IoT製品に対するセキュリティ適合性評価制度構築方針案に対する意見公募手続きの結果について
（別紙）提出意見に対する考え方

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
1	M01	M01-001	制度構築方針案	2.3.	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、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。	方針案において「政府機関、重要インフラ等を優先的に検討すべきである」と結論づけながら、「【別添】☆1セキュリティ要件・適合基準では「☆1」の低レベルの基準しか定められておらず、初期ターゲットである「☆3」レベルでの基準が明らかになっておりません。 「☆3」レベルではセキュリティ対策としてより厳格なものが求められると思いますが、その内容が明らかになっておりません。それとも適合基準はレベル☆1～☆3で共通であり、☆3以上は第三者評価が求められるということでしょうか。そうであれば、方針案ではそのことを明記すべきであると考えます。	優先検討されるべき☆3レベルの適合基準が☆1と違うのか、違うならどのように異なるのかなどの想定がつかず困惑します。少なくとも適合基準の方針は示されるべきであると考えます。	3.4.に記載のとおり、「☆１、☆２、☆３、・・・」でそれぞれ適合基準は異なるものとなります。また、5.に記載のとおり、☆２以上の基準は、2024年度下期以降に検討する予定です。 ご指摘のとおり、政府機関や重要インフラ事業者等に向けた☆３以上の検討優先度が高いものの、ベースとなる製品類型共通の☆１の基準がないと、製品類型別の☆２以上の基準の検討が難しいため、このようなステップでの検討としています。また、3.8.1.に記載のとおり、例えば政府機関等であっても「重要度：低」のシステムでは☆１以上の製品調達を求める等を考えており、「☆１ラベル取得製品を政府機関等が調達しない」という意味合いではなく、☆１も政府機関等でも活用することとなります。
2	M01	M01-002	制度構築方針案	3.2.	図 3.2-1	図では、ネットワークカメラ等が例示されていますが、前述でも言及した「☆」のレベル分けについて、 同一の対象製品であっても政府機関、重要インフラの重要な監視対象で使用される場合、そうでない場合で利用ケースにより異なるレベルで使用される可能性があり、これについて方針案で言及しておく必要があると考えます。	同じルーター、ネットワークカメラ、複合機であっても政府機関や重要インフラで使用される場合と、家庭等で利用される場合には、第三者評価だけの話けではなく、セキュリティ基準、適合基準にも当然違いが出てくるものと想像しますが、単に製品カテゴリだけでレベル分けをしようとしているのか、同一の製品カテゴリでも、複数のレベルが存在するのか、その方針だけでも方針案に記載いただいた方が将来混乱を起こさずに良いと考えます。	同じ製品類型と定義して☆２～☆４のレベルを設定する場合、上位の基準は下位の基準（例えば、☆３の基準は☆２の基準）を包含する形で設定する想定です。そのことも考慮し、各製品類型の範囲を定義します。当該製品の利用・調達ニーズに応じて、最も高いレベルの「☆」を取得いただくことが望ましいと考えます。
3	M01	M01-003	制度構築方針案	3.3.	「☆3 以上」等	レベルの表記に「☆3、☆2」等を「☆」の記号を用いるのは不適切かつわかりにくいと考えます。また、諸外国制度との連携を謳っており「☆」の表記を用いることは諸外国への説明の際に困惑すると考えます。	例えば、欧州eIDASではHIGH, SUBSTANTIAL, LOWなどのレベル分となっており、レベル分けを見れば、どちらが高位であるか欧州外から見てもわかりやすいようになっています。「☆」の表記が海外向けに使用できず、また、レベルを数値で示す場合、1と3でどちらが厳格なセキュリティ基準なのかわかれるケースなどもあり、「☆」と数値で示すのは適切ではないと考えます。	最終的にどのようなロゴや表記にするかは、正式な制度発表（2024年秋頃）までに決定し、公表する予定です。 現時点においては、制度構築方針案の英訳版において「☆１」、「☆２」の表記を用いております。海外向けへの説明にも使用しておりますが、特に混乱するというご意見はいただいておりません。日本語フォントが表示されない点については、 「Star 1」、「Star 2」等の表記を使用しています。 https://www.meti.go.jp/policy/netsecurity/IoT_policy_draft.html
4	M01	M01-004	制度構築方針案	4.1.		各種補助金制度との連携によるIoT製品ベンダーのラベル取得負担軽減が施策に含まれていることに賛同いたします。ここで、利用者の商品選定の自由度の観点から☆レベルに応じた負担軽減施策を講じることにより、各レベルにおいて十分な製品数が提供できているかを制度でモニタリングし、製品数が不足する場合には追加の促進施策を講じられることを期待します。	調査者・利用者が必要とするレベルの製品がないという事態を避けるためにレベルに応じた普及施策が必要であると考えます。	2.1.に記載のとおり、調達者・利用者が求めるセキュリティ水準の製品を選択するために本制度のラベルを活用できるようにすることを本制度の目的としています。そのためには、調達者・利用者が同水準内での製品比較や、☆１と☆２での比較等を行えるよう、ラベル取得を普及させる必要があると考えています。補助金も含め、そのために必要な施策を検討します。
5	M01	M01-005	☆1セキュリティ要件・適合基準	1.		ユーザー認証、管理者認証がパスワードでしか行われない前提になっているように読み取れます。これは「☆1」だからということでしょうか。方針案では「☆1」の前提条件について述べておく必要があると考えます。	ユーザー認証や管理者認証はIDパスワード以外の方式が使われるケースがあり、特に厳格なセキュリティを求められるケースではIDパスワード以外の方式を用いられることがあります。現状の適合基準では、IDパスワードしか想定していないように誤解され、将来強固な認証が求められるようなケースに対応できません。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
6	M01	M01-006	☆1セキュリティ要件・適合基準	5.		このカテゴリにおいてWi-FiやBluetoothについてのみが言及されており、多くのIoT機器で使用され主要な暗号通信プロトコルであるTLSについて言及の必要があると考えます。その上で、以下の3つの観点から要件の追加が必要と考えます。 (a) 使用される暗号アルゴリズム、鍵長に関する要件 (b) 通信先の証明書の検証に関する要件 (c) (☆3以上等では)mTLS認証(TLS相互認証,TLSサーバー/クライアント認証)に関する要件	IoT製品のTLSの機能について確認することは使用されるTLS通信の安全性を確認する上で必須の基準であると考えます。 ・(a)を基準に含めない場合、弱い暗号により盗聴、改ざんの恐れがあります。 ・(b)を基準に含めない場合、不正な通信相手と通信することとなり盗聴等の恐れがあります。(b)の機能の不備があるIoT製品が散見されます。 ・☆3以上の政府機関、重要インフラではTLS通信においてはTLSサーバー認証だけではなく、クライアント側もIDパスワード等の弱い認証方式ではなく証明書と秘密鍵で認証するmTLS(TLS相互認証)が推奨されるか必須とする基準を含めるべきと考えます。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
7	M02	M02-001	制度構築方針案	1.	P2 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….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、IoT製品を主要な認証対象としておらず、	本認証制度の対象であるIoT機器の定義に「産業用製品」は入っていないのであれば、その旨明記するべき。 上記の意図ではないのであれば、左記記述を含む矛盾する表現を改定するべき。 いずれにしろ文書内に矛盾が生じない表現でIoT製品の定義を記載するべき。	左記を見ると「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」等は、「IoT製品を主要な認証対象としておらず、」とあり本評価制度の対象であるIoT製品には産業用製品が含まれないとの認識に見える。	産業用製品であっても定義に合致するIoT製品は、本制度の対象となります。本記載は、「（消費者向けの）IoT製品を主要な認証対象としておらず、」というニュアンスで使用しておりましたが、矛盾があるように読めるため、「IoT製品を主要な認証対象としておらず、また」の部分を削除します。
8	M02	M02-002	制度構築方針案	1.	P2 また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。	上記、とも関連するが、既存制度の問題点である「金銭的・時間的コスト」を軽減可能なもの（つまり簡素化されたもの）を構築しようと考えているのであれば、目的に明記するべき。	既存の認証制度の問題点として「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」ことを挙げているので、本認証制度はこの課題に解を与えるものと読み取れるため。	「IoT製品ベンダーにとって金銭的・時間的コストを軽減可能な制度であること」は、制度の目的ではなく、2.1.で示している、IoT製品ベンダーが積極的にラベルを取得するようになり、ラベルを取得した製品を広く普及させるために解決すべき課題のひとつに対する手段と考えており、3.5.等で示しています。
9	M02	M02-003	制度構築方針案	1.	P3 国内だけではなく世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。	グローバルで通用する認証とするために、少なくとも欧米（特にCRAや英国PSTI法）とは相互認証とするべき。そのためには、ターゲットとする先行する法規制とその法規制との差分を明確にするべき。例えば、CRAの認証を取っていれば、国内のものは不要とする、他国のものと差分を明確にし国内の認証を取っていれば差分のみで他国の認証も取れるなどが必要。	既に、認証を伴う法規制が各国で出てきており、各社それらに向け準備をしている。後から認証を追加する場合、よほどきちんと制度設計を考えないと、企業にとっては負担でしかない状況となることは容易に想像できる。	いただいた意見を考慮しながら、国際連携を図っていきます。
10	M02	M02-004	制度構築方針案	2.2.	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。	上記にも記載したが、内容の齟齬だけではなく、差分を明示し、各国主要な法規制で採用される認証制度と相互認証の協定を結んだうえで発行するべきである。	既に、認証を伴う法規制が各国で出てきており、各社それらに向け準備をしている。後から認証を追加する場合、よほどきちんと制度設計を考えないと、企業にとっては負担でしかない状況となることは容易に想像できる。	いただいた意見を考慮しながら、国際連携を図っていきます。
11	M02	M02-005	制度構築方針案	3.4.	P12 制度の位置づけならびに要件の範囲（図3.4-2 セキュリティ要件の整理方針）	諸団体にて複数の規格が似て非なる規格が乱立する中、国内独自の認定制度を導入することは更なる混乱を招くのみ。要件範囲も全ての規格を包含する方針となっており、ベンダー（さらには製品コストに上乗せとなるユーザーにも）へのデメリットしかないと考える。諸外国の認証制度との相互認証制度を確立するべきである。	国の活動として実施するのであれば、国内メリットに配慮すべき（むしろ諸外国の乱立規定を集約するよう対外的な働きかけを行い、負担軽減になるような活動を行うべき）	いただいた意見を考慮しながら、国際連携を図っていきます。 なお、要件範囲も全ての規格を包含するのは制度のセキュリティ要件（全体）であり、その中から☆１～☆４の各セキュリティ水準(☆２以上は製品類型ごと)において必要な要件を選定して適合基準を作成します。
12	M02	M02-006	制度構築方針案	3.4.	P13 ☆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。	左記をベースとするのであれば対象を「民生用IoT機器」と明示した上で、他のより厳しい基準でカバーすることが求められている製品群を除外する旨も記載するべきである。	左記基準は「民生用IoT機器」であり、多重の認証を要求されることを避けるべきであるため	制度発足時点では☆１の適合基準から始めるが、更に適合基準が厳しくなる☆２以上を順次整備していく計画です。したがって、本制度は☆１の「民生用IoT機器」に限定しているわけではなく、現行記載のままとします。
13	M02	M02-007	制度構築方針案	3.8.3.	P23 ☆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（中略）、相互承認の調整を図っていく。	当面は任意制度のようであるが、認証取得を必須とする計画があるのであれば、必須化の前に主要な諸外国の認証制度との相互認証制度を確立するべきである。	相互認証確立の前段としてレベル合わせをするべきであるが、現状あっているようには見えない（すくなくともCRAとは全く合っていない上に、この文書と下記記事などで報じられている経産省の格付けのレベルがあっていない。 https://www.nikkei.com/article/DGXZQOUA039VJ0T00C24A4000000/	いただいた記事にある「企業のサイバー攻撃対策を格付けする制度」は、経済産業省で今年度から検討を始めている制度ですが、企業・組織のサイバーセキュリティ対策状況が対象であり、本IoTセキュリティ適合制度とは別の制度となります。また、本制度のラベルを取得していないと販売できない、何か罰則がある等の観点での必須化について、具体的な計画は現時点でありません。
14	M02	M02-008	制度構築方針案	3.8.2.	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。	本案では、製品単体に実装するセキュリティ機能のみを論じており、システム全体でセキュリティを担保した場合については、本案の外部に責任を転嫁しており、また、システム全体でのセキュリティに関する本制度の拡張性についても論じていない。	諸外国の関連法規案では定義されているシステムのリスク分析を行うスキームを設けているが、本案では、リスク分析の前提となる利用方法をユーザに提示することを将来計画としても論じていない(いわゆる多層防御の考え方がない)。 導入障壁を低くするという意味(指定された機能を実装すればよいという単純化)では良いのかもしれないが、一方で、製品観点では不要な機能が実装される可能性がある。	3.1.に記載のとおり、☆２以上の基準は、各IoT製品類型ごとに適合基準検討WGを設置し、当該製品類型のIoT製品ベンダー、調達組織、関連団体等を中心に検討を行います。 その中で、当該IoT製品類型が使用されるシステム環境やネットワーク環境等のユースケース、守るべき資産等を設定し、想定される脅威と、それに対抗するために必要なセキュリティ対策を検討していきます。
15	M02	M02-009	☆1セキュリティ要件・適合基準	1-2,1-3,3-7	6文字以上のパスワードであること。 8文字以上のパスワードの設定を強制させること。 適切な認証に基づくアクセス制御 ベストプラクティスの暗号技術を使用し	要件によって、具体的なセキュリティ強度が記載されていることもあれば、達成基準が明確でない要件が混在している。具体的なセキュリティ強度を記載するケースにおいては、その基準を選定した根拠・理由を記載してほしい。また、達成基準が明確でない要件については、例などによってどのような手段であればその要件が達成されたとみなすのか示してほしい。	達成基準の記載が不明確であると、その解釈によって実現手段が異なり、特に自己宣言においてはその解釈の違いによって大幅なセキュリティレベルの差異が発生する可能性があるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
16	M03	M03-001	制度構築方針案	3.2.		・医療分野においては規制の対象となる医療機器と規制の対象とならない非医療機器があり、この方針案はヘルスソフトウェア機器も含めてGHSの置き換えとしても非医療機器に適応できるのではないかと思っています。 ・医療機器もIoT機器と同じであると考えていますので、この方針の対象となることは理解できます。しかし医療機器となると厚労省の規制の対象となりますので、今後厚労省医療機器審査管理課との調整、検討が必要であると考えます。 ・規制対象となる医療機器では、開発における品質の確保やサイバーセキュリティについては2024年3月31日に厚労省通知（医療機器の基本要件基準第12条第３項の適用について、医療機器のサイバーセキュリティ導入に関する手引書の改訂について）が発出されています。		いただいた意見を考慮し、関係省庁や関係団体とも連携しながら、制度構築を図っていきます。
17	M04	M04-001	制度構築方針案	3.2.	P.8 10、11行目	インターネットに接続されず、管理されたローカルネットワークで施工される事でセキュリティを担保するネットワーク製品は対象にすべきではない。したがって、「・・・IP を使用してデータを送受信する機能を持つ機器。但し、DMZなどの機構により、インターネットと直接的な通信が不可能となるように管理されているローカルネットワークに、専ら接続する機器は対象外とする。」と明確に記載すべきである。	ビルシステムにおけるBACnet/IPや工場設備におけるModbus/IPなどは、管理されたローカルネットワークで施工される事でセキュリティを担保する前提にたったネットワークシステムであり、方針案のままで規制されると、システムが構築できなくなってしまう。	本制度は任意制度であり、「対象機器」の意味合いは、「ラベル取得が求められ得る機器」ではなく、「ラベル取得が可能な機器」となります。その観点で、利用が主にローカルネットワークであっても、「ラベル取得を不可」とする理由はなく対象とします。ローカルネットワークや制御系ネットワークであっても、何かしら外部と接続されており、サイバー攻撃を受ける事案が発生している以上、それだけで機器のセキュリティ対策が不要な理由にはならないと考えています。 ただし、実際には、調達者がその利用形態やリスク（管理されたローカルネットワークでの利用など）を考慮し、どの機器にどのレベルのラベルを取得しているのことを求めるか（取得していないことを許容することも含む）を判断することとなります。 また、ビルシステムに関しては、3.8.2.に記載のとおり、業界団体等と連携して、システム全体のセキュリティの検討と、そこからどのような機器にどのレベルのセキュリティを求めるかを検討する予定です。
18	M04	M04-002	☆1セキュリティ要件・適合基準	17-3		業務用の製品・サービスは、商流によっては販売先経由でユーザに通知しなければならない。したがって、「・・・いる場合、製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザ、または販売先から順次説明する必要がある商流にあっては販売先に通知しなければならない。」と直接取引のある顧客までの通知だけも認めて欲しい。	業務用空調システムは、商習慣上、商流への説明責任が発生するため、販売先から順々に製品やシステムを購入する顧客へと説明していく必要がある。	本項目では、ユーザに確実に情報が提供されることを求めています。販売代理店までの情報公開のみでは不十分となります。 商習慣上、販売先から順々に"確実に"顧客へ情報伝達される仕組み(例えば、代理店契約上、そのような条項が含まれている等)があるのであれば、その点を含めて評価してください。
19	M05	M05-001	制度構築方針案	3.2.	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	ネットワークに接続するためのIoT機能がオプション・別売品の扱い（専用部材を別途ご購入いただき、取り付けが必要となる構成）となる製品の場合、製品単体では、本制度の対象外となる認識でよろしいでしょうか。		オプションを含まずネットワークへの接続機能を有しない製品の場合、本制度のラベルは取得できません。 一方で、（特定のオプション製品しか取り付けられない場合は）オプションとなる通信モジュールを取り付けたものを対象とし、ラベル取得していただくことは可能です。あるいは、他製品でも共通の通信モジュールを使用しており、当該通信モジュールが単体で販売されているような場合は、通信モジュールをIoT製品とみなし、ラベルを取得いただく方法も考えられます。その場合、「本体製品自体がラベル取得」という表現は使用できず、「ラベル取得済み通信モジュール搭載可能な製品」のような表現になるかと思います。
20	M05	M05-002	制度構築方針案	3.3.	3.3項　制度における適合性評価レベル 「IoT製品ベンダー」 3.7項　ラベルの信頼性確保のための仕組み 「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」	認証期間中に、事業移管やM＆Aなどで、IoT製品ベンダーの正式名称が変わった場合も、付与したラベルが取り消され、再申請になりますか？		事業移管やM＆Aなどにより、ラベル取得済み製品のIoT製品ベンダーが変更となった場合は、登録情報の変更申請を行ってください。取得済みラベルの適合基準に関するセキュリティ機能・管理等に変更がなないなど、一定の条件を満たせばラベルの継続利用を認める予定です。 詳細はIPAにて策定予定の本制度の規程等で定めます。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
21	M05	M05-003	制度構築方針案	3.8.2.		「特定分野のシステムに組み込まれて調達され、利用されるケースがある」、の具体的な例として、「スマートホームシステム」をあげていただいています。 ☆２以上の検討になるかと思いますが、たとえば、このスマートホームの場合、スマートホームシステム全体ではなく、組み込まれる機器側を対象として、☆2以上に適合する必要があるということでしょうか。		本制度の対象とするのはIoT製品であり、ラベルの取得単位は「組み込まれる機器側」となります。 「スマートホームシステム全体」として考慮すべきセキュリティとしては、ネットワーク構成、システム管理等もあり、組み込む機器に求めるセキュリティ（＝本制度のどのレベルの☆を求めるか）はその一部になります。3.8.2.に記載のとおり、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認証制度等の整備は、各業界団体やワーキンググループにで検討する想定であり、本制度としてはそれらと連携する方針となります。
22	M05	M05-004	☆1セキュリティ要件・適合基準	全般	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性	下記5-1などの「【参考】国内既存制度・文書で求められるセキュリティ要件との関係性」の列の記載内容について 【CCDSサーティフィケーションプログラム】1-2データ保護【必須】②、1-4-1Wi-Fi認証方式【必須】①、1-4-2Bluetoothの対策【必須】①などの記載において、これは、この5-1のセキュリティ要件を満たすためには対応が必須という意味なのか、それとも参考文書の中の必須要件という意味なのか、何が必須なのかがわかりにくいので、おそれいりますが、既存制度との関係性を明確にしていただきたいです。		「【参考】国内既存制度・文書で求められるセキュリティ要件との関係性」の列の記載はあくまで各制度や基準との関連性を示す参考情報であり、その適合を求めるものではありません。
23	M06	M06-001	☆1セキュリティ要件・適合基準	全般	なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。	適合基準として以下のように記載されているアクセス制御は、ローカルネットワークからのアクセスも制御対象となりますでしょうか。 「TCP/UDP通信を介した守るべき情報資産への他の機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。」	☆1適合基準欄に但し書きとして「なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品は、本適合基準に適合しているとみなす。」とありますが、該当の適合認定の対象は電気通信回線設備（＝インターネット）からのアクセスを対象としているため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
24	M06	M06-002	☆1セキュリティ要件・適合基準	用語集	「制約のある機器」の意味 説明文(注2)	誤記があります。 誤)「～制約のある機器のある機器ではない。」 正)「～制約のある機器ではない。」	誤記	誤記となりますので、修正します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映）
25	M07	M07-001	制度構築方針案	3.7.	検証事業者、評価機関の説明は、0 節を参照のこと。	誤記		「4.3節」への参照の誤植となりますので、修正します。
26	M07	M07-002	☆1セキュリティ要件・適合基準	1-2	NAとなるための条件、基準の補足説明	☆１適合基準の列では、「ユーザ認証の仕組み、又は、（中略）クライアント認証の仕組み」となっている。NAとなるための条件でも、クライアント認証の仕組みがないことを記載するべきではないか？	現状の記載では、クライアント認証の仕組みのみを利用する場合には汎用のデフォルトパスワードが利用できてしまう。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
27	M08	M08-001	制度構築方針案	全般	IoT製品ベンダー	「IoT製品ベンダー」には、どの様な事業者が含まれるのか、例えばp24 4.1に海外のIoTベンダーの言及があるものの範囲が不明確である。例えば、製造事業者（原産国が外国の場合を含む）、外国製品を日本国内で販売する外国の製造事業者、製品を輸入して国内で販売する事業者なども対象であることを明確化していただきたい。 そのため、適用範囲と事業者の例の記載を追加いただきたい。 なお、別添☆１のセキュリティ要件・適合基準の用語集の「製造業者」の「意味」に記載の内容と同じであれば、それを制度構築方針案本体にも記載いただきたい。	国内に流通するあらゆるIoT製品のベンダーを対象とし、ラベリング制度を広く浸透させるため。	「1.はじめに」にて、「IoT製品ベンダー」は「IoT製品を製造又は販売するベンダー」と定義しています。 ☆１適合基準では、別途IPAから公開しているETSI EN 303 645の和訳との整合も意識しており、「manufacturer」の和訳として「製造業者」を採用します。一方で、制度構築方針案の「IoT製品ベンダー」に相当する定義であり、用語集の「製造業者」の注記に以下の記載を追加します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映） ・この定義は、「IoT製品に対するセキュリティ適合性評価制度構築方針」における「IoT製品ベンダー」に相当する。
28	M08	M08-002	制度構築方針案	2.2.	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	自己認証でIPAがラベル発行することになっているが、ラベルの発行、作成はIPAが実施し、各ベンダーに無償提供するのか。有償の場合はメーカが負担することになるため、無償にしていただきたい。	多くのベンダーのラベル取得を目指すのであれば、取得のハードルを下げるために無償にするべきと考えるため。	IPAでの確認の上でラベルは発行されるため、ラベル取得のためにはIPAへの申請料の支払いが必要となります。IPAの確認後、ラベル取得可となった場合、ロゴとQRコードが記載されたラベルを電子データとしてIPAから申請者に提供されます（申請料の中での対応で、追加費用はありません）。 そのラベルを物理的に掲示するために貼り付け用のシール（物理的なラベル）等の作成は、当該電子データを用いて、IoT製品ベンダーにて実施してください。
29	M08	M08-003	制度構築方針案	2.1.	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。	本適合性評価制度の対象製品なのにラベルがつけられていない製品と、対象外製品だからラベルがついていない製品の判別はどうするのか。	消費者はラベルがついていない製品は全てセキュリティ品質の低い、良くない製品と捉えてしまわないか心配なため。	3.2.に記載のとおり、「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）」以外は、定義を満たすものは全て対象となり、少なくとも☆１の取得は可能となります。 例示されている、パソコン、タブレット端末、スマートフォン等が制度の対象外となる点は、特に消費者向けに説明していくようにしますが、比較対象の製品もラベル取得はできないため、大きな混乱には至らないと考えています。
30	M08	M08-004	制度構築方針案	3.2.	これらの IoT 機器にその関連サービスを含めた IoT 製品を本制度の対象範囲とする。	IoTサービスを提供する場合に、IoT製品の中にインターネット上（クラウドサーバー上）で提供するサービスも含まれるように明記すべきです（図3.2-1には含まれていない）。 【修正案】 これらの IoT 機器にその関連サービスを含めた IoT 製品を本制度の対象範囲とする。但し、関連サービスにおける適合基準の対象は、IoT機器の直接の通信相手となる機器またはサーバーとする。	評価対象が曖昧なため。	「インターネット上（クラウドサーバー上）で提供するサービス」は、それがIoT機器の利用に必要なものである場合、「付随サービス」としてIoT製品の範囲に含みラベル取得することが可能です。 図3.2-1については、「付随サービス」まで含めた「IoT製品」のイメージを記載できておらず、その前段落の「～の送受信機能を持つ以下の機器を対象に含める。」の部分のイメージとなるため、その記述をそちらに移動させます。 いただいた修正案は、「IoT機器の直接の通信相手となる機器またはサーバー」のみが「付随サービス」に該当するとはいえないため、見送りとします。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
31	M08	M08-005	制度構築方針案	3.2.	関連サービスとは、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。	IoT機器と異なる事業者によるサービスとの組合せも想定されるが、申請時の対象範囲の解釈の余地が少ないように定義をお願いしたい。	IoT製品ベンダー、調達者・利用者における解釈のわかり易さ向上のため。	「IoT機器と異なる事業者によるサービス」は、それがIoT機器の利用に必要なものである場合、「付随サービス」としてIoT製品の範囲に含みラベル取得することが可能です。 連携できるが、必ずしもIoT機器の利用に必要でないサービスは、ラベル取得の対象外とします。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
32	M08	M08-006	制度構築方針案	3.2.	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	インターネットには接続せずイントラネットに接続する製品は対象になるか。対象を判別するための事例がもう少し欲しい。 また、IPとはTCP/IPのことでしょうか？LON通信の機器は対象外になるのでしょうか。	対象製品の判別を明確にしたいため。	3.2.に記載のとおり、「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」は本制度の対象範囲となります。 イントラネットに接続する製品であってもインターネットプロトコル（TCP/IP）を使用するものは対象となりますので、その観点で判断してください。
33	M08	M08-007	制度構築方針案	3.2.	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	ECHONET-Liteの規格で通信している機器は、基本的に非暗号で通信していると思うが、こういった規格に対応している機器は、ラベル取得が不可能ということなのか。	セキュリティ対策が行われているプロトコルとECHONET-Liteの両方に対応するような製品があった場合に、ラベル取得が可能なのかと疑問に思ったためです。	非暗号の通信を許可していればラベルを取得できないという訳ではありません。☆１の場合は、☆１評価項目番号12を満たしているまたは対象外(NA)と判断できる場合は、☆１のラベル取得が可能です。
34	M08	M08-008	制度構築方針案	3.2.	ETSI EN 303 645 の定義では、IoT 製品（IoT product）とは、IoT 機器（IoT device）とその関連サービスを含むものである。・・・これらのIoT 機器にその関連サービスを含めたIoT 製品を本制度の対象範囲とする。対象製品のイメージを図 3.2-1 に示す。	本制度の対象範囲が機器＋サービスと定められております、☆１セキュリティ要件・適合基準の内容をみると、IoT機器をターゲットとして要件が定められているように読めます。図3.2-1をみても、サービス部分を実現するサーバーやスマートフォンアプリのような記載がなく、実際に試験対象となる通信ノード（例えば家電製品、サーバー、スマートフォンアプリ）が分かり難いです。明確な記載にして欲しい。	☆１セキュリティ要件・適合基準に記載されている内容が、どの通信ノードに対して行うべき内容なのか不明確のため。	図3.2-1については、「付随サービス」まで含めた「IoT製品」のイメージを記載できておらず、その前段落の「～の送受信機能を持つ以下の機器を対象に含める。」の部分のイメージとなるため、その記述をそちらに移動させます。 なお、☆１は様々なIoT製品類型共通の基準を示しており、特定の「付随サービス」の存在を想定したユースケースを設定していないため、基本的にはIoT機器にて評価可能な基準となっています。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
35	M08	M08-009	制度構築方針案	3.2.	これらの IoT機器にその関連サービスを含めた IoT製品を本制度の対象範囲とする。対象製品のイメージを図 3.2-1 に示す。	IoT製品は、IoT機器と、タブレット端末やスマートフォン等のソフトウェア製品（アプリケーション）が一体となってサービスを構成することがある。 適合性の評価対象は、IoT機器単体なのか、ソフトウェア製品が含まれるのかを明確化願いたい。 また、適合性評価対象にソフトウェア製品が含まれる場合、ソフトウェア製品を更新しても一体として用いるIoT機器については、変更申請や情報提供等を不要とするなど運用の簡素化をお願いしたい。	適合評価時の評価対象とソフトウェア製品のバージョンなどが異なる場合が想定される。 申請の頻度や申請書類の簡素化をお願いしたい。	制度の対象は、「IoT製品＝IoT機器（＋付随サービス）」となります。IoT機器の利用に必要なものである場合、「付随サービス」としてIoT製品の範囲に含みラベル取得することが可能です。 なお、ソフトウェア製品をラベル取得製品の範囲に含む場合、3.7.に記載のとおり、評価に影響を及ぼすレベルでの製品仕様の変更があった場合は、☆１、☆２のラベルは失効し、継続する場合は、自己適合宣言を再度実施することとなります。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
36	M08	M08-010	制度構築方針案	3.3.	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。	IoT機器はネットワークに接続するための通信回線を分離して(モジュール化して)構成することが想定される。この場合、通信回線(モジュール)単独での申請を可能として欲しい。適合性を評価された同じ通信回線(モジュール)を搭載する派生機種の申請の簡素化をお願いしたい。	申請の頻度や申請書類の簡素化をお願いしたい。	セキュリティ上の機能や管理（将来的なソフトウェアのアップデート等を含む）が同一であれば、同一製品の範囲としてラベルを取得することを可能とする予定です。各製品が「通信回線(モジュール)」部分以外に適合基準に関するセキュリティ機能等を有していない前提となりますが、派生機種も含め、「同一の通信回線(モジュール)を搭載した製品群」としてラベルを取得することが可能です。その際は、各製品の型番等を登録することとなり、ラベル取得後に新規の派生機種を販売する場合は、その登録情報を更新いただくこととなります。
