VDA | QMC
Qualitäts Management Center
im Verband der Automobilindustrie

自動車業界における品質管理

Automotive SPICE®

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兼プロセスアセスメントモデル

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 QMC プロジェクトグループ 13
バージョン:	1.0
日付:	2021 年 7 月 16 日
ステータス:	発行済
機密保持:	一般公開

翻訳について

本書は、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第 1 版の翻訳版である。

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、www.automotivespice.com 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、およびプロジェクトグループ 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

本書は Automotive SPICE プロセスアセスメントモデル 3.1 を補完するものであり、ドイツ自動車工業会の品質マネジメントセンター (QMC) のプロジェクトグループ 13 によって作成された。

本書は以下の文書からの複製がある。

- **ISO/IEC 33020:2015**
  情報技術 – プロセスアセスメント – プロセス能力のアセスメントのためのプロセス測定の枠組み

ISO/IEC 33020:2015 には、著作権放棄について、以下のように記載されている。

「本国際標準規格の利用者は、それが所期の目的のために利用されるように、あらゆるプロセスアセスメントモデル、又はプロセス成熟度モデルの一部として、従属節 5.2、5.3、5.4 及び 5.6 を複製してよい。」

上記の標準規格からの複製は、著作権放棄通知の下で組み入れられている。

サイバーセキュリティのための Automotive SPICE® のプロセスアセスメントモデルは www.automotivespice.com のウェブサイトから無料でダウンロードして入手できる。

商標

Automotive SPICE® はドイツ自動車工業会 (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。

目次

図の一覧

表の一覧

序文

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込むために、追加プロセスがサイバーセキュリティエンジニアリングのプロセス参照モデル及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。

本書のパート I* 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 PAM 3.1 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 スコープに対して同等のアセスメント範囲での ASPICE 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 及び VDA スコープのプロセスに対する ASPICE 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。

本書のパート II* は既存の Automotive SPICE ガイドライン (初版) を補完するものであり、パート I* で定義されたプロセスに対する解釈及び評定ガイドラインを含んでいる。Automotive SPICE ガイドライン (初版) のセクション 1 及び 2 はパート II* にも適用されるので、ここでは説明を省略する。

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作業成果物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。

備考：無料でダウンロードできる本書には、VDA-QMC より有料で出版されている「サイバーセキュリティのための Automotive SPICE®」のうち、パート II*および付録 D が含まれていない。

訳注*：本書のパート I、II とは有料版の章構成を指しており、パート I が無料版の「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及びプロセスアセスメントモデル」に相当し、パート II には無料版に含まれていない「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実施の評定ガイドライン (レベル 1) 」が記載されている。

適合証明

Automotive SPICE のプロセスアセスメントモデル及びプロセス参照モデルは ISO/IEC 33004:2015 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土台として使用できる。

ISO/IEC 33020:2015 は ISO/IEC 33003 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及びプロセス参照モデルが ISO/IEC 33004:2015 の要件に適合していることを示す証明は付録 A に記載する。

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、管理プロセス、及び支援プロセスにおける系統的な弱みを特定することである。

Automotive SPICE PAM3.1 及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及びソフト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及びハードウェア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。

ISO/SAE 21434 のいくつかの側面は開発プロジェクトのコンテキストでは実行されないため、本書の範囲には含まれていない。本書の範囲に含まれていない側面とは、サイバーセキュリティ管理、継続的なサイバーセキュリティ活動、開発後のフェーズなどが該当し、これらは自動車用サイバーセキュリティマネジメントシステム (ACSMS) によって対処され、サイバーセキュリティマネジメントシステム監査の対象となる。

本書では、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、及び脅威分析とリスク評価に対するプロセス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 2.1.5:プロセスを実施するための責任及び権限を定義する」

- サイバーセキュリティの計画: 「GP 2.1.2：識別した目標を遂行するためにプロセスの実施を計画する」及び「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：プロセス展開」及び「GP 2.1.2：識別した目標を遂行するために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.BP6：ソフトウェアアーキテクチャの選択肢の評価」、「SYS.3.BP5：システムアーキテクチャの選択肢の評価」及び「REU.2：再利用プログラム管理」
- 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・シェルのコンポーネント: 「ACQ.2：サプライヤー依頼及び選定」並びに「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「結果の要約及び伝達」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 ASPICE 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 ASPICE のアセスメントに含まれていない。
- 開発後のリリース: 「SPL.2：製品リリース」、「SUP.8：構成管理プロセス」及び「SUP.1：品質保証プロセス」

付録 C に記載されている用語「アイテム」は、システム又はソフトウェアの識別可能な部分を定義するために Automotive SPICE で使用されている (この定義内容は他の規格で使用されるものと異なる場合がある)。

訳注：ISO/SAE 21434 英和対訳版 (日本規格協会発行) では、「Cybersecurity requirements」を「サイバーセキュリティ要求」と訳しているが、本書では Automotive SPICE v3.1 日本語版との整合性を確保するため、「Cybersecurity requirements」を「サイバーセキュリティ要件」と訳している。また、ISO21434 では、リスク対応オプションの 1 つを「保有 (retain) 」としているが、本書原文では「保有」ではなく「受容 (accept) 」と表記してあるため、本書翻訳版も原文どおりに訳している。

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及びプロセスアセスメントモデル

1 プロセス能力アセスメント

プロセスアセスメントモデルを使用したプロセス能力アセスメントのコンセプトは、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し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択し、指標を補足している。この指標は、客観的な証拠の収集に役立てられ、アセッサーが能力判定に基づいてプロセスの評定を割当てることを可能にする。

関係性を図 1 に示す。

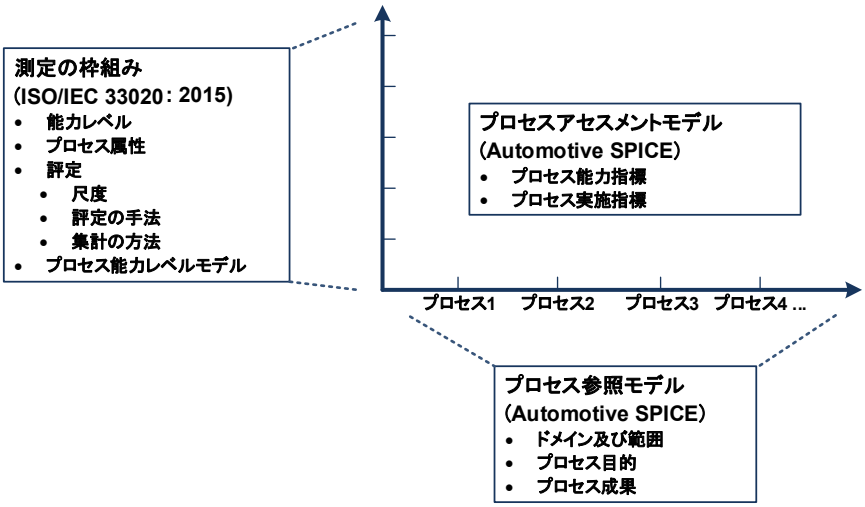

図 1 — プロセスアセスメントモデルの関係性

1.1 プロセス参照モデル

プロセスは、プロセスが扱う活動の種類に基づいてプロセスカテゴリ毎に分類し、さらにプロセス群へ分類する。

プロセスカテゴリは、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、及び支援ライフサイクルプロセスの 3 つで構成される。

