

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

令和2年3月

株式会社エヌ・ティ・ティ・データ経営研究所

目次

1. 調査の背景・目的	3
1.1. 背景	3
1.2. 目的	3
1.3. 事業概要	4
1.4. 実施期間	4
2. 事業内容	4
2.1. 電気用品等製品の安全性確保に係る実態調査	4
(1) 将来（3～5年後）想定され得るIoT化等が考えられる電気用品等製品の調査.....	4
(2) 遠隔操作機構を有する電気用品等製品ごとのフェールセーフ機構（物理的安全性）及びソフトウェアによる安全制御（機能安全）に関することの調査.....	10
(3) IoT化等が考えられる電気用品等製品ごとにセキュリティ対策を組み込む場合のフェールセーフ機構（物理的安全性）及び機能安全に与える影響に関することの調査.....	13
2.2. IoT化等された製品に関するトラブル、事故の実態調査	16
(1) 公知文献の検索・収集	16
(2) 有識者へのヒアリング調査	20
(3) 調査結果のまとめ	21
2.3. IoT化等された若しくはIoT化等が考えられる電気用品等製品の安全に関する海外政府・産業界等の動向調査	23
(1) 文献調査	23
(2) 海外ヒアリング結果.....	43
(3) 調査結果のとりまとめ	45
2.4. IoT化等が考えられる電気用品等機器に係る消費者の生命、身体への危害発生の防止を図るための製品安全の確保の在り方に関する検討.....	47
(1) 検討会について.....	47
(2) WGについて	48
2.5. IoT化等が考えられる電気用品等製品において今後想定される消費者の生命、身体への危害発生等のリスクシナリオ及びユースケースの整理・検討	49
(1) IoT化された電気用品等のリスク対応の在り方に関する検討の実施方針.....	49
(2) IoT化された電気用品等のユースケース/リスクシナリオ例	69
(3) 今後の課題：ソフトウェアのダウンロードについて.....	80
3. まとめ	83
(1) 検討内容のまとめ	83
(2) 今後の課題及び検討の方向性について.....	84

1. 調査の背景・目的

1.1. 背景

経済産業省では、第四次産業革命の技術変化を踏まえ、データ連携を中心とする **Connected Industries** と、それに対応したデータ利活用を促進する制度などの新たな経済社会システムの構築を通じて、サイバー空間と実空間が高度に融合した **Society5.0** の実現を目指しているところ。「**Society5.0**」の実現に向け、産業構造、社会環境の変化に伴うサイバー攻撃の脅威の増大に対応するため、セキュリティ対策の全体像を整理し、産業界のセキュリティ対策例を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」が取りまとめられた。

一方、英国デジタル・文化・メディア・スポーツ省（以後、「英国 **DCMS**」という。）では、消費者向け **IoT** 製品を利用するユーザのセキュリティに関する負担を軽減するため、製造事業者等が実践すべき行動規範を 2018 年 10 月に取り纏められた。また、米国カリフォルニア州では、インターネットに接続する機器にセキュリティ機能を備えることを製造者に求める法律が 2018 年 9 月に制定された。

こうした産業構造の変化の中、現状、社会的関心を引くような **IoT** 製品による消費者の生命身体へ脅威を及ぼす事故は見受けられていない。しかしながら、家庭内の電気製品においても、スマートフォン等による遠隔操作が行われるなど社会的な需要も高まってきている一方で、ソフトウェアやセンシング不良、外部からの攻撃等により、**IoT** 製品が消費者の生命身体へ脅威を及ぼす事故を発生させるリスクも増大していくと考えられる。

他方、電気用品等製品（スマートハウス、**HEMS** で用いられる電気用品等消費生活用製品等（関連電気製品（ルータ、**PC** 等）を含む））に対して規制している製品安全関連法（電気用品安全法、消費生活用製品安全法、**PL** 法等）は、ハードウェアの欠陥に起因する生命身体に脅威を及ぼす製品事故の防止や救済の目的で整備されてきており、ソフトウェアやデータ不良、複合的なシステムの相互作用が生命身体に脅威を及ぼす製品事故を引き起こすようなリスクに対して現行法が必ずしも十分に整備されているとは言い切れない。

1.2. 目的

このような状況を踏まえ、国内外の電気用品等製品の **IoT** 化（人工知能（**AI**）の活用を含む。以下「**IoT** 化等」という）を起因としたトラブルや事故、遠隔操作機構を有する電気用品等製品のフェールセーフ機構の実態、**IoT** 化等された電気用品等製品のソフトウェアによる安全制御（機能安全）の組み込み等について情報収集し、将来（3～5 年後）懸念される **IoT** 化等が考えられる電気用品等製品の利用に伴うリスクやユースケースを体系的に整理・検討する。また、**IoT** 化等された若しくは **IoT** 化等が考えられる電気用品等製品に対する規制や業界規格の策定等に関する国内外の政府・事業者の動向調査も行い、今後の電気用品等製品の **IoT** 化等に係る製品安全確保の在り方について検討を行うもの。

1.3. 事業概要

- ・電気用品等製品の安全性確保に係る実態調査
- ・IoT化等された製品に関するトラブル、事故の実態調査
- ・IoT化等された若しくはIoT化等が考えられる電気用品等製品の安全に関する海外政府・産業界等の動向調査
- ・IoT化等が考えられる電気用品等機器に係る消費者の生命、身体への危害発生防止を図るための製品安全の確保の在り方に関する検討会およびWGの開催
- ・IoT化等が考えられる電気用品等製品において今後想定される消費者の生命、身体への危害発生等のリスクシナリオ、ユースケース及びリスク評価の整理・検討

1.4. 実施期間

令和元年7月22日～令和2年3月31日

2. 事業内容

2.1. 電気用品等製品の安全性確保に係る実態調査

(1) 将来（3～5年後）想定され得るIoT化等が考えられる電気用品等製品の調査

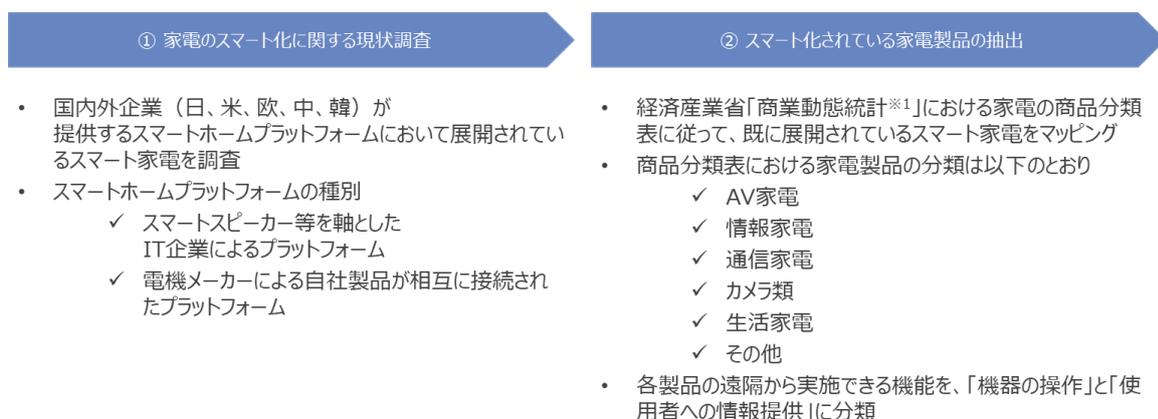
インターネット、業界紙、学会誌・論文集・予稿集等を調査し、IoT化等された電気用品等製品を製造する国内外の事業者の、製品安全確保に対する先進的な取組みを抽出して取りまとめた。

1) IoTスマートホームプラットフォームにて展開されているスマート家電の調査

IoTスマートホームプラットフォームにて展開されているスマート家電の調査を行い、経済産業省「商業動態統計」における家電製品分類をもとにスマート化の状況を整理した。

具体的には、①家電のスマート化に関する現状調査、②スマート化されている家電製品の抽出と、2つのステップで調査を行った。

図表1 将来（3～5年後）想定され得るIoT化等が考えられる電気用品等製品の調査ステップ



(ア) 家電のスマート化に関する現状調査

国内外（日本、米国、欧州、中国、韓国）の企業が提供するスマートホームプラットフォーム

において展開されているスマート家電を調査した。本節では、スマートホームプラットフォームに関して、①スマートスピーカー等を軸とした IT 企業によるプラットフォーム、②電機メーカーによる自社製品が相互に接続されたプラットフォームの 2 つに分類したうえでそれぞれの概要について述べる。

i. スマートスピーカー等を軸とした IT 企業によるプラットフォーム

a. Google Home (Google)

Google Home とは、Google 社が開発した AI アシスタントである Google Assistant が搭載されたスマートスピーカーである。対応する家電製品を接続又はプラットフォーム上で家電製品メーカー等サードパーティが提供する家電連携のためのアドオン機能「Actions on Google」を有効化することで、対象機器を音声操作することができる。

なお、連携できる家電製品又は家電製品や設備を操作するための「Actions on Google」の一覧は Google アシスタントの Web ページで一覧化されている。

今回、Google Home の Web ページ上でパートナーと位置付けられている製品を抽出対象とした（サードパーティが提供する「Actions on Google」を通じて連携できる家電製品は抽出の対象外）¹。

b. Amazon Echo (Amazon)

Amazon Echo とは、Amazon 社が開発した AI アシスタントである Alexa が搭載されたスマートスピーカーである。Google Home と同様に対応する家電製品を接続又はプラットフォーム上で家電製品メーカー等サードパーティが提供する家電連携のためのアドオン機能「Alexa Skills (スキル)」を有効化することで、対象機器を音声操作することができる。

なお、Google Home と同様に、Web ページ上で Alexa 対応スマートホームデバイスと位置付けられている製品を抽出対象とした（サードパーティが提供するスキルを通じて連携できる家電製品は抽出の対象外）²。

c. HOME Kit (Apple)

HomeKit とは、Apple 社が開発している IoT システムのサービス名及びソフトウェア名である。HomeKit に対応する家電製品等（HomeKit 対応アクセサリ）は、Apple デバイス上で操作することが可能となる。また、Google や Amazon と同様に、Apple 社が開発した AI アシスタントの「Siri」によって、スマートフォン又は Apple 社のスマートスピーカー「HomePod」を介した音声操作機能が提供されている。

また、Apple 社は HomeKit のフレームワークに対応するアクセサリに関して自らレビューと承認を行っている点が特徴として挙げられる。本調査においても、Apple 社によって HomeKit

¹ <https://assistant.google.com/explore/c/19/>

² <https://www.amazon.co.jp/b?ie=UTF8&node=5364379051>

対応アクセサリと承認された家電製品等を抽出の対象とした³。

d. LINE Clova (LINE)

LINE Clova とは、LINE 社が開発した AI アシスタントである。Google や Amazon、Apple と同様に AI アシスタントが搭載されたスマートスピーカーやワイヤレスステレオヘッドセット⁴など、Clova デバイスを介して家電製品を音声操作することを可能としている。

また、Clova デバイスの付属製品（外付け製品）として、「Clova Friends Dock」も展開している。「Clova Friends Dock」は赤外線リモコン機能を有しており、赤外線リモコンを通じて操作可能な家電製品であれば、Clova デバイスに対応した製品でなくても音声操作等、遠隔操作を行うことができる。

Clova で操作できる IoT サービスは LINE 社の Web ページ⁵から確認することができる。本調査においても、Clova Friends Dock を介して操作できる家電製品は抽出の対象外とし、Clova で操作できる IoT サービスとみなす製品等を抽出の対象とした。

e. The connected life (Microsoft)

The connected life とは、互換性のあるスマートフォンや Windows 10 デバイスを使用してスマートデバイスを操作することができる Microsoft 社が提供するスマートホームソリューションである⁶。Microsoft 社が開発し Windows 10 にも搭載されている AI アシスタント「Cortana」を介した音声操作機能も具備されている。

なお、Microsoft 社の Web ページでは IFTTT 社が提供する異なるソーシャルメディアやプラットフォームを連携させる Web サービスである「IFTTT (IF This Then That)」と連携可能であることも紹介されているが、抽出の対象外としている。

f. インテリジェントホーム (イツツ・コミュニケーションズ)

インテリジェントホームとは、イツツ・コミュニケーションズ社が提供する外出先から家電製品等、家の中を自由にコントロールすることができるサービスである⁷。カメラやセンサーを使った子供の帰宅確認や高齢者やペットの見守り、鍵の施錠確認や照明のオンオフについて遠隔操作をすることを可能としている。

ii. 電機メーカーによる自社製品が相互に接続されたプラットフォーム

a. Rinnai IoT Service (リンナイ)

Rinnai IoT Service とは、リンナイ社が提供するスマートフォンアプリ「どこでもリンナイ

³ <https://www.apple.com/jp/ios/home/>

⁴ <https://clova.line.me/device/>

⁵ <https://clova.line.me/clovahome/iot/>

⁶ <https://www.microsoft.com/en-us/store/b/connected-life>

⁷ <https://www.itscom.co.jp/service/intelligenthome/>

アプリ⁸」を通じてお風呂や床暖房の遠隔操作や光熱費の確認ができるサービスである。

b. コネクテッド家電（日立製作所）

日立製作所（日立アプライアンス株式会社：現日立グローバルライフソリューションズ）はインターネットやスマートフォンとデータを送受信する機能を持つ家電製品「コネクテッド家電」を中心に、多様化する消費者ニーズに対応するプラットフォームを構築すると2018年2月1日の記者会見で宣言した⁹。

2020年2月現在、アップル社が運営するiPhoneやiPad向けのアプリケーションプラットフォームであるApp Storeにおいて、複数種類のアプリケーションが展開されている¹⁰。

c. パナソニックスマートアプリ（Panasonic）

パナソニックスマートアプリとは、Panasonic社が提供する家電製品に対応したスマートフォンアプリである。個人が家電製品の設定をカスタマイズできたり、家電の遠隔操作や使用状況（節電状況）の確認したりすることなどがアプリケーションを介して可能となる¹¹。

d. IoLIFE（東芝）

IoLIFEとは、東芝社の家電製品を遠隔操作や設定変更を行うことができるスマートフォンアプリである。2020年2月現在、エアコン、洗濯機、冷蔵庫の3製品に対応している¹²。

e. ME.App（三菱電機）

ME.Appとは、三菱電機社の家電製品を遠隔操作や設定変更を行うことができるスマートフォンアプリである。2020年2月現在、エアコン、炊飯器、掃除機、テレビ、調理機器に加え、HEMSに関するアプリケーションや電気自動車の車両認証アプリが展開されている¹³。

f. COCORO+（SHARP）

COCORO+とは、シャープ社のスマート家電向けサービスブランドである。あらゆるものを

⁸ https://rinnai.jp/app/remocon/mc302vc_a/

⁹ 日立アプライアンス株式会社 ニュースリリース「新宣伝キャンペーン「ハロー！ハピネス」を展開」（2018年2月1日）

<http://www.hitachi.co.jp/New/cnews/month/2018/02/0201.pdf>

¹⁰ <https://apps.apple.com/jp/developer/hitachi-appliances-inc/id533693913#see-all/i-iphone-ipad-apps>

¹¹ Panasonic Web ページ

<https://panasonic.jp/pss/ap.html>

¹² 東芝 Web ページ

<https://www.toshiba-lifestyle.co.jp/living/iolife/app/>

¹³ 三菱電機 Web ページ

<http://www.mitsubishielectric.co.jp/consumer/application/>

クラウドの人工知能と繋ぎ人に寄り添う存在に変えていくビジョン「AIoT」に基づくサービスとされている。2020年2月現在、キッチン家電、空調家電、オーディオなど生活家電に対して展開されている。¹⁴

g. MANOMA (ソニー)

MANOMA とは、IoT デバイスとスマートフォンを連動させ、顧客の暮らしに安全と便利を提供するスマートホームサービスである。主に家族・ペットの見守り、防犯、家電の遠隔操作を実施することができる¹⁵。

h. Home connect (B/S/H)

Home connect とは、欧州最大の家電メーカーである B/S/H 社が提供するスマートホームプラットフォームである¹⁶。

i. Smart Devices (Xiaomi)

中国の総合家電メーカーである Xiaomi 社も各種 Smart Device を展開している¹⁷。また、Xiaomi 社は製品のユーザや開発者が情報交換など交流することができるコミュニティである「Xiaomi Global Community」も運営している。

j. Smart Thing (Samsung)

韓国の家電メーカーである Samsung 社も、「Smart Thing」と名されたスマートホームソリューションを展開している。対象製品は Samsung 社 Web ページから確認できる¹⁸。

k. ThinQ (LG エレクトロニクス)

韓国の総合家電、情報通信メーカーである LG エレクトロニクス社は「ThinQ」とのブランドで LG エレクトロニクス社の家電製品の主要機能を制御可能なアプリケーションを提供している¹⁹。また、Google Home や Alexa などスマートスピーカーとの互換性も確保している。

¹⁴ SHARP Web ページ

<https://cocoroplus.jp.sharp/products/>

¹⁵ ソニー Web ページ

<https://manoma.jp/service/>

¹⁶ B/S/H Web サイト

<https://www.home-connect.com/global/connected-household>

¹⁷ Xiaomi Web サイト

<https://xiaomi-mi.com/mi-smart-home/>

¹⁸ Samsung Web ページ

<https://www.smarthings.com/products>

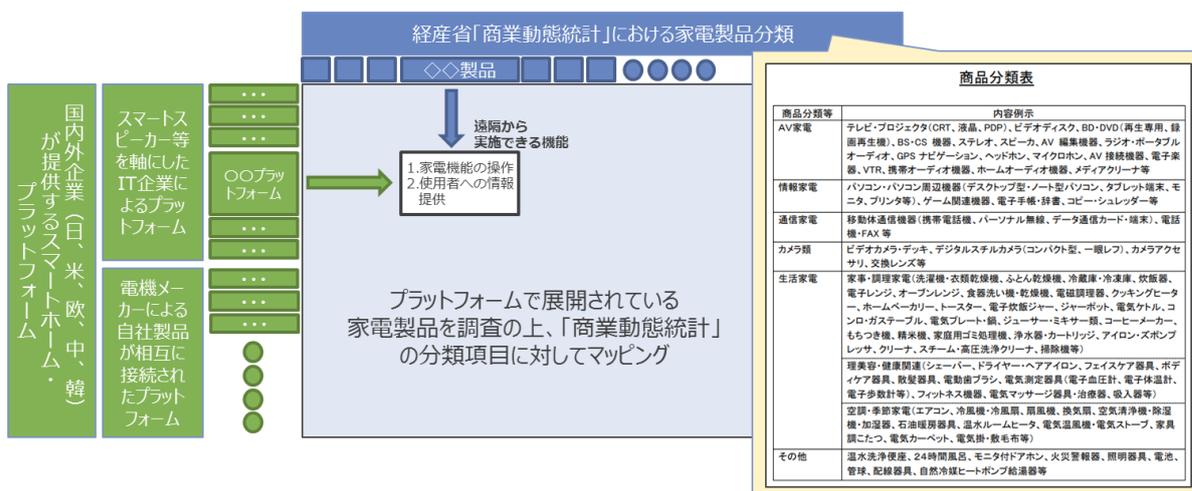
¹⁹ LG エレクトロニクス Web ページ

<https://www.lg.com/us/discover/thinq>

(イ) スマート化されている家電製品の抽出

2.1(1)1(ア)において調査したスマート家電を、経済産業省「商業動態統計²⁰」の商品分類表(家電大型専門店)をベースにマッピングした(図表2)。マッピングに際しては、各製品の遠隔から実施できる機能を「対象家電の機能の操作」「使用者への情報提供」の二段階に分けた。

図表2 家電のスマート化に関する現状調査におけるマッピングイメージ



(ウ) 調査結果

調査の結果、殆どの家電製品が IoT 化されてきていることが分かった。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・加湿器などは IoT 化が進んでいる家電であると考えられる。

更に、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・加湿器に関しては遠隔操作でできる機能に関して別途調査を行った(図表3)。電気用品安全法では、利用者が遠隔操作で機器を OFF→ON する行為を規制しているが、利用者が機器を ON→OFF する行為もユーザーズとして確実に存在すると考えられる。

²⁰ 経済産業省「商業動態統計」商品分類表(家電大型専門店)
<https://www.meti.go.jp/statistics/tyo/syoudou/result-4.html>

図表 3 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)	<ul style="list-style-type: none"> 運転モード変更 温度設定変更 掃除等変更 	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> レシピ登録 献立提案 	—	—
その他		<ul style="list-style-type: none"> 高齢者見守り機能 (ドア開閉から安否を通知) 伝言機能 			

(2) 遠隔操作機構を有する電気用品等製品ごとのフェールセーフ機構 (物理的安全性) 及びソフトウェアによる安全制御 (機能安全) に関することの調査

IEC 60335-1 第 6 版の検討を通じ、国際的に認識が高まっている遠隔操作等に係る動向を調査するとともに、附属書 R と遠隔操作との関わりに変化が生じたかも合わせて確認を行った。

1) 電気用品安全法が求める『遠隔操作』の概要—法令上のスコープと規定の概要

『遠隔操作』は「見えない位置からの操作」が前提としてあることに加え、遠隔操作機構を有するものに対する要求事項は電源回路の閉路 (機器を off から on にする行為) に対してのみ規定している。

電気用品安全法では、遠隔操作機構を有する機器に、遠隔操作によるリスク低減対策や通信途絶による安全状態の維持等を要求する。

図表 4 電気用品安全法の法令における遠隔操作に関する規定

電気用品安全法の法令における遠隔操作に関する規定	
<ul style="list-style-type: none"> 電気用品安全法の技術基準省令のうち、『遠隔操作』に直接的に係る条文は第十四条（使用方法を考慮した安全設計） 	<p>(使用方法を考慮した安全設計)</p> <p>第十四条 電気用品は、当該電気用品に通常想定される無監視状態での運転においても、人体に危害を及ぼし、又は物件に損傷を与えるおそれがないように設計され、及び必要に応じて適切な表示をされているものとする。</p>
<ul style="list-style-type: none"> また、電気用品の近くに操作者がいない状態に加えて、電気用品の近くに操作者ではない人がいる状態など、電気用品の近くにいる人に対する危害防止に関する技術基準としては、第十五条（指導、再始動及び停止による危害の防止）、操作者の位置に関係なく遠隔操作機構を有する電気用品においては、電気的、時期的または電磁氣的妨害による誤動作によって安全機能に障害があつてはならないことを求める技術基準としては、第十七条（電磁的妨害に対する耐性） IEC 60335-1における定義^{※1}と同等に『遠隔操作』の前提には「見えない位置からの操作」であることが挙げられている 	
遠隔操作機構を有するものに対する要求事項	
<ul style="list-style-type: none"> 技術基準解釈通達における『遠隔操作』に関する要求事項（解釈別表第八1（2）ロ）では、「遠隔操作に伴う危険源がない又はリスク低減策を講じることにより、遠隔操作に伴う危険源がない機器と評価されるもの」、「通信回線が故障等により途絶しても遠隔操作される機器は安全状態を維持し、通信回線に復旧の見込みがない場合は遠隔操作される機器の安全機能により安全な状態が確保できること」等が定められている。 	

※1：電気通信、音響制御、電力線通信などの手段を用いて、電気用品の見えない位置から発するコマンドによって、電気用品を制御する動作

さらに、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）では、遠隔操作において配慮すべき危険源を一覧化するとともに、考慮すべきリスクとリスク低減策を例示している（図表5）²¹。

図表 5 遠隔操作において配慮すべき危険源・リスク及びリスク低減策の例示

1. 表 6：電気用品を遠隔操作する際に配慮すべき危険源
2. 表 7：遠隔操作に対する考慮すべきリスクの例
3. 表 8：遠隔操作におけるリスク低減策の例

2) IEC60335-1における『遠隔操作』の範囲と主な機器の例

我が国の電気用品安全法が参考にできる、遠隔操作に関する IEC の考え方について調査した。

JIS C 9335-1 (<https://kikakurui.com/c9/C9335-1-2014-01.html>) の 22.49 では、「遠隔操作の場合、運転持続時間を設定しない限り、機器が始動できないようにしなければならない。ただし、機器がサイクルの最後で自動的に電源を遮断する場合、又は危険を生じさせることなく連続的に運転することができる場合を除く。」と規定している。

²¹ 出典：「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 電気用品調査委員会）
http://www.eam-rc.jp/pdf/result/remote_control_BP8_report20191118.pdf

図表 6 JIS C 9335-1 の 22.49 が定める『遠隔操作』の範囲と該当する機器の例

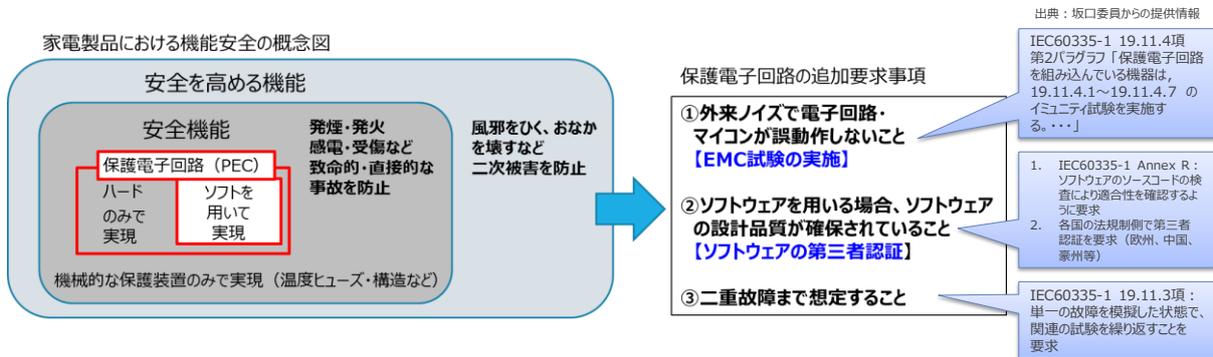
種別	機器が有している機能	該当する機器例
「遠隔操作のための基本機能」として整理	運転持続時間を設定しなければ機器が始動できないようになっている機能	・ オープン
「基本機能を代替できる機能」として整理	サイクルの最後で自動的に電源を遮断する機能	・ 洗濯機 ・ 食洗器
	危険 ^(注) を生じさせることなしに連続的に運転できる機能	・ ファン ・ 貯湯式温水器 ・ エアコン ・ 冷蔵庫