37	M08	M08-011	制度構築方針案	3.3.	☆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。	☆1、☆2、☆3のレベルによって、ラベルの色などの見た目は変わるのか。	消費者が視覚的に違いを判別できた方がよいと考えるため。	ラベルの星の数で視覚的に☆１～☆４の違いを判別可能とする予定です。
38	M08	M08-012	制度構築方針案	4.1.	適合性評価を受けるにあたり、IoT 製品ベンダーには様々なコストが発生する。	ラベル取得にかかる費用だけでなく、実際のラベル、および貼り付け or 同梱する作業についても支援策を検討していただきたい。 【修正案】 適合性評価を受けるにあたり、IoT製品ベンダーにはラベルの取得費用に加えて、貼り付け、同梱作業など様々なコストが発生する。	企業側もラベルにより販売機会損失につながるため対応せざるを得ないが、その後の作業についても企業側で工数全負担となる点について、国から企業への補助も検討して欲しいため。	評価や申請費用だけでなく、IoT製品ベンダーに様々な負担が生じることは認識しています。そのため、3.7.に記載のとおり、ラベルの表示義務は設けず、IoT製品ベンダーが任意に様々な手法でラベルを掲示できるようにする予定です。 今後、例えば、消費者向けの特定のIoT製品類型に対してラベルの掲示を義務化するような場合には、支援策を検討します。
39	M08	M08-013	制度構築方針案	3.3.		☆2以上の適合基準が今後検討されると思うが、製品が用いられる用途などで要求される基準が変わることが想定されるので、調達者・利用者が判断しやすいように製品類型の曖昧さをなくして明確にするようお願いしたい。	調達者・利用者におけるわかりやすさのため	☆２以上を整備予定の製品類型の対象や、どのようなセキュリティ水準の製品を☆２以上として想定するのかの方針等の情報を早期に公開するようにします。
40	M08	M08-014	制度構築方針案	3.4.	図3.4-2	「国内外のセキュリティ要件を踏まえ、本制度におけるセキュリティ要件を策定」諸外国の制度との相互運用性について検討されていることは非常に好ましいことです。一方で複数国の制度を反映することにより、日本の制度が単一国の制度よりも過剰な制度（規則）とならないように検討いただきたいと考えます。	総和をとることで、日本の基準にて諸外国と異なる条項が設けられ、認証取得が難しくなることを懸念します。	既に一部の協議は開始していますが、諸外国とは積極的に連携し、最終的には相互承認を確立する方針で検討を進めています。 なお、3.4に記載のとおり、セキュリティ要件（全体リスト）は国内外の基準等の総和を取って作成していますが、ラベル取得の際に満たすべき適合基準は、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威を設定し、必要なセキュリティ要件をセキュリティ要件（全体リスト）から抽出して定めます。
41	M08	M08-015	制度構築方針案	3.4.	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。	申請はどのくらいの分類をすればよいか。同じ無線モジュールを搭載していれば代表１機種でよいか。エアコン、冷蔵庫など製品が違っても同じ無線モジュールを搭載していれば代表１機種でよいか。	無線モジュールを搭載することでIoTを実現する家電においては、セキュリティは無線モジュールに依存するため、無線モジュールが同じであれば申請は共通でよいと思う。 ただし、複数年にわたり同じ無線モジュールを採用すると2年経過後はユーザ購入時からすでに無効となってしまう場合がある。 逆に年度毎や製品毎に申請を行った場合、申請は順次行うため、同じセキュリティレベルであるが、認証有効な製品と無効となった製品が市場に混在することになる。	セキュリティ上の機能や管理（将来的なソフトウェアのアップデート等を含む）が同一であれば、同一製品の範囲としてラベルを取得することを可能とする予定です。各製品が「無線モジュール」部分以外に適合基準に関するセキュリティ機能等を有していない前提となりますが、「同一の無線モジュールを搭載した製品群」としてラベルを取得することが可能です。その際は、各製品の型番等を登録することとなります。ラベルは取得から２年間有効ですが、必要であれば再評価し、更新してください。ラベルが有効か無効かは、ラベルのQRコードからラベル取得製品の情報提供ページにて確認いただくこととなります。
42	M08	M08-016	制度構築方針案	3.4.	☆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。	サポート文章(FAQ)が提供可能な時期を図5-1 今後のスケジュール案に載せて欲しい	サポートが受けられる時期を明確にして頂けると、本件に対応するためのスケジュールが立て易いため。	2025年度以降、準備ができたものから公開する予定です。
43	M08	M08-017	制度構築方針案	3.5.	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。	自己認証であればPSTI法のように自己でマーキングや宣言書を手配するようなスキームにしていただきたい。	ベンダー側は申請してくる時点でチェックリストは全てOKとしているはずなので、IPAによるチェックリストの形式確認は不要な作業だと感じる。また、このようなスキームでは第三者認証と手間はあまり変わらないと考えるため。	自己適合宣言であっても、問合せ先情報の確認、ぜい弱性情報の集約や早期警戒パートナーシップ等のぜい弱性対応の促進、サプライチェーン・リスクの考慮など、セキュリティ要件以外の視点での活用も想定しているため、IPAによる申請受付・ラベル付与のスキームとします。
44	M08	M08-018	制度構築方針案	3.5.	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。	ラベルの発行をIPAが実施する場合、申請から発行までの日数はどの程度を想定していますでしょうか。	日数がかなりあると製品の製造工程、販売に影響があるため	申請手続方法の詳細については、年内（2024年12月末まで）に公表する予定です。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
45	M08	M08-019	制度構築方針案	3.5.	表3.5-2 ☆ 1、☆ 2（自己適合宣言）×評価機関 （評価機関や検証事業者の利用は任意）	（評価機関や検証事業者の利用は任意）とだけ記載があるが、評価機関や検証事業者を利用する場合のそれらの者の責務を記載いただきたい。	自己適合宣言の場合の評価機関や検証事業者の責務の明確化をお願いします。	自己適合宣言の場合、評価機関や検証事業者を利用したとしても、最終的な責任はIoT製品ベンダーとなり、その責務の一部を委託することとなります。そのため、その責務は、本制度で規定されるものではなく、IoT製品ベンダーと評価機関や検証事業者の間で決められるものとなります。
46	M08	M08-020	制度構築方針案	3.7.		「情報提供ページの掲載情報は日本語で表記する」ことを記載すべきです。 【修正案】 情報提供ページの掲載情報案を表3.7-1に示す。情報提供ページの掲載情報は日本語で表記する。	今後、海外からのIoT製品が輸入されるに伴い、海外母国語でのサポートのみとなる可能性が高いと考えております。 日本の利用者に向けてのガイドラインであれば、その状態ではサポートが厳しくなるかと思うので、日本語であることを記載しておくことが、日本の利用者に対して適切かと思います。（UKのPSTIには、英語での記載という旨が法令に記載されております。）	「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。」と記載を見直します。
47	M08	M08-021	制度構築方針案	3.7.	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。・・・	ラベルの信頼性確保の仕組みとしての、検証事業者、評価機関の要件について記載がないので記載願いたい。 4.3. 評価機関 ・検証事業者に対する支援策に、評価機関や検証事業者の要件に該当する記述があるため、その内容を本項にも記載願いたい。	検証事業者、評価機関に評価を依頼することが信頼性確保に役立つことの明確化。	参照先の節番号が誤植となっていましたが、「検証事業者、評価機関の説明は、4.3節を参照のこと。」と修正しました。
48	M08	M08-022	制度構築方針案	3.7.	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（略）	本制度の運用が開始されるにあたってWebサイトの運用者の明示をお願いしたい。	IPAが運用すると推測しますが、明示されていないため。	「本制度の」は、「本制度のスキームオーナー（IPA）の」を意味しています。
49	M08	M08-023	制度構築方針案	3.7.	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	情報提供ページへのアクセス数などの結果を報告もしくは公開してほしい。	本制度の有効性を確認するため。	情報提供ページの設計の際の参考とします。
50	M08	M08-024	制度構築方針案	3.7.	調達者・利用者からの申請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、申請者に対して評価に使用した証跡の提出を求めることや検査・サーベイランスを実施する。証跡の提出に当たっては、必要に応じて 秘密保持契約(NDA)を申請者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、申請者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。	ここで言う「申請者」が誰を表すのかが不明確です。基準への適合に疑義を生じて「申請」をする調達者・利用者のことであるのか、ラベル付与を申請するベンダーであるのか。 例えば、調達者・利用者からの「申請」を、調達者・利用者からの「請求」と別の表現に置き換え、「申請者」を「ラベル付与申請者」とするなど、明確になるよう記載・修正願いたい。	申請者が誰を表すのかの明確化。	以下のとおり記載を見直しました。 「調達者・利用者からの申請」→「調達者・利用者からの指摘」 「申請者」→「（ラベルを取得した）IoT製品ベンダー」
51	M08	M08-025	制度構築方針案	3.7.	☆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。	変化の激しい分野であることを考えると有効期限を2年以内とすることに合理性はあるものの、海外製品も対象とすることを考えれば、比較対象としてIEC62443の有効期限は3年なので整合をとることを提案します。	更新のための評価に要する負担とコストを考慮。	諸外国の制度との比較及び制度開始当初の☆１では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から、☆１の有効期限の設定は、最大２年とすることが妥当と考えています。 (参考)第7回検討会資料　資料4 P.14 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.html
52	M08	M08-026	制度構築方針案	3.7.	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	再度適合性評価→ラベル申請の手順になるのでしょうか。製品仕様と適合基準に変更がなく、適合性評価に影響がないと判断できる場合に限り、延長申請を簡略化していただきたい。	延長時の不要な工数を削減したいため。	自己適合宣言の場合、延長申請に当たって、申請するIoT製品ベンダーの責任において作成したチェックリストを準備する必要があります。どこまでの再評価を実施する必要があるかは、製品仕様の変更や適合基準の変更有無を考慮した上で判断してください。少なくとも前回の自己適合宣言に使用した際のチェックリストに記載されている評価内容や証跡に変更がないか等の確認は必要となります。
53	M08	M08-027	制度構築方針案	3.7.	☆1 、☆2 の有効期限はラベル取得日から最大2年間	有効期限は必要であるのでしょうか。もしくはベンダー側で有効期限を申請可能にした方がよい。と考えます。	製品によって、ライフサイクルや開発プロセスが異なるため。	ラベルの信頼性を維持するため、諸外国の制度との比較及び制度開始当初の☆１では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から、☆１の有効期限の設定は、最大２年とし、延長する場合は再申請を求めることが妥当と考えています。
54	M08	M08-028	制度構築方針案	3.7.	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。	失効済みではなく、有効期限を記載する方がよい。と考えます。	掲載時に有効期限のみ記載すればよい。失効済みと記載する場合、随時チェックが必要となり、負荷が大きい。	情報提供ページには有効期限も記載されます。なお、有効期限内であってもラベルの取消・失効が行われたり、有効期限が経過していても失効済みかがすぐにわからない、といったことが考えられるので、ステータス表示を合わせて実施します。 なお、ラベルの再申請（継続）する際のラベル貼り替えの負担を考慮し、ラベルはロゴとQRコードのみとし、有効期限の掲載はしない方針です。
55	M08	M08-029	制度構築方針案	3.7.	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。	内部監査などで適合違反が見つかった場合等の報告先はあるのでしょうか。	何かあったときの連絡先を明確にしたいため。	スキームオーナー（IPA）に申告いただくことになります。詳細はIPAにて策定予定の本制度の規程等で定めます。
56	M08	M08-030	制度構築方針案	3.7.	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。	取り消しの判断基準や不服申し立ての方法など、取り消す仕組みの手順を明示していただきたい。	実際に取り消し対応する際の手順を明確にしたいため。	詳細はIPAにて策定予定の本制度の規程等で定めます。
57	M08	M08-031	制度構築方針案	3.8.	2.1節の主目的を三つの主目的を達成するため、・・・	誤植だと思われる。以下への修正を提案します。 2.1.節の三つの主目的を達成するため、・・・	エディトリアルな修正	誤植となりますので、修正します。
58	M08	M08-032	制度構築方針案	5.1.	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していただきたい。	ラベル取得にかかる費用がいつ頃になるか図5-1今後のスケジュール案に載せて欲しい。（できるだけ早く決めて欲しい）	費用感がつかめないと、本認証に対するGo/NoGoの判断が遅れてしまい、対応が遅くなる恐れがある。	正式な制度発表（2024年秋頃）までに決定し、公表する予定です。
59	M08	M08-033	制度構築方針案	4.1.	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。	ドキュメントの提供時期を　図5-1　今後のスケジュール案にて明確にして頂ければと考えます。	対応を進めるにあたり、時期を明確にしていただけると対応スケジュールが立てやすくなるため。	正式な制度発表（2024年秋頃）までに決定し、公表する予定です。
60	M08	M08-034	☆1セキュリティ要件・適合基準	全般	NAとなるための条件	「NA」の定義が無く、またNAとなる条件を満たす場合の措置についての記載がないため、「該当なし(NA)として適用除外とするための条件」への変更を提案します。	適合基準の明確化	項目名を「対象外（NA）となるための条件、基準の補足説明」と見直します。 （2024年秋頃に公表予定の☆１適合基準の最終版に反映）
61	M08	M08-035	☆1セキュリティ要件・適合基準	全般	セキュリティ要件	「製造業者」という言葉は、諸外国の制度に記載の”manufacturer”を和訳したものと推測しますが、当該製品に対して責任を持つ様々な事業者(販売事業者、輸入事業者等)をイメージしにくいため、本制度構築方針案本体に記載の「IoTベンダー」という表現に変更することを提案します。	分かりやすい表現の採用、制度構築方針案本体と別添の記載の整合	☆１適合基準では、別途IPAから公開しているETSI EN 303 645の和訳との整合も意識しており、「manufacturer」の和訳として「製造業者」を採用します。一方で、制度構築方針案の「IoT製品ベンダー」に相当する定義であり、用語集の「製造業者」の注記に以下の記載を追加します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映） ・この定義は、「IoT製品に対するセキュリティ適合性評価制度構築方針」における「IoT製品ベンダー」に相当する。
62	M08	M08-036	☆1セキュリティ要件・適合基準	1-2	（NAとなるための条件、基準の補足説明） プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への体制をもつために、パスワードは十分にランダム性を保有しなければならない。	【NAとなるための条件】の根拠として認められるものと認められないものの基準を明確にするか事例を示していただきたい。 【修正案】 【NAとなるための条件】 ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、脅威に対抗するためにユーザ認証が必要ない根拠を記載すること） 必要ない根拠の例. Wi-fi機器の接続において、初回起動時のSSIDのKEYは以下の条件のもとNAとする。 初回起動時、共通のSSIDのKEYを使用し接続するが、物理的なセキュリティを担保した状態（対象機器が持つ入力装置からの有効化および時間的制約がある）であり、正統なユーザ以外がアクセスできないため。	対応方針を決めることができない。 開発には一定の時間がかかるため、事前に対応方針を明確にしていなければ、認証の取得を計画するのが困難である。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
63	M08	M08-037	☆1セキュリティ要件・適合基準	1-3	☆１適合基準 適切な認証に基づくアクセス制御が行われていること。	「適切な認証」の具体的なレベルがわからない。明確化していただきたい。 【修正案】 TCP/UDP通信を介した守るべき情報資産への他の機器又はユーザからのアクセスに対して、ユーザによって定義されたパスワードなどにより適切な認証に基づくアクセス制御が行われていること。	評価の基準が不明確なため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
64	M08	M08-038	☆1セキュリティ要件・適合基準	1-3	TCP/UDP通信を介した守るべき情報資産への他の機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。	「適切な認証に基づくアクセス制御」という表現が曖昧。どういった制御ならOKなのか、具体例を示していただきたい。	全ての通信において、ユーザ認証の上での制御が必要なのか、TLSによる証明書確認による通信機器の正当性確認で良いのか、文章だけでは判断つかないため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
65	M08	M08-039	☆1セキュリティ要件・適合基準	1-3	製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	“ユーザ”の定義は、“自然人もしくは組織”となっているが、そのユーザ定義ではこのパスワード認証というものが何の為のパスワード認証なのか具体的にベストプラクティスを紹介する等でイメージ出来るようにすべき。と考えます。	“ユーザ”の定義は、“自然人もしくは組織”となっているが、そのユーザ定義ではこのパスワード認証というものが何の為のパスワード認証なのか設計する際にイメージしにくい。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
66	M08	M08-040	☆1セキュリティ要件・適合基準	1-4	製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	機器としては、市場でのデバッグ用にSSHのポートをもっておくという事は多いと思います。 このポートのアクセスには開発者しか持ちえないSSH用の秘密鍵を使用して認証を行います（この秘密鍵は全機器共通になると考えます）。 ある検証機関に、EN303645の本項目について確認をとったところ、開発者しか持ちえない共通の秘密鍵をもとに認証を行うことは本項目を満たさないという判断を受けました。 【修正案】 1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。ただし、専らメンテナンスに使用するインタフェースはこれに含まない。	ユーザ認証という言葉の対象としているのが、システム利用者をターゲットにしていると思うのですが、開発者までターゲットにする内容になりますでしょうか？ もし、開発までターゲットにして、SSHの秘密鍵を認証情報としてとらえられたら、こういった開発用デバッグポートについて取り扱いが難しくなるかと思います。 “ユーザ”という言葉の定義をもう少し明確にしておいた方がよいかと考えました。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
67	M08	M08-041	☆1セキュリティ要件・適合基準	1-4	☆１適合基準 機器に対するネットワークを介したユーザ認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。	認証値の変更が可能であることに加え、その変更方法が簡単であることが必要だと思います。 (修正後の文章案) 「その認証値の変更を可能とすること」を「その認証値を簡単な方法で変更できること」とする。	要件1-4に「シンプルなメカニズムを（中略）提供しなければならない」と記載されているため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
68	M08	M08-042	☆1セキュリティ要件・適合基準	1-4	製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	証対象は、製品単品であるのか、サーバーやスマホアプリも含めたシステムとして認証されるのでしょうか。アプリでアカウントを作成する場合は、本項の対象となりますでしょうか。	方針案の図3.2-1を見ると製品単品に見える。関連サービスはどの部分を指すのかわからない。	「サービス(IoT製品ベンダーのサーバ上で稼働するクラウドサービスのようなものを想定)やスマホアプリ」は、それがIoT機器の利用に必要なものである場合、「付随サービス」としてIoT製品の範囲に含みラベル取得することとなります。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
69	M08	M08-043	☆1セキュリティ要件・適合基準	1-5	☆１適合基準1行目、3 制約のある機器	制約のある機器の場合の要件がない。 ※「制約のある機器」についての規制が記されていないため、対象となる機器を「制約のある機器」と騙って規制から逃れる恐れがある。「制約のある機器」についても規制を設けるべきではないか。(例えば、ソフトのアップデートの代わりに分離・交換を行うなど) 【修正案】 3-10（製品において・・・・・）と3-14（製品のモデル名称は・・・）の要件の間に以下の新しい要件を追記 【追記】 ソフトウェアアップデートできない制約のある機器については、製品は分離可能で、ハードウェアは交換可能であることが望ましい。	制約のある機器でない場合については規制をうけるが、制約のある機器の場合規制を受けない形になっています。 それであれば、制約のある機器であるという形に判断する事によって本規約を回避する事ができてしまう。制約のある機器でも最低限実施する事（分離・交換など）を述べて置く必要がある。 EN303645の5.3-15には記載があります。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
70	M08	M08-044	☆1セキュリティ要件・適合基準	1-5	機器が、制約のある機器ではない場合、・・・	用語集で、「制約のある機器」の例の中で、例6でコンセントを使って給電され、・・・ という記載があるが、一般的なIoT対応の家電製品は、例6に当てはまると考える。例6は、どのあたりに「制約がある」ということなのか？	「制約がある」とは思えない例が記載されているため、「制約がある機器」という定義が不明確に感じたため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
71	M08	M08-045	☆1セキュリティ要件・適合基準	3-1	製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	特定のコンポーネントとはセキュリティに関する部分（例：無線モジュール）のソフトウェアをアップデートできればよいという意味か。 家電制御のソフトウェアはアップデートできなくてもよいという認識でよいか。	白物家電においては、ベースの家電機能にアドオンする形で無線モジュールを搭載してIoTを実現している場合が多い。この構成においては、セキュリティは無線モジュールが担っているため。 また、家電機能を制御するマイコンを複数搭載している場合に全てのソフトウェアをアップデートできるとは限らない。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
72	M08	M08-046	☆1セキュリティ要件・適合基準	3-1	製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	最新のファームウェアがインストールされていることはユーザが自ら確認できる必要があるか。	製品に表示できない場合に、メーカに問合せいただき確認することもOKとしたい。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
73	M08	M08-047	☆1セキュリティ要件・適合基準	3-1	製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	製品メーカのシステムに接続されず、他社のシステムに接続して使われる場合（EchonetLiteやMatterなど）はアップデートできないことも考えられるが、OKか。	製品メーカのシステムに接続することでアップデートできればOKでなければ成り立たない。	セキュリティ要件3-1に紐づく☆１評価項目番号＃6の☆１適合基準①では、「アップデートが可能であること」を求めています。 「製品メーカのシステムに接続することでアップデートできればOK」は、アップデートが可能とのことなので、①を満たしていると解釈できます。 「他社のシステムに接続して使われる場合（EchonetLiteやMatterなど）はアップデートできないことも考えられる」については、この文面だけでは①を満たしていないと解釈されます。リスクを低減するために、なにか代替手段がないか等をご確認ください。
74	M08	M08-048	☆1セキュリティ要件・適合基準	3-1	製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	「特定のソフトウェアコンポーネント」とは何か？ また、製品の中には複数のソフトウェア（マイコン）が存在していることがあるが、セキュリティに関与するソフトウェアの更新ができれば良いという形にして欲しい。	アップデートが必要な対象が不明確であり、セキュリティに無関係な全てのソフトウェアが対象となると対応が困難になるため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
75	M08	M08-049	☆1セキュリティ要件・適合基準	3-1,3-7	セキュリティ要件	ソフトウェアコンポーネントをアップデート可能であること(要件3-1)とその方法がセキュアであること(要件3-7)が分けられていますが、これらはセットで1つの要件にすべきだと思います。	偽のファイルでアップデートできてしまうと、そこが却って攻撃の口となってしまうため、アップデート方法がセキュアであることが望ましい。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
76	M08	M08-050	☆1セキュリティ要件・適合基準	3-3	製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。	ユーザが操作せず、自動（強制）アップデートする仕様でもよいか。明確化していただきたい。	セキュリティに関することはユーザに任せるのではなく、メーカ側に強制力があった方がよい。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
77	M08	M08-051	☆1セキュリティ要件・適合基準	3-3	ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすること。	「容易かつ分かりやすい手順」について、事例などを含めてもう少し具体的に記載していただきたい。	自己宣言の場合、評価者によって判断基準が変わりそうなため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
78	M08	M08-052	☆1セキュリティ要件・適合基準	3-7,3-10	☆１適合基準 ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。	完全性のみが記載されていますが、真正性の確認も必要だと思います。 (修正後の文章案) 「ソフトウェアの完全性」を「ソフトウェアの真正性と完全性」とする。	ソフトウェアをセキュアな方法でアップデートすると言った場合、真正性と完全性の両方を検証することが一般的であるため。 また、要件3-10においても真正性が求められているため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
79	M08	M08-053	☆1セキュリティ要件・適合基準	3-7	ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。	「ソフトウェアの完全性をアップデート前に確認できる仕組み」について、事例などを含めてもう少し具体的に記載してほしい。	自己宣言の場合、評価者によって判断基準が変わりそうなため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
80	M08	M08-054	☆1セキュリティ要件・適合基準	3-7	製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。	ベストプラクティスの暗号化技術とは何か。ベストプラクティスの暗号技術リストを明示すべき	ベストプラクティスの参照先を明確にすべき	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
81	M08	M08-055	☆1セキュリティ要件・適合基準	3-8	製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。 製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、セキュリティアップデートの優先度を決定するための方針や指針を文書化すること。 ドキュメント評価：対象とする実機テスト：なし	「適時」とは何を意味しているのか？ 方針や指針を文章化することとなっているが、どういったことを文章かすべきなか？（問題が発生してからアップデートまでにかかる期間など？）を明確にしていただきたい。 また、アップデートはユーザ操作を伴う場合があると思うので、アップデートの実行ではなく、提供が「適時」ということが分かるような記載にしていただきたい。	「適時」の意図が、アップデートの提供タイミングを意味しているのか、実際にアップデートが行われることのタイミングを意味しているか、不明確に感じたため。（自動更新機能がないとNGなのか？）	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
82	M08	M08-056	☆1セキュリティ要件・適合基準	3-8	製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、セキュリティアップデートの優先度を決定するための方針や指針を文書化すること。	これは重要度に応じた緊急アップデート、計画アップデートということか？明確に記載していただきたい。	どのような方針をどのような粒度で書くのか明確ではないため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
83	M08	M08-057	☆1セキュリティ要件・適合基準	4-1	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。	これはデータの保存する際に暗号化することを指しているのか、不正アクセスによって保存してある内容が読めない仕組みがあれば良いかが分かり難い。	要件には、セキュアに保存と記載されているが、基準としては、ネットワーク経由の不正アクセスに言及されており、要件と基準が一致していないように感じたため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
84	M08	M08-058	☆1セキュリティ要件・適合基準	4-1	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。	セキュアに保存とは具体的な手段は何を意味するのか、ベストプラクティスで説明必要と考えます。	ベストプラクティスでイメージ出来るよう詳細事例の記載がない。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
85	M08	M08-059	☆1セキュリティ要件・適合基準	5-1	製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。	ベストプラクティスの暗号技術の定義を考えておく必要があります。具体的にはTLSの暗号スイートなどです。 【修正案】 5-1 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。 使用する暗号技術は、Cryptrecにおいて電子政府推奨暗号リストに含まれるものをサポートする。	EN303645をベースに本項目の検証を依頼したところ、TLSの暗号スイートがCryptorecでは使用可能という判断をした認証機関があった一方で、ianaではno recommendedという内容でNGと判断された事がありました。 暗号技術の定義について考えておかないと、考えがぶれてしまいます。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
86	M08	M08-060	☆1セキュリティ要件・適合基準	6-1	要件： すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。 基準： 製品において、外部からサイバー攻撃を受けるリスクを低減するために、製品の利用上不要かつ攻撃を受けるリスクがある物理的インタフェース及び論理的インタフェースを無効化するとともに、製品に対する脆弱性検査を実施すること	外部からのサイバー攻撃を受けるリスクを低減するためという記載があるため、外部に露出していないデバッグポートに対する、製品の改造を伴う直接的な攻撃については対象外と認識しているが、これが分かるような記載にして欲しい。	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性の欄には、デバッグポートの記載があるが、基準としては、製品として公開している端子のみが対象という記載になっており、対策範囲が不明確に感じたため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
