経済産業省

資料４

一部非公開

IoT製品に対するセキュリティ適合性評価制度の構築について

2024年 3月 4日

第6回検討会のご指摘事項（1/2）

カテゴリ	主なご指摘事項
対象製品について	• ハードウェアだけでなくIoT製品に組み込まれているソフトウェアも対象に含まれる点について、明確に記載しておくと良い。 • 諸外国においても同様の制度を検討している際に、日本においてソフトウェア単体についての検討が抜けていると、制度として不十分であると判断される可能性がある。ソフトウェア単体については、別途考える旨を明記しておくと良い。 • 製品に限らず、Google OSなどの汎用OSが搭載されたスマートTVなどが存在する。これらはPCやタブレットではないが、第三者がアプリケーションを作成し、組み込むことができるIoT製品である。NASもこのような類の製品が存在する。今回の対象製品を考えたときに、これらの製品はグレーゾーンにあると感じた。
各レベルの位置づけについて	• ☆1から☆4が具体的にどのような用途で必要とされているかを明確に定義する必要がある。消費者にとって、システムにおいて適切な☆のレベルを理解しやすくするために、マトリックスなどを用いて示す必要がある。 • ☆1を取得しているからといって、☆2の適合基準を満たせていないわけではない。☆１の製品であるから調達しないと判断されないよう、調達者側に訴求していただきたい。 • 実証を行ったが、☆1を満たせば、一般的な攻撃には対抗できるとの印象を受けた。一般企業においては、☆1の基準を満たす製品で十分と考える。ただし、センシティブな情報を扱う企業では、☆2以上の製品を選択することになると考える。 • 人的資産が☆2から考慮されていることについて、☆1ではユーザの生命は守らなくて良いと捉えられる可能性があるため、表現の工夫が求められる。 • ☆3および☆4と経済安全保障推進法の基幹インフラとの関連性について、検討いただきたい。
適合性評価の要件・基準について	• 評価項目には、企画開発段階で注視すべき事項や、ソフトウェアコンポーネントが最新版であることなど、出荷前に確認が必要な項目が含まれている。このような事柄について、開発者向けのガイドブックなどを作成することも検討いただきたい。 • SBOMに関する議論の状況について、報告書に記載いただきたい。SBOMについては、プレ委員会で検討しているロングリストにも含まれており、同時に、ほかのグループでも同様のテーマに基づく議論が進行中である。この点を明記すると良い。
評価方式について	• 実証結果に関して、自己評価の妥当性に疑問を感じる。詳細な分析をプレ委員会で行っていただきたい。 • 自己評価と第三者評価の実証結果の差に注意し、自己評価が適切に行える体制を整えることが必要である。 • 国際的な場で議論した際、自己評価で評価の妥当性が担保されるかについて指摘があった。
展開戦略について	• ベンダーに対して、少なくとも政府は認証された製品を確実に使用するという宣言をすると良い。 • 特定分野のシステムに組み込まれるIoT製品に求めるセキュリティ要件の検討を進めるための参考資料があると良い。 • 報告書には優先度が高いと思われる分野についての議論に関しても詳細に記載していただきたい。また展開戦略の詳細についても、明記しておく必要がある。 • スマートホームのテーマに取り組んでいるグループも既に存在するため、実際に動作し、適用されている実例を参考にして、具体的かつ誤解のない形で検討を進めることが良いと考える。 • 制度全体としては大きな流れが見える中で、スマートホームや医療などの個別のケースにおいて、それらの環境への適用方法については検討の余地がある。これらの点についてもうまくまとめていけるような方針を策定することが望ましいが、まとめきれない領域については一時保留という形も考えられる。 • 本制度を海外ベンダーに対しても普及させることが重要な課題である。

第6回検討会のご指摘事項（2/2）

カテゴリ	主なご指摘事項
有効期限について	• 認証取り消しに関しては、有効期限を設けて失効させる方針が良い。 • IoT製品はセキュリティ的に1、2年で陳腐化する可能性もあるため、有効期限による登録廃止も検討されるが、有効期限の設定方法については検討が必要である。
調達者、消費者における活用について	• ユーザには、リスクがあることを理解いただいた上で、IoT製品を使用していただくことが重要である。
ラベル付与製品の管理について	• サーベイランスに加えて、通報制度や苦情処理の制度も検討すべきである。製品について通報できる仕組みや疑問を解消するための処理が必要である。 • 自己評価が正確に行えることを前提として、コストとのバランスを取りながら、定期的に試買テストを行い、自己評価の妥当性を確保するための対策を検討していただきたい。
諸外国制度との連携について	• ISO/IEC27404の活動に本制度の活動をうまく組み込めれば、相互認証の実現においても理想である。
実証について	• 実証結果のNの項目に対する製品の修正可能性についてもヒアリングしていただきたい。
今後のスケジュールについて	• 来年度の下期以降に制度運用を開始させる予定としているが、制度に関する周知期間が半年未満となっている。半年という短い周知期間から、ベンダーとして対応に十分な時間が確保できるか懸念している。弊社の製品でも、来年度にラベル申請をすることは難しいと考えている。来年度はPSTIが義務化されるため、そちらの対応に手一杯になることが予想される。 • 制度構築におけるロードマップを、横軸を時間にして作成いただきたい。ロードマップを作成することで、ベンダー側、消費者側双方で理解が進むと考えている。
その他	• 医療機器のSBOMに関して、JIS Tでは推奨されており、対応しようとしているベンダーや医療機器団体が動き出している。そのため、調整を行い、整合性を確保する必要がある。 • 多くの古いシステムが存在し、一部の製品は☆1を満たしていない。情報通信研究機構（NICT）と情報を共有することが有益であると考える。 • 本制度の検討において、安全保障や重要インフラの文脈でセキュアなネット社会を築くための制度であると位置づけるとまとまりのある方向性になるのではないか。責任のリバランスの考えは、セキュリティ・バイ・デザインなどに結びついていくものだと考えている。「責任のリバランス」という言葉を用いることで、方針をまとめやすくなり、本制度の検討がスムーズになると考えている。

本日の議題

【ご報告事項】

- 適合性評価の実証結果について（資料3）
- 各レベル（☆１～☆４）の位置付け（資料4）
- 調達者の本制度活用に関する調整状況（資料4）
- 本制度の賛同団体（資料4）

