VDA QMC

AUTOMOTIVE SPICE®

サイバーセキュリティエンジニアリングのための

Automotive SPICE®

プロセス参照モデル兼プロセスアセスメントモデル

バージョン 2.0

タイトル：	サイバーセキュリティのための Automotive SPICE® プロセス参照モデル兼プロセスアセスメントモデル
著者：	VDA ワーキンググループ 13
バージョン：	2.0
日付：	2025 年 3 月 28 日
ステータス：	リリース済

翻訳について

本翻訳文書は、英語版原文の内容についてより良い理解を得られるようにするために提供する。本翻訳文書は参考情報につき、内容に疑義がある場合は、 VDA QMC ウェブサイト (www.vda-qmc.de) で提供しているサイバーセキュリティのための Automotive SPICE® プロセス参照モデル兼プロセスアセスメントモデルの英語版のみを有効な文書として取り扱わなければならない。

本翻訳は、以下の企業による支援に基づいて実施された。

ビジネスキューブ・アンド・パートナーズ株式会社

〒150-0012

東京都渋谷区広尾一丁目 13 番 1 号

電話：+81-3-5791-2121

URL：https://biz3.co.jp/

VDA、VDA QMC、およびワーキンググループ 13 は、日本語版作成にあたり、ビジネスキューブ・アンド・パートナーズ株式会社の貢献に深く感謝する。

著作権通知

本文書は Automotive SPICE® プロセス参照モデル／プロセスアセスメントモデル（PRM/PAM）バージョン 4.0 を補完するものであり、ドイツ自動車工業会（VDA）によって作成された。

サイバーセキュリティのための Automotive SPICE® プロセスアセスメントモデルは、 VDA QMC ウェブサイト (www.vda-qmc.de) にある Automotive SPICE® のページから無料でダウンロードして入手できる。

謝辞

VDA、VDA QMC、およびワーキンググループ 13 は、intacs®のワーキンググループメンバーによって実施された質の高い作業に対して多大な感謝を表す。Automotive SPICE® の執筆および発行に貢献されたすべての関係者に感謝する。

派生著作物

本文書は、VDA QMC の事前承諾なしに、改変、変換、または構築してはならない。承諾は、ISO の著作権侵害がない限り与えられる。

本文書の詳細記述は、有償で提供されないのであれば、プロセスアセスメントの実施を支援し、本プロセスアセスメントモデルをその意図された目的で使用できるように、いかなるツールまたは資料に取り入れてもよい。

全派生著作物は、無償で提供しなければならない。

文書配布

Automotive SPICE® プロセスアセスメントモデルは、 www.vda-qmc.de からのダウンロードによりのみ入手可能である。本文書を二次配布することは認められない。

変更依頼

問題点または変更依頼は、 www.vda-qmc.de で指定した仕組みを通して報告すること。

商標

Automotive SPICE® は、Verband der Automobilindustrie e.V. (VDA)の登録商標である。

Automotive SPICE® の詳細な情報は、 www.vda-qmc.de で確認すること。

文書履歴

バージョン	日付	発行者	備考
1.0	2021 年 7 月 16 日	VDA QMC PG13	初版
2.0	**2025 年 3 月 28 日**	**VDA QMC WG13**	**CS PAM の改訂、4.0 への対応**

目次

図の一覧

表の一覧

1. 序文

1.1. 適用範囲

UNECE 規則 R155 は、とりわけ、自動車メーカーがサプライチェーンにおけるサイバーセキュリティリスクを特定し、管理することを要求している。Automotive SPICE® のプロセスアセスメントモデルは、適切なアセスメント手法で使用される場合に、プロセス関連の製品リスクを特定するために役立つ。サイバーセキュリティ関連のプロセスを Automotive SPICE® の実証済の適用範囲に組み込むために、追加のプロセスがサイバーセキュリティエンジニアリングのためのプロセス参照モデルおよびプロセスアセスメントモデル（サイバーセキュリティ PAM）に定義された。

本文書は、サイバーセキュリティ関連の開発プロセスの評価を可能にすることによって、Automotive SPICE® 4.0 を補完している。

サイバーセキュリティのための Automotive SPICE® PAM を用いてアセスメントを実施するための前提条件は、VDA 推奨スコープに対して Automotive SPICE® のアセスメント結果が存在することである。それ以外の場合は、サイバーセキュリティのための Automotive SPICE® PAM および VDA 推奨スコープのプロセスに対する Automotive SPICE® PAM の両方を用いたアセスメントが実施されなければならない。

付録 B には、サイバーセキュリティのための Automotive SPICE® のプロセスに関連する情報項目特性のサブセットが含まれている。

付録 C には、サイバーセキュリティのための Automotive SPICE® のプロセスに関連する用語のサブセットが含まれている。

1.2. ISO/SAE 21434 との関係

Automotive SPICE® アセスメントの目的は、主要ライフサイクルプロセス、組織ライフサイクルプロセス、および支援ライフサイクルプロセスにおける系統的な弱みを特定することである。

サイバーセキュリティのための Automotive SPICE® のアセスメントでは、サイバーセキュリティ活動を実施しているプロジェクトにおけるギャップおよびプロセスの弱みを特定することができる。これらのギャップおよび弱みは、組織内のサイバーセキュリティプロセスを改善するための貴重なインプットである。アセスメント結果から導出された効果的な改善策を実施することで、組織はサイバーセキュリティマネジメントシステムを調整し、改良することができる。

Automotive SPICE® 4.0 およびサイバーセキュリティのための Automotive SPICE® は、システムエンジニアリング、ソフトウェアエンジニアリングおよびハードウェアエンジニアリングを対象としている。メカニカルエンジニアリングに対する指標は、現在の Automotive SPICE® PAM には含まれていない。

Automotive SPICE® のリスク範囲は、意図的に ISO/SAE 21434 で定義された範囲よりも広げている。ISO/SAE 21434 は道路利用者に焦点を当てているのに対し、サイバーセキュリティのための Automotive SPICE® は、サイバーセキュリティに関連するソフトウェアベースシステムの開発に影響を与える可能性のある、自動車エコシステム全体におけるリスクに対処している。

ISO/SAE 21434 のある特定の側面は、開発プロジェクトのコンテキストで実施されないため、本文書の範囲外である。これらは ISO PAS 5112 で扱われ、サイバーセキュリティマネジメントシステムの監査対象となる。

本文書では、分散サイバーセキュリティ活動、コンセプト開発、製品開発、サイバーセキュリティの妥当性確認、ならびに脅威分析およびリスク評価に対するプロセスの能力判定を支援している。

プロジェクトに依存するサイバーセキュリティ管理は、以下のように支援されている。

- サイバーセキュリティの責任：
  GP 2.1.3：リソースニーズを決定する。
- サイバーセキュリティの計画：
  GP 2.1.2：プロセスの実施を計画する。
  MAN.3 プロジェクト管理
- サイバーセキュリティ活動のテーラリング：
  PA 3.2：プロセスの展開
  GP 2.1.2：プロセスの実施を計画する。
- 再利用：
  内製、外製、再利用の分析を含む。SWE.2.BP3：ソフトウェアアーキテクチャの分析
  SYS.3.BP3：システムアーキテクチャの分析
  REU.2 製品の再使用管理
- コンテキスト外のコンポーネント：サイバーセキュリティゴールに関する想定に基づき、サイバーセキュリティエンジニアリングプロセス群（SEC）によって網羅される。
- オフ・ザ・シェルフのコンポーネント：
  MAN.3.BP7 プロジェクトの窓口および合意されたコミットメントの定義および監視
  Automotive SPICE® ガイドライン v2.0 第 2.5.3 章 アセスメント対象プロジェクト（DEX）に対する外部開発
  MAN.7 サイバーセキュリティリスク管理
- サイバーセキュリティケース：
  エンジニアリングプロセスの基本プラクティス「結果の要約および伝達」によって提供されるインプット
- サイバーセキュリティアセスメント：
  サイバーセキュリティのための Automotive SPICE® はプロセス能力を判定するためのモデルである。詳細な技術分析は、サイバーセキュリティのための Automotive SPICE® のアセスメントに含まれない。
- 開発後工程へのリリース：
  SPL.2 製品リリース
  SUP.8 構成管理
  SUP.1 品質保証
- 見積依頼（RFQ）：
  ACQ.2 サプライヤー依頼および選定
- 責任の調整：
  ACQ.4 サプライヤー監視

1.3. アセスメント範囲に関する要求

一般的に、アセスメント範囲の決定はスポンサーの裁量に委ねられる。

既存のアセスメントを活用してプロセスプロファイル全体を評価する場合、SUP プロセス群のプロセスを再評価する必要はない。アセスメントがサイバーセキュリティに関連する開発のコンテ

キストで実施される場合には、PRM および PAM におけるサイバーセキュリティ特有のすべての側面を考慮しなければならない。

既存のアセスメントの有効性については、Automotive SPICE® ガイドライン v2.0 第 10.2 章に記載されている。

根拠：

リスク対応妥当性確認プロセスは、サイバーセキュリティゴールに焦点を当てるが、妥当性確認プロセスは、すべての利害関係者の目標または利害関係者要求に言及している。

それぞれのプロセス目的を比較すれば、これが明らかである。

SEC.4 の目的は、統合されたシステムが関連するサイバーセキュリティゴールを達成していることを確認することであると宣言している。

しかし、VAL.1 の目的は、納入された製品がその運用対象環境において意図された使用上の期待事項を満足しているという証拠を提供することである。

サイバーセキュリティゴールは、通常、意図しない使用を含めて損害シナリオおよび攻撃経路分析を考慮してセキュリティ特性から導出される。これは、実際の環境またはシミュレーション環境で妥当性が確認される。

リスク対応妥当性確認（プロセス）は、意図しない使用が望ましくない製品の振る舞いにつながらないことを証明することである。妥当性確認（プロセス）は、納入された製品において受け取る側の期待事項が満たされていることを確実にすることである。

ACQ.2 は、サイバーセキュリティに関連する製品を開発するサプライヤーに対して、ポテンシャルアナリシスという意味合いで一回実施されるプロセスとして記述されている。したがって、このプロセスは、この特定のコンテキストの中で評価されるべきである。一方、Automotive SPICE® ポテンシャルアナリシスは、いかなる場合においても使用できる。

サイバーセキュリティのための Automotive SPICE® のアセスメント対象範囲は、必要に応じて調整してよい。例えば、サプライヤーがサイバーセキュリティゴールの妥当性確認に関与していない場合、SEC.4 は対象範囲から除外することができる。

2. 適合証明

Automotive SPICE® プロセスアセスメントモデルおよびプロセス参照モデルは、ISO/IEC33004:2015 に適合しており、プロセス能力アセスメントの実施における基礎として使用できる。