(注) IEC60335-1では、2次被害等は、危険の定義に含まれていない

3) 機能安全の概念と、保護電子回路への追加要求事項

IEC 60335-1 では、電気用品等の安全保護方策として、機械的な保護装置以外に保護電子回路による電氣的な安全機能が認められている。保護電子回路にソフトウェアを用いる場合は、①EMC 試験の実施、②ソフトウェアの第三者認証、③二重故障まで想定することの3つが追加で要求されている。機能安全の概念は、規格によってその範囲が異なることがあるが、この報告書では、ソフトウェアを用いた安全機能を（家電機器の）機能安全と称している。

図表 7 家電製品における機能安全の概念図



出典：WG 資料

さらに、IEC TC61 MT23 で議論されている IEC60335-1 の改訂作業に基づくと、通信ソフトウェアの分離を新たに求めていく方向である。

図表 8 IEC で議論されている通信回線に関する要求事項の概要

項目番号	要求事項の概要
22.XX	Public networkを経由したRemote communicationが家電製品の 安全担保に影響を与えないこと
XY.22.101	Public networkの通信ソフトウェアは 他の部分と分離 されていること。

上記を踏まえると、遠隔操作機構を有する機器について、今後、通信回線と安全機能の分離を検討することは自然な流れと言える。

安全機能については、利用者が一切変更できないことを考慮すると、遠隔操作による意図せざる改変からは厳に防御する必要がある。

(3) IoT 化等が考えられる電気用品等製品ごとにセキュリティ対策を組み込む場合のフェールセーフ機構（物理的安全性）及び機能安全に与える影響に関することの調査

IoT 化等が考えられる電気用品等製品ごとにセキュリティ対策を組み込む場合のフェールセーフ機構（物理的安全性）及び機能安全に与える影響について、国内外の状況の整理を行った。

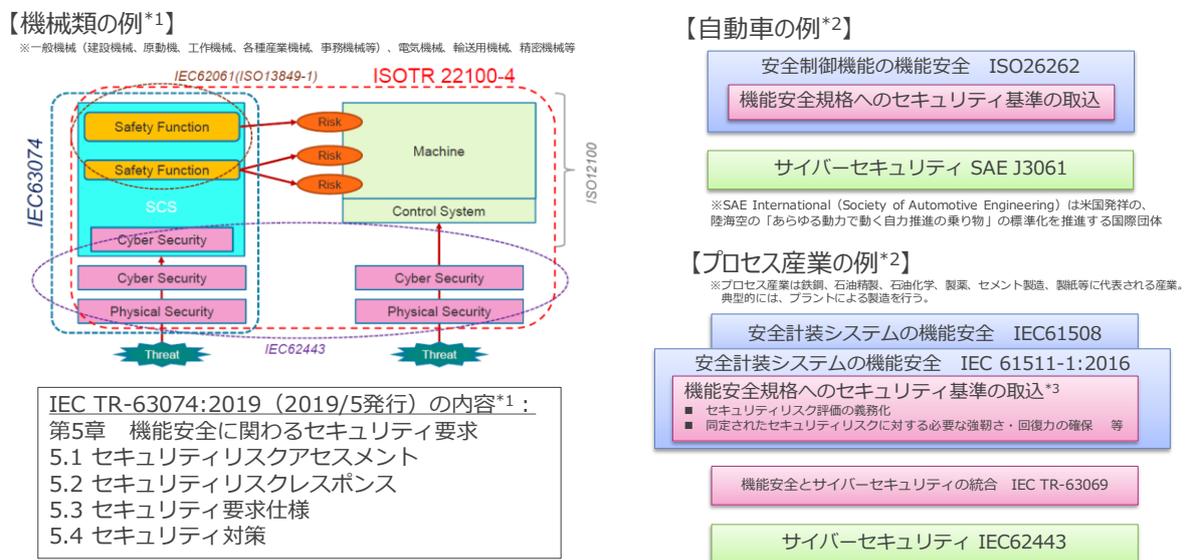
1) 機能安全を実現する安全制御システムのセキュリティに関する国際標準化

機械、自動車、プロセス制御等の分野においては、機能安全を実現する安全制御システムのセキュリティについての国際標準化が進展している。

一方、電気用品等製品では、IEC60335-1 附属書 R がこの役割を果たすと考えられている。

IEC60730（家電等の機能安全規格）に対してセキュリティ基準を取り込む動きや、機能安全とサイバーセキュリティを統合する国際基準を作る動きは、現時点では把握できていない。

図表 9 安全制御システムのセキュリティについての国際標準化動向

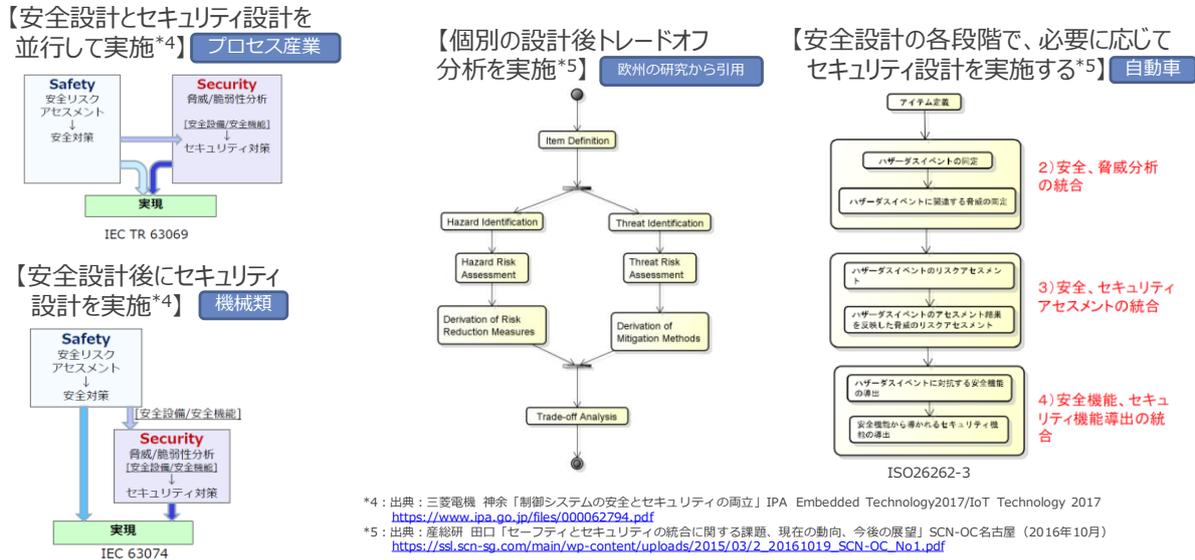


安全設計とセキュリティ設計をどのような手順で統合するべきかについては、IEC TR-63069:2019²²では、安全設計とセキュリティ設計を並列で実施する手法を取る（個別の設計後、トレ

²² Industrial-process measurement, control and automation - Framework for functional safety and security

ードオフ分析を行う手法もあり)。一方で、IEC TR-63074:2019²³では先に安全設計を実施し、その後セキュリティ設計を行う手法を取っている。また、ISO26262-3:2018²⁴では、安全設計の各段階で、必要に応じてセキュリティ設計を実施する方式を取っている。

図表 10 安全設計とセキュリティ設計の統合



2) 国際規格の最新動向に見る安全規格の進化

「安全機能の故障の回避・緩和の確認 (=機能安全)」に留まらず、「非故障 (性能限界、意図しない操作、AI の誤認識等) により安全が脅かされる事態 (=SOTIF : Safety of the intended functionality、意図された機能の安全性) への対処」を記述した新しい国際規格が登場しつつある。

SOTIF では、例えば自動運転が気象状況などで視認装置の限界を超えた場合や、自動運転中の運転者の意図しない操作、人に対する画像認識装置の誤認識などの事象に対処することで、安全がさらに向上する。このことから、SOTIF については安全機能との関わりで検討するよりも、むしろ通常機能の範疇で組み込まれる「安全を向上させる機能 (予防安全機能)」を改善するという切り口で検討していく方が有益であると考えられる。

製品安全 4 法対象製品では SOTIF は未導入であるため、過信により性能限界を超えて使用すること、遠隔操作が (目で確認しないため) 意図しない操作となること等が、安全を脅かす事態に繋がりにくことに留意していく必要がある。

²³ Safety of machinery - Security aspects related to functional safety of safety-related control systems

²⁴ Road vehicles -- Functional safety -- Part 3: Concept phase

図表 11 国際規格の最新動向



2.2. IoT 化等された製品に関するトラブル、事故の実態調査

(1) 公知文献の検索・収集

製品安全に関する各法が定める人の生命・身体に危害を与えうる製品に加えて、自動運転車・その他の電動の移動手段、医療・ヘルスケア機器等を調査対象として、製品が IoT 化等された環境で受けた影響によるトラブル・事故（インターネット等外部からの影響が大きいものを主）並びに脆弱性・ヒヤリハットの事例を公知文献から検索の上、収集を行った。

1) 検索・収集の方法

国内外で発生したトラブル・事故事例（製品が IoT 化された環境で受けた影響によって生じたものであって、インターネット等外部からの影響が大きいもの）を公知文献から検索の上、収集を行った。

収集した事例の観点は以下のとおりである。

- ・ 製品安全に関する各法が定める人の生命・身体に危害を与えうる製品
- ・ 自動運転車・その他の電動の移動手段、医療・ヘルスケア機器等

検索する公知文献は、以下を確認した。

図表 12 確認した資料の例

N o	項目	調査先	URL
1	各府省・関連団体の事故事例データベース	経済産業省事故事例データベース	http://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/jikoboushi/database.html
2		NITE 製品事故 100 選	http://www.nite.go.jp/jiko/journal/index.html
3		NITE 事故情報・リコール情報データベース	https://www.nite.go.jp/jiko/jikojohou/index.html
4		事故情報 消費者庁	https://www.caa.go.jp/policies/policy/consumer_safety/child/project_006/
5		消防庁事故事例・事故統計資料	https://www.fdma.go.jp/relocation/neuter/topics/fieldList4_16/jiko_shiryo.html
6		移動支援ロボット ～ 交通用具(公道上) 交通事故統合データベース (ITARDA)	http://www.itarda.or.jp/
7		医療事故情報収集等事業(厚労省) 医療事故/ヒヤリ・ハット報告事例検索 ((公財)日本医療機能評価機構)	http://www.med-safe.jp/mpsearch/SearchReport.action
8		事故事例データバンク	http://www.kokusen.go.jp/jikojoho_db/
9		内閣サイバーセキュリティセンター (NISC)	https://www.nisc.go.jp/security-site/
10		サイバーセキュリティ戦略本部	https://www.nisc.go.jp/conference/cs/index.html
11		(一社)重要機器連携セキュリティ協議会 (CCDS) 重要生活機器の脅威事例集 Ver.1.2	https://www.ccds.or.jp/public/document/other/CCDS_CaseStudies_v1_2.pdf
12		重要生活機器の脅威事例集 2016 年度	https://www.ccds.or.jp/public/document/other/CCDS_CaseStudies_2016.pdf
13	海外政府における事故事例データベース	CONSUMER PRODUCTS SAFETY COMMISSION (CPSC) 全米傷害調査電子システム (National Electronic Injury Surveillance System)	https://www.cpsc.gov/Research-Statistics/Injury-Statistics

No	項目	調査先	URL
14		全米消費者苦情データベース	https://www.saferproducts.gov/Default.aspx
15		欧州委員会障害データベース IDB: Injury Data Base	https://ec.europa.eu/health/indicators_data/idb_en
16		サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) レポート	https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01
17	メーカーの事故事例発表情報	事故事例インデックス (Panasonic)	https://www.panasonic.com/jp/support/kaden/case.html
18	報道発表資料	東京消防庁	https://www.tfd.metro.tokyo.lg.jp/
19	IT 系専門	Itmedia	https://www.itmedia.co.jp/
20	インターネット	インターネットウォッチ	https://internet.watch.impress.co.jp/
21	ネットメディア	WIRED	https://wired.jp/
22	ア	ITPro	https://xtech.nikkei.com/it/atcl/column/14/090100053/
23	海外インターネットメディア	THE VERGE	https://www.theverge.com/

2) 検索・収集の結果

ここでは、検索・収集を実施した結果、国内外で発生したトラブル・事故事例（製品が IoT 化された環境で受けた影響によって生じたものであって、インターネット等外部からの影響が大きいもの）をとりあげる。

(ア) 家電製品×ロボット掃除機による火災事故

i. トラブル、事故の概要

2018 年度、東京都消防庁管内においてロボット掃除機が電気ストーブを押し動かして、可燃物に接触して燃える火災が 2 件発生した。

図表 13 家電製品×ロボットによる火災事故 事例 1

日時	2018 年 12 月
被害状況	共同住宅の住戸内、家具等燃損。死傷者なし。
トラブル、事故の状況	出火した住戸の住人が 1 階にいたところ、自動火災報知設備が鳴動したので 2 階のリビングに戻ると、電気ストーブとソファが接触して出火していたもの。出火前は 2 階で電気ストーブがソファから 50 cm の位置に置かれており、室内はロボット掃除機が運転状態であった。

図表 14 家電製品×ロボットによる火災事故 事例 2

日時	2019 年 2 月
被害状況	共同住宅の住戸 1 室 20 m ² 焼損。死傷者なし。
トラブル、事故の状況	近隣の社員が出火建物の窓から煙が出ているのに気付いた。出火した住戸の住人は外出中であり、机の下に置いていた電気ストーブの位置が変わって出火したもの。ロボット掃除機はタイマー設定がされていた。

ii. **トラブル、事故等に至った主な原因**

消費者がロボット掃除機の特長や危険性を十分に理解できていないことが主な原因であると考えられる。東京消防庁の出火危険性の確認実験からは、電気ストーブがある室内でロボット掃除機を使用した場合、次の危険性があることが報告された。

- ・電気ストーブが押されて移動する。
- ・電気ストーブが押され、移動しながら向きを変える。
- ・電気ストーブのコードに絡まり、思わぬ方向にストーブが動く。

iii. **設計段階におけるフェールセーフ機構（物理的安全性）とソフトウェアによる安全制御（機能安全）に関する脆弱性の顕在化等、設計段階当初に想定してなかった事案との因果関係**
公知情報なし

iv. **当該トラブル、事故に対する責任の所在（IoT 化等された電気用品等製品の製造事業者とインターネット等外部からクラウドサービスを提供する事業者との関係を含む）**

公知情報なし

v. **事故後の当該製品への対応（特に製造事業者、輸入事業者、クラウドサービス提供事業者、消費者との関係）**

事故後、東京消防庁によって出火危険性の確認実験が行われた後に、消費者に対する注意喚起が行われた²⁵。注意喚起では、同様の火災事故を防ぐための方策として下記が示された。

・取扱説明書等に記載されている使用条件や注意点をよく読み、危険な状態とならないように注意すること

- ・ロボット掃除機を自動運転する場合は、電気ストーブのコードを抜くこと

(イ) **通行中における自動車の FOTA（Firmware Over-The-Air）による立ち往生**

i. **トラブル、事故の概要**

図表 15 自動車のトラブル、事故の概要

日時	2019年2月
被害状況	交通渋滞。死傷者なし。
トラブル、事故の状況	South China Morning Post の報道によると、中国北京で中国の電気自動車メーカーである上海蔚来汽車（NIO）社製の電気自動車が長安街（天安門などがある北京の要所）の路上で1時間ほど立ち往生したことで渋滞が発生した。立ち往生中、自動車のドアはロックされてしまい運転者は自動車の中に閉じ込められてしまった。

²⁵ 東京消防庁報道発表資料 平成 31 年 2 月 8 日

<https://www.tfd.metro.tokyo.lg.jp/hp-kouhouka/pdf/310208.pdf>

ii. **トラブル、事故等に至った主な原因**

試乗中の客が誤って車両のシステムアップデートを実行してしまったことにある。

iii. **設計段階におけるフェールセーフ機構（物理的安全性）とソフトウェアによる安全制御（機能安全）に関する脆弱性の顕在化等、設計段階当初に想定してなかった事案との因果関係**
通行中に車両のシステムアップデートが実施されることを設計段階当初に想定できていないことと、当該事象が発生したとは因果関係があるとみなすことができる。

iv. **当該トラブル、事故に対する責任の所在（IoT 化等された電気用品等製品の製造事業者とインターネット等外部からクラウドサービスを提供する事業者との関係を含む）**

ユーザの操作によって引き起こされた事象であるが、偶発的な誤操作を想定したシステム設計になっていないため、責任の所在は自動車メーカーの NIO にあると考えられる。

v. **事故後の当該製品への対応（特に製造事業者、輸入事業者、クラウドサービス提供事業者、消費者との関係）**

NIO は中国ミニブログサイトの Weibo 上において、当該事象に対する公式声明を出した²⁶。公式声明では、自社製品が FOTA によって公道上立ち往生を引き起こした事実関係を認めた上で、ユーザの偶発的な誤動作によって FOTA が実行されてしまったこと、アップデートの所要時間は事前にユーザに通知されていたこと、アップデートにおいては駐車場など適切な場所で実行することが適切な操作条件であることについて述べられた。

また、アップデートに際しての内容確認や実行に関するロジックを見直す方針が示された。

(ウ) **医療機器等における脆弱性**

i. **トラブル、事故の概要**

図表 16 心臓ペースメーカーの脆弱性に関する概要

日時	2019年3月
被害状況	心臓除細動器で使われる通信プロトコルに脆弱性
トラブル、事故の状況	2019年3月、米国土安全保障省(DHS)は、Medtronic社の心臓ペースメーカー関連製品20種が短距離からのハッキングに脆弱だと警告した。

ii. **トラブル、事故等に至った主な原因**

DHSによれば、ハッキングされる可能性のある製品の多くは埋め込み型心臓除細動器で、残

²⁶ <https://www.theverge.com/2019/1/31/18205774/nio-ota-update-traffic-china-es8>

りは家庭のベッド脇に置く除細動器モニタと、医師が使用するプログラミング用コンピュータであるという。脆弱性が悪用された場合、影響を受ける製品の通信が干渉され機能に影響したり、送信された機密データにアクセスされたりするおそれがあると、DHS の勧告に記載されている²⁷。

iii. 設計段階におけるフェールセーフ機構（物理的安全性）とソフトウェアによる安全制御（機能安全）に関する脆弱性の顕在化等、設計段階当初に想定してなかった事案との因果関係
この脆弱性は、最大 75 万台の機器に影響を及ぼす可能性がある。DHS の勧告によると、Medtronic 社が除細動器に採用している独自の無線通信プロトコル「Conexus」には認証の仕組みが備わっておらず、暗号化も実装されていなかった。

iv. 当該トラブル、事故に対する責任の所在（IoT 化等された電気用品等製品の製造事業者とインターネット等外部からクラウドサービスを提供する事業者との関係を含む）

Medtronic 社は電子メールの声明で、これらの問題はペースメーカーや埋め込み型心臓モニタなどの機器に影響していないと発表。また、これらの問題に関連するサイバー攻撃やプライバシー侵害、患者への危害は確認されていないとしている。

v. 事故後の当該製品への対応（特に製造事業者、輸入事業者、クラウドサービス提供事業者、消費者との関係）

Medtronic 社は、無線通信の安全性を高めるために、一連のソフトウェアアップデートを開発した。まず、移植心臓デバイスモデルのサブセット用の緩和パッチのアップデート後、ユーザに追加の防御手段を講じることを推奨している。

なお、医療機器等の事故調査に関しては、「医療事故／ヒヤリ・ハット報告事例検索」といった事事故例データベースや公知情報を広く確認したが、ほとんど重大事故等は確認されなかった。これは、医療機器等はインターネット等の外部影響に繋げるより、病院内部のオンプレミス環境による機器連携が多いからであると想定される。

なお、介護ベッド、ベビーカー等の一部でインターネット接続を行っている機器もあるが、重大事故は見つからなかった。

(2) 有識者へのヒアリング調査

調査目的に資する家電以外の製品におけるトラブル、事故の現状や、トラブル、事故に対する責任分解の明確化について、クラウド事業者側からの先進的な取り組み等について、国内有識者に意見を聴取した。

²⁷ CISA 「ICS Medical Advisory (ICSMA-19-080-01)」
<https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01>

さまざまなメーカーによって製造された多様なモノとモノ、モノとサービス、サービスとサービスが IoT 化によりつながるようになると、事故やトラブルが発生した場合の責任分担が不明確になりがちである。

この点について、多様なモノやサービスをすばやく安全につなげる『相互接続 IoT プラットフォーム』をサービス提供し、リスクシナリオに基づいて IoT 由来の脅威を多重かつ継続的に防護できる仕組みを組み込むクラウド事業者が登場している。

例えば BizMobile 株式会社では、機器を監視・操作するアプリケーションはクラウド上が前提であり、プラットフォームの中核となる IoT ハブもクラウドであり、ホワイトリストに登録され、証明書認証されたアプリケーション/ドライバとしか接続させない（閉域網の役割）。相互接続を許可するアプリケーションと機器/機器と機器の組合せもホワイトリストで管理を行っている。さらに FaaS（Function as a Service）による IoT ハブの高信頼化を行っている。

機器は IoT ハブに機器メーカーのドライバ経由で直結するか、機器メーカーのクラウド・ドライバ経由（例：スマートスピーカ）で接続するが、典型的には、IoT ルータとしてスマートフォンを用い、その上にドライバを搭載する。IoT ハブとの接続は、SIM、eSIM、WiFi、イーサネットで多重化可能であり、MDM で管理を行う。その上で、繋がるアプリ・機器及びその用途（利用・保守等）により、メーカーのドライバが提供機能を制限する。（例：他社機器からの接続の場合、機器停止/停止確認のコマンドしか提供しない等）

関所²⁸とドライバはアプリケーションと機器のメーカーの裁量と責任で提供するため、責任分担が明確であり、クラウド連携と安全確保のサービス事例として参考になる取り組みであると考えられる。

(3) 調査結果のまとめ

各種データベースでは、国内外ヒアリングにおいても、IoT 化に伴うトラブルはもちろんのこと人に危害を及ぼす脆弱性は今のところ多くは見つからなかった。

本年度の欧州ヒアリング時にも確認したが、電気用品等に限って見れば、サイバー攻撃が人に危害を及ぼしうる脆弱性やインシデントの事例を見たことがないという見解で一致している。

各国・地域とも、電気用品等の安全設計の現状を考えると、サイバー攻撃が人に危害を及ぼしうる脆弱性やインシデントの発生は考えにくいとらえているものと考えられる。

この現状を踏まえると、電気用品等のサイバー攻撃対策を考えるにあたり、以下を行うことが重要であると言える。

- ・ セーフティに関する部分は、既存の製品安全設計を徹底
- ・ 遠隔操作に対する安全設計（リスクアセスメント、その他の技術基準の順守）については、サイバー攻撃対策としても有効に働くので、確実に実施
- ・ 電気用品等の高度化や変革により、機能安全の組込等、製品安全設計の実態が変化

²⁸ IoT 由来の脅威を回避する仕組み

していく可能性があるため、国内外の最新の動きにも配慮

- 多様なモノとモノ、モノとサービス、サービスとサービスをすばやく安全につなげる『相互接続 IoT プラットフォーム』をサービス提供し、IoT 由来の脅威を多重かつ継続的に防護できる仕組みを組み込んでいるクラウド事業者も登場してきている。責任分解を明確にするという点で、引き続き今後の動きを注視する。

2.3. IoT 化等された若しくは IoT 化等が考えられる電気用品等製品の安全に関する海外政府・産業界等の動向調査

(1) 文献調査

1) 我が国及び諸外国の「IoT 製品の安全・セキュリティ」に係る取組

我が国及び諸外国の「IoT 製品の安全・セキュリティ・製造物責任」に係る取組について調査したところ、英国では、消費者 IoT 製品のセキュリティラベル義務化に積極的であり、法案を検討中である。

また、強靭さ・回復力の向上による遠隔操作時の安全確保については、英国をフロントランナーとして、今後欧州全体にその考え方が浸透する方向である。

電気用品調査委員会「遠隔操作に関する報告書等の見直しについて中間報告書」（2018 年 11 月）によると、IEC は、製品の「遠隔操作」に加えて、「不正アクセス及び通信異常」に対しても、安全状態の確保を要求する変更を検討中である。

