★3セキュリティ要件・適合基準案に対する意見公募手続きの結果について
別紙）★3セキュリティ要件・適合基準の提出意見に対する考え方

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
1	製品共通 通信機器 S3.1-05	カメラ S3.2-05	IoT製品において認証のために使用する電子証明書は、十分なセキュリティ強度を持つこと。IoT製品で使用する電子証明書は、更新可能とすること。	証明書の中でも、TPMやセキュアエレメントに格納された、例えば IEEE 802.1ARに準拠した証明書の場合、逆に更新と称して書き換え出来る事が問題となります。 ここで想定する「証明書」について、より厳密な定義が必要に思います。	たとえば、IEEE 802.1AR によるセキュアデバイスアイデンティティの標準では、いわゆる IDevID 証明書を製造時に製品へ書き込むことが求められています。 https://1.ieee802.org/security/802-1ar/ この証明書はあくまで初期のセキュア接続のためだけに用いられるべきもので、その後は使用されず、顧客側で導入する別の証明書へ置き換えられるべきものです。 IEEE 802.1AR の基準では、この証明書は「不変であるべき」、つまり削除できない形で保持されることが求められています。 ※なお、当社では、万が一、当社の証明書インフラ（PKI）が侵害された場合には、製品交換プロセスを通じて Axis Device ID を更新し、旧証明書を失効させることを可能としています。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
2	製品共通 通信機器 S3.1-10	カメラ S3.2-09	④自動アップデート機能を有すること	自動アップデートを必須化するのではなく、新しいファームウェアがリリースされたことを確実かつ迅速にユーザーへ通知する仕組みを設けることで、本来の目的を達成するという運用方針の方が、実際の CCTV システムに適した現実的なアプローチではないかと考えます。	ごちらの要件については、主に二つの懸念があります。 第一に、システムの互換性が損なわれることで、利用者が意図しないシステムダウンタイムが発生し得る点です。 一般的に、カメラを含む IoT 機器は単体で利用されることは少なく、クリティカルインフラや公共交通のような大規模システムでは、他の機器やサブシステムと密接に統合されて運用されています。ここで、自動アップデートを必須とした場合、個々のデバイスのサイバーセキュリティ上の安全性は向上したとしても、アップデート内容によっては他のコンポーネントとの互換性が損なわれ、結果としてシステムが機能不全に陥る危険性があります。 また、互換性に問題がなかったとしても、アップデート完了時には再起動が必要となりますので、その過程で、ライブ映像および録画に予定外・予期しない中断も生じます。 このような背景から、CCTV の運用現場では、自動アップデートを必須とする要件は、これまで広く受け入れられてきませんでした。 システムの互換性を保ち、ライブ映像および録画に予定外・予期しない中断を生じることを避けるためには、アップデート後もシステムの互換性が維持できることを確認したうえで、人間が計画的にアップデートを手作業で実施できることが重要と考えます。 第二に、オフラインまたはクローズド環境でデバイスを運用するユーザーも多く存在することを考慮する必要があります。自動アップデート機能を実装するためには、ネットワークカメラが単体でインターネットにアクセスしメーカーサイトへログインして更新を確認できるようにするか、あるいはインターネット接続可能なゲートウェイ側で更新確認を行い、意図的に外部接続を遮断しているデバイスへ更新を適用する、といった方式が必要になります。しかし、セキュリティポリシーの観点から前者を許容しないユーザーも存在し、製造業などではそもそもオフライン環境での運用が前提となるケースもあります。 当社は、これまで、BIS IT-Security Label、EN 303 645、シンガポール CLS Level 4 の認証を受けており、そこでも自動アップデート要件が規定されていましたが、上記のユースケースを説明した結果、自動アップデート要件は、適用除外とされてきました。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 自動アップデートの機能を有すること。あるいは、アップデートが実施されていないことの警告を自動表示する機能を有すること。 <補足説明> 自動アップデート機能を初期状態で有効にすることは求めない。
3	製品共通 通信機器 S3.1-12	カメラ S3.2-11	③アンチロールバックの機能を有すること。 「ただし、本適合要件は、必要に応じて過去のバージョンのソフトウェアをインストールする手段を有することを妨げないが、デフォルトで過去のバージョンの更新ソフトウェアでアップデート可能としてはならない」	デバイスのユースケースを考えたときに、どのバージョンを製品に使用するかは、デバイスを管理するユーザーの判断にゆだね、製品側が特定のバージョンを厳密に強制しない方が好ましいと思います	理由は、S3.2-9と類似しますが、大規模システムなどではシステム統合が必須となるなかで、互換性を保つためには、出荷時搭載のバージョンから、少し前バージョンではあってもシステムとの互換性を保てる長期サポートバージョン(長期的にセキュリティパッチなどが提供されるバージョン)が採用されるケースもあります。 デバイスにおけるソフトウェアアップデートの開始時にユーザーが認証を行い、管理者権限を持っている場合にのみ実行できることや、真正性・完全性を精査することを大前提として、その上で旧バージョン・同一バージョン・新バージョンのいずれのソフトウェアであっても受け入れ可能とすることが好ましいです。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 更新ソフトウェアでアップデートする前に、更新ソフトウェアのバージョンを確認し、現在のバージョンと同じまたは以前のバージョンであることが確認されてた場合にはアップデートが中止されること。 ただし、本適合要件は、必要に応じて過去のバージョンのソフトウェアをインストールする手段を有することを妨げないが、デフォルトで過去のバージョンの更新ソフトウェアでアップデート可能としてはならない。
4	製品共通 通信機器 S3.1-22	カメラ S3.2-21	無線LAN機能をもつIoT製品は、無線通信区間において適切な方式による通信の暗号化、及びIEEE 802.1Xによる機器認証を行う機能を有すること。	有線接続時についても言及したほうが良いように思います。	IEEE 802.1Xは、無線LANに限らず有線LANでも要件として必要と考えます	まず前提としまして無線、有線を問わず、S3.1-01（通信機器）、S3.2-01（ネットワークカメラ）において認証を求めております。接続方式が無線接続の場合は、盗聴による危険性が大きいことを考慮し、本セキュリティ要件において、無線通信区間の802.1XによるL2レイヤでの認証を求めております。
5	製品共通	カメラ S3.2-42 通信機器 S3.1-44	ユーザに提供する製品のセキュリティに関する情報は、指定され た言語でなければならない。	現時点では「指定された言語」との記載のみで、言語が明記されていません。こちらは最終版までに明記されますでしょうか。	なお、日本においても英語を基本とするユーザーが多数存在しますので、言語に関しては英語もご考慮いただければと思います。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
6	製品共通	カメラ S3.2-45 通信機器 S3.1-47	筐体（エンクロージャ）に対する物理的な破壊・改変行為によって、機器内のコンポーネントやインタフェースへ不正にアクセスされることを防ぐために、筐体の耐タンパー性を向上させる仕組みを実装すること	物理的な手段に限らず、幅広い手段を考慮いただければと思います	一般的にIoTデバイスは、用途や設置場所に応じた大きさ・デザインが施されており、すべての製品に対してケーシング開放センサーなどの物理的なタンパープロテクションの実装を求めるのは現実的ではないように思います。 機密データの保護や運用上の機能維持に関しては、追加の物理的センサーや、筐体エンクロージャーのデザイン変更に限らず、他の手段も組み合わせた方法を総合的に提示いただければ幸いです。たとえば当社のネットワークデバイスを例に挙げますと、AI画像解析を用いて映像を妨げる要素が発生した時に検知する仕組みや、画像の改ざんを自動的に検知する機能により、製品に対する不正ないたずらを自動で検出できます。また、機密データは CC EAL6+/4+ や FIPS 140-3 Level 3 認証を受けた暗号化ハードウェアモジュール上に保存されるほか、Linux ファイルシステムおよび SD カードも暗号化されており、物理的な改ざんやデータ抜き取りの試みを防止しています。	物理的な攻撃対策として、どの程度の対策を取るかについては、具体的な基準を適合要件・評価ガイドにて検討いたします。
7	ネットワークカメラ	S3.2-45	セキュリティネジの適応範囲について	JC-STAR レベル3の要件番号 S3.2-45 では、「筐体（エンクロージャ）に対する物理的な破壊・改変行為によって、機器内のコンポーネントやインタフェースへ不正にアクセスされることを防ぐために、筐体の耐タンパー性を向上させる仕組みを実装すること」 と規定されています。 この要件に関連して、以下の点について確認させてください。 ①Bullet型ネットワークカメラにおける PAN/TILT/YAW 調整用のネジ についても、耐タンパー性を確保するためにセキュリティネジとする必要があるのでしょうか。 ②SDカードスロットやイニシャルスイッチ は機器内のインターフェースに該当すると認識していますが、この認識に誤りはないでしょうか。 ③飾りカバーなどについて、取り外しても機器内のコンポーネントやインターフェースへアクセスできないものであれば、手で容易に取り外し可能であっても適合と認識して問題ないでしょうか。 ④機器内のコンポーネントやインターフェースにRJ45コネクタやAudioジャック（IN・OUT）、MonitorOutジャック、外部端子（IN・OUT）、電源（12V/24V）は含まれますでしょうか？	適合要件の明確化のため	本項目では筐体内部への物理的なアクセスを保護、もしくは検知するための仕組みの実装を要求しております。そのため筐体保護に関わらないカバーやネジに関しては言及しておりません。また本項目では筐体内に保護すべきインタフェースに関して言及しておりません。（S3.2-24において、不必要な物理的インタフェースを露出から保護する仕組みを要求しております）
8	ネットワークカメラ	S3.2-01	※下記は★1 から削除した。ご意見を伺いたい。 E） 通信を許可する対象を IP アドレスなどで制限する機能の実装 F） 通信を許可する対象を LAN 内の機器のみに制限する機能の実装	通信経路の制限（E/F）は、ユーザーの本人確認（認証）の代替にはなり得ないので、削除するのが妥当である。ユーザー認証ではない。 ネットワークのアクセス制限（ファイアウォール機能など）を、認証機能の代わりにしてはならない。ネットワーク制限の有無に関わらず、必ずA~Dのような確実な本人確認機能を実装しなければならない。	内部脅威への脆弱性：もし攻撃者が何らかの方法（マルウェア感染したPCの乗っ取りなど）でLAN内に侵入した場合、F（LAN内制限）の実装だけでは、パスワードなしでカメラ映像が見放題になってしまいます。 　IP偽装のリスク: IPアドレスは偽装が可能です。E（IP制限）だけでは、高度な攻撃者に対して無防備になります。 　従来のセキュリティは「LANの内側は安全」と考える「境界型防御」が主流でしたが、現在は「ネットワークの内側も危険である」と前提するゼロトラスト（Zero Trust）の考え方が標準になりつつあります。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
9	通信機器	ガイダンス文書 p12	規定に合致する鍵長を用いた 暗号技術 ー	規定に合致する鍵長を用いた 暗号技術	ゴミあり	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
10	ネットワークカメラ	ガイダンス文書 p17	誤： 一般的に安全と認知されているブ VPN ロトコル	正： 一般的に安全と認知されているVPNプロトコル	内容： 「プロトコル」の中に「VPN」が混入しています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
11	ネットワークカメラ	ガイダンス文書 P3	誤： 警告を表示する機能を有することが、が明記されていること	正： 警告を表示する機能を有することが明記されていること	内容： 助詞「が」が重複しています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
12	ネットワークカメラ	ガイダンス文書 p23	誤： 手動でのアップデートをサポートしない倍は	正： 手動でのアップデートをサポートしない場合は	内容： 「場合」の誤変換と思われます。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
13	ネットワークカメラ	ガイダンス文書 p25	誤： バージョンであることが確認されてた場合には	正： バージョンであることが確認された場合には	内容： 不要な「て」が入っています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
14	ネットワークカメラ	ガイダンス文書 p26	誤： 更新ソフトウェアウェア	正： 更新ソフトウェア	内容： 「ウェア」が重複しています（2箇所）。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
15	ネットワークカメラ	ガイダンス文書 p46	誤： CRYPTREC で認められれない暗号技術	正： CRYPTREC で認められていない暗号技術	内容： 「て」が抜けています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
16	ネットワークカメラ	ガイダンス文書 p47	誤： キュリティに関連する情報	正： セキュリティに関連する情報	内容： 先頭の「セ」が脱落しています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
17	ネットワークカメラ	ガイダンス文書 p52	誤： インタフ エース	正： インタフェース	内容： 不自然な空白、または改行の不備が見られます	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
18	ネットワークカメラ	ガイダンス文書 p55	誤： 全てをを満たしている	正： 全てを満たしている	内容： 助詞「を」が重複しています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
19	ネットワークカメラ	ガイダンス文書 p65	誤： 「root」 ユーザではく	正： 「root」 ユーザではなく	内容： 「な」が抜けています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
20	ネットワークカメラ	ガイダンス文書 p69	誤： 静的アプリケーションセ キュリティテスト	正： 静的アプリケーションセキュリティテスト	内容： 単語の途中に不自然なスペースがあります。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
21	ネットワークカメラ	ガイダンス文書 P.88	誤： 一覧化されていること。**の リスト。**一覧には少なくとも	正： 一覧化されていること。一覧には少なくとも	内容： 「の リスト。」という断片的な文言が混入しており、文脈が切れています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
22	ネットワークカメラ	ガイダンス文書 p59,60,95	「デバッグ」と「デバック」(p59,60,95)の混在	デバッグに統一		いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
23	ネットワークカメラ	ガイダンス文書 p1	現状： パスワード利用した認証の仕組み	修正案： パスワードを利用した認証の仕組み	理由： 助詞があったほうが自然な日本語になります。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
24	ネットワークカメラ	ガイダンス文書 P.75	現状： 通信ケーブルや無線接続が切断し、再接続した後	修正案： 通信ケーブルや無線接続を切断し、再接続した後	由： 直後の （実機テスト項目）では「切断する」という能動的な操作になっています。文脈として意図的に切断テストを行う場面であれば「を」が適切です。自然故障を指すなら「が切断され」などが適切です。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
25	通信機器	ガイダンス文書 P3	誤： 警告を表示する機能を有することが、が明記されていること	正： 警告を表示する機能を有することが明記されていること	内容： 助詞「が」が重複しています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
26	通信機器	ガイダンス文書 p17	誤： 一般的に安全と認知されているブ VPN ロトコル	正： 一般的に安全と認知されているVPNプロトコル	内容： 「プロトコル」の中に「VPN」が混入し、文字順序が乱れています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
27	通信機器	ガイダンス文書 p27	誤： 更新ソフトウェアウェア	正： 更新ソフトウェア	内容： 「ウェア」が重複しています（2箇所）。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
28	通信機器	ガイダンス文書 p67	誤： ユーザではく	正： ユーザではなく	内容： 「な」が抜けています。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
29	通信機器	ガイダンス文書 p61,62,97	「デバッグ」と「デバック」の混在	一般的には「デバッグ」が推奨されます。		いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
30	通信機器	ガイダンス文書 複数箇所	「ハードコード」と「ハードコーディング」の混在	ハードコードされた または ハードコーディングされた		いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
31	通信機器	ガイダンス文書 p1	現状： パスワード利用した認証の仕組み	修正案： パスワードを利用した認証の仕組み	理由： 助詞があったほうが自然です。（同様の箇所が複数あります）	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
32	通信機器	ガイダンス文書 p22	現状： 自動アップデート機能を初期状態で有効にすることを求めない。	修正案： 自動アップデート機能を初期状態で有効にすることは求めない。	必須要件ではない（推奨や任意である）ことを示す場合、「～することは求めない」とするのが一般的です。「を」でも間違いではありませんが、ニュアンスとして「は」が適切です。	いただいたご意見を参考に、適合要件・評価ガイドを修正いたします。
33	ネットワークカメラ	S3.2-04	対象外（NA）となるための条件、基準の補足説明	・以下を追加いただきたい 【対象外（NA）となるための条件】 IoT製品において、認証のためにパスワードを使用していない	・他の要件番号(S3.2-03)では認証メカニズムとしてパスワード以外の認証方法（トークン、指紋等）を認めている。一方、総当たり攻撃の対策はパスワードに対するものと考えられるため。	いただいたご意見は、以下のようにセキュリティ要件に反映いたしました。 【対象外（NA）となるための条件】 IoT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 （「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アクセスが必要ない根拠を記載すること）
34	ネットワークカメラ	S3.2-08	★３適合基準	・脆弱性開示ポリシーは、IEC 29147 9条 Vulnerability disclosure policyとの整合を図ることを考慮いただきたい	・複数の海外セキュリティとの関係性が示されているが、ベースとなるIEC 29147との整合を図ることにより、他の規格との重複を避けられると考えられるため。	国際規格と、セキュリティ要件・適合要件・評価ガイドとの整合については、直接IoT機器に関わるものを対象としております。 脆弱性開示ポリシーが他の規格に整合することは求めてはおりません。JC-STARにおける脆弱性開示ポリシーの要件を満たす必要があります。
35	ネットワークカメラ	S3.2-22	★３適合基準	・以下に変更いただきたい。 「IoT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ーフェースについて、IoT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ーフェースを無効化すること。A)TCP/UDPポート B)Bluetooth C)USB」⇒「IoT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ーフェースについて、当該インターフェースが必要であることを明示し、適切なセキュリティ対策を講じた場合を除いて、インターフェースを無効化すること。A)TCP/UDPポート B)Bluetooth C)USB」	・変更前の文章では、IoT製品において利用上必要であったとしてもインターフェースを無効化しなければならないと読み取れる。攻撃のリスクが高いことは理解するものの、適切な理由と適切なセキュリティ対策が実施されていれば、必ずしも無効化する偏然性はないと考えるため。	「IoT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。」と記載しており、利用上必要なインターフェースについては無効化の対象から除外されることが明示されております。
36	製品共通	全体	全体	通信機器、ネットワークカメラのそれぞれについて、対象製品となる条件・機能を示していただきたい。	「通信機器」はルータ、「ネットワークカメラ」は監視用カメラが主ターゲットかと推察しますが、分野別の基準についてはその分野の定義が無いと、適切な妥当性判断は難しいと考えます。多様な製品に対して一意には定められないと思いますが、指標となる条件や機能(要素)などは、ある程度示していただきたいです。	「通信機器」、「ネットワークカメラ」それぞれにおける対象について、セキュリティ要件の文書に補足説明を追加いたしました。
37	製品共通	S3.1-17 S3.2-16 (要件4-2)	(★3適合基準より) ②すべての機密セキュリティパラメータは、物理的、電気的、又はソフトウェアなどの手段により改ざんに耐えられるように実装されていること。	「ソフトウェアなど」の表現により基準があいまいになる懸念があるため、もう少し具体的に示すべきだと考えます。	ガイダンス文書では例として暗号化や難読化が示されていますが、特に難読化はその程度も示されておらず、容易に解読できるものも含まれてしまうと推察されるため、本要件・基準の有効性が低下していると考えます。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
38	通信機器	S3.1-20 (要件5-1)	(★3適合基準より) ① IoT製品は守るべき情報資産の送信先の正当性を確認する。	ガイダンス文書やネットワークカメラでは「送信先」ではなく「通信先」となっているので表現を揃えた方が良いと考えます	文書での表現統一のため	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
39	製品共通	S3.1-42 S3.2-40 (要件14-6)	(★3適合基準より) (通信機器) IoT製品は収集や処理の範囲を限定する機能および不要になった個人情報を削除する機能を有すること。 (ネットワークカメラ) IoT製品は収集や処理の範囲を限定するために、不要になった個人情報を削除する機能を有すること。	適合基準の記載が、通信機器では「限定機能および削除機能」と2機能のAND条件になっているのに対し、ネットワークカメラでは「限定のための削除機能」と目的を明示した1機能となっています。 ガイダンス文書の説明内容では特に差異もなく、どちらも削除に関する機能の評価について示されていることから、もしこの差異に具体的な意図が無いのであれば、表現は揃えて良いのではと考えます。	(位置づけに差異が無い場合の)文書での表現統一のため	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