87	M08	M08-061	☆1セキュリティ要件・適合基準	11-1	セキュリティ要件 ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。	ユーザを主語にすると、ユーザに対する責務に見える。 (修正後の文章案) 要件17-2等に合わせて製造業者を主語とし、「製造業者は、簡単な方法で製品からユーザデータを消去できるような機能をユーザに提供しなければならない」に変更する。	ユーザを主語にすると、ユーザに対する責務に見える。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
88	M08	M08-062	☆1セキュリティ要件・適合基準	11-1	① ユーザによって、機器本体や関連サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下のデータを削除できること。 A) 製品利用中に取得した情報資産（個人情報含む） B) ユーザ設定値 C) ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名	データの削除が、実際のIoT機器に保存しているデータなのか、サーバー上にあるストレージまで含めているのか分かり難い。また、製品利用中に取得した情報資産が何を意味しているのか、明確にすべき。と考える。	データの削除対象が不明確に感じました。削除対象として、個人情報は理解できますが、通信ログや過去の動作情報などを遡って削除するのはかなり難しい。個人情報を削除することでデータのヒモ付けが失われるため、削除情報を絞り込みたい。また、そのことを明確にして欲しい。	☆１適合基準に記載のとおり、「製品のストレージに保存されたデータ」が対象であり、「IoT製品のストレージ」という意味です。 それは、申請者がラベル取得する「IoT製品」がどの範囲になるかにもよります。付随サービスがなく「IoT機器」がラベル取得範囲となる場合は、「IoT機器の内蔵ストレージ」という解釈になります。一方で、外部ストレージが付随サービスとなる場合は、当該外部ストレージまで含め「IoT製品」となり、評価の対象となります。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
89	M08	M08-063	☆1セキュリティ要件・適合基準	11-1	☆１適合基準 製品利用中に製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。(以下略)	データを削除できることに加え、その方法が簡単であることが必要だと考えます。 (修正後の文章案) 「以下の①・②のすべての基準を満たすこと」を「以下の①・②・③のすべての基準を満たすこと」とし、末尾に「③簡単な方法としてユーザに提供されること。」を追加する。	要件11-1に「簡単な方法で」と記載されているため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
90	M08	M08-064	☆1セキュリティ要件・適合基準	17-2	製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。	提供方法としてはWEBのユーザマニュアルで問題無いのか。事例や事例集を公表していただきたい。	提供方法を明確にして欲しい	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
91	M08	M08-065	☆1セキュリティ要件・適合基準	17-2	製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。	セキュアな廃棄方法を具体化していただきたい。	家電製品は家電リサイクル法に基づいて業者によって廃棄されるなど、廃棄方法が限定されるため、その辺も考慮した上で決めてほしい	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
92	M08	M08-066	☆1セキュリティ要件・適合基準	17-5	製造業者は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。	「指定された方法」とは、どのように指定されたものか不明確なため「適合基準に指定された方法」への修正を提案します。	明確化していただきたい。	3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
93	M08	M08-067	☆1セキュリティ要件・適合基準	17-10	製造業者は、セキュリティリスクを引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。	「指定された方法」とは、どのように指定されたものか不明確なため「適合基準に指定された方法」への修正を提案します。	明確化していただきたい。	3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
94	M09	M09-001	制度構築方針案	3.3.	関係性イメージ図	本制度におけるセキュリティ要件のカバレッジはIEC62443, EU-CRAと同等以上と読み取れます。本制度の認証を取得すれば欧州で上市出来るような相互承認(P4「2.目的と位置付け」目的③)が得られるようにしていただきたい。 (逆も同様でIEC62443の認証を取得すれば本制度の認証が申請のみで付与されることも必要です。)	少しずつ要件の範囲が異なる各国のセキュリティ要件個々に対応させるには必要以上に時間、費用がかかります。	既に一部の協議は開始していますが、EUのCRAも含め、諸外国とは積極的に連携し、最終的には相互承認を確立する方針で検討を進めています。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
95	M09	M09-002	制度構築方針案	3.3.	表3.3.-1	☆3は想定した製品の記載があるため、☆1と☆2の記載も合わせて頂き、違いを明確にしていただきたいです。	☆1と☆2の評価基準が異なることはわかりますが、どのような製品がどちらを取得しているのがいいのか、混乱しないか懸念しています。	☆２以上は、対象となる製品類型の定義に合致するIoT製品のみ取得可能となります。☆２以上が整備された製品類型以外のIoT製品は、☆１のみしか取得することはできません。 ☆２以上を整備予定の製品類型においては、各レベルで想定するユースケースや脅威を定め、基準を検討し、公開する予定です。それらの情報を参考に、調達者が、例えば☆１と☆２の何れを求めるかを決定し、調達要件に含めていくこととなります。
96	M09	M09-003	制度構築方針案	3.5.	図 3.5-1 ②、③、④のフロー ※自己適合宣言でもIPAへ申請し、IPAよりラベルが付与される流れ。	IPAへの申請対象は第三者認証の製品のみにできないか検討いただきたい。	欧州CEマーキングでは、自己宣言する際は欧州当局へCEマーク使用の申請(使用許可を貰う事)はしておらず、IoT製品ベンダーの判断の下、エビデンス資料を整備の上でCEマークを表示している。 自己宣言の製品まで申請の対象とすると、申請量が膨大となることが予想され、申請からラベル付与までに多くの期間を要することになり、IoT製品ベンダーの円滑な製品の市場投入の妨げになる。	自己適合宣言であっても、問合せ先情報の確認、ぜい弱性情報の集約や早期警戒パートナーシップ等のぜい弱性対応の促進、サプライチェーン・リスクの考慮など、セキュリティ要件以外の視点での活用も想定しているため、IPAによる申請受付・ラベル付与のスキームとします。
97	M09	M09-004	制度構築方針案	3.7.	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。	付与されるラベルには有効期限があるとの事だが、更新手続き(再申請)の手続きを簡略化いただきたいです。	ラベルの有効期限：2年はIoT製品ベンダーにとって短い期間です。有効期間延長のためには再申請が必要とのことですが、再申請手続き作業のためだけにマンパワーを割くことになり、本来の製品開発・円滑な市場供給の妨げになると予想されます。再申請は最低限の作業としていただきたいです。	チェックリストによる自己適合という簡易な申請という形式上、☆１、☆２の有効期限は最大２年間とし、それを超える長期間の有効期間を与えることは想定していません。２年以内であれば、申請者が有効期限を設定できるようにする予定であり、ある程度更新時期を合わせていただくことは可能かと思います。 複数製品をまとめて手続できるようにすることなどは今後考慮します。
98	M09	M09-005	制度構築方針案	3.7.	☆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。	ラベルの有効期限が2年と短いです。他国の法令(例：EAC)に倣い、有効期限を5年等に設定していただきたいです。	多くの製品がラインナップされている場合、ラベルの有効期限が短いと有効期限及び再申請手続きの管理でマンパワーを割かれることが予想されます。	諸外国の制度との比較及び制度開始当初の☆１では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から、☆１の有効期限の設定は、最大２年とすることが妥当と考えています。 (参考)第7回検討会資料　資料4 P.14 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.html
99	M09	M09-006	制度構築方針案	3.7.	☆1、☆2の有効期限はラベル取得日から最大2年間とし、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	製品のファームウェアやハードウェアの変更で、ラベル再取得が必要な場合と再取得が不要な場合を明確に定義して頂きたいです。	海外の規格の定期更新に加えて、国内の規格でも定期更新が必要になると、費用面・工数面で増大することを懸念しています。	製品のファームウェアやハードウェアの変更が「評価に影響を与えるレベルでの製品仕様の変更」に該当するか否かが判断基準となります。 詳細については、別途、申請ガイドなどを用意する予定です。
100	M09	M09-007	制度構築方針案	3.8.3.	国際連携のあり方を検討する 。	FA分野では、IEC 62443-4-2 の認証を取得する製品も出てきています。同認証を取得済みの製品に対しては、同認証書をもって今回の適合性を評価できるようにしていただきたいです。	機器を開発するベンダーにとっては、同じような認証を何度も実施することになり、費用面・工数面で増大することを懸念しています。	相互承認を行わない認証制度等について、特に基準や評価ガイドに明記されている場合を除き、当該認証を取得していることをもって本制度の基準に適合することとはしませんが、当該認証を取得する際に実施した検証結果等を利活用することは認めることを検討しています。
101	M09	M09-008	☆1セキュリティ要件・適合基準	用語集		「ネットワーク」の定義を追記頂けないでしょうか。	方針案などでもインターネットやネットワークが使い分けられている印象ですが、適合基準は、ネットワークで記載が統一されているように見えました。今回の対象はIPを使用したデータ送受信を対象とされているため、明確にしたほうが良いかと思いました。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。 なお、参考としたETSI EN 303 645には、「1.適用範囲」に「ネットワークインフラ（インターネットやホームネットワークなど）に接続される民生用IoT機器と、～」という記載があります。 本制度は、民生用に限定しないため、それらに加え、WANや社内LAN等も含んだ一般的用語として使用しています。 制度構築方針案の3.2.では、「インターネット」と書き分ける形で「ネットワーク」と使用しており、本節では「インターネット以外のネットワーク」と解釈してください。
102	M10	M10-001	制度構築方針案	2.2.	自主的アプローチ	我々は、IoTラベリングスキーム案を自主的なスキームとして策定するという経済産業省のアプローチを称賛する。自主的なスキームにより、最もサイバーセキュアなIoTベンダーは、自社製品の強化されたサイバー回復力を示すことで、他ベンダーとの差別化を図ることができる。IoTベンダーは、消費者が購入するIoT製品のサイバーセキュリティへの配慮を求めるレベルが高まるにつれ、競争力を維持するためにこのスキームを選択することが増えるだろう。最終的には、義務的なラベル付けをしなくても、サイバーセキュリティの水準を高めることができるようになる。 強制的なラベリング制度は、技術開発へのアクセスを遅らせる認証のバックログを生み出すという意図せざる結果をもたらす。		制度構築方針案への賛同の御意見として承りました。
103	M10	M10-002	制度構築方針案	3.8.3.	相互運用性	我々は、IoT製品に対するセキュリティ適合性評価制度構築方針案草案（仮英訳）から、IoTラベリングスキーム草案が、ETSI EN 303 645や、シンガポールのサイバーセキュリティラベリングスキーム（シンガポールCLS）、米国のサイバートラストマーク、英国の製品セキュリティ及び電気通信インフラ（関連する接続可能な製品に対するセキュリティ要件）規則、EUのサイバーレジリエンス法などの既存のラベリングスキームを参考にして策定されたと理解している。 我々は、既存のラベリング制度との相互承認に向けた日本政府の取り組みを称賛する。これは、サイバーセキュリティ基準の世界的な相互運用性を促進するものである。コネクティビティ・スタンダード・アライアンス（CSA）とシンガポール CSA はこのほど相互承認取決め（MRA）に調印し、民生用 IoT 機器に対す るそれぞれのサイバーセキュリティ・ラベルの承認に向けた取り組みを強化した。このMRAは、世界的な協力を促進し、規格の調和を進め、製造業者にとって重複する試験手順とコストを削減し、地理的な境界を越えて消費者向けIoTのセキュリティを向上させることを目的とした協働協議の成果です。 https://csa-iot.org/newsroom/the-connectivity-standards-alliance-and-the-cyber-security-agency-of-singapore-sign-mutual-recognition-arrangement-on-cybersecurity-labels-for-consumer-iot/		制度構築方針案への賛同の御意見として承りました。
104	M11	M11-001	制度構築方針案	3.5.	P14文章 下から４行目からの部分	「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。」とあるが、☆２については☆１を取得した機器同士をつなげてサービスを提供する「サービス事業者」も対象とすべき。	例えばスマートホームサービスを提供する事業者は、機器同士が安全に接続してサービスを提供する必要がある。機器が☆１を満たしていても、相手認証や通信内容の暗号化など必要な機能を装備し、かつデータ管理や処理に対する責任も発生する。このため☆２はIoT製品ベンダーというより、「サービス提供事業者」とするのが正しい。 CCDS製品分野別サーティフィケーションプログラム☆☆スマートホーム編ガイドライン CCDS製品分野別セキュリティガイドライン_スマートホーム編_Ver.1.0 https://www.ccds.or.jp/public/document/other/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E3%82%B9%E3%83%9E%E3%83%BC%E3%83%88%E3%83%9B%E3%83%BC%E3%83%A0%E7%B7%A8_Ver.1.0_2.pdf	3.2.に記載のとおり、本制度の対象は、IoT製品（IoT機器に付随サービスを含めたもの）となります。 IoT製品を組み合わせて提供されるシステムやサービスにおいてもセキュリティの考慮は必要となりますが、3.8.2.に記載のとおり、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認証制度等の検討は、本制度の直接の対象とはせず、本制度の活用も含めて連携しながら、各業界団体やワーキンググループで別途検討する想定です。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
105	M11	M11-002	制度構築方針案	3.5.	P15の文章 上から１行目から２行目にかけての箇所	「☆3 以上は政府機関等や重要インフラ事業者での活用を想定しており、高い信頼性が求められるため、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。」とあるが、☆３以上の対象を「政府機関等や重要インフラ事業者」に限定するのは如何なものかと。民間企業でも高い信頼性が求められるサービスを提供する場合、☆２より高度な施策が必要と考える。	民間企業でも生命や財産にリスクを及ぼすサービスを提供する場合、☆２以上の対策をすべき。 修正案 「高い信頼性が求められる機能やサービスを提供する事業者は、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。」 CCDS製品分野別サーティフィケーションプログラム☆☆スマートホーム編ガイドライン CCDS製品分野別セキュリティガイドライン_スマートホーム編_Ver.1.0 https://www.ccds.or.jp/public/document/other/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E3%82%B9%E3%83%9E%E3%83%BC%E3%83%88%E3%83%9B%E3%83%BC%E3%83%A0%E7%B7%A8_Ver.1.0_2.pdf	2.3.や3.3.に記載のとおり☆３以上の初期ターゲットを意識した記載としていました。政府機関等と重要インフラ事業者に限っての活用ではないため、いただいた意見を参考に、以下のとおり見直します。 「☆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（以下略）」とします。
106	M11	M11-003	制度構築方針案	全般		随所に「IoT製品ベンダー」と記載があるが、対象者はサービス提供する事業者も対象とすべき。	読む人によっては「製品」を扱っている企業が対象のように取ってしまう可能性がある。また同じ理由で「ベンダー」も違和感がある。 修正案として「IoT製品ベンダーおよびサービス提供事業者」とするか、IoT製品ベンダーの言葉の定義を冒頭で記載するべき。	「1.はじめに」にて、「IoT製品ベンダー」は「IoT製品を製造又は販売するベンダー」と定義しています。 「サービス提供する事業者」がどのような事業者を指すのか次第ですが、「IoT製品を組み込んだサービスを提供する事業者」という意味合いであれば、IoT製品をサービスに組み込んで販売していることとなるため、本定義の対象に含まれると解釈でき、当該事業者がラベル申請することを否定しているものではありません。
107	M11	M11-004	制度構築方針案	3.8.2.		本制度が業界団体やワーキンググループと連携し、IoT製品に対するセキュリティ要件の検討を行い、認証制度として整備されること、特に検討優先度の高い「特定分野のシステム」として、スマートホームシステム、ビルシステム、工場システム、電力システム等を候補としていることに賛成いたします。これにより、消費者がより安心してIoT製品を利用できるようになります。	本制度の☆2以降のセキュリティ要件を、IoT製品を選定する立場の事業者、又は製造ベンダーから、一定割合以上の賛同が得られる場合としています。これにより、一部の事業者又は製造ベンダーに偏らず、消費者が利用する様々な製品のセキュリティ対応状況を反映することができるとともに、市場への高いセキュリティ製品の浸透を妨げることなく推進を行うことができると考えます。	制度構築方針案への賛同の御意見として承りました。
108	M11	M11-005	制度構築方針案	4.1.		ラベル取得促進策として、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検討に賛成致します。IoT製品を選定する立場の事業者、又は製造ベンダーが抱える開発コストの問題を軽減することができ、IoT製品を選定する立場の事業者の採用を進めることができます。さらに消費者により高いセキュリティ要件に対応した製品を提供することができます。	IoT製品ベンダーが、セキュリティ要件に関する十分な知識を持っていない場合、開発費の増大により、その製品の市場への導入やセキュリティ強化の取り組みが遅れることがあります。しかし、適合性評価制度に加えて、補助金制度を提供することにより、中小企業を含む幅広い製造ベンダーがこの制度を利用することができます。	制度構築方針案への賛同の御意見として承りました。
109	M11	M11-006	制度構築方針案	4.2.		ラベル付与製品の積極的な導入促進に向けて、調達者又は利用者に対して、セキュリティリスクとラベルの意味、ラベル付与製品のメリット、購入後に利用者が実施すべき啓発の実施に賛成いたします。サイバーセキュリティ犯罪を防ぎ、安心して便利・有用な技術を享受するために、起こりうる危険と防ぐ方法を啓発することは、調達者や利用者の利益を守るために非常に重要です。	ラベル制度の設立と普及促進策、調達者・利用者が自らを守るための方法を啓発することを同時に行うことにより、目的を実現することができると考えます。	制度構築方針案への賛同の御意見として承りました。
110	M12	M12-001	制度構築方針案	2.1.		制度を適用しない製品の販売や利用により何らかの法的ペナルティを与える、もしくは法的に不利になることがある、と想定しているのか。	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。	義務制度ではないため、ラベルを取得していない製品を購入・利用することに対して法的なペナルティを課す想定はありません。
111	M12	M12-002	制度構築方針案	3.2.		産業用機器（工作機械やロボットなど）等は、社内の工場ネットワークには接続されているが、インターネットとは隔離されているケースもあると考える。その場合、ネットワークには接続されていてもインターネット接続が想定されなく、本制度の対象外製品としてほしい。 また、ユーザー企業によって、インターネット接続を行ったり、クローズドネットワークとしてIoT機器を利用したりとまちまちではないかと推測する。ユーザーの利用シーンまでを想定して、IoT機器の製造事業者は対処（本制度対応要否判断）できないと考える。製品機能要件として本制度対象としても、実態としてユーザー企業がインターネット接続しなければファームウェアのアップデートなどもできない。その点について、何らかの補足追記をお願いしたい。		本制度は任意制度であり、「対象機器」の意味合いは、「ラベル取得が求められ得る機器」ではなく、「ラベル取得が可能な機器」となります。その観点で、利用が主にインターネットから隔離されたネットワークであっても、「ラベル取得を不可」とする理由はなく対象とします。ローカルネットワークや制御系ネットワークであっても、何かしら外部と接続されており、サイバー攻撃を受ける事案が発生している以上、それだけで機器のセキュリティ対策が不要な理由にはならないと考えています。 また、工場システムに関しては、3.8.2.に記載のとおり、業界団体等と連携して、システム全体のセキュリティの検討と、そこからどのような機器にどのレベルのセキュリティを求めるかを検討する予定です。
112	M12	M12-003	制度構築方針案	3.2.		IoT機器は、単体でIoT機器であるもの（ホームルータやIPカメラなど）と他の機器に組み込まれて稼働するIoT機器（医療機器、工作機械など）がある。後者の場合、ラベル表示は組み込まれたIoT機器に表示できない場合がある。その場合、工作機械側にラベル表示することになるかどうか、記載をお願いしたい。		3.7.に記載のとおり、ラベルの表示は任意となります。そのため、例示いただいた他の機器に組み込まれて稼働するIoT機器においてラベル表示できない場合は、本体へのラベル表示の必要はありません。 もし、ラベル取得のアピールとしてラベル表示を希望される場合は、組み込まれる本体側に、ラベル取得している範囲を明記した上でラベル表示する方法が考えられますが、詳細な運用や条件は制度開始までに検討します。
113	M12	M12-004	制度構築方針案	3.2.		本制度の対象機器について、エンドユーザーからみた場合、ラベルが必要なのに付与されていないのか、それとも対象外なのかは判断が難しい。「ラベル対象外」のマーク付与も考えていただきたい。あるいは、☆1も出来ていないIoT機器は「☆ゼロ」のマーク表示を義務化するなどを検討いただきたい。		本制度は任意制度であり、「ラベルが必要」や「マーク表示を義務化」等の考え自体が該当しません。 調達者が「ラベル取得製品」を必要と考えた際に、それを求めることとなります。ラベル取得製品は、別途構築する本制度のWebサイトにて検索可能とするため、仮にラベルを本体等に貼り付けていなくても、調達者が調べることを可能とする予定です。
114	M12	M12-005	制度構築方針案	3.3.	表3.3-1	IoT製品類型は具体的に定義すべきと考える。	IoT製品の利用については製造業者の想定と異なることが考えられるため。	☆２以上を整備予定の製品類型の対象や、どのようなセキュリティ水準の製品を☆２以上として想定するのかの方針等の情報を早期に公開するようにします。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
115	M12	M12-006	制度構築方針案	3.5.		疑義に対する証跡の提出は、製造ベンダーの一存ではできない場合もあるため、そのケースについての対応を記載してほしい。	証跡については、ステークホルダーである顧客、通信事業者などの都合もあり、ベンダーの一存で提供できない可能性もある。	3.7.に記載のとおり、スキームオーナー（IPA）の判断により、基準への適合に疑義が生じた場合に、評価に使用した証跡の提出を求めることがあります。 「ステークホルダーである顧客、通信事業者などの都合」との懸念点ですが、例えば、当該IoT製品を利用して特定顧客でインシデントが発生し、それをきっかけに調査を行う場合、本制度としては、そのインシデント自体の調査ではなく、当該IoT製品が適合基準を満たしているかの調査となります。求める証跡は、あくまで評価時点のものとなるため、一般的に当該顧客の了承が必要とは想定されません。 または、特定顧客の示したセキュリティ仕様に従ったIoT製品を開発し、その製品でラベルを取得する場合、評価証跡に当該顧客の秘密情報やナレッジ等が含まれることが想定されます。その場合は、ラベル取得の要否や、取得する場合にスキームオーナー（IPA）に開示可能な証跡の範囲を当該顧客と事前に協議した上で、取得の判断を実施してください。
116	M12	M12-007	制度構築方針案	3.7.		たとえばホームルータなどを店舗に陳列する際に「ラベルの有効期限」が迫ったものを陳列することを店舗の経営者などがためらう恐れがある。食品の賞味期限とは異なる制度であり、「ラベルの有効期限」が迫っている又は更新された場合、市場に既に投入したホームルータ等の機器に張り付けた有効期限の更新について明確なルール形成をお願いしたい。たとえば、シールを店舗の経営者側で張り替える、QRコードで読み込むとポータルサイトでは有効期日が更新されている旨が表示されるなど。この際、後者の場合、物理的に目につく有効期限（例：表示自体は有効期限切れだが、実際は有効期限の更新は済んでいるケース）のラベル表示がきっかけとなり、該当製品を販売事業者が販売しない、エンドユーザーが購入しなくならないようなルール形成をお願いしたい。		有効期限はラベルには掲載せず、QRコードを読み取った先の情報提供ページにて最新の情報を確認いただく想定です。
117	M12	M12-008	制度構築方針案	3.7.		出荷装置への認証ラベルの有効期限は装置ベンダーでの製造タイミングとリンクすることを明記してほしい。エンドユーザーの手元に届くタイミングでの話とは解釈しないようにしてほしい。		有効期限はラベルには掲載せず、QRコードを読み取った先の情報提供ページにて最新の情報を確認いただく想定です。 3.7.の3段落目に記載のとおり、ラベル失効後も意図的にラベルを貼り付けた製品を出荷し続けることは禁止しますが、有効期限切れのタイミングで、既に出荷（製造開始）済みの製品のラベル取り外しまで求める予定はありません。ラベルの有効期限、継続申請をするか否か、製品製造開始のタイミング、その製品の出荷予定等を加味し、判断してください。
118	M12	M12-009	制度構築方針案	3.7.	表3.7-1	製品のバージョン情報なども必要と考える。	既出荷中の製品に対し適合性評価を実施した場合を考慮のため。	バージョン情報を入れることを含めて検討します。
119	M12	M12-010	制度構築方針案	3.7.	表3.7-1	「当該製品に関わる脆弱性情報」とは、例えばCVEなどに一般公開された既知の脆弱性情報でよいのか、それとも製品の使用方法によってはセキュリティ上脆弱になり得る場合もあるため、その注意喚起をすることになるのか。		両方を含みます。なお、制度開始時点では、ラベル申請者又はIoT製品の製造ベンダーからの申告をベースとすることを想定しています。
120	M12	M12-011	制度構築方針案	3.7.		☆２以上では定期的なサーベイランスが行われると理解したが、2年の有効期間中にどのような頻度で行うことを想定しているのか、サーベイランスで実行することは何か例示してほしい。	コストの観点で☆１は定期的なサーベイランス実施見送りと理解。☆２でも同等で良いのではないか。	現時点では☆１に対して定期的なサーベイランスを実施しないという方針までであり、☆２以上で定期的なサーベイランスを行うか否かは未定となります。
121	M12	M12-012	制度構築方針案	3.7.		それぞれ猶予期間とはどの程度の期間か例示してほしい。	最大1年程度と想定するが、内容により猶予期間が決まるのか。	猶予期間（移行期間）については半年程度以上は確保することを想定しています。
122	M12	M12-013	制度構築方針案	3.8.3.		諸外国の制度にて認定された製品を輸入する場合、国内制度と同等の扱いとしてラベル貼付は可能であることが望ましいと考える。	輸入品の扱いが表現されていないと思われたため	今後の交渉次第ではありますが、相互承認が実現した制度とは、一方の制度でラベル・認証を得れば、もう一方の制度でもラベル・認証を受けたものとみなす（本制度のどの☆レベルかは調整次第）ことを想定しています。 なお、相互承認が実現した場合のラベル貼付等の取り扱いは、相互承認の協定次第となります。
123	M12	M12-014	☆1セキュリティ要件・適合基準	1-2		文字種類によって同じ6，8文字でもパスワードの複雑さは変わってくる。パスワードの複雑さを表す指標を入れたほうが良いと考える。		いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
124	M12	M12-015	☆1セキュリティ要件・適合基準	1-2,1-3,1-5		以下のようなN/Aとなるための条件が必要と考える 【N/Aとなるための条件】 ・脅威に対抗するために、システムまたは人的にセキュリティ対策を設けることでユーザー認証が必要ない根拠を記載することでNAと判定可能 ・リスク軽減策をとっていることをユーザーマニュアルに明記されていること 例①：本製品(IOT機器)は閉域網運用が前提条件としており、IOT機器を管理するサーバからのみアクセスが可能な仕組みを設けている。管理サーバ ログイン時の認証で評価項目番号＃2の適合基準を満たす仕組みがある。 例②：専用治具を接続しない限りアクセスができない仕組みを設けている。	評価方針として、☆１評価のハードルを可能な限り下げると記載があったため、対応する脅威の発生頻度によっては、装置単体ではなくシステムまたは人的対応でセキュリティ対策を行い、リスク軽減をすることで明確な理由があればNA判定可能にするのはありと考えたため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
125	M12	M12-016	☆1セキュリティ要件・適合基準	1-3,3-1,9-1		なぜいくつかの項目だけ技適[T][A] の対象とするか理由が不明。これらだけ守れていても、ユーザー目線、装置選定社目線では価値がないと考える。		技適認定製品の場合に、相当する本制度の一部の適合基準を満たしていると判断することとしています。 技適認定を受けている製品であっても、それら以外の基準への適合は評価する必要があります。
126	M12	M12-017	☆1セキュリティ要件・適合基準	1-5		具体的に総当たり攻撃を回避する手段の例示をしたほうがよい。	自己認証のため、解釈の差が生じそうなポイントと思われる。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
127	M12	M12-018	☆1セキュリティ要件・適合基準	1.		カテゴリ「1. 汎用のデフォルトパスワードを使用しない」に以下のような要件追加が必要と考える ①バックドアのない設計にする ②安易にパスワードを初期化できない設計にする	①生産用、保守用、調査用等、ユーザーの知らないアクセス手段が実装されていると、その認証情報が漏えいしたとたん、ユーザーが知り得ない形で悪意の侵入を許してしまう。その場合、検知が遅れ、被害は拡大しやすいため ②パスワードが容易にリセットできると、初期パスワード対策を行っていても、新たなパスワードが設定され、悪用を許してしまうため特に遠隔では簡単にはできない仕組みが必要と考える	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
128	M12	M12-019	☆1セキュリティ要件・適合基準	3-3		ユーザー操作させない方法もOKとするように明記してほしい。	自己認証のため、解釈の差が生じそうなポイントと思われる。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
129	M12	M12-020	☆1セキュリティ要件・適合基準	3-3,3-7		以下のようなN/Aとなるための条件が必要と考える 【N/Aとなるための条件】 ・脅威に対抗するために、システムまたは人的にセキュリティ対策を設けることでユーザー認証が必要ない根拠を記載することでNAと判定可能 ・リスク軽減策をとっていることをユーザーマニュアルに明記されていること	評価方針として、☆１評価のハードルを可能な限り下げると記載があったため、対応する脅威の発生頻度によっては、装置単体ではなくシステムまたは人的対応でセキュリティ対策を行い、リスク軽減をすることで明確な理由があればNA判定可能にするのはありと考えたため	「脅威に対抗するために、システムまたは人的にセキュリティ対策を設ける」ことで、装置単体(IoT製品)に求めるセキュリティ要件を下げることは合理的ですが、それを判断するのは調達者となります。その判断に使用するため、☆４～☆１というラベルを本制度にて提供することとなります。 「リスク軽減策をとっていること」で適合基準相当のセキュリティ対策がなされていると判断できると考える場合、具体例をお示しください。
130	M12	M12-021	☆1セキュリティ要件・適合基準	3-7,5-1		ベストプラクティスな暗号化技術を具体的に定義、例示してほしい。	自己認証のため、解釈の差が生じそうなポイントと思われる。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
131	M12	M12-022	☆1セキュリティ要件・適合基準	4-1		セキュアに保存するレベルがいろいろ考えられる。明確に定義したほうがよいと考える	自己認証のため、解釈の差が生じそうなポイントと思われる。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
132	M12	M12-023	☆1セキュリティ要件・適合基準	5-1		「ネットワークを介して」は、LAN，WAN両方含むということか。LAN環境での盗聴対策の必須化はやりすぎと考える。	LAN環境に存在するリソースpoorなIoT機器と通信するケースがあると、それらの機器と通信する機器全てがNGとなる。	「ネットワークを介して」は、LAN環境も含む定義です。 なお、本制度の最終とりまとめの別添2として別途公開している「☆１評価ガイド」において、①-A(通信の暗号化)に加え、①-Bと②に該当すれば本評価項目はOKとなります。
