11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

申請についての質問	
質問	回答
申請書の書き方については、説明会で口頭説明のあった事項についても注記等として案内はありますか。 例> 製造方法区分、ファームウェア開発・保守方法区分、OEM/ODM製造企業名	申請書の記載方法についての説明はホームページで公開します。
申請できるのは法人のみであるようにお話がありましたが、団体や個人事業主では申請できないのですか。	申請企業になれるのは自社ブランドのIoT製品を作っているという前提があります。ですので、団体や個人事業主であっても自社ブランドのIoT製品を作っているであれば申請できます。
申請は企業ごとに定められた同一人物によるものである必要がありますか。	そのような制限はありません。
一申請に対し、複数の製品型番を紐付けて申請することが可能とのことですが、ラベル発行後何らかの理由カラーバリエーションが増えるなどで、製品型番が増加した場合、これを追加いただく仕組みは用意されますでしょうか。別途申請が必要でしょうか。	同一のファームウェアを使っている製品で型番が増えた場合に同じように追加をするのであれば、変更届けを提出していただきます。
製品名が変わる場合は変更もしくは追加の手続きをすればよろしいでしょうか。	説明いただいて、適切な手続きを案内します。
★1申請の問い合わせ窓口等は準備予定でしょうか。	申請ラベルの申請のための問い合わせ窓口を用意する予定はありませんが、申請窓口を用意する可能性はあります。

会社の合併があって、URLが変わることは当然あり得ますが、単純に変更申請で済むのでしょうか。それとも、その場合はもう再申請が必要になったりするのでしょうか。	URLや連絡先等の単純な変更に関しては、変更届出をしていただければ、ホームページ上の記載を変更することが可能です。 しかし、合併もしくは分社化、あるいは売却等、企業が変わるという場合には、継承手続をしていただきます。継承手続の結果、継承が認められればそのままスライドしますが、継承が認められない可能性もあり、その場合にはラベル失効の手続を取ります。
製品類型がいくつか定められていますが、自社の製品でどこに該当するかが不明、もしくは該当しないと考えられる製品があります。	製品類型の中には「その他」の項目がありますので、どれにも当てはまらない場合には「その他」を選んで記入していただければ結構です。
チェックリストの確認をする方向けの教育予定があったら教えていただきたい。	現時点では予定していませんが検討させてください。
メール添付ファイル申請でしょうか、それともweb申請でしょうか。	当初はメールベースでの申請となります。エクセルベースの申請書を作成していただきます。 ※申請書を公開しました。
運用条件による基準の対象／非対象の判断が入るということになると、実際問題として審査期間が延びるのではないでしょうか。申請から確認作業が約2週間となっていますが、申請者と運用条件の確認がこの期間に収めるのは難しいように思います。	あくまでも、★1に関しては自己チェックに基づきますので、ベンダーの責任として判断をしてください。基準の対象／非対象の判断に関して、申請内容に外形的に不備がある、明らかに論理矛盾をしている等、確認の必要があると判断された場合を除き、IPAがその内容を確認することはありませんので、審査が伸びるということはないと考えています。 なお、対象／非対象の判断の根拠は、技術文書として残しておく責任がベンダーにあります。
海外のベンダーから仕入れて日本国内の代理店で販売するケースがかなり多いが、日本法人がない場合は申請できますか。代理店が製造ベンダーに対して確認を行った上でチェックリストを仕上げて申請するというスキームを取れますか。	理論的には日本の代理店業者なら申請できなくはありません。ただし、その製品の製造ベンダー企業の同意や委任が要ります。また、製造方法やファームウェアの開発・保守に関する情報が必要になりますので、そこまで開示・協力してもらえるかどうかというハードルがあると考えられます。それらがないと代理申請がそもそもできません。 また、適合ラベルはその製造ベンダーの製品に対して発行されますので、同意・委任が要るということになります。
代理申請の際は、申請代理会社がエビデンスを保有する形でもできるか。	サーベイランスなど、必要な時に、申請代理会社自身、又は少なくとも製造ベンダーと交渉や契約などを事前に行っておき、製造ベンダーからエビデンスを出せるようにしておいていただきたいと思います。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

