セキュリティ要件適合評価
及びラベリング制度（JC-STAR）
★1 評価補足ガイダンス

令和 7 年 5 月 22 日版

独立行政法人情報処理推進機構

目次

はじめに

本補足ガイダンスは、「★1 レベル適合基準・評価手法（JST-CR-01-01-2024/2024R1）」及び「★1 評価ガイド（JST-EG-01-01-2024/2024R1）」に記載された評価手法で求められる評価内容や評価項目の解釈等について、発行後にいただいた質問への回答等を中心に補足・追記するものです。

次回の評価ガイド改訂時に組み込まれる場合もありますが、速報として取りまとめていますので、評価ガイドと合わせて参考にしてください。

改訂履歴

改訂日	内　容
2025.05.22	初版公開

【★1 適合基準の考え方】

【質問 00-1】

★1 評価ガイド 2.4 章 「守るべき（保護すべき）情報資産の考え方」において【★1 での守るべき情報資産】の例としてあげられている「IoT 機能（通信機能）に関する設定情報」は、具体的にはどのような情報を想定しているでしょうか？

Appendix A 用語説明には、無線通信での事例として WiFi の SSID や WPA 暗号キーが例示されていますが、IoT 機器を制御するための制御サーバや情報サーバの IP アドレスやホスト名などの設定情報も該当すると判断するべきでしょうか？

【ガイダンス】

「通信機能に関する設定情報」は、IoT 機器の運用中に通信機能を使う上で利用される設定情報すべてを想定しています。

また、「保護」とは「機密性の保護」だけを意味するのではなく、「完全性の保護」や「真正性の保護」もあります。それぞれの設定情報について、機密性、完全性、真正性の観点からどのような保護が必要かを判断し、必要な対策を行うことが求められます。ただし、検討の結果、保護までは必要としない設定情報と判断されることもあり得ます。

例えば、同じ IP アドレスであっても「保護すべき設定情報」と「保護までは必要としない設定情報」に分かれる可能性があります。前者の例としては、IoT 機器から制御サーバの IP アドレスが読み取られた場合、次に制御サーバに対して攻撃してくるかもしれないという意味において、「アップデートファイル提供サーバ」の IP アドレスなどが該当する可能性があります。一方、後者の例としては、IP アドレス自体が公知となっている「公開サーバ」の IP アドレスなどが該当すると考えられます。

このように、通信機能に関する設定情報であっても、製品の状況や設定情報の種類等により保護を必要とする設定情報であるかどうかが変わると考えられますので、「通信機能に関する設定情報」は「**保護の必要性を検討すべき情報の候補**」としてとらえ、その中から「**ベンダーの責任において保護の必要がある設定情報を選定**」してください。

保護の必要があると判断した設定情報については、適切な保護手段を適用ください。また、保護までは必要ないと判断した設定情報については、必要がないと判断した根拠・理由を証跡として技術文書等に残しておいてください。

【質問 00-2】

★1 評価ガイド 2.4 章「守るべき（保護すべき）情報資産」の例に挙げられている情報資産は全て保護しなければならないのでしょうか？

また、「機器が収集し、保存又は通信」する情報の一部に「一般的に機密性が高い情報」が含まれる場合、それ以外の情報を含めて「守るべき（保護すべき）情報資産」として扱う必要がありますか？

【ガイダンス】

「守るべき（保護すべき）情報資産」の例に挙げられている情報資産は「**保護の必要性を検討すべき情報の候補**」を示したものであって、そこに挙げられている全ての情報資産を保護しなければならないということではありません。機器が収集する情報の性質に応じて、「**ベンダーの責任において保護を必要とする情報資産であるかどうかを検討**」し、「**保護の必要がある情報資産を選定**」してください。保護の必要があると判断した情報資産については、適切な保護手段を適用ください。また、保護までは必要ないと判断した情報資産については、必要がないと判断した根拠・理由を証跡として技術文書等に残しておいてください。

上記に関連する内容として、機器が収集、保存又は通信する情報の一部に「一般的に機密性が高い情報」が含まれる場合には、当該機器の主たる利用環境や利用目的に照らして、その機器が収集、保存又は通信する情報の中にどの程度「一般的に機密性が高い情報」が含まれるかを踏まえて、ベンダーの責任において「守るべき（保護すべき）情報資産」として扱うかどうかを判断することができます。

例えば、一般消費者向けの機器であり、その機器の主たる利用環境や利用目的に照らせば、当該機器が収集、保存又は通信する情報の大半は「一般的に機密性が高いには該当しない情報」であると合理的に想定できるのであれば、たとえ「一般的に機密性が高い情報」を含む可能性があっても、当該機器が収集、保存又は通信する情報すべてを保護を必要としない情報資産であると判断してもかまいません。一方、企業向けの機器であり、当該機器が収集、保存又は通信する情報の中に「一般的に機密性が高い情報」が無視できない程度に含まれると想定されるのであれば、当該機器が収集、保存又は通信する情報すべてを保護を必要とする情報資産であると判断すべきです。

【質問 00-3】

利用者が設定を変更することにより利用可否を変更できる機能について、チェックリストではどこまでを確認する必要がありますか？

【ガイダンス】

チェックリストでの適合評価をする必要がある機能は**デフォルト設定で有効**となっているものとし、デフォルト設定で無効化されているものは対象外とします。

ただし、設定変更を説明する箇所（例えばマニュアルなど）に、デフォルト設定で無効化されているものを有効化した場合のリスクや機能制限など、セキュリティ上の注意が利用者にわかるように明示ください。

【質問 00-4】

「必須付随サービス」に対して求められる評価項目は以下でよいでしょうか？

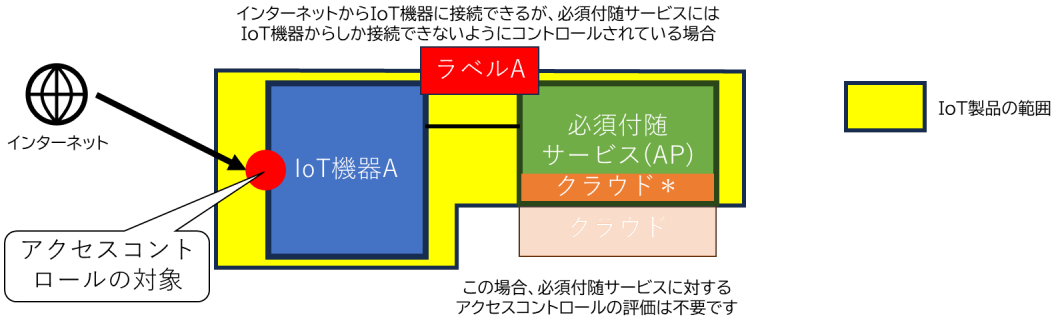
- ラベル取得対象 IoT 機器からアクセスされる「必須付随サービス」上の「守るべき情報資産」への認証保護

