経済産業省

資料３

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

2023年 2月 6日

１．前回の検討会のご指摘事項

２．適合性評価制度の位置づけ

３．本適合性評価制度で対象とする製品範囲について

４．本適合性評価制度で用いる適合性評価基準について

５．本適合性評価制度で活用する適合性評価スキームについて

６．本日の討議事項

前回の検討会のご指摘事項

- 制度の位置づけについて、本制度を法的に義務化すれば制度が活用される一方で、義務化には責任も伴うため、慎重に検討すべきとの意見が挙げられた。
- 対象製品に関して、消費者向けIoT製品からスタートして課題を整理することが重要との意見のほか、消費者向け製品も産業向け製品のどちらも制度の対象とするべきとの意見も挙げられた。
- 適合性評価基準に関して、IoT製品メーカーに与える影響やメリットを鑑みた検討の必要性が提示された。
- 採用する適合性評価スキームについて、簡易的な方法で評価を行うことが望ましいとの意見が挙げられた。

カテゴリ	主なご指摘事項
制度の位置づけ（義務／任意）について	• 法的に義務化すれば、制度が活用されるようになると思われる一方で、義務化には責任も伴うため、慎重に検討した方が良い。 • 義務的な法制度としなければ、制度は広がらない。強制力がない限り、メーカは重い腰を上げられないのが現状である。
制度の対象製品について	• 消費者向け製品も産業向け製品のどちらも制度の対象とするべきだと考えているが、レベルは分けるべきであり、消費者向け製品であっても最低限のセキュリティ対策は求められるべき。 • ラベリング制度を設けるのであれば、有効なのは消費者向けIoT製品である。 • 消費者向けIoT製品からスタートし、様々な課題を整理していくことが重要である。 • 同じIoT機器であっても、消費者向けとして使われる場合と重要インフラ向けに使われる場合があるため、対象とする機器の検討が必要である。
制度で用いる適合性評価基準について	• 適合性評価制度に取り組んだメーカや輸入業者が泣きを見るような事態にならないよう、レベルは適切に設定する必要がある。 • どのような基準を定めるのかについては、メーカのメリットを鑑みつつ検討を行っていくべきである。
制度で用いる適合性評価スキームについて	• 簡易的かつ適切な方法で評価を行っていく必要がある。 • IoT機器の脆弱性や脅威分析に関する取組と連動するようなスキームがあればより良い。
その他	• 制度な目的として、誰の利益を想定するかを明らかにした方が良い。 • 制度のスコープをきちんと定め、誰が、どのように本制度を活かしていくのかを議論していくべきである。 • IoT製品の適合性評価制度は、ベンダーに負担をかけないような形で実現していくべきである。 • 制度の知名度を上げる努力をしない限り、メーカの説明コストは変わらないため、本制度の普及活動を消費者向けに行う必要がある。 • IT導入補助金との連携や政府の調達要件になる等、取り組んだ企業にメリットがあるような制度になれば良い。

- ✓ 前回の検討会で挙げられた意見を踏まえ、本適合性評価制度で対象とする製品範囲、用いる基準、活用する適合性評価スキームに関し、IoT製品ベンダー・業界団体に対するヒアリングを実施した。
- ✓ 本日の検討会では、IPA様・SCEA様から提供いただく情報も加味しつつ、ヒアリングを踏まえて整理した適合性評価制度の方向性のイメージについて、御意見を頂戴したい。

（参考）IoT製品ベンダー・業界団体に対するヒアリングについて

一部非公開

- ヒアリング対象組織及びヒアリング項目は以下のとおり。

ヒアリング対象組織一覧

構成員限りの開示

ヒアリング質問事項 一覧

【①：製品範囲】

1. 適合性評価制度で対象とする製品の範囲について、「直接的又は間接的にインターネットに接続する製品」とする考え方について、この対象範囲に懸念はあるか。
2. 高いセキュリティレベルが求められる一方でその多くが法規制対象外である産業用ルーターや産業用制御機器を、本適合性評価制度の対象製品範囲に含めるべきか。
3. 諸外国制度では対象外であるPC、スマートフォン等の汎用IT製品について、本制度でも対象範囲外とすることに懸念はあるか。

【②：評価基準】

1. 適合性評価制度で採用する基準について、本制度と諸外国制度とのハーモナイゼーションのために、国際的な標準（ETSI EN 303 645、NISTIR 8425等）を基軸とした基準とすることに懸念はあるか。
2. 適合性評価制度で採用する基準について、ETSI EN 303 645やNISTIR 8425のそれぞれを採用した場合に、どの程度のコスト増などの影響に繋がるか。

【③：適合性評価スキーム】

1. 既に認知・普及されている既存任意認証スキームにサイバーセキュリティ要件を追加する方針で検討を進めることに懸念はあるか。
2. 既存のSマーク認証制度に基づくセキュリティ適合性評価制度とすることに懸念はあるか。

１．前回の検討会のご指摘事項

２．適合性評価制度の位置づけ

３．本適合性評価制度で対象とする製品範囲について

４．本適合性評価制度で用いる適合性評価基準について

５．本適合性評価制度で活用する適合性評価スキームについて

６．本日の討議事項

適合性評価制度の背景となる課題

前回検討会での 関連するご指摘事項	• 制度な目的として、誰の利益を想定するかを明らかにした方が良い。 • 制度のスコープをきちんと定め、誰が、どのように本制度を活かしていくのかを議論していくべきである。

- IoT製品のセキュリティ対策に関して、製品ベンダー、製品ユーザー、国民全体のそれぞれの課題が存在する。
- IoT製品の類型は多岐にわたり、各製品でサイバーリスクの度合いや既存の取組状況が異なることを踏まえつつ、これらの課題解決に資するよう、本適合性評価制度で対象とする製品や採用する適合性評価基準等を検討する必要がある。

【IoT製品ベンダーの課題】

- IoT製品のセキュリティ対策状況が適切に評価されず製品価値に繋がらないおそれ。
- 海外の制度と協調的な制度を構築しない場合、海外の制度の適合性評価を受ける際に別途の負担となる。

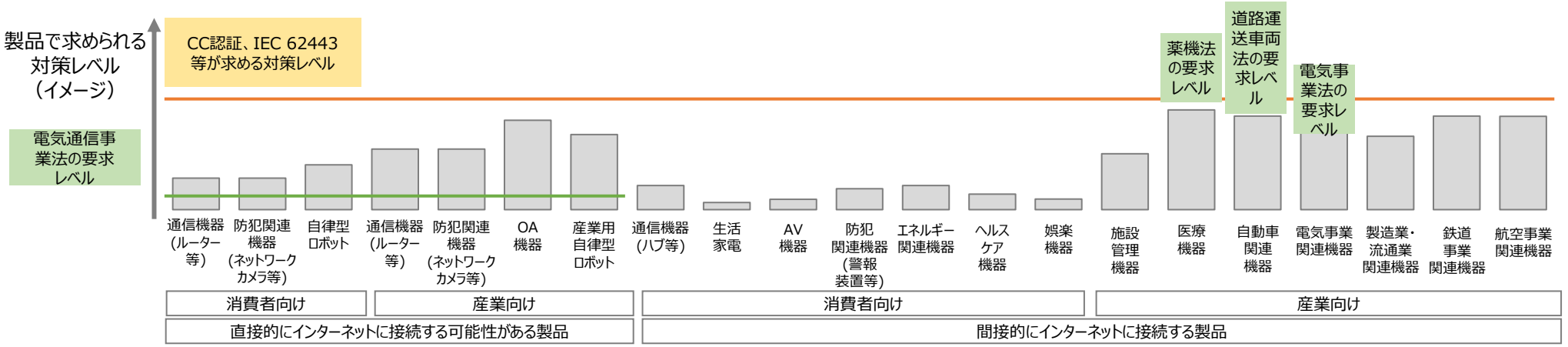
【IoT製品ユーザーの課題】

- 現状ではセキュリティ対策状況が可視化されていないため、適切な対策が施されたIoT製品を選ぶことができないおそれ。

【国民全体の課題】

- マルウェア攻撃によりIoT製品がボット化して他のシステムに悪影響を及ぼすリスク、不正アクセスにより利用者のプライバシー侵害に関するリスク、サイバー攻撃により人体への物理的影響を及ぼすリスク等、IoT製品を狙ったサイバー脅威が高まっている。
- 諸外国はIoT製品に対するセキュリティ対策の取組を進めているところ、十分な取組を実施しない場合に我が国のIoT製品が集中的に狙われ、国内のシステムや国民の生活に悪影響を及ぼすおそれ。

