



Federal Office  
for Information Security

# 技術ガイドライン TR-03183 : 製造者と製品に対する サイバーレジリエンス要件

パート 1 : 一般要求事項



# 文書履歴

バージョン	日付	説明
0.9.0	2024-09-20	初稿

表 1 : 履歴

連邦情報セキュリティ局

私書箱 20 03 63

53133 ボン

ドイツ

E メール [TR03183@bsi.bund.de](mailto:TR03183@bsi.bund.de)

インターネット : <https://www.bsi.bund.de>

連邦情報セキュリティ局 2024

目次

# 目次

<b>1. はじめに</b> .....	<b>5</b>
1.1 重要な注意事項.....	6
<b>2. 要求言語</b> .....	<b>7</b>
<b>3. 基本事項</b> .....	<b>8</b>
3.1 セキュリティの目的と範囲.....	8
3.2 役割.....	8
3.2.1 消費者/ユーザ.....	8
3.2.2 製造者.....	9
3.2.3 評価者.....	9
3.3 適合性評価.....	9
3.3.1 評価対象 (TOE) .....	9
3.3.2 評価の時期.....	9
3.3.3 要件構造.....	10
3.3.4 評価手順.....	10
<b>4 リスク評価</b> .....	<b>12</b>
4.1 重要な注意事項.....	12
4.2 REQ_RA 1 - リスクアセスメント.....	12
4.2.1 REQ_RA 1.1.....	12
<b>5. セキュリティ要件</b> .....	<b>14</b>
5.1 重要な注意事項.....	14
5.2 適用ガイダンス.....	14
5.3 製品特性に関連する必須要件.....	16
5.3.1 REQ_ER 1 - デザインによるセキュリティ.....	16
5.3.2 REQ_ER 2 - 既知の脆弱性はない.....	16
5.3.3 REQ_ER 3 - 安全なデフォルト設定.....	17
5.3.4 REQ_ER 4 - セキュリティアップデート.....	18
5.3.5 REQ_ER 5 - アクセス制御.....	20
5.3.6 REQ_ER 6 - 機密保護.....	23
5.3.7 REQ_ER 7 - 完全性保護.....	26
5.3.8 REQ_ER 8 - データの最小化.....	27
5.3.9 REQ_ER 9 - 必須および基本的機能の利用可能性.....	28
5.3.10 REQ_ER 10 - マイナス影響の最小化.....	29
5.3.11 REQ_ER 11 - 攻撃面を制限する.....	30
5.3.12 REQ_ER 12 - インシデントの緩和.....	31
5.3.13 REQ_ER 13 - 記録とモニタリング.....	31

5.3.14 REQ_ER 14 - データと設定の削除.....	34
5.4 脆弱性の取り扱いに関する必須要件 .....	36
5.4.1 REQ_VH 1 - コンポーネントとバーネラビリティを特定する .....	37
5.4.2 REQ_VH 2 - 脆弱性に対処する.....	37
5.4.3 REQ_VH 3 - 定期検査 .....	38
5.4.4 REQ_VH 4 - 対応済みの脆弱性を公表する .....	39
5.4.5 REQ_VH 5 - 協調的な脆弱性開示ポリシー .....	40
5.4.6 REQ_VH 6 - アップデートの安全な配布 .....	40
5.4.7 REQ_VH 7 - アップデートの普及.....	41
<b>6 文書作成義務 .....</b>	<b>42</b>
6.1 技術文書.....	42
6.1.1 REQ_TD 1 - 一般文書 .....	42
6.1.2 REQ_TD 2 - プロセスの文書化.....	42
6.1.3 REQ_TD 3 - サイバーセキュリティリスクの文書化 .....	43
6.1.4 REQ_TD 4 - サポート期間の文書化 .....	43
6.1.5 REQ_TD 5 - 実施した試験の文書化 .....	44
6.1.6 REQ_TD 6 - コンポーネントの文書化 .....	44
6.2 ユーザ文書.....	45
6.2.1 REQ_UD 1 - 製造者の文書化 .....	45
6.2.2 REQ_UD 2 - 固有識別子の文書化.....	45
6.2.3 REQ_UD 3 - 使用目的の文書化.....	45
6.2.4 REQ_UD 4 - サポート期間の文書化.....	46
6.2.5 REQ_UD 5 - ユーザガイダンス.....	47
6.2.6 REQ_UD 6 - コンポーネントの文書化 .....	48
<b>7 附属書.....</b>	<b>49</b>

# 1. はじめに

サイバーセキュリティの脆弱性に関する緊迫した状況には、複数の理由がある。主な理由としては、第一に、デジタル要素を含む製品のサイバーセキュリティに関する成熟度が低いこと、第二に、脆弱性に対処するためのセキュリティ更新プログラムの提供が不十分で一貫性がないことが挙げられる。さらに、ユーザが適切なレベルのサイバーセキュリティを備えた製品を選択し、安全に使用するための情報にアクセスできないことも挙げられる。利用者は、使用しているソフトウェアに悪用可能な既知の脆弱性があるかどうかを評価することが困難である。例えば、多くのサイバーセキュリティ管理者は、導入している製品が Log4shell の脆弱性の影響を受けているかどうかについての情報を持っていなかったり、製造者から必要な情報を受け取るまでに長い時間を待たなければならなかったりした。したがって、サイバー攻撃や技術的混乱に対する回復力を高めることは、行政、企業、社会にとってのサイバーセキュリティの脅威状況をもたらす悪影響を軽減するための重要な課題である。したがって、すべての製品は少なくとも基本的なサイバーセキュリティ要件を満たす必要がある。これには、上記のようなサイバーセキュリティ・レベルやアップデートだけでなく、どの製品が適切なサイバーセキュリティ・レベルを有しているかについてのユーザの教育も含まれる。

サイバーレジリエンス法 (CRA) <sup>1</sup> は、欧州連合 (EU) 域内市場全体に対するサイバーセキュリティの水平的な法的枠組みを構築するものである。CRA は、EU 域内市場にデジタル要素を含む製品を流通させるためのサイバーセキュリティ要件を定めるものである。これには、デジタル要素を含むすべての製品が準拠しなければならないサイバーセキュリティレベルの最低要件が含まれる。

本技術ガイドライン (TR) は、CRA 附属書 I (必須要求事項) 及び附属書 II (使用者に対する情報及び指示事項) に記載された、又は附属書 II から導き出された (セキュリティ) 目的に基づく要求事項、推奨事項、試験方法及び評価基準という形で、デジタル要素を含む製品の製造者が来るべき CRA に備えることを支援することを意図している。

本技術ガイドラインへのフィードバックは、デジタル要素を含む製品のサイバーセキュリティ要件に関する欧州連合の政策を支援するための標準化要求の草案に関する現在および将来の作業へのインプットとなる。この要請は、特に整合規格となることを目指した標準化成果物の開発を求めている。これらの整合規格に適合することで、その範囲内での適合が推定されることになる。

- 本技術ガイドラインは、今後、生きている文書としてさらに適応されていく：  
本技術ガイドラインは、CRA の欧州標準化努力の過程で、生きた文書として適応され、要求事項がさらに具体化される可能性がある。
- その内容が、上述の標準化要請の下、対応する標準化成果物でカバーされ次第、現行の形で置き換えられる。

---

<sup>1</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html)

## 1.1 重要な注意事項

本技術ガイドラインにおける適合性は、本技術ガイドラインの要求事項にのみ適用され、必ずしも CRA に記載された要求事項に適用されるものではない。本技術ガイドラインは、今後予定されている欧州規制の最初の解釈を示すものである。

- **警告：**本技術ガイドラインの適用は、今後予定されている CRA および CRA に起因するいかなる法的義務にも取って代わるものではない：  
本技術ガイドラインの適用は、今後予定されている CRA および CRA に起因する法的義務に取って代わるものではない。
- これらの義務を果たすことを保証するものではない。

## 2. 要求言語

本文書のキーワード "MUST"、"MUST NOT"、"REQUIRED"、"SHALL"、"SHALL NOT"、"SHOULD"、"SHOULD NOT"、"RECOMMENDED"、"NOT RECOMMENDED"、"MAY"、および "OPTIONAL" は、ここに示すように、すべて大文字で表示される場合に限り、BCP 14<sup>2</sup>（RFC 2119<sup>3</sup>、RFC 8174<sup>4</sup>）に記述されているとおりに解釈される。

---

<sup>2</sup> <https://www.rfc-editor.org/info/bcp14>

<sup>3</sup> <https://www.rfc-editor.org/rfc/rfc2119>

<sup>4</sup><https://www.rfc-editor.org/rfc/rfc8174>

## 3. 基本事項

### 3.1 セキュリティの目的と範囲

本技術ガイドラインに記載された要件は、市場に投入されたデジタル要素を含むすべての製品に適用され、その中にはリモートデータ処理ソリューションも含まれる。本ガイドラインは、主に直接製品、及び対応するリモートデータ処理ソリューションとの通信及び相互作用に焦点を当てる。リモート・データ・プロセッシング・ソリューションの運用に関する組織的要件は、この文書には含まれず、情報セキュリティ・マネジメント・システム（ISMS）のベスト・プラクティス、例えば "IT-Grundschutz"<sup>5</sup> に基づく ISO 27001 に従うべきである。

本技術ガイドラインに記載された要件は、例えば、一般家庭のユースケースや、クリティカルでないビジネスプロセスの専門的なユースケースで通常考えられる基本的な脅威を軽減することを意図している。一般に、デジタル要素を含む製品のセキュリティ特性は、製造者が決定した製品の意図された目的と合理的に予見可能な用途に適切でなければならず、それに応じて設計、製造、保守されなければならない。

本技術ガイドラインの要求事項は、技術や製品にとらわれないレベルでのアセスメントに使用できる。特に、5.3 項の必須要求事項の実施は、製品の種類、意図された目的及び合理的に予見可能な使用方法によって大きく異なる可能性があるためである。このような状況に対応するため、本技術ガイドラインでは、要求事項が適用される場合を示すガイダンスを示す。

本文書は、現状での評価に使用することができる。しかしながら、ユースケースに応じて要求事項の実装を容易にするため、将来的に追加の技術情報や例を提供する予定である。

セクション 5.4 の脆弱性処理プロセスに関する要求事項およびセクション 6 の文書化義務は、一般的にあらゆる種類の製品に有効であり、製品の意図された目的や予見可能な使用方法とは無関係である。

### 3.2 役割

本技術ガイドラインに記載されている要求事項は、以下のエンティティ間の相互作用に基づいている。

#### 3.2.1 消費者／ユーザ

本技術ガイドラインの適用範囲に含まれる消費者とは、個人または業務用として製品を購入する最終消費者である。一般的に、消費者はこれらの製品を商業的に再配布／再販することはない。消費者とユーザという用語は同じ意味で使用される。

サプライチェーンの一部として、消費者がデジタル要素を持つ製品を、デジタル要素を持つ新製品の

---

<sup>5</sup> [https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/ITGrundschutz/it-grundschutz\\_node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/ITGrundschutz/it-grundschutz_node.html)

部品として再利用し、市場に出す場合、消費者は製造者の役割を担うことになる。

### 3.2.2 製造者

CRA は「製造者」を、デジタル要素を含む製品を開発・製造する、またはデジタル要素を含む製品を設計・開発・製造させ、収益化・無償を問わず、その名称または商標で販売する自然人または法人と定義している。

CRA は市場アクセス規制であるため、「製造者」は「ベンダー」と「クリエイター」の役割を兼ね備えていると解釈される。

「ベンダー」(独: "Anbieter") は、製品にデジタル要素を提供する主体の役割を表す。また、必ずしも商業的な背景があるわけではないが、「サプライヤー」(ドイツ語: "Lieferant") という用語も使われる。

「クリエイター」(ドイツ語では「Ersteller」) は、デジタル要素を含む製品をオーサリングまたは作成したエンティティの役割を表す。

本技術ガイドラインは、技術的要求事項を規定するものであるため、異なる用語を使用し、「製造者」を、機器等の有形財を製造する事業者と、ソフトウェア及びソフトウェア部品等の無形財を創造又は提供する事業者の組み合わせとして解釈している。したがって、本技術ガイドラインでは、CRA が定義する「経済的事業者」、「流通業者」、「輸入業者」については、これらの当事者の役割はここに記載する技術的要件とは無関係であるため、言及しない。これらの技術的要件は、それを満たす役割とは無関係である。

