セキュリティ要件適合評価 及びラベリング制度（JC-STAR）

通信機器★３セキュリティ要件 新旧対照表

（新）JST-SR-03-01-2026

（旧）JST-CR-03-01-2026R1

【凡例】赤字：更新箇所を示す。

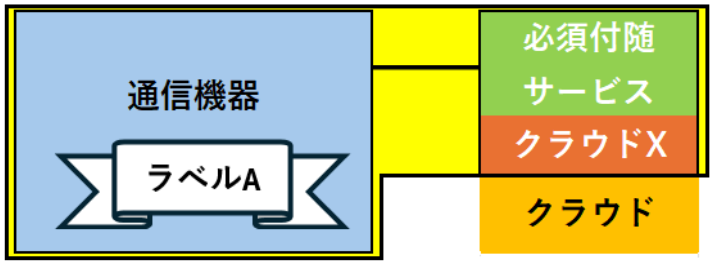
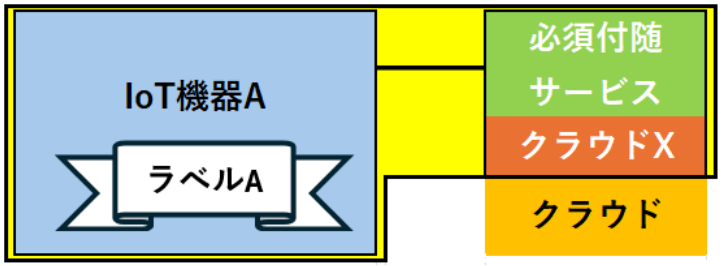
新 JST-SR-03-01-2026	旧 JST-CR-03-01-2026R1	備考
新文書番号 JST-SR-03-01-2026	旧文書番号 JST-CR-03-01-2026R1	●文書番号の文書種類「CR」(Conformance Requirements)から、「SR」(Security Requirements)に変更
1.5 ★3適合基準類の構成 ★3適合基準類は、**「★3セキュリティ要件」、「★3適合要件」、「★3評価ガイド」**の3点より構成される。 ● **「★3セキュリティ要件」とは、**★3レベルのIoT製品として、満たす必要のあるセキュリティ対策や要件等のことである。 ● **「★3適合要件」とは、**★3セキュリティ要件に記載してある対策、要件に対して、★3レベルのIoT製品として具備する必要がある機能や、IoT製品ベンダーが対応する必要のある対策など、具体的に満たす必要のある要件のことである。 (略) (削除)	**1.5 ★3適合基準類の構成** ★3適合基準類は、**「★3セキュリティ要件」、「★3適合要件」、「★3評価ガイド」**の3点より構成される。 ● **「★3セキュリティ要件」とは、**★3レベルのIoT製品として、満たす必要のあるセキュリティ対策や基準等のことである。 ● **「★3適合要件」とは、**★3セキュリティ要件に記載してある対策、基準に対して、★3レベルのIoT製品として具備する必要がある機能や、IoT製品ベンダーが対応する必要のある対策など、具体的に満たす必要のある要件のことである。 (略) 【注意】 本文書「★3セキュリティ要件」は、「★1レベル適合基準・評価手法」に相当する文書である。 「★3セキュリティ要件」は、「★1レベル適合基準・評価手法」と項目名、記載事項の位置づけを変更しているので注意されたい。	●基準から要件へ変更 ●★1からの文書構成の変更に関する説明のため、削除

「★3 セキュリティ要件」と、「★1 レベル適合基準・評価手法」の項目名、記載事項の違いを表 4 に示す。

表 1. 「★3 セキュリティ要件」と「★1 レベル適合基準・評価手法」の項目名、記載事項

記載事項	★1 レベル適合基準・評価手法	★3 セキュリティ要件
セキュリティ要件の分類	セキュリティ要件カテゴリ	カテゴリ
セキュリティ要件の表題	セキュリティ要件	(廃止)
JC-STAR の求めるセキュリティ要件の記述	適合基準	セキュリティ要件
対象外(NA)となるための条件、基準の補足説明	対象外(NA)となるための条件、基準の補足説明	対象外(NA)となるための条件、基準の補足説明
評価手法の概要	評価手法	(削除、★3 評価ガイドに記載)

★1 レベル適合基準・評価手法での、「セキュリティ要件」はセキュリティ要件の表題であるにもかかわらず、要件内容とも読み取れる表記になっており、JC-STAR で求める要件と紛らわしい記載となっていた。このため、JC-STAR で求めるセキュリティ要件を明確にするため、上記のように記載項目を変更した。
また、本文書は★3 セキュリティ要件を定義するための文書であるため、「評価手法」の記載は本文書から削除し、「★3 評価ガイド」にて詳細を解説する。
★1 レベル適合基準・評価手法(JST-CR-01-01-2024R1、セキュリティ要件適合評価及びラベリング制度(JC-STAR)★1 レベル適合基準・評価手法、令和 6 年 12 月)

	も次回の改定時に、上記の表記内容に従って項目名を変更する予定である。	
1.6 「必須付随サービス」の考え方 JC-STAR における「IoT 製品」とは、供給者により販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独の「IoT 機器」、又は「IoT 機器」と「必須付随サービス」とで構成される一式を指す。「必須付随サービス」とは、対象となる「IoT 機器」が「必ずセットで利用するサービス」のことを指す。具体的には、【当該 IoT 機器本体だけでは、当該 IoT 製品が意図した目的を提供できない】場合に、当該 IoT 機器に付随して提供されるデジタルサービスのことである。 例えば、通信機器が保存した通信アクセスに関するログを特定のクラウドサービスに送信、保存するように設定されている場合、当該サービスは必須付随サービスである。この場合、適合ラベルの評価対象範囲は、「通信機器」、「クラウドサービス」及びその両者をつなぐ通信路全体となる。なお、適合ラベルは「通信機器」に対して付与される。  (注釈)クラウド X: サービスが直接的に利用するクラウド領域 **図 3. IoT 製品、IoT 製品の区分例** 必須付随サービスの提供形態については「対抗となる IoT 機器とセットで提供」されるという条件以外の制約はない。例えば、必須付随サービスには、モバイルアプリケーション、クラウドコンピューティング/ストレージ、及びサードパーティのアプリケーションプログラミングインタフェース(API)などのデジタルサービスを含めることができる。	**1.6 「IoT 製品」と「IoT 機器」の説明** 「IoT 製品」の定義には、「IoT 機器」と「必須付随サービス」が含まれている。「必須付随サービス」とは、対象となる「IoT 機器」が「必ずセットで利用するサービス」のことを指す。具体的には、【当該 IoT 機器本体だけでは、当該 IoT 製品が意図した目的を提供できない】場合に、当該 IoT 機器に付随して提供されるサービスのことである。 ➢ 例：IoT 機器 A で生成されたデータを特定のクラウドサービス X に保存するように設定されている場合、当該サービス X は必須付随サービスである。この場合、適合ラベルの評価対象範囲は、「IoT 機器 A」、「クラウドサービス X」及びその両者をつなぐ通信路全体となる。なお、適合ラベルは「IoT 機器 A」に対して付与される。 「IoT 製品」とは、供給者により販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独の「IoT 機器」、又は「IoT 機器」と「必須付随サービス」とで構成される一式を指す。  **クラウド X: サービスが直接的に利用するクランド領域** **図 3. IoT 製品、IoT 製品の区分例** 必須付随サービスの提供形態については「対抗となる IoT 機器とセットで提供」されるという条件以外の制約はない。ただし、IoT 機器からみて対向となるサービスが特定されない場合、そのサービスは必須付随サービスに該当しないので、注意すること。	●「必須付随サービス」の説明を明確化 ●外部システム連携の説明を追加