【ご議論いただきたい事項】

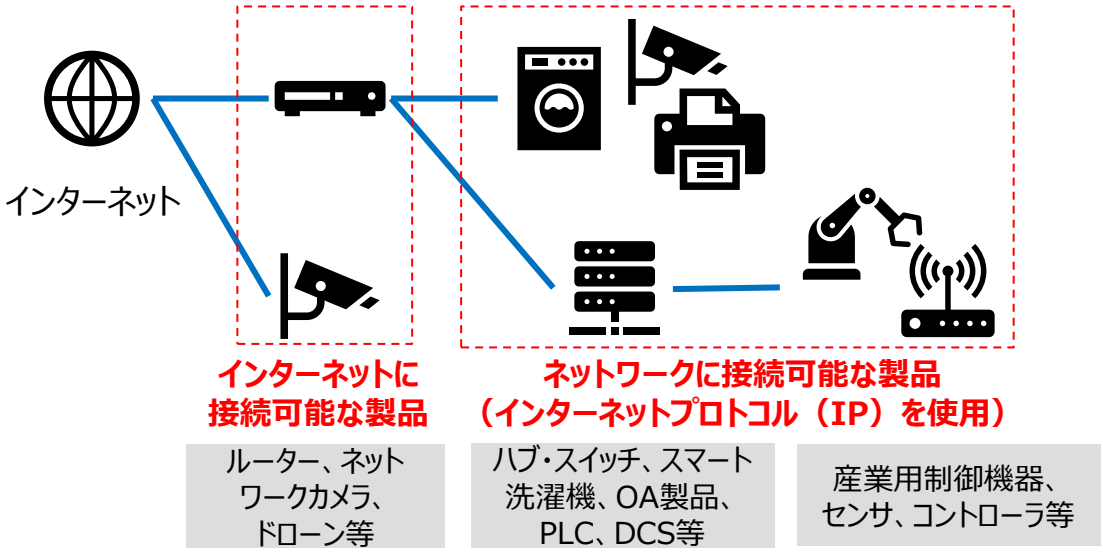
- 有効期限の設定（資料4）
- ラベル及び情報提供ページ（資料4）
- 本制度のロードマップ案（資料4）
- 最終とりまとめ案（資料5）

各レベル（☆１～☆４）の位置付け

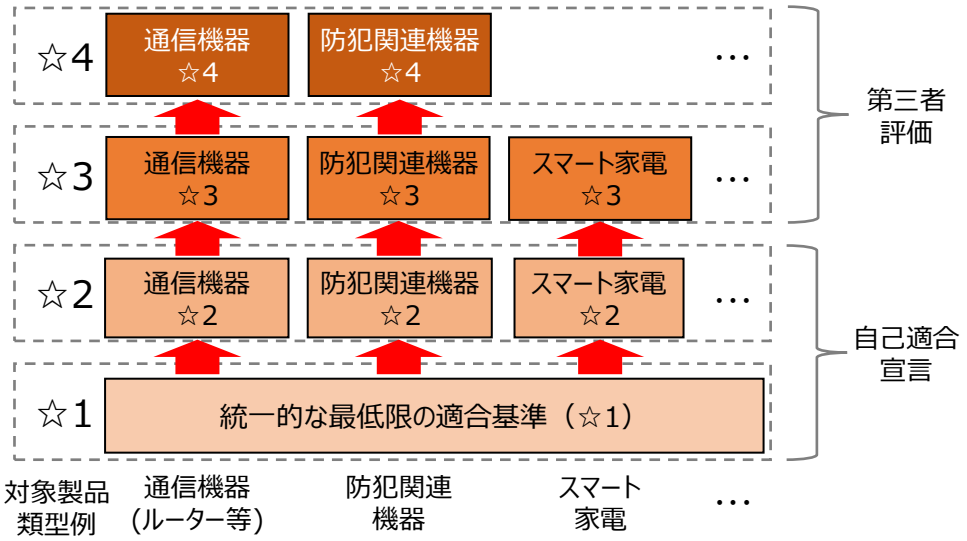
- 前回の検討会でのご意見を踏まえ、これまでの検討会での議論をもとに、各レベルの位置付けについて整理した。

レベル	位置付け	適合基準	評価方式
☆３以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆２	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型別	自己適合宣言
☆１	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	自己適合宣言

対象製品の概要



各レベル（☆１～☆４）のイメージ



調達者の本制度活用に関する調整状況

- 政府機関等、重要インフラ事業者、地方公共団体におけるIoT製品調達時に、用途やそのリスクに応じて、本制度のラベル取得製品を選定・調達することを求めていくように、関係者と以下の方向性で調整している。

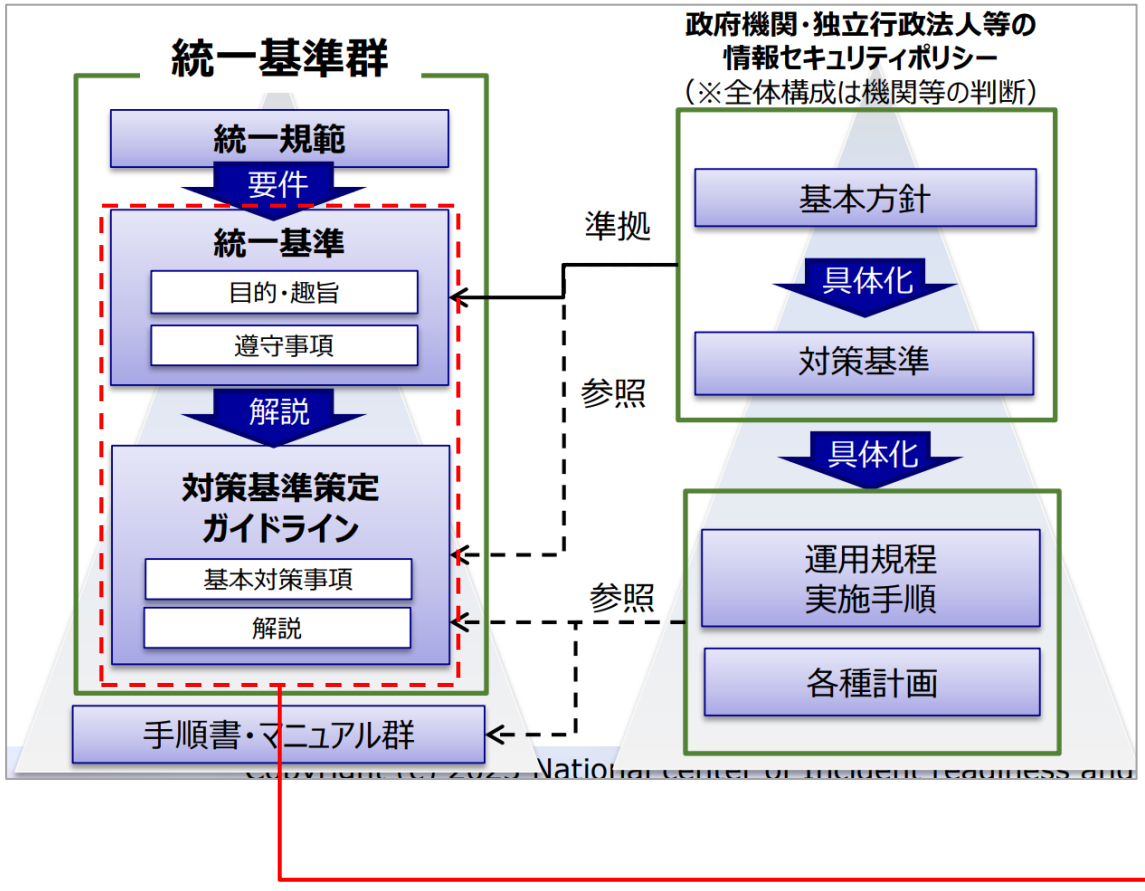
対象	主な調整先	調整状況・方向性
政府機関等	NISC 政府機関総合対策グループ 基本戦略第２グループ	• **来年度以降の改定に合わせて、「政府機関等のサイバーセキュリティ対策のための統一基準」およびそのガイドラインに**、情報システムの重要度に応じて**「重要度：低」は☆1以上、「重要度：高～中」は少なくとも☆3以上のIoT製品を各機関等の選定基準に含める**ことの追加を検討する。 • ラベル取得済み製品が普及する時期をめどに、**政府機関等ではラベル取得済みIoT製品の調達を必須化**する方針。 • 統一基準やガイドラインへの反映に向けて、今後、各府省庁の参加する会議の場などで、本制度を活用した製品調達に関する周知を行っていくことも重要となる。
重要インフラ事業者	NISC 重要インフラ第１グループ	• 調達要件に関する記載は、**「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針および手引書に入れる**こととなる。制度立ち上げのタイミングに合わせて、**来年度以降、専門調査会(※1)の議案に指針への反映を入れていく**。 • 重要インフラ事業者への調達ルールへの反映に関する働きかけおよび各業界固有のシステムで用いられているIoT製品への☆2以上の必要性の確認は、**四半期毎に実施しているセプターカウンシル(※2)の運営委員会を活用**する。
地方公共団体	総務省 デジタル基盤推進室	• 政府統一基準群に記載された後、地方公共団体の状況に合わせて、**地方公共団体セキュリティポリシーガイドラインに記載**することが通例となっている。 • **来年度以降、検討会(※3)、自治体意見照会、パブコメを経て改定を検討**することとなる。