対象製品についての質問	
本制度の対象外となるIoT製品について、お客様の調達要件にJC-STAR適合ラベル取得が必須と提示された場合に「適合ラベルの対象外です」という申し入れは、入札する立場の方からできるものでしょうか？	原則として調達者と調整をしていただくことになります。その際、PCやタブレットなどのように、どのベンダーの製品であれ、同じように対象外となるものについては、比較的外す外さないの交渉・調整はしやすいと考えています。 ただし、注意していただきたい点として、IoT製品の仕様や設計等の違いにより、筐体の外見的には同じような機能を有するIoT製品でありながら、「適合ラベルの対象となる製品」と「適合ラベルの対象外となる製品」とが混在してしまうケースがありうる点です。この場合、「適合ラベルがない製品」は、「対象だがラベルを取得していない（できない）製品」なのか「対象外なのでラベルがそもそもない製品」なのかの判断がつきにくいことが想定されます。そのようなケースでは、ベンダーのビジネス判断に基づき、調達者に対して「対象外であることを説明しご理解いただく」か、「本来は対象外だが、ベンダーの独自判断として対象とみなしラベル取得申請を行う」かのどちらでも選択できるようにします。
ハードウェアが例えば汎用のもので、そこに自社のアプリケーションをのせてIot機器とする場合、ベンダーのインプリの仕方によって外見上は本制度のIoT製品の対象となるかどうかがわからない場合が出てくると想定される。そうした場合は、本制度のIoT製品の定義上は「対象外」であったとしても、ベンダーの判断でラベル取得を進めていったほうがよいということでしょうか。	適合ラベルを取るには一定のコストがかかることになるので、あくまで自社のビジネス判断を踏まえて、ラベル取得を進めるかどうかの対応を決めていただきたい。
必須付随サービスとしてIoT機器を操作するスマホアプリがある場合、そのスマホアプリに対しても適合ラベルを付けることができますか。	適合ラベルがつくのは、あくまでIoT機器に対してのみです。必須付随サービスであるスマホアプリに対して適合ラベルがつくことはありません。

PCやタブレットが本制度の対象製品ではないという説明がありました。これは基本OSをベンダが開発していないためと理解しています。この論理からAndroid TVなどのスマートTVも対象外となるのでしょうか？	PCやタブレットが本制度の対象外となる理由は、別のベンダが提供しているソフトウェアを通常の手順を使えば利用者が自らの意志で後からインストールすることができるためです（要件④を満たさない）。OSをベンダが開発していないからという理由ではありません。 その観点で、Android TVについて対象になるかどうかは、購入者が別のソフトウェアをインストールをしたいと思った場合に、ベンダーのコントロール下で行われるのか、そうでないのかというところで判断してください。 ※Android TVの取り扱いについては、評価ガイドにも追記します。
サードパーティーのアプリケーションの管理もベンダが行うという話だが、Android TVでは中身がよく分からないアプリケーションを入れないといけない場合がある。その場合はどのように対応すればいいのでしょうか。	Android TVは基本的にAndroid OSを使っているはずなので、OSの管理という意味であるならばOSディストリビューションとしてのアップデートの仕方を整理しておいてください。 Android OSからも管理されていないサードパーティーのアプリケーションについては、ベンダーが管理を行うか、ベンダーが管理を行わない責任分界点外とするかを明確にしてください。なお、責任分界点外とする場合、利用者が容易に確認できる場所に「利用者自身が安全性を確認する必要があります。」等、ベンダーとしてどこまで確認・管理しており、どこから先が利用者の責任になるのかといった責任分界点及び利用者が行うべき行為等の注意喚起を明示することが必要であることに留意してください。
Windows IoT Enterpiseなど組込OSを組み込んだIoT機器は適合ラベルの対象になるでしょうか。また、自社以外が開発したソフトウェア（ウイルス対策ソフトなど）を顧客が組込OSにインストールできる製品の場合、適合ラベルの対象外になるでしょうか。また、例えば、顧客がドライバー（USBのドライバーなど）をインストールできる場合はどうでしょうか。	自社以外のソフトウェアを利用者が自らの意志でインストールできるのであれば対象外となります。対象になるかならないかの判断基準は汎用のOSかどうかということではなくて、あくまで利用者が自らの意思で他者のものを導入できるかどうかになります。
IP通信以外、例えばUSB通信やbluetooth通信などによるデータ送受信機能を持つ機器も★1認証の対象になるでしょうか。例えば、最初はbluetoothで通信するが、途中からインターネットにつながる可能性のある場合にどうなるか教えてください。	基本的にはインターネット側からダイレクトに侵入される可能性があるかどうかという観点で判断してください。 例えば、自らの機器の内部でIPとbluetoothの変換を行うのだとすれば、当該機器は当然IPの口を持っているということになるので対象です。また、途中の別の機器でIPとbluetoothの変換が行われ、当該機器自身はbluetoothしか使わないが、つないだ機器の先でIPでインターネット側につないでいることを想定した質問であるならば、自分のbluetootがそのつながった機器を経由してインターネット側から攻撃される可能性があるかどうかで判断します。

IP以外、例えばUDPマルチキャストでゲートウェイを通過する通信プロトコルは★1対象外でしょうか。	★1では、基本的にプロトコルに関して言及しているところはありません。通信プロトコルがIPをベースにしているかどうかで判断ください。
制御向けIoTいわゆるインダストリアルIoTにつきましても、今回は評価対象とされる認識で相違ありませんでしょうか。例えば、制御システムの場合、一般ユーザはおりませんので、例外申請の対象になるものと考えております。	インターネットに間接的にでもつながる可能性がある場合には対象の範囲に含めますので、それに該当する制御系IoTに関しても対象になり得ると思ってください。一方で、各評価項目の評価結果、あるいは評価の判断について、一般的なIoT機器とは異なるということは考えられます。
2025年3月から受付が開始する★1対象製品は、「幅広いIoT機器」という認識でよかったでしょうか。	その通りです。★1に該当する製品であれば、全て受付の対象となります。
IoT機器は海外製品も多いと思うが、海外ベンダへの本制度の周知や取得見込みはあるのでしょうか。	申請に関しては日本語対応、特にサポートは日本語で提供していただくことになります。海外ベンダーの日本法人は大丈夫だと思いますが、そうでない場合は輸入代理店などが代行する必要があるかもしれません。 なお、海外ベンダーに対して、ホームページとして英語版を提供しますが、説明会は特に予定していません。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

