第 2 回　IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会　議事要旨

日　時：2023 年 2 月 6 日（月）13:00 ～ 15:00
場　所：Teams によるオンライン会議
出席者（以下敬称略）：

委　　員：高倉委員（座長）、猪俣委員、稲垣委員、岩﨑委員、高橋委員、中尾委員、中野委員、花見委員、広瀬委員、松浦委員、唯根委員

オブザーバー：内閣官房内閣サイバーセキュリティセンター、総務省 サイバーセキュリティ統括官室、経済産業省製品安全課、産業機械課、国際電気標準課、独立行政法人情報処理推進機構（IPA）、独立行政法人 日本貿易振興機構（JETRO）、独立行政法人 製品評価技術基盤機構、公益社団法人日本通信販売協会（JADMA）、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）、一般社団法人情報通信ネットワーク産業協会(CIAJ)、一般財団法人電気安全環境研究所(JET)、一般社団法人日本電機工業会（JEMA）、一般社団法人ビジネス機械・情報システム産業協会（JBMIA）、一般社団法人 電子情報技術産業協会（JEITA）、一般財団法人 日本品質保証機構（JQA）、電気製品認証協議会（SCEA）、技術研究組合 制御システムセキュリティセンター（CSSC）

経済産業省：大臣官房　上村サイバーセキュリティ・情報化審議官、
商務情報政策局　サイバーセキュリティ課　奥田課長、塚本課長補佐

議　事：

資料 3 に基づき、前回の検討会のご指摘事項について、事務局より説明が行われた。また、資料 4、資料 5 に基づき、構成員によるプレゼンテーションが行われた。さらに、資料 3 に基づき、適合性評価制度の位置づけや本適合性評価制度で対象とする製品範囲、用いる適合性評価基準や活用する適合性評価スキーム、討議事項等について、事務局より説明が行われた。主な質疑・議論は以下のとおり。

【主な質疑・議論】

- 討議事項①（適合性評価制度で対象とする製品範囲について）、討議事項②（適合性評価制度で用いる適合性評価基準について）、討議事項③（適合性評価制度で活用する適合性評価スキームについて）で示されている提起の理由について補足説明をしていただきたい。
  - 総じて、ベンダーや業界団体の意見に立脚しているほか、国際的な動向も加味している。製品範囲に関して、総務省の技適の対象は直接的にインターネットに接続する製品であるが、これだけで十分か検討を行った。諸外国では、直接的か間接的かは区別せずに対策を求めている。この背景を踏まえ、今回の制度でも広く「間接的又は直接的にインターネットに接続する製品」を対象範囲として提起している。他方、製品類型ごとにリスクの度合いや求められるセキュリティ対策のレベルは異なるため、優先度が高い製品が存在するという仮説に基づき、「新たな制度において特に優先度の高い製品」や「既存の制度で対応すべき製品」等の峻別を精緻に行っていくべきではないかと提起した。適合性評価基準に関しては、ヒアリング結果をもとに提起させていただいている。初回検討会でも、日本独自の基準を新たに作りガラパゴス化した制度を構築することは避けるべきとのご意見をいただいた。国際的な標準を基軸とした適合性評価基準を前提とすることについて、メーカーの方からも賛成の意見を多くいただいており、このような提起をさせていただいている。他方、製品類型ごとにリスクは異なるため、具体的にどういった基準を適用するかについては、個別に検討する必要があると考えている。適合性評価スキームに関しては、本制度をいかに活用していただくか、そして本制度によっていかにセキュアな製品を企業や消費者に調達いただくかが重要だと

考えている。特に自己適合宣言を認めるべきか否かについては、判断ができていないため、討議事項として示している。

- 諸外国では、速いスピードで適合性評価制度の検討が進んでいる。日本が諸外国に遅れをとることのないよう、製品範囲や評価基準、評価スキームといった具体的な部分を議論することが適当だと考えている。他方、本制度の背景となる課題や目的といった、討議事項①～③で示している部分以外についても、議論をしっかりと行っていきたいと考えている。

