第5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10月3日（火）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、江崎委員、高橋委員、中尾委員、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（NISC）、総務省サイバーセキュリティ統括官室、経済産業省航空機武器宇宙産業課、国際電気標準課、独立行政法人情報処理推進機構（IPA）、独立行政法人製品評価技術基盤機構（NITE）、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）、公益社団法人日本防犯設備協会（SSAJ）、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）、一般社団法人日本電機工業会（JEMA）、一般財団法人日本品質保証機構（JQA）、一般社団法人ビジネス機械・情報システム産業協会（JBMIA）、一般社団法人セキュアIoTプラットフォーム協議会（SIOTP協議会）、ロボット革命・産業IoTイニシアティブ協議会（RRI）
事　務　局：経済産業省　商務情報政策局　サイバーセキュリティ課　山田企画官、味木課長補佐、木本課長補佐、前田課長補佐

議　事：

資料3「IoT製品に対するセキュリティ適合性評価制度に関する実証について」に基づき、適合性評価制度の実証方針について事務局より説明が行われた。つづいて、資料4「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、認証スキーム体制、本制度における☆1 の位置づけ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】

- 本制度が☆1から☆4までの4段階に分かれている根拠をご説明いただきたい。
  - ☆2以降については今後詳細化する。シンガポールのCLS(Cybersecurity Labelling Scheme)を参考に、一旦☆1から☆4の4段階としている。☆2以降については今後の検討会で意見をいただきたい。
  - 表において☆2以降の内容が埋まっているが、今後議論して詳細を決めると理解した。
  - 本制度を4段階にすることについては、まだ決定されていない。☆1は全ての製品類型に共通する最低基準で、☆2 から☆4 は製品類型ごとに異なる基準を設ける予定である。制度の観点から言えば、☆2 では検証事業者の利用が想定されるが、第三者評価を必須とするわけではない。一方、☆3と☆4では第三者評価を必須とする予定である。☆3と☆4を2段階に分けた理由は、一部の製品類型には2段階の要件が必要と想定しているため。☆3のみにするか、☆4も設けるかについては今後の検討に委ねられる。
- ☆1の位置づけについて、セキュリティ脅威に関連する部分で、個人情報に言及すべきである。ユーザに対してIoT製品が個人情報を扱うことを明示することも、非常に重要な要素だと考える。また、扱う個人情報を具体的に列挙することは、☆1の段階で要求するべきと感じる。
  - 個人情報の取り扱いについて、プレ検討委員会においても議論となっている。プレ検討委員会の議論を踏まえ、☆1 で具体的にどのような個人情報を保護すべきかを明確に記述する予定である。

- 資料 4 P.11 に示されている☆2 以上の守るべき資産について、「製品本来の機能」「セーフティ関連機能」「人的資産」「物理的資産」などを含み、広範である。セーフティ関連機能については既に標準が整備されている。また、製品本来の機能に関しても、例えばドローンの場合、国土交通省で耐空性に関連するセキュリティ要件についての規格の検討が進められている。将来的な検討においては、これらの既存の取り組みと調和させる必要がある。
- 「ラベル取得が想定される主な製品」の 2 つの記述について、同意できない。IoT 製品は広範で多様なものに接続されている。したがって、☆1 で、ホームユースやプライベートユースに限るべきではない。☆1 は IoT 製品に最低限適用すべき基準であり、☆2 は製品類型ごとに存在する特殊なセキュリティ要件に対応するために満たすべき基準と考えている。ホームユースやプライベートユースに絞り込むと、☆1 が不十分なものになる可能性がある。
- 「考慮すべき主なセキュリティ脅威」について、選定した理由を明確にし、論理的な図を作成するべきである。
- システム全体でのセキュリティ防御に関して、産業サイバーセキュリティのガイドラインが作成されている。現在、工場 SWG がガイドラインを作成し、さまざまな業界での強化策を実施している。これらの業界には、化学、鉄鋼、半導体、自動車などが含まれている。
  - 防御だけでなく、システムが侵害された場合の復旧力（レジリエンス）も考慮する必要がある。
  - 機器に関する基準と、システム全体に関する基準の 2 つが扱われている。また、システムが侵害された場合の事前対策と、インシデントが発生した場合の対応に関する体制、ガバナンス、技術についても記述されている。大企業だけでなく、人員を十分確保することが難しい中小企業における議論も行っている。
  - システム機能停止に至った際の、システム全体や制御系における許容時間など、デグレードの許容範囲について設計者が考慮する必要がある。そのための判断材料として、本制度の認証レベルを参考にしていただけると良い。
  - 対策の等級については、各業界で議論されていると考えられる。ただし、国の施設や経済安全保障に関連する重要なインフラなどについては、国と産業界での議論が必要になる場合がある。