133	M12	M12-024	☆1セキュリティ要件・適合基準	5-7		「リモートアクセス可能な」とあるが，リモートアクセスの定義は、インターネットからのアクセスか、それともローカルアクセスを含むかを明確にしてほしい。		「用語集」に記載しているとおり、「リモートアクセス可能」とは、「ローカルネットワークの外部からアクセスできるよう意図されている。」ことを意味します。よって、ローカルネットワーク内のアクセスは含まれません。
134	M12	M12-025	☆1セキュリティ要件・適合基準	6-1		不要なインターフェースの無効化に「TCP/UDPポート」とある。これはLANの物理的なインターフェースポートとの理解でよいか。それともTCP/UDPの論理的なポートすべてか。他に例示されているインターフェースとしてBluetooth，USBとあり、物理的または論理的インターフェースのことを指しているのか内容が混在しているように思える。		いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
135	M12	M12-026	☆1セキュリティ要件・適合基準	6-1		対象とするインターフェースにLAN，無線LANインターフェースは含まずとした方がよいと考える。	もし上記インターフェースが含まれるとなると、相当にユーザーの利便性を損なうものとなる。インターフェース接続がない場合に自動的にOFFにする要件を含むかなど、あいまいにもなる。	「ユーザーの利便性を損なう」ということは、製品の利用上必要なものと解釈され、それは無効化を求められる対象とはならないと考えます。 例えば、通常は有線LANでの利用を想定しているが、無線LANの機能も搭載されているような製品の場合、無線LANはデフォルトでは無効化しておく等が想定されるので、一律で含まないとはいえません。
136	M12	M12-027	☆1セキュリティ要件・適合基準	9-1		ファームウェアupdate中の電源断は想定していないと理解する。ファームウェアアップデート中の電源断は対象外としてほしい。	ファームウェアupdate中の電源断で装置が起動不能になっても、セキュリティ上支障があるわけではなく、本基準の主旨から少し外れていると考える。 また、ファームウェアupdate中の電源断に対しての考え方は、製品の性質により考え方が変わる。flashROMなどの不揮発性領域がファームウェアに大した倍のサイズを要求されるので、コストに直結する。一方、SEがバージョンアップするような装置の場合、必ずしも本対策は必要としない。製品の位置づけや状況に応じて判断されるべき内容である。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
137	M12	M12-028	☆1セキュリティ要件・適合基準	11-1		②を必須とすると、ファームアップデートにクライアント証明書の認証を要求するポリシが実現できなくなるので、②の要件は削除したほうがよいのではと考える。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
138	M12	M12-029	☆1セキュリティ要件・適合基準	4-1		以下のようなN/Aとなるための条件が必要と考える 【N/Aとなるための条件】 ・守るべき情報資産を保持していない。 ・守るべき情報資産にネットワーク経由でアクセスができない。 ・脅威に対抗するために、システムまたは人的にセキュリティ対策を設けることでユーザー認証が必要ない根拠を記載することでNAと判定可能 ・リスク軽減策をとっていることをユーザーマニュアルに明記されていること	4-1にN/Aとなる条件が掲載されていないため	【N/Aとなるための条件】の2点目～4点目は、N/Aではなく、なにかしら対策を実施しているものと思われますので、その点を評価ガイドに従って評価してください。 1点目は、「守るべき情報資産」として定義されている「通信機能に関する設定情報」や「セキュリティ機能に関する設定情報」を一切保持していないIoT製品は想定できないため、N/A条件は設定していません。 なお、参考としたETSI EN 303 645においても、5.4-1は、「M：規定は必須要件である。」とされており、「M C：規定は必須要件であり、かつ条件付きである。」とはなっていません。
139	M12	M12-030	☆1セキュリティ要件・適合基準	4-1		用語の定義の「通信機能に関する設定情報」について、人によって解釈が異なることが想定されるため、齟齬を減らす意味でも、具体例を追加したほうが良いと考える。		いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
140	M12	M12-031	☆1セキュリティ要件・適合基準	4.		カテゴリ「4. 機密セキュリティパラメータをセキュアに保存する」に以下のような要件追加が必要と考える ①不正に機密データアクセスするルートが排除されている ②証跡を得るための仕組みを持っている	①機密データへのアクセス方法を漏れなく明らかにしておかないと、過失（プログラムミス、誤操作等）または不正（バックドアからの侵入、脆弱性を突く攻撃等）により被害が発生する可能性があるため ②脅威：否認防止の対策として機密データアクセスのログを残す対応が必要と考える	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
141	M12	M12-032	☆1セキュリティ要件・適合基準	全般		物理的なセキュリティ対策が必要ではないか。	要件として、製品の盗難対策や物理的不正操作への対処項目がないため。守るべき情報資産の有無、製品特性に依存する点も多いので☆１ではなく、☆２以上での要件として定義されるのも良いかと考える。	盗難対策や物理的不正操作等の物理的なセキュリティ対策が求められる脅威は、☆１の想定には含めておりません。各製品類型ごとの☆２以上の検討で考慮します。
142	M12	M12-033	制度構築方針案	全般		適合評価認証された装置に、適合上の瑕疵が見つかった場合は、ユーザーへの周知を実施後ファームウェアのアップデートを公開する等で対処すればよいことを明記してほしい。		評価時点の適合基準を満たしている場合は、ラベルが発行されます。その後の「適合上の瑕疵」がどのようなもので、どのような理由により生じたのかにより、ラベル継続可否の判断は変わってきますので、個別にご相談ください。 基本的には、出荷段階の製品において、適合基準を満たしていることを求めているため、「ファームウェアアップデートをしないと適合基準を満たさない製品」にラベルを付与することはできません。その段階で、「アップデート後のファームウェアで出荷される製品モデル」のみをラベル取得対象としつつ、旧モデル(ファームウェアアップデート前のモデル)に関しては、情報提供ページにて「ファームウェアをアップデートすることでラベル取得相当になること」を周知いただくことになるかと思います。 なお、3.7.に関連する記載があるとおり、ラベル失効後に出荷予定の製品や適合基準を満たしていない製品に対して、故意に物理的なラベルを貼り付けることは許容できませんが、それがやむを得ない事情の場合、製品の回収やラベルの取り外し/貼り替え等を求める予定はありません。
143	M12	M12-034	制度構築方針案	全般		適合性評価制度の認証マークのサイズは、小さく表示可能としてほしい。	IoT機器によっては、表示スペースがあまりない	3.7.に記載のとおり、小型のIoT製品のことも考慮し、ラベルの掲載及び掲載する際の場所は、IoT製品ベンダーが任意で決定できることとしています。 また、ラベルのサイズも考慮し、ラベルは、ロゴとQRコード等の最小限の情報のみを含める予定です。
144	M12	M12-035	制度構築方針案	全般		各項目について疑義が生じた場合に、実機評価で確認がしにくい項目について製品ベンダーはどのように証明するか例示してほしい。	仕様書そのものを製造ベンダーの一存で提出できない可能性もあるし、パスワードの生成ロジックそのものを公開するのも情報管理上好ましくないと考える。マニュアル等に、初期パスワードの条件を記載する場合、セキュリティを脆弱にする方向と考える。	3.7.のP.19に記載のとおり、スキームオーナー（IPA）の判断によりサーベイランスを実施する場合は、評価に使用した証跡の提出を求めることを想定しています。 開示が困難な場合は、提示可能な範囲の説明文書を用意し、説明いただくこととなります。
145	M13	M13-001	制度構築方針案	2.1.	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。	一般消費者向けの製品で、本制度の周知をはかるため、家電量販店等の販売事業者への周知、一般消費者への啓発活動などに取り組んでいただきたい。	制度に適合した機器を増やすためにも、機器メーカにとって本制度に取り組むモチベーションがあがるような取り組みが必要となる。	4.2.に記載のとおり、特に消費者向けには小売事業者等と連携したプロモーションを検討する予定です。
146	M13	M13-002	制度構築方針案	2.1.	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。	既に同様の制度が導入されているシンガポールや英国などとの相互承認に加えて、現在具体的な適合基準の策定を進めるアメリカや欧州との連携により、適合基準の国際標準化に取り組んでいただきたい。	IoT製品を海外に輸出する場合に加えて、IoT製品のセキュリティ設計は、グローバル標準で、共通的に行うことが想定される。このためにも、国際標準化が重要となる。	3.8.3.に記載のとおり、米国や欧州との連携も重視しています。 また、国際標準化に向けて検討が進んでいるISO/IEC27404等との連携も図っています。
147	M13	M13-003	制度構築方針案	3.2.	関連サービスとは、 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。	IoT機器と異なる事業者によるサービスとの組合せも想定されるが、申請時の対象範囲の解釈の余地が少ないように定義をお願いしたい	本制度はあくまで、IoT機器を対象としており、関連サービスは認証の対象外と考えている。 IoT製品ベンダー、調達者・利用者における解釈のわかり易さを与えるために、対象範囲について明確化をお願いしたい。	「IoT機器と異なる事業者によるサービス」は、それがIoT機器の利用に必要なものである場合、「付随サービス」としてIoT製品の範囲に含みラベル取得することが可能です。 連携できるが、必ずしもIoT機器の利用に必要でないサービスは、ラベル取得の対象外とします。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
148	M13	M13-004	制度構築方針案	3.2.	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。	制度の対象とする製品範囲の説明において、LAN（有線・無線）を持たず、BluetoothやUSBやRS232C等のインターフェースを持つ機器を対象とするかどうかについて明記してほしい。	「インターネットプロトコル（IP）」を、OSI参照モデルの第3層のネットワーク層のIPプロトコルと考えると、BluetoothやUSBやRS232C等はこれを使用していないため本制度の対象外と考えます。	BluetoothやUSBやRS232C等のインターフェースのみを持つ機器であり、インターネットプロトコルを使用した通信を行わない機器は、本制度の対象外となります。
149	M13	M13-005	制度構築方針案	3.2.	これらの IoT機器にその関連サービスを含めた IoT製品を本制度の対象範囲とする。対象製品のイメージを図 3.2-1 に示す。	IoT製品は、IoT機器と、タブレット端末やスマートフォン等のソフトウェア製品（アプリケーション）が一体となってサービスを構成することがある。 適合性の評価対象は、IoT機器単体なのか、ソフトウェア製品が含まれるのかを明確化願いたい。 また、適合性評価対象にソフトウェア製品が含まれる場合、ソフトウェア製品を更新しても一体として用いるIoT機器については、変更申請や情報提供等を不要とするなど運用の簡素化をお願いしたい。	現状の記載では、ソフトウェア製品が対象となるか判断が難しい。また、ソフトウェア製品が含まれる場合、適合評価時の評価対象とソフトウェア製品のバージョンなどが異なる場合が想定される。 申請の頻度や申請書類の簡素化をお願いしたい。	制度の対象は、「IoT製品＝IoT機器（＋付随サービス）」となります。IoT機器の利用に必要なものである場合、「付随サービス」としてIoT製品の範囲に含みラベル取得することが可能です。 なお、ソフトウェア製品をラベル取得製品の範囲に含む場合、3.7.に記載のとおり、評価に影響を及ぼすレベルでの製品仕様の変更があった場合は、☆１、☆２のラベルは失効し、継続する場合は、自己適合宣言を再度実施することとなります。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
150	M13	M13-006	制度構築方針案	3.3.	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 。	IoT機器にはネットワークに接続するための通信回線を分離して(モジュール化して)構成するものがある。この通信回線(モジュール)単独でセキュリティ適合基準を担保する場合は、機器本体を含まず通信回線（モジュール）単独での申請を可能として欲しい。加えて、適合性を評価された同じ通信回線(モジュール)を搭載する派生機種の申請の簡素化をお願いしたい。	申請の頻度や申請書類の簡素化をお願いしたい。	セキュリティ上の機能や管理（将来的なソフトウェアのアップデート等を含む）が同一であれば、同一製品の範囲としてラベルを取得することを可能とする予定です。各製品が「通信回線(モジュール)」部分以外に適合基準に関するセキュリティ機能等を有していない前提となりますが、派生機種も含め、「同一の通信回線(モジュール)を搭載した製品群」としてラベルを取得することが可能です。その際は、各製品の型番等を登録することとなり、ラベル取得後に新規の派生機種を販売する場合は、その登録情報を更新いただくこととなります。
151	M13	M13-007	制度構築方針案	3.2.	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。	「容易にセキュリティ対策を追加できない場合」の具体例について説明してほしい。	技術的にセキュリティ対策ができないのか、利用者のスキル不足によって対策ができないのか判断できないため。 また、例えば、ウイルス対策としてOSのホワイトリスト方式等を施すことにより容易にアップデートができない製品は対象製品とみなすか判断がつかない。	「容易に」は、前文の「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」ことを示しています。利用者が通常の手順に従い、任意のセキュリティ対策ソフトウェア等を追加でインストールし、セキュリティ対策を実施できるような製品か否かで判断してください。 基本的には、例示している「パソコン、タブレット端末、スマートフォン等」は対象外となりますが、それ以外は対象（適合基準を満たせば、ラベル取得が可能）と考えてください。
152	M13	M13-008	制度構築方針案	3.2.	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 。	”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）”と記載があるが、”容易”の定義が不明確であり対象製品か否かの判断が困難であるため、何をもって”容易”とするのか明確に記載するべきである。	パソコンやタブレット端末、スマートフォン以外にも昨今はSW(FW)の更新が容易にできるものが存在する。そのような機器と汎用的な IT 製品を分類するのは難しいため、何をもって”容易”とするのか明確に記載していただきたい。 例えば、ユーザーの意図により更新が必要な場合、ユーザーにそれを伝える手段がない場合は”容易でない”と判断する、等。また、ユーザーの意図にかかわらず自動的に更新されるものは”容易”とする等、お示しいただきたい。	「容易に」は、前文の「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」ことを示しています。利用者が通常の手順に従い、任意のセキュリティ対策ソフトウェア等を追加でインストールし、セキュリティ対策を実施できるような製品か否かで判断してください。 基本的には、例示している「パソコン、タブレット端末、スマートフォン等」は対象外となりますが、それ以外は対象（適合基準を満たせば、ラベル取得が可能）と考えてください。
153	M13	M13-009	制度構築方針案	3.2.	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。	「容易にセキュリティ対策を追加できない」ようにしている医療機器や医療情報システムも、本評価制度の対象に含まれることになるのか？ そもそも「容易」の定義を説明してほしい。 （セキュリティ要件3-3からではわかりませんでした）	医療機器や医療情報システムは一般的に、ユーザーが「容易にセキュリティ対策を追加できない」ようにしているが、この場合、医療機器や医療情報システムも広く、本評価制度の対象に含まれることになるのか？セキュリティのみのアップデートのため、薬機法に対しても問題ないという認識での議論となっているのか？	「容易に」は、前文の「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」ことを示しています。利用者が通常の手順に従い、任意のセキュリティ対策ソフトウェア等を追加でインストールし、セキュリティ対策を実施できるような製品か否かで判断してください。 基本的には、例示している「パソコン、タブレット端末、スマートフォン等」は対象外となりますが、それ以外は対象（適合基準を満たせば、ラベル取得が可能）と考えてください。 なお、医療機器や医療情報システムで利用されるIoT製品についても、本制度の適合基準を満たせば、本制度のラベル取得が可能ではありますが、別途実施されている医療機器のサイバーセキュリティに係る審査の対象となる製品は、そちらの審査を引き続き受けていただく必要があります。
154	M13	M13-010	制度構築方針案	3.3.	N/A	☆2以上の適合基準が今後検討されると思うが、製品が用いられる用途などで要求される基準が変わることが想定されるので、調達者・利用者が判断しやすいように製品類型の曖昧さをなくして明確にするようお願いしたい。	調達者・利用者におけるわかりやすさのため	☆２以上を整備予定の製品類型の対象や、どのようなセキュリティ水準の製品を☆２以上として想定するのかの方針等の情報を早期に公開するようにします。
155	M13	M13-011	制度構築方針案	3.4.	図3.4-2 セキュリティ要件の整理方針 「国内外のセキュリティ要件を踏まえ、本制度におけるセキュリティ要件を策定」	諸外国の制度との相互運用性について検討されていることは非常に好ましいことです。一方で複数国の制度を反映することにより、日本の制度が単一国の制度よりも過剰な制度（規則）とならないように検討いただきたいと考えます。	総和をとることで、日本の基準にて諸外国と異なる条項が設けられ、認証取得が難しくなることを懸念します。	本制度は、任意制度であり、基準を満たしていないと国内で販売できないような義務的なものではありません。 また、3.4に記載のとおり、総和を取って作成したものはセキュリティ要件（全体リスト）であり、ラベル取得の際に満たすべき適合基準は、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威を設定し、必要なセキュリティ要件をセキュリティ要件（全体リスト）から抽出して定めます。 例えば、☆１の場合は、101項目のセキュリティ要件（全体リスト）の中から、25項目を抽出し、それを16項目の適合基準に集約させています。 セキュリティ要件（全体リスト）は、以下の「最終とりまとめ 別添1 セキュリティ要件一覧」を参照ください。 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
156	M13	M13-012	制度構築方針案	3.4.	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。	想定される見直しの頻度、周知期間について公表いただきたい。	製品開発には年単位の時間がかかるものであり、本制度の見直し時期にあわせてセキュリティ設計の見直しも行いたい。	適合基準の見直しは必要に応じて実施するので、現時点で決まった頻度はありませんが、同じ適合基準でメジャーな改訂を年に数回も行う想定はありません。改訂予定が決まれば、早期に周知するようにします。 また、3.7に記載の猶予期間（旧版と並存させる移行期間）は、半年程度以上は確保することを想定しています。
157	M13	M13-013	制度構築方針案	3.5.	図 3.5-1、図 3.5-2 図中に登場する「評価機関」の記載	日本国内での評価機関を早期に複数設置していただきたい。	メーカにとっての試験機関の早期立ち上げにより、実運用時の事例蓄積と関係メーカとの伴走が期待されます。	3.4.に記載のとおり、2023年度に実施した検討会の中で、☆１の適合基準案に対する実証を行っており、複数の評価機関候補や検証事業者候補となる事業者に協力いただいています。 また、4.3.に記載の検証事業者の条件と想定している情報セキュリティサービス基準審査登録制度の機器検証サービスには、2024年5月時点で、10サービス（10事業者）が登録済みとなります。 これらの事業者を中心に、本制度の評価機関や検証事業者として参画いただくように働きかけます。 （参考）情報セキュリティサービス基準審査登録制度 機器検証サービス 登録事業者一覧 https://sss-erc.org/iss_book/devvs/
158	M13	M13-014	制度構築方針案	3.5.	表3.5-2 ☆ 1 、☆ 2（自己適合宣言）×評価機関 （評価機関や検証事業者の利用は任意）	（評価機関や検証事業者の利用は任意）とだけ記載があるが、評価機関や検証事業者を利用する場合のそれらの者の責務を記載いただきたい	自己適合宣言の場合の評価機関や検証事業者の責務の明確化	自己適合宣言の場合、評価機関や検証事業者を利用したとしても、最終的な責任はIoT製品ベンダーとなり、その責務の一部を委託することとなります。そのため、その責務は、本制度で規定されるものではなく、IoT製品ベンダーと評価機関や検証事業者の間で決められるものとなります。
159	M13	M13-015	制度構築方針案	3.6.	ラベル表記について	ラベル表記は、物理的表記のみならず、画面等をもつ機器においては電子的表記を認めて欲しい	製品を販売後、ラベリング要求が高度になる中で、本ラベリングを維持していくことは難しい。電子的に対応を実施することで、有効期限等への対応や外部環境変化によってラベリングが保たれなくなった時にも、効果的にラベリング表示ができるようになるため	3.7.に記載のとおり、ラベルの貼り付けやその場所・方法は任意としています。 電子的表記を否定しているものではありません。 ラベルの利用方法の詳細については、利用ガイドを別途用意します。
160	M13	M13-016	制度構築方針案	3.7.	評価者区分としては、I oT 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。・・・	ラベルの信頼性確保の仕組みとしての、検証事業者、評価機関の要件について記載がないので記載願いたい。 4.3. 評価機関 ・ 検証事業者に対する支援策 に、評価機関や検証事業者の要件に該当する記述があるため、その内容を本項にも記載願いたい。	検証事業者、評価機関に評価を依頼することが信頼性確保に役立つことの明確化	参照先の節番号が誤植となっていましたが、「検証事業者、評価機関の説明は、4.3節を参照のこと。」と修正しました。
161	M13	M13-017	制度構築方針案	3.7.	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、、、、	本制度の運用が開始されるにあたってWebサイトの運用者の明示をお願いしたい。	IPAが運用すると推測しますが、明示されていないため	「本制度の」は、「本制度のスキームオーナー（IPA）の」を意味しています。
162	M13	M13-018	制度構築方針案	3.7.	表3.7-1 製品情報	【質問】 URLや連絡先はラベル有効期限内は都度更新可能で、有効期限後に無効な情報になっていても問題ないとの理解で正しいでしょうか?		URLや連絡先はラベル有効期限内は都度更新可能です。有効期限後の扱いについては各社の判断となります。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
163	M13	M13-019	制度構築方針案	3.7.	表3.7-1 安全情報	【質問】 当該製品に関わる脆弱性情報とはどのようなものでしょうか? 脆弱性が見つかれば都度更新するものでしょうか?		制度開始時点では、IoT製品ベンダーからの申告により、公開済みのぜい弱性情報や、パッチ適用依頼等の情報を掲載することを想定しています。
164	M13	M13-020	制度構築方針案	3.7.	表3.7-1 型式番号	申請にかかる手間およびコストを削減するため、同一のセキュリティ対策を行う複数の型式番号については、一括で申請ができる仕組みを導入いただきたい。	一般消費者向けのIoT機器では、ファームウェアなどセキュリティに関わる機能は同一であるものの、カラーバリエーション、流通経路違い（量販店、専門店など）、サイズ違い（エアコンのKw数など）で多数の型式番号が必要となる場合がある。	ラベル取得の単位は、セキュリティ上の機能や管理（将来的なアップデート等を含む）が同一であればまとめて一つとし、該当する製品は同じラベルを利用することを可能とする予定です。なお、申請時に該当する製品の型番すべてを明記していただくことになります。 詳細については、申請ガイドなどを用意する予定です。
165	M13	M13-021	制度構築方針案	3.7.	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仕様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。	【質問】 有効期限内において、機能追加（脆弱性対応は含まない）などで製品のファーム更新を実施した場合は、再度適合申請取得の必要は無い認識で合っているでしょうか？		製品のファームウェアの更新が「評価に影響を与えるレベルでの製品のセキュリティ仕様等の変更」に該当するか否かが判断基準となります。 詳細については、別途、申請ガイドなどを用意する予定です。
166	M13	M13-022	制度構築方針案	3.7.	調達者・利用者からの申請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、申請者に対して評価に使用した証跡の提出を求めることや検査・サーベイランスを実施する。証跡の提出に当たっては、必要に応じて 秘密保持契約(NDA)を申請者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、申請者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。	ここで言う「申請者」が誰を表すのか不明確。基準への適合に疑義を生じて「申請」をする調達者・利用者のことなのか、ラベル付与を申請するベンダーなのか。 例えば、調達者・利用者からの「申請」を、調達者・利用者からの「請求」と別の表現に置き換え、「申請者」を「ラベル付与申請者」とするなど、明確になるよう記載・修正願いたい。	申請者が誰を表すのかの明確化	以下のとおり記載を見直しました。 「調達者・利用者からの申請」→「調達者・利用者からの指摘」 「申請者」→「（ラベルを取得した）IoT製品ベンダー」
167	M13	M13-023	制度構築方針案	3.7.	☆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。	変化の激しい分野であることを考えると有効期限を2年以内とすることに合理性はあるものの、海外製品も対象とすることを考えれば、比較対象としてIEC62443の有効期限は3年なので整合をとることを提案します。	更新のための評価に要する負担とコストを考慮	諸外国の制度との比較及び制度開始当初の☆１では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から、☆１の有効期限の設定は、最大２年とすることが妥当と考えています。 (参考)第7回検討会資料　資料4 P.14 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.html
168	M13	M13-024	制度構築方針案	3.8.	2.1節の主目的を三つの主目的を達成するため、・・・	誤植だと思われる。以下への修正を提案します。 2.1節の三つの主目的を達成するため、・・・	エディトリアルな修正	誤植となりますので、修正します。
169	M13	M13-025	制度構築方針案	3.7.	調達者・利用者からの申請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、申請者に対 して評価に使用した証跡の提出を求めることや検査・サーベイランスを実施する。	【質問】 サーベイランスなどで非適合となってしまった場合、情報提供ページのステータスを「ラベル失効済み」と変更することでユーザーに告知するのでしょうか？また、失効により補助金対象でなくなった場合の損害賠償などのリスクに対して保険制度が適用されるとの理解でよろしいでしょうか？		サーベイランスなどで不適合となった場合、情報提供ページのステータスを「ラベル失効済み」と変更することでユーザーが確認可能とします。 当初設定していた期間内にラベルが失効する可能性は、サーベイランスで不適合となる以外に、3.7.に記載の製品仕様の変更等の可能性があります。本制度のラベルは、基本的には、購入時の判断基準として活用される想定であり、調達者・利用者が、機器を利用する期間においてラベル取得の維持を求める場合、個別にIoT製品ベンダーと協議していただく必要があります。また、失効による損害賠償についても、必要に応じて協議による取り決めや契約等を個別に実施していただくこととなります。
170	M13	M13-026	制度構築方針案	3.8.2.	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。	重要インフラ分野に含まれる「医療」については、厚生労働省をはじめ、医療関連業界団体との連携をお願いしたい。	いわゆる「3省2ガイドライン」の対象となる医療情報システムに対するセキュリティ要件と、同システムの一部として導入されたり、システム間連携で利用されるルーター・ハブ・スイッチなどの本書が対象とするIoT機器に対するセキュリティ要件の整合性が崩れないようにするため。	重要インフラ分野は検討の対象と考えております。関係省庁や関係団体とも連携しながら、調整を進めて行きます。
171	M13	M13-027	制度構築方針案	全般	IoT製品ベンダー	IoT製品ベンダーには、どの様な事業者が含まれるのか、例えばp24 4.1に海外のIoTベンダーの言及があるものの範囲が不明確。例えば、製造事業者(原産国が外国の場合を含む)、外国製品を日本国内で販売する外国の製造事業者、製品を輸入して国内で販売する事業者なども対象であることを明確化していただきたい。 そのため、適用範囲と事業者の例の記載を追加いただきたい。 なお、別添☆1セキュリティ要件・適合基準の用語集の「製造業者」の「意味」に記載の内容と同じであれば、それを制度構築方針案本体にも記載いただきたい。	国内に流通するあらゆるIoT製品のベンダーを対象とし、ラベリング制度を広く浸透させるため	「1.はじめに」にて、「IoT製品ベンダー」は「IoT製品を製造又は販売するベンダー」と定義しています。 ☆１適合基準では、別途IPAから公開しているETSI EN 303 645の和訳との整合も意識しており、「manufacturer」の和訳として「製造業者」を採用します。一方で、制度構築方針案の「IoT製品ベンダー」に相当する定義であり、用語集の「製造業者」の注記に以下の記載を追加します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映） ・この定義は、「IoT製品に対するセキュリティ適合性評価制度構築方針」における「IoT製品ベンダー」に相当する。
172	M13	M13-028	☆1セキュリティ要件・適合基準	3-1	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	【質問】 製品には複数のソフトウェアが搭載されている場合がありますので、本基準の「特定のソフトウェアコンポーネント」について定義を明確にして頂きたいと思います。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
173	M13	M13-029	☆1セキュリティ要件・適合基準	1-2	1-2. ブリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性を持つために、パスワードは十分なランダム性を保有しなければならない。	「セキュリティ要件」に対して、何をもってランダム性を確保できるかの評価手順を、より具体的に記載したガイドを作成していただきたい。	例えば、シンガポール政府が医療機器のラベリングスキームで要求(アセスメント内容：*1 31-32ページ、試験内容：*2　18ページ)しているものは、裏付けとなる証拠の具体説明であり、国内の新制度においても、類似の記述が必要と考えます。“ガイド”などの形式を以て具体的な基準を明示していただきたい。 シンガポールにおいては、非医療機器に対しても具体的説明が要求されています(*3 9ページ)のでそれを加味しての意見です。 *1：https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls(md)/-pub-cls(md)-pub-4---assessment-methodology-v0.3.pdf?sfvrsn=26df2a87_1 *2：https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls(md)/-pub-cls(md)-pub-5---minimum-test-specification-v0.5.pdf?sfvrsn=d86deb94_1 *3：https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/-pub-ccc-sp-151-4-cls(iot)-assessment-methodology-v1.0.pdf?sfvrsn=7661147f_1	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
174	M13	M13-030	☆1セキュリティ要件・適合基準	1-3,4-1,5-1	・機器の意図する使用において、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	"一般的に機密性が高い情報"とはどの程度のレベルを指しているのか？ 個人情報等とのことだが、消費電力量などの利用情報（パーソナルデータに該当する情報）は”一般的に機密性が高い情報”に該当しない認識であっているか？	現状の記載内容では抽象度が高く、受け取り側でレベル感が異なる可能性があるため	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
175	M13	M13-031	☆1セキュリティ要件・適合基準	1-4	「☆1適合基準」列 機器に対するネットワークを介したユーザ認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。	(1)「その認証値の変更を可能とすること」を「その認証値をシンプルなメカニズムで変更できること」に修正願いたい。 (2) 実際の適合性評価には、シンプルなメカニズムについて具体的に示すものが必要であり、別途作成されるガイドラインに具体的な記載をお願いしたい。	(1) 要件では、認証値を変更するためのシンプルなメカニズムを提供、とあるが、☆1適合基準には、"シンプルなメカニズム"の記載がなく、乖離が見られるため。 (2) シンプルなメカニズムが具体的には不明確なため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