ただし、IoT 機器からみて対向となるサービスが特定されない場合、そのサービスは必須付随サービスに該当しない「外部システム」となるので、注意すること。 本文書では、必須付随サービスと外部システムとを区別する要素は、システム上で提供するサービスが IoT 機器の製造業者の管理下で提供されるか否かである。つまり、製造業者の管理下で提供される場合は「必須付随サービス」といい、製造業者ではなく利用者の管理下で利用する場合は「外部システム」という。		
2.1 ★3 適合ラベル(通信機器)の主な対象範囲 ★3 適合ラベルが想定する「通信機器」とは、一般家庭向けの通信機器(ホームルータや家庭用 Wi-Fi ルータ等)よりも、**政府機関等や重要インフラ事業者、地方自治体、大企業において主に調達・設置される、IP パケットを扱う代表機能及び管理機能等を有する通信機器**を想定している。 例えば、以下のような場所に設置されることを想定している。 ● 要管理対策区域(例：セキュリティエリア、サーバールーム等) ● 施設内の施錠管理されたラック等の内部 ● 物理的セキュリティに配慮された施設内の共用エリアの区画(例：政府機関の執務室、関係者エリア等) ● 施設内の共用エリアの区画(例：市役所の待合ホール、共有エリア、アトリウム等) 対象範囲は、図 4 に示すような利用形態における、ルーティング/スイッチング、フィルタリング、VPN 等の機能を有する通信機器が該当する(例：赤枠の機器＋緑枠の必須付随サービス)。	**2.1 ★3 適合ラベル(通信機器)の主な対象範囲** ★3 適合ラベルが想定する「通信機器」とは、一般家庭向けの通信機器(ホームルータや家庭用 Wi-Fi ルータ等)ではなく、**政府機関等や重要インフラ事業者、地方自治体、大企業において主に調達・設置される、IP パケットを扱う代表機能及び管理機能等を有する通信機器**である。 例えば、以下のような場所に設置されることを想定している。 ● 要管理対策区域(例：セキュリティエリア、サーバールーム等) ● 施設内の施錠管理されたラック等の内部 ● 物理的セキュリティに配慮された施設内の共用エリアの区画(例：政府機関の執務室、関係者エリア等) ● 施設内の共用エリアの区画(例：市役所の待合ホール、共有エリア、アトリウム等) 図 4 に示すような利用形態における、ルーティング／スイッチング、フィルタリング、VPN 等の機能を有する通信機器が該当する(例：赤枠の機器＋緑枠の必須付随サービス)。	●表現を修正
3.1 ★3 通信機器のセキュリティ要件導出の考え方 表 4. 攻撃手法に対抗するために★3 で実現すべきセキュリティ要件 **★3 で考慮すべき主な攻撃手法**	**3.1 ★3 通信機器のセキュリティ要件導出の考え方** 表 5. 攻撃手法に対抗するために★3 で実現すべきセキュリティ要件 **★3 で考慮すべき主な攻撃手法**	●「マルウェア感染や踏み台攻撃への対策」を追記

2.脆弱性の放置により未対応の脆弱性を含んだ状態による、情報漏洩、改ざん、機能異常の発生につながる攻撃、マルウェア感染や踏み台攻撃への対策
3.意図しないインタフェース経由による外部からのアクセスによる、情報漏洩、改ざん、機能異常の発生につながる攻撃、マルウェア感染や踏み台攻撃への対策
4. 通信において機密通信情報の盗聴
5.廃棄・転売等された機器から、セキュア保存情報の盗み取り
8.保存されているセキュア保存情報への攻撃

IoT 製品が担う対策		
対策種別	**★3 適合要件の概要**	**要件番号**
脆弱性対策、ソフトウェアの更新	•深刻度の高い既知の脆弱性及び主要な CWE に対する対策を行う	S3.1-42
	・不正なアップデートパッケージが適用されない対策を行う	S3.1-12
		S3.1-19
データ保護	•インターネット経由で伝送される通信において守るべき情報を保護するために情報の漏洩や変更に対する保護対策を実装する	S3.1-20
		S3.1-22
データ保護	•機器が保有するセキュア保存情報を保護するための機能を提供する	S3.1-16
		S3.1-17
		S3.1-18

2.脆弱性の放置により未対応の脆弱性を含んだ状態による、情報漏洩、改ざん、機能異常の発生につながる攻撃
3.意図しないインタフェース経由による外部からのアクセスによる、情報漏洩、改ざん、機能異常の発生につながる攻撃
4.守るべき情報資産の機器間通信の盗聴
5.廃棄・転売等された機器から、守るべき情報資産の盗み取り
8.保存されている守るべき情報資産への攻撃

IoT 製品が担う対策		
対策種別	**★3 適合要件の概要**	**要件番号**
脆弱性対策、ソフトウェアの更新	•深刻度の高い既知の脆弱性及び主要な CWE に対する対策を行う	S3.1-43
	・不正なアップデートパッケージが適応されない対策を行う	S3.1-12
		S3.1-19
データ保護	•インターネット経由で伝送される守るべき情報を保護するために情報の漏洩や変更に対する保護対策を実装する	S3.1-20
		S3.1-22
データ保護	•機器が保有する守るべき情報資産を保護するための機能を提供する	S3.1-16
		S3.1-17
		S3.1-18

●「守るべき情報資産」を「通信において機密通信情報」に修正

●「守るべき情報資産」を「セキュア保存情報」に修正

●S3.1-39～41 の 3 つを S3.1-39～40 と 2 つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ

	•ユーザーが個人情報や設定情報等を削除/破棄できる機能の実装を提供する	S3.1-36
		S3.1-41
レジリエンスの向上	•サービス不能攻撃によるネットワーク負荷状態からの復元機能を提供する	S3.1-45
筐体のタンパー性	•筐体に対する物理的な破壊・改変行為を防ぐ仕組みを提供する	S3.1-46

IoT 製品ベンダーが担う対策

対策種別	★3 適合要件の概要	要件番号
情報・問い合わせの受付、情報提供	•脆弱性開示ポリシーの公開	S3.1-09
		S3.1-43
情報提供	•セキュアな廃棄方法に関する情報を提供する	S3.1-44
	•機器に収集されるテレメトリデータのデータ種別に関する情報を提供する	S3.1-32
		S3.1-40

3.2 ★3 通信機器での守るべき情報資産の種類

「情報を守る」には二つの意味がある。一つは「不正な開示や暴露により、本

	•ユーザーが個人情報や設定情報等を削除/破棄できる機能の実装を提供する	S3.1-36
		S3.1-42
レジリエンスの向上	•サービス不能攻撃によるネットワーク負荷状態からの復元機能を提供する	S3.1-46
筐体のタンパー性	•筐体に対する物理的な破壊・改変行為を防ぐ仕組みを提供する	S3.1-47

IoT 製品ベンダーが担う対策

対策種別	★3 適合要件の概要	要件番号
情報・問い合わせの受付、情報提供	•脆弱性開示ポリシーの公開	S3.1-09
		S3.1-44
情報提供	•セキュアな廃棄方法に関する情報を提供する	S3.1-45
	•機器に収集されるテレメトリデータのデータ種別に関する情報を提供する	S3.1-32
		S3.1-41

3.2 ★3 通信機器での守るべき情報資産

★3 通信機器として、守るべき情報資産を表 6 のように定義する。

●「守るべき情報資産」の扱い方を

来は保護されているべき情報が非権限者に漏洩し、不正アクセスやデータ漏洩などのセキュリティ上の問題が生じないように対策する」、すなわち「情報の機密性(Confidentiality)を守る」という意味であり、もう一つは「情報の改ざんや偽造により、情報の信頼性や完全性が損なわれ、危険な状態になっているにもかかわらず、その情報を信じて使用してしまうことがないように対策する」、すなわち「情報の完全性(Integrity)を守る」という意味である。

