製品の遠隔操作と安全

一般財団法人 電気安全環境研究所
理事
住谷 淳吉

スマートフォン等により、宅外から遠隔操作できる電気製品の安全性に関しては、電気用品安全法の技術基準の解釈において、遠隔操作機構を有する電気用品に関する規定があります。本稿では、この概略について紹介するとともに、2021年4月28日付けで経済産業省のホームページで公表された「電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドラインについて」(以下、「ガイドライン」[1]という。)に記載されている予防安全機能の概念を紹介させていただきます。

1. はじめに

遠隔操作できる電気製品の安全・安心に関しては、個人情報漏洩や悪意のある操作などのセキュリティに関する検討が議論の中心になることが多いですが、最終的にはセキュリティ対策は、メーカーによる一定のセキュリティレベルは確保しつつも、個人のパスワードの定期的な変更など使用者にも頼る必要があるものと考えられます。一方、電気用品安全法の技術基準の解釈では、誤操作等を含めた考えらえる使用範囲において、感電、火災、傷害といった危険が生じるおそれがないこと(以下、「安全」という。)が要求されており、これらの対策は原則機器側で対応し、それでも社会的に許される範囲の残留リスクがあればそれを使用者に示す必要があるという考え方です。言い換えれば、電気用品安全法では、誤操作は必ずあることを考慮し、「誤操作されても安全」という趣旨で技術基準の解釈が規定され、この結果として、「悪意のある操作があっても安全」という電気用品だけが遠隔操作できるものとして認められているものと考えます。

また、遠隔操作する人は、電気製品の近くにいないので、近くにいる人と遠隔操作される電気製品とは、互いに協調して(例えば、電気製品側から製品が動いていることを近くにいる人に知らせるなどにより)安全確保をするケースも増えてくると思います。ガイドラインでは、この人と機器とが協調して安全(以下、「協調安全」という。)を確保するために必要な予防安全機能というリスク低減策について言及されています。

本稿では、電気用品安全法の概要と法律ではカバーできにない予防安全機能の一般的な概念について紹介させていただきます。なお、電気用品安全法の技術基準に関する遠隔操作の詳しい内容は、一般社団法人日本電気協会発行の「電気用品の技術基準の解説(分冊)遠隔操作に関する報告書等」[2]で解説されています。

https://store.denki.or.jp/products/detail/492

2. 電気用品安全法の技術基準の解釈概略

電気用品安全法の技術基準の解釈では、通信回線を利用した遠隔操作機構を有する機器に対して、次の要求事項を規定しています。

電気用品の技術上の基準を定める省令の解釈別表第八1(2)ロ(ロ)b

通信回線(別表第四1(2)ロ(イ)に掲げるものを除く。)を利用した遠隔操作機構を有する機器で次の全てに適合するもの。

(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。

(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。

(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

(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確認ができること

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等への記載

(e) 通信回線(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)

(f) 通信回線のうち、公衆回線を利用するものにあっては、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。

(g) 同時に2箇所以上からの遠隔操作を受けつけない対策を講じること。

(h) 適切な誤操作防止対策を講じること。

(i) 出荷状態において、遠隔操作機能を無効にすること。

2.1 リスクアセスメント

2.の(a)では、遠隔操作によって増大するリスクの有無をリスクアセスメントにより評価することが要求されています。電気用品安全法は、旧来は、「赤熱式の電気ストーブは遠隔操作機構による操作は不可」といった電気用品名に対する規定がほとんどでしたが、遠隔操作に関しては、電気用品名によって遠隔操作の可否を判断するのでなく、リスクアセスメントによって判断することとした初めての規定になります。規格にリスクアセスメントを採用するのは、比較的新しい機器に対する規格では、IEC規格等でも用いられるようになっています。

2.2 通信途絶

2.の(b)では、通信回線は不安定なものなので、故障等により途絶し、遠隔からでは復旧が不可能となった場合でも、最終的に電気用品が安全状態に移行することが要求されています。安全状態への移行とは、遠隔操作と同時にスタートするタイマーなどによる停止がありますが、照明器具のように連続運転状態でも安全状態と見なせる電気用品もあります。これらの安全状態については、2.1のリスクアセスメントにおいて、通信回線途絶に対するリスク評価を行い、安全状態を確認しておくことが求められています。