代表的な製品において求められる対策レベルのイメージ



注）あくまでイメージ図であり、求められる対策のレベルを厳密に図示したものではないことに留意。また、産業用通信機器、コントローラー、センサーについては、用いられる産業分野によってリスクが異なるため、本イメージ図からは除外している。

１．はじめに

２．本日議論する適合性評価制度の位置づけ

３．本適合性評価制度で対象とする製品範囲について

４．本適合性評価制度で用いる適合性評価基準について

５．本適合性評価制度で活用する適合性評価スキームについて

６．本日の討議事項

ヒアリング結果①-1：「直接的又は間接的にインターネット接続する製品」

【質問事項①-1】適合性評価制度で対象とする製品の範囲について、「**直接的又は間接的にインターネットに接続する製品**」とすべきと考えられるが、この対象範囲に懸念はあるか。

- 上記の対象製品の範囲の考え方について、**おおむね賛成とする意見**もあった一方で、より丁寧に議論すべき点として、**製品ごとのリスクの優先度を踏まえるべき**、対象製品を具体化すべき、といった意見もあった。

意見区分	ヒアリング結果概要
おおむね賛成	**《「直接的又は間接的にインターネットに接続する製品」を範囲とすることにおおむね賛成の意見》** • 間接接続するIoT製品であってもアタックサーフェスは存在するため、提案の対象製品範囲で良い。 • 任意制度であるため、今回の制度の対象範囲を広く「直接的又は間接的にインターネットに接続するIoT製品」とすることに、特に懸念はない。 • インターネットからの直接アクセス、間接的なアクセスに依存したセキュリティ対策ではないため、懸念はない。 • 端末設備等規則のようにインターネットに直接接続する製品だけを対象にするのは、実効性の観点で疑問があるため、「直接的又は間接的にインターネットに接続するIoT製品」を対象とすることは良い。 • 今回の認証制度の考え方が「最低限のセキュリティレベル」を求めるということであれば、提案の対象製品範囲で良い。一部の機器を除くとなると、その機器の定義が必要となるため、範囲としては「直接的又は間接的にインターネットに接続するIoT製品」で良いのではないか。
より丁寧に議論すべき点	**《製品ごとのリスクの優先度を踏まえた議論をすべきとの意見》** • リスクが高いのは直接接続している機器であり、優先度としては、直接的にインターネットに接続するIoT製品で十分ではないか。 • 直接的間接的にネット接続する製品も無条件で一律に対象範囲内とすることには懸念がある。 • まずは直接的にインターネットに接続する製品を適切に保護することが重要で、間接的に繋がる機器についてはレベルを分ける等の仕組みが必要ではないか。 **《対象製品を具体化すべきとの意見》** • 対象製品範囲を広く定義すると、ベンダーとしては迷う可能性がある。具体的に明記したほうがベンダーとしては対応しやすい。
その他	• 任意の認証制度であれば懸念はないが、製品カテゴリ毎に異なる要求基準/認証スキームの検討が必要ではないか。 • 自動車や医療機器など、独自規格が進んでいる製品は対象から除外しても良いのではないか。 • 間接的なIoT製品も範囲に含めるべきだが、「間接的にインターネットに接続する」という表現を明確化すべきである。

ヒアリング結果①-2：産業用IoT製品

【質問事項①-2】高いセキュリティレベルが求められる一方でその多くが法規制対象外である産業用ルーターや産業用制御機器を、本適合性評価制度の対象製品範囲に含めるべきか。

- 任意制度であること、国際調和の観点、ベンダーの選択肢を広げる観点で、**産業用製品を対象範囲に含めることに肯定的**であるとの意見があった一方で、**高いセキュリティレベルを求める既存認証制度（CC認証、CSA認証等）の対策を追求すべき**という意見もあった。（製品の認証のみならず事業継続の観点からの業種別セキュリティガイドラインを活用する等。）

意見区分	ヒアリング結果概要
おおむね賛成	**《任意制度であることを前提に、あえて対象外とする必要がないとの意見》** • あえて除外する必要は無いが、別途業界で議論し、それぞれの業界の中で何が必要なのか、という事を判断していくことが必要となる。 • 産業用IoT機器であっても、消費者向けIoT機器のセキュリティ水準以上と言って販売してもよいので、あえて対象外とする必要もない。 • 除外するか否かの議論をすると、線引きが難しく、どの機器を含めるか否かの議論が紛糾すると思う。 • 境界線が不明確となる可能性があるため、抜け漏れを無くすために、今回の任意認証制度としてカバーしておく方針は良いと考えている。 **《国際ハーモナイゼーションの観点で、産業用製品を含めることに賛成の意見》** • 国際整合を図る前提で対象範囲に含めるべきである。 **《ベンダーの選択肢の一つとして、産業用製品を含めることに賛成の意見》** • 産業用IoTも対象に含め、CC認証やEDSA認証への橋渡し的な役割の制度するのが良いのではないか。PLCやSCADAにおいてどれだけ対策が進んでいるか未知数であるため、橋渡し的な制度があると、業界としてセキュリティレベルは高まっていくのではないか。 • 今回の制度を土台としつつ、追加で産業用ルーターや制御機器に対する対策を求めたほうが良いのではないか。ベースラインを定めつつ、各産業分野にて追加で求める対策を検討する方針が良いと思う。 • 産業用ルーターや産業用制御機器は高いセキュリティレベルが求められるが、メーカーが取り組む選択肢の一つとして、今回の適合性評価制度の範囲に含めても良いのではないか。
より丁寧に議論すべき点	**《高いセキュリティレベルの対策を追求すべきとの意見》** • 高いセキュリティレベルが求められることを踏まえると、今回の制度の対象とはせず、既存の認証制度の訴求を促すべき。 • 社会インフラのセキュリティ対策に注目が集まっており、産業制御系の機器に対しても適切なセキュリティ対策を求める必要があるため、別の取組で対策を推進する方針もあり得る。
その他の意見	**《認証を実施するか否かは市場原理に基づき判断されるとの意見》** • 産業用ルーターや産業制御機器については、既にCC認証やEDSA認証のような任意認証制度が存在し、市場原理に基づいてベンダーが取捨選択している。

ヒアリング結果①-3：汎用IT製品

【質問事項①-3】諸外国制度では対象外であるPC、スマートフォン等の汎用IT製品について、本制度でも対象範囲外とすることに懸念はあるか。

- 汎用IT製品の扱いについて、販売後の利用者の設定でセキュリティレベルが変わることや、国際調和の観点で、**汎用IT製品を対象範囲外とすることに賛成**といった意見があった一方で、より詳細にリスクの優先度を踏まえるべき、という意見もあり、**リスクの影響度合いを参照しつつ検討することが求められる**。