### 3.2.3 評価者

本技術ガイドラインの要求事項に評価基準を適用する主体。評価者は、製造者自身又は第三者試験機関とすることができる。

## 3.3 適合性評価

本技術ガイドラインに規定された要求事項に対する適合性評価は、製造者による自己評価、または製造者に代わって第三者適合性評価機関による評価が中心である。

本技術ガイドラインには、5.3 項と 5.4 項に記載された要求事項に関する具体的な実施案は含まれていない。それらは追加ガイダンス文書で提供される予定である。

### 3.3.1 評価対象 (TOE)

適合性評価は、評価対象 (TOE) である製品の単一インスタンス (デジタル要素を含む) に対して実施される。TOE には、評価時に製品の一部である、製品のすべての部品とそのリモートデータプロセッシングソリューションが含まれる。

### 3.3.2 評価の時期

本技術ガイドラインに規定されたすべての要件は、TOE が意図された耐用年数全体にわたって満たされなければならない。

- TOE がユーザによって安全でない状態に変更されることは避けられないため、ユーザマニュアルの推奨事項に従った初期設定と、(潜在的な) 最新バージョンへのアップデート後の状態のみが評価に関係する。この状態は、以下の手順を実行することで達成できる：  
新しい製品を入手するか、工場出荷時のリセットや新規インストールなど、製品を元の状態にリセットする。
- 取扱説明書の推奨事項に従い、製品の起動と初期設定を行う。
- もし初期セットアップ中にアップデートが行われなかった場合は、最新のソフトウェア・バージョンへのアップデートを行う。

### 3.3.3 要件構造

- 各要件は以下の部分で構成される：  
**要求事項/推奨事項**：要件/推奨：TOE が満たさなければならない本技術ガイドラインの要件/推奨。これらの記述は、対応するモーダル動詞によって示されるように、推奨または必須である。
- **条件** (オプション)：条件付き要求事項/推奨事項は、その条件が満たされた場合に製品に適用される。条件は、どの要求事項が製品に適用されるかを製造者に示すことを意図している。
- **評価基準**：評価基準：本技術指針の適合性評価を行うために評価者が適用する必要がある単位及び基準。

### 3.3.4 評価手順

本節では、本技術ガイドラインに記載されているセキュリティ要求事項及び推奨事項が満たされていることを評価する方法について、評価手順を規定する。再現性と一貫性を確保するために、評価中に行われたすべての決定、使用された方法及び結果は、6.1 項に従って評価者によって文書化されなければならない。評価者は、各要件及び推奨事項に対して、以下の順序を適用する：

1. 条件をチェックし、要件または勧告が該当するかどうかを確認する。該当する場合、または条件が与えられていない場合は、次の評価ステップに進む。要件または勧告が適用されない場合は、要件を「該当なし」とマークし、その決定を文書化し、次の要件に進む。
2. 評価基準の各ステップを実行し、結果を評価し、要件または勧告に「PASS」、「FAIL」、または「INCONCLUSIVE」のいずれかをマークする。すべての評価ステップが正常に実行された場合、要件または推奨は「PASS」とマークされ、そうでない場合は「FAIL」とマークされる。評価ステップの実行は、しばしば「assessment that/if/whether」で示される評価を含む。評価者による被評価財産の評価が肯定的である場合のみ、評価ステップは正常に完了することができる。評価者が評価された特性を疑いなく証明できないために評価ステップを完了できない場合、テストステップは不合格となり、要求事項または勧告は "INCONCLUSIVE" とマークされる。

要求事項と推奨事項には、ファーストアセスメントとサードパーティアセスメントに柔軟性を持たせ

るため、アセスメントの証拠や手順に関する詳細は含まれていない。一般的に、アセスメントは少なくとも概念的なレベルで実施されるものと想定される。概念的な評価には、別途文書がない場合、設定ファイルやソースコードの検査も含まれる。

実行可能であれば、この手順は、機能評価、すなわち TOE の実際の動作の評価、または実装されたプロセスの監査またはレトロスペクティブ検査によって強化されなければならない。機能評価を実施できない場合、評価者は機能評価を実施しない十分な理由を文書化しなければならない。

評価は、可能であれば自動化された形で、開発プロセスや継続的品質保証プロセスに組み込まれることが望ましい。

- 評価ステップには、以下の用語のいずれかが含まれる可能性があり、それらは評価者によって解釈されなければならない：  
**チェックする**：単純な比較によって結果を生成する。
- **評価する**：評価者の専門知識を用いた分析によって結果を出す。
- **ベストプラクティス**：この要件は、特定のユースケースにおいて最新技術とみなされるものに従って実装されなければならない。この表現は主に暗号と組み合わせて使用される。例えば、BSI TR-02102、SOG-IS Agreed Cryptographic Mechanisms、または同等の標準などである。
- **過度な遅れは許されない**：要求された処置はできるだけ早く実行されなければならない。評価者は、要求された処置が特定のシナリオに必要な時間を大幅に超えない時間で実行されたかどうかを評価しなければならない (MUST)。比較のために、他の類似した現実のシナリオを使用してもよい [MAY]。疑問がある場合、評価者は製造者に追加情報を要求し、遅延を正当化し、製造者が可能な限り早急に対応したことを確認してもよい (MAY)。
- **文書化し、公表する**：要件に「文書化しなければならない」と記載されている場合、これは製造者が記録を保有していることを意味するが、その記録は必ずしも一般に公開されているとは限らない。公開とは、何かが文書化され、一般公開されていることを意味する。
- 該当する必須要件 (MUST) がすべて「PASS」とマークされ、該当する推奨事項 (SHOULD) がすべて「PASS」とマークされている場合、総合判定は「PASS」となる：  
「PASS」または
- "FAIL" または "INCONCLUSIVE" とし、勧告に適合しない理由を十分に説明する。

そうでなければ、総合的な評価は「不合格」である。

## 4 リスク評価

TOE に関連するサイバーセキュリティリスクを評価するために、製造者はリスク評価を実施する必要があります。TOE に関連するリスクの全体像を把握するために、リスクアセスメントは TOE の完全なライフサイクルを考慮する必要があります。これには、計画、設計、開発、製造段階、および納入、保守段階/サポート期間、ユーザによる廃棄が含まれる。リスクアセスメントはまた、製品の意図された目的と、顧客による合理的に予見可能な使用も考慮しなければならない。意図された目的と合理的に予見可能な使用に基づいて、製造者は、潜在的な脅威と脅威要因、およびそれらの発生確率と TOE のセキュリティへの影響（消費者の健康と安全に対するリスクを含む）を導き出さなければならない。

### 4.1 重要な注意事項

本技術ガイドラインのリスクアセスメントの焦点は、特定の製品について、必須要件と必要な追加セキュリティ機能の実装の詳細を特定することである。

**警告：**本技術ガイドラインのリスクアセスメントは、5.3 項の要求事項を省略するために使用してはならない。

### 4.2 REQ\_RA 1 - リスクアセスメント

**CRA Annex I Part 1 の現行草案に記載されている要件：**デジタル要素を含む製品は、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、製造されなければならない。

#### 4.2.1 REQ\_RA 1.1

##### 要件

- 製造者は TOE のリスクアセスメントを実施し、文書化しなければならない。
- リスクアセスメントの一環として、製造者はサポート期間をどのように決定し、それが TOE のライフサイクルにどのように影響するかを文書化しなければならない (MUST)。

##### 評価基準

- 評価者は、TOE のリスクアセスメントが実施され、文書化されていることを評価しなければならない。
- 評価者は、TOE のリスクアセスメントに脅威と脅威エージェントが含まれていることを評価しなければならない (MUST)。
- 評価者は、TOE のリスクアセスメントに関連する脅威のセキュリティ影響と確率が含まれていることを評価しなければならない (MUST)。

- 評価者は、TOE のリスクアセスメントが、サポート期間がどのように決定され、それが TOE のライフサイクルにどのように影響するかを文書化していることを評価しなければならない。

## 5. セキュリティ要件

サードパーティのコンポーネントを使用する場合も含め、TOE のライフサイクル（計画、設計、開発、製造、引渡し、保守、ユーザによる廃棄）を通して、またサポート期間中も含めて、サイバーセキュリティリスクを最小化するために、製造者は、少なくとも 5.3 節に規定される必須要件への自社製品の適合性を確保しなければならない。これらは、ベストプラクティスに従って、サイバーセキュリティの適切なベースラインレベルを確保することを意図している。

本技術ガイドラインは、完全性を主張するものではなく、また、特定の製品や製造者によって決定される関連リスクに大きく依存するため、オーダーメイドの解決策を提供するものでもない。

### 5.1 重要な注意事項

本技術ガイドラインへの適合については、4.2 項のリスクアセスメントに基づき、5.3 項の要求事項を省略することはできない。

**警告：**このアプローチは、CRA のリスクベースアプローチよりも柔軟性に欠ける。

### 5.2 適用ガイダンス

特定のリスクアセスメントとは関係なくとも、各要件をいつ適用しなければならないかについての指針を示すために、以下の指標を用いる。

TOE がどのようなデータ資産を保存または処理するか、例えばシステムデータ、個人データ、重要なセキュリティデータなどを考慮しなければならない。

#### システムデータ：

一般的な非重要かつ非機密（セキュリティ）データであり、特定の人物に関連せず、データの可用性、完全性、機密性が危険にさらされた場合でも、TOE のセキュリティおよびユーザの安全・セキュリティに関連する影響を及ぼさないもの。

#### 機微なシステムデータ：

特定の個人とは関係がなく、TOE のセキュリティに関連する影響もないが、データの可用性、完全性、機密性が損なわれた場合に、金銭的またはその他の損害、またはユーザの安全やセキュリティに重大な影響を与える可能性があるデータ。これには、例えば業務上の機密情報や監視カメラの録画などが含まれる。

#### 個人データ：

特定の個人に関する一般的なデータで、データの可用性、完全性、機密性が危険にさらされた場合でも、ユーザに重大な損害を与える可能性のないもの。これには氏名や公開写真などが含まれる。

#### 機微な個人データ：

特定の個人に関するデータで、データの可用性、完全性、機密性が損なわれた場合に、利用者に重大な損害が発生する可能性があるもの。これには、健康データ、個人的なメッセージ、個人的な財務情報が含まれる。

### **セキュリティ・データ：**

特定の個人とは関係ないが、データの可用性、完全性、機密性が損なわれた場合に TOE のセキュリティに重大な影響を与えるセキュリティ関連データ。これには、パスワード、セキュリティ上重要な設定などが含まれる。

### **重要なセキュリティ・データ：**

特定の個人とは関係ないが、データの完全性と機密性が損なわれた場合に TOE や他の製品のセキュリティに重大な影響を与えるセキュリティ関連データ。これにはマスターキーなどが含まれる。

もう一つの基準は、潜在的な攻撃対象と機会である。これは、TOE がデジタル要素を持つ他の製品とどのように通信し、どのように物理的にアクセスできるかに関連する。ローカル・インターフェースを介してのみ通信する TOE は、パブリック・ネットワークに常時接続する TOE よりも、セキュリティに関するリスクが低い可能性がある。

### **公衆ネットワーク：**

TOE は WAN (Wide Area Network) を介して通信する。

### **ローカル・ネットワーク：**

TOE はローカルネットワーク (WLAN、Bluetooth など) を介して通信するが、WAN にアクセスする機能はない。

### **ローカル (パブリック)：**

TOE は、ネットワーク・アクセスのないローカル・インターフェース (USB、NFC、ローカル・アプリケーション・プログラミング・インターフェース (API) など) を使用する。TOE は公共の場で使用されることが予想され、自動化されたキオスク端末のように、実質的な時間内に誰でもローカルに操作することができる。

### **ローカル (制限付き公開)：**

TOE は、ネットワークアクセスのないローカル・インターフェース (USB、NFC、ローカル・アプリケーション・プログラミング・インターフェース (API) など) を使用する。TOE は公共の場で使用されることが予見され、短期間であれば監視なしで誰でもローカルに操作できる。

### **ローカル (制限付き)：**

TOE は、ネットワーク・アクセスのないローカル・インターフェース (USB、NFC、ローカル・アプリケーション・プログラミング・インターフェース (API)) を使用する。TOE は物理的に制限された環境で使用されることが予想され、例えばホームエンターテイメント用のスマート TV やオフィスのプリンタなど、選ばれた個人のみがアクセスできる。