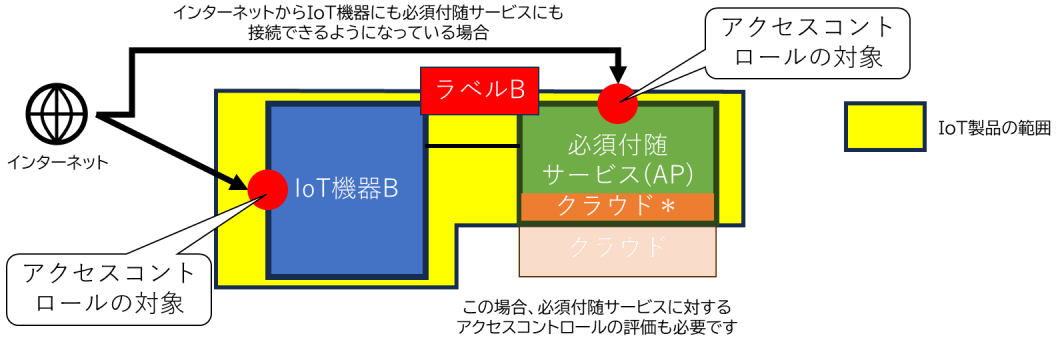
- 「必須付随サービス」にストレージされる「守るべき情報資産」の保護
- インターネットを介するラベル取得対象 IoT 機器と「必須付随サービス」との通信の盗聴対策
- 「必須付随サービス」上のデータ削除

【ガイダンス】

「必須付随サービス」に**インターネット側から直接アクセス可能かどうか**で異なります。インターネットから直接「必須付随サービス」にアクセスできるとは、例えば、外出先からインターネットを経由してクラウド上などで提供される必須付随サービスにアクセスし、必須付随サービスから IoT 機器を操作するなどの形態を想定したものです。この場合、必須付随サービス側にもアクセスコントロールが必要となります。

したがって、IoT 機器側からしか必須付随サービスにアクセスできないのであれば上記の 4 つの評価が対象となりますが、インターネット側からも必須付随サービスに直接アクセス可能な場合には「必須付随サービス」側でのアクセスコントロールについても評価の対象に含める必要があります。





【質問 00-5】

評価項目では、「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」に記載されたアルゴリズムとの記載がありますが、他のリストを使ってはいけないのでしょうか？

また、暗号技術のセキュリティ強度についての指定が無いと考えてよいでしょうか？あるいは、CRYPTREC の「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」内の(https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf)に従う必要があるでしょうか？

【ガイダンス】

CRYPTREC 暗号リストのうち、「電子政府推奨暗号リスト」のほか、「推奨候補暗号リスト」に記載されたアルゴリズムを採用することは可能です。「運用監視暗号リスト」は互換性維持のための継続利用として認められたアルゴリズムですので、できるだけ採用しないようにしてください。

また、暗号技術のセキュリティ強度については、「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」に必ず従ってください。CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に記載されていたアルゴリズムを採用したとしても、「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」に従った使い方になっていない場合には、「電子政府推奨暗号リストのアルゴリズムを利用しているとは見なさない」と注意書きがされています。

【質問 00-6】

マニュアルやホームページ等を利用した利用者への周知について、代行申請企業が実施することができますか？それとも、申請企業がしなければなりませんか？

【ガイダンス】

原則として、**申請企業が行う**必要があります。

ただし、申請企業からの委託を受けて代行申請企業が**日本国内での販売を独占的に実施している場合に限って**当該代行申請企業が対応することで構いません。チェックリストでは、その旨を説明してください。

【質問 00-7】

IP 通信を行っていない機器で、TCP ポートは無いのですが未使用の USB/Bluetooth/D-sub などを有している機器は対象となりますか？

【ガイダンス】

IP 通信ができなければ対象外です。ただし、TCP ポートがなくても USB や Bluetooth などを通じて IP 通信ができる場合には対象となる場合があると考えられます。

【質問 00-8】

「製品運用時の物理的接触」には、製品デバイスの操作パネルや、NFC のような近接距離通信による接触も含まれますか？

【ガイダンス】

「製品運用時の物理的接触を想定しない」とは、接触方法の種類のことではなく、攻撃者が当該製品の近くに侵入しない（つまり、運用中の装置に攻撃者が操作パネルや NFC、USB を直接触ることはない）という意味です。そのような環境が整備されていることを前提とします。

一方、「廃棄時の物理的接触」には、製品デバイスの操作パネルや、NFC のような近接距離通信による接触も含まれますので、それらに対する対策が必要です。

【質問 00-9】

“(4)潜在的攻撃点”にある”故障や悪用で危害を及ぼす機能”への攻撃手段は、インターネット経由の攻撃だけに限られたケースと考えて宜しいでしょうか？

【ガイダンス】

★1 ではインターネット経由の攻撃を想定してください。

【質問 00-10】

ホームページにて必要な情報を周知する予定ですが、適合ラベルの申請時にはまだ当該ホームページができていない場合、ホームページが完成してからしか申請できませんか？それとも、掲載予定の URL 情報などを提示し、「掲載予定」としてチェックリストに回答しても問題無いでしょうか？

【ガイダンス】

掲載予定の URL 情報などを提示し、「掲載予定」でも構いません。

その際、いつ頃掲載する予定かのスケジュールも合わせて記載ください。

【★1 適合基準 S1.1-01】

【質問 01-1】
NFC ツールを利用したアクセス制御は、適切な認証に基づくアクセス制御が行われていると解釈してよいでしょうか？

【ガイダンス】

NFC ツールが物理的所持による認証として機能し、NFC ツールがなければ IP 通信を介した守るべき情報資産へのアクセスができない仕組みであれば、「②以下のいずれかに類する実装又はそれ以上の実装であること」のそれ以上の実装によるアクセス制御が行われていると認められます。

一方、「IP アドレス変更には NFC 利用」が必要であっても、「（NFC ツールを利用しなくても）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」ができるのであれば、「NFC 利用」は「適切な認証に基づくアクセス制御」とみなすことはできません。

【★1 適合基準 S1.1-02】

【質問 02-1】
IoT 製品導入時にデフォルトパスワードが【使用されない】（＝適合要件としては対象外と読める）が、ネットワークを介したパスワード利用したユーザ認証の仕組みが【ある】（＝対象外(NA)になる条件を満たさない）ケースをどう判断すればよいでしょうか？

【ガイダンス】
デフォルトパスワードが使用されない場合は「空白（つまり、長さ 0 文字のパスワード）のデフォルトパスワードが使用されている」と判断して評価を実施してください。

【質問 02-2】
IoT 機器ベンダーが設置前にパスワードを設定し、利用者はそのパスワードを知らず、かつ利用者側では機器のメンテナンスも実施しない場合、デフォルトパスワードの設定ルールに関する本適合基準は対象外となるでしょうか？

【ガイダンス】
対象外にはなりません。補足説明　例外的なケースでの適合判断　2.2.1.管理者およびカスタマーエンジニアの認証を参照ください。

【質問 02-3】
デフォルトパスワードの代わりに NFC ツールを利用して接続情報の設定をしてからしか接続できない機器の場合、パスワード変更を要求しなくても基準②を満たしていると解釈してよいですか？

【ガイダンス】
「NFC 利用によるアクセス制御」と「パスワード利用によるアクセス制御」は別物として扱います。
つまり、「NFC 利用」しなければアクセスできない（パスワードを一切利用しない）構成であれば「ネットワークを介したパスワード利用したユーザ認証の仕組み」が存在しないため、本適合基準は対象外と判断されます。
一方、「ネットワーク経由で（NFC を利用しなくても）パスワード利用」してアクセスできる構成であれば「ネットワークを介したパスワード利用したユーザ認証の仕組み」が必要です。この場合のデフォルトパスワードは 0 文字パスワードと解釈し、基準②に記載の仕組みがなければ評価項目 2 が非適合となります。