適合ラベルについての質問	
適合ラベルをIoT機器、マニュアル以外に、当該IoT機器を操作するためのスマホアプリに表示することをしてもよいですか。不特定多数向け媒体（製品カタログや製品ホームページなど）に掲載して問題ないでしょうか。	適合ラベル自体の表示の場所は任意ですので、スマホアプリに表示するということも可能です。適合ラベルの使い方ガイドを出す予定であり、その使い方に違反しない限りは、ベンダーの判断で利用していただいて問題ありません。
製品に貼付する適合ラベル（のステッカー／シール）はIPAに発行していただく形になりますでしょうか、それとも自社で印刷して貼付する形になりますでしょうか。	IPAからは適合ラベルのファイルを送付しますので、自社の方で対応してください。
ラベル自体の値段は1枚当たりいくらですか。	ラベル自体は無料で使えます。ラベルは電子データで送付しますので、ラベルをどう作るかは各社にお任せします。
jpeg等画像、adobe illustrator、または選択できるのでしょうか。	ラベルにつきましてはPDFを想定していますが、そのほかJPEG、PNGを想定しています。Adobe illustratorに関しては、必要があるかどうか含めて、現在内部で検討中です。
ラベルの有効期間は、申請日または付与日から2年でしょうか。	ラベルの発行決裁日から２年になります。発行決裁日からラベル付与までは１週間程度を想定しておりますので、実質的にはラベル付与から約２年とご理解いただければと思います。
有効期限数か月前に有効期限切れの案内(予定)はございますか。	今後の検討とさせてください。
jpeg等画像、Adobe Illustratorが選択できるのでしょうか。紙系の原稿を作ることを想定すると、必ずaiファイルも提供していただけるようお願いします。	ラベルにつきましてはPDFを基本として想定しています。そのほか、JPEG、PNGを想定しています。Adobe Illustratorに関しては、現在内部で検討中です。
自社が本制度認証済み製品を導入後に、更新されず2年後に確認すると無効となっていた場合、調達側としてできることはないのでしょうか（失効していることをIPAから通知してもらい更新を促す等）	調達側に対しては、ホームページやベンダーに確認してくださいということになります。IPAは利用者情報を管理していないので、そういう形になります。

よくある質問のA-4について、セキュリティ機能の条件が変わらない場合「ラベル取得製品のセキュリティ機能を使っていると表示可能」ということですが、変わらないと判断できる基準、誤認されないための表示方法についてはガイドラインなど展開されますか。	表示できるのは、セキュリティ機能に一切手を入れていないことが条件となります。例えば製品Yの取扱説明書の中に、製品Xというものを使っていますというような表現にしてください。 誤認されないとは、製品Xのラベルに書かれている内容が製品Yのもののように見えてしまう使い方はしないということを意味します。例えば、製品Yに製品Xのラベルを貼らないということです。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

取得インセンティブについての質問	
取得しない場合は、ペナルティなどどのような問題がありますか。	任意制度であり、調達者がどう判断するかというところにかかっていますので、制度としては別にペナルティなどはありません。
重要インフラに対して機器やソフトの登録を促すといったニュースが出ていますが、本制度のラベルが活用されるなどの計画ありますでしょうか。例えば、うまく活用されれば、ベンダとしては、別途SBOMなどを自前で準備する必要はなくなる可能性はあるでしょうか。	★１に関してはないと思ってください。SBOMなどの情報提供を求めませんし、適合基準の中にも入ってません。 ただし、★3以上は政府機関、重要インフラ機関が使うという前提に立っていますので、場合によっては適合基準の中にSBOMの情報を提出させる、もしくは記入させることが入ってくる可能性はあります。その場合、適合ラベルによって当該機器のSBOMデータの代用となる可能性はあります。
購入者、企業を対象に、本制度についてのメリットを説明される計画はありますでしょうか。	利用者に関するプロモーション等については、今後、経済産業省も含めて考えていきたいと思っています。明確な計画は現状ありませんが、重要なことだ認識しています。
本制度は将来義務化されますか。	現時点で、将来義務化するかどうかは決まっていません。なお、政府調達等に関しましては、本制度でのラベル取得製品が一定程度広がり、ラベル取得製品が調達できる状況になってくれば、徐々に義務化という形を取っていくことも視野に入れて検討をしています。
医療機器については2024年度以降、JIS T 81001-5-1の準拠が必要となっておりますが、本制度についても、今後対応が必要となるのでしょうか。	医療機器等に限らず、JC-STARの対象製品の中で、別の法的規制やガイドライン等で何らかの制限を受けているようなものがJC-STARとどういう関係にあるのかというのは、それぞれの調達者、監督官庁等を含めての判断に委ねられますので、関係部局にご確認いただいて判断いただければと思います。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