2.3 手元優先／通信回線の切り離し

2.(c)では、家庭用の電気用品について、近くにいる人の危険回避を目的に、遠隔操作中であっても操作される機器の近くにいる人によって操作が可能であることが要求されています。ただし、デパートの照明器具など業務用の機器においては、手元操作をされることが危険につながるケースもあるので、そのような場合は、手元操作に対するリスク評価も実施しておくとよいと考えます。

また、手元操作だけでは安全が回避できず、さらに通信回線を切り離して遠隔操作ができないようにする必要がある場合は、通信回線の切り離しが要求されます。この場合、その危険を回避するために、プラグを抜くなども考えられますが、近くにいる人が機器を使用する必要がある場合は、機器を動かした状態で通信回線を切り離

す必要があります。例えば、エアコンの熱中症対策として、遠隔操作で機器を停止することをリスクとする場合は、プラグを抜くことは、リスク回避にはなりません。通信回線の切り離しは、背景としては、悪意のある操作があった場合の最終的な回避策として検討されましたので、そのことを踏まえて、リスク評価を行うと良いと考えます。

2.4 操作結果のフィードバック

2(d)では、電気用品を遠隔操作したときは、その操作内容を電気用品側が受け取った後、その結果をスマートフォン等にフィードバックすることが要求されています。

この要求事項は、電気用品が確実に動作したことを操作者に確実にお知らせすることを規定したもので、リスクには直接は関係していません。動作が確実に行われたことを確認することで、間接的に生じるかもしれないリスクを回避することが目的です。

なお、赤外線を利用するものは、単方向通信となるため、操作結果のフィードバックはできません。このため、動作させるための条件を明確化し、かつ、それでも環境によって動作しないことがあることという注意喚起を取扱説明書等に記載することが要求されています。

2.5 識別管理／誤動作防止／再接続

2.の(e)のiでは、遠隔操作する人が操作を意図している電気用品以外を動作させないように遠隔操作される電気用品がユーザーIDや端末ID等で識別できていることが要求されています。

2.の(e)のiiでは、外乱(ノイズ)に対する耐久性があることが要求されています。外乱に対しては、一般的な汎用の通信方式であれば、規格に応じて対応していることが多いと考えますが、不明確な場合は、電気用品にイミュニティ試験を実施して確認します。

2.の(e)のiiiでは、宅内通信が不安定となり、一時的に途絶した後に、通信が元に戻って安定したときは、電気用品に通信回線を再接続して、電気用品が遠隔操作できる状態になることが要求されています。2.2は、復旧の見込みがない通信途絶に対する対応ですが、この項では、一時的な不接続に対する確実な動作が要求されています。

2.6 公衆回線の途絶

2.(f)では、公衆回線において、トンネル走行中など、一時的に途絶したり、また通信会社の都合で通信遮断したりするなどがありますが、それが復旧した後は、電気用品が安全に遠隔操作できる状態になることが要求されています。

2.7 同時に2箇所からの操作

2.(g)は、遠隔から同時に相反する操作(ONとOFFなど)を行った場合のリスクに関する要求となります。リスクがあると判断した場合、同時に2箇所からの操作ができないように排他制御を行うか、又は、同じ電気用品に対して一方が操作した場合は、すぐには他方が操作できないようにする時間差の制御を行うなどが必要なります。

2.8 誤操作防止

2.(h)では、遠隔操作機構に対するUIを考慮すること以外に、遠隔操作を間違えて行わないようにダブルアクション(例えば、「この操作をしてよいか」と確認する追加操作)や操作内容のフィードバック(操作した内容の表示)などが要求されます。電気用品側の要求ではなく、電気用品安全法の対象外の遠隔操作機構のアプリなどに対する要求事項であることに注意する必要があります。

2.9 出荷状態の遠隔操作機能の無効化

2.(i)では、出荷状態において、遠隔操作はできない初期状態になっていることが要求されています。遠隔操作は、比較的知識がある人が設定して利用するようにし、遠隔操作に詳しくない人は遠隔操作ができないようにすることが目的です。