次に、資料 4「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、セキュリティ事案への対応、制度活用を促す仕掛け、今年度の検討方針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】
- 資料 4 P.13 注釈 2 の「一定基準のセキュリティ対策を行っているとみなせる」の意味について、明確な理解が必要である。ここでの「みなせる」は法的な文脈での使用に関連しており、命題に対する反証を許さないことを指す。「認証を受けたこと」に関しては否定されない事実である。ただし、「適合基準に適合していること」については、反証を許さないものではない。事故が発生した場合、認証自体や認証に関連する行動の妥当性などが争点となる。この場合、認証を受けたことが直接的に対策を行ったという結論を意味するわけではないが、間接的な事実として、一定の対策が行われたと推定される可能性はある。
- 自己適合宣言時に、サーベイランスにコストをかけることについて疑問を抱いている。自己適合宣言は、メーカが規格と評価基準、認定方法に関する情報を適切に収集し、合理的な推論で認証したことを宣言するものであり、製品の品質に関する宣言にとどまる。本制度において、IPA は責任を負わないとしている。責任を負わない主体が制度を構築した場合、制度を利用する側には、メリットが不明確で、運用者のための制度と感じられる。また、サーベイランスを行うことでメーカに追加のコストがかかることも問題である。自己適合宣言ではなく、第三者認証で責任を負

う主体が存在する場合、サーベイランスが適切かどうかを考慮する余地はある。レベルに応じて検討することが良い。

- 認証機関の責任については、免責が設けられているが、サーベイランスは制度を悪用しようとする者に対する抑止力になると考えている。実際にどの程度のサーベイランスを実施するかは、認証取得製品によるところがあるため、判断が難しい部分もある。通報が寄せられた場合、品質確保のために認証機関でサーベイランスを実施する可能性もある。予算の確保といった課題や、メーカにとって価値のある制度とすることが重要なことは認識している。
- 責任を負う主体によって制度が構築されることを強く望む。日本国の競争力を培うためには責任を負う主体が制度を構築する必要がある。メーカからすると、責任やファンドについてどのように対処するかという問題が解決されない限り、制度への参加が難しい。実際には多くの制度で同様の問題が存在し、セキュリティ監査、システム監査、会計監査などもその一例である。したがって、段階的に進める必要があると考えているが、少なくとも IPA においては、制度運営者の監督、製品に関する評価、そして設計レベルの評価等について責任を負う必要があり、何らかの責任を果たさない限り、制度自体が活用されない可能性が高い。サーベイランスに関しても、中央集権型の組織が責任を負うことで成り立っている。責任の所在が明確でない制度でサーベイランスを進めるべきかどうかについて疑問が残る。保険数理には適合しないが、責任や需要のレベルが明確になった段階で、民間でファンドを設立する、税金によって国民の負担でファンドを設立するなど、保険制度についても検討すべきである。また、責任の追及を容易にする制度設計も重要である。被害が発生した場合、集団訴訟のような手続きで被害者全体を救済できる制度も検討するべきである。他国の制度を単純に模倣して実現できるような簡単なものではないことを理解していただきたい。
- サーベイランスに関して、メーカとしては自己適合宣言を得るために必要な要素とも理解できる。本来、第三者認証が必要なはずの製品が、自己適合宣言を通じて低コストで認証を得ることができる。しかし、その代わりに、サーベイランスによってランダムに検査され、違反があれば認証が取り消されるという抑止策が存在するため、不適切な自己検査は行えない。