【★1 適合基準 S1.1-03】

【質問 1】

IoT 機器の認証画面には、ネットワークを介してアクセス可能ですが、このネットワークが閉域網（VPN-SIM）を介したものであり、不特定多数からのアクセスができるネットワークではない場合に、NA に該当するでしょうか？すなわち、「IoT 機器に対するネットワークを介したユーザ認証の仕組みがない」の「ネットワーク」とは、どのようなネットワークでしょうか？

例えば、リモートからは VPN-SIM を経由（閉域網を経由）し、ローカルのネットワークは施錠・管理された建屋内の有線ネットワークであり、建屋内に侵入し、直接機器を触らない限りは、認証画面にアクセスできない構成である場合は、どのように判断できるでしょうか？

【ガイダンス】

以下の条件をすべて満たす場合に限り、例外的に、ネットワークを介したユーザ認証の仕組みがない機器として「対象外（NA）」とすることができます。この場合、「対象外（NA）」と判断した根拠を証跡（エビデンス）に明記しておく必要があります。

① ネットワークを介する場合、閉域網（VPN-SIM）を介してのみ接続ができることが確認されていること。

② 当該 IoT 機器を「ネットワークを介して利用する場合には、閉域網（VPN-SIM）を介して接続する」旨の注意が明示されていること。

【★1 適合基準 S1.1-04】

【質問 04-1】
総当たり攻撃を困難にする対策は、例えば VPN 接続でインターネットを経由した外部からのアクセスに対してブロックしている場合でも、必要な機能（基準）となりますか？

【ガイダンス】

以下の条件をすべて満たす場合に限り、例外的に、ネットワークを介したユーザ認証の仕組みがない機器として「対象外（NA）」とすることができます。この場合、「対象外（NA）」と判断した根拠を証跡（エビデンス）に明記しておく必要があります。

① ネットワークを介する場合、閉域網（VPN）を介してのみ接続ができることが確認されていること。

② 当該 IoT 機器を「ネットワークを介して利用する場合には、閉域網（VPN）を介して接続する」旨の注意が明示されていること。なお、通常は利用者に対して周知するものですが、VPN 接続の設定メンテナンスを実施できる者が設置事業者やカスタマーエンジニア、システム管理者に限定される仕組み（例えば、施錠管理されている、設置時に組込みなど）を有している場合には、技術文書として証跡に残すことでも OK とします。

【質問 04-2】
古いモデルとの互換性を維持するために残している機能（デフォルトの設定では無効）は実機テストの対象外でしょうか？

【ガイダンス】

デフォルト設定で無効化されているものは実機テスト対象外とします。

ただし、設定変更を説明する箇所（例えばマニュアルなど）に、設定変更をした場合のリスクや機能制限など、セキュリティ上の注意が利用者にわかるように明示ください。

【質問 04-3】
認証試行制限の機能は有しているが、デフォルトで有効となっていない場合、ユーザに対して追認試行制限の有効化を推奨する記載がユーザ向けマニュアル等に書かれていれば適合の判断になりますでしょうか？

【ガイダンス】

S1.1-12 補足説明 2.2.2 と同様の考え方とします。つまり、原則としてデフォルトで有効化されていない場合は非適合になります。例外として「設置時に工事設置業者やシステム管理者が有効化する処理を同時に行う」場合に限り、説明でも適合とすることができます。

【質問 04-4】

評価項目 1 において、ネットワークを介したユーザ認証の連続失敗に対する認証試行制限の対応として、以下の 3 つの方法が示されています。

A） 追加の認証禁止

B） 認証の一定期間停止

C） 認証応答発行の一定時間遅延

こちらの対応について、A～C のすべてを実施する必要があるのでしょうか？それとも、いずれか 1 つを選択して実施すればよいのでしょうか？

【ガイダンス】

いずれか一つでも実装されていれば適合となります。

【★1 適合基準 S1.1-05】

【質問 05-1】
IoT 機器の脆弱性開示について、契約をした利用者にのみ IoT 機器を配布する場合、契約する利用者への個別開示の形でもよいでしょうか？

【ガイダンス】
契約者への個別配布でも OK とします。ただし、チェックリストには、その根拠として契約者への配布だけでよいことの理由も一緒に記載ください。また、申請書の脆弱性開示ポリシーURL の欄には「契約者限定配布製品のため、情報非公開」と記入してください。

【質問 05-2】
海外製品の代理申請にあたって、日本国内向けのホームページは代理申請会社が管理しているため、代理申請会社のホームページ内に脆弱性開示ポリシーを掲載することでもよいでしょうか？

【ガイダンス】
日本語としての参考情報をして、代理申請会社のホームページに掲載していただくことは可能です。ただし、脆弱性開示ポリシーの原文は申請会社のホームページに掲載されていることとその情報へのリンク、及び、実際の対応として代理申請会社が（日本語での）どのように対応するのかについて、追加で説明を載せてください。

【質問 05-3】
善意の報告に対する法的免責付与の宣言とはどのようなものですか？

【ガイダンス】
脆弱性を報告してもらうために、どこまでの行為を免責範囲として許容するのかを製造ベンダーが宣言することです。その範囲内の行為であれば、法的措置がとられないことを保証することが期待されます。

【★1 適合基準 S1.1-06】

【質問 06-1】

ファームウェアパッケージのバージョン確認について、粒度感としては製品(全体)を見れば問題ないでしょうか？

【ガイダンス】

申請書に記載いただくファームウェアがバージョン確認の対象となります。

一方、申請書に記載していないファームウェアについてはバージョン確認の対象外です。

【質問 06-2】

★1 では OSS 等のパッケージ毎のバージョン確認まで必要でしょうか？

【ガイダンス】

申請書に記載したファームウェアのバージョン確認が必要になります。そのファームウェアが複数あったり、OSS であったりした場合でも同様に全てのバージョン確認が必要です。

【★1 適合基準 S1.1-07】

【質問 07-1】
ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすることとありますが、保守要員や製造メーカ側でアップデートを管理する場合は対象外との理解でよいでしょうか？

【ガイダンス】
対象外にはなりません。
ただし、保守要員等が実際に実行・管理するアップデート手順を整理しておくことで適合とすることができます。

【質問 07-2】
要件に「製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。」とありますが、セキュリティ要件適合評価及びラベリング制度（JST-CR-01-01-2024/2024R1）の P5 の下部に、IoT 機器とは利用者自身が機器に対して SW のインストールなど容易にセキュリティ対策を追加するのが困難なものと定義されています。整合性が無いように見受けられるのですが、どのように解釈すればよいでしょうか？

【ガイダンス】
アップデートは不具合・脆弱性対応のための【製品の基本機能】としてユーザ（又は保守要員等）が実施できることを求めています。特に、ユーザがアップデートを実施する場合には容易にアップデートが実施できるようにしなければならない、というのが S1.1-07 の意味です。一方、セキュリティ対策を追加するのが困難という条件は、【別の対策ソフトウェア等を当該製品に組み込むことができない／困難】という意味です。
つまり、前者は IoT 製造ベンダー自身の責任で当該 IoT 製品に対して供給されるもの、後者は当該IoT製品に対してIoT製造ベンダー以外のものが利用できるものという違いがあり、それらに対して、前者はユーザが容易に適用できるが、後者は適用困難ということです。

