第3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3月17日（金）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、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、経済産業省製品安全課、産業機械課、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 日本貿易振興機構（JETRO）、独立行政法人 製品評価技術基盤機構、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）、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 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）、電気製品認証協議会（SCEA）、技術研究組合 制御システムセキュリティセンター（CSSC）

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　サイバーセキュリティ課　奥田課長、塚本課長補佐

議　事：

資料3に基づき、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 中間とりまとめ（案）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】

- 議論した内容が概ね網羅されていると感じた。論点はいくつか残っていると思われるが、特に今後議論が必要な点として挙げられていた評価基準等を検討する委員会の構築は、ベンダーにとっても関心が強い。この点に関する検討については、今後我々も関与していきたい。
- 諸外国との適合性評価制度の国際連携も重要なポイントだと考えている。諸外国の制度と全く異なった制度ができることは望ましくないため、しっかりと議論していただきたい。
- 中間とりまとめ案は、よく目配りがされており、論点がきめ細かく取り上げられ、工夫されたものだと感じた。
- 制度の具体的な議論や上流の議論を行ったり、政策への結びつきを検討したりするうえで、委員会は重要な働きをすることが期待される。国の政策や実業界の負担の問題、制度の実施にあたっての各論等、本検討会で議論を行った点について見識を持つ学者や有識者を交え、IoT 製品を供給する実業界に力点をおいた実務的な委員会を構築いただきたい。
- 中間とりまとめ案からは、これまでに行われた議論の事実のみが反映されているという印象を受けた。これまでの議論における発言の中には、本制度を定着させることでどのような社会を作りたいかといった目的や思いも含まれていた。制度構築の目的を記載している2.1の部分において、もう少し具体的に記載いただきたい。例えば、産業競争力の強化・支え、デバイス・アプリケーション・制御の関係で支えられる国民生活の安心・安全の実現、そしてそれを通じた世界への貢献といった、本制度の仕組みや議論が果たすべき役割や目標について、一言触れられていると良い。このような基盤的な部分について議論を行ったという記録は、今後の議論をリードするうえでも、しっかりと残すべきだと思われる。また、本制度は今後のIoTと生活基盤・産業基盤を結ぶインフラになると認識している。本制度が果たすべき役割としては、まずは産業力を強化して

日本の産業界を豊かにし、それを通じた社会・人々の安心を実現することだと考えている。中間とりまとめ案で産業競争力について述べられているのは、4 ページの「適合性評価制度の目的として、国際的に商品展開をするベンダーの競争力を削がないようにすることがあり、産業分野のベンダーの利益のための取組はしっかりと進めた方が良い。」という部分のみであり、位置づけが消極的である。これまでの議論では、競争力を削がないことのみならず、向上させることにも資するべきだという意見が挙がっており、自身もそのように考えている。本制度の位置づけとして産業競争力の強化を支えるものであることは、中間とりまとめ案に一言記載いただきたい。

