# 第７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：2024 年 3 月 4 日（月）10:00 ～ 12:00
場　所： Teams 開催
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、松浦委員、唯根委員

オブザーバ：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、経済産業省製品安全課、航空機武器宇宙産業課、国際電気標準課、産業機械課、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）、一般社団法人組込みシステム技術協会（JASA）、技術研究組合制御システムセキュリティセンター（CSSC）、一般社団法人電子情報技術産業協会（JEITA）

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　武尾課長、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結果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、各レベル（☆1～☆4）の位置付け、調達者の本制度活用に関する調整状況、本制度の賛同団体、有効期限の設定、ラベル及び情報提供ページ、本制度のロードマップ案について事務局より説明が行われた。最後に、「IoT 適合性評価制度に関連する ISO 国際規格化の動向」に基づき、ISO/IEC 27404 の動向について中尾委員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】

- ラベル発行者についての要件と定義は、国際規格ではどのように規定しているのか。我々が検討している制度との調和を図るため、この点を参考にしたい。
  - 現時点では、ラベル発行者について、ISO/IEC 27404（Draft）では明記していない。この点については今後整理が必要であるが、国際規格に単純に合わせるのではなく、シンガポールやイギリスなど、既に検討が進んでいる国を参考にしつつ、様々な国も含めて調整を行う形になると考える。

- 1 点目、ラベル発行者に関する記載の拡充が必要である。スキームオーナーと認証機関が存在するが、IPA はいずれに属するのか。また、スキームオーナーを、公的組織または民間組織のいずれが担うかについても検討が必要である。時間の制約もある中、国際規格とのハーモナイゼーションが優先される場合は、これらの検討を後で行うことも構わない。前述の検討が必要な理由を

2 点述べる。1 点目、ラベル発行に関しては、特定の手続きで何かしら条件を満たすことを確認した上でラベルを発行することとなり、この行為には責任が伴うからである。2 点目、ラベルの情報に信頼性を与えて表示することから、ラベルが偽造された場合には差し止めるための法的な権限を持つ主体が必要なためである。具体的な事例として、☆1 のラベルが偽装され、宣伝や勧誘に利用される可能性が考えられる。これを阻止・是正するためには、ラベルを付与する主体を適切に配置する必要がある。ラベルを付与する主体に公的組織を仮定する場合、ラベルの偽造に対しては刑法における公文書偽造が関連する。一方、ラベルを付与する主体に民間組織を仮定する場合、ラベルの偽造に対しては商標による保護が考えられる。そのため、商標の帰属先を明確にすることが重要である。商標の場合、日本国内での刑法の適用範囲も考慮に入れ、国際的なハーモナイゼーションについても包括的に検討する必要がある。

- 2 点目、消費者契約法の観点においても検討が必要である。ラベル取得製品の利益を示し、国としてラベル取得製品の使用を推奨していく予定であると認識している。したがって、消費者は製品を選定する際に、ラベルがある製品を優先的に選ぶ可能性がある。このように消費者にとって重要な情報となる場合、ラベルが消費者契約法の「重要事項」に該当する可能性がある。欧州において、セキュリティ機能に関する要素は EU 消費者法の対象である。日本においても消費者保護法が存在し、重要事項に該当するものに虚偽があった場合、契約を取り消せる法的な効果が発生する。ラベル情報が消費者契約法の重要事項に該当するかに関し、我々は 2 つのアプローチをとることができる。1 つ目、裁判所の司法判断に任せる方法である。2 つ目、裁判所がどのように判断するかは不明確であるが、消費者契約法の重要事項に該当することが望まれる旨を明記しておくことである。消費者契約法との関係について触れるか否かで、大きな違いを生む可能性がある。
- 以上の 2 つの観点、ラベルの発行権限を有する者以外が無断でラベルを作成し、使用した場合の阻止権限に関する根拠、及びラベルと消費者契約法との関係については、最終とりまとめの中で言及されることが望ましい。最終的な記載の判断に関しては、経済産業省に委ねる。
  - 1 点目に関して、図でも示している通り、IPA がラベルを発行する責任者となる。ロゴなどの知的財産に関しても、IPA が管理を行う想定である。2 点目に関して、消費者向け IoT 製品に普及させていく上で重要な観点であるため、最終とりまとめへの記載について事務局で検討する。
  - 最終とりまとめの中で「スキームオーナー」という言葉が使われているが、具体的に誰を指すのか読み取れなかった。スキームオーナーとなる主体について明示的に述べるべきである。