【質問 07-3】
適合基準で指す、セキュリティソフトとは、本制度のセキュリティ要件を満たすべき機能・処理を具備するソフトウェアを示すとの解釈で正しいでしょうか？

【ガイダンス】
簡単な考え方は、はじめから IoT 機器に入っているソフトウェア（試供品やインストーラ等は除く）は IoT 製造ベンダーが利用するものを特定していることから、「顧客によるセキュリティ機能の追加」とはみなさず、IoT 製造ベンダーの管理下で「具備された（具備される）セキュリティ機能」とみなします。これは、そのようなソフトウェアであれば、IoT 製造

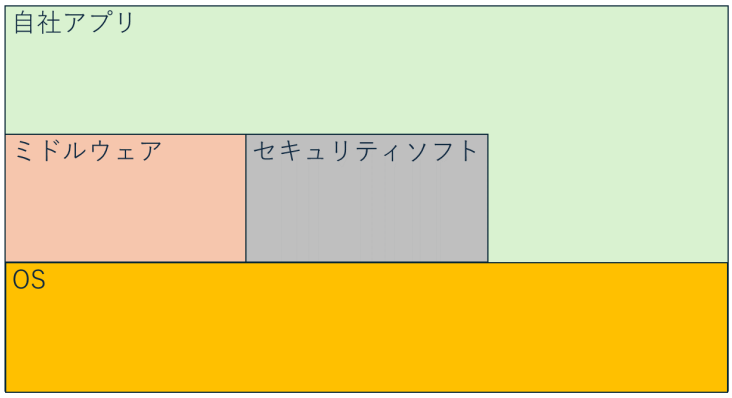
ベンダーからアップデートファイルの提供が何らかの形で保証されていたり、代替のアップデート方法が提供されるなどによって、IoT 製造ベンダーがサポート状況を把握でき、利用者は一律にアップデートを受けられることを想定しているためです。

一方、サードパーティが作成するソフトウェアについては、利用者の利用状態がバラバラであり、IoT 製造ベンダーがサポート状況を把握できません。したがって、このような場合は「顧客自身によるセキュリティ機能の追加」に当たり、本制度の対象外になります。

なお、当初から搭載された OS アップデート機能は「自らの意志で（セキュリティ機能を追加）」に該当せず、「自動的に（アップデートが実行）」に該当します。確かにキャンセルを選択することはできますが、意図的にキャンセルをしない限り、アップデートが強制されるためです。

以下、具体例を用いて説明します。

図 1　IoT 機器のソフトウェア構成



※　ミドルウェア、セキュリティソフト、OS は汎用ソフトウェアを使用するものとします。（例：OS：Windows、ミドルウェア：SQL サーバ、セキュリティソフト：ウィルスバスター等）

セキュリティソフトの実装例

＃A：★1 セキュリティ要件を実施する機能を全て自社アプリで実現
セキュリティアップデートは全て IoT 機器ベンダーが提供

＃B：★1 セキュリティ要件を実施する機能をセキュリティソフト（汎用）で実現
セキュリティアップデートは利用者が自らの意思でアップデート版セキュリティソフトを適用可

＃C：★1 セキュリティ要件を実施する機能が全て OS(汎用)で実現
セキュリティアップデートは利用者が自らの意思でアップデート版 OS を適用可
ただし、アップデート方法は、IoT 機器ベンダーから提供された手順で実施する必要がある

＃D：★1 ラベル セキュリティ要件を実施する機能が自社アプリと汎用 OS で実現

要件を実現するセキュリティ機能が、ベンダーから提供される自社アプリと、汎用OS と複数から構成される場合であり、求められるセキュリティアップデート内容によって、調達者・利用者が自らの意思でアップデートできる場合とできない場合とがある

＃E：★1 ラベル セキュリティ要件を実施する機能が自社アプリ以外で実現
セキュリティアップデートは、利用者が自らの意志で市販されるアップデート版ソフトウェア（セキュリティソフト、ミドルウェア、OS）を適用可
汎用 OS やミドルウェアは、アップデート適用にあたりベンダーからの注意事項を留意の上、実施しないといけない制約がある。（例：アップデート時／後のアプリ操作等）

「セキュリティ機能を含む」ファームウェア（ソフトウェア）のサポートを要求しますので、#A は対象となります。

#B と#E は、セキュリティソフトを利用者が入れるものであるならば IoT 機器ベンダーはセキュリティ機能に関し何ら関与していないので対象外になります。ただし、当該セキュリティソフトを製品コンポーネントとして固定的に組み込むものであるならば、「セキュリティ機能を含む」ファームウェア（ソフトウェア）として別会社から供給を受けるコンポーネントを組み込んでいるとみなし、対象となります。

#C と#D は、アプリの動作上、OS を IoT 機器ベンダーが関与して特定したはずなので、IoT 機器ベンダーの管理下で具備されたものとみなし、対象となります。

【★1 適合基準 S1.1-08】

【質問 08-1】

- ソフトウェアの完全性を確認する手段として、独自の差分ファイル形式と CRC チェックの組み合わせにより、S1.1-08 の評価基準に適合することは可能でしょうか？
- S1.1-08 の評価基準に適合するためには、ファームウェアをハッシュ値、もしくはデジタル署名による暗号化が必須なのでしょうか？

【ガイダンス】

他国（欧米、シンガポール等）の類似制度との相互承認に向け、それらの制度での技術要件と同等にしておくことが望ましいと考えています。このため、アップデートファイルの完全性確認で利用するメカニズムは「暗号技術」を利用するものとします。CRC は「暗号技術」として認められていませんので、評価基準不適合として扱います。

【質問 08-2】

アップデートソフトウェアのダウンロードには HTTPS 通信を利用し、ダウンロードしたソフトウェアの完全性を確認する手段として CRC チェックを利用する場合、その組み合わせにより、S1.1-08 の評価基準に適合することは可能でしょうか？

【ガイダンス】

アップデートファイルが HTTPS などの安全性が確保された通信路を利用して伝送される場合には、インストール前の完全性確認は CRC チェックでもよいものとします。

その場合、チェックリストには、完全性の確認メカニズムとして

- HTTPS 通信を利用してアップデートファイルをダウンロード＜＝アップデートファイルのダウンロード開始時から完了時まで間の改ざん防止＞
- アップデートファイルの完全性はチェックサムで検証＜＝アップデートファイルの作成～ダウンロード開始時までのエラー防止＞

の両方を明記してください。また、その場合の S1.1-08 評価項目 5 の暗号技術についての確認は HTTPS 通信で利用する暗号技術について評価します。

その両方の記載があることで、アップデートファイルの作成からダウンロード完了時までの改ざん防止が確保され、デジタル署名やハッシュ関数での検証と同程度の完全性が担保されることになりますので、評価基準適合とします。