176	M13	M13-032	☆1セキュリティ要件・適合基準	4-1	【用語定義：守るべき情報資産】 以下のすべての情報： ・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	用語定義のみならず、具体的な例を合わせて記載するべきである。	「通信機能に関する設定情報」とあるが、具体的にどういった製品のどういった情報がそれにあたるのか、読み手によってばらつきが生じるリスクがあるため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
177	M13	M13-033	☆1セキュリティ要件・適合基準	3-8	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。	適時にアップデートできているかどうかを判断するための基準や考え方を記載してほしい。	セキュリティパッチの作成やインストール作業（ネットワーク経由ではない場合など）に関して、適合性評価レベルによって基準は異なるかなど保守体制整備の基準にしたいため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
178	M13	M13-035	☆1セキュリティ要件・適合基準	4-1	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。	”セキュアに保存”のセキュアとはどの程度のレベルが求められるのか？	現状の記載内容では抽象度が高く、受け取り側でレベル感が異なる可能性があるため	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
179	M13	M13-036	☆1セキュリティ要件・適合基準	3-1,3-7	セキュリティ要件	ソフトウェアコンポーネントをアップデート可能であること(要件3-1)とその方法がセキュアであること(要件3-7)が分けられていますが、これらはセットで1つの要件にすべきだと思います。	偽のファイルでアップデートできてしまうと、そこが却って攻撃の口となってしまうため、アップデート方法がセキュアであることが望ましい。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
180	M13	M13-037	☆1セキュリティ要件・適合基準	3-7,3-10	「☆1適合基準」列 ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。	完全性のみが記載されていますが、真正性の確認も必要だと思います。 (修正後の文章案) 「ソフトウェアの完全性」を「ソフトウェアの真正性と完全性」とする。	ソフトウェアをセキュアな方法でアップデートすると言った場合、真正性と完全性の両方を検証することが一般的であるため。 また、要件3-10においても真正性が求められているため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
181	M13	M13-038	☆1セキュリティ要件・適合基準	11-1	☆１適合基準	削除すべき項目・内容について、具体例を示してもらいたい	評価・判断するための参考にしたいため	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
182	M13	M13-039	☆1セキュリティ要件・適合基準	17-10	製造業者は、セキュリティリスクを引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。	「指定された方法」とは、どのように指定されたもののか不明確なため「適合基準に指定された方法」への修正を提案します。	明確化のため	3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
183	M13	M13-040	☆1セキュリティ要件・適合基準	17-5	製造業者は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。	「指定された方法」とは、どのように指定されたもののか不明確なため「適合基準に指定された方法」への修正を提案します。	明確化のため	3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
184	M13	M13-041	☆1セキュリティ要件・適合基準	11-1	「要件」列 ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。	ユーザを主語にすると、ユーザに対する責務に見える。 (修正後の文章案) 要件17-2等に合わせて製造業者を主語とし、「製造業者は、簡単な方法で製品からユーザデータを消去できるような機能をユーザに提供しなければならない」に変更する。	ユーザを主語にすると、ユーザに対する責務に見える。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
185	M13	M13-042	☆1セキュリティ要件・適合基準	11-1	「☆1適合基準」列 製品利用中に製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。(以下略)	データを削除できることに加え、その方法が簡単であることが必要だと思います。 (修正後の文章案) 「以下の①・②のすべての基準を満たすこと」を「以下の①・②・③のすべての基準を満たすこと」とし、末尾に「③簡単な方法としてユーザに提供されること。」を追加する。	要件11-1に「簡単な方法で」と記載されているため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
186	M13	M13-043	☆1セキュリティ要件・適合基準	用語集	サプライチェーン内の関連事業者（機器の製造業者を含む）。 注： この定義は、IoTエコシステムに関与する多様な主体及びそれらの主体が責任を共有する複雑な方法を認めている。機器の製造業者以外にも、例えば目前の特定のケースに応じて、輸入業者、販売業者、インテグレータ、コンポーネント及びプラットフォームプロバイダ、ソフトウェアプロバイダ、IT及び電気通信サービスプロバイダ、マネージドサービスプロバイダ及び関連サービスのプロバイダなどがある。	製造業者はあくまでも対象機器の設計開発そして製造を行う者とし、サプライチェーン内の関連事業者については、輸入業者、販売業者、電気通信サービスプロバイダ個々を主語とした要件を定めるべきである。	製造業者の定義が必要以上に広範であり、かえって責任所在が不明確となることで本制度の実効性に懸念が生じる。主体が責任を共有するとしつつも、輸入業者、販売業者、さらには 電気通信サービスプロバイダまでが含まれており、市場から調達している事業者にとっては、本要件で多数の製造業者が主語として求められるものを満たすことは合理性に欠ける。	適合基準で求められるセキュリティ機能の実装等を行う主体は、基本的にはIoT製品の製造業者となります。 IoT製品ベンダーの定義に含まれる輸入業者や販売業者が、本制度のラベルの申請を行うことは可能としていますが、評価はIoT製品の製造業者の協力を得た上で実施する想定です。
187	M13	M13-044	☆1セキュリティ要件・適合基準	全般	セキュリティ要件 製造業者	(1)「製造業者」という言葉は、諸外国の制度に記載の”manufacturer”を和訳したものと推測しますが、当該製品に対して責任を持つ様々な事業者(販売事業者、輸入事業者等)をイメージしにくいため、本制度構築方針案本体に記載の「IoTベンダー」という表現に変更することを提案します。 (2) また、特に海外製品は輸入業者が国内販売するもの、ネット通販サイトを通して海外販売事業者から消費者が直接輸入するものなど、国内販売形態が多様化する中、責任者不在の製品が多く流通することを防ぐため、設計製造者からサプライチェーン事業者まで、国内の誰かがセキュリティに関して責任を持つ必要があると考えます。そのようことを踏まえた制度設計をお願いします。	(1) 分かりやすい表現の採用、制度構築方針案本体と別添の記載の整合。 (2) 海外製品を含めた国内流通製品のセキュリティ確保のため。	（１）☆１適合基準では、別途IPAから公開しているETSI EN 303 645の和訳との整合も意識しており、「manufacturer」の和訳として「製造業者」を採用します。一方で、制度構築方針案の「IoT製品ベンダー」に相当する定義であり、用語集の「製造業者」の注記に以下の記載を追加します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映） ・この定義は、「IoT製品に対するセキュリティ適合性評価制度構築方針」における「IoT製品ベンダー」に相当する。 （２）ラベルの申請は「IoT製品ベンダー」に含まれる販売業者や輸入業者も可能ですが、表 3.7 1に記載のとおり、申請時にIoT製品の製造業者名等を明確にするように求める予定です。
188	M13	M13-045	☆1セキュリティ要件・適合基準	全般	NAとなるための条件	「NA」の定義が無く、またNAとなる条件を満たす場合の措置についての記載がないため、「該当なし(NA)として適用除外とするための条件」への変更を提案します	適合基準の明確化	項目名を「対象外（NA）となるための条件、基準の補足説明」と見直します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映）
189	M14	M14-001	制度構築方針案	全般	制度の要件について	IoT機器のセキュリティを向上させる観点から提示いただいた内容はぜひ進めてもらいたいが、本制度の制度設計においては安全保障や経済安全保障の観点も考慮すべきではないか。例えば、悪意を持った事業者が提供する製品にバックドア等を仕掛け、当該製品を通じて不正なアクセス等が行われるリスクが大変懸念される。このようなバックドアは巧妙に隠蔽されるため、評価機関等の第三者が検査をしたとしても発見することは一般的に難しい。特に、現在の地政学的な情勢を踏まえると、そのようなリスクは増していると考えられる。したがって、制度の趣旨に経済安全保障の観点も入れつつ、要件において技術的な側面だけではなく、そのようなリスクがある事業者（例えば、外国政府の影響下にある企業等）を排除するような要件の追加を検討頂きたい。		サイバーセキュリティ戦略（令和３年９月 28日閣議決定）でも示されているサプライチェーン・リスクに関して、本制度でも考慮することを3.5.に記載します。
190	M15	M15-001	制度構築方針案	3.	適合基準及び評価方式について	国際基準に比較して過剰な規則や運用とならないように注意して基準及び評価方式を制定して頂きたい。	例えば、技術基準適合証明において、商用化時では無くPOCやトライアル試験のためにも正規のR認定、T認定を取らなければならないという他国に比べて明確に厳しい要求があり、製造業者のコスト増加に繋がっているため。	いただいた意見は、今後の検討の参考にします。
191	M15	M15-002	制度構築方針案	1.	P.2のIoT製品ベンダーについて	「IoT製品を製造もしくは販売するベンダー（IoT製品ベンダー）」について、定義が明確でない。最終製品を扱うOEM(Original Equipment Manufacturer)への適用なのか、設計主体であるODM(Original Design Manufacturing)への適用なのか、IoT向けのモジュール製品を扱うベンダーへの適用なのかなどについて明確にして頂きたい。	IoT製品は最終製品までのエコシステムが多層のレイヤーとなっている。よって、どのレイヤーのプレイヤーに制度を適用するかの基準が提示されないと、実行上の混乱や非効率化が予想されるため。	「IoT製品を製造するベンダー」には、「OEM/ODM委託先」や「IoT向けのモジュール製品の製造ベンダー」も含まれます。各適合基準において、どの主体がそれを提供するかは、各製品を製造する役割に依存するものであり、一律に指定するのは困難であると認識しています。最終的なIoT製品を製造するベンダーが、それぞれの役割に応じた責任主体に確認しながら、適合基準を満たしていることの評価を実施して（第三者評価の場合、評価を受けて）ください。
192	M15	M15-003	制度構築方針案	3.8.3.	P.21の諸外国制度との比較について	本制度の対象機器に関して必要最小限となるよう、内容の吟味をして頂きたい。	米国、英国、シンガポールは消費者向けIoT機器が対象であるが、本制度は幅広いIoT製品を対象としており、他国と比較してより多くのコストが必要となる事が懸念されるため。	他制度等で、既に本制度と同等以上のセキュリティが一般的に確保されているIoT製品に対し、本制度のラベル取得を無理に推進する予定はありません。 しかしながら、それ以外のIoT製品については、広く対象とし、本制度のラベル取得又はラベルは取得しないもののそのセキュリティ基準を意識した製品開発を促すことで、国内で生産されるまたは流通されるIoT製品のセキュリティ水準を高めることを目指します。
193	M16	M16-001	制度構築方針案	3.2.		自己完結型環境で利用する機器 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・・・ 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）や、自己完結型の環境での利用を前提とする場合は対象外とする。	ETSI EN 303 645は「ネットワークインフラ（インターネットやホームネットワークなど）に接続される民生用IoT機器」に対する適用となっている。明らかに自己完結型環境で利用されるものは、サイバー攻撃の対象とはなり辛く、対応措置も異なってくるため、対象外とすることが望ましい。	本制度は、ETSI EN 303 645を考慮しているが準拠した制度ではなく、適合基準で定めた必要なセキュリティ機能をその機器が備えることを求めています。したがって、そのようなセキュリティ機能を有しない機器は、対象外というよりもラベルを取得できないということを意味します。 ラベル取得は任意であり、自己完結型環境で利用される前提で、ラベル未取得でもセキュリティ上問題ないと考えるのであれば、それを調達者に訴求してください。
194	M16	M16-002	☆1セキュリティ要件・適合基準	6-1		利用しないインターフェース 「製品の利用上不要かつ攻撃を受けるリスクがある物理的インタフェースまたは論理的インタフェースを無効化する～製品に対する脆弱性検査を実施する」に変更	①方針案１６頁 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 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」 ②方針案１８頁 3.7 ラベル信頼性確保のための仕組み 有効期限内に評価に影響を及ぼすレベルでの製品仕様の変更があった場合は、IoT製品ベンター自身で確認を行った上で～ラベルは失効する。 ①②に則ると、ラベル付与された機器で、付与時不要としていたインタフェースを有効化する仕様変更を行った場合、評価に影響を及ぼすと判断され、ラベル失効するのではないか。結果、IoT製品ベンダーの負荷が高まる。 「１．はじめに」の２頁記載で、産業用製品に対する認証制度はIoT製品にとってハードルが高いと記載していることとも相違する。 ☆１が消費者向け製品への評価であることを考えると、or条件での評価でも十分と考える。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
195	M16	M16-003	☆1セキュリティ要件・適合基準	11-1		「削除」のレベルが不明確。	構築方針案12頁の「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」を前提とするのであれば「完全な削除」を求めるべきだが、IoT製品で汎用OSが使用されている場合、「完全な削除」操作が要件に記載される「簡単な方法」とならない場合がある。「簡単」を優先するか、「完全」を優先するか明確にすべき。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
196	M16	M16-004	☆1セキュリティ要件・適合基準	1-2		①デフォルトパスワード(６文字)、②のデフォルトパスワード(８文字)と異なっている。共に8文字以上のパスワード設定でよいのではないか。	パスワードの文字数を変える理由が不明確。	①の場合は、IoT製品ベンダー側で「容易に推測できない」つまり一程度の複雑性を持ったパスワードが設定される想定であり、桁数は6桁としています。 一方で②の場合は、ユーザが複雑でない任意のパスワードを設定できることも想定し、最低限の桁数として8桁を求めています。 ①の適合基準は、「6文字以上」なので、「8文字」で設定いただくことも可能です。
197	M16	M16-005	制度構築方針案	3.5.	表3.5-2	[ラベル]の有効期限に関する質問 例: ProductA(Ver.1.0)を2024年4月1日にリリース リリースに伴う製品型式登録手続きの一環としてラベルを2024年4月1日付けで取したとすると, 2026年3月31日まで有効という理解でよいのか。 ProductA(Ver.1.0)の個体番号1111を2024年5月1日に販売するとした時に貼り付けるラベルの有効期限の解釈は次の内どれに該当するか。 ①ProductA(Ver.1.0)として4月1日取得した物と同じで、有効期限は2026年3月31日まで ②個体番号ごとの手続きは不要で5月1日付けとして貼り付けて、有効期限は2026年4月30日まで ③個体番号ごとの手続きが必要で5月1日付けとして貼り付けて、有効期限は2026年4月30日まで		①となります。 3.7.に記載のとおり、☆１、☆２の有効期限はラベル取得日から最大２年間となります。 製品に対するラベル付与であり、製品の特定個体に対する手続は不要です。
198	M16	M16-006	☆1セキュリティ要件・適合基準	5-1		温度、圧力センサーなどの計測値を機器間で通信しているような場合のデータに対しても暗号化処理が必要か？ あるいは、守るべき情報資産かどうかをベンダーが定義して暗号化処理の有無を選択しても良いのか？		定義に従い、「守るべき情報資産」に該当するか判断いただくこととなります。 なお、一般的には、「温度、圧力センサーなどの計測値」が「守るべき情報資産」には該当しないと考えられますが、どのようなシステムで利用されるIoT製品で、どのような計測値なのかにもよるかと思われます。
199	M16	M16-008	☆1セキュリティ要件・適合基準	5.		・「最終とりまとめ」では、個人情報保護への言及があるがプライバシーへの言及がない。 ・個人情報に該当しない情報でも、プライバシー上およびセキュリティ上の問題を引き起こす恐れがある[2][3][4][5][6]。 ・現在でも、IoT機器による不透明な情報収集が問題視されている[1]。 ・消費者は、IoT機器による情報収集についてIoT機器ベンダーから十分な情報を知らされていない[1]。 ・IoT機器による情報収集の状況について消費者自身が監査することは技術的に容易ではない[1][2]。 ・IoT機器の情報収集に関する問い合わせに対して、IoT機器ベンダーが十分な回答を行わないケースが報告されている[1]。 ・セキュリティ上の観点からも、IoT機器における通信の透明性を確保することが望ましい[1][2]。（通信の透明性が無い場合、通信の監査、異常判定、フィルタリングが困難になり、セキュリティ対策の障害になる。） 提案 ・IoT機器における、通信の目的、相手先、タイミング、内容、通信量の見積方法を表示させるべき。 ・通信で取得した情報の保存先、保存期間、共有先、問い合わせ先、削除リクエスト等の取扱いについて表示させるべき。 ・通信に関する表示や利用許諾条件等が適切であるかを認証条件に追加するべき。 ・IoT機器における通信の暗号化を要求する場合には、次の対策を盛り込むべき。 ・通信に関してベンダーが表示した情報と実態が合致していることを監査するべき。（通信が暗号化された場合、消費者自身が通信を監査することができないため。） ・通信に関してベンダーが表示した情報と実態が異なることが疑われる場合の連絡窓口を認証者側に設けるべき。（通信が暗号化された場合、消費者自身が証拠を持ってIoT機器ベンダーに問い合わせることができないため。）	[1] Anna Ida Hudig et al.: “Transparency in the consumer Internet of Things” https://www.iot-transparency.org/ (2023) [2] Keith Winstain, “Introducing the ‘right to eavesdrop on your things”, https://www.politico.com/agenda/story/2015/06/internet-of-things-privacy-concerns-000107/ (2015) [3] Roman Cuprik, “Gathering dust and data: How robotic vacuums can spy on you”, https://www.welivesecurity.com/en/privacy/gathering-dust-and-data-how-robotic-vacuums-can-spy-on-you/ (2023) [4] Caspersky, “アダルト向けグッズがハッキングされる”, https://blog.kaspersky.co.jp/insecure-vibrator/12287/ (2016) [5] Office of the Privacy Commissioner of Canada, “Making playtime safer in the Internet of Toys”, https://www.priv.gc.ca/en/blog/20211202/ (2021) [6] Shane Harris, “Your Samsung SmartTV Is Spying on You, Basically”, https://www.thedailybeast.com/your-samsung-smarttv-is-spying-on-you-basically (2015)	いただいた意見は、☆２以上の基準を検討する際に技術審議委員会で考慮します。
200	M16	M16-009	☆1セキュリティ要件・適合基準	全般		☆1評価手法に「ドキュメント評価」がある場合、どのような種類のドキュメントにどのような内容が記載されている必要があるか、が分かりやすく示されているとベンダとしては対応しやすくなります。 例： ・ユーザマニュアルに、○○○についての記載があること。 ・設計文書に、△△△についての記載があること。 ・試験文書に、□□□の試験仕様および結果が記載されていること。		いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
201	M16	M16-010	☆1セキュリティ要件・適合基準	1-2		カテゴリ「1. 汎用のデフォルトパスワードを使用しない」は、パスワード認証を前提としており、更にその中でのデフォルトパスワードを対象にした、非常に範囲が狭い定義になっています。これに対し、要件1-1～1-5および対応する☆1適合評価項目（適合基準など）は認証全般を対象とした表現になっています。 その結果として、いくつかの要件や適合基準、ベンダに対して何を求めているのかが具体的に把握しにくくなっていると思います（詳細は別意見として後述）。 他のカテゴリは、カテゴリの方が要件・適合基準を包含する関係にあり、要件・適合基準の方が範囲が限定され具体的であるため、ベンダに対して何を求めているのかが比較的把握しやすいと思います。 認証に関しても、カテゴリと要件・適合基準の包含関係が他のカテゴリと同様になるように、以下の見直しをしていただきたく存じます。 ・☆1ではパスワード認証を前提とし、デフォルトパスワードに関する要件のみに限定するのであれば、☆1適合基準の記載をその範囲内の具体的な内容に変更する。 ・パスワード認証全般や認証全般に対する共通要件であれば、カテゴリ名をそれに合わせた範囲の名称に変更する。 ・パスワード認証以外（パスワードレス、証明書など）のより高度なユーザ認証を採用している場合の評価の扱いを明確化する。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
202	M16	M16-011	☆1セキュリティ要件・適合基準	1-3		カテゴリ「1. 汎用のデフォルトパスワードを使用しない」は、要件1-3の「想定するリスクを低減」および☆1適合基準の「適切な認証」を実現するための要件です。つまり、包含関係が逆転しています。 このため、カテゴリ「1. 汎用のデフォルトパスワードを使用しない」に対してであれば、この評価項目番号1は不要と思います。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
203	M16	M16-012	☆1セキュリティ要件・適合基準	1-4		☆1評価項目番号3の☆1適合基準に対しては、「汎用のデフォルトパスワード」に限らずパスワード変更を可能にすることを求めています。 これを☆1の要件に含めるのであれば、それにふさわしいカテゴリ名に変えた方がよいと思います。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
204	M16	M16-013	☆1セキュリティ要件・適合基準	1-5		☆1評価項目番号3の☆1適合基準に対しては、「汎用のデフォルトパスワード」に限らずネットワークからのパスワード総当たり攻撃への対策を求めています。 これを☆1の要件に含めるのであれば、それにふさわしいカテゴリ名に変えた方がよいと思います。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
205	M16	M16-015	☆1セキュリティ要件・適合基準	5-5		要求5-5の以下の記載が、具体的にどのようなケースなのかが想像できません。「基準の補足説明」などに、説明を追記いただければと思います。 ・ただし、製品が依存するネットワークサービスプロトコルで、製品の動作に必要な設定を製造業者が保証できない場合は、例外とする。		ETSI EN 303 645の5.5 注3に記載のある「例外となるプロトコルには、ARP、DHCP、DNS、ICMP、NTP が含まれる。」を意図しています。 セキュリティ要件5-5に対する☆１適合基準は、☆１評価項目番号#1に包含されており、本制度の最終とりまとめの別添２として別途公開している「☆１評価ガイド」において、【参考情報：例外となるプロトコルの例】としてこれらを示しています。
206	M16	M16-016	☆1セキュリティ要件・適合基準	6-1		☆1適合基準の①に「製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること」とありますが、攻撃を受けるリスクの有無は適合評価においてどのように判断されるのでしょうか。		いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
207	M16	M16-017	☆1セキュリティ要件・適合基準	6-1		☆1評価手法に「※①は、ドキュメント評価と実機テストの双方を実施すること」とあります。 これは、☆1適合基準の①を踏まえると、 ・ドキュメントに全ての有効化されているポートが記載されていること。 ・実機テストにおいて、ドキュメントに記載されていないポートが有効化されていないことという意味だと思いますが、これを明記していただいた方が、ベンダとしては対応がしやすくなります。		いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
208	M17	M17-001	制度構築方針案	3.7.		[指摘内容] 「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。」とあるが、「研修」がここにしか言及されない。 [修正案] まだ未確定であっても「IoTセキュリティ評価に関する研修については今後、本制度の技術審議委員会で検討する」などの補足が必要。	「研修」に関する情報がないため読者の混乱を招く。	以下のとおり、研修制度の整備も今後の検討事項である旨、追記します。 「指定資格を～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。」
209	M17	M17-002	☆1セキュリティ要件・適合基準	1-2	NAとなるための条件、基準の補足説明	[指摘内容] 適合基準にて「パスワードやパスコードを使用する製品において」と対象を限定している。 このため、認証に「パスワードやパスコードを使用しない（パスワードやパスコード以外の仕組みを使用する）製品」は対象外となるのではないか。 [修正案] NAとなるための条件、基準の補足説明 以下のいずれかの条件に該当する。（OR条件） ・ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、脅威に対抗するためにユーザ認証が必要ない根拠を記載すること） ・認証の仕組みにパスワードやパスコードを使用しない（「NAであることの理由」に、使用している認証の仕組みを記載すること）	＃３の☆１適合基準において、認証の種類として「パスワード、トークン、指紋等」と記載しており、パスワード/パスコード以外の認証を示唆している。＃３と整合を取るとともに、そのような製品をカバーする必要がある。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
210	M17	M17-003	☆1セキュリティ要件・適合基準	1-5	NAとなるための条件、基準の補足説明	[指摘内容] 「機器に対するネットワークを介したユーザアクセスの仕組みがない」とあるが、ユーザアクセスはあるがユーザ認証がない場合もNAになると思われる。 [修正案（青字箇所）] NAとなるための条件、基準の補足説明 ・機器に対するネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること）	＃２、＃３の「NAとなるための条件、基準の補足説明」の記載（ネットワークを介したユーザ認証の仕組みがない）と整合させる必要がある。 もし、当該要件において意図的に違う用語を使っているのであれば、その意図を明確にしないと、読者の混乱を招く恐れがある。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
211	M17	M17-004	☆1セキュリティ要件・適合基準	3-1	NAとなるための条件、基準の補足説明	[指摘内容] 対象機器によっては、消防法などの適用により、ソフトウェアコンポーネントの更新に制約が生じる製品が存在する。正当な理由がある製品については、理由及び代替手段を示すことで、NAとすることを許容すべきと考える。 [修正案（青字箇所）] NAとなるための条件、基準の補足説明（以下の文章を追記） ソフトウェアコンポーネントの更新に制限がある製品 （「NAであることの理由」にソフトウェアコンポーネントの更新ができない理由と共に、ハードウェアの交換などの代替手段及び、対応期限（期間）を記載すること）	消防法（昭和二十三年法律第百八十六号）に関連し、火災報知設備又はガス漏れ火災警報設備に使用する受信機は、下記の省令によりソフトウェアのアップデートに制約がある。 昭和五十六年自治省令第十九号受信機に係る技術上の規格を定める省令 第五条他 https://elaws.e-gov.go.jp/document?lawid=356M50000008019	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
212	M17	M17-005	☆1セキュリティ要件・適合基準	5-1	☆１適合基準	[指摘内容] 適合基準①は、「情報の盗聴」に対する保護対策であることが明示されているが、②では同様の記載がないため、対策すべきリスクが、曖昧であるように読めてしまう。 冒頭に「情報の盗聴に対する以下のいずれかの保護対策を行うこと」と、対策するリスクが明示されているので、①の「情報の盗聴に対する」の記述は削除する。 [修正案（青字箇所）] ☆1適合基準 ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する以下のいずれかの保護対策が行われていること。 ① 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、~~情報の盗聴に対する~~保護対策を機器自らが行う。 ② 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ伝送される。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
213	M17	M17-006	☆1セキュリティ要件・適合基準	6-1	☆１適合基準、NAとなるための条件、基準の補足説明	[指摘内容] 適合基準②には、「脆弱性スキャンツールによる既知の脆弱性検査を実施」とあるが、評価ガイドでは「B）Bluetooth」、「C）USB」は検査対象外となる。公開文書では、評価ガイドが対象外となるため、誤解を避ける上で、「B）Bluetooth」、「C）USB」については脆弱性スキャンの対象外となる旨を、追記した方が良い。 [修正案（青字箇所）] NAとなるための条件、基準の補足説明（以下の文章を追記） 適合基準②の「脆弱性スキャンツールによる既知の脆弱性検査」は、「A）TCP/UDPポート」のみを対象とし、「B）Bluetooth」、「C）USB」については対象外とする。 ※ただし物理的なインターフェースにかかわらず、上位レイヤーでTCP/UDPポートを利用する場合は対象とする。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
214	M17	M17-007	☆1セキュリティ要件・適合基準	11-1	☆１適合基準	[指摘内容] 適合基準①記載の「C）ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名」について、「暗号鍵やデジタル署名」は削除すべき対象データの解釈が、読み手によって齟齬を生じやすく、対策のハードルが高い情報が含まれる。例えば電子証明書については、製造段階でICチップのセキュリティ秘匿領域に格納されており、データ消去が困難なケースが想定される。 また、「ユーザが設定した認証値」については、「B）のユーザ設定値」に含まれるものと解釈可能である。 従って、「C）ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名」については、記述を削除することが望ましい。 [修正案（青字箇所）] ☆1適合基準 ① ユーザによって、製品本体や関連サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下の情報を削除できること。 A) 機器利用中に取得した情報資産（個人情報含む） B) ユーザ設定値 ~~C) ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名~~		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
215	M17	M17-008	☆1セキュリティ要件・適合基準	11-1	セキュリティ要件	[指摘内容] 「ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。」とあるが、日本語としては主語がユーザとなっているため、ユーザの義務のように誤解を与える。 [修正案（青字箇所）] ☆1適合基準 製造業者は、ユーザが簡単な方法で製品からユーザデータを消去できるような機能を提供しなければならない。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
216	M17	M17-009	☆1セキュリティ要件・適合基準	17-2	☆１適合基準	[指摘内容] 適合基準「④対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること」について、製造メーカとしては、「サポート期限」を明確化することが難しいという意見も出ている。また「方針」という記述は、曖昧な点があるため、文章の変更を提案する。 [修正案（青字箇所）] ☆1適合基準 ④セキュリティに関するサポートを終了する場合、終了となるサポート内容の詳細を、サポート期限が満了する前に利用者へ周知すること。		いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