- 1 点目、自己適合宣言について、事前説明で IPA の「SECURITY ACTION」において自己適合宣言が行われていると伺った。この制度のように、自己適合宣言でラベルを取得した場合のラベルの使用方法が明確に示されていると良いと感じた。これまでの議論で、自己適合宣言においても認証を受けたことになる印象があったが、あくまで自己適合宣言だということを取得した側も理解する必要がある。自己適合宣言と第三者認証の結果付与されたラベルの使用方法についても、明確に説明するべきである。現状、ラベル付与までしか言及されていないが、付与された後のラベルの使い方についても記載すると良い。
- 2 点目、☆3 以上の有効期限について、パターン A と B が示され、コストとセキュリティ機能の担保の度合いがトレードオフの関係にあると理解した。しかし、セキュリティはトレンドが変化した際に全体的な強化が求められる。そのため、数年に 1 度ではなく、大きなトレンド変化が発生した時には改めて確認を行うと良いのではないか。それに伴い、☆3 以上のラベル取得製品の申請者に対して、再確認のタイミングを通知するスキームがあると良く、再確認のタイミングを IPA がコントロールできれば理想である。トレンド変化による再確認がされない場合は、コストをかけずに実施できる定期的な自己評価で良いと考えており、パターン A に加え、IPA がトレンドの変化に応じて各自に再確認を依頼するパターン C を推奨する。

- 3 点目について、政府調達において☆3 以上の対策を要求されると、中小企業において対応が難しいと予想される。調達要件として☆3 以上が要求されることで中小企業の参入余地が狭まる可能性があり、中小企業のセキュリティレベル向上につながらない可能性がある。そのため、調達要件において☆3 以上を必須とするのではなく、☆3 以上を推奨とし、合理的な理由があれば☆1 の製品を使用可とするなど、☆1 取得製品を利用できる余地を残すと良い。IoT 製品単体ではなく、システム全体でセキュリティを確保することが重要であり、☆3 以上の IoT 製品が使用されていても必ずしもセキュリティが確保されているわけではない。システム全体でのセキュリティ担保の基準を設けた上で☆1 の製品を使用するという判断を認めるべきである。中小企業が有する優れた技術を活かす余地を残して調達要件を検討いただきたい。調達要件において、無条件に☆3 以上を必須とするのではなく、☆1 取得製品も利用できる余地を残すようなルールを構築していただきたい。ただし、セキュリティを確保する必要はあるため、☆1 や☆2 の製品を利用する場合には、明確な理由を提示していただくといった制約も検討していただくと良い。
  - 1 点目について、自己適合宣言後のラベルの活用方法についても具体的に示していきたい。詳細については、事務局で検討を行う。2 点目、IPA による任意のタイミングでの更新に関して、パターン A 及び B はメジャーな改訂が相当すると考えている。メジャーな改訂を頻繁に行うことは難しく、提案いただいたパターン C を含めて、トレンドに柔軟に対応していく方法を検討する。3 点目、政府調達において、全てのシステムに☆3 以上を必須とするわけではなく、システムの重要度によって要求レベルを変える想定である。システムの重要度が低いと判断される場合、☆1 以上での対応で問題ないとしており、中小企業でも対応可能と考えている。