評価方法などについての質問	
IoT機器としては適合しているが、必須付随サービスが適合していない場合はどのような評価になるでしょうか。	必須付随サービスが加わったことによってチェックリストの判断結果が変わると判断されれば、当然不適合になります。
「通信機器で★3や★4が取れている場合、そこにつながる機器も運用としては適合となる」ということにはならないという理解でよろしいですか。	その通り、適合ということにはなりません。
対象製品に必須付随サービスが存在するが、そのサービスがIP以外の通信を行う場合、どう扱えば良いですか。	IoT機器と必須付随サービスとの通信の部分についてIPかどうかということは言及していません。チェックリストでは、必須付随サービスとIoT機器とセットで使うことに伴ってどのような影響を受けるかをベンダーが評価してください。
IoT製品に技適マーク取得済みモジュールを搭載する場合、エビデンスとして必要な資料はモジュールの認証書のみで問題ないでしょうか。それとも技適マーク認証時のレポートが必要でしょうか。認証時のレポートは、モジュールメーカーに提供を断られることが多く、入手困難である場合が多いです。	モジュールを自社が作っているわけではないとの前提での回答となりますが、この場合のモジュールは「コンポーネント」に相当するものになります。そのコンポーネントをそのまま使っているとの前提において、当該コンポーネントの管理はそのコンポーネント製造会社の責任になりますので、当該モジュールの認証書をエビデンスとすることで問題ありません。
ルータでインターネットから区切られた家の中のローカルネットワークに接続されたIoT機器であっても、同じネットワークに正規のデバイスとして接続されたスマホやPCのソフトウェアから攻撃や盗聴などを受けることが考えられます。結果的にスマホやPCがインターネットからの間接的な攻撃の踏み台になるようなルートの攻撃に関しては対象外と考えるのでしょうか。あるいは★1では対象外であるが、★2からは個別に検討するべき内容という整理でしょうか。	スマホやPCがインターネットからの間接的な攻撃の踏み台になるようなルートの攻撃に関して無条件に対象外としているわけではなく、「（そういった攻撃を受けないように）安全なネットワーク（例えば家の中のローカルネットワークなど）を確保したうえで、そのネットワークにつないでください」という注釈や注意喚起を行うことを条件として、必要な技術的対策の代替とすることを★1では認めることにしているということになります。もちろん、技術的にスマホやPCが踏み台になるようなルートの攻撃に対しても技術的な対策をすべきということも考えられ、もっと強いレベルの要件を★2以上、あるいは★3以上で採用するということは十分にあり得ます。

S1.1−11について、暗号化すればいいように読めますが、暗号鍵はセキュアストレージに保管しなくても要件を満たすと考えて良いですか。	暗号鍵については当然ながらセキュアに保存する必要があります。 ただし、★1においては、セキュアストレージ保存までの強い制限は設けていません。OS、サンドボックス、セキュアチップ等々、容易に取り出せないようにある程度きちんと管理されたところに暗号鍵があるという状態であれば、基本的には要件を満たしていると判断できます。
★１適合基準S1.1-02について質問です。 デフォルトパスワードが無く、初回起動時にユーザによるパスワード設定が必須である場合、評価項目2よりも優れた実装ですが、評価基準に合致しません。一方、「対象外となるための条件」は「ネットワークを介したパスワードやパスコードを利用したユーザ認証の仕組みがない」となっているため、対象外となるための条件も満たしません。 基準には「IoT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」との但し書きがあるため、S1.1-02の対象外とすべきでしょうか。	対象外にはなりません。デフォルトパスワードを利用しないネットワークを介したユーザ認証の仕組みの場合、デフォルトパスワードは「空欄（＝0文字）」とみなして扱ってください。 ※「★1評価ガイド」の補足説明も参考にしてください。
S1.1-16のアップデートの目的、影響などの要件ですが、これらが公開できるのは販売後になると思います。方針を書いた文書の準備で良いでしょうか。	評価項目①③④⑤については、事前に媒体で明示してください。 評価項目②のセキュリティアップデートリリースの条件については、周知のための仕組みや実施方法について記載してください。ここではそういった仕組みがあるということを評価いたしますので、その方針あるいは体制、仕組みを用意しておいてくださいということです。
技術文書の具体的な記載レベルが知りたいのですが、今後、提出する技術文書についてサンプルや記載方法の公開などはありますでしょうか。	技術文書に関してはIPAに提出していただきませんので、現時点において記載レベルの指定をしてございません。ベンダー各社それぞれの部門において記載内容の範囲を判断して、記載してください。ただし、サーベイランス時に説明を求めますので、その際にきちんと説明・回答できるようなレベルで証跡や根拠といったものを記載しておいていただきたいと考えています。 なお、将来的にはレベル感を合わせた方がいいということも考えられますので、そうなった時には、ヨーロッパなどの認証で採用しているIXIT報告書のような技術文書フォーマットを用意することも検討したいと考えています。