以下に、今年度新たに把握した動きの概観を整理した。

図表 17 我が国及び諸外国の「IoT 製品の安全・セキュリティ・製造物責任に係る取組」の俯瞰

凡例：■製品/サービス全般 ■コンシューマプロダクトに特化 赤字は最新動向

項目	日本	国際標準化機関	米国	欧州	中国
IoT製品の遠隔操作の安全	国等の行政 電気用品安全法技術基準 解釈別表第四、第八			英国政府「消費者向けIoT製品のセキュリティに関する行動規範」 ETSI TS 103 645 v1.1.1 (Cyber Security for IoT)	CCC認証制度 スマート家電一般技術基準 スマートホーム自動制御設備一般技術要求 IoT家電第三者認証（コンフォーマンステスト）規範 IoT家電システムアーキテクチャ及びアプリケーションモデル
	民間 電気用品安全法技術基準の解釈別表第八に係る遠隔操作機構に関するSマーク認証の運用基準	IEC60335-1改定検討 <small>【安全で信頼性の高い自動電子制御（家電向け機能安全）の基盤】</small> IEC 60730-1 IEC 60730-2-X	UL 60730-1 UL 60730-1A UL 60730-2-X		
サイバーセキュリティ	国等の行政 サイバー・フィジカル・セキュリティ対策フレームワークの検討 総務省がIoT機器にセキュリティ認証マークを付与する機器認証制度を検討中		カリフォルニア州 IoTセキュリティ法	ENISA 「EU全体のサイバーセキュリティ認証フレームワーク」検討 英国政府「消費者向けIoT製品のセキュリティに関する行動規範」 ETSI TS 103 645 v1.1.1	インターネット安全法 (IoT製品特化ではない)
	民間 IoTセキュリティガイドライン (IoT推進コンソーシアム) 重要生活機器連携セキュリティ要件ガイドライン改訂	IEC60335-1改定検討*	UL 2900-1 UL 2900-2-X 照明製品に対する規格を検討中 UL CAP認証 UL 5500 <small>ULはWiFi接続用ボードと製品制御用ボードの分離を推奨（高リスクの製品種別の場合）</small>		
製造物責任	製造物責任法		製造物責任法	ECの製造物責任指令の見直し検討（概念の再整理）	製品品質法、消費者権益保護法、権利侵害責任法、民法通則、反不当競争法

図表 18 今年度新たに把握した動きの外観

視点	欧州の新たな動向	米国の新たな動向	(参考) 我が国における新しい動き ²⁹
新たな動向	<ul style="list-style-type: none"> ■ 英国 DCMS の「消費者向け IoT 製品のセキュリティに関する行動規範」に基づくラベリングについての新法案³⁰ ■ ETSI³¹の「Cyber Security for Consumer Internet of Things」³² 	<p>認証・ラベリングについては、今の所、特筆すべきものが新たに見つっていない</p>	<p>業界の自主活動を含めた自己適合宣言・認証等の確認の在り方等の検討を開始（特に高いセキュリティを求める機器に対する要件等を検討）</p>
(参考) 昨年度報告済みの動き	<ul style="list-style-type: none"> ■ 英国 DCMS 「消費者向け IoT 製品のセキュリティに関する行動規範」 	<ul style="list-style-type: none"> ■ CTIA による IoT セキュリティ認証 ■ UL CAP (IoT のサイバーセキュリティ認証プログラム) 	-
(参考) 消費者 IoT 製品に特化しない新たな動向	<ul style="list-style-type: none"> ■ ETSI の技術基準・試験方法に基づく「IoT 製品のための標準化されたサイバーセキュリティ認証フレームワーク」についての研究³³ ■ EU サイバーセキュリティ認証フレームワーク (2019 年 6 月) ■ 英国国家サイバーセキュリティセンター (NCSC) の CAPS (政府調達品の認証)³⁴ ■ TUV ラインランドの OT サイバーセキュリティ認証 	<p>認証・ラベリングについては、今の所、特筆すべきものが新たに見つっていない</p>	-

²⁹ 産業サイバーセキュリティ研究会 WG1 分野別 SWG 『第 2 層』TF 経済産業省サイバーセキュリティ課 『第 2 層』TF 資料 (2019 年 8 月)

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/001_04_00.pdf

³⁰ 英国政府 HP, “Consultation on regulatory proposals on consumer IoT security”, 5/2019

<https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>

³¹ The European Telecommunications Standards Institute (欧州電気通信標準化機構)

³² ETSI TS 103 645 v1.1.1 (2/2019)

https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

³³ Sara N. Matheu-Garcia et al, “Towards a Standardized Cybersecurity Certification Framework for the IoT”, Joint collaboration of H2020 ARMOUR project and University of Murcia

https://www.armour-project.eu/wp-content/uploads/2018/01/white_paper_ARMOUR-IoT-Certification.pdf

³⁴ 英国国家サイバーセキュリティセンター (NCSC) HP, “CAP Assisted Products”

<https://www.ncsc.gov.uk/information/products-cesg-assisted-products-service>

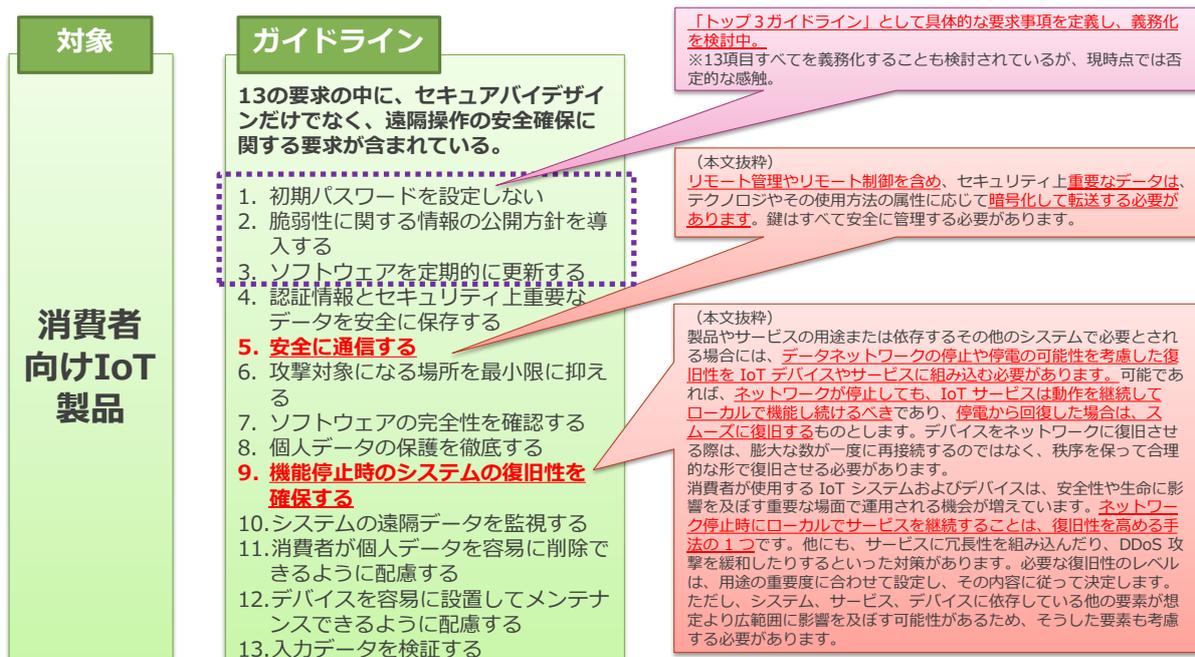
視点	欧州の新たな動向	米国の新たな動向	(参考) 我が国における新しい動き
消費者 IoT 製品セキュリティの認証・ラベリングの義務化	<ul style="list-style-type: none"> ■ 英国 DCMS は自己確認によるラベリング義務化を前向きに検討中。 ■ 大局的には、EU サイバーセキュリティ認証フレームワークにおいて定期的に認証義務化の必要性を見直すことになっており、欧州ではネット接続デバイスに対する認証と表示の義務化が広がるものと予想される。但し、リスクが高くないものについては自己確認で、第三者認証までは求めない方向。 ■ IoT 製品に特化した EU 全体の動きはまだ見えてこない（研究段階）。 	一般的傾向として、米国は国による義務化には消極的な立場である	現時点で方向性は未定
消費者 IoT 製品の安全・セキュリティの体系的な設計・実装等	<ul style="list-style-type: none"> ■ ラベリング義務化の前提となる「順守が義務化される要求事項」の中に、強靭さ・回復力向上による遠隔操作時の安全確保は入らない見込み（つまり、確認は任意）。 ■ ETSI は、EU 全体の視野で、消費者 IoT 製品に対し、強靭さ・回復力向上による遠隔操作時の安全確保の必要性を、義務のない任意のガイドラインとして示した。 	UL 規格において、製品安全と製品セキュリティは別々の標準として構成されている。遠隔からの操作の安全基準は、基本的に製品安全側の規格に含まれる。	サイバーリスクの安全への影響の増大への対応について検討を開始（安全も考慮に入れたセキュリティ対策等について検討）

2) 英国 DCMS 「消費者向け IoT 製品のセキュリティに関する行動規範」(2018 年 10 月)

英国 DCMS は、2018 年 10 月に「消費者向け IoT 製品のセキュリティに関する行動規範」を公表した。

セキュリティとセーフティに関する 13 の要求について、IoT 製品の設計をレビューし、その達成度をラベリングによって示すことを目指す新しい発想の制度である。我が国の電安法は遠隔操作する電気用品がネットワーク・通信側に異常があっても安全状態を維持するよう要求しているが、英国の行動規範は、ネットワーク・通信側の視点から捉えていると考えられる。

図表 19 英国 DCMS 「消費者向け IoT 製品のセキュリティに関する行動規範」の概要



検討の背景として、英国政府は、Secure by Design: Improving the cyber security of consumer internet of things に係るレポートを2018年3月7日に発行したことが挙げられる。

また、2018年10月、英国政府は、消費者IoTセキュリティの行動規範および消費者ラベリングスキームなどを公開している。行動規範の公開とともに、既存の13のガイドラインを世界中のIoTセキュリティとプライバシーに関する既存の標準、推奨事項と比較し、リンクするマッピングドキュメントも公開されている。

英国政府はNCSCおよび官民の専門家と相談し、行動規範のどの側面を最初に必須にするかを決定し「トップ3ガイドライン」として提示している。

具体的には以下の3点があげられている。

- IoTデバイスのパスワードはユニークである必要があり、工場設定時の設定にリセットできない
- IoTデバイスのメーカーは、脆弱性開示ポリシーの一部として公開連絡先を提供する必要がある
- IoTデバイスのメーカーは、製品がセキュリティ更新プログラムを受信する最短期間を明示的に述べる必要がある

今後数年間にわたって、脅威の状況と、より高度なセキュリティ対策を義務付ける必要性を業界と引き続き協議し、法律にセキュリティ条項を追加することの実用性を評価する予定である。

規制への段階的アプローチの一環として、行動規範からのさらなる要件を義務付けることも意図している。

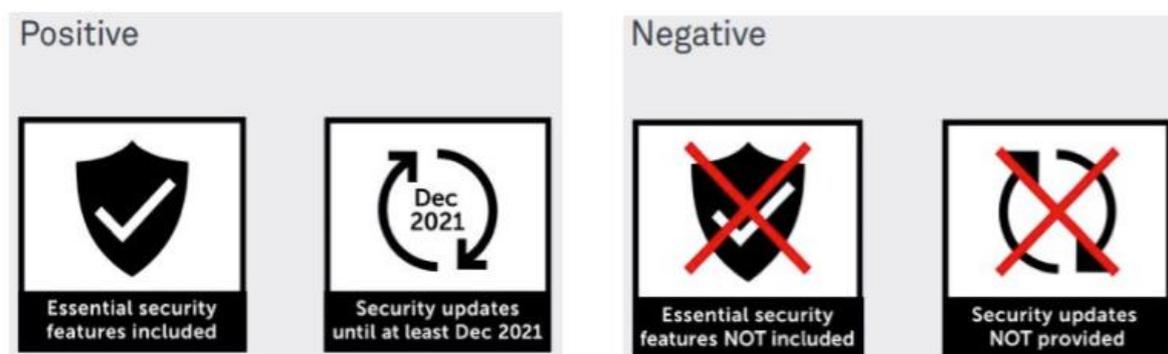
具体的には、消費者 IoT 製品のラベリングスキームを作成して消費者購入の決定を支援し、規範を遵守する製造業者に対する消費者の信頼を促進するオプションの検討がなされた。

ラベリングスキームは、NCSC、ビジネス・エネルギー・産業戦略部（BEIS）、内務省、および業界団体、製造業者、国際政府、小売業者、消費者団体、学者、IoT 専門家などの外部の利害関係者と協議して開発。

ラベルは、「トップ 3 ガイドライン」に基づき、「ポジティブラベル」の資格を得るには、メーカーはデバイスのパスワードが一意であり、工場出荷時の設定にリセットできないこと、および脆弱性開示ポリシーを実装していることを自ら証明する必要がある。さらに、メーカーは、デバイスがセキュリティ更新プログラムを受信する最短期間（月と年）を明示する必要がある。

英国政府は制度設計に関するフィードバックを歓迎しており、2019 年の後半に自主的なスキームとして開始する前に、ラベルの設計を変更することを検討したものである。

図表 20 英国における消費者 IoT 製品のラベル



出典：：英国政府 HP, “Consultation on regulatory proposals on consumer IoT security”, 5/2019 <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>

英国 DCMS は、以前は、業界が自主規制し、自主的に高い基準を採用し、組み込みのサイバーセキュリティ対策の基準に関するレベルを向上させることを優先していた。しかしながら、消費者 IoT 製品の普及が進展するにつれて、個人およびより広い経済に対するリスクも増加しているため、2018 年 10 月の「消費者 IoT 製品セキュリティの行動規範」、および ETSI の「技術仕様 103 645」に規定されているガイドラインの必要性を確認した。

このプロセスの一環として、英国 DCMS は、すべての消費者 IoT 製品が基本レベルのセキュリティを順守することを確実にするために実装すべき措置内容について、3つの案を設計し、業界および専門家と協議および意見招請を実施した。

提示された 3つの案の概要を以下に示す。

図表 21 消費者 IoT 製品のラベルリングに関する 3 つの案の概要

	小売業者	メーカー	備考
案 A	IoT セキュリティラベルのある消費者 IoT 製品のみを販売するように義務付け	<ul style="list-style-type: none"> • トップ 3 ガイドラインへの準拠を義務付け • ラベルの義務付けなし (ただし、セキュリティラベルにより上記を証明することを期待) 	社会的な影響、コスト等から英国政府はプラン A を推奨 。現在英国政府から公開されているラベリングスキームには、この案 A と同じ要件が含まれている
案 B	トップ 3 ガイドラインに準拠した消費者 IoT 製品のみを販売するよう義務付け	<ul style="list-style-type: none"> • トップ 3 ガイドラインへの準拠を義務付け • ラベルの義務付けなし (自社の消費者 IoT 製品が上記のトップ 3 ガイドラインのセキュリティ要件を満たしているかどうかを自己申告し、小売業者に通知 (契約に含めるなど)) 	
案 C	行動規範の 13 のガイドラインすべてに準拠していることを証明するラベル付きの消費者 IoT 製品のみを販売することを義務付け	<ul style="list-style-type: none"> • メーカーは既存の 13 のガイドラインすべてに準拠していること義務付け • ラベルの義務付けあり (上記を証明するラベルを、すべてを満足している製品パッケージに確実に実装することを義務付け) 	全てのメーカーが行動規範に定められている 13 の全てのガイドラインを順守することを義務付けることは、実用的でもコスト効率的でもないと評価されている

出典：：英国政府 HP, “Consultation on regulatory proposals on consumer IoT security”, 5/2019 <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>

英国 DCMS は、3 つの案について業界団体の協議を通じて受け取った回答の分析に基づき、どの措置を規制として立案するかを決定するとしていたが、コンサルテーションの結果が 2020 年 1 月に公表された³⁵。

パブリックコメントに対する英国 DCMS の回答の骨子は以下の通りである。

- 消費者向け IoT 製品のセキュリティについて最小限のベースライン要求 (トップ 3 ガイドライン) を義務化することについては賛成意見が多く、ステークホルダーの意見を聴取しながら規制の計画策定を進める方針。これに加えて、国際標準の場でも ETSI の欧州規格 (EN) として策定することに取り組んでいる。
- 一方で、セキュリティラベルの義務化を立法化することには反対意見が多かった。
- 製造事業者が小売業者に、「トップ 3 ガイドライン以外の 10 ガイドラインにも準拠しているか」に関する情報を提供できるかを検討する。
- 政府の狙いは、サプライチェーンが現実的に利用可能な、行動規範と一貫性を持つ業界主導の保証・認証スキームを推奨することであり、製造業者が従うべき特定の評価プロセス (セキュリティラベルの義務化等) を提唱するものではない。従って、

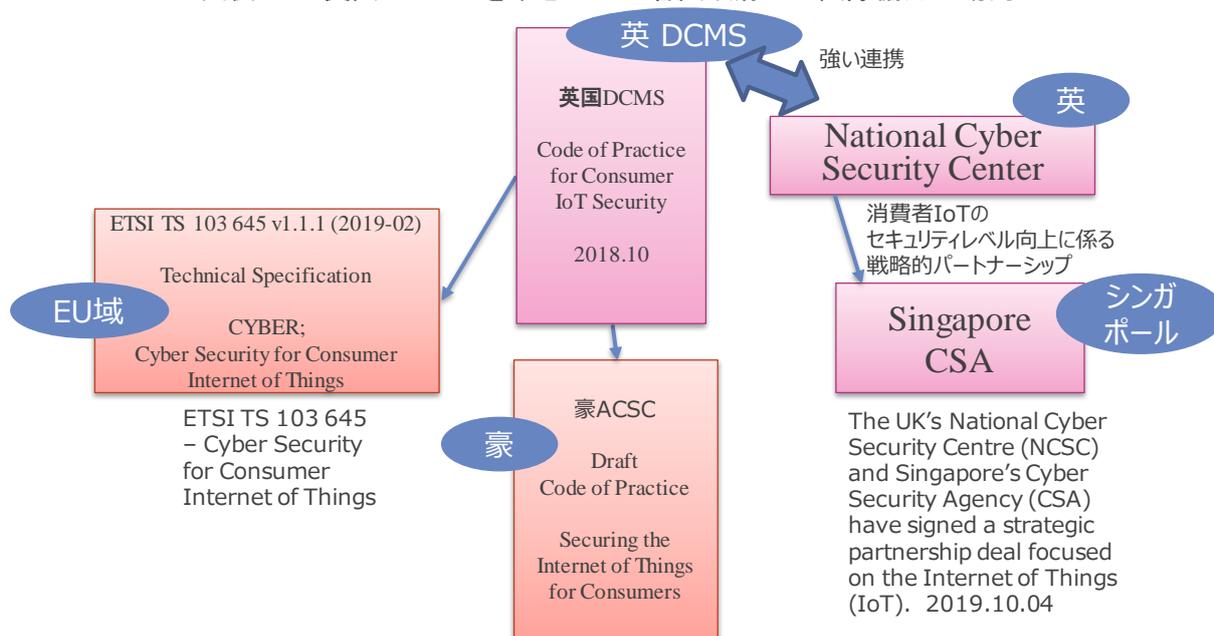
³⁵ Government response to the “Regulatory proposals for consumer Internet of Things (IoT) security” consultation (1/2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/862952/Government_response_to_consultation_Regulatory_proposals_for_consumer_IoT_security.pdf

特定の評価手法を義務付けることはしない。

- 英国の小売業者（または英国に販売する小売業者）が販売時点で消費者にセキュリティ情報を最もよく証明する方法について、さらに政策検討を進めて行く。これには、小売業者が販売時点（オンラインと店舗の両方）で消費者に情報を提供する責任を負う制度の検討を含む。この手法により、IoTデバイスの製造者、開発者、小売業者、消費者の間で、サイバーセキュリティに関する重要な情報が共有されることを保証したいと考えている。
- 2020年の下期に、規制導入の影響評価を公表したいと考えている。
- 行動規範は2年毎に見直す予定。将来的には、トップ3ガイドラインを超えて、さらなるセキュリティ要件を義務化するべく、段階的に取り組む予定である。

この他、英国 DCMS は、消費者 IoT 製品のセキュリティに関する国際協力に積極的に取り組んでいる。例えば、2019年7月29日には、オーストラリア、カナダ、ニュージーランド、米国と共同で閣僚声明に署名し、5カ国でIoTデバイスのセキュリティ強化のための政策を調整していくことを宣言した。また、IoTデバイスのセキュリティに関するシンガポールとのパートナーシップを強化する合意にも署名している。直近の英国 DCMS を中心とした国際動向について、下図に整理した。

図表 22 英国 DCMS を中心とした各国政府との国際協力の動向³⁶



³⁶ <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>
<https://www.iottechnews.com/news/2019/oct/04/uk-and-singapore-team-iot-security-consumer-products/>
<https://www.iottechnews.com/news/2019/oct/04/uk-and-singapore-team-iot-security-consumer-products/>

3) 欧州：ETSI Cyber Security for Consumer Internet of Things の動き³⁷

ETSI（欧州電気通信標準化機構）では、2019年2月に、ETSI TS 103 645 v1.1.1「消費者IoTのためのサイバーセキュリティ」を発行し、各種の既存のガイドを参照しつつ、一般消費者向けIoT家電の開発・製造者向けの、セキュリティ関連のガイドラインをまとめている。

対象としては、玩具・幼児見守り機器、テレビ・オーディオ等黒物家電、ウェアラブルヘルスマニタ、ホームセキュリティ（煙探知、ドアロック、アラーム等）、洗濯機・冷蔵庫等白物家電、スマートホーム等が含まれている。

このガイドラインの取りまとめにあたっては、英国 DCMS「消費者向けIoT製品のセキュリティに関する行動規範」の13のガイドラインを出発点とし、ETSI及びそれ以外（ISO/IEC、NIST、ENISA、GSMA等）の機関が公表した基準等も参考にしている。この中には、2019年時点では高度な要求と考えられる以下に示すガイドラインも含まれている。

- ・ 脆弱性報告の管理手段の実装（例：PSIRT機能の要求等）
- ・ ソフトウェアの完全性の確保
信頼できるルート権限を用いたセキュアブート
不正な変更を検知した際の、管理者や消費者へのアラートと緊急モードへの切り替え
- ・ 停止時の強靭さ・回復力向上
電力と通信停止を考慮
(上記の際)単体での動作と、瑕疵のない復旧
(輻輳を発生させない)規則正しいかつ安定的な再接続
- ・ 入力データの検証 等

「停止時の強靭さ・回復力向上に関するガイドライン」の書きぶり等に現れているように、ETSI TS 103 405 は、遠隔操作の安全を製品側の視点から見ており、我が国の電安法と共通している部分が多いと考えられる。これについては、ETSI へのヒアリング調査で実状を把握したので、後述する。

4) 欧州：ENISA の動き

EU全体を代表するセキュリティ専門機関であるENISAでは、2018年10月に「Draft opinion – Consumers and IoT Security (ENISA PSG WG on Consumer Perspective)³⁸」を公表し、消費者IoTのサイバーセキュリティの鍵として6項目（バイデザイン・バイデフォルト、認証、ライフサイクルのカバーとソフトウェアアップデート、接続はON/OFF可能等）を提言している。

³⁷ ETSI TS 103 645 v1.1.1 (2/2019) https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

³⁸ <https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/psg-meeting-october-2018-documentation/8-2018-10-22-draft-opinion-enisa-psg-working-group-on-consumer-perspective-v-2.pdf>

5) 欧州：IoT 製品のためのサイバーセキュリティ認証フレームワーク研究の動き

EU Horizon 2020 research and innovation programme³⁹の「ARMOUR project」⁴⁰とスペインのムルシア大学が共同で公表した「IoT 製品のための標準化されたサイバーセキュリティ認証フレームワーク」に関する研究成果によると、IoT 製品の認証はライフサイクルの各フェーズをカバーできる必要があり、新しい脅威・脆弱性が発見された際の認証の見直し（＝セキュリティラベルの再発行、ラベルの QR コード化）にも動的かつスケーラブルに対応できること（＝大量のデバイスに対応できる軽量の自動化された再認証プロセス）などが求められるとしている。

6) 米国：CPSC の動向

米国 CPSC は 2019 年 9 月 25 日に「Status report on the Internet of Things (IoT) and Consumer Product Safety⁴¹」を公表し、IoT 化された製品は、ソフトウェアのアップデートまたはカスタマイズ、インターネットへの接続、またはデータに問題があるため、不当に危害を受けるリスクがあると指摘している。また、製品のソフトウェア、または製品が接続されているデバイスを変更すると、安全機能が無効になる可能性があることを指摘している。ソフトウェアのアップデート終了後、IoT デバイスの使用期限を明確にすることにも言及している。

この文書において、CPSC は IoT デバイスが人に危害を与えうる危険源として以下の 4 点を指摘した。

- ・ 悪意のハッキング
- ・ 欠陥のあるサードパーティソフトウェア（オープンソースや委託先に開発させたソフトウェア等）
- ・ 製造事業者が提供した、欠陥のあるソフトウェアアップデート
- ・ 消費者による勝手な変更

さらに、CPSC は、IoT 化された消費者製品の安全性を、データセキュリティとプライバシーとの関係の中で定義する必要性について指摘している。

その他の今後の取組としては以下を報告している。

- ・ IoT 化された消費者製品の安全性に関する省庁間 WG を形成する。
- ・ NPTEC（Nevada National Security Site 内の Non Proliferation Test and

³⁹ 複数のパートナーによる研究・イノベーションプロジェクトを助成する EU の枠組み。世界で最大かつ最もオープンな研究助成プログラム。2014-2020 にかけて総額 800 億ユーロの資金を助成。

https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_intro_en_jp.pdf

⁴⁰ セキュアかつ信頼性が高い大規模 IoT のベンチマーク、フレームワーク、認証について研究する EU ホライゾン 2020 のプロジェクト。欧州 5 カ国（フランス、ギリシャ、ポルトガル、スペイン、イタリア）から 8 団体（EC を含む）が参加している。<https://www.armour-project.eu/>

⁴¹ https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf?6sv9HwTXKHrkdmAyAkQ0_TsKCkpl11R2

Evaluation Center) に IoT 化された製品の評価ラボを構築する。。

- ・ ASTM と連携し、IoT 化された消費者製品の安全性を確保するための任意の標準ガイドラインのドラフト作成に取り組んでいる。

7) 米国：NIST の動向

NIST は 2019 年 7 月に、IoT セキュリティリスクを緩和するためのベストプラクティスを示したガイダンスのドラフト (Draft NISTIR 8259: Core Cybersecurity Feature Baseline for Securable IoT Devices: A Startig point for IoT Device Manufacturers⁴²⁾) を公表した。