そこで、「機密性」「完全性」のどちらかでも守る必要がある情報のことを「守るべき情報資産」と呼ぶこととし、通信機器でのユースケースや実装環境などを考慮して、★3通信機器としての「守るべき情報資産」を表5に定める。これらについては、情報資産ごとに必要性に応じて「機密性」もしくは「完全性」を守ることを要求する。

また、「ネットワークを介して通信されるときに機密性を守るべき情報資産」のことを「機密通信情報」と呼び、適切な暗号化を行う通信プロトコルで通信することを要求する。この対象となる情報資産を表5①に定める。

「IoT 機器へ保存される守るべき情報資産」のことを「セキュア保存情報」と呼び、適切に「機密性」もしくは「完全性」を守ることを要求する。この対象となる情報資産を表5②に定める。

なお、表5はすべての★3通信機器に対して共通してセキュアな管理を要求する最低限の「守るべき情報資産」の種類であり、独自にこれらに含まれない情報資産を「守るべき情報資産」として扱うことを妨げるものではない。

表5. 通信機器での守るべき情報資産の種類

①：機密通信情報、②：セキュア保存情報

凡例：〇が対象、－は対象外

★3通信機器が扱う情報資産	保護対象となる情報	①	②

なお、「守る」には、「不正な開示や暴露により、本来は保護されているべき情報が非権限者に漏洩し、不正アクセスやデータ漏洩などのセキュリティ上の問題が生じないように対策する」という意味の「機密性を守る」という場合と、「改ざんにより、情報の信頼性や完全性が損なわれ、危険な状態になっているにも関わらず、その情報を信じて使用してしまうことがないように対策する」という意味の「完全性を守る」という場合がある。

表6において、CSP(Critical Security Parameter)はいかなる場合でも例外なく「機密性」と「完全性」の両方を守る必要がある情報資産に該当する。それ以外の情報資産は、「完全性」を守る必要はあるが、「機密性」を守るところまで求められるかは利用環境やユースケースなどに依存することに留意する。

表6.通信機器での守るべき情報資産

守るべき情報資産	保護対象となる情報
CSP (Critical Security Parameter)	曝露又は改ざんによってセキュリティモジュールのセキュリティが侵害される可能性がある、セキュリティ関連の秘密情報 例：秘密の暗号鍵、パスワードなどの認証値、PIN、証明書のプライベート要素
SSP (Sensitive Security Parameter)	CSP(Critical Security Parameter)に以下の要素を加えたもの ・ソフトウェア検証に使用される公開鍵 ・証明書の公開要素 ・機器固有の ID

「機密通信情報」と「セキュア保存情報」の2つとして再度説明

●機密通信情報とセキュア保存情報の差分を明確にするため CSP と PSP を含む SSP(Sensitive Security Parameter)を削除し、PSP(Public Security Parameter)を追加

●「通信機能に関する設定情報」と「セキュリティ機能に関する設定情報」の説明を修正

●「アラート情報」の追加

CSP (Critical Security Parameter)	曝露又は改ざんによってセキュリティモジュールのセキュリティが侵害される可能性がある、セキュリティ関連の秘密情報 例：秘密の暗号鍵、パスワードや PIN などの認証値、証明書のプライベート要素	○	○
PSP (Public Security Parameter)	セキュリティ関連の公開情報で、改ざんされるとセキュリティモジュールのセキュリティが侵害される可能性があるもの。 例 1： ソフトウェアアップデートの真正性/完全性を検証するための公開鍵。 例 2： 証明書の公開要素。	－	○
通信機能に関する設定情報(*1)	通信を行うための前準備として事前に設定する情報。 例： 通信設定：IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバ、ドメイン名など。 ルーター設定機能：ルーティング、QoS、DHCP（サーバ/リレーエージェント）など。 機能設定：HTTP ポートの変更設定(HTTP/HTTPS)、IEEE 802.1X ネットワークアクセスコントロール設定。	○	○
セキュリティ機能に関する設定情報(*1)	セキュリティ機能を有効にするための前準備として事前に設定する情報。 例： ルーターでの設定情報：ファイアウォール、VPN、ログ、統計管理など。	○	○

セキュリティ機能に関する設定情報	認証情報(ユーザ認証/ホスト認証)、電子証明書、改ざん検出設定、ユーザ権限設定
通信機能に関する設定情報	設定した IP アドレス情報(IPv4、IPv6)、VLAN 設定、DHCP サーバー設定、Wi-Fi の SSID
ログ(テレメトリデータ・監査ログ)	テレメトリデータ、監査ログ
プログラムコード(ソフトウェア)	ソフトウェア
その他	IoT 製品の意図する使用において、IoT 製品が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

	ファイアウォールでの設定情報：フィルタリング、管理者アクセスを許可するネットワーク、アプリケーションコントロールなど。 機能に関する設定情報：認証情報(ユーザ認証/ホスト認証)、電子証明書、ユーザ権限設定。		
アラート情報	通信機器にて異常を知らせる信号、異常の具体的な内容、セキュリティに関する異常などを検知したときに発報されるアラート情報	○	－
プログラムコード	ソフトウェア	－	○
ログ(テレメトリデータ・監査ログ)	通信機器動作中のテレメトリデータ(例：メトリック)	－	○
	通信機器動作中の監査ログ(通信ログ、イベントログ等も含む)(*2)	○	○

(*1)： 機能を有効にするための前準備として通信することを想定する。

(*2)：通信機器動作中の監査ログ

通信機器での監査ログは、通信ログやイベントログ等を想定し、監査ログに個人情報が含まれている可能性があるので、「機密性」を守る対象とする。

3.3 対策の分類カテゴリ

表 6. 対策の分類カテゴリ

カテゴリ 5： セキュアに通信する	通信経路において伝送される通信において機密通信情報を盗聴や改ざんから保護するための対策

3.3 対策の分類カテゴリ

表 7. 対策の分類カテゴリ

カテゴリ 5： セキュアに通信する	通信経路において伝送される守るべき情報資産を盗聴や改ざんから保護するための対策

●「守るべき情報資産」を「機密通信情報」と「セキュア保存情報」の 2 つに再定義したことによる文言修正

<table>
<tr>
<td>

★3 通信機器のセキュリティ要件

表 7. セキュリティ要件の構成

★3 セキュリティ要件	★3 レベルの IoT 製品として、満たす必要のあるセキュリティ対策や要件。
対象外(NA)となるための条件、 要件の補足説明	★3 セキュリティ要件の対象外となるための条件、及び★3 セキュリティ要件の補足説明。 対象外(NA)に該当すると主張する場合には、本項目に記載された「対象外(NA)となるための条件」を満たしていることの説明資料を評価機関に提供する必要がある。

</td>
<td>

★3 通信機器のセキュリティ要件

表 8. セキュリティ要件の構成

★3 セキュリティ要件	★3 レベルの IoT 製品として、満たす必要のあるセキュリティ対策や基準。
対象外(NA)となるための条件、 基準の補足説明	★3 セキュリティ要件の対象外となるための条件、及び★3 セキュリティ要件の補足説明。 対象外(NA)と判定する場合には、評価者は本項目に記載された「対象外(NA)となるための条件」を満たしていることの証跡(エビデンス)を保管する必要がある。

</td>
<td>

●基準から要件へ変更

●対象外(NA)を主張する時に説明資料の提出が必要であるという説明に修正

</td>
</tr>
<tr>
<td>

セキュリティ要件番号 ：S3.1-01

★3 セキュリティ要件

IoT 製品に対する他の 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なければならない。
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しなければならない。

対象外(NA)となるための条件

アクセスの仕組みがない(「対象外(NA)となることの理由」に、外部からのアクセスがない根拠を記載すること)。

要件の補足説明

【用語：ユーザ】

</td>
<td>

セキュリティ要件番号 ：S3.1-01

★3 セキュリティ要件

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なければならない。
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しなければならない。

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(「対象外(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)。