S1.1-06について、最新ファームウェアバージョンの確認方法ですが、取説などに確認先のURLを明記することでも大丈夫でしょうか。	最新ファームウェアバージョンの情報提供だけでは基準を満たしません。S1.1-06で求めていることは、IoT機器に最新のファームウェアバージョンが適用されているかどうかを確認するための方法です。 例えば、IoT機器に適用されているファームウェアバージョンを確認するためのURLを明記することでもよいかという意味であればOKになる可能性がありますが、最新バージョンがこれですという情報提供だけでは不十分です。そこは明確に分けて考えていただく必要があります。
S1.1-01：パスワード認証に関して、GUI経由のものを想定でよいでしょうか。プロトコル上での認証も対象でしょうか。	基本的にはパスワードを使う認証のことを指していると考えてください。必ずしもGUI経由ではない可能性もありますので、それぞれに応じて判断をいただくという形になります。
エビデンスは、設計書だけでは不十分でしょうか。検証（テスト）記録が必要になりますか。	通常は設計書だけでは根拠として不十分だと思われます。なぜそういう設計にしたのか、どのようにそれでOKだと判断したのかという根拠がいりますので、それを説明する技術文書として用意ください。 当然、実機テストに関してはそのテスト結果がはいりますので、それについても保存しておいてくださいということになります。
S1.1-03のトークンの変更とは、ユーザによる変更が必須になりますか。一般的には、有効期限が設けられており、自動で更新＝ユーザ操作で変更するものではないとの認識です。	トークンを含めて適切な変更ができればOKです。
「セキュアな保存」に暗号化の方法で三種類ぐらい記載がされていますが、これを満たさないと要件を満たせないのか、それとも対象外（NA）があってそれを満たしていれば非該当であるということを主張できますか。	「評価項目1～5のいずれかに類する」ですので、全部を満たしている必要はありません。「セキュアな保存」には、機密性の保護なのか完全性の保護なのかに応じて、必要な対策が取られているかという判断になります。 なお、守るべき情報資産をセキュアに保存することが前提なので、守られるべき情報資産がないという状態はあり得ないため、対象外（NA）はありません。 ただし、保護しなければならない情報に対してどのような対策を行うかについては選択の余地があります。

「機器が収集し、保存又は通信する、一般的に機密性が高い情報」に当たるデータをストレージに保存するということを一般的にやるわけですが、最初の三つのいずれかの暗号化技術を使って保存していないと適合しないという考え方でしょうか。 必ず暗号化して保存しなくてはならないのでしょうか。	インターネットから呼び出せる情報であれば暗号化をして保存しておいてください。「保存できる」という意味はデフォルト暗号化になっているということです。つまり、意図的にユーザーがオフにするといったところまでベンダーが責任を負うことはありませんが、設定としてはデフォルトオンにしておいてください。
JC-STARのチェックリストに対して実際に基準に準拠してるかどうかを迷う局面があるのではないかと思いますが、相談先はIPAでよろしいですか。また、評価機関、検証事業者向けに説明会がありますか。	基本的には★1、★2のチェックリストに関して言えば、評価ガイドをまず見てください。また、よくある質問や解説なども出す予定ですので、それらを見て判断していただくことを想定しています。自ら評価することが難しければ、JC-STARの評価機関・検証事業者にコンサルティングをお願いをするというのも一つのやり方としてあるかと思います。 なお、JC-STARの評価機関・検証事業者向けの説明会を実施するかどうかは今後検討します。
S1.1-12 IoT機器は宅内にあり、宅外のスマホがクラウドサーバで認証する場合（IoT機器はこの通信に関与しない)、スマホとクラウドサーバ間の通信路は対象外と扱えますか。	※回答内容を変更する可能性があります。後程、別途回答を記載します。 （説明会での回答：あくまでIoT機器との関係となりますので対象外になります。逆に言うとIoT機器とクラウドサーバーが何らかの通信が発生してれば、その部分が対象になるとご理解ください。）
必須付随サービスを含みたい場合、必須付随サービスそのものの評価も必要でしょうか。他社サービスの場合評価が難しい場合が考えられます。 また付随サービス間の通信についても評価対象でしょうか。	※回答内容を変更する可能性があります。後程、別途回答を記載します。 （説明会での回答：★１では必須付随サービスそのものの評価は必要ありませんが、ラベルを取る上では、必須付随サービス部分を含め、一義的に申請会社が責任を持っているという形を取らせていただきます。したがって、ラベルを取る上で必須付随サービスを含んだ形で全体のチェックをしていただきます。例えば、IoT機器と必須付随サービス間の通信は保護されなければならない範囲内に入っています。 なお、必須付随サービスの提供会社が他社の場合、自らチェックを実施するか、責任分解点についてあらかじめ協議・契約等で明確化しておいてください。申請会社と必須付随サービスの提供会社との間がどういう関係であるかという具体的なところには立ち入りませんので、両社で協議の上、決定いただければと思います。）