40	通信機器	S3.1-42	「★3適合基準」： IoT製品は収集や処理の範囲を限定する機能および不要になった個人情報を削除する機能を有すること。	通信機器「S3.1-42」は、ネットワークカメラ「S3.2-40」の「★3適合基準」と同様に「不要な個人情報を削除する機能」のみを求めるような記載にすべきではないか。 または、通信機器のみに「収集や処理の範囲を限定する機能」を求める場合は、どのような機能を想定しているのか掲載していただきたい。	通信機器「S3.1-42」とネットワークカメラ「S3.2-40」の「★3適合基準」に表現の差異がある。 通信機器の適合基準では、「不要な個人情報を削除する機能」とは別に「収集や処理の範囲を限定する機能」を求めれているように読み取れるが、ガイダンス文書には「不要となった情報の削除を行う機能」の記載のみである。	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
41	製品共通	ネットワークカメラ「S3.2-28] 通信機器「S3.1-29」	「セキュリティ要件：要件」： 6-9. 製造業者は、製品に展開されるソフトウェアについて、セキュアな開発プロセスに従わなくてはならない。	サードパーティ製コンポーネントについては、本要件の対象外に設定すべきではないか。	要件カテゴリ「6.露出した攻撃面を最小化する」に対し、サードパーティー製コンポーネントに対してはネットワークカメラ「S3.2-29」/通信機器「S3.1-30」が適用されるという認識である。 サードパーティ製コンポーネント(例：OSS)に対して、セキュアな開発プロセス(コーディング規約や実装原則などの規程、技術者教育等)を求めることは困難であるため、ネットワークカメラ「S3.2-28」/通信機器「S3.1-29」は対象外とすべきと考える。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
42	通信機器	S3.1.18	適合基準の記述 ①ソースコードにハードコードされている機密セキュリティパラメータの全容を把握し、一覧化できていること。	ドキュメント評価となっていますが、セキュリティパラメータの一覧の公開は不要という理解で正しいですか?	開示自体が脆弱性を生むため。	機密セキュリティパラメータ=SSP(Sensitive Security Parameter)の一覧については、公開は不要です。第三者評価の際には必要な情報ですので、情報提供の際は、評価機関との間でNDAを締結するなど、秘密が保持されるように対応してください。
43	通信機器	S3.1.29	要件の記述 6-9. 製造業者は、製品に展開されるソフトウェアについて、セキュアな 開発プロセスに従わなくてはならない。	レビュー後に、悪意を持ったコードが混入できないよう開発プロセスの管理を行い、レビュー時のコードが、そのまま製品ソースコードリポジトリへの反映されることを確認する仕組みがあった方が良いのではないでしょうか?	規則や原則を規定しただけでは、差し替えられる危険性が排除できていないように見えます。 「作成されたコードのレビュー・セキュリティテストを行う」とは、製品に適用する最終コードの意味であることを強調すれば良いのかもとも思います。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
44	通信機器	S3.1-07	★3適合基準 ①ユーザ認証において多要素認証を行う機能を有すること。	IoT製品単体で多要素認証（FIDOサーバー等）の機能を保持していなくとも、SAMLやOIDC (OpenID Connect) 等の標準プロトコルを用いて外部のIDプロバイダ（IdP）と連携し、結果として多要素認証を強制できる機能（SP/RP機能）を有している場合、本要件を満たすと解釈してよいか明確化をお願いします。 また、その解釈で相違ない場合、その旨を注釈等に追記することを要望します。	ルーター等のネットワーク機器においては、ハードウェアリソースの制約上、機器単体でFIDO認証等の多要素認証基盤を構築・運用することは困難な場合が多くあります。 実運用においては、機器側はSAML/OIDCクライアントとして振る舞い、多要素認証機能を備えた外部IdP（認証基盤）と連携することでセキュアな認証を実現する構成が一般的かつ現実的であると考えます。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
45	通信機器	S.3.1-08	★3適合基準 IoT製品は、接続する機器を識別し、無許可の機器の接続を拒否する機能を有すること。	「接続を拒否する」という基準について、対象範囲の明確化を要望します。 以下のどちら、もしくは両方を指しているのかについて明記して下さい。 ・IoT製品自体へのアクセス ・IoT製品を経由する通信	「IoT製品自体へのアクセス制御」と、「通信中継の制御」は、実装技術および運用目的が異なります。 対象範囲が不明確な場合、実装すべき機能に不足が生じたり、あるいは過剰な実装を求められたりする等の齟齬が発生する恐れがあるためです。	通信機器自体への管理接続を含めて、通信機器へ接続される機器を識別し、通信を拒否する機能を求めております。例えばインテリジェントL2スイッチにおけるMACアドレスフィルタリングが該当します。
46	通信機器	S.3.1-10	★3適合基準 ④自動アップデート機能を有すること。	「機能を有すること」の適合判定基準について明確化をお願いします。 具体的には、インターネットに接続されないクローズドネットワーク環境等での運用により、物理的に更新情報が取得できず当該機能が実質的に動作しない場合であっても、製品として当該機能が「実装」されていれば適合となる旨の追加を要望します。	IoT製品は、セキュリティポリシーや設置環境の制約により、外部ネットワークへ接続できない環境で運用されるケースが多々あります。 そのような環境下では、自動アップデート機能や更新確認による警告機能が実装されていても、通信不可により機能しません。そのため、環境要因によって動作しない場合でも、機能の実装自体が確認できれば適合と判断されるべきと考えるためです。	製品として当該機能が「実装」されていれば適合となります。該当箇所については、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 自動アップデートの機能を有すること。あるいは、アップデートが実施されていないことの警告を自動表示する機能を有すること。 <補足説明> 自動アップデート機能を初期状態で有効にすることは求めない。
47	通信機器	S3.1-12	★3適合基準 ③アンチロールバックの機能を有すること。	本基準について、保守運用上の必要性から管理者が意図的に行うロールバック操作については、例外として許容される旨を注釈等で明記することを要望します。 あるいは、「原則として中止されること。ただし、適切な権限を持つ利用者が明示的に承認した場合はこの限りではない」といった表現への変更を提案します。	新ファームウェア適用後に致命的な不具合が判明した場合、迅速に旧バージョンへ戻すことができないと、長期間にわたりシステムが停止するリスクがあるためです。 脆弱性の再発防止（アンチロールバック）と、障害復旧手段の確保は両立されるべきであり、利用者による強制適用手段が残されている必要があります。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 更新ソフトウェアでアップデートする前に、更新ソフトウェアのバージョンを確認し、現在のバージョンと同じまたは以前のバージョンであることが確認されてた場合にはアップデートが中止されること。 ただし、本適合要件は、必要に応じて過去のバージョンのソフトウェアをインストールする手段を有することを妨げないが、デフォルトで過去のバージョンの更新ソフトウェアでアップデート可能としてはならない。
48	通信機器	S3.1-25	★3適合基準 ②IoT機器のデバッグインタフェースを物理的または論理的に無効化していること。	「デバッグインタフェースを物理的または論理的に無効化」という基準について、出荷時の通常ファームウェアでは機能が無効化されているものの、故障解析時等にメーカーの正規の手順（正当な署名を持つメンテナンス用ファームウェアへの書き換えや、認証を経たAdd-onプログラムの適用等）によってデバッグインタフェースを有効化するなど、適切な処理による有効化は認める旨の追加することを要望します。	市場から回収した製品の不具合解析（RMA対応）において、デバッグインタフェースの利用は不可欠です。 一般利用者が利用できないよう適切に制限（無効化）されていれば、メーカーが保守目的で利用するための再有効化手段が残されていることは許容されるべきと考えるためです。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 【補足３：デバッグインタフェースの無効化の例】 ・製造業者のメンテナンスにおける一時的なデバックインタフェースの無効化の解除を妨げるものではない。
49	通信機器	S3.1-34	★3適合基準 IoT製品は、特定のタイミングの構成情報を正しく保持、復元できるバックアップ機能を有すること。	「保持、復元できる」の前提条件として、バックアップデータの取得時と復元時において、ソフトウェアのバージョンおよびハードウェア構成が同一である場合に限定されるという理解でよいか、明確化をお願いします。	ファームウェアの更新等により内部データ構造や設定パラメータが変更された場合、異なるバージョン間でバックアップデータを適用（リストア）すると、互換性の問題から正常に動作しない、あるいは設定の不整合が発生するリスクがあるためです。「直前の状態に復元」するためには、その動作環境も取得時と同一であることが技術的な前提となると考えます。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします
50	通信機器	S3.1-41	適合要件の追加	どのような情報が取得されるのかということとともに「いつ取得されるのか」をポリシーとして明示することが必要と考えます。	個人情報の収集種利用は、何時、何にのために、どのような情報を取得するのかが明示されていることが必要と考えます。基準案では収集したデータが何時取得されるのかが明示されない恐れがあります。	いただいたご意見を参考に、セキュリティ要件を修正いたしました。適合要件・評価ガイドについては別途、検討いたします。
51	通信機器	S3.1-43	★3適合基準 製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。	評価機関が実施するペネトレーションテストについて、具体的な検査項目、観点、および合否判定に用いる基準（参照するガイドラインや、検出された脆弱性の深刻度閾値など）を事前に公開することを強く要望します。 また、製造業者が評価申請前に自社で行うべき「事前テスト」の推奨項目があれば、あわせて明示してください。	OSやミドルウェア、サードパーティ製コンポーネントに起因する脆弱性は、製品の設計・選定段階で対策を講じる必要があります。 評価基準がブラックボックスのままであると、開発完了後の評価段階で根本的な問題（コンポーネントの選定ミス等）が発覚した場合に、修正が不可能あるいは大規模な手戻りが発生し、製品提供に重大な影響を及ぼすためです。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 評価項目１： ネットワークインタフェースにおいて解放されている全てのTCP/UDPポートへの診断を行い、公知の脆弱性が検出されないこと。 評価項目２： Webページのユーザインタフェースの診断を行い、ロジックや作りこみによるものを含む脆弱性が検出されないこと。 評価項目３： 物理的にアクセス可能なデバッグインタフェースがあった場合、デバッグ行為が行えないこと。なお、物理的にアクセス可能なデバッグインタフェースには「S3.1-47」の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。また、デバッグインタフェースの接続においては、製造業者の協力を得て実施する。 全ての実機テストの評価項目において、CVSS v3基本評価基準4.0以上の脆弱性、もしくはセキュリティ要件が不適合となる挙動が検証された項目をセキュリティ課題として、評価者は製造業者に、再現可能な形式（再現手順、画面キャプチャーなど）で報告し、是正を求めるものとする。 評価項目４： IoT機器からの不正な通信（通信先一覧以外への通信）が検出されないこと。 この評価は評価項目１，２を実施する際に常時通信をキャプチャすることにより実施する。
52	通信機器	S3.1-44	★3適合基準 ユーザに提供する製品のセキュリティに関する情報は、指定された言語でなければならない。	「指定された言語」の定義について、具体的な基準の明記をお願いします。 本制度が日本国内の制度であることを踏まえ、日本国内で販売される製品については「日本語」での記載が必須要件となるのか、あるいは、製品がターゲットユーザが理解可能であれば「英語」等の他言語での記載も適合と認められるのか、判断基準をご教示ください。	「指定された言語」という表現では、誰が指定するのかが不明確です。 グローバル製品において、日本語マニュアルやUIのローカライズが適合のための必須条件となるか否かは、開発コストおよび製品展開に大きく影響するため、明確な定義が必要です。	適合要件・評価ガイドの記載内容を検討いたします。
53	通信機器	S3.1-46	★3適合基準 IoT機器はサービス不能攻撃によるネットワーク過負荷状態から復元の仕組みを有すること。	サービス不能攻撃の試験条件について、「ネットワーク過負荷状態」の定義（負荷量や攻撃継続時間等）を、製造業者が技術文書等で定義している場合、その定義を試験条件として認める旨を追加することを要望します。	IoT製品は製品種別によってハードウェアリソースや熱設計が大きく異なり、一律の攻撃継続時間（例：1時間、24時間等）を基準とすることは現実的ではありません。 攻撃が長時間継続した場合、通信処理自体の問題ではなく、発熱によるハードウェア保護停止やログ書き込みによるストレージ枯渇などが発生しうるため、製品仕様に即したテスト条件が必要となるためです。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
54	通信機器	S3.1-47	★3適合基準 筐体の耐タンパー性を向上させる仕組みを実装すること。	「筐体の耐タンパー性を向上させる仕組み」という基準について、具体的な判定基準（参照すべき規格や数値）の明示を強く要望します。 例えば、IEC 62262で定義される IKコード（耐衝撃保護等級）の閾値や、FIPS 140-2 等のセキュリティ規格における物理セキュリティ要件など、客観的に合否を判断できる基準を示してください。	筐体設計および金型の製作は製品開発の極めて初期段階で決定されるものであり、評価段階での指摘による修正（金型の作り直し等）は事実上不可能です。 「高強度」という定性的な表現では、評価者の主観によって合否が左右される恐れがあり、設計目標を定めることができないため、定量的な基準が必要です。	物理的な攻撃対策として、どの程度の対策を取るかについては、具体的な基準を適合要件・評価ガイドにて検討いたします。
55	通信機器			「通信機器」はかなり広い範囲を指す言葉であるため、対象機器を特定できる補足説明を記載していただきたい。 例） ・「通信機器（通信端末、ネットワーク機器など）」等の記載 ・「ちっぱら通信を行うことを主目的とする機器を「通信機器」とし、その機器の主目的を達成するために副次的に通信を行う機器は含まない」等の記載	「通信機器」を通信機能を持つあらゆる機器と広義に捉えることも可能だが、その解釈は本来の趣旨を逸脱しており、読み手に無用な誤解を与えかねないと思われるため。	「通信機器」の対象については、セキュリティ要件の文書に補足説明を追加いたしました。
56	通信機器	すべて （S3.1-01～S3.1-47）	・★３適合基準 ・対象外（NA）となるための条件、基準の補足説明	文中に「IoT製品」と「IoT機器」が混在しているが、それぞれの定義や使い分けの意図を明示していただきたい。	読み手の誤解や混乱を避けるため。	「IoT製品」と「IoT機器」の使い分けについては、セキュリティ要件の文書に補足説明を追加いたしました。
57	通信機器	S.3.1-14	★３適合基準	製造番号以外にも,機器個別の仕様を特定できるものがあれば、それで代用することを認めていただきたい。	同一生産ロットであれば同一機器仕様であることが保証されるような場合が多いと思われるため、その場合は製造番号の代わりに製造ロット番号を用いてもよいのではないか。	型式番号とシリアル番号の両方を確認できることを求めております。原則として製造ロット番号は、型式番号の代わりになりますが、機器を特定する情報ではないため、製造番号の代わりにはなりません。
58	通信機器	S.3.1-15	対象外（NA）となるための条件	対象外（NA）となるための条件の設定をお願いしたい。	小規模のソフトウェアにおいて、ソフトウェアコンポーネントを適用せずにモノリシックなコードベースで開発する場合には、SBOMを作成できないため。	アーキテクチャにかかわらず、SBOMの作成は要求しております。モノリシックな場合は自社開発のソフトウェアだけで構成されていることを宣言してください。
59	通信機器	S.3.1-28	対象外（NA）となるための条件	対象外（NA）となるための条件の設定をお願いしたい。	「権限」という概念を持たない機器が想定されるため。	管理機能があり、管理機能のためには権限管理機能を持つような機器を★3の通信機器として想定しております。
60	通信機器	S.3.1-35	対象外（NA）となるための条件	対象外（NA）となるための条件の設定をお願いしたい。	狭義の通信機器（ルーター等）にとっては当然の機能であるが、ゲートウェイとして単なるプロトコル変換を目的とする通信機器には過剰な機能であるため。	管理機能があり、管理機能のためには権限管理機能を持つような機器を★3の通信機器として想定しております。
61	通信機器	S.3.1-40	・★３適合基準 ・対象外（NA）となるための条件、基準の補足説明	文中の「IoT製品」は、★３認証対象の「通信機器」そのものではなく、当該通信機器の通信対象となるIoT製品を指すと理解している。 上記の理解に相違がないかご教示いただきたい。	用語の意味・意図を正確に理解するため。	該当の「IoT製品」は★３認証対象の「通信機器」を指しております。セキュリティ要件を修正いたしました。適合要件・評価ガイドの記載内容を検討いたします。
62	通信機器	S.3.1-42	★３適合基準	文中の「IoT製品」は、★３認証対象の「通信機器」そのものではなく、当該通信機器の通信対象となるIoT製品を指すと理解している。 上記の理解に相違がないかご教示いただきたい。	用語の意味・意図を正確に理解するため。	該当の「IoT製品」は★３認証対象の「通信機器」を指しております。セキュリティ要件を修正いたしました。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
63	通信機器	S.3.1-47		項目を削除していただくか、具体的な設計目標値を示していただきたい。	民生機器の場合、一般的な使用者が通常の使用をする範囲では破損しないことを基準に筐体設計がされており、破壊を前提とした物理的脅威に対応することは極めて困難であるため。 また、機器の設置や施工を専門業者が実施するとは限らず、特殊工具が必要となるセキュリティネジなどの適用も極めて困難であるため。	物理的な破壊・改変行為による脅威は、無視できないと判断したため、削除はいたしません。 ただし、どの程度の対策を取るかについて、具体的な基準を適合要件・評価ガイドにて検討いたします。
64	製品共通	1-3	参考資料_★3 適合基準案_ガイダンス文書あり>適合基準番号：S3.2-01 >★3 適合ガイド（製造業者向け） >適合要件1　注釈	IPアドレスやLAN内機器のみを対象とした制限は、クラウド連携や動的なネットワーク構成が一般的となった現在、運用面やセキュリティ要件に必ずしも適合しなくなっていると考えます。これらの制限については、適合要件1のAからDの条件に見られるように、上位のアクセス制御や認証・認可の仕組みによって十分にカバーされているため、実装要件から削除することに賛同いたします。	※「本参考資料は、意見募集の対象外」と記載がございましたが、ガイダンスに「ご意見を伺いたい」と記載がございましたので記載させていただきました。	ご賛同ありがとうございます。ご意見を承りました。
65	製品共通	1-6	★3適合基準	「IoT製品で使用する電子証明書は、更新可能とすること」について、運用面や安全性の観点から、より実態に即した対応が望ましいと考えます。現行の基準案を適用する際には、セキュリティを確保しつつ、実装や運用の現場で発生し得る課題を含めた柔軟な指針が必要であると考えます。IoTデバイスにおける電子証明書の運用に関して、以下の事項を考慮いただくことを希望します。 ・閉域ネットワークでの運用制約 インターネットから隔離された閉域ネットワーク環境では、証明書の取り消し情報を確認できない場合があり、失効証明書の検証が困難です。この場合、更新要件を満たすための代替案が必要となります。		危殆化した証明書の変更と無効化までを求めており、証明書の失効を検証することまでは求めておりません。該当箇所については、いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 「適合要件３：IoT製品において使用する電子証明書を失効する仕組み、あるいは、その他の方法でIoT製品への認証ができなくする仕組みを持つこと」
66	製品共通	1-7	★3適合基準	「IoT製品でSSHを公開鍵認証により利用する場合、公開鍵認証機能はセキュアな暗号アルゴリズムを使用すること」とありますが、現状、暗号アルゴリズムの選定においてはCRYPTRECの推奨リストが広く推奨されています。しかし、本パブリックコメント募集時点では、耐量子暗号の評価が進行中であり、リスト掲載には至っていません。 この要件の解釈によっては、暗号の利用ケースによって耐量子暗号の採用が困難となり、ライフサイクル全体で不適切な実装を選択する懸念があります。将来的な暗号技術の進展に対応可能な柔軟性を確保することが望ましいと考えます。	・政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（第１回）議事要旨 ・政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（第２回）配布資料 ・金融庁「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」配布資料「耐量子計算機暗号（PQC）に関する概況等について」 を参照しました。	JC-STARは日本の制度であるため、日本で認められているCRYPTRECを参照することとしております。 なお、PQCの扱いに関しては、CRYPTRECでも検討しております。
67	製品共通	6-6	★3適合基準	「IoT製品に展開されるソフトウェアの実装およびテストにおいて、コード最小化のための手法を採用すること。」とありますが、コード以外の領域についても考慮が必要であると考えます。特に、削除漏れが比較的多く、攻撃者に有利な情報となり得る「デバッグ情報の削除」などについても、適合要件に明記することが望ましいと考えます。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
68	製品共通	6-7	★3適合基準	①デフォルト権限の最小化において、「デフォルトの権限設定を必要最小限に留めること。」とありますが、「どこまでが最小限か」の線引きが製造業者と評価者によって異なると考えられます。 そのため、どのような場合を「最小限」とするのか、例外が存在する場合の説明や許容される範囲などについて、より明確な基準をガイドラインや評価手順に明記いただくことを希望します。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
69	製品共通	13-1	★3適合基準	すべてのインタフェースに対して、入力されたデータの妥当性を検証する点について、どの程度の異常値やパターンをテストすれば「適合」とみなされるのか、その範囲を評価者が実施すべき内容としてガイドラインや評価手順に明記いただきたいです。また、代表的な異常値や攻撃パターンの例示、自動化ツール（ファジングツール）の活用範囲についても明記いただくことを希望します。これにより、評価者側の運用負担の軽減や評価の一貫性につながると考えます。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２： 適合要件１で一覧化されたインタフェース毎に、入力データの妥当性検証の内容が定義されていること。検証内容には以下が含まれること。 A) 正しいタイプ B) 許可された値 C) 許可された基数 D) 許可された順序 E) サニタイズやエスケープ処理、破棄など不正データに対する処理の方法
70	製品共通	14-6	★3適合基準	「不要になった個人情報を削除する機能を有すること。」とありますが、削除後の状態についても、より安全性を確保する観点から明示することが望ましいと考えます。 具体的には、以下のような文言を追加することを提案します。 ・削除は、単純な論理削除にとどめず、記憶媒体上のデータを復元困難な状態にすること。暗号化消去または安全な上書き等の手法を用いること。	・NIST SP 800-88（媒体のデータ抹消処理（サニタイズ）に関するガイドライン） ・ISO/IEC 27040（情報技術－セキュリティ技術－ストレージセキュリティ） を参照・参考としました。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
71	製品共通	S3.1-01 S3.2-01	「また重要な設定変更等の操作については上記認証手段を再度実施すること。」	「重要な設定変更等」がどのようなものかが分からないため、定義をしていただきたい。	何が「重要な設定変更等」に該当するのかが分からないと「また重要な設定変更等の操作については上記認証手段を再度実施すること。」への対応ができない。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
