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

令和 5 年 5 月

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

目次

背景

インターネットに接続される IoT 製品の数は急速に増加しており、総務省の令和 4 年度情報通信白書によれば、世界の IoT 製品数について、2023 年には 358 億台、2024 年には 400 億台程度と、今後も増加の一途を辿ることが予想されている。IoT 製品数の増加に伴い、IoT 製品の脆弱性を狙ったサイバー脅威も増加傾向にあるところ、日本を含む各国は IoT 製品の安全性確保に向けた取組に力を入れている。諸外国における取組として、例えば、

- 米国では、2022 年 10 月にホワイトハウスにおいて、消費者向け IoT 製品のラベリング制度の構築に向けた企業、団体及び政府機関間の議論が行われた。
- 英国では、消費者向け IoT 製品に対してセキュリティ対策の義務化を求める PSTI 法[1]が 2022 年 12 月に成立した。
- EU では、EU 市場に投入されるあらゆるデジタル製品のセキュリティ対応を義務付ける EU サイバーレジリエンス法[2]の草案が 2022 年 9 月に発表された。
- ドイツ、シンガポール及びフィンランドでは、消費者向け IoT 製品に対するセキュリティラベリング制度が既に開始している。

我が国においても IoT 製品の安全性確保に向けた取組を推進してきた。代表的な取組として、IoT 製品メーカーのセキュリティ対策を支援するガイドラインを経済産業省、情報処理推進機構（IPA）、総務省等から複数発表しているほか、総務省は、端末設備等規則を 2020 年 4 月に一部改正し、電気通信業者のネットワークに直接接続する同規則の施行後に販売された IoT 製品について、アクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装を原則義務化した。また、IoT 製品を対象に含むセキュリティに関する認証制度として、CC（Common Criteria）に基づく IT セキュリティ評価及び認証制度（JISEC）が存在するほか、産業用 IoT 製品に対する認証制度としては、IEC 62443-4-2 に基づく CSA（Component Security Assurance）認証制度が存在する。

しかしながら、これらの取組ではカバーできていない課題が存在する。例えば、IoT 製品の安全性確保のためには、IoT 製品ベンダーにおけるセキュリティ対策の取組が必要不可欠であるが、現状では、ベンダーにおけるセキュリティ対策の取組を調達者や利用者にアピールすることができず、対策に要するコストを製品の販売価格に反映しづらい状況にある。そのため、諸外国の取組も踏まえつつ、IoT 製品の安全性を確保するために、あるセキュリティ要求基準に対するセキュリティ対策の適合性を評価しその結果を利用者や調達者が分かる形で可視化する制度（以下「適合性評価制度」という。）が求められる。

そもそも、IoT 製品は、サイバー空間とフィジカル空間を融合させ社会全体で付加価値を増大させていくために必要不可欠なデバイスである。他方、世界を取り巻く安全保障環境は不確実性を増し

[1] Product Security and Telecommunications Infrastructure Act 2022
https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

[2] European Commission, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

ており、これに対応するためには、安全・安心を確保する基盤の構築に向けた取組を進めることが求められている。今後、付加価値の増大をもたらす機能を具備していることのみならず、安全・安心であると評価された IoT 製品こそ、世界に求められている。そうした安全・安心を評価する基盤となる適合性評価制度を構築することは、単に IoT 製品のセキュリティ向上を促すことのみならず、世界的な需要に応えることで我が国の産業競争力強化に繋がり、かつ世界の不確実性の緩和に繋がる制度であると考えられる。この制度に適合したIoT製品を数多く世界に出していくことは、重要な国際的貢献の一つでもある。

このため、経済産業省は、令和 4 年 11 月より「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（以下「検討会」という。）」を開催し、現状の課題、適合性評価制度構築の目的、構築すべき適合性評価制度等について議論を行ってきた。

本中間とりまとめでは、検討会での議論結果を示すとともに、IoT 製品に対する適合性評価制度構築に向け、今後詳細に議論していくべき事項を示す。

1. 検討会において議論した事項

1.1. 現状の課題及び制度構築の目的

(1) 検討会における討議事項

IoT 製品の安全性確保に向けては、以下に示すとおり、IoT 製品ベンダーにおける課題、IoT 製品利用者・調達者における課題及び国民全体の課題が存在すると考えられることを提示した。

- IoT 製品ベンダーにおける課題
  - IoT 製品に対するセキュリティ対策状況が適切に評価されず、製品価値の向上につながらないおそれがある。
  - 既存制度の認証取得による明確なインセンティブが存在せず、認証を取得してもコスト増のみで、製品売上につながらないおそれがある。
  - 諸外国の制度と協調的な制度が構築されない場合、諸外国の制度の適合性評価を受ける際に別途の負担が必要となる。
- IoT 製品利用者・調達者における課題:
  - 現状ではセキュリティ対策状況が可視化されていないため、特に消費者をはじめとするセキュリティに関するスキルや知見が限定的な利用者において、適切な対策が施された IoT 製品を選ぶことができないおそれがある。
  - 適切な対策が施された IoT 製品を利用できない場合、当該 IoT 製品がサイバー攻撃を受け、利用者に対して悪影響を及ぼすおそれがある。
- 国民全体の課題
  - マルウェア攻撃により IoT 製品がボット化して他のシステムに悪影響を及ぼすリスク、不正アクセスにより利用者のプライバシー侵害に関するリスク、サイバー攻撃により人体への物理的影響を及ぼすリスク等、IoT 製品を狙ったサイバー脅威が高まっている。
  - 諸外国は IoT 製品に対するセキュリティ対策の取組を進めているところ、十分な取組を実施しない場合、我が国の IoT 製品が集中的に狙われ、国内のシステムや国民の生活に悪影響を及ぼすおそれがある。

検討会ではこれらの課題を示すとともに、以下の論点について議論を行った。

- IoT 製品ベンダーにおけるセキュリティ対策の取組を適切に評価し、適切な対策が講じられている IoT 製品が広まる仕組みの構築が必要ではないか。
- このような仕組みの構築にあたっては、我が国の IoT 製品がグローバルマーケットから弾き出されないよう、諸外国の取組を考慮することが必要ではないか。

(2) 検討会で挙げられた主な意見

- 適合性評価制度の直接的な目的として、誰の利益を想定するかを明らかにすべきである。
- 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よい。
- 様々な取組を行っている IoT 製品ベンダーを直接的なターゲットにする必要がある。また、ベンダーの取組を阻害することのないよう、検討する必要がある。
- 適合性評価制度があることで、消費者の安心感につながる。