基準の補足説明

【用語定義：守るべき情報資産】

</td>
<td>

●基準から要件へ修正

●★3 通信機器では物理的接触による攻撃を想定するため、「 IP 通信を介した守るべき情報資産への」を削除。

●それに伴い、「対象外(NA)となるための条件」の内容を修正

●「 IP 通信を介した守るべき情報資産
</td>
</tr>
</table>

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品へのアクセスができる当該 IoT 製品を使用する自然人及び組織すべてを含んでいなければならない。	以下の情報： ● CSP(Critical Security Parameter) ● SSP(Sensitive Security Parameter) ● 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 ● ログ(テレメトリデータ・監査ログ) ● プログラムコード(ソフトウェア) ● IoT 製品の意図する使用において、IoT 製品が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、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) 【用語定義：SSP(Sensitive Security Parameter)】 CSP(Critical Security Parameter)に以下の要素を加えたもの ● ソフトウェア検証に使用される公開鍵 ● 証明書の公開要素 ● 機器固有の ID	への」を削除したことによる補足説明の内容を整理 ●用語の修正 ●補足説明を基準から要件に修正
セキュリティ要件番号 ：S3.1-02 **★3 セキュリティ要件** IoT 製品に対する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のいずれかの要件を満たさなければならない。 ① デフォルトパスワードは、IoT 機器ごと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。 ② 初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、容易に推測可能でない 8 文字	**セキュリティ要件番号 ：S3.1-02** **★3 セキュリティ要件** 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さなければならない。 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。 ② デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、容易	●基準から要件へ修正 ●★3 通信機器では物理的接触による攻撃を想定するため、「 IP 通信を介した」を削除。 ●それに伴い、「対象外(NA)となるた

以上のパスワードの設定を強制させること。 **対象外(NA)となるための条件** パスワードを利用したユーザ認証の仕組みがない(「対象外(NA)となることの理由」に、脅威に対抗するためにパスワードを利用したユーザ認証が必要ない根拠を記載すること)。	に推測可能でない 8 文字以上のパスワードの設定を強制させること。 **対象外(NA)となるための条件** ネットワークを介したパスワードを利用したユーザ認証の仕組みがない(「対象外(NA)であることの理由」に、脅威に対抗するためにパスワードを利用したユーザ認証が必要ない根拠を記載すること)。	めの条件」の内容を修正 ●「 IP 通信を介した」を削除したことによる補足説明の内容を整理 ●用語の修正
セキュリティ要件番号 ：S3.1-03 **★3 セキュリティ要件** IoT 製品に対する他の IoT 機器又はユーザからのアクセスの認証において使用される認証値の変更について、認証の種類(パスワード、トークン、指紋等)によらず、その認証値の変更が可能でなければならない。 **対象外(NA)となるための条件** ユーザ認証及び機器認証の仕組みがない(「対象外(NA)となることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証及び機器認証が必要ない根拠を記載すること)。 **要件の補足説明** 【用語：認証値】 IoT 製品に対する認証の仕組みで使用される属性の個別値。(例：パスワードに基づく認証の仕組みである場合、認証値はパスワード情報となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。)	**セキュリティ要件番号 ：S3.1-03** **★3 セキュリティ要件** IoT 製品に対するネットワークを介した他の IoT 機器又はユーザからのアクセスの認証において使用される認証値の変更について、認証の種類(パスワード、トークン、指紋等)に依らず、その認証値の変更が可能でなければならない。 **対象外(NA)となるための条件** ネットワークを介したユーザ認証の仕組みがない(「対象外(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認証が必要ない根拠を記載すること)。 **基準の補足説明** 【用語定義：認証値】 IoT 製品に対する認証の仕組みで使用される属性の個別値。(例：パスワードに基づく認証の仕組みである場合、認証値は文字列となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。)	●文言を修正 ●★3 通信機器では物理的接触による攻撃を想定するため、「 IP 通信を介した」を削除。 ●それに伴い、「対象外(NA)となるための条件」の内容を修正 ●「 IP 通信を介した」を削除したことによる補足説明の内容を整理 ●用語の修正 ●補足説明を基準から要件に修正
セキュリティ要件番号 ：S3.1-04 **★3 セキュリティ要件** IoT 機器に対するユーザ認証の仕組みについて、総当たり攻撃を困難としなけれ	**セキュリティ要件番号 ：S3.1-04** **★3 セキュリティ要件** 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について、総当たり	●★3 通信機器では物理的接触による攻撃を想定するた

ばならない。 **対象外(NA)となるための条件** ユーザ認証の仕組みがない(「対象外(NA)となることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること)。	攻撃を困難としなければならない。 **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認証の仕組みがない(「対象外(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認証が必要ない根拠を記載すること)。	め、「 IP 通信を介した」を削除。 ●それに伴い、「対象外(NA)となるための条件」の内容を修正 ●「 IP 通信を介した」を削除したことによる補足説明の内容を整理 ●用語の修正
セキュリティ要件番号 : S3.1-07 **★3 セキュリティ要件** 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のすべての要件をすべて満たさなければならない。 (略)	**セキュリティ要件番号 : S3.1-07** **★3 セキュリティ要件** 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さなければならない。 (略)	●文言を修正
セキュリティ要件番号 : S3.1-08 **対象外(NA)となるための条件** IoT 機器に L2/L3 スイッチングを持たない(「対象外(NA)となることの理由」に、L2/L3 スイッチング又機能を持たないと記載すること)。	**セキュリティ要件番号 : S3.1-08** **対象外(NA)となるための条件** IoT 機器に L2/L3 スイッチング又はルーティング機能を持たない(「対象外(NA)となることの理由」に、L2/L3 スイッチング又はルーティング機能を持たないと記載すること)。	●要求している機能はスイッチング機能であり、ルーティング機能ではないので、対象外(NA)となる条件から「又はルーティング機能」を削除

セキュリティ要件番号 ：S3.1-09 **★3 セキュリティ要件** 製造業者は、以下の①～③の情報を含む脆弱性開示ポリシーを公開(例：製造業者のウェブサイトへの掲載)と、④のプロセスを有しなければならない。 ① IoT 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先。 ② 製造業者が IoT 製品のセキュリティに関する報告を受領した後に行う手続き及びその概要。 ③ 脆弱性が解決されるまでの IoT 製品や脆弱性の状況更新に関する手続き及びその概要。 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プロセスを有すること。	**セキュリティ要件番号 ：S3.1-09** **★3 セキュリティ要件** 製造業者は、以下の①～④のすべての情報を含む脆弱性開示ポリシーを公開(例：製造業者のウェブサイトへの掲載)しなければならない。 ① IoT 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先(例：製造業者等のウェブサイトの URL、電話番号、メールアドレス) ② 製造業者が IoT 製品のセキュリティに関する報告を受領した後に行う手続き(セキュリティに関する報告をどのように受付け、その後にどのような手続き・方法で報告者と連絡を取り合うのか、報告に対してどのような対応をするのか、善意の報告に対する法的免責付与の宣言等)及びその概要 ③ 脆弱性が解決されるまでの IoT 製品や脆弱性の状況更新に関する手続き(脆弱性が解決されるまでどのように調査や対策が行われ、どのようにその状況が管理・公表されるのか、報告者に対してどのような対応をするのか等)及びその概要 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	●セキュリティ要件に具体的な要件に関する記載があり、文章が冗長となっているため、冗長部分を削除 ●用語の修正
セキュリティ要件番号 ：S3.1-10 **★3 セキュリティ要件** IoT 製品に含まれるファームウェア(ソフトウェア)パッケージのアップデート機能について、以下の①～④のすべての要件を満たさなければならない。 ① ファームウェア(ソフトウェア)パッケージについて、アップデートが可能であること。 ② ファームウェア(ソフトウェア)パッケージのバージョンの確認が行えるなど、最新のファームウェア(ソフトウェア)がインストールされていることを確認する手段を有すること。 ③ アップデートされたファームウェア(ソフトウェア)パッケージのバージョンが電源 OFF 後も維持されること。	**セキュリティ要件番号 ：S3.1-10** **★3 セキュリティ要件** IoT 製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～④のすべての基準を満たさなければならない。 ① IoT 製品のファームウェア(ソフトウェア)パッケージについて、アップデートが可能であること。 ② ファームウェア(ソフトウェア)パッケージのバージョンの確認が行えるなど、最新のファームウェア(ソフトウェア)がインストールされていることを確認する手段を有すること。 ③ アップデートされたファームウェア(ソフトウェア)パッケージのバージョンが電源 OFF 後も維持されること。	●基準から要件へ修正 ●S3.1-10 での①～③の基準は必ずしもオンラインアップデートを前提としていないが、④だけはオンラインアップデートが前提となる基準である

