第 4 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 7 月 19 日（水）16:00 ～ 18:00
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、中野委員、花見委員、広瀬委員、唯根委員

オブザーバー：一般社団法人情報通信ネットワーク産業協会（CIAJ）、重要生活機器連携セキュリティ協議会（CCDS）、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）、一般財団法人電気安全環境研究所（JET）、経済産業省製品安全課、産業機械課、航空機武器宇宙産業課、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、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）、一般社団法人日本電機工業会（JEMA）、制御システムセキュリティセンター(CSSC)、独立行政法人製品評価技術基盤機構(NITE)、一般社団法人ビジネス機械・情報システム産業協会（JBMIA）、ロボット革命・産業 IoT イニシアティブ協議会（RRI）、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）、一般社団法人組込みシステム技術協会（JASA）

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

議　事：

資料 3-1「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。

資料 3-2「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、主な検討内容について事務局より説明が行われた。

資料 3-3「IoT 適合性評価検討会資料」に基づき、認証スキーム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】

- JISEC 制度を発展する方向性は大変よいと思う。人材育成や責任分界点の枠組みが既に検討されており、従来の認証に関する枠組みの反省を踏まえた検討がなされていると感じた。今後、保険等の責任を社会全体で負担する仕組みを考慮しつつ制度を構築していけると良い。
- 適合性評価の対象が設計段階に限られているように見受けられた。しかし、設計段階と実装段階で、ベンダー側で対応すべき内容は異なる。また、消費者向けと重要インフラ向けの IoT 製品でライフサイクルが大きく異なることに加え、利用者の保守・運用に係る知識の量も違う。評価基準を考慮する際には、対策の実装段階、ライフサイクル、利用者の保守運用能力を考慮していただきたい。
- コストについて検証することは優れた点である。制度の維持や人材育成にかかるコストが検討されてないために普及が進まない制度もある。今回の実証で評価者のコストを検討するとしているが、本制度は国際的な相互承認を視野に入れており評価基準が変化する可能性を加味して、追加で 2 つ検討いただきたい。
  - 評価者が基準の変化に追随するためのコスト。
  - 自社製品に対する社内の手続きを変える等、評価基準の変化に対応するためのベンダー側の

コスト。

- 本制度は社会インフラの一環になると感じる。そのため、医療費のように、社会的にコストを負担する構造も考えていく必要がある。これは個社が利益を受けるという考え方ではない。社会の関与の仕方も念頭に置きつつ、本制度について発信することが望ましい。
- 評価コストについて、時間的な流れを考える必要がある。IoT 製品は、ライフサイクルが比較的長く、ライフサイクル全体に渡ってサポートする必要がある一方で、消費者のようなセキュリティについての知見がない人も利用者として想定されることが懸念事項である。家電業界は機能維持の知見を持っているため、家電業界とも協力しつつ、製品の能力維持に関するコストについて検討していただきたい。
- 責任分解の問題を議論するにあたって、契約書モデルや契約条項モデルを作ることで具体的な議論を行うことができる。
- 制度において、コストとスケーラビリティは重要な観点である。本制度が成功した場合のことを考えておいたほうが良い。例えば、ISMAP の制度はすべて IPA で審査するという形式だが、さらに制度をスケールさせるために、軽量の位置づけである ISMAP-LIU を新たに構築した。IoT 製品は対象が膨大で、評価対象が多くなる懸念があるので、国が主導で実施する部分と産業界に委譲する部分を明確に分けた方が良い。本制度を運用するコストがすべて国に依存しない仕組みが必要となる。
- 適合性評価に用いるツールを OSS として無償提供することは制度にとってプラスに働く。ツールが無償提供されることで、検証ビジネス事業者にとってはビジネス展開が容易になるほか、制度運用側にとっては、評価方法が標準化されることで一定程度の品質保証に寄与する。携帯電話やスマートフォンの検証ビジネスはうまく運用されているため、このような既存の取組を参照しつつ、本制度を検討していくと良い。
- 今回の制度では IoT 製品を評価対象とするが、システム全体に対する対応は IPA のデジタルアーキテクチャ・デザインセンター（DADC）で検討していると認識している。DADC の取組と連携しつつ、本制度を構築することが重要である。
- 人材育成を IPA が意識していることは評価したい。資源エネルギー庁の会議において、システムを適切に発注できる人材の不足が問題視された。政府が調達するシステムに関しては、スペックを適切に確認する人材が必要となる。民間では、ビジネスを発展させるために、調達に関する知見を持った人材を保有している。人材育成に関して、IPA に閉じた検討をするのではなく、民間と連携することが重要である。
- 制度の基準に関する議論において、ユーザー（調達者）組織の参画が重要となる。政府もある意味ユーザー組織であるが、ベンダーだけで基準を議論するのではなく、ユーザーも含めて基準を議論することが重要である。
- ☆1 で自己適合宣言を採用する方針に同意する。そのうえで、セキュリティの知見が不足するベンダーも多く存在するため、本制度に関する教育プログラムやセミナーを開催することを検討いただきたい。関連する取組として、輸出管理規制に関する取組が挙げられる。輸出管理の法律が毎年変わることもあり、それに合わせて毎年セミナーが開かれる。ベンダーの視点では、変動する法律に対して質問する先を持つことになるほか、社内で知見を有した人材の育成にもつながる。
- 今年度はプレ検討委員会で適合基準を議論するということであるが、運用が始まった後でもベンダーの意見を反映できるような体制を構築していただきたい。
- 普及活動について、家電量販店や通販サイト等の販売者に対する広報も必要となる。販売者に対して、今回の適合性評価の制度やマークについて分かりやすく説明することも普及活動に含めていただきたい。特に家電量販店では製品に関する情報が過多となるため、本制度にうまく誘導できるような広報活動が必要となる。
- 資料で示された方針に賛同する。そのうえで、☆2 以降で製品類型ごとに基準等を策定するとのことであるが、どの製品類型に該当するか分からない製品も出てくるだろう。その場合に相談で