- 2.2.2.1 の(3)の「今後議論が必要な事項」で記載されている位置づけに関して、前述した点が薄いと感じている。義務的な制度とするか任意的な制度とするかについて、任意的な制度とすると広まりづらく、義務的な制度とすると産業界の桎梏となるといった消極面のみ捉えられていると感じている。また、まずは任意的な制度として始めるが規制を行うことも検討すべきだと書かれているが、産業経済や社会の活力向上に資するという積極的な位置づけで規制についても検討を行う必要があると思われる。企業のコンプライアンス活動に関わっているが、活動のレベルが上がると、企業活動に対する制約という位置づけから、具体的な収益にまで結びつくようになる。例えば、会計検査は、財務活動の健全さを社会や投資家に公表することを通じて、日本企業の国際市場への売り込みを支えている。これは、規制があるからこそ競争力が確保・向上しているという一つの例である。コンプライアンス活動を制約として捉えている企業は、活動のレベルが低い。レベルの高い企業は、どうすれば秩序だったあるいは設計通りに行われる収益活動をコンプライアンス活動と同時に行えるのかについて考えている。このような意味で、今後議論が必要な事項の記載が消極的だと感じた。「任意的な制度として始めるが、今後は稼げるような規制、もしくは企業を支えるため・発展させるための規制について積極的に考える必要がある。」と一言記載いただきたい。規制か任意かの議論は重要な問題であり、ベンダーとしても本制度を推進する支えになると考えている。
- IoT 機器そのものより、認証機関に対する考え方が重要と考える。TÜV Rheinland といった海外の認証機関がベースとなっている制御システムの認証が、国内で普及しない状況を見てきた。国内で様々な後押しが行われているが、ISMS であってもブランディング化に失敗している。認証について理解しているベンダーは多く、海外規格の認証を取得しているところは多い。国内展開を考えた際、認証取得企業が出ないと大きな問題となる。IoT 機器に重い規制をかけるのは、メーカーにとって負担が大きく、魅力も感じないと思われる。そのため、安価かつ短期間で認証が取得できるような形で検討いただきたい。認証機関が IoT について幅広く取組を行おうと思うような制度にする必要がある。ETSI EN 303 645 のような規格の国内展開を目指し、IoT 機器に対して広く対応していく認証機関を後押ししなければ、うまく制度が回らないと考えている。
- 認証においては一般的に定期監査が必要になるが、IoT 機器のライフタイムを考えると、サーベイランスまで要求する必要はなく、一回きりの認証でも十分と考える。厳密さばかりを意識しない形を検討いただけると、より良い制度設計ができると思われる。この点について、3.3.3 で記載いただけると良い。
- 中間とりまとめ案に関して、これまでの議論を良くまとめていただいたと考える。
- 国際的な基準やルールとの整合に関して、相互認証については諸外国の制度を見ながら、しっかりと議論させていただきたい。本制度を活用した製品がグローバルで通用するか否かは、本制度を活用するインセンティブに大きく関わる部分だと認識している。
- 安心な世の中を作っていくという前向きな意味で、製造物責任に関する明確化や深掘りの議論が今後なされても良いのではないか。セキュリティに関する事案が生じた際、その責任の話は必ず出てくると考えられるが、製品を作ったベンダーとして、本制度の認証を取得していればある時点で一定程度の責任を果たしていると判断されるのであれば、認証を取得するインセンティブに繋がると考える。この点は、製造物責任法（PL 法）の視点も入る。利用者側としても、粗悪な製

品ではなく、認証を取得している正しい製品を選んだという説明責任が果たせる。そういった世界観を作っていくことも重要である。こういった責任に関して、少し深掘った議論を行っても良いと考える。