本技術ガイドラインに記載されたセキュリティ要件は、TOE のデータ資産または通信能力に依存する場合がある。これは対応する条件によって示される。

TOE が通信能力に基づく要件を満たさない場合、その要件を別のプロキシ製品に委任することで、通信に関連するリスクを移転することが可能である。これは、例えばリモートネットワーク通信のためにプロキシとの信頼関係を確立するなどして、TOE が関連する通信がプロキシ製品を介してのみ可能であることを保証する場合にのみ可能である。

この条件は、要件が適用されるかどうかの判断を容易にするためのガイダンスである。

## 5.3 製品特性に関連する必須要件

### 5.3.1 REQ\_ER 1 - デザインによるセキュリティ

**CRA 附属書 I パート 1 の現行草案に記載されている要件：** デジタル要素を含む製品は、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、製造されなければならない。

#### 5.3.1.1 REQ\_ER 1.1

##### 要件

- 製造者は、4.2 項のリスクアセスメントに基づき、適切なレベルのサイバーセキュリティで TOE が設計、開発、製造されることを保証するプロセスを文書化し、実施しなければならない。

##### 評価基準

- 評価者は、プロセスがリスクアセスメントに基づき、文書化されたリスクに対する適切な緩和 戦略を含んでいることを評価しなければならない (MUST)。

#### 5.3.1.2 REQ\_ER 1.2

##### 要件

- 製造者は、OWASP SAMM、BSI TR-03185、ISO 27034 など、安全な (ソフトウェア) 開発ライフサイクルのベストプラクティスに従わなければならない。

##### 評価基準

- 評価者は、文書化されたプロセスに、OWASP SAMM、BSI TR-03185、ISO 27034 などに従った、安全なガバナンス、設計、実装、上市前および上市後の製品のテストのためのベストプラクティスが含まれていることを評価しなければならない (MUST)。

### 5.3.2 REQ\_ER 2 - 既知の脆弱性はない

**CRA 附属書 I 第 1 部の現行草案に記載された要件：** 第 13 条(2)で言及されているサイバーセキュリティリスク評価に基づき、該当する場合、デジタル要素を含む製品は、悪用可能な既知の脆弱性がない状態で市場に提供されなければならない。

#### 5.3.2.1 REQ\_ER 2.1

##### 要件

- 製造者は、初期セットアップ中または初期セットアップ前に、TOE が利用可能な最新のソフトウェア/ファームウェアバージョンに更新されていることを確認しなければならない。

### 評価基準

- 評価者は、ユーザが最初に使用する前に、最新のセキュリティアップデートが TOE にインストールされていることを評価しなければならない。

#### 5.3.2.2 REQ\_ER 2.2

##### 要件

- 製造者は、TOE を利用可能にする前に、5.4.3.1 項に従って TOE のセキュリティ特性が正しく動作するかどうかをテストしなければならない。
- 製造者は試験結果を文書化しなければならない。
- 製造者は、TOE を利用可能にする前に、積極的に悪用されている既知の脆弱性をすべて修正しなければならない。

##### 評価基準

- 評価者は、TOE を利用可能にする前に、5.4.3.1 項に従ってテストされていることを評価しなければならない。
- 評価者は、検査結果が文書化されていることを評価しなければならない (MUST)。
- 評価者は、製造者が知っている TOE の積極的に悪用される脆弱性が、利用可能になる前に修正されていることを確認しなければならない (MUST)。

#### 5.3.2.3 REQ\_ER 2.3

##### 推薦

- 製造者は、TOE を利用可能にする前に、悪用可能な既知の脆弱性をすべて修正すべきである。

##### 評価基準

- 評価者は、製造者が知っている TOE の悪用可能な脆弱性が、利用可能になる前に修正されていることを確認すべきである (SHOULD)。

#### 5.3.3 REQ\_ER 3 - 安全なデフォルト設定

**CRA 附属書 I 第 1 部の現行草案に記載された要件：**第 13 条(2)で言及されるサイバーセキュリティリスク評価に基づき、また該当する場合、デジタル要素を搭載した製品は、デフォルトで安全な構成で市場に提供されなければならない。ただし、デジタル要素を搭載したオーダーメイドの製品に関しては、製造者と事業者の間で別途合意がない限り、製品を元の状態にリセットする可能性を含む。

### 5.3.3.1 REQ\_ER 3.1

#### 要件

- TOE は元の状態にリセットできなければならない。元の状態とは、すべてのローカルユーザデータの削除、ソフトウェアの初期バージョンまたは最新バージョンへのリセット、およびデフォルト設定のリセットである。

#### コンディション

- TOE を構成することができる。

#### 評価基準

- 評価者は、TOE が工場出荷時のリセットまたは再インストールによって元の状態に戻せることを評価しなければならない。

### 5.3.3.2 REQ\_ER 3.2

#### 要件

- TOE のソフトウェアは、ハードコードされたセキュリティデータおよび重要なセキュリティデータを含んではならない。

#### コンディション

- TOE は、TOE に固有のセキュリティ・データまたは重要なセキュリティ・データを格納する。

#### 評価基準

- 評価者は、セキュリティデータ及び重要なセキュリティデータが TOE のソフトウェアにハードコードされていないことを評価しなければならない。

### 5.3.4 REQ\_ER 4 - セキュリティアップデート

**CRA 附属書 I パート 1 の現行草案に記載されている要件：**第 13 条(2)で言及されているサイバーセキュリティ・リスク評価に基づき、該当する場合、デジタル要素を含む製品は、セキュリティ更新を通じて脆弱性に対処できることを保証しなければならない。これには、該当する場合、利用可能な更新のユーザへの通知、一時的に延期するオプションを通じて、明確で使いやすいオプトアウト・メカニズムを備えた、デフォルト設定として有効な、適切な期間内にインストールされる自動セキュリティ更新が含まれる。

#### 5.3.4.1 REQ\_ER 4.1

#### 要件

- 製造者は、TOE とそのコンポーネントが更新可能であることを保証しなければならない。これは、セキュリティアーキテクチャーまたは技術的制限のために更新できないすべてのコンポーネントを除外してもよい (MAY)。

## 評価基準

- 評価者は、TOE の関連するすべての構成要素が更新可能であることを評価しなければならない。
- 更新不可能なコンポーネントについては、評価者は、セキュリティアーキテクチャまたは技術的な制約のために、そのコンポーネントに更新機能がないことが他の理由で正当化されると評価しなければならない (MUST)。

### 5.3.4.2 REQ\_ER 4.2

#### 要件

- TOE は、アップデートを安全にインストールするメカニズムを持たなければならない。これには、ベストプラクティスを用いてアップデートパッケージの完全性と真正性を検証することが含まれる。

#### コンディション

- TOE は更新できる。

#### 評価基準

- 評価者は、更新メカニズムに使用されている設計と暗号化方法が、攻撃者による悪用（悪意のある更新パッケージの偽造など）を防止していることを評価しなければならない (MUST)。これには、ベストプラクティス暗号を使用した更新パッケージの完全性と真正性の検証を含む。

### 5.3.4.3 REQ\_ER 4.3

#### 要件

- TOE は、デフォルト設定で有効になっている自動更新メカニズムを持たなければならない。

#### コンディション

- TOE は、少なくともアップデート・ソースへの一時的な接続を持つ。

#### 評価基準

- 評価者は、自動更新メカニズムがデフォルト設定で有効になっていることをチェックしなければならない (MUST)。
- 評価者は、TOE が適切な定期間隔で更新をチェックすることを評価しなければならない。
- 評価者は、TOE が自動的に最新版に更新されることを評価しなければならない。

### 5.3.4.4 REQ\_ER 4.4

#### 要件

- TOE は、自動更新のための使いやすいオプトアウト機構を持たなければならない。
- TOE は、アップデートが利用可能であることをユーザに通知しなければならない。

## 評価基準

- 評価者は、自動更新の仕組みを簡単に無効にできることを評価しなければならない (MUST)。
- 評価者は、アップデートが利用可能であることがユーザに通知されるが、自動アップデートが無効になっている場合は、ユーザの同意なしにアップデートがインストールされないことを評価しなければならない (MUST)。

### 5.3.4.5 REQ\_ER 4.5

#### 要件

- ユーザは自動アップデートを延期できなければならない。TOE は、適切な時間枠の後にアップデートをインストールするよう、ユーザに繰り返し思い出させなければならない。
- 新しい機能や製品の使用への影響を伴わないセキュリティアップデートやバグフィックスは、延期オプションなしでインストールすることができる。

#### コンディション

- TOE は、少なくともアップデート・ソースへの一時的な接続を持つ。
- 自動更新メカニズムが有効になっている。
- アップデートのインストールにより、TOE のコア機能が一時的に中断される。

#### 評価基準

- 評価者は、ユーザが機能アップデートや TOE の機能を中断するアップデート (TOE の再起動など) を延期できることを評価しなければならない。
- 評価者は、延期されたアップデートを適切な時間枠内にインストールするよう、ユーザに繰り返し思い出させることを評価しなければならない (MUST)。

### 5.3.4.6 REQ\_ER 4.6

#### 要件

- TOE は、アップデートをインストールできない場合、十分な情報をユーザに通知しなければならない。これには、アップデートをインストールできない理由も含めなければならない。

#### コンディション

- TOE は更新できる。

#### 評価基準

- 評価者は、一時的なストレージ不足や接続の失敗など、アップデートがインストールできない場合、ユーザに通知されることを評価しなければならない (MUST)。

### 5.3.5 REQ\_ER 5 - アクセス制御

**CRA 附属書 I 第 1 部の現行草案に記載されている要件：**第 13 条(2)で言及されるサイバーセキ

セキュリティリスク評価に基づき、また該当する場合、デジタル要素を持つ製品は、認証、ID またはアクセス管理システムを含むがこれに限定されない適切な管理メカニズムによって、不正アクセスからの保護を確保し、不正アクセスの可能性について報告しなければならない。

#### 5.3.5.1 REQ\_ER 5.1

##### 要件

- TOE は、異なるタイプのユーザ、可能な能力、およびアクセスシナリオに関するアクセス制御のメカニズムを実装しなければならない (MUST)。

##### 評価基準

- 評価者は、記述されたアクセス制御メカニズムが、関連するすべてのユーザ役割、製品機能、およびアクセスシナリオを処理することを評価しなければならない (MUST)。
- 評価者は、記述されたメカニズムが不正アクセスから TOE を保護するのに十分であることを評価しなければならない (MUST)。

#### 5.3.5.2 REQ\_ER 5.2

##### 要件

- TOE は、初期セットアップ後にデフォルトパスワード、すなわち製品の複数のインスタンスに共通するパスワードを使用してはならない。

##### コンディション

- TOE は認証にパスワードを使用する。

##### 評価基準

- 評価者は、製品がデフォルトパスワード、すなわち、TOE の複数のインスタンスで等しい事前設定されたパスワードを、初期セットアップ前以外の状態で使用していないことを評価しなければならない。
- 初期セットアップ前にデフォルトパスワードが使用されている場合、評価者は、TOE の初期セットアップ中にユーザが個別のパスワードを設定する必要があることを評価しなければならない (MUST)。

#### 5.3.5.3 REQ\_ER 5.3

##### 要件

- TOE は、生成されたパスワード、API キー、および認証に使用されるその他のシークレットが、クラスまたは製品タイプに対する自動的な攻撃のリスクを低減するメカニズムで生成されることを保証しなければならない (MUST)。これには、実行時に生成されるシークレットだけでなく、ファクトリ状態でのみ使用されるプレインストールされたシークレットも含まれる。

## コンディション

- TOE は、生成された秘密を認証に使用する。

## 評価基準

- 例えば、インクリメンタルカウンタ(「password1」、「password2」など)は **明らかな**規則性となりうる。
- 評価者は、生成メカニズムが、結果として得られるパスワードに共通の文字列やその他の**共通**パターンを誘発しないことを評価しなければならない (MUST)。
- 評価者は、生成メカニズムが、公開情報、例えば MAC アドレス、WLAN SSID、**デバイスの**名前、タイプ、説明などに明白な形で関連するパスワードを誘導することを評価しなければならない (MUST)。
- 評価者は、生成メカニズムが、複雑さの点で適切と考えられるパスワードを生成することを評価しなければならない (MUST)。