Automotive SPICE® 4.0 は、ISO/IEC 33003:2015 に適合した測定の枠組みとして使用する。

プロセスアセスメントモデルおよびプロセス参照モデルが ISO/IEC33004:2015 の要求に適合していることを示す証明は、付録 A に記載されている。

測定の枠組みが ISO/IEC33003:2015 の要求に適合していることを示す証明は、Automotive SPICE® 4.0 の付録 A に記載されている。

3. プロセス能力判定

プロセスアセスメントモデルを使用したプロセス能力判定のコンセプトは、2 つの座標軸の枠組みに基づく。1 つ目の座標は、プロセス参照モデルで定義されたプロセスによって提供される（プロセス座標）。2 つ目の座標は、能力レベルで構成されており、この能力レベルはさらにプロセス属性へ分割される（能力座標）。プロセス属性は、プロセス能力に対する測定可能な特性を提供する。

プロセスアセスメントモデルは、プロセス参照モデルからプロセスを選定し、指標で補足している。この指標は、客観的な証拠の収集に役立てられ、アセッサーが能力座標に基づいてプロセスの評定を割り当てることを可能にする。

関係性を図 1 に示す。

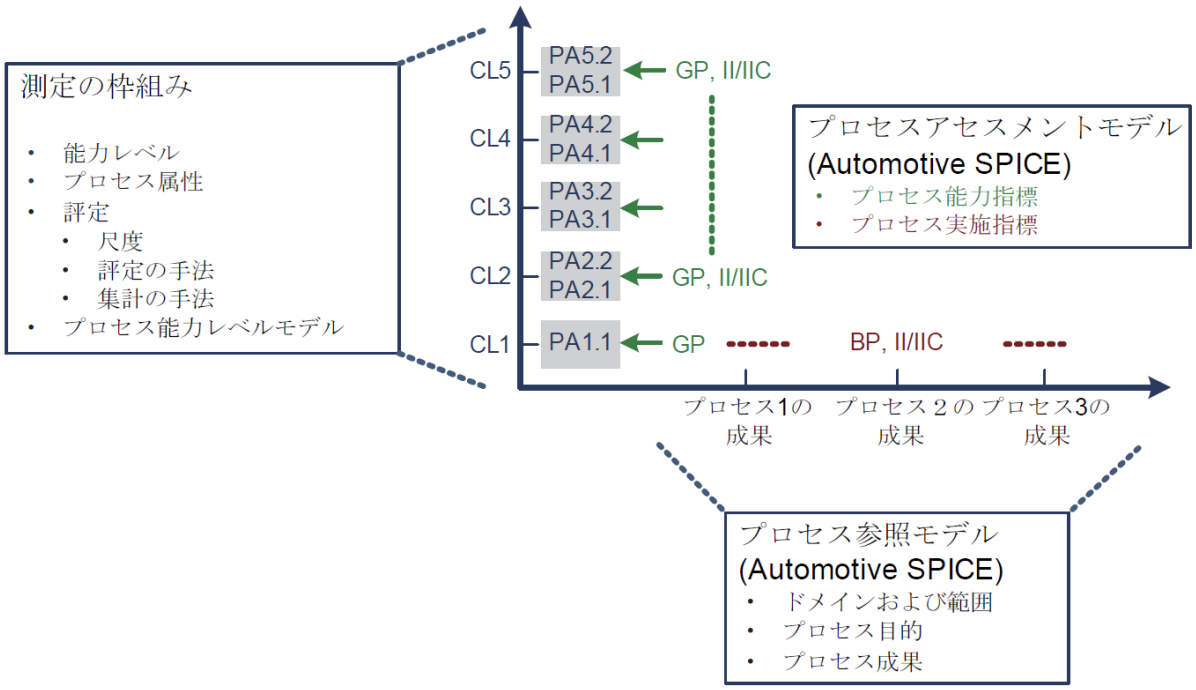

図 1 — プロセスアセスメントモデルの関係性

3.1. プロセス参照モデル

プロセスは、プロセスが扱う活動のドメインに従ってプロセス群へ分類される。

これらのプロセス群は、主要ライフサイクルプロセス、組織ライフサイクルプロセス、および支援ライフサイクルプロセスの 3 つのプロセスカテゴリーで構成される。

各プロセスには、プロセス目的の説明文が記載され、プロセスを特定の環境で実施する際のプロセス固有の機能目的が含まれる。各プロセス目的の説明文は、プロセス成果一覧と関連付けられている。このプロセス成果は、プロセスを実施した際に期待される望ましい結果の一覧である。

Automotive SPICE® およびサイバーセキュリティのための Automotive SPICE® のプロセス参照モデルは、プロセス座標に対して図 2 で示すプロセスの集合を提供している。本文書では、サイバ

ーセキュリティに関連するプロセスについて記述している。その他のプロセスについては、Automotive SPICE® 4.0 を参照すること。

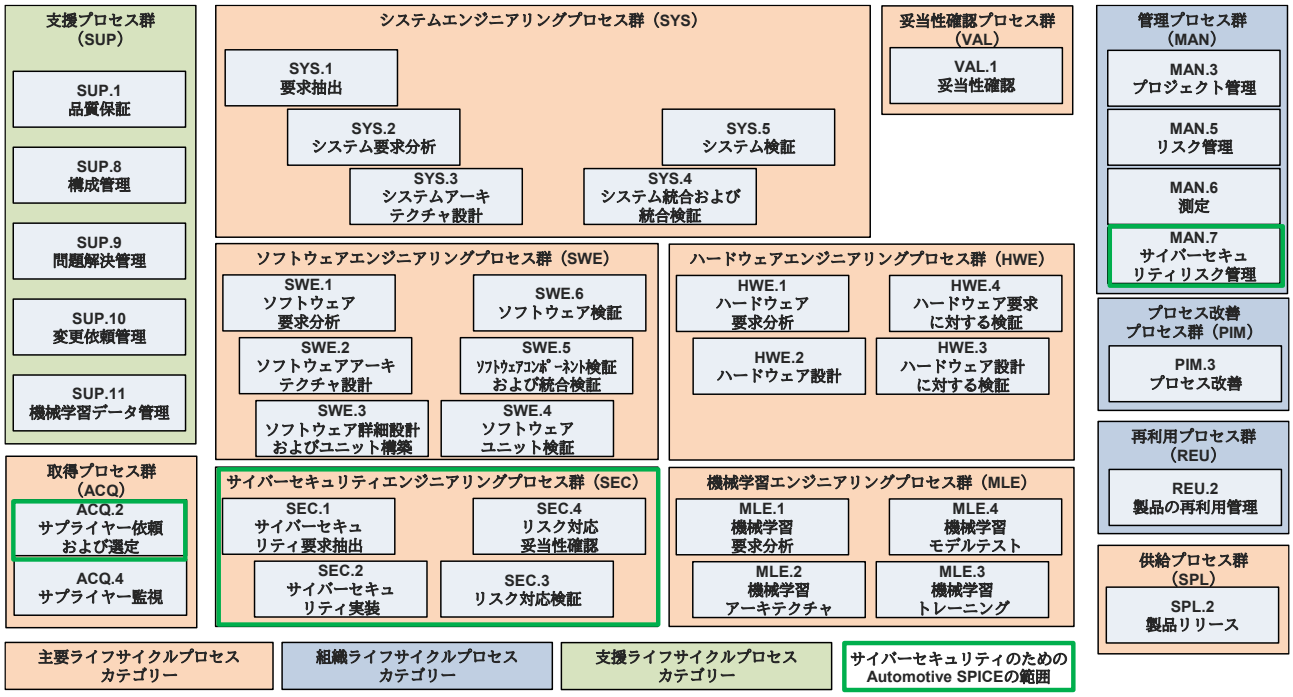

図 2 — Automotive SPICE® およびサイバーセキュリティのための Automotive SPICE® のプロセス参照モデル – 概要

3.1.1. 主要ライフサイクルプロセスカテゴリー

主要ライフサイクルプロセスカテゴリーは、取得者がサプライヤーから製品を取得する際に適用するプロセス、または利害関係者のニーズに対応する際および製品を納入する際の製品開発で適用するプロセスで構成され、仕様化、設計、実装、統合、および検証で必要とされるエンジニアリングプロセスを含む。

サイバーセキュリティのための Automotive SPICE® における主要ライフサイクルプロセスカテゴリーは、以下のプロセス群で構成される。

- 取得プロセス群
- サイバーセキュリティエンジニアリングプロセス群

取得プロセス群（ACQ）は、製品および／またはサービスを取得するために、顧客が実施するプロセス、またはサプライヤーが自社のサプライヤーに対して顧客として実施するプロセスで構成される。

ACQ.2	サプライヤー依頼および選定

表 1 — 主要ライフサイクルプロセス：ACQ

サイバーセキュリティエンジニアリングプロセス群（SEC）は、サイバーセキュリティゴールを達成するために実施されるプロセスで構成される。

SEC.1	サイバーセキュリティ要求抽出

SEC.2	サイバーセキュリティ実装
SEC.3	リスク対応検証
SEC.4	リスク対応妥当性確認

表 2 — 主要ライフサイクルプロセス：SEC

3.1.2. 組織ライフサイクルプロセスカテゴリー

組織ライフサイクルプロセスカテゴリーは、プロセス、製品、およびリソース資産を開発するためのプロセスで構成される。これらは、組織内のプロジェクトで使用された際、その組織の事業目標の達成に役立つ。

サイバーセキュリティのための Automotive SPICE® における組織ライフサイクルプロセスカテゴリーは、以下のプロセス群で構成される。

- 管理プロセス群

管理プロセス群（MAN）は、ライフサイクル内のあらゆる種類のプロジェクトまたはプロセスを管理する者が使用するプロセスで構成される。

MAN.7	サイバーセキュリティリスク管理

表 3 — 組織ライフサイクルプロセス：MAN

3.2. 測定の枠組み

プロセス能力レベル、プロセス属性、評価尺度、および能力レベル評定モデルは、Automotive SPICE® 4.0 で定義されたものと同じある。

3.3. PAM の抽象レベルの理解

用語「プロセス」は、3 段階の抽象レベルで理解できる。これらの抽象レベルは、厳密に白黒明確に定義する意図もなければ、科学的な分類構造を提供する意図もないことに注意する。ここでの要点は、実際には用語「プロセス」に複数の抽象レベルが存在し、PAM が最上位に置かれていることを理解することである。

