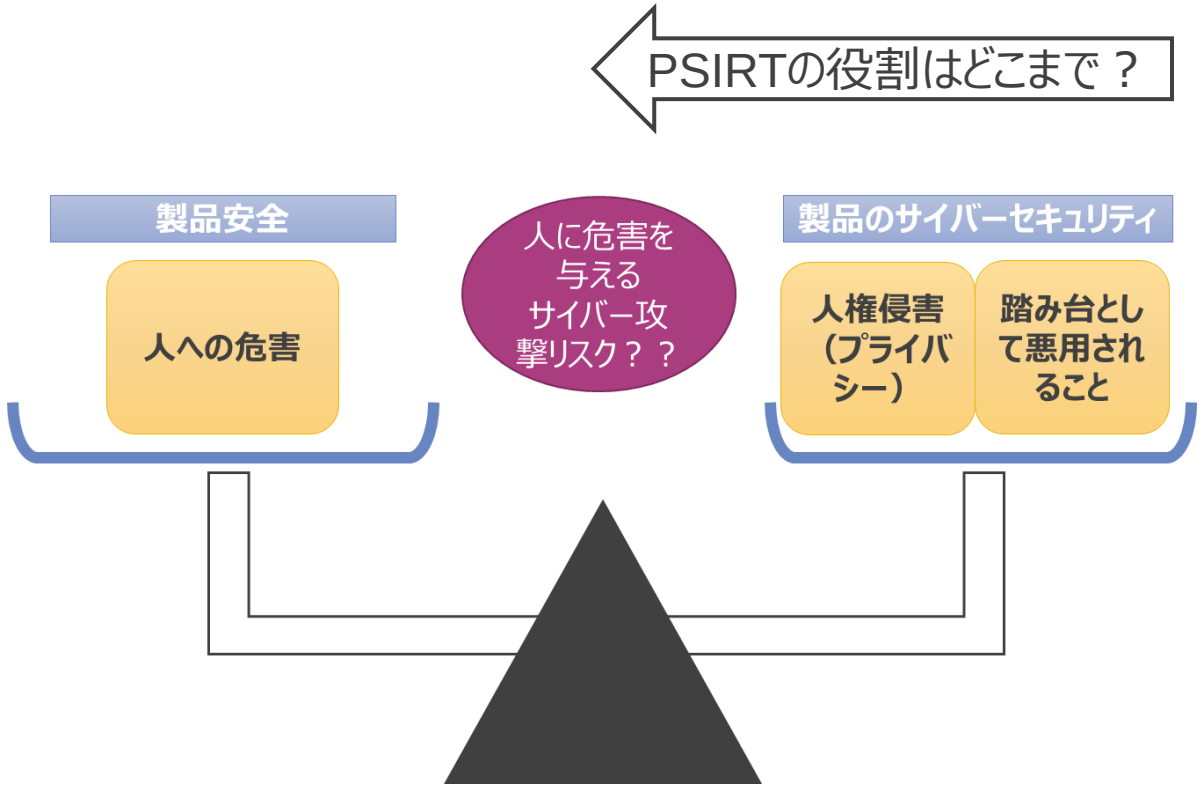
安全設計　VS　犯罪

誤使用・誤操作　VS　なりすまし

I（完全性）　＞　C（機密性）　A（可用性）

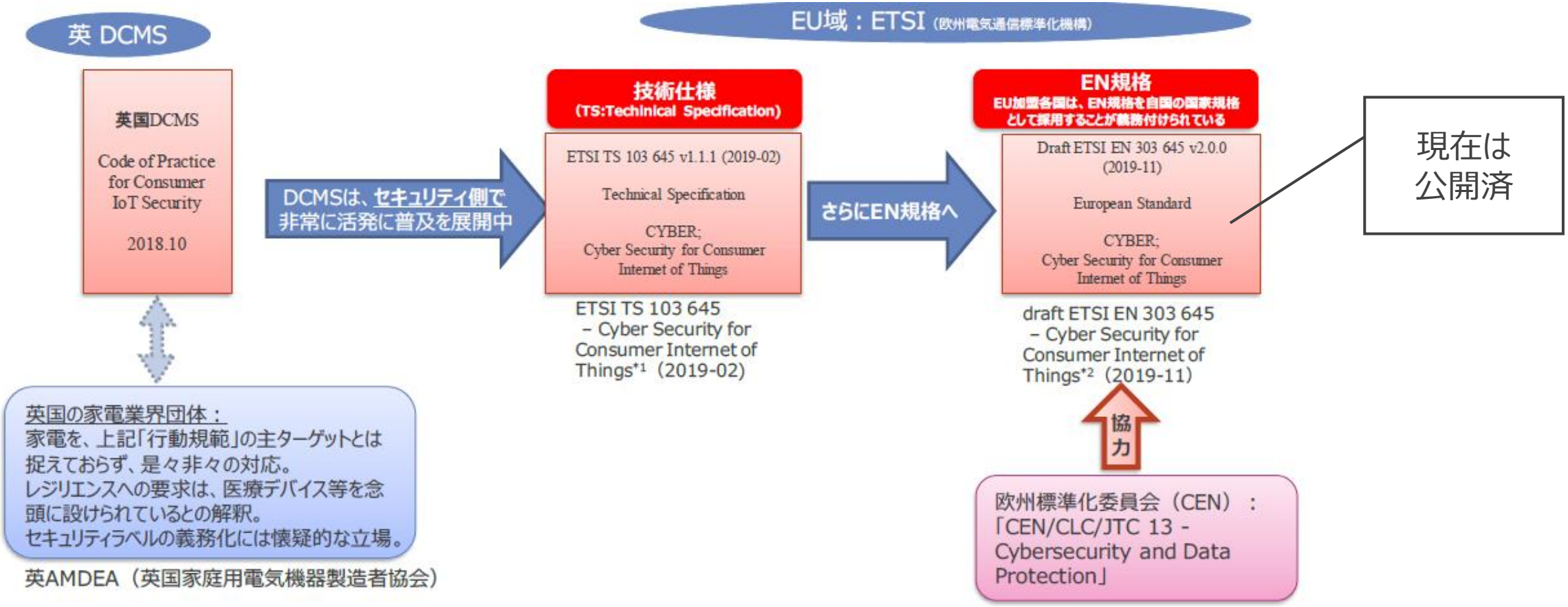
どこまでがPSIRTの果たすべき役割なのか？

PSIRTは、製品出荷前やソフトウェア・アップデートの公開前に徹底的にペネトレーションテストをするかもしれない。そうすることで、悪意のサイバー攻撃が抑止され、結果として人に危害を与えるサイバー攻撃リスクの低減を期待できる。しかし、これは製品安全設計ではなく、その枠外からの補完と捉えられる。



消費者向けIoT製品を対象としたサイバーセキュリティ対策基準の成立　– 欧州を中心とした動き

英国の「消費者向けIoT製品のセキュリティ行動規範」に端を発した動きは、欧州域に拡大し、欧州標準であるETSI EN 303 645が公開された。



出典：令和元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）報告書

欧州標準　ETSI EN 303 645の概要
“Cyber Security for Consumer Internet of Things　：　Baseline Requirements"

ETSI EN 303 645は、消費者向けIoT機器の開発・製造者等に向けた、消費者向けIoT機器のサイバーセキュリティを確保するために必要な13個の要求事項を定めている。

対象となる製品の例：
洗濯機や冷蔵庫などの家電製品、子供用玩具やベビーモニター、煙検知器、ドアロック、窓センサー、IoTゲートウェイ／基地局／ハブ、スマートカメラ、スマートテレビ、スマートスピーカー、ウェアラブルヘルストラッカー、ホームオートメーションと警報システム、スマートホームアシスタント等

要求事項（行動規範レベル）：
①デフォルトパスワードを実装しないこと、②脆弱性申告の手段を確立すること、③ソフトウェアの更新、④機密性の高いセキュリティパラメータの安全な保存、⑤安全な通信経路、⑥攻撃対象となるサービスや通信の最小化、⑦ソフトウェアの完全性の確保、⑧個人情報の安全性の確保、⑨システムのレジリエンスの高度化、⑩テレメトリーデータ（利用状況等）の異常の調査、⑪個人情報削除の仕組み、⑫機器の導入やメンテナンスの容易性の確保、⑬入力データの検証

