第６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 12 月 12 日（火）10:00 ～ 12:00
場　所：経済産業省本館 第５共用会議室及び Teams によるハイブリッド開催
出席者（以下敬称略）：

委　　員：高倉委員（座長）、江崎委員（※）、猪俣委員、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
※本検討会のみ会議の現地進行を江崎委員に委任

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、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）、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状況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、制度活用を促す仕掛け、適合性評価済製品におけるセキュリティ事案への対応について事務局より説明が行われた。資料 5「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 最終とりまとめ 骨子案」に基づき、最終とりまとめの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】

- 資料の方針について異論はない。来年度の下期以降に制度運用を開始させる予定としているが、制度に関する周知期間が半年未満となっている。英国の Product Security and Telecommunication Infrastructure Act（PSTI 法）では、法律の位置づけではあるが、事前情報が出てから実際の運用が始まるまでには 2、3 年の猶予がある。半年という短い周知期間から、ベンダーとして対応に十分な時間が確保できるか懸念している。弊社の製品でも、来年度にラベル申請をすることは難しいと考えている。来年度は PSTI 法が義務化されるため、そちらの対応で手一杯になることが予想される。
  - 制度運用開始後に申請数が少ないため失策とならないようにする必要がある。そのためにも、より早い段階から周知することを考慮する必要がある。

- サーベイランスに加えて、通報制度や苦情処理の制度も検討すべきである。製品について通報できる仕組みや疑問を解消するための処理が必要である。

- 責任のリバランスに関する話題をよく耳にする。責任のリバランスの考えは、セキュリティ・バイ・デザインに結びついていくものだと考えており、セキュリティ・バイ・デザインについては、内閣サイバーセキュリティセンター（NISC）が共同署名で合意したとも聞いている。本制度の検討において、安全保障や重要インフラの文脈でセキュアなネット社会を築くための制度であると位置づけるとまとまりのある方向性になるのではないか。
  - 通報制度や苦情受付については、今後検討する。疑義のある製品に関する問い合わせを受け付ける窓口は必要だと考えている。ただし、コールセンターを立ち上げると制度運用コストがかかるため、本当に必要な問い合わせだけを受け付ける窓口を想定している。
  - セキュアな社会の構築に向けて、まずは政府調達から着手し、その後に重要インフラ事業者や地方自治体の調達についても、今年度中に検討したいと考えている。大手企業にも働きかけていく予定であるが、民間企業のルールへ政府が直接介入することは難しい。サプライチェーンリスクを考慮して取引先にもセキュリティを求めるようなルールを広め、セキュアな社会を目指していきたいと考えている。そうした社会の実現のため、まずは政府機関等の検討から進めている。
  - 「責任のリバランス」という言葉を用いることで、方針をまとめやすくなり、本制度の検討がスムーズになると考えている。
  - セキュリティ・バイ・デザインの文書に関しては、米国の Cybersecurity and Infrastructure Security Agency（CISA）が主導で進め、欧州のセキュリティ機関や NISC が共同署名している。NISC の共同署名には関係省庁も合意している。セキュリティ・バイ・デザインの概念は広範であり、開発者が開発段階で堅実なセキュリティ対策を行うことを強調しており、開発者にセキュリティの責任をより負わせることを意図したもの。経済安全保障を本制度とどれほど関連付けるかは別として、セキュリティ・バイ・デザインの概念は本制度と関連し、方向性は一致していると考えている。この点において、ご指摘通りであると認識している。
  - デジタル庁が進めている検討においても同様のニュアンスで記載するために、経済産業省とデジタル庁の連携が重要であると認識している。さらに、いくつかの業界ではサプライチェーンを含む動きが見られる。これらの取り組みを整理し、まとめることで、ほかの業界が参照しやすくなり、サプライチェーンセキュリティ向上の助けになると考えている。