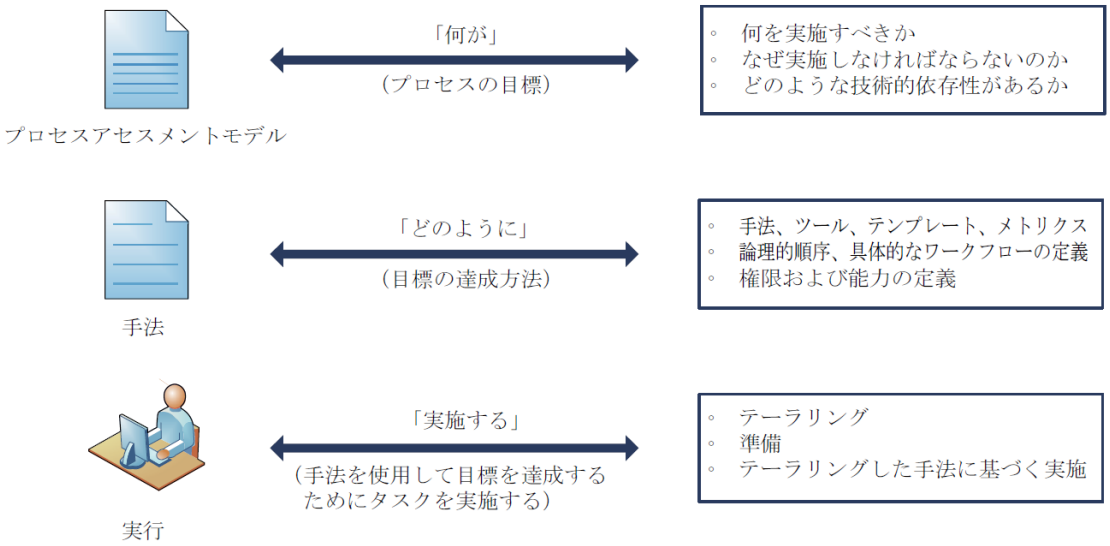

図 3 — 用語「プロセス」の抽象レベル

製品開発時に獲得した経験（「実施する」のレベル）を、他者と共有するためにその内容を反映させることは、「どのように」のレベルで行う。しかし、「どのように」は、企業、組織部門、またはプロダクトラインなどの特定のコンテキストに対して、常に固有である。例えば、あるプロジェクト、組織部門、または A 社の「どのように」は、別のプロジェクト、組織部門、または B 社にそのまま適用できない可能性がある。しかし、両者ともプロセス成果およびプロセス属性の達成成果に対して、PAM の指標で表される原則に遵守することが期待される。これらの指標は、「何が」のレベルで表され、具体的なテンプレート、手続き、ツールなどの対応に関する決定は、「どのように」のレベルで行われる。

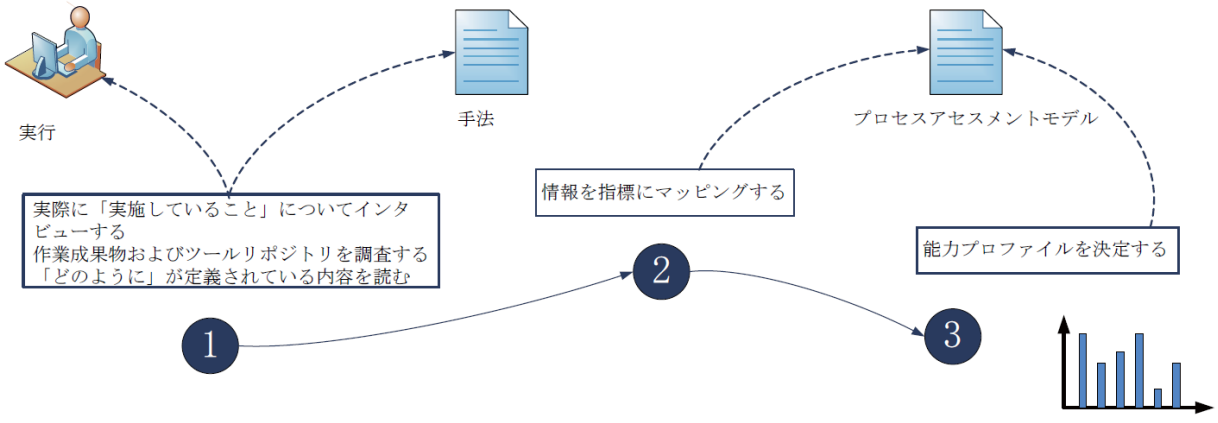

図 4 — プロセス能力判定のためのプロセスアセスメント実施

4. プロセス参照モデルおよびプロセス実施指標（レベル 1）

4.1. 取得プロセス群 (ACQ)

4.1.1. ACQ.2 サプライヤー依頼および選定

プロセス ID
ACQ.2
プロセス名
サプライヤー依頼および選定
プロセス目的
目的は、関連する基準に基づき、コミットメント／合意に向けたサプライヤーを選定することである。
プロセス成果
1) サプライヤーの評価基準が確立されている。 2) サプライヤーが定義された基準に対して評価されている。 3) 見積依頼がサプライヤー候補に発行されている。 4) コミットメント／合意書、是正処置が合意されている。評価結果を考慮して、サプライヤーとの契約が締結されている。

基本プラクティス
ACQ.2.BP1: サプライヤー評価基準の確立 サプライヤーの能力に対する評価基準を定義するために関連要求を分析する。 *備考 1: 評価基準の定義には、以下の内容を考慮する場合がある。* • *機能要求および非機能要求* • *サイバーセキュリティコンセプトおよび手法（脅威分析およびリスク評価、攻撃モデル、脆弱性分析など）を含む、サプライヤーのサイバーセキュリティ能力に関する技術的評価* • *サイバーセキュリティに関するサプライヤー組織の能力（例：開発活動、該当する開発後活動 [例：生産、運用、および廃棄]、ガバナンス、品質、および情報セキュリティからのサイバーセキュリティのベストプラクティス）* • *サイバーセキュリティを含む、継続的運用* • *過去のプロジェクトにおけるサプライヤー監視によって得られたサイバーセキュリティに関するサプライヤーの能力および実施の証拠*
ACQ.2.BP2: サプライヤー候補の評価 サプライヤーの能力に関する情報を収集し、確立された評価基準に対してそれを評価する。サプライヤー最終候補一覧を作成し、結果を文書化する。 *備考 2: サプライヤー候補の評価は、以下によって裏付けられる場合がある。* • *過去のサイバーセキュリティのための Automotive SPICE® アセスメントの要約* • *組織のサイバーセキュリティマネジメントシステムの証拠（例：該当する場合、組織の監査結果）* • *情報セキュリティマネジメントシステムの証拠*

- *組織の品質マネジメントシステムにおけるサイバーセキュリティエンジニアリングを支援するための適切性／能力の証拠*
- *過去の調達からの経験*

ACQ.2.BP3: 見積依頼（RFQ）の準備および発行
評価に基づき、サプライヤー候補を識別する。識別した逸脱に対する是正処置計画を含む見積依頼を準備し、発行する。

ACQ.2.BP4: コミットメント／合意に向けた交渉および発注
関連する要求および合意された是正処置が網羅された見積依頼回答の評価に基づき、コミットメント／合意を確立する。

備考 3: 分散サイバーセキュリティ活動は、関連するすべての側面（例：連絡先、テーラリング、責任、情報共有、マイルストーン、タイミング）を考慮して、サイバーセキュリティインタフェース協定に規定してもよい。

備考 4: サポートなしの納入物の場合（例：フリーソフトウェアおよびオープンソースソフトウェア）、インタフェース協定は不要である。

ACQ.2 サプライヤー依頼および選定	成果 1	成果 2	成果 3	成果 4
アウトプット情報項目				
02-01 コミットメント／合意				X
02-50 インタフェース協定				X
08-55 リスク対応				X
12-01 見積依頼（RFQ）			X	
14-02 是正処置			X	X
15-21 サプライヤー評価		X		
18-50 サプライヤー評価基準	X	X		
基本プラクティス				
BP1: サプライヤー評価基準の確立	X			
BP2: サプライヤー候補の評価		X		
BP3: 見積依頼（RFQ）の準備および発行			X	X
BP4: コミットメント／合意に向けた交渉および発注				X

4.2. 管理プロセス群（MAN）

4.2.1. MAN.7 サイバーセキュリティリスク管理

プロセス ID
MAN.7
プロセス名
サイバーセキュリティリスク管理
プロセス目的
目的は、関連する利害関係者への損害リスクを定期的に識別し、分析し、優先順位を付け、監視することである。
プロセス成果
1) アイテムが、その機能および境界を含めて定義されている。 2) 関連する資産、脅威、および損害シナリオが識別され、定期的に更新されている。 3) サイバーセキュリティリスクが、リスク対応の優先順位付けを支援するために、インパクト評価および攻撃実現可能性評価に基づいて分析されている。 4) リスクのステータスおよびリスク対応活動の進捗が確認されている。 5) リスクのインパクトを緩和するために、リスクの優先順位、尤度、および影響度、または他の定義されたリスク閾値に基づいて、適切な対応が実施されている。

基本プラクティス
MAN.7.BP1: サイバーセキュリティリスク管理の適用範囲の識別 アイテム、その機能、および影響を受ける関係者との境界を含むサイバーセキュリティリスク管理の適用範囲を識別し、定期的に更新する。 *備考 1: リスクには、技術的なリスク、コストに関するリスク、およびスケジュール的なリスクを含む場合がある。* *備考 2: リスク対象には、サプライヤーの成果物およびサービスを含む場合がある。* *備考 3: リスク源は、製品ライフサイクル全体に渡って変化する可能性がある。*
MAN.7.BP2: サイバーセキュリティイベントの識別 サイバーセキュリティ情報を識別し、定期的に評価し、潜在的なサイバーセキュリティイベントを導出する。影響を受ける関係者と共に、関連する資産、損害シナリオ、および脅威シナリオを更新する。
MAN.7.BP3: リスクの分析 リスク対応の優先順位付けを支援するために、潜在的なサイバーセキュリティイベントのリスクを、そのイベントがもたらす可能性のあるインパクトおよび悪用される攻撃経路の実現可能性に基づいて分析し、決定する。 *備考 4: システムの技術的なリスクを分析するために、各種技法（例：攻撃経路分析を含む TARA、シミュレーション、ETA、ATA、FTA など）が使用される場合がある。*

MAN.7.BP4: リスク対応オプションの定義
各リスクに対し、リスクを保有、低減、回避、または移転（共有）するための対応オプションを選択する。

MAN.7.BP5: リスク対応活動の定義および実施
リスク対応オプションのためのリスク活動を定義し、実施する。

MAN.7.BP6: リスクの監視
サイバーセキュリティリスクのステータス変更を決定し、リスク対応オプションを再評価し、リスク対応活動の進捗を確認するために、識別された潜在的なサイバーセキュリティイベントに関連するリスクを定期的に再評価する。