217	M17	M17-010	☆1セキュリティ要件・適合基準	全般	脚注表記	[指摘内容] 「The Security Requirements and ☆1 Conformance Criteria (1-1 to 17-3, 17-8) within this document are extracted from the ETSI EN 303 645 ©European Telecommunications Standards Institute 2020.」とあるが、「Conformance Criteria」はETSI EN 303 645から抽出したものではないと思われる。 [修正案] 脚注 「The Security Requirements (1-1 to 17-3, 17-8) within this document are extracted from the ETSI EN 303 645 ©European Telecommunications Standards Institute 2020.」	ETSI EN 303 645 には「Conformance Criteria」の記載は該当しないため。	誤記となりますので、修正します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映）

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
218	M17	M17-011	☆1セキュリティ要件・適合基準	用語集		[指摘内容] 「【別添】☆1セキュリティ要件・適合基準」の中に出てこない用語がある。 例：「外部感知機能」 [修正案] 「【別添】☆1セキュリティ要件・適合基準」の中に出てこない用語を削除する。	読者の混乱を招く可能性があるため。	「外部感知機能」は、別途公開している最終とりまとめの別添１「セキュリティ要件一覧」のセキュリティ要件8-3(☆１では対象外)で使用している用語となります。「用語集」は制度全体として使用する想定であり、「☆１セキュリティ要件・適合基準」で使用されていない用語が含まれることもあります。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
219	M17	M17-012	☆1セキュリティ要件・適合基準	用語集	機密セキュリティパラメータ	[指摘内容] 「機密セキュリティパラメータ」を「重要なセキュリティパラメータ及び公開セキュリティパラメータ。」と説明されているが、機密情報でありながら、公開パラメータを含んでいることは、矛盾する記述のように受け取れる。 [修正案] 「慎重に取り扱うべき」「重要な」「センシティブ」等と記載したほうがよい。	ETSI EN 303 645で定義されている「sensitive security parameters」のことだと思われるが、定義上明確に公開情報（公開セキュリティパラメータ）を含むのであれば「sensitive」の訳語として「機密」は避けたほうがよいと思われる。	こちら用語は、IPAから発行しているETSI EN 303 645 V2.1.1の「3.1 用語」の翻訳を基に作成しています。使用する訳語の見直し要否については、当該翻訳との整合性の観点も含めて今後検討します。 【参考】欧州規格 ETSI EN 303 645 V2.1.1 (2020-06)の翻訳(IPA) https://www.ipa.go.jp/security/controlsystem/etsien303645.html
220	M17	M17-013	☆1セキュリティ要件・適合基準	用語集	重要なセキュリティパラメータ	[指摘内容] 「機密セキュリティパラメータ」での指摘通り、「機密セキュリティパラメータ」の「機密」を「重要な」と変更した場合に訳語が重なる。 [修正案] 「機密の」「非常に重要な」「クリティカル」などとしたほうがよい。	ETSI EN 303 645で定義されている「critical security parameters」のことだと思われるが、定義上明確に秘密情報となっており、「sensitive security parameters」ではなく、こちらを「機密」としたほうがよいと思われる。また、「critical」なので、「非常に重要な」「クリティカル」なども候補に挙がると思われる。	こちら用語は、IPAから発行しているETSI EN 303 645 V2.1.1の「3.1 用語」の翻訳を基に作成しています。使用する訳語の見直し要否については、当該翻訳との整合性の観点も含めて今後検討します。 【参考】欧州規格 ETSI EN 303 645 V2.1.1 (2020-06)の翻訳(IPA) https://www.ipa.go.jp/security/controlsystem/etsien303645.html
221	M18	M18-001	☆1セキュリティ要件・適合基準	1-1,1-2,1-3	セキュリティ要件	・#1-1のセキュリティ要件案を☆１評価番号1として残し、#1-2のセキュリティ要件案は#1-1に統合する。 ・#1-2の適合基準案は#1-1に対する適合基準案とする。 ・☆１評価項目番号を以下に修正する。 要件　（現）評価項目番号　→　（変更）評価項目番号 #1-1　－（#1-2の適合基準に統合）　1 #1-2　2　－　（#1-1の適合基準に統合） #1-3　1　2	・#1-2のセキュリティ要件と適合基準の不整合の是正。 #1-2 セキュリティ要件を基に、適合基準案①、②を要求するのは無理がある。 #1-2の適合基準案①、②は、#1-1セキュリティ要件案に対する適合基準案とするのが妥当。 （#1の意見と意味合いは同じで、セキュリティ要件ではなく、適合基準を修正する案です）	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
222	M18	M18-002	☆1セキュリティ要件・適合基準	1-2	☆１適合基準	パスワード長に関する規定は、ブルートフォース攻撃への対抗を意図したものであるため、#1-5のブルートフォース対抗メカニズムの要件に移動すべき。 ☆１適合基準： 機器に対するネットワークを介したユーザ認証の仕組み、又は、機器初期設定時のクライアント認証の仕組みにてパスワードやパスコードを使用する製品において、~~製品導入時にデフォルトパスワードが使用される場合に、~~以下の①・②のいずれかの基準を満たすこと。 ① 製品導入時のデフォルトパスワードは、機器毎に異なる一意の値であること。 ② ~~デフォルトパスワードは、~~初回起動時にユーザによるパスワード変更または設定を必須とする機能を実装すること。 評価手順： ［ドキュメント評価］製品の技術文書において、製品導入時にデフォルトパスワードに関する対策が明示されていることを評価する。デフォルトパスワードに関して、以下の①～②のいずれかを満たす実装が明示されている場合に限り、本適合基準の評価結果が「Y」となる。 ①デフォルトパスワードは、機器毎に一意なパスワードである。 ②初回起動時にユーザによるパスワード変更または設定を必須とする機能を実装している。なお、ネットワーク機能を使用せずとも利用可能な製品の場合、初回起動時ではなく、ネットワーク機能を初めて使用する時にユーザによるパスワード変更を必須とすることで、本条件を満たしていると見なす。 ※ 管理者がメンテナンス時に利用するための認証についても対象とする。	■修正提案前の適合基準②においてデフォルトパスワードを変更する実装が前提になっているように読み取れるが、必ずしも変更に限定する必要は無いため、ユーザによってパスワードが変更または設定されること要件とすべきである。現状では初期パスワードなしに、初回起動時に新規にパスワードをユーザが設定する場合の規定が漏れている。 ■パスワード長に関する規定は、ブルートフォース攻撃への対抗を意図したものであるため、#1-5のブルートフォース対抗メカニズムに移動するのが適切である。 ■「機器毎に異なる一意」という表現は、「異なる」と「一意」が意味的に重複しているので、「機器ごとに一意」とすべきである。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
223	M18	M18-003	☆1セキュリティ要件・適合基準	1-5	☆１適合基準	#1-2のパスワード長に関する規定は、ブルートフォース攻撃への対応メカニズムの一部を構成するものであるため、本要件に記載することが適切である。 ☆１適合基準： 機器が、制約のある機器ではない場合、機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。 なおブルートフォース攻撃の対抗手段としてパスワード長を規定する場合は、以下の要件を満たすこと。 ① 機器ごとに一意なデフォルトパスワードである場合：6文字以上のパスワードであること。 ② 初回起動時にユーザがパスワードを変更または設定する場合：8文字以上のパスワードであること	パスワード長に関する要件は、ブルートフォース攻撃の対抗メカニズムと不可分であるため、本要件で規定するのが適切である。	パスワード長もブルートフォース攻撃の対策の一要素となりえますが、それだけでは十分とはいえず、1-5の適合基準に関しては、別途公開している☆１評価ガイドのとおり、認証試行回数や多要素認証を求めています。
224	M18	M18-004	☆1セキュリティ要件・適合基準	3-3	☆１適合基準	「製品においてアップデートメカニズムが実装されている場合、そのアップ デートは、ユーザが簡単に適用できるものでなければならない。」に関して、NAとなるための条件として「ファームウェアアップデートを第三者（運用担当者、保守担当者など）で行う場合」を追加すべき。	製品によっては第三者(運用担当者、保守担当者)がファームウェアアップデートを実行する運用形態となっているものがあるため。 また「17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない」の☆1評価ガイドには ［アップデートの実行者］－ユーザで行うのか、製造業者で行うのか、第三者（運用担当者、保守担当者など）で行うのかを明示する とあって、第三者の保守も想定されているため3-3の記載との矛盾が生じているため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
225	M18	M18-005	☆1セキュリティ要件・適合基準	4-1	☆１適合基準	「ネットワーク経由の不正アクセスに対して、セキュアに保存されること」という要件に対して、評価手順ではストレージの暗号化を求めているが、暗号化では「ネットワーク経由の不正アクセス」への対抗策にはならないと考えられる（例えばユーザーになりすましてネットワーク経由から不正アクセスした場合、暗号化されたデータが正しく復号されて読み出せてしまうため対抗出来ているとは言えない。また、正規I/Fを利用せず直接ストレージ内のデータに不正アクセスすることが出来れば暗号化が意味を成すが、この攻撃は非常に高度であり☆１が想定する脅威レベルを超えていると考えられる）。「ネットワーク経由の不正アクセス」に対する有効な対抗策はアクセス制御である。しかし、アクセス制御は既に要件1-3で定義されており重複している。 また、ストレージの暗号化が有効な対抗策となる脅威は、「ネットワーク経由の不正アクセス」ではなく、「ストレージの持ち出し」と考えられるが、☆１で想定する攻撃界面として運用環境内の物理的なアクセスは想定しない旨記載されているため、この脅威は対象外と考えらえる。 以上のことにより、本要件は適切ではないため削除が妥当と考えます。	脅威と対抗策の課題定義が合致していない。	正規ユーザになりすました不正アクセスに関しては、要件1-3で対策することとなります。本適合基準では、「正規ユーザのアクウント等ではないがストレージにアクセスされる状況」を想定した対策となります。 なお、誤解が生じないように表現方法について検討します。
226	M18	M18-006	☆1セキュリティ要件・適合基準	5-1	セキュリティ要件	セキュリティ要件の「製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。」に関して、以下の文言に修正すべき。 「製品は、製品用途の特性等に適した想定するリスクを低減できる技術を使用してセキュアに通信をしなくてはならない。」	通信について「ベストプラクティスの暗号技術」の使用を要求しているのに対して、ユーザ認証メカニズムについては「製品用途の特性等に適した想定するリスクを低減できる技術」の使用となっており、要求レベルに差異が生じている。☆1はIoT製品に最低限求められるセキュリティ要件であり、「製品用途の特性等に適した想定するリスクを低減できる技術」の使用に統一すべきである。 なお製品用途の特性等に適した想定するリスクを低減できる技術としては、#1-3評価ガイドに記載されたE）通信を許可する対象をIPアドレスなどで制限する。 F）通信を許可する対象をLAN内の機器のみに制限する などが該当する。	3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
227	M18	M18-007	☆1セキュリティ要件・適合基準	5-1	☆１適合基準	#5-1のセキュリティ要件を「製品は、製品用途の特性等に適した想定するリスクを低減できる技術を使用してセキュアに通信をしなくてはならない。」に修正する提案に伴い、☆1適合基準に関して下記のように変更すべき。 **適合基準：** ネットワーク経由で伝送される守るべき情報資産に対する保護対策を実施しなければならない。 なお想定する運用環境ごとに、機器で以下のような対策をする場合は、リスクを許容可能なレベルに低減したと見なしても良い。 ■保護されたネットワーク環境（例：イントラネット環境、VPN環境や専用線を経由したサーバへの接続）： ・通信機能およびセキュリティ機能に関する設定に関わる通信を暗号化する ・機密の個人データの送受信を主目的とする機能に関わる通信の暗号化する ・通信を許可する対象をIPアドレスなどで制限する ・通信を許可する対象をLAN内の機器のみに制限する ■インターネットを経由した通信 ・インターネット上を送受信する守るべき情報資産の暗号化	■通信の保護対策については、想定する運用環境ごとに整理する方が理解しやすい。 ■保護されたネットワーク環境における通信とインターネットを経由した通信とでは、脅威の強さと損害の発生の度合いが異なるため、リスクに応じた技術解を提示すべきである。保護された環境においては、盗聴の脅威に関して許容不可能なリスクの想定が限定的であるため、☆１適合基準としては、機器のセキュリティ機能に影響を与える通信機能およびセキュリティ機能に関わる設定と、開示が個人に害を及ぼす可能性の高い「機密の個人データ」の暗号化に限定した記載とすべきである。EN 303 645でも「機密の個人データ」の暗号化のみがshallになっていることも留意すべきである（規定5.8-2）。 ■多様な機器が対象となる☆１適合基準においては、技術解を限定するべきではない（☆2以降の製品分野別規格等での要請との矛盾が生じることを懸念）。一方で適切な技術での対応を促すためには、具体的な例示がある方が望ましい。従って規格において許容を表現する「良い(may)」を用いて具体的な技術解を列挙する形が望ましい。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
228	M18	M18-009	☆1セキュリティ要件・適合基準	6-1	☆１適合基準	①の記載が背景説明と要求事項とが混在しているので分かりにくくなっている。背景説明は注記として分離するのが望ましい。なお現状の記載だと「USBインタフェースはリスクが許容できないので必ず無効化しなければならない」とも読める。 Before: ①製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A) TCP/UDPポート　B) Bluetooth　C) USB After: ① 製品の利用上不要である場合、以下のインタフェースを無効化すること。 A) TCP/UDPポート　B) Bluetoothプロファイル　C) USBデバイスクラス 注）これらのインタフェースは、攻撃界面として典型的なものであり、攻撃にも使用可能な標準的なツールが存在すると共に、マルウェアなどの攻撃対象になる可能性も高い。従って、該当インタフェースが製品の意図する使用に無関係である場合は、あらかじめ無効化しておく対策が有効である。	■①の要求事項が誤解を受けやすい記載であるため修正を提案する。 ■USB/Bluetoothの無効化の方法については、評価手順においてプロファイルやデバイスクラスレベルでの無効化を検証しているので、評価手順に合わせるべき。なおBluetooth/USBに関しては、製品利用上搭載すべき要求が存在しない場合、コスト上の理由から、I/F自体搭載されることはない。従ってI/F自体の無効化については規定しなくても良い。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
229	M18	M18-010	☆1セキュリティ要件・適合基準	17-2	☆１適合基準	「②製品のセキュリティアップデートの内容や必要性、アップデートを行わない場合の影響などを周知すること。」という記載があるが、下記記載に修正いただきたい。(太字は差分箇所) 「②製品のセキュリティアップデート**のリリース時には、そのアップデートの**内容や必要性、アップデートを行わない場合の影響などを周知すること。」	要件の「セキュリティアップデート」が一般用語としてのセキュリティアップデートを指しているのか、個々のセキュリティアップデートを指しているのか、記載の文言では判断が難しいため	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
230	W01	W01-001	制度構築方針案	全般		IoT機器が一般国民の安心安全だけでなく、我が国、そして同盟国有志国などの国家安全保障にも深く関わる今日、重要インフラや防衛産業、機微技術といった領域、そしてそれに間接的副次的にIoT機器が選ばれる中、安直に、ハードウェア、ソフトウェア、ファームウェアなどの製造に関わるサプライチェーン（国、組織）を性善説的にとらえ製品が選ばれないよう、注釈すべきである。 （例として、取扱説明書などに記載される「高度な信頼性を必要とする設備や機器やシステムなどへの組み込みや使用は意図されておりません」のような表現で、「国家安全保障や重要インフラ、機微技術に関わる場面での利用に対する一定の保証や目安を与えるものではない」などを制度上明記するなど。 また、IoT機器を含んだサービスとして、実際にIoTの存在や、インターネットの利用が見えないようなサービスなどでは、システム構成を物理的に把握し、想定外のリスクがまぎれこまないように、など最近のアタックサーフェイス経由で攻撃をうけるリスクを想定した注意書きを明記すべきではないか。		サイバーセキュリティ戦略（令和３年９月 28日閣議決定）でも示されているサプライチェーン・リスクに関して、本制度でも考慮することを3.5.に記載します。
231	W02	W02-001	制度構築方針案	3.4.	１３ページの最下行の２行上	「また」は「また、」のほうがよい。		いただいた意見のとおり修正します。
232	W02	W02-002	制度構築方針案	3.8.1.	１９ページの本文の最下行の６行上	「NISC」は「内閣サイバーセキュリティセンター(NISC)」のほうがよい。		いただいた意見のとおり修正します。
233	W02	W02-003	制度構築方針案	4.1.	２４ページの３行目	１９ページの２行目「当たって」と、２４ページの３行目「あたり」とは、どちらかに字句を統一したほうがよい。		いただいた意見のとおり、P.24(4.1.の記載)を「当たり」に修正します。
234	W02	W02-004	制度構築方針案	1.	２ページの４行目	「情報処理推進機構」は「独立行政法人情報処理推進機構」のほうがよい。		いただいた意見のとおり修正します。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
235	W03	W03-001	その他	-		意見募集要項をPDFファイルに差し替えてください。		2024年3月18日にパブリック・コメントの資料にPDF版のファイルを追加しました。
236	W04	W04-001	制度構築方針案	5.		IoTサイバーセキュリティ研究会の最終とりまとめに2024年度上期に「IoT製品主要ベンダー・業界団体へ☆1の概要説明・ラベル取得準備依頼」、2024年度下期に「IoT製品主要ベンダーからの申請予定の受付・事前評価・QA対応」という記載がございます。本内容につきまして、企業が限定されず広く企業が参加できるよう実施して頂きたいです。		今後、関連業界団体や一般参加者が参加可能な説明会の開催等含めて、広く本制度の普及促進に向けて活動を進めて参ります。
237	W05	W05-001	☆1セキュリティ要件・適合基準	3.	「3. ソフトウェアを最新の状態に保つ」について	「古いソフトウェアで更新されないこと」を追加する必要があると考えます。 ※脆弱性のある古いバージョンのソフトウェアを攻撃者が所持していた場合のリプレイ攻撃対策のため。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
238	W05	W05-002	☆1セキュリティ要件・適合基準	4.	「4. 機密セキュリティパラメータをセキュアに保存する」について	次の項目を追加する必要があると考えます。 ・暗号化により保護する ・暗号鍵は、機器のソフトウェアのソースコードにハードコードしない。セキュアエレメント等に保管する。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
239	W05	W05-003	☆1セキュリティ要件・適合基準	5.	「5. セキュアに通信する」について	「同じ通信データを2回受信しないこと」を追加する必要があると考えます。 ※過去の通信データを攻撃者が所持していた場合のリプレイ攻撃対策のため。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
240	W05	W05-004	☆1セキュリティ要件・適合基準	6.	「6. 露出した攻撃面を最小化する」について	「内部基板上のSoC等のデバッグポートは無効、または、パスワード等で不正アクセスから防御する」を追加する必要があると考えます。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
241	W06	W06-001	制度構築方針案	3.1.	p7「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」を説明する文章	本制度の技術審議委員会と同格の委員会(もしくは技術審議委員会の配下のWG)の設置の可能性について提案する。「」で囲まれた文章が本提案による追記文章。 ==原文開始===== 運用体制案を図 3.1-1 に示す。(中略)☆2 以上の適合基準検討WG は、当該製品類型の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。 ==原文終了===== 「さらに、IoT におけるエマージングな製品の類型に対するセキュリティ適合性評価制度の整備に向けた中長期展望(ロードマップ)を検討する場として、本制度の技術審議委員会と同格の委員会(もしくは技術審議委員会の配下のWG)を設置することも視野に入れる。」	IoT 機器の製造・開発においては、適合基準案WG で審議するためのセキュリティ要求仕様に対して準備が不完全な中小企業が多数存在する可能性がある。また、多くのIoT製品が新たに開発される中、適合基準の定められた製品類型には当てはまらない製品が出てくることが想定される。 このため、中長期の視野に立ち、本制度が扱う製品類型をIoT 製品市場に合わせて適切に増やしていくための本委員会（もしくはWG）の設置が重要と考える。本委員会（もしくはWG）では、例えば、市場からボトムアップで新たな製品類型を追加することや、中小も含め多くの企業が自社製品に合わせたセキュリティ要求仕様書の策定を行うインセンティブを提供すること等を検討する。 これを実現するための一つの案として、セキュリティ要求仕様書の簡易な評価とそれを公知にするための仕組みを設けることが考えられる。より具体的には、一定のレベルのセキュリティ要求仕様書を、従来より軽量な形で評価した物について、公的機関や関係団体のホームページで「プレ評価済みセキュリティ要求仕様書」といった名称で公知にしてプロモーションをすることが考えられる。	いただいた意見は、図3.1-1の右側「運営事務局」欄に記載の「制度拡張（☆２）以上の検討」や「IoT製品ベンダーへの認証取得促進」の範疇と考えており、その審議は「運営審議委員会」で実施する想定です。
242	W07	W07-001	その他	-		「IoT製品に対するセキュリティ適合性評価制度構築 方針案」がPDFで公開されていますが、電子的な可読性を確保するため、最低限でもしおり付きPDFで公開されるべきだと思います。別添のセキュリティ要件・適合基準は、その利活用を考えると、Excelでも提供されるべきであると考えます。		2024年3月21日にしおり付きPDFファイルに差し替え済みです。別添のExcelファイルは制度開始時に必要に応じて公開します。
243	W07	W07-002	制度構築方針案	3.7.		「悪質であった場合、もしくは調達者・利用者に与える影響が大きい場合」と記載されています。公用文、法文等では、“又は”、“若しくは”等の使い方がルール化されており、階層が1つのorは、“もしくは”ではなく、“又は”を使うことになっています。特別な理由がない限りは、そのルールに準じた記載にしたほうがよいと考えます。		いただいた意見のとおり修正します。（1.の「もしくは」も修正）
244	W07	W07-003	制度構築方針案	3.8.		3.8.1が存在するときに、3.8の直下に文章を記載することをぶら下がり段落(hanging paragraph)といい、JIS(ISO, IEC等)では禁止されている文書構造である。本書はJISではないが、特別な理由がない限り、そのルールに準じたほうが望ましい。		3.8.直下の文章は、3.8.1.～3.8.3.の構成を説明する文章であり、その内容に影響を与えるものではありません。JISの当該ルールを確認しましたが、本文書では対応の必要がないと判断しました。
245	W07	W07-004	制度構築方針案	3.4.		本書の要求事項に関しては、JIS化及びISO/IEC化して不適切な貿易障害といわれないようにする必要がある。		消費者用IoT製品の適合性評価制度に関する要件は、ISO/IEC27404として現在検討されており、既に連携しています。今後もISO/IEC等の議論とは連携します。
246	W08	W08-001	☆1セキュリティ要件・適合基準	1-3,1-4	セキュリティ要件	要件1-3の☆1適合基準では「TCP/UDP通信」、要件1-4の☆1適合基準では「ネットワーク」という用語が使われている。 これらが同じ意味で使用されているのであれば、用語を統一していただきたい(例えば、すべての用語を「TCP/UDP通信」に統一する)。 異なる意味で使用している場合は、用語を分けている理由を説明いただきたい。	「ネットワーク」はBluetoothも含むことになると考えられるが、要件1-4においては、☆1適合基準や☆1評価ガイドを見る限り、その意図はないと思われる為	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
247	W08	W08-002	☆1セキュリティ要件・適合基準	6-1	☆1適合基準	「物理的インタフェース及び論理的インタフェースとして、A) TCP/UDPポート B) Bluetooth C) USB のみ記載されているが、この3つのインターフェースのみを無効化の対象とすればよいとしたことの理由を記載いただきたい。	物理的インタフェース及び論理的インタフェースは記載の3つの他にもMiracastやシリアルポート、SDカード等があるにもかかわらず、記載の3つのみをチェックすれば☆1のセキュリティ要件として十分であることの理由が不明であるため	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。 なお、☆１レベルでは、まずはA)～C)の三つのインターフェースの無効化の優先度が高いと判断し、このような適合基準としています。
248	W08	W08-003	☆1セキュリティ要件・適合基準	6-1	セキュリティ要件、☆1適合基準	【要件】「6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。」、 【☆1適合基準】「1 製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。」という記載がある。 これらを以下のように修正いただきたい。 【要件】「すべての未使用の物理的インタフェース及び論理的インタフェースは無効化できること」 【☆1適合基準】「1 製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、製品の利用上不要かつ攻撃を受けるリスクがある場合は、ユーザーがインタフェースを無効化できる手段を備えること。」	製品の利用上不要なら、通常はコストアップにつながるようなBluetoothやUSBは搭載しない。そのため、要件の「(製品として)すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。」という記載は、あまり現実的ではない。 製品としては必要なI/Fだが、お客様が使用しない場合はリスク回避のためにI/Fを無効化するということを意図していたのではないかと推測した為。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
249	W09	W09-001	☆1セキュリティ要件・適合基準	3-7		評価項目番号＃8の適合基準には記載のない、「ベストプラクティスの暗号技術を使用しなければならない」の記載があります。 これは削除すべきではないでしょうか。 「ソフトウェアの完全性をアップデート前に確認できる仕組み」の実装方法は、必ずしもベストプラクティスのハッシュを用いずとも、CRCチェックや暗号化（復号化が正しくできることの確認）で☆１のレベルではOKにすべきと考えます。		いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
250	W09	W09-002	☆1セキュリティ要件・適合基準	3-10		評価項目番号＃8の適合基準には記載のない、「信頼関係を介して～検証しなければならない」の記載があります。 これは削除すべきではないでしょうか。		3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
251	W09	W09-003	☆1セキュリティ要件・適合基準	17-3		「そのアップデートによって軽減されるリスクに関する情報とともに」とありますが、ETSI では推奨になっています。 推奨ではなく必須にする意図でしょうか。		重要性を考慮し、☆１評価項目番号＃16の☆１適合基準②の内容にて必須で求めることとしています。
252	W09	W09-004	制度構築方針案	3.8.3.		相互承認が得られると国内メーカーの海外での販売の障壁が大きく下がります。 当然、逆に海外メーカーの国内での販売の障壁も下がりますが、それでもセキュリティが強化された製品の選択肢が増え、日本社会全体の利益になると考えます。 ぜひ推進をお願いいたします。		制度構築方針案への賛同の御意見として承りました。
253	W10	W10-001	制度構築方針案	3.3.	P 10 図 3.3-1 適合性評価レベルのイメージ図 前後	自己適合宣言（★1,★2)の適合評価結果の内容において、実際にどのようなハードウェア構成、ソフトウェア構成で評価を行ったのかがわかるような内容となる証跡は必要と考える。	証跡が有ることにより、第三者認証（★3以降）において外部機関による検査が行われる場合に証跡に基づく必要とされる時間的・費用的なギャップを埋める効果が期待できる。	自己適合宣言における証跡は、評価ガイドに従い、IoT製品ベンダーにて保管することとなります。 いただいた意見のように証跡に求める要件を詳細に規定することは、IoT製品ベンダーの負荷が増加する懸念もあるため、現時点では想定していませんが、今後、評価のベストプラクティスや証跡のサンプル・テンプレートのようなものを整備する際の参考にします。
254	W10	W10-002	制度構築方針案	3.3.	P 10 図 3.3-1 適合性評価レベルのイメージ図 前後	一方で、この証跡を提出することにより自社のノウハウの流出（実際にはIPA/経産省が参照するのみの範疇だが）と考える企業はゼロとは言えない事は課題と考える。	評価実施額と、第三者機関による実施評価額とのギャップを埋めることにより、より高いセキュリティレベルでの機器実装と評価をスムーズに行う事を意図する。	表3.5-2に記載のとおり、自己適合宣言における証跡は、IoT製品ベンダーにて保管することとしています。なお、3.7.に記載のとおり、必要に応じてIPAは証跡の提出を求めることがあります。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方針です。
255	W10	W10-003	制度構築方針案	3.3.	P 10 図 3.3-1 適合性評価レベルのイメージ図 前後	将来的にAppendexとして方法（ハードウェア、ソフトウェア）として、この手法で行いましたと記載できるよう、オープンソースとして公開し、公開した方法の何を使って、どのような結果となった事によりＯＫとしたのかの証跡が残るようにした方が良いと考える。	オープンソースとすることについては、我が国においてはIPv6Readyスキームの事例と比べた場合に、その有無によって認証すべき技術の認定が信頼すべき手法によって行われた事による技術進化の速度を参考にしたい。	いただいた意見は、今後の検討の参考にします。
256	W10	W10-004	制度構築方針案	3.8.2.		先般、ファーストフード店において機器の整合が取れない事によるセキュリティインシデント(*)が発生、これが世界中に拡大被害された。この点から自販機協会との連携時期をより具体化して明記し、本適合性評価制度により、セキュリティインシデントを未然に防ぐ事を企図した記載が必要と考える。 *https://corporate.mcdonalds.com/corpmcd/our-stories/article/global-tech-outage.html	それ以前のセルラーの大規模障害から俯瞰して見ても同様のセキュリティインシデントは悪意のある攻撃以外の手段、この場合は人によって発生している事が繰り返されている事から、IoT機器、特にIT/OTのマネージメントシステムの一環としてPDCAの対応は必要。	いただいた意見は、今後の検討の参考にします。
257	W10	W10-005	制度構築方針案	3.8.2.		ドローンの応用、実用は予想より早く、世界中で利用されている。この点からドローンについて★1，2について決めておく必要がある。	セキュリティ要件、認定要件は既にNEDOのプログラムで確定している筈。よって認定スキームを速やかに載せる必要がある。	いただいた意見を考慮し、関係省庁や関係団体とも連携しながら、制度構築を図っていきます。
258	W10	W10-006	制度構築方針案	3.8.3.		元々は、英国政府のCode of Practiceから派生したものであることから、各国が前広に捉えて連携できる仕組みが望ましい。	世界的に労働人口が不足傾向にある事から、保守的に縛るよりも労働人口の不足を各国間で補う仕組み作りが望ましい。	既に一部の協議は開始していますが、諸外国とは積極的に連携し、最終的には相互承認を確立する方針で検討を進めています。
259	W10	W10-007	☆1セキュリティ要件・適合基準	全般		適合基準評価制度における制度のアップデートのきっかけとして、アタックベクタが企図しない用途で悪用される場合について、任意のタイミングで見直し、補正をする必要がある。	ここ数年のセキュリティインシデントを見ても、企図しない用途に転用する事によってセキュリティインシデントが発生している傾向にある。 また、本件、SBOMでは精度面でばらつきの課題がありSBOM導入に関しては特にスタートアップ企業への負担が大きい。	制度構築方針案の3.4.に記載のとおり、「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。」こととしています。
260	W11	W11-001	制度構築方針案	全般		今回提案のセキュリティ適合性評価制度について賛同いたします。 今回の取り組みはルータ単体ではどうしても防ぎきれないネットワーク内IoT機器のセキュリティ向上に資すると考えており、国内のサイバーセキュリティ防御を一層高めるものとして当会も制度の具体化に協力させていただきたいと考えております。		制度構築方針案への賛同の御意見として承りました。
261	W11	W11-002	制度構築方針案	3.5.	図 3.5-1 ☆1、☆2 における適合性評価の流れ (本文p15)	2～3までの期間はどれくらいを想定しているか具体的な例の記載をお願いいたします。	記述があいまいであるため。	申請手続方法の詳細については、年内（2024年12月末まで）に公表する予定です。