- IoT 製品では、いつまでも製造責任が続くという考えは馴染まないものであり、アップデートをし続けなければならないものでもない。サポート期間・期限に関しても、責任に伴って議論する必要がある。任意制度からでよいと考えるが、対策を講じていたことを示すことに繋がる制度になれば良い。
- これまでの様々な意見を中間とりまとめ案に取り入れていただき感謝する。こういった取組に積極的に参加していきたい。
- 品質と異なりセキュリティは変化するため、今年取得した認証が来年にも通用するかという技術的進歩による変化については検討する必要がある。本制度の認証を取得することでどこまでの責任分界に繋がるか、どこまで何の保証を行うのかについて、今後議論する必要がある。
- どのように制度をプロモーションしていくか、どのような技術要件を定めるか、政府としてどのように制度に関わるか等様々な論点があるが、それを一つの委員会で全て検討する方法もある一方、技術部会やプロモーション部会といった専門的な知見を有した人を集めた部会に分けて議論を行うのも一つの方法と考える。参考にしていただきたい。
- 3.3.2 の記述はよく検討されたものだと感じた。免責や責任分界点をどうするか、またそれによる認証取得の具体的なインセンティブや利益について、今後検討していくという宣言だと認識している。加えて、その検討ポイントについても、よく書かれていると感じた。責任分担の整理に関して、最終的な責任の取り方は賠償と差し止めの二つがある。賠償を行うには、損害が発生したことについての立証が必要となる。例えば保険制度のような、被害救済や原因是正に繋がる資源の確保策と認証制度が結び付くと、損害が発生してもすぐに回復し、損害発生の原因について今後どうすべきなのかという議論に移ることができる。従来とは異なる、国際的に今後必ず必要となるような、IoT 時代における責任分担のあり方、すなわち誰かの責任を追及することなく被害が公平に分担される社会の構築に資する制度の提言について、日本がリードできると良い。こういった取組を行わない限り、原因となった者に対する裁判が行われ、企業も付き合えない状態となる。制度面における日本の国際競争力を高められるチャンスと捉えている。3.3.2 は、「どのような策が効果的か等について、必要に応じて検討する必要がある」とまとめられ、頼もしく感じた。実務的には対策をしっかりと講じたということを主張したいが、むしろそういった主張をしなくて済むような制度設計も併せて検討するという、将来の課題を設けたことは高く評価したい。これまでの責任制度とは異なる、尖った提言ができる政策形成力を持った有識者を委員会に集め、国際的な議論をリードしていただきたい。可能であれば、委員会のメンバーに加えていただけるとありがたい。
- 中間とりまとめ案に関して、論点のカバーやまとめ方が的確だと感じた。
- 2023 年 2 月 17 日に米国に行く機会があり、そこで IoT に関する意見交換を行った。その中で、Consumer Technology Association（CTA）の方から、中間とりまとめ案の付録の米国の部分にも記載されているナショナルラベルプログラムについて検討している話を伺った。このプログラムは、ホワイトハウスの National Security Council が主導し、民間がイニシアチブをとって、IoT 機器のセキュリティ対策に関する米国共通のラベルを作ることを目的としている。過去は、このラベリング制度について否定的な意見が多かったとのことだが、最近は連邦政府や業界団体大手からも支持されている。ラベルの要件には NISTIR 8259 が用いられており、デフォルトパスワードの禁止やアクセス制限といった技術要件だけでなく、文書化や問い合わせの受付といった非技術要件も含まれている。この要件に従い、様々なラベルプログラムが並行で動くとのことである。コンシューマルータ、カメラ、スマートテレビ、ドローン等に対してのラベリングスキームやジェネラルなラベリングスキームといった、クライテリアを満たしたものに対するスキームが並列に存在することになる。もしかすると ISO/IEC 27404 のシンガポールのようなラベリングスキー

ムも設けられるかもしれない。最終的には、米国共通のセキュリティ確保のための QR コード付きマークを発行するとのことである。これは、2.2 で示されている構築すべき適合性評価制度と同じような話である。米国と EU の Trade and Technology Council で IoT セキュリティに関するワーキンググループを立ち上げ、同じ土俵で議論したいという話がある。日本もその土俵の中で同じような議論をした方が良いと思う反面、日本の特徴を出していく必要がある。要件は NISTIR 8259 にならないかもしれないが、ETSI EN 303 645 も含めて、我々の中で検討すべきだと考えている。

- 適合性評価制度は、あるクライテリアをベースとして IoT 機器を認証するスキームだが、米国のラベリングプログラムは、入口となる要件があり、それを満たした製品に付与されるラベルがいくつも並列して存在し、最終的にはマークが提供されるスキームである。そういった考え方も今後の課題として押さえておいても良いのではないか。
- 安心を購入できるようにという議論があったが、粗悪品があるからこそ市場が形成されているという側面があるほか、セキュリティについて考えるきっかけにもなるとも感じる。粗悪品ともうまく付き合っていくための制度設計を行い、市場にセキュリティの認知を広められれば良いと思われる。保険も含めてリスクをどう考えるかご意見を伺う中で、購入者や利用者に対して本制度を通じて、技術的な担保とは別の安心を提供するためにはどうすべきか議論することが大きな論点になると感じた。
- 背景において、利用者については一言しか書かれていないが、超高齢化社会の中でスマホを含む通信機器や IoT 製品の進化や普及のスピードについていくことができず、セキュリティに関する知識やスキルを持っていない消費者が少なくないことについても言及いただきたい。本制度によるメリットを一番感じるのは消費者だと思われるため、そういった現状について背景に追記いただきたい。
- 本制度をプロモーションするうえで、2025 年の大阪万博が期待できると考えている。国民の方々や事業者の方々、そして世界の方々に注目される機会であるため、それまでに制度の構築が間に合えば良いと思われる。
- 医療系の JIS T において、ライフタイムを考えて製品を作ることが産業規格化し始めているため、注視しながら検討を行う必要がある。