(※1)NISC「重要インフラ専門調査会」 https://www.nisc.go.jp/council/cs/ciip/index.html
(※2)NISC「セプターカウンシル総会資料（セプターカウンシルの概要）」 https://www.nisc.go.jp/policy/group/infra/siryou/#si09
(※3)総務省「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

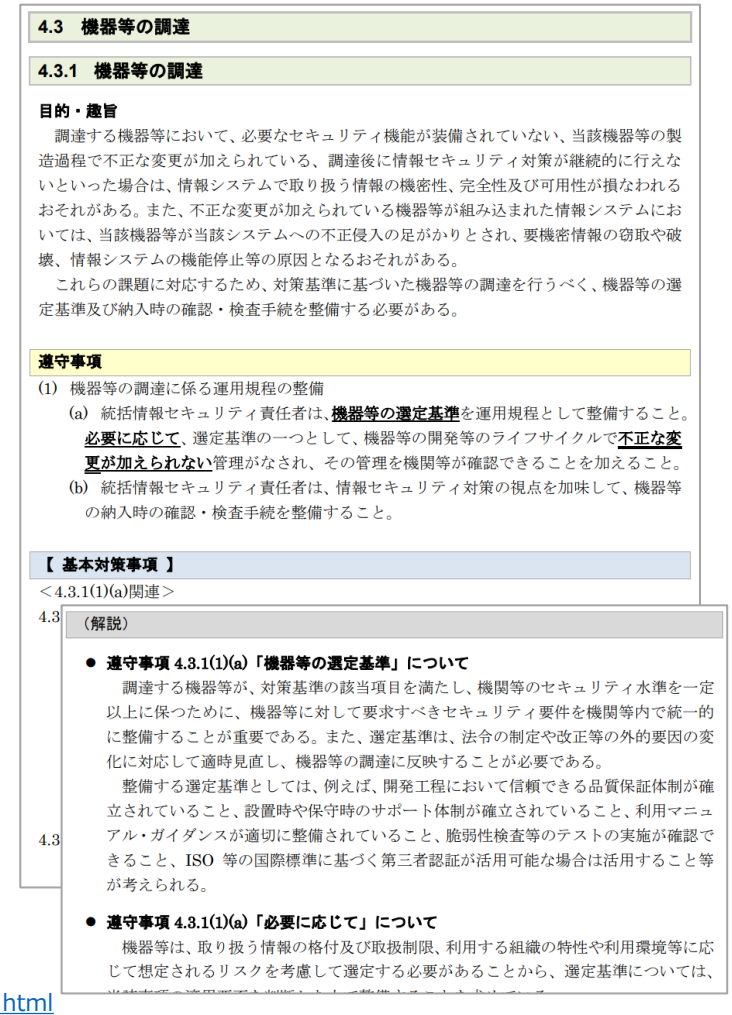
調達者の本制度活用に関する調整状況（政府機関等）

- 政府機関等が遵守すべき事項を定めた「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」およびそのガイドラインに、情報システムの重要度に応じ、**「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NISCと検討している。
- ラベル取得済み製品が普及する時期をめどに、政府機関等では**ラベル取得済みIoT製品の調達を必須化する方針**。

統一基準群（令和５年度版）文書体系



対策基準策定ガイドラインの「4.3.1 機器等の調達」の記載



4.3 機器等の調達

4.3.1 機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、**機器等の選定基準**を運用規程として整備すること。**必要に応じて**、選定基準の一つとして、機器等の開発等のライフサイクルで**不正な変更が加えられない**管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

4.3

（解説）

- **遵守事項 4.3.1(1)(a)「機器等の選定基準」について**

調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 4.3.1(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、