(3) 今後議論が必要な事項

適合性評価制度は、関係者が多数に渡り、あらゆる面で細部の検討が必要になるところ、今後の制度検討が脱線しないためには、関係者間において、適合性評価制度の目的や、どのような利益や負担が関係者に生じるか、利益と負担のバランスをどう取っていくかの課題意識を、常に共有し、共通認識を持つべき目的や課題の認識について、必要に応じてブラッシュアップしていくことが必要である。

1.2. 構築すべき適合性評価制度

1.2.1. 制度の位置づけ

(1) 検討会における討議事項

適合性評価制度の構築に伴う効果や関係者の負担を考慮する観点から、適合性評価制度を法令に基づく義務とするか、任意制度とするかという点について議論を行った。義務とした場合、中小企業をはじめとする IoT 製品ベンダーの負担が増大する可能性があり、国内産業の成長を停滞させるおそれがあることや、規制要求さえ満たせばよいというマインドにつながるおそれもあり、結果、IoT 製品の安全性確保につながらない可能性があること、を提示した。他方で、任意制度とした場合、適合性評価を受けることが製品の付加価値向上につながり得るものであるため、能動的なセキュリティ向上につながりやすい可能性があることを提示した。

以上を踏まえ、以下の論点を設定し、議論を行った。

- 今回構築する適合性評価制度について、まずは任意制度として制度を運用することが適当と考えられるのではないか。

(2) 検討会で挙げられた主な意見

- 適合性評価制度を任意制度としてまず運用する方針について、異論はない。
- 任意制度であるため、市場原理を考慮して制度設計を行う必要がある。

(3) 今後議論が必要な事項

検討会での議論を踏まえると、適合性評価制度はまずは任意制度として運用することが適当である。なお、任意制度として運用を開始しつつも、制度の浸透・活用の程度、国内 IoT 製品ベンダーによる対応状況、IoT 製品に対する脅威の状況、諸外国の取組との整合性や国際的な動向等によっては、任意制度で措置されていた製品類型に対し、法令に基づく義務化に向けた検討を新たに行うことも必要になり得ると考えられる。なお、適切なルール設計は産業活動や社会の活力向上にも繋がるものであるため、こうした点も義務化に向けた検討を新たに行う場合に踏まえるべき重要な観点である。

1.2.2. 制度の対象とする製品範囲

(1) 検討会における討議事項

IoT 製品の類型は多岐にわたり、用途に基づき、消費者向け製品と産業向け製品との区分が想定されるほか、インターネットへの接続方式について、直接的にインターネットに接続する可能性がある製品[3]と間接的にインターネットに接続する製品[4]との区分[5]が想定されることを提示した。そして、各製品類型によって、リスクの度合いが異なる、既存の取組状況[6]も異なる、等を踏まえ、以下の論点を設定し、議論を行った。

- 適合性評価制度で対象とする製品の範囲について、「間接的又は直接的にインターネットに接続する製品」としてはどうか。
- その上で、製品ごとのリスクやシステム全体で対策を実施していくべき産業分野等を考慮し、「新たな制度において特に優先度の高い製品」や「既存の制度で対応すべき製品」等の峻別を精緻に行っていくべきではないか。

精緻な検討に当たっての論点の例として、以下のような論点を提示した。

---

[3] 「直接的にインターネットに接続する製品」とは、総務省「端末設備等規則（省令）」第三十四条の十の対象となる製品を指し、インターネットプロトコル（IP）の一部を構成する通信プロトコルを使用してインターネットに直接接続してデータの送受信を行う製品を指すことを想定する（ルーター、ネットワークカメラ等）。

[4] 「間接的にインターネットに接続する製品」とは、以下のいずれかに該当する製品を指すことを想定する。ただし、製品を他製品に接続するためにのみ使用される電線又はケーブルから成る製品は除外することを想定する。

1) インターネットプロトコル（IP）の一部を構成する通信プロトコルを使用して「直接的にインターネットに接続する製品」に接続し、データの送受信が可能である製品
2) 2 つ以上の製品が併せて利用されることを想定しており、少なくとも 1 つの製品（「上流製品」という。）が「直接的にインターネットに接続する製品」に接続可能であり、それ以外の製品（「下流製品」という。）が上流製品に接続してデータの送受信を行う場合の下流製品

[5] 消費者向け・産業向けの両方の用途で使われる製品も存在することに留意。

[6] 例えば、直接的にインターネットに接続する可能性がある製品については、総務省の端末設備等規則により、アクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装が原則義務化されているが、間接的にインターネットに接続する消費者向け製品の多くは、製品個別のセキュリティ対策に関するガイドラインや認証制度等に乏しいため、適切なセキュリティ対策が行われていることの証明が困難な場合がある。

- 直接的にインターネットに接続する可能性がある製品については総務省「端末設備等規則」に基づくセキュリティ対策が法的に求められているが、ETSI EN 303 645、NISTIR 8425 等の国際的な標準が要求する事項との差異を踏まえた検討をしていくべきではないか。
- 間接的にインターネットに接続する製品のうち、消費者向けの製品について、多くの製品は製品個別のセキュリティ対策要件を定めた文書や認証制度等に乏しいことから、既存制度で普及効果が高いと考えられる制度にセキュリティ要件を組込むことを検討すべきではないか。
- 産業向け製品については、CC 認証、CSA 認証等の高い基準の適用を行っていくべきと考えられるが、普及率は低い現状がある。このような現状を鑑み、CC 認証、CSA 認証等の普及を促進していく必要があるものの、広くセキュリティレベルを確保するために、適合性評価制度の対象製品範囲に含めるべき産業向け製品もあると考えられるのではないか。その際に、いかなる製品を対象とすべきかについては、製品が有するリスク、事業継続等を考慮し、分野ごとに個別に検討していくべきではないか。また、産業システム全体としてのセキュリティ対策を求めたガイドラインが存在する分野もあるため、適合性評価制度の対象とするかについては、業所管部局と議論を進めていくべきではないか。