また、資料 4 に基づき、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、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】

- 16 ページの適合性評価スキームの方式 1、方式 2 に関して、早く社会実装するという観点から選択することが大切である。早く社会実装を行うためには、産業界のニーズを強めることがアクションの一つとして考えられる。また、諸外国では囲い込みを行っており、時間をかけて制度を作っても蓋を開けてみると国際的には陳腐化した制度となってしまう懸念がある。国際的なハーモナイゼーションとは、要するにどれほど覇権を取れるかという話である。そのため、どれほど急いで本制度を構築するのかについて、慎重に考える必要がある。そういった意味で一般論を言うと、方式 1 の統一的なスキームを検討するうえでは、様々な議論との妥協が考えられ、その間に諸外国が先に進んでしまうことを懸念する。また、ニーズの強さに関して、産業界における製品の製造ラインの必要性や収益に結び付いている領域も含めて考えなければならず、論理的な部分のみではなく産業界の必要性やニーズに従って、進められるものを進めていくという点では、方式 2 が適していると考えている。
- 早く制度が構築できるよう順番に取組み、最終的には方式 1 と方式 2 のハイブリットになることがベストだと考えている。方式 2 の場合、IoT 領域で新しいビジネスが生じた場合に、分類が難しく、どのカテゴリーに合致するかの判断ができないおそれがあるのではないか。カテゴリーの

隙間に落ちてしまう製品が出てくることを懸念している。早く制度を立ち上げるという観点では、既存のスキームを活かすことは良いと思われる一方、最低限求められるレベルを設定する意味では、方式1も検討すべきと考える。スキームオーナーはそれぞれ異なると思われ、レベル合わせは課題になると認識している。そういった課題について、既に制度が導入されている日本以外の国ではどのように取り組まれているのか調査いただきたい。