きる窓口があると良い。

- ☆1 の自己適合宣言に関して、ランダムで製品の試買テストを行うなど、自己適合宣言の品質を担保するための仕組みが必要になる。
- コストがかかる取組であるので、インセンティブも検討していただけると良い。適合性評価ラベルを取得していれば補助金対象にするなど、ベンダーが取り組みやすくなる仕組みがあると良い。
- 本制度は非常によく練られていると感じる。そのうえで、本制度を活用・運用していくため、時間軸を意識する必要がある。例えば、技術的な進歩に合わせて基準を更新する必要があり、どれほどの頻度で更新するのか等、別途更新の仕組みを考えておくことが重要である。また、ベンダーが認証を受けた際に、何年度に認証を受けたのか確認する仕組みが必要である。加えて、ライフサイクルが長い製品では、部分認証・部分評価ということも起こりうると考えている。時間軸を意識した検討をお願いしたい。
- 4 段階のレベル分けについて各段階の定義を詳細化する必要がある。本制度は製品ベースの認証制度であるが、同じ型式・製品であっても用途が違えば、求められるレベルは異なると考えている。例えば、サーバやルータは重要な場所で使用されている場合もあれば、家庭レベルで使用されている場合もある。そのため、レベル分けにあたって、製品の用途を考慮いただきたい。これは責任分界の議論にもつながると考えており、調達者として特定のシステムに利用する製品を選定する際、どのレベルの製品を調達すべきかの判断材料となり、結果として調達者や利用者においても責任が生じることになる。
- 今回の検討会は、今後制度設計を具体的に行う上での非常に良いスタート地点だと感じる。実証を行う際に、実証結果から制度の改善点を見つけ出せると良い。
- 全ての IoT 製品の類型に対して基準を作ることは不可能であるため、製品をうまくグルーピングする必要がある。ISO/IEC 27404 では消費者用 IoT 製品のみを対象としているが、産業用 IoT 製品が対象に入ると整理がかなり困難になる。シンガポールの CLS においても消費者用 IoT 製品のみを対象にしているが、別途、医療機器を対象としたラベリング制度を構築している。諸外国の取組等を参照しつつ、本制度の検討を進められると良い。
- 国内で複数のスキームが林立することは良くないので、スキームの統合について引き続き検討していただきたい。
- 相互承認の仕組みは非常に重要である。ISO/IEC 27404 においても相互承認の重要性が挙げられている。日本の制度が国際的にガラパゴス化しないようにしたほうが良い。諸外国の制度を整理し、日本が相互承認を発信するための基盤を構築することが理想である。
- 時間軸を持った制度設計に賛成である。ISMS では年に一回の頻度で見直しを行うなど、有効期限を設定して、認証を行う仕組みを採用している。IoT 製品のライフサイクルの話題が挙がったが、IoT 製品の脆弱性をどのように検知・共有・活用するかといった課題もある。IoT 製品独特の事象を考慮して制度を設計する必要がある。米国で検討している制度では、認証した製品に対して QR コードを発行し、利用者がそのコードをスキャンすることで、Web 上で製品の詳細なプロファイルを確認できる。アップデートはリンク先で反映するといった手法もあるので、脆弱性管理とうまく連動できればと感じる。
- 基準更新のタイミングは重要である。技術進歩や脅威の状況により求められるセキュリティ対策は日々変化する。更新のパターンやタイミングを検討するとともに、更新した基準を満たしていることを利用者にどのように提示すべきか、今後議論が必要である。特に消費者は見た目を重視して製品を選定することが多く、更新のタイミングでマークを変更することも想定される。一方で、ベンダーの視点から言えば、マークの変更やパッケージの変更に対応することはコストになる。適切な対応方法が議論できると良い。
- 海外との連携について、国際的な相互承認が理想であるが、困難であれば、制度間の要件の差分を確認して部分的に評価するといった仕組みも考えていければ良い。
- 自己適合宣言の運用モデルをいくつか考える必要がある。ベンダーによっては、開発部門が自己