8) IEC60335-1 の改定作業の動向

日本における「電気用品安全法 技術基準 解釈別表第十二」や「JIS C 9335-1」をはじめ、各国の製品安全規格・法令に引用されている IEC 60335 シリーズは IEC TC61 委員会 (家庭用及びこれに類する電気機器の安全性) の MT23 (機能安全) で検討されている⁴³⁾。

地域/各国規格における IEC 規格の引用例を図表 23 に示す。

図表 23 地域/各国規格における IEC 規格の引用例

地域	法令	地域/各国規格	IEC 規格との関係
欧州	低電圧指令	EN 60335-1	IEC 60335-1 とほぼ同じ
		EN 378-1~4 (エアコンの個別要求)	IEC 60335-2-40 をベースに作成
米国	消費者製品安全法	UL 60335-1	IEC 60335-1 とほぼ同じ
日本	電気用品安全法	技術基準 解釈別表第八	無し
		技術基準 解釈別表第十二 JIS C 9335-1	IEC 60335-1 とほぼ同じ
中国	産品質量法	GB 4706.1	IEC 60335-1 とほぼ同じ
タイ	工業製品標準法	TIS 1375	IEC 60335-1 とほぼ同じ

出典：WG 資料を基に NTT データ経営研究所が作成

MT23 においては、2014 年以前 IEC61508 機能安全への対応として、保護電子回路 (PEC) の考え方を導入する方針が審議されてきた。

具体的には、機能安全を「ソフトウェアによる安全担保」と定義したうえで、ソフトウェアの品質確保を開発プロセスで担保することに加え、マイクロコントローラー (マイコン) の誤動作回避を確認するために EMC 試験を行うことが示されている。

2015 年以降は、IoT への対応として、家電等製品のネットワーク経由での①遠隔操作、②ソ

⁴²⁾ <https://csrc.nist.gov/publications/detail/nistir/8259/draft>

⁴³⁾ IEC Web ページ https://www.iec.ch/dyn/www/f?p=103:14:0:::FSP_ORG_ID,FSP_LANG_ID:2454,25

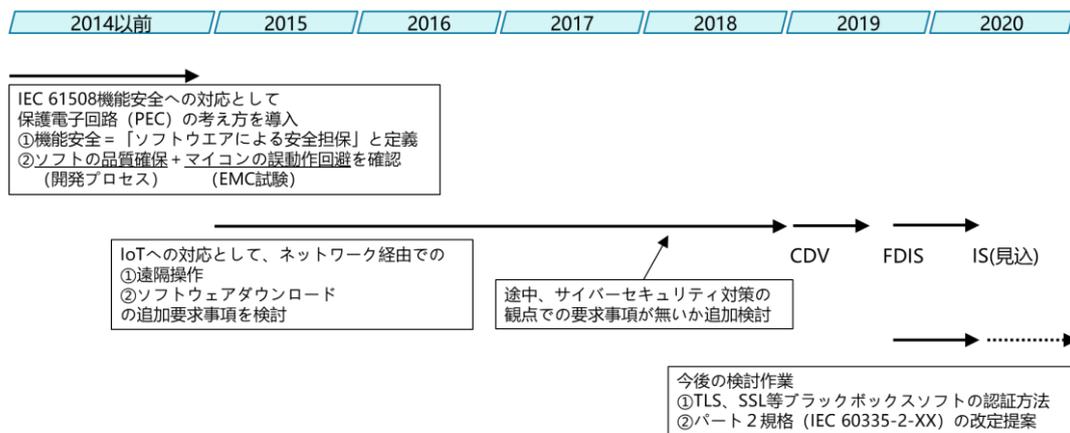
ソフトウェアダウンロードの2点に関して、追加要求事項の検討が始まった。IoT への対応に関する検討は2018年頃にサイバーセキュリティ対策の観点での要求事項に関する追加検討を行ったうえで、2019年前半にCVD (Committee Draft for Vote : 国際規格原案) まで進んでおり、現在FDIS (Final Draft International Standard : 最終国際規格案) の発行を待っている。本件の内容とは別の理由で、IS (International Standard : 国際規格) の発行が遅れる見込みである。

今後の検討作業としては、以下2点があげられている。

- ①TLS、SSL等ブラックボックスソフトの認証方法
- ②パート2規格 (IEC 60335-2-XX) の改訂原案

上記のIEC TC61 MT23における審議の経緯を図表24に示す。

図表24 MT23における審議の経緯



出典：WG資料

(注) FDIS/IS の発行や承認は、本件の内容とは別の理由で遅れる見込みである。

IEC TC61 MT23 では、遠隔操作のリスクを検討するにあたって、それぞれの機器に対して、「人が付いて使う機器 (attended appliance)」と「人が付いていない状態で使う機器 (unattended appliance)」の考えのもとで整理している。人が付いて使う機器 (attended appliance) に相当する機器 (調理器具 (こんろ、てんぷら鍋) アイロン、電動工具、ストーブなど) に関しては機器の設計段階で遠隔操作を想定していないためリスクが大きいと示している。他方、人が付いていない状態で使う機器 (unattended appliance) に相当する機器 (冷蔵庫、洗濯機、AV機器など) に関しては、もともと無人状態でも使うことを想定しているため遠隔操作時のリスクはあまり増えないとしている。これらの整理も踏まえた上で、IEC TC61 MT23 においては、各機器共通の要求事項は一般要求事項としてIEC 60335-1規格で対応し、機器ごとに使い方が異なる部分は個別要求事項としてIEC 60335-2-XX規格で対応する方針を取っている。

今後IS化が見込まれるIoT化への対応に向けたネットワーク経由での遠隔操作に関する改訂内容を図表25に示す。なお、IEC 60335-1では、家庭内LANやモバイル回線など直接・間接

的に Public network に繋がるものは全て Public network の対象としている（図表 26）。

図表 26 を俯瞰して見ると、多少の重複はあるが、遠隔操作に関する改訂内容は概ね以下の 4 つの観点に分類することができる。本調査における検討は上から 2 つの観点との関わりが深いが、将来的にはソフトウェアのダウンロードとインストールが重要性を帯びてくると言える。

- ・ パブリックネットワークの不確実性とこれを用いたリモートコミュニケーションの保護に関するもの
- ・ 安全機能とそのソフトウェアの保護に関するもの
- ・ ソフトウェアのダウンロードとインストールに関するもの
- ・ その他（同時に複数個所から操作した時の対策等）

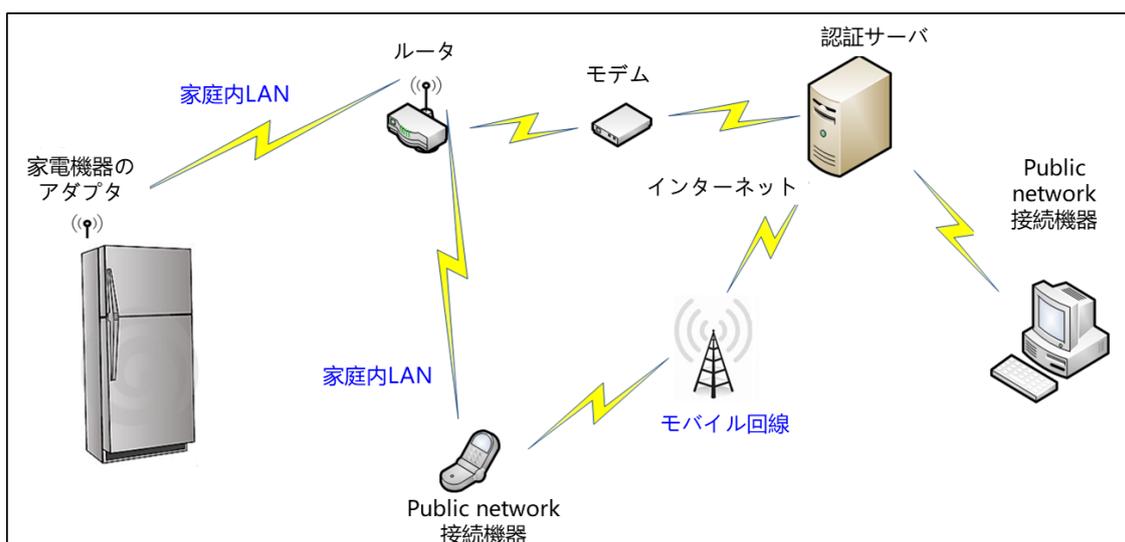
図表 25 遠隔操作改定案の内容

項目番号	要求事項の概要	備考
22.XX	Public network を経由した Remote communication が家電製品の 安全担保に影響を与えないこと	
	Remote communication にはソフトウェアのダウンロードを含む。	
	家電製品の安全担保、及びソフトウェアのダウンロードに係るソフトウェアは、 他の部分と分離され 、かつ保護電子回路に用いるソフトウェアへの要求事項と同様の要件を満たすこと。 (Annex R)	Annex R の要求事項 バージョン管理、 変更の必然性、 モジュール化設計
XY.7.12.101	ソフトウェアのダウンロード時には、手順とバージョン情報をユーザに示すこと。	対象機器、ソフトウェアの組み合わせ
XY.22.101	Public network の通信ソフトウェアは 他の部分と分離 されていること。	モジュール化設計
XY.22.102	Remote communication は、データの衝突、欠落などの 通信エラーに対して、異常検出、再送などの対策を講じていること。	通信の不確実性への対策
XY.11.103	同時に複数の操作元 からの操作要求があった時、異常を引き起こさない対策を講じていること。	同時に複数個所から操作した時の対策
XY.22.104	Remote communication は 出荷時は無効 とし、承認された人による認証手続きを経てから、機能を有効にすること。	出荷時は遠隔操作無効
	認証手続きの通信は暗号化されていること。	
XY.22.105	Remote communication は、 不正なアクセス、及び通信異常 に対する対策が講じられていること。	

項目番号	要求事項の概要	備考
XY.22.106	家電製品の安全担保が Remote communication に依存しないこと。	クラウドに依存した安全機能の禁止
XY.22.107	Remote communication は暗号化されていること。	
XY.22.108	ダウンロードするソフトウェアはメーカーによりあらかじめソフトウェアの互換性、通信異常時の動作、バージョンチェックなどの確認が取られていること。	
XY.11.109	ダウンロードしたソフトウェアのインストールは、家電製品の管理者の許可を得て行わなければならない。	ユーザが知らない間にソフトウェアを書き換えることを禁止
XY.22.110	ダウンロードしたソフトウェアのインストールは、家電製品の安全担保に影響を与えてはならない。	

出典： WG 資料を基に NTT データ経営研究所が作成

図表 26 Public network の範囲



出典： WG 資料を基に NTT データ経営研究所が作成

一般に、情報セキュリティについては CIA（機密性・完全性・可用性）が重視されるが、IEC 60335-1 においては、これに加えて Authenticity：信憑性（認証）と Non-Repudiation：否認不可性（操作記録を残していること）も重視している。これらのうち、製品安全との関わりにおいては、「Public network の不確実性」の観点からは完全性が、「正しいユーザによる操作か」という観点からは信憑性が特に重視されている。

次に、電気用品安全法と IEC 60335-1 規格及び改定版の FDIS (Final Draft International Draft) 案との比較について図表 27 に示す。この表は電気用品調査委員会からも公表されている

が、ここに提示するものは **FDIS** 案との比較になっており、最新の情報にアップデートされている。

図表 27 電気用品安全法と IEC 60335-1 規格及び改定版の FDIS 案との比較

	電安法 通信回線による遠隔操作（解釈別表第八）	IEC 60335-1 規格及び改定版の FDIS 案	
適用範囲	1 項(2) ロ (1) 赤外線を利用した遠隔操作機構 (2) 電力搬送波を利用した遠隔操作機構 (3) 音声を利用した遠隔操作機構 (4) 通信回線を利用した遠隔操作機構 注；(1)～(4)の遠隔操作機構毎に個別の要求事項を規定	現行	電気通信、音響制御、バスシステムなどを用いて、機器の見えないところから発するコマンドによって、機器を制御する動作（赤外線制御自体は、遠隔操作とはみなさない。）
		改定案	遠隔操作の定義が下記の内容に変更されている。 ・公衆回線を用いて、機器の見えないところから無線、音声、バスシステム等の通信により機器を制御する動作。 ・公衆回線には宅内の LAN 部分も含まれる。 ・公衆回線につながらない有線通信は除外される。
電気ストーブの遠隔操作の禁止	2 項(1)イ (ハ) 赤熱する発熱体を有し、その発熱体が外部から見える構造のものにあっては、遠隔操作（有線式のものを除く）の操作によって電源回路を閉路できないこと。	現行	IEC60335-2-30 22.109 項 スイッチを有する機器は、電子スイッチに依存してはならない。
		改定案	要求事項の変更は無い。（技術的な変更はない。以下同じ）

以下；通信回線を利用する遠隔操作に対して規定		以下；全ての遠隔操作に対して規定	
5.1 リスクアセスメント	<p>リスクアセスメント</p> <p>(a)遠隔操作に伴う危険源がない又はリスク低減策を講じることにより遠隔操作に伴う危険源がない機器と評価されるもの。</p>	現行	<ul style="list-style-type: none"> ・ 22.40 項 <p>遠隔操作時に機器の動作を停止させるスイッチが不要な、危険を生じさせることなしに、連続的、自動的、又は遠隔的に運転できる機器の例としてファン、貯湯式温水器、エアコンディショナ、冷蔵庫並びに日除け、窓、ドア、門及びロールシャッタ用の駆動装置が示されている。</p> <ul style="list-style-type: none"> ・ リスクアセスメントに対する要求は無い。
		改定案	要求事項の変更は無い。
5.2 通信回線の故障等による安全状態	<p>(b)通信回線が故障等により途絶しても遠隔操作される機器は安全状態を維持し、通信回線に復旧の見込みがない場合は遠隔操作される機器の安全機能により安全な状態が確保できること。</p>	現行	<ul style="list-style-type: none"> ・ 22.49 項 <p>遠隔操作により電源回路の開路ができない場合を考慮して、連続運転で危険が生じるおそれがある機器に、遠隔操作の前に運転持続時間の設定を行うことを要求している。</p>
		改定案	<p>以下の要求事項を追加。</p> <ul style="list-style-type: none"> ・ XY.22.105 項 <p>不正なアクセス及び通信異常に対し、安全状態の確保(IEC 60335-1 規格の要求事項を満足すること)を要求。</p> <ul style="list-style-type: none"> ・ XY.22.106 項 <p>安全状態の確保に寄与する機能が遠隔操作の通信に依存しないことを要求。</p>

5.3 手元操作の優先／通信回線の切り離し	(c)遠隔操作される機器の近くにいる人の危険を回避するため、次に掲げる対策を講じていること。 i 手元操作が最優先されること ii 遠隔操作される機器の近くにいる人により、容易に通信回線の切り離しができること。	現行	(手元操作) ・ 22.40 項 危険を生じさせることなしに、連続的、自動的、又は遠隔的に運転できる機器を除き、遠隔操作の機器には、機器の動作を停止させるためのスイッチを取り付けなければならない。 ・ 22.50 項 機器内に組み込んだ制御装置がある場合、それが遠隔操作によって操作される制御装置よりも優先されなければならない。(通信回線の切り離し) ・ 要求事項の規定は無い
		改定案	要求事項の変更は無い。
5.4 操作結果のフィードバック／動作確認	(d)遠隔操作による動作が確実に行われるよう、次に掲げるいずれかの対策を講じること。 i 操作結果のフィードバックができること ii 動作保証試験の実施及び使用者への注意喚起の取扱説明書への記載	現行	(操作結果のフィードバック) ・ 特に具体的な要求事項は無いが、表示に関連して、22.51 項に連続的、自動的、又は遠隔的に運転できる機器を除き、手作業による設定と遠隔操作モードであることの視覚的な表示要求がある。 (動作保証試験及び使用者への注意喚起) ・ 要求事項の規定は無い
		改定案	要求事項の変更は無い。

5.5 識別管理 / 外乱に対する誤動作 / 再接続	(e)通信回線（解釈別表第四1(2)ロ(イ)に掲げるもの及び公衆回線を除く。）において、次の対策を遠隔操作される機器側に講じていること。 i 操作機器の識別管理 ii 外乱に対する誤動作防止 iii 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に限る）	現行	(外乱に対する誤動作防止) ・ 19.11.4 項 危険な誤動作をする可能性のあるものは、19.11.4.1～19.11.4.7 項 (IEC 61000-4-**) の試験を実施する。 (通信回線接続時の再接続) ・ 要求事項の規定は無い
		改定案	以下の要求事項を追加。 (識別管理) ・ XY.22.104 項 遠隔操作の通信を有効にする前に、適切な責任者による承認と認証、及び通信暗号化を要求。 ・ 認証時に機器を特定するため、識別管理も含まれていると考えられる。 (外乱に対する誤動作防止) ・ XY.22.105 項 不正なアクセス及び通信異常に対し、安全状態の確保 (IEC 60335-1 規格の要求事項を満足すること) を要求。

5.6 公衆回線の一時的途絶	(f)通信回線のうち、公衆回線を利用するものにあつては、回線の一時的途絶や故障等により安全性に影響を与えない対策が講じられていること。	現行	・要求事項の規定は無い。
		改定案	以下の要求事項を追加。 <ul style="list-style-type: none"> ・ XY.22.105 項 不正なアクセス及び通信異常に対し、安全状態の確保(IEC 60335-1 規格の要求事項を満足すること)を要求。 ・ XY.22.106 項 安全状態の確保に寄与する機能が遠隔操作の通信に依存しないことを要求。
5.7 同時に2箇所以上の遠隔操作	(g)同時に2箇所以上からの遠隔操作を受け付けない対策を講じること。	現行	・要求事項の規定は無い
		改定案	以下の要求事項を追加。 <ul style="list-style-type: none"> ・ XY.22.103 項 複数箇所から同時または順次遠隔操作された時でも安全状態が確保できることを要求。受け付けること自体は構わない。
5.8 誤操作防止	(h)適切な誤操作防止対策を講じること。	現行	・要求事項の規定は無い
		改定案	・要求事項の変更は無い

5.9 出荷状態の遠隔操作機能の無効化	(i)出荷状態において、遠隔操作機能を無効にすること。	現行	<ul style="list-style-type: none"> ・ 22.51 項 <p>機器が遠隔操作モードで操作できるようになる前に、機器上の制御装置を手作業で遠隔操作モードに設定できなければならない。機器上には、機器が遠隔操作モードに設定されていることを示す視覚的表示がなければならない。連続的、自動的、又は遠隔的に運転できる機器については、手作業による設定及び遠隔操作モードであることの視覚的表示は不要。</p>
		改定案	<p>以下の要求事項を追加。</p> <ul style="list-style-type: none"> ・ XY.22.104 項 <p>遠隔操作の通信を有効にする前に、適切な責任者による承認と認証、及び通信暗号化を要求。</p>

(2) 海外ヒアリング結果

1) AMDEA

英国における家電製品製造者の業界団体である The Association of Manufacturers of Domestic Appliance（英国家庭用電気機器製造者協会。以下、AMDEA）を訪問し、①英国 DCMS の政策（「消費者 IoT セキュリティの行動規範」の公表と国際標準化への展開、セキュリティラベル義務化に向けた検討等）に対する民間業界団体側のスタンス、②英国における IEC60335-1 第 6 版公表に向けた準備動向等について明らかにすることを目的として、ヒアリング調査を実施した。

(ア) 英国 DCMS の政策に対する民間業界団体側のスタンス

英国 DCMS は、2018 年に策定した「Code of Practice for Consumer IoT Security」を国内に広く根付かせるため、13 個のガイドラインのうち最も基盤的な 3 つを選択し、法で義務化することによって規制化する検討を進めている。この規制を導入するにあたり、英国 DCMS は義務化のアプローチとして、セキュリティラベルの義務化を提案し、パブリックコメントを実施した。これらの 3 つのガイドラインは製品安全に直接関わるものではなく、サイバーセキュリティ上の要件に留まっている。

これに対し、AMDEA はどのようなスタンスなのかについて意見を聴取した。その結果、AMDEA は以下のような考えを持っていることが分かった。

- ・ 英国 DCMS の取組は、5G サービスの開始を間近に控え、ベンチャーや中小企業を含む簡易 IoT デバイスメーカーを統制するため、最大限急いで検討を進めているものと理解している。白物家電は、一連の取組の主たるターゲットであるとは考えておらず、従ってこの取組には是々非々で対応している。
- ・ 規制の導入にあたり、セキュリティラベルを義務化することは難しいと考えている。

また、当該行動規範にはレジリエンスの確保を求めるガイドラインが組み入れられており、製品安全に関わりが深いと考えられるが、その内容は製品安全におけるフェールセーフの考え方とは逆行するものとなっている（通信が途絶してもデバイスを止めることは求めず、逆に動き続けることを推奨している）。AMDEA がこの点についてどのような見解を持っているかを尋ねたところ、レジリエンスの要求は止まると人の命や健康に直接被害が生じる組込型医療 IoT デバイスを念頭に置いたものであり、白物家電に適用されるものとは想定していないという回答を得た。

以上を総括すると、英国 DCMS の一連の政策は、電気用品等製品の安全との関わりが必ずしも深くなく、英国の家電製品製造者の事業者団体は、これに消極的な姿勢で臨んでいるという結論となる。

(イ) 英国における IEC60335-1 第 6 版公表に向けた準備動向等

AMDEA としても、IEC60335-1 第 6 版の国際標準化検討には積極的に関与している。

同標準が公開された後は、EU レベルでの規格化と国内レベルでの規格化（英国規格協会：BSI によるもの）が進められる。製品安全に関しては、こちらの動きへの積極的な参加が主眼とな

るとのことである。この対応プロセスは、我が国における JIS 規格化と同等であると言える。

2) ETSI

英国 DCMS は、2018 年に策定した「Code of Practice for Consumer IoT Security」を、セキュリティ側コミュニティにおいて EU 全体に普及させるため、ETSI において技術仕様の国際標準化にまず取り組んだ。こうして 2019 年 2 月に公表されたのが、「ETSI TS 103 645 v1.1.1」である。本調査では、ETSI を訪問し、「ETSI TS 103 645 v1.1.1」を策定した経緯とその後の対応の方向性、当該規格と電気用品等製品の安全との関わり等について明らかにすることを目的として、ヒアリング調査を実施した。

英国 DCMS は、2018 年に策定した「Code of Practice for Consumer IoT Security」を、セキュリティ側コミュニティにおいて EU 全体に普及させるべく、技術仕様の国際標準化を ETSI に提案した。ETSI はこの提案に基づき、EU 加盟各国のステークホルダーによる討議を実施し、2019 年 2 月に TS を公表している。

ETSI によれば、この検討はセキュリティ側コミュニティのみで実施したものであり、製品安全側コミュニティは検討に参加していないとのことである。このように、欧州地域では、我が国と同様、セキュリティとセーフティは違うコミュニティで別々に議論されている。

AMDEA に対してと同様に、ETSI に対しても、レジリエンスの確保を求めるガイドラインがなぜフェールセーフの考え方と逆行しているのかについて尋ねてみた。その結果、得られた答えは AMDEA と同じであった。すなわち、レジリエンスの要求は、止まると人の命や健康に直接被害が生じる組込型医療 IoT デバイス等を念頭に置いて策定したものである。

現在進行中の新しい展開としては、英国 DCMS が引き続きイニシアチブを取り、さらに欧州標準化委員会（CEN : Comité Européen de Normalisation）の協力を得て、ETSI が TS を起点として、新しい EN 規格の策定を進めている。この EN 規格のドラフト第 2 版は、2019 年 11 月に公表されている⁴⁴。EN 規格として公表されると、EU 加盟各国はこれを独自の国内規格（英国であれば、BSI-EN）に反映すると共に、EN 規格と相反する規格が自国内に存在しないよう調整することが義務付けられる。このため、英国 DCMS が策定した「Code of Practice for Consumer IoT Security」の 13 のガイドラインを、EU 各国において強力で推進することができるようになる。

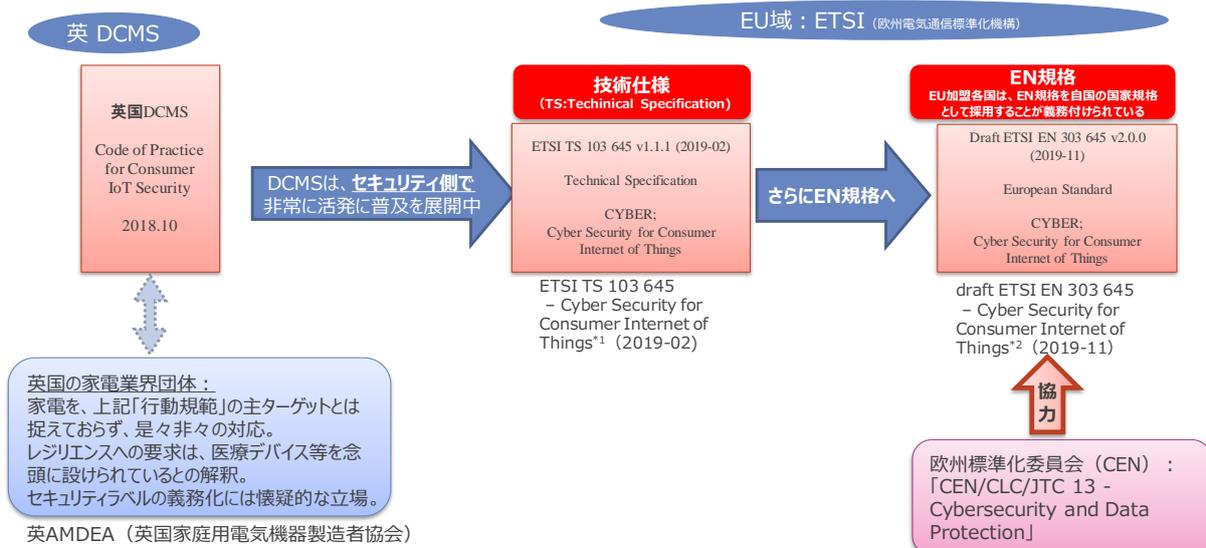
3) 英国 DCMS の EU 域内標準化活動の全体像と、AMDEA との関係

上記の調査結果に基づき、英国 DCMS の EU 域内標準化活動の全体像と、AMDEA との関係について図表 28 に整理した。

⁴⁴

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf

図表 28 英国の行動規範をめぐる最新動向



出典：*1:https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

*2: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf

(3) 調査結果のとりまとめ

1) 英国を中心とした消費者向け IoT 機器のセキュリティに関するベースライン引き上げの動き

英国 DCMS を中心とした「消費者向け IoT 機器のセキュリティに関する行動規範」の急速な欧州域内拡大の動きは、目前に控えた 5G 時代に備えるためのものであり、製品安全との関係が薄いまま別個に進展している。ETSI はこの動きを進めるための主たる場として機能しており、近いうちに EN 規格化が実現して、EU 加盟国はこの行動規範に沿う国内規格を策定する義務を負うことになる見込みである。