消費者向けIoT製品を対象とした製品安全基準の成立　－米国ASTM F3463-20の概要 “Standard Guide for Ensuring the Safety of Connected Consumer Products"

ASTMが昨年10月に公表した製品安全確保のためのガイダンス。IoT化された消費者製品に生じる製品安全上の危害を防止するための共通規範と、当該規範への適合を評価するための手法について、要求事項をまとめている。ソフトウェア、ファームウェア及びその遠隔アップデートに起因する物理的リスクについても多く言及している。

対象となる製品の例：

ネットワーク接続される子供用のおもちゃ、ネットワーク接続される煙探知機やドアロック等の安全関係製品、ネットワーク接続されるテレビやスピーカー、ネットワーク接続されるウェアラブルなヘルスモニター／スマートアパレル、ネットワーク接続されるホームオートメーション、セキュリティまたは監視カメラ、及び警報システム、ネットワーク接続される家電製品（洗濯機や冷蔵庫など）、ネットワーク接続されるスマートホームアシスタント、ネットワーク接続される赤ちゃんモニター等

要求事項（情報セキュリティ（ソフトウェアのアップデート）に関する要求事項）：

- 製品安全設計に関する要件
  ソフトウェアのアップデートができること
- 製造メーカー、輸入業者及び／又は流通業者への要件
  ソフトウェアのアップデートに対する安全性評価、ファームウェア／ソフトウェアのアップデートを市場に出す前に、安全性を損なわないことを試験・確認、製品のライフサイクル全体での適切なソフトウェア構成管理とトレーサビリティの維持

人に危害を及ぼす遠隔操作への対策の現状

製品の遠隔操作における「人への危害」についての考え方

製品の遠隔操作においては、社会情勢の変化を受けて、リスク評価の対象となる「製品から直接発生する被害」を考慮するだけでは追い付かなくなってきている。新たに間接被害への配慮が求められるようになってきている。

【製品から直接発生する被害】
電気用品調査委員会の「「解釈別表第八に係わる遠隔操作」に関する報告書(2019年11月18日)」等で配慮すべき危険源

- 電気的ハザード(感電)、火災ハザード(発煙・発火)、火傷ハザード、機械的ハザード(可動部、回転部、振動、爆発、爆縮など)
- 化学的及び生物学的ハザード
- 電気用品から発せられる電磁波等による危害の防止
- 人間工学原則無視によるハザード
- 危険源の組み合わせ、電気用品が使用される環境に関連する危険源