72	製品共通	S3.1-01 S3.2-01	「IoT 製品に対するIP通信を介した守るべき情報資産への他の IoT 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。 また重要な設定変更等の操作については上記認証手段を再度実施すること。」	「守るべき情報資産」と「重要な設定変更等」の関連を明確にしていただきたい。守るべき情報資産には「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」が含まれているが、「重要な設定変更等」とはこれらを指すという理解で合っているか。	何が「重要な設定変更等」に該当するのかが分からないと「また重要な設定変更等の操作については上記認証手段を再度実施すること。」への対応ができない。	「守るべき情報資産」と「重要な設定変更等」とは直接的な関連性はありません。「重要な設定変更等」とは、「機能に大きな影響を与えるような設定」や「通常変更する必要がない設定」をあえて変更するなどの場合を意図しており、そのような変更を行う際には再度の認証を求めるべき、ということを意味しています。 なお、機密セキュリティパラメータ=SSP(Sensitive Security Parameter)の変更は「機能に大きな影響を与えるような設定」に該当する一例であり、適合要件・評価ガイドの記載内容を検討いたします。 例えば、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２：機密セキュリティパラメータの変更においては、たとえ認証済みであっても改めて認証を要求すること。
73	製品共通	S3.1-05 S3.2-05	「電子証明書は、十分なセキュリティ強度を持つこと。」	「十分なセキュリティ強度を持つこと」の説明として、参考資料：★3 適合基準案_ガイダンス文書あり には、「CRYPTREC 暗号リストのうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いた暗号技術」とある。 海外セキュリティ制度要件と同様の意味の用語があるのであれば、それと統一した用語を使用したほうがよいと考える。	JC-STARは海外セキュリティ制度要件との相互承認を目指しているため。	JC-STARは日本の制度であるため、日本で認められているCRYPTRECを参照することとしております。
74	製品共通	S3.1-06 S3.2-06	「SSHを公開鍵認証にて利用する場合は」	当該要件がSSHを対象とする理由・背景を説明いただきたい	SSHのセキュリティ要件が出てくることに唐突感があるため。	認証に利用されている暗号技術の代表的なものとしてSSHと証明書を抽出し、それぞれについて要件化しております。S3.1-01、S3.2-01で取り上げているFIDO, Open ID Connectは、プロトコルの仕様として明確化されているため、★3レベルとして追加の要件を設定することは不要と判断いたしました。
75	製品共通	S3.1-07 S3.2-07	「①ユーザ認証において多要素認証を行う機能を有すること」	通信機器やネットワークカメラで多要素認証は可能なのか？可能な場合、どのような多要素認証(知識、所有、生体のどの組み合わせの多要素認証)を想定しているのか。具体的な事例を示していただきたい。	通信機器やネットワークカメラで多要素認証の必要性や可能なのか疑問がある。	本適合基準では、IoT製品においてVPNゲートウェイ機能をもつ機器が対象であり、当該機器のVPN接続*1)において厳格なユーザ認証及び機器の接続制限を行う方式を実装することを求めております。 *1)VPN接続： 利用者が利用する機器から内部ネットワークへのリモートアクセスVPNが対象である。拠点間VPNは対象外である。
76	通信機器	S3.1-08	「IoT機器は、接続する機器を識別し」	機器の識別情報としてIPアドレスも認めていただきたい。	参考資料に機器を一意に識別する情報としてMACアドレスが書かれているが、MACアドレスは偽装可能であるため、その意味ではIPアドレスと同等である。また、MACアドレスは基本的に同一ネットワークセグメント内でのみ直接取得可能(ルータ越しに取得不可)であるため、MACアドレスによる機器管理には大きなコストがかかる。	MACアドレスなど一意に機器を識別できる値を使用したもの、もしくはクライアント証明書を用いた方式を求めております。該当箇所については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： 利用される識別方式が、MACアドレスなど一意に機器を識別できる値を使用したもの、もしくはクライアント証明書を用いた方式であること。
77	製品共通	S3.1-09 S3.2-08	「④脆弱性の対応について、適切な報告先機関へタイムリーに報告することの宣言」	適切な報告先機関を定義していただきたい。	どこに報告するのかを正しく理解していないと適切な対応が取れないため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
78	製品共通	S3.1-09 S3.2-08	「④脆弱性の対応について、適切な報告先機関へタイムリーに報告することの宣言」	タイムリーの定義をしていただきたい。もし報告タイミングをメーカー側で決めてよいならその旨を規定いただきたい。	タイムリーの意味を正しく理解していないと適切な対応が取れないため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件５： 脆弱性の対応について以下のようなIPAまたは指定機関に報告するタイムラインの宣言がされていること。なお、報告する脆弱性対象については製造業者にて判断基準を定めること。 製造業者が設定するタイムライン例 ・早期警戒通知：製造業者が脆弱性を認知してから24時間以内 ・脆弱性通知：製造業者が脆弱性を認知してから72時間以内 ・最終報告：是正措置・緩和措置が利用可能となってから14日以内
79	製品共通	S3.1-10 S3.2-09	「④自動アップデート機能を有すること。」	④の要件について、自動アップデート機能に相当する機能も認めていただきたい。 たとえば、ユーザーがアップデートがあることに気付くことができる機能。	EU無線機器指令(RED)の要件に合わせた要件としたほうが、JC-STAR特有要件として対応するよりメーカは対応がしやすく、JC-STARの普及に寄与すると考えるため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 自動アップデートの機能を有すること。あるいは、アップデートが実施されていないことの警告を自動表示する機能を有すること。 <補足説明> 自動アップデート機能を初期状態で有効にすることは求めない。
80	通信機器	S3.1-17	「②すべての機密セキュリティパラメータは、物理的、電気的、又はソフトウエアなどの手段により改ざんに耐えられるように実装されていること。」	②の要件について、メーカーは業務上必要な場合は機密セキュリティパラメータを変更することを認めていただきたい。	メーカーは製造工程やリサイクル時に機器固有のIDを変更する必要があるため。	製造業者やユーザが意図して書き換える場合には、「改ざん」には相当いたしません。
81	通信機器	S3.1-19	「～に使用される重要なセキュリティパラメータは、IoT機器毎に固有であること」	重要なセキュリティパラメータは、IoT機器毎に固有だけではなく、ユーザ設定が可能なものを使用することも認めていただきたい。	機器固有の情報も機器使用開始後は変更されるケースがあるため。	製造業者として設定する場合は、IoT機器ごとに固有の値としてください。その後の運用においてユーザが変更する分には、それを妨げるものではございません。 適合要件・評価ガイドでの解説を検討いたします。
82	通信機器	S3.1-20	「② IoT製品が保護されたネットワーク以外のネットワークを介して守るべき情報資産を通信する場合は、IoT製品が自ら情 報の盗聴・改ざんに対する保護対策を行う」	保護されていない通信を使用する場合は、その旨をユーザーに通知するという手段も認めていただきたい。	EU無線機器指令(RED)の要件に合わせた要件としたほうが、JC-STAR特有要件として対応するよりメーカは対応がしやすく、JC-STARの普及に寄与すると考えるため。 REDでは、古い機器との通信の互換性確保のため、保護されていない通信を使用する際にはその旨を示すという要件になっている。	★3では守るべき情報資産を通信する際、通信の保護が必須となります。通信保護の方法については、適合要件・評価ガイドの記載内容を検討いたします。
83	通信機器	S3.1-21	「セキュアな管理プロセスを実施していること。」	本要件を削除、または、「IoT製品で利用する重要なセキュリティパラメータの生成・配布・保管・更新等の各ライフサイクルを管理する機能を有すること」に修正いただきたい。	・重要なセキュリティパラメータはユーザ資産であるため、メーカーが管理するのは適切ではないため。製品がそのような機能を備えるという要件であれば理解できる。	共通鍵や秘密鍵など、製造業者が設定する重要なセキュリティパラメータ=CSP(Critical Security Parameter)がある場合に、製造事業者が実施する範囲においてセキュアな管理プロセスを求めています。
84	通信機器	S3.1-24	「以下を含むセキュリティ関連情報を最小化していること。」	「セキュリティ関連情報を最小化」するという言葉の意味を明確にしていただきたい。もしくは、最小化するというあいまいな表現ではなく「以下を含むセキュリティ関連情報は認証なしでは閲覧不可能である」と記載していただきたい。	最小化の意味を正しく理解していないと適切な対応が取れないため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
85	通信機器	S3.1-25	「①IoT機器の不必要な物理的インフェースは、露出から保護する仕組みを有すること。 ②IoT機器のデバッグインタフェースを物理的または論理的に無効化していること」	①②を統合して、「IoT機器の不必要なインターフェース(含デバッグインターフェース)を物理的または論理的に無効化していること」という要件にしていただきたい。	①の要件では、例えばUSBメモリを使用しないユーザのためにUSBポートを板金でふさぐといった対応が必要になる。②で論理的なインターフェース無効化が認められるならば、左記で提案した要件にすることは許容できると考える。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 【補足５：不必要な物理的インタフェースの定義】 ・IoT機器として、恒久的に使用されない物理的インタフェースのこと
86	通信機器	S3.1-27	「コード最小化のための手法を採用すること。」	当要件は取り下げていただきたい。	オープンソース(OSS)を採用する場合、使用しないコードも含めてOSS全体を搭載する必要があるため。OSSから必要な機能のみ抽出することは非常にコストがかかるため。	対象となるコンポーネントを明確にする形で、適合要件・評価ガイドの記載内容を検討いたします。
87	通信機器	S3.1-34	「IoT製品は、特定のタイミングの構成情報を正しく保持、復元できるバックアップ機能を有すること。」	特定のタイミングを定義をしていただきたい。もしタイミングをメーカー側で決めてよいならその旨を規定いただきたい。	特定のタイミングの意味を正しく理解していないと適切な対応が取れないため。	ユーザがバックアップ操作を行ったタイミングとなります。 ユーザが実施する場合はそのタイミングですが、もしベンダーが定期的に実施する場合のタイミングはベンダーで規定してもかまいません。
88	通信機器	S3.1-35	「(①(中略)記録するセキュリティイベントの対象として(中略) 閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録」について、「それに対する機器側の対応の記録」は冗長ではないか。	「閾値を越えるログイン試行の記録」があればログとして十分であるため。	「閾値を越えるログイン試行の記録」があればログとして十分であるため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
89	通信機器	S3.1-35	「(①(中略)記録するセキュリティイベントの対象として(中略) 閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、(中略)、ハードウェア変更時の記録（監査ログ取得が可能な場合）を取得・保存する機能を有する。」	閾値を越えるログイン施行への対策が有効化されているか否かに依らず、「閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録をとる」という理解で合っているか。	本要件の適用条件を正しく理解していないと適切な対応が取れないため。	ご認識の通りです。
90	通信機器	S3.1-35	「(①(中略)記録するセキュリティイベントの対象として(中略) 閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、(中略)、ハードウェア変更時の記録（監査ログ取得が可能な場合）を取得・保存する機能を有する。」	「ハードウェア変更時の記録（監査ログ取得が可能な場合）」は「ハードウェア変更時の記録（セキュリティに関係するハードウェア変更の場合）」とするのが妥当ではないか。	ハードウェア変更時の記録の条件を「監査ログ取得が可能な場合」とすると、セキュリティ上必要なログが記録されないケースが起こりえるため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
91	通信機器	S3.1-41	「製造業者は、どのようなログ（テレメトリデータ・監査ログ）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周知すること。」	ユーザーの守るべき情報資産に影響しない、企業にとっての知的財産であるデータ(例えば、機器の動作記録は技術情報)は、周知の対象外としていただきたい。	企業の知的財産は社外に知られるべきものではなく、それが周知されると企業活動に影響があるため。	それが誰によって、どのような目的で使用されているかを周知することを要求しており、その内容を開示することを求めるものではありません。 ただし、ユーザーの知らないところでデータを収集することは認めておりません。
92	通信機器	S3.1-43	「製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。」	ペネトレーションテストに限定せず、種々の静的、動的検査も認めていただきたい(選択肢を広げるような要件としていただきたい)。	EU無線機器指令(RED)やEUサイバー・レジリエンス法(CRA)ではペネトレーションテストに限定していないため、REDやCRAの要件に合わせた要件としたほうが、JC-STAR特有要件として対応するよりメーカは対応がしやすく、JC-STARの普及に寄与すると考えるため。	JC-STARの★3としては第三者によるペネトレーションテストの実施を必須条件としております。
93	通信機器	S3.1-47	「筐体の耐タンパー性を向上させる仕 組みを実装すること。」	製品の特性によって対応判断できるといった、柔軟性のある要件にしていただきたい。また、筐体の対タンパー性を向上させる仕組みの実装を有償対応で行うことを認めていただきたい。	筐体の対タンパー性を向上させる仕組みの実装はコスト増につながるため。	物理的な攻撃対策として、どの程度の対策を取るかについては、具体的な基準を適合要件・評価ガイドにて検討いたします。
94	通信機器	S3.1-01	★3 適合ガイド（製造業者向け） 適合要件１ ②A)	本項目では下記文言がありますが、★３適合基準で認識合いますでしょうか。 A)ユーザ認証に使用されるパスワードによるユーザ認証が、「★1 適合基準S3.1-02」に準拠した実装	要件の認識確認のため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
95	製品共通	S3.1-02	NA条件	ＮＡ条件には「ＩＰを介した」の文言がありませんが、要件には「ネットワークを介した」の文言があります。そのため、★１と同様にシリアルのようなＩＰを介さない通信での認証は対象外になる認識で合いますでしょうか。 例）下記のような２つの認証経路を実装している場合、①は対象外、②は対象 ①シリアル（IPを介さない） ②WebUI（IPを介す）	★１準拠製品を★３にする際の対応内容を把握したい	以下のようにセキュリティ要件に反映いたしました。 【対象外（NA）となるための条件】 IP通信を介した守るべき情報資産への認証及びアクセスの仕組みがない （「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認証及びアクセスが必要ない根拠を記載すること）
96	通信機器	S3.1-20	ー	★１ではデフォルト無効となる通信は対象外となっていたが、★３は対象になるのか？	★１準拠製品を★３にする際の対応内容を把握したい	★3はデフォルト無効となる通信も対象となります。 ただし、本適合基準に適合しない通信をオンにするための設定変更において、特別な権限（管理者権限等）を必要としている場合は例外として本適合基準への適合範囲から除外することを認めます。
97	通信機器	S3.1-05	IoT製品において認証のために使用する電子証明書は、十分なセキュリティ強度を持つこと。	十分な強度の定義は何か？	守るべき情報資産によっても異なるのではないかと思う。	適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１：電子証明書で使用する暗号技術は、CRYPTRECで認められた暗号技術*)を使用すること
98	通信機器	S3.1-05	IoT製品で使用する電子証明書は、更新可能とすること	ファームウェアごと更新する作りでも要求を満たせるか		ご意見いただいた方法でも要求を満たすことができます。
99	通信機器	S3.1-06	「セキュアな暗号アルゴリズム」「セキュアに保つ」	セキュアの定義は何か？	守るべき情報資産によっても異なるのではないかと思う。	適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１：SSHの公開鍵認証機能で使用する暗号技術は、CRYPTRECで認められた暗号技術*)を使用すること

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
100	製品共通	S3.1-07	「①ユーザ認証において多要素認証を行う機能を有すること」	VPN機能を持つ製品のユーザ認証はすべて多要素認証必須なのか？	S3.1-04の適合要件１では多要素認証がなくても適合できる要件があるため、VPN機能を持つ製品の多要素認証必要な範囲を明確化したい。	本適合基準では、外部から内部ネットワークへの接続のゲートウェイとなる機器（VPNルータ等）に関しては、VPN接続において、より強固な多要素認証を要求いたします。
101	通信機器	S3.1-07	脆弱な認証・認可メカニズムを使用しない	VPNゲートウェイ機能機器は①多要素認証機能、②接続元制限機能を両立について両立しなくても許されるか。	装置単体で「VPNゲートウェイ機能機器は①多要素認証機能、②接続元制限機能を両立」をすることはクローズドなネットワークを利用している場合など、対応できない環境も多数あり	本評価基準では、VPN接続機能に対する多要素認証について、①多要素認証機能、②接続元制限機能の両方を満たす必要があります。
102	通信機器	S3.1-08	L2/L3スイッチング	L2スイッチは通信機器の対象ではないと思いますが。マルチレイヤスイッチといいたいのでしょうか		インテリジェントL2スイッチは対象となります。通信機器の対象については、セキュリティ要件の文書に補足説明を追加いたしました。
103	通信機器	S3.1-08	脆弱な認証・認可メカニズムを使用しない	「機器を識別して無許可接続を拒否する機能」 は機能を有することを求めているのか？	必ず拒否ではなく、識別して拒否できる機能を有していれば問題ないか	ご認識の通りです。接続する機器を識別し、接続を許可または拒否する仕組みの実装を求めています。
104	通信機器	S3.1-10	④自動アップデート機能	通信機器単体で具備するものか？ SD-WANのシステム連携で実現可能であればよいものか？	SD-WANシステムを利用して機能を実現している場合では要件を満たすことができるか	適合要件・評価ガイドにて利用条件などの記載内容を検討いたします。
105	通信機器	S3.1-12	アンチロールバックの機能を有すること	フィールド不具合対応都合で、バージョンを下げて一時的に運用するケースがある。「新しいファームにアップデートしたが不具合が出たので、古いバージョンに戻したい」というケースである。不具合内容によっては、NW停止となりセキュリティに優先する事象のため、アンチロールバックする場合は利用者へリスク通知（リスク移転）する形ではどうか	新バージョンでの不具合回避、バージョン固定などお客様の要望や状況によって古いバージョンを理由したいケースは多数ある (フィールドでは受け入れてもらえない)	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 更新ソフトウェアでアップデートする前に、更新ソフトウェアのバージョンを確認し、現在のバージョンと同じまたは以前のバージョンであることが確認されていた場合にはアップデートが中止されること。 ただし、本適合要件は、必要に応じて過去のバージョンのソフトウェアをインストールする手段を有することを妨げないが、デフォルトで過去のバージョンの更新ソフトウェアでアップデート可能としてはならない。
106	通信機器	S3.1-14	製品のモデル名称は、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	モデル名称とラベルは違うことがある。 本条項については梱包箱も含めていただきたい。	AtermにKP/KCモデルといった例がある	IoT製品をユニークに特定できる情報が、設置されているIoT製品本体から判別できる必要があります。 そのため基準では、IoT製品本体に、IoT製品の型番及びシリアル番号を直接記載されている、もしくはIoT製品のGUI、ウェブUI等や、IoT製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）のGUI、ウェブUI等から、ユーザが型番及びシリアル番号を認識できることを要求しております。
107	通信機器	S3.1-16	製品ストレージ内の守るべき情報資産はセキュアに保存しなければならない	セキュアに保存の条件があいまい	暗号化やアクセス制限されたパーティションに保存されていることで満たせるものなのか	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 セキュアに保存されていることは、以下の適合要件１～6のいずれかに類する保護対策又はそれ以上の対策（情報資産ごとに異なる対策を採用してもよい。また、複数の対策を併用してもよい。）が取られていること。 適合要件１： 機密性の保護が必要な守るべき情報資産は、CRYPTRECで認められた暗号技術*)によって暗号化された上で保存されること。 適合要件２： 完全性の保護が必要な守るべき情報資産は、CRYPTRECで認められた暗号技術*)を採用した署名によってデータの完全性が確認できる形で保存されること。 適合要件３： 完全性の保護が必要な守るべき情報資産は、CRYPTRECで認められた暗号技術*)であるハッシュ関数を用いたメッセージダイジェストによってデータの完全性が確認できる形で保存されること。 適合要件４： 守るべき情報資産は、仮想化技術、iOS/Android等のOSの機能として提供されるサンドボックス、又はセキュリティチップによるセキュア領域に保存されること。 適合要件５： 守るべき情報資産は、IoT機器に組み込まれた容易に取り外せないストレージ領域にあって、外部から呼び出すインタフェースを経由した直接的なデータの読み書きができない領域又はそのようなインタフェースを備えない領域に保存されること。 適合要件６： 守るべき情報資産のうちログ（テレメトリデータ・監査ログ）については適合要件１による保護が行われていること
108	通信機器	S3.1-17	【補足１：物理的保護の例外事項】 ・機器の設置環境が、セキュリティエリア(*1)への設置を前提としている場合、 (*1)：物理的セキュリティに配慮された施設内の共用エリア以外の区画	物理的セキュリティに配慮された施設内の共用エリア以外の区画とは、第３者がアクセスできないエリアと考えてよろしいでしょうか。	第３者からの改ざんに対するセキュリティ対応かどうかを把握したいため	入退室を許可されていない者の立ち入りを禁止したエリアを指しております。
109	製品共通	S3.1-18	技術文書２に記載された重要なセキュリティパラメータが IoT 製品運用中では無効状態になっていることを確認する。	無効状態になっているとは、具体例を記載いただけないでしょうか	技術文書2で整理する内容を把握したいため	適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２： 一覧化されたセキュリティパラメータに、IoT製品の運用中*)に利用される重要なセキュリティパラメータが含まれていないこと。 *)IoT製品の運用中: IoT製品がユーザによって利用されている期間。開発時や出荷時のテスト、初期設定時、改修・故障解析時などを除くもの。