④　オンラインアップデートを行える場合には自動アップデート機能を有すること。	④　自動アップデート機能を有すること。	ことから、条件を明確化 ●用語の統一
セキュリティ要件番号：S3.1-12 **★3 セキュリティ要件** ソフトウェアをアップデートする際に以下の①から③のすべての要件を満たす機能を実装しなければならない。 ①　アップデート前にソフトウェアの完全性及び真正性を確認できる仕組みを IoT 製品が有すること。 ②　真正性もしくは完全性を満たさない場合は更新を中断すること。 ③　アンチロールバックの機能を有すること。 **対象外(NA)となるための条件** 脆弱性対応をアップデートではない代替手段によって行う(「対象外(NA)となることの理由」に、アップデートによらずに脆弱性対応ができることの根拠を記載すること)。	**セキュリティ要件番号：S3.1-12** **★3 セキュリティ要件** ソフトウェアをアップデートする際に以下①から③全てを満たす機能を実装しなければならない。 ①　ソフトウェアの完全性及び真正性をアップデート前に IoT 製品が確認できる仕組みを有すること。 ②　真正性を満たさない場合は更新を中断すること。 ③　アンチロールバックの機能を有すること。	●基準から要件へ修正 ●①の文章を修正 ●更新を中断する条件で「完全性が満たさない」場合が抜けていたため、追加 ●対象外（NA）となるための条件が不足している箇所に「対象外（NA）となるための条件」を追加
セキュリティ要件番号：S3.1-13 **★3 セキュリティ要件** 製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、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しなければならない。	**セキュリティ要件番号：S3.1-13** **★3 セキュリティ要件** 製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、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すること。	●文言を修正
セキュリティ要件番号：S3.1-15 **★3 セキュリティ要件** IoT 製品で使用されるサードパーティコンポーネントを含めた一意に識別可能な	**セキュリティ要件番号：S3.1-15** **★3 セキュリティ要件** IoT 製品で使用されるサードパーティコンポーネントを含めた一意に識別可能な	●基準から要件へ修正 ●④の追加

ソフトウェア部品表(SBOM)を作成し、運用を行わなければならない。具体的には以下の①～④のすべての要件を満たさなければならない。 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。 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うえで、更新あるいは運用対処等を行うプロセスを有すること。 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。 ④ 製品出荷後に正規のアップデート以外の手段によってソフトウェアをインストールできないようにしておくこと、又は許可されたソフトウェアのみがインストールできる仕組みを設けること。	ソフトウェア部品表(SBOM)を作成し、運用を行わなければならない。具体的には以下の①～③のすべての基準を満たさなければならない。 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。 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。 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。	少なくとも許可されていないソフトウェアがインストールされることはないようにすることが必要と判断し、④を追加 ●文言の修正
セキュリティ要件番号 ：S3.1-16 **★3 セキュリティ要件** IoT 製品のストレージに保存されるセキュア保存情報(SD カード等、ストレージメディアに保存されるセキュア保存情報も含む。)は、セキュアに保存されなければならない。 **要件の補足説明** 【用語：セキュア保存情報】 以下の情報のこと。3.2 節を参照。 ● CSP (Critical Security Parameter) ● PSP(Public Security Parameter) ● 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 ● プログラムコード	**セキュリティ要件番号 ：S3.1-16** **★3 セキュリティ要件** 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なければならない。 **基準の補足説明** 【用語定義：守るべき情報資産】 以下の情報： ● CSP(Critical Security Parameter) ● SSP(Sensitive Security Parameter) ● 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 ● ログ(テレメトリデータ・監査ログ)	●本要件で該当する「守るべき情報資産」を「セキュア保存情報」に再定義したことによる文言の修正 ●「セキュア保存情報」の再定義を行ったことによる補足説明の内容修正 ●補足説明を基準から要件に修正

● ログ(テレメトリデータ・監査ログ)	● プログラムコード(ソフトウェア) ● IoT 製品の意図する使用において、IoT 製品が収集し、保存又は通信する、個人情報等 の一般的に機密性が高い情報 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、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) 【用語定義：SSP(Sensitive Security Parameter)】 CSP(Critical Security Parameter)に以下の要素を加えたもの ● ソフトウェア検証に使用される公開鍵 ● 証明書の公開要素 ● 機器固有の ID	
セキュリティ要件番号 ：S3.1-17 **★3 セキュリティ要件** IoT 製品で使用する CSP(Critical Security Parameter)は IoT 機器にハードコードしてはならない。 また、IoT 機器にハードコードされた PSP(Public Security Parameter)(機器固有の識別子やアイデンティティを証明するための認証コードなど)の改ざん防止のため、以下の①・②のすべての要件を満たさなければならない。 ① IoT 機器にハードコードされた PSP(Public Security Parameter)の全容を把握し、一覧化できていること。 ② ①の一覧に記載されたすべての PSP(Public Security Parameter)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。 **対象外(NA)となるための条件** ハードコードした CSP(Critical Security Parameter)や PSP(Public Security	**セキュリティ要件番号 ：S3.1-17** **★3 セキュリティ要件** IoT 製品で使用されるハードコードされた SSP(Sensitive Security Parameter)(機器固有の識別子やアイデンティティを証明するための認証コードなど)の改ざん防止のため、以下①・②すべての基準を満たさなければならない。 ① ハードコードされた SSP(Sensitive Security Parameter)の全容を把握し、一覧化できていること。 ② すべての SSP(Sensitive Security Parameter)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。 **対象外(NA)となるための条件** 対象製品においてハードコードされた SSP(Sensitive Security Parameter)が存	●基準から要件へ修正 ●各要件にて対象となる Security Parameter を明確化 ●それぞれのセキュリティ要件にて使用していた「ハードコード」という言葉について、用語の意味を明確化 ●CSP をハードコードしてしまうと脆弱性があった場合の対処ができない

Parameter)が存在しない(「対象外(NA)となることの理由」に、ハードコードしたCSP(Critical Security Parameter)やPSP(Public Security Parameter)が存在しないことを明示すること)。 **要件の補足説明** 【用語：CSP(Critical Security Parameter)】 【用語：PSP(Public Security Parameter)】 3.2節を参照。	在しない(「NA であることの理由」に、ハードコードされた SSP(Sensitive Security Parameter)が存在しないことを明示すること)。 **基準の補足説明** 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、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) 【用語定義：SSP(Sensitive Security Parameter)】 CSP(Critical Security Parameter)に以下の要素を加えたもの ● ソフトウェア検証に使用される公開鍵 ● 証明書の公開要素 ● 機器固有の ID	ことから、S3.1-17 では CSP のハードコードを明確に禁止する要件を追加 ●「CSP」、「PSP」、「SSP」の用語説明を修正 ●補足説明を基準から要件に修正
セキュリティ要件番号：S3.1-18 **★3 セキュリティ要件** ソースコードに直接記述された SSP(Sensitive Security Parameter)に CSP(Critical Security Parameter)が含まれていないことを確認するため、以下の①・②のすべての要件を満たさなければならない。 ① ソースコードに直接記述されている SSP(Sensitive Security Parameter)の全容を把握し、一覧化できていること。 ② SSP(Sensitive Security Parameter)のうち、IoT 製品の運用中に利用される CSP(Critical Security Parameter)が、①の一覧に含まれていないこと。 **要件の補足説明** 【用語：CSP(Critical Security Parameter)】 【用語：PSP(Public Security Parameter)】	**セキュリティ要件番号：S3.1-18** **★3 セキュリティ要件** ソースコードに記載された SSP(Sensitive Security Parameter)に CSP(Critical Security Parameter)が含まれていないことを確認するため、以下①・②すべての基準を満たさなければならない。 ① ソースコードにハードコードされている SSP(Sensitive Security Parameter)の全容を把握し、一覧化できていること。 ② SSP(Sensitive Security Parameter)のうち、IoT 製品の運用中に利用される CSP(Critical Security Parameter)が、①の一覧に含まれていないこと。 **基準の補足説明** 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、暗号モジュール	

