

IoT 製品に対する セキュリティ適合性評価制度構築方針

令和6年8月

経済産業省 商務情報政策局
サイバーセキュリティ課

目次

1.	はじめに.....	1
2.	構築するセキュリティ適合性評価制度の目的と位置付け.....	4
2.1.	制度の必要性及び目的.....	4
2.2.	制度の位置付け.....	5
2.3.	制度の初期ターゲット.....	5
3.	構築するセキュリティ適合性評価制度	6
3.1.	制度の運用体制	6
3.2.	制度の対象とする製品範囲	7
3.3.	制度における適合性評価レベル	8
3.4.	制度で用いるセキュリティ要件・適合基準・評価手順	9
3.5.	制度における適合性評価の主体.....	12
3.6.	ラベルの意味合い	14
3.7.	ラベルの信頼性確保のための仕組み.....	15
3.8.	関連機関や国内外の関連制度等との連携の仕組み	17
3.8.1.	各組織の調達要件への反映に関する働きかけ	17
3.8.2.	特定分野のシステムに関する業界団体・WG との連携	18
3.8.3.	諸外国制度との連携.....	19
4.	制度の発展に向けた施策.....	22
4.1.	IoT 製品ベンダーに対するラベル取得促進策.....	22
4.2.	調達者・利用者に対する制度普及促進策	22
4.3.	評価機関・検証事業者に対する支援策	23
4.4.	リスクに対応するための資源の確保策	24
4.5.	制度全体の効率化	24
5.	今後の検討の進め方及びスケジュール	25

別紙 IoT 製品ベンダー関連の賛同団体一覧

別添 ☆1 セキュリティ要件・適合基準

1. はじめに

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 5 年度情報通信白書¹によれば、世界の IoT 製品数について、2024 年には 399 億台、2025 年には 440 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 製品のセキュリティ確保に向けた取組に力を入れている。諸外国における主な取組として、以下が挙げられる。

- 米国では、消費者用無線 IoT 製品に対する任意のサイバーセキュリティラベリング制度「U.S. Cyber Trust Mark²」について、2024 年 7 月 30 日に最終規則 (Final Rule)³を公表した。2024 年中に制度を開始する予定であり、消費者向けルータ、スマートメーター等一部製品については、個別のセキュリティ要件が定義される見込み。
- EU では、一部例外を除き EU 市場に上市するデジタル要素を備えた全ての製品を対象に、製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける EU サイバーレジリエンス法の草案が 2022 年 9 月に発表され、2024 年後半に発効、報告義務を除き 2027 年に施行される見込み⁴。
- 英国では、消費者向け IoT 製品の製造者に対し、最低限のセキュリティ基準への自己適合を求める PSTI 法⁵が 2022 年 12 月に成立し、2023 年 9 月の下位法⁶の成立を経て 2024 年 4 月に施行された。
- シンガポールでは、消費者向け IoT 機器に対する任意のセキュリティラベリング制度を 2020 年 10 月より開始しており、ドイツ、フィンランドの類似制度と相互承認を実施している。

我が国においても IoT 製品のセキュリティ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 製品を製造する事業者等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、独立行政法人情報処理推進機構 (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

¹ 総務省, 情報通信白書令和 5 年版 <https://www.soumu.go.jp/johotsusintokei/whitepaper/r05.html>

² The White House, Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/>

³ Federal Register, Cybersecurity Labeling for Internet of Things <https://www.federalregister.gov/documents/2024/07/30/2024-14148/cybersecurity-labeling-for-internet-of-things>

⁴ European Commission, Cyber Resilience Act <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

⁵ legislation.gov.uk, Product Security and Telecommunications Infrastructure Act 2022 <https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted>

⁶ legislation.gov.uk, The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 <https://www.legislation.gov.uk/uksi/2023/1007/contents/made>

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。

しかしながら、端末設備等規則は、電気通信事業法に基づく端末機器の技術基準等への適合性に係るセキュリティ基準等を定めたものであり、誰もが安心して安定的に利用できるネットワーク環境を確保するためにIoT製品のマルウェア感染を抑制することを期待したものである。その他の施策は、IoT製品のセキュリティ確保のため、IoT製品を製造又は販売する事業者（以下「IoT製品ベンダー」という。）に対してセキュリティ対策の自主的な取組を求める側面が大きい。このため、現状では、IoT製品ベンダーにおけるセキュリティ対策の取組について調達者・利用者にアピールすることが難しい。一方、調達者・利用者から見ても、セキュリティ対策が適切か否か判断できないという課題がある。また、政府機関や企業等でのセキュリティ対策において、調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーン・リスク管理の取組が広がっている。その中で本来自組織が実施すべき、製品のセキュリティ機能や対策状況を確認するプロセスを選定・調達時に実行できているところは少ない。

これらの課題を解決する方法として、共通的な物差しで製品のセキュリティ機能を評価・可視化するためのセキュリティ製品に対する認証制度がある。例えば、CC(Common Criteria)に基づくITセキュリティ評価及び認証制度(JISEC)⁷、産業用製品に対するIEC 62443-4-2に基づくCSA(Component Security Assurance)認証制度等である。しかしながら、これらの認証制度は、要求されるセキュリティ水準が比較的高いため、認証を取得するための金銭的・時間的コストが大きい。このため、多くのIoT製品にとって、これらの認証制度を活用するハードルが高い。また、一部のIoT製品類型を対象とした民間団体による認証制度も存在するが、政府機関等が調達時に行う製品セキュリティ評価として活用するためには、調達され得るIoT製品を広く対象とし、国内で広く浸透している認証制度であることが望ましい。

そのため、金銭的・時間的コストを抑え、多くのIoT製品を対象とする認証制度として、諸外国の取組も踏まえつつ、一定水準のセキュリティ要件に対するセキュリティ対策の適合性を評価し、その結果を認証やラベルの付与等により、調達者・利用者が分かる形で可視化する制度を政府主導で構築することが求められる。これにより、IoT製品ベンダーは適切なセキュリティ対策が取られたIoT製品であることをアピールすることができ、調達者・利用者が製品を選択しやすくなる。

IoT製品は、サイバー空間とフィジカル空間の高度な融合によって社会全体の付加価値を増大させるために、人とモノをつなげる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ており、IoT製品においても脆弱性を狙ったサイバー脅威は深刻化するものと推測される。このため、IoT製品は、サイバー空間とフィジカル空間を相互につなげるだけでなく、適切なセキュリティ対策が取られることも必要不可欠となっており、これは国内のみならず、世界的な要望でもある。このような背景のもと、セキュリティ適合性評価制度は、適合性評価・ラベル付与等を通じて、IoT製品が適切なセキュリティ対策が取られていることを明示することで、国内だけではなく世

⁷ IPA, ITセキュリティ評価及び認証制度(JISEC) <https://www.ipa.go.jp/security/jisec/index.html>

界的な要望に応えるための制度でもある。この制度に適合した IoT 製品を数多く市場に投入していくことは、重要な国際的貢献のひとつとして位置付けることもできる。

このため、経済産業省は、2022 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⁸(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の内容等について議論を行ってきた。さらに、2022 年度の検討会での議論を踏まえ、2023 年 8 月より「IoT 製品のセキュリティ適合性評価制度における基準等の策定に向けたプレ検討委員会」(以下「プレ委員会」という。)を開催し、構築する適合性評価制度において求めるべきセキュリティ要件案、適合基準案、評価手順案を議論・策定し、これらに基づき実際の製品に対する適合性評価の検証(以下「実証」という。)を行った。検討会及びプレ委員会での議論結果を踏まえて、2024 年 3 月に「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」を公表した。

本方針は、「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」の内容を踏まえ、構築する IoT 製品に対するセキュリティ適合性評価制度(以下「本制度」という。)の方針について示す。

⁸ 経済産業省, ワーキンググループ 3(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)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

2. 構築するセキュリティ適合性評価制度の目的と位置付け

2.1. 制度の必要性及び目的

IoT 製品のセキュリティ確保に向けて、IoT 製品ベンダーにおける課題、IoT 製品調達者・利用者における課題及び国民全体における課題が存在すると考えられることを踏まえ、IoT 製品に対する適合性評価制度を国内で構築し、広く普及させ、そして社会に浸透させる必要がある。そのためには、まずは調達者・利用者が自身を守るために、求めるセキュリティ水準のラベルが付与された製品を優先的に選択するようになることが必要不可欠である。そのような需要が生まれれば、ラベルを取得していない IoT 製品は市場で選ばれにくくなるため、IoT 製品ベンダーは積極的にラベルを取得することとなる。また、IoT 製品ベンダーが、自己でセキュリティ評価を行うための人的負担を下げつつ、評価の信頼性、客観性を高めるために、外部の専門家や専門事業者に評価を委託することも考えられる。