【★1 適合基準 S1.1-09】

【質問 09-1】
　質問なし

【ガイダンス】
　―

【★1 適合基準 S1.1-10】

【質問 10-1】
　質問なし

【ガイダンス】
　―

【★1 適合基準 S1.1-11】

【質問 11-1】

経済産業省のサイトで公開されていたチェックリストの★1 評価ガイドでは“守るべき情報資産は、「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」に記載のハッシュ関数によってハッシュ化された上で保存される。”という記載がありましたが、これが削除されています。

この結果、パスワードの機密性を保護するためにハッシュ化して保存する方法が使えなくなったように読めますが、この理解は正しいでしょうか？

【ガイダンス】

パスワードの機密性を保護するためにハッシュ化して保存する方法が使えなくなったわけではありません。パスワードの機密性を保護するためにハッシュ化して保存する方法は、評価項目 1 に適合しているとみなすことができます。

【質問 11-2】

Linux 等を採用している IoT 機器で、Wi-Fi などのネットワーク接続の設定に NetworkManager を使用している場合、NetworkManager はネットワーク接続情報（Wi-Fi の SSID やパスワードなど）を平文でファイルシステム上に保存します。(ただし、このファイルへのアクセス権限は root ユーザにのみ与えられるため、一定の保護はされているとも言えます)

Wi-Fi の SSID 及びパスワードを機密性を守るべき情報資産と考えた場合、これらの情報は暗号化した上で保存・使用すべきなのでしょうか？

【ガイダンス】

適切なアクセス制御がされている場合、S1.1-11 評価項目 5「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」に類する保護対策が利用されているものとします。

特に「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。」を「パスワードなどによって保護されたアカウントにアクセスを制限するアクセスコントロールによって保護された領域に保存されること」と解釈できることとします。

そのため、NetworkManager の管理する情報の機密性を確保するためには、root だけでなく、一般ユーザのアカウントも保護する必要があります。例えば、NetworkManager を操作するコマンド nmcli の実行に root 権限を要求する設定変更を合わせて行ってください。

【質問 11-3】

「IoT 製品のストレージに保存される守るべき情報資産（SD カード等、ストレージメディアに保存される守るべき情報資産も含む。）は、セキュアに保存されること」について、

- NAS に保存されるユーザのファイルデータは、一般的に NAS のファイルシステム上に暗号化されずに保存されます(HDD を取り出して他の PC に接続してデータを読み出すことは可能)が、★1 を取得するために暗号化は必須でしょうか？
- NAS に外付け USB ドライブを接続して、ユーザのファイルを保存する場合、一般的にユーザが他の PC に該当外付け USB ドライブを接続することにより参照できるようになっていると思いますが、暗号化を実施するとそれが困難になります。このような場合にも★1 を取得するために暗号化は必要でしょうか？

【ガイダンス】

NAS に関しては、すでに暗号化対応できる製品が数多く発売されておりますので、デフォルトでの暗号化対応を必要とします。

ただし、ユーザが自らの意志で暗号化解除できるような設定を設けることを妨げるものではありません。その場合、設定変更の方法を説明する箇所（例えばマニュアルなど）に、暗号化されていない場合のリスクなど、セキュリティ上の注意が利用者にわかるように明示してください。

なお、実機テストの範囲はデフォルトで有効化されている部分に対してとします。

【質問 11-4】

「IoT 製品のストレージに保存される守るべき情報資産（SD カード等、ストレージメディアに保存される守るべき情報資産も含む。）は、セキュアに保存されること」について、

- NW カメラに SD カードを取り付けて映像データを保存するとき、PC 等で再生可能な映像フォーマットで暗号化せずに保存しますが、暗号化を実施するとそれが困難になります。このような場合にも★1 を取得するために暗号化は必要でしょうか？
- SD カードに暗号技術を採用し保存する機能の実装が難しい場合、録画情報を閲覧する際に適切なアクセス制御が行われていれば、セキュアに保存されていると判断することは可能でしょうか？
- SD カードに対し暗号技術を採用し保存する機能を有しているが、デフォルトでは機能が無効となっており、機能の利用はユーザの判断に任せる場合は適合の判断と判断することは可能でしょうか？
- SD カードに暗号化して保存する機能は有しているが、デフォルトで非暗号化での保存も選択可能な場合、録画機能の初回利用時に「暗号化機能を有効化」するよう指示する文書をマニュアル等に記載しておけば、適合と判断してよいでしょうか？

【ガイダンス】

SD カードへの保存については、機器の利用用途や利便性の観点から、守るべき（保護すべき）情報資産の種類に応じて暗号化対象にするか暗号化非対象にするかをベンダーが決めることができます。その場合、以下のような対応をすべて満たしていることを確認ください。これを満たしていれば「適合」となります。

1）利用者が容易に確認できる場所（取扱説明書、ユーザマニュアル等）に、機器の利用用途として保護対象となる代表的なデータやセキュリティに関するデータそれぞれが「暗号化対象」となるのか「暗号化非対象」となるのかを説明する。特に「暗号化非対象」となる代表的なデータの説明は必須

2）機器の利用用途として保護対象となる代表的なデータが「非暗号化で保存」される場合には、利用者が購入前に確認できる場所（箱、パンフレット、Web 等）に、「代表的なデータは非暗号化で保存される」旨の注釈を記載する

3）ユーザが設定変更することにより「暗号化」「非暗号化」を選択できる場合には、設定変更の方法を説明する箇所（例えばマニュアルなど）に、暗号化されていない場合のリスクなど、セキュリティ上の注意が利用者にわかるように明示する

【質問 11-5】

2.1.3. 評価項目 5 における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について、「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とは、外部から呼び出すインタフェースを持たないソフトウェアコンポーネント（ブートモニタ、BIOS 等）からのみ読み書きができるストレージ領域であって、他のソフトウェアコンポーネントは直接・間接を問わず読み書きできない領域のことである。」と書かれていますが、その解釈を教えて下さい。

【ガイダンス】

「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。」とは、「パスワードなどによって保護されたアカウントにアクセスを制限するアクセスコントロールによって保護された領域に保存されること」と解釈します。つまり、設定を保存する場合には、パスワードなどによって保護されたアカウントでのアクセスコントロールの認可を受けてその領域にアクセスすることで行います。

「その他のソフトウェアコンポーネント」とは「その領域へのアクセスコントロールを行うインタフェースをもつソフトウェアコンポーネント以外のコンポーネント」のことです。「間接」の意味は、「その領域へのアクセスコントロールを行うインタフェースをもつソフトウェアコンポーネント」を介さずにそれ以外のソフトウェアコンポーネントをいくつ介してもという意味で、「その領域へのアクセスコントロールを行うインタフェースをもつソフトウェアコンポーネント」へのアクセスは「間接」に含みません。

【質問 11-6】

★1 で想定する守るべき資産でのセキュアな保存方法について、

① WebGUI など内部プログラムでのみ情報更新できる仕組みであり、外部インタフェースからのアクセスではアクセス不可にしておく対策を実施した場合、S1.1-11 の要件は満たす理解でよろしいでしょうか？
② トラブルシューティングやメンテナンスなどでカスタマーエンジニアのみ変更できる対策を実施した場合、S1.1-11 の要件は満たす理解でよろしいでしょうか？

【ガイダンス】

「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。」とは、「パスワードなどによって保護されたアカウントにアクセスを制限するアクセスコントロールによって保護された領域に保存されること」と解釈します。つまり、設定を保存する場合には、パスワードなどによって保護されたアカウントでのアクセスコントロールの認可を受けてその領域にアクセスすることで行います。