- 適合性評価スキームに関しては、最低限のレベルを統一的なスキームでカバーする方式1の方が望ましいと考える。日々新しい攻撃手法が出てくるため、それに応じてセキュリティ要件も早いペースで更新していく必要がある。その意味では、統一的に管理されている方が、実効的なセキュリティ評価スキームになると考える。セキュリティではなくセーフティの話になるが、数年前、IEC 60065 と IEC 60950 が IEC 62368 に統合された。弊社は両方の製品を作っていたため、当時は大混乱が生じた。初めは製品ごとに求められる安全性が違ったが、複合的な製品が増え統一されたと理解している。セキュリティについては、統一的なスキームで最初から管理した方が良いと考える。
- 討議事項 1 に関して、認定機関の機能を有する独立行政法人は現時点で NITE しかないとのことだが、NITE はセーフティ領域を管轄する組織であり、セキュリティ領域に関する経済産業省の関係組織でいえば、IPA が最も馴染みある。そのため、認定機関の部分に関して IPA も関与いただくことが必要ではないか。また、S マークの話が出てきたが、セキュリティの分野に馴染まない部分もあるのではないかという意見も内部の議論ではあった。
- 自身も方式1のイメージを持っていた。米国では、方式1と方式2の間をとった方式1.5のようなスキームを採用しており、統一的なクライテリアが方式2の下に存在するような形である。そのクライテリアについて、例えばNISTIR 8259 はETSI EN 303 645 を含めて考えても、そこまで深い要件ではない。ベーシックな統一的スキームが一番下にあり、その上に既存スキームが乗っているイメージである。本制度でも、そのような方式1.5を採用するのが良いと思われる。
- IoT 系のマルウェアについて解析を行っているが、直近1、2年でリブートしても残ってしまう持続感染性のマルウェアが多く出るようになった。そういった背景を踏まえると、IoT 機器の定期レビューをどのようなタイミングで行い、持続感染性のマルウェアの脅威をどのように排除していくかという点は重要な課題になると考えている。このような点について、課題として明確にしていただきたい。
- ISMS といった制度の設計に関わってきた反省として、論理的な正しさ・合理性・美しさ・完全性といったことよりも、制度の機能が誰に何をもたらすのかを忘れないでいただきたい。NISC の重要インフラ領域においてもセキュリティの概念は変わり、最終的には任務保証の観念になった。セキュリティが果たす効果や機能は様々な側面から評価できるが、社会全体の中でベンダーにとっての利益があり、国民や世界の人々がどういった利益を受けるのかという、本制度がもたらすものを中心として考える必要がある。制度や論理の完全さのみを考えていると、現実に合わない制度となってしまう。そういった視点を忘れないでいただきたい。
- 世界的なハーモナイゼーションは必要だと考えているが、誰が決めた基準・規格が有力なのかという問題がある。米国の CTA は、米国で事業を行っており、収益を上げている団体しか会員になれない利益集団である。CTA の取組をベースとして、世界との様々な議論がなされている。日本でも、守るべき人やベンダー、産業を想定する必要がある。そして、そのような人々が具体的に何をどのように必要としているかを細かく見ていかなければならない。製品には、物理的なものだけでなく、システムや要素部品等もある。ハーモナイゼーションを考える際、既にできあがった仕組みの中で優位性を確立することは難しい。それを踏まえ、製品については先手を取られているため、要素や責任の部分で勝負する、新機軸を打ち出す、といった視点があっても良い。使われる制度を構築しなければ意味がない。相互認証という方法もあるが、先様が取り組んでいる中で、日本の認証機関による日本語が使える同様の認証制度というレベルで提案を行うのは、よろしくない。CSSC で制御システムのセキュリティ認証の仕組みを作ろうとしたときにも同じよう