262	W11	W11-003	制度構築方針案	3.6.	ラベル制度について (本文p16)	ラベルデザインに関する運用ルールについて、過度にコストがかからないよう配慮をお願いいたします。また、有効期間の延長を行った際、ラベルの貼り替えを要するなど無いよう、過度な負担のかからない制度となるよう配慮をお願いいたします。	ラベルが大きすぎたり、材質にコストのかかるデザインの設計がされる場合は製品コストに少なからず影響を与えることを懸念しております。また、製品在庫に貼り替えなど加工が必要となると金銭的な負担だけではなくサプライチェーンの上下流にも負担を強いることになりかねません。	3.7.に記載のとおり、ラベルの貼り付けは任意とし、また有効期限等はラベルに掲示せずQRコードから本制度の情報提供ページにアクセスし、最新情報を確認できる仕組みを想定しています。
263	W11	W11-004	制度構築方針案	3.7.	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。(本文p17)	ラベルは製品本体やパッケージに記載せずに、Webサイトのみ表記の運用でも問題は無いか不明なため、具体例や必須範囲の記載、もしくは製造業者に一任するなど記載の追加をお願いいたします。	記述があいまいであるため。	引用箇所の本文に記載のとおり、ラベル（ロゴ等）の掲載は、IoT製品ベンダーの任意であり、一任していると明記しています。消費者向け製品の場合は、本体等への掲載を推奨する等は今後検討します。
264	W11	W11-005	制度構築方針案	3.7.	検証事業者、評価機関の説明は、0節を参照のこと。(本文p17)	参照先の誤りと思われます。		「4.3節」への参照の誤植となりますので、修正します。
265	W11	W11-006	制度構築方針案	3.7.	☆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。(本文p18)	機器の特性や実情に応じた有効期間の延長、ないし有効期間延長手続きの簡素化を検討いただきたいです。	IoT製品は機械可動部が少なく、製品によっては10年以上の設計寿命を持つ製品も少なくありません。また、市場競争に伴う型番の細分化、需要者の細分化により多くの型式番号の更新・維持が必要となり、2年ごとの更新業務の維持管理は中小企業にとっては大きな負担になると考えます。機器それぞれの実情を勘案した柔軟な有効期間の設定、もしくは事前にまとめて延長処理ができる手続きの効率化の検討をお願いいたします。	チェックリストによる自己適合という簡易な申請という形式上、☆１、☆２の有効期限は最大２年間とし、それを超える長期間の有効期間を与えることは想定していません。２年以内であれば、申請者が有効期限を設定できるようにする予定であり、ある程度更新時期を合わせていただくことは可能かと思います。 複数製品をまとめて手続できるようにすることなどは今後考慮します。
266	W11	W11-007	制度構築方針案	5.	図 5-1 今後のスケジュール案 (本文p27)	施行時期の延期（25年3月->26年3月）	本案の適合要件にはハードウェア対応が必要なものがあるため新規設計が必要な場合があります。制度施行時における周知を高める目的においては、主要となるIoT機器のラベル付与と歩調を合わせた訴求が必要と考えるため、実施時期は後ろ倒しが望ましいと考えます。	本制度は任意制度であり、順次取得可能な製品からラベル取得いただくことを想定しています。また、本制度を活用した調達が本格化する時期は、早くても2025年度半ばになると想定しており、現時点から十分な準備期間が確保されているものと考えています。そのため、現時点では、開始時期を見直す予定はありません。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
267	W11	W11-008	☆1セキュリティ要件・適合基準	全般	NAとなるための条件	「NA」の定義がないため、多義的に捉えられる恐れがあると考えます。	自己宣言においては様々な知識レベル・母国語話者が参照する可能性があり、用語の定義は正確に行うことを期待します。	項目名を「対象外（NA）となるための条件、基準の補足説明」と見直します。（2024年秋頃に公表予定の☆１適合基準の最終版に反映）
268	W11	W11-009	☆1セキュリティ要件・適合基準	1-3,3-1,9-1	なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）（別添pp.1～3）	同認定を受けた製品については技術基準適合認定番号を記載するのではなく、認証を取得したことをIoT製品ベンダーが自ら担保する制度にしていただきたいと考えます。	技術基準適合認定を受けたことを宣言の要件であることを仮定すると、i)認定を受けたのちにスキームオーナーへ申請するという手順が必要となるため開発期間の長期化につながる、ii)認定の取得制度や法改正などの経緯によって番号が変更となるケースに対して対応できない恐れがある、等の問題が発生する懸念があります。	技術基準適合認定を受けたことは自己適合宣言の要件ではなく、自己適合宣言の当該項目の評価を代替可能な条件となります。技術基準適合認定に依拠せず、個別に自己適合宣言の評価を実施しただくことは可能です。依拠することを許容する以上、認定番号の確認は必須と考えています。 なお、理由i)については、技術基準適合認定と本制度の申請～ラベル付与のプロセスやタイムラインを考慮し、例えば技術基準適合認定の申請中でも本制度の申請を受付け、その合格を前提に審査し、合格後にラベル発行（ラベル利用可）にするようなことを検討します。 理由ii)については、都度、情報を更新いただく想定です。
269	W11	W11-010	☆1セキュリティ要件・適合基準	1-5	機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。(別添pp.1)	総当たり攻撃を回避する手段の例示をお願いいたします。	記述があいまいであるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
270	W11	W11-011	☆1セキュリティ要件・適合基準	2-1,17-3,17-10	製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新 (別添pp.1)	指摘された情報の公開を義務化されると余計に攻撃に使用される可能性があるので、公開については努力義務にさせていただきたいと考えております。また公開する対象、公開方法は製造業者に一任する等方法についても製造業者側が選択できるようにしていただきたいと考えております。またタイムラインに関する具体例を挙げていただきたいと考えております。	IoT製品ベンダーが開発／販売している機種が過去から多岐に渡っており、同じような脆弱性が指摘されたとしても複数の機種に対する対処に時間が掛かる場合があります。また、サポートが終了した機種に関しては修正できないことも有り得ます。脆弱性のレベルにおいてはリスクが低いものもあり得ます。そういった状況を考慮せず、公開することは、よりリスクを高めるものと考えます。	セキュリティ要件2-1に紐付く☆１評価項目番号＃5の適合基準として、公開を求めているものは、要約すると以下3点です。 ①セキュリティの問題を報告するための連絡先 ②報告を受領した後に行う手続概要 ③ぜい弱性が解決されるまでの状況更新に関する手続概要 ②と③については、別途公開している☆１評価ガイドの中で、「詳細な手続きを公開する必要はなく、当該手続きがあることと、その手続きの概要を公開することが求められる」と補足しています。攻撃者に使用されない範囲で、これらの情報を公開することは可能と考えています。 また、タイムラインに関しては、☆１適合基準では特に求められていません。
271	W11	W11-012	☆1セキュリティ要件・適合基準	3-3	ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすること。(別添pp.1)	基準が定性的であるため、不適合であるケースの例示をお願いいたします。 例：マニュアル指示のほかにIoT製品ベンダーに問い合わせが必要、日本語での案内記述のないもの、文書の正当性が製造業者に保証されないもの（機械翻訳文書など）	記述があいまいであるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
272	W11	W11-013	☆1セキュリティ要件・適合基準	3-7,4-1,5-1,6-1	☆1適合基準	具体的な判断基準の記載がなく、今後検討されるものと認識しております。その際には、具体的な判断基準に対する意見募集の機会も設けていただきたいと考えております。	判断基準に対し、実装面の技術的可否・コストの検討が必要と考えられるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
273	W11	W11-014	☆1セキュリティ要件・適合基準	3-7	製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。(別添p.2)	アップデートにかかる通信路を暗号化するもののように読み取れますが、完全性の確認は暗号化とは関係なくハッシュ等にて確認することができると考えております。具体的な内容について記載をお願いしたいと考えております。	記述があいまいであるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
274	W11	W11-015	☆1セキュリティ要件・適合基準	3-8	製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。(別添p.2)	方針や指針はどの程度の粒度で設定すれば良いか、具体例の記載をお願いしたいと考えております。また、適時に行うべき行動が不明瞭と考えるため、いずれかの表記に変更すべきと考えます。 ・アップデート情報を準備するタイミング ・準備したアップデート情報をお客様に提供するタイミング	記述があいまいであるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
275	W11	W11-016	☆1セキュリティ要件・適合基準	3-14	製品の型式番号は、以下のいずれかの方法でユーザへ提供すること。(別添p.2)	型式番号の定義と適用範囲を明示頂きたいです。例えば、ハードウェア・ソフトウェアを同一とし、販売チャネルが異なる類似の番号（例：ABC/Retail, ABC/ECなど）について、一つの型式番号とみなしてもよいか。	上記の例のような製品が存在するため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
276	W11	W11-017	☆1セキュリティ要件・適合基準	4-1	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。(別添p.2)	製品の基板に直付けのメモリ(フラッシュやRAM)も対象になるか不明なため、対象の明確化をお願いいたします。また、不揮発領域のみを対象とするよう限定していただきたいです。	記述があいまいであるため。また、揮発領域も対象となると、そもそもセキュアに保存されたデータを展開することができなくなるため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
277	W11	W11-018	☆1セキュリティ要件・適合基準	4-1	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。(別添p.2)	ユーザによって製品のストレージに保存された、製品自体とは無関係の情報資産（例えば、NAS製品に保存されたユーザのファイル等）については、本要件の対象外となるよう明記していただきたいです。	「NAとなるための条件、基準の補足説明」には、製品の設定情報や、機器が収集した情報が対象と記載されているが、このうち後者について、ユーザが製品のストレージに保存したファイル等が「機器が収集した情報」にはあたらない解釈でよいかどうかがあいまいのため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
278	W11	W11-019	☆1セキュリティ要件・適合基準	6-1	製品において、外部からサイバー攻撃を受けるリスクを低減するために、製品の利用上不要かつ攻撃を受けるリスクがある物理的インタフェース及び論理的インタフェースを無効化するとともに、製品に対する脆弱性検査を実施すること。具体的には、以下の１・２のすべての基準を満たすこと。(別添p.3)	USBやBluetoothを具備していても、IP通信をおこなわない機器は対象外で良いのか？USBやBluetoothについても脆弱性検査が必要なのか不明であるので、具体例の提示や記載の明確化をお願いいたします。また検査が可能になるツールは提供いただけるのであれば、そのツールの情報などの記載をお願いいたします。	記述があいまいであるため。また、Bluetooth, USBについては実機評価方法に一般的な基準がなく、一部の製造業者においては困難であることが懸念されるため。	IP通信を行わない機器は、制度構築方針案3.2.の定義に当てはまらないため、本制度の対象外となります。 本項では、IP通信を行う機器が具備しているUSBやBluetoothへの対策を求めています。 なお、それらの評価手順は、本制度の最終とりまとめの別添２として別途公開している☆１評価ガイドを参照してください。
279	W11	W11-020	☆1セキュリティ要件・適合基準	6-1	すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。(別添p.3)	無効化にする手段、未使用の定義について明確にしていただきたいです。また具体的な論理インターフェース例を記載いただきたいです。	記述があいまいであるため。	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
280	W11	W11-021	☆1セキュリティ要件・適合基準	9-1	停電等による電力供給の停止やネットワークの停止により、機器の電源がOFFになった後、電力供給が再開され、ネットワーク機能が復帰した際に、アクセス制御の際に使用する認証値（パスワード、秘密鍵など）の設定及びアップデートが完了したソフトウェアが工場出荷時の初期状態に戻ることなく、電源OFFになる直前の状態を維持できること。(別添p.3)	イレギュラー状態におけるセーフティ機能やハードウェア故障を伴うセーフティ機能により、状態維持が出来なくなるケースも存在すると考えております。例外のケースも記載するなどお願いしたいと考えております。	記述があいまいであるため。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
281	W11	W11-022	☆1セキュリティ要件・適合基準	11-1	ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。(別添p.4)	「簡単な方法」についての判断基準を明記いただきたいです。ハードウェアボタン押下等による極端に「簡単な方法」を目指したものではなく、一般のユーザが利用可能な機能となっていれば良いという意図だと思いますが、その意図が分かる記載としていただきたいです。	記述が定性的であるため。また、サービスの形態（サービス業者が製品にユーザ固有の設定を書き込んで提供するなど）によっては、極端に「簡単な方法」で消去できることによって弊害が発生する恐れがあるため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
282	W12	W12-001	制度構築方針案	3.1.		CCが現行の制度であるが、EUはすでにNIS2のためのEU CCの導入を宣言していることもあり、このギャップを埋める必要がある。		いただいた意見を考慮しながら、国際連携を図っていきます。
283	W12	W12-002	制度構築方針案	3.2.		対象となる機器がラベル取得後にソフトウェア含む機能を拡張更新した場合は、自己宣言による再度ラベルの取得が必要だと考える。		3.7.に記載のとおり、評価に影響を及ぼすレベルでの製品仕様の変更があった場合は、☆１、☆２のラベルは失効し、継続する場合は、自己適合宣言を再度実施することとなります。
284	W12	W12-003	制度構築方針案	3.4.		「図3.4-2セキュリティ要件の整理方針」にはREDも含めるべき。CRAやRED、PSTIなどでは脆弱性やインシデントに関連した報告義務がある。日本ではJPCERT/CCおよびIPAが窓口となり、協調した運用が可能と考えられることから、義務化を並行して行うべきと考える。欧州で製品を販売する組織はそのための体制を構築する必要があることから、大きな負担にはならないと考えられ、寧ろ欧州のビジネスへの対応により製品のセキュリティおよび脆弱性やインシデント発生時の対処が、より速やかに行えるようになることは日本国内のサイバーセキュリティ態勢の向上の観点からも望ましいと考えられ、製造業社や販売業社が当該製品の脆弱性やインシデントに対処する窓口を設けるためにもIoTラベリングの議論と並行して進めるべき。		いただいた意見を考慮しながら、制度構築を図っていきます。
285	W13	W13-001	制度構築方針案	3.7.		「サーベイランス」について注釈を記載いただけないでしょうか	サーベイランスと検索すると医療関係の用語が検索上位となっており、文書中で意図していると思われるISOとしてのサーベイランスが表示されないため	3.7.に以下の記載を追加します。 「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する。」
286	W13	W13-002	制度構築方針案	全般		本制度の申請は製品開発の最終段階で行われるケースが多いのではないかと想定しています。 しかしその段階でチェックリストの不適合項目が見つかっても改修が難しいものが発生し、自己適合宣言においては、不適切な申請がなされる可能性があるのではないかと思われます。 上記対策として、ラベルの取り消しや一般周知の記載がありますが、そもそも設計段階からチェックリストの内容を踏まえたセキュア開発を促す記述も併せて記載いただくことで不正申請の防止に繋がると考えます。		本制度として、ラベル取得するIoT製品を普及させることにありますが、それは、完成品に対する評価で選別することではなく、セキュリティ・バイ・デザインの考え方の元、設計段階から適合基準を意識して、セキュアなIoT製品を開発し、ラベルを取得し、販売され、利用されていくことにあります。 制度周知の中で、そのようなメッセージを伝えていくこととします。
287	W13	W13-003	制度構築方針案	4.1.		本取組に賛同します。ラベル取得推進活動について、弊社も協力できるところがあれば支援させていただきます。		制度構築方針案への賛同の御意見として承りました。
288	W13	W13-004	☆1セキュリティ要件・適合基準	3.		以下項目を「セキュリティ要件・適合基準」に追加するのはどうでしょうか。 製品の利用バージョンは、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。	バージョンアップの必要可否を判断するためには利用しているバージョンも把握できるようにする必要があると考えます。	セキュリティ要件3-1に紐づく☆１評価項目番号＃6の☆１適合基準②にて、「ファームウェア（ソフトウェア）のバージョン確認が行えるなど、」としています。
289	W13	W13-005	制度構築方針案	4.1.		制度の早期利用による優遇措置を設ける、もしくは☆1開始段階からの補助金開始を検討するのはどうでしょうか。	☆1の制度開始後1年で☆2を開始するスケジュールのため、☆2開始まで審査を行わない企業・組織が一定数存在すると思われます。 ☆1開始段階から☆1の取得を促すのであれば、早期取得による優遇措置・補助金等の対策が必要かと思われます。	☆２以上の取得を視野に☆１取得控えとなることを避けるため、☆２以上を整備予定の製品類型の対象や、どのようなセキュリティ水準の製品を☆２以上として想定するのかの方針等の情報を早期に公開するようにします。 また、☆１取得済み製品が☆２以上を取得する場合の優遇措置等について今後検討していく予定です。
290	W14	W14-001	制度構築方針案	3.4.	図3.4-2	本制度は、国内外のセキュリティ制度の要件を網羅したものと解釈致します。 産業用機械業界としては、Cyber Resilience ActとIEC62443-4-1/4-2の認証を進めていると考えます。 つきましては、これらの制度との相互運用を目指し、どちらかの制度に適合していれば、他の制度の一部の要件については、適合ずみと判定できるようにして頂きたいと考えます。	昨今、深刻化するサイバー攻撃に対応するため、各国においてセキュリティ関連法令が整備されてきております。 これらの関連法令に対応するためには、各企業がいて、多くの労力が必要となることが予想されます。 つきましては、その労力を少しでも軽減するため、各制度間の相互運用についてご検討いただければ幸いです。	EUのCyber Resilience Actとは、相互承認に向けた調整を進めています。 相互承認を行わない認証制度等について、特に基準や評価ガイドに明記されている場合を除き、当該認証を取得していることをもって本制度の基準に適合することとはしませんが、当該認証を取得する際に実施した検証結果等を利活用することは認めることを検討しています。
291	W15	W15-001	制度構築方針案	3.5.		☆1,2のIoT製品ベンダーの責務に、「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」と書かれてあるが、それについて説明する責任の限度が不明確なため、調達者・利用者が要求すれば企業秘密の設計情報まで開示しなければならない懸念がある。 企業秘密を保護する方法の一案として、企業秘密に関わる情報は、調達者・利用者に開示するのではなく、スキームオーナー(IPA)が仲裁して、調達者・利用者の要求が妥当な要求であるかの判断も含め、調達者・利用者に企業秘密が開示されないようにするのがよいと考える(3.7章の最終段落に関連する記述あり)。	自己宣言の評価ルートがある例としてCEマークの場合、technical documentationは、authorityから正当な理由で要求された場合にのみauthorityに提出することが義務付けられている一方で、製品のユーザーにtechnical doucmentationを提出することは義務づけられていない。このようにCEマークは営業秘密の保護に留意が払われている。	表3.5-2に記載のとおり、評価の証跡の情報開示責任は、スキームオーナー（IPA）までとしています。
292	W15	W15-002	制度構築方針案	2.2.		既存法制度との整合性や製品ベンダーの負担軽減のために任意制度とすることに依存はないが、任意制度であることが原因となって諸外国との相互認証が困難になることが予測される。諸外国と連携を密にして是非相互認証を実現していただきたい	諸外国の法制度に適応するためのコスト、能力に限界があるため。	いただいた意見を考慮しながら、国際連携を図っていきます。
293	W15	W15-003	制度構築方針案	2.3.		ラベル取得を促進するために政府調達から導入することに異論はないが、実際の制度運用開始時にはより具体的な制度の活用・展開シナリオの提示をお願いしたい	ベンダの立場としては、2025年3月末までに全製品において対策が完了するのは困難なので、中期的なロードマップを策定して対応を進めたい、という意向があるため。	☆２以上を整備予定の製品類型の対象や、どのようなセキュリティ水準の製品を☆２以上として想定するのかの方針等の情報を早期に公開するようにします。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
294	W15	W15-004	制度構築方針案	3.2.		既存製品やシステムについての考え方を示していただきたい	図3.2-1に基づいて制度開始時のスナップショットで対象となる製品範囲はわかるが、時間軸が加わった場合の考え方がわからないため	既に販売され、流通している製品であっても、適合基準を満たせばラベルを取得することは可能です。 また、本制度の対象とするのはIoT製品であり、システム全体での取得は想定していません。3.8.2.に記載のとおり、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認証制度等の整備は、各業界団体やワーキンググループにで検討する想定であり、本制度としてはそれらと連携する方針となります。
295	W15	W15-005	制度構築方針案	3.5.		自己適合宣言、第三者認証の各々で、IoT製品ベンダー、IPA、評価機関の各々の責任を明文化していただきたい	3.5章では自己適合宣言、第三者認証のワークフローは記載されているが、各主体の責任について言及されておらず、表3.5-2も実行時の責務を述べているだけなので、マークの使用を許可することによって生じる責任や、製品にマークを付けることによって生じる責任について不明瞭である。そのため、マーク付き製品に対するインシデント発生時の責任が IoT製品ベンダーのみにかかってくる恐れがあるため	3.6.に記載のとおり、本制度のラベルは、当該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ありません。 当該IoT製品に関するインシデントが発生したとしても、その設定や利用環境、運用環境等にもよるため、一般的には利用者自身に責任があると考えられます。 販売するIoT製品にて、提供すると訴求されているセキュリティ機能が想定どおりに動作しない場合は、ラベル取得の有無に関わらず、一般的にはIoT製品ベンダーにその責任があると考えられます。それがラベル取得製品の場合でも、本制度のラベルがIoT製造ベンダーに免責を与えるものではありません。
296	W15	W15-006	制度構築方針案	3.6.		自己適合宣言、第三者認証の各々で、IoT製品ベンダー、IPA、評価機関の各々の責任を明文化していただきたい	表3.6-1でラベルの意味合いは示されているものの、それに伴う責任が記載されていないため	3.6.に記載のとおり、本制度のラベルは、当該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ありません。 当該IoT製品に関するインシデントが発生したとしても、その設定や利用環境、運用環境等にもよるため、一般的には利用者自身に責任があると考えられます。 販売するIoT製品にて、提供すると訴求されているセキュリティ機能が想定どおりに動作しない場合は、ラベル取得の有無に関わらず、一般的にはIoT製品ベンダーにその責任があると考えられます。それがラベル取得製品の場合でも、本制度のラベルがIoT製造ベンダーに免責を与えるものではありません。
297	W15	W15-007	制度構築方針案	3.7.		「自己適合宣言の有効期限はラベル取得日を起点として最大2年間」とあるが、2年以内に製品をバージョンアップした場合、バージョンアップした機能については認証が取得できていないと考える。 バージョンアップしたときの考え方を明文化していただきたい	適合宣言した商品において、バージョンアップした機能に対して、提供者、使用者との間でのトラブル発生を回避するため	製品のバージョンアップが「評価に影響を与えるレベルでの製品仕様の変更」に該当するのであれば、バージョンアップ後の製品には、バージョンアップ前の製品向けのラベルは適用されません。バージョンアップ後の製品で（必要に応じて、バージョンアップ前の製品も包含される形で評価して）新たなラベルを取得してください。 詳細については、別途、申請ガイドなどを用意する予定です。
298	W15	W15-008	制度構築方針案	4.5.		ラベル付与は製品の型式ごとではなく、シリーズごと、としていただきたい。	技術的に差異がほとんどなく、例えばメモリ容量のみの違いのような機種を型式ごと付与、となると、非効率的なため。	ラベル取得の単位は、必ずしも製品の型式単位と指定する予定はありません。セキュリティ上の機能や管理（将来的なソフトウェアのアップデート等を含む）が同一であれば、同一製品の範囲としてラベルを取得することを可能とする予定です。 詳細については、申請ガイドなどを用意する予定です。
299	W15	W15-009	☆1セキュリティ要件・適合基準	全般	NAとなるための条件	各産業の事情を考慮した場合に、NAとなるための条件に追加すべきものがないかを確認いただきたい。 例：「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」の検討メンバでNAとなるための条件を確認する。	☆1についても、例えば、産業サイバーセキュリティ研究会 WG1 工場サブワーキンググループの「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」の考え方（3.2.1 ステップ 2-1 セキュリティ対策方針の策定）に沿って弾力性をもたせられないか。	NA条件に追記すべきものがある場合、本制度事務局にご連絡ください。技術審議員会にて見直しの検討を行います。 現在のNA条件の記載の解釈の範疇（より具体的な例示など）であれば、本制度事務局と連携した上で、当該ガイドラインに判断基準に関して分野別に補足いただく（評価ガイドの参考情報としてリンクさせる）ことも検討します。 また、適合性評価の中で判断に迷うケースがあれば、別途設置する問い合わせ窓口からご連絡ください。
300	W15	W15-010	制度構築方針案	3.3.		IoT製品ベンダが☆1、☆2を取得するメリットをもう少し具体的に提示いただきたい。例：本チェックリストの提出およびラベル付与した製品は〇〇規格の認証の一部をパスできるなど。	諸外国制度との相互認証を図ることを目的とされているため、段階的にでも各規格との紐づけを具体化していくべきであると考えます。	IoT製品ベンダーが☆１、☆２を取得するメリットは、2.1.に記載しているとおりです。海外制度との相互承認の実現はその中で記載しています。国内の関連制度において、本制度のラベル取得済み製品をどのように取り扱うかは、各分野や各関連制度のオーナー等と今後協議していきます。 なお、各規格との関連性は、「別添 ☆１セキュリティ要件・適合基準」の右側の以下の列に示しています。 ・【参考】海外既存制度・文書で求められるセキュリティ要件との関係性 ・【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
301	W15	W15-011	☆1セキュリティ要件・適合基準	1-2		実装上の容易性やセキュリティレベルの高い方に合わせるために、１、2も8文字で良いのではないかと考えます。文字数を分けるのであれば、その必要性や背景について説明を追記頂きたい。	意見内容欄に記載	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
302	W15	W15-012	☆1セキュリティ要件・適合基準	1-5		IoT機器自体で認証機能を持たず、接続する機器・ソフトウェアが認証機能を保有する場合は許容されるのか、明記頂きたい。 本項目以外においても、機能のアロケーションが許容されるかについて明記頂きたい。	IoT機器によっては認証機能を機器自身が持つわけではなく、設定用ソフトウェアにて認証機能を持つ場合もあり得ると考えるため。	「NAとなるための条件」として、「ネットワークを介したユーザ認証の仕組みがない」こととしていますので、それに合致するのであればNAとしていただくことは可能です。 あるいは、IoT機器の設定用ソフトウェアが「付随サービス」として位置づけられ、付随サービスを含む「IoT製品」を対象として評価・ラベル取得いただく方が適切である可能性もあります。 また、本項以外についても、「NAとなるための条件」に合致するか否かで判断してください。 ※制度構築方針案の「関連サービス」は「付随サービス」という用語に変更しました。
303	W15	W15-013	☆1セキュリティ要件・適合基準	3-1		ソフトウェアコンポーネントとは何か明記頂きたい。 「特定のソフトウェアコンポーネント」とあるが、製品に複数のソフトウェアが含まれる場合、「必ずそれらを個別にアップデートできないといけないのか」、もしくは、「全体でアップデートする手段しか持たない場合も許容されるのか」が判断できるように記載頂きたい。	意見内容欄に記載	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
304	W15	W15-014	☆1セキュリティ要件・適合基準	3-3		「ユーザが簡単に適用できる」の「簡単に」を判断できる記載をして頂きたい。アップデートが誰でも出来てしまうと可用性に影響を与えてしまうため、権限のある人のみが実行できるようにするべきだと考えます。（これは「簡単に」に反しないか、判断できるように記載いただきたい）	意見内容欄に記載	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
305	W15	W15-015	☆1セキュリティ要件・適合基準	3-7		要件と適合基準が合致していないため、再確認頂きたい。要件は暗号化について、適合基準は完全性について記載されています。	意見内容欄に記載	3.4.に記載のとおり、適合性評価レベル（☆１～☆４）と対象製品類型にて想定する脅威に対し、セキュリティ要件（全体リスト）から必要なセキュリティ要件を抽出し、対象となるセキュリティ要件に対して各適合性評価レベル（☆１～☆４）で満たすべき基準を定めたものが適合基準となります。 ラベル取得のためには、各「適合基準」への適合性を評価いただくこととなり、「セキュリティ要件」を全てカバーする必要はありません。
306	W15	W15-016	☆1セキュリティ要件・適合基準	4-1		「セキュアに保存」とは、どのような対応が妥当であるのか判断できるような記載をして頂きたい。	–	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
307	W15	W15-017	☆1セキュリティ要件・適合基準	5-1		採用しているプロトコルが暗号化に対応していない場合はNA条件とするべきと考える（評価番号1、2のNAとなる条件と同じ）	–	暗号化可能か否かも含め、どのようなプロトコルを採用するかはIoT製品ベンダーの判断によるものと考えます。「暗号化に対応していないプロトコル」でセキュリティ要件に示したリスクへの対応ができていると判断できる場合、適合基準①・②又はNA条件に該当するかを確認ください。
308	W15	W15-018	☆1セキュリティ要件・適合基準	9-1		機器自体での対策が困難な場合、UPSを利用し、不意の電源の停止が発生しない条件での使用を推奨とすることは、許容されるのか明記頂きたい。 本要件に関わず、機器自体での対策が困難な場合に外部周辺機器でのアロケーションで対応することについて許容するか否かについて記載頂きたい。	–	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
309	W15	W15-019	☆1セキュリティ要件・適合基準	11-1		「簡単な方法」であるかを判断できる記載をして頂きたい。ユーザデータの消去が誰でも出来てしまうと可用性に影響を与えてしまうため、権限のある人のみが実行できるようにするべきだと考えますが、これが「簡単に」に抵触しないしないと考えています。（適切な権限を持ったユーザが簡単に適用できる、のような記載が良いと考えます）	–	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
310	W16	W16-001	☆1セキュリティ要件・適合基準	1-2	パスワードの要件	英国PSTIでは以下のような詳細まで記載されています。 (3) 製品ごとに一意のパスワードは次のとおりであってはなりません。 (a) 増分カウンターに基づく。 (b) 公開情報に基づく、または公開情報から派生したもの。 (c) 業界の優良慣行の一部として認められている暗号化方法またはキー付きハッシュ アルゴリズムを使用して行われない限り、シリアル番号などの一意の製品識別子に基づく、またはそこから導出される。 (d) その他、業界の適正慣行の一環として容認できない方法で推測できるもの。 現状の要件・適合基準であれば、3(a)(b)(c)に相当する簡易なパスワードを容認するような状況に見えてしまいますので、これらの内容は取り入れた方がよいのではないでしょうか？	今後、PSTIとの相互認証を視野においたときに検討しておいてよい内容であると考えたため	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