- 弊社の製品は一般消費者向けに製造しているが、企業からも導入を検討されている。認証を取得するためには、コストがかかるため、ニーズに応じて☆の取得が行われ、弊社製品は☆1 の認証を受けることを考えている。しかし、政府調達で☆2 を要求され、弊社製品が調達されなくなることを懸念している。☆1 を取得しているからといって、☆2 の適合基準を満たせていないわけではない。☆1 の製品であるから調達しないと判断されないよう、調達者側に訴求していただきたい。
  - ☆3 を取得する政府調達用製品については、認証取得コストの適切な価格転嫁ができることが重要である。
  - ☆2 が要件とされる調達においては、認証取得コストを転嫁してでも☆2 を取得いただくことになる。一方で、☆1 を取得した製品は、その製品が「☆1 の基準を満たしている」ということを示すものであり、「☆2 の基準を満たしていない」ということを示すものではない。この点は、調達者に誤解を与えないように伝えていく。最終的に、☆2 が調達要件として定められた場合、「☆2 の製品に限定する」のか、「☆1 やラベル未取得の製品でも、☆2 相当のセキュリティの実装が確認できれば、調達候補とする」のかは、各調達者の判断に委ねられる。

- 具体的な整理が必要な事項はいくつかある。総務省では脆弱性を持つ機器やマルウェア感染を特定し、識別する活動を行っている。その半数がルータであり、ほかにもプリンターやネットワークカメラも含まれている。昨年はデジタルビデオレコーダや NAS でも脆弱性が見つかり、ランサ

ムウェアに感染する可能性もある。☆3 や☆4 の対象にはルータやネットワークカメラが含まれ、☆1 の対象には含まれていない場合、実際に被害に遭っているルータは☆1 の対象外となり、☆3 以上から対象となるのか。☆1 は基本的な要件とされているが、ほとんどの脅威に対する対策が要求され、☆1 でも対策には相当な労力が必要である。☆1 と☆3 以上の差は、自己適合宣言か第三者評価の評価手法の差になるのか。国際的な場で議論した際、自己評価で評価の妥当性が担保されるかについて指摘があった。その他、認証レベルと対象製品の整理について問われたので、対応関係について整理した表を別途作成することが望ましい。

- 上位の評価として、優先的に☆3、☆4 を目指す製品類型としてルータを挙げているが、ルータも☆1 は取得可能である。重要度が低いシステムを対象にしたルータでは☆1 を取得し、重要度が高～中のシステムを対象にしたルータでは☆3、☆4 を目指す。つまり、ルータだからといって必ずしも☆3、☆4 を取得しなければならないというわけではない。
- IoT 製品よりも、使用されるシステムによって要求される認証レベルが変わると理解した。この内容はどこかで具体的に明記されているか。
- 資料 4 の特定分野で使用される IoT 製品の最低限のセキュリティ確保において触れている。例えばスマートホームにおいては、ホームゲートウェイは☆2 以上の取得が理想であり、工場においては、規模や停止の影響度合いに基づいて☆2 や☆3 以上の取得が求められる。最終的には各企業の導入しているシステムによって環境が異なるため、標準を提示し、各社で検討する形になる。
- 多くの古いシステムが存在し、一部の製品は☆1 を満たしていない。情報通信研究機構(NICT)は総務省の管轄であり、直接協力を得ることは難しいかもしれないが、中尾委員を通じて情報を共有することが有益であると考える。古くて脆弱なままのルータや NAS が多く残っており、これらが攻撃に悪用される可能性が高まっている。
- NICT の脆弱性試験や SHODAN のデータベースにおいて、自社製品がリストアップされていることを認識している。一部の製品はセキュリティ・バイ・デザインの概念が導入される以前から存在しており、脆弱性の対応がされていないまま使用されている製品も多々ある。実証を行ったが、☆1 を満たせば、一般的な攻撃には対抗できるとの印象を受けた。一般企業においては、☆1 の基準を満たす製品で十分と考える。ただし、センシティブな情報を扱う企業では、☆2 以上の製品を選択することになると考える。また、本制度を海外ベンダーに対しても普及させることが重要な課題であると存じる。
- システム全体として評価する件について、本制度では IoT 製品を対象としているが、経済産業省はシステムにおけるセキュリティに関するガイドラインも策定している。半導体産業では、SEMI E187 や SEMI E188 の規格が存在し、前者はバックエンド機器について、後者はフィールドサービスについて規定している。現在、ハブのシステム構成に関する検討も進行中である。システム全体でセキュリティを確認するガイドラインや評価方法が出てきつつあり、コーポレートガバナンスやオペレーションガバナンスが非常に重要視されている。
- 各 IoT 製品において求める認証レベルについては、来年度以降、業界団体で検討する方針と理解している。例えば、家庭用ルータについては、☆2 を満たす必要性について討論を進める。同様に、食品会社の工場で使用される PLC に関しても、☆2 で十分かどうか、また製薬会社で使用される PLC については、微量の薬の変動が人体に危害を及ぼす可能性があるため、☆4 相当が妥当かどうかについても協議を進めるものと認識している。
- その認識で正しい。スマートホームや工場など、ある程度汎用的でニーズがある箇所を絞り込んで、来年度に具体的に議論を進めていく予定である。必要な認証のレベルについては、必要性そのものを含めて業界側と制度側で検討していくことになる。業界団体からの検討結果を受け、制度側ではそれを元により上位のレベルを作成するかどうかを検討する。
- 経済産業省としては、本議論を進めるための参考資料を作成する予定か。
- 経済産業省で作成している工場やビルのガイドラインなどをモデルにして、検討の概要を説