適合宣言する場合もあれば、品質保証部門が自己適合宣言に対応する場合も想定される。自己適合宣言の運用モデルやベストプラクティスが提示されることで、ベンダーとしては対応しやすくなる。

- ISO/IEC 17025 のレベルで全ての評価機関の適格性を担保することは難しいのではないか。評価ビジネスが成立するためには、評価機関が多数の製品を評価する必要がある。新規参入した評価機関の場合、評価の人材が不足する可能性があるため、評価を行う人材の育成も意識することが重要である。
- 消費者の視点では、IoT 製品のセキュリティ対策状況が可視化される本制度は非常に有用である。可視化の仕組みの例として、冷蔵庫の性能に関するスターマーク（JIS C 9607:2015）や統一省エネラベルが挙げられる。セキュリティについても同様に、消費者が調達時に参考にする指標の 1 つになっていければ良い。本制度は社会インフラの一部となるので、消費者も社会的コストを担っていく一員としての理解や知識を持つために行政等からの教育や啓発が必要である。
- 本日の検討会の一番の論点は、製品安全の制度をベースとした適合性評価制度から、JISEC 制度を発展させた制度に舵を切ったことと理解している。そのうえで、特に時間軸に関する議論は重要である。本制度を立ち上げると、10 年～20 年と基準は変わりつつ継続していくものである。JISEC 制度は IPA が運営しており、本制度も IPA が運用していくことになると思うが、制度維持に向けた予算については検討しているのか。METI から予算が捻出されると推測しているが、その予算が削られると制度運用は認証申請費用との兼ね合いになり、ベンダーの負担が大きくなる可能性がある。制度の継続的維持のためには、開発・認証・購入のサイクルを回す必要がある。そうでないと、制度が利用されず、予算も多く割かないと維持できない制度になってしまう。如何にして本制度の認証を取得した製品が、利用者に優先的に購入してもらうのかを検討することが重要である。
- 適合性評価済み製品に関する最新情報に辿り着けるような仕組みを検討していく必要がある。いつ認証を取得したのか、いつまで有効なのか等の情報が明確に取得できるラベルを検討する必要がある。QR コードを付けることも 1 つの手段である。
- 各国制度との連携方針は悩ましい。経済産業省や IPA でまとめていくことになると思うが、国内だけの独自ルールとならないようにしていただきたい。
- 政府調達時にセキュリティが脆弱な製品が紛れた場合の対処法についても検討する必要がある。本制度も重要であるが、仮に本制度をすり抜けた場合にどのような対応をするかについても、別途検討が必要である。
- 中古の IoT 製品を入手した際に、どれほどのセキュリティ対策が講じられているかが分かるような仕組みも構築できると良い。
- 怪しい製品を紛れ込ませないような仕掛けとして、適合取得年度を示すことも考えられる。サプライチェーン全体でトレーサビリティを確保することも重要であり、QR コードで情報を示していくことは、昨今の一つのトレンドであると感じる。例えば欧州の GAIA-X においても、製品の情報を QR コードで取得し、システム構築時には、構成要素となっている全ての製品の管理を行えるといった取組も行われている。このような技術は参考になるのではないか。
- 本制度の主眼の一つは、IoT 機器へのサイバー攻撃から消費者、会社、そして国を守ることである。IoT 機器の脆弱性を減らすために、広くセキュリティレベルを上げていければ良い。
- 技術の進歩に従って、セキュリティ要件を更新していくことが大切である。
- IoT 機器だけでなく、IoT 機器を活用したシステムやサービスにも対応した適合性評価制度の検討を進める必要がある。調達者側に役立つスキームを構築することで、広く普及すると考える。

以上