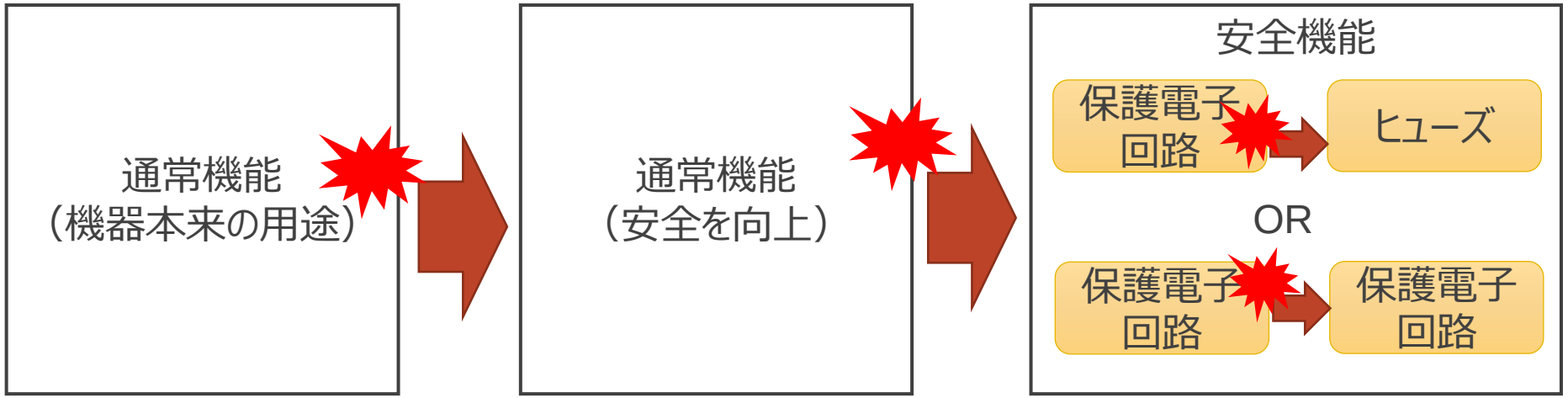
これらは基本的に、IEC Guide 104の附属書の記述に基づいている。

【遠隔操作による間接被害】
しかし、遠隔操作においては、社会情勢の変化によって、機器の近くにいる家族や周囲において直接発生する被害、機器が運転／停止し続けることによる被害（熱中症、やけど、間接的に生じる健康被害、間接的に生じる火災）なども無視できなくなってきている。

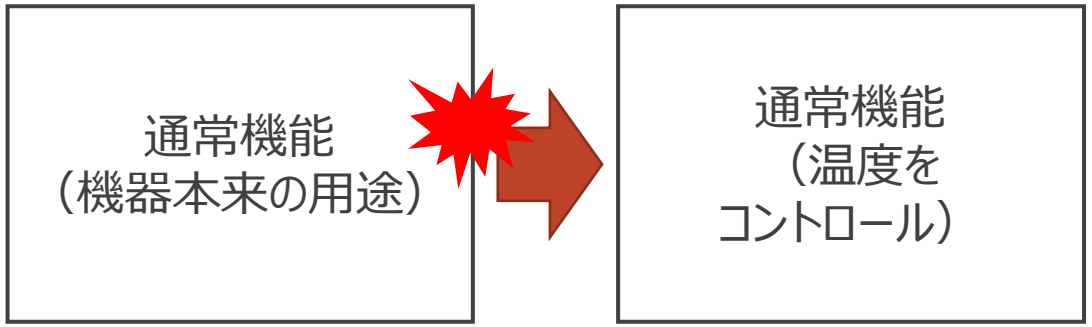
製品安全における多重防護の考え方

電気用品等の場合、製品単体で製品安全を確保するという考え方であるため、製品の通常機能に加えて、安全機能を用いた多重防護が構成される。安全機能の中でも二重の防護が構築されており、最後はヒューズで物理的に止めるというのが基本的考えである。しかし、現在はヒューズの代わりに保護電子回路を使うことも可能。

火災、感電、死傷の場合：



やけどの場合：



※多重防護の考えなし

電気用品等の製品安全に関する国内外の法制度や技術規格のカバレージ

現在、電気用品等の製品安全に関する国内の法制度や技術規格は、設計・開発時の直接被害対策を対象としており、間接被害や出荷後はスコープとしていない。

	設計・開発時	出荷後
直接被害	現在の 法制度（電気用品安全法等）、 技術規格（法令の解釈別表等）の カバレージ	スコープ外
間接被害	スコープ外	スコープ外

電気用品安全法における遠隔操作

人に危害を及ぼす遠隔操作に対する対策要求においては、危険源、通信回線の途絶や故障に対するフェイルセーフ、外乱への耐性、いざとなったら手元優先、予見できる誤操作防止、使用者への注意喚起、デフォルトでは使えない等が求められており、セキュリティ対策で重要になる機密性や可用性については基本的にスコープ外となる。