各プロセスは、プロセス目的を説明する観点で記載される。プロセス目的の説明文には、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を含む。プロセス目的は、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 プロセス参照モデル及び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は、プロセス座標に対して、図 2 で示す一連のプロセスを提供している。

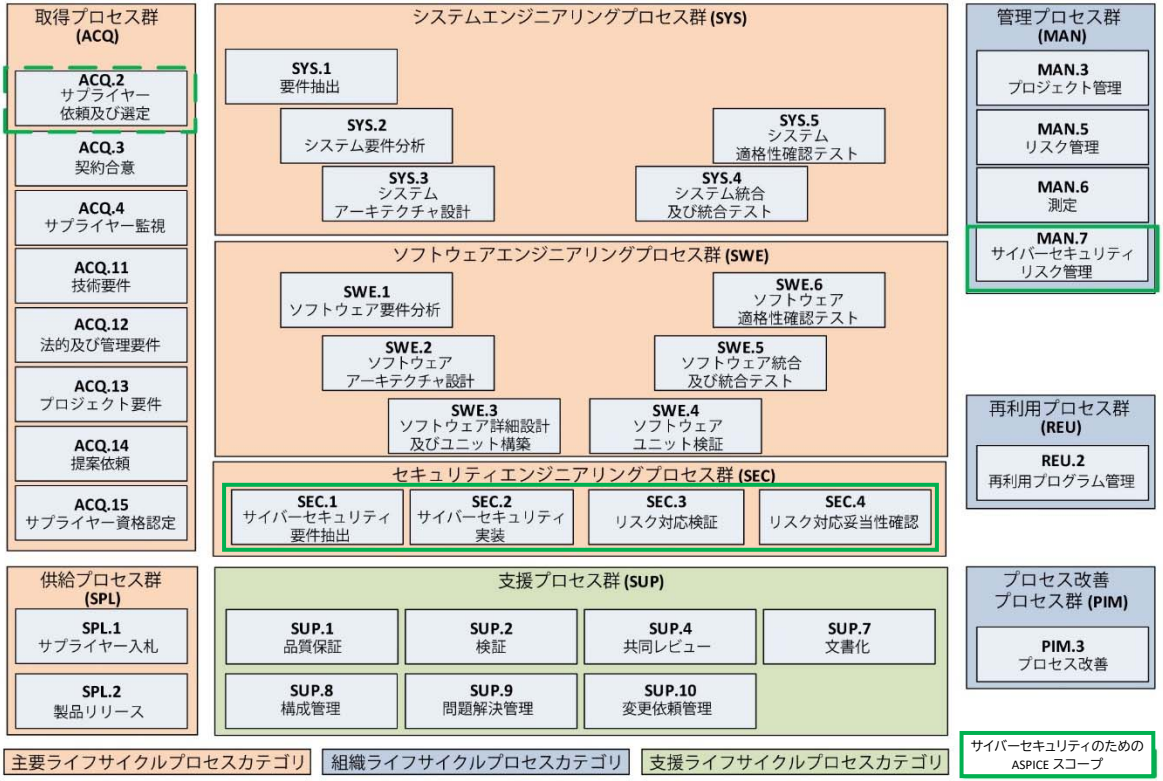

図 2 — Automotive SPICE 及びサイバーセキュリティのための Automotive SPICE のプロセス参照モデル – 概要

1.1.1 主要ライフサイクルプロセスカテゴリ

主要ライフサイクルプロセスカテゴリは、顧客がサプライヤーから製品を取得する際に使用するプロセス、及びサプライヤーが顧客に対応し、製品を納入する際に使用するプロセスで構成され、仕様、設計、開発、統合及びテストで必要となるエンジニアリングプロセスを含む。

主要ライフサイクルプロセスカテゴリは以下のプロセス群で構成される。

- 取得プロセス群
- 供給プロセス群
- セキュリティエンジニアリングプロセス群
- システムエンジニアリングプロセス群
- ソフトウェアエンジニアリングプロセス群

取得プロセス群 (ACQ) は、製品及び/又はサービスを取得するために、顧客が実施するプロセス、又はサプライヤーが別のサプライヤーにとっての顧客となる際にサプライヤーが実施するプロセスで構成される。

ACQ.2	サプライヤー依頼及び選定
ACQ.3	契約合意
ACQ.4	サプライヤー監視
ACQ.11	技術要件
ACQ.12	法的及び管理要件
ACQ.13	プロジェクト要件
ACQ.14	提案依頼
ACQ.15	サプライヤー資格認定

表 1 — 主要ライフサイクルプロセス – ACQ

供給プロセス群 (SPL) は、製品及び/又はサービスを供給するために、サプライヤーが実施するプロセスで構成される。

SPL.1	サプライヤー入札
SPL.2	製品リリース

表 2 — 主要ライフサイクルプロセス – SPL

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件抽出
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 3 — 主要ライフサイクルプロセス – SEC

システムエンジニアリングプロセス群 (SYS) は、顧客要件及び内部要件を抽出して管理するためのプロセス、システムアーキテクチャを定義するプロセス、並びにシステムレベルで統合及びテストを実施するためのプロセスで構成される。

SYS.1	要件抽出
SYS.2	システム要件分析
SYS.3	システムアーキテクチャ設計
SYS.4	システム統合及び統合テスト
SYS.5	システム適格性確認テスト

表 4 — 主要ライフサイクルプロセス – SYS

ソフトウェアエンジニアリングプロセス群 (SWE) は、システム要件およびシステムアーキテクチャから抽出したソフトウェア要件を管理するためのプロセス、該当するソフトウェアのアーキテクチャ及び設計書を作成して実装するためのプロセス、並びにソフトウェアの統合及びテストを実施するためのプロセスで構成される。

SWE.1	ソフトウェア要件分析
SWE.2	ソフトウェアアーキテクチャ設計
SWE.3	ソフトウェア詳細設計及びユニット構築
SWE.4	ソフトウェアユニット検証
SWE.5	ソフトウェア統合及び統合テスト
SWE.6	ソフトウェア適格性確認テスト

表 5 — 主要ライフサイクルプロセス – SWE

1.1.2 支援ライフサイクルプロセスカテゴリ

支援ライフサイクルプロセス (SUP) カテゴリは、ライフサイクルの様々な時点において、他のプロセスによって使用されるプロセスで構成される。

SUP.1	品質保証
SUP.2	検証
SUP.4	共同レビュー
SUP.7	文書化
SUP.8	構成管理
SUP.9	問題解決管理
SUP.10	変更依頼管理

表 6 — 支援ライフサイクルプロセス – SUP

1.1.3 組織ライフサイクルプロセスカテゴリ

組織ライフサイクルプロセスカテゴリは、プロセス、成果物及びリソース資産を構築するためのプロセスで構成される。これらのプロセス、成果物及びリソース資産は組織内のプロジェクトで使用した際、組織の事業目標の達成に役立つ。

組織ライフサイクルプロセスカテゴリは、以下の群で構成される。

- 管理プロセス群
- プロセス改善プロセス群
- 再利用プロセス群

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又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.3	プロジェクト管理
MAN.5	リスク管理
MAN.6	測定
MAN.7	サイバーセキュリティリスク管理