このようなサイクルを生み出すため、①政府機関等、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高く確かな制度利用が見込まれる組織の IoT 製品の調達要件の中にラベルが付与された製品の選定を取り入れること、②業界標準として IoT 製品ベンダーと調達者・利用者が、ラベルが付与された製品の製造・販売と選定・調達する分野を確保することを目指す。これらにより制度が着実に広まる中で、民間の大企業の調達要件での活用、中小企業や消費者への普及を図る。

また、海外製の IoT 製品も広く利用されていることや国内の IoT 製品ベンダーの海外展開を考慮すると、本制度を国内に閉じたものとするのではなく、③諸外国の制度と協調的な制度を構築して相互承認を図る。

以上から、まずは以下の三つの目的を主目的として、それに沿った制度の構築を目指す。

- ① 政府機関や企業等で調達する製品について、共通的な物差しで IoT 製品のセキュリティを評価・可視化できるようにすることで、各組織の求めるセキュリティ水準を満たした IoT 製品の選定・調達を容易にする。
- ② 特定分野のシステムに組み込まれて調達・利用される IoT 製品に求められるセキュリティ要件を定め、必要な認証・ラベルを各業界団体等で指定できるようにすることで、当該特定分野において求められるセキュリティが確保された IoT 製品のみが採用されるようにする。
- ③ 諸外国の制度と協調的な制度を構築し、相互承認を図ることで、IoT 製品を海外に輸出する際に求められる適合性評価にかかる IoT 製品ベンダーの負担を軽減する。

また、将来的には、以下のような IoT 製品のセキュリティを社会全体として確保していくことの実現に本制度が貢献することが望ましい。

- IoT 製品のセキュリティ対策状況を調達者・利用者が価値として認め、IoT 製品ベンダーが対策に要するコストを適切に製品販売価格に反映できるようになる。

- セキュリティに関するスキルや知見に依存することなく、消費者を含む調達者・利用者が、適切な対策が施された IoT 製品を選べるようになる。
- ラベルが付与された製品を調達・利用することで、調達者・利用者としての一定の責務を果たしたと見なされるようになる。
- 調達者・利用者が、セキュリティ機能を備えた IoT 製品を購入するだけでなく、購入後の適切なパスワードの設定、セキュリティアップデートの実施等、自らのセキュリティ対策・管理も必要であることを理解するようになる。

2.2. 制度の位置付け

本制度はまずは任意制度として運用する制度とする。適合性評価を受けた製品に対してセキュリティ要件に応じたラベルを付与することで、製品の付加価値向上に繋げることを意図する。特に、政府機関等で調達する製品については、各組織の求めるセキュリティ水準に合致するラベルが付与された IoT 製品を選定・調達することを推奨し、将来的には義務化も視野に入れることで、IoT 製品ベンダーにラベル取得のインセンティブを与えることが求められる。

既存の関連制度との関係について、諸外国制度や国内既存制度で採用されているスキームや基準と比較検討を行ったうえで、本制度を構築すべきである。また、端末設備等規則を考慮した制度を設計することで、既存の国内法規制との齟齬が生じない制度とする。また、関連する既存の国内任意制度とは、将来的な統合や棲み分け・連携の方針を合意し、IoT 製品ベンダーに制度乱立による混乱や冗長による負担を与えないように考慮する。

2.3. 制度の初期ターゲット

本制度の主目的を踏まえ、自己適合宣言や第三者認証により本制度のラベルが付与された IoT 製品(以下「ラベル付与製品」という。)を調達する主な初期ターゲットを、3.3 節で示す適合性評価レベルに応じて定める。まずは、政府機関等、重要インフラ事業者、地方公共団体等が必要なセキュリティ要件を満たすラベル付与製品の選定を調達要件に含めることを働きかけ、それらの IoT 製品ベンダーに本制度のラベル取得を促していく。また、特定分野のシステムに IoT 製品が使用されており、業界標準として当該 IoT 製品のセキュリティ要件を定め、それを満たしていることを調達者・利用者がラベルという形で確認できるようにしたいという要望がある場合、関連する業界団体やワーキンググループ(WG)と連携し、本制度の活用について検討していく。特に重要インフラ分野のシステムや社会で活用・展開が進んでいるシステムを優先的に検討すべきである。各種調達要件への取り込みについての詳細は 3.8.1 項、特定分野のシステムに関する業界団体・WG との連携についての詳細は 3.8.2 項を参照のこと。

3. 構築するセキュリティ適合性評価制度

3.1. 制度の運用体制

任意制度において知名度のない制度をゼロから普及させるには高いハードルがあるほか、調達者・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等を踏まえ、既存の評価スキームを活用した制度とする。また、本制度に責任を持ち、基本的な規則を維持管理するスキームオーナーには、政府機関等が調達時に行う製品セキュリティ評価の代替として活用することや諸外国の制度との相互承認を今後調整していくことから、政府のガバナンスが効くことが重要となる。こうした点を踏まえ、経済産業省の示す本方針に従い制度を構築し、同省の監督のもと制度を運営するスキームオーナーは、同省が所管官庁である独立行政法人情報処理推進機構 (IPA) とする。IPA は、現在運営している JISEC 制度を、CC 認証のみの対象から本制度を含む形に拡張させる枠組み (セキュリティ製品認証・ラベリング制度) として、本制度を構築、運営する。

運用体制案を図 3.1-1 に示す。IPA の理事長の配下に運営審議委員会と本制度の技術審議委員会を設置する。運営審議委員会は、既存の JISEC 制度の運営審議委員会を拡張する形で設置し、CC 認証及び本制度の業務運営方針・マネジメントに関する事項等を審議する。本制度の技術審議委員会は、プレ委員会を引き継ぐ形で新設し、本制度についての適合基準の承認・技術的事項等を審議する。また、製品類型ごとの適合基準案の策定は、本制度の技術審議委員会の配下に設置する適合基準検討 WG にて行う。☆2 以上の適合基準検討 WG は、当該製品タイプの IoT 製品ベンダーや主な調達組織、それらの関連機関・団体を中心に構成され、策定した適合基準案を本制度の技術審議委員会に付議する想定である。加えて、IPA と経済産業省による本制度の運営事務局を設置し、制度拡張、国内既存制度との統合・連携、相互承認等の海外連携の調整、政府調達要件等への働きかけ、民間企業・消費者への制度普及促進、IoT 製品ベンダーへの認証取得促進等について推進する。

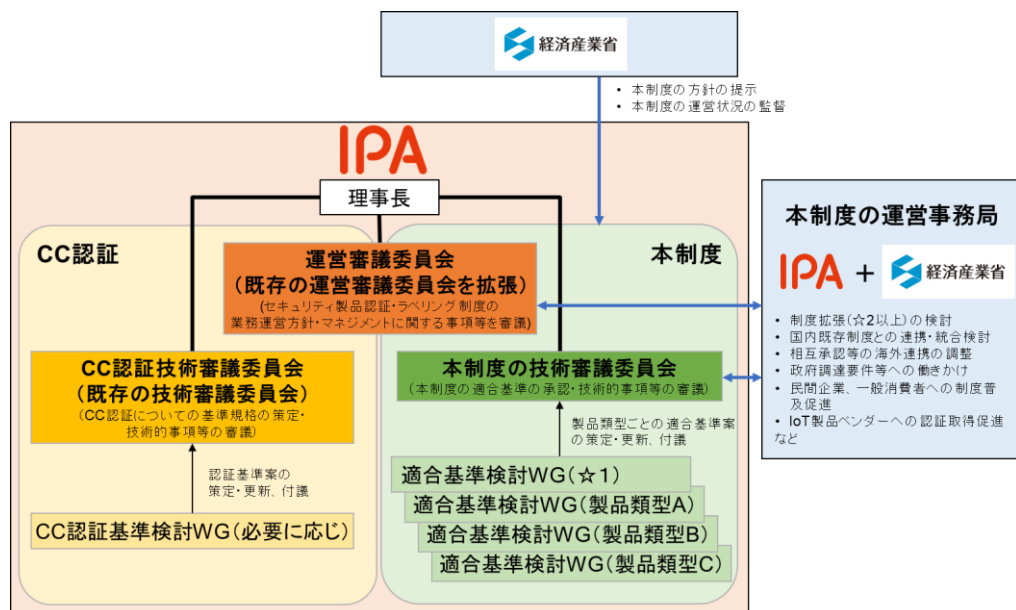


図 3.1-1 セキュリティ製品認証・ラベリング制度の運用体制案

3.2. 制度の対象とする製品範囲

消費者向けの IoT 機器を対象にした ETSI EN 303 645 の定義では、IoT 製品 (IoT product) とは、IoT 機器 (IoT device) とその付随サービスを含むものである。IoT 機器とは、ネットワークに接続された (及びネットワークに接続可能な) 機器で、付随サービスとの関係を持ち、電子機器として使用される機器のことである。付随サービスとは、IoT 機器と共に IoT 製品全体の一部であり、通常は製品の意図された機能を提供するために必要なデジタルサービスのことである。