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

ファームウェアについての質問	
ファームウェアが同じバージョン単位での申請ができるとのことだが、同じファームウェアを使用している製品であれば、製品カテゴリが異なる場合でも申請は認められますか。	同じバージョンのファームウェアであれば申請は可能です。 ただし、製品のライフサイクルや販売周期などが異なる製品群をまとめてしまうと、製品の販売状況等によって適合ラベル（の登録番号）が変わるといったことが発生しうるので、あまり製品区分が違うのはまとめない方がよいかもしれません。ただし、そこはあくまでビジネス的な問題として判断していただくという形になります。
IoT製品の中に複数のセキュリティ機能を担っているファームウェアを利用している場合、どのように記載すればよろしいでしょうか。	該当するファームウェア名及びバージョン名をすべて併記してください。
ファームウェアのバージョンは、通常のファームウェアのバージョンとは別にJC-STAR用のバージョンを新たに設けて管理しても良いという理解で正しいでしょうか。	別につけていただいても構いません。ただし、そのバージョンを公開しますので、新たにJC-STAR用のバージョンとして設けるのであれば、JC-STAR用のバージョンも利用者が認識・確認できるようにしていただく必要があります。ですので、そこその点を考慮して、そのバージョンでどのように扱うのかで判断いただければと思います。
発売前に申請を行う場合、市場に提供するファームウェアバージョンは確定せず、開発時のバージョンで申請作業を行うこととなります。 ・ファームウェアバージョンを申請後に変更することは可能でしょうか。 ・もしくは、記載するバージョンは見込みのバージョンの記載が許容されますでしょうか。	ファームウェアは申請後に変更することが可能です。別途変更手続きを用意しますので、必要な届出を行ってください。また、申請段階では出荷時で利用することを想定したバージョン名を記入してください。見込みのバージョン名の記載など、管理しやすい方法で構いません。 手続きをしていただければ、ラベル自体は有効期間内であれば変わりません。そのまま利用できます。
１つ製品型番に対し下記の状況の場合、それぞれ製造ベンダー毎、製造毎に申請が必要ですか。もしくは、１申請に纏めることができますか。 1. 複数のOEM/ODMで製造 2. 複数の国に工場があり、COOがロットによってことなる	同じ型番でも、複数のOEM/ODM製造をしている場合にはODM/OEM先は全て列挙していただきます。申請としてはまとめることができますが、企業名としては列挙していただくことになります。また、複数の工場があって、製造国が複数の国にまたがっている場合は、製造国・地域の欄に列挙していただければ結構です。 ファームウェアの部分が同じであれば申請してまとめることは可能です。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

アップデート／脆弱性対応についての質問	
製品不具合・脆弱性対応のためのセキュリティアップデートの提供が放置されないようにするとあるが、本制度で要求される無償サポートの対象範囲はセキュリティ問題に関する不具合に対するものか、もしくはセキュリティ問題に関係しない機能的不具合も含まれるのでしょうか。	セキュリティ機能を提供するファームウェアに対する不具合・脆弱性対応を求めるもので、基本的には当該ファームウェアに関しての部分のアップデートをサポート対象としています。セキュリティに関係しない、あるいはそのファームウェアに関係しないアップデートは、提供義務の中に含まれないと理解ください。
ファームウェアのバージョンで、更新した場合、申請が必要な場合と必要ではない場合があるようですが、セキュリティに関係ないファームウェアのバージョンアップであれば申請は不要で、関係するものは申請が必要ということですか。その申請はどのようにすればよいでしょうか。また、申請料はかかりますか。 例えば、適合ラベル発行後、セキュリティとは関係のないマイナーバグ修正によるファームウェアアップデートが有効期間内に発生した場合も再申請が必要になるでしょうか。ラベルとファームウェアバージョンが紐付けられていることが気になりました。	申請段階で、今回のチェックリストを作る上で必要なセキュリティ機能（つまり、チェックリストに影響を及ぼす範囲）を含んでいるファームウェアの名称・バージョンを申請書に記入いただきます。この情報は製品情報提供ページにて公開されます。ユーザが、脆弱性がないファームウェアであるかどうかをこの番号で確認することとなります。 したがって、ファームウェアを更新した時に変更手続きがいるかどうかは、製品情報提供ページでの記載内容、特に「脆弱性対策済バージョン名」の情報に変更がいるかどうかに依存します。情報の更新がいる場合には変更届出を行ってください（新規申請ではありません）。なお、変更手数料はかかりません。 なお、申請時に書かれているファームウェア以外については、セキュリティに関係がないのであれば、変更手続きは必要ありません。
チェックリストの項目の判定に影響がない前提で、ファームウェアのバージョンが上がったら申請をし直す必要がありますか。また、新たな脆弱性が見つかり、対策を講じたバージョンを出す場合でも申請が必要ですか。その場合、都度申請費用がかかるとすればいくらになりますか。	チェックリストの項目の判定に影響がないのであれば、申請をし直す必要はありません。製品情報を更新しますので、バージョンが上がったことを通知ください。その際に費用は掛かりません。