備考 5: 優先順位の高いリスクは、より上位の管理層へ伝達され、その管理層によってリスクが監視されることが必要な場合もある。

MAN.7.BP7: 是正処置の実施
リスク対応活動が効果的でない場合、適切な是正処置を講じる。

備考 6: 是正処置には、リスクの再評価、新規の緩和コンセプトの作成および実装、または既存のコンセプトの調整を含む場合がある。

MAN.7 サイバーセキュリティリスク管理	成果 1	成果 2	成果 3	成果 4	成果 5
アウトプット情報項目					
08-55 リスク対応			X	X	X
14-02 是正処置				X	X
15-09 リスクのステータス				X	X
15-51 分析結果	X	X	X		
17-53 サイバーセキュリティ脅威シナリオ		X			
基本プラクティス					
BP1: サイバーセキュリティリスク管理の適用範囲の識別	X	X			
BP2: 潜在的なサイバーセキュリティイベントの識別		X			
BP3: リスクの分析			X		
BP4: リスク対応オプションの定義				X	X
BP5: リスク対応活動の定義および実施				X	X
BP6: リスクの監視				X	
BP7: 是正処置の実施					X

4.3. サイバーセキュリティエンジニアリングプロセス群（SEC）

4.3.1. SEC.1 サイバーセキュリティ要求抽出

プロセス ID
SEC.1
プロセス名
サイバーセキュリティ要求抽出
プロセス目的
目的は、脅威シナリオを対象としたサイバーセキュリティリスク管理の成果から、サイバーセキュリティゴールおよびサイバーセキュリティ要求を仕様化することである。
プロセス成果
1) サイバーセキュリティゴールが規定されている。 2) サイバーセキュリティ要求がサイバーセキュリティゴールから導出されている。 3) 一貫性および双方向トレーサビリティが、サイバーセキュリティ要求とサイバーセキュリティゴールとの間、およびサイバーセキュリティゴールと脅威シナリオとの間で維持されている。 4) サイバーセキュリティ要求が合意され、影響を受けるすべての関係者へ伝達されている。

基本プラクティス

SEC.1.BP1: サイバーセキュリティゴールおよびサイバーセキュリティ要求の仕様化
リスクの低減を達成するためにリスク対応の決定に従って、脅威シナリオに対するサイバーセキュリティゴールを規定する。
サイバーセキュリティゴールに対するサイバーセキュリティの機能要求および非機能要求を仕様化する。
これらの要求は、定義された要求特性に従って仕様化する。

備考 1: これには、本プロセスを反復実行することによる要求の詳細化を含む。

備考 2: これには、生産、運用、保守、廃棄を含む開発後のフェーズに対する要求を含む。

備考 3: 要求特性は、ISO IEEE 29148、ISO 26262-8:2018、または INCOSE Guide to Writing Requirements などの規格に定義されている。

備考 4: 技術規格に共通して定義されている要求特性の例には、検証可能性（すなわち、検証基準が要求の文章に内在していること）、曖昧さがないこと／理解しやすいこと、設計および実装からの自由度、ならびに他の要求と矛盾しないことがある。

SEC.1.BP2: 一貫性の確保および双方向トレーサビリティの確立
サイバーセキュリティ要求とサイバーセキュリティゴールとの間の一貫性を確保し、双方向トレーサビリティを確立する。サイバーセキュリティゴールと脅威シナリオとの間の一貫性を確保し、双方向トレーサビリティを確立する。

SEC.1.BP3: 合意されたサイバーセキュリティ要求の伝達
合意されたサイバーセキュリティ要求を、影響を受けるすべての関係者へ伝達する。

備考 5: 導出されたサイバーセキュリティ要求に対して追加のコンテキスト情報を提供するために、サイバーセキュリティゴールも伝達される場合がある。

SEC.1 サイバーセキュリティ要求抽出	成果 1	成果 2	成果 3	成果 4
アウトプット情報項目				
17-00 要求	X	X		
17-54 要求の属性	X	X		
15-51 分析結果	X	X		
13-51 一貫性の証拠			X	
13-52 情報伝達の証拠				X
17-51 サイバーセキュリティゴール	X			
基本プラクティス				
BP1: サイバーセキュリティゴールおよびサイバーセキュリティ要求の仕様化	X	X		
BP2: 一貫性の確保および双方向トレーサビリティの確立			X	
BP3: 合意されたサイバーセキュリティ要求の伝達				X

4.3.2. SEC.2 サイバーセキュリティ実装

プロセス ID
SEC.2
プロセス名
サイバーセキュリティ実装
プロセス目的
目的は、システム、ソフトウェアおよびハードウェアの設計をサイバーセキュリティ要求と一貫性を保ちつつ詳細化し、それらの実装を確実なものにすることである。
プロセス成果
1) システム、ソフトウェアおよびハードウェアのアーキテクチャが詳細化されている。 2) 一貫性および双方向トレーサビリティが、サイバーセキュリティ要求とシステムアーキテクチャ、ソフトウェアアーキテクチャ、ハードウェアアーキテクチャコンポーネントとの間で確立されている。一貫性および双方向トレーサビリティが、サイバーセキュリティ要求とソフトウェア詳細設計、ハードウェア詳細設計との間で確立されている。 3) 適切なサイバーセキュリティコントロールが選定されている。 4) 弱みが分析されている。 5) ソフトウェアおよびハードウェアの詳細設計が詳細化されている。 6) 一貫性および双方向トレーサビリティが、ソフトウェアアーキテクチャとソフトウェア詳細設計との間で確立されている。また、一貫性および双方向トレーサビリティが、ハードウェアアーキテクチャコンポーネントとハードウェア詳細設計との間で確立されている。 7) 合意されたサイバーセキュリティの実装が、影響を受けるすべての関係者へ伝達されている。

基本プラクティス
SEC.2.BP1: アーキテクチャ細部の詳細化 システム、ソフトウェアおよびハードウェアのアーキテクチャを、サイバーセキュリティ要求に基づいて詳細化する。 *備考 1: ここでの詳細化とは、アーキテクチャのエレメントを追加、適応、または変更することを意味する。*
SEC.2.BP2 サイバーセキュリティ要求に対する一貫性の確保および双方向トレーサビリティの確立 サイバーセキュリティ要求とシステムアーキテクチャ、ソフトウェアアーキテクチャ、ハードウェアアーキテクチャコンポーネントとの間の一貫性を確保し、双方向トレーサビリティを確立する。サイバーセキュリティ要求とソフトウェア詳細設計、ハードウェア詳細設計との間の一貫性を確保し、双方向トレーサビリティを確立する。
SEC.2.BP3: サイバーセキュリティコントロールの選定 関連するリスクの緩和方法の説明を含めて、サイバーセキュリティ要求を達成または支援するための適切なサイバーセキュリティコントロールを選定する。 *備考 2: 一般的に、サイバーセキュリティコントロールとは、サイバーセキュリティリスクを検出、対処もしくは緩和するための技術的手段、またはその他の対応策を指す。*
SEC.2.BP4: アーキテクチャにおける弱みの分析 システム、ソフトウェアおよびハードウェアのアーキテクチャにおける弱みを、インタフェースおよび詳細設計を含めて分析し、脆弱性を識別する。設計上の決定を文書化する。
SEC.2.BP5: 詳細設計の詳細化 ソフトウェアおよびハードウェアのアーキテクチャに基づき、詳細設計を詳細化する。 *備考 3: ここでの詳細化とは、詳細設計のエレメントを追加、適応、または変更することを意味する。*
SEC.2.BP6: アーキテクチャおよび詳細設計に対する一貫性の確保および双方向トレーサビリティの確立 ソフトウェアアーキテクチャとソフトウェア詳細設計との間の一貫性を確保し、双方向トレーサビリティを確立する。ハードウェアアーキテクチャコンポーネントとハードウェア詳細設計との間の一貫性を確保し、双方向トレーサビリティを確立する。
SEC.2.BP7: 合意されたサイバーセキュリティの実装結果の伝達 合意されたサイバーセキュリティの実装結果を、影響を受けるすべての関係者へ伝達する。 *備考 4: 伝達内容には、サイバーセキュリティの実装結果およびアーキテクチャ内で識別された脆弱性の両方を含む場合がある。*

SEC.2 サイバーセキュリティ実装	成果 1	成果 2	成果 3	成果 4	成果 5	成果 6	成果 7
アウトプット情報項目							
04-04 ソフトウェアアーキテクチャ	X	X					
04-05 ソフトウェア詳細設計		X			X		
04-06 システムアーキテクチャ	X	X					
04-52 ハードウェアアーキテクチャ	X	X					
04-53 ハードウェア詳細設計		X			X		
13-51 一貫性の証拠		X				X	
13-52 情報伝達の証拠							X
15-50 脆弱性分析の証拠				X			
17-52 サイバーセキュリティコントロール			X				
基本プラクティス							
BP1: アーキテクチャ細部の詳細化	X						
BP2: サイバーセキュリティ要求に対する一貫性の確保および双方向トレーサビリティの確立		X					
BP3: サイバーセキュリティコントロールの選定			X				
BP4: アーキテクチャにおける弱みの分析				X			
BP5: 詳細設計の詳細化					X		
BP6: アーキテクチャおよび詳細設計に対する一貫性の確保および双方向トレーサビリティの確立						X	
BP7: 合意されたサイバーセキュリティの実装結果の伝達							X

4.3.3. SEC.3 リスク対応検証

プロセス ID
SEC.3
プロセス名
リスク対応検証
プロセス目的
目的は、設計の実装およびコンポーネントの統合がサイバーセキュリティ要求、詳細化されたアーキテクチャ設計、および詳細設計に遵守していることを確認することである。

プロセス成果

1) リスク対応検証手段が作成されている。
2) 検証手段が、リリース範囲に従って選定されている。
3) 設計の実装およびコンポーネントの統合が検証されている。検証結果が記録されている。
4) 一貫性および双方向トレーサビリティが、リスク対応検証手段とサイバーセキュリティ要求との間、およびリスク対応検証手段と詳細化されたアーキテクチャ設計、詳細設計、ソフトウェアユニットとの間で確立されている。双方向トレーサビリティが、検証結果とリスク対応検証手段との間で確立されている。
5) リスク対応検証結果が要約され、影響を受けるすべての関係者へ伝達されている。

基本プラクティス

SEC.3.BP1: リスク対応検証手段の仕様化
実装がサイバーセキュリティ要求、詳細化されたアーキテクチャ設計および詳細設計に遵守しているという証拠を提供するために、適切なリスク対応検証手段を仕様化する。

備考 1: リスク対応検証では、システム、ソフトウェアおよびハードウェアの開発ライフサイクルにおける特定のフェーズ（例：要求、設計、実装、テスト）のアウトプットが、そのフェーズに対して指定された要求を満たしているという客観的な証拠を提供する場合がある。

備考 2: リスク対応検証手段には、さらに、仕様化されていない機能の確認、制御フローおよびデータフローの動的検証、ならびにセキュアコーディング標準に焦点を当てた静的解析を含む場合がある。

備考 3: リスク対応検証の手法および技法には、攻撃をシミュレーションしたネットワークテスト（認可されていないコマンド、不正なハッシュキーを使用した信号、大量のメッセージ送信による接続の妨害など）、およびブルートフォース攻撃のシミュレーションを含む場合がある。