4.3

統一基準の記載内容

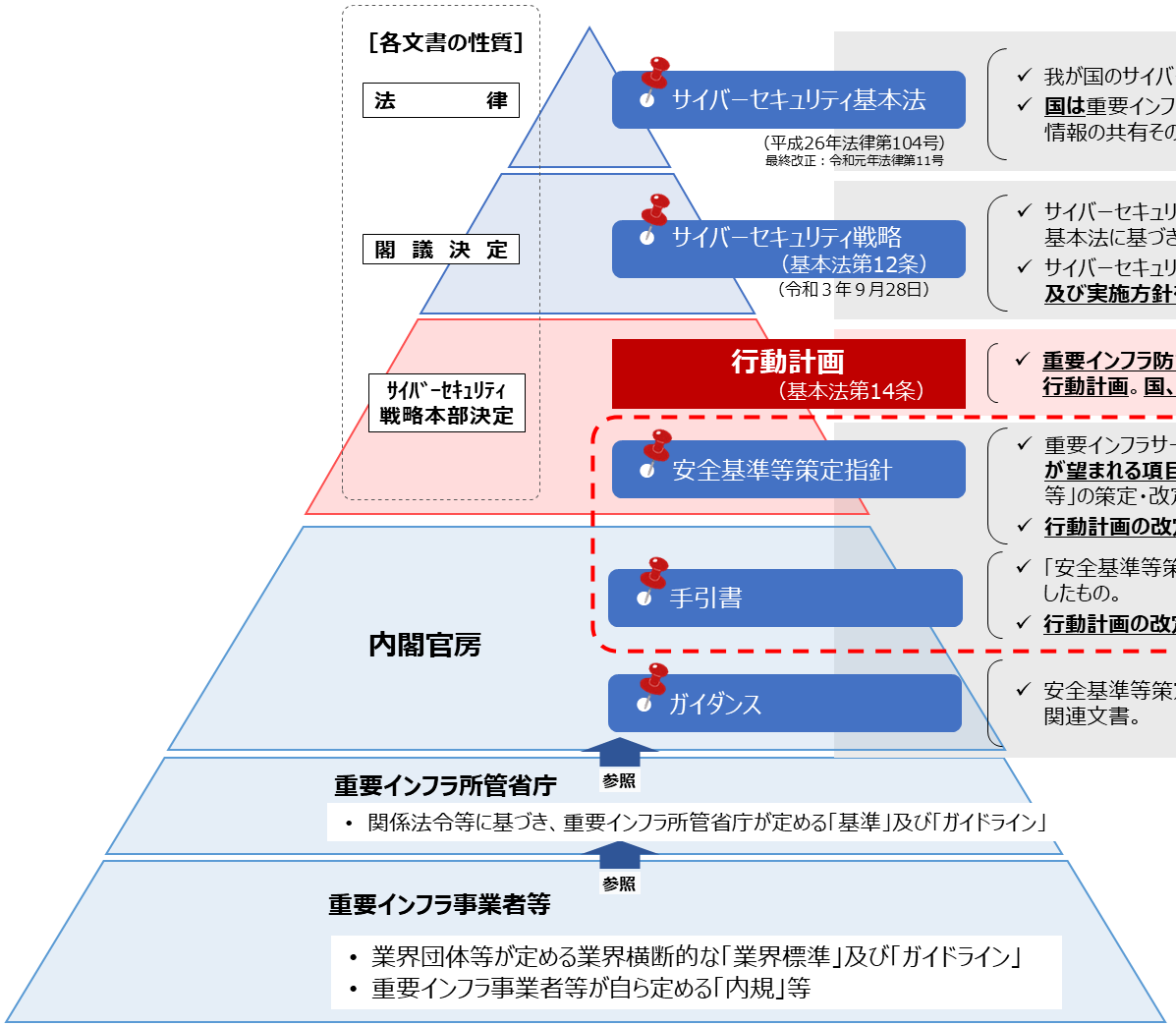
上記遵守事項に対する基本対策事項と解説をガイドラインに記載

出所）NISC「統一基準群改定のポイント（令和５年度版）」https://www.nisc.go.jp/policy/group/general/kijun.html
NISC「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

調達者の本制度活用に関する調整状況（重要インフラ事業者）

- 重要インフラのサイバーセキュリティに係る行動計画は、「重要インフラのサイバーセキュリティに係る行動計画」を基本としつつ、重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図っている。
- 「重要インフラのサイバーセキュリティに係る安全基準等策定指針」に、**調達製品への要求事項の策定および調達時の確認を明示**した上で、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」に詳細な記載を追加する方向で検討中。

重要インフラ防護に関する戦略・指針等



サイバーセキュリティ基本法
（平成26年法律第104号）
最終改正：令和元年法律第11号

- ✓ 我が国のサイバーセキュリティ政策に関し、基本理念、**国、事業者等の責務を定める**。
- ✓ **国は**重要インフラ事業者等におけるサイバーセキュリティに関し、**基準の策定**、演習及び訓練、情報の共有その他の自主的な取組の促進その他の**必要な施策を講ずるもの**とされている。

サイバーセキュリティ戦略
（基本法第12条）
（令和３年９月28日）

- ✓ サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティ基本法に基づき策定される**サイバーセキュリティに関する基本的な計画**。
- ✓ サイバーセキュリティに係る我が国としての基本的な立場を明らかにするとともに、**諸施策の目標及び実施方針を国内外に示す**ことを目的とする。３年ごとに改定。

行動計画
（基本法第14条）

- ✓ **重要インフラ防護に係る基本的な枠組み**を定めた政府と重要インフラ事業者との**官民共通の行動計画**。**国、重要インフラ事業者等が取り組むべき事項が規定**。

安全基準等策定指針

- ✓ 重要インフラサービスの安全かつ持続的な提供を図る観点から、**「安全基準等」において規定が望まれる項目を整理・記載**し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。
- ✓ **行動計画の改定、サイバーセキュリティを取り巻く環境の変化等を踏まえて見直し**を実施。

手引書

- ✓ 「安全基準等策定指針」で定めたリスクアセスメントや情報共有を行う際の手順を具体的に示したもの。
- ✓ **行動計画の改定、サイバーセキュリティを取り巻く環境の変化を踏まえて見直し**を実施。

追記を検討

ガイダンス

- ✓ 安全基準等策定指針及び手引書に付随する文書として、個別の対処方法、留意点等を示す関連文書。

国際標準、他国の基準等

ISO/IEC　NIST　…

調達者の本制度活用に関する調整状況（地方公共団体）

- 総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」では、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説されている。
- その中の「情報セキュリティ対策基準」では、IoT機器を含む特定用途機器のセキュリティ管理や情報システムの調達について言及されており、政府統一基準の改定を踏まえ、IoTセキュリティ適合性評価制度のラベルを取得した製品の調達についての追記を検討する。

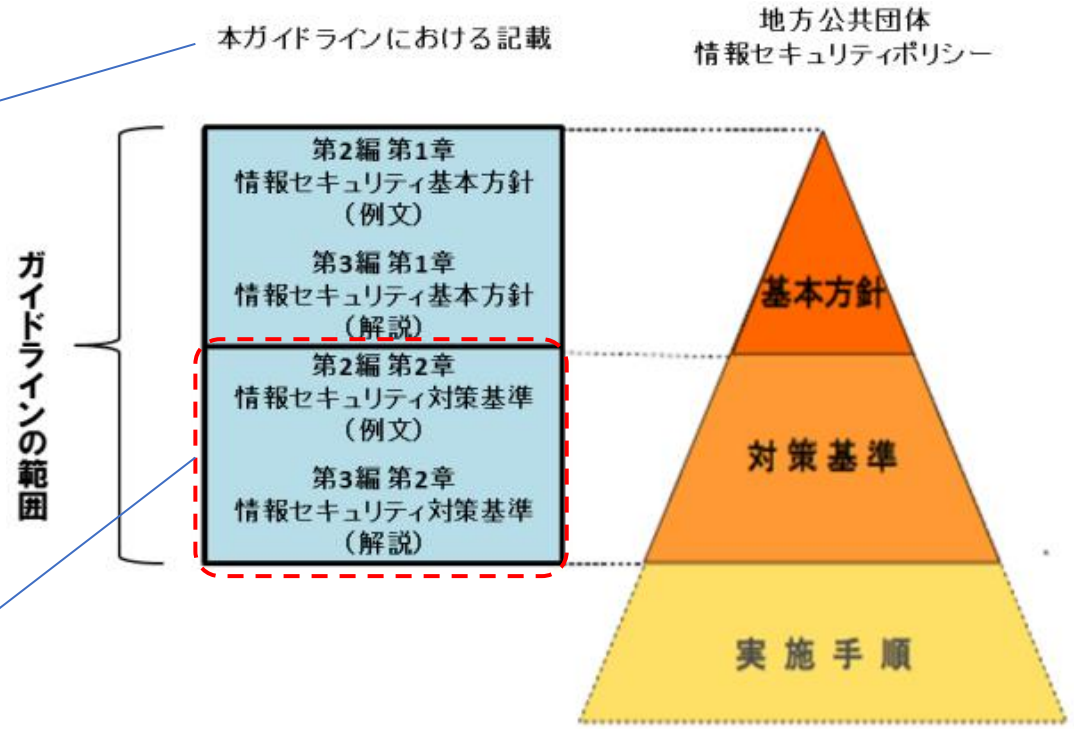
ガイドラインでは以下が示されており、各地方公共団体において、組織の実態に合わせ、必要に応じて推奨事項も含めて、情報セキュリティポリシーを策定することが期待されている。
（第１編 第４章 2.本ガイドラインにおける対策レベルの設定）

- 特段の理由がない限り**対策を講じることが望まれる事項**
  ＋
- **推奨事項**（必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項）