- 1 点目、☆2 以上の適合基準及び評価手順は来年度以降検討すると理解している。特に通信機器においては、適合基準や評価手順の検討に非常に労力を要すると考えている。ルータやスイッチ等の通信機器について、☆2 を省略し、☆1 と☆3 のみを設けることも考えられる。また、☆2 と☆3 で同一の適合基準や評価手順を設定し、自己適合宣言であれば☆2、第三者評価であれば☆3 を付与する仕組みも考えられる。
- 2 点目、☆3 以上の有効期限について、先に提案されたパターン C のような案も考えられるが、IoT 製品ベンダーとしては、予算や行動計画を年単位で定めているため、規制等に予測できない変更が発生すると対応が難しい。パターン A 及び B のどちらが良いか決めかねているが、メジャーな改訂を行う際には、事前に情報提供を行い、改訂内容や時期について事前に公開いただけると助かる。例えば、猶予期間は 1 年間と記載しているが、事前に情報共有を行うことで実質 1 年半や 2 年にすることも可能である。この点も考慮して、メジャーな改訂の枠組みについて検討していただきたい。本検討会に関して、資料が基本的に非公開であり、会員企業等に対して情報の共有が難しい状況である。制度が運用されたらできるだけ情報を公開しながら検討いただきたい。
  - 1 点目に関して、☆2 を省略し☆3 を設けるなどレベルの設計に特に制限は設けない方針である。☆2 や☆3 で要求するレベルは、製品類型間で一定程度合わせていく必要があり、各業界団体と協力しながら業界の特性に合わせた適合基準や評価方法を検討していきたい。2 点目、メジャーな改訂前の情報公開については限界もあるが、できる限り情報はオープンにし、IoT 製品ベンダーにとって不意な変更とならないよう、メジャーな改訂の枠組みについて今後検討を進めていく。

- 1 点目、適合性評価の結果は、あくまで評価時の確認結果であり、ユーザが購入するタイミングや将来的なセキュリティまでは担保されていない。当該事項について、ユーザも同じ認識となるように、制度開始後を含めて周知等の取組をしていただきたい。注意書きが多くなることは好ましくないのでバランスは難しいが、評価時点での確認結果であり、購入時に必ずしも安全というわけではない旨を明確にしていただきたい。

- 2 点目、☆3 以上を取得する IoT 製品では、製品寿命が 5 年を超えるようなものが多く存在すると考えており、有効期限の検討において 5 年以上の長期利用がなされる可能性についても考慮した方がいい。評価時からの延長期間を最大 5 年とすると、ユーザの製品利用期間中にラベルが失効することも考えられるため、長期に渡って使用される IoT 製品についても考慮いただきたい。一方、セキュリティ確保のためには継続した取組が必要であり、継続的なアップデート等が必要になる点についても考慮の上で前述の事項を検討いただきたい。
  - 1 点目、IoT 製品に付与する情報提供ページの QR コードを読み取ることで、ユーザが当該情報にアクセスできるようにする予定である。今後、よりユーザに情報が伝わりやすい方法を検討していく。制度の周知においては、指摘いただいた点も留意し、普及啓発を行っていく。2 点目、ライフサイクルは製品ごとに異なるため、当該事項も考慮しつつ有効期限について検討する。