本制度では国内外の規格や制度の定義を参照し、インターネットプロトコル (IP) を使用したデータの送受信機能を持つ以下の機器を対象に含める。そのイメージを図 3.2-1 に示す。

- インターネットに接続可能な機器: IP を使用してインターネット上でデータを送受信する機能を持つ機器
- ネットワークに接続可能な機器: 他の「インターネットに接続可能な製品」や「ネットワークに接続可能な製品」に接続し、IP を使用してデータを送受信する機能を持つ機器

これらの IoT 機器にその付随サービスを含めた IoT 製品を本制度の対象範囲とする。

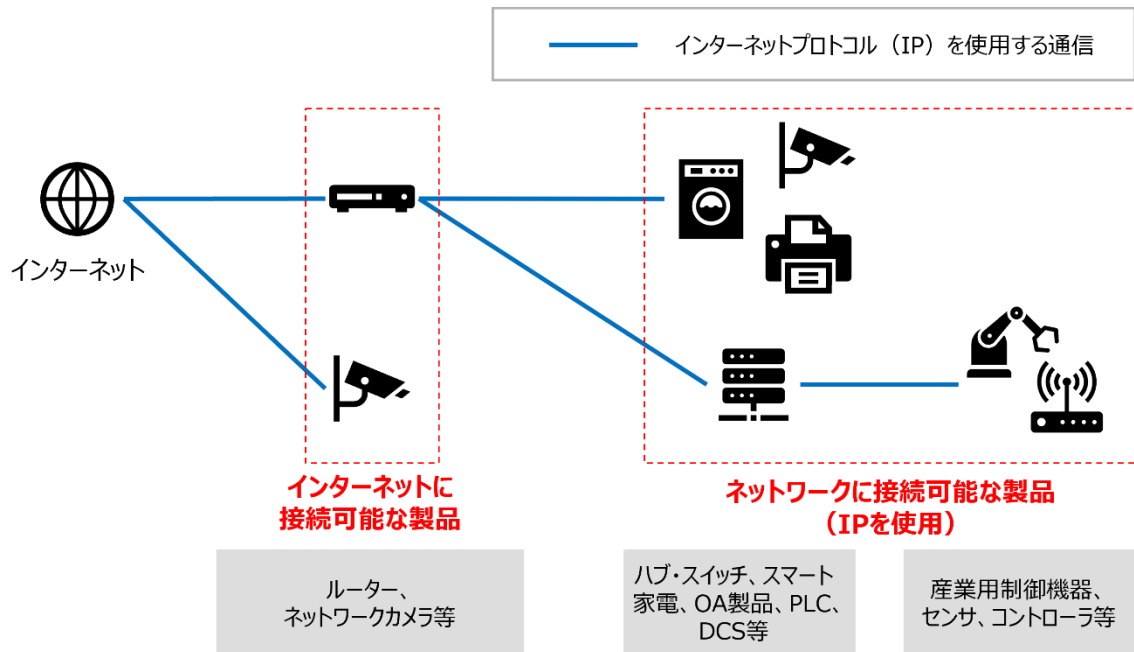


図 3.2-1 本制度の対象とする製品のイメージ

また、国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的な IT 製品 (パソコン、タブレット端末、スマートフォン等) は対象外とする。なお、汎用 OS を搭載した IoT 製品については、利用者が製品本体に対して、容易にセキュリティ対策を追加できない場合は、対象製品とみなす。

3.3. 制度における適合性評価レベル

製品類型ごとの特性に応じて、求められるセキュリティ要件、適合基準、評価手順や評価方式を設定する制度とする。各適合性評価レベルの位置付けを表 3.3-1 に示す。☆1 では、IoT 製品共通の最低限の脅威に対応することを想定し製品類型共通のセキュリティ要件、適合基準、評価手順を整理する。☆2 以上では、製品類型ごとの特徴を考慮して、セキュリティ要件、適合基準、評価手順を整理する。また、3.5 節でも示しているとおり、☆1、☆2 では IoT 製品ベンダーによる自己適合宣言を認める一方、☆3 以上では第三者認証とする。適合性評価レベルのイメージを図 3.3-1 に示す。

表 3.3-1 各適合性評価レベルの位置付け

レベル	位置付け
☆3 以上	政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定した IoT 製品類型ごとの汎用的な適合基準を定め、それを満たすことを独立した第三者が評価し認証するもの
☆2	IoT 製品類型ごとの特徴を考慮し、☆1 に追加すべき基本的な適合基準を定め、それを満たすことを IoT 製品ベンダーが自ら宣言するもの
☆1	IoT 製品として共通して求められる最低限の適合基準を定め、それを満たすことを IoT 製品ベンダーが自ら宣言するもの

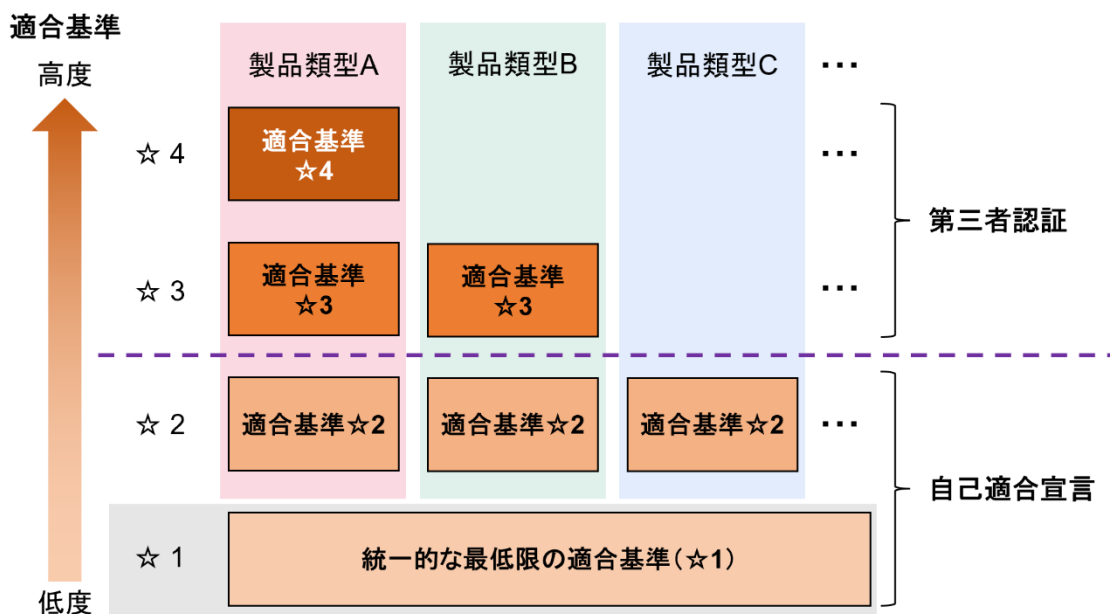


図 3.3-1 適合性評価レベルのイメージ図

3.4. 制度で用いるセキュリティ要件・適合基準・評価手順

本制度で対象とする IoT 製品に求められ得る「セキュリティ要件」、各適合性評価レベルで対象製品が適合すべき基準を示した「適合基準」、当該適合基準に適合しているかを評価するための手順を示した「評価手順」について、それぞれの関係性を図 3.4-1 に示す。

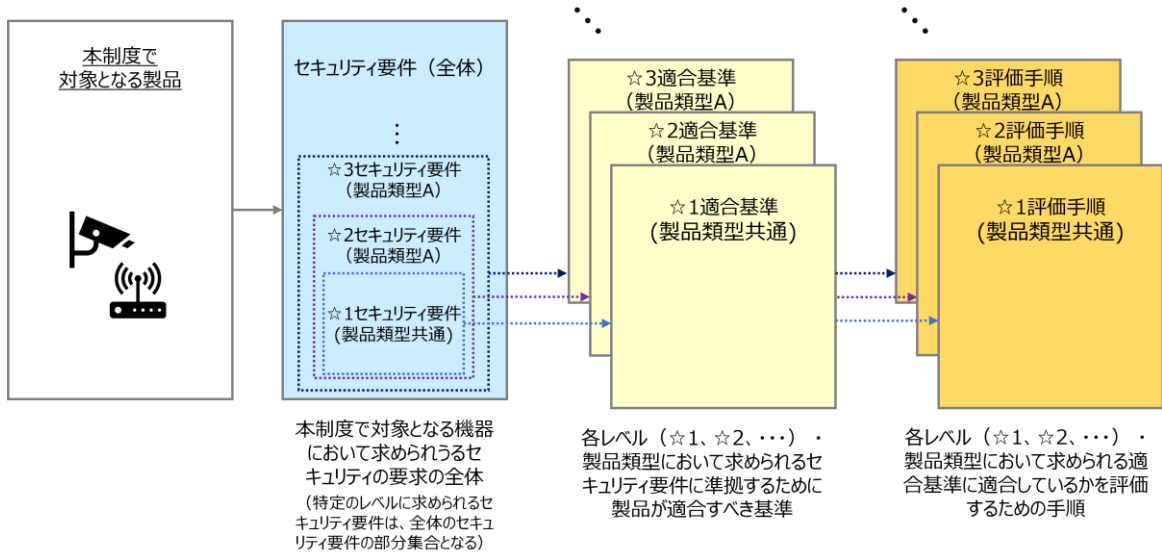


図 3.4-1 セキュリティ要件・適合基準・評価手順の関係性

2023 年度の検討会及びプレ委員会では、セキュリティ要件の全体のほか、本制度の最低レベルである☆1 のセキュリティ要件、適合基準、評価手順を中心に議論を行った。プレ委員会においてそれぞれの案について議論を行った後、当該案を用いた実証を行った。そして、実証で得られた改善点や修正点を踏まえて修正したセキュリティ要件、適合基準、評価手順について再度プレ委員会で議論を行った。