### 5.3.5.4 REQ\_ER 5.4

#### 要件

- TOE は、技術、リスク、および使用法の特性に適したベストプラクティスの暗号技術を使用してユーザを 認証しなければならない (MUST)。

## コンディション

- TOE は認証を使用する。

評価者は、認証データが暗号化されていない**チャンネル**で平文で送信されないことを評価しなければならない (MUST)。

- 評価者は、認証データがベストプラクティスの暗号を用いて保護されていることを評価しなければならない (MUST)。

### 5.3.5.5 REQ\_ER 5.5

#### 要件

- TOE は、認証されたユーザまたは認証された管理者が使用する認証データを変更する簡単なメカニズムを提供しなければならない (MUST)。

## コンディション

- TOE は認証を使用する。

## 評価基準

- 評価者は、認証されたユーザまたは認証された管理者が、パスワードや鍵な どの認証データを変更できることを評価しなければならない (MUST)。

### 5.3.5.6 REQ\_ER 5.6

#### 要件

- TOE は、ネットワークインタフェースを介した認証メカニズムに対する総当たり攻撃を実行不可能にするメカニズムを実装しなければならない。

#### コンディション

- TOE は認証を使用する。

#### 評価基準

- 評価者は、TOE が無制限かつ無制限に認証の失敗を許さず、ブルートフォース攻撃が実用的でないように、例えば、X 回の失敗の後に時間を遅らせる、アクセスをロックする、第 2 因子を要求するなどの適切な方法で、ある回数の失敗の後に対応することを評価しなければならない (MUST)。
- 評価者は、認証に使用されるパスワードまたはその他の秘密が、ブルートフォースアタックを回避するのに十分複雑であることを評価しなければならない (例えば、十分な長さ、複数の種類の文字、辞書との照合、その他の認証機能または要素による強化など)。

### 5.3.5.7 REQ\_ER 5.7

#### 要件

- TOE は、失敗した認証試行について、どの認証データが不正であったかについての情報を提供してはならない (MUST NOT)。

#### 評価基準

- 評価者は、TOE が認証試行失敗時に正しい認証データに関する情報を提供しないことを評価しなければならない (MUST)。

### 5.3.5.8 REQ\_ER 5.8

#### 要件

- TOE は、不正アクセスの可能性を報告し、特定する手段を実装しなければならない。

評価者は、TOE が失敗した認証試行、すなわち無効なクレデンシャルを使用した認証試行を識別し、報告できることを評価しなければならない (MUST)。

評価者は、失敗したログイン試行をユーザがレビューできることを評価しなければならない (MUST)。

### 5.3.6 REQ\_ER 6 - 機密保護

**CRA 附属書 I パート 1 の現行草案に記載されている要件：**第 13 条(2)で言及されたサイバーセキュリティリスク評価に基づき、また該当する場合、デジタル要素を含む製品は、最新のメカニズムにより、静止時または転送時に関連するデータを暗号化し、その他の技術的手段を使用するなどして、保存、転送、またはその他の方法で処理された個人またはその他のデータの機密性を保護しなければ

ならない。

### 5.3.6.1 REQ\_ER 6.1

#### 要件

- TOE は、対応するユースケースに適したベストプラクティスの暗号を使用して安全に通信しなければならない。

#### コンディション

- TOE はローカルまたはパブリック・ネットワーク上で通信し、個人データ、機密個人データ、機密システム・データ、またはセキュリティ・データを送信する。

#### 評価基準

- 評価者は、TOE がベストプラクティスの暗号を使用していることを評価しなければならない。これには、ブルートフォース攻撃やリプレイ攻撃に対する保護だけでなく、暗号プリミティブやアルゴリズムも含まれる。

### 5.3.6.2 REQ\_ER 6.2

#### 推薦

- TOE は、特に暗号の分野において、積極的に保守されるネットワークとセキュリティの機能を提供するために、レビュー済みまたは評価済みの実装を使用するべきである (SHOULD)。

#### コンディション

- TOE は、個人データ、機密個人データ、機密システム・データ、またはセキュリティ・データをローカル・ネットワークまたはパブリック・ネットワーク上で送信するために暗号を使用する。

#### 評価基準

- 評価者は、TOE がレビュー済みまたは評価済みの暗号実装を使用していることを評価しなければならない。
- 評価者は、暗号実装が積極的に保守されていることを評価しなければならない (MUST)。

### 5.3.6.3 REQ\_ER 6.3

#### 推薦

- TOE は長期セキュリティデータ<sup>6</sup>を送信すべきではない。
- 長期的なセキュリティデータの代わりに、TOE は通信に有効期限が限定された一時的なセキュリティデータ、例えばメッセージダイジェスト鍵、セッション鍵、Nonces を使用すべきである (SHOULD)。

---

<sup>6</sup> 長期セキュリティ・データは、ユーザによって積極的に変更されるまで、無期限または相当期間、例えば 180 日間有効である。

- 評価者は、TOE が再構築可能な方法で長期セキュリティデータを送信することを可能な限り避けなければならない。
- 長期セキュリティデータが再構築可能な方法で送信される場合、評価者は、送信の理由が技術、リスク及び使用法の特性に対して適切であることを評価しなければならない (MUST)。

#### 5.3.6.4 REQ\_ER 6.4

##### 要件

- TOE が保管するセキュリティデータおよび重要なセキュリティデータの機密性は保護されなければならない。暗号化およびその他の暗号化メカニズムは、ベストプラクティスに従わなければならない。

##### コンディション

- TOE は、セキュリティ・データと重要なセキュリティ・データを保存する。

##### 評価基準

- TOE が保存されたセキュリティデータおよび重要なセキュリティデータの機密性を保護するために暗号を使用する場合、評価者は TOE がベストプラクティスに従って暗号を使用していることを評価しなければならない。
- TOE が、保存されたセキュリティデータ及び重要なセキュリティデータを保護するために、例えば、許可システムや暗号化機能を持つ特別に保護されたストレージなど、他の又は追加のメカニズムを使用する場合、評価者は、これらのメカニズムがセキュリティデータ及び重要なセキュリティデータを保護するために適切であることを評価しなければならない (MUST)。

#### 5.3.6.5 REQ\_ER 6.5

##### 要件

- 製造者は、TOE または関連サービスに関連するセキュリティデータの安全な管理プロセスに従わなければならない。

##### コンディション

- TOE は、製造者が生成したセキュリティ・データを使用する。

##### 評価基準

- 評価者は、重要なセキュリティデータの安全な管理が、重要なセキュリティパラメータのライフサイクルの以下のすべての側面を考慮することによって、そのライフサイクル全体に及んでいることを評価しなければならない (MUST) :
  - 世代、そして
  - プロビジョニング
  - ストレージ

- 更新情報
- 期限切れと危殆化に対処するための廃止、アーカイブ、破棄プロセス。

### 5.3.7 REQ\_ER 7 - 完全性保護

**CRA 附属書 I パート 1 の現行草案に記載されている要件：**第 13 条(2)で言及されているサイバーセキュリティ・リスク評価に基づき、また該当する場合、デジタル要素を持つ製品は、保存、送信、またはその他の方法で処理されたデータ、個人またはその他のデータ、コマンド、プログラム、設定の完全性を、ユーザによって許可されていない操作または変更から保護し、破損について報告しなければならない。

#### 5.3.7.1 REQ\_ER 7.1

##### 推薦

- TOE は、TOE のセキュリティ特性の改ざんを防止するために、自身の完全性を検証できるべきである (SHOULD)。検証に失敗した場合、TOE は TOE の完全性を復元するオプションをユーザに与えなければならない。通常、検証に必要な外部コンポーネントまたは内部コンポーネントは、それ自体を検証することができないため、不要な改ざんから保護する必要がある。

##### コンディション

- TOE は、機密性の高いユーザデータまたはシステムデータを保存する。

##### 評価基準

- 評価者は、セキュリティデータの改ざんを防止するのに十分な方法で、TOE が使用前にそれ自身の完全性を検証することを評価しなければならない (MUST)。
- 評価者は、バリデーションが失敗した場合、ユーザに警告が出され、復旧の選択肢が与えられることを評価しなければならない (MUST)。
- ハッシュ値や署名など、TOE がその完全性を保証するために暗号を使用する場合、評価者は TOE がベストプラクティスに従って暗号を使用していることを評価しなければならない (MUST)。

#### 5.3.7.2 REQ\_ER 7.2

##### 要件

- TOE は、追加ソフトウェアのインストールをアトミックな方法で実行しなければならない。例えば、インストールプロセス中にエラーやキャンセルが発生した場合は、TOE を新しいソフトウェアのインストール前の状態にリセットしなければならない。

##### コンディション

- TOE は、アプリやプラグインなどの追加ソフトウェアのインストールを可能にする。

### 評価基準

- 評価者は、失敗またはキャンセルされたインストールが、TOE またはユーザに影響を与えず、インストールを再試行できるような方法で元に戻されることを評価しなければならない (MUST)。

### 5.3.7.3 REQ\_ER 7.3

#### 要件

- ユーザは、ユーザ自身がインストールしたソフトウェアをアンインストールできなければならない。

#### コンディション

- TOE は、アプリやプラグインなどの追加ソフトウェアのインストールを可能にする。

### 評価基準

- 評価者は、ユーザがユーザ自身によってインストールされたソフトウェアをアンインストールできることを評価しなければならない (MUST)。

### 5.3.7.4 REQ\_ER 7.4

#### 要件

- 例えば、セキュリティに関連するデータを書き込む際にトランザクション/排他的アクセスを使用する、割り当てられたプログラム・メモリのみを使用する、未使用時にリソースを解放する、などである。

### 評価基準

- これには、ファイルシステムへのアクセス、ネットワーク接続の使用、使用済み/割り当て済みメモリ、その他の共有リソースの処理などが含まれる。

### 5.3.8 REQ\_ER 8 - データの最小化

**CRA 附属書 I パート 1 の現行草案に記載されている要件：**第 13 条 (2) で言及されたサイバーセキュリティ・リスク評価に基づき、かつ該当する場合、デジタル要素を含む製品は、適切かつ関連性があり、デジタル要素を含む製品の意図された目的に関連して必要なものに限定された個人データまたはその他のデータのみを処理しなければならない (データの最小化)。

#### 5.3.8.1 REQ\_ER 8.1

#### 要件

- TOE は、意図された目的および合理的に予測可能な用途を果たすために必要なデータのみを収集し、処理しなければならない。

## 評価基準

- 評価者は、指定されたデータの処理が、TOE の意図された目的および合理的に予見可能な使用にとって必要であることを評価しなければならない (MUST)。
- 評価者は、指定されたデータのみが TOE によって収集され、処理されることを確認しなければならない。

### 5.3.9 REQ\_ER 9 - 必須および基本的機能の利用可能性

**CRA 附属書 I パート 1 の現行草案に記載されている要件：**第 13 条(2)で言及されるサイバーセキュリティリスク評価に基づき、また該当する場合、デジタル要素を含む製品は、サービス妨害 (DoS) 攻撃に対する回復力および緩和策を含め、インシデント発生後においても、重要かつ基本的な機能の可用性を保護しなければならない。

#### 5.3.9.1 REQ\_ER 9.1

##### 要件

- TOE をデフォルト構成で動作させることができなければならない。このコンフィギュレーションでは、TOE のコア機能に必要なインタフェースのみが有効化される。

##### 評価基準

- 評価者は、TOE がデフォルトコンフィギュレーションで動作可能であることを確認しなければならない。
- 評価者は、不要なインターフェイスがすべて無効化されていることを確認しなければならない (MUST)。

#### 5.3.9.2 REQ\_ER 9.2

##### 要件

- TOE は、一時的な中断後、安全な動作を再開できなければならない。

##### 評価基準

- 評価者は、TOE が一時的な中断の後に安全な動作を再開できることを評価しなければならない。これには、停電、ネットワーク損失、ネットワークトラフィックの過負荷、利用可能なサービスがないなどの一般的な中断が含まれる。

#### 5.3.9.3 REQ\_ER 9.3

##### 要件

- TOE は、ネットワークが失われた場合でも、ローカルの安全機能を維持しなければならない。

##### コンディション

- TOE は、スマートロックや煙探知機など、基本的な安全機能を果たす。

## 評価基準

- ・ 評価者は、ネットワーク喪失時にローカルな安全機能が維持されることを評価しなければならない (MUST)。

### 5.3.9.4 REQ\_ER 9.4

#### 要件

- TOE は、利用可能な遠隔データ処理ソリューションがなくても、その中核機能を維持しなければならない。

#### コンディション

- ・ TOE は、テレメトリ・データ処理、デジタル著作権管理など、意図された目的のためのリモート・データ処理ソリューションを必要としない。

## 評価基準

- ・ 評価者は、利用可能なリモートデータ処理ソリューションがなくても、TOE がそのコア機能を維持することを評価しなければならない (MUST)。

### 5.3.10 REQ\_ER 10 - マイナス影響の最小化

**CRA 附属書 I 第 1 部の現行草案に記載された要件：**第 13 条(2)で言及されているサイバーセキュリティリスク評価に基づき、また該当する場合、デジタル要素を含む製品は、製品自体または接続された機器によって、他の機器またはネットワークによって提供されるサービスの可用性に与える悪影響を最小限に抑えなければならない。