(2) 検討会で挙げられた主な意見

- 対象製品範囲を「間接的又は直接的にインターネットに接続する製品」とする方針に同意する。ただし、製品用途に関して、間接的にインターネットに接続する産業用 IoT 製品には特異性があるため、適合性評価制度に組み込むことが困難である可能性がある。産業用 IoT 製品については、消費者向け製品と共通的に考えられる製品のみを対象にするといった整理方針も想定される。
- 産業用 IoT 製品の場合、製品利用者側にも専門家がいるという前提でセキュリティ対策を検討できる一方で、消費者が利用する IoT 製品では、利用者自身でのセキュリティ対策を期待することが困難であるため、こうした点を踏まえ調査・整理を進めるべきである。
- 対象製品範囲を「間接的又は直接的にインターネットに接続する製品」とする方針に同意する。ただし、技術的な定義が曖昧であるため、明確化する必要がある。

(3) 今後議論が必要な事項

検討会での議論を踏まえると、適合性評価制度の対象製品範囲は「間接的又は直接的にインターネットに接続する製品」とすることが適当である。その上で、いかなる製品を対象にするかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。

1.2.3. 制度で用いる適合性評価基準

(1) 検討会における討議事項

適合性評価制度で用いる適合性評価基準について、国際的な標準を活用する方針と、国内独自の基準を活用する方針という 2 つの方針に大別できるが、諸外国では IoT 製品の安全性確保に向けた適合性評価制度に関する取組が進められている[7]ことを踏まえ、以下の論点を設定し、議論を行った。

- 適合性評価制度で採用する基準について、ETSI EN 303 645 や NISTIR 8425 等、国際的な標準を基軸とした適合性評価基準を前提とすべきではないか。
- 直接的にインターネットに接続する製品については、端末設備等規則との関係の整理が必要と考えられる。総務省の端末設備等規則によるセキュリティ対策が求められているが、ETSI EN 303 645 や NISTIR 8425 が要求する事項との差異を踏まえた検討をしていくべきではないか。
- なお、ETSI EN 303 645 や NISTIR 8425 で定められている要求基準のうち、具体的にどの基準を、どの製品類型に適用するかについては、個別に検討が必要ではないか。

(2) 検討会で挙げられた主な意見

- 国際的な標準を基軸とした適合性評価基準とする方針に同意する。その上で、どの程度の基準を設けるか、今後詳細に議論すべきである。
- 適合性評価基準の策定に当たって、小規模な検討グループを組成し、ETSI EN 303 645、NISTIR 8425、ISO/IEC DIS 27402 等の国際的な標準における要求事項を整理したうえで、基準を策定することが必要である。
- 国際的な基準を参考に適合性評価基準を策定する際、どの基準を採用したかを明確にしつつ策定する必要がある。
- IoT 製品ベンダーの負担を軽減する観点では、一つの適合性評価基準で広い範囲をカバーする方がよい。

(3) 今後議論が必要な事項

検討会での議論を踏まえると、適合性評価制度で用いる適合性評価基準については、国際的な標準を参照の上、国際的な標準と整合的な形で構築していくことが適当である。その上で、具体的な適合性評価基準の策定に当たっては、どのような体制で検討を行っていくか、いくつかのリスクレベ

[7] 英国の PSTI 法やドイツ、シンガポール及びフィンランドのラベリング制度では、ETSI EN 303 645 に基づく基準が用いられているほか、米国のラベリング制度では、NISTIR 8425 に基づく基準が検討されている。さらに、国際標準としては、ISO/IEC DIS 27402 が開発されている。

ルが想定されるところどの程度の基準を策定するべきか、いかなる製品類型に対しどのような考え方で基準を適用していくか、等の考え方について、国内外の関連する動向を踏まえつつ、詳細に検討を行っていく必要がある。

1.2.4. 制度で活用する適合性評価スキーム

(1) 検討会における討議事項

適合性評価制度で活用する適合性評価スキームについて、既に運用されている適合性評価スキームを活用する方針と、新たな適合性評価スキームを構築する方針という 2 つの方針に大別できるが、任意制度において知名度のない制度を 0 から普及させるには高いハードルがあるほか、利用者から見て制度が林立し分かりづらくなる可能性もあることなどを踏まえ、以下の論点を設定し、議論を行った。

- 任意制度において、知名度のない制度を 0 から普及させるには高いハードルがあることや、消費者から見て制度が林立し分かりづらくなる可能性があることから、新たに制度を構築することは避け、既存の適合性評価スキームを活用した制度とすることが適当ではないか。
- その際に、どの既存制度を活用するかは、製品類型と現に対象となっている既存制度の関係、製品類型ごとのリスク等も勘案して判断していくべきではないか。

なお、IoT 製品ベンダーの自己適合宣言による適合性評価の可否についても、以下の論点を設定し、議論を行った。

- 自己適合宣言の許容可否について、製品範囲、適合性評価基準及び評価スキームを具体化した上で、実効性やコスト等を勘案して検討していくべきではないか。

(2) 検討会で挙げられた主な意見

- 既存スキームを活用した制度とする方針に同意する。既に基準やスキームが存在する製品類型があるため、それらの取組を阻害しないよう、適合性評価制度の検討を進めることが重要である。
- 認証機関の負担が大きいスキームは継続しないため、どのようなスキームを構築することで制度が適切に運用されるのか、適合性評価コストを踏まえた検討が必要である。
- 既存スキームと海外制度との連携可能性について、今後整理する必要がある。
- 既存スキームを活用した制度とする場合、既存スキームで既に適合性評価を受けている製品との整合を図る必要がある。

自己適合宣言の可否に関する上記の論点について、特に異論は示されなかった。

(3) 今後議論が必要な事項

適合性評価制度の運用に当たっては、既存の評価スキームを活用した制度とすることが適当である。具体的に、どの製品類型に対して、どの既存スキームを活用するかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。検討に当たっては、諸外国の制度との連携や、現行制度との整合性、運用能力等について、既存の評価スキームを所掌している機関と丁寧に検討を進めていくことが重要と考えられる。