3.2 節を参照。 【SSP(Sensitive Security Parameter)】 CSP と PSP を合わせた情報資産のこと。	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) 【用語定義：SSP(Sensitive Security Parameter)】 CSP(Critical Security Parameter)に以下の要素を加えたもの ● ソフトウェア検証に使用される公開鍵 ● 証明書の公開要素 ● 機器固有の ID 基準の補足説明 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、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) 【用語定義：SSP(Sensitive Security Parameter)】 CSP(Critical Security Parameter)に以下の要素を加えたもの ● ソフトウェア検証に使用される公開鍵 ● 証明書の公開要素 ● 機器固有の ID	
セキュリティ要件番号 ：S3.1-19 **★3 セキュリティ要件** IoT 製品で使用される CSP(Critical Security Parameter)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、及び必須付随サービスとの通信の保護に使用される CSP(Critical Security Parameter)は、IoT 機器ごとに固有でなければならない。 **対象外(NA)となるための条件** 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、及び必須付随サービスとの通信の保護で CSP を利用しない場合(「対象外(NA) となることの理由」	**セキュリティ要件番号 ：S3.1-19** **★3 セキュリティ要件** IoT 製品で使用される CSP(Critical Security Parameter)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 CSP(Critical Security Parameter)は、IoT 機器毎に固有でなければならない。 **基準の補足説明** 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、暗号モジュール	●脱字を修正 ●文言の修正 ●対象外（NA）となるための条件を修正 ●「CSP」の用語説明を修正 ●補足説明を基準から要件に修正

に、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、及び必須付随サービスとの通信の保護で CSP を使用していないと記載すること)。 **要件の補足説明** 【用語：CSP(Critical Security Parameter)】 3.2 節を参照。	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)	
セキュリティ要件番号 ：S3.1-20 **★3 セキュリティ要件** ネットワーク経由で伝送される機密通信情報について以下の①・②のすべての保護対策が行われていなければならない。 ① IoT 製品は機密通信情報の通信先の正当性を確認すること。 ② 機密通信情報は、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こと。 **対象外(NA)となるための条件** ネットワーク経由で伝送される機密通信情報がない(「対象外(NA)となることの理由」に、ネットワーク経由で伝送される機密通信情報がないことを記載すること)。 **要件の補足説明** 【用語：機密通信情報】 以下の情報のこと。3.2 節を参照。 ● CSP(Critical Security Parameter) ● 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 ● アラート情報 ● 監査ログ	**セキュリティ要件番号 ：S3.1-20** ★3 セキュリティ要件 ネットワーク経由で伝送される守るべき情報資産について以下のすべての保護対策が行われていなければならない。 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。 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。 ③ IoT 製品が保護されたネットワークのみを介して守るべき情報資産を通信する場合は、IoT 製品自ら情報の改ざんに対する保護対策を行う。 **基準の補足説明** 【用語定義：守るべき情報資産】 以下の情報： ● CSP(Critical Security Parameter) ● SSP(Sensitive Security Parameter) ● 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 ● ログ(テレメトリデータ・監査ログ)	●文言を修正 ●本要件で該当する「守るべき情報資産」を「機密通信情報」に再定義したことによる文言の修正 ●「保護されたネットワーク」というネットワークの範囲を除外し、要件を修正 ●対象外（NA）となるための条件が不足している箇所に「対象外（NA）となるための条件」を追加 ●「機密通信情報」の再定義を行った

	● プログラムコード(ソフトウェア) ● IoT 製品の意図する使用において、IoT 製品が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、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) 【用語定義：SSP(Sensitive Security Parameter)】 CSP(Critical Security Parameter)に以下の要素を加えたもの ● ソフトウェア検証に使用される公開鍵 ● 証明書の公開要素 ● 機器固有の ID 【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	ことによる補足説明の内容修正 ●補足説明を基準から要件に修正
セキュリティ要件番号 ：S3.1-21 **要件の補足説明** 【用語：CSP(Critical Security Parameter)】 3.2 節を参照。	**セキュリティ要件番号 ：S3.1-21** **基準の補足説明** 【用語定義：CSP(Critical Security Parameter)】 セキュリティに関連する情報であって、その開示又は変更が、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)	●「CSP」の用語説明を修正 ●補足説明を基準から要件に修正
セキュリティ要件番号 ：S3.1-28 **★3 セキュリティ要件**	**セキュリティ要件番号 ：S3.1-28** **★3 セキュリティ要件**	●基準から要件へ修正

製造業者は、IoT 製品に展開されるソフトウェアについて、最小権限の原則に基づいた設計 及び実装を行っていなければならない。具体的には、以下の要件を満たさなければならない。 ① 不必要に広範な権限が付与されないようデフォ ルトの権限設定を必要最小限に留めること。	製造業者は、IoT 製品に展開されるソフトウェアについて、最小権限の原則に基づいた設計 及び実装を行っていなければならない。具体的には、以下の基準を満たさなければならない。 ① デフォルト権限の最小化 ユーザがデバイスを初めて使用する際に、不必要に広範な権限が付与されないようデフォ ルトの権限設定を必要最小限に留めること。	●「最小化 ユーザがデバイスを初めて使用する際に、」が、ソフトウェア開発時とは関係がない条件であるので削除
セキュリティ要件番号 ：S3.1-29 **★3 セキュリティ要件** 製品の実装・テストフェーズにおいて、セキュアコーディングのプラクティスを実践し、作成したソースコードに対してレビューを実施しなければならない。具体的には、最低でも以下の実施を含まなければならない。 ① セキュリティに配慮したコーディング規約や実装原則を規定すること。 ② コーディング規約を技術者に周知し教育を行うこと。 ③ 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こと。 ④ コーディング規約や実装原則を更新すること。	**セキュリティ要件番号 ：S3.1-29** **★3 セキュリティ要件** 製品の実装・テストフェーズにおいて、セキュアコーディングのプラクティスを実践し、作成したソースコードに対してレビューを実施しなければならない。具体的には、最低限以下の実施を含まなければならない。 ① セキュリティに配慮したコーディング規約や実装原則を規程する ② コーディング規約を技術者に周知し教育を行う ③ 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 ④ コーディング規約や実装原則を更新する	●文言を修正 ●誤字を修正
セキュリティ要件番号 ：S3.1-32 **★3 セキュリティ要件** 製造業者は、IoT 機器がセンシングを行う場合に、以下の要件を満す対応を行わなければならない。 ① センシングする情報について、収集の目的及び機能の概要についてユーザマニュアル等に容易に理解できる内容を記載する。 **対象外(NA)となるための条件** IoT 機器にセンシングを行う機能がない場合(「対象外(NA)となることの理由」に、センシングを行う機能がないと記載すること)。	**セキュリティ要件番号 ：S3.1-32** **★3 セキュリティ要件** 製造業者は、IoT 機器がセンシングを行う場合に、以下の基準を満す対応を行わなければならない。 ① センシングする情報について、収集の目的及び機能の概要についてユーザマニュアル等に容易に理解できる内容を記載する。 **対象外(NA)となるための条件** 通信機器がセンシングを行わない場合。	●文言を修正 ●センシング機能があっても使わない場合には NA の対象と読める記載になっていたが、利用有無にかかわらず機能がある場合は対象となるため、記載を明確化