110	通信機器	S3.1-19	ソフトウェアアップデートやサービス通信に使う重要なパラメータは機器毎に固有で自動生成	求められているものがあいまいであり何が必要かが不明	求められている自動生成されるものが不明である 装置単位、製品単位、バージョン単位も不明	基準として自動生成を求めるものではありません。 IoT機器ごとに固有のパラメータを有することを求めています。
111	通信機器	S3.1-20	ベストプラクティスの暗号技術で通信がセキュアでなければならない	「ユーザの設定次第で安全性がぶれる」ことを防ぐための設計を求めていることが想定されるが、どこまで想定していれば要件に合致しているといえるか？	ユーザが選択する設定できまるため、ベストプラクティスが条件では対応が難しい	JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
112	通信機器	S3.1-21	重要なセキュリティパラメータの管理プロセス	RAM上に一時的に保持されている運用データは管理プロセスに含まれるか？	管理対象は何か、セキュアな管理プロセスの条件は何か	RAMは対象外となります。管理プロセスの詳細については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 評価項目1： 技術文書１に記載された重要なセキュリティパラメータについて、技術文書２に、生成・配布・保管・更新・廃棄・失効の各ライフサイクルで、アクセスコントロールや権限分離、暗号化による保護、システム的な対応等によるセキュアな管理プロセスが規定されていることを確認する。 セキュアな管理プロセスの例： １）生成（Generation） ・安全な方法で生成する：信頼できる乱数生成器（CSPRNG）を使用する。 ・属性設定：種類（対称鍵／非対称鍵／PIN／パスワード）、用途（暗号化／署名／認証など）、有効期間などを定義する。 ２）登録・配布（Registration & Distribution） ・登録の管理：生成されたデータをCKMS（暗号鍵管理システム）等に登録し、メタ情報（ID、用途、有効期限など）を付与する。 ・安全な配布：安全なチャネル（例えばTLS、ハードウェアセキュリティモジュール）を通して、利用者やシステムに重要なセキュリティパラメータを配布する。 ３）保管（Storage） ・安全な場所に保管する：例えば、HSM（Hardware Security Module）や暗号化されたストレージに保存する。 ・バックアップを行う：災害対策として、暗号化されたバックアップを安全な場所に保管する。 ・アクセスログを残し、監査可能な状態にする。 ４）更新（Update） ・定期的な更新：有効期間が終了する前に新しい重要なセキュリティパラメータを生成・配布し、定期的な更新を行う。 ・影響範囲の確認：更新による影響（データ再暗号化など）を事前に評価し更新方法を決定する。 ５）破棄（Destruction） ・完全な削除：復元不可能な方法で破棄（例：ゼロ化、物理破壊）。 ・記録保持：破棄の日時、方法、責任者などを記録する。破棄処理のログを残し、監査可能な状態にする。 ６）失効（Revocation） ・失効理由の管理：漏洩、使用終了、ポリシー変更など。 ・通知と対応：関係者への通知、代替データの配布、再暗号化、サービスの停止、製品の破棄などの対応が必要。
113	通信機器	S3.1-22	無線通信区間において適切な方式による通信の暗号	適切な方式の定義とは？		該当箇所については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 IoT製品の無線通信の暗号化機能は、以下の適合要件１を満たすこと 適合要件１： 利用される無線通信のセキュリティ規格が、WPA3 Enterprise（Wi-Fi Protected Access 3 Enterprise）、またはWPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式をサポートしていること。 IoT製品の802.1Xによる機器認証機能は、以下の適合要件２を満たすこと 適合要件２： IEEE 802.1X認証で用いるEAP（PPP Extensible Authentication Protocol）の規格がTLS、TTLS、PEAP、またはEAP-FASTの認証方式をサポートしていること。
114	通信機器	S3.1-24	機器設定/OSカーネル/SWバージョンなど、認証なしで得られるセキュリティ情報を最小限に	初期アクセス情報などでどこまでなら最小限なのか	ログイン認証の前ではどこにアクセスしているかが不明となる運用しかできないのか 不明な装置にアカウント情報を入力することにならないか	適合要件・評価ガイドの記載内容を検討いたします。
115	通信機器	S3.1-25	6-3. 機器のハードウェアは、物理インタフェースを不必要に攻撃にさらしてはならない。	S3.1-17には【補足１：物理的保護の例外事項】として例外事項ありますが、S3.1-25には例外事項はありますでしょうか。	例外事項の環境ではセキュリティリスクは低いと考えたため	適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 【補足４：物理的保護の例外事項】 ・機器の設置環境が、セキュリティエリア(*1)への設置を前提としている場合、その旨の注意をユーザに明示することを条件に、適合要件１．2を満たしているとみなす。 (*1)：物理的セキュリティに配慮された施設内の共用エリア以外の区画
116	通信機器	S3.1-27	評価項目1 コードの最小化を行うため、以下のいずれかに類する手法又はそれ以上の手法を採用していることを確認する。 A) 自動化ツールを使用して、デッドコードや未使用のコードを識別し、削除する。 B) パッケージマネージャーを使用して、サービスやソフトウェアの操作に必要なコンポーネントのみをインストールする。	評価機関としては何を確認するのでしょうか。 プロセスが規定されている文書のみでしょうか。であればS3.1-29セキュアな開発プロセスに含む形にはできないでしょうか。	最小化、不要コードの削除などについてどのように検証、証明するのか.また、自動化ツールを用いて、デッドコードがないことがわかるエビデンスまで必要かどうかを確認したいため S3.1-29との差分を把握したいため	適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 【ドキュメント評価】 評価機関は、製造業者から提供された技術文書１，２によって、評価項目1，２の評価を実施する。評価項目１，２の全ての評価結果が「適合（Y）」の場合にのみドキュメント評価の評価結果は「適合（Y）」となる。 評価項目１： コードの最小化を行うため、以下のいずれかに類する手法又はそれ以上の手法を採用していることを確認する。 A) 自動化ツールを使用して、デッドコードや未使用のコードを識別し、削除する。 B) パッケージマネージャーを使用して、サービスやソフトウェアの操作に必要なコンポーネントのみをインストールする。 評価項目２： IoT製品の機能について網羅的に記載されたドキュメントが存在することを確認する。
117	通信機器	S3.1-28	ソフトウェアは必要最小限の権限で実行	検証方法が不明	安易なRoot権限運用などを制限したい意図は理解するが、検証証明方法が不明	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 以下デフォルト設定における権限最小化の例である。 例1：「root」権限で実行される最小限のデーモン／プロセス。特に、ネットワークインタフェースを使用するプロセスには、「root」ユーザではなく、非特権ユーザを必要とする。 例2：マルチユーザオペレーティングシステム（例： Linux®）を含む機器上で動作するソフトウェアは、コンポーネントやサービスごとに異なるユーザを使用する。
118	通信機器	S3.1-30	サードパーティコンポーネントは安全性確認して組み込み	安全性確認はどこまで確認が必要か、実装時点での脆弱性確認などで問題ないか	コンテナ/Dockerや外部VM対応した通信機器における認証は難しい	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
119	通信機器	S3.1-33	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、IoT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。	現在動作中の設定をあえて保存しない仕様で動作する装置もあります。保存していない場合は、電源OFF/ONで保存されている設定で起動します。 従い、設定保存操作後は直前の状態を維持する、としてほしいです		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
120	通信機器	S3.1-33	電源・ネットワーク停止時も認証値やソフトウェア更新状態を維持	毎起動後に設定値をシステムから取得するような保持しない運用がある	運用として設定を保存しない場合に満たせないこととなる	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
121	通信機器	S3.1-34	IoT製品は、特定のタイミングの構成情報を正しく保持、復元 できるバックアップ機能を有すること。	これはIoT機器に求められる機能としては、IoT機器外へ構成情報を自動・手動を問わずバックアップできればよいという理解でしょうか？ また、「構成情報」とは具体的には何になるでしょうか？		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： バックアップ実施機能を有し、バックアップを実施した直前の構成（バックアップが必要と判断した設定値、認証値等）がバックアップファイルに保存されること。
122	通信機器	S3.1-34	構成情報等を正しく保持・復元できるバックアップ機能	構成復元とソフトウェアのアンチロールバックの整合性が取れていないように読めます		いただいたご意見に関しましては、参考資料として公開している「★3適合基準案_ガイダンス文書あり」）の適合ガイド・評価ガイド（案）において、実施した直前の構成（バックアップが必要と判断した設定値、認証値等）と記載しており、ソフトウェアのバージョンは含んでおりません。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
123	通信機器	S3.1-34	バックアップ機能を有し、バックアップを実施した直前の構成（設定値、認証値等）がバックアップファイルに保存される機能が明記されていることを確認する。	OT製品におけるバックアップ機能として　認証値もバックアップするものでしょうか？	バックアップしたファイルの中に認証値がはいるのはリスクないのか？漏洩リスクが高まると考えました。認証値もバックアップしたほうがセキュリティ対応できる場合は理由をご教示いただけると幸いです。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： バックアップ実施機能を有し、バックアップを実施した直前の構成（バックアップが必要と判断した設定値、認証値等）がバックアップファイルに保存されること。
124	通信機器	S3.1-35	ログ（テレメトリデータ・監査ログ）は監査に必要な容量を確保し、保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行う。なお、必要な保存容量については、製品ごとの利用用途を踏まえ、別途検討を行う。	通信機器単体で具備するものか？（保存場所はIoT機器外でもよいか） サーバとのシステム連携で実現可能であればよいものか？	サーバ等IoT機器以外のシステムを利用して機能を実現している場合では要件を満たすことができるか	適合要件・評価ガイドにて利用条件などの記載内容を検討いたします。
125	通信機器	S3.1-35	10-1. テレメトリデータが収集される場合、セキュリティ上の異常がないかどうかを調べなければならない。	テレメトリデータの要件に見えますが、中身はログについての要件に見えます、テレメトリデータについて具体的な要件の記載は不要でしょうか。	テレメトリデータ収集を設計する際に、何を取得すればよいのか判断材料が欲しい。通信機器の例として、CPU使用率、トラフィック量を収集するなど記載があるとわかりやすいと考えました。	テレメトリデータについては下記用語定義をご参照ください。 【用語定義：テレメトリデータ】 製品の使用に関する問題や情報を製造業者が特定するのに役立つ情報を提供することができる機器からのデータを指す。
126	通信機器	S3.1-37	IoT機器は、安全なデフォルト構成設定に復元できること。	「安全なデフォルト構成設定」とは？		適合要件・評価ガイドの記載内容を検討いたします。
127	通信機器	S3.1-38	入力データが無効で不正である場合は、要求を拒否する機能を実装すること	「無効で不正」の定義は？		入力データが無効で不正となる条件については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２： 適合要件１で一覧化されたインタフェース毎に、入力データの妥当性検証の内容が定義されていること。検証内容には以下が含まれること。 A) 正しいタイプ B) 許可された値 C) 許可された基数 D) 許可された順序 E) サニタイズやエスケープ処理、破棄など不正データに対する処理の方法
128	通信機器	S3.1-38	転送・入力データの妥当性確認	入力データの定義、妥当性検証・不正チェックの条件があいまいであり不明	入力データの範囲チェックなどで問題ないのか。 通信パケットも入力データとすると妥当性検証が膨大となる	入力データの定義、妥当性検証・不正チェックの詳細については、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： 入力データを受け入れて処理するすべてのインタフェースが一覧化されていることのリスト。当該リストには少なくとも以下が含まれていること。 A) ユーザからのデータ入力を可能にするユーザインタフェース B) 外部ソースからのデータ入力を可能にするアプリケーションプログラミングインタフェース (API) C) リモートアクセス可能な通信方法に従ってデータ入力を可能にするネットワークインタフェース 適合要件２： 適合要件１で一覧化されたインタフェース毎に、入力データの妥当性検証の内容が定義されていること。検証内容には以下が含まれること。 A) 正しいタイプ B) 許可された値 C) 許可された基数 D) 許可された順序 E) サニタイズやエスケープ処理、破棄など不正データに対する処理の方法
129	通信機器	S3.1-38	・すべてのインタフェースについて、入力データの妥当性検証機能および不正な要求の拒否機能が動作しているこ	すべて　でしょうか？　評価項目１をみるとユーザ公開または外部リソースからデータ入力可能な範囲と見えます。	すべての場合、内部インターフェースを含む理解のため、単体テスト用のFWが必要になると考えます。評価機関としても対応が困難と考えたため	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： 入力データを受け入れて処理するすべてのインタフェースが一覧化されていることのリスト。一覧には少なくとも以下が一覧化されていること。 A) ユーザからのデータ入力を可能にするユーザインタフェース B) 外部ソースからのデータ入力を可能にするアプリケーションプログラミングインタフェース (API) C) リモートアクセス可能な通信方法に従ってデータ入力を可能にするネットワークインタフェース
130	通信機器	S3.1-43	第３者によるペネトレーションテスト	・ファーム更新ごとにペネトレーションテストを実施するのであるとすると、緊急リリースなどが不可能になる。開発コストもあがり市場への提供価格もあがりJC-STAR★3そのものの市場価値の妥当性に問題が出る。 ・ペネトレーションテストは金額、期間、対応ベンダーにより検出範囲、検出レベルが大きく異なる。セキュリティレベルを保証するにはなりえないため、セキュリティ認証項目として挙げることには違和感がある。 ・そもそも、有効なペネトレーションテストを実施可能なセキュリティベンダが存在しているか疑問があり、これがネックになりFWリリース活動が遅延するリスクがある。	費用、期間などの課題が大きい 緊急リリース、メンテナンスリリースなど実施する際に対応に時間がかかり現実的ではない	★3では、第三者評価機関による評価を必須としております。評価機関が実施するペネトレーションテストの実施概要は、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 評価項目１： ネットワークインタフェースにおいて解放されている全てのTCP/UDPポートへの診断を行い、公知の脆弱性が検出されないこと。 評価項目２： Webベースのユーザインタフェースの診断を行い、ロジックや作りこみによるものを含む脆弱性が検出されないこと。 評価項目３： 物理的にアクセス可能なデバッグインタフェースがあった場合、デバッグ行為が行えないこと。なお、物理的にアクセス可能なデバッグインタフェースには「S3.1-47」の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。また、デバッグインタフェースの接続においては、製造業者の協力を得て実施する。 全ての実機テストの評価項目において、CVSS v3基本評価基準4.0以上の脆弱性、もしくはセキュリティ要件が不適合となる挙動が検証された項目をセキュリティ課題として、評価者は製造業者に、再現可能な形式（再現手順、画面キャプチャーなど）で報告し、是正を求めるものとする。 評価項目４： IoT機器からの不正な通信（通信先一覧以外への通信）が検出されないこと。この評価は評価項目１，２を実施する際に常時通信をキャプチャすることにより実施する。
131	通信機器	S3.1-43	第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること	JC-STAR★３申請する前に実施するのでしょうか？	要件はペネトレーションテストの結果検出されたセキュリティ課題が解消されていることとあるため。申請前となる場合、評価機関にペネトレーションテストとJC-STAR★３評価2回依頼する必要があるのか	申請や第三者評価のプロセスについては、適合要件・評価ガイドの記載内容を検討いたします。
132	通信機器	S3.1-43	第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること	第三者が実施するのは必須でしょうか。自社で実施後に、評価機関によるペネトレーションテストを行う方法でも把握できると考えました。	S3.1-23には第三者による脆弱性検査とは記載されていないため。 ペネトレーションテストは第三者、脆弱性検査は自社と差があるため	★3以上では最終的には第三者評価機関による適合性評価実施が必須となります。その前に自社で行うことは問題ありません。
133	通信機器	S3.1-46	サービス不能攻撃に耐え復旧機能を有する	攻撃探知、復旧は運用と合わせシステム全体で検討するものであり装置単体では対応が難しい（サービスとはサーバと組んで有効になるものもある。装置側の設計で対応できないものもあるので項目として適切ではない。削除していただきたい。） 必須付随サービスやシステムとしてで可用性を確保しているケースもあり、システムとして対応できている場合は適合とできる形にできないでしょうか。	重要インフラ、政府機関となると、製品毎に役割分担がされていることもあると考えるためAWS ShieldなどDDOS対応サービスを利用するなど、製品サービスとして対応するのはいかがでしょうか。	復旧の条件については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： IoT機器へのサービス不能攻撃によるネットワーク過負荷状態解消後に、通信が再開されること。
134	通信機器	S3.1-46	IoT 機器へのサービス不能攻撃を一定時間再現した後、正常に通信が再開されること。	サービス不能攻撃を具体的に定義してほしい。	製造者と評価機関でのサービス不能攻撃の齟齬を無くすため	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
135	通信機器	S3.1-47	物理的な攻撃を防ぐ筐体（耐タンパー）機能を実装する	「耐タンパー性」として具体的には何を求めるか？	機械的/電子的な改ざん検知機構などが求められるとするとコストの大幅増となり現実的ではない	物理的な攻撃対策として、どの程度の対策を取るかについては、具体的な基準を適合要件・評価ガイドにて検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
136	通信機器	全体	－	下記3つのワードはすべて機密性の高いデータと理解しており、重要度の違いと考えております。 ・重要なセキュリティパラメータ ・機密セキュリティパラメータ ・守るべき情報資産 データが３つのうちどれに該当するか判断が難しいため具体的な指標等や例、比較表などを示していただけますと幸いです。	★１準拠製品を★３にする際の対応内容を把握したい	重要なセキュリティパラメータ、機密セキュリティパラメータについては、それぞれCSP(Critical Security Parameter)、SSP(Sensitive Security Parameter)と用語を変更しました。守るべき情報資産については、上記を含めセキュリティ要件に説明を記載いたしました。
137	通信機器	全体	－	★３以上では外部認証機関による評価が必要となっておりますが、提出用の技術文書についてテンプレート等は作成する予定等ありますでしょうか。	エビデンスで求められる内容の粒度感を把握したい	技術文書については、IPAとしてテンプレートを定義する予定はありません。評価機関にご相談ください。
138	通信機器	全体	－	JC-STAR★３で想定する脅威、攻撃者の能力、守るべき情報資産の記載をお願いできますでしょうか。	要件が多いのか少ないのかの判断ができないため。ネットワークカメラのほうが守るべき情報資産は多いが、要件数は少なく 想定が違うと考えておりますが判断材料が欲しいです。以下、★１評価ガイドに記載していただいた内容の旨があると判断しやすいと考えます。 https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/begoj90000004zgc-att/JC-STAR1_evaluation_guide_20250513.pdf	適合要件・評価ガイドの記載内容を検討いたします。
139	通信機器	S3.1-12 S3.1-16 S3.1-20	要件「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」 要件「製品によってセキュアに保存されなければならない。」 要件「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技術とは何か？ JC-STARで許容される暗号技術として推奨される方法を教えてほしい。	－	JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。
140	通信機器	S3.1-12 S3.1-16 S3.1-20	要件「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」 要件「製品によってセキュアに保存されなければならない。」 要件「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」	「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版」に掲載されている暗号方式（TWINE）であれば問題ないか？	TWINE, TWINE-OTR参考 https://jpn.nec.com/techrep/journal/g17/n01/170114.html 4. NECの軽量暗号 4.1 ブロック暗号TWINE 4.2 認証暗号OTR	JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。 軽量暗号の扱いについては、CRYPTRECと調整中です。
141	通信機器	S3.1-12 S3.1-16 S3.1-20	要件「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」 要件「製品によってセキュアに保存されなければならない。」 要件「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」	TWINEを使用した認証暗号方式（TWINE-OTR）は許容されるか？		JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。 軽量暗号の扱いについては、CRYPTRECと調整中です。
142	ネットワークカメラ	S3.2-15 S3.2-19	要件「製品によってセキュアに保存されなければならない。」 要件「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」	ベストプラクティスの暗号技術とは何か？ JC-STARで許容される暗号技術として推奨される方法を教えてほしい。	－	JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。