明できればと考えている。

- 制度設立の目的の箇所に記されている「リスクの高いサービス分野」は、「特定分野」と同じか。リスクの高いサービス分野の具体例を教えていただきたい。
  - 優先度が高い分野については、資料4 P.9に詳細が記載されている。例えば、工場システムや、消費者に近い領域としてはスマートホームが挙げられる。これらの分野を重点的に優先度付けしながら検討を進めていく。
  - スマートホームでは、自宅で医療を受ける人も存在し、セキュリティがますます重要視されている。報告書には以上の議論についても詳細に記載していただきたい。

- リモートメンテナンスにおいて、システムを管理する際にはVPNやトンネリングの利用が一般的であり、これらの手法で事故が発生している。医療分野でも同様で、病院のシステムと医療系デバイスをつなぐ際にはVPNやトンネリングの使用が推奨されている。ホームゲートウェイがセキュアであれば、配下にある機器は☆1でも良いと誤解が生まれる可能性がある。
  - 同感である。ホームゲートウェイのセキュリティ対策がしっかりしているからほかは問題ない、という考えは危険である。
  - VPNを利用する場合を含めた具体的な議論は、Step2で行う予定である。配下に接続される機器についても、必要な要件を考慮し、例えば☆2に組み込むことも検討する。本議論を進めるためにも、Step1及びStep2において利用シーンを検討することが重要と考えている。資料4 P.8の図は、分かりやすいモデルを示したものであり、上位の機器が配下の機器を守っていると意味しているわけではない。
  - 簡略化した図を使用する際にも、誤解を招かないように注意が必要である。危険な考え方や誤解されている考え方を明記すると良い。

- 認証レベルと製品の用途の関係を分かりやすく示す必要がある。これまでの議論では、製品に対する取り扱いに焦点を当ててきたが、ルータといっても家庭用や産業用がある。消費者にとって、システムにおいて適切な☆のレベルを理解しやすくするために、マトリックスなどを用いて示す必要がある。政府調達や防災、重要インフラに関連するシステムにおいては、☆3や☆4が必要とされることは理解できる。他方、☆1から☆4が具体的にどのような用途で必要とされているかを明確に定義する必要がある。
- 資料の表記からは、政府調達が全て☆3や☆4である必要があるとの誤解が生まれる可能性がある。政府調達においても、軽微な用途の場合は☆3や☆4は必要ないと感じる。先程も意見があったが、用途によっては☆3や☆4が必要ではない場合も考えられる。また、初期ターゲットを☆3や☆4から始める方針が示唆されたが、この点については検討の余地がある。重要な箇所から検討して一般に展開していくことは一つのアプローチであり、否定はしない。ただし、セキュリティの意識を広めることを優先するのであれば、最初に最低限の☆1から進めることも検討すべきである。政府調達や重要インフラの☆1用途について検討していくことから始めても良いのではないか。
  - 政府調達においては、「重要度:低」のシステムにおいては☆1の製品でも十分と考えている。一方で、重要度が中高のシステムでは☆3や☆4の製品が対象となると考えている。政府調達における全ての製品で必ずしも☆3や☆4を要求するわけではない。
  - 初期ターゲットについて、来年度予定している制度開始時点では実質的に☆1しか取得できないが、セキュリティを強く求める領域も示す必要があると考えている。具体的に☆2～4の検討を進めていく製品類型として、ルータやネットワークカメラを挙げている。これらの領域でまずは☆1を取得していただき、☆2や☆3については、制度ができ次第、取得していただく形で浸透させる方針を考えている。調達において強制力が不足していると、制度が利用