2. 今後議論が必要な事項

令和 4 年度に開催した検討会では、第 1 章で示した意見のほか、以下のような意見が挙げられた。これらの意見を踏まえ、令和5年度以降議論すべき事項を記載する。

(1) 検討会で挙げられた主な意見

- 適合性評価制度が広まることによる社会的なメリットを示すことが重要である。IoT 製品ベンダーにおいても様々な社会的貢献が求められており、安全な製品をベンダーが開発・販売することで、サイバー公衆衛生の向上という一つの社会的貢献に寄与し得る。
- 調達要件と連携して市場を守るといった取組を講じることができれば、IoT 製品ベンダーに対して適合性評価制度を普及させることができるのではないか。
- IoT 製品ベンダーの利益に寄与するために、国際的なハーモナイゼーションについて検討していく必要がある。
- 海外の状況等も踏まえた上で、フィージビリティ・スタディを行っていただきたい。
- 任意制度とする場合、制度の知名度を上げる努力をしない限り IoT 製品ベンダーの説明コストは変わらないため、適合性評価制度のプロモーションを製品の利用者や調達者に対しても適切に行う必要がある。制度の検討段階から積極的なプロモーションを行い、制度の活用促進を図っていくことが重要である。
- 任意制度が活用されるために、製品ベンダーや製品利用者のインセンティブやモチベーションを高めるための取組を整理する必要がある。
- 制度活用のインセンティブの設計に関して、補助金や各種調達要件との連携など、適合性評価を行った IoT 製品ベンダーに対する明確なインセンティブの設計が必要である。
- 適合性評価基準や評価品質によって、評価に要する期間やコストが大きく変わる。認証機関に負担の大きな評価方法とした場合に、スキームの継続は難しい。
- セキュリティや製品安全における責任範囲に関して、一義的には製品開発者や販売者が責任を負うこととなるが、サプライチェーンの複雑化に伴い、現実的には部品の製造者やサービス関連事業者に責任が及ぶ可能性がある。
- セキュリティ事案が発生した際の利用者保護の観点では、保険制度を取り入れるべきである。
- IoT 製品のライフサイクルを踏まえ、サーベイランスの必要性を検討すべきである。

(2) 今後議論が必要な事項

2.1. 政府の関与や検討体制のあり方

2.1.1. 認証機関との連携

複数の既存スキームを活用する場合、適合性評価を行う認証機関が複数となり得ることや、認証取得数の増加に向けては認証機関の適格性が重要となることから、各主体の適格性について、政府のガバナンスが効く構造を構築することが重要となる。

2.1.2. 評価基準等を検討する委員会の構築

具体的な適合性評価基準の策定に当たっては、IoT 製品の性質やリスク、海外制度等について専門的な知見が必要となるため、各分野の専門家を招聘し、評価基準等を検討する委員会を設置することが適当と考えられることから、あるべき具体的な体制や方針について、詳細に検討を行っていく必要がある。

2.1.3. 政府基本方針の策定

認証機関の適格性を向上させる観点や、基準等を検討する委員会のガバナンスの観点、複数になり得る認証機関の方向性を束ねる観点、企業の社会貢献の観点等から、政府は基本方針のような形で大きな方向性を示していく必要がある。

2.2. IoT 製品ベンダーの能動的な制度活用を促す仕掛け

2.2.1. 各種調達要件との連携、消費者に対する需要喚起策

ベンダーの能動的な制度活用を促す仕掛けとして、各種調達要件[8]との連携や消費者に対する需要喚起策が想定される。今後、各種調達要件と連携について、その効果や、いかなる調達要件とどのように連携すべきか等について、その根拠付けと共に検討する必要がある。

また、消費者に対する需要喚起策についても、適合性評価制度がどう安全・安心に繋がるのか、適合性の評価がなされていない製品とはどのような差があるのか、等の観点も踏まえ、その効果、他の取組との連携可能性、具体的な喚起方法等について、検討する必要がある。

---

[8] 例えば、政府調達におけるセキュリティの取組として、経済産業省はデジタル複合機、ファイアウォール等の製品類型ごとに考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめた「IT 製品の調達におけるセキュリティ要件リスト」を公開している。IPA では、当該リストの活用方法をまとめた「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」を公開している。内閣官房内閣サイバーセキュリティセンター（NISC）では、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」において、政府機関等が IT 製品を調達する際に、NISC に対してサプライチェーン・リスクの観点から講ずべき措置について助言を求めることを関係省庁間で申合せしている。デジタル庁では、デジタル臨時行政調査会が、規制所管省庁が規制の見直しに当たってどのような技術が活用可能であるかを把握できるよう、アナログ規制の類型と、その見直しに活用可能な技術の対応関係を整理、可視化したテクノロジーマップ等を整備していく予定。

2.2.2. 諸外国の適合性評価制度との国際連携

諸外国ではIoT製品の適合性評価制度の検討が進んでおり、この認証取得のために日本企業の負担が増えることが想定されるところ、適合性評価制度と諸外国の制度の連携を図ることで、負担幅を抑えることが重要と考えられる。今後、諸外国制度の動向を踏まえつつ、どの諸外国制度と、どのような国際相互承認方式で連携し、基準について具体的にどのように整合的に連携するか等について、検討する必要がある。

2.2.3. IoT製品ベンダーや認証機関等に対する支援策

適合性評価を行うには認証機関やベンダー、消費者等の関係者に様々なコストが発生すると考えられる。まずは、どのような製品類型に対し、いかなる基準を適用することで、関係者にどの程度のコストが発生するかについて実証等を通じて検証する必要がある。その上で、制度普及を後押しする観点から、関係者において発生するコストを抑制するため支援策[9]について、必要に応じて検討する必要がある。

2.3. 適合性評価済製品におけるセキュリティ事案への対応

2.3.1. 法的な論点整理

適合性評価を受けた製品に脆弱性が見つかり、セキュリティ事案につながるおそれがあることから、適合性評価を受けることでどのような責任分界につながるか、事案発生時にどのような関係者がどのような責任を負う必要があるか、どのような備えをしておくべきか、等について検討する必要がある。利用者の立場から見ても、認証を取得した製品を選んだという説明責任が果たせることは重要であると考えられる。

2.3.2. リスクに対応するための資源の確保策

事案発生時の法的な責任分担の整理に加え、例えば保険制度のような、事案発生時に対処を適切に行い、被害救済や原因是正に繋がる資源の確保策についても、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。

[9] シンガポールが実施しているセキュリティラベリング制度であるCybersecurity Labelling Schemeでは、制度開始後1年間、適合性評価にかかる申請料を無償とすることで制度活用促進を図った。この結果、2023年2月時点で230製品以上にラベルが付与されている。

2.3.3. 評価済製品のサーベイランス、取り消し

一度適合性評価を行った後の製品が、市中に流通した際に、不適合の状態でないかを監視（サーベイランス）し、不適合であった場合には取消措置を行える制度[10]を整えることは、粗悪な製品の流通を防止することに有効であると考えられる。一方で、特にサーベイランスについて、IoT 製品のライフサイクルによっては、必ずしもそぐわない場合もあると想定される。したがって、現行制度の状況や、どのような製品類型を対象とするか、どのような者が運用するか、どのような仕組みとするか、適合性評価結果の有効期限についてどう考えるか、どの程度コストが発生するか、等の想定される基本的な事項について、必要性も含めて検討をする必要がある。