意見区分	ヒアリング結果概要
おおむね賛成	**《汎用IT製品では、販売後の利用者の設定でセキュリティレベルが変わるため、範囲外とすることに賛成の意見》** • 技術的に対象範囲外にせざるを得ないのではないか。PCやスマートフォン等の汎用IT製品では、購入後に利用者でアプリケーションをインストールでき、セキュリティ対策レベルも変わる。そのため、セキュリティをメーカーで担保することは難しい。 • 汎用IT製品の場合、販売後にセキュリティの対策状況が変わる可能性があるため、対象範囲外とすることに懸念は無い。ただし、もし範囲外とする場合には丁寧な説明が必要となる。 • 多くのIoT製品はなるべく無駄な機能を削っているため、汎用IT製品とは位置づけが異なる。そのため、現状では範囲外とすることに賛成である。 **《国際ハーモナイゼーションの観点で、汎用IT製品を対象範囲外とすることに賛成の意見》** • 国際的な相互運用性の確保を優先すべきと考える。 • 諸外国制度での議論と同様に、容易にセキュリティ対策できるため対象外が良い。あえて日本で追加する必要はない。 • 国際的な整合性と一致させている点において矛盾はなく、懸念はない。 • 汎用IT製品については、後からセキュリティソフトウェアを導入することで対策ができる。諸外国の動向も踏まえると、あえて今回の制度に含める必要はない。
より丁寧に議論すべき点	**《製品ごとのリスクの優先度を踏まえた議論をすべきとの意見》** • 汎用IT製品・IoT製品ともに、論理的に見れば違いは無いため、範囲に含めるべきと考えている。 • 工場設備のセキュリティ対策を考えたとき、PC及びそのソフトウェアで設備のメンテナンスを管理しているため、対策を求めることは重要となる。
その他の意見	• 最初からPC・スマートフォンを対象に含めると制度設計に時間がかかり、制度構築がつまずくのではないか。

IoT製品に関する類型・既存のガイドライン等

- 直接的又は間接的にインターネットに接続する製品に関する類型と、各製品類型のセキュリティ対策に関する既存の文書、認証制度等の関係は次頁に示すとおり。
- 直接的にインターネットに接続する可能性がある製品※1に対しては、総務省の端末設備等規則によるセキュリティ対策が求められている。
- 一方で、間接的にインターネットに接続する製品※2の多くは、製品個別の義務的なセキュリティ対策は現状求められていない。
- 間接的にインターネットに接続する製品のうち、消費者向けの製品について、監視カメラや一部の電力設備には製品個別のセキュリティ対策要件を定めた文書、認証制度等が存在するものの、その他多くの製品については個別の義務的な対策要件を定めた文書、認証制度等は存在しない。なお、これらの製品のうち、半数程度はSマークによる認証が行われている製品である。
- 間接的にインターネットに接続する製品のうち、産業向けの製品について、個別のセキュリティ対策が規定された製品は一部に留まるものの、複数の産業分野において、産業システム全体のセキュリティ対策に関するガイドラインが策定されており、システム全体のセキュリティ対策が求められている。

※1：「直接的にインターネットに接続する製品」とは、総務省端末設備等規則第三十四条の十の対象となる製品を指し、インターネットプロトコル（IP）の一部を構成する通信プロトコルを使用してインターネットに直接接続してデータの送受信を行う製品を指す（ルーター、ネットワークカメラ等）。ただし、製品の利用者が、任意のソフトウェアにより機能を随時かつ容易に変更することができる汎用IT製品（PC、スマートフォン、タブレット端末等）は除外する。

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

・インターネットプロトコル（IP）の一部を構成する通信プロトコルを使用して「直接的にインターネットに接続する製品」に接続し、データの送受信が可能である製品

・2つ以上の製品が併せて利用されることを想定しており、少なくとも1つの製品（「上流製品」という。）が「直接的にインターネットに接続する製品」に接続可能であり、それ以外の製品（「下流製品」という。）が上流製品に接続してデータの送受信を行う場合の下流製品

出所）直接的・間接的にインターネットに接続する製品の定義について、総務省「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第２版)」、英国「Product Security and Telecommunications Infrastructure Act 2022」等に基づき三菱総合研究所作成

製品に関する類型・既存の文書、認証制度等

【凡例】
- 製品個別のセキュリティ対策に関するガイドライン
- 製品個別のセキュリティ対策基準を定めた文書等（下線は義務）
- 製品個別のセキュリティ対策要件を含む認証制度
- システム全体のセキュリティ対策に関する文書等

赤字：Sマークによる認証が行われている製品

注）各製品類型に対するセキュリティ対策要件を定めたガイドラインや認証制度のうち、代表的なガイドライン、制度等をマッピングしている。ただし、CC（ISO/IEC 15408）に基づく認証制度(JISEC制度)については、グローバルで認証付与されている代表的な製品類型又はcPP(Collaborative Protection Profile)が用意されている製品類型に対してマッピングをしている。また、IEC 62443-4に基づく認証について、IEC 62443-4の対象である通信機能を有する産業用自動制御システムのコンポーネントに対してマッピングしている。

製品類型	製品個別の対策に関するガイドライン、基準を定めた文書、認証制度等	高いレベルの基準に基づく認証制度	システム全体の対策に関する文書等
直接的又は間接的にインターネットに接続する製品			
直接的にインターネットに接続する可能性がある製品			
消費者向け			
通信機器（ブロードバンドルーター、Wi-Fiルーターなど）	総務省：技術基準適合認定及び設計についての認証 CCDS：分野別ガイドライン（IoT-GW編） CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる）		経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン(スマートホーム編)
防犯関連機器（ネットワークカメラなど）	日本防犯設備協会：RBSS（監視カメラ、デジタルレコーダー）		
自律型ロボット（ドローンなど）	NEDO：無人航空機分野 サイバーセキュリティガイドライン		
産業向け			
通信機器（ルーター、アクセスポイント、ファイアウォール、UTMなど）		CCに基づく認証 IEC 62443-4に基づく認証	
防犯関連機器（ネットワークカメラなど）	日本防犯設備協会：RBSS CCDSサーティフィケーションプログラム(カメラで実績あり) IPA：情報セキュリティ対策要件チェックリスト(ネットワークカメラ)		
産業用自律型ロボット（産業用ドローン、AGVなど）	NEDO：無人航空機分野 サイバーセキュリティガイドライン 国交省：機体認証制度		
間接的にインターネットに接続する製品			
消費者向け			
通信機器（ハブ・スイッチなど）			経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン(スマートホーム編)
生活家電（掃除機、洗濯機、冷蔵庫、レンジ、エアコンなど）			
AV機器（スマートTV、レコーダー、スマートスピーカーなど）			
防犯関連機器（警報装置、電気錠システムなど）	日本防犯設備協会：RBSS CCDS：CCDSサーティフィケーションプログラム（電気錠操作盤、電子シャッターで取得実績あり）		
エネルギー関連機器（エネファーム、PCS、ガス給湯器など）	JET：系統連系保護装置等認証制度（PCSのみ） CCDSサーティフィケーションプログラム（ガス給湯器リモコンで実績あり） 各一般送配電事業者：系統連系技術要件		
ヘルスケア機器（ウェアラブル端末、電動トレーニングマシンなど）			
娯楽機器（ゲーム機、スマート玩具など）			
産業向け			
通信機器（ハブ・スイッチなど）		CCに基づく認証 IEC 62443-4に基づく認証	※
産業用コントローラー（PLC、DCSコントローラーなど）			※
産業用センサー（温度センサー、圧力センサー、変位センサーなど）			※
OA機器（複合機など）	JBMIA：BMsec	CCに基づく認証	
金融関係機器（決済端末、POS端末など）	CCDS：分野別ガイドライン（ATM編、オープンPOS編） CCDS：CCDSサーティフィケーションプログラム（ATM、決済端末で取得実績あり）		FISC：安全対策基準
施設管理機器（入退室機器、受変電設備、照明、昇降機など）	IPA：情報セキュリティ対策要件チェックリスト(入退室管理)	IEC 62443-4に基づく認証	経産省：ビルガイドライン
医療機器（人工呼吸器、人工心臓弁、輸液ポンプなど）	厚労省：医療機器のサイバーセキュリティの確保及び徹底に係る手引書 厚労省：医療機器の薬事承認等		厚労省：医療情報ガイドライン
自動車関連機器（ECU、IVI、TCUなど）	国交省：道路運送車両の保安基準 CCDS：分野別ガイドライン（車載器編）	CCに基づく認証	
電気事業関連機器（スマートメーター、発電設備、PCSなど）	JESC：スマートメーターシステムセキュリティガイドライン		JESC：電制ガイドライン
製造業・流通業関連機器（生産設備、自動倉庫など）			経産省：工場ガイド 国交省：物流ガイド
鉄道事業関連機器（CTC装置、PRC装置など）			国交省：鉄道ガイドライン
航空事業関連機器（IMS、iDMUなど）			国交省：航空ガイドライン