- 誰のため、そして何のための制度なのかという部分が考慮されていないと感じる。本検討会に参画するにあたって「IoT 製品の安全性を確保するとともに、メーカーのセキュリティ対策の取組を適切に評価し、多少高価であっても適切なセキュリティ対策を講じる IoT 製品が積極的に購入されるような社会の仕組みを構築する」と記された文書を共有いただいた。この部分が検討を行ううえで肝になると考えており、その考えに基づき、二点意見を述べさせていただく。一点目として、評価や認証にかかる費用及び期間を算出する必要があると考えている。政府調達を意図した CC 認証では、取得費用は数百万円から一千万円ほど、取得期間は半年から一年ほどかかるが、これはハードルが高いと感じている。費用算出の条件として、セキュリティ要件や評価品質を均一化するための方法論によっても、取得期間やコストは変わってくる。例えば、セキュリティ要件に関して、製品開発の部分だけを扱うのか、対応組織の維持まで含めるか、評価品質の確保を認定機関連絡会議といったスキームで済ますのか、ISO/IEC 17024、ISO/IEC 17025、ISO/IEC 17065 といった要件まで求めるのかは、評価認証のコストに影響する筈である。二点目として、そのような制度を検討したうえで、プロモーションをどのように行うかを検討すべきだと考えている。評価認証費用や期間が一定程度かかるのであれば、CC 認証と同じ道を辿る可能性がある。多少高価であっても適切なセキュリティ対策を講じる IoT 製品が積極的に購入されるような社会の仕組みの構築に向けたプロモーションの具体的な検討をお願いしたい。差し当たり、海外の状況等も踏まえた上で、フィージビリティ・スタディを行っていただきたいということである。
  - おっしゃられたことと同じことを考えており、取得費用や期間を算出すべきだと認識している。資料 3 で示した製品類型に対して、ある基準を適用した結果、どれくらいの費用や期間がかかるのかについての情報を持ち合わせていないため、そういった検証を進めていくべきという課題認識を持っている。今年度は時間が限られており、検証を十分に実施することは難しいが、引き続きその問題意識は持っておきたい。また、本制度をプロモーションするにあたって、経済産業省をはじめとした政府としてどのように関わっていくべきかについても検討を行っていきたい。

- スキームをどのように定めるかにもよるが、認証機関にとって負担が大きい認証規格を新たに作れば、スキームの継続は難しいと思われる。他方、ETSI EN 303 645 はセキュリティ要件として過度に厳密ではないため、基準として適していると思われる。また、IoT 製品は制御システムと比べて製品寿命が長くないため、サーベイランスの視点から更新制度を設けるかについては微妙な問題だと感じている。そのため、認証機関が一度きりの評価を数多くこなしていく体制にすることが重要だと考えている。
  - どういったスキームオーナーが求められ、どのような認証レベルや能力が必要なのかといった点と関連する話だと思われる。認証機関がサステナブルな形で認証を行えるようにすることが重要であり、しっかりと検討することが必要だと感じている。

- JISEC 認証制度において、デジタル複合機における普及は進んだ一方、それ以外の製品では普及しなかったという話がヒントになると感じている。一方で、S マークは普及が進んでいるが、消費者の立場としては、S マークがついているからといって優先的に製品を選ぶことはなく、業界を守るための取組として、S マークの普及が進んでいるのではないかと考えている。消費者に選ばれやすくするという観点よりも、業界を守るという観点で、普及の働きかけを検討した方が良いと感じた。また、JISEC 認証制度でデジタル複合機における普及が進んだのは、調達要件になったからであり、それ以外の製品では認証の取得をアピールせずとも市場が作れたということだ