備考 4: リスク対応検証の手法および技法には、監査、レビュー、およびその他の技法も含む場合がある。

備考 5: 検証手段に対するテストケースを導出するための手法には、同値クラスの生成および分析、境界値分析、ならびに／または知識もしくは経験に基づくエラー推測を含む場合がある。

SEC.3.BP2: 検証手段の選定
回帰検証の基準を含む選定基準を考慮して、検証手段の選定内容を文書化する。検証手段の選定内容の文書化においては、リリースの範囲に従って十分な網羅性を持たなければならない。

備考 6: 選定基準の例には、要求の優先順位、継続的開発、（ソフトウェア要求の変更などによる）回帰検証の必要性、または納入される製品リリースの使用意図（テストベンチ、テストトラック、公道など）がある。

SEC.3.BP3: リスク対応検証活動の実施
選定したリスク対応検証手段を使用して、設計の実装およびコンポーネントの統合を検証する。合否ステータスを含むリスク対応検証結果、および対応する検証測定データを記録する。

備考 7: 期待された結果から逸脱している検証結果の取り扱いについては、SUP.9 を参照のこと。

SEC.3.BP4: 一貫性の確保および双方向トレーサビリティの確立
リスク対応検証手段とサイバーセキュリティ要求との間の一貫性を確保し、双方向トレーサビリティを確立する。リスク対応検証手段と詳細化されたアーキテクチャ設計、詳細設計、ソフトウェアユニットとの間の一貫性を確保し、双方向トレーサビリティを確立する。検証結果とリスク対応検証手段との間の双方向トレーサビリティを確立する。

備考 8: 双方向トレーサビリティは、一貫性を支援し、影響分析を容易にし、検証網羅性の実証を支援する。トレーサビリティだけ（例：リンクの存在だけ）では、情報に必ずしも一貫性があるとは限らない。

SEC.3.BP5: 結果の要約および伝達

リスク対応検証結果を要約し、影響を受けるすべての関係者へ伝達する。

備考 9: リスク対応検証の実行に関するすべての必要な情報を要約して提供することで、他の関係者がその結果を判断できるようになる。

SEC.3 リスク対応検証	成果 1	成果 2	成果 3	成果 4	成果 5
アウトプット情報項目					
08-60 検証手段	X				
03-50 検証測定データ			X		
08-58 検証手段選定一式		X			
15-52 検証結果			X		
13-51 一貫性の証拠				X	
13-52 情報伝達の証拠					X
基本プラクティス					
BP1: リスク対応検証手段の仕様化	X				
BP2: 検証手段の選定		X			
BP3: リスク対応検証活動の実施			X		
BP4: 一貫性の確保および双方向トレーサビリティの確立				X	
BP5: 結果の要約および伝達					X

4.3.4. SEC.4 リスク対応妥当性確認

プロセス ID
SEC.4
プロセス名
リスク対応妥当性確認
プロセス目的
目的は、統合されたシステムが関連するサイバーセキュリティゴールを達成していることを確認することである。

プロセス成果

1) サイバーセキュリティゴールに基づき、リスク対応妥当性確認手段が仕様化されている。
2) 妥当性確認手段が、回帰妥当性確認の基準を含む定義された基準に従って選定されている。
3) 統合されたシステムの妥当性が、仕様化された妥当性確認手段を使用して確認され、妥当性確認結果が記録されている。
4) 一貫性および双方向トレーサビリティが、妥当性確認手段とサイバーセキュリティゴールとの間で確立されている。また、双方向トレーサビリティが、妥当性確認結果と妥当性確認手段との間で確立されている。
5) リスク対応妥当性確認結果が要約され、影響を受けるすべての関係者へ伝達されている。

基本プラクティス

SEC.4.BP1: リスク対応妥当性確認手段の仕様化
関連するサイバーセキュリティゴールの達成に対する証拠を提供するために、リスク対応妥当性確認手段を仕様化する。

備考 1: 通常、リスク対応妥当性確認手段では、未確認の脆弱性を検出するためのサイバーセキュリティ関連の手法を使用する（例：ペネトレーションテスト）。

備考 2: テストケースを導出するための手法には、同値クラスの生成および分析、境界値分析、否定テスト、ならびに／または知識もしくは経験に基づくエラー推測を含む場合がある。

SEC.4.BP2: 妥当性確認手段の選定
回帰妥当性確認の基準を含む定義された選定基準に従って、妥当性確認手段の選定内容を文書化する。妥当性確認手段の選定内容の文書化においては、サイバーセキュリティゴールに対する十分な網羅性を持たなければならない。

SEC.4.BP3: リスク対応妥当性確認活動の実施
選定したリスク対応妥当性確認手段を使用して、統合されたシステムの妥当性を確認する。妥当性確認結果、および対応する妥当性確認測定データを記録する。

備考 3: 期待された結果から逸脱している妥当性確認結果の取り扱いについては、SUP.9 を参照のこと。

SEC.4.BP4: 一貫性の確保および双方向トレーサビリティの確立
リスク対応妥当性確認手段とサイバーセキュリティゴールとの間の一貫性を確保し、双方向トレーサビリティを確立する。妥当性確認結果と妥当性確認手段との間の双方向トレーサビリティを確立する。

備考 4: 双方向トレーサビリティは、一貫性を支援し、影響分析を容易にし、妥当性確認の網羅性の実証を支援する。トレーサビリティだけ（例：リンクの存在だけ）では、情報に必ずしも一貫性があるとは限らない。

SEC.4.BP5 結果の要約および伝達
リスク対応妥当性確認結果を要約し、影響を受けるすべての関係者へ伝達する。

備考 5: これには、他の関係者が結果を判断できるように、リスク対応妥当性確認活動からの情報、および新たに検出された脆弱性に関する重要な所見を含む場合がある。

SEC.4 リスク対応妥当性確認	成果 1	成果 2	成果 3	成果 4	成果 5
アウトプット情報項目					
08-59 妥当性確認手段	X				
03-55 妥当性確認測定データ			X		
08-57 妥当性確認手段選定一式		X			
13-24 妥当性確認結果			X		
13-51 一貫性の証拠				X	
13-52 情報伝達の証拠					X
基本プラクティス					
BP1: リスク対応妥当性確認手段の仕様化	X				
BP2: 妥当性確認手段の選定		X			
BP3: リスク対応妥当性確認活動の実施			X		
BP4: 一貫性の確保および双方向トレーサビリティの確立				X	
BP5: 結果の要約および伝達					X

付録 A　プロセスアセスメントモデルおよびプロセス参照モデルの適合性

このプロセスアセスメントモデルおよびプロセス参照モデルは、Automotive SPICE® 4.0 コアモデルの宣言および定義に沿ったものある。そのため、適合証明は Automotive SPICE® 付録 A に記載されている。

プロセス参照モデルおよびプロセスアセスメントモデル（バージョン 4.0）が適用される。[Automotive SPICE® 4.0]

付録 B　情報項目特性

情報項目特性は、表 B.1 の形式で定義される。情報項目およびその特性の解釈方法は、それらを定義および説明している Automotive SPICE® 4.0 第 3.3.2 章を参照のこと。

表 B.1 — 情報項目特性（IIC）の構成

情報項目 ID	情報項目を参照するために使用される情報項目の識別番号
情報項目名	情報項目特性と関連のある一般的な名称の例を提供している。この名称は、プラクティスまたはプロセスによって生成される情報項目の識別子として提供されている。各組織は、これらの情報項目を別の名称で呼んでもよい。組織における情報項目の名称は重要ではない。同様に、組織は一種類の情報項目の中に定義された特性を有する複数の同等の情報項目を保有してもよい。情報項目のフォーマットは様々でよい。組織によって生成された実際の情報項目をここで与えられた例にマッピングすることは、アセッサーおよび組織部門のコーディネーターの責任である。
情報項目特性	情報項目の種類に関連のある潜在的な特性の例を提供している。アセッサーは、組織部門によって提供されたサンプルを評価する際にこれらを使用してよい。これらの一覧化された特性は、チェックリストとして使用されることを意図していない。一部の特性は、アセスメント対象組織において適切であるとみなされる場合には、他の作業成果物に含めてよい。

表 B.2 —情報項目特性

この表には、サイバーセキュリティのための Automotive SPICE® に関連する情報項目の特性のみが含まれる。

ID	名称	特性
02-01	コミットメント／合意	• コミットメント／合意に関与するすべての関係者によって締結されている。 • コミットメントの対象を確立している。 • コミットメントを履行するために必要となる以下のようなリソースを確立している。 - 時間 - 要員 - 予算 - 機器 - 設備
02-50	インタフェース協定	• インタフェース協定には以下に関する定義を含むべきである。 - 顧客およびサプライヤーの利害関係者、ならびに連絡先 - テーラリング合意 - 開発時および開発後に必要となる行為を含む、分散活動における顧客／サプライヤーの責任（例: 役割、RASIC チャート）

ID	名称	特性
		課題（例: 脆弱性、指摘事項、リスク）が発生した際の情報／作業成果物の共有 合意された顧客／サプライヤーのマイルストーン サプライヤーの支援および保守の期間
03-50	検証測定データ	• 検証測定データは、検証手段の実行時に記録されるデータである。 例： - テストケース：生データ、ログ、トレース、ツールによって生成されたアウトプット - 測定：値 - 計算：値 - シミュレーション：プロトコル - 光学検査および所見記録などのレビュー - 分析：値
03-55	妥当性確認測定データ	• 妥当性確認測定データは、妥当性確認手段の実行時に記録されるデータである。 例：ログ、トレース、生データ、クラッシュダンプ、レビュープロトコル
04-04	ソフトウェアアーキテクチャ	• 選択したアーキテクチャを正当化する根拠 • ソフトウェアコンポーネントの機能的および非機能的な個々の振る舞い • アプリケーションパラメーターの設定（コンフィギュレーション向けの要求に対する技術的な実装のソリューション） • 以下のようなソフトウェアコンポーネント間の関係性を表すインタフェースの技術的な特性： - プロセスおよびタスクの同期 - プログラミング言語の呼び出し - API - SW ライブラリの仕様 - オブジェクト指向のクラス定義におけるメソッドの定義、または UML/SysML のインタフェースクラス - コールバック関数、「フック」 • 以下のようなソフトウェアコンポーネントおよびソフトウェアの状態のダイナミクス： - 論理的なソフトウェアの運用モード（例：スタートアップ、シャットダウン、通常モード、キャリブレーション、診断など） - 相互通信（プロセス、タスク、スレッド）および優先順位 - タイムスライスおよびサイクルタイム - 優先順位に基づく割り込み - ソフトウェアコンポーネント間の相互作用 • 例えば自然言語を用いた、単一エレメントまたは図／モデル全体に対する説明の注釈
04-05	ソフトウェア詳細設計	• ソフトウェア詳細設計のエレメント： - 制御フローの定義 - インプット／アウトプットデータのフォーマット - アルゴリズム - 定義されたデータ構造 - 正当化されたグローバル変数 - 例えば自然言語を用いた、単一エレメントまたは図／モデル全体に対する説明の注釈 • ソフトウェアユニットの複雑度または重要度に応じた表現言語の例：