セキュリティ要件は、本制度で対象となる製品において求められ得るセキュリティの要求事項の全体であり、各適合性評価レベルに求められるセキュリティ要件は、全体のセキュリティ要件の一部となる。2022 年度の検討会の議論を踏まえ、本制度で用いるセキュリティ要件については、国際的な要件と整合的な形で構築する。この方針に従い、まず図 3.4-2 に示すとおり、ETSI EN 303 645、NISTIR 8425、EU-CRA、端末設備等規則等の国内外のセキュリティ要件の集合関係を踏まえ、重ね合わせの関係にあるセキュリティ要件の全体リストを整理した。

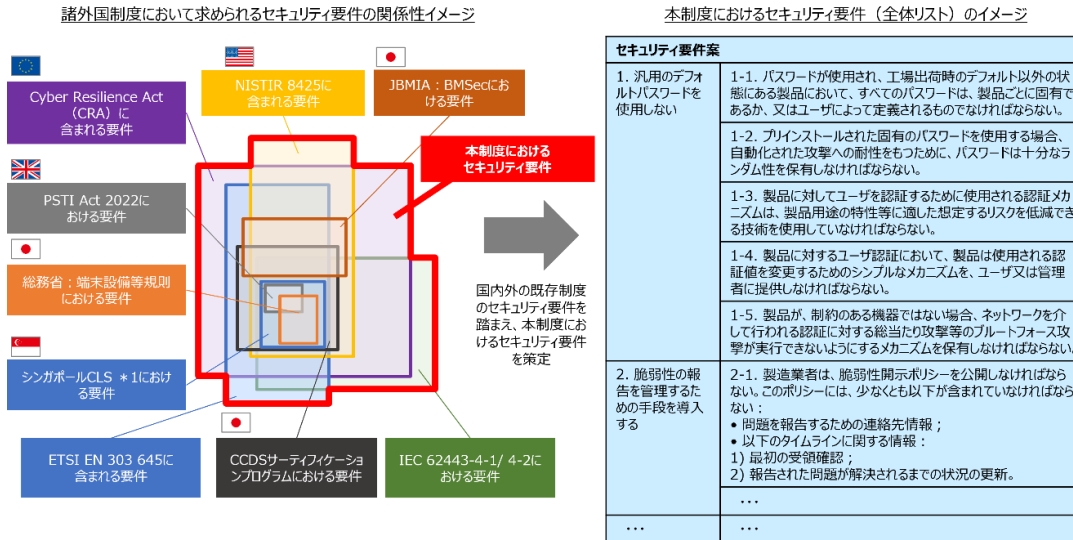


図 3.4-2 セキュリティ要件の整理方針

セキュリティ要件の全体のうち、☆1 で設定するセキュリティ要件に関して、本制度における☆1 の位置付け、☆1 で主に想定する守るべき資産、対象製品におけるアタックサーフェスを踏まえ、☆1 で考慮すべき想定脅威をまず整理した。そのうえで、この想定脅威に対して実現すべき対策を整理し、当該対策を実現するためのセキュリティ要件を全体のリストから抽出する形で、☆1 のセキュリティ要件を設定した。☆1 で考慮する主な脅威として、以下の脅威を整理した。

- ①弱い認証機能、②脆弱性の放置、③未使用インタフェースの有効化により、外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威
- 機器の通信が盗聴され、守るべき情報が漏えいする脅威
- 廃棄・転売等された機器から、守るべき情報が漏えいする脅威
- ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威

また、☆1 で守るべき情報に関して、以下の情報を整理した。

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- 機器の意図する使用⁹において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報¹⁰

⁹ 製品もしくはシステムとともに提供される情報に従った使用、又はそのような情報がない場合には、一般的に理解されている方法による使用のこと。(JIS Z 8051:2015)

¹⁰ 例えば、個人情報に関する意図する使用はないが、その機器によって扱われるデータに個人情報が含まれる機器の場合、想定される運用環境において盗聴の脅威に関して許容不可能なリスクがある場合に限り、

☆1 の適合基準について、将来的な制度の国際連携を見据え、国際的に広く活用されている ETSI EN 303 645 の基準をベースとしつつ、シンガポールの Cybersecurity Labelling Scheme (CLS)、CCDS サーフティフィケーションプログラム等の国内外の既存制度の基準を参照して整理した。

☆1 の評価手順について、シンガポール CLS、CCDS サーフティフィケーションプログラム等の国内外の既存制度の評価手順を参照し、「ドキュメント評価」又は「実機テスト」を評価手法として設定し、具体的な評価ガイドを策定した。なお、☆1 では、IoT 製品ベンダーによる自己適合宣言を許容し、可能な限り低コストでの評価を目標とするため、評価工数が小さいと想定される「ドキュメント評価」を中心とした。

整理した適合基準及び評価手順の内容について検討会及びプレ委員会にて議論を行うとともに、実証において、当該基準及び手順に基づく評価工数を計測した。実証では、10 製品に対して、IoT 製品ベンダーによる自己評価及び評価機関による第三者評価の両方を実施するとともに、一部の製品については、検証事業者による第三者評価を行った(評価主体の定義は 3.5 節参照)。実証の結果、評価に要した工数は平均して 23.9 人時間であり、自己評価と第三者評価とで大きな差異は無かった。特に多くの工数を要した評価項目は実機に対するポートスキャン及び脆弱性診断に関する評価項目であったが、これはツール環境構築に多くの工数を要したことに起因しており、2 回目以降の評価は短時間で実施できる見込みであることを確認した。

実証では、複数の製品における評価項目において、自己評価と第三者評価とで評価結果に差異が生じた。差異の理由は、適合基準や評価手順等が曖昧であったこと、第三者においてドキュメント評価用の文書を受領できなかったことの主に 2 点であった。前者について、実証で得られた結果を踏まえ、可能な限り結果の一意性が保証されるよう適合基準、評価手順等の見直しを行った。後者について、ドキュメント評価用の文書の取扱いについて整理した。

策定・修正した☆1 におけるセキュリティ要件及び適合基準は別添に示すとおりである。また☆1 の適合基準に対する評価手順や評価ガイド等についても、検討会及びプレ委員会での議論並びに実証の結果を踏まえて作成した。今年度プレ委員会策定した☆1 のセキュリティ要件、適合基準、評価手順等については、2024 年度に本制度の技術審議委員会に付議して最終確定する。また、☆2 以上のセキュリティ要件、適合基準、評価手順等については、2024 年度以降、本制度の技術審議委員会及びその配下に設置する適合基準検討 WG で議論を行う予定である。

☆1 評価のハードルを可能な限り下げるため、実機テストに必要なツール環境構築に関する内容を含むサポート文書(FAQ)等を作成し、提供する。また、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が日々変化することを踏まえ、本制度開始以降も、セキュリティ要件、適合基準、評価手順等を定期的に見直す。

3.5 節で示すとおり、☆1 では、IoT 製品ベンダー自身による自己適合宣言を認め、IoT 製品ベンダー自身による自己評価結果を踏まえて記載したチェックリストに基づきラベル申請を行う。IoT 製品

対象データを守るべき情報として扱う。具体例としては、防犯カメラが収集する特定の個人が識別可能な映像(個人情報)等が該当するが、ルータに伝送される個人情報は「意図された機器の使用において、機器が収集」することに該当しないため、対象外となる。

ベンダー自身で自己評価を行い、ラベルを申請する場合、ラベルの申請段階においては、必ずしも他者にドキュメント評価用の文書を提供する必要はない。また、IoT 製品ベンダー自身での自己評価が困難な場合、評価機関等の第三者に評価を依頼し、第三者の評価結果を基にラベル申請を行うことも可能である。ただし、この場合、当該の第三者に対してドキュメント評価用の文書を提供する必要がある。加えて、3.7 節で示すとおり、ラベル取得後に申請内容に疑義が生じた場合に、IPA が疑義に関連して評価に使用した証拠の提出を求める可能性がある。