表 7 — 組織ライフサイクルプロセス – MAN

プロセス改善プロセス群 (PIM) は、1 プロセスで構成され、組織部門で実施するプロセスを改善するためのプラクティスがその中に含まれる。

PIM.3	プロセス改善

表 8 — 組織ライフサイクルプロセス – PIM

再利用プロセス群 (REU) は、1 プロセスで構成され、組織の再利用プログラムにおいて再利用の機会を体系的に活用するためのプロセスである。

REU.2	再利用プログラム管理

表 9 — 組織ライフサイクルプロセス – REU

1.2 測定の枠組み

プロセス能力レベル、プロセス属性、評定尺度及び能力レベル評定モデルは、ISO/IEC 33020:2015 の従属節 5.2 で定義されている内容と同一である。能力レベル及びそれに対応するプロセス属性の詳細は、Automotive SPICE PAM 3.1 で説明されている。

1.3 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。ここでの狙いは、PAM を最上位に置き、用語「プロセス」を各抽象レベルで理解させることである。

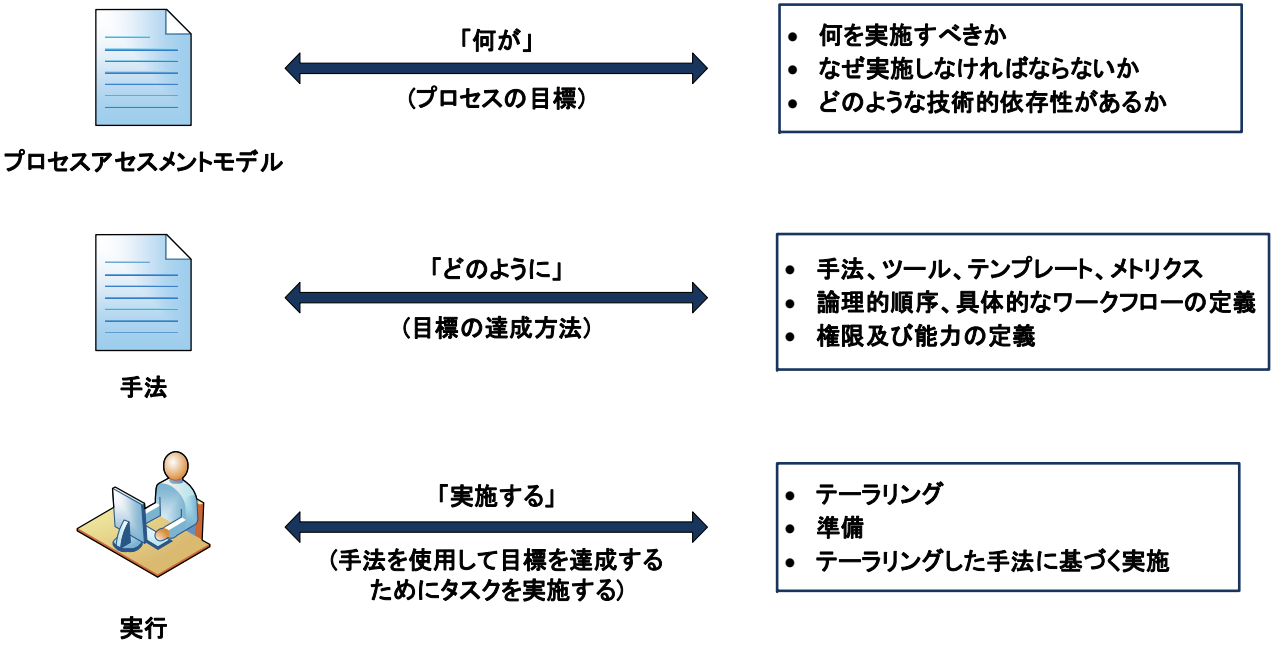

図 3 — 用語「プロセス」の抽象レベル

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。「どのように」は、企業、組織部門、又は製品ライン等の特定の状況に対して、常に固有である。例えば、あるプロジェクト、組織部門、又は A 社の「どのように」は、別のプロジェクト、組織部門、又は 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及びプロセス属性達成成果に対して、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、手順、ツール等の対応に対する決定は、「どのように」のレベルで行われる。

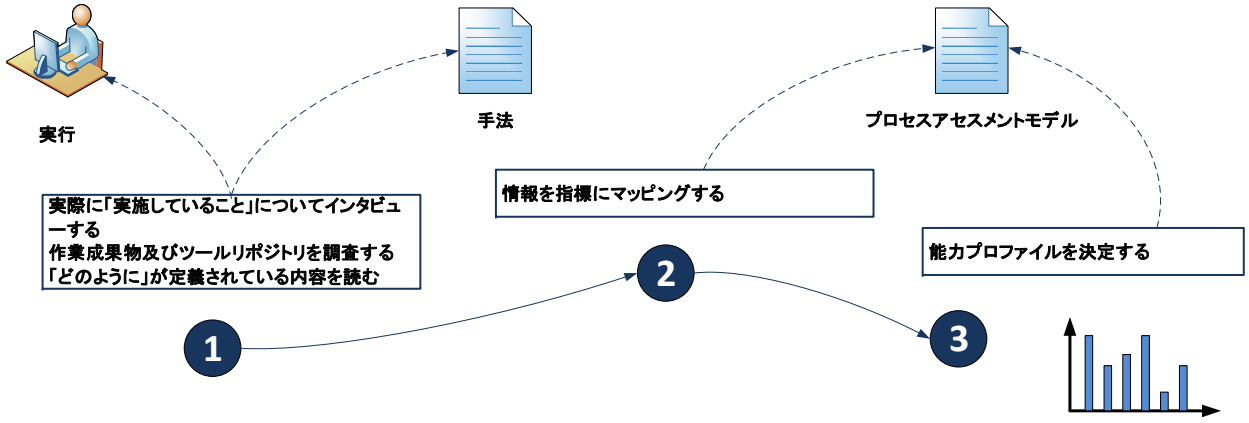

図 4 — プロセス能力判定のためのプロセスアセスメントの実施

2 プロセス参照モデル及びプロセス実施指標 (レベル 1)

2.1 取得プロセス群 (ACQ)

2.1.1 ACQ.2 サプライヤー依頼及び選定

プロセス ID	**ACQ.2**
プロセス名	**サプライヤー依頼及び選定**
プロセス目的	サプライヤー依頼及び選定プロセスの目的は、関連基準に基づき、サプライヤーに契約/合意を授与することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 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) 見積依頼書がサプライヤー候補に発行されている。 4) 契約書、対応計画書及びリスク低減計画書が合意されている。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件を分析する。[成果 1] *備考 1: 基準には、以下の内容を考慮する。* • *機能要件及び非機能要件* • *サイバーセキュリティコンセプト及び手法 (脅威分析及びリスク評価、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、開発後、ガバナンス、品質、及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及び実施の証拠*

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、確立した評価基準に基づいて評価する。サプライヤー最終候補一覧を作成し、評価結果を文書化する。[成果 2]

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。
- *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*
- *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に、組織の品質マネジメントシステムに対する適切性/能力の証拠*