#### 5.3.10.1 REQ\_ER 10.1

#### 要件

- ・ TOE は、通常動作中、ネットワークリソースを秩序正しく扱わなければならない。

#### 評価基準

- ・ すなわち、ネットワークリソースが TOE の意図された目的および合理的に予見可能な用途に対してのみ適切に使用され、必要なくなれば解放されるようにしなければならない。

#### 5.3.10.2 REQ\_ER 10.2

#### 要件

- ・ TOE は他の製品と整然と通信し、他の製品がエラーに対応できるようにしなければならない。

#### 評価基準

- ・ 評価者は、TOE が十分に定義されたプロトコルに従ってサービスを提供し、提供されたサービスのエラーに対して外部製品が適切に対応できるようにすることを評価しなければならない (MUST)。

- 評価者は、外部使用を意図して使用されるプロトコルやインターフェースが、外部製品による使用のために十分に文書化されていることを評価しなければならない (MUST)。この文書化は必ずしも無償ではない。

### 5.3.11 REQ\_ER 11 - 攻撃面を制限する

**CRA 附属書 I Part 1 の現行草案に記載されている要件：**第 13 条(2)で言及されているサイバーセキュリティリスク評価に基づき、また該当する場合、デジタル要素を含む製品は、外部インターフェースを含む攻撃面を制限するように設計、開発、製造されなければならない。

#### 5.3.11.1 REQ\_ER 11.1

##### 要件

- TOE は、デフォルトで使用する必要のないインターフェースとサービスを停止しなければならない。

##### 評価基準

- 評価者は、ユーザが最初に使用する前に、初期設定に必要なインターフェースとサービスだけが有効になっていることを評価しなければならない (MUST)。
- 評価者は、TOE の使用にどのインターフェースとサービスが必要かを評価しなければならない。
- 評価者は、これらのインターフェースとサービスだけがデフォルトで有効になっていることを評価しなければならない (MUST)。

#### 5.3.11.2 REQ\_ER 11.2

##### 要件

- TOE は、TOE のセキュリティ機能をバイパスするために使用可能なデバッグインターフェースおよび機能を、デフォルトで非アクティブにしなければならない (MUST)。TOE のデバッグインターフェースは、権限を付与されたユーザまたは管理者によって、過去にさかのぼって再アクティブ化することができる。

##### コンディション

- TOE は、ローカル (パブリック)、ローカル (パブリック制限付き)、ローカルネットワーク、またはパブリックネットワークアクセスのデバッグインターフェースを持つ。

##### 評価基準

- 評価者は、すべてのデバッグインターフェースがデフォルトで無効になっていることを評価しなければならない (MUST)。
- TOE に再有効化可能なデバッグインターフェースまたはサービスが含まれている場合、評価者は、それらのインターフェースが許可されたユーザによってのみ有効にされることを評価しなければならない。

- ・ 評価者は、デバッグインターフェイスがアクティブになったとき、ユーザに十分な警告がなされることを評価しなければならない (MUST)。

### 5.3.12 REQ\_ER 12 - インシデントの緩和

**CRA 附属書 I 第 1 部の現行草案に記載されている要件：**第 13 条(2)で言及されたサイバーセキュリティリスク評価に基づき、また該当する場合、デジタル要素を含む製品は、適切な悪用緩和メカニズムおよび技術を使用して、インシデントの影響を低減するように設計、開発、製造されなければならない。

注：セクション 5.3.3、5.3.4、5.3.6、5.3.7、5.3.9、5.3.10 に記載されている要件は、悪用緩和のメカニズムや技術についてすでに検討しているため、ここでは改めて検討しない。

#### 5.3.12.1 REQ\_ER 12.1

##### 要件

- ・ TOE は、デフォルトで必要最小限の権限で運用されなければならない。

##### 評価基準

- ・ 評価者は、TOE がその現在の機能を果たすために必要な最小限の権限のみをデフォルトで使用することを評価しなければならない (MUST)。

#### 5.3.12.2 REQ\_ER 12.2

##### 要件

- ・ TOE は、他の製品のために提供されるインターフェースに対して許可システムを強制しなければならない。許可システムは、インターフェースの使用を制御するのに十分な粒度でなければならない。

##### コンディション

- ・ TOE は、他の製品と通信するためのインターフェースを提供する。

##### 評価基準

- ・ 評価者は、TOE が他の製品に提供するインターフェースの許可システムを有していることを評価しなければならない。
- ・ 評価者は、TOE の権限システムがインターフェースを介したアクセスを制御するのに十分な粒度であり、インターフェースと通信する製品が最低限必要な権限で動作できることを評価しなければならない (MUST)。
- ・ 評価者は、TOE によって権限システムが強制され、他の製品が TOE によって付与されていない追加権限を取得できないこと、すなわち意図しない権限昇格がないことを評価しなければならない (MUST)。

### 5.3.13 REQ\_ER 13 - 記録とモニタリング

**CRA 附属書 I パート 1 の現行草案に記載されている要件：**第 13 条(2)で言及されたサイバーセキ

ユリティ・リスク評価に基づき、該当する場合、デジタル要素を含む製品は、データ、サービス、機能へのアクセスや変更を含む関連する内部活動を記録・監視することにより、セキュリティ関連情報を提供しなければならない。

#### 5.3.13.1 REQ\_ER 13.1

##### 要件

- TOE は、すべてのセキュリティ関連設定の変更を記録し、監視するメカニズムを実装しなければならない。
- TOE は、デフォルトですべての設定変更を記録しなければならない。

##### 評価基準

- 評価者は、すべての設定変更を記録し監視する仕組みが TOE に実装されていることを評価しなければならない。
- 評価者は、記録されたデータにセキュリティ関連の設定変更の異常を分析するのに十分な情報が含まれていることを評価しなければならない (MUST)。これには少なくとも、開始者、時刻、設定変更の内容/種類が含まれる。
- 評価者は、設定変更がデフォルトで記録されることをチェックしなければならない (MUST)。

#### 5.3.13.2 REQ\_ER 13.2

##### 要件

- TOE は、すべてのユーザ認証を記録し、監視するメカニズムを実装しなければならない。
- TOE は、デフォルトですべてのユーザ認証を記録しなければならない (MUST)。

##### 評価基準

- 評価者は、すべてのユーザ認証を記録し監視するメカニズムが TOE に実装されていることを評価しなければならない (MUST)。
- 評価者は、記録されたデータに、ユーザ認証の異常を分析するのに十分な情報が含まれていることを評価しなければならない (MUST)。これには、少なくとも認証時刻、アクセスされたインターフェイスまたは機能、利用可能な場合は認証のソース、および認証試行の結果が含まれる。
- 評価者は、ユーザ認証がデフォルトで記録されていることを確認しなければならない (MUST)。

#### 5.3.13.3 REQ\_ER 13.3

##### 要件

- TOE は、TOE に属するすべてのサービスのステータスを記録し、監視するメカニズムを実装しなければならない。

- TOE は、デフォルトで TOE に属するすべてのサービスのステータスを記録しなければならない。

#### **評価基準**

- 評価者は、TOE に属するすべてのサービスのステータスを記録し、監視するメカニズムが TOE に実装されていることを評価しなければならない。
- 評価者は、記録された情報がサービス活動の異常を分析するのに十分な情報を含んでいることを評価しなければならない (MUST)。これには、少なくともサービスの開始時間と定期的なステータス更新が含まれる。
- 評価者は、TOE に属するすべてのサービスの状態がデフォルトで記録されていることを確認しなければならない。

#### **5.3.13.4 REQ\_ER 13.4**

##### **要件**

- 許可されたユーザによって、録画と監視活動を停止することが可能でなければならない (MUST)。

##### **評価基準**

- 評価者は、許可されたユーザが録画と監視を解除し、再度有効にすることが可能であることを確認しなければならない (MUST)。
- 評価者は、記録およびモニタリング活動の起動と停止が記録されていることを確認しなければならない (MUST)。

#### **5.3.13.5 REQ\_ER 13.5**

##### **要件**

- TOE は、ネットワーク通信におけるセキュリティ異常の可能性を検出するために、ネットワークデータを記録・監視できなければならない。

##### **コンディション**

- TOE はローカルまたはパブリック・ネットワークと通信する。

##### **評価基準**

- 評価者は、TOE がネットワーク接続の異常を検出するのに適したネットワークデータを記録し、監視していることを評価しなければならない。記録されたデータには、少なくとも時刻、ソース/ターゲット、および関連するネットワークイベントの詳細が含まれなければならない (MUST)。

### 5.3.13.6 REQ\_ER 13.6

#### 要件

- TOE は、レトロスペクティブな分析を容易にするために、十分な期間の記録データを提供できなければならない。

#### 評価基準

- 評価者は、収集した記録データを、例えば、記録データを（ローカル又はリモートで）分析可能な十分な期間保存することによって、セキュリティ異常の可能性を遡及的に検知するために分析できることを評価しなければならない（MUST）。

### 5.3.13.7 REQ\_ER 13.7

#### 要件

- TOE は、記録されたデータがセキュリティ・インシデントを促進するために使用できないことを保証しなければならない。

#### 評価基準

- 評価者は、セキュリティリスクを露呈している記録データが、許可されたエンティティによってのみアクセス可能であることを評価しなければならない（MUST）。
- 評価者は、記録されたデータに不必要なデータが含まれておらず、デフォルトで必要以上のリスクを露呈していないことを評価しなければならない（例えば、個人データや秘密をデフォルトのログレベルで記録しないなど）。
- デバッグのため、ケースバイケースで追加情報を記録することがある。

### 5.3.13.8 REQ\_ER 13.8

#### 要件

- TOE は、再コード化とモニタリングが一般的な中断に対して回復力があり、セキュリティ関連データの記録とモニタリング中の問題が TOE の機能に影響を与えないことを保証しなければならない。

#### 評価基準

- 評価者は、再コード化とモニタリングの仕組みが、一般的な障害、例えば電源喪失、ストレージの低下、ネットワーク停止などに対して回復力があることを評価しなければならない（MUST）。
- 評価者は、記録とモニタリングの仕組みに問題があっても、TOE の基本的な機能に影響がないことを評価しなければならない。

### 5.3.14 REQ\_ER 14 - データと設定の削除

**CRA 附属書 I パート 1 の現行草案に記載された要件：**第 13 条(2)で言及されているサイバーセキュリティ・リスク評価に基づき、該当する場合、デジタル要素を持つ製品は、利用者がすべての

データと設定を安全かつ容易に永久的に削除できる可能性を提供し、そのようなデータを他の製品またはシステムに転送できる場合、安全な方法でこれが行われることを保証しなければならない。

#### 5.3.14.1 REQ\_ER 14.1

##### 要件

- TOE は、TOE 上のすべての個人データを削除するための使いやすいメカニズムを実装しなければならない。

##### 評価基準

- 評価者は、TOE に保存されているすべての個人データを削除するための使いやすいメカニズムが TOE に実装されていることを評価しなければならない。
- 評価者は、すべての個人データが TOE 上で削除されていることを確認しなければならない。

#### 5.3.14.2 REQ\_ER 14.2

##### 要件

- TOE は、すべてのシステムデータを削除し、変更されたすべての設定を TOE のデフォルト値に戻すための使いやすいメカニズムを実装しなければならない。

##### 評価基準

- 評価者は、TOE に保存されているすべてのシステムデータと設定を削除するための使いやすいメカニズムが TOE に実装されていることを評価しなければならない。
- 評価者は、TOE 上ですべてのシステムデータと設定が削除されていることを確認しなければならない。
- 評価者は、変更された設定が TOE 上でデフォルト値に戻されていることを確認しなければならない。

#### 5.3.14.3 REQ\_ER 14.3

##### 要件

- TOE は、クラウドサービスなどの TOE のリモートデータプロセッシングソリューションに保存されているユーザの全データを削除するための使いやすいメカニズムを実装しなければならない。

##### 評価基準

- 評価者は、TOE に属するリモートデータプロセッシングソリューションに保存されたユーザの全データを削除するための使いやすいメカニズムが TOE に実装されていることを評価しなければならない (MUST)。
- 評価者は、TOE のリモートデータプロセッシングソリューションにおいて、ユーザに属するすべてのデータが削除されていることを確認しなければならない。