※ 各産業分野に設置される機器については、各ガイドラインにおいて、システム全体に求められるセキュリティ対策が示されている。

（参考）諸外国制度における対象外製品の定義

- デジタル製品全般を対象としたEUのサイバーレジリエンス法案を除き、ほとんどの諸外国制度が、サーバ、PC、モバイル端末等の汎用IT製品を対象外としている。

国/地域	制度名	対象外製品の定義	対象となる「IoT製品」の定義
	Cybersecurity Labeling for Consumer IoT Product	• サーバ、PC、モバイル端末等の汎用IT製品 ※ なお、セキュリティレベルの高い産業用IoT製品に対するラベリング制度の構築についても米国内で検討されている	• 少なくとも1つのトランスデューサ（センサー又はアクチュエータ）及び少なくとも1つのネットワークインタフェースを備えたコンピューティング機器を「IoT機器」と定義し、IoT機器単体及びIoT機器を使用するために必要な追加の製品コンポーネントを「IoT製品」と定義。
	PSTI Act	• コネクティッドカー、スマートメーター、医療機器など、他法令で対象となっている機器 • サーバ、PC、モバイル端末等の汎用IT製品	• インターネット接続可能な製品及びIPを利用しインターネット接続可能な製品に接続できる製品を「IoT製品」と定義。
	EU Cyber Resilience Act	• 医療機器、体外診療用医療機器、自動車、航空機関連のデジタル製品といった既存のEU法令で対象となっている製品 • 今後策定されるNIS2指令の対象であるSaaSなどのソフトウェアサービス • 国家安全保障又は軍事目的にのみ開発されたデジタル製品及び機密情報を処理するために特別に設計された製品	– （「IoT製品」が対象ではなく、より範囲の広い「デジタル要素を備えた製品」を対象としている。）
	IT Security Label	– （現状では、「IoT製品」すべてを対象ではなく、個別のIoT製品を対象としている。）	– （現状では、「IoT製品」すべてを対象ではなく、個別のIoT製品を対象としている。）
	Cybersecurity Labelling Scheme	• サーバ、PC、モバイル端末等の汎用IT製品	• ネットワークに接続するスマートデバイスを「IoT製品」と定義。
	Finnish Cybersecurity Label	• サーバ、PC、モバイル端末等の汎用IT製品	• インターネットに接続され、デジタル形式でデータを処理・伝送する製品を「IoT製品」と定義。
	Labelling for Smart Devices	現状未定	• インターネットやホームネットワークに接続される前提で開発されたスマートデバイスを「IoT製品」と定義。

出所）各国制度に関する情報に基づき三菱総合研究所作成

１．はじめに

２．本日議論する適合性評価制度の位置づけ

３．本適合性評価制度で対象とする製品範囲について

４．本適合性評価制度で用いる適合性評価基準について

５．本適合性評価制度で活用する適合性評価スキームについて

６．本日の討議事項

ヒアリング結果：②-1　国際的な標準の活用

【質問事項②-1】適合性評価制度で採用する基準について、本制度と諸外国制度とのハーモナイゼーションのために、国際的な標準※を基軸とした基準とすることに懸念はあるか。　（※この場合の国際的な標準とは、欧州地域整合規格や米国基準等も含む。）

- 本適合性評価制度で用いる基準を国際的な標準を基軸とした基準とすることについて、**<u>ほとんどが賛成の意見</u>**であった。
- ただし、基準の日本語版の作成に関する要望や、必要に応じて日本独自の基準を追加検討することの必要性が意見されたほか、より丁寧に議論すべき点として、特定の分野における新たな国際基準策定の必要性について意見が挙げられた。

意見区分	ヒアリング結果概要
おおむね賛成	**《国際ハーモナイゼーションの観点で、国際的な標準を基軸とした基準とすることに賛成の意見》** • 採用する基準について、日本独自の基準を採用することは得策ではなく、グローバルで活用されている国際的な基準を用いるべきである。 • 海外との相互運用性は考慮すべきであり、基本的には国際的な標準に則った形が良い。 • ETSI EN 303 645やNISTIR 8425を基軸とする方針に異論はない。 • 諸外国制度とのハーモナイゼーションのために、国際的に広く使われている基準を用いるのが良い。特に、グローバル企業にとって重要となる。 • 目的から考えると国際的な標準をベースとすることが現実的である。できるだけダブルスタンダードとなることは避けたい。 • 国際的な標準を基軸とした基準とすることに賛成である。しかし、ETSI EN 303 645やNISTIR 8425は英語版のみ公開されているため、JIS化する等、正式な日本語版の基準を作成いただきたい。 • 国際的な標準を基軸とすることに賛同するが、国際的にコンセンサスを得た単一の基準は無いため、何を「国際標準」とみなして活用するか、国際的な動向に加えて認証制度の趣旨も踏まえたうえで判断することが必要である。 • 日本独自の基準や項目の導入は認証制度の利用を妨げることにもつながるため避けることが望ましい。 • 似て非なるものを日本独自で求められることは、コスト・心理的に厳しく、グローバルの制度で採用している基準を元に設計することが望まれる。 • 一部だけを抽出した基準とするのであれば、ETSIやNISTとの対応づけを整理しつつ、独自の基準とした方が良い。 • ETSI EN 303 645は基本的事項が記載されたものと認識しており、ここから削るという議論でもよいし、削る項目が決められなかったらETSI EN 303 645と同じでもよい。 • 基本的な項目は同盟国の基準と整合を図りつつも、必要に応じて、日本独自の経済安全戦略に合わせた基準を策定すべきである。 **《特定分野について、新たに国際基準を策定すべきとの意見》** • 欧州基準、米国基準はいずれも受け入れられない。自動車分野でWP29国際基準策定のように、家電機器・住設機器分野でも「国際基準」の策定が求められる。経済産業省においては、各国政府機関とも連携の上で、策定に向けて主導的な取り組みをお願いしたい。
その他の意見	• どの規格であっても、国内で評価できる体制が必要である。