人に危害を及ぼす遠隔操作への対策の構成　ー電気用品安全法の場合

遠隔操作に伴う危険源がない

通信回線が途絶しても安全を維持、復旧の見込みが無い時は安全な状態を確保できる

手元操作優先
容易に通信回線の切り離しができる

遠隔操作結果のフィードバックができる　又は
動作保証試験＋使用者への注意喚起

操作機器の識別管理、外乱に対する誤動作防止、通信回線接続時の再接続（常時ペアリングが必要な通信方式）

公衆回線を利用する場合、回線の一時途絶や故障等による安全性に影響を与えない対策を講じる

同時に２か所以上からの遠隔操作を受け付けない

誤操作防止対策

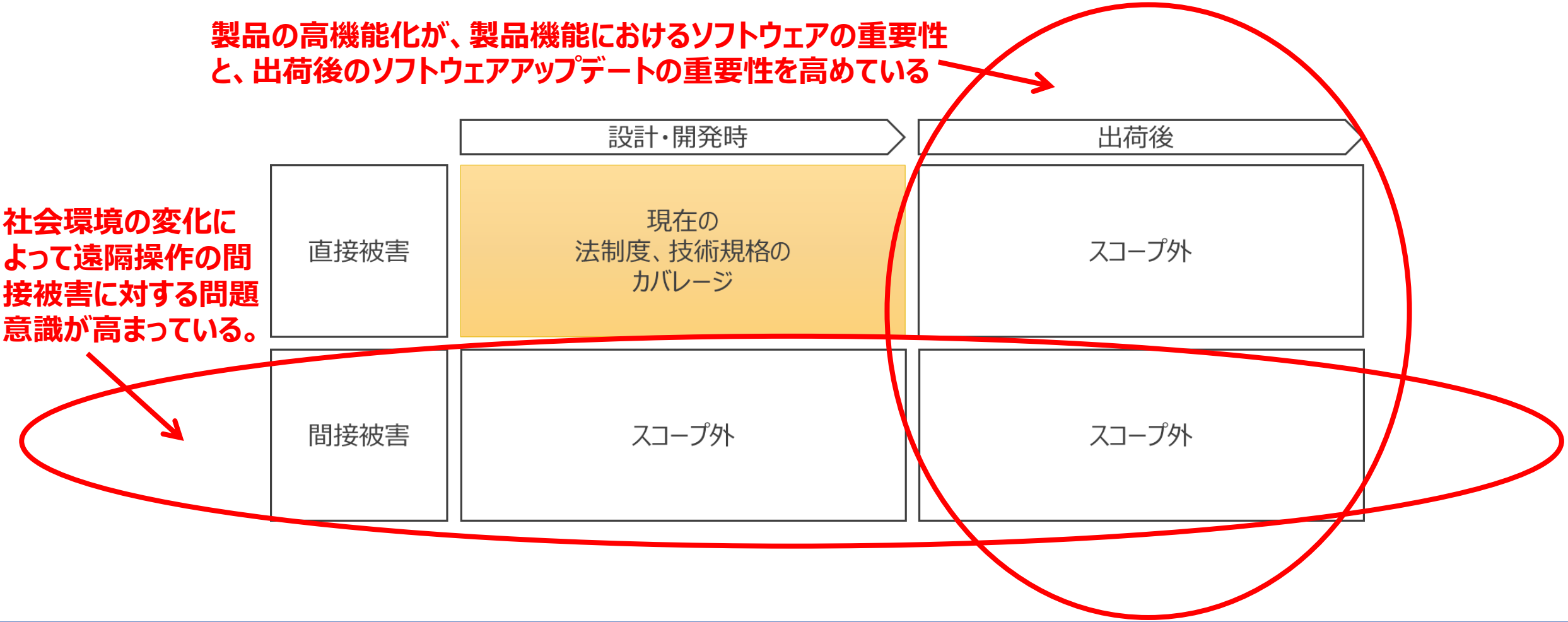
出荷状態において、遠隔操作機能を無効化

人に危害を及ぼす遠隔操作への対策の現状

遠隔操作とソフトウェアのアップデートに係る安全確保のために、従来の法制度、技術規格ではカバーされていなかった間接被害や出荷後にも配慮することが必要になってきた。

製品の高機能化が、製品機能におけるソフトウェアの重要性と、出荷後のソフトウェアアップデートの重要性を高めている

社会環境の変化によって遠隔操作の間接被害に対する問題意識が高まっている。



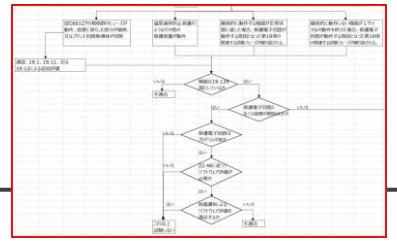
IEC60335-1第６版が求める
ソフトウェアと遠隔操作に対する要求事項

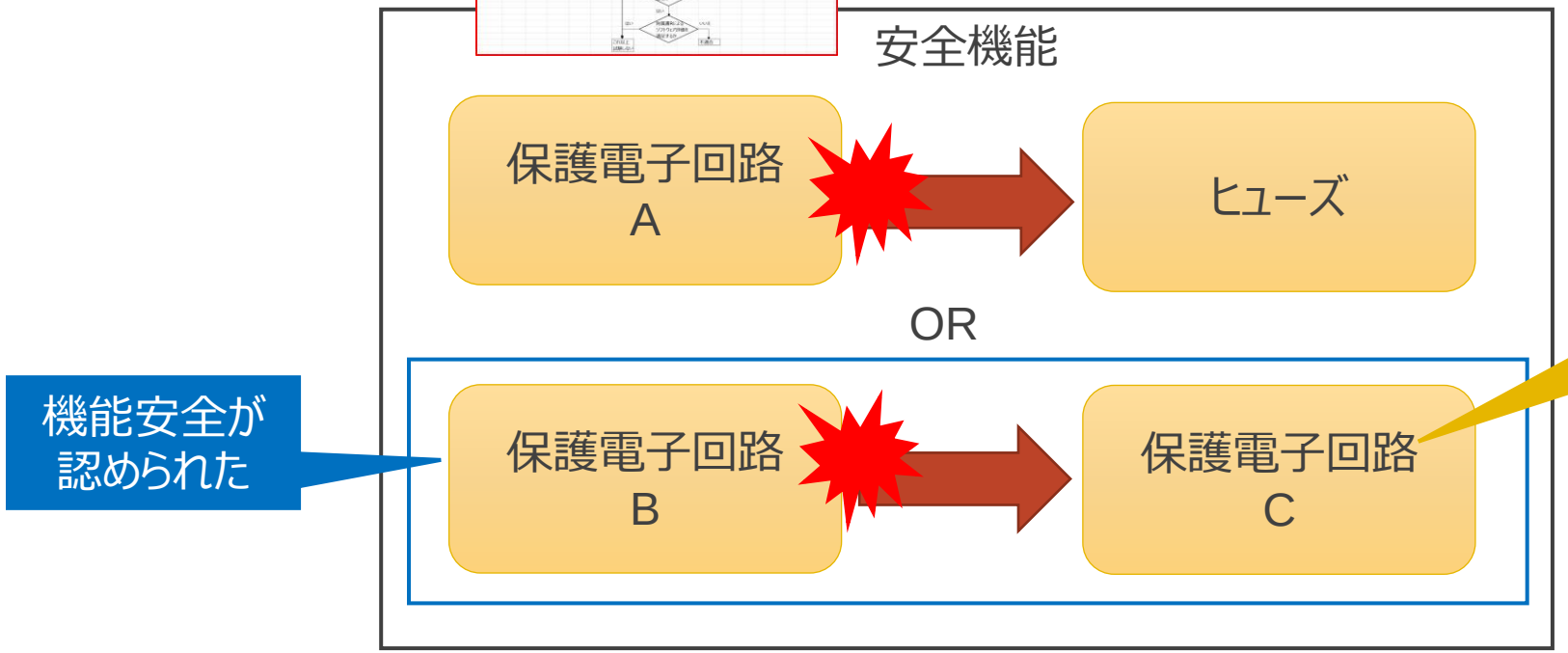
IEC60335-1　機能安全とソフトウェア評価に関する要求事項の追加

第５版の段階で、附属書Qと附属書Rが適用された。

これによって、最終的に安全を確保する保護電子回路Cのソフトウェアに附属書Rのソフトウェア評価を適用することで、保護電子回路Bと保護電子回路Cの二重化からなる機能安全の適用が認められた。

附属書Q





但し、
附属書Rによるソフトウェア
評価の実施が条件

※なりすましによる遠隔操作はともかくとして、悪意のサイバー攻撃を考慮すると通信回線から完全に遮断することは厳しい。

IEC60335-1第６版の公開　－第６版は情報セキュリティ対策にどこまで踏み込んだか？

IEC TC61は、ISO/IEC JT1と協力して、家電製品の安全評価のための包括的な規格を維持したままで、IoT技術に関する安全関連リスクに対応するため、附属書Uを新たに策定した。

附属書Uの要求事項が最新であることを確実にするため、JTC1/SC27（セキュリティ技術）とJTC1/SC41（モノのインターネットと関連技術）の作業と出版物を監視するとのこと。

製品安全に影響を及ぼさない

機密性

非否認性
（ログ）

可用性

附属書Uのカバレージ：製品安全に影響を及ぼしうる

完全性

真正性
（対なりすまし）

※悪意あるサイバー攻撃（犯罪行為等）は対象としていない。

附属書Uの要求の主要な構成要素　－情報セキュリティ対策

【適用範囲 22.62項】

a) 以下のソフトウェアのダウンロードまたはデータの伝送を含む遠隔通信：
- 22.46 に準拠するために必要な附属書 R（必ず守る必要がある） に従った措置（機能安全）
- 本規格の第8～32節に準拠するために必要な手段

b) ソフトウェアのダウンロード又はデータの送信を含む遠隔通信であって、上記のケースa)でカバーされないソフトウェアの部分にのみ影響を与えるものであって、上記のケースa)におけるソフトウェア又はデータとの不適切な分離又は分割によって本規格の遵守が損なわれる可能性があるもの。