- 1 点目、話を伺った会員企業の多くが海外との相互承認に興味を持っている。具体的には、U.S. Cyber Trust Mark プログラムや EU Cyber Resilience Act(EU CRA)の動向に特に注目している。また、欧米では、米国 EU 貿易技術評議会 (TTC) が IoT セキュリティに関する検討を進めており、本制度との連携についても検討いただきたい。本制度のガラパゴス化やダブルスタンダードを回避する上での重要な観点となる。
- 2 点目、政府機関等の調達において、「重要度：高～中は、少なくとも☆3 以上の IoT 製品を各機関等の選定基準に含める」と記載されており、重要度が高～中の場合は☆3 以上を取得した IoT 製品でなければ政府調達の際に購入されないとしている。しかし、製品類型ごとに、本制度で要求するセキュリティレベルを明確に定めないと、ラベルの情報を購入時の判断材料とすることは難しいと考えている。来年度以降、製品類型ごとに要求するレベルについて迅速に検討していただきたい。
- 3 点目、資料 3 P.23「☆1 で想定する守るべき資産」、参考資料 1「守るべき情報資産」、資料 3 P.25「想定される脅威」がそれぞれ定義されている。「有線通信機能」「無線通信機能」「セキュリティ機能」を含めて「想定する守るべき資産」としているが、参考資料 1 では「守るべき情報資産」で情報資産だけが考慮されているのは何故か。
  - 1 点目について、相互承認は重要と認識している。欧米とは情報交換の場を設け、相互承認についての検討を進めている。来年度の本制度開始の正式案内の際に、シンガポールと英国については相互承認の方向性を提示する。欧州と米国については制度検討段階であるため、方向性が確定次第、情報を公開していく予定である。2 点目について、政府調達の対象となる IoT 製品において適合基準をどのように設定するかは重要な観点であり、業界団体等と協議の上、適合基準に関する検討を進める予定である。
  - 3 点目について、「有線通信機能」「無線通信機能」はアタックサーフェスの一つとして考慮しているほか、☆1 で想定する脅威として、「セキュリティ機能」に対する脅威も考慮している。参考資料 1 の☆1 適合基準ではこれら機能に関する明示的な記載は無いが、☆1 で想定する脅威や☆1 セキュリティ要件を抽出する過程で考慮しており、情報資産のみを☆1 で考慮しているわけではない。

- ISO/IEC 27404 では、スキームオーナーについて、“Governing body can be authorized scheme owner”と記載されており、スキームオーナーとなる組織を限定していない。別途詳細を確認し、回答できる部分があれば事務局を通して連絡する。
- 適合性評価制度において、脅威が変わるたびにスキームを変更し、認証を行うことは難しい。一方、脅威に対処する必要はあり、通常、IoT 製品にはソフトウェアやファームウェアが内蔵されていることから、対応策としてはパッチの適用が考えられる。例えば、暗号化技術が危殆化した場合、新しい暗号化スキームを導入するためにパッチの適用を行う。パッチの適用に対する定期

的な確認を本制度の評価スキームにどのように組み込むかについては、別途検討が必要である。なお、大きなトレンドの変化があった場合、ETSI EN 303 645 でも対応がなされるはずであり、本制度においてのメジャーな改訂になるであろう。脅威の変化が本制度に与える影響も注視するべき重要な観点である。

- IoT 製品ベンダーが、☆1 を取得した IoT 製品に対してパッチを適用することで、セキュリティのレベルを向上させることも考えられる。この場合、IoT 製品のセキュリティレベルを途中で☆1 から☆3 以上に変更することは可能なのか。
  - パターン B では、2 年に一度の頻度で再評定及び形式チェックを行い、攻撃に関わる各種状況の変化に対応し、同じレベルの耐性にあるかを確認する想定である。メジャーな改訂に該当しない部分については、IPA が指定した項目について再評定を求めることを想定している。☆1 から☆3 への変更については、改めて申請いただき、取得し直すことを予定している。