されない可能性が懸念される。まずは調達において本制度のラベルが活用されることを具体的に示し、ベンダーがラベル取得することの普及を進める。ある程度、広いIoT製品にラベル取得が普及することで、民間企業の調達や一般消費者の購入でも参考にされるという循環になると考えている。

- その点はしっかり明記しておく必要がある。
- 制度構築におけるロードマップを、横軸を時間にして作成いただきたい。全体像については☆4まで作り、重要なシステムにおける製品には☆3、☆4を要求すると明記する。こうすることで、ベンダー側に身構えてもらう必要がある。ロードマップを作成することで、ベンダー側、消費者側双方で理解が進むと考えている。
- 次回の会議では、2～3年後までの想定ステップを提示したいと考えている。また、ベンダーに対しても、制度の方針が一定程度固まった段階で、制度概要の説明とラベル取得に向けた働きかけを行う必要があると認識している。
- ベンダーに対して、少なくとも政府は認証された製品を確実に使用するという宣言をすると良い。
- 政府の影響が強く及ぶのは、政府機関や重要なインフラである。ピラミッドの下の部分に行くほど政府の影響が薄れ、企業が自主的に製品を選択することとなる。この観点から、政策的なアプローチにおいて初期のターゲットはピラミッドの上部に位置するとしている。
- 資料4 P.20の赤字の内容を、展開戦略と初期ターゲットに記載いただくと良い。
- ☆3および☆4と経済安全保障推進法の基幹インフラとの関連性について、検討し、その結果を資料に追加いただきたい。
- 経済安全保障推進法との関連性についても詳細な検討を進めたいと考えている。また、地方自治体においても☆1を進める重要性があり、総務省と連携していく。地方自治体が積極的に取り組むことで、大手の民間企業も少なくとも☆1のラベル取得済み製品を使用することのメッセージとなると考えている。

- 資料3に関して、論理的な構成で良いと存じる。対象範囲の定義について、IoT製品とされており、ハードウェアは明確に対象となっていると考えるが、ソフトウェアについても検討が必要である。EU Cyber Resilience Act（CRA）では、対象にフリーソフトやOSS、SIEMなどのセキュリティ関連のソフトウェアも入っている。本制度では、この点がまだ明確にされていないため、ソフトウェアの取り扱いについてご教示いただきたい。
  - ソフトウェアアップデートに関する要件は既に含まれており、脆弱性に対する確認も行っている。検出ソフトウェアについても、どのレベルで入るかは、具体的な基準を作成していく上で意識することになる。
  - IoT製品に組み込まれているソフトウェアは対象であるが、OSやアプリケーションソフトウェアなどのソフトウェア単体は含まない。ソフトウェアについては、別途検討が行われる可能性もあり、将来的には本制度と合流する可能性もゼロではない。検討の際には、CRAの動向にも留意しつつ議論していく。
  - 諸外国においても同様の制度を検討している際に、日本においてソフトウェアの検討が抜けていると、制度として不十分であると判断される可能性がある。ソフトウェアについては、別途考える旨を明記しておくと良い。
  - この観点から考えると、システムとしてのセキュリティガイドライン（工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン）は同様の理念に基づいている。本ガイドラインには、SOC機能やガバナンスの導入が必要であると記載されている。国としては既にこれらのポートフォリオを有しており、それらの要素に関する調整や統括においては経済産業省が役割を果たすべきである。
  - 米国の医療関係者は、IoT製品のセキュリティに非常に注力しており、Software Bill of

Materials(SBOM)を使用してソフトウェアを管理している。脆弱性が新たに発見された場合、情報を共有し、パッチを適用する手続きを迅速に行っている。ソフトウェアに関する話題は一般的に広く議論されているが、医療関連のIoT製品に関してはスコープを絞って議論しているようである。ベンダーにSBOMへの対応を求めるのは難しいかもしれないが、本制度のロングリストに基準として含まれている。