（参考）ETSI EN 303 645及びNISTIR 8425の要求基準の概要

- ETSI EN 303 645では、消費者向けIoT機器のセキュリティに関する13項目が規定されているほか、個人データ保護に関する規定も整理されている。
- NISTIR 8425では、消費者向けIoT機器のセキュリティ機能に関する6項目に加え、メーカーの非技術的サポート機能に関する4項目が規定されている。

ETSI EN 303 645の要求基準概要

機器のセキュリティに関する13項目

4.1 報告書を作成すること。
5.1 共通の初期パスワードを設定しない。
5.2 脆弱性報告の管理手段を導入する。
5.3 ソフトウェアを定期的に更新する。
5.4 機密性の高いセキュリティパラメータを安全に保存する。
5.5 安全に通信する。
5.6 攻撃対象となる領域を最小限に抑える。
5.7 ソフトウェアの整合性を確保する。
5.8 個人データの安全性を確保する。
5.9 機能停止時のシステムの復旧性を確保する。
5.10 システムのテレメトリデータを検証する。
5.11 ユーザーがユーザーデータを容易に削除できるようにする。
5.12 デバイスを容易に設置してメンテナンスできるようにする。
5.13 入力データを検証する。

個人データ保護に関する6項目

6.1 製造者は、消費者に対し、機器やサービスごとに、どのような個人データが、誰によって、どのような目的で処理されているかについての明確かつ透明性のある情報を提供するものとする。これは、広告主を含む関与しうる第三者にも適用される。
6.2 個人データが消費者の同意に基づいて処理される場合、この同意は有効な方法で取得されるものとする。
6.3 個人データの処理に同意した消費者は、いつでもその同意を撤回することができるものとする。
6.4 消費者向けIoT機器やサービスからテレメトリーデータを収集する場合、個人データの処理は意図した機能に必要な最小限のものにとどめるべき。
6.5 消費者向けIoT機器やサービスから遠隔測定データを収集する場合、消費者はどのような遠隔測定データが収集され、それが誰によって、どのような目的で使用されているかについての情報を提供されるものとする。

NISTIR 8425の要求基準概要

機器のセキュリティ機能に関する6項目

- 機器の識別：IoT製品を論理的・物理的に一意に識別できる。
- 機器の構成：IoT製品のソフトウェアの構成変更を正規のエンティティのみが行える。
- データの保護：IoT製品が保存・伝送するデータを、不正アクセス及び改ざんから保護できる。
- インタフェースへの論理アクセス：IoT製品のインタフェース及びインタフェースで利用されるプロトコルとサービスへの論理的アクセスを、正規のエンティティのみに制限できる。
- ソフトウェアの更新：IoT製品のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティによってのみ更新できる。
- サイバーセキュリティの状態認識：IoT製品は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限する。

メーカーの非技術的サポート機能に関する4項目

- ドキュメンテーション：メーカーやその支援機関が、顧客の購入前、そして機器の開発やその後のライフサイクルを通じて、IoT製品のサイバーセキュリティに関する情報を作成、収集及び保存する機能を有する。
- 情報及び問い合わせの受付：メーカーやその支援機関が、IoT製品のサイバーセキュリティに関する情報や問い合わせを顧客等から受け付ける機能を有する。
- 情報発信：メーカーやその支援機関が、IoT製品のサイバーセキュリティに関する情報を発信する機能を有する。（発信対象の例：顧客やIoT製品に関するステークホルダー）
- 教育及び意識向上：メーカーやその支援機関が、IoT製品のサイバーセキュリティに関する情報や考慮事項、機能等に関して、顧客やIoT製品に関するステークホルダーの認識を高め、教育する機能を有する。

※ いずれの文書についても、各項目に複数の対策要求基準が規定されていることに留意。

（参考）ETSI EN 303 645及びNISTIR 8425の要求基準の関係性イメージ

- ETSI EN 303 645とNISTIR 8425の対策要求基準について、多くの対策要求基準が共通しているものの、一部の要求基準は片方の文書のみに明記されている。

③ NISTIR 8425のみに規定されている要求基準

- 機器の識別：IoT製品を論理的・物理的に一意に識別できる。
- 機器の構成：IoT製品のソフトウェアの構成変更を正規のエンティティのみが行える。

① ETSI EN 303 645のみに規定されている要求基準

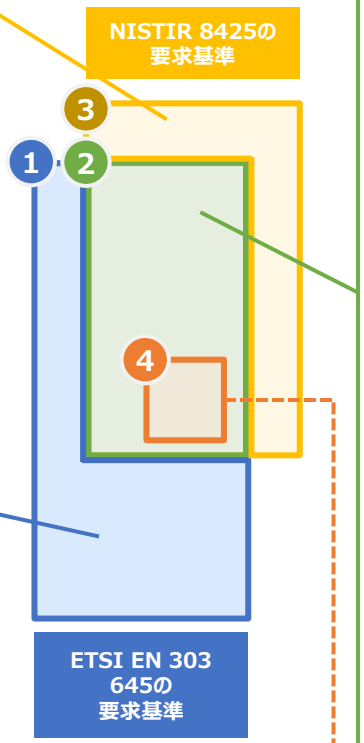
5.8 個人情報の安全性を確保する。

5.13 入力データを検証する。

6.2 個人データが消費者の同意に基づいて処理される場合、この同意は有効な方法で取得されるものとする。

6.3 個人データの処理に同意した消費者は、いつでもその同意を撤回することができるものとする。

6.4 消費者向けIoT機器やサービスからテレメトリーデータを収集する場合、個人データの処理は意図した機能に必要な最小限のものにとどめるべき。



② ETSI EN 303 645とNISTIR 8425の両方に規定されている要求基準

ETSI EN 303 645ベース	NISTIR 8425ベース	総務省：端末設備等規則ベース
4.1 報告書を作成すること。	ドキュメンテーション	–
5.1 共通の初期パスワードを設定しない。	インターフェイスへの論理アクセス	第三十四条の十 一（アクセス制御機能） 第三十四条の十 二（初期設定のパスワードの変更を促す等の機能）
5.2 脆弱性報告の管理手段を導入する。	情報及び問合せの受付、教育及び意識向上	–
5.3 ソフトウェアを定期的に更新する。	ソフトウェアの更新、情報発信	第三十四条の十 三（ソフトウェアの更新機能）
5.4 機密性の高いセキュリティパラメータを安全に保存する。	データ保護、インターフェイスへの論理アクセス	–
5.5 安全に通信する。	データ保護	–
5.6 攻撃対象となる領域を最小限に抑える。	インターフェイスへの論理アクセス	–
5.7 ソフトウェアの整合性を確保する。	サイバーセキュリティの状態認識	–
5.9 機能停止時のシステムの復旧性を確保する。	インターフェイスへの論理アクセス、ソフトウェアの更新	第三十四条の十 四（電力供給が停止した場合でも、出荷状態に戻ることなく、アクセス制御機能に係る設定や更新されたソフトウェアの維持）
5.10 システムのテレメトリデータを検証する。	サイバーセキュリティの状態認識	–
5.11 ユーザーがユーザーデータを容易に削除できるようにする。	データ保護、教育及び意識向上	–
5.12 デバイスを容易に設置してメンテナンスできるようにする。	教育及び意識向上	–
6.1 製造者は、消費者に対し、機器やサービスごとに、どのような個人データが、誰によって、どのような目的で処理されているかについての明確かつ透明性のある情報を提供するものとする。これは、広告主を含む関与しうる第三者にも適用される。	教育及び意識向上	–
6.5 消費者向けIoT機器やサービスから遠隔測定データを収集する場合、消費者はどのような遠隔測定データが収集され、それが誰によって、どのような目的で使用されているかについての情報を提供されるものとする。	教育及び意識向上	–