- コメントを 3 点、質問を 2 点行わせていただく。
- コメントの 1 点目、☆1 開始の正式案内が 2024 年 9 月であり、☆1 の開始が 2025 年 4 月であると、メーカとしては対応が難しい。
- 2 点目、アップデート期間については☆2 以降の検討となろうが、EU CRA のアップデート期間が 5 年であることも考慮して、本制度においてのアップデートの時期的な定めについても検討いただきたい。
- 3 点目、消費者向け IoT 製品においては、ラベル表示が課題と考えている。製品開発の際には、パッケージデザインを早めに検討しているため、ラベル取得まで待つとパッケージの用意が間に合わない。ラベルをシール状にした場合、シールの貼り付けにはコストがかかる点が懸念される。米国と同様に、家電量販店や販売者と連携したアクションについても検討いただきたい。
- 質問の 1 点目、本制度に関する説明会を経済産業省や IPA からメーカに対して実施していただきたい。正式版の評価項目が実証時のものと大きく変わる可能性があると考えているので、実証に参加した企業に対してフォローしていただきたい。また、評価項目についてのコメントをどのように反映したのかご教示いただきたい。
- 2 点目、評価項目について、前回のプレ検討委員会から大きく変わっていると感じた。変更点について明確にしていただきたい。
  - 質問の 1 点目、説明会に関しては、賛同団体を通じて説明機会を設ける調整を進めている。団体に所属していない企業に対する説明会の実施も検討する。質問の 2 点目、資料の変更点については後程共有する。
  - 開発現場へのフィードバックは非常に重要である。メーカの担当者も協力するので、協力が必要な際には相談いただきたい。

- Wi-Fi ルータなどの IoT 製品において、有効期限延長の必要性を感じられない。あるベンダーは、ビジネス用 Wi-Fi ルータでも 5 年ほどで製品のライフサイクルを終了させている。有効期限延長は OT 分野では重要な事項であるが、Wi-Fi ルータ等の IoT 製品に対して有効期限の長期延長を認めることは現実的ではないと考える。

- 1 点目、最終とりまとめの 3.6 に関して、評価に使用した判断資料の保管及び開示先についての追記が必要である。自己適合宣言の信頼性を確保するためには、評価に関わる部分に透明性があることが必要である。このためには、適合を判断した資料の保管と開示が必要となる。自己適合宣言が虚偽である場合、ラベルを取り消される可能性があるとしているが、自己適合宣言は一定の時期における一定の判断の結果であるため、虚偽かどうかを判断することが難しいという課題も存在する。
- 2 点目、☆3 以上に関して、スキームオーナーは、セキュリティ要件についての解釈情報を蓄積及

び提供することで、適合するための基準を明確にしていただきたい。セキュリティ要件に対する解釈が IoT 製品ベンダーやユーザにとって一義的とする必要がある。

- 3 点目、各関係主体が負う責任について明示いただきたい。責任を明示することで、制度を利用する際に IoT 製品ベンダーやユーザが安心できる。特に、ラベルは製品品質に関する保証を示す法的な根拠となるのか明確にしていただきたい。ラベルは、IoT 製品ベンダーが出荷時に一定の検査を行ったことを示すものであり、ラベル発行者は IPA が所定の手続きで検査をし、齟齬がなかったとしてラベルを発行する。このため、IoT 製品ベンダーと IPA がリスク情報を提示することになる。ユーザは、ラベルの付与された製品を購入することは「セキュリティの品質が担保された製品を購入する契約」と捉えるであろう。しかし、自己適合宣言の際には、ラベル発行者は法的責任を負わないということであれば、その旨を明記しないとユーザに誤解を与える可能性がある。ラベル発行者が製品のセキュリティにおける品質保証の責任を負うのか明示いただきたい。同様に、IPA も自身の手続きについて責任を負うのか明示いただきたい。
- 4 点目、販売時だけではなくラベルの更新時にも自己適合宣言もしくは認証が行われるため、その際にもリスク情報の提供を行うことになる。
  - 判断資料の保管について、疑義が生じた場合に備えて、根拠の保管は求めていく予定である。また、利用者への開示義務までは制度としては求めず、疑義が生じた場合に IPA が確認を行うスキームを想定している。責任範囲について、自己適合宣言の場合、責任は IoT 製品ベンダーにある。IPA はラベル付与機関として、セキュリティ機能に関する法的責任は負わないが、ラベルの適切な使用に関する責任を負う。
  - 言葉が不明確である。責任とした場合、「法的責任」となる。IoT 製品ベンダーは、セキュリティ要件の存在を確認し、その旨を宣言したことで、製品販売に関する法的責任を負うことになるのか。自己適合宣言の際に、製品品質を保証する法的責任が発生するのかはっきりさせるべきである。
  - 本制度は任意制度であり、ラベルの掲示は IoT 製品ベンダーの判断に依存する。本制度の任意性を考慮すると、ラベルの掲示は、IoT 製品ベンダーが、求められる要件に対してセキュリティが担保されていると自己宣言を行うことに等しいため、品質の保証と見なされる。品質が満たされていない場合、IoT 製品ベンダーが返金や製品回収等の対応を検討することになると理解している。
  - 同意である。その点を明記する必要があると存じる。
  - チェックリストに含まれているセキュリティ要件については保証することになるが、チェックリストに含まれていないセキュリティ要件については、保証の対象外である。その点が明確になるように記載いただきたい。
  - ISO 規格でも保証の限界が示され、品質について保証しない旨が明記されている。IPA としては、ISO 規格に基づいて実施する。
  - ISO 規格は、日本の裁判所での判断の規範とはならない。ISO 規格では、セキュリティ機能に対する責任を問わない旨を示している。そのため、IPA は、自身の認証作業・手続に関する責任を負うが、それ以外については責任を負わないという整理になる。
  - ご認識の通りである。