#### 5.3.14.4 REQ\_ER 14.4

##### 要件

- TOE は、すべてのデータと変更された設定を工場出荷時のデフォルトに戻すための使いやすいメカニズムを実装しなければならない。

##### 評価基準

- 評価者は、すべてのデータを工場出荷時のデフォルトに戻すための使いやすいメカニズムが TOE に実装されていることを評価しなければならない。
- 評価者は、すべての個人データが TOE 上で削除されていることを確認しなければならない。
- 評価者は、TOE 上のすべてのシステムデータと変更された設定が削除されていることを確認しなければならない。
- 評価者は、変更された設定が TOE 上でデフォルト値に戻されていることを確認しなければならない。
- 評価者は、TOE に属するサービスにおいて、すべての個人データが削除されていることを確認しなければならない。

評価者は、TOE に属するサービスにおいて、変更されたすべてのシステムデータが削除されていることを確認しなければならない (MUST)。

- 評価者は、TOE のリモートデータプロセッシングソリューションを使用するために、すべての設定がデフォルト値に戻されていることを確認しなければならない。

#### 5.3.14.5 REQ\_ER 14.5

##### 要件

- TOE は、5.3.6 項および 5.3.7 項の要件に従い、個人データおよびシステムデータを安全な方法で転送しなければならない。

##### 評価基準

- 評価者は、5.3.6 項と 5.3.7 項のすべての要件が満たされていることを確認しなければならない (MUST)。

### 5.4 脆弱性の取り扱いに関する必須要件

製造者は、提供する TOE に、積極的に悪用可能な脆弱性が存在しないことを保証し、さらに、サポート期間中、脆弱性が判明した場合、速やかに対処しなければならない。この要件を満たすために、製造者は少なくとも以下に示す脆弱性対応の基本要件を含む脆弱性対応システムを運用しなければならない。

注：効果的な脆弱性処理を行うためには、可能な限り自動化されるべきであり、したがって機械処理可能なフォーマットを使用すべきである。

### 5.4.1 REQ\_VH 1 - コンポーネントとバーネラビリティを特定する

**CRA 附属書 I パート 2 の現行草案に記載されている要件：** デジタル要素を含む製品の製造者は、デジタル要素を含む製品に含まれる脆弱性とコンポーネントを特定し、文書化しなければならない。これには、少なくとも製品のトップレベルの依存関係を網羅する、一般的に使用され機械で読み取り可能な形式のソフトウェア部品表を作成することが含まれる。

#### 5.4.1.1 REQ\_VH 1.1

##### 要件

- ・ 製造者は、BSI TR-03183-2 に従って TOE のすべてのソフトウェアコンポーネントをソフトウェア部品表 (SBOM) に文書化しなければならない。
- ・ 製造者は、TOE のデジタル要素を持つすべてのハードウェアコンポーネントを文書化しなければならない。

##### 評価基準

- ・ 評価者は、TOE のソフトウェアコンポーネントを文書化した SBOM が存在することを確認しなければならない。
- ・ 評価者は、SBOM が BSI TR-03183-2 に準拠していることを評価しなければならない。
- ・ 評価者は、デジタル要素を持つハードウェアコンポーネントが文書化されていることを評価しなければならない (MUST)。

#### 5.4.1.2 REQ\_VH 1.2

##### 要件

- ・ 製造者は、TOE に影響する脆弱性を特定するプロセスを持たなければならない。
- ・ 製造者は、TOE の SBOM を使用して、例えば共通/欧州/国内脆弱性データベース (CVD/EUVD/NVD) のような脆弱性データベースとコンポーネントを照合してもよい。
- ・ 製造者は、これらの脆弱性、それらが TOE にどのような影響を与え、どのように軽減できるかを文書化しなければならない。

##### 評価基準

- ・ 評価者は、TOE に影響を及ぼす脆弱性を特定するプロセスが存在することを評価しなければならない。
- ・ 評価者は、脆弱性とその緩和策が文書化されていることを評価しなければならない (MUST)。

### 5.4.2 REQ\_VH 2 - 脆弱性に対処する

**CRA 附属書 I パート 2 の現行草案に記載されている要件：** デジタル要素を有する製品の製造者は、デジタル要素を有する製品にもたらされるリスクに関連して、セキュリティアップデートの提供を含め、遅滞なく脆弱性に対処し、是正しなければならない。

### 5.4.2.1 REQ\_VH 2.1

#### 要件

- 製造者は、特定された脆弱性に対し、アップデートを提供する、または脆弱性を緩和するなどして、タイムリーに実行可能な方法で対処し、修正することを保証しなければならない。

#### 評価基準

- 評価者は、製造者が、特定された脆弱性を過度な遅延なく分析し、脆弱性の関連リスクに応じて評価するプロセスを文書化し、実施していることを評価しなければならない (MUST)。この評価には、脆弱性が積極的に悪用されるか、または悪用される可能性があるかどうかを含めなければならない (MUST)。
- 評価者は、製造者が脆弱性に対処し、適時に実行可能な方法で修正するプロセスを文書化し、実施していることを評価しなければならない (MUST)。
- 評価者は、文書化され実装されたプロセスが、機能更新やその他の計画された更新を待たずに、セキュリティ更新やその他の緩和策を可能な限り速やかに提供することによって、高リスクの脆弱性や積極的に悪用された脆弱性に対処していることを評価しなければならない (MUST)。

### 5.4.3 REQ\_VH 3 - 定期検査

**CRA 附属書 I パート 2 の現行草案に記載されている要件：** デジタル要素を含む製品の製造者は、デジタル要素を含む製品のセキュリティについて、効果的かつ定期的なテストとレビューを適用しなければならない。

#### 5.4.3.1 REQ\_VH 3.1

#### 要件

- 製造者は、TOE のセキュリティ特性が正しく実装されているかどうかをテストするプロセスを文書化し、実装しなければならない。
- 製造者は、TOE のセキュリティ特性を定期的にテストしなければならない。

#### 評価基準

- 評価者は、製造者が TOE のセキュリティ特性をテストするプロセスを文書化し、実施したことを評価しなければならない (MUST)。
- 評価者は、製造者が TOE のセキュリティ特性を定期的にテストしていることを評価しなければならない、

例えば、3 ヶ月ごと、あるいは製品に大きな変更があるたびに、である。

評価者は、少なくとも本技術ガイドラインのセキュリティ要求事項を満たす評価基準がテストに含まれていることを評価しなければならない (MUST)。

- 評価者は、評価基準にすべてのセキュリティ要件に対する十分な機能評価が含まれていること、または、機能評価が実施されない場合は、3.3.4 節に従って十分に妥当な正当性が示され、文書化されていることを評価しなければならない (MUST)。

#### 5.4.4 REQ\_VH 4 - 対応済みの脆弱性を公表する

**CRA Annex I Part 2 の現行草案に記載されている要件：**これには、脆弱性の説明、影響を受けるデジタル要素を持つ製品をユーザが特定できる情報、脆弱性の影響、深刻度、ユーザが脆弱性を修正するのに役立つ明確でアクセス可能な情報などが含まれる。製造者が、公表によるセキュリティ上のリスクがセキュリティ上の利益を上回ると考える正当な場合には、ユーザが関連するパッチを適用する可能性が与えられるまで、修正された脆弱性に関する情報の公表を延期することができる。

##### 5.4.4.1 REQ\_VH 4.1

###### 要件

- 製造者は、TOE に影響を及ぼす脆弱性について、セキュリティアドバイザリを用いてユーザに通知しなければならない (MUST)。
- 製造者は、セキュリティ勧告を使用して、TOE に影響を与える脆弱性について公表してもよい。
- セキュリティ勧告には、脆弱性の影響とその緩和方法に関する情報を含めなければならない (MUST)。

###### 評価基準

- 評価者は、製造者が TOE に影響する脆弱性についてセキュリティアドバイザリで通知するプロセスを文書化し、実施していることを評価しなければならない (MUST)。
- 評価者は、セキュリティ勧告に、影響、一時的な緩和策、脆弱性を修正する方法に関する情報が含まれていることを確認しなければならない (MUST)。

##### 5.4.4.2 REQ\_VH 4.2

###### 要件

- 製造者は、機械処理可能な方法でセキュリティ勧告を提供しなければならない (MUST)。

###### 評価基準

- 評価者は、セキュリティアドバイザリが機械処理可能な方法で発行されていることを評価しなければならない (MUST)。

#### 5.4.4.3 REQ\_VH 4.3

##### 推薦

- ・ 製造者は、BSI TR-03191 に従い、Common Security Advisory Framework<sup>7</sup> (CSAF) を使用すべきである。

##### 評価基準

- ・ 評価者は、共通セキュリティ勧告フレームワークがセキュリティ勧告の発行に使用されていることを評価しなければならない (MUST)。

#### 5.4.5 REQ\_VH 5 - 協調的な脆弱性開示ポリシー

**CRA 附属書 I パート 2 の現行草案に記載されている要件：** デジタル要素を持つ製品の製造者は、協調的な脆弱性の開示に関する方針を定め、実施しなければならない。

デジタル要素を含む製品の製造者は、デジタル要素を含む製品で発見された脆弱性を報告するための連絡先を提供することを含め、デジタル要素を含む製品およびその製品に含まれるサードパーティ製コンポーネントの潜在的な脆弱性に関する情報の共有を促進するための措置を講じなければならない。

##### 5.4.5.1 REQ\_VH 5.1

##### 要件

- ・ 製造者は、BSI TR-03183-3 に従って脆弱性開示プロセスを公表し、実施しなければならない。

##### 評価基準

- ・ 評価者は、製造者が脆弱性開示プロセスを文書化し、実施していることを評価しなければならない (MUST)。
- ・ 評価者は、製造者が脆弱性開示方針の一環として、脆弱性を報告するための連絡しやすいオプションを公表していることを評価しなければならない (MUST)。
- ・ 評価者は、脆弱性開示プロセスが BSI TR-03183-3 に準拠していることを評価しなければならない。

#### 5.4.6 REQ\_VH 6 - アップデートの安全な配布

**CRA 附属書 I パート 2 の現行草案に記載されている要件：** デジタル要素を含む製品の製造者は、脆弱性が適時に修正または緩和され、セキュリティアップデートに該当する場合は自動的な方法で修正または緩和されることを保証するために、デジタル要素を含む製品のアップデートを安全に配布する仕組みを提供しなければならない。

---

<sup>7</sup> <https://csaf.io/>

#### 5.4.6.1 REQ\_VH 6.1

##### 要件

- 製造者は、5.3.4 項に従って、アップデートを配布する仕組みを提供しなければならない (MUST)。

##### 評価基準

- 評価者は、5.3.4 節のすべての要件が満たされていることを確認しなければならない (MUST)。

#### 5.4.7 REQ\_VH 7 - アップデートの普及

**CRA 附属書 I パート 2 の現行草案に記載されている要件：** デジタル要素を含む製品の製造者は、特定されたセキュリティ問題に対処するためのセキュリティアップデートが利用可能な場合、遅滞なく、また、デジタル要素を含むオーダーメイド製品に関して製造者と企業ユーザとの間で別段の合意がない限り、無償で、ユーザに、取るべき潜在的な措置を含む関連情報を提供する勧告メッセージを添付して配布されることを確保しなければならない。

#### 5.4.7.1 REQ\_VH 7.1

##### 要件

- 製造者は、5.3.2 項、5.3.4 項、5.3.6 項に従って、更新のアドレス指定メカニズムを提供しなければならない (MUST)。

##### 評価基準

- 評価者は、5.3.2 項、5.3.4 項、5.3.6 項のすべての要件が満たされていることを確認しなければならない (MUST)。

#### 5.4.7.2 REQ\_VH 7.2

##### 要件

- 製造者は、6.2.4 項に従って、更新の適用に関するユーザ文書またはガイダンスを提供しなければならない (MUST)。

##### 評価基準

- 評価者は、6.2.4 節のすべての要件が満たされていることを確認しなければならない (MUST)。

## 6 文書作成義務

### 6.1 技術文書

技術文書は、以下の要件に従って製造者が作成しなければならない。製造者が発行する場合もあるが、これらの文書には機密情報が含まれているものもあるため、必須ではない。

#### 6.1.1 REQ\_TD 1 - 一般文書

**CRA 附属書 VII の現行草案に記載されている要件：** 技術文書には、意図された目的、本質的なサイバーセキュリティ要件への準拠に影響するソフトウェアのバージョン、デジタル要素を含む製品がハードウェア製品である場合は、外観の特徴、表示、内部レイアウトを示す写真またはイラストを含む、デジタル要素を含む製品の一般的な説明を [...] 含まなければならない。