ソフトウェアの分割
U.3.1項

完全性　U.3.2項

使用者の承認
U.3.9項

ソフトウェアのアップデートに対する安全性評価　22.46項

暗号技術の適用　U.3.7項

クラウド上などへの安全制御ソフトウェアの実装禁止　U.3.6項

適正な版のダウンロード
U2.1項

遠隔通信の監視　U.3.5項

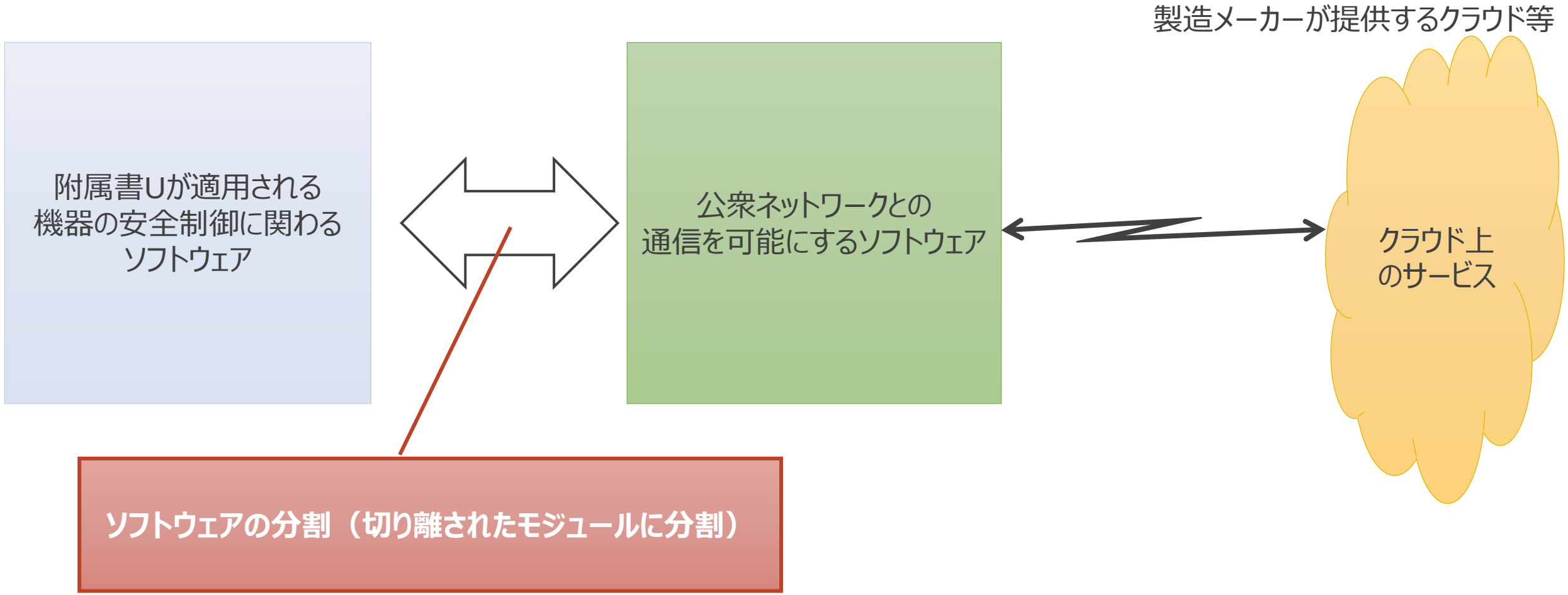
機器使用中のアップデートの安全性　U3.10項

真正性（アクセス権限管理と認証）U.3.4項

アップデート前の確認
U.3.8項

ソフトウェアの分割とは？　（U.3.1項）

U.3.1 公衆ネットワークとの通信を可能にするソフトウェアは、本標準の他の要求を遵守するために必要なソフトウェア（＝安全担保に使用しているソフトウェア）と切り離されたモジュールに分割しなければならない。



クラウド上などへの安全制御ソフトウェアの実装禁止とは？　（U.3.6項）

U.3.6 機器の安全制御は、遠隔通信に依存してはならない。

製造メーカーが提供するクラウド等

附属書Uが適用される
機器の安全制御に関わる
ソフトウェア

遠隔通信

クラウド上のサービス

例えば、

1. IPアドレス解決のための機能
2. ユーザーが遠隔操作する際の認証情報管理・適用
3. ユーザーのスマートフォンに向けて、他者による操作や機器の停止などがあったことをプッシュ機能で通知
4. スマートフォンアプリ・家電製品用のファームウェアの配信用のサーバ
5. 家電製品とインターネットの接続状態の監視のための定期通信
6. ユーザーの家電製品の操作履歴、故障履歴、運転データの収集
7. ユーザがアプリ上でカスタマイズした設定情報のバックアップ　等

遠隔通信に依存しない
＝遠隔通信が切れてもソフトウェアの
機能が維持されて安全が守られる
（分離）

（参考）附属書Uの主要な要求内容

附属書Uの適用範囲	22.62 公共ネットワークを介した遠隔通信は、この規格への準拠を損なうものであってはならない。この要求は以下にのみ適用される。 a) 以下のソフトウェアのダウンロードまたはデータの伝送を含む遠隔通信： - 22.46 に準拠するために必要な附属書 R（必ず守る必要がある） に従った措置（機能安全）　　- 本規格の第8～32節に準拠するために必要な手段 b) ソフトウェアのダウンロード又はデータの送信を含む遠隔通信であって、上記のケースa)でカバーされないソフトウェアの部分にのみ影響を与えるものであって、上記のケースa)におけるソフトウェア又はデータとの不適切な分離又は分割によって本規格の遵守が損なわれる可能性があるもの。 なお、本要求事項は下記のような機器には適用されない： - この規格に準拠するためのすべての手段がソフトウェアから独立しているもの　　- データの送信のみを目的として公衆ネットワークを介した遠隔通信を使用するもの - イベント駆動型のメッセージまたはプッシュ型の遠隔監視のみを提供するもの
通信回線との分離（22.62のa)またはb)を満足するソフトウェアの遠隔通信に適用）	U.3.1 公衆ネットワークとの通信を可能にするソフトウェアは、本標準の他の要求を遵守するために必要なソフトウェア（＝安全担保に使用しているソフトウェア）と切り離されたモジュールに分割しなければならない。
ソフトウェアのアップデートに対する安全性評価	22.46 この規格に適合することを確実にするために，プログラマブル保護電子回路を用いる場合，ソフトウェアは，表R.1に規定する故障／エラー状態を制御するための手段を含まなければならない。 必要な場合，表R.2に規定する故障／エラー状態を制御するための手段を含むソフトウェアを，特定の構造又は特定の危険への対処のために第2部の個別規格に規定する。 これらの要求事項は，機能目的又は箇条11に適合するために用いるソフトウェアには適用しない。 適否は，附属書Rの関連する要求事項に従って，ソフトウェアの評価によって判定する。 ソフトウェアを変更したとき，その変更が保護電子回路に関わる試験の結果に影響を及ぼす場合，評価及び関連試験を繰り返す。