- 例えば、ファームウェアのアップデートがある場合、特に発売後に実施されるアップデートの判断方法について、今後議論させていただければと考えている。ラベルの表示や QR コードの遷移先による情報提供を通じて、前提条件（評価日、評価時のファームウェアなど）を確認できると良い。なお、アップデートができない又はしないユーザも存在するため、そのような場合の対応についても検討が必要である。セキュリティアップデートの提供は、製造者としての責任と考える。一方で、セキュリティアップデートを適切に適用することも、ユーザとしての責務であることを強調すべきである。諸外国で既に運用されている取り組みで、この点に参考になるものがあれば、ご紹介いただきたい。
  - 消費者がアップデートを行わないという問題は、非常に重要な指摘だと考えており、ユーザの設定や使用方法に起因してインシデントが発生する可能性は十分にある。制度全体で、利用者と調達者に対する啓発活動に取り組むべきだと認識している。消費者に対して、適合性評価制度そのものの普及だけでなく、セキュリティに関する消費者の責務についても伝える必要がある。具体的なアプローチを検討しながら、国内外の状況についても調査を進めていく予定である。
- 有効期限について、本制度案では有効期限がサポート期限と解釈される可能性がある。アップデートだけがサポートではない。サポート期間に関する要求もメーカに求める場合は、その内容も含めて要件に明示的に記載する必要がある。一方で、セキュリティは時間とともに弱化するものであるため、設定された要件を満たすことはその時点での証明であり、有効期限を設ける必要はない。サポート期間の設定が必要であれば、それに関する要件を明確に制定する必要がある。
- 有効期限について、メーカ側から見た有効期限と認識した。製品のリリース日を起点としている一方、ユーザの視点からは購入日が重要である。期限の設定ついては、複雑で、継続的な議論が

必要だと考えている。

- アップデートに関しては、提供者側とユーザ側の責任が存在する。責任の範囲についても検討課題として考慮されるべきである。
  - ベンダーの視点からすると、有効期限の設定が柔軟にできる方が良いと思われる。他方、消費者への通知を適切に行う必要がある。通知方法について、ラベルや QR コードを使用した方法を考案しているが、より分かりやすい通知方法について具体的に検討する。
  - アップデートに関して、消費者が適切に行わないこともある一方で、メーカがその手法や重要性を分かりやすく伝える責務があると考える。両者における責任のバランス感覚は非常に重要だと認識しており、そうした観点も踏まえて適合基準や普及啓発について検討していきたい。
  - EU CRA（Cyber Resilience Act）では、製品の寿命を明示し、アップデートの目安を 10 年と設定することなどについて議論している。この点も考慮しつつ検討していただきたい。
- 認証取得を訴求し、セキュリティレベルを向上させようとする取り組みは素晴らしいと考えるが、その要求方法が重要である。認証取得製品の使用を強制するアプローチは違和感がある。なぜなら、認証を取得していないという情報も、システムのセキュリティを向上させる上では、重要だからである。製品自体のセキュリティレベルと、システム全体で保護する方法には密接な関係がある。そのため、認証を取得していない製品や、製品の認証レベルに基づいて、システム設計時に検討すべき要素を訴求する方法が良い。初めは認証を取得していない製品が多いため、調達要件を普及度に合わせることが重要である。
- ユーザの責任や普及啓発策、需要喚起策について、消費者のレベル（セキュリティに対する知識への有無）を分けて考える必要がある。また、製品の生活への影響度を考慮に入れるべきであり、セキュリティ対策について受動的な姿勢の消費者がいることを考慮すべきである。それぞれの区分けに基づいて、具体的な対策と費用を考えることが重要である。例えば、家電製品などでは、消費者にバージョンアップを要求すべきでないと考える。何故ならば、バージョンアップを適切に行わない場合に責任を追及することは、これまでの家電製品の文化とは大きく異なるためである。また、制度運用にかかる費用は相当なものとなる可能性があり、負担できる主体が責任を負う必要がある。消費者のレベル分け、責任の範囲、費用、社会的な資金の流れを考慮しながら検討していただきたい。
  - 同意である。消費者側の知識や能力の差異を考慮していただきたい。
  - ユーザの責務について、ユーザを消費者及び法人で分けて考えるべきである。今回の☆1 において主要なユーザが消費者であることを考えると、ユーザに過度な責務を負わせることは問題であると感じる。例えば、セキュリティアップデートについては、自動的に実施される仕組み（Windows Update など）をメーカが提供することが理想的である。ただし、ユーザが設定で自動更新をオフにすることも可能な場合がある。そのような場合にユーザを免責にすることは、メーカとしては納得できない。
- 製品の寿命が長い場合、サーベイランスが適切だが、IoT 製品など寿命の短い製品に対してサーベイランスを行うことは、コスト面で疑問視される。評価機関が積極的に参入するかどうかも不明瞭である。日本国内の企業が国外の評価機関を使用している中で、この制度が普及するかどうか不透明である。責任問題は重要であるが、審査を簡素化し評価機関の持続可能性を確保する必要があると認識している。
  - サーベイランスの仕組みや評価機関を含む制度の仕組みについては、今後も検討を継続していく。
- 有効期限について、言及されている「サポート」は、セキュリティアップデートを含むものと理解している。表現がわかりにくい場合、言葉の更新を検討するべきである。メーカにとっての「サポート」はセキュリティアップデートに限定されず、セキュリティアップデート以外の内容が含まれないようにしたい。