- 1 点目、「一般消費者」と「消費者」という用語が使われており、それぞれの用語についての定義を明確にしていただきたい。
- 2 点目、対象製品について、IT 製品の PC やスマートフォン、タブレット等が除外されているが、IT 製品と IoT 製品の違いが不明確である。踏み台攻撃は、PC が対象となる攻撃だと理解しているため、本制度の対象に PC 等が含まれないことに違和感がある。対象製品の表記について、誤解が生じないように明確に示していただきたい。
  - 1 点目について、用語は改めて確認し、統一する。2 点目について、汎用 IT 製品である PC や

スマートフォン、タブレットなどは、本制度の対象から除外されている。踏み台攻撃では、IoT 製品も攻撃の対象になり得る。消費者に対する啓発活動においては、分かりやすい形で伝えていく

- 1 点目、有効期限について、個人的にはパターン B が望ましいと考える。メーカの経営判断もあるが、ソフトウェアのパッチ適用を適切に行うことで長く使用できる環境が良い。脅威のトレンド変化に合わせてアップデートを行うことが重要であり、2 年ごとに簡易的に確認を行う形が IoT 製品ベンダーのモチベーション向上にも繋がると考えている。
- 2 点目、本制度の運用方針について定めるべきである。今年度作成された手順書やチェックリストは非常に実用的だと考えているが、脅威のトレンドが大きく変化した場合には更新する必要がある。具体的な運用ルールや変更担当者などを定めるべきである。
  - 2 点目について、資料 5 図 3.1-1 でも示しているように、本制度の技術審議委員会で適合基準の承認や技術的事項等の審議を行う。また、適合基準検討 WG も設置し、製品類型ごとに適合基準案の検討を進めていく予定である。本制度の運営事務局は、引き続き IPA 及び経済産業省が担う。運用ルールについても重要な指摘と認識しており、来年度以降に検討していく予定である。
  - 脅威のトレンドが大きく変化した場合、IPA がリーダーシップをとりながら改訂を進めると理解した。

- 国際会議の場において、欧州が ETSI EN 303 645 に紐づく ETSI TS 103 701 の評価方法に対応した自動化ツールや、ISO/IEC 27404 に関連するツールを開発し、それに基づいてビジネスを展開する話題が上がった。欧州では規格を検討する際には、ビジネスの観点から検証環境などの整備を重視して動くことが一般的であり、その点で日本が取り残されている印象を受けた。
- 調達要件で☆3 以上の製品を使用することを求めているところ、☆1 の製品を使用する場合は、システムの他の要素においてセキュリティ対策を実施し、全体としては☆3 相当のセキュリティレベルを確保するという運用も考えられる。ただし、今年度の議論ではこのような利用方法を検討していないため、再度詳細な検討が必要である。

以上