対策基準の以下の関連項目に、IoT製品を選定・調達する際にIoTセキュリティ適合性評価制度を活用することの記載追加を検討したい。（文案は次頁）

- 6.1. コンピュータ及びネットワークの管理
  （１２）IoT 機器を含む特定用途機器のセキュリティ管理
- 6.3. システム開発、導入、保守等
  （１）情報システムの調達

「地方公共団体における情報セキュリティポリシーに関するガイドライン」の構成と地方公共団体情報セキュリティポリシーの対応関係

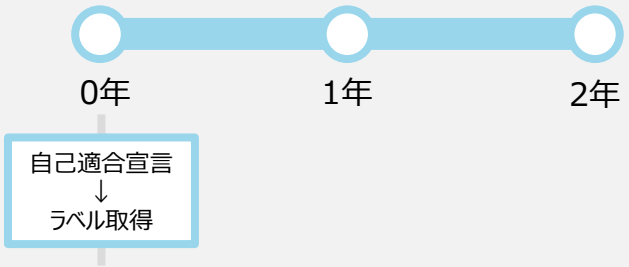


出所）総務省「「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

自己適合宣言（☆１、☆２）の場合の有効期限案

- 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**とする。（申請時に申し出れば、2年以内の有効期限も設定可能とする。）
- 有効期限の2年経過後にラベルを継続する場合は、**再度、自己適合宣言**を行い、ラベル取得申請を行う。
- 有効期限内に適合基準・評価手順の**メジャーな改訂があった場合も途中でラベルが失効することはない**。

通常の場合

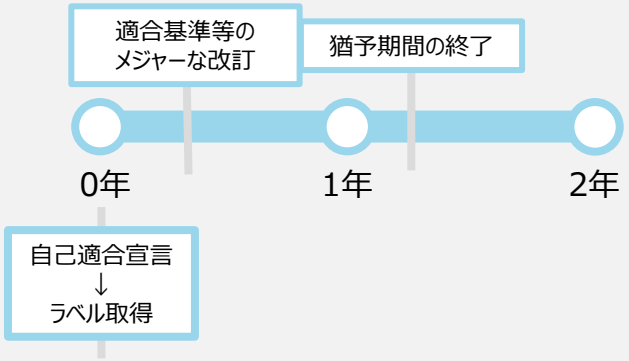


諸外国制度における有効期限の設定

国・地域	シンガポール	ドイツ	フィンランド
制度名	Cybersecurity Labelling Scheme (CLS)	IT Security Label	Finnish Cybersecurity Label
有効期限	最大3年間 （開発者が製品に対するセキュリティアップデートを行ってサポートする期間）	製品カテゴリーごとの別段の定めがない限り通常2年間	申請プロセスの開始時に指定することができるが製品のセキュリティアップデートが提供される期間を超えることはできない （製品のセキュリティ機能が依然として要件を満たしていることを確認するため、年次審査が行われる）

適合基準・評価手順のメジャーな改訂※があった場合の有効期限

有効期限内に適合基準・評価手順のメジャーな改訂に関する猶予期間が終了したとしても、途中でラベルが失効することはない。



※適合基準・評価手順の変更・新項目の追加等

※製品仕様の変更がある場合は、この限りではない。

第三者認証（☆３以上）の場合の有効期限

- 第三者認証の場合の有効期限について、**ラベル付与製品の信頼性の担保やベンダーの負担、適合基準・評価手順のメジャーな改訂の行いやすさ等**を考慮して、検討を行う必要がある。
- 下表で示すような案が考えられるが、それらの利点や懸念事項を踏まえ、**第三者認証の場合の有効期限について広くご意見をいただきたい**。

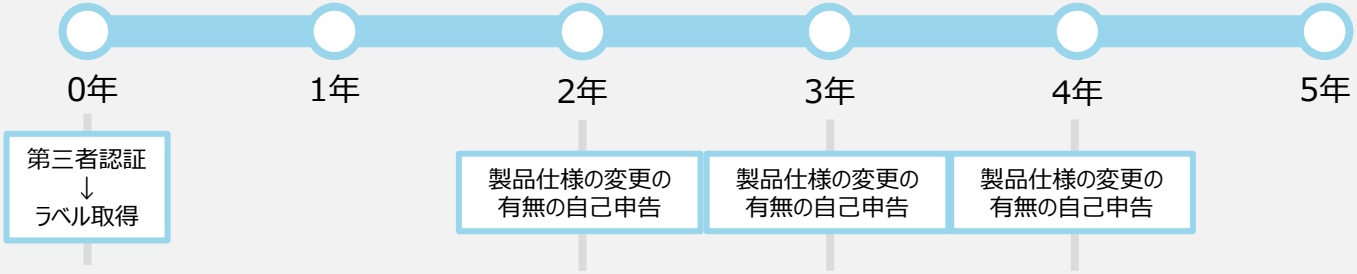
	パターンA	パターンB
	2年経過後、1年ごとに製品仕様の変更の有無の自己申告を求め、最大5年までの延長を認める	2年ごとに、IPAが指定した項目は評価機関による再評定、その他の項目は評価機関による形式チェックを行い、問題がなければ追加で2年の延長を認める
利点	• 製品仕様の自己申告を行えば良いので、**延長にかかるベンダーの負担が小さくなり、製品価格への転嫁額も小さくなる**。	• 指定項目について2年ごとに評価機関による再評定を行うため、**経年によるラベルへの信頼性の低下を防ぐ**ことができ、**調達者が安心して製品を選定**できる。 • **再評定を通過している限り、延長が認められ続ける**ため、特に5年や10年を超えるようなライフサイクルの長い製品では、再申請（5年毎の全体の再評価）を行うより延長にかかるベンダーの負担が小さくなる可能性がある。
懸念事項	• **評価機関による評価を1度も行わないまま5年間ラベルが継続**されるため、その間の変更の有無については、**調達者がベンダーによる自己申告を信用する他ない**。 • 適合基準・評価手順のメジャーな改訂があると、ベンダーとしては5年の期限を想定していたところ、急な短縮となってしまうため、アップデートへの反発が予想される。	• 2年に1度、評価機関による再評定を受ける必要があるため、ベンダーの負担が大きい。 • 適合基準・評価手順のメジャーな改訂の猶予期間終了のタイミングによっては、**旧バージョンでのラベルが最大2年間＋猶予期間の間、市場に流通**することになる。（パターンAの場合は最大1年間＋猶予期間）