セキュリティ要件番号 ：S3.1-35 **★3 セキュリティ要件** セキュリティ上の異常を検知するために、IoT 製品はログ(テレメトリデータ・監査ログ)を記録する機能を実装しなければならない。具体的には、以下の①～③のすべての要件を満たさなければならない。 ① IoT 製品に対し、ログ(テレメトリデータ・監査ログ)の取得機能及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、閾値を超える超えるログイン試行の記録、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こと。 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、別途検討を行うこと。 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こと。	**セキュリティ要件番号 ：S3.1-35** **★3 セキュリティ要件** セキュリティ上の異常を検知するために、IoT 製品はログ(テレメトリデータ・監査ログ)を記録する機能を実装しなければならない。具体的には、以下①～③すべての基準を満たさなければならない。 ① IoT 製品に対し、ログ(テレメトリデータ・監査ログ)の取得機能及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、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。 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。	●文言を修正 ●誤字を修正
セキュリティ要件番号 ：S3.1-36 **★3 セキュリティ要件** 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、以下の①・②のすべての要件を満たさなければならない。	**セキュリティ要件番号 ：S3.1-36** **★3 セキュリティ要件** 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、以下の①・②のすべての基準を満たさなければならない。	●基準から要件へ修正 ●「D) ログ(テレメトリデータ・監査

① 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。 A) IoT 製品利用中に取得した情報資産(個人情報含む) B) ユーザ設定値 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 ② データ削除後も、アップデートされたセキュリティ機能に関するファームウェア(ソフトウェア)パッケージのバージョンは維持されること。	① 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。 A) IoT 製品利用中に取得した情報資産(個人情報含む) B) ユーザ設定値 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 D) ログ(テレメトリデータ・監査ログ) ② データ削除後も、アップデートされたセキュリティ機能に関するファームウェア(ソフトウェア)パッケージのバージョンは維持されること。	ログ)」は、デジタルフォレンジックにて利用する情報であり、ユーザが簡単に削除できることが妥当ではないため、削除対象より除外
セキュリティ要件番号 ：S3.1-39 **★3 セキュリティ要件** 製造業者は IoT 製品から得られた個人情報が処理される場合、どのような個人情報が収集され、どのように処理される機能があるかを説明しなければならない。 **対象外(NA)となるための条件** 個人情報を収集・処理する機能を有しない場合(「対象外(NA)となることの理由」に、個人情報を収集・処理する機能を有しないと記載すること)。 **セキュリティ要件番号 ：S3.1-40** **★3 セキュリティ要件** IoT 製品がログ(テレメトリデータ、監査ログ)の収集にあたり、それに個人情報(個人関連情報を含む)が含まれる場合、収集する個人情報は監査の目的を達成するために必要最小限な範囲にとどめなければならない。 **対象外(NA)となるための条件** ログに個人情報が含まれない場合(「対象外(NA)となることの理由」に、ログに個人情報が含まれないことを記載すること)。	**セキュリティ要件番号 ：S3.1-39** **★3 セキュリティ要件** 製造業者は IoT 製品から得られた個人情報が処理される場合、どのような個人情報が収集され、どのように処理される機能があるかを説明しなければならない。 **対象外(NA)となるための条件** IoT 製品が個人情報を収集・処理しない場合。 **セキュリティ要件番号 ：S3.1-40** **★3 セキュリティ要件** IoT 製品がログ(テレメトリデータ、監査ログ)を収集し、それに含まれる個人情報の処理を行う場合、以下の基準を満たさなければならない。 ① 個人情報の処理を、意図された機能にとって必要最小限のものに留めること。 **対象外(NA)となるための条件** IoT 製品がログ(テレメトリデータ、監査ログ)を取得しない又は IoT 製品がログ(テレメトリデータ、監査ログ)を取得するが、個人情報の処理を行わない場	●監査ログに含まれる個人情報について、監査目的で利用する場合と、個人情報を監査以外の目的で利用する場合とに大別できることから、「個人情報を含む監査ログを監査目的で利用」するか「それに該当しないか」で整理し、3 つの要件を 2 つに再集約 ●この集約に伴い、修正前の S3.1-41 以降のセキュリテ

	合。(「NA であることの理由」に、IoT 製品からログ(テレメトリデータ、監査ログ)を取得しない又は機器からログ(テレメトリデータ、監査ログ)を取得するが、個人情報の処理を行わないことを示す根拠を記載すること) **セキュリティ要件番号 :S3.1-41** **★3 セキュリティ要件** 製造業者は、IoT 製品がどのようなログ(テレメトリデータ・監査ログ)を記録し、どのような目的で使用するかについてユーザに開示しなければならない。 **対象外(NA)となるための条件** 該当事項なし	ィ要件番号が 1 つ繰り上がり、全要件数が 4 7 から 4 6 になる。
セキュリティ要件番号 :S3.1-44 **★3 セキュリティ要件** 製造業者は、IoT 製品のセキュリティに関する情報提供について、以下の①～⑤のすべての要件を満たす対応を行わなければならない。 ① 初期設定の方法など、IoT 製品の利用上、セキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。 ② IoT 製品のセキュリティアップデートのリリース時にそのアップデートの内容や必要性、アップデートを行わない場合の影響などを周知する仕組みがあること。 ③ アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。 ④ 対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。 ⑤ IoT 製品内にセキュア保存情報が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む IoT 製品の安全な利用終了方法を	**セキュリティ要件番号 :S3.1-45** **★3 セキュリティ要件** 製造業者は、IoT 製品のサイバーセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行わなければならない。 ① 初期設定の方法など、IoT 製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。 ② IoT 製品のセキュリティアップデートのリリース時にそのアップデートの内容や必要性、アップデートを行わない場合の影響などを周知する仕組みがあること。 ③ アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。 ④ 対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。 ⑤ IoT 製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む IoT 製品の安全な利用終了方法を	●基準から要件へ修正 ●S3.1-39～41 の 3 つを S3.1-39～40 と 2 つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ ●用語の統一 ●本要件で該当する「守るべき情報資産」を「セキュア保存情報」に再定義したことによる文言の修正

周知すること。	周知すること。	
セキュリティ要件番号：S3.1-23 **★3 セキュリティ要件** IoT 製品において、外部からサイバー攻撃を受けるリスクを低減するために、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とともに、IoT 製品に対する脆弱性検査を実施しなければならない。具体的には、以下の①・②のすべての要件を満たさなければならない。 (略) **セキュリティ要件番号：S3.1-30** **★3 セキュリティ要件** IoT 製品にサードパーティコンポーネントを組み込む際に、既知の脆弱性が含まれないよう、以下の①・②のすべての要件を満たすプロセスを採用していなければならない。 (略) **セキュリティ要件番号：S3.1-44** **★3 セキュリティ要件** 製造業者は、IoT 製品のセキュリティに関する情報提供について、以下の①～⑤のすべての要件を満たす対応を行わなければならない。 (略)	**セキュリティ要件番号：S3.1-23** **★3 セキュリティ要件** IoT 製品において、外部からサイバー攻撃を受けるリスクを低減するために、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とともに、IoT 製品に対する脆弱性検査を実施しなければならない。具体的には、以下の①・②のすべての基準を満たさなければならない。 (略) **セキュリティ要件番号：S3.1-30** **★3 セキュリティ要件** IoT 製品にサードパーティコンポーネントを組み込む際に、既知の脆弱性が含まれないよう、以下の①・②のすべての基準を満たすプロセスを採用していなければならない。 (略) **セキュリティ要件番号：S3.1-45** **★3 セキュリティ要件** 製造業者は、IoT 製品のセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行わなければならない。 (略)	●基準から要件へ修正 ●S3.1-39～41 の 3 つを S3.1-39～40 と 2 つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ
セキュリティ要件番号：S3.1-10 **対象外(NA)となるための条件** 脆弱性対応をアップデートではない代替手段によって行う(「対象外(NA)となることの理由」に、アップデートによらずに脆弱性対応ができることの根拠を記載すること)。	**セキュリティ要件番号：S3.1-10** 「対象外(NA)となるための条件」の記述無し	●対象外（NA）となるための条件が不足している箇所に「対象外（NA）と