と認識している。調達要件として市場を守るといった取組を行えれば、足並みを揃えて本制度を普及させることができるのではないかと考えている。

- 強制要件対応については、経済産業省だけで検討することは難しいため、調達担当者と意見交換を密に行う必要がある。
- S マークは、製品安全について消費者が分かりやすく知る手立てになっている。学校教育の中でもＳマークが紹介されている。特に高齢者は、自身で製品のセキュリティ設定を変えることが難しい。そのため、購入したときの初期設定のまま使い続け、事故が起きたときにメーカーや販売店を頼るのが実態である。こういった背景を踏まえると、セキュリティ対策を施した製品を分かりやすいマークで確認できるのであれば、消費者はその製品を優先的に選ぶのではないかと思われる。
  - 消費者は製品の安全性をそこまで意識していないと思われる。知識のある消費者団体がメーカーに働きかけたからこそ、メーカーがＳマークに対応せざるを得なくなったという構図ではないかと推測している。食品にも様々なマークがついているが、それを見て商品を購入したことは一度もない。パッケージデザインや宣伝文句、ネットで調べた情報をもとに購入を決めることが多い。安全性を示すマークは大切だと思うが、それでメリットを感じるのは、エンドユーザーに自信をもって販促ができる小売りなのではないかと感じている。
- 一般消費者に向けてＳマークの認知度調査を行ったが、昨年の結果では 28%に留まり、認知度は決して高くない。大手の電機メーカーにヒアリングを行ったところ、消費者はブランドで製品を選んでおり、S マークを見て選んでいるわけではないとのことだった。そういった状況にもかかわらず、S マークを取得する理由についてメーカーに尋ねたところ、自分たちの身を守るためという回答をいただいた。一度でも失敗をしたり事故を起こしたりすると、即座に市場から退場させられるという状況であるため、身贔屓になりやすい内部評価だけでなく、客観的な第三者認証を受けるため、Ｓマークを取得しているとのことであった。一方、海外メーカーはそういった感覚を持っていないことが多く、例えば、リチウムイオン蓄電池モバイルバッテリーで事故を起こしているのは全て海外製である。そういった部分が日本のブランドメーカーとの違いであり、日本企業の取組を消費者にもなるべく知っていただきたい。
- メーカーが自ら安全性を守る必要があると考えるようになったきっかけが重要だと思われる。セキュリティを自ら守る必要があるとメーカーに認識いただかなければ、本制度は普及しないのではないかと感じた。

- 討議事項①②については、提起された内容に賛同する。最終的には全ての消費者向け・産業向け製品が対象になると認識しているが、ガイドラインや文書、認証制度が存在しない製品カテゴリーをまずは優先的に対象とする方針で異論はない。また、製品カテゴリーによっては厳密な第三者認証が求められる可能性がある。加えて、可能な限り国際基準と整合性が取れ、流用も容易であるような制度であるとありがたい。討議事項③に関して、商品を企画し国内外のメーカーに製作いただいたり、海外メーカーの製品を仕入れ、それを日本で販売したりしている立場からすると、日本市場が魅力的なマーケットでなくなりつつあると感じている。そういった中で、海外メーカーが日本での販売に二の足を踏むことがないようにしたい。適切なセキュリティレベルは担保したいと考えているが､EC サイトでは､S マークを取得しているか識別しづらいケースが多い。S マークの取得率が高い理由についての深掘りは、ぜひ行っていただきたい。
- 産業向け製品に対しては補助金の対象にするといったインセンティブを設けやすいが、消費者向け製品に対するインセンティブを設けることは難しい。企業で購入する場合、調達担当としては事故が生じる可能性を下げるという発想になるが、個人で購入する場合は自身で責任が取れるため安い方が良いという考えになりやすい。メーカーや販売側に対して適切なインセンティブを設けることと、購入する側が安心できる製品を適切に選択できることの両立が、重要だと認識して

いる。

- おっしゃる通りである。消費者向け製品については、インセンティブ設計の手段が限られてしまう部分があり、例えば調達要件に組み込むことは難しい。ブランドアピールといった部分については把握していないところもあるため、丁寧に考えていきたい。