3.5. 制度における適合性評価の主体

適合性評価において、レビュー及び証明を行う主体が第一者の場合は自己適合宣言、第三者の場合は第三者認証と呼ばれる。各評価活動の定義について、表 3.5-1 に示す。

表 3.5-1 各評価活動に関する用語の説明

用語	説明 (ISO/IEC 17000 の記載等をもとに整理)
第一者	適合性評価の対象を提供する人又は組織のこと。
第三者	適合性評価の対象を提供する人又は組織、及びその対象について使用者側の利害をもつ人又は組織の双方から独立した、人又は機関のこと。
確定活動	適合性を判断するために必要な全ての情報を取得する活動、いわば事実を確認する活動のこと。
レビュー	適合性評価の対象が、規定要求事項を満たしていることに関する選択活動(確定活動の準備を整える活動)及び確定活動、並びにこれらの活動の結果の適切性、十分さ及び有効性の検証を行うこと。
証明	レビューに従った決定に基づいて、規定要求事項の充足が実証されたという表明を発行すること。

本制度を広く普及させるうえでも、☆1、☆2 では自己適合宣言を認める。☆1、☆2 では、IoT 製品ベンダー自身による自己評価を行い、評価結果を記載したチェックリストに基づきラベル申請を行う。申請を受けた IPA は、チェックリストの形式確認を行った上でラベルを付与する。なお、評価を有資格者や検証事業者、評価機関等に委託してもよい。

☆3 以上は政府機関等や重要インフラ事業者をはじめとした、高い信頼性が求められる機能やサービスを提供する組織や事業者での活用を想定しており、独立した第三者である評価機関によって評価を行い、IPA が認証機関となり、認証を行う。

IPA は、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスク¹¹ について経済産業省を含めた政府関係機関に照会をかけ、その照会結果¹² に基づきラベルを付与する。

各適合性評価レベルにおける適合性評価の流れを図 3.5-1 及び図 3.5-2 に示す。また、各適合性評価レベルにおける各主体の主な責務は表 3.5-2 のとおりとする。有資格者の詳細は 3.7 節を、検証事業者及び評価機関の詳細は 4.3 節を参照のこと。

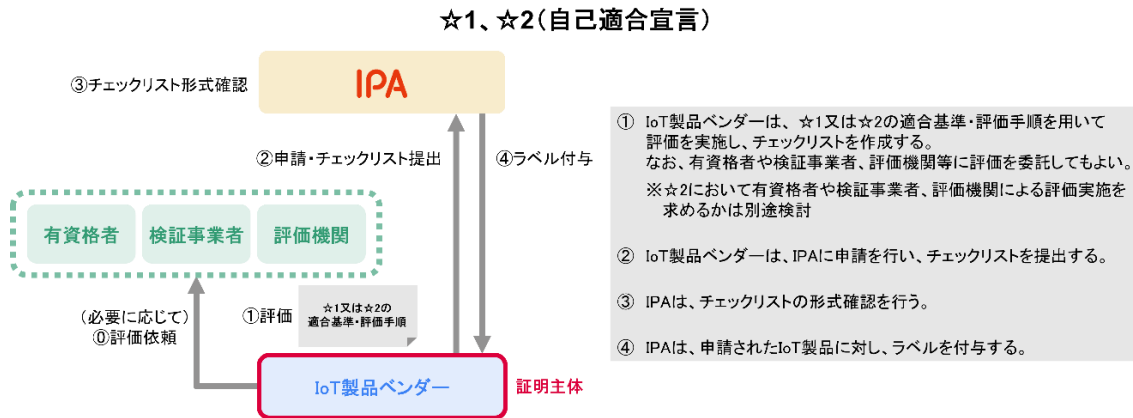


図 3.5-1 ☆1、☆2 における適合性評価の流れ

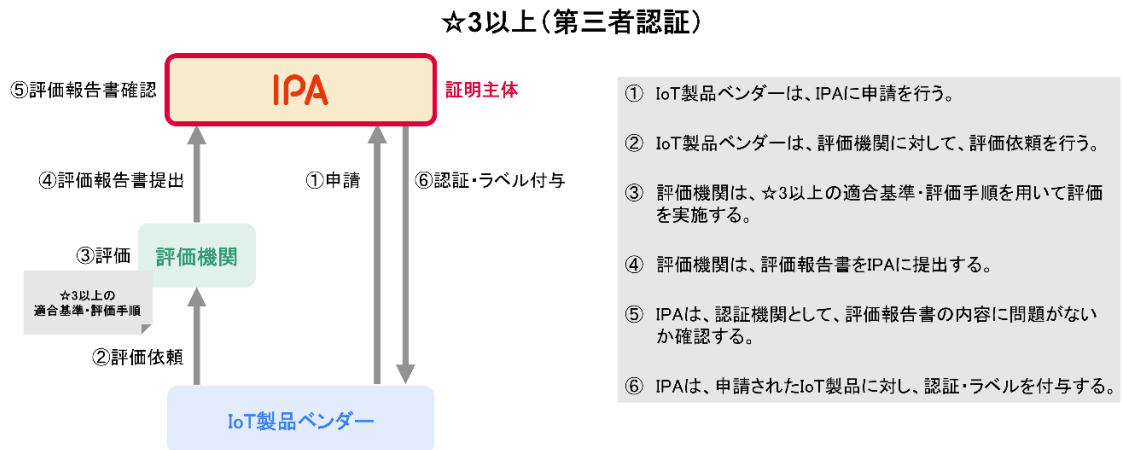


図 3.5-2 ☆3 以上における適合性評価の流れ

¹¹ サイバー空間を構成するシステムのサプライチェーンの複雑化やグローバル化を通じ、サプライチェーンの過程で製品に不正機能等が埋め込まれるリスクや政治経済情勢による機器・サービスの供給途絶など、サイバー空間自体の信頼性や供給安定性に係るリスク(サプライチェーン・リスク)

サイバーセキュリティ戦略(令和3年9月28日閣議決定)
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf>

¹² 政府関係機関は、以下のような観点でサプライチェーン・リスクの懸念の有無を判断する。

- 申請するIoT製品のIoT製品ベンダーは、過去の実績を含め、我が国の法令や国際的に受け入れられた基準等に遵守しているか。
- IoT製品ベンダーは、申請するIoT製品のサイバーセキュリティ確保について外国の法的環境等により影響を受けるものではないか。

表 3.5-2 各適合性評価レベルにおける各主体の主な責務

	IoT 製品ベンダー	評価機関	IPA
☆1、☆2 (自己適合宣言)	<ul style="list-style-type: none"> 適切に評価を行い、チェックリストに記載した内容について責任を持ち、調達者・利用者から求められれば、それについて説明する責任を持つこと 付与されたラベルを適切に利用すること 評価の証跡を、ラベル有効期間中、適切に保管し、評価の適切な実施をスキームオーナーに対して説明できるように情報開示を行うこと ラベル有効期限内は、申請内容や製品仕様の変更の有無を管理し、変更があった場合、定められた適切な対処を行うこと 	- (評価機関や検証事業者の利用は任意)	<ul style="list-style-type: none"> チェックリストの形式を適切に確認したうえで、ラベルを付与すること ラベル付与製品に関する情報を調達者・利用者に対して公開すること ラベルが適切に利用されるよう管理をすること ラベルの不適切な利用を認識した場合、適切な対処を行うこと
☆3 以上 (第三者認証)	<ul style="list-style-type: none"> 付与されたラベルを適切に利用すること ラベル有効期限内は、申請内容や製品仕様の変更の有無を管理し、変更があった場合、定められた適切な対処を行うこと 	<ul style="list-style-type: none"> 適切に評価を行うこと 	<ul style="list-style-type: none"> 評価報告書の内容を適切に確認したうえで、認証及びラベル付与を行うこと ラベル付与製品に関する情報を調達者・利用者に対して公開すること ラベルが適切に利用されるよう管理をすること ラベルの不適切な利用を認識した場合、適切な対処を行うこと

3.6. ラベルの意味合い

各適合性評価レベルにおける各主体の責務を踏まえ、IoT 製品に付与されるラベルの意味合いは表 3.6-1 のとおりとなる。本ラベルは、あくまで定められた適合基準への適合を示すものであり、ラベルが付与されているからといって、IoT 製品のセキュリティが完全に確保されていることを保証するものではない。各種法令(消費者契約法等)との関係については、今後整理・検討を行う。