適正な版のダウンロード	U.2.1 ソフトウェアのダウンロードを提供する場合には、機器内で実行されているソフトウェアの現バージョンを識別するための、製造者によって与えられた固有の名称またはコードを取得する方法または場所についての指示が提供されなければならない。また、指示書には、ソフトウェアのアップデート手続きにおいて従わなければならない手順を記載しなければならない。
真正性（アクセス権限管理と認証）	U.3.4 アクセス権限承認の前に遠隔通信を有効にしてはならない。権限承認は認証に基づかなければならない。通信する両者のIDを保証するために、認証プロセスは暗号技術を用いなければならない。 上記要求の目的のために、認証／権限承認プロセスの準備のための両者間の通信は遠隔通信とは考えない。
完全性	U.3.2 遠隔通信は機器により、以下を提供するソフトウェアを介して確立、実装、終了されなければならない。 - 以下に関連したデータ完全性保護 ・データ破損　　・破損への対処　　・間違ったタイミングまたは順序　　・永続的な”自動送信”または繰り返し　　・データ伝送の中断 - どんな理由であれ、不完全な、途中で切り捨てられた、エラーを含んだ、または正しい書式ではあってもそのタイプのメッセージに期待される範囲外の情報を伝達する通信を検知し、これに対応する手段 - 表R.1で指定された故障／エラー条件を制御する手段
暗号技術の適用	U.3.7 遠隔通信の権限がひとたび承認されたら、データ完全性を保護するために暗号技術が実装されなければならない。 採用される暗号技術は、付属品を含む機器の一部でなければならず、ルーターの一部や類似のデータ伝送デバイスそれ自体に異存してはならない。また、暗号技術は、伝送に先立って実行されなければならない。
遠隔通信の監視	U.3.5 不正アクセスを防止し、遠隔通信における伝送故障／エラーを検知するための措置を講じなければならない。
アップデート前の確認	U.3.8 製造者によって提供され、遠隔通信を介して機器に送信されるソフトウェアアップデートは、インストール前に必ず以下について検証されることを確実にしなければならない： - 通信中のデータ破損がないこと - ソフトウェアの版が、その版を設計した対象である機器と適合していること さらに、上記のチェックを実行するソフトウェアは、表R.1で指定した故障／エラー条件を制御するための手段を具備していなければならない。 ※附属書Rの高信頼性ソフトウェア設計手法を転用。従って、ソフトウェア管理については、赤字と同じ取扱いが求められることになる。
使用者の承認等	U.3.9 ソフトウェアの機器への各インストールは、機器に責任を持つ人物の許可を得なければならない。 使用者が、自動的なソフトウェアアップデートを可能にするモードを起動することは、許容される。
同時または順次行われる複数の主体による遠隔操作からの保護	U.3.3 複数の主体からメッセージを同時または順次受信することで生じるハザードから保護する措置を講じなければならない。
クラウド上等への安全制御ソフトウェアの実装禁止	U.3.6 機器の安全制御は、遠隔通信に依存してはならない。
機器使用中のアップデートの安全性	U.3.10 ソフトウェアのインストールが、そのインストール中またはインストール後に、この規格の要求遵守を無効にしてはならない（＝製品の安全が担保される必要がある）。

