第１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：2022 年 11 月 1 日（火）14:00 ～ 16:00
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、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 情報産業課、製品安全課、産業機械課、国際電気標準課、通商機構部、独立行政法人情報処理推進機構（IPA）、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）、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）
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　奥田サイバーセキュリティ課長

議　事：

資料 4～資料 7 に基づき、構成員によるプレゼンテーションが行われた。また、資料 8「IoT 製品に対するセキュリティ適合性評価制度の構築について」に基づき、本検討会の背景や設置趣旨、主な検討内容等について、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】

- すべての論点に共通する指摘として、誰のための制度なのかを明確にする必要があると考えている。ステークホルダーは様々であるが、制度の直接的な目的として、誰の利益を想定するかを最初に明らかにした方が良い。そうすることで、論点について具体的に検討できるようになると思う。構成員によるプレゼンテーションに感銘を受けたが「適合性評価結果としての認証」で何を保証すべきかを検討する前に、誰に何をもたらすための制度であるかを検討すべきである。多様な製品のセキュリティに関する様々な取組を行うためには、製品セキュリティに対して長年尽力を重ね、莫大な費用及び人的リソースをかける必要がある。その事実を無視すると利用されない制度になってしまうのではないか。
- ISO に関する議論の中で、規格の具体的な対象やその対象者の利益について、どのような話し合いが行われているのか。対象は一つに定まっておらず、それぞれ分散していると考えるべきか。
  - 規格の対象は規格の内容に依存して変わる。例えば、ISO/IEC 27402 では、IoT デバイスの開発者をターゲットにしようと米国は想定していたと記憶している。また、IoT サービスを提供する者を対象とする規格も存在する。ジェネラルな規格になるほど、規格の対象も広がっていく。適合性評価制度については、対象者を具体的に絞らなければ、議論が発散してしまうと感じている。
- メーカとしては、認証を受けた製品をどのように展開するのか、そして、それが顧客の利益や満足度にどう繋げていくのかが重要と考えている。スコープをきちんと定め、誰がどのように本制度を活かしていくのかを議論していきたい。
- 資料 8 の 21 ページ目の「①消費者向け IoT 製品を対象とした簡易的な適合性評価」と「②Common Criteria 認証・CSA 認証等(IoT 関連製品を対象とした既存の適合性評価)」の間には大きな差がある。Common Criteria 認証や重要インフラや DCS を対象とした ISCI（ISA Security Compliance Institute）は評価基準が厳しい。セキュリティに関するコストは最終的に製品に反映される。ま

た、製品の認証には時間がかかる。ISO/IEC 17025 で認定された試験場を利用しているかは定かではないが、ETSI EN 303 645 の評価を行う台湾の企業が日本に進出してきた。IoT 製品の適合性評価制度はベンダーに負担をかけないような形で実現していくべきだと考えている。その意味で、厳しすぎない規格である ISO/IEC 17025 で認定された試験場を支援することが重要だと感じる。

- 高リスクな製品については、海外で業界標準となっているスキームオーナーが強く、新たな制度をこれから設けるのは難しいと感じている。CSSC をはじめとした国内の制度は、TÜV と比較しても認証数が少ない。そのため、海外の制度と競争を行うより、海外の制度をうまく活用するという方針が良いと感じる。
- 事務局の説明資料にあった課題意識はその通りだと感じる。消費者向け IoT 製品も産業向け IoT 製品も制度の対象とするべきだと考えているが、仮説として示されていたとおり、レベルは分けるべきだと感じる。消費者向け IoT 製品に関する制度は軽いものにするべきだと感じている一方、消費者向け IoT 製品であっても高性能な IoT 製品が増えており、規模によっては企業の拠点で使われることもあると認識している。一番低いセキュリティレベルに企業全体が引っ張られることがあると考えているため、消費者向け IoT 製品であっても最低限のセキュリティ対策は求められるべきだと感じる。監視カメラや SOHO ルータのような IoT 製品を購入する購入者のリテラシーが高いとは限らない。例えば、米国のエンティティリストに載っているようなベンダーのカメラは価格面での競争力が高く、日本で一定のシェアを得ている。エンティティリストに載っているからといって技術的な課題や脅威があるわけではないが、購入者がエンティティリストに掲載されていることを認識して購入しているわけではないと考えている。エンティティリストに載っている IoT 製品よりも危険な IoT 製品についても同様のことが生じる可能性を考えると、これは憂慮すべき事態だと感じており、適切なラベリングを行うことは良いことだと考えている。他方、こうした取組を行うにはコストがかかることは否定できない。適合性評価制度に取り組んだメーカや輸入業者が泣きを見るような事態にならないよう、レベルを適切に設定する必要がある。機器の利用者と提供者それぞれにメリットがある仕組みにしていただきたい。例えば、IT 導入補助金との連携や政府の調達要件になる等、制度に取り組んだ企業にメリットがあるような制度になれば良いと考えている。
- 第三者認証を取得した IoT 製品をどのように購入してもらうかについて検討を行ったうえで、制度設計に取り組んでいく必要がある。この点は普及啓発にも関わる話かもしれない。補助金といった取組は短期的には良いかもしれないが、10 年 20 年と制度を継続していくためには、認証を取得した IoT 製品を購入してもらう必要がある。例えば、国内には Common Criteria 認証で JISEC という制度があるが、国内で認証を取得している IoT 製品の約 8 割が複合機である。複合機の Common Criteria 認証は、米国の連邦調達で成り立っている。制度設計にあたっては、どのような IoT 製品が誰に購入、調達されるかの検討が必要である。
- 構成員によるプレゼンテーションで示されていた「メーカとして適合性評価を検討していく上で、ご検討頂きたい事項」に共感した。
- ラベリング制度を設けるのであれば、有効なのは消費者向け IoT 製品だと思う。産業向け IoT 製品のラベリング制度は無理に設けなくても良いと考えている。産業向け IoT 製品はその製品を組み込んだシステム全体でセキュリティを担保するという考え方があり、IoT 製品を含む個々の要素のセキュリティ要件はシステム設計者の判断に委ねられるべきである。
  - 電安法でも同様の考え方があり、業務用機器は電安法の対象から外されている。業務用機器はプロが扱うものであり、プロは電気機器の取り扱いを熟知しているので電安法により安全を担保する必要はない、という考え方である。
- 義務的な法制度としなければ、制度は広がらないと感じている。Common Criteria 認証を取得したことがあるが、時間やコストがかかる一方、認証の取得が売上に影響を与えなかったため、次の製品からは取得をやめた。認証を取得しても製品の売り上げが向上しないのであれば、認証を