表 3.6-1 各適合性評価レベルにおけるラベルの意味合い

適合性評価レベル	ラベルの意味合い
<p>☆1、☆2 (自己適合宣言)</p>	<p>ラベル取得(継続更新時の再取得を含む)時点において定められた適合基準へ適合していることについて、IoT 製品ベンダー自らが宣言したことを示すもの。(証明主体はIoT 製品ベンダー自身) IPA はラベル付与機関として評価結果を記載したチェックリストの形式確認は行うが、IoT 製品のセキュリティ適合性等を、IPA が認証するものではない。</p>
<p>☆3 以上 (第三者認証)</p>	<p>ラベル取得時点(再評価時を含む)において定められた適合基準へ適合していることについて、認証機関となる IPA が認証したことを示すもの。(証明主体は IPA) IPA は、独立した第三者である評価機関が本制度の定める適合基準及び評価手順に従い評価した結果を確認したうえで、当該基準への適合に対する認証を行う。ただし、IPA は、評価機関による評価の結果を適切に確認する責任を負う一方、ラベルを取得した当該 IoT 製品に対して、明示あるいは黙示を問わず、いかなる保証も行わない。</p>

3.7. ラベルの信頼性確保のための仕組み

本制度は任意制度であるため、ラベルの表示義務は設けず、IoT 製品ベンダーがラベル取得済みであることを訴求するために、製品本体、パッケージ、マニュアル、パンフレット、Web サイト等に、本制度のロゴ等を任意に掲載できるようにする。

ラベル付与製品に対して、本制度の概要、製品情報、ラベル情報、適合評価結果、安全情報等の多岐に渡る情報を最新に維持しながら調達者・利用者に提供するため、本制度の Web サイトにラベル付与製品毎の情報提供ページを設け、当該ページの URL を埋め込んだ QR コードを本制度のロゴと合わせて掲示することとする。情報提供ページは日本語での表記とし、その掲載情報案を表 3.7-1 に示す。ラベル情報の中には、評価者区分を含め、評価能力のある者が評価を行ったかについて調達者・利用者が識別できるようにする。評価者区分としては、IoT 製品ベンダー、IoT 製品ベンダー(有資格者)、外部有資格者、検証事業者、評価機関を想定している。有資格者が評価したと掲載するための条件として、指定資格の保有者(情報処理安全確保支援士等)が、IoT セキュリティ評価に関する研修受講完了又は評価ガイドを理解していることを宣誓したうえで、評価又は評価結果の確認を実施することを求める。指定資格を情報処理安全確保支援士に限定するか、同等の他資格も許容するか、必要な研修制度の整備等は今後、本制度の技術審議委員会で検討する。検証事業者、評価機関の説明は、4.3 節を参照のこと。

ラベルを掲示している製品に対しては、IoT 製品ベンダーの対応負荷を考慮すると、ラベル失効後(再申請予定がない場合の有効期限以降)に出荷予定の製品へのラベル掲載は禁止とするものの、既に製造が完了している製品や製造仕掛中の製品へのラベル掲載の取り消しは求めず、リンク先の情報提供ページのステータスを「ラベル失効済み」等にすることで対応する。

表 3.7-1 情報提供ページの掲載情報案

掲載情報	掲載内容
本制度の概要	<ul style="list-style-type: none"> 本制度の概要及び詳細説明 HP の URL
製品情報	<ul style="list-style-type: none"> 製品名 型式番号 IoT 製品の製造業者名 ※公開/非公開は任意 製造国又は地域 ※公開/非公開は任意 製品概要 製品 Web サイトの URL 製品の問い合わせ先 他認証の認証番号等
ラベル情報	<ul style="list-style-type: none"> ラベル識別番号 当該製品の適合性評価レベル(☆1～☆4) 当該製品の製品類型の名称 ※☆2～☆4 の場合 評価された適合基準のバージョン 適合評価結果(チェックリスト又は評価報告書等) ラベルステータス情報 ラベル発行・更新日 ラベルの有効期限 ラベルの申請者名 (IoT 製品ベンダー) 評価者区分
安全情報	<ul style="list-style-type: none"> 当該製品に関わる脆弱性情報 脆弱性の報告窓口の URL
その他セキュリティ関連情報	<ul style="list-style-type: none"> 必要があれば、IoT 製品ベンダーから調達者・利用者に向けたセキュリティ関連情報

☆1、☆2 の有効期限はラベル取得日から最大 2 年間(申請すれば 2 年以内の有効期限も設定可能とする)とし、有効期限を延長したい場合は改めて自己適合宣言を行うこととする。有効期限内に適合基準のメジャーな改訂(適合基準の項目追加や大幅な変更等)があり、その猶予期間(旧版と並存させる移行期間)が終了したとしても、途中でラベルを失効とはしないこととする。ただし、有効期限内に評価に影響を及ぼすレベルでの製品のセキュリティ仕様等の変更があった場合は、IoT 製品ベンダー自身で確認を行ったうえでスキームオーナーに報告し、その時点でラベルは失効とする。

☆3 以上の有効期限については、セキュリティトレンドへの対応や、製品のライフタイム、評価に要するコストや調達者・利用者におけるわかりやすさ等を考慮して、2024 年度以降も引き続き検討を行っていく。

スキームオーナーは、ラベル付与製品が流通した際に、不適合の状態でないかを確認し、その信頼性を担保するため、ラベル付与製品に対して検査やサーベイランスを行える権利を有することとし、

ラベルを取得した IoT 製品ベンダーはそれに協力することとする。ただし、制度開始当初の☆1 に関しては、コストの観点から、サンプリング等による定期的なサーベイランスは行わないこととし、調達者・利用者からの指摘やスキームオーナーの判断により、基準への適合に疑義が生じた場合に、IoT 製品ベンダーに対して評価に使用した証跡の提出を求めるとや検査・サーベイランスを実施することとする。証跡の提出に当たっては、必要に応じて秘密保持契約 (NDA) を IoT 製品ベンダーとスキームオーナー間で締結するほか、NDA 締結の有無によらず証跡の開示が困難な場合には、IoT 製品ベンダーが説明文書を用意し、疑義に対する説明を行うことを認める。また、本制度の信頼性確保のため、付与したラベルを取り消す仕組みを設ける。具体的には、以下のような状況が発覚した場合、付与したラベルの取り消しを行う。

- 申請内容が虚偽であることが発覚した場合
- IoT 製品ベンダー等が定められている義務を履行しない場合
- 製品が適合基準を満たさなくなった場合
- サーベイランスで不適合であることが発覚し、猶予期間中に適切な是正措置が行われなかった場合

悪質であった場合、又は調達者・利用者に与える影響が大きい場合には、スキームオーナーがその旨を一般に周知する。

3.8. 関連機関や国内外の関連制度等との連携の仕組み

2.1 節の三つの主目的を達成するため、関連機関や国内外の関連制度との連携を図る。

3.8.1. 各組織の調達要件への反映に関する働きかけ

IoT 製品の選定・調達において、本制度をベースとして活用しながら、必要に応じて追加的な確認を実施することで、各組織の求めるセキュリティ水準の IoT 製品を選定・調達できるようになることを目指す。

政府機関等については、強制力を持たせるため、本制度との連携の必要性及び「政府機関等のサイバーセキュリティ対策のための統一基準群¹³」に盛り込むことを内閣サイバーセキュリティセンター (NISC) との間で合意している。具体的には、情報システムの重要度に応じて「重要度:低」は☆1 以上、「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ことの追加を検討する。なお、ラベル付与製品が普及する時期をめぐり、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針で合意している。また、政府機関等の調達において☆3 以上の活用が想定される製品類型として、ネットワークカメラ、ドローン、ファイアウォール、ル

¹³ NISC, 政府機関等のサイバーセキュリティ対策のための統一基準群
<https://www.nisc.go.jp/policy/group/general/kijun.html>

ータ(有線・無線)等の優先度が高いことを確認している。統一基準群への盛り込みや☆3 以上の整備優先度の高い製品類型の特定に加え、今後、各府省庁の参加する会議の場等で、本制度を活用した製品調達に関する周知を行っていくことも重要となる。

重要インフラ事業者については、NISC と「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針及び手引書¹⁴に本制度の活用に関する記載を追加する方針で合意している。また、各重要インフラ事業者の調達ルールへの反映や重要インフラ分野の特定システムにおける☆2 以上の制度活用の要望について、セプターカウンシル¹⁵の運営委員会を活用しながら取り組むことを合意している。

地方公共団体については、総務省と調整の上、政府統一基準群が改定された後、地方公共団体の状況に合わせて、「地方公共団体における情報セキュリティポリシーに関するガイドライン¹⁶」への記載追加を検討している。

本制度の運営事務局とNISC 及び総務省等で協力・連携し、これらの取り組みを進める。その他の民間企業の調達要件に対して直接的にアプローチすることは難しいため、各業界団体や各業種のISAC 等と連携して取組を促す方針で、本制度の運営事務局が働きかけを行っていく。

また、政府機関等、重要インフラ事業者、地方公共団体等の調達要件の中にラベル付与製品の選定を取り入れたとしても、実際に調達する際にラベル付与製品が広く普及していないと、セキュリティ面以外の比較ができず、選定時の選択肢が限定されてしまう。そのため、これらの組織で主に調達されるIoT 製品を中心に、その関連団体に対して、本制度との連携や会員企業への積極的なラベル取得の働きかけを行うことの賛同を得ることが必要である。現時点で、賛同が得られている団体を「別紙 IoT 製品ベンダー関連の賛同団体一覧」に示す。