この趣旨から、2.5の識別管理を使用者が設定する場合は、この要求を満たしているものと考えられていますが、有線LANケーブルを挿入すると自動的に遠隔操作が可能になるようなケースは、無効化とはみなされていません。また、2.3で通信回線の切り離しを機械的なスイッチで行

う場合は、出荷状態ではOFFの位置にして出荷することが求められています。

3. 他社が遠隔操作機構を提供する場合の対応

電気用品の製造事業者が遠隔操作機構(スマートフォンのアプリを含む)を電気用品ともに提供する場合は、遠隔操作機構に対する要求事項(2.4のフィードバックや2.8の誤操作防止)に対応できますが、電気用品の製造事業者とは別の事業者が遠隔操作機構を提供する場合は、電気用品側だけでは対応できないケースが生じます。IoT家電が普及するとともにそのようなケースが増えてくることが予想されますが、電気用品安全法は、電気用品単体が規制対象であるため、遠隔操作システムといった他社製品間の組み合わせに対してはカバーできません。

一般財団法人電気安全環境研究所(JET)では、このようなケース(他社が遠隔操作機構を提供するケース)を想定し、遠隔操作機構側及び電気製品側の要求事項を明確にした上で、遠隔操作機構側の事業者又は電気製品側の事業者にそれぞれ認証を取得していただくことで、双方を組み合わせたとき、電気用品安全法の技術基準の解釈レベルの安全性が確保できるとしたJET遠隔操作システム認証のサービスを提供しています(図1参照)。

https://www.jet.or.jp/products/rc_ready/index.html

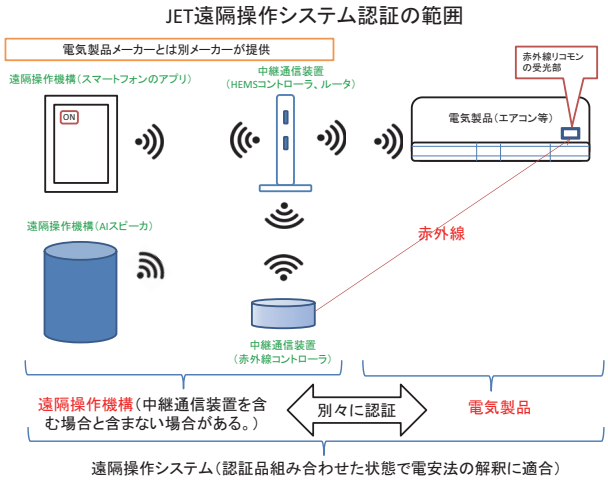

図1　JET遠隔操作システム認証の概念図

4. 予防安全機能

予防安全機能に関しては、ガイドラインで紹介されています。

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

通常機能や安全機能といった用語は、製品安全規格でよく聞かれると思いますが、予防安全機能は、IEC規格や電気用品の技術基準解釈といった既存の規格・基準では、規定されておらず、規定されていたとしても通常機能の一部として扱われています。

以下に、規格で扱われている通常機能及び安全機能の概念を示します。

【通常機能】

通常状態で働く機能。通常機能に対する安全性は、製品安全規格において、平常温度上昇試験、漏洩電流試験、定格消費電力測定試験などの運転試験で確認される。この機能が壊れても安全でなくてはならいことが原則。この機能は、使用者によって設定することできてもよい。

【安全機能】

異常状態で働く機能。通常状態では動作してはならない。安全機能に対する安全性は、製品安全規格において、主に異常運転試験や電子部品の故障試験で危険な状態にならないことで確認される。信頼性評価が必要で、この機能は、使用者によって設定できない。

遠隔操作との関係においては、次のようになります。

【通常機能】

電気用品安全法で遠隔操作に対するONについて解釈が明確にされている。危険な機能は、遠隔操作できてはならない。

【安全機能】

国際規格では、安全機能は通常機能とは分離・分割が要求される。このため、遠隔操作できる機能は、通常機能のみとなる。

一方、予防安全機能は、安全規格上は、通常機能として扱われますが、世間的には安全機能と誤解されやすい

です。一般的に予防安全機能に対する評価基準はないことが多く、通常機能の一部ですが、特に協調安全を考慮すべき状態において、危険状態になることを予防し、危険状態になる前に動作する機能となることが多いです。