143	ネットワークカメラ	S3.2-15 S3.2-19	要件「製品によってセキュアに保存されなければならない。」 要件「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」	「CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版」に掲載されている暗号方式（TWINE）であれば問題ないか？	－	JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。 軽量暗号の扱いについては、CRYPTRECと調整中です。
144	ネットワークカメラ	S3.2-15 S3.2-19	要件「製品によってセキュアに保存されなければならない。」 要件「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」	TWINEを使用した認証暗号方式（TWINE-OTR）は許容されるか？	－	JC-STARは日本の制度なので、日本で認められているCRYPTRECを参照することとしております。 軽量暗号の扱いについては、CRYPTRECと調整中です。
145	製品共通	S3.1-31 S3.2-30	★3適合基準「デジタル署名の検証と同等のセキュリティ対策」	デジタル署名の検証と同等のセキュリティ対策は起動するOS（ブートメカニズム）の真正性（改ざん検知）と完全性を確保ができれば問題ないか。	－	ご認識の通りです。
146	製品共通	S3.1-01 S3.2-01	★3適合基準「重要な設定変更等の操作については上記認証手段を再度実施すること」	「重要な設定変更」の例示はありますか？ 開発者が技術文書2の中で、重要かそうでないかを示すのでしょうか？	重要な設定変更等の操作において確実に再認証されるようにするため	「守るべき情報資産」と「重要な設定変更等」とは直接的な関連性はありません。「重要な設定変更等」とは、「機能に大きな影響を与えるような設定」や「通常変更する必要がない設定」をあえて変更するなどの場合を意図しており、そのような変更を行う際には再度の認証を求めるべき、ということを意味しています。 なお、機密セキュリティパラメータ=SSP(Sensitive Security Parameter)の変更は「機能に大きな影響を与えるような設定」に該当する一例であり、適合要件・評価ガイドの記載内容を検討いたします。 例えば、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２：機密セキュリティパラメータの変更においては、たとえ認証済みであっても改めて認証を要求すること。
147	製品共通	S3.1-01 S3.2-01	適合要件３： 認証メカニズムにおいて継続的なアクセスをセッション等で管理する場合、タイムアウト制限を設けること。 評価項目４： 守るべき情報資産について該当する技術文書２に記載されたアクセス制御が実装されていること、および接続が技術文書２の通りにタイムアウトすることを確認する。	タイムアウトの数値（技術文書2に記載）として許容される範囲はありますか？	許容されないほど長いタイムアウトの数値を設定しないようにするため	原則的にはタイムアウトの数値については製造業者側で設定いただく形となります。
148	製品共通	S3.1-35 S3.2-35	記録するセキュリティイベント	記載されている内容以上の事項が含まれることは問題ありませんか？	念のための確認です。 通常ですと、パスワードの変更や、秘密鍵の生成・破棄もログを記録することがあります（秘密鍵の変更についてはファームウェア更新に含むケースもあります）。	記載されている以外のセキュリティイベントの取得を妨げるものではありません。
149	通信機器	S3.1-35 S3.2-35	適合要件１： ログ（テレメトリデータ・監査ログ）の取得機能および保存機能が実装され、取得するログ（テレメトリデータ・監査ログ）には以下すべてのセキュリティイベントが含まれている。 <中略> C) 閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録	「閾値」の妥当性は評価されますか？ 評価される場合、どのように／何を基に評価されますか？		閾値については、製造業者もしくはユーザが設定した値となります。閾値を越えるログイン試行をログとして取得できることを要求しています。
150	通信機器	S3.1-35 S3.2-35	★3適合基準 IoT 製品から収集したログ（テレメトリデータ・監査ログ）を検証し、セキュリティ上の異常を検知すること。具体的には、以下①～③すべての基準を満たすこと。	★3適合基準の①～③には、「セキュリティ上の以上を検知すること」が含まれていません。 検知は、機能でなく運用（定期的にログを確認する）ことでも問題ないでしょうか？（機器運用者向けのマニュアルには記載するとして）		セキュリティ異常の検知までは要求しておりません。いただいたご意見は、以下のようにセキュリティ要件に反映いたしました。 セキュリティ上の異常を検知するために、IoT製品はログ（テレメトリーデータ・監査ログ)を記録する機能を有すること。
151	製品共通	5-1.	【用語定義:保護されたネットワーク】 以下のネットワーク: ・VPN環境 ・専用線を経由した接続環境 ・物理的／論理的に保護されたネットワーク環境	専用線を経由した接続環境は境界防御として非常に有効的な手段として賛同したい。	インターネットとの接続、特にサイバー攻撃集団からの侵入経路への対策が重要であり、専用線を経由した接続環境を利用することでその侵入リスクを大きく減らすことができるため。	ご賛同ありがとうございます。ご意見を承りました。
152	製品共通	5-8.	IoT製品で利用する重要なセキュリティパラメータの生成・配布・保管・更新等の各ライフサイクルにおいて、セキュアな管理プロセスを実施していること。	LTEを使用する場合は国際規格GSMAで定義されているIoT SAFEを推奨したい。	IoT SAFEは鍵・証明書のセキュアな管理方法を標準化したものであり、セキュアな管理プロセスを効率的に普及できると想定されるため。 また、SIMをハードウェアセキュリティモジュールとして利用できるため、セキュリティ向上のためのコストを削減可能。	対応方法については様々な形が想定されるため、セキュリティ要件を満たしている規格であれば、どの規格を利用していただいても問題ありません。
153	製品共通	10-1.	①IoT製品に対し、ログ（テレメトリデータ・監査ログ）の取得機能および保存機能を実装すること。最低でも、ファームウェア（ソフトウェア）又はOSにより生成されたログ（テレメトリデータ・監査ログ）を取得・保存する。記録するセキュリティイベントの対象として機器やネットワークの切断（再接続）の記録、ログイン試行（成功時、失敗時）の記録、閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、時間変更時の記録（変更前と変更後の時刻を含む）、バックアップの取得・復元をはじめとする管理機能の利用記録、ソフトウェア変更時の記録、ハードウェア変更時の記録（監査ログ取得が可能な場合）を取得・保存する機能を有する。	ログの種類として、通信先に関する情報も必須項目として加えて頂きたい。 また、推奨項目としてポート番号、プロトコルについても加えて頂きたい。	昨今のサイバー攻撃集団の手法からC&Cサーバとの通信が発生する可能性が高く、そのフォレンジック調査として通信先の情報は非常に有効であり、ポート番号やプロトコルも活用することで迅速な事実確認・調査に繋げることができる。	いただいたご意見は、以下のようにセキュリティ要件に反映いたしました。 ①IoT製品に対し、ログ（テレメトリデータ・監査ログ）の取得機能および保存機能を実装すること。最低でも、ファームウェア（ソフトウェア）又はOSにより生成されたログ（テレメトリデータ・監査ログ）を取得・保存する。記録するセキュリティイベントの対象として機器やネットワークの切断（再接続）の記録、ログイン試行（成功時、失敗時）の記録、閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、時間変更時の記録（変更前と変更後の時刻を含む）、バックアップの取得・復元をはじめとする管理機能の利用記録、ソフトウェア変更時の記録、ハードウェア変更時の記録（監査ログ取得が可能な場合）、ファイアウォールの動作状況の記録（ファイアウォール機能が実装されている場合）、リモート管理サービスの動作状況の記録（CWMPなどが有効化されている場合） を取得・保存する機能を有する。）

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
154	製品共通	19-1.	IoT機器はサービス不能攻撃によるネットワーク過負荷状態から復元の仕組みを有すること。	デバイス側が困難な場合に備え、『ネットワークでの遮断』を選択肢として明記し、IPS/NDR/WAF/レートリミット/ブラックホールルーティングなどの活用指針を追加して頂きたい。	IPS/NDR/WAF/レートリミット/ブラックホールルーティングなどの機器やサービスを利用することで、多層防御も可能となり効率よく対応できるため。	本セキュリティ要件は、IoT機器がネットワーク過負荷状態になった場合に、ネットワーク過負荷状態が解消した後で自動的な機能回復を求めておりますので、IoT機器の要求事項になっております。
155	通信機器	全体		製品のカテゴリ別で追加の要件が発生することがありますか。		製品のカテゴリが、製品類型（通信機器、ネットワークカメラなど）を指すのであれば、それぞれで異なる要件が定義されております。通信機器における製品を指すのであれば、現状で要件の追加は想定しておりません。
156	通信機器	1-6	電子証明書	SSLの証明書は自己証明書でよいか。もしそうであればその旨を明示してほしいです。		サーバ証明書・クライアント証明書は自己署名証明書の利用を否定するものではありませんが、安全な管理プロセスの元で運用されることが必要です。詳細については、適合要件・評価ガイドの記載内容を検討いたします。
157	通信機器	1-7	セキュアな暗号アルゴリズム	対象のアルゴリズムは「CRYPTREC掲載のアルゴリズム」で良いでしょうか。もしそうであればその旨を明示してほしいです。		適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１：SSHの公開鍵認証機能で使用する暗号技術は、CRYPTRECで認められた暗号技術*)を使用すること ※対象の暗号技術には、公開鍵認証で使用する公開鍵アルゴリズム、ハッシュアルゴリズムを含む 適合要件２：SSHの公開鍵認証で使用する公開鍵は更新可能であること *)CRYPTRECで認められた暗号技術: 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」の規定に合致する鍵長を用いた暗号技術
158	通信機器	5-11	機器認証	機器認証とは端末の特定のことでしょうか。固有の機器の特定を目的としているのであればその旨を記載してほしいです。		機器認証は、クライアント端末を認証することを指しております。
159	通信機器	6-2	認証されていないセキュリティ関連情報の開示を最小化	示されているA~Cの情報で認証なしで表示してはいけない情報を明示してほしいです。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
160	通信機器	6-3	物理インターフェースの攻撃面を最小化	「不必要な物理的インタフェースは、露出から保護する仕組み」の具体例を示してほしいです。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
161	通信機器	6-6	コードの最小化	コードの最小化の例を示してほしいです。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： コードの最小化を行うため、製品特性に併せて、以下に類する手法を採用していること。 A) 自動化ツール（静的解析ツール、コンパイラ等）を使用して、デッドコードや未使用のコードを識別し、削除する。 B) パッケージマネージャー等を使用して、サービスやソフトウェアの操作に必要なコンポーネントのみをインストールする。
162	通信機器	7-1	セキュアブートメカニズム	「デジタル署名」は、「コードサイニング証明書」のことを示しているということで問題ありませんでしょうか。 また、本証明書は自己証明書でも問題ありませんでしょうか。		「デジタル署名」は「コードサイニング証明書」ことを示しているということで問題ありません。証明書は自己署名証明書の利用を否定するものではありませんが、安全な管理プロセスの元で運用されることが必要です。詳細については、適合要件・評価ガイドの記載内容を検討いたします。
163	通信機器	7-1	セキュアブートメカニズム	「デジタル署名の検証と同等のセキュリティ対策」について何か具体的な例があれば、示して頂きたい。		完全性を担保できる仕組みであれば、問題ありません。例えば、ハッシュによる検証などが同等のセキュリティ対策に相当します。
164	通信機器	8-3	センシングする情報	「センシングする情報」の範囲(※)を明確にしてほしいです。 (※通信機器自体でセンシングする場合のみか、別の機器でセンシングしたデータについて通信機器を介して取得する場合も含まれるか)		通信機器自体がセンシングする場合となります。
165	通信機器	9-5	バックアップ	バックアップはユーザが行うための機能か、IoT機器内部の機能かを明確にしてほしいです。		ユーザが実行するバックアップ機能を対象としています。
166	通信機器	10-1	システムのテレメトリデータを検証・保護	「③ログ（テレメトリデータ・監査ログ）上のセキュリティイベントの 発生日時を記録するため、時間管理機能を有する。」の「時間管理機能」が具体的にどのような機能を示すかを明確にしてほしい。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件３： ログ（テレメトリデータ・監査ログ）上のセキュリティイベントの発生日時を記録するための時間管理機能・時刻ソースによるIoT機器の時刻同期機能が実装されている。
167	通信機器	13-1	データの入力の妥当性	具体例を示してほしいです。		入力データの定義、妥当性検証・不正チェックの詳細については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２： 適合要件１で一覧化されたインタフェース毎に、入力データの妥当性検証の内容が定義されていること。検証内容には以下が含まれること。 A) 正しいタイプ B) 許可された値 C) 許可された基数 D) 許可された順序 E) サニタイズやエスケープ処理、破棄など不正データに対する処理の方法
168	通信機器	21-1	IoT機器に対する物理的な攻撃を防ぐ仕組	基準があれば具体的に示してほしい。		物理的な攻撃対策として、どの程度の対策を取るかについては、具体的な基準を適合要件・評価ガイドにて検討いたします。
169	通信機器	S3.1-10	④自動アップデート機能	通信機器単体で具備するものか？ SD-WANのシステム連携で実現可能であればよいものか？	SD-WANシステムを利用して機能を実現している場合では要件を満たすことができるか	適合要件・評価ガイドにて利用条件などの記載内容を検討いたします。
170	通信機器	S3.1-14	製品のモデル名称は、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	モデル名称とラベルは違うことがある。 本条項については梱包箱も含めていただきたい。	元々の製品名称はそのままで出荷先ごとにモデル名称を変更するケースも存在するため、梱包箱と製品に記載のモデル名が若干違うケースがあります。	IoT製品をユニークに特定できる情報が、設置されているIoT製品本体から判別できる必要があります。そのため基準では、IoT製品本体に、IoT製品の型番及びシリアル番号を直接記載されている。もしくはIoT製品のGUI、ウェブUI等や、IoT製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）のGUI、ウェブUI等から、ユーザが型番及びシリアル番号を認識できることとしております。
171	通信機器	S3.1-19	ソフトウェアアップデートの完全性及び真正性チェック、及び製品のソフトウェアにおける付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、機器ごとに固有でなければならず、製品のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。	重要なセキュリティパラメータについて、求められているものがあいまいであり何が必要かが不明	求められているものが不明である 装置単位、製品単位、バージョン単位も不明	該当の重要なセキュリティパラメータ=CSP(Critical Security Parameter）は、IoT機器ごとに固有であることを求めています。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
172	通信機器	S3.1-21	重要なセキュリティパラメータの管理プロセス	RAM上に一時的に保持されている運用データは管理プロセスに含まれるか？	管理対象は何か、セキュアな管理プロセスの条件は何か	RAMは対象外となります。管理プロセスの詳細については、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 評価項目1： 技術文書１に記載された重要なセキュリティパラメータについて、技術文書２に、生成・配布・保管・更新・廃棄・失効の各ライフサイクルで、アクセスコントロールや権限分離、暗号化による保護、システム的な対応等によるセキュアな管理プロセスが規定されていることを確認する。 セキュアな管理プロセスの例： １）生成（Generation） ・安全な方法で生成する：信頼できる乱数生成器（CSPRNG）を使用する。 ・属性設定：種類（対称鍵／非対称鍵／PIN／パスワード）、用途（暗号化／署名／認証など）、有効期間などを定義する。 ２）登録・配布（Registration & Distribution） ・登録の管理：生成されたデータをCKMS（暗号鍵管理システム）等に登録し、メタ情報（ID、用途、有効期限など）を付与する。 ・安全な配布：安全なチャネル（例えばTLS、ハードウェアセキュリティモジュール）を通じて、利用者やシステムに重要なセキュリティパラメータを配布する。 ３）保管（Storage） ・安全な場所に保管する：例えば、HSM（Hardware Security Module）や暗号化されたストレージに保存する。 ・バックアップを行う：災害対策として、暗号化されたバックアップを安全な場所に保管する。 ・アクセスログを残し、監査可能な状態にする。 ４）更新（Update） ・定期的な更新：有効期間が終了する前に新しい重要なセキュリティパラメータを生成・配布し、定期的な更新を行う。 ・影響範囲の確認：更新による影響（データ再暗号化など）を事前に評価し更新方法を決定する。 ５）破棄（Destruction） ・完全な削除：復元不可能な方法で破棄（例：ゼロ化、物理破壊）。 ・記録保持：破棄の日時、方法、責任者などを記録する。破棄処理のログを残し、監査可能な状態にする。 ６）失効（Revocation） ・失効理由の管理：漏洩、使用終了、ポリシー変更など。 ・通知と対応：関係者への通知、代替データの配布、再暗号化、サービスの停止、製品の破棄などの対応が必要。
173	通信機器	S3.1-24	機器設定/OSカーネル/SWバージョンなど、認証なしで得られるセキュリティ情報を最小限に	初期アクセス情報などでどこまでなら最小限なのか	ログイン認証の前ではどこにアクセスしているかが不明となる運用しかできないのか 不明な装置にアカウント情報を入力することにならないか	適合要件・評価ガイドの記載内容を検討いたします。
174	通信機器	S3.1-27	コード最小化の手法を採用（設計・テストに反映	認証機関において技術的検証が難しくまたドキュメント評価のみであることから、実質的にメーカー自己宣言に近い性質になるものと考えるが制度の趣旨として問題ないか？	コード最小化や不要コードの削除の証明などソースコードを読み込まないと適正に運用されているのか第三者での判断が困難であるため。	コードを最小化するためのプロセス、手順が定められていることまでを求めております。そのプロセス、手順について、第三者評価機関により、客観的なドキュメント評価が行われる形としています。
175	通信機器	S3.1-28	ソフトウェアは必要最小限の権限で実行	認証機関において技術的検証が難しくまたドキュメント評価のみであることから、実質的にメーカー自己宣言に近い性質になるものと考えるが制度の趣旨として問題ないか？	内部プロセスの動作など製品の内部設計に精通していないと適切に運用されているか第三者での判断が困難であるため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： デーモン／プロセスなどのデフォルトの権限が、最小になるよう設定されていること。 以下デフォルト設定における権限最小化の例である。 　例1：「root」権限で実行される最小限のデーモン／プロセス。特に、ネットワークインタフェースを使用するプロセスには、「root」ユーザではく、非特権ユーザを必要とする。 　例2：マルチユーザオペレーティングシステム（例： Linux®）を含む機器上で動作するソフトウェアは、コンポーネントやサービスごとに異なるユーザを使用する。
176	通信機器	S3.1-33	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、IoT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。	設定保存操作後は直前の状態を維持する、としていただきたい。 もしくはセキュリティ上問題ないことをドキュメントに記載する事で上記のような仕様も認める形としていただきたい。	製品によっては現在動作中の設定をあえて保存しない仕様で動作する装置もあり、保存していない場合は、電源OFF/ONで保存されている設定で起動するため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
177	通信機器	S3.1-33	電源・ネットワーク停止時も認証値やソフトウェア更新状態を維持	設定値を装置内に保存せずシステムから取得するような場合はセキュリティ上問題ないことをドキュメントに記載する事で上記のような仕様も認める形としていただきたい。	設定値を装置内に保存せず、システムから取得するような運用も存在するため。	本要件については、機器単体で対応できる範囲の要求としており、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： IoT機器に対する電源供給を停止させる（バッテリー駆動製品の場合、バッテリーを外すことで電源供給を停止させる）。その後、電源を復帰させた後、工場出荷時の初期状態に戻ることなく、電源OFFとなる直前の認証値、アップデート状態及び設定値等が維持されていること。 適合要件２： 通信ケーブルや無線接続を切断し、再接続した後、工場出荷時の初期状態に戻ることなく、電源OFFとなる直前の認証値、アップデート状態及び設定値等が維持されていること。
178	通信機器	S3.1-35	IoT製品から収集したログ（テレメトリデータ・監査ログ）を検証し、セキュリティ上の異常を検知すること。具体的には、以下①～③すべての基準を満たすこと。 ①IoT製品に対し、ログ（テレメトリデータ・監査ログ）の取得機能および保存機能を実装すること。最低でも、ファームウェア（ソフトウェア）又はOSにより生成されたログ（テレメトリデー タ・監査ログ）を取得・保存する。記録するセキュリティイベントの対象として機器やネットワークの切断（再接続）の記録、ログイン試行（成功時、失敗時）の記録、閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、時間変更時の記録（変更前と変更後の時刻を含む）、バックアップの取得・復元をはじめとする管理機能の利用記録、ソフトウェア変更時の記録、ハードウェア変更時の記録（監査ログ取得が可能な場合）を取得・保存する機能を有する。 ②ログ（テレメトリデータ・監査ログ）は監査に必要な容量を確保し、保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行う。なお、必要な保存容量については、製品ごとの利用用途を踏まえ、別途検討を行う。 ③ログ（テレメトリデータ・監査ログ）上のセキュリティイベントの発生日時を記録するため、時間管理機能を有する。	現行の①②は、ログの取得および保存をIoT機器内のストレージで完結させることを前提としているように読めるが、IoT機器はストレージ容量や書き込み寿命等の制約が大きく、監査に必要な期間のログを十分に保存することは現実的に困難な場合が多い。 また、セキュリティの観点からも、ログをクラウド等の外部基盤に集約することで長期保管・改ざん防止・相関分析が容易になり、機器の盗難・破壊時にも証跡を保持できるなどの利点がある。 そのため、本要件においては、IoT機器側にログ取得機能および短期間の一時保存機能を実装したうえで、安全に管理された外部ログ保存基盤（例：クラウドサービス）にログを送信・保存する構成も認める形に文言を緩和し、「IoT製品内又は外部ストレージへの保存機能」といった表現とすることが望ましい。	> ①IoT製品に対し、ログ（…）の 取得機能および保存機能を実装すること。 ・「取得機能」は明らかにIoT製品側に必要 ・「保存機能」が"ローカルストレージ"を意味しているように読めるのがネック ②も「ログ保存容量の確保」「容量超過時のローテーション」を前提にしており、ストレージを「装置内」に持つ想定っぽい書き方になっている。 以上のように、この適合基準は、かなり「IoT機器の中に保存領域を持つ」ことを前提に書かれていますが、実務的には「ログはクラウドに集約して監査・分析したい」というニーズも強いと思われるので、この方向で緩和提案をしてはどうか。 提案するするときのロジックとしては… 1. 検知・監査という目的からは、クラウド集中の方がむしろ有利な場合が多い - 大量のログを長期間保持・分析しやすい - 相関分析／アラート運用など、SOC的な運用がしやすい 2. IoT機器自体のリソースは限られており、長期保存は現実的でない - フラッシュ容量・書き込み寿命の制約 - 大容量ストレージの追加によるコスト増・故障リスク 3. セキュリティ上も、機器内にだけログがあるよりクラウド側に複製がある方が堅牢 - 機器ごと盗難・破壊された場合でも、クラウド側に証跡が残る - ログ改ざん検知（WORM相当の保持）をクラウド側で実現しやすい 4. したがって、 - 「IoT製品側に一定のバッファ（短期保存）＋クラウドへの送信・保存」 - または「クラウド直送＋送信失敗時の一時バッファ」 を認める方が、目的（異常検知・監査）の達成には現実的である という説明が使えます。	いただいたご意見を参考に、適合要件・評価ガイドにて利用条件などの記載内容を検討いたします。