- 討議事項①の製品範囲に関して、基本的に「間接的又は直接的にインターネットに接続する製品」で良いと感じている。総務省の技適では直接的にインターネットに接続する製品のみを対象としているため、より広げた形になるのは方向性として良い。一点気になるのは、製品によって使われる環境が異なるため、リスクも変わってくることである。その点については議論する必要があると思われる。直接的にインターネットに接続する製品に関しては、消費者向けか産業向けかに関わらず対象として良いと思われる一方で、間接的にインターネットに接続する産業向け製品は特異的な部分がある。例えば、医療分野では IoT 製品の使い方が特殊な部分もある。こういった特異性があると、本制度の中に組み込むことは難しいと考えられる。間接的にインターネットに接続する産業向け製品については、消費者向け製品と共通的に考えられるもののみを対象にするといった整理の方が分かりやすいと思われる。
- 討議事項②に関して、ETSI EN 303 645 や他の国際標準化されている規格基準が前提になっているのは良いと思われるが、問題は基準の作り方だと考えている。今年度中に一定のコンセンサスを得ることを考えているのであれば、小規模な検討グループを作り、ETSI EN 303 645 や NISTIR 8425、ISO/IEC 27402 といった基準について、重なっている部分をまとめたうえで、我々としてどの部分を中心として採用するのかを整理すると良いのではないか。その成果について、次回の検討会でご意見をいただくという進め方が良いと思われる。
- 討議事項③に関して、S マークの S はセーフティの S であるため、S の二乗マークといった修正を行うだけで S マーク制度をうまく活用できるのではないかと感じている。消費者やメーカーのインセンティブやモチベーションを高める部分についての整理については、大賛成である。ISMS 認証も第三者認証であるが、はじめはマークについて意識されていなかった。しかしながら、時間が経つと、車に ISMS 認証取得済みのシールが付いているようになった。そういった背景を踏まえると、時間の経過も必要だと思われる。その一つのひな形として、S マーク制度を活用する方針は候補になるのではないかと感じた。
  - RBSS の事例のように、個別の機器に対して基準を定めている分野もあれば、特に産業向け製品に関しては、システム全体で対策を求めている分野が多くなっている。製品類型ごとにリスクが全く異なるというのはご指摘の通りである。リスク評価をどのように行うかについては課題であるが、観念的にはリスクの峻別を行い、それに準じた要件も定義していくべきだと考えている。産業向け製品については特異的に対策が求められているというご指摘をいただいたが、システム全体に関するガイドラインで対策を委ねている分野があると認識しており、リスク分析と要件についてしっかりと検討していく必要があると認識している。討議事項②の評価基準に関して、どのような検討方法が良いかについては事務局内で検討する必要があるが、いただいたご提案についてもその中でしっかりと検討を行っていく。評価基準を専門家の方からも評価いただくことは必要だと考えている。
- 本制度を検討していく際、目的及び論点を把握することが重要である。本制度の目的として明確になっているのは、国際的に商品展開をするベンダーの競争力を削がないようにすることである。産業分野のベンダーの利益のための取組はしっかりと進めた方が良い。既に基準やスキームが存在するところもあり、ベンダー自身も戦略部門で様々な認証スキームの基準について検討し、市場調査をしたうえで対策に取り組んでいる。その取組を阻害しないよう、皆の意見を聞きながら、本制度を検討することが重要である。各論については、ベンダーの意見を聴取しながら知見をまとめつつ、検討を進めていくと良い。
- 家電といった消費者向け製品の安心安全については別の考え方をとる必要があると考えている。産業分野の場合は、作り手だけでなく実装部門や運用部門にも専門家がいるという前提で検討す

ることができる。一方、家電は消費者にとってブラックボックスであり、スイッチを入れればその機能を発揮できる。製品安全法では人損・物損・火災を起こさないことが最低限定められているが、スマート家電の場合、マイナンバーをはじめとした個人情報と紐づくことになる。そうするとプライバシーの関係で様々な守るものが生じてくる。テレビショッピングにおける商品の売り方を見ていると、物を売るだけでなく、保守・メンテナンスのサービスもつけ、割引を行っている。売り手のパワーがあることもあり、安心安全を確保するサービスも一緒に販売している。消費者のセキュリティに関する利益を守る者はたくさんおり、例えば製品安全の S マークでは、損害が生じた場合に補填を行う保険制度も社会的な仕組みとして確立している。