この動きは欧州域外にも広がっている。例えば、2019 年 7 月 29 日には、英国は、オーストラリア、カナダ、ニュージーランド、米国と共同で閣僚声明に署名し、5 カ国で IoT デバイスのセキュリティ強化のための政策を調整していくことを宣言した。また、IoT デバイスのセキュリティに関するシンガポールとのパートナーシップを強化する合意にも署名している。

他方で、英国の電気用品等製品の製造事業者の事業者団体 (AMDEA) はこの動きとは距離を置き、是々非々の対応を行っている。これは既に述べた通り、欧州域内の製品安全のステークホルダーとは一線を画した動きとなっているからである。

2) 英国国内におけるセキュリティラベル義務化の動き

英国内では、1)の行動規範のうち特に基盤的な 3 つのガイドラインについて義務化するべく政策検討を進めており、一旦はセキュリティラベルの義務化によってこの目的を達する方針を立てたが、パブリックコメントの結果が芳しくなかった。このため英国 DCMS は、規制として義務化する方針は堅持しているものの、アプローチを「ラベルの義務化」から「小売業者による消費者への情報提供の義務化」へと変更し、さらに検討を進める意思を見せている。しかし、まだ時間がかかりそうである。

3) 米国 CPSC の動き

欧州域内では、消費者向け IoT 機器のベースラインセキュリティを強化しようとする動きと、IEC60335-1 の改定によって遠隔操作の安全を向上させようとする動きが独立して進展しているが、米国 CPSC は消費者向け IoT 機器の製品安全をセキュリティと一体化して検討しようという意思を見せている。この方針に基づき、省庁間 WG を形成する等の新しい動きが見え始めた。

米国 CPSC のアプローチは、我が国や欧州における製品安全とセキュリティを別々に検討する動きとは一線を画しているため、今後の CPSC の動向には注目する必要がある。但し、米国の民間関連事業者団体は必ずしも CPSC と考え方を共有しておらず、民間の自主的な取組を優先する意識に変わりはない。

4) IEC60335-1 の改定作業の動き

IEC60335-1 第 6 版の検討は、現在 FDIS の公表を待っている。本件の内容とは別の理由で IS (International Standard) の発行は遅れるものと見込まれるが、この発行を受けて、国内外において国内規格の見直しの動きが顕在化するものとみられるため、電気用品調査委員会の動きと連携を図りつつ、海外においては各国の国内規格の改定の検討動向を引き続き注視していくことが必要である。

遠隔操作に関する改訂内容は概ね以下の 4 つの観点に分類することができる。本調査における検討は上から 2 つの観点との関わりが深い。将来的にはソフトウェアのダウンロードとインストールが重要性を帯びてくると言える。

- ・ パブリックネットワークの不確実性とこれを用いたリモートコミュニケーションの保護に関するもの
- ・ 安全機能とそのソフトウェアの保護に関するもの
- ・ ソフトウェアのダウンロードとインストールに関するもの
- ・ その他（同時に複数箇所から操作した時の対策等）

IEC60335-1 においては、情報セキュリティに関し、機密性、完全性、可用性、信憑性（認証）、否認不可性（操作記録を残していること）が重視される。これらのうち、製品安全との関わりにおいては、「Public network の不確実性」の観点からは完全性が、「正しいユーザによる操作か」という観点からは信憑性が特に重視されることになる。

2.4. IoT 化等が考えられる電気用品等機器に係る消費者の生命、身体への危害発生の防止を図るための製品安全の確保の在り方に関する検討

上記の実態調査等の結果を踏まえ、IoT 化等が考えられる電気用品等機器に係る消費者の生命、身体への危害発生の防止を図るための製品安全の確保の在り方に関して検討すべく、検討会およびワーキンググループ（以下、WG）を開催した。

(1) 検討会について

検討会の委員は、「製品安全/IoT（含むサイバーセキュリティ）」のいずれかのバックグラウンドを保有、及び「アカデミック/民間/業界団体/法曹/保険業」といった多彩な所属の双方を満たしたメンバーを選任して構成した。構成員（座長、副座長、その他の委員）を図表 29 に示す。

図表 29 構成員一覧

座長	氏名(敬称略)	所属及び役職
座長	向殿 政男	明治大学名誉教授
	有村 浩一	一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC) 常務理事
	小野 亮	東京大学新領域創生科学研究科 教授
副座長	梶屋 俊幸	一般社団法人セーフティグローバル推進機構理事 IEC/IECEE CMC(認証管理委員会)代表委員
	源田 浩	三井住友海上火災保険株式会社 公務開発部 部長(企画開発担当)
	郷原 信郎	郷原総合コンプライアンス法律事務所代表
	後藤 厚宏	情報セキュリティ大学院大学 学長
	住谷 淳吉	一般財団法人 電気安全環境研究所(JET) 経営企画部 理事
	高橋 茂樹	コンサルタント (元国際電気標準会議(IEC)WG 座長)
	升田 純	升田法律事務所 代表弁護士
	森 亮二	弁護士法人 英知法律事務所 弁護士
	渡部 利範	株式会社テクノクオリティ 代表取締役社長

また、以下に示す業界団体及び経済産業省の関連部署が、オブザーバーとして参加した。

- ・ 経済産業省 産業保安グループ製品安全課、サイバーセキュリティ課、情報産業課、
- ・ 一般社団法人電子情報技術産業協会 (JEITA)
- ・ 一般社団法人日本電機工業会 (JEMA)
- ・ 一般社団法人日本ガス石油機器工業会 (JGKA)
- ・ 独立行政法人製品評価技術基盤機構 (NITE)
- ・ 独立行政法人情報処理推進機構(IPA)
- ・ 独立行政法人労働者健康安全機構 労働安全衛生総合研究所 (JNIOOSH)
- ・ 一般財団法人家電製品協会 (AEHA)
- ・ 一般財団法人日本ガス機器検査協会 (JIA)

事務局は株式会社エヌ・ティ・ティ・データ経営研究所が担当した。

(2) WGについて

「リスクシナリオ、ユースケース及びリスク評価の整理・検討」について、実態に則して具体的に議論すべく、検討会のオブザーバーメンバーを中心としたWGを新たに設置し、WG委員に調査・検討作業への支援を賜った。構成員（座長、その他の委員）を図表30に示す。

図表 30 構成員一覧

座長	氏名(敬称略)	所属及び役職
座長	住谷 淳吉	一般財団法人 電気安全環境研究所(JET) 経営企画部 理事
	岡本 修	独立行政法人製品評価技術基盤機構(NITE)
	小川 隆一	独立行政法人情報処理推進機構(IPA)
	木村 雅之	一般社団法人日本電機工業会(JEMA)
	小原 章二	一般社団法人電子情報技術産業協会(JEITA)
	坂口 正	IEC/TC61/MT23 セクレタリ
	真田 巧	一般財団法人家電製品協会(AEHA)
	清水 尚憲	独立行政法人労働者健康安全機構 労働安全衛生総合研究所(JNIOOSH)
	豊田 浩寿	一般社団法人日本ガス石油機器工業会(JGKA)
	森廣 泰則	一般財団法人日本ガス機器検査協会(JIA)

また、以下に示す企業及び経済産業省の関連部署が、オブザーバーとして参加した。

- ・ 経済産業省 産業保安グループ製品安全課、同省サイバーセキュリティ課、同省情報産業課
- ・ テュフ・ラインランドジャパン株式会社

事務局は株式会社エヌ・ティ・ティ・データ経営研究所が担当した。

2.5. IoT 化等が考えられる電気用品等製品において今後想定される消費者の生命、身体への危害発生等のリスクシナリオ及びユースケースの整理・検討

(1) IoT 化された電気用品等のリスク対応の在り方に関する検討の実施方針

1) 遠隔操作を行う機器に関する定義

IEC60335-1 及び IEC60335-2-××シリーズにおける『遠隔操作』に関係のある部分を抽出すると、大きく3つに分類される。

① 遠隔操作が禁止又は事実上禁止されている機器

② ①に当たらない機器

②-1：人の注意が行き届く状態で動作する機器

②-2：人の注意が行き届かない状態で動作する機器

今後、各個別機器での配慮すべき危険源、考慮すべきリスク、リスク低減対策などの検討やそもそものユースケースやリスクシナリオ、対応策の検討を進める機器の決め方を考える上でも、①及び②の定義づけが必要になると考えられることから、それぞれ対象となる機器を整理した。

ただし、②については、IEC60335-2-××の対象機器であっても、タイマー、使用用途等の違いで「人の注意が行き届く状態で動作する機器」と「人の注意が行き届かない状態で動作する機器」に分かれている。この2つの分類は明確であるべき（概念、用語の定義等）とのご意見があり、さらに検討が必要な状況である。

(ア) 遠隔操作の OFF→ON を禁止している機器など

「据え置き型ホブ(コンロ)」は IEC60335-2-6 において遠隔操作が禁止されており、「高所取付用ヒータ以外の可視赤熱放射ヒータ」についても、IEC60335-2-30 において遠隔操作が事実上禁止されている。なお、コンロ及び可視赤熱放射ヒータ以外の個別機器の IEC60335-2-××シリーズにおいて、同様の整理がなされている機器は確認できていない。

図表 31 遠隔操作の OFF→ON を禁止している機器の具体例

据え置き型ホブ（コンロ）

JIS C 9335-1の22.40項の規定

運転中に移動させるか、又は触れることができる運動部をもつモータ駆動機器及び複合機器には、モータを制御するスイッチを取り付けなければならない。このスイッチの操作部は、容易に視認でき、触れることができなければならない。危険を生じさせることなしに、連続的、自動的、又は遠隔的に運転できる機器を除き、遠隔操作の機器には、機器の動作を停止させるためのスイッチを取り付けなければならない。このスイッチの操作部は、容易に視認でき、触れることができなければならない。
注記 危険を生じさせることなしに、連続的、自動的、又は遠隔的に運転できる機器の例には、ファン、貯湯式温水器、エアコンディショナ、冷蔵庫並びに日除け、窓、ドア、門及びロールシャッタ用の駆動装置がある。適否は、目視検査によって判定する。

JIS C 9335-2-6の22.40項の規定

※他の製品別基準（JIS化されたもの）も全て調べたが、遠隔操作の禁止を求められている機器は見いだせていない。

追加（“適否は、目視検査”で始まる段落の前に、次を追加する）

ホブは、遠隔操作してはならない。

高所取付用ヒータ以外の可視赤熱放射ヒータ

JIS C 9335-2-30の22.109項の規定

高所取付用ヒータ以外の可視赤熱放射ヒータは、OFF位置のスイッチによる電源の断路は、電子部品に依存してはならない。
適否は、目視検査によって判定する。

※電子スイッチでない、遠隔操作はできない。よって、遠隔操作できないこと同義。

また、「S マーク認証の運用基準（エアコンを除く）」において、IH 調理器は人がついて使用することを意図した機器であるため、遠隔操作の電源 ON は禁止、電源 OFF に関しても、同様に考えられている。

1. 適用範囲

注記 2 この運用基準における遠隔操作とは、電気用品安全法の技術基準の解釈別表第八1(2) 口により電源回路の閉路を行うものをいう。ただし、リスク評価の結果、閉路以外の操作についてリスクがあると判断された場合には、閉路以外の操作を含む。

3.1 遠隔操作を行うことができる製品の判定方法

D. 遠隔操作に向かない機器（短時間定格、手持ち型など）、人がついて使用することを意図した機器（IH 調理器など）及び A～C に該当しない機器は、特に見えない位置からの遠隔操作を不可として、不適合とする。

なお、ガス機器の場合は遠隔操作に係る技術基準が整備されていないため、現在関係団体等で省令・通達改正に向けた基準の整備を行っている。具体的には、遠隔操作 OFF→ON に係る技術基準については、電気用品安全法で整備された基準に準じつつ遠隔操作 ON→OFF も含めた形で基準を策定し、省令・通達を改正する予定（2020年6月改正・施行（一部経過措置）予定）。

(イ) 人の注意が行き届く状態で動作する機器/人の注意が行き届かない状態で操作する機器
IEC60335-2- “Household and similar electrical appliances – Safety - Part 2” シリーズにおける個別規格のうち、「30 Resistance to heat and fire」の記載内容を対象として調査を実施した。調査に当たっては JIS C 9335-2- 「家庭用及びこれに類する電気製品の安全性-第2-」を主に確認し、必要に応じて上記の IEC 規格を参照した。

具体的には、人の注意が行き届く状態で操作することを前提として耐熱性及び耐火性に関する試験の要求事項を定めた 30.2.2 項及び人の注意が行き届かない状態で操作することを前提と

して耐熱性及び耐火性に関する試験の要求事項を定めた 30.2.3 項が、それぞれの個別規格においてどのように取り扱われているのかを確認した。この調査により、どのような機器が「人の注意が行き届く状態で動作する機器」／「人の注意が行き届かない状態で操作する機器」であると考えられているかを特定することができる。

調査の結果を図表 32 に示す。

なお、リスクシナリオやユースケースの検討対象となる家電製品等の抽出を行う観点で、人の注意が行き届かない状況で操作することを想定した機器には例えば以下のようなものがある（※カッコ内は規格番号）。

- セントラル掃除機又はロボット掃除機（JISC9335-2-2）
- 電気洗濯機（JISC9335-2-7）
- タイマを持つ機器又は取扱説明書で1時間以上の調理動作を記載しているコンロ（JISC9335-2-9）
- 回転ドラム式電気乾燥機（JISC9335-2-11）
- エアコンディショナ及び除湿機（JISC9335-2-40）
- 暖房、換気、冷房装置用加湿器（JISC9335-2-88） 等

図表 32 家庭用及びこれに類する電気機器を人の注意が行き届く状態で動作する機器と人の注意が行き届かない状態で動作する機器への分類状況

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-2	真空掃除機及び吸水式掃除機	(右記以外の機器)	セントラル電気掃除機
JISC9335-2-3	電気アイロン	○	—
JISC9335-2-4	電気脱水機	○	—
JISC9335-2-5	電気食器洗機	(右記以外の機器)	プログラム又はタイマーが組み込まれている機器
JISC9335-2-6	据置形クッキングレンジ、ホブ、オーブン及びこれらに類する機器	タイマーを持たない電磁中華鍋エレメント、グリル及びグリドル	(左記以外の機器)
JISC9335-2-7	電気洗濯機	(右記以外の機器)	プログラム又はタイマーを組み込んだ機器
JISC9335-2-8	電気かみそり及び毛髪バリカン	○	—
JISC9335-2-9	可搬形ホブ、オーブン、トースタ及びこれらに類する機器	(右記以外の機器)	パン焼き器及び食品脱水機、タイマーを持つ機器又は取扱説明書で1時間以上の調理動作を記載している次の機器(クッカ、コンロ、オーブン、トースタ、回転式グリル)
JISC9335-2-10	床処理機及び湿式洗いブラシ機	○	—
JISC9335-2-11	回転ドラム式電気乾燥機	—	○
JISC9335-2-12	ウォームプレート及びこれに類する機器	—	○
JISC9335-2-13	深めのフライなべ、フライパン及びこれに類する機器	フライパン	深いフライ鍋
JISC9335-2-14	ちゅう房機器	(右記以外の機器)	アイスクリーム製造機及びかく乳機

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-15	液体加熱機器	○	水蒸留器並びに液体及び食品をある特定の温度に維持する機器
JISC9335-2-16	食品くずディスポーザ	○	—
JISC9335-2-17	毛布、パッド及びこれに類する可とう電熱機器	パッド	毛布及びマットレス及びソフトあんか
JISC9335-2-21	貯湯式電気温水器	—	○
JISC9335-2-23	スキンケア又はヘアケア用機器	(右記以外の機器)	着脱式カーラ用ヒータ
JISC9335-2-24	冷却用機器、アイスクリーム機器及び製氷機	—	○
JISC9335-2-25	電子レンジ及び複合形電子レンジ	(右記以外の機器)	開始時間をあらかじめ選択できる電子レンジ及び保温機能を持つ電子レンジ
JISC9335-2-26	クロック	—	○
JISC9335-2-27	紫外線及び赤外線による皮膚照射用装置	○	—
JISC9335-2-28	ミシン	○	—
JISC9335-2-29	バッテリーチャージャ	—	○
JISC9335-2-30	ルームヒータ	—	○
JISC9335-2-31	レンジフード及びその他の調理煙換気装置	—	○
JISC9335-2-32	マッサージ器	○	—
JISC9335-2-34	電動圧縮機	—	○

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-35	瞬間湯沸器	—	○
JISC9335-2-36	業務用電気レンジ, オープン, こんろ及びこんろ部	—	○
JISC9335-2-37	業務用フライヤ	—	○
JISC9335-2-38	業務用電気グリドル及びグリドルグリル	—	○
JISC9335-2-39	業務用多目的調理鍋	—	○
JISC9335-2-40	エアコンディショナ及び除湿機	—	○
JISC9335-2-41	ポンプ	取り扱い説明書に「30mA 以下の定格感度電流の漏電遮断器 (RCD) を通して供給する」旨の記載がある水中ポンプ	(左記以外の機器)
JISC9335-2-42	業務用コンベクションオーブン, 蒸し器及びスチームコンベクションオーブン	—	○
JISC9335-2-43	衣類乾燥機及びタオルレール	—	○
JISC9335-2-44	電気アイロナ	(右記以外の機器)	ズボンプレス
JISC9335-2-45	可搬形加熱工具及びこれに類する機器	(右記以外の機器)	接触形ファイアライター
JISC9335-2-47	業務用電気煮炊き鍋	—	○
JISC9335-2-48	業務用グリル及びトースタ	—	○

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-49	食品及び容器類用保温式業務用電気機器	—	○
JISC9335-2-50	業務用湯せん器	—	○
JISC9335-2-51	給湯及び給水設備用据置形循環ポンプ	—	○
JISC9335-2-52	口こう（腔）衛生機器	○	—
JISC9335-2-53	サウナ用電熱装置及び赤外線キャビン	—	○
JISC9335-2-54	液体又は蒸気利用表面掃除機器	○	—
JISC9335-2-55	水槽用及び庭池用電気機器	汚泥吸引機器	(左記以外の機器)
JISC9335-2-56	プロジェクタ及びこれに類する機器	フィルムビューワ、手動フィルムストリップ映写機、手動スライド映写機、マイクروسコープ映写機、オーバヘッドプロジェクタ、反射投影機、写真引伸し器、写真複製器、半自動フィルムストリップ映写機、半自動スライド映写機、スライド仕分け器、ビューワ	(左記以外の機器)
JISC9335-2-58	業務用食器洗浄機	—	○
JISC9335-2-59	電撃殺虫器	—	○
JISC9335-2-60	渦流浴槽機器、渦流スパ及びこれらに類する機器	—	○
JISC9335-2-61	蓄熱形ルームヒータ	—	○

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-64	モータ駆動の業務用ちゅう（厨）房 機器	—	○
JISC9335-2-65	空気清浄機	—	○
JISC9335-2-66	ウォータベッド用ヒータ	—	○
JISC9335-2-67	工業用及び業務用床処理並びに床磨 き機	○	—
JISC9335-2-71	動物ふ卵及び飼育用電熱器具	—	○
JISC9335-2-73	固定形浸せきヒータ	—	○
JISC9335-2-74	可搬形浸せきヒータ	○	かいばおけなどの動物用水桶の凍結防止用の機器
JISC9335-2-75	業務用ディスペンサ及び自動販売機	—	○
JISC9335-2-76	電気さく用電源装置	—	○
JISC9335-2-77	手押し式制御芝刈り機	○（規格には未記載であるが社会通念的な判断 のもと判別）	—
JISC9335-2-78	屋外用バーベキュー台	—	○
JISC9335-2-79	高圧洗浄機及びスチーム洗浄機	○（規格には未記載であるが社会通念的な判断 のもと判別）	—
JISC9335-2-80	ファン	—	○
JISC9335-2-81	足温器及び電熱マット	—	○
JISC9335-2-82	サービス機器及びアミューズメント 機器	—	○
JISC9335-2-83	電熱式雨どい凍結防止器	—	○

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-84	トイレ機器	—	○
JISC9335-2-85	ファブックスチーマ	○ (規格には未記載であるが社会通念的な判断のもと判別)	—
JISC9335-2-88	暖房, 換気, 冷房装置用加湿器	—	○
JISC9335-2-89	業務用冷凍冷蔵機器	—	○
JISC9335-2-90	業務用電子レンジ	(右記以外の機器)	開始時間をあらかじめ選択できる電子レンジ及び保温機能を持つ電子レンジ
JISC9335-2-91	電気後押し式及び手持ち式の芝刈り込み機及び芝縁刈り込み機	○ (規格には未記載であるが社会通念的な判断のもと判別)	—
JISC9335-2-92	歩行式芝生用スカリファイア及びエアレータ	○ (規格には未記載であるが社会通念的な判断のもと判別)	—
JISC9335-2-94	はさみ形草刈り機	○ (規格には未記載であるが社会通念的な判断のもと判別)	—
JISC9335-2-96	室内暖房のためのシート状の可とう性電熱素子及びこれを用いる機器	—	○
JISC9335-2-98	加湿器	—	○
JISC9335-2-100	手持形のガーデンブロワ, バキューム及びブロワバキューム	(規格には未記載)	(規格には未記載)
JISC9335-2-101	電気くん蒸器	—	○
JISC9335-2-102	商用電源に接続するガス, 石油及び固形燃料燃焼機器	手動操作火花点火回路	(左記以外の機器)

該当 JIS 規格番号	家庭用及びこれに類する電気機器 (分類)	人の注意が行き届く状態で動作する機器	人の注意が行き届かない状態で動作する機器
JISC9335-2-105	多機能シャワーキャビネット	(規格には未記載)	(規格には未記載)
JISC9335-2-106	電気カーペット及び取外し可能な床 仕上げ材の下に設置する室内暖房用 ヒーティングユニット	—	○

2) 個別機器の対策検討とガイドラインに向けた整理

個別機器に対し、①配慮すべき危険源、②考慮すべきリスク、③リスク低減対策の3つの観点から機器側に求める内容やリスクを低減させる方策、消費者への注意喚起の内容などについて検討を深め、ガイドライン策定に向けた整理を行った。

検討に当たっては、「IoT（すなわち、機器の遠隔操作）とセーフティ」にまで視野を広げ、機能安全やセキュリティについては、この中の個別の主題として検討を実施した。

機能安全については、電気用品等製品については、「ソフトウェアを用いた安全機能」として捉えている。安全機能に組み込まれたソフトウェアは利用者が一切の変更を加えることができないため、IoT化においては安全機能に組み込まれたソフトウェアに対する格別の保護が求められることになる。これを踏まえ、機能安全については、ユースケース／リスクシナリオの事例に基づく検討を行うのではなく、大前提として「安全機能と通信回線との関わり」がどうあるべきかを検討することとした。

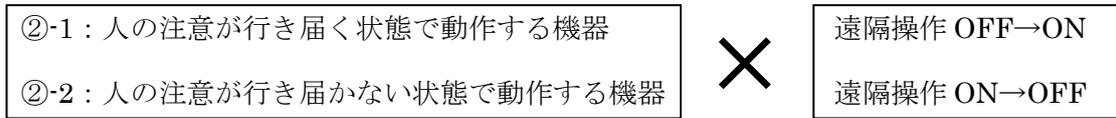
他方でそれ以外の機能については、常に重大製品事故を生じないということを念頭に置いた上で、ガイドライン策定に向けて求めるべき方策・対策の在り方を実態に基づいて検討するために、IoT化された電気用品等のユースケース／リスクシナリオの例示を検討することに取り組んだ。この例示においては、製品種別毎に、人に危害を及ぼすユースケース／リスクシナリオの事例を示した。さらに、方策・対策の在り方の議論に資するべく、スリーステップメソッドの観点（本質的安全設計、安全機能による保護、使用上の注意）から、個々の事例に対し、方策・対策の一例（案）を検討して取りまとめた。なお、セキュリティについては、「意図せざる遠隔操作」の1つの形態として位置付けることとしたため、ユースケース／リスクシナリオの事例においては、一貫して「意図せざる遠隔操作」を示す用語を用いている。

ところで、電気用品安全法では、「機器をOFF→ONすることによりリスクが高まる」という前提に基づき、遠隔操作で機器をOFF→ONにすることを選択的に規制している。換言すれば、機器は停止させると安全に帰着するというフェールセーフの考え方が活かされていると言える。しかし、実際には連続的に稼働していることで人の安全を守っている機器も存在しており、この場合は機器のON→OFFが人への危害を生じることになる。さらに、「IoTとセーフティ」を検討する上では、遠隔操作を行う者が機器の見えない位置にいるため、「機器のON→OFFに失敗したことに気付かない」「連続運転している機器が意図せざる遠隔操作でON→OFFされたことに気付かない」等の新たなリスクが発生しうる。これらを考慮し、本調査では、電気用品安全法の規制範囲を超えて、遠隔操作によるON→OFFのリスクも検討範囲に含めることとする。