①、②ともに、アクセスコントロールの実施形態（誰にどのようにアクセス権が付与されるのか、そのアクセスコントロールを回避してデータの保存領域にアクセスができないような対策が取られているか）を確認ください。

【質問 11-7】

「以下の評価項目 1 ～ 5 のいずれかに類する保護対策」とありますが、守るべき情報資産の内容によっては機密性と完全性の両方を担保しなければならない場合があると思います。そのような場合でも評価項目 1 ～ 5 のいずれかの対策が出来ていれば「適合（Y）」になるのでしょうか？例えば、評価項目 1 のみ対応できていたとしても、完全性については対応できていないということにならないでしょうか？

【ガイダンス】

異なる保護対策が必要な情報資産があれば、それぞれについて別々に評価をしていただく必要があります。機密性と完全性が必要な情報資産であれば機密性と完全性の両方の評価基準を満たす必要があります。

【質問 11-8】

評価項目 5 の「外部から呼び出すインタフェースを経由した」とは、どの様なものを指しますか？

【ガイダンス】

ストレージへのアクセスを管理する機能を回避して、外部からストレージにアクセスできる可能性があるインタフェースは全て「外部から呼び出すインタフェース」に該当します。詳しくは、評価ガイド S1.1-11 の 2.1.3 を参照ください。

【★1 適合基準 S1.1-12】

【質問 12-1】
どのような通信が「ネットワーク経由で伝送される」の項目に該当するのでしょうか？
ユーザがデフォルトの設定で使用している場合に、ユーザが意図しなくとも伝送される通信のみが該当するのでしょうか？あるいは、ユーザの設定によっては syslog(RFC5424)や SNMPv1 のようなプロトコルを使って守るべき情報資産（機器のシステムログやログイン情報）が保護対策をせずにインターネットに伝送されてしまう通信も該当するでしょうか？

【ガイダンス】
デフォルト設定で有効となっている通信は対象、無効化されているものは対象外とします。
設定変更で利用ができるようになるものについては、設定変更を説明する箇所（例えばマニュアルなど）に、設定変更をした場合のリスクや機能制限など、セキュリティ上の注意が利用者にわかるように明示ください。

【質問 12-2】
暗号技術を採用した通信プロトコル(https 等)にて伝送する機能をデフォルトで有効化しているが、同時に暗号化していない通信（http 等）もデフォルトで有効になっている場合は、非適合という認識でしょうか？初期設定では https 等の暗号化通信を強制し、暗号化していない通信方式は無効化することを必須とする必要があるでしょうか？

【ガイダンス】
デフォルト設定で有効となっている通信は対象、無効化されているものは対象外とします。
https と http の両方が使えるようになっている場合には、以下の対応をすべて満たしていることを確認ください。これを満たしていれば「適合」となります。

1) デフォルト設定では https のみが使えるように設定（つまり、デフォルト設定では http は受け付けない）
2) 利用者が設定変更することで http が使えるようにすることは可
3) 設定変更の方法を説明する箇所（例えばマニュアルなど）に、設定変更をした場合のリスクや機能制限など、セキュリティ上の注意が利用者にわかるように明示

なお、2.2.2 の例外を適用する場合、「設置する際に暗号化されていない http を無効にし、暗号化されている https を有効化して下さい。」との注釈標記だけでなく、「工事設置業者による IoT 装置の設置が前提となっている（工事設置業者又はシステム管理者以外が設置しないことがマニュアル等に文書化されている）」ことも必要です。両方の注釈表記があることで適合となります（片方だけでは非適合）。また、http を有効とする設定変更を説明する箇所（例えばマニュアルなど）に、設定変更をした場合のリスクや機能制限など、セキュリティ上の注意が利用者にわかるように明示ください。

【質問 12-3】

データ送信先の指定として、http/https のデフォルト設定は無く、ユーザが送信先の指定を"http://"、"https://"の記述も含めて設定する必要ある場合について教えて下さい。

例えば、

"https://sample.com/" を送信先に設定　→通信可能

"sample.com" を送信先に設定("https://" を省略）→記述形式エラーとして通信不可

設定を省略（空欄）にした場合　→通信先無しとして通信しない

このような仕様の IoT 製品において、以下の対策を考えます。

1) デフォルト設定では https のみが使えるように設定する。（つまり、デフォルト設定では http は受け付けない。）
2) 利用者が設定変更することで http が使えるようにすることは可とする。
3) 設定変更の方法を説明する箇所（例えばマニュアルなど）に、設定変更をした場合のリスクや機能制限など､セキュリティ上の注意が利用者にわかるように明示する。

この場合に、a.と b,のどちらと解釈すべきでしょうか？

a. デフォルト設定そのものがない前提では、1)は該当しないため、2)と 3)を満たせば「適合」と解釈してよい
b. 1)を満たすため、別の設定として"http 通信を許可する"（デフォルトは https を指定しないと通信できない）というような設定項目を設ける必要がある

【ガイダンス】

b.（1）を満たすため、別の設定として"http 通信を許可する"（デフォルトは https を指定しないと通信できない）というような設定項目を設ける必要がある）を意図しています。

【質問 12-4】

評価ガイド 2.6（P12）「セキュアな通信が求められる（or 除外可能な）範囲の考え方」について B)の条件の後半の記述「例えば、ホームルータの設定によって～」について、例えば屋外に設置されるメーター機器やドアホンについて、有線接続できないように何らかの物理的な防御（筐体による保護等）があれば、この条件に当てはまる（「セキュアな通信が求められる範囲」外）とすることができると考えてよいでしょうか？

【ガイダンス】

ご認識の通りです。

【質問 12-5】

ネットワーク経由で伝送される「守るべき情報資産」の盗聴保護について、★1 評価ガイド補足説明「2.2.1. インターネットとは通信ができない環境下において利用する場合の取

り扱い」には「通信が暗号化されていなくても…(中略)…旨の注意をユーザに明示することを条件に、評価項目 2 を満たしているとみなす」と記載されています。

一方で、暗号化できないネットワークにおいて、補足説明に該当する場合（評価項目 2 を満たす）であっても、評価項目 1 （暗号化を求めている）を満足できず、本適合基準を満たすことができないため、矛盾した記述になっているように見えます。

【ガイダンス】

「評価項目 3 を満たしているとみなす」の誤りです。更新版の★1 評価ガイド（JST-EG-01-01-2024R1）の補足説明では修正されています。

【質問 12-6】

HTTPS を利用する際のガイドラインなどはありませんでしょうか？

【ガイダンス】

TLS サーバークライアント（ブラウザ）型のシステムを対象としたものですが、TLS 暗号設定ガイドラインが参考になるかと思われます。特に、利用すべき暗号スイートの選択にお役立てください。

https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html

【質問 12-7】

HTTPS で採用されている全ての暗号技術が「電子政府推奨暗号リスト」に合致することが必須となりますでしょうか？

【ガイダンス】

「電子政府推奨暗号リスト」又は「推奨候補暗号リスト」に含まれない暗号技術をサポートすること自体は問題ありませんが、それらの暗号技術は「デフォルト無効」にしておくことが必要です。「デフォルト無効」にしていなければ非適合となります。また、それらの暗号技術を有効とする設定変更を説明する箇所（例えばマニュアルなど）に、設定変更をした場合のリスクや機能制限など、セキュリティ上の注意が利用者にわかるように明示ください。