※製品仕様の変更がある場合は、この限りではない。

第三者認証（☆３以上）の場合の有効期限案（パターンA）

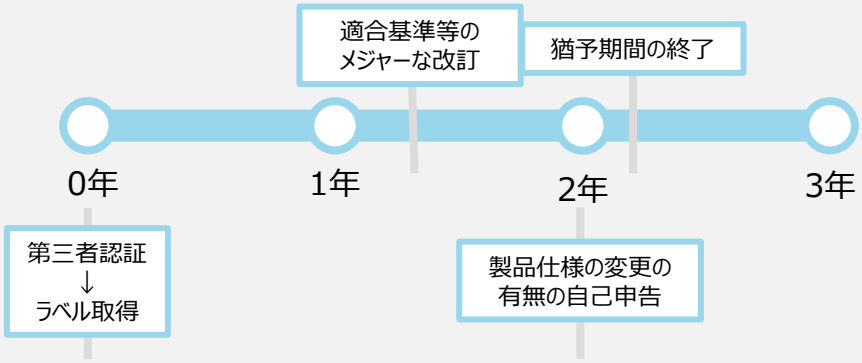
通常の場合

2年経過後、1年ごとに製品仕様の変更の有無の自己申告を求め、最大5年までの延長を認める。



適合基準・評価手順のメジャーな改訂※があった場合の有効期限

適合基準・評価手順のメジャーな改訂に関する猶予期間が終了した直後の自己報告タイミングで、ラベル失効とする。

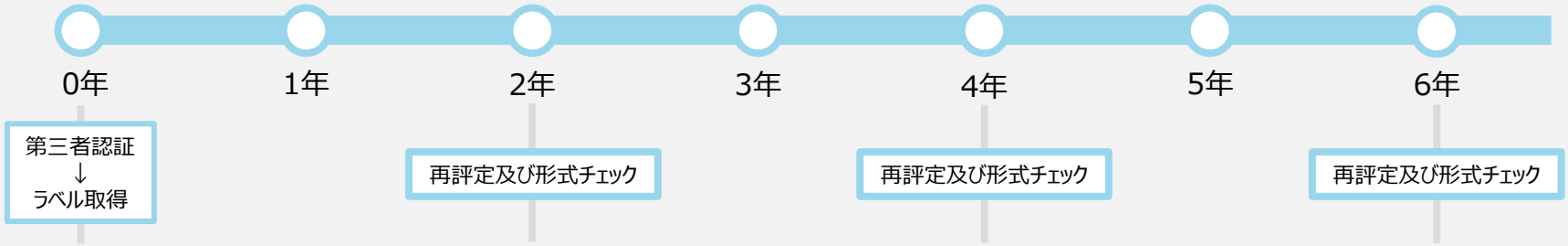


※適合基準・評価手順の変更・新項目の追加等

第三者認証（☆３以上）の場合の有効期限案（パターンB）

通常の場合

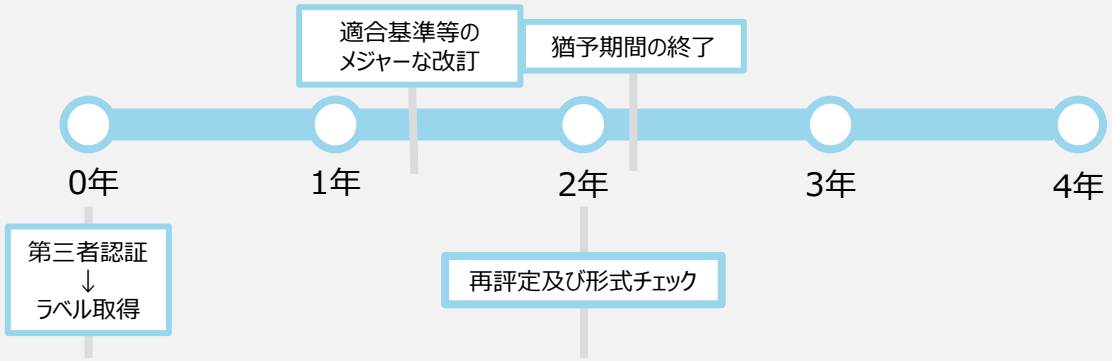
2年ごとに、IPAが指定した項目は評価機関による再評定※、その他の項目は評価機関による形式チェック（インタビューベースでの確認）を行い、問題がなければ追加で2年の延長を認める。