ガイドラインの検討に向けては、1)の「機器の『遠隔操作』リスクの分類」と上記の「遠隔操作OFF→ONとON→OFFの分類」という2つの分類軸が存在しており、それぞれの分類軸についてリスクの特性が異なるものと考えられる。そこで、本調査においては、この2つの分類軸を掛け合わせたマトリックスで構成されるフレームワークを設定し、その区分毎にリスクシナリオ／ユースケースの事例を分類・整理することとした。これによって、区画毎に個別に望ましい方策・対策を検討することができるようになり、今後のガイドライン検討に資するものと思量される。

本調査で取り入れた検討フレームワークの考え方を下記に示す。

- ① 遠隔操作が禁止又は事実上禁止されている機器
- ② ①に当たらない機器



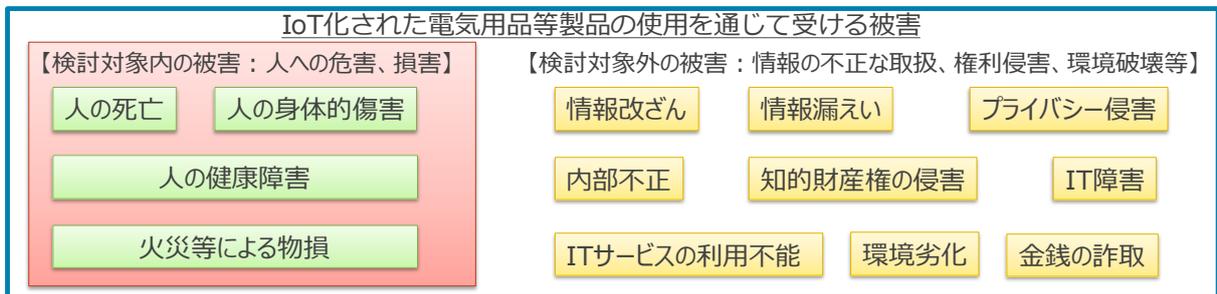
(ア) 検討対象とするリスクの範囲

本検討では、対象を人に危害を及ぼすリスク（死亡、身体的傷害、健康障害、火災等による物損）に限定して、検討をすすめる。

また、検討に際しては、消費生活用製品安全法に規定する重大製品事故を生じさせないことを念頭に置く。

なお、今後のIoT化の進展を踏まえ、「人への危害」には、生活環境の変化に伴い熱中症を引き起こし、体調を崩すことなども遠隔操作の誤操作による二次被害と考え、これを含んだ整理とする。但し、二次被害に関しては、今後より定義を明確化させた上で、被害を法的にどのような基準で捉えるか等を検討していく必要がある。

図表 33 IoT化された電気用品等製品の仕様を通じて受ける被害



重大製品事故の定義については、消費生活用製品安全法第2条第6項によると、以下の①及び②に示される危害が発生するような製品事故は、重大製品事故と判断される。

- ①一般消費者の生命又は身体に対する危害が発生した事故のうち、危害が重大であるもの。
 - ・死亡事故
 - ・重傷病事故（治療に要する期間が30日以上を負傷・疾病）
 - ・後遺障害事故
 - ・一酸化炭素中毒事故

②消費生活用製品が滅失し、又はき損した事故であって、一般消費者の生命又は身体に対する重大な危害が生ずるおそれのあるもの。

・火災（消防が確認したもの）

(イ) 遠隔操作リスクの高低を分類する考え方

IEC60335-1 及び IEC60335-2-xx シリーズにおける『遠隔操作』に関係のある部分を抽出すると、「遠隔操作を禁止又は事実上禁止されている機器」と「それ以外の機器」に分類され、後者はさらに「人の注意が行き届く状態で動作する機器」と「人の注意が行き届かない状態で動作する機器」に細分される。

- ①遠隔操作を禁止又は事実上禁止されている機器
- ②遠隔操作が可能な機器：
 - ②-1 人の注意が行き届く状態で動作する機器
 - ②-2 人の注意が行き届かない状態で動作する機器

今後、ユースケース、リスクシナリオ及び方策・対策の検討を進める機器の決め方を考えるにあたり、さらには各個別機器での配慮すべき危険源、考慮すべきリスク、リスク低減対策などを検討するにあたり、下図のような定義づけが求められてくる。

図表 34 遠隔操作リスクの高低を分類する考え方

分類方法		定義づけの考え方
① 遠隔操作を禁止又は事実上禁止されている機器（5ページ参照）		IEC60335-2-xxの22.40項、22.109項の規定等）： IEC規格において遠隔操作を禁止又は事実上禁止されている機器 →据え置き型コンロ、可視赤熱放射ヒータ等
② 遠 隔 操 作 が 可 能 な 機 器	②-1 人の注意が行き届く状態で動作する機器*	(1) IEC60335-2-xxの19.7項の規定： 手持型機器、手又は足でスイッチを入れ続けなければならない機器、手によって連続負荷をかけ続ける機器 (2) IEC60335-2-xxの30.2.2項の規定： 人の注意が行き届く状態で動作することを前提として耐熱性及び耐火性に関する試験の要求事項を定めた30.2.2項が適用される機器
	②-2 人の注意が行き届かない状態で動作する機器*	IEC60335-2-xxの30.2.3項の規定： 人の注意が行き届かない状態で動作することを前提として耐熱性及び耐火性に関する試験の要求事項を定めた30.2.3項が適用される機器

*IEC60335-2-xxの対象機器であっても、タイマー、使用用途等の違いで「人の注意が行き届く状態で動作する機器」と「人の注意が行き届かない状態で動作する機器」に分かれている（詳細は参考資料3参照）。この2つの分類は明確であるべき（概念、用語の定義等）とのご意見があり、さらに検討が必要。

また、「人の注意が行き届く状態で動作する機器かどうか」×「遠隔操作の種別（OFF→ON or ON→OFF）」の2×2マトリクス+「IEC規格において遠隔操作を禁止又は事実上禁止されている機器」の行を検討のためのフレームワークとして設定し、各区分に対して個別機器毎にユースケース/リスクシナリオの事例を当てはめて検討を行う（図表 35）。なお、遠隔操作には、当該機器が周辺環境に変化を与える温度を調節する機能も含める。

図表 35 の分類については、何名かの検討会委員より課題についてご指摘をいただいた。これらのご指摘は、まずは②-1 と②-2 を明確に分類できる方策が必要ということで共通している。このためには、IEC の国際標準にならって用語の定義を明確にすること、人が見ていれば大丈夫といったルール付けを行うこと、人が機器の傍を離れることを可能にする機能（例：協調安全機

能（人間が近くにいるかどうかで動作を変える機能）、予防安全機能等）の具備を考慮すること等が考えられ、今後さらに検討していくことが求められる。

図表 35 対応策例の検討のフレームワーク

電気用品安全法等のカバレッジ		遠隔操作	
		OFF→ON	ON→OFF
遠隔操作が可能な機器	人の注意が行き届く状態で動作する機器 例：ミシン、電気アイロン、マッサージ器、電気かみそり、毛髪バリカン等	遠隔操作の諾否：… 法令（電安法等）で求められている要件 ⁴⁵ の充足を精査（機器毎） IEC60335-1 の改訂作業及び SOTIF の概念から盛り込むべき内容を検討（機器毎）	遠隔操作の諾否：… 法令に囚われず、必要なリスク低減対策 ⁴⁶ を検討 IEC60335-1 の改訂作業及び SOTIF の概念から盛り込むべき内容を検討（機器毎）
	人の注意が行き届かない状態で動作する機器 例：エアコン、除湿機、電気カーペット、電気洗濯機、回転ドラム式電気乾燥機、貯湯式電気温水器、ファン等	遠隔操作の諾否：… 法令（電安法等）で求められている要件 ⁴⁷ の充足を精査（機器毎） IEC60335-1 の改訂作業及び SOTIF の概念から盛り込むべき内容を検討（機器毎）	遠隔操作の諾否：… 法令に囚われず、必要なリスク低減対策 ⁴⁸ の概念から盛り込むべき内容を検討（機器毎） IEC60335-1 の改訂作業及び SOTIF の概念から盛り込むべき内容を検討（機器毎）
IEC 規格において遠隔操作を禁止又は事実上禁止されている機器		据え置き型コンロ、可視赤熱放射ヒータ等	

3) 機能安全にソフトウェア評価が求められている機器

JIS の製品別安全規格及びこれより新しい最新の IEC 規格について調査し、ソフトウェアを用いた安全機能（機能安全）の評価が要求されている製品を抽出した（図表 36）。これらの機器については、今後、安全機能と通信回線を分離する方向で検討することが考えられる。またこれらは、その安全確保にあたり積極的にソフトウェアが適用される機器ともみなせるので、遠隔からの意図しない操作を防止する設計にも気を配る必要がある。

⁴⁵ 遠隔操作に伴う危険源がない又はリスク低減対策の実施と評価、通信回線が故障等しても機器は安全状態を維持、手元操作最優先、容易な通信回線の切り離し、2 か所以上からの遠隔操作を受け付けない対策、適切な誤操作防止対策、出荷時の遠隔操作機能の無効化等

⁴⁶ 機器が遠隔操作できることによる遠隔操作者による過信、機器の近くにいる人による意図しない操作、高齢者など生活弱者が自力で近くにある機器を操作することが困難な場合等を防止する対策（機器が動作していることの可視化、リスクアセスメント、取扱説明書の充実等）を実施

⁴⁷ 遠隔操作に伴う危険源がない又はリスク低減対策の実施と評価、通信回線が故障等しても機器は安全状態を維持、手元操作最優先、容易な通信回線の切り離し、2 か所以上からの遠隔操作を受け付けない対策、適切な誤操作防止対策、出荷時の遠隔操作機能の無効化等

⁴⁸ 法令で求められている要件以外に方策・対策として何が必要かを検討

図表 36 機能安全にソフトウェア評価が求められている機器

調査した規格名 (JIS/IEC)	最新の IEC 規格名	記載 箇所	規格の要求事項	機能安全に関する要求事項
JIS C 9335-2-2:2004 家庭用及びこれに類する 電気機器の安全性－第 2-2 部：真空掃除機及び 吸水式掃除機の個別要求 事項	IEC60335-2-2:2019 Household and similar electrical appliances - Safety - Part 2-2: Particular requirements for vacuum cleaners and water-suction cleaning appliances	Annex B 22.201	Mobile parts of automatic battery-operated cleaners shall be equipped with - a device to stop movement within 1 s of accessible hazardous moving parts when they lose contact with the surface being cleaned; and - a device to protect the appliance from dropping off the cleaning surface (e.g. stairways etc). When the mobile part senses that it has reached a critical edge, it shall - stop; or - reverse and move away from the edge of the cleaning surface and then continue to operate normally.	If the electronic circuit is programmable, the software shall contain measures to control the fault/error conditions specified in Table R.1. and is evaluated in accordance with the relevant requirements of Annex R.
	Annex B Appliances powered by rechargeable batteries that are recharged in the appliances	Annex S Battery-operated appliances powered by batteries that are non-rechargeable or not recharged in the appliances	Annex S 22.201	Same as Annex B 22.201
JIS C 9335-2-4:2017 家庭用及びこれに類する 電気機器の安全性－第 2-4 部：電気脱水機の個 別要求事項	IEC 60335-2-4:2018 Household and similar electrical appliances-Safety- Part 2-4: Particular requirements for spin extractors	20.103	次のいずれかの機器は、ドラムが動作している間、 蓋が開かない構造でなければならない。	プログラマブル電子回路の場 合、ソフトウェアは、表 R.1 で 規定する故障/エラー状態を制 御する手段を含まなければなら ず、附属書 R の関連した要求事 項に従って評価する。
		20.104	運動エネルギーが 1500 J 以下で、かつ、次に規定 する最大周速度以下のものは、モータの動作中又 はドラム速度が毎分 60 回転を超えるときに、運動 部に触れることが可能であってはならない。	プログラマブル電子回路の場 合、ソフトウェアは、表 R.1 で 規定する故障/エラー状態を制 御する手段を含まなければなら ず、附属書 R の関連した要求に 従って評価する。
JIS C 9335-2-6:2004 家庭用及びこれに類する 電気機器の安全性－第 2 －6 部：据置形ホブ、オー ブン、クッキングレンジ 及びこれらに類する機 器の個別要求事項	IEC 60335-2- 6:2014/AMD1:2018 Amendment 1 - Household and similar electrical appliances - Safety - Part 2- 6: Particular requirements for stationary cooking ranges, hobs, ovens and similar appliances	22.102	Remote operation and timers intended to delay the operation of a heating element shall not control a grill, unless the grill is thermally controlled, incorporated to operate the grill with the door of the oven or compartment being closed.	Compliance is checked by inspection. However, if monitoring of the door is by a programmable electronic circuit, the software shall contain measures to control the fault/error conditions specified in Table R.1 and is evaluated in accordance with the relevant requirements in Annex R.
JIS C 9335-2-7:2017 家庭用及びこれに類する 電気機器の安全性－2-7 部：電気洗濯機の個別要 求事項	IEC60335-2-7:2019 Household and similar electrical appliances - Safety - Part 2-7: Particular requirements for washing machines	20.104	ドラムの速度が 60 r/min を超えている間、機器の 蓋又はドアは、開いてはならない。ただし、ドラム が 1 500 J を超える回転運動エネルギーをもつか、 又は次の最大周速を超える場合に限る。 － 水平軸の周りを回転するドラムの場合、20 m/s － 垂直軸の周りを回転するドラムの場合、40 m/s	プログラマブル電子回路の場 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んでいな ければならない。また、附属書 R の関連要求事項に従って評価し なければならない。
		20.105	機器には、蓋又はドアが開いたときに、モータのス イッチを切るか又は 60 r/min までドラム速度を下 げる自動装置をもっていなければならない。ただ し、ドラムの回転運動エネルギーが 1 500 J 以下 か、又は次の最大周速以下の場合に限る。 － 水平軸の周りを回転するドラムの場合、20 m/s － 垂直軸の周りを回転するドラムの場合、40 m/s 注記 回転運動エネルギーは、20.104 の式に基づき 算出する。	同上

調査した規格名 (JIS/IEC)	最新の IEC 規格名	記載 箇所	規格の要求事項	機能安全に関する要求事項
JIS C 9335-2-7:2017 家庭用及びこれに類する 電気機器の安全性－2-7 部：電気洗濯機の個別要 求事項（続き）	IEC60335-2-7:2019 Household and similar electrical appliances - Safety - Part 2-7: Particular requirements for washing machines（続き）	22.101	機器中の水位が、ドアの開口部の低い方の縁を超えている場合、機器が動作している間、単純な操作によってドアが開放されてはならない。この要求事項は、インターロックが作動したドア、又はキーによって、若しくは押し、回しなどの2回の個別動作によって開くようなドアを取り付けた機器には、適用しない。	同上
※2017年の規格にはない部分	※後から追記	22.108	For appliances that are controlled by programmable electronic circuits that limit the number of heating elements and motors from being and energised at the same time, simultaneous activation of any combination of heating elements and motors shall not render the appliance unsafe.	Compliance is checked as follows: -the fault/error conditions specified in Table R.1 are applied and evaluated in accordance with the relevant requirements of Annex R or -the appliance is operated under the conditions of Clause 11 while being supplied rated voltage, the programmable electronic circuits being modified to allow simultaneous activation of all heaters and motors under their control. under these conditions, compliance with 19.13 shall be fulfilled.
JIS C 9335-2-9:2017 家庭用及びこれに類する 電気機器の安全性－第2 －9部：可搬形ホブ、オー プン、トースタ及びこれ らに類する機器の個別 要求事項	IEC 60335-2-9:2019 Household and similar electrical appliances - Safety - Part 2-9: Particular requirements for grills, toasters and similar portable cooking appliances	22.115	電子回路によって制御する発熱体を一つ以上もつこ んろを組み込んでいる機器の場合、電子回路の故障 時に安全性が損なわれてはならない。	要求事項に適合するために使用 するソフトウェアは、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んでい なければならない。また、附属書 R の関連要求事項に従って評価し なければならない。
JIS C 9335-2-11:2017 家庭用及びこれに類する 電気機器の安全性－第2 －11部：回転ドラム式 電気乾燥機の個別要求事 項	IEC60335-2-11:2019 Household and similar electrical appliances - Safety - Part 2-11: Particular requirements for tumble dryers	20.104	開口部が 200 mm を超える垂直面のドアをもち、 ドラム内容積が 60 dm ³ を超える機器は、ドラムの 動作を制御する別個の手段を手によって操作するま で、ドアを開めた後にドラムモータを始動するこ とができてはならない。 注記1 容積は、ドラムの最大深さと最大内径と から計算できる。	プログラマブル電子回路の場 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んでい なければならない。また、附属書 R の関連要求事項に従って評価し なければならない。
※2017年の規格にはない部分	※後から追記	22.108	For appliances that are controlled by programmable electronic circuits that limit the number of heating elements and motors from being and energised at the same time, simultaneous activation of any combination of heating elements and motors shall not render the appliance unsafe.	Compliance is checked by the following test. -the fault/error conditions specified in Table R.1 are applied and evaluated in accordance with the relevant requirements of Annex R or -the appliance is operated under the conditions of Clause 11 while being supplied rated voltage, the programmable electronic circuits being modified to allow simultaneous activation of all heaters and motors under their control. Under these conditions, compliance with 19.13 shall be fulfilled.
JIS C 9335-2-14:2005 家庭用及びこれに類する 電気機器の安全性－第 2-14部：ちゅう房機器 の個別要求事項	IEC 60335-2-14:2016 Household and similar electrical appliances – Safety – Part 2- 14 : Particular requirements for kitchen machines	20.101	Accessories for cream whippers, egg beaters and hand-held food mixer shall not have knife edges, unless a suitable guard prevents accidental contact with their rotating parts. It shall not be possible to release beaters, kneaders and similar accessories of hand-held food mixer by pressing a button or a similar action while the accessory is rotating at a speed exceeding 1500 r/min.	If the electronic circuit is programmable, the software shall contain measures to control the fault/error conditions specified in Table R.1 and is evaluated in accordance with the relevant requirements of Annex R.

調査した規格名 (JIS/IEC)	最新の IEC 規格名	記載 箇所	規格の要求事項	機能安全に関する要求事項
JIS C 9335-2-21:2019 家庭用及びこれに類する 電気機器の安全性－第 2 － 2 1 部：貯湯式電気温 水器の個別要求事項	IEC 60335-2- 21:2012/AMD1:2018 Amendment 1 - Household and similar electrical appliances - Safety - Part 2- 21: Particular requirements for storage water heaters	24.102.1	温度制御を電子回路に依存する場合、試験は、別に 適用する次の状況の下で繰り返す。 － 19.11.2 の a)～g)による故障状態を、一つずつ電 子回路に適用する。 － 19.11.4.1～19.11.4.7 によるイミュニティ試験を 機器に適用する。 出湯口の水の温度は、各々の試験中及び試験後であ っても、99 °Cを超えてはならない。	プログラマブル電子回路を用い る場合、ソフトウェアは、表 R.1 による故障/エラー状態を制御 する手段を含んでいなければな らない。附属書 R による関連要 求事項に従って評価する。
JIS C 9335-2-27:2005 家庭用及びこれに類する 電気機器の安全性－第 2-27 部：紫外線及び赤 外線による皮膚照射用装 置の個別要求事項	IEC 60335-2-27:2019 RLV Household and similar electrical appliances Safety Part 2-27 : Particular requirements for appliances for skin exposure to ultraviolet and infrared radiation	22.105	UV appliances that are inclined at an angle of more than 35° to the vertical shall be constructed so that the emission of ultraviolet radiation is stopped if the timer fails.	If the electric circuit is programmable, the software shall contain measures to control the fault/error conditions specified in Table R.1 and is evaluated in accordance with the relevant requirements of Annex R.
		22.112	Appliances fitted with UV filters shall be constructed so that the emission of UV radiation is not increased if the filter is removed.	上に同じ
JIS C 9335-2-35:2019 家庭用及びこれに類する 電気機器の安全性－第 2 － 3 5 部：瞬間湯沸器の 個別要求事項	IEC 60335-2- 35:2012/AMD1:2016 Amendment 1 - Household and similar electrical appliances - Safety - Part 2- 35: Particular requirements for instantaneous water heaters	22.105	フローズスイッチを組み込んだ出口開放形湯沸器は、 水の流れがない場合、発熱体への通電ができてはな らない。また、水の流れが止まった場合、発熱体へ の通電を遮断する構造でなければならない。	プログラマブル電子回路を用い る場合、ソフトウェアは、表 R.1 による故障/エラー状態を制御 する手段を含んでいなければな らない。附属書 R による関連要 求事項に従って評価する。
		22.108	瞬間湯沸器の出湯は、給水圧力の突発的な低下があ っても過度な温度になってはならない。	プログラマブル電子回路を用い る場合、ソフトウェアは、表 R.1 による故障/エラー状態を制御 する手段を含んでいなければな らない。附属書 R による関連要 求事項に従って評価する。
JIS C 9335-2-40:2004 家庭用及びこれに類する 電気機器の安全性－第 2 － 4 0 部：エアコンディ ションナ及び除湿機の個別 要求事項	IEC 60335-2-40:2018 Household and similar electrical appliances - Safety - Part 2-40: Particular requirements for electrical heat pumps, air-conditioners and dehumidifiers	22.46	Same as the requirements of IEC60335-1.	Modification: Add after the 1st paragraph: if the protective electronic circuit software is a part of the normal operation control, inspection of software shall be limited to relevant source code of safety controls or related software controls. Alternative methods may be used if they demonstrate equivalent levels of safety.
JIS C 9335-2-53:2015 家庭用及びこれに類する 電気機器の安全性－第 2-53 部：サウナ用電熱 装置及び赤外線キャビン の個別要求事項	IEC 60335-2-53:2017 Household and similar electrical appliances-Safety- Part 2-53: Particular requirements for sauna heating appliances and infrared cabins	22.108	For prefabricated saunas that incorporate a stand-by mode setting for remote operation, the door shall be fitted with an interlock such that the stand-by mode setting for remote operation is disabled if the sauna door is opened when stand- by mode setting for remote operation is set. This requirement also applies for the time pre- selection mode.	If the electric circuit is programmable, the software shall contain measures to control the fault/error conditions specified in Table R.1 and is evaluated in accordance with the relevant requirements of Annex R.
JIS C 9335-2-58:2019 家庭用及びこれに類する 電気機器の安全性－第 2- 58 部：業務用食器洗浄 機の個別要求事項	IEC 60335-2-58:2017 RLV Household and similar electrical appliances – Safety – Part 2-58: Particular requirements for commercial electric dishwashing machines	22.109	同時通電される電熱素子及びモータの数を制限する プログラマブル電子回路によって制御される機器の 場合には、電熱素子及びモータの全ての組合せにお ける同時駆動が、機器を不安全な状態にしてはなら ない。	適否は、次のいずれかによって 判定する。 － 表 R.1 に規定する故障/エラ ー状態が、附属書 R の関連する 要求事項に適合することを評価 する。 － 箇条 11 に規定する条件の 下、定格電圧で機器を運転し、 プログラマブル電子回路を修正 して、全ての電熱素子及びモー タを同時駆動させる。この条件 下で、機器が 19.13 に適合する ことを評価する。

調査した規格名 (JIS/IEC)	最新の IEC 規格名	記載 箇所	規格の要求事項	機能安全に関する要求事項
JIS C 9335-2-76:2017 家庭用及びこれに類する 電気機器の安全性 - 第 2-76 部 : 電気さく用電 源装置の個別要求事項	IEC 60335-2-76:2018 Household and similar electrical appliances-Safety- Part 2-76: Particular requirements for electric fence energizers	22.46	Same as the requirements of IEC60335-1.	If programmable protective electronic circuits alone are used to ensure compliance with the output characteristics specified in 19.13, the software shall contain measures to control the fault/error conditions specified in Table R.2.
JIS C 9335-2-82:2017 家庭用及びこれに類する 電気機器の安全性 - 第 2-82 部 : サービス機器 及びアミューズメント機 器の個別要求事項	IEC 60335-2-82:2017 Household and similar electrical appliances-Safety- Part 2-82: Particular requirements for amusement machines and personal service machines	22.106	For appliances that are controlled by programmable electronic circuits that limit the number of heating elements and motors from being energised at the same time, simultaneous activation of any combination of heating elements and motors shall not render the appliance unsafe.	The fault/error conditions specified in Table R.1 are applied and evaluated in accordance with the relevant requirements of Annex R; or ...
JIS C 9335-2-84:2019 家庭用及びこれに類する 電気機器の安全性 - 第 2-84 部 : トイレ機器の 個別要求事項	IEC 60335-2-84:2019 RLV Household and similar electrical appliances-Safety- Part 2-84: Particular requirements for toilet appliances	22.105	For appliances that are controlled by programmable electronic circuits that limit the number of heating elements and motors from being energised at the same time, simultaneous activation of any combination of heating elements and motors shall not render the appliance unsafe.	The fault/error conditions specified in Table R.1 are applied and evaluated in accordance with the relevant requirements of Annex R; or ...
JIS C 9335-2-89:2005 家庭用及びこれに類する 電気機器の安全性 - 第 2-89 部 : 業務用冷凍冷 蔵機器の個別要求事項	IEC 60335-2-89:2019 Household and similar electrical appliances - Safety - Part 2- 89: Particular requirements for commercial refrigerating appliances with an incorporated or remote refrigerant condensing units or compressor	22.116	Appliances having a refrigerant charge exceeding 150 g of flammable refrigerant in any refrigerating circuit shall be constructed such that a leak of refrigerant shall not result in a flammable refrigerant concentration surrounding the appliance, In the event of leak from the appliance while energised, if airflow is required to meet these requirements, the airflow shall be guaranteed. If airflow is not maintained at a level of sufficient to comply with the requirements of Annex CC, the motor-compressors and heating elements shall be switched off within 5 minutes and an alarm shall be given. The motor-compressor and heating elements shall only be capable of restarting after the required airflow level has been reinstalled.	If the electric circuit is programmable, the software shall contain measures to control the fault/error conditions specified in Table R.1 and is evaluated in accordance with the relevant requirements of Annex R.
JIS C 9335-2-90:2019 家庭用及びこれに類する 電気機器の安全性 - 第 2-90 部 : 業務用電子レ ンジの個別要求事項	IEC 60335-2- 90:2015+AMD1:2019 CSV Household and similar electrical appliances-Safety- Part 2-90: Particular requirements for commercial microwave ovens	22.121	For appliances that are controlled by programmable electronic circuits that limit the number of heating elements and motors from being energised at the same time, simultaneous activation of any combination of heating elements and motors shall not render the appliance unsafe.	The fault/error conditions specified in Table R.1 are applied and evaluated in accordance with the relevant requirements of Annex R; or ...
JIS C 9335-2-102:2017 家庭用及びこれに類する 電気機器の安全性 - 第 2- 102 部 : 商用電源に接続 するガス、石油及び固形 燃料燃焼機器の個別要求 事項	IEC60335-2-102:2017 Household and similar electrical appliances - Safety - Part 2-102: Particular requirements for gas, oil and solid-fuel burning appliances having electrical connections	22.46 ※JISで は削除さ れている	Same as the requirements of IEC60335-1.	Software used in protective electronic circuits to ensure compliance with this standard for gaseous and liquid fuels shall be software that contains measures to control the fault/error conditions specified in Table R.2.
JIS C 9335-2-105:2007 家庭用及びこれに類する 電気機器の安全性 - 第 2-105 部 : 多機能シャワ ーキャビネットの個別要 求事項	IEC 60335-2- 105:2016+AMD1:2019 CSV Household and similar electrical appliances Safety Part 2-105 : Particular requirements for multifunctional shower cabinets	22.103	For appliances that are controlled by programmable electronic circuits that limit the number of heating elements and motors from being energised at the same time, simultaneous activation of any combination of heating elements and motors shall not render the appliance unsafe.	The fault/error conditions specified in Table R.1 are applied and evaluated in accordance with the relevant requirements of Annex R; or ...