【質問 12-8】

rtsp 通信に関しては、rtsps や srtp の暗号化通信の機能を実装しておらず、設置時の有効化の指示はできない場合、非適合となるでしょうか？

また、仮に適合とする場合は下記のいずれかの方法でよろしいでしょうか？

1) デフォルトで rtsp 通信をオフにする。
2) 暗号化された通信(rtsps や srtp)の機能を実装する。
3) rtsp で通信される映像や音声のリアルタイムストリーミングは、非暗号化対象（守るべき情報資産には該当しない）とベンダが判断する。

4） 評価項目 1-2 を満たすことは難しいため、評価項目 3 を満たせるように、ユーザがアクセス可能な媒体において「保護された通信環境（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）においてのみ IoT 製品を利用する」旨の内容を明示する。

【ガイダンス】

ご認識の通りです。

【質問 12-9】

「守るべき情報資産」が暗号化されずに一時的に伝送されるものの、運用時にはクローズされアクセス不可となるポートがある場合、当該ポートで伝送される情報は運用時には盗聴不可となるため【S1.1-12】の対象外となる認識でよいでしょうか？それとも、一時的であっても「守るべき情報資産」が暗号化されずに伝送される場合は、必ず盗聴に対する保護対策が要求されるでしょうか？

【ガイダンス】

初期設定においては、以下の条件 A）と B）の両方を満たす場合に限り、その手続きを文書化して証跡（エビデンス）として残すことにより、例外的に「IoT 製品出荷時点では保護対策が無効」であっても、IoT 機器の工事設置時での初期設定の変更により「盗聴に対する保護対策が有効」であるとみなすことができます。

A） 工事設置業者による IoT 装置の設置が前提となっている（工事設置業者又はシステム管理者以外が設置しないことがマニュアル等に文書化されている）

B） 設置時に当該 IoT 機器の設定で「盗聴に対する保護対策を有効化」するように指示する項目を、設置作業指示書やマニュアル等に注意・警告表示されている

この内容は、★1 評価ガイド S1.1-12 2.2.2. 評価項目 2 の初期設定時の考え方に記載されています。

【★1 適合基準 S1.1-13】

【質問 13-1】

評価項目 3 について、「攻撃状況を把握し、必要に応じて適切な対処ができる管理プロセス」という記載ありますが、

① 「攻撃状況を把握し」というのは、IoT 製品が攻撃を検知する必要があるということでしょうか？

② 「適切な対処」というのは、管理者による対処も対象となるという理解であっていますでしょうか？

③ 例えば、攻撃を検知した場合、記録する管理プロセスが存在し、管理者は記録を見ることで必要に応じた適切な対処を行う旨を記載した場合、「適合」となりますでしょうか？

【ガイダンス】

S1.1-13 で要求しているのは「管理プロセス」であり、技術的対応だけでなく、運用的対処でも構いません。

① IoT 製品自体が攻撃を検知しなければならないということではありません。NICT や IPA、その他の機関などからの注意喚起情報等を適時・適切に収集する体制を構築しておくことでも構いません。

② 攻撃状況の深刻度に応じてどのような対策をするのかを予め決めておくことを求めています。例えば、もっとも深刻な状況では「即時利用不可にすること」が必要になることが想定されるので「どのように」利用不可に設定変更するかを決めておく必要があります。「管理者による対処」も管理プロセスの一つの選択肢とあり得ますが、その場合であっても管理者によって「どのような」対処をさせるのかまでを決める必要があります。「管理者によって適切な対処を行う」だけでは不十分です。また、「管理者による対処」だけで最も深刻な攻撃状況になったとき（すなわち、具体的な攻撃を受けていることが判明した時）に対処できるのかどうかも検討しておく必要があります。

③ 上記②のとおり、「適切な対処を行う」旨の記載だけでは不十分です。
「必要に応じた適切な対処」がどのようなものであるのか、何をもとにどのように対処・判断するのか、といったプロセスを決めておく必要があります。

【質問 13-2】

推奨される脆弱性検査ツール、ポートスキャンツールが何かを教えて頂けますでしょうか？

【ガイダンス】

推奨された脆弱性検査ツールは、一般的に認知されているツールを IoT 製品ベンダーが適切に選定して頂くことを想定しています。但し、★1 評価ガイド（S1.1-13）の評価項目 5 のⅰ）とⅱ）の確認が出来る必要が有ります。

無償で利用できる脆弱性検査ツールの例としては、OpenVAS、Vuls、Greenbone Vulnerability Management（GVM)等があります。その他、有償で提供される脆弱性検査ツール（Nessus など）も選択可能です。

無償で利用できるポートスキャンツールとしては、NMAP 等があります。

これらのツールは IoT 機器ベンダーが利用目的や予算などに合わせて適切なものを選定して下さい。また、経済産業省が公表している「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」も参考にしてください。

https://www.meti.go.jp/policy/netsecurity/wg3/akakenshou_tebiki_202205kaitei.pdf

【質問 13-3】

「※原則ドキュメント評価と実機テストの双方を実施すること。ただし、実機テストに関しては、推奨のポートスキャンツール及び脆弱性検査ツールが無い場合は、対象外（ドキュメント評価のみ）とする。」との注釈に関連して、

① 現時点では Bluetooth と USB は推奨される脆弱性検査ツールがない場合に該当するので、脆弱性確認テストの代替として記載の内容を評価すればよいでしょうか？

② 推奨のポートスキャンツール及び脆弱性検査ツールが無い場合とは、試験を実施する会社において、ポートスキャンツール及び脆弱性検査ツールを保有していない場合も含まれますか？

③ 機器自体に、http/https プロトコルを使用する機能がある場合のみ、ガイドラインに記載のある既知の脆弱性 CVE-ID に該当する脆弱性が検出されないことを確認するとの解釈でよろしいでしょうか？

【ガイダンス】

① 質問の通り、現時点では Bluetooth と USB には脆弱性確認テストの代替として記載の内容を評価してください。

② 「推奨されるツールがない」には「単に保有していない」ということは含みません。あくまで一般に「推奨されるツールそのものがない」場合に限ります。

③ 質問の通り、http/https プロトコルを使用する機能がある場合のみ、CVE-ID に該当する脆弱性が検出されないことを確認してください。

【質問 13-4】

Bluetooth の確認方法について、実機テストは「Bluetooth」でペアリングし、機器に IP アドレスが付与されて TCP/IP のポートスキャンを想定しているのでしょうか？

【ガイダンス】

評価項目 4 において A)の TCP/UDP では接続方法を問わないため、Bluetooth を使って TCP/IP 通信を行うようなプロファイル（DUN、PAN、IPSP 等）が利用されている場合に

おいては、同接続方法による TCP/IP のポートスキャン（および脆弱性スキャン）を求めています。

【質問 13-5】
USB の確認方法について、実機テストは「USB」を接続し、機器に IP アドレスが付与されて TCP/IP のポートスキャンを想定しているのでしょうか？