ACQ.2.BP3: 見積依頼書 (RFQ) の準備及び実行
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書を準備し、発行する。[成果 3, 4]

備考 3: 見積依頼書には、以下の内容を含む。
- *すべての顧客関連基準及び法的基準に準拠させるための正式な依頼*
- *サプライヤーのサイバーセキュリティの責任*
- *サプライヤーの見積対象に基づいたサイバーセキュリティゴール、又は一連の関連するサイバーセキュリティ要件及びそれらの属性を含むサイバーセキュリティに関する作業範囲*
- *識別した逸脱及びリスクに対する対応計画書*

ACQ.2.BP4: 契約/合意の交渉及び授与
関連する要件及び合意した是正処置を網羅した見積依頼書に対する結果の評価に基づき、契約を確立する。[成果 4]

備考 4: 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記載してもよい。 *備考 5: サポートなしの納入物の場合 (例:フリーソフトウェア及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。*

アウトプット作業成果物	02-00 契約書	[成果 4]
	02-01 コミットメント/合意書	[成果 4]
	02-50 インタフェース協定	[成果 4]
	08-20 リスク低減計画書	[成果 4]
	12-01 見積依頼書	[成果 3]
	14-02 是正処置登録	[成果 3, 4]
	14-05 サプライヤー候補登録	[成果 2]
	15-21 サプライヤー評価報告書	[成果 2]
	18-50 サプライヤー資格認定基準	[成果 1]

	成果 1	成果 2	成果 3	成果 4
基本プラクティス				
ACQ.2.BP1	x			
ACQ.2.BP2		x		
ACQ.2.BP3			x	x
ACQ.2.BP4				x
アウトプット作業成果物				
02-00 契約書				x
02-01 コミットメント/合意書				x
02-50 インタフェース協定				x
08-20 リスク低減計画書				x

12-01 見積依頼書			x	
14-02 是正処置登録			x	x
14-05 サプライヤー候補登録		x		
15-21 サプライヤー評価報告書		x		
18-50 サプライヤー資格認定基準	x			

2.2 管理プロセス群 (MAN)

2.2.1 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	サイバーセキュリティリスク管理プロセスの目的は、利害関係者への損害リスクについて識別、優先順位付け及び分析を実施し、それぞれのリスク対応オプションを継続的に監視し、制御することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1) 実施すべきリスク管理の適用範囲が決定されている。 2) 適切なリスク管理プラクティスが定義され、実装されている。 3) 潜在的リスクは、それらが進化するものとして識別されている。 4) 潜在的リスクに対する初期の優先順位が、見積られた損害及び影響に基づいて割当てられている。 5) 潜在的リスクが分析され、リスクが評価されている。 6) リスク対応オプションが決定されている。 7) リスクが継続的に監視され、関連する変化に応じてリスクが識別されている。 8) 是正処置が、関連する変化に応じて実施されている。
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決定** プロジェクト及びサイバーセキュリティ属性を伴うプロジェクト資産、損害シナリオ、利害関係者、影響カテゴリ、並びに関連する製品フェーズを含めて、実施すべきサイバーセキュリティリスク管理の適用範囲を決定する。 運用環境及び組織のリスク管理方針に基づき適用範囲を決定する。[成果 1] *備考 1: 資産のサイバーセキュリティ属性には、機密性、完全性、及び可用性を含む。* *備考 2: 典型的な影響カテゴリとは、安全、金銭的、運用及びプライ*

	バシーを指す。 **MAN.7.BP2: サイバーセキュリティリスク管理プラクティスの定義** 定義した適用範囲に基づき、サイバーセキュリティリスクを管理するための適切なプラクティスを、以下の内容を含めて定義する。 • 潜在的リスクの識別 • リスク分析 • リスク評価 • リスク決定 • リスク対応の決定 [成果 2] *備考 3: 関連するリスク評価のプラクティスは、FMEA、TARA、HARA、FTA のようなプラクティスを網羅している確立された基準から含める。* **MAN.7.BP3: 潜在的リスクの識別** プロジェクトの適用範囲内における潜在的リスクを、プロジェクトの初期及び実施中に識別し、技術的な意思決定又は管理上の意思決定の発生時にリスク要因を継続的に検索する。[成果 3] *備考 4: 適用範囲内のすべての関連する属性及び資産において、潜在的リスクの識別には、利害関係者に影響を及ぼす損害シナリオの起点となる特定のリスクを生じさせる脅威シナリオの決定を含めなければならない。* **MAN.7.BP4: 損害に対する潜在的リスクの初期の優先順位付け** 関連するカテゴリ及び利害関係者に対する損害及び影響の観点から、潜在的リスクに優先順位を割当てる。[成果 4] *備考 5: 潜在的リスクの優先順位は、リスク評価の範囲 (訳注:結果を指す) と一致する可能性がある。* **MAN.7.BP5: 潜在的リスクの分析及びリスクの評価** リスクの確率、影響度及び重大度を決定するために、潜在的リスクを分析する。[成果 5] *備考 6: リスクは、脅威シナリオを実現できることが識別された攻撃経路と、その識別された攻撃経路の実行容易性に基づき分析され*

	る。 *備考 7: メトリクス、評定及びスコアリングスキームを評価するために、例えば、機能分析、シミュレーション、FMEA、FTA、ATA などの様々な技法がシステムの分析に使用される。* **MAN.7.BP6: リスク対応オプションの定義** 各リスク (又は一連のリスク) に対して、リスクを受容、低減、回避又は共有 (移転) するために、選択した対応オプションを定義する。[成果 6] *備考 8: 通常、受容したリスクおよび共有したリスクには、サイバーセキュリティクレームを定義する。* **MAN.7.BP7: リスクの監視** 各リスク (又は一連のリスク) に対して、リスクのステータスの変化を判断し、リスク対応活動の進捗を評価する。[成果 7] *備考 9: 主要なリスクは、より上位レベルの管理層に伝達され、監視されることが必要な場合もある。* *備考 10: リスク対応の決定は、条件変更が生じた際に改訂される場合、又は新規及び更新された見積並びに分析結果から生じる場合がある。* **MAN.7.BP8: 是正処置の実施** リスクに関連する変化を識別した際は、適切な是正処置を実施する。[成果 8] *備考 11: 是正処置には、リスクの再評価、新規のリスク対応プラクティスの作成及び実施、又は既存プラクティスの調整を含む。*
アウトプット作業成果物	07-07 リスク測定項目 [成果 6] 08-14 復旧計画書 [成果 6, 7, 8] 08-19 リスク管理計画書 [成果 1, 2, 4, 5, 6, 7, 8] 13-20 リスク対策依頼 [成果 6, 7, 8] 14-08 追跡システム [成果 4, 5, 6, 7, 8] 14-51 サイバーセキュリティシナリオ登録 [成果 1, 3, 5]

	14-52 資産ライブラリ [成果 1, 3] 15-08 リスク分析報告書 [成果 5, 6] 15-09 リスクステータス報告書 [成果 6, 7, 8]