179	通信機器	S3.1-35	ログ（テレメトリデータ・監査ログ）は監査に必要な容量を確保し、保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行う。なお、必要な保存容量については、製品ごとの利用用途を踏まえ、別途検討を行う。	通信機器単体で具備するものか？（保存場所はIoT機器外でもよいか） サーバとのシステム連携で実現可能であればよいものか？	サーバ等IoT機器以外のシステムを利用して機能を実現している場合では要件を満たすことができるか	適合要件・評価ガイドにて利用条件などの記載内容を検討いたします。
180	通信機器	S3.1-37	IoT機器は、安全なデフォルト構成設定に復元できること。	「安全なデフォルト構成設定」の定義を明確化していただきたい。		いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
181	通信機器	S3.1-38	転送・入力データの妥当性確認	通信パケットを入力データとする場合の入力データの定義、妥当性検証・不正チェックの条件が定義されておらずどのように設計すべきか判断できないと考える。	通信パケットも入力データとすると妥当性検証が膨大となる	入力データの定義、妥当性検証・不正チェックの詳細については、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： 入力データを受け入れて処理するすべてのインタフェースが一覧化されていることのリスト。当該リストには少なくとも以下が含まれていること。 A) ユーザからのデータ入力を可能にするユーザインタフェース B) 外部ソースからのデータ入力を可能にするアプリケーションプログラミングインタフェース (API) C) リモートアクセス可能な通信方法に従ってデータ入力を可能にするネットワークインタフェース 適合要件２： 適合要件１で一覧化されたインタフェース毎に、入力データの妥当性検証の内容が定義されていること。検証内容には以下が含まれること。 A) 正しいタイプ B) 許可された値 C) 許可された基数 D) 許可された順序 E) サニタイズやエスケープ処理、破棄など不正データに対する処理の方法
182	通信機器	S3.1-43	製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。	本適合基準は、全ての製品に対して第三者によるペネトレーションテストの実施と、検出された課題の解消を一律に要求しているように読めるが、ペネトレーションテストは高額かつ工数負荷の大きい評価手法であり、製品ラインナップやバージョン数が多い事業者にとっては、全製品・全リリースでの実施は現実的ではない。 また、重要インフラ向け製品と家庭向け周辺機器とではリスクレベルが大きく異なるにもかかわらず、同一レベルの第三者ペネトレーションテストを一律に要求することは、コストとセキュリティ向上効果のバランスを欠くおそれがある。 したがって、第三者ペネトレーションテストは高リスク用途の製品に限定して必須とし、それ以外の製品については、第三者又は開発部門から独立した社内組織による脆弱性診断やセキュリティレビューを組み合わせることでも適合とみなす等、リスクに応じた柔軟な要件設定とすることが望ましい。	この適合基準をかみ砕くと、だいたい次の意味になります。 「外部の第三者にペネトレーションテストをやってもらい、そのテストで見つかったセキュリティ上の問題について、放置せずにきちんと対応（修正 or リスク評価の上での対処）していること」 「第三者によるペネトレーションテスト」とは 製造業者自身ではない組織・部門（外部セキュリティベンダー、認証機関など）による攻撃テスト。 この適合基準の「重いポイント」は以下の2点 A：毎回「第三者ペネトレーションテスト」を要求していそうに読める B：製品種別・リスクに関係なく"一律"に求めていそうに読める 論点A：コストと実効性のバランスが悪くなり得る ・すべてのIoT製品・全バージョンに対して第三者ペネテストを一律に求めると、 ・テスト単価 × 製品数 × バージョン数 → コスト爆発 ・製品ライフサイクルが短い・バージョンアップ頻度が高い場合、 ・テストが完了する頃には次バージョンに切り替わっている ・実利用に対するセキュリティ向上効果が相対的に小さい →「高コストの割に、セキュリティ投資対効果が悪くなりうる」 論点B：リスクに応じたテストレベルが合理的 ・全てのIoT製品が同じリスクではない： ・重要インフラ／医療／工場制御など → 侵害時の影響が大 ・家庭向け周辺機器など → 相対的に小さい ・国際的な規格（62443-4-1等）も、「セキュリティテスト」「脆弱性テスト」「ペンテスト」をリスクや開発プロセスの一部として位置づけており、すべての製品に常にフルセットを義務化しているわけではない → 高リスク用途には第三者ベンテを強く推奨／必須としつつ、それ以外は脆弱性診断＋社内評価で十分とするのが現実的ではないか	★3では、第三者評価機関による評価を必須としております。評価機関が実施するペネトレーションテストの実施概要は、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 評価項目１： ネットワークインタフェースにおいて解放されている全てのTCP/UDPポートへの診断を行い、公知の脆弱性が検出されないこと。 評価項目２： Webベースのユーザインタフェースの診断を行い、ロジックや作りこみによるものを含む脆弱性が検出されないこと。 評価項目３： 物理的にアクセス可能なデバッグインタフェースがあった場合、デバッグ行為が行えないこと。なお、物理的にアクセス可能なデバッグインタフェースには「S3.1-4?」の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。また、デバッグインタフェースの接続においては、製造業者の協力を得て実施する。 全ての実機テストの評価項目において、CVSS v3基本評価基準4.0以上の脆弱性、もしくはセキュリティ要件が不適合となる挙動が検証された項目をセキュリティ課題として、評価者は製造業者に、再現可能な形式（再現手順、画面キャプチャーなど）で報告し、是正を求めるものとする。 評価項目４： IoT機器からの不正な通信（通信先一覧以外への通信）が検出されないこと。 この評価は評価項目１，２を実施する際に常時通信をキャプチャすることにより実施する。
183	通信機器	S3.1-43	第３者によるペネトレーションテスト	・ファーム更新ごとにペネトレーションテストを実施するのであるとすると、緊急リリースなどが不可能になる。開発コストもあがり市場への提供価格もあがりJC-STAR★3そのものの市場価値の妥当性に問題が出る。 ・ペネトレーションテストは金額、期間、対応ベンダーにより検出範囲、検出レベルが大きく異なる。セキュリティレベルを保証するにはなりえないため、セキュリティ認証項目として挙げることには違和感がある。 ・そもそも、有効なペネトレーションテストを実施可能なセキュリティベンダが存在しているか疑問があり、これがネックになりFWリリース活動が遅延するリスクがある。	費用、期間などの課題が大きい 緊急リリース、メンテナンスリリースなど実施する際に対応に時間がかかり現実的ではない	★3では、第三者評価機関による評価を必須としております。評価機関が実施するペネトレーションテストの実施概要は、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 評価項目１： ネットワークインタフェースにおいて解放されている全てのTCP/UDPポートへの診断を行い、公知の脆弱性が検出されないこと。 評価項目２： Webベースのユーザインタフェースの診断を行い、ロジックや作りこみによるものを含む脆弱性が検出されないこと。 評価項目３： 物理的にアクセス可能なデバッグインタフェースがあった場合、デバッグ行為が行えないこと。なお、物理的にアクセス可能なデバッグインタフェースには「S3.1-4?」の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。また、デバッグインタフェースの接続においては、製造業者の協力を得て実施する。 全ての実機テストの評価項目において、CVSS v3基本評価基準4.0以上の脆弱性、もしくはセキュリティ要件が不適合となる挙動が検証された項目をセキュリティ課題として、評価者は製造業者に、再現可能な形式（再現手順、画面キャプチャーなど）で報告し、是正を求めるものとする。 評価項目４： IoT機器からの不正な通信（通信先一覧以外への通信）が検出されないこと。 この評価は評価項目１，２を実施する際に常時通信をキャプチャすることにより実施する。
184	通信機器	S3.1-46	サービス不能攻撃に耐え復旧機能を有する	本要件は削除していただきたい。	攻撃探知、復旧は運用と合わせシステム全体で検討するものであり装置単体では対応が難しい（サービスとはサーバと組んで有効になるものもあり装置側の設計で対応できないものもある。）	本セキュリティ要件は、IoT機器がネットワーク過負荷状態になった場合に、ネットワーク過負荷状態が解消した後で自動的な機能回復を求めておりますので、IoT機器の要求事項になっています。
185	通信機器	S3.1-07	IoT製品においてVPNゲートウェイ機能をもつ場合は、以下の①～②の基準をすべて満たすこと。 ①ユーザ認証において多要素認証を行う機能を有すること。 ②接続元の機器等を制限する機能を有すること。	VPNゲートウェイ機能機器は①多要素認証機能、②接続元制限機能を両立について両立しなくても許されるか。	装置単体で「VPNゲートウェイ機能機器は①多要素認証機能、②接続元制限機能を両立」をすることはクローズドなネットワークを利用している場合など、対応できない環境も多数あり	本セキュリティ要件では、VPN接続機能に対する多要素認証について、①多要素認証機能、②接続元制限機能の両方を満たす必要があります。
186	通信機器	S3.1-08	L2/L3スイッチング	L2スイッチは通信機器の対象ではないと思いますが。マルチレイヤスイッチといったいのでしょうか		インテリジェントL2スイッチは対象となります。通信機器の対象については、セキュリティ要件の文書に補足説明を追加いたしました。
187	通信機器	S3.1-19	IoT 製品で使用される重要なセキュリティパラメータのうち、ソフトウェアアップデートの完全性及び真正性チェック、及び付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、IoT 機器毎に固有であること。	現行の適合基準は、 「アップデートの完全性・真正性チェックに用いるセキュリティパラメータも機器固有でなければならない」と読めてしまい、実装上不適切な解釈を招くため、文言を明確化して欲しい。	アップデートの完全性・真正性チェックは署名＋共通公開鍵検証で確保でき、この公開鍵は秘密情報ではなく固有性を要求すべき対象ではないと考えられる。	IoT 機器毎に固有であることが求められるのは、重要なセキュリティパラメータに対してです。 なお、公開鍵は重要なセキュリティパラメータ=CSP(Critical Security Parameter)に含まれないため、この要件の対象にはなりません。以下の用語定義をご参照ください。 【重要なセキュリティパラメータ】 セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。 （例：共通鍵・秘密鍵・パスワードやPINなどの認証データなど）
188	製品共通			IEC 62443 4-2 CR3.3に適合する要件がありませんが、★３に関しては不要との認識で良いでしょうか。	セキュリティ機能の検証の継続性を図るために通常の操作中の検証が必要だと考えます。	★3の通信機器、ネットワークカメラではIEC 62443の要件全てを要求しているわけではありません。
189	製品共通	全体	全体	★3の要件や適合基準の内容を検討するには、★4との棲み分けがある程度明確になっていないと難しい部分があると感じました。		現状の基準は★3として求められる対策を定義したものとなります。★4については、★3を超える要求事項がある場合に策定することとしております。
190	製品共通	S3.1-22 S3.2-21	セキュアに通信する	本要件は★4レベル以降が適切だと考えます。	通信機器＆ネットワークカメラともに、市場の標準的な製品に照らし合わせると、 現ドラフト案レベルを満たしているものが少ないと認識しています。 紐付けられている既存制度・文書との整合の観点からも過剰な要求となる可能性があり、本要件の★3での必須化は普及促進の障壁となる懸念があります。 重要インフラ施設など、★3より一段上のレベルが適切と考えます。	★3は政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した通信機器および、ネットワークカメラを対象としておりますので、市場の標準的な製品よりも厳格な基準を要求しております。
191	製品共通	S3.1-31 S3.2-30	ソフトウェアの完全性を確実にする	本要件は★4レベル以降が適切だと考えます。	通信機器＆ネットワークカメラともに、市場の標準的な製品に照らし合わせると、 現ドラフト案レベルを満たしているものが少ないと認識しています。 紐付けられている既存制度・文書との整合の観点からも過剰な要求となる可能性があり、本要件の★3での必須化は普及促進の障壁となる懸念があります。 重要インフラ施設など、★3より一段上のレベルが適切と考えます。	★3は政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した通信機器および、ネットワークカメラを対象としておりますので、市場の標準的な製品よりも厳格な基準を要求しております。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
192	製品共通	S3.1-47 S3.2-45	ハードウェアの完全性を確実にする	本要件は★4レベル以降が適切だと考えます。	通信機器＆ネットワークカメラともに、市場の標準的な製品に照らし合わせると、 現ドラフト案レベルを満たしているものが少ないと認識しています。 紐付けられている既存制度・文書との整合の観点からも過剰な要求となる可能性があり、本要件の★3での必須化は普及促進の障壁となる懸念があります。 加えて、ネットワークカメラに関しては、屋内設置用途で耐衝撃性能を持つものが少ない認識です。 以上から、重要インフラ施設など、★3より一段上のレベルが適切と考えます。	物理的な破壊・改変行為による脅威は、無視できないと判断したため、削除はいたしません。 ただし、どの程度の対策を取るかについて、具体的な基準を適合要件・評価ガイドにて検討いたします。
193	製品共通	S3.1-02 S3.2-02	①デフォルトパスワードは、IoT機器毎に異なる一意の値で、容易に推測可能でない8文字以上のパスワードであること。	8文字以上としているところNISTの最新の基準に合わせ、パスワードのみで認証する場合15文字以上とすべき	https://www.cybertrust.co.jp/blog/certificate-authority/client-authentication/nist-password-guidelines.html	ベストプラクティスとしてNISTSP800-63B-3に準じる対応としております。 将来15文字とすることを想定し、15文字以上を推奨することをガイドにて説明します。
194	製品共通	S3.1-02 S3.2-02	IoT製品に対するネットワークを介したユーザ認証の仕組みにて、パスワードを使用するIoT製品において、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、以下の①・②のいずれかの基準を満たすこと。	設定可能なパスワードのエントロピーを増やすため、数字、英大小文字、特殊記号を許容する（必ず含めろという意味ではなく）ことを要件とすべき	現状では、英小文字や特殊記号を指定できない機器が散見され、採用する機器ごとのパスワード管理が煩雑である	ベストプラクティスとしてNISTSP800-63B-3に準じる対応としております。 製品の特性に依存するものですので、現状はこのままとします。
195	製品共通	S3.1-05 S3.2-05	IoT製品で使用する電子証明書は、更新可能とすること	電子署名法等の要件を基に、電子証明書を使用する場合の有効期間について5年以下（更新猶予期間を含め6年以下）とする	運用上特別な事情がある場合においても10年以下（更新猶予期間を含め11年以下）とすることを要件とすべき	危殆化した場合に変更可能であることまでを要求し、失効（有効期間）については、具体的な期限を求めておりません。
196	製品共通	S3.1-05 S3.2-05	IoT製品で使用する電子証明書は、更新可能とすること	人手を介さず、機器が自律的に電子証明書を更新する場合、なりすまし困難な手段により機器の真正性を確認する機能を実装することを要件とすべき	機器製造時に耐タンパ領域に格納した認証鍵による認証、署名等が必要と考える	証明書のライフサイクル管理はS3.1-21、S3.2-20で要求しております。セキュアに保存した鍵や証明書を利用して更新することしております。
197	製品共通	S3.1-05 S3.2-05	IoT製品で使用する電子証明書は、更新可能とすること	トラストアンカーの更新時は、二重登録期間（old/new の並存）を設け、後方互換性と安全な切替を担保することの明示	S3.1-19では、ソフトウェアアップデートの完全性・真正性チェックや通信保護に使用される重要なセキュリティパラメータについて、機器ごとに固有であることを要求しています。これは、攻撃の自動化を防ぐ観点で有効ですが、証明書や鍵のライフサイクル管理（発行・更新・失効・ローテーション）については明示されていません。 IoT機器は長期運用されるため、証明書や鍵の有効期限切れ、失効、署名者交代などのイベントに対応できなければ、アップデートや通信の信頼性が失われ、サプライチェーン攻撃や中間者攻撃のリスクが高まります。	証明書のライフサイクル管理はS3.1-21、S3.2-20の中で含まれると考えており、具体的な対応方法については製造業者側で判断いただく形としております。 トラストアンカーの更新に関しては、適合要件・評価ガイドにて記載内容を検討いたします。
198	製品共通	S3.1-12 S3.2-11	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。	① アップデートパッケージは、信頼できる配布元から配布されていることを要件に加えるべき。 　例えば真正性を電子証明書で実装する場合、署名者の証明書チェーン検証（ルート／中間CAを含む）により確認していることを必須要件とする。	S3.1-12は「完全性・真正性」をアップデート時に検証することを要求していますが、証明書のライフサイクル管理やトラストアンカーの更新、配布元の継続的な信頼性保証までは明記していません。	真正性の確認は、証明書の検証に含まれます。具体的な対応方法については製造業者側で判断いただく形としております。 証明書のセキュアな管理については、S1.1-05で要件化しています。
199	製品共通	S3.1-13 S3.2-12	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。	① 適合基準に「リスクアセスメントの実施とエビデンス提出」を明記する。 ②「リスクベースアプローチ」や「サイバーセキュリティケース」などの手法を例示する。 ③ ISO/IEC 27005やIEC 62443-3-2など、国際的なリスク評価規格を参照する。	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により、リスクアセスメントを示唆していると思われる。ガイドラインの適合要件2を参照すると「インシデントレスポンスをハンドリングするための組織体制（PSIRT、インシデント対応体制等）、及び脆弱性情報の収集、トリアージや分析、対策、アップデートなど、一連の対応プロセスや方針が規定されていること。」とあるので、加味されていると想定される一方で、本要求の適合基準だけではそれを判断できない。 S3.1-01においても「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。」としているのにもかかわらず、全体的にリスクアセスメント等によるリスク評価について明示的でない。サイバーセキュリティ対策を実施するにあたって、被害・脅威の分析は必須であり、「サイバーセキュリティケース」「リスクベースアプローチ」といった手法は例示しつつ、評価とそのエビデンスが必須であることを明記するべきである。	JC-STARでは、一定の利用環境や脅威を想定して、製品類型ごとに必要な機能を要求しています。リスクアセスメントなどは別途実施していただくことを想定しています。
200	製品共通	S3.1-15 S3.2-14	3-15. ソフトウェア識別情報及びコンポーネント情報等を含んだ、機 械可読な形式のソフトウェア部品表（SBOM）を作成しなければなら ない。	S3.1-15の適合基準に「②サポート期間内においては、SBOM の情報に基づいて定期的に脆弱性の確認を行い、対応優先度を判断した上で、更新あるいは運用対処等を行うプロセスを有すること。」とありますが、SBOMを作成可能な場合にはSBOMを作成するために使われる元情報を直接用いて脆弱性を確認することも認めていただきたいです（あるいは、そのようなケースもSBOMの情報に基づいた確認とみなしていただきたいです）。	組込みLinuxを作成する際の事実上の標準であるYocto ProjectではSBOM作成とは別に脆弱性チェック（cve-check）の機能がありますが、脆弱性チェックにおいてはSBOM作成を経由することなくSBOM作成にも使われる元情報（Yocto Projectの用語では「レシピ」の情報）を直接使用して脆弱性の該当判定を行います。現時点では組込みLinuxを使用する機器ベンダーでこのような機能も使われていると考えられるため「SBOMの情報に基づいて」の解釈を広くしていただくことで機器ベンダーが実質的な脆弱性確認のプロセスを構築しやすくなると考えます。その場合でもEU CRAとの相互運用を見据えて「SBOM作成が可能であること」という条件をつける必要はあるかと考えます（EU CRAではSBOMを使って脆弱性を確認しないといけないとまでは書かれていないと認識しています）。	★3におけるSBOMについては省庁やIPAの他部門でも方針を検討しており、各関係部門との調整の上で決定する予定となっております。 適合要件２に関しては、元データをもとにSBOMが作成できることを条件として、元データによって脆弱性を管理することを認めることができるか検討いたします。
201	製品共通	S3.1-15 S3.2-14	3-15. ソフトウェア識別情報及びコンポーネント情報等を含んだ、機械可読な形式のソフトウェア部品表（SBOM）を作成しなければならない。	SBOMの作成範囲については、明記し事業者単位で判断させないようにするべき	作成範囲が業者によって変わるため、明確にした方がよい。もしくは最低限記載すべき内容を提示したほうがよいと考える	現時点ではどこまでの範囲とするかは定まっていないため、ベンダーに判断いただくことになります。なお、★3におけるSBOMについては省庁やIPAの他部門でも方針を検討しており、各関係部門との調整の上で決定する予定となっております。これによって今後作成範囲が変わる可能性があります。
202	製品共通	S3.1-15 S3.2-14	3-15. ソフトウェア識別情報及びコンポーネント情報等を含んだ、機械可読な形式のソフトウェア部品表（SBOM）を作成しなければならない。	「定期的に脆弱性の確認を行う」という記載について、長くても1年以内等、具体的な基準を設けるべき。	「定期的に脆弱性の確認を行う」という記載はあるが、期間の定義がなく、長期化すれば脆弱性放置のリスクが高まる。CRAではタイムラインが明確化されており、同様に適合基準に期間の目安（例：月次、重大脆弱性発見時は即時確認）を明記すべき。また、S3.1-13（優先度判断）とS3.1-15（SBOM）の関係性が不明確であり、SBOMを活用した脆弱性評価→優先度付け→アップデートのプロセスを適合基準に明記することで、感覚的な判断を防ぐべき。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。