- 本制度の対象は広いため、まだリサーチや目配りができていない領域があると思われる。具体的には、可用性や機密性といったセキュリティに関する観点を考える必要がある。また、どのレベルのセキュリティマネジメントを求めるのかについて検討する必要がある。仕様書に記載された事実を評価するのか、実装された製品の現実的な対策状況を評価するのかの区別もできていない。我々が議論の対象としているセキュリティの要素まで立ち入った議論ができていない。
- 誰のための制度なのかについて想定した方が良い。IoT 製品のうち、弱電分野は要素に分解して検討する必要があり、製品単位で評価する方針で良いのか、構成部品やプログラムまで評価すべきかについて検討した方が良い。また、プライバシー侵害や事故が生じて消費者側から訴えられた場合、設定や宣伝の仕方、保守サービスといった部分も追及の対象となる。関連事業者や費用の負担者といったステークホルダーが複数存在する可能性があるため、間接的にインターネットに接続する消費者向け製品も対象にするのであれば、広く考慮や目配りが必要である。専門家が製造・設置・運用に関わることのできる産業向け製品と消費者向け製品を分けてリサーチし、検討を進めるべきである。
- 特に産業向け製品についての取組は積極的に進めると良い。基準やスキームに関しては国際競争力を考えると国際標準に合わせる必要があるため、その検討を進めるべきである。国際標準が存在しない分野については、我々がどこまで優位を取るべきかについて検討する必要がある。家電といった弱電分野の IoT 製品に関する既存の国際標準があるが、それで十分だとは認識していない。むしろ我々が優位性を取れるのではないかと考えている。優位性を持った認証基準やスキームを作ることができるのかも含めて、検討していく必要がある。対象製品を広く設定し、その中で既に取組が行われている製品を除く方針は現実的であり、産業向け製品についてはその方針で良いと思われる。日本の産業を守り、日本製の製品を国際的に普及させるという視点で考えると、戦略的・攻撃的な観点を持っても良いのではないかと認識している。その検討を行う中で、自己適合宣言か第三者認証かについても検討が進んでいくと思われる。また、サプライチェーンについても検討する必要がある。
- 本制度は法的に重要であるため、必ず普及していただきたい。法的に見ると、セキュリティや安全の責任範囲の分界点は、古典的な考え方のもと成り立っている。要するに、原因を作った者しか責任を負わないということである。本件の場合、原因を作った者とは、製品を作った者や販売した者ということになる。しかし、部品を作った者や販売に関わった者も様々な形で責任を負うことが必要になってくる。端末のセキュリティについては利用者の責任ということになっているが、それで本当に良いのかについて問題提起がなされている。消費者に委ねられていたセキュリティに関する責任は、メーカーや販売者、サービス関連事業者が負うべきだという判決が出ている。これはセキュリティ対策のスコープに関わる議論であり、どれくらいのセキュリティレベルを確保していたかということを伝え合うことが必要になってくるため、認証制度は重要である。あまり急ぐことなく、必要なものを備えた良い制度を作っていただきたい。
  - 皆様からいただいたご意見をしっかりと咀嚼しなければならない部分がある。第 3 回検討会で年度内の議論をまとめて整理を行い、そのうえで大きな考え方を示す必要があると考えているが、それで検討が終わるわけではなく、細かい点から戦略の部分に至るまで、今後もしっかりと検討していきたい。引き続き、ご協力いただきたい。