※攻撃に関わる各種状況（手法、能力、設備）の変化に対し、同じレベルの耐性にあるか確認すること

適合基準・評価手順のメジャーな改訂※があった場合の有効期限

適合基準・評価手順のメジャーな改訂に関する猶予期間が終了した後は、延長を認めない。



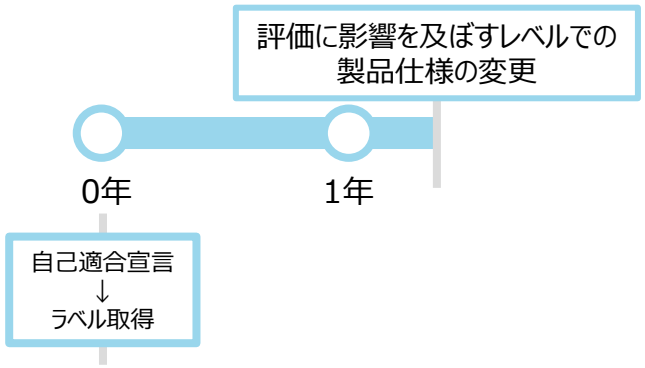
※適合基準・評価手順の変更・新項目の追加等

※申請時に申し出れば、2年以内の有効期限も設定可能とする。
※起点はラベル取得日とする。

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の有効期限

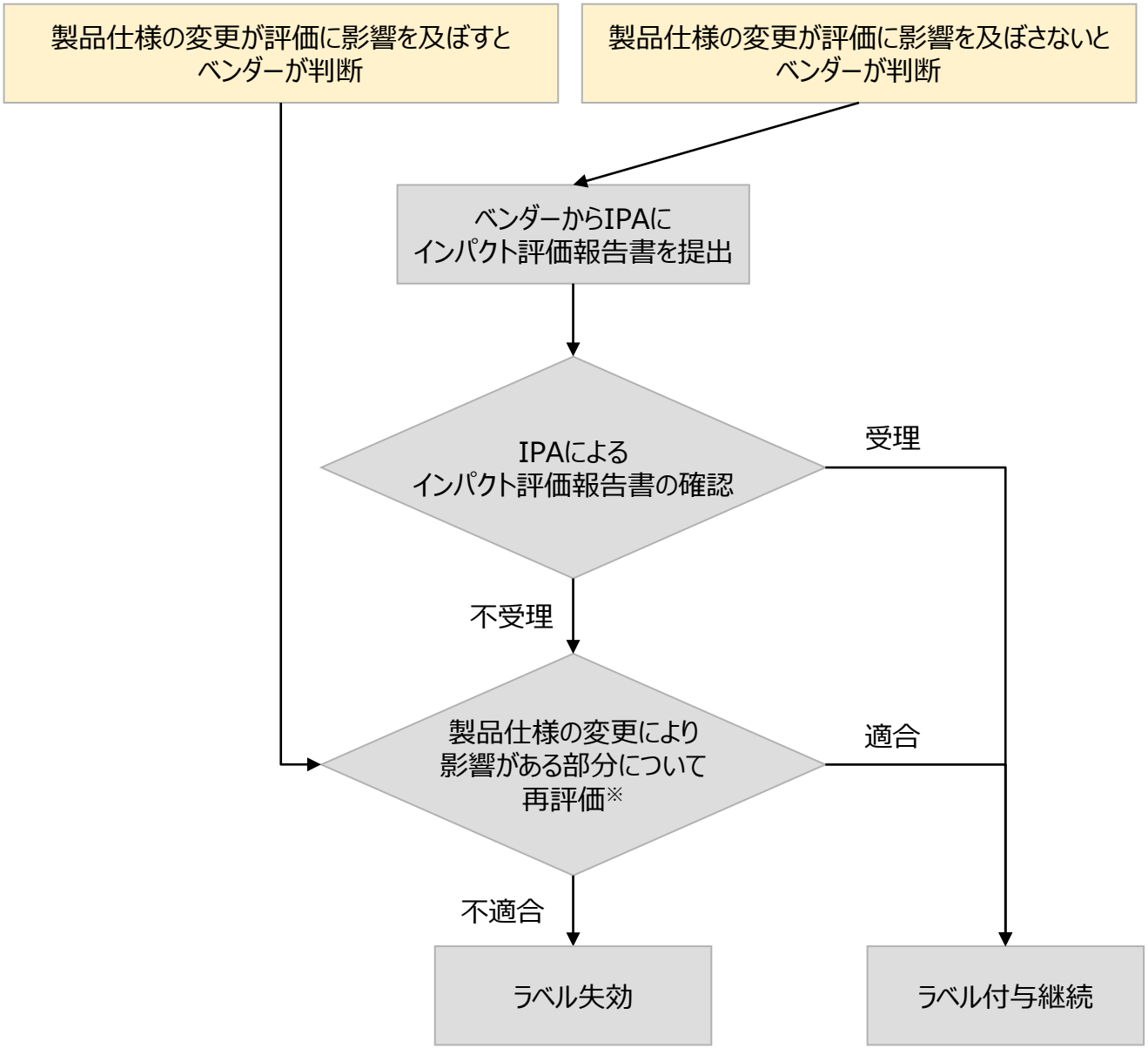
自己適合宣言（☆１、☆２）の場合

- 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、ベンダー自身で確認を行ったうえでIPAに報告し、その時点で**ラベルは失効**する。
- ラベル使用を継続する場合は、変更後の製品仕様にて**新たに自己適合宣言**を行い、ラベル取得申請を行う。



第三者認証（☆３以上）の場合

- 製品仕様の変更により影響がある部分について、**再評価を実施**する。



※再評価：以前の評価結果をできるだけ再利用しつつ、変更部分に対して再度評価すること。

ラベル及び情報提供ページ

- 本制度は任意制度であるため、**ラベルの表示義務は設けない**。製品本体、パッケージ、マニュアル、パンフレット、Webサイト等に掲載する場合は、**本制度のロゴ**及びラベル付与製品毎の**情報提供ページのURLを埋め込んだQRコードを掲載**することを想定している。
- 有効期限の経過後に再申請されることを想定し、情報提供ページのURLはラベル付与製品単位で固定し、初回取得年月は記載しない。
- 情報提供ページには、**本制度の概要、製品情報、ラベル情報、適合評価結果、安全情報等を掲載**する想定である。
- 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が、**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ない**。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。

情報提供ページの掲載情報案

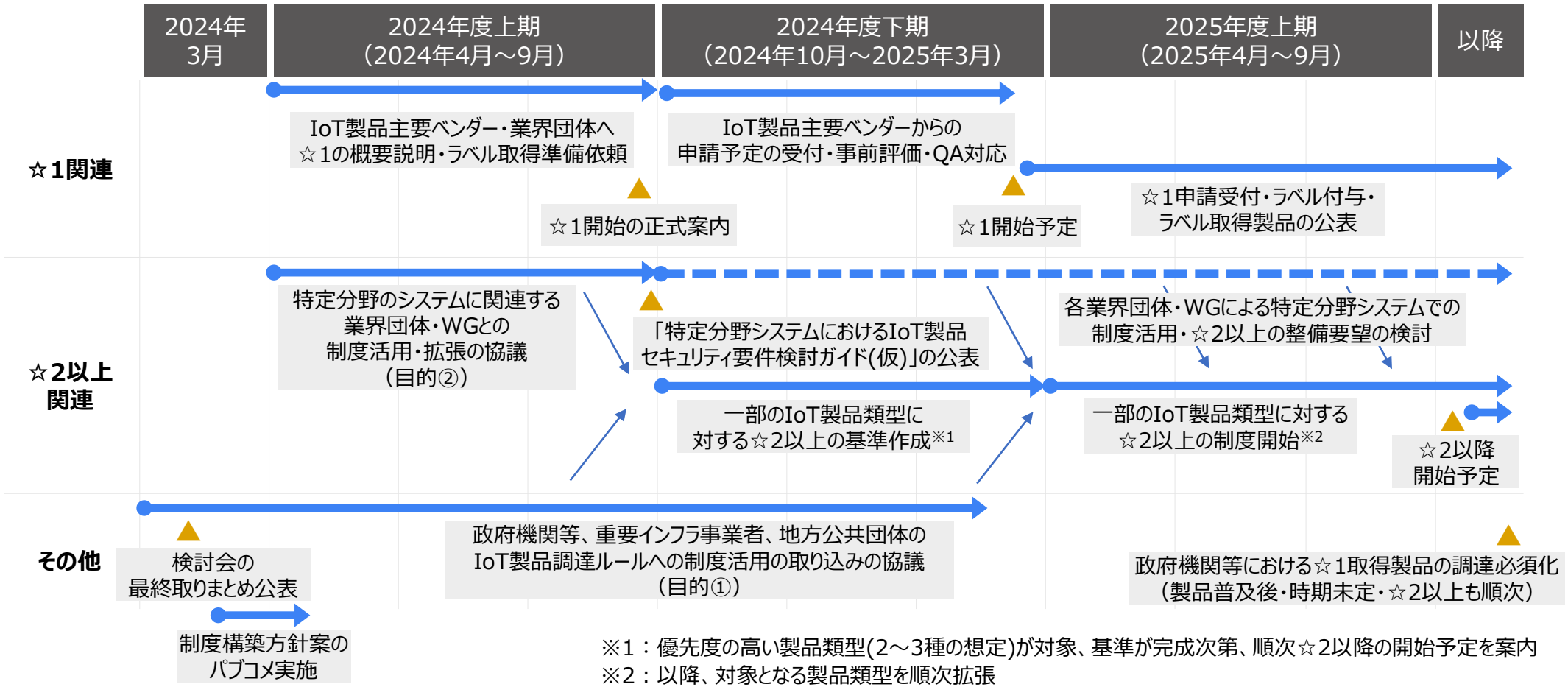
掲載情報	掲載内容
本制度の概要	• 本制度の概要及び詳細説明HPのURL
製品情報	• 製品名 • 型式番号 • 製造業者名　※公開/非公開は任意 • 製造国又は地域　※公開/非公開は任意 • 製品概要 • 製品WebサイトのURL • 製品の問い合わせ先 • 他認証の認証番号等
ラベル情報	• ラベル識別番号 • 当該製品の適合性評価レベル（☆１～☆４） • 当該製品の製品類型の名称　※☆2～☆４の場合 • 評価された適合基準のバージョン • 適合基準のうちN/Aだった項目 • ラベルステータス情報 • ラベル発行・更新日 • ラベルの有効期限 • 申請者名 • 評価者区分
安全情報	• 当該製品に関わる脆弱性情報 • 脆弱性の報告窓口のURL
その他セキュリティ関連情報	• 必要があれば、製品ベンダーから調達者に向けたセキュリティ関連情報

【参考】ドイツ ITセキュリティラベルの情報提供ページ

出所）BSI「Xiaomi - Mesh System AX3000」
https://www.bsi.bund.de/SharedDocs/IT-Sicherheitskennzeichen/DE/2023/sik-02023_xiaomi_Mesh-System-AX3000.html?nn=1069038