203	製品共通	S3.1-15 S3.2-14	3-15. ソフトウェア識別情報及びコンポーネント情報等を含んだ、機械可読な形式のソフトウェア部品表（SBOM）を作成しなければならない。	SBOMは脆弱性確認と優先度判断の基盤であり、S3.1-13とS3.1-15の連携を明記すべき。	同上	SBOMについては、S3.1-13で要求する優先度判断及び対処のプロセスに対応する形で、S3.1-15の適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２： 作成したSBOMに基づいて、使用されるコンポーネント（サードパーティコンポーネントを含む）に、脆弱性が含まれる古いバージョンのものが含まれていないかを定期的に確認するプロセスを規定していること。脆弱性が含まれるコンポーネントについては、IoT製品への影響から対応優先度を判断し、更新もしくは運用対処を決定するプロセスを規定していること。
204	製品共通	S3.1-15 S3.2-14	3-15. ソフトウェア識別情報及びコンポーネント情報等を含んだ、機械可読な形式のソフトウェア部品表（SBOM）を作成しなければならない。	CRAのように「脆弱性評価→優先度付け→アップデート」のプロセスを適合基準に組み込むことで、感覚的な判断を防ぐ。	同上	ご意見いただいた内容については、S3.1-15（S3.2-14）およびS3.1-13（S3.2-12）でそれぞれ要求しており、セキュリティ要件全体としては対応されております。
205	製品共通	S3.1-20 S3.2-19	① IoT製品は守るべき情報資産の送信先の正当性を確認する。 ② IoT製品が保護されたネットワーク以外のネットワークを介して守るべき情報資産を通信する場合は、IoT製品が自ら情報の盗聴・改ざんに対する保護対策を行う。	特に②においては、MACアドレスやIPアドレス等通信制御情報による識別は不可とし、なりすまし困難な手法による認証を要件とすべき	IMEI／UDID／ICCID等機器固有情報を基にした代替識別子や事前共有鍵、電子証明書等による認証等	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件２－１： IoT機器が守るべき情報資産を送受信する通信が、保護された通信環境以外を経由する場合においては、以下のA）、B）のいずれかの対策が取られること。 A）CRYPTRECで認められた暗号技術*)を採用した通信プロトコルにて伝送すること。 B）「★1適合基準S3.1-16」の評価項目1に準拠した暗号化をされたうえで保存された守るべき情報資産を復号せずにネットワークを経由して伝送すること。 適合要件２－２： IoT機器が守るべき情報資産を送受信する通信が、保護された通信環境のみを経由する場合においては、保護された通信環境においてのみ使用するようユーザ向けに明示していること、ならびに、以下のC）、D）のいずれかの対策が取られること。 C)CRYPTRECで認められた暗号技術*)を採用した通信プロトコルにて伝送すること。 D)CRYPTRECで認められた暗号技術*)を採用したメッセージダイジェスト、電子署名により守るべき情報資産の改ざんを防止する、又は、CRCコード等により守るべき情報資産の改ざんを防止すること。
206	製品共通	S3.1-31 S3.2-30	7-1. 製品は、セキュアブートメカニズムを使用してそのソフトウェアを検証しなければならない。	稼働中の不正コード検知機能（シグネチャベースまたは挙動検知）を有するようにする。	本書全体で「最小限の原則」は複数箇所に登場しており、マルウェア感染および被害拡大を防ぐ上で有効と考えられます。一方で、マルウェア感染自体を防止する仕組みについては言及がありません。既存要件（S3.1-12、S3.1-13）ではアップデート時や起動時の整合性検証を要求していますが、実行時の検証は明記されていません。IoT機器はストレージを持っているため、管理用PCによるファームウェアアップデート時に、当該PCから二次感染する可能性が否めません。 したがって、起動時だけでなく、実行時検証と不正コード検知・隔離の仕組みを追加することを求めます。	★3の要求では稼働中の不正コード検知機能までを求めないものとします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
207	製品共通	S3.1-36 S3.2-36	11-1. 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。	① 削除機能は適切な権限管理下で実施する ② 監査証跡の完全削除は原則禁止する	「ユーザによって、IoT機器本体や必須付随サービス（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。」として、項目D にログ（テレメトリデータ・監査ログ）が含まれています。 IoT製品利用中にIoT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、ログの削除は慎重であるべきで、容易に削除できるのならば、攻撃が成立した場合のトランザクションログ等も削除されかねない。個人情報等の機微データを判定し適切な権限をもって削除できることが保証されなければならないのではないでしょうか。 ガイダンス文書（パブコメ対象外）を参照すると、「製品特性の維持に必要であり、かつ機器の性能・健全性の保持や確認に必要な情報はユーザーが削除できる情報の対象外」と記載されているが、S3.1-36 の適合基準だけではそれを判断できないのが問題です。	「① 削除機能は適切な権限管理下で実施する」 ご意見いただいた内容については、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 本セキュリティ要件では、 ・他の IoT 機器又はユーザからの守るべき情報資産へのアクセス（読出、書込、更新、削除）において適切な認証に基づいてアクセス制御されていること を要求する。 「② 監査証跡の完全削除は原則禁止する」 ★3（通信機器、ネットワークカメラ）のユースケースにおいて、ユーザが機器の管理者であることを想定しています。管理者が適切な権限において、情報を削除することを妨げないものとします。
208	製品共通	S3.1-10 S3.2-9	④自動アップデート機能を有すること。	自動アップデート機能を要件とすることには反対	インフラシステムにおいては、顧客の要望に応じてアップデートを行うことが主であるため、自動アップデート機能をあえて設けない場合も多い。	自動アップデート機能は管理者側のメンテンナンス上の効率性を鑑みて、要求するものとしております。
209	製品共通	S3.1-12 S3.2-11	アンチロールバックの機能を有すること	ロールバックを許容する条件を設けてほしい	不具合発生時などにあえてロールバックする場合があるため、何らかの条件下で元に戻すことを許容してほしい	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件４： 更新ソフトウェアでアップデートする前に、更新ソフトウェアのバージョンを確認し、現在のバージョンと同じまたは以前のバージョンであることが確認された場合にはアップデートが中止されること。 ただし、本適合要件は、必要に応じて過去のバージョンのソフトウェアをインストールする手段を有することを妨げないが、デフォルトで過去のバージョンの更新ソフトウェアでアップデート可能としてはならない。
210	製品共通	S3.1.15 S3.2.14	①製品出荷後の運用フェーズにおける既知の脆弱性管理のため、製品の構成要素であるソフトウェア（サードパーティコンポーネントを含む）のSBOMを作成し、サポート期間内において更新を行うこと。	サードパーティコンポーネントのSBOM作成はサードパーティベンダに ゆだねるべきで機器ベンダに責任を負わせるべきではない	サードパーティベンダのSBOM作成の義務を機器ベンダに負わせることは、負荷を過大に増やすものである。一方で、OSSなどのSBOM作成については議論の余地あり。	現時点ではどこまでの範囲とするかは定まっていないため、ベンダーに判断いただくことになります。なお、★3におけるSBOMについては省庁やIPAの他部門でも方針を検討しており、各関係部門との調整の上で決定する予定となっております。これによって今後作成範囲が変わる可能性があります。
211	製品共通	S3.1.15 S3.2.14	③サポート期間内においては、SBOMの情報に基づき、使用するコンポーネントのライセンス管理を行うプロセスを有すること。	削除すべき	ライセンス管理の観点は、JC-STARのスコープから外れるため	一般的にライセンス管理は、セキュリティ管理の一部と位置付けらるため、ライセンス管理のプロセスを明確にすることを要求しております。
212	製品共通	S3.1-46 S3.2-44	IoT機器はサービス不能攻撃によるネットワーク過負荷状態から復元の仕組みを有すること。	ネットワーク過負荷状態から復元とは、ネットワーク過負荷が回復したら、機器が正しく動くようにすること。という記載にしてもらいたい。	現状の記載が不明確なため。	いただいたご意見を参考に、適合要件・評価ガイドの記載内容を検討いたします。 なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： IoT機器へのサービス不能攻撃によるネットワーク過負荷状態解消後に、通信が再開されること。 ネットワーク過負荷状態は以下のように用語定義しております。 【用語定義：ネットワーク過負荷状態】 ネットワークに過剰な負荷がかかり、通信機器が正常に動作出来ない状態
213	製品共通	S3.1-30 S3.2-29	ベネトレーションテストやコードレビューなどを通じて安全性が確保されたサードパーティ製コンポーネントのみを組み込まなくてはならない。	OSSなどのサードパーティ製コンポーネントについては、製造者などの属性や開発体制から安全性を判断し、SBOMでの脆弱性管理ができていれば十分で、ペネトレーションテスト・コードレビューなどの要件は削除してほしい	OSSの作成者がペネトレーションテストなどで安全性を確保できているか確認することは困難。また、Linuxのような巨大コンポーネントについて、利用側がペネトレーションテスト・コードレビューすることも非現実的。	SBOMのソフトウェア構成分析（SCA）ツールによる診断であっても要求を満たすことは可能となり、適合要件・評価ガイドの記載内容を検討いたします。なお、パブコメ募集時に参考資料として公開した適合ガイド・評価ガイド（案）において、以下のように記載しております。 適合要件１： 明示的に利用しているサードパーティコンポーネントについて、脆弱性を管理するプロセスが規定されていること。以下はプロセスの例となる。 A) サードパーティからソースコードが提供された場合に、静的アプリケーションセキュリティテスト（SAST）を実施する。 B) サードパーティコンポーネントを含むSBOMを作成し、ソフトウェア構成分析（SCA）を実施する。 C) サードパーティコンポーネントについて、サードパーティから脆弱性情報を入手することを契約により保証する。 D) CVEなど公開された脆弱性情報を収集するツールまたはサービスを利用する。
214	製品共通	S3.1-43 S3.2-41	製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。	第三者とは、別法人であれば関連企業でもよいか。ペネトレーションテストを実施する第三者に要件はあるか。	IEC62443 (SVV-5) では、ペネトレーションテスト実施は independent department or organization となっている。 どこまでの独立性を確保すべきか、またどの程度の能力を持った人によるペネトレーションテストを求めるかを明確化してほしい。	第三者とは、NITEに認定され、かつ、IPAに承認された第三者評価機関となります。 今後公開される規定に条件が記載されます。
215	製品共通	S3.1-43 S3.2-41	製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。	（質問）ガイダンス文書では、ペネトレーションテストは評価機関が実施するとなっているが、第三者＝評価機関　なのか。		第三者とは、NITEに認定され、かつ、IPAに承認された第三者評価機関となります。 今後公開される規定に条件が記載されます。
216	製品共通	ー	ー	（質問）CRAと相互認証をやろうと思うと、製品運用時の脆弱性ハンドリングと報告義務対応が必須になるが、それはどう考えるか。相互認証対象は、★いくつのレベルを想定しているのか。		CRAとの国際連携については、今後、相互認証において検討していくこととなります。
217	製品共通	ー	ー	（質問）★3以上の普及について、業界の調達要件にする等の働きかけをしているのか。重要インフラ事業者、政府調達要件は★３か★４か。いくつのレベルを要求することを想定しているのか。		必要な業界等に対する働きかけは検討していきます。なお、調達においてどのレベルを要求するかについては、調達者が決定することになります。
218	製品共通	S3.1-43 S3.2-41	製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。	ガイダンス文書のペネトレーションテスト要件は、既知の脆弱性検査にデバッグインタフェースの確認を加えた程度であり、ペネトレーションテストと呼ぶには不十分である。脅威ベースのテスト、すなわち既知の攻撃手法を用いた検証が不足しているため、この要件を追加すべきである。もし追加しないのであれば、用語は「脆弱性診断」とすべきである。なお、★3で追加しない場合でも、★4では既知の攻撃手法を用いたテストを必須とすべきである。	NIST SP800-115 ペネトレーションテストの定義より: Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers.	JC-STARではペネトレーションテストとし、その実施概要については、適合要件・評価ガイドの記載内容を検討いたします。
219	製品共通	全て	全て	欠番などを利用し、同じ内容の適合基準の適合基準番号を合わせて欲しい。	製品によって、基準番号が異なると管理が難しい。	セキュリティ要件の番号記載を統一することは運用上困難ですので、現状のままとさせていただきます。
220	製品共通	全て	全て	適合基準番号を順番に並べて欲しい。	S3.1-02が、S3.1-01の前となっている。 同様に、S3.2-02が、S3.2-01の前となっている。	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
221	製品共通	S3.1-44 S3.2-42	指定された言語	「指定された言語」とはどういう定義でしょうか？	参考資料にも定義の記載がなかったので確認です。	適合要件・評価ガイドの記載内容を検討いたします。
222	通信機器	S3.1-02	p.3 評価項目1： 適合要件1 A)～D)の条件に一致しないパスワード	適合要件1を満たすパスワード	「適合要件1 A)～D)の条件に一致しないパスワード」という記載だけだと、「8桁以上のパスワード」の条件が適用されないため。 ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
223	ネットワークカメラ	S3.2-01	p.5 適合要件1：② A) 「★1 適合基準 S1.1-02」	「★3 適合基準 S3.2-02」	番号の誤り。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
224	ネットワークカメラ	S3.2-01	p.5 ※下記は★1 から削除した。ご意見を伺いたい。 E)　通信を許可する対象を IP アドレスなどで制限する機能の実装 F)　通信を許可する対象を LAN 内の機器のみに制限する機能の実装	削除に賛成する。	E)については、IPアドレスの詐称への対策について、 F)については、一度内部ネットワークに侵入を許すと、そのネットワーク内での攻撃や情報漏洩を防げなくなる問題について、 結局のところ、認証機能が必要となる。 ★1では、E)、F)を認めて、 ★3では、E)、F)を認めないという方針は、特に問題ない。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
225	通信機器	S3.1-01	p.6 評価項目1： また、そのアクセス制御の方法が適合要件１の要件を満たすことを確認する。	また、そのアクセス制御の方法が適合要件１・適合要件３の要件を満たすことを確認する。	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
226	ネットワークカメラ	S3.2-03	p.8 評価項目2： 技術文書３に、その認証値を変更する手順が明記されいることを確認する。	技術文書３に、その認証値を変更する手順が明記されていることを確認する。	誤記修正 「明記されいる」→「明記されている」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
227	ネットワークカメラ	S3.2-04	p.10 適合要件1：② 特定の IP からの認証試行の「一定回数※」の連続失敗に対し、…	特定の IP アドレスからの認証試行の「一定回数※」の連続失敗に対し、…	通信機器の記述と合わせるため。 「IP」→「IPアドレス」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
228	ネットワークカメラ	S3.2-04	p.10 ※★3 では、パスワード総当たり攻撃だけでなく、…	注）★3 では、パスワード総当たり攻撃だけでなく、	通信機器の記述と合わせるため。 「※」→「注）」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
229	通信機器	S3.1-05	p.11 適合要件3： あるいは、その他の方法で IoT 製品への認証ができなくする仕組み	あるいは、その他の方法で IoT 製品への認証をできなくする仕組み	ネットワークカメラの記述と合わせるため。 「認証が」→「認証を」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
230	通信機器	S3.1-05	p.12 技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムについて、技術文書２を提出する。 技術文書２：電子証明書・生成メカニズムを使用する認証機能の仕様が記載された文書であり、適合要件１～４のすべてに適合することの根拠が記載されている文書	技術文書２：技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムの仕様が記載された文書であり、適合要件１～４のすべてに適合することの根拠が記載されている文書	「電子証明書・生成メカニズムを使用する認証機能の仕様」 →「技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムの仕様」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
231	ネットワークカメラ	S3.2-05	p.12 技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムについて、技術文書２を提出する。 技術文書２：電子証明書を使用する認証機能・生成メカニズムの仕様が記載された文書であり、適合要件１～４のすべてに適合することの根拠が記載されている文書	技術文書２：技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムの仕様が記載された文書であり、適合要件１～４のすべてに適合することの根拠が記載されている文書	「電子証明書を使用する認証機能・生成メカニズムの仕様」 →「技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムの仕様」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
232	通信機器	S3.1-05	p.12 評価項目3： あるいは、その他の方法で IoT 製品への認証ができなくする仕組み	あるいは、その他の方法で IoT 製品への認証をできなくする仕組み	ネットワークカメラの記述と合わせるため。 「認証が」→「認証を」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
233	ネットワークカメラ	S3.2-10	p.23 適合要件４： ユーザが、IoT 製品ベンダーのウェブサイトからアップデートファイルをダウンロードし、インストールによるアップデートを実行する手順が明示されていること。	ユーザが、IoT 製品ベンダーのウェブサイトからアップデートファイルをダウンロード等の方法により、アップデートファイルを入手し、インストールによるアップデートを実行する手順が明示されていること。	通信機器の記述と合わせるため。 「ダウンロードし、」 →「ダウンロード等の方法により、アップデートファイルを入手し、」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
234	ネットワークカメラ	S3.2-10	p.23 技術文書1： （上記技術文書は、S1.1-06（3-1)の技術文書３と記載すべき内容は同一）	（上記技術文書は、S3.2-09の技術文書３と記載すべき内容は同一）	番号の誤り。 (3-1)は不要。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
235	通信機器	S3.1-11	p.25 技術文書1： （上記技術文書は、S3.1-10（3-1)の技術文書３と記載すべき内容は同一）	（上記技術文書は、S3.1-10の技術文書３と記載すべき内容は同一）	(3-1)は不要。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
236	ネットワークカメラ	S3.2-10	p.23 【ドキュメント評価】 （手動でのアップデートをサポートしない倍は、評価項目1 のみが評価対象となる。）	（手動でのアップデートをサポートしない場合は、評価項目1及び2が評価対象となる。）	誤記修正。評価項目2を追記。または通信機器の記述と合わせて、かっこ書き自体を削除してもいいと考えます。 「倍は、」→「場合は、」 手動アップデートをサポートする場合は評価項目1、2、3が評価対象となるが、 手動アップデートをサポートしない場合は評価項目1、2が評価対象となる。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
237	ネットワークカメラ	S3.2-10	p.23 評価項目3： ソフトウェアコンポーネントをアップデートを実行する手順	ソフトウェアコンポーネントのアップデートを実行する手順	誤記修正 「を」→「の」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
238	通信機器	S3.1-11	p.25 評価項目3： ソフトウェアコンポーネントをアップデート実行する手順	ソフトウェアコンポーネントのアップデートを実行する手順	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
239	ネットワークカメラ	S3.2-11	p.25 適合要件4： 現在のバージョンと同じまたは以前のバージョンであることが確認されてた場合には	現在のバージョンと同じまたは以前のバージョンであることが確認された場合には	誤記修正 「確認されてた」→「確認された」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
240	通信機器	S3.1-12	p.26 適合要件4： 現在のバージョンと同じまたは以前のバージョンであることが確認されていた場合には	現在のバージョンと同じまたは以前のバージョンであることが確認された場合には	誤記修正 「確認されていた」→「確認された」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
241	ネットワークカメラ	S3.2-12	p.28 適合要件3： 複数のステークホルダー	複数のステークホルダー（※） ※： ソフトウェアサプライチェーンのパートナー、製品のサービスに関わるプロバイダ等	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
242	ネットワークカメラ	S3.2-14	p.33 【補足4：SBOM のフォーマットの例】 1)構造フォーマットの例 - CycloneDX - Software Package Data Exchange (SPDX)	- CycloneDX , バージョン1.4 以上 - Software Package Data Exchange (SPDX)、バージョン 2.3 以上	通信機器の記述と合わせるため。 なお、当該文書内にバージョンを明記すると、バージョン変更時に当該文書の改訂が必要になるため要注意。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
243	通信機器	S3.1-16	p.38 技術文書3： 守るべき情報資産のストレージ上での保存の仕様が記載された文書であり、適合要件１～５のいずれかに類する保護対策	守るべき情報資産のストレージ上での保存の仕様が記載された文書であり、適合要件１～６のいずれかに類する保護対策	ネットワークカメラの記述と合わせるため。 「適合要件１～５」→「適合要件１～６」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