[10] 例えば、シンガポールのラベリング制度では、ラベル取得済み製品に対する無作為のサーベイランスが実施され、基準に適合していないと判断される場合にはラベルの取り消しがなされる。ドイツのラベリング制度においても、ランダムサンプリングに基づき基準に適合しているかが確認され、申請内容に反していることが明らかになった場合には、製品ベンダーに対して監査が行われる可能性がある。

3. 付録

3.1. 諸外国政府における IoT 製品の安全性確保に向けた取組

3.1.1. 米国における取組

米国政府における IoT 製品の安全性確保に向けた近年の代表的な取組として、2020 年に成立した「IoT Cybersecurity Improvement Act of 2020」[11]が挙げられる。この法律では、NIST に対して、政府機関が所有・管理する情報システムに接続された IoT 製品を適切に使用・管理するための標準やガイドラインの作成が指示された。また、本法律の制定を受け、2021 年 11 月、NIST より、連邦政府が IoT 製品を調達する際のガイドラインである NIST SP 800-213 及び NIST SP 800-213A が公表された。これらのガイドラインでは、具体的なセキュリティ対策内容について、NISTIR 8259 シリーズが引用されている。NISTIR 8259 シリーズに関連して、2022 年 9 月には、消費者向け IoT 製品に共通して求められるサイバーセキュリティ能力を示した NISTIR 8425 を公開した。

また、2021 年に署名されたサイバーセキュリティを強化する大統領令（Executive Order on Improving the Nation's Cybersecurity）[12]に基づく動向も挙げられる。この大統領令では、NIST に対して、消費者向け IoT 製品に対するセキュリティラベリング制度の検討を指示した。2022 年 2 月、NIST は消費者向け IoT 製品に対するラベリング制度に関する考慮事項を示した文書を発表し、ラベリングのためのベースライン基準として、NISTIR 8259 に基づく基準を推奨した。ただし、具体的な制度オーナー、評価方法、ラベルの種類等は定められておらず、今後の検討事項に位置づけられている。大統領令に関連して、2022 年 10 月、ホワイトハウスは、消費者向け IoT 製品のラベリング制度の構築に向け、企業、団体及び政府機関のステークホルダー間で議論を実施した。ラベル付与の方法について、米国政府の基準に基づき、審査・承認された機関によってテストする方針を示しつつ、基準については、NISTIR 8259 に基づき策定された NISTIR 8425 をベースライン基準とした制度が検討されている。そして、まずルーター及びホームカメラ[13]から着手し、2023 年春の制度展開を目指すと発表した。

そのほか、州の取組として、カリフォルニア州（SB-327：Information privacy: connected devices）やオレゴン州（HB-2395：Oregon Cybersecurity Bill）では IoT 製品に対するセキュリティ対策が州法に基づき義務化されている。それぞれの州法では、インターネットに接続するコネクテッドデバイスに対するセキュリティ強化を目的としており、それぞれの州で IoT 製品を販売するメーカーに対し、パスワードの管理等を含む合理的なセキュリティ機能を具備することを求めている。対象となる IoT 製品について、インターネットに直接的・間接的に接続される機器が対象となるが、他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品（産業用 IoT 製品、PC、サーバー、モバイル端末等の IT 製品等）は対象外である。

---

[11] IoT Cybersecurity Improvement Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/1668

[12] White House, Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[13] この 2 機器の選定理由として、最も一般的かつリスクが高い機器であることを挙げている。

3.1.2. 英国における取組

英国政府におけるIoT製品の安全性確保に向けた近年の代表的な取組として、2018年にDCMS（デジタル・文化・メディア・スポーツ省）が発表した消費者向けIoT製品のセキュリティに関する13の行動規範である「Code of Practice for Consumer IoT Security」[14]が挙げられる。この行動規範では、消費者向けIoT製品の設計段階で安全性が確保されること、また、利用者がデジタルの世界を安心して楽しめるようにガイドラインを設けることで、IoT製品の開発、製造、販売に携わる利害関係者を支援することを目的としている。対象製品について、インターネットやホームネットワーク（両方又はその一方）と関連サービスに接続する消費者向けIoT製品を対象としている。英国DCMSは本行動規範をEU全体に普及させるべく、技術仕様の国際標準化をETSIに提案した。ETSIはこの提案に基づき、EU加盟各国のステークホルダーによる討議を実施し、2019年2月にTS（技術仕様）であるETSI TS 103 645を公表、2019年11月には、EN 303 645として欧州規格化された。なお、ETSI EN 303 645はフィンランド、ドイツ、シンガポールのラベリング制度のベースとなっているほか、後述するPSTI法のベースにもなっている。

また、消費者向けIoT製品に対してセキュリティ対策の義務化を求める「Product Security and Telecommunications Infrastructure Act（PSTI法）」[15]が2022年12月に成立した。この法律の文面には明確なセキュリティ要件や経過措置の期間などは明記されておらず、具体化については担当国務大臣に委ねられている。法案検討段階では、具体的な対策として、デフォルトパスワードの禁止、脆弱性開示ポリシーの開示、セキュリティアップデートを受ける期間に関する情報の開示の3点が含まれており、これらの対策実施に関して、第三者評価による適合性評価が必要となる見込みである。なお、法律には、これらの対策に遵守しない企業に対する罰金に関する条項も含まれており、最高1,000万ポンド又は当該企業の全世界売上高の4%以内の罰金が科せられる内容となっている。また、対象となる企業について、IoT製品のメーカーだけでなく、輸入業者や販売業者も含まれる。

3.1.3. EUにおける取組

EU全体のIoT製品の安全性確保に向けた近年の代表的な取組として、2019年に規則(EU) 2019/881「Cybersecurity Act」[16]が施行され、IoT製品を含む製品の認証スキームであるEUCC（Common Criteria based European Candidate Cybersecurity Certification Scheme）が検討されている。EUCCはサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存のCC（Common Criteria）のスキームの後継として機能させることを目的としている。2021年5

[14] DCMS, Code of Practice for Consumer IoT Security https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[15] Product Security and Telecommunications Infrastructure Act 2022 https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