- 有効期限の「ラベルへの表示」は、ラベルを交換しなければならない手間を考慮すると避けるべきである。情報へのアクセスが QR コードを介して行われる場合、小さな製品では本体への表示が難しいこともあるので、梱包箱や取扱説明書に情報を記載する方法も許容していただきたい。
- 保険制度の活用について、前例がないことを理由に導入しないと結論付けることに疑念がある。また、資料には「☆1 では自己適合宣言をするため保険料の料率が高く、IPA と保険会社が一括契約を結ぶことは現実的でない」と記載されているが、「検証事業者の評価機関のとりまとめ団体を契約者とすれば保険料が安くなる」旨が記載されており、矛盾を感じる。CCDS のように、制度内で保険を適用し、運用している民間企業が存在するため、公的機関が同じように対応できないことに疑問を感じる。制度の普及を促進するためにも、セーフティネットとしての保険が必要であり、公的機関としてその負担を引き受けるべきだと考える。
  - 誤解を招く表現であったため、「いくつかの方向性が考えられるが、公的機関がサイバーセキュリティ保険を一括契約した前例がなく、自己適合宣言を採用する以上は認証機関が確認できるセキュリティ深度に限界があることを踏まえると、IPA が保険会社と一括契約を結ぶことは現実的ではない。」と訂正させていただきたい。公的機関が保険を契約することは実現が難しいと理解していただきたい。
  - 自己適合宣言において保険料が高くなることから、保険を提供できないという状況は、誰を守るための制度なのか明確でない点に疑問を感じている。我々は消費者保護とボット化対策に焦点を当てており、現在の状況を改善し、制度設計を進めるために、責任の所在を明確にしながら検討を進めていただきたい。
- 既存の保険や情報セキュリティ早期警戒パートナーシップ制度だけでなく、より包括的なアプローチが必要である。保険数理と業規制の拘束を強く受ける保険だけでなく、より柔軟な制度設計が可能となる信託制度を活用し、社会的に校正して制度運用の資金供給に利用するなども考慮し、より幅広い視野で検討することが望ましい。
- 情報セキュリティ早期警戒パートナーシップとの連携について、高いレベルでは早期対応につながると感じる。しかし、IoT 製品を対象とした脆弱性の共有に関して、パッチが完成し、メーカの準備が整った段階で情報を提供する仕組みがまだ整備されていないように感じる。今後この箇所について具体的に考えていく必要がある。
- アップデートのタイミング、有効期限の起点、責任範囲、費用負担など未確定な点が多い。保険は、技術や制度では対応できない、想定外の事態に備えるためのものである。しかし、誰も責任を負わない状況で保険を導入すると、事故率を計算できない状態で保険が提供されることになりかねない。制度を構築する責任、検査を実施する責任など、責任の範囲を明確にしないと保険制度が機能しない。
- 情報セキュリティ早期警戒パートナーシップについて、国内に数が多い製品であれば情報共有が可能だが、国内に数台しかない製品では情報共有が難しい場合がある。制度の対象製品に関して、使用されているデバイスに関してはパートナーシップが効果的であると認識しているが、輸入の妨げにならない範囲で検討する必要があると感じる。
  - 情報セキュリティ早期警戒パートナーシップだけに依存することは難しいと感じる。現実には様々な状況があるため、これらを考慮しつつ検討を進めたい。

以上