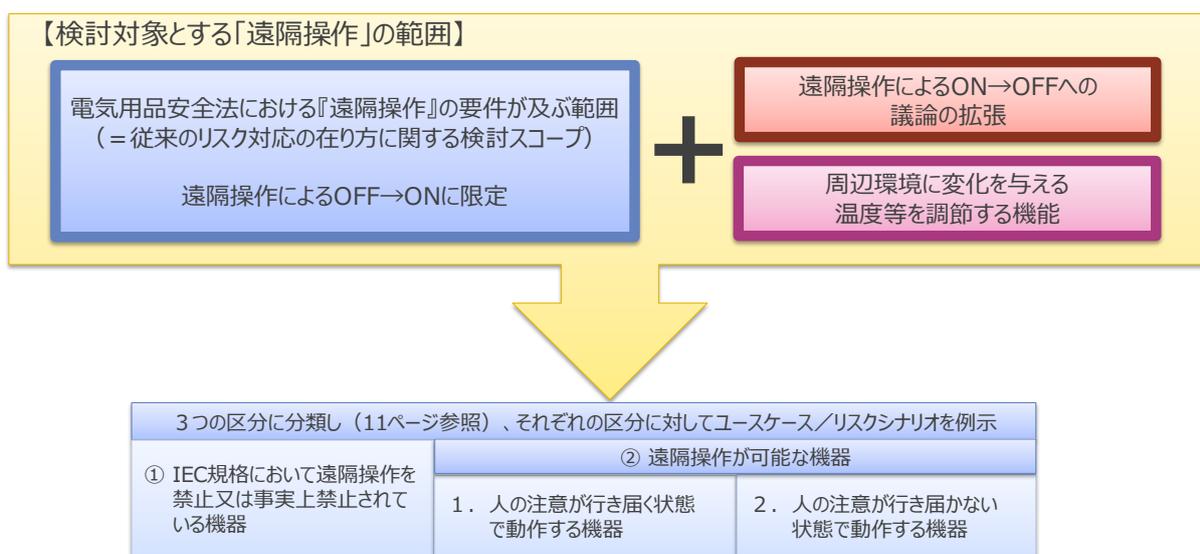
※英語で記載されている箇所は、IEC 規格の方が新しく、まだ JIS 化されていない基準を示している。

4) IoT 化された電気用品等のユースケース／リスクシナリオの例示

遠隔操作のリスク対応について広く議論するための素材として、以下では、IoT 化された電気用品等のユースケース／リスクシナリオの例示に取り組む。

今回、遠隔操作の対象範囲として、「OFF→ON」に留まらず、「ON→OFF」や「周辺環境に変化を与える温度等を調節する機能」までも対象とし、「遠隔操作が事実上禁じられている機器」「人の注意が行き届く状態で動作する機器」「人の注意が行き届かない状態で動作する機器」の分類毎に例示を検討する（図表 37）。

図表 37 議論の素材として例示する範囲



一方、遠隔操作する人が機器及び周辺の状況を目で確認できないことから、通信回線や機能の信頼性・性能限界を過信する（または遠隔操作そのものを忘れる）と、気付かないうちに危険に陥る場合がある。同様に、機器の傍にいる人に不意の危害を与えてしまう恐れが生じる。今回の検討では、上記のような「利用者の過信」と「機器の傍らにいる別の人への不意の危害」にも十分に留意しながら、ユースケース／リスクシナリオの例示を行う（図表 38）。

図表 38 利用者の過信と不意の危害について



自動車業界では、車線はみ出しアラート、障害物お知らせ機能といった、ドライバーを支援して事故を未然に防ぐ先進機能を組み込むことを、「予防安全」と呼んでいる。

次ページ以降の各個別機器のユースケース／リスクシナリオを考える上では、通常利用する製品の機能（以後、「通常機能」という。）ではなく、自動車の機能と同様にリスク低減に一定の効果を発揮することを目的として組み込まれた機能（以後、「予防安全機能」という。）であるものが存在する。予防安全機能が組み込まれた機器の場合、予防安全機能を停止させると危険側となる。このため、遠隔操作で ON→OFF し、予防安全機能を停止させると人に危害が及ぶことも問題になる。

図表 39 予防安全機能について

<p>通常機能 ⇒ OFF→ONが危険側</p>	<p>※通常機能の信頼性や、遠隔操作ON→OFFを過信すると危険</p>
<p>予防安全機能 ⇒ ON→OFFが危険側</p>	<p>※予防安全機能の性能限界や、遠隔操作OFF→ONを過信すると危険</p>

また、自動車業界では「予防安全機能を過信せず（性能限界を超えないように）正しく使ってください」というような説明がされている。

(2) IoT化された電気用品等のユースケース／リスクシナリオ例

1) ユースケース／リスクシナリオの事例の取りまとめ結果

以下に、具体的なユースケース／リスクシナリオの事例取りまとめ結果を示す（図表 40、図表 41、図表 42、図表 43）。但し、「遠隔操作で ON→OFF × 人の注意が行き届く状態で動作する機器」の категорияについては、課題となる論点を提示するユースケース／リスクシナリオを例示することができなかつたことを付記しておく。

なお、以下で示すユースケース／リスクシナリオの事例は、関連する業界団体のレビューを受けて質の向上を図っているものの、さらに内容について吟味し、記述の正確性を高めていく必要がある。

(ア) 遠隔操作で OFF→ON × 人の注意が行き届く状態で動作する機器

図表 40 遠隔操作で OFF→ON × 人の注意が行き届く状態で動作する機器の例

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） ※現段階では例示であり今後要検討	備考
人の注意が行き届く状態で操作する機器 ・アイロン ・ミシン ・フードプロセッサ など	OFF→ONの遠隔操作中に近くに人がいることが分からず、機器が動作する。	不意な動作により、近くにいる人がけが又はやけどをする。	<p><本質的安全設計></p> <ul style="list-style-type: none"> 危険な部分を露出させないで目的を果たせるような画期的な製品を作る。 遠隔操作及び自動運転を禁止する。 （この問題点は、スマートプラグに対して注意。） <p>→ この件は、電気用品安全法では検討済みであるが、あえてガイドラインとして検討する必要があるか。</p> <p><安全機能による保護> - <使用者に対する注意> -</p>	<ul style="list-style-type: none"> 直接被害 機器の傍にいる人が操作に気付かず危害を受ける 遠隔操作の禁止に対し、議論の余地はほとんどない。

(注) 通信回線を使用するが見える位置からの操作を意図したアシスト機能等はこのなかに含まない。

(イ) 遠隔操作で OFF→ON × 人の注意が行き届かない状態で動作する機器

図表 41 遠隔操作で OFF→ON × 人の注意が行き届かない状態で動作する機器の例

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) ※現段階では例示であり、今後要検討	備考
ロボット掃除機	<p>家の中にいる人が、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。</p> <p>この家族が、買い物の間に掃除をすませようと、警告表示(備考参照)を破ってロボット掃除機を遠隔操作で OFF→ON したが、家の中にいた人はたまたまロボット掃除機が見えない位置にいた。</p>	<p>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人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。</p>	<p><本質的安全設計、使用者に対する注意> ロボット掃除機に停止用ストoppa又は通信回線切り離し用の機械的スイッチを用意し、意図せずに動く可能性を考慮して、電気ストーブなどを使用するときは、必ず停止用ストoppaを用いる又は通信回線の切り離しスイッチをOFFにすることを本体に表示する。 取扱説明書/注意書き等の表示媒体による啓発を行う。</p> <p>遠隔操作時(OFF→ON)に、走行経路で暖房機器等を使用していないかを、都度注意喚起する。</p> <p><安全機能による保護、使用者に対する注意> あらゆる危険物に対して動作するように障害物回避機能を安全機能として設計する。この場合、障害物回避機能の信頼性を評価し、かつ、通信機能と障害物回避機能を完全に分離する。 遠隔操作を切るスイッチを設け、取扱説明書等による啓発を行う。</p>	<p>間接被害</p> <ul style="list-style-type: none"> ■ 機器の傍にいる人が操作に気付かず、火災に至り、自分も危害にさらされる(あるいは危害を受ける) ■ 警告表示としては、一般に次のようなものがある。 <ul style="list-style-type: none"> -本体が接触して事故をまねくおそれのあるものは移動させる。 -本体を使用している部屋では、火気(火のついたろうそく、たばこ、線香、熱器具等)を使用しない。 -暖房器具(ストーブ)など高温になる電気製品がある室内では使わない。 ■ 次年度、議論を十分に深めやすいように、オブザーバーからいただいたコメントも併記した。
給湯機	<p>家族や子供を家に残して外出した人が、遠隔からお湯張り機能を OFF→ON した。</p> <p>その時たまたま子供が浴槽の中で遊んでいた。</p>	<p>浴槽で遊んでいた子供が、お湯が増えたことでおぼれてしまった。</p>	<p><本質的安全設計> 遠隔からは湯張り機能を使えないようにする。</p> <p><安全機能による保護> いきなり、お湯がいっぱいにならないように、湯はり速度を制限する。</p> <p><使用者に対する注意> 小さな子供が自宅にいるときは、遠隔からお湯張り機能をOFF→ONしないように周知する。</p>	<p>直接被害</p> <ul style="list-style-type: none"> ■ 機器の傍にいる子供が被害を受ける。

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） ※現段階では例示であり、今後要検討	備考
温風暖房機 （ガス・石油）	温風暖房機の上部に洗濯物を乾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。	<p><本質的安全設計> 可燃性物質が温風暖房機に触れても燃えない構造にする。</p> <p><安全機能による保護> 可燃性物質が温風暖房機にふれたとき温風暖房機を停止させる機能を装備する。</p> <p><使用者に対する注意> 温風暖房機の上部に洗濯物を乾さないように、周知する。</p>	間接被害 ■ 無人で目視確認ができない。
扇風機	普段、部屋干ししている洗濯物の乾燥を早めるために扇風機をつけている。通勤途中、扇風機のスイッチをONにしていないことに気が付いたため、遠隔操作で OFF→ON にした。	扇風機の羽根に触って遊んでいた子供が怪我をする ※子供が扇風機の羽根に触ることによるリスクは、遠隔操作時に限定されないため、取扱いに注意が必要。	<p><本質的安全設計> 子供の指が入らないように設計する。 扇風機の遠隔操作を禁止する。</p> <p><安全機能による保護> -</p> <p><使用上の注意> 遠隔操作により扇風機の傍にいる子供が危害を受ける可能性があることを分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。</p>	直接被害 ■ 機器の近くにいる子供が意図しない危害を受ける。
電気スタンド （ランプが露出している場合に限る）	長期間、旅行に出かけることになったため、空き家の状態が続いてしまう。新聞の購読の停止申請は済ませたが、不安はぬぐえないため、電気スタンドの遠隔操作機能を使用して夜間はスイッチを OFF→ON にすることで家に人がいるように見せることとした。 しかし、出かける際に、電気スタンドの近くに可燃物を掛けたり置いたりしたまま出かけてしまった。 一方、電気スタンドに使われるランプ(特に白熱灯)がとても明るいいため、その表面温度が高くなる。	（特にガード上部開放型の電気スタンドを使用している場合）ランプ（特に白熱灯）に新聞紙など可燃性物質が触れている状態で電気スタンドのスイッチがOFF→ONになることで火災となる。 または、地震等で電気スタンドが倒れたことで可燃性物質に触れている状態で遠隔操作によってスイッチがOFF→ONになることで火災となる。	<p><本質的安全設計> 電気スタンドの回りに一定時間、人、動物等がいない場合、自動的に照度が下がる。 使用者によってランプ交換ができる電気スタンドは、遠隔操作を禁止する。</p> <p><安全機能による保護> 電気スタンドが倒れたら自動的に消灯する安全機能を装備する。</p> <p><使用者に対する注意> 白熱灯への交換について、本体表示により注意喚起する。 ランプ(特に白熱灯)表面の温度が高く、可燃物に触れると火災になる可能性があることを分かりやすく周知する。周知方法は取扱説明書だけでは不十分。</p>	直接被害 ■ 無人で目視確認ができない。

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） ※現段階では例示であり、今後要検討	備考
ドラム式洗濯機・乾燥機	出かけた後でチャイルドロックを OFF→ON にし忘れたことに気付いたため、遠隔操作で OFF→ON に変更した。	通信障害（電池切れを含む）等により、チャイルドロックが実際には ON になっておらず、子供がドラムに入って閉じ込められ、窒息する。 ※遠隔操作に失敗してチャイルドロックが OFF になっていると、子供が閉じ込められることが考えられ、この場合、内側からフタを開けることができずより危険な状態である。	<p><本質的安全設計> –</p> <p><安全機能による保護> 子供が洗濯機の中に入った状態では、チャイルドロックは OFF→ON にできないようにする。また、遠隔操作した者に操作結果（ON に失敗等）をフィードバックする。</p> <p><使用者に対する注意> 通信故障等により、チャイルドロックを遠隔から OFF→ON できないことがあるため、遠隔操作を過信しないように使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。</p>	<p>直接被害</p> <ul style="list-style-type: none"> ■ 機器の傍にいたる子供が被害を受ける。 ■ 遠隔操作スタンバイ状態にする際、フタはロックされ、フタロックを遠隔操作で ON・OFF 設定することはできない。しかし、本事例では議論のため、フタロックはない仮の想定で例示している。
炊飯器	出かけた後で炊飯中のフタ自動ロック機能を OFF→ON にし忘れたことに気付いたため、遠隔操作で OFF→ON に変更した。	通信障害（電池切れを含む）等により、炊飯中のフタ自動ロック機能が実際には ON になっておらず、遠隔から炊飯器を OFF→ON して炊飯したところ、子供が炊飯中にフタ開閉ボタンを触ってフタが開き蒸気により火傷した。	<p><本質的安全設計> 炊飯中のフタ自動ロック機能に対する遠隔からの OFF→ON を禁止する。</p> <p><安全機能による保護> フタ自動ロック機能が OFF の状態では、遠隔操作ができないようにする。</p> <p><使用者に対する注意> 通信故障等により、炊飯中のフタ自動ロック機能を遠隔から OFF→ON できないことがあるため、遠隔操作を過信しないように使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。</p>	<p>直接被害</p> <ul style="list-style-type: none"> ■ 遠隔からの通常機能の操作と連携することで、機器の傍にいたる子供が被害を受ける。 ■ フタ自動ロック機能はすべての機種に搭載されている機能ではなく、ON/OFF を設定できる機能でもない。遠隔操作に限らず、予防安全機能として別途議論が必要。 ■ このユースケース/リスクシナリオは、議論することを目的として、事務局で仮想的に想定したもの。

(ウ) 遠隔操作で ON→OFF × 人の注意が行き届かない状態で動作する機器

図表 42 遠隔操作で ON→OFF × 人の注意が行き届かない状態で動作する機器の例

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） ※現段階では例示であり、今後要検討	備考
エアコン	エアコンが操作できない人が家に一人である状態で、エアコン以外の熱中症対策を特にせずに、遠隔からエアコンを操作していたところ、遠隔操作の誤操作により、エアコンの電源が ON→OFF されてしまった。	家にいたエアコンが操作できない人が熱中症となる。	<p><本質的安全設計> – <安全機能による保護> 誤操作防止対策として、電源 ON→OFF に対してもダブルアクションを追加する。</p> <p><使用者に対する注意> エアコンは熱さ対策として役立つ通常機能であり、熱中症対策の安全機能ではないことを使用者に分かりやすく説明する。例えば、エアコンは何らかの原因で停止する可能性があるため、部屋の温度が高温になる場合、エアコンが操作できない人を一人で長い時間部屋に居てもらうことは避けるように伝えるなど。</p> <p>（予防安全機能については、通常レベルでのセキュリティ対策は必要なものの、そもそも、エアコンを操作できないような人を長時間一人で放置しておいてもよいかという別観点での検討が必要。）</p>	間接的被害 ■ 機器の傍にいるエアコンが操作できない人が意図しない危害を受ける。
換気扇	外からの意図しない遠隔操作によって、常時換気の換気扇が停止させられた (ON→OFF)。建材等の対策が十分でなく、換気扇を常時運転することで健康被害を抑制していた。	建材などに含まれる化学物質が揮発し、室内に滞留 部屋に滞留した化学物質によって、めまい、吐き気、頭痛・眼・鼻・などの痛み等の症状が発生した。	<p><本質的安全設計> 建材等の対策を補う形で24時間運転が不可欠な換気扇については、遠隔操作を禁止する。</p> <p><安全機能による保護> 建材等の対策を補う形で24時間運転が不可欠な換気扇については、通常機能と通信回線を切り離す。</p> <p><使用者に対する注意> –</p>	間接的被害 ■ 機器の傍にいる人が意図しない健康被害を受ける。 ※健康被害を人への危害と同列に考えるか？

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） ※現段階では例示であり、今後要検討	備考
ドラム式洗濯機・乾燥機	洗濯機のチャイルドロックを操作し出かけたが、遠隔操作により間違えて操作してチャイルドロックが外れてしまい（ON→OFF）、そのことに気がつかなかった。	留守番していた子供が洗濯槽に入って閉じ込められた結果、窒息する。	<p><本質的安全設計> チャイルドロックは、遠隔操作による ON→OFF を禁止する。</p> <p><安全機能による保護> チャイルドロックを通信機能回路と完全に分離する。</p> <p><使用者に対する注意> —</p>	<p>直接被害</p> <ul style="list-style-type: none"> ■ 機器の傍にいる子供が被害を受ける。 ■ 遠隔操作スタンバイ状態にする際、フタはロックされ、フタロックを遠隔操作で ON・OFF 設定することはない。しかし、本事例では議論のため、フタロックはない仮の想定で例示している。 ■ 子供が入ることができる大きなドラムのもものは、扉の内側から子供の力でも開けることができるように基準が改正されている。

(エ) 遠隔操作で OFF→ON が禁止又は事実上禁止されている機器

図表 43 IEC 規格において遠隔操作を禁止又は事実上禁止されている機器の例

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) ※現段階では例示であり、今後要検討	備考
据置型 IH コンロ/ ガスコン ロ	あと 10 分程度で終了する調理の最中に少し離れた場所に住む親からすぐに来てほしいという連絡があった。スマートフォンで ON→OFF できる機能があったので、親の家に向かう途中の電車内で OFF すればよいと考えて、コンロを ON 状態のまま出かけた。	通信故障（電池切れを含む）等により、コンロを遠隔から OFF できない状態となり、最終的に鍋が焦げて火災となる。	<p><本質的安全設計> 遠隔からの操作を禁止する。</p> <p><安全機能による保護> 鍋等に対する高温検知機能により、コンロを OFF する。この場合、検知機能の信頼性評価が必要。</p> <p><使用者に対する注意> 遠隔からの OFF 操作は、万が一消し忘れたときに役立つ機能であるが、通信故障等により OFF 操作できないため、通常使用としては使用しない（安全機能としては機能しない）ことを分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。</p>	直接被害 ■ 無人で目視確認ができない。
据置型 IH コンロ/ ガスコン ロ	出かけた後でコンロを ON→OFF にし忘れたかが心配になったので、遠隔操作で消し忘れ防止機能を OFF→ON にして、万一火が付いていても消えるように備えをした。実際には、本当に火を消し忘れていた。	通信故障（電池切れを含む）等により、コンロの消し忘れ防止機能を遠隔から ON できない状態となり、最終的に鍋が焦げて火災となる。	<p><本質的安全設計> 消し忘れ防止機能は常に動作させ（ON 状態にし）、遠隔からの操作を禁止する。</p> <p><安全機能による保護> 鍋等に対する高温検知機能により、コンロを OFF する。この場合、検知機能の信頼性評価が必要。</p> <p><使用者に対する注意> 通信故障等により、消し忘れ防止機能を遠隔から OFF→ON できないことがあるため、遠隔操作を過信しないように使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。</p>	直接被害 ■ 無人で目視確認ができない。
据置型 IH コンロ/ ガスコン ロ	出先から、家につく 5 分前に、帰宅時刻に合わせて料理の温め直しをしようとして、スマートフォンからコンロを遠隔操作で OFF→ON した。	家を出る前にコンロの上にライターを置き忘れていたのを忘れていたため、コンロを OFF→ON して数分後に破裂、火災になった。	<p><本質的安全設計> 遠隔操作の禁止</p> <p><安全機能による保護> グリル部分など、蓋がある部分を遠隔操作で ON/OFF できる機能を限定し、更に遠隔操作で設定を変更した後に、蓋の開閉が行われたら、遠隔操作による ON/OFF をキャンセルする機能を設ける。</p> <p><使用者に対する注意> -</p>	直接被害 ■ 無人で目視確認ができない。

(注 1) 据置型コンロは揚げ物等の際に機器のそばを離れないという警告表示があり、S マー

ク認証における遠隔操作の運用基準（エアコン以外）でも禁止されてきたため、遠隔操作できる機種はない。また、実際の切り忘れ防止機能として搭載されている高温検知電源 OFF 機能、切り忘れ電源 OFF 機能は ON・OFF を設定できない機能である。

(注 2) 据置型コンロに鍋なし検知機能/小物検知機能が装備されている場合は、コンロ上のライターは、単独で加熱されない。

(注 3) 記載のユースケース、リスクシナリオは事務局により、議論を行うことを目的として、上記の注記を考慮せず、仮想的に創作したものである。

(オ) 安全機能の保護に関する要求事項の方向性

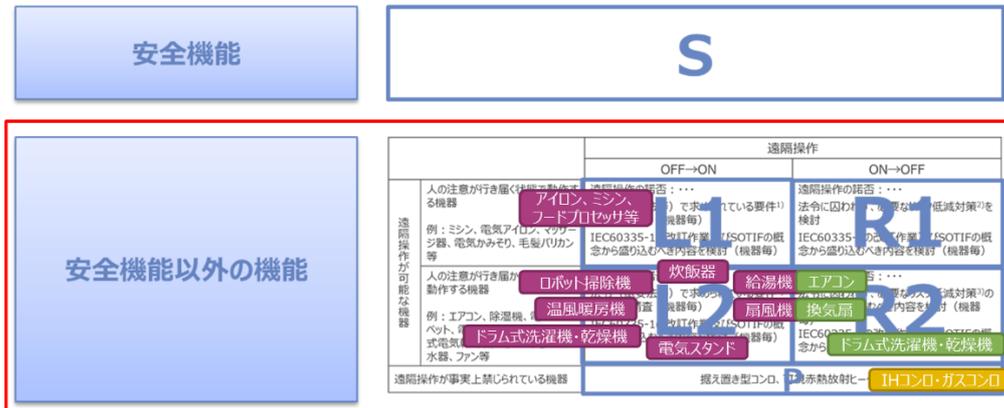
通信回線を利用した遠隔操作機構を有する機器は、通信回線と安全機能とを分離し、遠隔操作が安全機能に影響を与えないこととする（図表 44）。

図表 44 通信回線と安全機能の分離



ユースケース／リスクシナリオ及び対応策の一例（案）を例示した機器は、下記（L1、L2、R1、R2、P）のように分類される（図表 45）。

図表 45 安全機能を除く電気用品等の機能と機器の分類例



2) 予防安全機能について

遠隔操作している機能が通常利用している機能である場合は「『通常機能』を対象としたユースケース／リスクシナリオの例」、リスク低減のための保護機能（安全機能ではないもの）である場合は「『予防安全機能』を対象としたユースケース／リスクシナリオの例」と区分できる。