- 討議事項②について、欧州や米国による国際標準を軸とすることは賛成だが、それらの基準の要素をどれだけ取り入れたかについては明確にしながら検討を進めていただきたい。欧州向け・米国向け・国内向けのそれぞれで要件が変わってしまうと、工場のラインを複数作らなければならなくなる。基準に関して、重なる部分とオリジナルの部分は明確にしていただきたい。また、誰に対してどのようなメリットを与えるために本制度を立ち上げるかについて、メーカーやサプライチェーン、調達者やユーザといったプレイヤーベースで整理をした方が良い。コストをかけることなくすべてのプレイヤーが幸せになるようなことはない。この整理を前提としなければ、議論が立ち返ってしまう。「今回の議論では誰々のメリットを重視する/重視しない」といった方針を決め、議論をするうえでの前提条件を共有する必要がある。
- 社会に対する貢献も重要であるため、視点に入れていただきたい。メーカーにも、二酸化炭素の排出制限や雇用の保護といった様々な社会貢献が求められてきている。セキュリティ対策が十分でない機器が駆逐され、世の中が安全になり、自社製品が踏み台にされることも少なくなるといった、本制度が広まることによる社会的なメリットを示すことで、セキュリティに対する投資やコスト負担、労働力の確保といった議論にも繋がると思われる。
  - 今回の資料はスキームオーナー側の視点がメインになっていると思われる。メーカーのからの見え方についても、今後検討を深めていきたい。社会貢献の部分についても、観点として入れていきたい。
- 討議事項①の対象範囲には概ね同意しているが、「間接的又は直接的にインターネットに接続する製品」という表現は、技術的な観点で見ると曖昧である。より範囲が明確になるように議論を行っていきたい。
- 討議事項②の国際的なハーモナイゼーションが重要であるという点については、皆様の意見と同様に賛成である。任意制度のマークによる簡易表示を前提とするのであれば、評価基準を細分化せず、一つの基準で広い範囲をカバーいただいた方がメーカーとしてはありがたい。同じ製品を出荷しているにもかかわらず、ユーザの使い方によって必要なマークが変わるのはメーカーとしては対応が難しい。法律で定められるのであれば仕方ないが、任意制度のマークであるならば、広い範囲を一つの基準でカバーいただきたい。
- S マークの知名度を活用するメリットは理解するが、S マークを取得している製品が既に数多く存在する中で、セーフティだけでなくセキュリティの意味も付与されることになると、混乱が生じるのではないかと懸念している。既存のマークと新しいマークは違う意味を持つことをはっきりさせた方が良い。
- 特に産業向け機器では、単品で機能することは少なく、センサーやコントローラーといった別の機器と組み合わせてはじめて機能することが多い。そのため、システムとしてセキュリティを守るという観点で作られた様々なガイドラインが既に存在しており、そのガイドラインに沿って対応を行っているという現状がある。単品の機器を本制度で対象とするのであれば、重複する部分が生じると思われる。IEC 62443 に代表されるようなシステムで守るという考え方と単品で守るという考え方がある中で、認証を 2 つ取得するのはコストの観点で現実的でない。そういった動向を確認しながら、議論を進めていきたい。
- メーカーの立場からすると、認証を取ることでどのようなメリットがあるかについて、投資対効果として考える必要がある。強制的な制度であれば対応するしかないが、任意制度とするのであれば、市場原理を考慮して制度設計を行う必要がある。CC 認証や EDSA 認証に取り組んだことがあるが、掛けるコストが市場に見合わず、再度の認証取得には繋がらなかった経験がある。そういった点について、しっかりと議論させていただきたい。
  - 承った。
- PSE マークを取得していない製品が通販で試供品として郵送され、その製品が出火した事例がある。サイバーセキュリティに関しても、対策が十分でない製品について同様の事例が起こり得る。そのような消費者向け IoT 機器がデジタル田園社会基盤に繋がることを危惧している。

- 消費者向けの話なのか作り手側の話なのか、またCIAのどれを扱うのかといった視点が出てきた。観点が広い範囲に及んでいる。
- 用途ごとに認証制度を設けるとメーカーとしては対応できないという意見が挙がっており、何らかの最低ラインが決まるような仕組みとする必要があると考えている。

以上