※ 右表はETSI EN 303 645を軸とした項目レベルでの対応関係のマッピングであり、詳細な対策要求項目を比較するとより多くの差異が存在することに留意。ETSI/NISTの対応関係のマッピングは、NISTIR 8259A及びNISTIR 8259Bの記載に基づき作成。

※ 総務省の端末設備等規則は義務要件であり、必要最低限の規程となっていることに留意。

出所）公開情報に基づき三菱総合研究所作成

（参考）ETSI／NISTの各要求基準を採用した場合の影響に関するヒアリング結果

【質問事項②-2】適合性評価制度で採用する基準について、ETSI EN 303 645やNISTIR 8425のそれぞれを採用した場合に、どの程度のコスト増などの影響に繋がるか。

- 採用する基準によって、ベンダーのコスト増などの影響が変わるところ、今後、メーカーに与える影響、適合性評価に要するコスト、国際動向等を踏まえ、一部の基準の取捨選択や独自基準の追加も視野に入れた詳細な検討を行うこととする。

ヒアリング結果概要

《ETSI EN 303 645で求められる基準のみを採用した場合（①＋②の範囲）の影響に関する意見》
- ETSI EN 303 645は基礎的な事項とプライバシーが考慮されている。プライバシーをどこまで見るかはあるが、ETSI EN 303 645を元に考えることになるのではないか。
- ETSI EN 303 645の基準をすべて採用することは過剰である。
- 産業用機器では個人データの取扱いがないことが多いため、冗長だと考えらえる。
- ETSI EN 303 645は少しハードルが高く、大手企業のような体力がある企業に限られるのではないか。
- 欧州は強制法規となる一方で、NISTIRは任意基準なので、強制法規のETSI EN 303 645が優先されるのではないか。
- ETSI EN 303 645を採用している各国制度においても一部の要求基準を抽出していると思う。日本においても、必要な要件を取捨選択するのが良いのではないか。

《NISTIR 8425で求められる基準のみを採用した場合（②＋③の範囲）の影響に関する意見》
- NISTIR 8425の基準をすべて採用することは過剰である。
- ETSI EN 303 645よりも対応しやすいと考えられるが、中小企業等のリソースが限られる事業者にとって「非技術的サポート機能」の対応が困難となる可能性がある。
- グローバルで共通的に求められる基準であれば、国内の適合性評価制度に対応するためのコスト増にはならない。NISTIR 8425の場合、米国では任意制度なので、日本企業としては取得のインセンティブが低い。
- NISTIR 8425は比較的対応しやすいが、組織的対策も含まれているので、リソースが限られている中小企業のような会社は対応が難しいかもしれない。

《ETSI EN 303 645とNISTIR 8425の両方で求められる基準を採用した場合（②の範囲）の影響に関する意見》
- メーカーにとって、そこまで負担にはならないと思う。
- レベル分け次第ではあるが、まずはNISTとESTIの両方で求められる基準を考えるのが良いのではないか。

《ETSI EN 303 645とNISTIR 8425のいずれかのみを採用した場合（①＋②又は②＋③の範囲）の影響に関する意見》
- ETSI EN 303 645とNISTIR 8425をベースするでのあれば、どちらかの規格に適合していれば、「適合」と見なすと影響は小さくなる可能性がある
- 製品によって国内向け、欧州向け、米国向け、グローバル展開など様々であり、基準・規定が多いと手間暇がかかるので、ETSI基準、NISTIR基準の少なくとも一方を求める、とすることが実用的である。

《ETSI EN 303 645とNISTIR 8425のいずれかで求められる基準すべてを採用した場合（①＋②＋③の範囲）の影響に関する意見》
- ETSIとNISTのいずれかで求められている基準に全て対応するとなると正直かなり厳しい。対策コストが倍増することとなる。
- 最も高コストになると考えられ、事業者が対応できずに普及が進まなくなる可能性がある。
- 対応コストがかかり、競争力が低下する。

《その他の意見》
- ETSI EN 303 645、NISTIR 8425のどちらもコスト増に繋がる。
- 現状達成している基準より低い基準であっても、対応コストはかかることとなる。
- 大手メーカーにおいては、ETSIやNISTの基準を採用することの影響は限定的ではないか。他方で、国内向けのみに製品販売している中小企業等の場合、追加の対応が必要なケースが多く、大きな影響を及ぼすのではないか。

１．はじめに

２．本日議論する適合性評価制度の位置づけ

３．本適合性評価制度で対象とする製品範囲について

４．本適合性評価制度で用いる適合性評価基準について

５．本適合性評価制度で活用する適合性評価スキームについて

６．本日の討議事項

ヒアリング結果：③-1　既存任意認証スキームの活用

【質問事項③-1】既に認知・普及されている既存任意認証スキームにサイバーセキュリティ要件を追加する方針で検討を進めることに懸念はあるか。

- 効率的に制度を普及・促進する観点で、**既存任意認証スキームにサイバーセキュリティ要件を追加する方針に賛成**の意見が挙げられた一方で、より丁寧に議論すべき点として、制度間の整合化が図れないことへの懸念、市場の混乱、将来の発展可能性等の観点で、**独自認証制度を新たに構築すべき**との意見が挙げられた。
- 関連して、第三者認証のみを許容する場合、評価にコストかかり、IoT製品ベンダーの負担が増加することから、**自己適合宣言による評価を求める**意見が挙げられた。

意見区分	ヒアリング結果概要
おおむね賛成	**《効率的に制度を普及・促進する観点で、既存任意認証スキームにサイバーセキュリティ要件を追加する方針に賛成の意見》** • 新しいスキームを作るよりは既存のスキームを活用できた方が効率的と考える。 • 既存の認証スキームを利用している企業は既存制度を活用した方が負担は少ない。 • 認証申請の手間が省けるため良いと考える。 • 既存の任意認証スキームを用いることで、既に認証取得している企業としては受け入れやすく、新たに制度を構築して広報するより良いと思う。 • 社内に訴求する際は、既存の仕組みにセキュリティ要件が追加されたほうが動きやすい。新たな制度を構築し、それをメーカーに訴求することは大変な作業となるため、既存の仕組みに入れ込んだほうが導入のハードルは低い。
より丁寧に議論すべき点	**《様々な既存任意認証スキームにセキュリティ要件を追加した場合、制度間の整合化が図れない可能性があるため、既存任意認証スキームにサイバーセキュリティ要件を追加すべきではないとの意見》** • 様々な既存の評価制度にセキュリティ要件が含まれる場合、それぞれの評価制度のセキュリティ要件が重複、あるいは相反する事も考えられるため、現状では現状では既存制度に絡めた評価制度とすることには反対する。 **《市場の混乱を防ぐために、独自認証制度を新たに構築すべきとの意見》** • セキュリティの任意認証制度としては、新たな制度(例: Sマーク セキュリティ版など)の導入が市場混乱も少ないと考えられる。 **《既存任意認証スキームの制約を受けるため、将来の発展可能性のために、独自認証制度を新たに構築すべきとの意見》** • 既存の任意認証スキームを活用することで広く活用される可能性はあるが、当該スキームの制約条件を受けることとなる。活用拡大は、制度の普及など運用面でカバーする話であるが、制約条件はどうしようもない可能性がある。そのため、将来的なことを考えると、独自の認証制度を作ったほうが良いのではないか。
自己適合宣言に関する意見	**《自己適合宣言を許容する認証スキームとすべきとの意見》** • 多くのIoT製品メーカーは自社でセキュリティ対策の確認を実施しているため、追加コストを避けるために、自己適合宣言を許容することが望まれる。 • コスト面からは自己宣言型が望ましい。レベルを分け、自己宣言と第三者認証が分かれるという考えがある。
その他の意見	• いずれの任意認証スキームを活用する場合でも各国との相互認証が必要となる。 • セキュリティ要件が足されることによって、現行普及している制度の普及率が減る可能性も高いため、慎重な議論が必要である。 • 消費者において任意の制度であることが理解されるかどうかが疑問である。制度の品格を高めないとメーカーとしても動きづらく、制度が活用されない懸念がある。