取得するインセンティブがない。事務局説明にもあったとおり、2023 年～2025 年には英国や EU のセキュリティ制度が義務化されるため、その対応が社内で喫緊の課題となっている。こうした強制力がない限り、メーカは重い腰を上げないのが現状である。

- バランスを取っていかなければ、議論は収束しないと感じている。自社製品の購入者の中には、IT に詳しくない方も多い。そのような方に対して、自社で作成した資料をもとに説明を行っており、その説明に納得して購入する方も少なくない。一方で、ラベルを付与することでセキュリティ対策について購入者が理解や納得するかを懸念しており、むしろメーカがセキュリティ面での安全性を丁寧に説明することが大切だと考えている。つまり、ラベリング制度の知名度を上げる努力をしない限り、メーカの説明コストは変わらないという印象を持っている。そのため、本制度の普及活動を消費者向けに行う必要があると考える。
- IoT 製品のサイバー保険のような目に見えるメリットがあるのは良いと感じた。消費者に対しても説明が行いやすくなる。制度設計を行うにあたって、どのような基準を定めるのかについてはメーカのメリットを鑑みつつ、検討を行っていただきたい。
- 消費者によってスキルやリテラシーには大きな差がある。
- どこまでが消費者向けで、どこまでが産業向けなのかが不明瞭である。日本には、中小企業や個人事業主のように、消費者に近い立場の事業者が多く、消費者向け IoT 製品の範囲をどのように定めるかが難しいと感じた。消費者としては安心感が生まれるため、ラベリング制度があると良い。また、強制的な制度にすることで、少し値段が高くても安全性の高い IoT 製品を選びたいという消費者のニーズに応えられる。制度の検討を始めた段階から広報を行い、セキュリティの確保を行ってラベリングを付与するためにはコストがかかるということを啓発していく良いと感じた。
- 強制的な制度としなければ、事業者は制度に参画しづらいと思う。CCDS サーティフィケーションプログラムのように保険がつくような制度であれば、何か問題が生じた際に保証されることが分かるため、消費者にとって理解がしやすい。
- 消費者の概念は多様であり、事業者や製品によっても変わるため、「消費者」を定義することは難しい。PL 法のように、個別の使い方という観点から考えるも一つの手かもしれない。
- 法的に義務化すれば、制度が活用されるようになると思う一方、義務化には責任も伴うため、慎重に検討した方が良い。
- リテラシーの低い利用者に対して、安全な IoT 製品を届けることが本制度の最終的な目的だと考える。また、本来は問題が生じた際の法的な責任の追及を容易にするという目的も設けられることが望ましいが、実現には課題も多く，まずは直接的な目的とせずに出発するのはやむを得ないであろう。消費者を保護するためには、保険制度をうまく取り入れるべきだと感じた。様々な取組を行っているメーカを制度の直接的なターゲットにする必要があり、市場の確保や国際的なハーモナイゼーションといったメーカの利益について検討していく必要がある。また、大きな投資のもと行われているメーカの現在の取組を阻害することのないよう、それを守って育てていくような方向でも制度を検討する必要がある。
- 既に販売されて運用されている IoT 機器は本制度の対象とせず、これから開発する IoT 機器を対象とすることが大前提である。同じ IoT 機器であっても、消費者向けに使われる場合と重要インフラ向けに使われる場合があるため、対象とする機器の検討が必要となる。
- 米国の CISA が試験制度を設け、実験環境での評価を行うという制度を立ち上げたが、失敗したこともあり簡易的で適切な方法で評価を行っていく必要がある。
- IoT 機器の脆弱性や脅威分析に関する取組と連動するようなスキームがあればより良いと感じる。
- 消費者向け IoT 製品からスタートし、様々な課題を整理していくことが重要だと考える。
- 強制的な制度とするのか、対象製品をどのように定めるのかという点は、まだ定まっていないが、今後の検討で少しずつスコープを絞っていければ良いと思う。

以上