[16] Regulation (EU) 2019/881: Cybersecurity Act https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG

月には、EUCC のスキーム候補に関する報告書（Ver 1.1.1）を公表し、ISO/IEC 15408 と ISO/IEC 18045 に基づいて、ICT 製品のサイバーセキュリティの認証を検討していることを発表した。

また、2022 年 1 月、欧州委員会は、Radio Equipment Directive（RED：欧州無線機器指令）のサイバーセキュリティ関連条項の施行に関する委任規則（EU） 2022/30[17] を発行し、EU 市場に投入される無線機器に対してセキュリティの強化を求めた。具体的な規則は 2024 年 8 月 1 日より義務化となる予定であり、対象機器について、直接・間接問わずインターネットに接続される無線機器が対象となる。求められる対策として、許容できないサービスの低下を引き起こさないこと、個人データ及びプライバシーを保護するための手段を組み込んでいること、不正行為から保護するための一定の機能をサポートすることの 3 点が求められているが、具体的な規格要件は 2023 年 10 月までに準備される予定である。

加えて、2022 年 9 月、欧州委員会は、EU 市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EU Cyber Resilience Act（CRA）」[18]の草案を発表した。EU CRA と他の EU 法令との関係性は図 3-1 に示すとおりである。EU CRA は、2022 年 5 月に欧州議会・欧州理事会が改訂に合意し、2023 年 1 月に発効された NIS2 指令（Network and Information Security 2 Directive）を補間する目的で策定された。EU CRA は、前述した RED の対策要件を包含する位置づけであるため、EU CRA が施行された後、RED のセキュリティ関連要件は廃止となる。また、EU CRA と EUCC との関係について、EUCC に基づく適合性証明書を EU CRA で求められる適合性証明に用いることが可能である。対象について、ICT サービスやプロセスも対象としている EUCC の方が対象範囲は広いものの、製品自体の定義に大きな差異はない。

[17] Commission Delegated Regulation (EU) 2022/30 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.007.01.0006.01.ENG

[18] European Commission, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

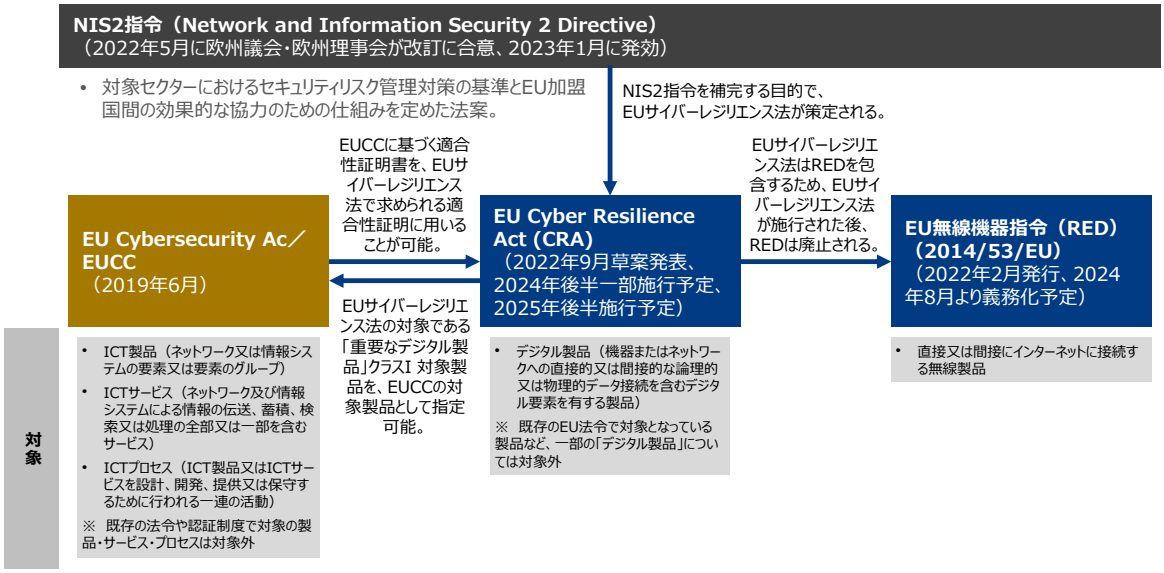

図 3-1 EU CRA と他の EU 法令との関係性

EU CRA の対象となる製品について、ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆる「デジタル製品」が対象となる。ただし、既存の規則で対象となる製品は対象外であり、医療機器・体外診療用医療機器、自動車、航空機関連のデジタル製品、SaaS 等のソフトウェアサービス、国家安全保障又は軍事目的にのみ開発されたデジタル製品及び機密情報を処理するために特別に設計された製品は対象外である。対象となる「デジタル製品」のうち、重要な「デジタル製品」のうちリスクが低い製品をクラスⅠ、リスクが高い製品をクラスⅡとして詳細に定義（図 3-2 参照）しており、クラスに応じて、選択できる適合性証明の方法が異なる。適合性証明のスキームとして、EU 適合宣言（CE マーク）のスキームを採用している。

これらの対象製品に求められる対策として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産することのほか、悪用可能な既知の脆弱性がない状態とすること、製品の SBOM（ソフトウェア部品表）を作成すること等、多岐にわたる対策が求められる。英国の PSTI 法と同様に罰則が規定されており、要件に違反した場合には、罰金として 1,500 万ユーロ又は全世界売上高の 2.5%のいずれか高い方が科される可能性がある。本法案では、法制化された後の経過措置として、24 ヶ月の猶予期間が設定されているが、製造業者における脆弱性とインシデントの報告に関しては、12 ヶ月のみの猶予期間が設定されている。