セキュリティアップデートのサポートを途中でやめることはできますか。	脆弱性に対するアップデートについて、基本的にはラベルの有効期間内は無償を原則としてサポートをお願いしますということにしています。ラベルの有効期間が終了したら、その後のサポートは求めません。 なお、有効期間の途中でサポートをやめるといった場合、申請により（「有効期間切れ」ではなく）「自主取り下げ」になります。あらかじめ二年はサポートしない、例えば一年後に終了するというのがわかっているが延長するという場合には、一年間の延長など、サポート終了日までの期間を決めた申請もできます。
IoT機器にベンダが開発していないサードパーティーのアプリケーションがあって、独自にアップデートが可能である場合、ベースのファームウェアのバージョンもそれに応じて更新する必要がありますか。	基本的にIoT機器はベンダが管理しているという前提としていますので、ベンダが管理していないサードパーティーのアプリケーションを入れているという想定はあまりしていません。もしサードパーティーのアプリケーションが入っていたとして、それがセキュリティのファームウェアに影響を与えるのであれば、当然ながらベンダの責任としてそのアプリケーションとファームウェアの両方を管理してください。
IoT機器で使うハードウェアの交換が発生した場合、そのファームウェアなどのコンポーネントが変わらない場合であれば変更申請で対応すればよろしいでしょうか。	本制度で管理する単位は基本的にファームウェアの部分です。したがって、ベースのハードウェアが変わってもファームウェアが変わらなければ、特に手続きは必要ありません。ただし、ベースのハードウェアが変わったことによって、ファームウェアは同じでもセキュリティ評価に影響が出るようなことがもしあれば、別途、ご相談ください。
常時ネットワークに接続しない製品の場合、保守用I/Fによるアップデートでも問題ないですか。	保守用インタフェースを使ったアップデートでも問題はありません。ただし、そうすることがきちんと保守の仕方として明記されている文書を作っておいてください。その文書について証跡と見なします。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

サーベイランスなどについての質問	
適合ラベルの偽造とかの話が出てくるのではないかと思うが、それに対する対策は考えていますか。	検討課題として認識しています。 正規に発行していないラベルが偽造されているケースについて、例えば通報があったりすれば、当然調査し、偽造が確認されれば、当然ホームページで注意喚起を行います。また、正規に発行されているラベルを別の人が勝手に使ったケースについても何らかの対策は必要ではないかとの認識はしているというところですので、引き続き検討させていただきたいと思います。
例外的なパターンとして、例えば、会社がいきなり廃棄をしてしまうような場合だと担当者も何も連絡もできないこともあり得る。例えば定期的にメールを送って連絡先が有効かどうかの確認はしますか。	今のところは、まだそこまでは考えていません。ただ、なにか一般からの連絡等があれば、当然IPAとしても適宜確認を行い、必要があれば適合ラベルの取消しなども含めて対応するという形にしています。
適当なもので一つ適合ラベルを取得して別の機種にも貼付するみたいな不正をする企業も出そうな気がします。	少なくともそういう情報が発覚すれば、失効などの適切な対応は当然行います。悪質な場合は、別途公表などを行います。
JC-STARの不適合申請に対する行政処分としてはラベルの取り消しのみでしょうか。悪意の有無に関わらず、取り消し事由に該当する製品を一定期間内に相当数出したなどの理由で、当該ベンダーに対して、一定期間本ラベルの申請拒否などはありえますか。 また、評価委託先が上記同様に不適合を多数見逃しているという状況になった場合、委託先について各規程による登録の取り消しがありえる、という点をもって評価者の信頼性を担保するという認識でよろしいですか。	不適合申請の場合は申請が却下されるだけで、特段のペナルティはありません。また、有効期間切れや自主取下げは失効扱いであり、取消し事由には該当しません。 一方、取消し事由に該当するのは、基本的にはセキュリティ確保のための義務を果たさない、悪意がある若しくは悪質であると判断された場合とご理解ください。その場合、一定期間ラベル申請ができなくなるなどのペナルティはありえます。 また、評価委託先の信頼性確保について、JC-STAR評価機関についてはNITEによる認定審査を定期的に受監していただきます。JC-STAR検証事業者については教育訓練実績や要員資格実績などの確認が定期的に行われます。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