##### 6.1.1.1 REQ\_TD 1.1

###### 要件

- 技術文書には TOE の意図された目的を記載しなければならない。
- 技術文書には、5.3 項に記載された必須要件への適合に影響を及ぼすソフトウェアのバージョンを含めなければならない。

###### 評価基準

- 評価者は、TOE の意図された目的が文書化されていることを評価しなければならない。
- 評価者は、必須要件への準拠に影響を与えるソフトウェアのバージョンが文書化されていることを評価しなければならない (MUST)。

##### 6.1.1.2 REQ\_TD 1.2

###### 要件

- 技術文書には、TOE の外観、マーキング、内部レイアウトを示す写真またはイラストを含まなければならない。

###### コンディション

- TOE はハードウェア・デバイスであるか、ハードウェア・コンポーネントを持つ。

###### 評価基準

- 評価者は、文書に TOE の外形的特徴、マーキング、内部レイアウトを示す写真または図版が含まれていることを確認しなければならない。

#### 6.1.2 REQ\_TD 2 - プロセスの文書化

**CRA 附属書 VII の現行草案に記載されている要件：** 技術文書には、デジタル要素を含む製品の設計、開発、製造、および脆弱性処理プロセスの説明を含まなければならない [...]

### 6.1.2.1 REQ\_TD 2.1

#### 要件

- 技術文書には、セキュリティ特性に関する TOE の設計、開発、製造に関する情報を含めなければならない (MUST)。

#### 評価基準

- 評価者は、技術文書に TOE の設計、開発、製造に関するセキュリティ特性に関する情報が含まれていることを評価しなければならない (MUST)。これには、該当する場合、図面、図式、及び、ソフトウェアコンポーネントがどのように互いの上に構築されるか、あるいは、どのように互いに影響し合い、全体的なプロセスに統合されるかを説明するシステムアーキテクチャの記述が含まれる。

### 6.1.2.2 REQ\_TD 2.2

#### 要件

- 技術文書には、第 0 節で文書化した脆弱性処理プロセスを含めなければならない (MUST)。

#### 評価基準

- 評価者は、5.4 項の要求事項に従った文書が入手可能であることを確認しなければならない (MUST)。

### 6.1.3 REQ\_TD 3 - サイバーセキュリティリスクの文書化

**CRA 附属書 VII の現行草案に記載されている要件：**技術文書には、CRA の附属書 I 第 1 部に規定されている必須要件がどのように適用されるかを含め、CRA の第 13 条に規定されているように、デジタル要素を含む製品が設計、開発、生産、提供、維持されるサイバーセキュリティリスクの評価を含めなければならない。

#### 6.1.3.1 REQ\_TD 3.1

#### 要件

- 技術文書には、4.2 節で文書化されたリスクアセスメントのプロセスを含めなければならない (MUST)。

#### 評価基準

- 評価者は、4.2 項の要件に従った文書が入手可能であることを確認しなければならない (MUST)。

### 6.1.4 REQ\_TD 4 - サポート期間の文書化

**CRA 附属書 VII の現行草案に記載されている要件：**技術文書には、サポート期間を決定するために考慮された関連情報を記載しなければならない。

#### 6.1.4.1 REQ\_TD 4.1

##### 要件

- 技術文書には、4.2 項のリスクアセスメント要求事項に従ってサポート期間をどのように決定するかを記載しなければならない。

##### 評価基準

- 評価者は、4.2 節の要件が満たされていることをチェックしなければならない (MUST)。

#### 6.1.5 REQ\_TD 5 - 実施した試験の文書化

注：附属書 VII 番号 5 は、整合規格がまだ存在しないため、意図的に省略した。

**CRA 附属書 VII の現行草案に記載されている要件：**技術文書には、デジタル要素を含む製品の適合性、及び適用される必須要件に対する脆弱性処理プロセスの適合性を検証するために実施された試験の報告書を含まなければならない。

##### 6.1.5.1 REQ\_TD 5.1

##### 要件

- 技術文書には、5.3 節に規定された必須要件と 5.4 節に規定された脆弱性ハンドリング要件の評価がどのように行われたかを含めなければならない (MUST)。
- 評価中に行われたすべての決定、使用された方法、または結果は文書化されなければならない。これには意思決定の理由も含まれる。

##### 評価基準

- 評価者は、実施された評価基準のプロセスが適切に文書化されていることを評価しなければならない (MUST)。

#### 6.1.6 REQ\_TD 6 - コンポーネントの文書化

注：EU 適合宣言は本文書から独立しているため、附属書 VII 番号 7 は意図的に省略した。

**CRA 附属書 VII の現行草案に記載されている要件：**技術文書には、市場監視当局が附属書 I に定める必須要件への準拠をチェックするために必要であることを条件として、市場監視当局からの合理的な要求があれば、該当する場合、ソフトウェア部品表を含めなければならない。

##### 6.1.6.1 REQ\_TD 6.1

##### 要件

- 技術文書には、5.4.1 項に従って作成された SBOM を含めなければならない。

##### 評価基準

- 評価者は、5.4.1 節に規定された要件に合格していることをチェックしなければならない (MUST)。

## 6.2 ユーザ文書

ユーザ文書は一般に公開され、関連製品とともに提供されなければならない。

### 6.2.1 REQ\_UD 1 - 製造者の文書化

**CRA 附属書 II の現行草案に記載されている要件：**デジタル要素を含む製品には、製造者の名称、登録商号または登録商標、郵便番号、電子メールアドレスまたはその他のデジタル連絡先、および入手可能な場合は製造者と連絡可能なウェブサイトを添付しなければならない。

#### 6.2.1.1 REQ\_UD 1.1

##### 要件

- TOE に関連する公開ユーザ文書には、製造者の名称、登録商号または登録商標、郵送先住所、E メールアドレスまたはその他のデジタル連絡先、および可能な場合は製造者に連絡する手段のあるウェブサイトを含めなければならない (MUST)。

##### 評価基準

- 評価者は、ユーザマニュアルが発行され、製造者の名称、登録商号または登録商標、郵送先住所、電子メールアドレスまたはその他のデジタル連絡先、さらに可能であれば、製造者に連絡する手段のあるウェブサイトが記載されていることを確認しなければならない (MUST)。

### 6.2.2 REQ\_UD 2 - 固有識別子の文書化

**CRA 附属書 II の現行草案に記載されている要件：**デジタル要素を含む製品には、名称、型式、およびデジタル要素を含む製品の一意な識別を可能にする追加情報を添付しなければならない。

#### 6.2.2.1 REQ\_UD 2.1

##### 要件

- TOE に関連するユーザ文書には、TOE の名前とタイプ、および TOE を一意に識別するための追加情報を含めなければならない。

##### 評価基準

- 評価者は、ユーザ文書に TOE の名前とタイプ、および TOE を一意に識別するための追加情報が含まれていることを確認しなければならない (MUST)。
- 評価者は、TOE が一意に識別可能であることを評価しなければならない。

### 6.2.3 REQ\_UD 3 - 使用目的の文書化

注：附属書 II 番号 3 は、脆弱性の扱いがすでに 5.4 節で扱われているため、意図的に省略した。

**CRA 附属書 II の現行草案に記載されている要件：**デジタル要素を含む製品には、製造者が提供するセキュリティ環境を含むデジタル要素を含む製品の意図された目的、製品の本質的な機能、セキュリティ特性に関する情報、デジタル要素を含む製品の意図された目的に従って、または合理的に予

見可能な誤用 の状況下で、重大なサイバーセキュリティリスクにつながる可能性のあるデジタル要素を含む製品の使用に関連する既知のまたは予見可能な状況を添付しなければならない。

#### 6.2.3.1 REQ\_UD 3.1

##### 要件

- TOE に関連するユーザ文書には、TOE の意図された目的に関する情報を含めなければならない。

##### 評価基準

- 評価者は、TOE の意図された目的がユーザ文書に文書化されていることを評価しなければならない。

#### 6.2.3.2 REQ\_UD 3.2

##### 要件

- TOE に関連するユーザ文書には、意図された目的に従って、または合理的に予見可能な誤用の条件下で、重大なサイバーセキュリティ・リスクにつながる可能性のある、デジタル要素を含む製品の使用に関連する、既知のまたは予見可能な状況に関する情報を含めなければならない (MUST)。

##### 評価基準

- 評価者は、意図された目的に従って、または合理的に予見可能な誤用の条件下で、デジタル要素を含む製品を使用することに関連する、重大なサイバーセキュリティリスクを引き起こしかねない既知のまたは予見可能な状況に関する情報が、ユーザ文書に含まれているかどうかを評価しなければならない (MUST)。

#### 6.2.4 REQ\_UD 4 - サポート期間の文書化

注：EU 適合宣言は本文書から独立しているため、附属書 II 番号 6 は意図的に省略した。

**CRA 附属書 II の現行草案に記載されている要件：** デジタル要素を含む製品には、製造者が提供する技術的セキュリティサポートの種類と、ユーザが脆弱性への対応とセキュリティ更新プログラムの提供を期待できるサポート期間の終了日を明記しなければならない。

#### 6.2.4.1 REQ\_UD 4.1

##### 要件

- TOE に関連するユーザ文書には、製造者が提供する技術セキュリティサポートの種類と、ユーザが脆弱性の対応とセキュリティアップデートの受領を期待できるサポート期間の終了日を含めなければならない。

## 評価基準

- 評価者は、ユーザ文書に、製造者が提供する技術セキュリティサポートの種類と、ユーザが脆弱性の対応とセキュリティ更新の受領を期待できるサポート期間の終了日が記載されていることを評価しなければならない (MUST)。

### 6.2.5 REQ\_UD 5 - ユーザガイダンス

**CRA 附属書Ⅱの現行草案に記載されている要件：** デジタル要素を含む製品には、詳細な説明書、またはそのような詳細な説明書やユーザに関連する情報を参照するユニバーサル・リソース・ロケータ (URL) を添付しなければならない。

#### 6.2.5.1 REQ\_UD 5.1

##### 要件

- TOE に関連するユーザ文書には、TOE の安全な使用を保証するために、最初のコミッショニング時および TOE のライフタイムを通じて必要な措置に関する詳細な情報を含めなければならない (MUST)。
- TOE に関連するユーザ文書には、TOE への変更がデータのセキュリティにどのような影響を与えるかに関する詳細な情報を含めなければならない。
- TOE に関連するユーザ文書には、セキュリティ関連のアップデートをインストールする方法に関する詳細な情報を含めなければならない。
- TOE に関連するユーザ文書には、ユーザデータを安全に削除する方法に関する情報を含め、デジタル要素を含む製品の安全な廃棄に関する詳細情報を含めなければならない (MUST)。
- TOE に関連するユーザ文書には、セキュリティ更新の自動インストールを有効にするデフォルト設定をオフにする方法に関する詳細情報を含めなければならない。
- TOE に関連するユーザ文書には、TOE がデジタル要素を持つ他の製品に統合されることを意図している場合の詳細情報と、統合者が必須要件に準拠するために必要な情報を含めなければならない。

##### 評価基準

- 評価者は、TOE の安全な使用を保証するために、初期立上げ時及び TOE のライフタイムを通じて必要な措置に関する詳細な情報がユーザ文書に含まれていることを評価しなければならない (MUST)。
- 評価者は、ユーザ文書に、TOE に対する変更がデータのセキュリティにどのように影響するかについての詳細な情報が含まれていることを評価しなければならない (MUST)。
- 評価者は、ユーザ文書に、セキュリティ関連の更新をインストールする方法に関する詳細な情報が含まれていることを評価しなければならない (MUST)。

- 評価者は、ユーザ文書に、ユーザデータを安全に削除する方法に関する情報を含め、デジタル要素を含む製品の安全な廃止に関する詳細な情報が含まれていることを評価しなければならない (MUST)。
- 評価者は、セキュリティ更新プログラムの自動インストールを有効にするデフォルト設定をオフにする方法に関する詳細な情報が、ユーザ文書に含まれていることを評価しなければならない (MUST)。
- 評価者は、TOE がデジタル要素を持つ他の製品への統合を意図している場合、及び統合者が必須要件に準拠するために必要な情報の詳細がユーザ文書に含まれていることを評価しなければならない (MUST)。