	成果 1	成果 2	成果 3	成果 4	成果 5	成果 6	成果 7	成果 8
基本プラクティス								
MAN.7.BP1	x							
MAN.7.BP2		x						
MAN.7.BP3			x					
MAN.7.BP4				x				
MAN.7.BP5					x			
MAN.7.BP6						x		
MAN.7.BP7							x	
MAN.7.BP8								x
アウトプット作業成果物								
07-07 リスク測定項目						x		
08-14 復旧計画書						x	x	x
08-19 リスク管理計画書	x	x		x	x	x	x	x
13-20 リスク対策依頼						x	x	x
14-08 追跡システム				x	x	x	x	x
14-51 サイバーセキュリティシナリオ登録	x		x		x			
14-52 資産ライブラリ	x		x					
15-08 リスク分析報告書					x	x		
15-09 リスクステータス報告書						x	x	x

2.3 セキュリティエンジニアリングプロセス群 (SEC)

2.3.1 SEC.1 サイバーセキュリティ要件抽出

プロセス ID	**SEC.1**
プロセス名	**サイバーセキュリティ要件抽出**
プロセス目的	サイバーセキュリティ要件抽出プロセスの目的は、リスク管理の成果からサイバーセキュリティゴール及びサイバーセキュリティ要件を導出し、リスク評価、サイバーセキュリティゴール、及びサイバーセキュリティ要件との間の一貫性を確保することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1) サイバーセキュリティゴールが定義されている。 2) サイバーセキュリティ要件がサイバーセキュリティゴールから導出されている。 3) 一貫性及び双方向トレーサビリティが、サイバーセキュリティ要件とサイバーセキュリティゴールとの間、及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確立されている。 4) サイバーセキュリティ要件が合意され、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及びサイバーセキュリティ要件の導出** リスク対応の決定によりリスクの低減を必要とする場合、それらの脅威シナリオに対するサイバーセキュリティゴールを導出する。サイバーセキュリティゴールを達成するための基準を含め、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件及び非機能要件を明記する。[成果 1, 2] *備考 1: このプラクティスには、本プロセスを反復実行することによる要件の更新を含む。* *備考 2: このプラクティスには、開発後のフェーズにおける生産、運用、保守及び廃棄に関する要件を含む。*

	SEC.1.BP2: 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件とサイバーセキュリティゴールとの間の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双方向トレーサビリティを確立する。[成果 3] **SEC.1.BP3: 一貫性の確保** サイバーセキュリティ要件とサイバーセキュリティゴールとの間の一貫性を確保する。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する。[成果 3] **SEC.1.BP4: 合意したサイバーセキュリティ要件の伝達** 合意したサイバーセキュリティゴール及びサイバーセキュリティ要件を、影響を受けるすべての関係者へ伝達する。[成果 4]
アウトプット作業成果物	13-04 情報伝達記録 [成果 4] 13-19 レビュー記録 [成果 3] 13-22 トレーサビリティ記録 [成果 3] 15-01 分析報告書 [成果 1, 2] 17-11 ソフトウェア要件仕様書 [成果 1, 2] 17-12 システム要件仕様書 [成果 1, 2] 17-51 サイバーセキュリティゴール [成果 1]

	成果 1	成果 2	成果 3	成果 4
基本プラクティス				
SEC.1.BP1	x	x		
SEC.1.BP2			x	
SEC.1.BP3			x	
SEC.1.BP4				x
アウトプット作業成果物				

13-04 情報伝達記録				x
13-19 レビュー記録			x	
13-22 トレーサビリティ記録			x	
15-01 分析報告書	x	x		
17-11 ソフトウェア要件仕様書	x	x		
17-12 システム要件仕様書	x	x		
17-51 サイバーセキュリティゴール	x			

2.3.2 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	サイバーセキュリティ実装プロセスの目的は、システム及びソフトウェアのエレメントにサイバーセキュリティ要件を割当て、それらを確実に実装することである。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1) アーキテクチャ設計が更新されている。 2) サイバーセキュリティ要件がアーキテクチャ設計のエレメントに割当てられている。 3) 適切なサイバーセキュリティコントロールが選択されている。 4) 脆弱性が分析されている。 5) 詳細設計が更新されている。 6) ソフトウェアユニットが作成されている。 7) 一貫性及び双方向トレーサビリティが、アーキテクチャ設計と詳細設計との間で確立されている。 8) サイバーセキュリティリスク対応の実装が合意され、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.2.BP1: アーキテクチャ設計の記載内容の更新** サイバーセキュリティゴール及びサイバーセキュリティ要件に基づ

	き、アーキテクチャ設計を更新する。[成果 1] *備考 1: 更新は、システムレベル及びソフトウェアレベルのアーキテクチャに対して実施する。* *備考 2: この文脈における更新とは、アーキテクチャのエレメントを追加、調整、又は修正することを意味する。* **SEC.2.BP2: サイバーセキュリティ要件の割当** サイバーセキュリティ要件を一つ以上のアーキテクチャ設計エレメントに割当てる。[成果 2] *備考 3: システムレベル及びソフトウェアレベルのサイバーセキュリティ要件が対象である。* **SEC.2.BP3: サイバーセキュリティコントロールの選択** サイバーセキュリティ要件を達成又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択する。[成果 3] *備考 4: 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回避、検出、抑制及び低減するための技術的な対応策、又はその他の対応策を指す。* **SEC.2.BP4: インタフェースの定義** アーキテクチャ設計エレメントと運用環境との間のサイバーセキュリティに関連するインタフェースを更新し、記述する。[成果 1] **SEC.2.BP5: アーキテクチャ設計の分析** 脆弱性を識別して解析するために、アーキテクチャ設計を分析する。[成果 4] **SEC.2.BP6: 詳細設計の記載内容の更新** アーキテクチャ設計に基づき、詳細設計を更新する。[成果 5] *備考 5: この文脈における更新とは、詳細設計のコンポーネントを追加、調整、または修正することを意味する。* **SEC.2.BP7: ソフトウェアユニットの作成** 適切なモデリング言語又はプログラミング言語を使用して、ソフトウェアを実装する。[成果 6] *備考 6: サイバーセキュリティのための適切なモデリング言語及び*

	プログラミング言語に対する基準には、言語サブセットの使用、強い型付けの実施、及び/又は防御的な実装技法の使用を含む。 *備考 7: 上記で定義された基準を網羅するための例として、コーディングガイドライン又は適切な開発環境の使用を挙げることができる。* **SEC.2.BP8: 双方向トレーサビリティの確立** 更新されたアーキテクチャ設計と詳細設計との間の双方向トレーサビリティを確立する。[成果 2, 7] **SEC.2.BP9: 一貫性の確保** 更新されたアーキテクチャ設計と詳細設計との間の一貫性を確保する。[成果 7] **SEC.2.BP10: サイバーセキュリティ実装に対する合意した結果の伝達** 開発後のフェーズにおける利害関係者を含む、影響を受けるすべての関係者へ、サイバーセキュリティ実装に対する合意した結果を伝達する。[成果 8] *備考 8: 伝達内容には、サイバーセキュリティ実装の結果及びアーキテクチャ設計分析において識別した脆弱性の両方を含む。*
アウトプット作業成果物	04-04 ソフトウェアアーキテクチャ設計書 [成果 1] 04-05 ソフトウェア詳細設計書 [成果 5] 04-06 システムアーキテクチャ設計書 [成果 1] 11-05 ソフトウェアユニット [成果 6] 13-04 情報伝達記録 [成果 8] 13-19 レビュー記録 [成果 7] 13-22 トレーサビリティ記録 [成果 2, 7] 15-50 脆弱性分析報告書 [成果 4] 17-52 サイバーセキュリティコントロール [成果 3]