今後の予定についての質問	
スケジュールでは2025年から★２以上の受付開始予定とあるが、この時点で★3、★4の受付もスタートする、ないしその認証要件の内容などが公開されると思ってよろしいでしょうか。	★2以上になると分野ごとに区分が作られます。そのため、一気に様々な製品の★2以上の適合基準ができるということはないと思ってください。 現時点では、ネットワークカメラとルータなどの通信機器に対する検討が進んでいます。また区分も★1から★2、★3、★4と順番にできるわけでもありません。どのレベルのものが必要かという要件に応じて決めますので、★1だけで十分だという領域であれば★1しかない基準がありますし、逆に政府機関で使うので★2を飛ばしていきなり★3ができるという場合もあります。実際、通信機器とネットワークカメラの検討では、特に政府系が使うことを想定しているので、★3、★4クラスの適合基準を想定して検討を始めています。
★2の適合基準として、通信機器、防犯関連機器、スマート家電等が例示として挙げられていますが、これら製品以外の適合基準についても計画されているのでしょうか、もしくは、リクエストすれば検討していただけるのでしょうか。	★３、★4に関しては、政策判断として要望がある製品分野から順次整備していきます。★２については、基本的には業界団体として必要であると判断し、かつその業界団体での合計シェアが一定規模になる企業の賛同がある場合に、当該業界団体から適合基準作成のリクエストがあれば、その必要性を含めて検討し、適合基準WGを立ち上げるかどうかを判断します。WGが立ち上がれば適合基準が作られます。
★１で取得した場合、同一の登録番号で★２～４に昇格できるのですか。それとも、登録番号は新たなものが発行されますか。	★１から★２～４に変わるとラベルそのもの（星のマークの数）が変わりますので、登録番号は変わります。なお、製品情報提供ページに、いわゆる後継機種もしくはラベルが変更になったことがわかるような情報を記載するところを作るつもりです。

11/28、12/2、12/6の説明会で出された質疑応答をまとめています。
なお、多数のご質問をいただいたため、同内容の質問・類似の質問はまとめています。また、質問の内容について、個別企業特有の情報などが含まれている場合には一般化又は削除しております。

相互承認についての質問	
先週EUサイバーレジリエント法が官報に公示されたと聞いております。現時点ではRED指令によるIoTセキュリティ強化条項が追加となり規格案が8月に発行されると聞いております。RED指令との相互承認も検討の余地に入っておりますでしょうか。	RED指令が対象というわけではありませんが、EUとは相互承認等に向けて、経済産業省とも基準検討にIPAとしても加わっているというところです。
EUのサイバーレジリエンス法(CRA)との相互認証制度は、将来の目標に入っているのでしょうか。 EUサイバーレジリエンス法その他デジタル製品において、CEマーク(自己認証）の取得が求められています。JC-STARTにおいて★１もしくは、★2を取得すればCEマーク(自己認証)と同等のレベルという認識であっていますでしょうか。	相互承認の考え方は二種類あります。一つは認証を取るのが日本であろうと相手国であろうとどちらも同じ効力を持った認証として扱われるケース（CC認証がこれに該当します）、もう一つはあくまで自国の認証は自国で行うが、相手国で取った認証と同等の検査は省略・簡略化するなどして認証取得手続きが簡素化されるケースです。 今回のJC-STARに関しては、現在、二国間協議を行っている段階ですので、CRAとの相互承認に関しても、どちらの形での相互承認になるかを含め、今後の協議次第となります。 また、現時点ではCEマークと同等レベルかどうかについて欧州との技術基準のすり合わせは行われてません。この点についても今後の協議次第となります。
Connectivity Standards AllianceのProduct Security Certification Programとシンガポール政府が相互承認協定を結んでいます。上記Product Security Certification ProgramとJC-STARも相互認証の対象となるでしょうか。	Product Security Certification ProgramとJC-STARがダイレクトに相互承認になるかどうかというと、おそらくならない可能性が高いと思われます。 現時点では少なくとも相互認証の検討対象にはなっていないとご理解いただければと思います。

各国での罰則や基準の強さが違うなかで、具体的にどのような相互承認になりそうでしょうか。	相互承認に関して具体的にどうなるかは今後の交渉、結果次第なのでわからないという前提でお話しします。 相互承認には、二つのやり方が考えられます。一つは、JC-STARで取ったラベルをその相互承認の相手国も無条件で受け入れ、相手国で取られているものをこちらも無条件で受け入れますというものです。例えばCC認証ではCCRAという相互承認アレンジメントという枠組みがあり、CC認証国のどこの国でCC認証を取ったとしてもCCRA加盟国は全部同じように扱わなければならないというルールがあります。それと同様の相互承認のやり方であり、必要があれば罰則なども含まれる可能性があります。 もう一つのやり方は、JC-STARでラベルを取るためにチェックした項目と、相手国がチェックしている項目で共通になっているものはどちらかで取っていればOKとみなし、差分のところだけをチェックして、別個にラベルを発行しますというスタイルです。基準が各国で微妙に違ってて、それぞれの国で特に要求したいレベルが若干違ったり、重視する項目が違ったりしますので、現時点では後者の形になる可能性の方が高いかと思います。
相互承認が実現する時期について、計画として何年後とか見通しがありますか。	現時点で決まったものはありません。ただ、シンガポールやイギリスは制度がすでにスタートしているので、基準を受け入れる受け入れないのすり合わせが中心となり、比較的早い段階で決まる可能性があります。 一方で、アメリカやEUに関しては、これから基準を作る議論などを一緒にやっていく形になるので時間がかかるかもしれません。