244	通信機器	S3.1-16	p.38 評価項目1： 技術文書３に、守るべき情報資産の保護対策が、適合要件1～５のいずれかに類する保 護対策	技術文書３に、守るべき情報資産の保護対策が、適合要件1～６のいずれかに類する保護対策	ネットワークカメラの記述と合わせるため。 「適合要件１～５」→「適合要件１～６」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
245	ネットワークカメラ	S3.2-17	p.40（複数個所） ハードコード	ハードコーティング	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
246	通信機器	S3.1-19	p.43 【重要なセキュリティパラメータ】	【用語定義：重要なセキュリティパラメータ】	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
247	通信機器	S3.1-19	p.43 ★3 適合ガイド（製造業者向け） これらの要求に対して、以下の適合要件を満たすこと。	これらの要求に対して、以下の適合要件１～２のすべてを満たすこと。	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
248	ネットワークカメラ	S3.2-18	p.42 技術文書1： 秘密鍵の生成メカニズムの仕様書	秘密鍵の生成メカニズムが記載されている仕様書	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
249	通信機器	S3.1-20	p.44 ★3 適合基準 ① IoT 製品は守るべき情報資産の送信先の正当性を確認する。	① IoT 製品は守るべき情報資産の通信先の正当性を確認する。	ネットワークカメラの記述と合わせるため。 「送信先」→「通信先」 送信も受信も対象となる。	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
250	通信機器	S3.1-20	p.46 適合要件２－１： B）「★1 適合基準S3.1-16」の評価項目1 に準拠した暗号化	B）「★3 適合基準S3.1-16」の評価項目1 に準拠した暗号化	「★1」→「★3」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
251	ネットワークカメラ	S3.2-19	p.44 適合要件２－１： B）「★1 適合基準S1.1-11」の評価項目1 に準拠した暗号化	B）「★3 適合基準S3.2-15」の評価項目1 に準拠した暗号化	番号の誤り。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
252	ネットワークカメラ	S3.2-20	p.47 【重要なセキュリティパラメータ】 キュリティに関連する情報であって、	セキュリティに関連する情報であって、	誤記修正 「キュリティ」→「セキュリティ」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
253	ネットワークカメラ	S3.2-20	p.48 2）登録・配布（Registration & Distribution） 利用者やシステムに重要なセキュリティパラメータをを配布する。	利用者やシステムに重要なセキュリティパラメータを配布する。	誤記修正 「をを」→「を」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
254	ネットワークカメラ	S3.2-22	p.55 【実機テスト】 以下の評価項目６～８の全てをを満たしていることが確認できた場合に限り、	以下の評価項目６～８の全てをを満たしていることが確認できた場合に限り、	誤記修正 「をを」→「を」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
255	通信機器	S3.1-23	p.57 評価項目6： ii） http/https プロトコルを使用する設定や機能が実装されている場合、URL に一覧 表示される既知の脆弱性CVE-ID に該当する脆弱性が検出されないことを確認する。 [URL] : https://nvd.nist.gov/vuln/search	ii） http/https プロトコルを使用する設定や機能が実装されている場合、下記URL に一覧表示される既知の脆弱性CVE-ID に該当する脆弱性が検出されないことを確認する。 [URL] NIST : NATIONAL VULNERABILITY DATABASE https://nvd.nist.gov/vuln/search [検索条件] Search Type : Advanced Category :「CWE-78 OS Command Injection」「CWE-89 SQL Injection」「CWE-352 Cross-Site Request Forgery (CSRF)」「CWE-22 Path Traversal」「CWE-300: Channel Accessible by Non-Endpoint」 「CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')」「CWE-384: Session Fixation」のすべてを対象とする	ネットワークカメラの記述と合わせるため。 「URL」→「下記URL」 検索条件の追記。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
256	ネットワークカメラ	S3.2-23	p.58 【実機テスト】 評価機関は、実機テストにより評価項目２の評価をの実施する。	評価機関は、実機テストにより評価項目２の評価を実施する。	誤記修正 「をの」→「を」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
257	ネットワークカメラ	S3.2-23	p.58 評価項目２： 技術文書１の一覧にあるセキュリティ関連情報が確認できること、及び一覧に無いセキュリティ関連情報は一切開示されないことを確認する。	技術文書１の一覧にあるセキュリティ関連情報が認証なしで確認できること、及び一覧に無いセキュリティ関連情報は認証なしで一切開示されないことを確認する。	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
258	通信機器	S3.1-26	p.64 【実機テスト】 また、評価項目４の不要なサービスポートの無効化について、要件16-3 の実機テスト結果により評価する。	また、評価項目４の不要なサービスポートの無効化について、S3.1-43の実機テスト結果により評価する。	適合基準番号で記載。 「要件16-3 」→「S3.1-43」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
259	通信機器	S3.1-27	p.65 ★3 適合ガイド（製造業者向け） この要求に関して、以下の適合要件１，２を満たすこと。	この要求に関して、以下の全ての適合要件を満たすこと。	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
260	ネットワークカメラ	S3.2-26	p.63 適合要件１： コードの最小化を行うため、以下のいずれかに類する手法又はそれ以上の手法を採用 していること。 A) 自動化ツールを使用して、デッドコードや未使用のコードを識別し、削除する。 B) パッケージマネージャーを使用して、サービスやソフトウェアの操作に必要なコ ンポーネントのみをインストールする。	コードの最小化を行うため、製品特性に併せて、以下に類する手法を採用していること。 A) 自動化ツール（静的解析ツール、コンパイラ等）を使用して、デッドコードや未使用のコードを識別し、削除する。 B) パッケージマネージャー等を使用して、サービスやソフトウェアの操作に必要なコンポーネントのみをインストールする。	通信機器の記述と合わせるため。 「自動化ツール」 →「自動化ツール（静的解析ツール、コンパイラ等）」 「パッケージマネージャー」 →「パッケージマネージャー等」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
261	通信機器	S3.1-32	p.74 【ドキュメント評価】 評価機関は、製造業者から提供されたドキュメント（ユーザマニュアル等）によって、評価項目１，２の評価を実施する。評価結果が「適合（Y）」の場合にのみドキュメント評価の評価結果は「適合（Y）」となる。	評価機関は、製造業者から提供された技術文書１によって、評価項目１，２の評価を実施する。全ての評価項目の評価結果が「適合（Y）」の場合にのみドキュメント評価の評価結果は「適合（Y）」となる。	ネットワークカメラの記述と合わせるため。 「ドキュメント（ユーザマニュアル等）」→「技術文書１」 「評価結果が」→「全ての評価項目の評価結果が」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
262	ネットワークカメラ	S3.2-32	p.74 適合要件１： 電源OFF となる直前の認証値及びアップデートが維持されていること。	電源OFF となる直前の認証値、アップデート状態及び設定値等が 維持されていること。	通信機器の記述と合わせるため。 「認証値及びアップデート」 →「認証値、アップデート状態及び設定値等」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
263	通信機器	S3.1-33	p.76 技術文書１： IoT 機器の電源供給が停止時のふるまいの仕様	IoT 機器の電源供給停止時のふるまいの仕様	ネットワークカメラの記述と合わせるため。 「電源供給が停止時」→「電源供給停止時」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
264	通信機器	S3.1-34	p.77 ★3 適合ガイド（製造業者向け） バックアップ実施機能　<3か所>	バックアップ機能	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
265	ネットワークカメラ	S3.2-34	p.78 バックアップを実施した直前の構成（設定値、認証値等）	バックアップを実施した直前の構成（バックアップが必要と判断した設定値、認証値等）	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
266	通信機器	S3.1-34	p.78 【実機テスト】 評価機関は、評価項目3 に従ってバックアップ機能が実装されていることを、実機テストにより評価する。	評価機関は、評価項目1, 2に従って確認したバックアップ機能が実装されていることを、実機テストにより評価する。	評価項目番号の誤り。 「評価項目3に従って」→「評価項目1, 2に従って確認した」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
267	ネットワークカメラ	S3.2-34	p.79 【実機テスト】 評価機関は、評価項目１，２に従ってバックアップ機能が実装されていることを、実機テストにより評価する。	評価機関は、評価項目1, 2に従って確認したバックアップ機能が実装されていることを、実機テストにより評価する。	上記に合わせる。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
268	通信機器	S3.1-35	p.80 ★3 適合ガイド（製造業者向け） 本適合基準では、 ・IoT 製品の技術文書において、IoT 製品から収集したログ（テレメトリデータ・監査ログ）を検証するための、セキュリティ上の異常を検知する機能を有すること を要求する。	本適合基準では、 ・IoT 製品の技術文書において、IoT 製品から収集したログ（テレメトリデータ・監査ログ）を検証し、セキュリティ上の異常を検知する機能を有することを要求する。	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
269	ネットワークカメラ	S3.2-35	p.82 評価項目４： 技術文書１、及び４に記載されたセキュリティイベント	技術文書１に記載されたセキュリティイベント	技術文書4が存在しない。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
270	ネットワークカメラ	S3.2-36	p.84 適合要件１： IoT 製品利用中に当該IoT 製品のストレージに保存されたユーザに関する少なくとも以下のA）～C）のすべての情報（データ）を削除するための消去方法を有すること。	IoT 製品利用中に当該IoT 製品のストレージに保存されたユーザに関する少なくとも以下のA）～D）のすべての情報（データ）を削除するための消去方法を有すること。	通信機器の記述と合わせるため。 「D) ログ」も含めるべき。 「A) ～ C)」→「A) ～ D)」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
271	通信機器	S3.1-36	p.83 適合要件１： ただし、ユーザに関する情報であっても、製品特性の維持に必要であり、かつ機器の性能・健全性の保持や確認に必要な情報はユーザが削除できる情報の対象外とする	ただし、ユーザに関する情報であっても、ユーザに公開されないIoT 製品の設定情報（製品特性として必要な情報）及び製造業者がIoT 製品の性能やシステムの健全性を監視するために生成される技術データはユーザが削除できる情報の対象外とする	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
272	通信機器	S3.1-36	p.83 適合要件１： C） ユーザが設定した認証値、IoT 製品利用中に取得した暗号鍵や署名	C） ユーザが設定した認証値、IoT 製品利用中に取得した暗号鍵やデジタル署名	「署名」→「デジタル署名」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
273	ネットワークカメラ	S3.2-36	p.84 適合要件１： C） ユーザが設定した認証値、IoT 製品利用中に取得した暗号鍵や署名	C） ユーザが設定した認証値、IoT 製品利用中に取得した暗号鍵やデジタル署名	「署名」→「デジタル署名」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。

提出意見No.	対象製品	該当箇所		提出意見		提出意見に対する考え方
		要件番号	該当箇所詳細	意見内容	理由	
274	ネットワークカメラ	S3.2-36	p.84 適合要件１： D)　{～～～記載なし～～～}	D) ログ（テレメトリデータ・監査ログ）	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
275	通信機器	S3.1-36	p.84 技術文書１： D)　{～～～記載なし～～～}	D) ログ（テレメトリデータ・監査ログ）	「D) ログ」も含めるべき。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
276	ネットワークカメラ	S3.2-36	p.84 技術文書１： D)　{～～～記載なし～～～}	D) ログ（テレメトリデータ・監査ログ）	「D) ログ」も含めるべき。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
277	ネットワークカメラ	S3.2-36	p.85 評価項目１： 技術文書２に、評価項目1 の消去方法が、データの種類、保存するストレージに応じて適切な消去方法を選定したこと、及びその理由が明記されていることを確認する。	評価項目１： 技術文書２に、技術文書１に記載された全てのユーザに関する情報の消去方法が、データの種類、保存するストレージに応じて適切な消去方法を選定したこと、及びその理由が明記されていることを確認する。	通信機器の記述と合わせるため。 「評価項目1」→「技術文書1」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
278	ネットワークカメラ	S3.2-36	p.85 評価項目４： 技術文書３に記載された手順に従って、ユーザに関する情報の削除を行い、実際にデータが削除されていることを確認する。削除されたことが確認できた場合、本評価項目は「適合（Y)」、削除できていなければ本評価項目は「非適合（Y)」となる。	技術文書３に記載された手順に従って、ユーザに関する情報の削除を行い、実際にデータが削除されていることを確認する。削除されたことが確認できた場合、本評価項目は「適合（Y)」、削除できていなければ本評価項目は「非適合（N)」となる。	誤記修正。 「非適合（Y)」→「非適合（N)」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
279	通信機器	S3.1-37	p.86 適合要件３： デフォルト構成設定への復元が実施された場合、復元以前のユーザに関する情報は適合基準11-1 と同等のレベルで削除されること。	デフォルト構成設定への復元が実施された場合、復元以前のユーザに関する情報はS3.1-36と同等のレベルで削除されること。	「適合基準11-1 」→「S3.1-36」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
280	ネットワークカメラ	S3.2-37	p.86 適合要件３： デフォルト構成設定への復元が実施された場合、復元以前のユーザに関する情報は適合基準11-1 と同等のレベルで削除されること。	適合要件３： デフォルト構成設定への復元が実施された場合、復元以前のユーザに関する情報はS3.2-36 と同等のレベルで削除されること。	「適合基準11-1 」→「S3.2-36」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
281	通信機器	S3.1-37	p.86 評価項目1： 評価項目2： 評価項目3： 機器	IoT製品	「機器」→「IoT製品」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
282	ネットワークカメラ	S3.2-37	p.87 評価項目1： 評価項目2： 評価項目3： 製品	IoT製品	「製品」→「IoT製品」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
283	通信機器	S3.1-37	p.86 評価項目３： 機器を安全なデフォルト構成設定に復元できる機能によってユーザ情報が適合基準11-1 と同等のレベルで削除されること。	IoT製品を安全なデフォルト構成設定に復元できる機能によってユーザ情報が適合基準S3.1-36と同等のレベルで削除されること。	「適合基準11-1 」→「S3.1-36」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
284	ネットワークカメラ	S3.2-37	p.87 評価項目３： 製品を安全なデフォルト構成設定に復元できる機能によってユーザ情報が適合基準11-1 と同等のレベルで削除されること。	IoT製品を安全なデフォルト構成設定に復元できる機能によってユーザ情報がS3.2-36と同等のレベルで削除されること。	「適合基準11-1 」→「S3.2-36」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
285	通信機器	S3.1-38	p.88 適合要件１： 入力データを受け入れて処理するすべてのインタフェースが一覧化されていることのリスト。一覧には少なくとも以下が一覧化されていること。	入力データを受け入れて処理するすべてのインタフェースが一覧化されていることのリスト。当該リストには少なくとも以下が含まれていること。	「一覧」→「当該リスト」 「一覧化されていること」→「含まれていること」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
286	ネットワークカメラ	S3.2-38	p.88 適合要件１： 入力データを受け入れて処理するすべてのインタフェースが一覧化されていること。のリスト。一覧には少なくとも以下がリストに含まれていること。	入力データを受け入れて処理するすべてのインタフェースが一覧化されていることのリスト。当該リストには少なくとも以下が含まれていること。	上記に合わせる。 「一覧化されていること。のリスト。」 →「一覧化されていることのリスト。」 「一覧には少なくとも以下がリストに含まれていること。」 →「当該リストには少なくとも以下が含まれていること。」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
287	通信機器	S3.1-38	p.88 適合要件２： A) 正しいタイプ	A) 正しいタイプ (許可されたデータ形式とデータ構造)	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
288	通信機器	S3.1-38	p.88 適合要件３： IoT 製品において入力検証（Validation）機能が、仕様通りに動作していること。	適合要件３： IoT 製品において入力検証（Validation）機能が、仕様通りに無効で不正なリクエストを拒否する機能が動作していること。	ネットワークカメラの記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
289	通信機器	S3.1-39	p.90 ★3 適合ガイド（製造業者向け） 個人データ　<4か所>	個人情報	ネットワークカメラの記述と合わせるため。 「個人データ」→「個人情報」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
290	ネットワークカメラ	S3.2-39	p.92 評価項目３： 評価項目１，２の記載内容について、専門用語等を多用せず平易で理解しやすい表現で示した情報であることを確認する。	技術文書1の記載内容について、専門用語等を多用せず平易で理解しやすい表現で示した情報であることを確認する。	通信機器の記述と合わせるため。 「評価項目1, 2」→「技術文書1」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
291	通信機器	S3.1-42	p.94 ★3 適合基準 IoT 製品から得られた個人情報が処理される場合、IoT 製品は収集や処理の範囲を限定する機能および不要になった個人情報を削除する機能を有すること。	IoT 製品から得られた個人情報が処理される場合、IoT 製品は収集や処理の範囲を限定するために、不要になった個人情報を削除する機能を有すること。	ネットワークカメラの記述と合わせるため。 「収集や処理の範囲を限定する機能および」 →「収集や処理の範囲を限定するために、」 「収集や処理の範囲を限定する機能」は議論されていない。	いただいたご意見を参考に、セキュリティ要件を修正いたしました。
292	通信機器	S3.1-42	p.95 ★3 適合ガイド（製造業者向け） 個人データ　<1か所>	個人情報	ネットワークカメラの記述と合わせるため。 「個人データ」→「個人情報」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
293	ネットワークカメラ	S3.2-41	p.94 {～～～記載なし～～～}	【ドキュメント評価】 無し	通信機器の記述と合わせるため。	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
294	通信機器	S3.1-43	p.97 評価項目３： なお、物理的にアクセス可能なデバッグインタフェースには（21-1）の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。	なお、物理的にアクセス可能なデバッグインタフェースにはS3.1-47の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。	「（21-1）」→「S3.1-47」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
295	ネットワークカメラ	S3.2-41	p.95 評価項目３： なお、物理的にアクセス可能なデバッグインタフェースには（21-1）の適合要件１もしくは２を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。	なお、物理的にアクセス可能なデバッグインタフェースにはS3.2-45の適合要件１もしくは２を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。	「（21-1）」→「S3.2-45」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。
296	ネットワークカメラ	S3.2-41	p.95 評価項目４： IoT 機器から不正な通信（通信先一覧以外への通信）が検出されないこと。	IoT 機器からの不正な通信（通信先一覧以外への通信）が検出されないこと。	通信機器の記述と合わせるため。 「IoT 機器から」→「IoT 機器からの」	いただいたご意見を参考に、適合要件・評価ガイドの修正を検討いたします。