	成果 1	成果 2	成果 3	成果 4	成果 5	成果 6	成果 7	成果 8
基本プラクティス								
SEC.2.BP1	x							
SEC.2.BP2		x						
SEC.2.BP3			x					
SEC.2.BP4	x							
SEC.2.BP5				x				
SEC.2.BP6					x			
SEC.2.BP7						x		
SEC.2.BP8							x	
SEC.2.BP9							x	
SEC.2.BP10								x
アウトプット作業成果物								
04-04 ソフトウェアアーキテクチャ設計書	x	x						
04-05 ソフトウェア詳細設計書		x			x			
04-06 システムアーキテクチャ設計書	x	x						
11-05 ソフトウェアユニット						x		
13-04 情報伝達記録								x
13-19 レビュー記録							x	
13-22 トレーサビリティ記録							x	
15-50 脆弱性分析報告書				x				
17-52 サイバーセキュリティコントロール			x					

2.3.3 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	リスク対応検証プロセスの目的は、設計の実装及びコンポーネントの統合がサイバーセキュリティ要件、更新されたアーキテクチャ設計及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	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1) リスク対応検証及び統合の戦略が策定され、実装され、維持されている。 2) サイバーセキュリティ要件、更新されたアーキテクチャ設計及び詳細設計に遵守して実装されている証拠を提供するために、リスク対応検証戦略に基づき、リスク対応検証仕様が作成されている。 3) 識別された作業成果物が、リスク対応検証ためのリスク対応検証戦略に基づき、検証されている。設計の実装及びコンポーネントの統合に対するテストが、定義されたテストケースを使用して実施されている。検証及びテスト結果が記録されている。 4) サイバーセキュリティ要件とリスク対応検証仕様 (テストケースを含む) との間の双方向トレーサビリティ、更新されたアーキテクチャ設計 (詳細設計を含む) とリスク対応検証仕様 (テストケースを含む) との間の双方向トレーサビリティ、及びリスク対応検証仕様に含まれるテストケース間と検証結果との間の双方向トレーサビリティが確立されている。 5) サイバーセキュリティ要件とリスク対応検証仕様 (テストケースを含む) との間の一貫性、及び更新されたアーキテクチャ設計 (詳細設計を含む) とリスク対応検証仕様 (テストケースを含む) との間の一貫性が確立されている。 6) 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: リスク対応検証及び統合の戦略の策定** リスク対応検証及び統合に対する戦略を、回帰戦略を含めて策定

し、実装する。本戦略には以下を含む。

- 関連する手法、技法及びツールを伴う活動
- 検証対象の作業成果物又はプロセス
- 検証活動を実施するための検証に対する独立性の程度
- 検証基準 [成果 1]

備考 1: リスク対応検証では、システム及びソフトウェア開発ライフサイクルのある特定のフェーズ (例:要件、設計、実装、テスト) のアウトプットが、そのフェーズで明記された要件に満足している客観的な証拠を提供する。

備考 2: リスク対応検証戦略には、以下を含む。

- *システムレベル及びソフトウェアレベルにおける要件ベースのテスト、並びにインタフェーステスト*
- *仕様に存在しない機能の確認*
- *リソース消費量の評価*
- *制御フロー及びデータフローの検証*
- *静的解析:ソフトウェアの場合:静的コード解析 (例:業界で認知されているセキュリティに特化したコーディング標準)*

備考 3: リスク対応検証の手法及び技法には、以下は含む。

- *攻撃をシミュレートするネットワークテスト (不正なコマンド、不正なハッシュキーを用いた信号、大量のメッセージの接続など)*
- *総当り攻撃のシミュレーション*

備考 4: リスク対応検証の手法及び技法には、監査、インスペクション、ピアレビュー、ウォークスルー、コードレビュー、及びその他の技法も含む。

SEC.3.BP2: リスク対応検証仕様の作成

リスク対応検証戦略に基づき、リスク対応検証仕様 (テストケースを含む) を作成する。この仕様は、実装したものがサイバーセキュリティ要件、並びに更新されたアーキテクチャ設計及び詳細設計に遵守している証拠を提供することに適していなければならない。[成果 2]

備考 5: テストケースを導出する手法には以下を含む。

- *要件の分析*
- *同値クラスの生成及び分析*
- *境界値の分析*
- *知識又は経験に基づくエラー推測*

SEC.3.BP3: 検証活動の実施
作業成果物が明示された要件に満足していることを確認するために、明記した戦略に基づき、識別した作業成果物を検証する。
リスク対応検証仕様に基づき、設計の実装及びコンポーネントの統合に対してテストを実施する。
リスク対応検証結果及び検証ログを記録する。[成果 3]

SEC.3.BP4: 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件とリスク対応検証仕様 (リスク対応検証仕様に記載されているテストケースを含む) との間の双方向トレーサビリティを確立する。

更新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及びリスク対応検証仕様との間の双方向トレーサビリティを確立する。

リスク対応検証仕様に含まれるテストケースと検証結果との間の双方向トレーサビリティを確立する。[成果 4]

備考 6: 双方向トレーサビリティは、網羅性、一貫性、及び影響分析に役立つ。

SEC.3.BP5: 一貫性の確保
サイバーセキュリティ要件とリスク対応検証仕様 (リスク対応検証仕様に記載されているテストケースを含む) との間の一貫性を確保する。

更新されたアーキテクチャ設計及び詳細設計と、リスク対応検証仕様との間の一貫性を確保する。[成果 5]

備考 7: 一貫性は、双方向トレーサビリティによって裏付けられ、レビュー記録によって実証できる。

SEC.3.BP6: 結果の要約及び伝達

	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。[成果 6] *備考 8: リスク対応検証の実施に必要な情報すべてを要約の中に記述することで、他の関係者はその結果の判断が可能となる。*

アウトプット作業成果物	08-50 テスト仕様書	[成果 2]
	08-52 テスト計画書	[成果 1]
	13-04 情報伝達記録	[成果 6]
	13-19 レビュー記録	[成果 3, 5]
	13-22 トレーサビリティ記録	[成果 4]
	13-25 検証結果	[成果 3, 6]
	13-50 テスト結果	[成果 3, 6]
	19-10 検証戦略	[成果 1]

	成果 1	成果 2	成果 3	成果 4	成果 5	成果 6
基本プラクティス						
SEC.3 BP1	x					
SEC.3 BP2		x				
SEC.3 BP3			x			
SEC.3 BP4				x		
SEC.3 BP5					x	
SEC.3 BP6						x
アウトプット作業成果物						
08-50 テスト仕様書		x				
08-52 テスト計画書	x					
13-04 情報伝達記録						x
13-19 レビュー記録			x		x	
13-22 トレーサビリティ記録				x		
13-25 検証結果			x			x