セキュリティ要件番号 ：S3.1-11 **対象外(NA)となるための条件** 脆弱性対応をユーザによるアップデートではない代替手段によって行う(「対象外(NA)となることの理由」に、ユーザによるアップデートによらずに脆弱性対応ができることの根拠を記載すること)。	**セキュリティ要件番号 ：S3.1-11** 「対象外(NA)となるための条件」の記述無し	なるための条件」を追加
セキュリティ要件番号 ：S3.1-05 **対象外(NA)となるための条件** 認証のために電子証明書を使用していない(「対象外(NA)となることの理由」に、認証のために電子証明書を使用していないと記載すること)。 **セキュリティ要件番号 ：S3.1-06** **対象外(NA)となるための条件** SSH を公開鍵認証にて利用していない(「対象外(NA)となることの理由」に、SSH を公開鍵認証にて使用していないと記載すること)。 **セキュリティ要件番号 ：S3.1-07** **対象外(NA)となるための条件** IoT 製品に VPN ゲートウェイ機能を持たない(「対象外(NA)となることの理由」に、VPN ゲートウェイ機能を持たないと記載すること)。 **セキュリティ要件番号 ：S3.1-22** **対象外(NA)となるための条件** IoT 製品に無線 LAN 機能を持たない(「対象外(NA)となることの理由」に、無線 LAN 機能を持たないことを記載すること)。	**セキュリティ要件番号 ：S3.1-05** **対象外(NA)となるための条件** IoT 製品において、認証のために電子証明書を使用していない。 **セキュリティ要件番号 ：S3.1-06** **対象外(NA)となるための条件** IoT 製品において、SSH を公開鍵認証にて利用していない。 **セキュリティ要件番号 ：S3.1-07** **対象外(NA)となるための条件** IoT 製品において、VPN ゲートウェイ機能を持たない。 **セキュリティ要件番号 ：S3.1-22** **対象外(NA)となるための条件** IoT 製品において、無線 LAN 機能を持たない。	●対象外（NA）となるための条件に説明が不足している箇所に説明を追加

セキュリティ要件番号 ：S3.1-41 **対象外(NA)となるための条件** 個人情報を収集・処理する機能を有しない場合(「対象外(NA)となることの理由」に、「個人情報を収集・処理する機能を有しない」と記載すること)。	**セキュリティ要件番号 ：S3.1-42** **対象外(NA)となるための条件** IoT 製品が個人情報を収集・処理しない場合。	●対象外（NA）となるための条件の説明を修正 ●S3.1-39～41 の 3 つを S3.1-39～40 と 2 つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ
セキュリティ要件番号 ：S3.1-01, S3.1-02, S3.1-03, S3.1-04, S3.1-11,S3.1-14, S3.1-28, S3.1-36, S3.1-43 **要件の補足説明** 【用語：ユーザ】 ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品へのアクセスができる当該 IoT 製品を使用する自然人及び組織すべてを含んでいなければならない。 **セキュリティ要件番号 ：S3.1-35** **要件の補足説明** 【用語：監査ログ】 セキュリティ上の異常を検知できるようにするため、製品の処理内容やプロセス、及び操作の履歴を、時系列かつ連続的に記録したデータを指す。	**セキュリティ要件番号 ：S3.1-01, S3.1-02, S3.1-03, S3.1-04, S3.1-11,S3.1-14, S3.1-28, S3.1-36, S3.1-44** **基準の補足説明** 【用語定義：ユーザ】 ユーザの対象範囲には、IoT 製品の利用者、管理者、ベンダーのカスタマーエンジニア、所有者等、当該 IoT 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品を使用する自然人及び組織すべてを含んでいなければならない。 **セキュリティ要件番号 ：S3.1-35** **基準の補足説明** 【用語定義：監査ログ】 ユーザが製品におけるセキュリティ上の異常を検知できるようにするため、製品の処理内容やプロセス、及び操作の履歴を、時系列かつ連続的に記録したデータを指す。	●基準から要件に修正 ●S3.1-39～41 の 3 つを S3.1-39～40 と 2 つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ ●説明の修正
セキュリティ要件番号 ：S3.1-09、S3.1-13、S3.1-14、S3.1-15、S3.1-16、S3.1-19、S3.1-21、S3.1-23、S3.1-24、S3.1-25、S3.1-26、S3.1-27、S3.1-28、S3.1-29、S3.1-31、S3.1-33、S3.1-34、S3.1-35、S3.1-36、S3.1-37、S3.1-38、S3.1-	**セキュリティ要件番号 ：S3.1-09、S3.1-13、S3.1-14、S3.1-15、S3.1-16、S3.1-19、S3.1-21、S3.1-23、S3.1-24、S3.1-25、S3.1-26、S3.1-27、S3.1-28、S3.1-29、S3.1-31、S3.1-33、S3.1-34、S3.1-35、S3.1-36、S3.1-37、S3.1-38、S3.1-**	●「対象外(NA)となるための条件　該当事項なし」場合

<table>
<tr>
<td>42、S3.1-43、S3.1-44、S3.1-45、S3.1-46
対象外(NA)となるための条件
該当事項なし</td>
<td>43、S3.1-44、S3.1-45、S3.1-46、S3.1-47
「対象外(NA)となるための条件」の記述無し</td>
<td>の記載を以下に追加
●S3.1-39～41 の３つを S3.1-39～40 と２つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ</td>
</tr>
<tr>
<td>セキュリティ要件番号 ：S3.1-04、S3.1-07、S3.1-11、S3.1-14、S3.1-28、S3.1-35、S3.1-43、S3.1-44
要件の補足説明
(略)</td>
<td>セキュリティ要件番号 ：S3.1-04、S3.1-07、S3.1-11、S3.1-14、S3.1-28、S3.1-35、S3.1-44、S3.1-45
基準の補足説明
(略)</td>
<td>●基準から要件へ修正
●S3.1-39～41 の３つを S3.1-39～40 と２つに統合したことによる、S3.1-41 以降の要件番号の繰り上げ</td>
</tr>
<tr>
<td>Appendix A: 用語集
<table><tr><td>SSP (Sensitive Security Parameter)</td><td>CSP と PSP を合わせた情報資産のこと。</td></tr><tr><td>VPN ゲートウェイ機能</td><td>内部ネットワークとインターネット等の外部ネットワークの境界に置かれ、利用者が利用する機器との間に暗号化された通信経路を作成する機能のこと。</td></tr></table></td>
<td>Appendix A: 用語集
<table><tr><td>SSP (Sensitive Security Parameter)</td><td>CSP(Critical Security Parameter)に以下の要素を加えたもの
・ソフトウェア検証に使用される公開鍵
・証明書の公開要素
・機器固有の ID</td></tr><tr><td>VPN ゲートウェイ機能</td><td>内部ネットワークとインターネット等の外部ネットワークの境界に置かれ、ユーザーとの間に暗号化された通信経路を作成する機能</td></tr></table></td>
<td>●「SSP」、「VPN ゲートウェイ機能」、「ネットワーク負荷状態」の説明を修正
●「保護されたネットワーク」の説明を削除</td>
</tr>
</table>

（削除）		保護されたネットワーク	・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	
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できない状態。	ネットワーク過負荷状態	IoT 機器から外部へ通信が行えない状態	