このように言われて、どのような機能を想像するのが難しいと思いますが、現在、一番説明しやすいものは、自動車の自動ブレーキです。自動ブレーキは、何らかの理由でフットブレーキを踏めない状態となったときの、予防安全機能となります。確実な動作が確約されている分けではないので、フットブレーキを踏まなくても安全という機能ではありません。

予防安全機能は、このように最終手段(安全機能)以外の方法で危険状態を予防する機能ですが、過信すると逆にリスクを増やしてしまうことがあります。例えば、自動ブレーキ(予防安全機能)は、今後も使用者が過信しなければ、確実に交通事故というリスクを低減することは明らかですが、過信するとフットブレーキを踏まない人が続出してリスクは増えてしまいます。また、予防安全機能は、技術が発達すると安全機能となる可能性があります。例えば、完全自動運転の世界では、自動ブレーキは安全機能としての厳しい評価が必要になる可能性があります。

安全機能(最終手段)か予防安全機能なのかは、製造事業者の設計意図にもよるため使用者側からはわかりづらいですが、「条件によって動作しない」や「使用者が機能を解除できる」としているものは、安全目的でも安全機能ではなく、予防安全機能となるケースが多いです。例えば、家電機器の世界では、使用者が選択できる機能として、チェイルドロックがあります。また、新しく追加された機能で「〇〇しても安全」などで広告されている新機能は、ほとんどのケースで予防安全機能からスタートしていると思われます。

遠隔操作の話題から少し離れてしまいましたが、ガイドラインでは、この予防安全機能により、遠隔操作のリスク低減が可能であるが、使用者に過信させないようにすることが重要ということが記載されています。ガイドラインを読む入口として、上述により予防安全機能の概念を理解していただければ、よりガイドラインが読みやすくなると思いますので、是非参考にして下さい。

その他、ガイドラインには、予防安全機能の他に、遠隔操作に不向きな機器、安全機能と通信回線との分離、ソフトウェアのアップデートなどについて記載がありますので、ガイドラインを遵守することにより、電気用品安全法の技術基準の解釈よりさらに詳しい安全対策となるものと考えます。

5. おわりに

電気用品安全法については、現在のところ技術基準やその解釈改正とことは予定されていませんが、ガイドラインについては、技術の進歩や社会情勢により、今後、見直し等がされるものと思います。

規制と技術の進歩は、時に相反するものとなることもありますが、そのバランスは重要となります。遠隔操作に限らず、新しい機能についても同様のことが言えますが、一般的に規制は事故の再発防止対策として増えていきます。逆に言えば、規制が増えるのは、事故が起こったことを意味しますが、これからの新しい技術に関しては、事故が起こってからでは遅いと言われる時代であり、今後は、事故が起こったことによって安全基準や設計を考えるのではなく、事故未然防止の観点から関係者が安全性を考える必要があると感じています。本稿で紹介した電気用品安全法の技術基準の遠隔操作に関する解釈やガイドラインは、両方とも事故未然防止の視点で制定されています。このように、これからの安全規格・基準づくりは、事故を未然に防ぐための想像する力とバランス力とが求められると考えます。

参考文献

[1] 経済産業省、「電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドラインについて」、令和3年4月28日.

[2] 一般社団法人日本電気協会、「電気用品の技術基準の解説(分冊)遠隔操作に関する報告書等」、2019年11月更新.

住谷 淳吉(すみや じゅんきち)

1988年　財団法人日本電気用品試験所(現在の一般財団法人電気安全環境研究所)に入所
入所から5年間は試験部で、電気用品安全法の技術基準に関する試験を実施

1993年～
1993年より20年間は、技術規格部で電気用品安全法の技術基準に関する規格開発

2012年　経営企画部で新規事業に関する企画立案を担当
現在に至る