311	W16	W16-002	☆1セキュリティ要件・適合基準	1-2	パスワードの定義	英国PSTIでは以下のような詳細まで記載されています。 (4) この段落では、パスワードには次のものは含まれません。 (a) 暗号鍵。 (b) インターネット プロトコル スイートの一部を形成しない通信プロトコルでのペアリングに使用される個人識別番号。または (c) アプリケーション プログラミング インターフェイス キー。 パスワードの定義がないため、読み手に任されてしまいますが、PSTIでは上記のようなものは除くという記載があります。パスワードの定義としてどこかに定義しておいてもよいのだと思います。	今後、PSTIとの相互認証を視野においたときに検討しておいてよい内容である	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
312	W16	W16-003	☆1セキュリティ要件・適合基準	2-1	脆弱性の窓口の要件	英国PSTIでは以下のようなことが記載されています。 サブパラグラフ (2) の情報はアクセス可能で、明確かつ透明でなければならず、P が利用できるようにしなければなりません。 (a) かかる情報の事前の要求がない場合。 (b) 英語。 (c) 無料。そして (d) P の個人情報の提供を要求することなく。 上記の(b)の言語、(c)の費用面、(d)の対象者を絞ることをしない。という点について、検討しておいた方が良いかと思います。	今後、PSTIとの相互認証を視野においたときに検討しておいてよい内容である	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
313	W16	W16-004	☆1セキュリティ要件・適合基準	17-8	ソフトウェアサポート期間	サポート期限について、無料でサポートするのは製造メーカとしては大変な負担となるため、個別の有料のサポートでも本事項を満たせる旨を追加いただきたい。	今後、PSTIとの相互認証を視野においたときに検討しておいてよい内容である https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/uk_psti_act.html	いただいた意見を参考に、ラベル付与を開始までに公開予定の☆１評価ガイド等にて示すことを技術審議委員会にて検討します。
314	W17	W17-001	制度構築方針案	全般		例えば販売開始時にレベル3以上の認証を受けたIoT製品が大量に出回った後に不適合が発覚しても、型式停止のみとなり認証更新後にはレベル1未満の機器が大量に存在する状態となる。すなわち本制度の目的にそぐわない更新制度になってしまうことを懸念する。また海外では英国PSTI法のように、IoT機器が製造後にセキュリティ要件を満たさなくなった場合かつ適切な是正が実施されない場合に、罰則規定がある。 認証によるメリットとそれに相当する義務を課すことは、国際的な互換性としても重要であり、本制度にも罰則的なニュアンスの記載が必要と考える。		3.7.に記載のとおり、ラベル取得後に基準への不適合が発生した場合は、ラベル取消しの措置を講じるとともに製品情報ページにてラベルが取り消されたことがわかる表示を行います。本制度は任意制度であるため、制度として販売の停止やリコール等を求めることは困難と考えています。 なお、不適合を認識しながら虚偽の申告でラベルを取得するなど悪質な場合や、調達者・利用者に与える影響が大きい場合には、IPAがその旨を一般に周知する等の対応を検討します。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
315	W17	W17-002	制度構築方針案	全般		IoT機器の寿命は数年以上におよぶことある。例えば、政府機関や重要インフラ施設にレベル3以上のIoT機器が導入された後「ベンダが2年後の更新を停止し」かつ「途中でIoT機器のレベル３以上が取り消される事態が発生した」場合、このままでは３年目以降は無保証のままで利用し続けざる得ない状態となり、該当IoT機器を導入した政府機関のセキュリティ確保および本制度の目的達成が難しくなる懸念がある。 よって、調達要件だけでなく認証としても「将来罰則規程が追加される可能性がある」「IoT機器の利用実態を考慮し、ライフサイクルを考慮して数年程度は更新を続ける必要がある」等、製品ライフサイクルへの対応をIoT製造ベンダへ促すことが必要と考える。		本制度のラベルは、基本的には、購入時の判断基準として活用される想定であり、調達者・利用者が、機器を利用する期間においてラベル取得の維持を求める場合、個別にIoT製品ベンダーと協議していただく必要があります。
316	W17	W17-003	制度構築方針案	全般		適合性評価制度が浸透した後に調達業者（輸入業者）が機器ベンダによる表示の適正を確認する義務が生じた場合、機器ベンダが評価結果を調達業者へ開示する必要があるため、機器ベンダには調達業者への評価結果提供が必須になることを制度に取り込むことが重要と考える。		表3.7-1に記載のとおり、「適合評価結果（チェックリスト又は評価報告書等）」は情報提供ページに掲載する予定であり、調達者が閲覧可能な状態とする予定です。 なお、評価に使用した証跡にはIoT製品ベンダーの機密情報も含まれている可能性も考慮し、3.5.及び3.7.に記載のとおり、評価に使用した証跡はスキームオーナー（IPA）への開示を求めることとしています。
317	W17	W17-004	制度構築方針案	全般		IoT機器のフィンガープリントを参照して、識別・分類し可視化するアプリケーションやツールに、IoTデバイスのフィンガープリントを開示される仕組みが標準で実装される必要性の記載が必要と考える。またフィンガープリントには、脆弱性が発見された場合の対処（ソフトウェアもしくはファームウェアの更新）可否についてもデフォルトで含まれていることが望ましいと考える。 IoT機器を特定するためのアクティブスキャンをシステム運用中等に実施した際に、IoT機器側に応答するような仕組みもフィンガープリント等と同様に実装されるように示唆することが方針へ盛り込まれると、より良い制度になると考える。		いただいた意見は、今後の検討の参考にします。
318	W17	W17-005	制度構築方針案	全般		機器販売事業者とも連携し、ラベル対応済み製品を優先的に取り扱うことにメリットが生じる制度もあわせて検討することで、本制度の実効性を高めることも重要と考える。		4.2.に記載のとおり、特に消費者向けには小売事業者等と連携したプロモーションを検討する予定です。
319	W17	W17-006	制度構築方針案	2.2.		本方針案では「任意制度」とあるが、英国やEUが義務化を目指している以上、我が国においても義務化が前提である方が望ましいと考える。可能であれば、最初は任意制度とし、具体的な期限を設けていずれは義務化する方針が適当であると考える。		まずは任意制度として、セキュリティ適合基準を満たし、ラベルを取得する製品を広く普及させていく想定です。ラベルの普及状況や諸外国制度の動向等を加味しながら、将来的に義務化することの必要性については、今後の検討事項とさせていただきます。
320	W17	W17-007	制度構築方針案	3.1.		CC認証との違いについて簡単な記載があると、本制度についての理解の助けとなると考える。		制度周知の際の参考とさせていただきます。
321	W17	W17-008	制度構築方針案	3.2.		サプライチェーンの複雑化に伴う責任範囲の問題は、セキュリティや製品安全に関する重要な課題になると思われるが、本方針案では明確に言及されていない。本方針案での対象範囲は「IoT機器とその関連サービスを含む」と記載されており、下記資料を踏まえるなどして、IoT機器やサプライチェーンの各構成要素についてセキュリティの確保とその確認（信頼の証明）にも言及することが望ましいと考える。 内閣府発行「IoT社会に対応したサイバー・フィジカル・セキュリティ」推進委員会（第10回）」資料1 SIP第２期 最終課題評価WG PD自己点検結果説明資料 https://www8.cao.go.jp/cstp/gaiyo/sip/iinkai2/cybersecurity10/siryo1.pdf 「IoT社会に対応したサイバー・フィジカル・セキュリティ」		IoT機器内部で利用される各構成要素（部品）に関するセキュリティ適合基準は☆１には含まれていませんが、より上位の基準（☆３以上の想定）に含める想定です。 その議論の際の参考とさせていただきます。
322	W17	W17-009	制度構築方針案	3.2.		IoT機器の定義に汎用性を持たせているためか、曖昧な感がある。 本制度では「容易にセキュリティ対策を追加できない」IoT製品は対象とされているが、例えばスマートウォッチやテレビ等は対象該否か不明瞭である。個々の機器に対して適切した施策になるよう、具体例の記載を充実させることが重要と考える。		「容易に」は、前文の「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」ことを示しています。利用者が通常の手順に従い、任意のセキュリティ対策ソフトウェア等を追加でインストールし、セキュリティ対策を実施できるような製品か否かで判断してください。 基本的には、例示している「パソコン、タブレット端末、スマートフォン等」は対象外となりますが、それ以外は対象（適合基準を満たせば、ラベル取得が可能）と考えてください。
323	W17	W17-010	制度構築方針案	3.4.		「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。」とあるが、昨今の製造業における不正事例もあるので、併せて抜き打ち検査等による評価も考慮する必要があると考える。		スキームオーナー（IPA）が検査やサーベイランスを行う権利を有し、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を求める予定です。 制度開始当初は、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（抜き打ち検査）は実施せず、基準への適合に疑義が生じた製品に対して実施する予定です。 将来的に、抜き打ち形式でのサーベイランスの実施等も検討します。
324	W17	W17-011	制度構築方針案	3.5.		IoT製品ベンダが評価機関に対して評価依頼をする体制ではなく、IoT製品ベンダは評価機関を選定するのみで、IPAが評価機関に依頼する体制が良いと考える。 IoT製品ベンダが選定した評価機関に問題があれば、IoT製品ベンダの同意を得た上でIPAに評価機関を変更できる権限を持たせることも検討することが良いと考える。		☆３以上（第三者認証）の場合の評価機関に対する意見として回答します。 評価機関には、NITEによる認定審査を受け、組織運営的にも評価能力的にも問題がないと判定された機関だけがなれます。そのため、どの評価機関であっても適切な評価が実施できることから、申請者が評価機関を自由に選定できることで問題ないと考えます。 もし、評価機関に問題があった場合は、スキームオーナー（IPA）までご連絡ください。
325	W17	W17-012	制度構築方針案	3.6.	表3.6-1	適合基準の☆3適合について、独立した第三者である評価機関をIPAが認証するとあり、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、とある。 これを踏まえると、ラベルの信頼性確保のための仕組みなどの説明があっても、第三者の評価機関が責任を負わないのは、評価レベルの信用性担保が不十分となる懸念がある。		4.3.に記載のとおり、評価機関の認定は独立行政法人製品評価技術基盤機構（NITE）が行う予定です。 万が一、IoT製品の評価等において、評価機関が不正を行うなどの事実が発覚した場合は、認定の取消し等の措置がとられます。
326	W17	W17-013	制度構築方針案	3.7.		「指定資格」についてはIoTのセキュリティを評価するための専門資格を創設し、評価機関にはその指定資格保有者が一定数以上いることを必要要件とすることが望ましいと考える。 情報処理安全確保支援士は、サイバーセキュリティについての汎用的なスキルを有しているものの、IoTのセキュリティには特化していないためである。		4.3.に記載のとおり、評価機関の認定は独立行政法人製品評価技術基盤機構（NITE）が行う想定であり、認定基準の検討の際に参考にします。
327	W17	W17-014	制度構築方針案	3.7.		ラベルを付与する製品の開発企業自体に問題が無いかといった、セキュリティクリアランス的な要素を審査要件に加えることも重要と考える。		サイバーセキュリティ戦略（令和３年９月 28日閣議決定）でも示されているサプライチェーン・リスクに関して、本制度でも考慮することを3.5.に記載します。
328	W17	W17-015	制度構築方針案	3.8.2.		重要インフラ14分野に含まれる「医療」も、検討対象に含めることが望ましいと考える。		重要インフラ分野は検討の対象と考えております。関係省庁や関係団体とも連携しながら、調整を進めて行きます。
329	W17	W17-016	☆1セキュリティ要件・適合基準	全般		実施される審査が明確になっていないため、IoT製造ベンダがどういった対策を取ればいいかイメージが湧きづらい。IoT製造ベンダが具体的対策を取りやすいよう、審査イメージを記載することが望ましいと考える。		いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
330	W17	W17-017	☆1セキュリティ要件・適合基準	全般		単一のIoT機器が機能を実現するにあたり「内部に複数のIoT機器を内包して機能を実現している」場合の、認証やアップデート、バージョンの表示などの扱いを記載いただきたい。 内包する機器のうち１つでも、更新が停止された場合、もしくはネットワーク経由などでバージョンの確認や更新ができない場合等、認定取り消しに該当する事例を記載いただきたい。		「内部に複数のIoT機器を内包して機能を実現しているIoT機器」をIoT製品としてラベルを取得する方法と、「内包されているIoT機器」が単独で販売されておりIoT製品と見なせる場合は各IoT機器ごとにラベルを取得する方法が考えられます。 前者の場合は、内包しているIoT機器も含め、全体の評価を実施してください。あまりに広範な評価範囲となる場合は評価が複雑となりますし、内包する機器の何れかが更新停止なので適合基準を満たさなくなるとラベルは失効することとなります。 後者の場合は、全体のIoT機器に対して「本体製品自体がラベル取得」という表現は使用できず、「ラベル取得済みIoT機器を内包している製品」のような表現になるかと思います。
331	W17	W17-018	☆1セキュリティ要件・適合基準	1-1		「すべてのパスワードは、機器ごとに固有である」とは、rootやadminといった管理者権限を持つユーザのパスワードは、工場出荷時において全て一意なものを設定していればよいとの前提に基づくとも解釈できる。このような解釈について適切か否かについて記載されることが望ましい。 上記解釈が適切との前提であれば、機器においてパスワード変更機能の実装は不要であるという解釈もありうる。この解釈についても適切か否か記載されることが望ましい。上記解釈が適切でない場合は「パスワード変更機能を有すること」が必須要件であると考える。		パスワードを含む認証値の変更を可能とすることは、1-4(☆１評価項目番号：３)の適合基準に含まれています。
332	W17	W17-019	☆1セキュリティ要件・適合基準	1-1		昨今のIoT機器のスペックを踏まえ、パスワードは英字大文字小文字数字記号をランダムに使った８文字以上を強制することが望ましい。		いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
333	W17	W17-020	☆1セキュリティ要件・適合基準	17.		IoT製品内のパーツ（IC・CPU等）について、生産国や生産会社等の情報提供に関する要否を明確にすることが望ましい。		生産国や生産会社等の情報提供も含めたIoT製品内のパーツに関する適合基準は、☆２以上で検討する想定です。
334	W18	W18-001	☆1セキュリティ要件・適合基準	17-8		方針案では、（PSTI法）を内包するような方針を定めていますが、Lv1の適合基準に加入していませんでした。 方針案と適合基準の方針上の違いがあるとみられます。	「IoT製品に対するセキュリティ適合性評価制度構築方針案」 page 23では、下記「PSTI法を内包する」記述がありましたが、「別添 Lv1セキュリティ要件・適合基準」。 Lv1 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、Lv1 の適合基準の策定を行った。 セキュリティ業界の認識として、当該項目はSSDLC(セキュアな開発プロセス)に関するとても基礎的な要求となって来ました。 各国のセキュリティ要件と照合すれば、製造企業がエンドーユーザーに対する最低限の責任と思われている状況が判明します。	セキュリティ要件17-8は、☆１の対象となっており、その適合基準はセキュリティ要件17-2に対応する☆１評価項目番号＃16の☆１適合基準④に反映されています。
335	W18	W18-002	☆1セキュリティ要件・適合基準	全般	☆１評価手法	Lv1 Evaluation Method(Lv1評価手法)列中、Device check(実機テスト)に関する記述について、海外第三者機関、特に検証事業者としての視点では、METIがDevice check(実機テスト)を強制的に要求しているように見えます。 本制度において、通過方法に関して、METIがIoT製造ベンダーに要求している(IPAに提出すべき)のはChecklist(チェックリスト)と申請資料のみです。Document(ドキュメント評価)またはDevice check(実機テスト)は製造企業側の「申請通過においての選べる実現手法」ではないかと考えております。(←恐縮ですが、日本語の表現が完璧ではない可能性があります) また、当該制限の境目が曖昧であります。 例として、「別添 Lv1セキュリティ要件・適合基準」の下記項目は「Document(ドキュメント評価)：１、２・Device check(実機テスト)：なし」でした。 1．汎用のデフォルトパスワードを使用しない 1-2．プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。 １ デフォルトパスワードは、機器毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること。 ２ デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制せること。 対比として、「別添 Lv1セキュリティ要件・適合基準」の下記項目は「Document(ドキュメント評価)：なし・Device check(実機テスト)：１、２、３」でした。 3．ソフトウェアを最新の状態に保つ 3-1．製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。 １製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。 ２ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。 ３アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源OFF後も維持されること。 比較してみると、1-2-１に関して、Document(ドキュメント評価)が要求される事で、ユーザーマニュアル(≒Document/ドキュメント)のような公開資料などに記載された情報を評価すべき意味ととられます。公開資料２を確認した検証事業者やIoT製造ベンダーは実機テストで「6文字以下のパスワードが制限された事実」を確認した事が許容されないようにみえます。3-1-１に関して、Device check(実機テスト)要求される事で、実機テストで「アップデート機能」を評価すべき意味ととられます。公開資料１を確認した検証事業者やIoT製造ベンダーがユーザーマニュアル(≒Document/ドキュメント)のような公開資料などに記載された情報を確認する方法が許容されないようにみえます。「可能な限り低コストでの評価を目標とする」との方針のため、Document(ドキュメント評価)でもDevice check(実機テスト)でも要件が満たされた事実を確認できれば十分ではないかと思われます。 検討会メンバーの意図を確認できないため、正しい建言が難しい状況でした。	現在「IoT製品に対するセキュリティ適合性評価制度構築方針案」の方針案によりますと、「可能な限り低コストでの評価を目標とする」との方針のため、Document(ドキュメント評価)でもDevice check(実機テスト)でも要件が満たされた事実を確認できれば十分ではないかと思われます。 記述上の表現方法問題、又は方針の実践と記述との揺れが発生しているように見えます。 「IoT製品に対するセキュリティ適合性評価制度構築方針案」 page 13 Lv1 の評価手順について、シンガポール CLS、CCDS サー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、Lv1 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。	IoT製品ベンダーの自己評価において、ドキュメント評価だけでは十分な心証が得られないと考える評価項目に対しては、実機テストを求めており、実行ログや確認画面等を証跡として保管し、その結果をチェックリストに記載してIPAに提出することを求めています。

項番	提出意見No.	コメントNo.	該当箇所			提出意見		提出意見に対する考え方
			該当文書	該当項目	該当箇所詳細	意見内容	理由	
336	W18	W18-003	制度構築方針案	3.5.	本制度を広く普及させるうえでも、Lv1、Lv2 では自己適合宣言を認める。Lv1、Lv2 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。	IPAチェックリストの形式確認を行った上でラベルを付与しますが、IoT製品ベンダーが自己宣告して作成した宣告内容の検証は行いませんでした。 国内検証事業者の経験上、現在日本国内でセキュリティ要件を正しく理解/P-sirt組織や自己テストチームをもつ企業が少数の大手企業に限られています。 ラベル品質上の管理がある程度に実現されていない場合、同じLvレベルでも企業間の差が生じます。 海外においての日本国内認証の信憑性を強化すべく、シンガポールのCLSや欧州のRED・CRAなどの他国制度と同様に、専門家による評価/審査を行い、実質的に価値をもたらすべきと考えております。 尚、日本国内認証のラベル取得条件と他国の専門家評価制度との差が大きいと思われる場合、Mutual recognition(相互承認)の実現が不可能となる可能性が高くなります。	シンガポールのCLS制度などはLevel 1・Level 2でも専門家による評価が要求されています。	4.3.に記載のとおり、自己適合宣言を許容するものの、十分な評価能力を持っていないIoT製品ベンダーに対しては、検証事業者等の活用を推奨していくことを検討しています。 また、3.7.に記載のとおり、自己適合宣言の申請内容に、評価者の区分（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方針です。 ☆２以下での第三者評価の義務化については、今後の検討事項とします。
337	W18	W18-004	制度構築方針案	2.1.	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。	国と国としてのMutual recognition(相互承認)以外に、既存の海外セキュリティ組織とのIoTセキュリティ認証制度との相互承認も視野に入れる方がよろしいと思われます。 例として、CSA-IoTのIoT Device Security Specification 1.0はシンガポールのCLS制度とのMutual recognition(相互承認)が既に合意されていました。 グローバル企業が多い日本にあるIoT製品ベンダーにとって、コストの削減など大きなメリットが見込まれています。	現在グローバル的に展開されたMutual recognition(相互承認)状況によるコメントです。 例として、CSA-IoTのIoT Device Security Specification 1.0とシンガポールのCLS制度があります。	いただいた意見を考慮しながら、国際連携を図っていきます。
338	W19	W19-001	制度構築方針案	3.3.	表 3.3-1 各適合性評価レベルの位置付け 図 3.3-1 適合性評価レベルのイメージ図	製品類型によっては☆1, ☆2のみの適合性評価を想定しているものもあるように見受けられるが、いずれの製品類型であっても☆3の認定を取得できることが望ましいのではないか。	第三者認証による☆3の適合性評価を受けていることをいずれの製品類型であっても消費者へのアピールに活用できるべきであると考える。利用者・調達者への制度普及に際して、制度の周知とラベル付与製品の需要喚起を行う予定であると「4.2 調達者・利用者に対する制度普及促進策」の箇所に記載があるが、無事に周知等が進んで行った場合、製品類型によって☆2までしか取得できない状態であると、場合によってはその製品類型の購入意欲の減退につながりかねない懸念がある。	☆２以上や☆３以上の基準は、調達者・利用者やIoT製品ベンダーからのニーズを踏まえて優先度を決めて順次整備していきます。
339	W19	W19-002	制度構築方針案	3.7.	☆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。	☆3の有効期限の延長に関しては、認定時には第三者検証であることから延長に関しても第三者検証であることが望ましいのではないか。	同じ機器であっても同一の型式のままソフトウェアアップデートが行われたり、場合によっては利用するチップが変更される可能性も十分にあり得る。 また新しい攻撃手法の開発が行われたり、利用しているライブラリやコンポーネントに脆弱性が見つかることも十分にあり得るため、☆3の信頼性を確保していくためにも延長についても第三者検証で実施すべきと考える。	第三者評価を求める☆３以上の有効期限や延長の考え方の詳細は今後の検討となります。なお、延長に当たっては主にぜい弱性部分を再評価の対象にするなど、簡略化することも考えています。
340	W19	W19-003	制度構築方針案	3.7.	スキームオーナーは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する。（中略） 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。	サーベイランスを前提とする場合、認定の有効期限内までは申請者側で証跡を保全するべき旨を明記しておくことが望ましいのではないか。	サーベイランスの実施時にスキームオーナー側で適切な評価が行えるよう、申請者側においても証跡の保全を行うよう明記しておくべきと考える。 欧州のCyber-Resilience-Actにおいても草案において技術文書の保管が義務付けられており、本制度においても明記が望ましい。	表3.5-2にて、「☆１、☆２（自己適合宣言）」のIoT製品ベンダーの主な責務として記載しています。
341	W19	W19-004	制度構築方針案	3.7.	スキームオーナーは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する。（中略） 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。	「基準への適合に疑義が生じた場合」が発生していないか確認するため、定期的に一定の機器をサンプリングする等の形での評価機関によるランダムなサーベイランスを行うことが適当ではないか。 またランダムなサーベイランスについても申請者に協力義務がある旨を記載することが望ましいのではないか。	実際に「基準への適合に疑義が生じた場合」には社会的に対応コストが大きくなると推察される。そのような事態を未然に防ぎ、社会全体で必要最小限のコストで対応きるよう、ランダムサーベイランスの実施が望ましいと考える。	制度開始当初の☆１に関しては、コストの観点（ラベル普及のため申請費用を抑える観点）からサンプリングによる定期的なサーベイランスの実施は想定しておらず、有効期限を２年とすることで定期的な再評価・再申請を求めています。 ただし、サーベイランスの権利はスキームオーナー（IPA）が持ち、要望した際には申請者に協力する義務がある制度とするため、ラベルが普及した際に、将来的にサンプリング形式でのサーベイランスの実施も可能としています。 制度構築方針のサーベイランスに関する記載は、「制度の考え方」と、「制度開始当初の☆１」の話を明確に分けるように見直します。
342	W19	W19-005	制度構築方針案	3.8.1.	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12」に盛り込むことを 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。	政府機関での調達において「重要度:低」のシステムについても☆3以上の製品を選定すべきではないか。	脆弱なIoT機器への侵入が攻撃の起点となる可能性があるため、政府調達においてはその製品自体の重要度に関係なく☆3を必須にするべきと考える。 製品自体から情報が窃取される以外にも踏み台にされたり、内部NWへの攻撃への起点とされることは十分に考えられる。現状政府機関においてもゼロトラストの導入等が十分でないことを鑑みると脆弱なIoT機器経由で内部NWに侵入されることは大きな脅威となる。 合わせていずれの製品類型であっても☆3を取得可能なようにするべきと考える。	政府機関の「重要度:低」のシステムの調達が必ずしも☆１で十分とは考えていません。当面の方針としては、最低限☆１を取得している製品を調達することを求めますが、導入するIoT製品や利用形態によっては、「重要度:低」のシステムであっても、調達者の判断により、より高いセキュリティ要件を設定し、調達されることとなります。 まずは、☆１の制度開始とラベル取得の促進、政府調達要件での活用を進めつつ、政府調達で必要となる☆２以上のIoT製品類型の特定と、その基準整備を進めていきます。
343	W19	W19-006	制度構築方針案	4.3.	☆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り、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)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。	ISO/IEC17025の対象となるのは評価機関認定制度であり、評価機関自体にはiso/iec 17025への準拠は求められない認識であるが、相違ないか。 万が一、評価機関にもISO/IEC 17025を取得することが求められる場合は評価機関となる事業者の確保が難しくなるため、要件から外すことが望ましいと考える。	評価機関にもISO/IEC 17025を取得することが求められる場合は評価機関となる事業者の確保が難しくなるため	国際相互承認を目指す上で、世界的な動向も踏まえ、☆３以上の第三者評価を実施可能な評価機関には、ISO/IEC17025に基づく本制度の評価機関認定の取得を求める予定です。 当該評価機関認定制度は、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)の「試験事業者（IT）の認定」に、新たな認定区分として設ける予定です。 なお、検証事業者については当該認定を取得することは求めません。
344	W19	W19-007	制度構築方針案	4.3.	☆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り、そのような事業者を継続して確保していく必要がある。	評価機関の確保に際し、経済産業省＋IPAの「情報セキュリティサービス基準適合サービスリスト」にて機器検証サービスを提供するベンダの意見を参考に制度設計を進めるのが良いのではないか。	評価機関の認定に際しては事業者の確保が重要になる一方で、政府調達の要件となる☆3以上の基準について評価機関のみが審査を行う背景から、評価機関の認定条件が緩すぎても厳しすぎてもいけない。 そのため機器検証サービスを提供するベンダの意見を参考に、☆3を取得するベンダに求められる要件等を取り込みつつ、厳しすぎない認定要件を模索する必要があると考える。	「情報セキュリティサービス基準適合サービスリスト」の機器検証サービスに登録している事業者は、本制度の「検証事業者」という位置付けで本制度に関与いただく予定です。 自己適合宣言（☆１、☆２）における検証事業者の活用促進や、第三者認証（☆３以上）の制度整備等の検討において、必要に応じその意見を伺えればと思います。
345	W19	W19-008	☆1セキュリティ要件・適合基準	1-3		「なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は [A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく 技術基準適合認定番号等（技適[T]マークの設計認証番号又は [A]マークの技術基準適合認定番号）」を記入のこと。）」の箇所については削除が望ましいと考える。	電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定においては、「セキュリティ基準を含む電気通信事業法に基づく技術基準適合認定を取得したルーターの下に接続し、使用される機器」について、必ずしも認証に基づくアクセス制御がされていることを保証しないため。 特にローカルNWからの攻撃や、ルーターの下においてもグローバルIPが付与されるようなケースを想定すると、技適のみを元にアクセス制御が十分と判断するのは望ましくないと考える。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
346	W19	W19-009	☆1セキュリティ要件・適合基準	3-1		「なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は [A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく 技術基準適合認定番号等（技適[T]マークの設計認証番号又は [A]マークの技術基準適合認定番号）」を記入のこと。）」の箇所については削除が望ましい	電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定においては、「セキュリティ基準を含む電気通信事業法に基づく技術基準適合認定を取得したルーターの下に接続し、使用される機器」について、必ずしもファームウェアの更新機能が存在することを保証しないため。 特にローカルNWからの攻撃や、ルーターの下においてもグローバルIPが付与されるようなケースを想定すると、技適のみを元にファームウェアの更新機能が十分であると判断するのは望ましくないと考える。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。
347	W19	W19-010	☆1セキュリティ要件・適合基準	4-1		何を持ってセキュアと判断すべきか難しい点があり、ある程度ガイドを明記することが望ましい。 参考として欧州のETSIや自動車業界のEVITA等が挙げられる。	ETSI EN 303 645等の記載によると、セキュアな保存について、TEEや暗号化ストレージ、SE、DSC等への保存と記載がある。 IoT製品においてはこれらのセキュリティ機構を備えていない製品も数多くあり、☆1で共通で求められるようなレベルでは対応できない可能性がある。 どのような想定であるか例を挙げ、求められる「セキュア」のレベル感を示すことが望ましいと考える。	いただいたご意見は、プレ検討委員会で検討し、本制度の最終とりまとめの別添２の「☆１評価ガイド」等にて示しています。 【参考】本制度の最終とりまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html
348	W19	W19-011	☆1セキュリティ要件・適合基準	9-1		「なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は [A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく 技術基準適合認定番号等（技適[T]マークの設計認証番号又は [A]マークの技術基準適合認定番号）」を記入のこと。）」の箇所については削除が望ましい。	電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定においては、「セキュリティ基準を含む電気通信事業法に基づく技術基準適合認定を取得したルーターの下に接続し、使用される機器」について、必ずしもレジリエンスを保証しないため。	いただいた意見を参考に、ラベル付与を開始する際に使用する☆１適合基準を技術審議委員会にて決定します。また、必要に応じて☆１評価ガイド等による補足説明を検討します。