１．はじめに

２．本日議論する適合性評価制度の位置づけ

３．本適合性評価制度で対象とする製品範囲について

４．本適合性評価制度で用いる適合性評価基準について

５．本適合性評価制度で活用する適合性評価スキームについて

６．本日の討議事項

本日の討議事項①

適合性評価制度で対象とする製品範囲について

前回検討会での 関連するご指摘事項	• 消費者向け製品も産業向け製品のどちらも制度の対象とするべきだと考えているが、レベルは分けるべきであり、消費者向け製品であっても最低限のセキュリティ対策は求められるべき。 • ラベリング制度を設けるのであれば、有効なのは消費者向けIoT製品である。 • 消費者向けIoT製品からスタートし、様々な課題を整理していくことが重要である。 • 同じIoT機器であっても、消費者向けとして使われる場合と重要インフラ向けに使われる場合があるため、対象とする機器の検討が必要である。
IoT製品ベンダー・業界団体に対するヒアリング	• 対象製品範囲を「間接的又は直接的にインターネットに接続する製品」とすることについて、おおむね賛成とする意見もあった一方で、より丁寧に議論すべき点として、製品ごとのリスクの優先度を踏まえるべき、対象製品を具体化すべき、といった意見もあった。 • 産業用製品の扱いについて任意制度であること、国際調和の観点、ベンダーの選択肢を広げる観点で、産業用製品を対象範囲に含めることに肯定的であるとの意見があった一方で、高いセキュリティレベルを求める既存認証制度（CC認証、EDSA認証等）の対策を追求すべきという意見もあった。 • 汎用IT製品の扱いについて、販売後の利用者の設定でセキュリティレベルが変わることや、国際調和の観点で、汎用IT製品を対象範囲外とすることに賛成といった意見があった一方で、より詳細にリスクの優先度を踏まえるべき、という意見もあり、リスクの影響度合いを参照しつつ検討することが求められる。

【討議事項①】

✓ **<u>本制度で対象とする製品の範囲について、「間接的又は直接的にインターネットに接続する製品」としてはどうか</u>**。

✓ その上で、製品ごとのリスクやシステム全体で対策を実施していくべき産業分野等を考慮し、P.12の製品類型整理を参照しつつ、**<u>「新たな制度において特に優先度の高い製品」や「既存の制度で対応すべき製品」等の峻別を精緻に行っていくべきではないか</u>**。

＜精緻な検討にあたっての論点＞

- 直接的にインターネットに接続する可能性がある製品に対しては、総務省の端末設備等規則によるセキュリティ対策が求められているが、ETSI EN 303 645やNISTIR 8425が要求する事項との差異を踏まえた検討をしていくべきではないか。（討議事項②で議論）
- 間接的にインターネットに接続する製品のうち、消費者向けの製品について、多くの製品は個別の対策要件を定めた文書や認証制度等に乏しいことから、Sマーク等、既存制度で普及効果が高いと考えられる制度にセキュリティ要件を組込むことを検討すべきではないか。（討議事項③で議論）
- 産業向け製品については、CC認証等の高い基準の適用を行っていくべきと考えられるが、普及率は低い現状がある。このような現状を鑑み、CC認証等の普及を促進していく必要があるものの、広くセキュリティレベルを確保するために、本適合性評価制度の対象製品範囲に含めるべき産業向け製品もあると考えられるのではないか。その際に、いかなる製品を対象とすべきかについては、製品が有するリスク、事業継続等を考慮し、分野ごとに個別に検討していくべきではないか。また、産業システム全体としてのセキュリティ対策を求めたガイドラインが存在する分野もあるため、本適合性評価制度の対象とするかについては、業所管部局と議論を進めていくべきではないか※。

※我が国の基幹インフラに関する政府の動きとしては、経済安全保障推進法における基幹インフラの安全性、信頼性確保に関する今後の課題として、サイバー・セキュリティに関するリスクへの対応が挙げられている。
(https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai1/siryou3.pdf)

本日の討議事項②

適合性評価制度で用いる適合性評価基準について

前回検討会での 関連するご指摘事項	• 適合性評価制度に取り組んだメーカや輸入業者が泣きを見るような事態にならないよう、レベルは適切に設定する必要がある。 • どのような基準を定めるのかについては、メーカのメリットを鑑みつつ検討を行っていくべきである。

IoT製品ベンダー・業界団体に対するヒアリング	• 本適合性評価制度で用いる基準を国際的な標準を基軸とした基準とすることについて、ほとんどが賛成の意見であった。 • ただし、基準の日本語版の作成に関する要望や、必要に応じて日本独自の基準を追加検討することの必要性が意見されたほか、より丁寧に議論すべき点として、特定の分野における新たな国際基準の必要性について意見が挙げられた。

【討議事項②】

✓ 本制度で採用する基準について、**ETSI EN 303 645やNISTIR 8425等、国際的な標準を基軸とした適合性評価基準を前提とすべきではないか**。

✓ 直接的にインターネットに接続する製品については、端末設備等規則との関係の整理が必要と考えられる。総務省の端末設備等規則によるセキュリティ対策が求められているが、ETSI EN 303 645やNISTIR 8425が要求する事項との差異を踏まえた検討をしていくべきではないか。

✓ なお、ETSI EN 303 645やNISTIR 8425で定められている要求基準のうち、**具体的にどの基準を、P.12で整理されるどの製品類型に適用するかについては、個別に検討が必要ではないか**。

本日の討議事項③

適合性評価制度で活用する適合性評価スキームについて

前回検討会での関連するご指摘事項	• 簡易的かつ適切な方法で評価を行っていく必要がある。 • IoT機器の脆弱性や脅威分析に関する取組と連動するようなスキームがあればより良い。
IoT製品ベンダー・業界団体に対するヒアリング	• 効率的に制度を普及・促進する観点で、既存任意認証スキームにサイバーセキュリティ要件を追加する方針に賛成の意見が挙げられた一方で、より丁寧に議論すべき点として、制度間の整合化が図れないことへの懸念や市場の混乱や将来の発展可能性の観点で、独自認証制度を新たに構築すべきとの意見が挙げられた。 • 関連して、第三者認証のみを許容する場合、評価にコストかかり、IoT製品ベンダーの負担が増加することから、自己適合宣言による評価を求める意見が挙げられた。

【討議事項③】

✓ 適合性評価スキームについては様々な御意見をいただいているところ、以降に示すイメージを踏まえ、以下の点について御議論いただきたい。

《既存制度の活用について》

✓ 任意制度において、知名度のない制度を0から普及させるには高いハードルがあることや、消費者から見て制度が林立し分かりづらくなる可能性があることから、P.25のプランBのように新たに制度を構築することは避け、**P.25のプランAのように既存の適合性評価スキームを活用した制度とすることが適当ではないか**。