出荷後の製品安全の維持　－情報セキュリティからサイバーセキュリティへ

ETSI／ASTM等の消費者IoT製品に係る国際技術規格がサイバーセキュリティについて何を要求しているかを参考にすると、ソフトウェア管理、定期的なセキュリティアップデート、使用者等への情報提供等について、さらに追加で考慮すべき。

【附属書Uの情報セキュリティ対策】

- ソフトウェアの分割 U.3.1項
- 完全性　U.3.2項
- 使用者の承認 U.3.9項
- ソフトウェアのアップデートに対する安全性評価　22.46項
- 暗号技術の適用　U.3.7項
- クラウド上などへの安全制御ソフトウェアの実装禁止　U.3.6項
- 適正な版のダウンロード U2.1項
- 遠隔通信の監視　U.3.5項
- 機器使用中のアップデートの安全性　U3.10項
- 信憑性（アクセス権限管理と認証）U.3.4項
- アップデート前の確認 U.3.8項

【追加で考慮すべきサイバーセキュリティ対策】

ソフトウェア管理：
インシデントデータ収集システムの維持・更新、出荷・アップデート提供前の既知のサイバーセキュリティの脅威に対する脆弱性試験の実施、製品のライフサイクル全体を通じて適切なソフトウェアおよびハードウェア構成管理とトレーサビリティの維持を確実にするための合理的な措置、セキュアコーディングの原則

定期的なセキュリティアップデート：
初期化後、定期的にセキュリティアップデートが利用可能かどうかを確認

使用者等への情報提供：
- ■ 製造メーカーは、セキュリティアップデートが必要であることを、そのアップデートによって緩和されるリスクに関する情報とともに、認識可能かつ明白な方法で使用者等に通知
- ■ 製品のサポート期間（ソフトウェアのアップデートを提供する期間）を使用者等に情報提供
- ■ ソフトウェアに不正な変更が検出されたことを使用者等に警告