- SBOMやPSIRTは、ソフトウェアの構成要素を管理・把握するための手段だと考えている。対象を明確に絞り込んで管理されていると理解した。
- 以上の事項を報告書に入れていただきたい。本検討会での検討事項に関連する議論は、分科会で検討しているロングリストにも含まれており、同時に、ほかのグループでも同様のテーマに基づく議論が進行中である。この点を明記すると良い。

- 資料3について、実証結果は一巡した結果である。認証を取得する際にはNの項目をYにする必要があり、認証取得に必要な期間にはその対応期間も含まれる。また、開発中もしくは出荷後の製品かによって、Nの項目をYに変更できるかは変わってくる。Nの項目に対する製品の修正可能性についてもヒアリングしていただきたい。
- 評価項目には、企画開発段階で対応すべき事項や、ソフトウェアコンポーネントが最新版であることなどの出荷前に確認が必要な事項が含まれている。例えば、パスワード機能などは企画開発の段階でしっかり実装しないと、後から追加することが難しく、脆弱な機能になる可能性がある。このような事柄について、開発者向けのガイドブックなどを作成することも検討していただければと存じる。

- Google OSなどの汎用OSが搭載されたスマートTVなどが存在する。これらは本制度で対象外となるPCやタブレットではないが、第三者がアプリケーションを作成し、組み込むことができるIoT製品である。NASもこのような類の製品が存在する。今回の対象製品を考えたときに、これらの製品はグレーゾーンにあると感じた。

- 医療機器のSBOMに関して、JIS Tでは推奨されており、対応しようとしているベンダーや医療機器団体が動き出している。そのため、調整を行い、整合性を確保する必要がある。

- 資料4 P.23に関して、ISO/IEC27404が適合性評価においてラベルを付けるためのフレームワークを規定している。本制度のロングリストにおける要求基準の書き方を早期にISO/IEC27404に導入していくことを検討している。ISO/IEC27404は作業原案（Working Draft）の段階であるので、意見が入れやすく、1月がコメントの締め切りである。ISO/IEC27404の活動に本制度の活動をうまく組み込めれば、相互認証の実現においても理想であるので、別途相談させていただきたい。
  - 産業界が特に注視している点なので、幅広く関係者に呼びかけて調整いただきたく存じる。

- 本制度は、重要インフラにおける制御システムを対象にした重たい認証制度ではないので、サーベイランスによるラベル・認証取り消しではなく、登録廃止手順の簡略化が重要であると考えている。
  - サーベイランスの実施による登録廃止は理想的であるが、過去にCC認証を含めて取り消しに至った事例はIPAではない。取り消しの際には、その根拠を明確に提示する必要があり、その根拠の提示が極めて難しい。IPAとしては、有効期限を設けて失効させることが良いと考えている。
  - 関わっている認証で異議やクレームでの失効は見たことがない。登録期限や有効期限の設定はとても良い考えである。

- 人的資産が☆2 から考慮されていることについて、☆1 ではユーザの生命は守らなくて良いと捉えられる可能性があるため、表現の工夫が求められる。

- スマートホームの図についての議論があったが、その問題について適切に議論することは重要だと考える。スマートホームのテーマに取り組んでいるグループも既に存在するため、実際に動作し、適用されている実例を参考にして、具体的かつ誤解のない形で進めることが良いと考える。
  - スマートホームでは、ECHONET Lite など様々なプロトコルが利用されている。ワイヤレススピーカで使用されている DLNA は、セキュリティなどが考慮されていないプロトコルである。
  - ユーザには、リスクがあることを理解いただいた上で、使用していただくことが重要である。

- 制度全体としては大きな流れが見える中で、スマートホームや医療などの個別のケースにおいて、それらの環境への適用方法については検討の余地がある。これらの点についてもうまくまとめていけるような方針を策定することが望ましいが、まとめきれない領域については一時保留という形も考えられる。また、IoT 製品はセキュリティ的に 1、2 年で陳腐化する可能性もあるため、有効期限による登録廃止も検討されるが、有効期限の設定方法については検討が必要である。

以上