### 6.2.6 REQ\_UD 6 - コンポーネントの文書化

**CRA 附属書Ⅱの現行草案に記載されている要件：** デジタル要素を含む製品には、製造者がソフトウェアの部品表をユーザに提供することを決定した場合、ソフトウェアの部品表にアクセスできる場所に関する情報を添付しなければならない。

#### 6.2.6.1 REQ\_UD 6.1

##### 推薦

- TOE に関連するユーザ文書には、5.4.1 項に従って作成された SBOM を含めてもよい。

##### コンディション：

- TOE の SBOM が発表される。

##### 評価基準

- 評価者は、5.4.1 節に規定された要件に合格していることをチェックしなければならない (MUST)。
- 評価者は、SBOM が一般に入手可能であることを確認しなければならない (MUST)。

## 7 附属書

この附属書では、本文書で規定される要求事項の策定時に考慮され、基礎とされた関連規格の概要を示す。

要件	ETSI EN 303 645	EN IEC 62443	その他の規格
<b>REQ_RA 1 - リスクアセスメント</b>			
REQ_RA 1.1		SR-1, SR-2	ISO 27005
<b>REQ_ER 1 - デザインによるセキュリティ</b>			
REQ_ER 1.1		<b>62443-4-1:</b> SR-1、SR-2、SR-3、SR-4、SR-5、SVV-1、SVV-2、DM-3、DM-4	
REQ_ER 1.2	ETSI EN 303 645 (5.6-9)	<b>62443-4-1:</b> SD-1、SD-2、SD-3、SD-4	
<b>REQ_ER 2 - 既知の脆弱性はない</b>			
REQ_ER 2.1	ETSI EN 303 645 (5.3-4, 5.3-5)	<b>62443-4-1:</b> SUM-5	
REQ_ER 2.2	ETSI EN 303 645 (5.3-8)	<b>62443-4-1:</b> SV-1、SV-3、DM-1、DM-2、DM-3、DM-4	
REQ_ER 2.3	ETSI EN 303 645 (5.3-8)	<b>62443-4-1:</b> DM-1、DM-2、DM-3、DM-4	
<b>REQ_ER 3 - 安全なデフォルト設定</b>			
REQ_ER 3.1	ETSI EN 303 645 (5.11-1)	<b>62443-4-2:</b> CR 7.4	
REQ_ER 3.2	ETSI EN 303 645 (5.4-3)		
<b>REQ_ER 4 - セキュリティ・アップデート</b>			
REQ_ER 4.1	ETSI EN 303 645 (5.3-1)	<b>62443-4-2:</b> CR 3.10	
REQ_ER 4.2	ETSI EN 303 645 (5.3-2)	<b>62443-4-2:</b> CR 3.10	
REQ_ER 4.3	ETSI EN 303 645 (5.3-5)		
REQ_ER 4.4	ETSI EN 303 645 (5.3-5)		

要件	ETSI EN 303 645	EN IEC 62443	その他の規格
REQ_ER 4.5	ETSI EN 303 645 (5.3-3)		
REQ_ER 4.6	ETSI EN 303 645 (5.3-3)	<b>62443-4-2:</b> CR 3.7	
<b>REQ_ER 5 - アクセス・コントロール</b>			
REQ_ER 5.1		<b>62443-4-2:</b> CR 1.1、CR 1.2	ISO 27001 (附属書 A.9)
REQ_ER 5.2	ETSI EN 303 645 (5.1-1)	<b>62443-4-2:</b> CR 1.5	
REQ_ER 5.3	ETSI EN 303 645 (5.1-2)	<b>62443-4-2:</b> CR 1.7	
REQ_ER 5.4	ETSI EN 303 645 (5.1-3)	<b>62443-4-2:</b> CR 1.5	
REQ_ER 5.5	ETSI EN 303 645 (5.1-4)	<b>62443-4-2:</b> CR 1.5	
REQ_ER 5.6	ETSI EN 303 645 (5.1-5)	<b>62443-4-2:</b> CR 1.11	
REQ_ER 5.7		<b>62443-4-2:</b> CR 1.10	OWSP・ASVS (v2.1)
REQ_ER 5.8	ETSI EN 303 645 (5.1-5)	<b>62443-4-2:</b> CR 2.8	
<b>REQ_ER 6 - 機密保護</b>			
REQ_ER 6.1	ETSI EN 303 645 (5.5-1)	<b>62443-4-2:</b> CR 1.5	
REC_ER 6.2	ETSI EN 303 645 (5.5-2)	<b>62443-4-2:</b> CR 4.3	
REQ_ER 6.3		<b>62443-4-2:</b> CR 4.3	OWSP・ASVS (V3)
REC_ER 6.4	ETSI EN 303 645 (5.4-1)	<b>62443-4-2:</b> CR 4.3	
REQ_ER 6.5	ETSI EN 303 645 (5.5-8)	<b>62443-4-2:</b> CR 4.3	
<b>REQ_ER 7 - 完全性の保護</b>			
REC_ER 7.1	ETSI EN 303 645 (5.7-1, 5.7-2)	<b>62443-4-2:</b> CR3.1、CR3.4、 CR3.14、CR4.3	

要件	ETSI EN 303 645	EN IEC 62443	その他の規格
REQ_ER 7.2			ETSI TS 103 732-1 (fdp_acf.1.2)
REQ_ER 7.3			BSI TR-03180 A
REQ_ER 7.4		<b>62443-4-2:</b> CR 3.4、CR 3.6	OWASP・ASVS (v11)
<b>REQ_ER 8 - データの最小化</b>			
REQ_ER 8.1	ETSI EN 303 645 (5.6-7, 6-4)		
<b>REQ_ER 9 - 必要不可欠で基本的な機能の利用可能性</b>			
REQ_ER 9.1	ETSI EN 303 645 (5.6-1 - 5.6-5)	<b>62443-4-2:</b> CR 7.7	
REQ_ER 9.2	ETSI EN 303 645 (5.9-1, 5.9-2)	<b>62443-4-2:</b> CR 3.6	
REQ_ER 9.3	ETSI EN 303 645 (5.9-1, 5.9-2)	<b>62443-4-2:</b> CR 3.6	
REQ_ER 9.4	ETSI EN 303 645 (5.9-1, 5.9-2)		
<b>REQ_ER 10 - マイナス影響を最小限に抑える</b>			
REQ_ER 10.1	ETSI EN 303 645 (規定 5.9-3)	<b>62443-4-2:</b> CR 5.1	
REQ_ER 10.2	ETSI EN 303 645 (規定 5.9-3)	<b>62443-4-2:</b> CR 5.1	
<b>REQ_ER 11 - 攻撃面を制限する</b>			
REQ_ER 11.1	ETSI EN 303 645 (5.6-1 - 5.6-5)	<b>62443-4-2:</b> CR 5.1、CR 7.7	
REQ_ER 11.2	ETSI EN 303 645 (5.6-4)	<b>62443-4-2:</b> CR 5.2、CR 7.7	
<b>REQ_ER 12 - インシデントの軽減</b>			
REQ_ER 12.1	ETSI EN 303 645 (5.6-7)	<b>62443-4-2:</b> CR 2.1	
REQ_ER 12.2	ETSI EN 303 645 (5.6-7)	<b>62443-4-2:</b> CR2.1、CR1.3、CR1.5	
<b>REQ_ER 13 - 記録とモニタリング</b>			
REQ_ER 13.1	ETSI EN 303 645 (5.10-1)	<b>62443-4-2:</b> CR 2.8、CR 6.2	

要件	ETSI EN 303 645	EN IEC 62443	その他の規格
REQ_ER 13.2	ETSI EN 303 645 (5.10-1)	<b>62443-4-2:</b> CR 2.8、CR 6.2	
REQ_ER 13.3	ETSI EN 303 645 (5.10-1)	<b>62443-4-2:</b> CR 2.8、CR 6.2	
REQ_ER 13.4	ETSI EN 303 645 (5.10-1)		
REQ_ER 13.5	ETSI EN 303 645 (5.10-1)	<b>62443-4-2:</b> CR2.8、CR2.10、CR6.2	
REQ_ER 13.6	ETSI EN 303 645 (5.10-1)	<b>62443-4-2:</b> CR 2.8	
REQ_ER 13.7	ETSI EN 303 645 (5.10-1)	<b>62443-4-2:</b> CR 3.7	
REQ_ER 13.8	ETSI EN 303 645 (5.10-1)		
<b>REQ_ER 14 - データと設定の削除</b>			
REQ_ER 14.1	ETSI EN 303 645 (5.11-1)	<b>62443-4-2:</b> CR 4.2	
REQ_ER 14.2	ETSI EN 303 645 (5.11-2)	<b>62443-4-1:</b> SG-4 <b>62443-4-2:</b> CR 4.2	
REQ_ER 14.3	ETSI EN 303 645 (5.11-1)	<b>62443-4-1:</b> SG-4 <b>62443-4-2:</b> CR 4.2	
REQ_ER 14.4	ETSI EN 303 645 (5.11-1)	<b>62443-4-1:</b> SG-4 <b>62443-4-2:</b> CR 4.2	
REQ_ER 14.5	-	<b>62443-4-2:</b> CR 4.1、CR 4.3	
<b>REQ_VH 1 - コンポーネントとバーネラビリティを特定する</b>			
REQ_VH 1.1			
REQ_VH 1.2		<b>62443-4-1:</b> DM-1、DM-2、DM-3、 DM-4	
<b>REQ_VH 2 - 脆弱性に対処する</b>			

要件	ETSI EN 303 645	EN IEC 62443	その他の規格
REQ_VH 2.1		<b>62443-4-1:</b> DM-4、SUM-1、SUM-2、SUM-3、SUM-4、SUM-5	
<b>REQ_VH 3 - 定期テスト</b>			
REQ_VH 3.1	ETSI EN 303 645 (5.2-3)	<b>62443-4-1:</b> SVV-1、SVV-2、SVV-3、SVV-4	
<b>REQ_VH 4 - 対応済みの脆弱性を公表する</b>			
REQ_VH 4.1		<b>62443-4-1:</b> DM-5	
REQ_VH 4.2			
REC_VH 4.3			
<b>REQ_VH 5 - 脆弱性情報開示ポリシーの調整</b>			
REC_VH 5.1	ETSI EN 303 645 (5.2-1)	<b>62443-4-1:</b> DM-1	
<b>REQ_VH 6 - アップデートの安全な配布</b>			
REQ_VH 6.1		<b>62443-4-1:</b> SUM1、SUM-2、SUM-3、SUM-4、SUM-5	
<b>REQ_VH 7 - アップデートの普及</b>			
REQ_VH 7.1			
REQ_VH 7.2	ETSI EN 303 645 (5.3-3)	<b>62443-4-1:</b> SUM-2	
<b>REQ_TD 1 - 一般文書</b>			
REQ_TD 1.1		<b>62443-4-1:</b> SM-1、SM-3	
REQ_TD 1.2			
<b>REQ_TD 2 - プロセスの文書化</b>			
REQ_TD 2.1		<b>62443-4-1:</b> SM-1、SM-2、SM-7、SM-9	
REQ_TD 2.2		<b>62443-4-1:</b> SM-11	

要件	ETSI EN 303 645	EN IEC 62443	その他の規格
<b>REQ_TD 3 - サイバーセキュリティリスクの文書化</b>			
REQ_TD 3.1			
<b>REQ_TD 4 - サポート期間の文書化</b>			
REQ_TD 4.1		<b>62443-4-1:</b> SM-1	
<b>REQ_TD 5 - 実施した試験の文書化</b>			
REQ_TD 5.1		<b>62443-4-1:</b> SM-12	
<b>REQ_TD 6 - 構成部品の文書化</b>			
REQ_TD 6.1			
<b>REQ_UD 1 - 製造者の文書</b>			
REQ_UD 1.1			
<b>REQ_UD 2 - 固有識別子の文書化</b>			
REQ_UD 2.1	ETSI EN 303 645 (5.3-16)		
<b>REQ_UD 3 - 使用目的の文書化</b>			
REQ_UD 3.1			
REQ_UD 3.2			
<b>REQ_UD 4 - サポート期間の文書化</b>			
REQ_UD 4.1	ETSI EN 303 645 (5.3-13)		
<b>REQ_UD 5 - ユーザガイダンス</b>			
REQ_UD 5.1	ETSI EN 303 645 (5.8.3)	<b>62443-4-1:</b> SR-3、SR-4	
<b>REQ_UD 6 - コンポーネントの文書化</b>			
REQ_UD 6.1			