13-50 テスト結果			x			x
19-10 検証戦略	x					

2.3.4 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	リスク対応妥当性確認プロセスの目的は、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。
プロセス成果	このプロセスを適切に実装した場合の成果は、以下のとおりである。 1) リスク対応妥当性確認戦略が策定され、実装され、利害関係者と合意され、その実装により関連するサイバーセキュリティゴールが達成されている証拠を提供できるように適切に維持されている。 2) 実装された設計及び統合されたコンポーネントの妥当性が、定義されたリスク対応妥当性確認戦略に基づき確認されている。 3) 妥当性確認活動が文書化され、結果が記録されている。 4) サイバーセキュリティゴール、リスク対応妥当性確認仕様、妥当性確認結果の間の双方向トレーサビリティが確立されている。 5) サイバーセキュリティゴールとリスク対応妥当性確認仕様との間の一貫性が確立されている。 6) 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戦略の策定** 妥当性確認戦略を策定し、実装する。[成果 1] *備考 1: 通常、リスク対応妥当性確認の手法及び技法には、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含む (例:侵入テスト) 。* *備考 2: リスク対応妥当性確認においては、関連するサイバーセ*

	キュリティゴールが達成されているかどうかを検査する。 **SEC.4.BP2: リスク対応妥当性確認仕様の作成** リスク対応妥当性確認戦略に基づき、リスク対応妥当性確認仕様(テストケースを含む) を作成する。この仕様は、関連するサイバーセキュリティゴールの達成を示す証拠を提供することに適していなければならない。[成果 2] *備考 3: テストケースを導出する手法には以下を含む。* • *要件の分析* • *同値クラスの生成及び分析* • *境界値の分析* • *知識又は経験に基づくエラーの推測* **SEC.4.BP3: リスク対応妥当性確認活動の実施及び文書化** 定義したリスク対応妥当性確認戦略に基づき、実装した設計及び統合したコンポーネントの妥当性を確認する。 リスク対応妥当性確認活動を文書化し、結果を記録する。 [成果 2,3] *備考 4: 不適合及び脆弱性の取扱については、SUP.9 を参照のこと。* **SEC.4.BP4: 双方向トレーサビリティの確立** サイバーセキュリティゴールとリスク対応妥当性確認仕様との間の双方向トレーサビリティを確立する。リスク対応妥当性確認仕様と妥当性確認結果との間の双方向トレーサビリティを確立する。 [成果 4] *備考 5: 双方向トレーサビリティは、網羅性、一貫性及び影響分析に役立つ。* **SEC.4.BP5: 一貫性の確保** サイバーセキュリティゴールとリスク対応妥当性確認仕様との間の一貫性を確保する。[成果 5] *備考 6: 一貫性は双方向トレーサビリティによって裏付けられ、レビュー記録によって実証できる。* **SEC.4.BP6: 結果の要約及び伝達**

	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。[成果 3, 6] *備考 7: 通常、要約には、リスク対応妥当性確認活動からの情報、及び追加された脆弱性に関する重要な所見が含まれることで、他の関係者はその結果の判断が可能となる。*
アウトプット作業成果物	08-50 テスト仕様書 [成果 2] 13-04 情報伝達記録 [成果 6] 13-19 レビュー記録 [成果 2, 5] 13-22 トレーサビリティ記録 [成果 4] 13-24 妥当性確認結果 [成果 3] 19-11 妥当性確認戦略 [成果 1]

	成果 1	成果 2	成果 3	成果 4	成果 5	成果 6
基本プラクティス						
SEC.4 BP1	x					
SEC.4 BP2		x				
SEC.4 BP3		x	x			
SEC.4 BP4				x		
SEC.4 BP5					x	
SEC.4 BP6			x			x
アウトプット作業成果物						
08-50 テスト仕様書		x				
13-04 情報伝達記録						x
13-19 レビュー記録		x			x	
13-22 トレーサビリティ記録				x		
13-24 妥当性確認結果			x			
19-11 妥当性確認戦略	x					

付録 A　プロセスアセスメント及びプロセス参照モデルの適合性

A.1　序文

Automotive SPICE プロセスアセスメントモデル及びプロセス参照モデルは、ISO/IEC 33004:2015 に定められた適合要件を満たしている。このプロセスアセスメントモデルは、ISO/IEC 33002:2015 の要件を満たしたアセスメントの実施時に使用できる。

この節は ISO/IEC 33004:2015 に定められたプロセスアセスメントモデル及びプロセス参照モデルの要件に対する適合証明となる。

> *[ISO/IEC 33004:2015, 5.5, 6.4]*

著作権により、各要件はその番号のみで引用される。要件の全文は ISO/IEC 33004:2015 にて参照できる。

A.2　プロセス参照モデルに対する要件への適合

従属節 5.3:「プロセス参照モデルの要件」

下記情報は、本書の第 1 章 に記載している。

- プロセス参照モデルのドメインの宣言
- プロセス参照モデルと、その意図された使用背景との関係の記述
- プロセス参照モデル内に定義されたプロセス間の関係の記述

ISO/IEC 33004:2015 従属節 5.4 の要件を満たしたプロセス参照モデル範囲内のプロセスの記述は、本書の第 2 章にある。

> *[ISO/IEC 33004:2015, 5.3.1]*

本プロセス参照モデルの該当業界及びその適用方法、並びに本プロセス参照モデルに対する合意は、本書の著作権通知と適用範囲に明記している。

[ISO/IEC 33004:2015, 5.3.2]

プロセスの記述は一意である。本書における各プロセスは、一意の名称及び ID で識別する。

[ISO/IEC 33004:2015, 5.3.3]

従属節 5.4:「プロセス記述」

プロセス記述の要件は、本書の第 2 章におけるプロセス記述によって満たされている。

[ISO/IEC 33004:2015, 5.4]

A.3　プロセスアセスメントモデルに対する要件への適合

従属節 6.1:「序文」

本プロセスアセスメントモデルの目的は、ISO/IEC 33020:2015 に定義されたプロセス測定の枠組みを用いて、自動車ドメインにおけるプロセス能力のアセスメントを支援することである。

[ISO/IEC 33004:2015, 6.1]

従属節 6.2:「プロセスアセスメントモデル範囲」

本プロセスアセスメントモデルのプロセス範囲は、本書の第 3.1 章におけるプロセス参照モデルに定義されている。Automotive SPICE のプロセス参照モデルは、付録 A.2 に記述した通り、ISO/IEC 33004:2015 従属節 5 の要件を満たしている。

本プロセスアセスメントモデルのプロセス能力範囲は、ISO/IEC 33020:2015 に明示されたプロセス測定の枠組みで定義されている。ISO/IEC 33020 は、ISO/IEC 33003 の要件を満たしたプロセス能力測定の枠組みを定義している。

[ISO/IEC 33004:2015, 6.2]

従属節 6.3:「プロセスアセスメントモデルの要件」

Automotive SPICE プロセスアセスメントモデルは、プロセス能力と関連付けされている。

[ISO/IEC 33004:2015, 6.3.1]

本プロセスアセスメントモデルは、ISO/IEC 33020:2015 に明示されたプロセス測定の枠組みを織り込んでおり、ISO/IEC 33003 の要件を満たしている。

[ISO/IEC 33004:2015, 6.3.2]