✓ その際に、**どの既存制度を活用するかは、製品類型と現に対象となっている既存制度の関係、製品類型ごとのリスク等も勘案して判断していくべきではないか**。

＜既存制度を活用する例：Sマーク認証制度＞

- 特に、間接的にインターネットに接続する消費者向け製品について、○PSEマークの対象である製品については、Sマーク認証がメーカーに広く普及しているため、Sマーク認証制度を活用したセキュリティ適合性評価制度とした場合、普及効果が大きいと考えられる。
- また、Sマーク認証制度は○PSEマーク対象製品を中心に全ての電気製品を対象としているため、○PSEマークの対象外製品においても適用できるほか、新制度を0から立ち上げるよりもSマークの認知度を活用できるというメリットがある。

《自己適合宣言の可否について》

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

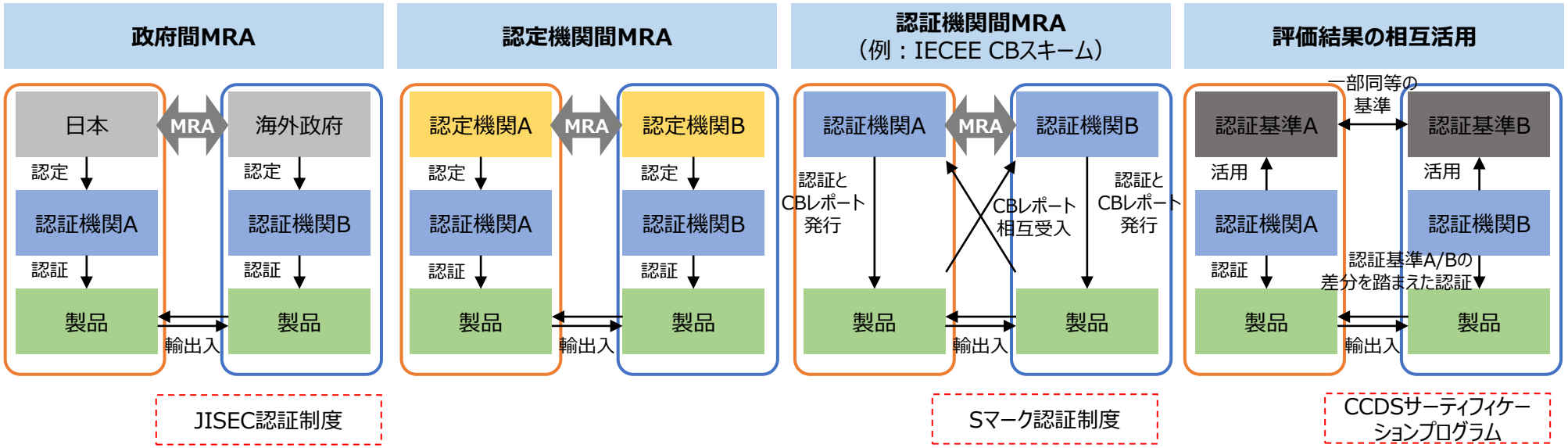
（参考）本適合性評価制度で活用する適合性評価スキームイメージ

本適合性評価制度の構築に関するプラン

本制度の構築に関するプラン	プランA：既存の適合性評価スキームを活用する		プランB：新たな適合性評価スキームを構築する
	プランA-1：既存の製品適合性評価スキームにサイバーセキュリティの要件を追加する	プランA-2：サイバーセキュリティに関する既存の適合性評価スキームを活用する	
メリット	• サイバーセキュリティに関する既存の適合性評価スキームと比較して広く普及している制度が複数存在するため、本制度の活用のハードルが比較的低くなるほか、広報コストを低減できる。	• サイバーセキュリティ要件が既に含まれているため、比較的短期間で制度構築に至る可能性が高い。	• 既存制度の制約に縛られること無く、制度を設計・構築・運用することができる。 • 既存制度の影響を受けないため、比較的短期間で制度構築に至る可能性が高い。
想定される懸念・課題	• 既存評価スキームの制約を受けるため、制度の構築や将来の運用が煩雑になるおそれがある。 • 既存評価スキームの認証機関においてセキュリティ基準に関する評価が困難なおそれがある。 • 新たにサイバーセキュリティ要件が追加されることにより、既に認証取得しているメーカーや市場が混乱するおそれがあるほか、現行の制度の普及率が低減するおそれがある。 （⇒ 既存制度の認証スキームを活用しつつ、セキュリティに関する新たな制度とすることも想定。）	• 左記の適合性評価スキームと比較して普及状況が限定的であるため、制度活用のインセンティブを明確化しない場合や普及促進を実施しない場合、制度が広く活用されないおそれがある。	• 知名度のない制度を0から普及させるには高いハードルがあるため、制度活用のインセンティブを明確化しない場合や普及促進を実施しない場合、制度が広く活用されないおそれがある。 • 消費者の視点から、複数の適合性評価制度が林立し、適切な適合性評価制度が分かりづらくなるおそれがある。
候補となる既存適合性評価スキーム	• 電気製品認証協議会：Sマーク認証制度 • 日本防犯設備協会：優良防犯機器認定制度（RBSS）等	• 総務省：端末設備等規則 • IPA：JISEC認証制度 • CCDS：CCDSサーティフィケーションプログラム • JBMIA：事務機セキュリティプログラム（BMSec） 等	－

（参考）国際相互承認の方式

- 認証結果の国際相互承認の方式として、政府間のMRAによるスキーム、認定機関間のMRAによるスキーム、認証機関間の協定によるスキームが存在する。
- Sマーク認証制度では、IECEE CBスキームに基づく認証機関間の相互承認が活用できるほか、JISEC認証制度の場合、CCRA（Common Criteria Recognition Arrangement）に基づく国際相互承認が活用できる。
- これらのスキームは認証結果の国際相互承認に関するスキームであるが、CCDSサーティフィケーションプログラムでは諸外国の適合性評価結果が活用可能である。具体的には、CCDSサーティフィケーションプログラムの基準と諸外国の基準とは一部整合性があるため、諸外国での適合性評価結果が既に存在する場合は、その結果を活用しつつ、CCDSサーティフィケーションプログラムのみで求められる基準を追加評価することで、効率的に認証付与が可能となる。



出所）初回検討会におけるJQA大塚様資料に基づき三菱総合研究所作成

（参考）自己適合宣言の許容可否に関するメリットと想定される懸念・課題

自己適合宣言に関する選択肢	自己適合宣言を許容する	自己適合宣言を許容せず、第三者評価のみを許容する
メリット	• 自己適合宣言が許容されることで、安価に評価ができ、様々なIoT製品メーカーに活用される可能性が高まる。	• 第三者評価のみとなるため、自己適合宣言と比較してより厳密にセキュリティ対策を確認できる。
想定される懸念・課題	• 第三者評価が行われないことで、厳密なセキュリティ対策の確認が難しいおそれがある。 （⇒ 適合宣言書や定期的なサーベイランス等の運用面でカバーする必要あり。）	• 第三者評価が必要となるためIoT製品メーカーが支払うコストが増加※1し、中小企業をはじめとする企業の活用ハードルが高まるおそれがある。 • 第三者評価機関に対して大量の評価の要望があった場合に、評価に時間を要するおそれがある。
採用している諸外国制度（予定含む）	EU Cyber Resilience Act Cybersecurity Labelling Scheme	Cybersecurity Labeling for Consumer IoT Product PSTI Act IT Security Label Finnish Cybersecurity Label

※1：第三者評価に要するコストは設定する基準に依存するが、関連するCCDSサーティフィケーションプログラムの場合、検査費用は50～200万円とされている。