IoTセキュリティラベリング制度(仮) ロードマップ案

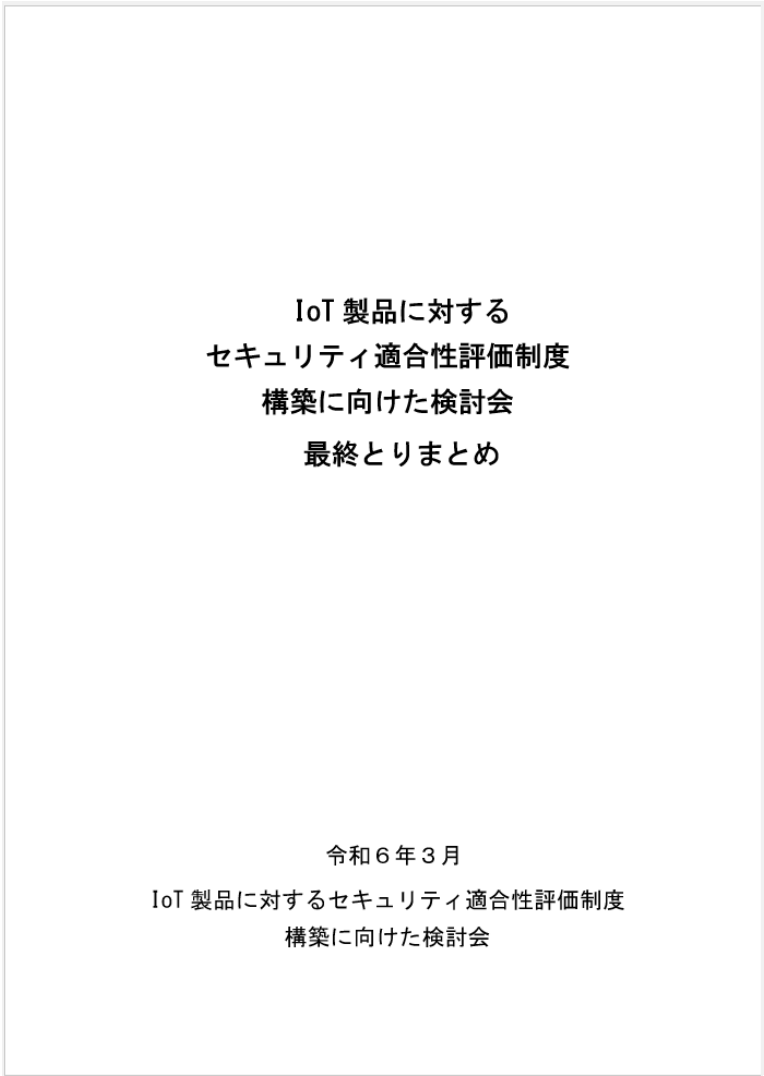
- **2024年7～9月頃に制度開始の正式案内**を行い、**2024年度中（2025年3月頃）に☆１制度の開始**を目指す。
- ☆2以上は、2024年度の上期に制度活用・拡張の協議を行い、選定した一部のIoT製品類型に対する基準を下期に作成する想定。**☆２以上の制度開始は2025年度下期以降**となる見込み。
- 並行して、**政府機関等へのラベル取得済みIoT製品調達の必須化**の調整および重要インフラ事業者・地方公共団体へのIoT製品調達ルールへの制度活用の取り込みの働きかけを行う。
- 欧米を含む主要国・地域とは、☆１基準案を共有し議論を進めている。☆１開始の正式案内時に制度が既に導入されているシンガポールと英国については、案内時に相互運用の方向性を提示。正式案内時に制度設計途中の見込みである欧米については、順次公表する。



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

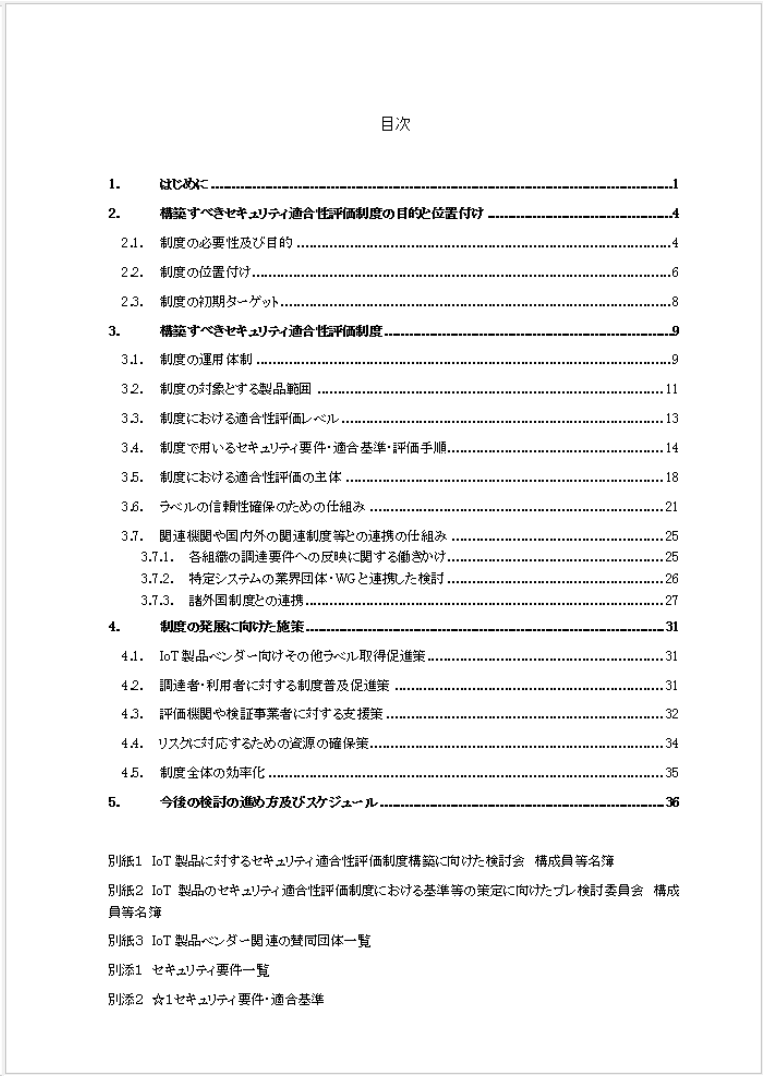
最終とりまとめ案及び制度方針案

- 本検討会での議論結果の**最終とりまとめ案（資料5）の内容**についてご確認いただきたい。いただいたご意見を踏まえて最終とりまとめを作成し、**3月中旬に公表**を行う予定。
- 最終とりまとめの各項の「(3) 議論を踏まえた構築すべき制度」を中心に**制度構築方針案を策定**する。
- 制度構築方針案および☆１セキュリティ要件・適合基準を対象に、**3月中旬から4月中旬にかけてパブリックコメントにかける**予定。制度**概要説明資料および☆１セキュリティ要件・適合基準は、英語版を参考資料として添付**する予定。



IoT 製品に対する
セキュリティ適合性評価制度
構築に向けた検討会
最終とりまとめ

令和６年３月
IoT 製品に対するセキュリティ適合性評価制度
構築に向けた検討会



目次