【ガイダンス】
評価項目 4 において A)の TCP/UDP では接続方法を問わないため、USB を使って TCP/IP 通信を行うようなプロファイル（IP over USB クラス）が利用されている場合においては、同接続方法による TCP/IP のポートスキャン（および脆弱性スキャン）を求めています。

【質問 13-6】
評価項目 5 の脆弱性検査の範囲について Web のインターネットに関しては全てのページを対象とするのでしょうか？それともログイン画面だけを検査するのでしょうか？
Web サーバ（ミドルウェアのサービス。例えば、Apache など）が対象でしょうか？それとも、Web インタフェース（IoT の管理画面など）も対象でしょうか？

【ガイダンス】
インターネットから接続可能な http/https を利用するすべての設定や実装（Web アプリケーションを含め）に対して脆弱性が含まれていないことの確認を重要な項目だけに絞り込んで実施するのが評価項目 5 の意図です。したがって、http/https を利用するログイン画面以外もインターネットから接続可能なページは対象となります。
また、IoT 機器上か必須付随サービス上かは問わずに、評価項目 5 の実機テストによる検証は必要です。ただし、Web アプリケーションや Web サイトの開発において、セキュアコーディングの一環として評価項目 5 の実機テストで確認するような脆弱性が含まれていないことの検査が別途行われていることが期待されることから、その脆弱性検査の結果をもって、評価項目 5 の実機テストの検証を代用することが可能です。その場合、Web アプリケーションや Web サイトの開発時に実施した脆弱性検査結果報告書を証跡（エビデンス）として保管ください。

S1.1-13 に関連し、必須付随サービスが動いているクラウド・サーバの保守状況は必須付随サービスの範囲に含まず、本制度の枠外で適切に保守がされているとみなします。つまり、クラウドやサーバそのものに対して実機テストは実施しなくてもかまいません。
なお、クラウドやサーバで不要ポートは閉じるなどの設定変更がベンダーによって可能な場合、必須付随サービス（を動かしているクラウドやサーバでの設定）に対して S1.1-13 評価項目 1～3 を準用して評価を行います。

【質問 13-7】

「露出した攻撃面の最小化」の方法として、設備に特殊鍵で施錠するといったハードウェア面での対応でもよいのでしょうか？

【ガイダンス】

通信インタフェースからのアクセスを想定していますので、基本的にハードウェア的な対策では保護できません。ただし、USB に関しては、例外的に筐体の保護によって USB インタフェースが実質的に使うことができないといった状況は考えられます。

【★1 適合基準 S1.1-14】

【質問 14-1】
　質問なし

【ガイダンス】
　―

【★1 適合基準 S1.1-15】

【質問 15-1】
ユーザが設定可能なパラメータが無い場合、消去機能を具備しなくてもよいですか？

【ガイダンス】

ユーザが運用中に生成される情報資産（個人情報含む）は消去の対象になりますので、そういった情報が生成されるかどうかによります。ユーザが設定するパラメータの有無だけで消去機能の要否が決まるわけではありません。

【★1 適合基準 S1.1-16】

【質問 16-1】

S1.1-16 の適合基準④について、対象機器が機器単体での買い切り販売ではなく、サービスの一環として以下の条件で提供されるものであった場合、「サポート期間」についてどのようにとらえればよろしいでしょうか？

- 他の機器を含むシステム単位での契約に基づいて提供される
- 機器単体としてのサポート期間の設定がない
- 契約期間内はサポートが保証されており、契約更改の期限は定められていない
- 契約期間内に何らかの必要性が生じた場合には、機器ごと入れ替える
- 契約終了時には機器が回収されるため、契約期間外（サポート外）で使用されることがない

【ガイダンス】

当該製品をいつまでシステムに組み込んで使う可能性があるかで判断してください。つまり、最長のサービス提供（可能）期間がサポート期間となるとお考え下さい。

また、周知に関しては「サービス提供契約期間内はサポートが保証される」としていただければ結構です。

【質問 16-2】

周知については評価ガイドの文言通り、WEB サイトである必要がございますでしょうか？言い換えれば、誰に対して周知される必要がございますでしょうか？

実際に使用する人（例えば、法人営業を介した契約者のみが使用）に周知されれば利用者全員に通知される状態であれば、契約時の案内に文言があれば要件に適合すると判断してよいでしょうか?

【ガイダンス】

申請製品としてのサポート期間については、申請書に記載いただく必要があり、またその情報は IPA が管理する「製品情報ページ」に Web 掲載されます。したがって、申請書での同意をもって、この時点で一定の周知はされていると判断していただいてかまいません。

評価項目 4 ではこれに反するようなサポート期間ではない、ということだけ確認していただければ結構です。つまり、申請書に記載されているサポート期間に反しないという前提で、自社のホームページ等でサポート期間を周知するでも構いませんし、契約者だけや購入希望者だけに伝えるということでも構いません。

なお、サポート契約期間を別途の契約書で定める場合は、申請書に記載のサポート期間と異なっても問題ありません。

【質問 16-3】

従来、製品のサポート終了時期や販売終了時期が決まってから情報発信しておりました。評価項目 4 で求められているメーカが公表する情報として、サポート期間に関する案内は、以下のような記載でもよいのでしょうか？

例 1）「サポート終了時期は未定」

例 2） 「サポート終了時期は 2 年後以降」

【ガイダンス】

サポート期間の公表については、IPA が管理する「製品情報ページ」に掲載されます。したがって、申請書での同意をもって、この時点で一定の周知はされていると判断していただいてかまいません。評価項目 4 ではこれに反するようなサポート期間ではない、ということだけ確認していただければ結構です。

なお、IPA が管理する「製品情報ページ」に掲載されているサポート期間に反しないという前提で、自社のホームページ等でサポート期間を周知していただいても構いませんし、サポート時期が未定の場合には表示そのものがなくても問題ありません。

【質問 16-4】

サポート期間についての証明は申請書をエビデンスとしてよいでしょうか？

その場合は技術文書による証明ができないが、チェックリストにはどのように記載すればよいでしょうか？

【ガイダンス】

申請書をエビデンスとすることもできます。その場合、「申請書に記載の通り」と記入していただければ結構です。

【質問 16-5】

販売開始前の製品の場合には、ユーザ等への公開情報になっていませんので予定の当該情報記載媒体名称を用いて、その入手手段[*]を記載すればよろしいでしょうか？

[*] 当該情報は製品購入時に同梱されているユーザーズマニュアルに記載する、または製品購入時に案内する手段でユーザが入手するユーザーズマニュアルに記載、という記載方法など。

例 1）適合基準 S1.1-16 の評価項目 1 の要件を満たす記載はユーザーズマニュアルに記載予定ですが、販売前製品のため公開できません。この場合、”製品のユーザーズマニュアルに記載”あるいは”製品のユーザーズマニュアルに記載予定”という記載で良いのでしょうか？

例 2）適合基準 S1.1-16 の評価項目 4 の要件を満たす記載はホームページに記載予定ですが、販売前製品のため URL 情報などを公開できないため、記載できません。この場合、”

メーカーホームページに記載”あるいは”メーカーホームページに記載予定”という記載で良いのでしょうか？

【ガイダンス】

公開予定の「周知手段」と「公開時期」についてチェックリストに記載してください。

周知手段としては、「製品のユーザーズマニュアルに記載予定」や「メーカーホームページに記載予定」などの記載で結構です。