3.8.2. 特定分野のシステムに関する業界団体・WG との連携

IoT 製品は、単体で比較・検討されて調達されるだけではなく、特定分野のシステムに組み込まれて調達され、利用されるケースもある。セキュリティ知識が不足している中小企業や消費者が、意識しないままセキュリティ対策が十分でないIoT 製品を利用することでサイバーセキュリティリスクに晒されているという課題を踏まえ、そのような調達者・利用者が多いと考えられる分野のシステムについて、優先的に検討を行う必要がある。また、重要インフラ分野のシステムについても、インシデント発生時の社会的な影響を考慮して優先的に検討を行う。具体的には、スマートホームシステム、ビルシステム、工場システム、電力システム等が候補となり得る。

¹⁴ NISC, 重要インフラのサイバーセキュリティの確保に関する主な資料

<https://www.nisc.go.jp/policy/group/infra/siryou/index.html>

¹⁵ NISC, セプターカウンシル総会資料(セプターカウンシルの概要)

<https://www.nisc.go.jp/policy/group/infra/siryou/#si09>

¹⁶ 総務省, 地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会

https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

本制度の運営事務局において、このような検討優先度の高い「特定分野のシステム」について、各システム全体のセキュリティを検討している業界団体やワーキンググループと連携して、各システムに組み込まれる IoT 製品に求めるセキュリティ要件や☆2 以上の適合基準をその必要性も含めて検討する。各システムにおいて、IoT 製品を選定する立場の事業者又は当該 IoT 製品を製造する事業者から、ラベル付与製品の製造・販売と選定・調達について一定割合以上の賛同が得られる場合（業界標準となり得ると判断される場合）、本制度として当該 IoT 製品に対する☆2 以降の整備を進める。各特定分野のシステム全体のセキュリティガイドラインの作成や、システム全体の認証制度等の整備は、各業界団体やワーキンググループで検討し、本制度の運営事務局はオブザーバーの立場で連携する方針とする。

3.8.3. 諸外国制度との連携

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、海外で IoT 製品を販売している国内の IoT 製品ベンダーは、諸外国制度のラベルの取得のための負担が増えることが想定される。本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。諸外国制度の動向(表 3.8-1)を踏まえつつ、国際連携のあり方を検討する。

表 3.8-1 諸外国制度の動向

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act (PSTI 法)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA) ※欧州委員会草案の内容
開始時期	2020 年 10 月制度開始	2024 年 4 月施行	2024 年中に開始予定	未定(報告義務を除き 2027 年開始想定)
任意/義務	任意	義務	任意	義務
対象	消費者向け IoT 機器	消費者向け IoT 製品	消費者用無線 IoT 製品	デジタル製品

適合基準	<ul style="list-style-type: none"> • *: ETSI EN 303 645 の基準の一部¹⁷ • **: *の基準に加え、ETSI EN 303 645 の基準の一部¹⁸ • ***及び****: **の基準に加え、IMDA「IoT Cyber Security Guide」の9つのライフサイクル基準 	ETSI EN 303 645 の基準の一部 (5.1-1、5.1-2、5.2-1、5.3-13)	NISTIR 8425 をベースとした基準となる見込み	<ul style="list-style-type: none"> • 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定 • 2024 年後半に発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定
評価方式	<ul style="list-style-type: none"> • *及び**: 自己適合宣言 • ***及び****: 自己適合宣言及び評価機関による試験 	自己適合宣言	第三者認証	<ul style="list-style-type: none"> • 「重要なデジタル製品」以外の製品: 自己適合宣言 • 「重要なデジタル製品」のクラス I (リスクが低い製品) で EUCC や EN 規格の対象外の製品及びクラス II (リスクが高い製品) の製品: 第三者認証

☆1 の制度開始時に既に制度が開始されているシンガポールの Cybersecurity Labelling Scheme (CLS) 及び英国の Product Security and Telecommunication Infrastructure Act (PSTI 法) を内包することも考慮し、3.4 節のとおり、☆1 の適合基準の策定を行った。☆1 の制度開始時には制度設計途中の見込みである EU の Cyber Resilience Act (CRA) 及び米国の U.S. Cyber Trust Mark について

¹⁷ ETSI EN 303 645 のサイバーセキュリティ規定 5.1-1、5.1-2、5.1-3、5.1-4、5.1-5、5.2-1、5.3-2、5.3-3、5.3-7、5.3-8、5.3-10、5.3-13、5.3-16

¹⁸ ETSI EN 303 645 のサイバーセキュリティ規定 5.4-1、5.4-2、5.4-3、5.4-4、5.5-5、5.5-7、5.5-8、5.6-1、5.6-2、5.6-4、5.8-2、5.8-3、5.11-1、5.13-1 及びデータ保護規定 6.1、6.2、6.3、6.5

は、適合基準間の差分を確認し、☆1 の適合基準のメジャーな改訂又は☆2 以上の基準の策定の際に国内基準で包含又は追加対応を要する差分の公表等に対応することで、相互承認の調整を図っていく。また、☆1 開始の正式案内時に制度が既に導入されているシンガポールと英国については、正式案内時に相互承認の方向性を提示し、正式案内時に制度設計途中の見込みである欧米については、順次方向性を公表する。加えて、国際標準化に向けて検討が進んでいる ISO/IEC 27404 等とも連携を図っていく必要がある。

4. 制度の発展に向けた施策

4.1. IoT 製品ベンダーに対するラベル取得促進策

適合性評価を受けるに当たり、IoT 製品ベンダーには様々なコストが発生する。また、適合性評価を受けるために必要なナレッジが足りていない IoT 製品ベンダーも多く存在すると思われる。制度普及を後押しする観点から、コスト抑制やナレッジ提供のための支援策について検討が必要である。

特に☆1は、幅広い IoT 製品ベンダーによるラベル取得を想定しているため、ラベル取得にかかる費用やコストは、大企業だけでなく中小企業でも対応できるような形にする。IoT 製品ベンダーに対する制度に関する説明や、自己適合宣言時に参考となるドキュメント(ベストプラクティス、評価ガイド等)の提供といった施策の実施について、本制度の運営事務局において検討する。将来的には、自己評価を行う際に活用できる自動化ツールの提供も検討する。また、各種補助金制度との連携や申請費用・第三者評価費用の割引キャンペーンの実施について、本制度の運営事務局において検討し、IoT 製品ベンダーの負担の軽減を目指す。加えて、海外の IoT 製品ベンダーへの本制度の普及についても、検討を行っていく。

4.2. 調達者・利用者に対する制度普及促進策

ラベル付与製品が積極的に購入されるようになることが、IoT 製品ベンダーにとってラベル取得の最も大きなインセンティブになる。また、IoT 製品が踏み台攻撃に利用されることも想定されるため、サイバー公衆衛生の観点からも、調達者・利用者に対して、IoT 製品のセキュリティリスク、ラベルの意味、ラベル付与製品を選択・購入するメリット、購入後に利用者が実施すべきセキュリティ対策等の啓発を実施することは重要である。調達者・利用者に対する制度の普及促進策について、その効果や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が必要である。

調達者・利用者に対して、本制度の概要を伝えるのみならず、本制度がどう安全・安心に繋がるのか、ラベル付与製品とそうではない製品とはどのような差があるのかも含めて、本制度の運営事務局が主導し、IoT 製品ベンダーや小売り事業者等と連携しながら消費者に伝えることで、ラベル付与製品の需要を喚起していく。また、各種補助金制度との連携等を検討し、中小企業・小規模事業者等の調達者・利用者への需要喚起を図っていく。

4.3. 評価機関・検証事業者に対する支援策

特に☆3 以上では、第三者評価を必須とするため、評価機関の本制度への参画は重要である。また、☆1、☆2 でも、自己評価が困難である IoT 製品ベンダーは、評価機関や検証事業者に対して評価を依頼することが考えられるため、評価機関や検証事業者による本制度に対応した評価・検証サービスの提供の後押しが求められると考えられる。以上を踏まえ、評価機関等に対する支援を実施すべきか、また実施するのであればどのような支援策が良いかについて検討が必要である。

☆3 以上の評価は、十分な評価・検証能力を保有し、IoT 製品ベンダーから独立した客観的な評価を行える事業者にて実施する必要がある、そのような事業者を継続して確保していく必要がある。そのためには、独立行政法人製品評価技術基盤機構 (NITE) の製品評価技術基盤機構認定制度 (ASNITE)¹⁹の中に、本制度の☆3 以上の評価を行える事業者について ISO/IEC17025 に基づく評価機関認定制度を設け、適切な能力及び体制を整備した事業者を「評価機関」として認定し、その事業者のみが☆3 以上の評価を実施できるようにする。評価機関を継続して確保するためには 3.8.1 項及び 3.8.2 項の取組により、☆3 以上の評価ニーズを継続的に確保することが重要である。