遠隔操作による間接被害への対応の在り方

遠隔操作による間接被害とは？　（再掲）

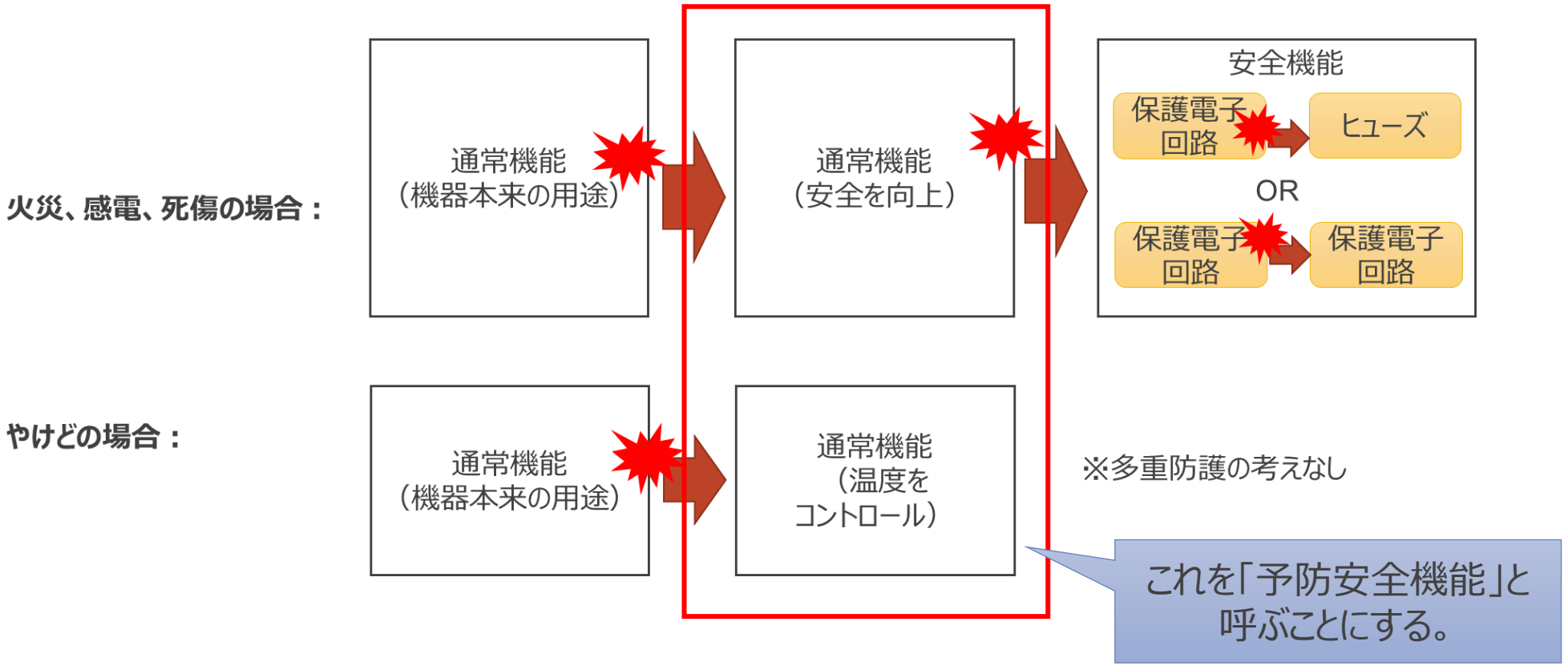
【遠隔操作による間接被害】

遠隔操作においては、社会情勢の変化によって、機器の近くにいる家族や周囲において直接発生する被害、機器が運転／停止し続けることによる被害（熱中症、やけど、間接的に生じる健康被害、間接的に生じる火災）なども無視できなくなってきている。

間接被害への備えの考え方

間接被害は、電気用品安全法やIEC60335-1のスコープ外。

従って、遠隔操作によって使用者に生じる間接被害に備えるために、これら法制度・技術規格が適用されない「安全を向上させる通常機能」を積極的に活用してはどうか。



予防安全機能とは？

【予防安全機能】　※この任意の予防安全機能を活用して、遠隔操作の間接被害に備える！

必ずしもすべての製品にある機能ではないが、リスク低減として一定の効果があると考えられる機能であって、安全機能ではないもの。機能の適用は操作者が選択できる。

例１：付加的に、又はオプションとして選択し、使用者（機器の近くにいる人：特に高齢者や子供）への危害を防止または低減する機能

例２：遠隔操作の操作者の過信／誤操作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：特に高齢者や子供）に及ぼす不意の危害を、防止または低減できる機能

例３：遠隔操作中であることの表示や製品の周囲等の安全を確認するシステムが、使用者（機器の近くにいる機器を操作可能な人）に対する警報も含めて、使用者に対応を要求して遠隔操作時のリスクを低減する機能

例４：遠隔操作する機器とは別の「周囲等の安全を確認する外部システム」が、遠隔操作時のリスクを回避／低減する制御／ロック機構等を自動的に作動させるもの

例５：内蔵される検知機能又は組み合わせて使用する外部の検知器が、操作者が機器のそばを離れたことを検知したら、機器を安全に停止させる機能

例６：先進技術とソフトウェアを取り入れたベストエフォートの制御（例：ロボット掃除機、自動運転等が具備する「周囲の使用者や物を感知し自動的に回避する技術等」）により、操作者や使用者への危害を防止、または低減する機能

予防安全機能は必ず機能するという保証がない（技術規格が求める試験をしていない）ため、過信をせずに用いる。

スリーステップからステップ４へ！　使用者の役割の拡大

遠隔操作においては、操作者の遠隔操作に、機器の近くにいる使用者が気付かずに、間接被害を受けてしまう恐れが生じる。能動的な「使用上の注意」を予防安全機能として装備し、使用者に対応を要求することで間接被害を低減するシナリオは、従来のスリーステップメソッドの枠に収まらない。これは、「ステップ４」とも呼べるこれからの新しい概念として期待される。

電気用品

製品安全設計のスリーステップメソッド

１．本質的安全設計

２．安全防護、追加防護

３．使用上の注意

予防安全機能：
遠隔操作中であることの表示や製品の周囲等の安全を確認するシステムが、**使用者に対する警報も含めて、使用者に対応を要求して**遠隔操作時のリスクを低減する機能

使用者を操作者に！

ステップ４：使用者が機器から提供された情報に基づき、能動的に、機器を安全に操作

連絡先

ご質問等、お気軽にご連絡ください。

三笠　武則
株式会社ＮＴＴデータ経営研究所
Eメール：mikasat@nttdata-strategy.com
電話：03-5213-4115

NTT DATA

Trusted Global Innovator