ID	名称	特性
		- 自然言語または非形式言語 - 準形式言語（例：UML、SysML） - 形式言語（例：モデルベースアプローチ）
04-06	システム アーキテクチャ	• 選択したアーキテクチャを正当化する根拠 • システムエレメントの個々の振る舞い • システムエレメント間の相互関係 - （アプリケーションパラメーターなどの）システムパラメーターの設定 - 例えば、STPA に従った手動／人為的な制御の行為 • インタフェースの定義： - 2 つのシステムエレメント間の関係性を表すインタフェースの技術的な特性 • システムエレメント間のインタフェース 例： - バスインタフェース（CAN、MOST、LIN、FlexRay など） - 熱の影響 - ハードウェアとソフトウェア間のインタフェース（HSI）、下記参照 - 電磁インタフェース - 光学インタフェース - ハードウェアと機械間のインタフェース（例：機械的および電気的な要求の両方を満足するケーブル、PCB との筐体インタフェース） - コネクタ、圧入などのハードウェアと機械間の相互接続技術 - 沿面距離および空間距離 • 接着接合、スクリューボルト／フィッティング、リベットボルト、溶接などの固定方法 • EE ハードウェアに関連するシステムインタフェース 例： - アナログまたはデジタルインタフェース（PWM、I/O）およびそのピン構成 - SPI バス、I2C バス、電気的相互接続 - 例えば、ハードウェアエレメント間の熱インタフェース（放熱）の配置 - ハンダ付け - 沿面距離および空間距離 • 機械エンジニアリングのためのインタフェース 例： - 摩擦 - 熱の影響 - 公差 - クラッチ - 接着接合、スクリューボルト／フィッティング、リベットボルト、溶接などの固定方法 - （例えば振動または摩擦の結果としての）力 - 配置 - 形状 • ハードウェアとソフトウェア間のインタフェース 例： - µC/MOSFET のコネクタピン構成およびフローティング IO - アプリケーションソフトウェアによって反映される信号のスケーリングおよび分解能

ID	名称	特性
		• 機械とハードウェア間のインタフェース 例： - 機械寸法 - コネクタの位置 - 例えば、バスバーに対するホールセンサーの位置 - 公差 • システムエレメントおよびシステムの状態のダイナミクス： - システムの状態および運用モードの記述（スタートアップ、シャットダウン、スリープモード、診断／キャリブレーションモード、生産モード、デグラデーション、「リンプホーム」などの緊急時など） - 運用モードに関するシステムコンポーネント間の依存性の記述 - ECU によって反映される機械部品の慣性、ハードウェアおよびソフトウェアを介した信号伝搬および処理時間、ならびにバスシステムなどのシステムエレメント間の相互作用 • 例えば自然言語を用いた、単一エレメントまたは図／モデル全体に対する説明の注釈
04-52	ハードウェアアーキテクチャ	• 初期のフロアプランおよびハードウェア構造全体について記述している。 • 必要なハードウェアコンポーネントを識別している。 • 選択したハードウェアアーキテクチャの選択根拠を含む。 • 自社開発および供給されたハードウェアコンポーネントを識別している。 • 必要なハードウェアコンポーネントの内部および外部インタフェースを識別している。 • ハードウェアコンポーネントのインタフェースを仕様化している。 • 動的な振る舞いを仕様化している。 • ハードウェアコンポーネント間の関係性および依存性を識別している。 • 作成されるすべてのハードウェアバリアントを記述している。 • 電源供給、熱および接地に関するコンセプトを記述している。
04-53	ハードウェア詳細設計	• ハードウェア部品間の相互接続について記述している。 • ハードウェア部品のインタフェースについて仕様化している。 • 動的な振る舞いについて（例：ハードウェア部品の電気的な状態間の遷移、パワーアップおよびパワーダウンのシーケンス、周波数、変調、信号遅延、デバウンス時間、フィルター、短絡の振る舞い、自己保護）仕様化している。 • 例えば、分析報告書、データシート、アプリケーションノートに基づく結論および決定を記述している。 • レイアウトの制約を記述している。
08-55	リスク対応	• 以下の内容を識別している。 - 低減、回避、保有または移転（共有）されるべきリスク - リスクを低減、回避、保有または移転（共有）するための活動 - 対策の立案者 - 実装の成功基準 - 活動を中止するための基準 - 監視頻度 • リスク対応の選択肢： - 選択した対応オプション：回避／低減／保有／移転（共有） - 選択肢の記述 - 推奨される選択肢 • 正当化の根拠

ID	名称	特性
08-57	妥当性確認手段 選定一式	• 変更（回帰）の場合における再度の妥当性確認の基準を含む。 • 妥当性確認手段の識別、回帰に対するものも含む。
08-58	検証手段 選定一式	• 変更（回帰）の場合における再度の検証の基準を含む。 • 検証手段の識別、回帰テストに対するものも含む。
08-59	妥当性確認手段	• 妥当性確認手段には、テストケース、測定、シミュレーション、エミュレーション、またはエンドユーザー調査があり得る。 • 妥当性確認手段の仕様には以下を含む。 - 妥当性確認手段の合否基準（完了基準および終了基準） - 妥当性確認手段に関する開始および終了基準、ならびに中断および再開基準の定義 • 技法 • 妥当性確認に必要な環境およびインフラ • 必要なシーケンスまたは順序
08-60	検証手段	• 検証手段には、テストケース、測定、計算、シミュレーション、レビュー、光学検査、または分析があり得る。 • 検証手段の仕様には以下を含む。 - 検証手段の合否基準（テストの完了基準および終了基準） - 検証手段に関する開始および終了基準、ならびに中断および再開基準の定義 • 技法（例：ブラックボックステストおよび／またはホワイトボックステスト、同値クラスおよび境界値、機能安全のためのフォールト注入、サイバーセキュリティのためのペネトレーションテスト、モデルベース開発のためのバックトゥバックテスト、ICT） • 検証に必要な環境およびインフラ • 必要なシーケンスまたは順序
12-01	見積依頼 （RFQ）	• 要求仕様書への参照 • サプライヤーのサイバーセキュリティ責任 • サイバーセキュリティゴール、または関連するサイバーセキュリティ要求一式およびその属性を含む、サイバーセキュリティに関する作業範囲 • 識別された逸脱およびリスクに対する行動計画 • 以下の様な要望特性を識別している。 - システムアーキテクチャ、コンフィギュレーション要求、またはサービス（コンサルタント、保守など）に対する要求 - 品質基準または品質要求 - プロジェクトのスケジュール要求 - 期待される納入日／サービス日 - コスト／価格への期待事項 - 規制に関する標準規格／要求 • 提出に関する制約を識別している。 - 回答の再提出日 • 回答形式に関する要求
13-24	妥当性確認結果	• 妥当性確認データ、ログ、フィードバック、または文書 • 合格した妥当性確認手段 • 合格しなかった妥当性確認手段 • 実施されなかった妥当性確認手段、および根拠 • 妥当性確認の実施に関する情報（実施日、参加者など） • 妥当性確認結果の抜粋または要約

ID	名称	特性
13-51	一貫性の証拠	• ライフサイクルの全フェーズを通じて、生成物間または生成物内の情報間の双方向トレーサビリティを以下によって実証している。 - ツールのリンク - ハイパーリンク - 編集上の参照先 - 命名規則 • 参照先の情報または対応付けられた情報の内容が、トレーサビリティチェーンに沿って意味的に一貫しているという証拠は、以下によって示されている。 - ペアワークまたはグループワークの実施 - 同僚による確認（例：抜き取り検査） - 文書の改訂履歴の維持 - データベースまたはリポジトリへの登録時に（例えばメタ情報による）変更コメントの提供 • *備考: この証拠は、例えば完成の定義（DoD: Definition of Done）のアプローチによって付随できる。*
13-52	情報伝達の証拠	• 以下のような要員間の情報伝達におけるすべての形式 - E メール、自動生成 E メール - ツールによって支援されるワークフロー - 会議、口頭、または会議議事録経由（例：デイリースタンドアップ） - ポッドキャスト - ブログ - 動画 - フォーラム - ライブチャット - ウィキ - 写真プロトコル
14-02	是正処置	• 初期の問題を識別している。 • 定義された処置を完了させる担当者を識別している。 • 解決策（問題を是正するための一連の処置）を定義している。 • 開始日および終結目標期日を識別している。 • ステータス指標を含む。 • フォローアップの監査活動を示している。
15-09	リスクのステータス	• 識別したリスクのステータス、またはその変更を識別している。 - リスクの説明文 - リスク源 - リスクのインパクトおよび尤度 - 例えば、優先順位付けまたはステータス設定に対する分類およびリスク閾値 - 進行中のリスク対応活動
15-21	サプライヤー評価	• 評価の目的を記述している。 • サプライヤーの選定基準を識別している。 • 評価に使用された手法および手段（チェックリスト、ツール） • 評価で使用された要求 • 想定および制約 • コンテキストおよび必要な情報の範囲を識別している（例: 評価日、関係者）。 • 評価要求の達成度

ID	名称	特性
15-50	脆弱性分析の証拠	• 以下の内容を識別している。 - ID - 記述 - 懸念される攻撃経路 • 攻撃実現可能性（例： CVSS〔共通脆弱性評価システム〕 の評価）
15-51	分析結果	• 分析対象の識別 • 使用された分析基準 例： - 使用された選定基準または優先順位体系 - 決定基準 - 品質基準 • 分析結果 例： - 決定事項／選定事項 - 選定の理由 - 想定 - 潜在的なマイナスの影響 • 分析の観点には以下を含む場合がある。 - 正確性 - 理解可能性 - 検証可能性 - 実現可能性 - 妥当性
15-52	検証結果	• 検証データおよびログ • 合格した検証手段 • 合格しなかった検証手段 • 実施されなかった検証手段 • テスト実施に関する情報（実施日、テスト担当者名など） • 検証結果の抜粋または要約
17-00	要求	• 機能および能力（例：非機能要求）、またはそのインタフェースの 1 つに対する期待事項 - ブラックボックスの視点 - 検証可能であり、設計または実装の決定を示唆せず、曖昧さがなく、他の要求との矛盾が生じないもの • 設計または実装の決定を示唆または表現している要求文は、「設計制約」と呼ばれる。 • システムレベルにおける要求の側面の例には、以下のような熱特性がある。 - 放熱 - 寸法 - 重量 - 素材 • システムインタフェースに関する要求の側面には以下の例がある。 - コネクタ - ケーブル - 筐体 • ハードウェアレベルにおける要求の例は以下の通りである。 - 耐用年数およびミッションプロファイル、耐用年数における堅牢性 - 最大価格