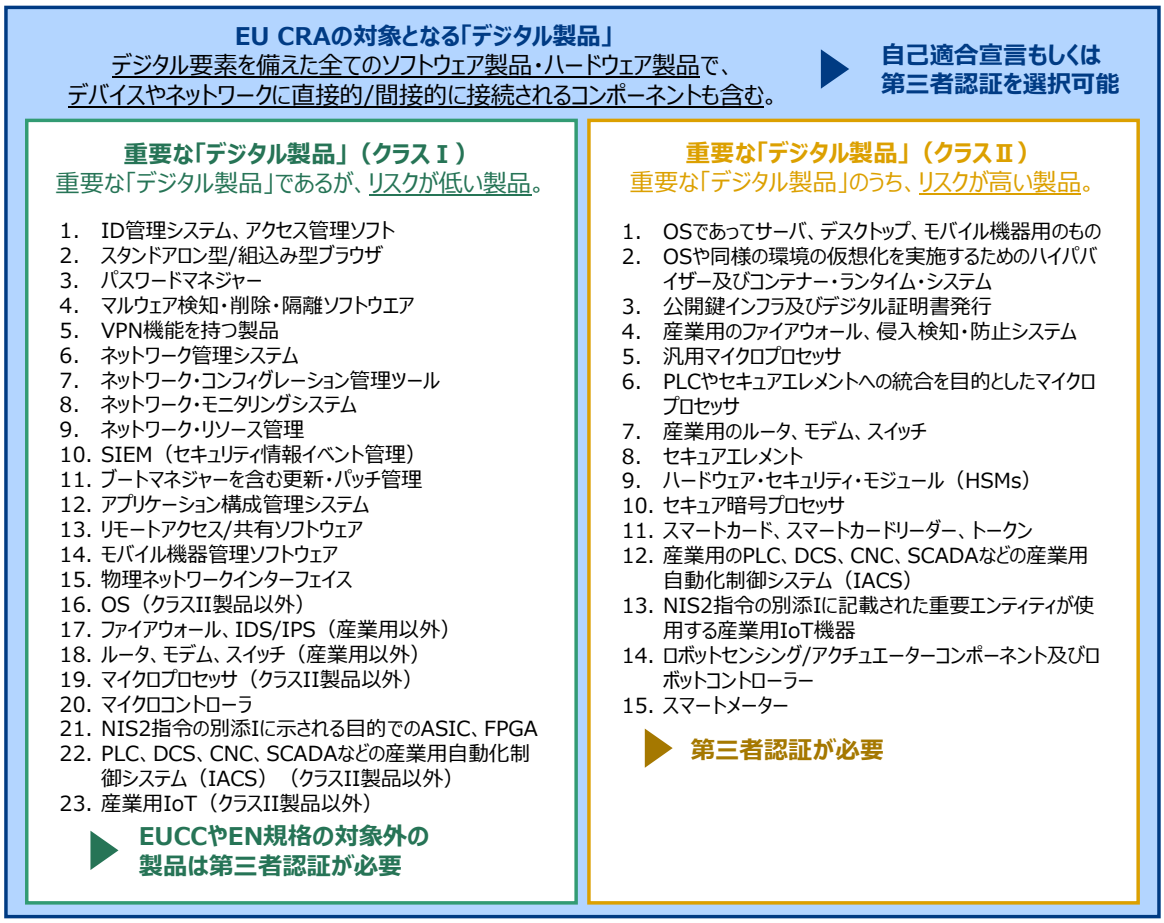

図 3-2 EU CRA の対象製品のうちクラスⅠ・クラスⅡに該当する製品

3.1.4. その他主要国における取組

その他諸外国政府における IoT 製品の安全性確保に向けた近年の代表的な取組として、ドイツ、シンガポール、フィンランドでは、消費者向け IoT 製品に対するセキュリティラベリング制度が既に開始しているほか、オーストラリアでも同様のラベリング制度の構築に向けた検討がなされている。

ドイツの BSI（連邦情報セキュリティ庁）の任意のラベリング制度（IT-Sicherheitskennzeichen）[19]は 2021 年 12 月から開始している。対象製品について、現状ではブロードバンドルーター、電子メールサービス、スマートテレビ、スマートスピーカー等の一部の消費者向け IoT 製品のみを対象としている。ただし、今後対象製品を拡大する方針を示している。ラベル付与のためには、ETSI EN 303 645 の要件に加え、BSI 及び ETSI が作成した各製品分野のセキュリティ要件を満たしていることを自己確認し、確認結果を BSI に承認されることが必要となる。2022 年 2 月時点で 37 製品・サービスがラベルを取得している。

[19] BSI, IT-Sicherheitskennzeichen https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html

シンガポールの CSA（サイバーセキュリティ庁）が運用するラベリング制度（Cybersecurity Labelling Scheme: CLS）[20]は、すべての消費者向け IoT 製品を対象とした任意のラベリング制度であり、2020 年 10 月から制度が開始している。付与されるラベルは 4 段階に分かれ、レベル 1・2 は開発者の自己適合宣言で取得可能、レベル 3・4 では第三者機関による検証が必要となる。ラベル付与のためには ETSI EN 303 645 の要件に加え、レベル 3 では、第三者機関によるバイナリ解析、レベル 4 では機器に対するペネトレーションテストにクリアする必要がある。2023 年 2 月時点で 233 製品がラベルを取得している。なお、本制度はドイツのラベリング制度やフィンランドのラベリング制度との相互運用を実施している。また、本制度の要件は ISO/IEC 27404 として、国際標準化に向けた提案がなされている。

フィンランドの TRAFICOM（運輸通信庁）が運用するラベリング制度（Finnish Cybersecurity Label）[21]は、すべての消費者向け IoT 製品を対象とした任意のラベリング制度であり、2020 年 1 月から制度が開始している。ラベル付与のためには、ETSI EN 303 645 をベースに作成された情報セキュリティ要件を満たしていることを、認定を受けたセキュリティ機関によって評価されることが必要となる。2023 年 2 月時点で 25 製品がラベルを取得している。

オーストラリアでも内務省を中心に、インターネットやホームネットワークに接続される前提で開発されたあらゆる消費者向け IoT 製品を対象としたセキュリティラベリング制度の検討が進められている[22]。ラベル付与のための基準として、ETSI EN 303 645 を採用する方針が示されている。なお、2022 年 3 月には、BETA（豪州政府行動経済学チーム）が IoT 製品のセキュリティラベルの有効性に関する調査結果[23]を発表し、セキュリティラベルが付与されることで、IoT 製品に対する消費者の支払意思額が増加することを示した。

3.2. 日本政府における IoT 製品の安全性確保に向けた取組

我が国における代表的な取組として、下表に示すとおり、IoT 製品メーカーのセキュリティ対策を支援するガイドラインが経済産業省、IPA、総務省等から複数発表されている。

[20] CSA, Cybersecurity Labelling Scheme https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls

[21] TRAFICOM, Finnish Cybersecurity Label https://tietoturvamerkki.fi/en/cybersecurity-label

[22] Department of Home Affairs, Strengthening Australia's cyber security regulations and incentives https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives

[23] BETA, Stay Smart – Helping consumers choose cyber secure smart devices https://behaviouraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf

表 3-1 IoT 製品メーカーのセキュリティ対策を支援するガイドライン

#	文書タイトル	発行時期	発行者	文書概要
1	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	2019 年 4 月	経済産業省	新たなサプライチェーン構造において求められるセキュリティ対策の全体像を整理し、セキュリティ対策例をまとめた文書
2	IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）	2020 年 11 月	経済産業省	IoT 機器・システムをリスクに応じてカテゴライズし、各カテゴリに対するセキュリティ・セーフティ要求の検討の考え方を示した文書
3	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き	2021 年 4 月	経済産業省	機器のセキュリティ検証において検証サービス事業者や検証依頼者が実施すべき事項等について整理した文書
4	電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン	2021 年 4 月	経済産業省	家電製品などがインターネット環境で使われることで想定されるリスクに対し、安全確保の在り方を示した文書
5	IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集	2022 年 4 月	経済産業省	一連の IoT-SSF の適用の流れを、複数のユースケースを用いて例示した文書
6	IoT セキュリティガイドライン ver 1.0	2016 年 7 月	IoT 推進コンソーシアム、総務省、経済産業省	リスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめた文書
7	つながる世界のセーフティ&セキュリティ設計入門	2015 年 10 月	IPA	IoT 製品のセーフティ設計・セキュリティ設計の手法の用い方について解説した文書
8	つながる世界の開発指針	2016 年 3 月	IPA	IoT 製品の開発時に考慮すべき安全安心に関わる事項を指針としてとりまとめた文書
9	IoT 開発におけるセキュリティ設計の手引き	2016 年 5 月	IPA	IoT 製品のセキュリティ設計を担当する開発者に向けた手引きとして、参考となる情報をまとめた文書

#	文書タイトル	発行時期	発行者	文書概要
10	つながる世界の品質確保に向けた手引き	2018 年 6 月	IPA	IoT 製品やシステムの品質をライフサイクルにわたり確保・維持するために注意が必要となるポイントをまとめた文書
11	脆弱性対処に向けた製品開発者向けガイド	2020 年 8 月	IPA	製品開発者において実施すべき脆弱性対処と、その開示方法を掲載した文書
12	IoT 機器等を開発する中小企業向け製品セキュリティ対策ガイド（仮称）	作成中	経済産業省（予定）	中小の IoT 機器メーカーが現実的に対応可能な範囲で実施が求められる対策を示した文書（予定）

ガイドラインに関する取組に加え、総務省は、端末設備等規則（省令）（第 34 条の 10）を 2020 年 4 月に一部改正し、電気通信業者のネットワークに直接接続する同規則の施行後に販売された IoT 機器においてアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装を原則義務化した。対象となる設備について、例えば、ルーターやインターネットに直接接続するウェブカメラ等は該当するが、電気通信回線設備（インターネット等）に直接接続して使用されない機器、PC・スマートフォン、専用線のみにつながる機器等は対象外である。また、総務省及び NICT は、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起の取組である NOTICE（National Operation Towards IoT Clean Environment）を 2019 年 2 月から開始している。

そのほか、IoT 製品を対象に含むセキュリティに関する認証制度として、IPA による CC（Common Criteria）に基づく IT セキュリティ評価及び認証制度（JISEC）が存在する。JISEC は、IT 関連製品のセキュリティ機能の適切性・確実性を CC（ISO/IEC 15408）に基づき適合性評価機関が評価し、その評価結果を認証機関が認証する制度であり、IT 関連製品の認証取得のためには、認定機関によって認定された適合性評価機関（試験機関）によって検証・評価が実施される必要がある。認証機関は、評価結果を確認した後、その製品に対する認証書を発行する。なお、認証は国際的承認アレンジメント加盟国（CCRA 加盟国）でも通用する。また、産業用 IoT 製品に対する認証制度としては、IEC 62443-4-2 に基づく CSA（Component Security Assurance）認証制度が存在する。CSA 認証では、ソフトウェア開発プロセスのセキュリティ評価、機能的セキュリティ評価、脆弱性テストの 3 つの観点から評価される。対象機器について、ソフトウェアアプリケーション、組込み機器、ホストデバイス、ネットワークデバイス等を含む産業用コンポーネント機器が対象となる。認証機関として、国内では技術研究組合制御システムセキュリティセンター CSSC 認証ラボラトリーが存在する。加えて、政府機関が主導する認証制度ではないが、重要生活機器連携セキュリティ協議会（CCDS）が運用する「CCDS サーティフィケーションプログラム」も存在する。これは、一定のセキュリティ確保のための要件を満たした IoT 製品に対する認証サービスであり、2019 年 10 月より開始している。認証は 3 段階のレベルに分かれ、レベル 1 は IoT 製品として共通する一般的要件、レベル 2 以上は製品分野別に設定された要

件への遵守が必要となる。対象製品について、インターネットにつながる IoT 製品全般が現状の対象であるが、今後 IoT 機器を利用したサービスも範囲に含むことが検討されている。認証は、CCDS が独自で策定した「IoT 機器セキュリティ要件ガイドライン」の要件に基づき行われる。

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

構成員等名簿

※　敬称略・五十音順（令和 5 年 3 月現在）

（委員）

副座長	猪俣　敦夫	大阪大学　情報セキュリティ本部　教授
	稲垣　隆一	稲垣隆一法律事務所　弁護士
	岩﨑　章彦	一般社団法人電子情報技術産業協会　セキュリティ専任部長
座長	高倉　弘喜	国立情報学研究所　アーキテクチャ科学研究系　教授
	高橋　範	株式会社ソラコム　事業開発ディレクター
	中尾　康二	国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　主管研究員
	中野　学	パナソニックホールディングス株式会社　技術部門　テクノロジー本部 製品セキュリティセンター　製品セキュリティグローバル戦略部　部長
	花見　英樹	株式会社日立製作所　インダストリアルデジタルビジネスユニット　CTO
	広瀬　良太	ヤマハ株式会社　音響事業本部　基盤技術開発部　部長
	松浦　芳樹	GROOVE X 株式会社　Software チーム　エリアプロダクトオーナー
	唯根　妙子	消費生活アドバイザー

（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　情報産業課、製品安全課、産業機械課、国際電気標準課、通商機構部

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）

技術研究組合制御システムセキュリティセンター（CSSC）

電気製品認証協議会（SCEA）

以上