な論点があった。この点について、ぜひご検討いただきたい。

- 認定機関は、認証機関による認証のあり方や認証基準のあり方を議論するということになっているが、本制度がどのように使われるか、そしてどのように優位性を確立できるかという点についても、認定機関で議論いただきたい。認定機関と認証機関の役割分担について、ISO の様々な規格との関係で決まったものはあるが、それに必ずしも囚われる必要はないと思われる。政府の関与のあり方も含めて、検討いただきたい。
- 弊社の製品セキュリティセンターでは、全製品の診断を行っている。車載器やカメラ、家電や工場システム等の診断を行っているが、直感として、それぞれの製品毎に特殊なことは行っていないと認識している。業界や機種によって大きな違いがないのであれば、方式 1 の方が良いと考える。
- 例えば、自走式電子レンジが作られた場合、ロボットの車両にあたるのか、白物家電にあたるのかといった判断が難しい。今後、様々な IoT サービスや機器が出てくる中で、複数の領域にまたがる製品があった場合、一番敷居の低い領域の認証を取得して販売することが行われかねない。その点を踏まえると、統一的な基準で全体として取り組むべきことを決めた方が良いと思われる。もちろん、命に関わる製品や使われる場所が異なる製品、高齢者向けの製品等、シチュエーションを鑑みた仕組みについても検討が必要である。
- 16 ページの方式 1 と方式 2 については、評価スキームというよりも、要件をどう切り分けるかだと認識している。横断的に要件を定めるのが方式 1 で、製品ごとに要件を定めるのが方式 2 というイメージを持っており、8 ページで示されているのがスキームだと考える。情報処理の促進に関する法律についてはさておき、IPA が運営する JISEC を利用した方が早く制度を構築できると感じた。JISEC 認証では、NITE が ISO/IEC 17025 に基づいて、IT セキュリティセンターや ECSEC Laboratory、TÜV Informationstechnik GmbH, Evaluation Body for IT-Security を評価機関として認定している。要件や評価の解釈の差を是正するような調整機構を JISEC のスキームの中で設けている。すぐに着手するという意味で、JISEC の仕組みを適用すれば良いのではないかと考える。この点について、ご検討いただきたい。
- 適合性評価スキームについて、方式 1 と方式 2 のどちらが良いかについては一概に言えないが、一般的な規格体系として、IEEE でもよくあるように、全体を統括するマザー規格があり、各業界・各分野の規格はそれにぶら下がるという形はある。テクニカルな話となるが、どのようにエンドースするかが検討できれば、制度としてまとまるのではないかと考える。業界や分野による大きな差はないと感じるが、何かがあったときは個別規格を優先することが多い。このような優先順位は専門家チームを立ち上げて検討すべきと思われる。様々な規格が存在する中で、改訂年度が異なることで時間差が生じてしまう点については割り切るしかない。
- 欧州でサイバーレジリエンス法の議論が行われているが、同じような課題が生じると思われる。彼らがどのように整合を取ろうとしているか、経済産業省に調べていただき、共有いただけるとありがたい。
- 消費者としては方式 1 の方が分かりやすいと考えていたが、皆様のご意見を伺っていると、それにプラスして分野ごとのスキームも必要になると感じた。方式に関わらず、消費者が理解しやすいような制度・スキームを構築いただきたい。
- セキュリティとセーフティを一緒にすべきでないという意見があるのは承知しているが、セキュリティの概念でいえば、レベル 1 の上にレベル 2、レベル 3 があるという階層だった仕組みが自然だが、セーフティの概念でいうと、レベル 1 の基準が機能しなくなった場合、すなわち認定が外れた場合、レベル 2 とレベル 3 でブロックする必要がある。どちらの方式を採用するにしても、レベル 1 は全ての製品で満たしてほしい機能要件だと思われるが、万が一レベル 1 が機能しなくなった場合、レベル 2 とレベル 3 でカバーできるのか否かについては整理すべきである。もしも基準を一部満たさなくなった製品が出てきた場合、方式 1 と方式 2 のどちらの方式でも構わないが、他の機能で補うことができるか否かが分かると、一部機能には危険が残るが、そのうえで使

用するか否かの判断ができる。そういった考え方をすることにより、セキュリティの意識向上にも繋がると考えられる。販売されているものを購入すれば安心なのではなく、それがきちんと使える環境なのかを考えて使うということを、消費者が分かりやすく意識できるような枠組みにしていく必要がある。

- 制度全体として諸外国の先行事例と競争するのは難しいというのはおっしゃる通りだと認識している。そのため、着手できる部分から早めに取り組んでいくこと、そして諸外国が考えついていない、手が届いていない部分について我々が先回りして取組み、国際的にも参考となるような制度を構築することが鍵になると感じた。
- 制御系の経験があるため、安全の考え方については理解する。セキュリティに関して特徴的なことは、技術の進歩があまりにも早いことだと認識している。適合はさることながら、どのようにルールをうまく運用させていくかという観点について、今後議論していく必要がある。どの時点、どの技術レベルで取得した認証なのか、そしてそれが陳腐化した際にどのように扱っていくべきかについて考える必要がある。引き続き、議論させていただきたい。
- ライフサイクルを考えた際、製品サポートが終了した場合に使用してはならない製品群なのか、それとも気をつければ使用を続けても良い製品群なのかという点について、ユーザ側が分かる形にする必要がある。ビジネスとしては、ライフタイムが終了した場合は新製品を購入いただきたいと思われるが、現実的にはそうはいかない。ユーザ側の事情もあるため、うまく折り合いがつくような形で、ビジネスがうまく回る仕組みにする必要があると感じた。

以上