☆1と☆2の自己適合宣言では、IoT 製品ベンダー自身による自己評価を許容しているものの、3.4 節で検討した☆1 の適合基準・評価手順にもツールを使用した実機テストが含まれており、☆2 以上では、より専門的な知識や検証環境が求められることが想定される。自社の既存体制や既存設備で十分な評価を実施できない IoT 製品ベンダー向けに、その評価を安心して委託できる一定の評価・検証能力を保有した事業者を「検証事業者」として示すこととする。自己適合宣言の対象となる☆1 と☆2 は、☆3 以上よりも多くの IoT 製品がラベルを取得することが想定されるため、評価機関だけではなく、より幅広い事業者を確保していく必要がある。経済産業省が定める情報セキュリティサービス基準²⁰への適合性について審査及び登録する情報セキュリティサービス基準審査登録制度²¹の機器検証サービス(2023 年 9 月より募集開始)にサービスが登録され、情報セキュリティサービス基準適合サービスリスト²²に掲載されている事業者を「検証事業者」とする。また、自己適合宣言における評価機関・検証事業者の活用を促すため、IoT 製品ベンダー向けに以下のような取組を実施することを検討する。

- 自己適合宣言の評価に必要な能力や前提条件、想定工数等を示し、評価を評価機関・検証事業者へ委託することのコストメリットを認識させる。
- 自己適合宣言の評価を IoT 製品ベンダー自身が実施したのか、第三者である評価機関・検証事業者が実施したのかをラベル付与製品毎の情報提供ページに掲載し、調達者・利用者が識別できるようにする。

¹⁹ NITE, 製品評価技術基盤機構認定制度 (ASNITE) <https://www.nite.go.jp/iajapan/asnite/index.html>

²⁰ 経済産業省, 情報セキュリティサービス審査登録制度
<https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html>

²¹ JASA, 情報セキュリティサービス基準審査登録制度 <https://sss-erc.org/>

²² IPA, 情報セキュリティサービス基準適合サービスリスト https://www.ipa.go.jp/security/service_list.html

- 特に自己評価を行う体制や設備が十分でなく、外部に委託する費用の確保が困難な中小企業の IoT 製品ベンダー向けに、評価機関・検証事業者に委託して自己適合宣言を実施する場合の補助金等の支援を検討する。

4.4. リスクに対応するための資源の確保策

IoT 製品ベンダー、調達者・利用者、評価機関、認証機関等が各々の責任を果たしていたとしても、サイバー攻撃によって被害が発生する可能性をゼロにすることはできない。事案発生時に適切に対処を行い、被害救済や原因是正に繋がる資源の確保策について、どのような策が効果的か等について検討が必要である。具体的には、社会的にリスク分散するための保険制度や脆弱性関連情報を適切に流通させるための枠組みである「情報セキュリティ早期警戒パートナーシップ」等との連携が考えられる。

事案が発生した場合に備え、損害を広く分散する社会の構築を目指していくことが適当である。例えば、評価機関・検証事業者が提供する評価・検証サービスを受けた製品が原因で発生したサイバー事故による賠償損害や費用損害を補償する商品付帯方式サイバー保険と連携することが考えられる。また、「情報セキュリティ早期警戒パートナーシップ」との連携を図り、ラベル付与製品に関わる脆弱性関連情報について適切な共有体制を設け、早期の対応を促す仕組みを構築することを本制度の運営事務局が中心となって検討する。

4.5. 制度全体の効率化

さまざまな種類のデバイスが IoT 製品として幅広く展開されており、その多様性ゆえに評価対象が増大することが予想される。このような状況においては、本制度における認証・管理業務の効率化が課題となる。効率的なプロセスを確立することにより、製品のラベル付与や認証プロセスにかかる時間とコストを削減し、本制度の持続可能性を確保することにつながる。以上を踏まえ、認証・管理業務の効率化について検討が必要である。

審査から登録廃止に至る業務プロセスの効率化・簡素化を実現するため、ラベル付与機関・認証機関における業務プロセスを具体化し、適用箇所と効率化手法を本制度の運営事務局が検討し、その後、実現可能性を評価する。また、☆3 以上の認証を受けた製品における脆弱性への対処に関して、SBOM や早期警戒パートナーシップの活用も視野に入れ、脆弱性情報を適切に共有し、迅速なパッチ適用を実現することを検討する。この際、既に SBOM に関する取組を進めている業界団体との調整に留意する。

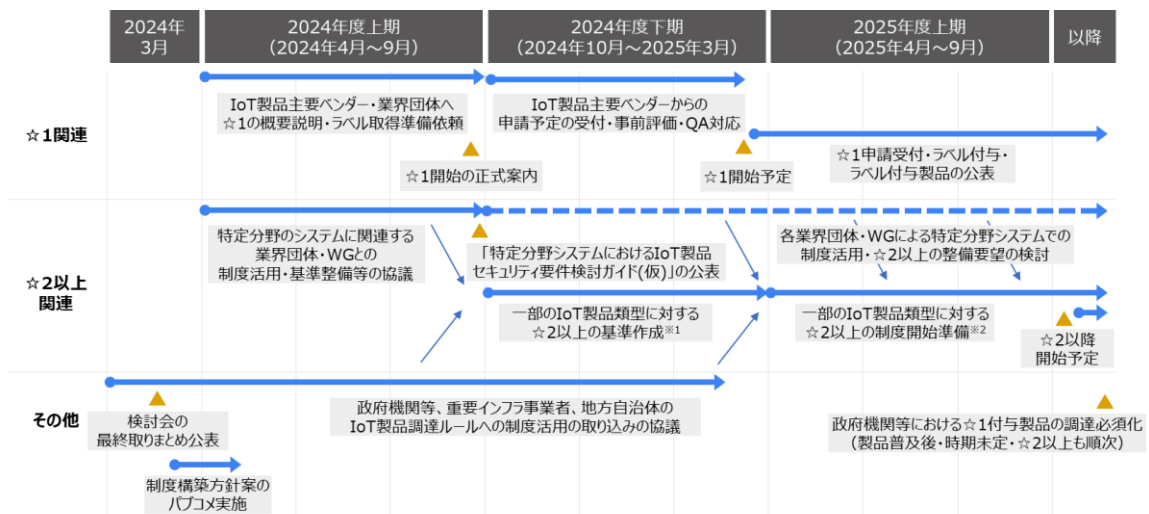
5. 今後の検討の進め方及びスケジュール

☆1 に関しては、2024 年度上期に、主要な IoT 製品ベンダーやその業界団体へ概要説明とラベル取得準備の依頼を行い、2024 年度半ば(9 月末頃)に制度開始の正式案内を行う想定である。その際、制度が既に導入されている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予定である。制度設計途中の見込みである欧米については、順次方向性を公表する。☆1 のラベル付与の開始は、2024 年度中(2025 年 3 月を想定)を目指す。

☆2 以上に関しては、2024 年度上期に IoT 製品が組み込まれる特定分野のシステムに関連する業界団体・ワーキンググループとの制度活用や基準整備等の協議を行い、2024 年度下期に一部の IoT 製品類型に対する基準を作成する想定である。2025 年度下期以降に一部の IoT 製品類型に対する☆2 以上のラベル付与の開始を目指す。

並行して、政府機関等へのラベル付与製品調達への必須化の調整及び重要インフラ事業者・地方公共団体への IoT 製品調達ルールへの制度活用の取り込みの働きかけを行う。

図 5-1 に今後のスケジュール案について示す。2024 年度以降の検討は、3.1 節で示したように運営審議委員会及び本制度の運営事務局を中心に、本ロードマップに従って推進していく。



※1：優先度の高い製品類型(2～3種の想定)が対象、基準が完成次第、順次☆2以降の開始予定を案内
 ※2：以降、対象となる製品類型を順次拡張

図 5-1 今後のスケジュール案

IoT 製品ベンダー関連の賛同団体一覧

※ 五十音順(2024年3月現在)

団体名称	略称	ホームページ	会員数
一般社団法人 情報通信ネットワーク産業協会 (Communications and Information network Association of Japan)	CIAJ	https://www.ciaj.or.jp/	140 社・団体 (2024年3月現在) • 正会員 89 社・団体 • 賛助会員 51 社・団体
一般社団法人 電子情報技術産業協会 (Japan Electronics and Information Technology Industries Association)	JEITA	https://www.jeita.or.jp/	380 社・団体 (2024年2月14日現在) • 正会員 343 社・団体 • 賛助会員 37 社・団体
公益社団法人 日本防犯設備協会 (Japan Security Systems Association)	SSAJ	https://www.ssaj.or.jp/	275 社・団体 (2023年6月現在) • 正会員 76 社 • 準会員 150 社 • 賛助会員 5 団体 • 特別会員 44 団体

以上