ID	名称	特性
		- 保管および輸送の要求 - アナログまたはデジタルの回路およびロジックの機能的な振る舞い - クランク、スタートストップ、ドロップアウト、ロードダンプに対する静止電流、電圧インパルス応答 - 温度、ハードウェアの最大放熱量 - スリープモード、スタートアップ、リセット条件などの運用状態に応じた消費電力 - 周波数、変調、信号遅延、フィルター、制御ループ - パワーアップおよびパワーダウンのシーケンス、信号取得の正確度および精度、または信号処理時間 - メモリ容量および CPU クロックの許容範囲などの計算リソース - 例えば、ピンまたはハンダの接合部における最大のアブレシブ磨耗およびせん断力 - 教訓から得られた要求 - 技術的安全コンセプトから導き出された安全関連の要求
17-51	サイバーセキュリティゴール	• サイバーセキュリティによって保護することが必要な資産の属性を記述している。 • これには以下を含む場合がある。 - 機密性のニーズ - 認可のニーズ - 完全性のニーズ - 可用性のニーズ - その他 • ゴールに含めることができる情報： - ゴールのタイトル - 目的 - 適用範囲 - 主要なメトリクスおよび成功基準 - マイルストーン（該当する場合） - 行動計画（該当する場合） - 利害関係者 - 潜在的なリスクへのリンク - 予算およびリソース - タイムライン - 適合性および規格 - 署名および承認
17-52	サイバーセキュリティコントロール	• サイバーセキュリティリスクを防止、検出、または緩和するための技術的な対応策 • 1 つ以上のサイバーセキュリティ要求に関連している。
17-53	サイバーセキュリティ脅威シナリオ	• 脅威がどのように弱み／脆弱性、または複数の弱み／脆弱性を悪用し、資産を危害にさらすかを説明したものであり、対応するリスク分析を可能にする。 • 実際の脅威もしくは脅威群、または仮定の脅威もしくは脅威群について、時系列的かつ機能的に詳細を説明したもの • 脅威シナリオをもたらすシステムとの相互作用を伴う一連の行動 • 脅威シナリオには以下を含めなければならない。 例： - 脅威の対象となる資産 - 侵害されるサイバーセキュリティ属性

ID	名称	特性
		- サイバーセキュリティ属性の侵害原因 • 脅威シナリオは、以下のような該当する脅威の詳細かつ具体的な説明を提供する。 - ランサムウェア - フィッシング - なりすまし - サービス拒否
17-54	要求の属性	• 要求の構造化およびリリース範囲の定義を支援するメタ属性 • ツールを利用して実現できる。 • 備考：要求属性を使用することによって、要求分析をさらに支援できる場合がある。
18-50	サプライヤー評価基準	• サプライヤーが満足すべき適合性に対する期待事項 • 期待事項から国内／国際／ドメイン特有の標準規格／法律／規制までのリンク • サプライヤー候補が提供した要求に対する適合性の証拠、または取得組織が評価した要求に対する適合性の証拠 • 合意された要求への例外事項

付録 C　用語

Automotive SPICE® は、以下の優先順位に基づいて用語を使用する。

a) ISO/IEC 33001 のアセスメント関連の用語
b) ISO/IEC/IEEE 24765 および ISO/IEC/IEEE 29119 の用語（付録 C に記載）
c) Automotive SPICE® に登場している用語（付録 C に記載）
d) ISO/SAE 21434 のサイバーセキュリティ関連の用語

付録 C は、ISO/IEC/IEEE 24765 および ISO/IEC/IEEE 29119 から適用可能な用語の参照を列挙している。また、Automotive SPICE® で具体的に定義した用語も提供している。一部の定義は ISO/IEC/IEEE 24765 に基づく。

表 C.1 — 用語

用語	出所	記述
受け入れテスト [Acceptance testing]	ISO/IEC/IEEE 24765	ユーザー、顧客、または権限を与えられた実体がシステムまたはコンポーネントを受理するか否かの判断を可能にするために実施される公式のテスト
アプリケーションパラメーター [Application parameter]	Automotive SPICE® 4.0	アプリケーションパラメーターは、システムまたはソフトウェアのレベルで変更可能なデータを含むソフトウェア変数であり、システムまたはソフトウェアの振る舞いおよびプロパティに影響を与える。アプリケーションパラメーターの概念は 2 通りで表現される。 • 仕様（変数名、ドメイン値の範囲、テクニカルデータタイプ、デフォルト値、物理単位 [該当する場合]、対応するメモリマップをそれぞれ含む） • データアプリケーションを用いて受信する実際の定量的なデータ値 アプリケーションパラメーターは要求ではない。これらは、コンフィギュレーション向けの要求に対する技術的な実装のソリューションである。
アーキテクチャエレメント [Architecture element]	Automotive SPICE® 4.0	システムおよびソフトウェアレベルにおけるアーキテクチャの分割結果： • システムは、適切な階層レベルでシステムアーキテクチャのエレメントに分割される。 • ソフトウェアは、ソフトウェアコンポーネント（ソフトウェアアーキテクチャの最下位レベルのエレメント）になるまで、適切な階層レベルでソフトウェアアーキテクチャのエレメントに分割される。
資産 [Asset]	ISO/SAE 21434	価値のある、または価値に貢献する対象
攻撃経路 [Attack path]	ISO/SAE 21434	脅威シナリオを実現するための一連の意図的な行為
攻撃実現可能性 [Attack feasibility]	ISO/SAE 21434	対応する一連の行為を成功裏に実行する容易さを説明する攻撃経路の属性
ブラックボックステスト [Black-box testing]	Automotive SPICE® 4.0	テスト対象アイテムの内部構造および仕組みの知識がない状態でテストを開発するための要求テストの手法

コードレビュー [Code review]	Automotive SPICE® 4.0	コードの使用目的に対する適合性の判断、ならびに仕様および標準規格との矛盾の識別を行うために、1 人以上の適格者によるコードのチェックのこと
コーディング [Coding]	ISO/IEC/IEEE 24765	設計仕様（設計記述）からプログラミング言語へ、ロジックおよびデータを変換すること
一貫性 [Consistency]	Automotive SPICE® 4.0	一貫性とは、内容および意味に焦点を当て、作業成果物が互いに矛盾していないことを確実なものにする。一貫性は、双方向トレーサビリティによって支援される。
サイバーセキュリティイベント [Cybersecurity event]	ISO/SAE 21434	アイテムまたはコンポーネントに関連するサイバーセキュリティ情報
サイバーセキュリティゴール [Cybersecurity goal]	ISO/SAE 21434	1 つ以上の脅威シナリオに対するコンセプトレベルのサイバーセキュリティ要求
サイバーセキュリティ情報 [Cybersecurity information]	ISO/SAE 21434	関連性がまだ決定されていないサイバーセキュリティに関する情報
サイバーセキュリティ属性 [Cybersecurity property]	ISO/SAE 21434	守るべき属性
損害シナリオ [Damage scenario]	Automotive SPICE® 4.0	車両または車両の機能に関係し、利害関係者に影響を与える有害事象
エレメント [Element]	Automotive SPICE® 4.0	エレメントとは、「V」字の左側のアーキテクチャおよび設計のレベルにおけるすべての構造オブジェクトのことである。これらのエレメントは、適切な階層レベルでアーキテクチャまたは設計のより詳細なサブエレメントへ、さらに分割することができる。
エラー [Error]	ISO/IEC/IEEE 24765	演算、観察または計測で得られた値／状態が、真値、規定値または理論的正確値／状態と相違していること
障害 [Fault]	ISO/IEC/IEEE 24765	ソフトウェア内のエラーの顕現
機能要求 [Functional requirement]	ISO/IEC/IEEE 24765	製品またはプロセスが要求される振る舞い、および／または結果を生成するために成し遂げなければならないものを識別した記述文
ハードウェア [Hardware]	ISO/IEC/IEEE 24765	コンピュータプログラムもしくはデータの加工、保存、または送信に使用される物理的な機器
統合 [Integration]	Automotive SPICE® 4.0	システム全体になるまで、アイテムをより大きなアイテムに結合するプロセス
アイテム [Item]	ISO 21434	車両レベルで機能を実装するコンポーネントまたはコンポーネント一組
品質保証 [Quality assurance]	ISO/IEC/IEEE 24765	アイテムまたは製品が確立された技術要求に適合しているという十分な信頼性を与えるために必要な計画的かつ体系的なすべての行動のパターン

回帰テスト [Regression testing]	Automotive SPICE® 4.0	変更が意図しない影響を引き起こさないこと、およびシステムまたはアイテムが依然としてその規定された要求に適合していることを検証するために、システムまたはアイテムを選択的に再テストすること
要求 [Requirement]	Automotive SPICE® 4.0	システム、システムアイテム、製品、またはサービスが契約書、標準規格、仕様書、または正式に課された文書を満足させるために、達成または保有しなければならない属性、または能力
要求仕様書 [Requirements specification]	Automotive SPICE® 4.0	システムまたはアイテムに対する要求を規定した文書。一般的には、機能要求、性能要求、インタフェース要求、設計要求、および開発標準が含まれる。
ソフトウェア [Software]	ISO/IEC/IEEE 24765	コンピュータプログラム、手順、ならびに（場合によっては）コンピュータシステムの運用に付随する関連の文書およびデータ
ソフトウェア コンポーネント [Software component]	Automotive SPICE® 4.0	設計および実装を重視したプロセスにおけるソフトウェアコンポーネント： ソフトウェアアーキテクチャでは、コンセプトモデルにおける最下位のソフトウェアコンポーネントになるまで、ソフトウェアを適切な階層レベルでソフトウェアコンポーネントに分割する。 検証を重視したプロセスにおけるソフトウェアコンポーネント： 検証対象の SW コンポーネントの実装は、例えばソースコード、オブジェクトファイル、ライブラリファイル、実行可能ファイル、または実行可能モデルとして表現される。
ソフトウェア エレメント [Software element]	Automotive SPICE® 4.0	ソフトウェアコンポーネントまたはソフトウェアユニットを参照のこと。
ソフトウェア ユニット [Software Unit]	Automotive SPICE® 4.0	設計および実装を重視したプロセスにおけるソフトウェアユニット： ソフトウェアコンポーネントの分割の結果、ソフトウェアはソフトウェアエレメントを表現したソフトウェアユニットに分割される。ソフトウェアユニットは、これ以上細分化しないことが決定されたものであり、コンセプトモデルにおいて、ソフトウェアコンポーネントの最下位レベルの部分である。 検証を重視したプロセスにおけるソフトウェアユニット： 検証対象の実装済 SW ユニットは、例えばソースコードファイルまたはオブジェクトファイルとして表現される。
静的解析 [Static analysis]	Automotive SPICE® 4.0	アイテムの形式、構造、内容または文書に基づいて、アイテムを評価するプロセス
システム [System]	Automotive SPICE® 4.0	特定の環境内において、特定の機能または機能の集合を実現するために編成された相互作用のあるアイテムの集合
テスト [Test]	Automotive SPICE® 4.0	特定の条件下でアイテム（システム、ハードウェアまたはソフトウェア）を実行させる活動。その結果は記録され、要約され、伝達される。
脅威シナリオ [Threat scenario]	ISO/SAE 21434	損害シナリオを実現するための 1 つ以上の資産のサイバーセキュリティ属性の侵害の潜在的原因