図表 46 「予防安全機能」について

『通常機能』を対象としたユースケース／リスクシナリオの例

温風暖房機の通常利用する機能（『通常機能』）として遠隔操作しているため、『通常機能』を対象としたユースケース／リスクシナリオと言える。

『予防安全機能』を対象としたユースケース／リスクシナリオの例

チャイルドロックは、通常利用する機能（『通常機能』）として、ドラム式洗濯機・乾燥機に組み込まれた機能であるが、チャイルドロックを遠隔操作できる機能（『予防安全機能』）を利用した例であるため、『予防安全機能』を対象としたユースケース／リスクシナリオと言える。

製品	ユースケース	リスクシナリオ
温風暖房機（ガス・石油）	温風暖房機の上に洗濯物を乾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。

製品	ユースケース	リスクシナリオ
ドラム式洗濯機・乾燥機	出かけた後でチャイルドロックをOFF→ONにしたことに気付いたため、遠隔操作でOFF→ONに変更した。	通信障害（電池切れを含む）等により、チャイルドロックが実際にはONになっておらず、子供がドラムに入って危害を受ける。

3) 『予防安全機能』を対象としたユースケース／リスクシナリオの事例について

予防安全機能を対象としたユースケース／リスクシナリオを以下に抜粋した（図表 47）。これ以外は、通常機能を対象としたものである。

図表 47 『予防安全機能』を対象としたユースケース／リスクシナリオの事例

製品／予防安全機能	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） ※現段階では例示であり、今後要検討	備考
ドラム式洗濯機・乾燥機／チャイルドロック <div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; text-align: center; margin: 10px auto;">L2</div>	出かけた後でチャイルドロックをOFF→ONにし忘れたことに気付いたため、遠隔操作でOFF→ONに変更した。	通信障害（電池切れを含む）等により、チャイルドロックが実際にはONになっておらず、子供がドラムに入って閉じ込められ、窒息する。	<本質的安全設計> – <安全機能による保護> 子供が洗濯機の中に入った状態では、チャイルドロックはOFF→ONにできないようにする。また、遠隔操作した者に操作結果（ONに失敗等）をフィードバックする。 <使用者に対する注意> 通信故障等により、チャイルドロックを遠隔からOFF→ONできないことがあるため、遠隔操作を過信しないように使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。	直接被害 ■ 機器の傍に いる子供が被害を受ける。
炊飯器／操作ボタンロック <div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; text-align: center; margin: 10px auto;">L2</div>	出かけた後で操作ボタンロックをOFF→ONにし忘れたことに気付いたため、遠隔操作でOFF→ONに変更した。	通信障害（電池切れを含む）等により、操作ボタンロックが実際にはONになっておらず、遠隔から炊飯器をOFF→ONして炊飯したところ、子供が操作ボタンに触って火傷した。	<本質的安全設計> 操作ボタンロックに対する遠隔からのOFF→ONを禁止する。 <安全機能による保護> – <使用者に対する注意> 通信故障等により、操作ボタンロックを遠隔からOFF→ONできないことがあるため、遠隔操作を過信しないように使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。	直接被害 ■ 遠隔からの通常機能の操作と連携することで、機器の傍らにいる子供が被害を受ける。
ドラム式洗濯機・乾燥機／チャイルドロック <div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; text-align: center; margin: 10px auto;">R2</div>	洗濯機のチャイルドロックを操作し出かけたが、遠隔操作により間違えて操作してチャイルドロックが外れてしまい（ON→OFF）、そのことに気がつかなかった。	留守番していた子供が洗濯槽に入って閉じ込められた結果、窒息する。	<本質的安全設計> チャイルドロックは、遠隔操作によるON→OFFを禁止する。 <安全機能による保護> チャイルドロックを通信機能回路と完全に分離する。 <使用者に対する注意> –	直接被害 ■ 機器の傍に いる子供が被害を受ける。

製品／予防安全機能	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） ※現段階では例示であり、今後要検討	備考
オープンの遠隔監視機能 <div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center; margin: 10px auto;">R2</div>	オープンでパイを長時間焼いているところ、その焼け具合を遠隔から監視していたが、急に監視ができなくなり、現状を見失った ^(注8) 。	通信障害（電池切れを含む）等により、遠隔からの監視に加えてON→OFF操作もできなくなり、過熱して火災が発生した。遠隔監視を過信していて、タイマーの時間設定が長すぎ、火災を起こす前にオープンを止めることができなかった。	<本質的安全設計> 遠隔監視と遠隔からのON→OFFを禁止する。 <安全機能による保護> オープンの過熱検知機能により、オープンをおFFする。この場合、検知機能の信頼性評価が必要。 <使用者に対する注意> 通信故障等により遠隔監視ができなくなる可能性があるため、遠隔監視を過信しないよう使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。	直接被害 ■ 無人で目視確認ができない。
IHコンロ、ガスコンロ／消し忘れ防止機能 <div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center; margin: 10px auto;">P</div>	出かけた後でコンロをON→OFFにし忘れたかが心配になったので、遠隔操作で消し忘れ防止機能をOFF→ONにして、万一火が付いていても消えるように備えをした。実際には、本当に火を消し忘れていた。	通信故障（電池切れを含む）等により、コンロの消し忘れ防止機能を遠隔からONできない状態となり、最終的に鍋が焦げて火災となる。	<本質的安全設計> 消し忘れ防止機能は常に動作させ（ON状態にし）、遠隔からの操作を禁止する。 <安全機能による保護> 鍋等に対する高温検知機能により、コンロをおFFする。この場合、検知機能の信頼性評価が必要。 <使用者に対する注意> 通信故障等により、消し忘れ防止機能を遠隔からOFF→ONできないことがあるため、遠隔操作を過信しないよう使用者に分かりやすく周知する。周知方法は、取扱説明書だけでは不十分。	直接被害 ■ 無人で目視確認ができない。

4) 『予防安全機能』の用語の定義

ここまでで顕在化した論点を議論するため、その前提となる準備として、リスクを低減できると考えられる機能であって安全機能以外の機能について新しい用語を定義した（図表 48）。

予防安全機能については、機能をON→OFFすることが危険側となるが、故障や意図せざる遠隔操作などによって不意に機能停止することも想定される。これに対する方策の考え方としては、予防安全機能そのものところを遠隔操作する機能の信頼性を高めることがまず必要となる。しかし、SOTIFの観点（非故障）にも配慮する必要があることから、将来的には、万一に備えて予防安全機能にフェールセーフを適用する等の検討も実施すべきと考えられる。

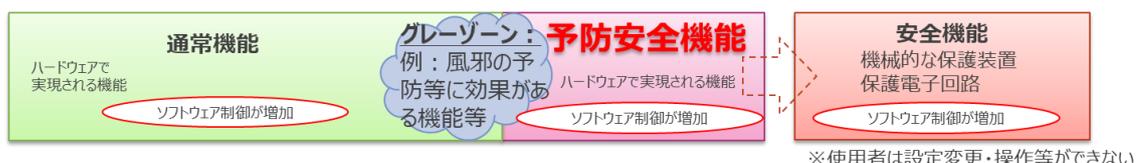
図表 48 『予防安全機能』の定義

【予防安全機能（仮称）の定義（案）】

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。

※ 例 1：遠隔操作の誤操作による二次被害を防止、または低減できる機能
 ※ 例 2：性能限界があり確実な動作を保証してはいるが、動作すれば人への危害を防止、または低減できる機能
 ※ 例 3：付加的に（or オプションとして選択し）人への危害を軽減するもの
 ※ 例 4：AI等を用いて実現する付加価値機能により、人への危害を軽減するもの

例示：自動車の車線はみ出しアラート、障害物お知らせ機能、インテリジェント温度センサーを用いたコンロ／グリルの検知機能（消し忘れ消火機能等）、等



5) 今後の検討の方向性

将来の技術発展の動向を踏まえた指摘をすることが、今後必要になってくる。さらに、今後は製品同士のコミュニケーション等も顕在化する見込みであることから、この観点から安全や信頼性を議論することにも配慮していくことが考えられる。

(3) 今後の課題：ソフトウェアのダウンロードについて

製品安全関連法は、製品出荷時のハードウェアの欠陥等が起因となる製品事故防止等を目的に整備されている。一方で、製品のソフトウェア制御の広がりを受けて、製品出荷後にダウンロード&適用したソフトウェアアップデートの安全性が重要な論点となってきている。現時点では、製品安全関連法において製品出荷後のソフトウェアアップデートの安全性をどのように整理するかは検討がなされていない状況である。しかし、将来に向けてこの検討が必要となる可能性があり、海外動向も含めて引き続き注視していくことが求められる。

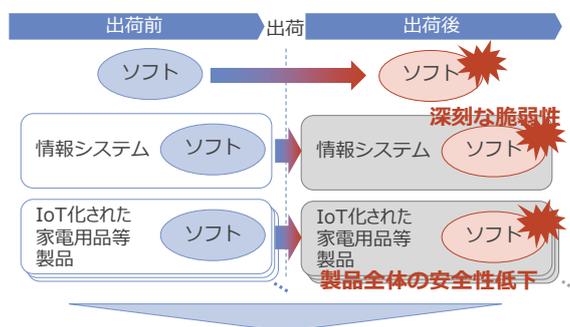
1) 出荷後も安全であり続けるためのソフトウェア上の課題

ソフトウェアのダウンロードに関しては、出荷後の「深刻な脆弱性の発覚による製品の安全性低下」に関する課題が存在する（図表 49）。また、ダウンロードしたアップデート側に安全性を低下させうる問題が潜在することもありうる。これにはソフトウェアサプライチェーンも関係してくる。このように、ソフトウェアは、製品のライフサイクル全体に亘る安全に大きな影響を持つと考えられる。

図表 49 深刻な脆弱性の発覚による製品の安全性低下

- 既に広く普及しているソフトウェア(部品)を新しいIoT化された家電用品等製品に組み込み、十分に安全対策を講じた上で検査し、出荷。
- 出荷後の時点で、当該ソフトウェア(部品)に深刻な脆弱性が発見されることにより、当該製品の安全性が低下*。

*将来は、ソフトウェアの開発・提供構造の多様化やこれに伴う責任分担の複雑化等の新たな論点も想定される。



- 今後、IoT化された家電用品等製品は「出荷した後も安全でありつづける。」ことが求められるのではないか。
- 今後、IoT化された電気用品等製品のリコールにも影響が及ぶのではないか。

2) IEC60335-1 の改正における関連動向

IEC60335-1 の改訂において、この動きが明確に顕在化している（図表 50）。

既に、家電本体のソフトウェアをスマートフォン経由で書き換え可能な製品も販売が開始されており、国際規格との整合を図る意味でも、ダウンロードとインストールの定義を国内でも明確にしておく必要がある。

図表 50 IEC60335-1 遠隔操作改定案の内容（ソフトウェアのダウンロードに関する項目の抜粋）

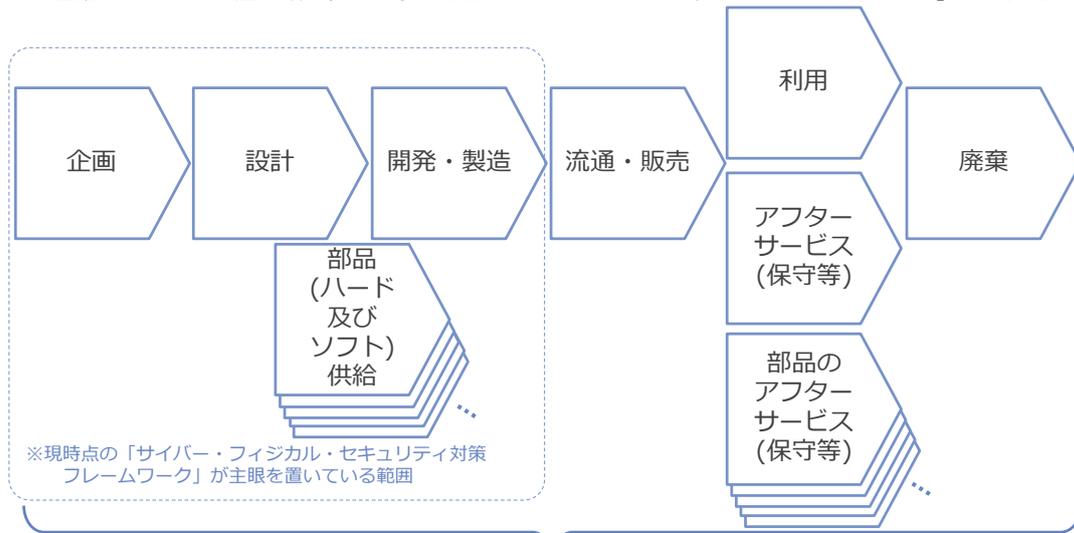
項目番号	要求事項の概要	備考
22.XX	Public networkを経由したRemote communicationが家電製品の 安全担保に影響を与えないこと	
	Remote communicationには ソフトウェアのダウンロード を含む。 家電製品の安全担保、及び ソフトウェアのダウンロード に関するソフトウェアは、 他の部分と分離 され、かつ保護電子回路に用いるソフトウェアへの要求事項と同様の要件を満たすこと。（Annex R）	Annex Rの要求事項 バージョン管理、変更の必然性、 モジュール化設計
XY.7.12.101	ソフトウェアのダウンロード 時には、手順とバージョン情報をユーザーに示すこと。	対象機器、ソフトウェアの組み合わせ
XY.22.108	ダウンロードするソフトウェア はメーカーによりあらかじめソフトウェアの互換性、通信異常時の動作、バージョンチェックなどの確認が取られていること。	
XY.11.109	ダウンロードしたソフトウェア のインストールは、家電製品の 管理者の許可を得て 行わなければならない。	ユーザーが知らない間にソフトウェアを書き換えることを禁止
XY.22.110	ダウンロードしたソフトウェア のインストールは、家電製品の安全担保に影響を与えてはならない。	

出典：第2回WG 坂口委員説明資料

3) 全工程を俯瞰して安全を守る「セーフティ・バイ・デザイン」の考え方

ISO 10377 で規定されているサプライチェーンに加え、製品安全とサイバーセキュリティが連携する形で、製品出荷後になされたダウンロード及び適用したソフトウェアアップデートに関しても今後検討が必要ではないかと考えられる。

図表 51 全工程を俯瞰して安全を守る「セーフティ・バイ・デザイン」の考え方



- ・サイバーセキュリティの領域では、全工程を俯瞰しつつ対策を検討・実装する「セキュア・バイ・デザイン」といった手法が提唱・推進されている。
- ・今後、IoT化された電気用品等製品についても「セーフティ・バイ・デザイン」といった考え方の検討も必要ではないか。

4) ダウンロードしたソフトウェアを機器にインストールする者の要件

ここまでの検討を勘案すると、ダウンロードしたソフトウェアを機器にインストールする者が機器自体やインストール操作について専門的な知識を有していることが望ましいケースが想定される。この点について、検討会委員より、「ソフトウェアをダウンロードして機器にインストールする者を認証する資格制度等を設け、有資格者が信頼できる方法でソフトウェアをダウンロードしてインストールするようにはどうか」というご意見をいただいたことを付記しておく。

3. まとめ

(1) 検討内容のまとめ

1) 検討対象とする被害

本検討では、情報漏洩、金銭の詐取といった被害ではなく、対象を人に危害を及ぼす被害である消費生活用製品安全法に規定する重大製品事故（死亡、身体的傷害、健康障害、火災等による物損）に限定して、検討を進めた。

なお、今後のIoT化の進展を踏まえ、「人への危害」には、生活環境の変化に伴い熱中症を引き起こし、体調を崩すことなども遠隔操作の誤操作による二次被害と考えられ、これも含むものとした。

2) 本検討における原則と電気用品安全法の既存スコープを超えた検討の方向性

遠隔操作における電気用品等製品の安全確保に関する検討においては、配慮すべき危険源、考慮すべきリスク、リスク低減対策の3つの観点から、機器側に求める内容やリスクを低減させる方策、消費者への注意喚起の内容などについて検討するという電気用品安全法のアプローチを堅持する。その上で、現行の電気用品安全法の範囲に含まれていない、遠隔操作によるON→OFFすることのリスクについて検討を行った。

さらに、将来に向けては、SOTIFが提示する非故障（性能限界、意図しない操作、AIの誤認識等）によるリスクや、ソフトウェアのダウンロード/インストールによるリスク等についても検討を広げる必要があるものとする。

3) 利用者の過信と不意の危害についての検討

遠隔操作する人が機器及び周辺の状態を目で確認できないことから、通信回線や機能の信頼性・性能限界を過信（または遠隔操作そのものを忘れる）すると、気付かぬうちに当該機器の周囲が危険に陥る場合がある。同様に、機器の傍にいる人に不意の危害を与えてしまう恐れが生じうる。

今回の検討では、上記のような「利用者の過信」と「機器の傍らにいる別の人への不意の危害」にも十分に留意しながら、遠隔操作リスクの検討を行った。

4) 機能安全（ソフトウェアを用いた安全機能）に対する方策の方向性

IEC60335-1 第6版の改定方針を参考として、通信回線を利用した遠隔操作機構を有する機器については、通信回線と安全機能を分離し、遠隔操作が安全機能に影響を与えないように設計するのが大前提となることを提言した。

5) 安全機能以外の機能についての検討フレームワークの提言

IEC60335-1 及び IEC60335-2-xx シリーズにおける『遠隔操作』に関係のある部分として個別機器の耐熱性及び耐火性に関する要求事項などから、IoT化された電気用品等製品を「遠隔操作を禁止又は事実上禁止されている機器」と「それ以外の機器」に分類し、後者をさらに「人の注意が行き届く状態で動作する機器」と「人の注意が行き届かない状態で動作する機器」に細分した。

①遠隔操作を禁止又は事実上禁止されている機器

②遠隔操作が可能な機器：

②-1 人の注意が行き届く状態で動作する機器

②-2 人の注意が行き届かない状態で動作する機器

次に、「人の注意が行き届く状態で動作する機器かどうか」×「遠隔操作の種別（OFF→ON or ON→OFF）」の2×2マトリクス+「IEC 規格において遠隔操作を禁止又は事実上禁止されている機器」の区分を検討のためのフレームワークとして設定し、各区分に対して個別機器毎にユースケース／リスクシナリオの事例を当てはめて検討を行った。なお、遠隔操作には、当該機器が周辺環境に変化を与える温度を調節する機能も含めると、遠隔操作で機器を通常利用する機能（通常機能）と、遠隔操作の誤操作による二次被害を防止又は低減することを目的として組み込まれた機能（以下「予防安全機能」という。）が存在する。これらの機能と3.(1)3の「利用者の過信」と「機器の傍らにいる別の人への不意の危害」にも留意し、遠隔操作のリスクの検討を行った。

このフレームワークについては、「②-1：人の注意が行き届く状態で動作する機器」と「②-2：人の注意が行き届かない状態で動作する機器」を明確に分類できる方策が必要であるとの課題が指摘されている。この課題を克服するため、IECの国際標準にならって用語の定義を明確にすること、人が見ていれば大丈夫といったルール付けを行うこと、人が機器の傍を離れることを可能にする機能（例：協調安全機能（人間が近くにいるかどうかで動作を変える機能）、製品の周囲等の安全を確認するシステム等）の具備を考慮すること等を検討していく必要がある。

6) ユースケース及びリスクシナリオについて

遠隔操作のリスク対応について広く議論するための素材として、IoT化された電気用品等製品のユースケース及びリスクシナリオの例示に取り組んだ。

今回、遠隔操作の対象範囲として、「OFF→ON」に留まらず、「ON→OFF」や「周辺環境に変化を与える温度等を調節する機能」までも対象とし、「遠隔操作が事実上禁じられている機器」「人の注意が行き届く状態で動作する機器」「人の注意が行き届かない状態で動作する機器」の分類毎に、IoT化された電気用品等のユースケース／リスクシナリオを検討・例示した。この検討にあたっては、WGの場を活用し、関連する事業者団体のご意見を集約しながら例示内容の改善を実施することができた。

各個別機器のユースケース／リスクシナリオの中には、通常利用する製品機能ではなく、リスク低減に一定の効果を発揮することを目的として組み込まれた予防安全機能を対象としたものも存在している。このケースでは、対象とした予防安全機能を停止させると危険側になることから、今後は通常利用する製品機能とは異なる観点で、方策・対策の一例の案出・例示を行う必要がある。

(2) 今後の課題及び検討の方向性について

1) ユースケース及びリスクシナリオについて

本年度の検討では、上記の通り、検討フレームワークを提案し、その区画毎にユースケース及びリスクシナリオの事例を作成した。各個別機器の事例については、方策・対策の一例（案）に

についても検討を行ったが、今後、より事例の充実化を図ることが必要となってくる。

アプローチとしては、新しい個別機器のユースケース及びリスクシナリオの事例を必要に応じて追加するとともに、各事例に対する方策・対策の精度を上げることが必要である。今回、ユースケース及びリスクシナリオを検討するにあたって、「利用者の過信」と「機器の傍らにいる別の人への不意の危害」を考慮したが、今後は問題が生じた際に利用者が正しく回復できるかという論点も加えて検討する必要がある。

これらのリスクは遠隔操作の特徴であると言えるが、方策・対策の検討にあたり、取扱説明書だけでは消費者への十分な説明に限界がある可能性もあるのではないかと考える。このため、例えば遠隔操作中はその旨を分かりやすく表示し、機器の傍らにいる人に可能な限り気付かせる等の、より能動的な方策・対策も検討していくことが望ましい。さらに概念上は、利用者が過信して使うことは誤使用にあたるのかという議論もありうる。製品安全設計において「予見可能な誤使用」は大きな意味を持ち、もし過信が誤使用に当たるのであれば、過信への方策・対策が持つ意味合いも異なってくるため、今後更なる検討、整理が必要ではないかと考えられる。

2) 検討フレームワークの明確化

IEC60335-1 及び IEC60335-2-xx シリーズにおける『遠隔操作』に関係のある部分として個別機器の耐熱性及び耐火性に関する要求事項などから、今回提言している検討フレームワーク(2×2のマトリクス+1行のもの)を整理したが、この実効性を高めるため、今後は「人の注意が行き届く状態／行き届かない状態」の分類を明確にする必要があるのではないかと考える。明確な分類を実現するためには、用語を明確に定義することや、分類基準を明確に定めることが必要になってくるのではないかと考える。将来、このフレームワークの国際標準化を目指すのであれば、用語や分類基準の明確化についての議論をさらに深めていく必要があるのではないかと考える。一方、既存の国際標準との整合性を確保していくことも求められてくる。

また本検討では、セキュリティリスク⁴⁹を「意図しない操作によるリスク」の中に入れて考えている。その理由は、製品に組み込まれたソフトウェアの脆弱性を使用した攻撃であっても、結果として人に危害を与えてしまう事象は従来と特に変わらないという立場に立っているためである。他方で、脆弱性に起因するセキュリティリスクを考慮しはじめると際限ないところがあり、製品の安全設計においては、多重防護による安全確保の方がより望ましいアプローチであると言える。

3) ガイドライン化に向けたアクションプラン

本検討で踏まえた結果をもとに、今後はガイドライン化に向けたアクションが必要となってくる。具体的には、現在 FDIS の発行を待っている IEC60335-1 第 6 版の内容を踏まえ、また、一般社団法人日本電気協会の電気用品調査委員会が行う解釈別表の見直しの検討やガス機器関係団体等の省令・通達改正の動向とも連携を図りつつ、今回提言したフレームワークの区画毎に、作成したユースケース及びリスクシナリオの事例(方策・対策の一例(案)を含む)を比較・整理する。その上で、将来的な技術の発展動向もフォローしながら、遠隔操作のリスク低減に資す

⁴⁹ 製品に組み込まれたソフトウェアの脆弱性を使用した攻撃により、結果として人に危害を与えてしまう事象

る「あるべき方策・対策のガイドライン」を検討し、とりまとめていくことが必要となるのではないか。

なお、今後、IoT化した電気用品等製品で人への危害が生じた場合のガイドラインへの効力の持たせ方や責任分担の考え方等も論点になりうると考えられ、IoT化した電気用品等製品の製造事業者等の成長を減速させないよう配慮しながら広く議論を進めることが必要である。

4) ソフトウェアのダウンロードやアップデートについて

本年度調査では、将来に向けた大きな課題として、IEC60335-1 第6版の改定予定内容に基づき、製品出荷後のソフトウェアのダウンロードやアップデートの重要性について指摘した。

ソフトウェアのダウンロードやアップデートについては、例えば、以下に示すように数多くの課題が存在している。

- ・ 利用者が適時適切にソフトウェアをアップデートしないことも想定される。
- ・ 責任の複雑化
これまでの製品を売り切るという概念が変わり、サブスクリプション方式⁵⁰のサービスが広がると、ソフトウェアのみを提供するベンダーが参入することで、製品に問題が生じた場合の利用者による回復操作の適切な手法の新たな確保など、新たにステークホルダーが増えることによる新たな問題も想定する必要があると考えられ、責任分担の明確化や消費者教育の必要性といったことも将来の課題となる。例えば Windows アップデートの例では、PC 上の利用者所有のソフトウェアに対し、ベンダー側からアップデートを自動送信しているが、人に危害が生じた場合に誰が責任を負うのかなども想定される。
- ・ ソフトウェアのダウンロードやアップデートと製造物責任の関係
ソフトウェアの作り手側の製造物責任に関する論点も想定される。
- ・ 将来、製品出荷後に脆弱性に起因する外部からの不正アクセスなどから始まるサイバー攻撃によりセキュリティインシデントが発生したとしても、多重に組み込んだ安全機能や予防安全機能により、重大製品事故に至らないといった方策の検討も必要になるのではないか。

上記について、今後さらに検討を継続していくことが望ましい。

(以上)

⁵⁰ 定期購入や定額購入の形式によって、サービスや商品を利用すること。