トレーサビリティ [Traceability]	ISO/IEC/IEEE 24765	開発プロセスの 2 つ以上の成果物間、特に、互いの前後関係または主従関係を持つ成果物間で確立される関係の程度
ユニット [Unit]	Automotive SPICE® 4.0	これ以上分割できないソフトウェアコンポーネントの一部分 → [ソフトウェアコンポーネント]
ユニットテスト [Unit test]	Automotive SPICE® 4.0	個々のソフトウェアユニット、または一連の結合されたソフトウェアユニットのテスト
妥当性確認 [Validation]	ISO/IEC/IEEE 29119	妥当性確認とは、ユーザーが特定のタスクのために作業品目を使用できることを実証することである。
検証 [Verification]	ISO/IEC/IEEE 29119	検証とは、客観的な証拠を提供することを通じて、規定された要求が所定の作業品目の中で達成されていることを確認することである。
脆弱性 [Vulnerability]	ISO/SAE 21434	攻撃経路の一部として悪用できる弱み
弱み [Weakness]	ISO/SAE 21434	望ましくない振る舞いにつながる欠陥または特性
ホワイトボックステスト [White-box testing]	Automotive SPICE® 4.0	テスト対象アイテムの内部構造および仕組みの知識に基づいてテストを開発するためのテスト手法

表 C.2 — 略語

AS	**A**utomotive **SPICE** オートモーティブスパイス
ACSMS	**A**utomotive **C**yber**s**ecurity **M**anagement **S**ystem 自動車用サイバーセキュリティマネジメントシステム
ATA	**A**ttack **T**ree **A**nalysis アタックツリー分析
BP	**B**ase **P**ractice 基本プラクティス
CAN	**C**ontroller **A**rea **N**etwork コントローラエリアネットワーク
CASE	**C**omputer-**A**ided **S**oftware **E**ngineering コンピュータ支援ソフトウェア工学
CCB	**C**hange **C**ontrol **B**oard 変更制御委員会
CFP	**C**all **F**or **P**roposals 提案依頼
CPU	**C**entral **P**rocessing **U**nit 中央処理装置
ECU	**E**lectronic **C**ontrol **U**nit 電子制御ユニット
EEPROM	**E**lectrically **E**rasable **P**rogrammable **R**ead **O**nly **M**emory 電気的消去可能プログラマブルリードオンリーメモリ

FMEA	**F**ailure **M**ode and **E**ffect **A**nalysis 故障モード影響解析
FTA	**F**ault **T**ree **A**nalysis 故障の木解析
GP	**G**eneric **P**ractice 共通プラクティス
GR	**G**eneric **R**esource 共通リソース
HARA	**H**azard **A**nalysis and **R**isk **A**ssessment ハザード分析およびリスク評価
IEC	**I**nternational **E**lectrotechnical **C**ommission 国際電気標準会議
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers アイトリプルイー
I/O	**I**nput / **O**utput インプット／アウトプット
ISO	**I**nternational **O**rganization for **S**tandardization 国際標準化機構
MISRA	**M**otor **I**ndustry **S**oftware **R**eliability **A**ssociation ミスラ
OII	**O**utput **I**nformation **I**tem アウトプット情報項目
PA	**P**rocess **A**ttribute プロセス属性
PAM	**P**rocess **A**ssessment **M**odel プロセスアセスメントモデル
PRM	**P**rocess **R**eference **M**odel プロセス参照モデル
RAM	**R**andom **A**ccess **M**emory ランダムアクセスメモリ
RC	**Rec**ommendation 推奨事項
RL	**Rul**e ルール
ROM	**R**ead **O**nly **M**emory リードオンリーメモリ
SPICE	**S**oftware-based systems **P**rocess **I**mprovement and **C**apability d**E**termination ソフトウェアベースシステムのプロセス改善および能力判定
TARA	**T**hreat **A**nalysis and **R**isk **A**ssessment 脅威分析およびリスク評価
UNECE	**U**nited **N**ations **E**conomic **C**ommission for **E**urope 国際連合欧州経済委員会
VDA	**V**erband **D**er **A**utomobilindustrie (German Association of the Automotive Industry) ドイツ自動車工業会

付録 D　トレーサビリティおよび一貫性

トレーサビリティおよび一貫性は、Automotive SPICE® 4.0 と同様に、サイバーセキュリティのための Automotive SPICE® においても、1 つの基本プラクティスで扱われる。

トレーサビリティは、参照先または作業成果物間のリンクを指すため、網羅性（確認）、影響分析、要求の実装状況の追跡等にも役立てられる。それとは対照的に、一貫性は内容および意味について扱う。

さらに、双方向トレーサビリティは、以下の間で明示的に定義されている。

- 脅威シナリオとサイバーセキュリティゴールの間
- サイバーセキュリティゴールと妥当性確認仕様の間
- サイバーセキュリティ要求／アーキテクチャ／ソフトウェア詳細設計／ハードウェア詳細設計と、リスク対応検証仕様の間
- 妥当性確認仕様と妥当性確認結果の間
- 検証手段と検証結果の間

双方向トレーサビリティおよび一貫性の概要を、次図に示す。

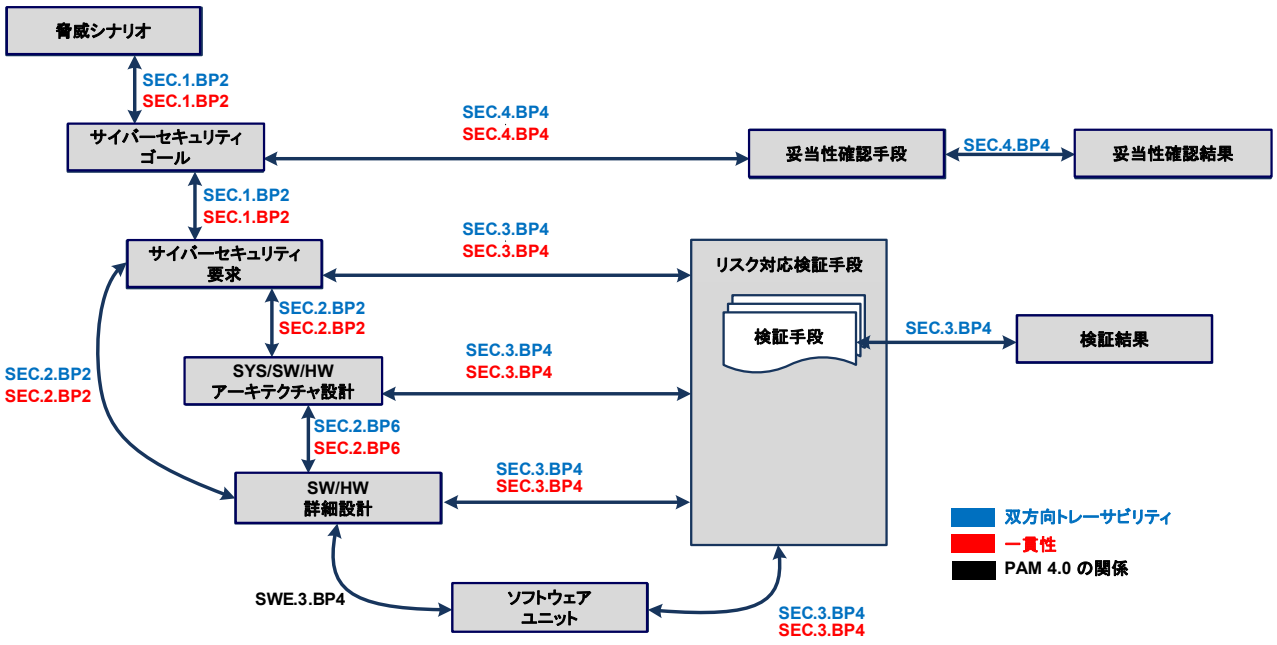

図 5 — 双方向トレーサビリティおよび一貫性

付録 E　サイバーセキュリティのための Automotive SPICE® における一般概念

本付録では、サイバーセキュリティのための Automotive SPICE® と ISO/SAE 21434 の関係について記述する。図 6 は、サイバーセキュリティのための Automotive SPICE® の基本プラクティスおよびそれに付随する IIC または作業成果物、ならびに ISO/SAE 21434 におけるそれぞれの要求事項 [RQ] を示す。

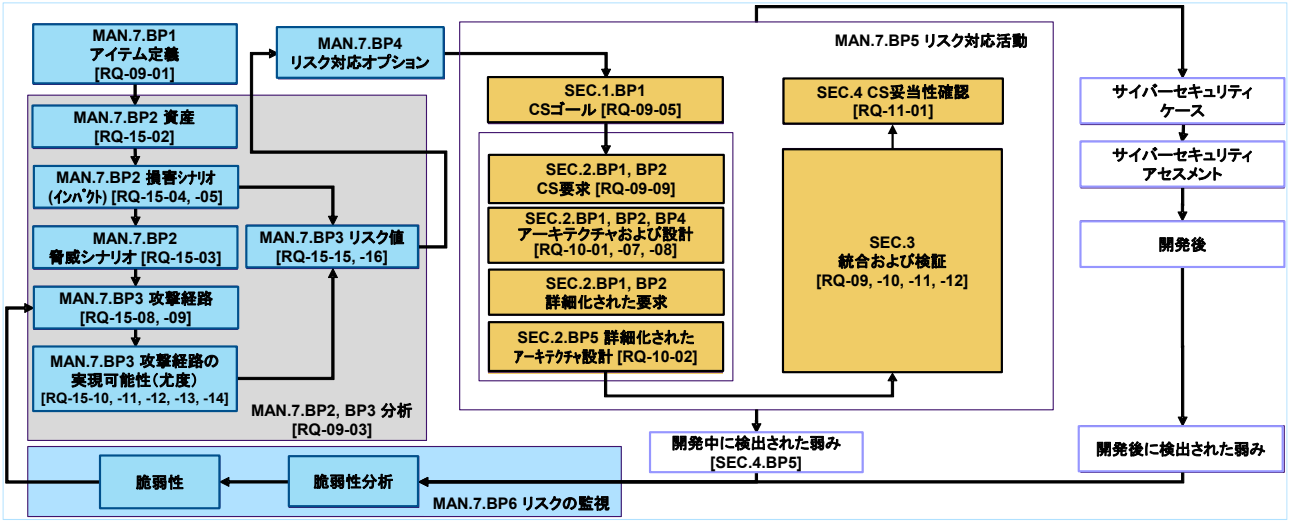

図 6 — サイバーセキュリティのための Automotive SPICE® における一般概念