本プロセスアセスメントモデルは、本書内の Automotive SPICE 参照モデルに基づく。

本プロセスアセスメントモデルは、ISO/IEC 33020:2015 に定義された測定の枠組みに基づく。

[ISO/IEC 33004:2015, 6.3.3]

本プロセスアセスメントモデルに含まれているプロセスは、プロセス参照モデル内で定義されたものと同一である。

[ISO/IEC 33004:2015, 6.3.4]

本プロセスアセスメントモデルのすべてのプロセスに対して、ISO/IEC 33020:2015 におけるプロセス測定の枠組みで定義されたすべてのレベルを表記している。

[ISO/IEC 33004:2015, 6.3.5]

本プロセスアセスメントモデルは、本書の第 3 章に下記内容を定義している。

- 選択したプロセス品質特性
- 選択したプロセス測定の枠組み
- 選択したプロセス参照モデル
- プロセス参照モデルから選択したプロセス

> *[ISO/IEC 33004:2015, 6.3.5 a-d]*

能力座標において、本プロセスアセスメントモデルは、ISO/IEC 33020:2015 のプロセス測定の枠組みに定義されたすべてのプロセス属性及び能力レベルを表記している。

> *[ISO/IEC 33004:2015, 6.3.5 e]*

従属節 6.3.1:「アセスメント指標」

備考: ISO/IEC 33004:2015 の出版物における番号のエラーによって、下記参照番号は上述のものと重複している。ISO/IEC 33004:2015 から正しい章節を参照できるように、従属節の表題のテキストを下記の 3 つの要件のために追記した。

Automotive SPICE プロセスアセスメントモデルは、第 3.3 章に定義されたアセスメント指標を含むことを通じて、プロセス参照モデルで定義されたプロセスに対するプロセス能力の 2 次元的視点を提供している。使用しているアセスメント指標は以下の通りである。

- 基本プラクティス及びアウトプット作業成果物

> *[ISO/IEC 33004:2015, 6.3.1 a:「アセスメント指標」]*

- 共通プラクティス及び共通リソース

> *[ISO/IEC 33004:2015, 6.3.1 b:「アセスメント指標」]*

従属節 6.3.2:「プロセス参照モデルに対するプロセスアセスメントモデルのマッピング」

プロセス参照モデルにおけるプロセス目的及びプロセス成果に対するアセスメント指標のマッピングは、第 4 章の各基本プラクティスの記述に含まれている。

プロセス測定の枠組みにおけるプロセス属性に対するアセスメント指標のマッピングは、プロセス属性のすべての達成成果を含め、第 5 章の各共通プラクティスの記述に含まれている。

各マッピングは角括弧の参照によって示されている。

> *[ISO/IEC 33004:2015, 6.3.2:「プロセスアセスメントモデルのマッピング」]*

従属節 6.3.3:「アセスメント結果の表現形式」

本プロセスアセスメントモデルにおけるプロセス属性及びその評定は、測定の枠組みで定義されたものと同一である。その結果、本プロセスアセスメントモデルに基づくアセスメント結果は、アセスメント範囲内の各プロセスに対する一連のプロセス属性評定として直接表現される。変換の形式は不要である。

[ISO/IEC 33004:2015, 6.3.3:「アセスメント結果の表現形式」]

付録 B　　作業成果物特性

本付録に記載した作業成果物特性は、プロセス実装の潜在的なアウトプットをレビューする際に使用できる。これらの特性は、あるプロセスのアセスメントを裏付けるための客観的な証拠を提供するために、サンプリングした作業成果物の中から属性を見つけ出すための手引きとして記載する。

本情報を使用する際は、プロセスの背景 (アプリケーションドメイン、事業目的、開発方法論、組織規模等) を確実に考慮するために、文書化したプロセス及びアセッサーの判断が必要である。

作業成果物は表 B.1 の図式で定義している。作業成果物及びそれらの特性は、与えられた背景において意図したプロセスの目的に貢献するかどうかを考慮する際の開始点として見なすべきであり、あらゆる組織が持たなければならないチェックリストの項目ではない。

表 B.1 — 作業成果物特性 (WPC) 表の構造

作業成果物の識別 (ID)	作業成果物を参照するために使用される作業成果物の識別番号
作業成果物名	作業成果物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、プラクティス又はプロセスによって作成される作業成果物の識別子として提供されている。各組織は、これらの作業成果物を別の名称で呼んでもよい。組織における作業成果物の名称は重要ではない。同様に、組織は、1 種類の作業成果物として定義された特性を含む複数の同等の作業成果物を持ってもよい。作業成果物のフォーマットは様々でよい。組織が作成した実際の作業成果物をここで与えられた例にマッピングすることは、アセッサー及び組織部門のコーディネーターの責任である。

作業成果物特性	作業成果物と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の中にあるこれらの特性を見つけ出す。

作業成果物 (NN-00 形式の ID 付) は、共通の種類の作業成果物において、属性を達成すると明白になると思われる一連の特性を示している。共通作業成果物は、プロセス実施指標として定義された特定の作業成果物の分類に対する基準を形成している。

通常、作業成果物は、特定のプロセス目的の成果を満足するためにプロセス設計担当者によって作成され、プロセス実施者によって適用される。

*備考: * で印した共通作業成果物は、Automotive SPICE プロセスアセスメントモデルで使用しないが、完全を期すために含まれている。*

表 B.2 — 作業成果物特性

[この表にはサイバーセキュリティのための Automotive SPICE に関連する作業成果物特性のみが含まれる。]

WP ID	作業成果物名	作業成果物特性
02-00	契約書	• 購入または納入すべきものを定義している • 納期または契約されたサービス提供日を識別している • あらゆる法的要件を識別している • 金銭的な考慮点を識別している • あらゆる保証情報を識別している • あらゆる著作権及びライセンス情報を識別している • あらゆる顧客サービス要件を識別している • サービスレベルの要件を識別している • 性能及び品質に対するあらゆる期待事項/制約/監視について言及している • 使用すべき標準規格及び手順 • レビュー及び承認の証拠 • 契約に応じて以下を考慮している

WP ID	作業成果物名	作業成果物特性
		- あらゆる検収基準について言及している - 顧客のあらゆる特別なニーズについて言及している (すなわち、守秘義務要件、セキュリティ、ハードウェア等) - 変更管理及び問題解決のあらゆる手順について言及している - 独立した代理業者及び下請け業者とのあらゆる窓口担当者を識別している - 開発及び保守プロセスにおける顧客の役割を識別している - 顧客が提供するリソースを識別している
02-01	コミットメント/ 合意書	• 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承認されている • コミットメントの対象を確立している • コミットメントを果たす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 - 顧客及びサプライヤーの利害関係者、並びに連絡先 - テーラリング合意 - 開発時及び開発後に必要となる対策を含む、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) - 問題 (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

WP ID	作業成果物名	作業成果物特性
		- サプライヤーの支援及び保守の期間
04-04	ソフトウェア アーキテクチャ 設計書	• ソフトウェア構造全体を記述している • タスク構造を含む運用システムを記述している • タスク間/プロセス間通信を識別している • 必要なソフトウェアエレメントを識別している • 自主開発コード及び外部供給コードを識別している • ソフトウェアエレメント間の関係性及び依存性を識別している • データ (アプリケーションパラメータ、変数等) の保管場所及びデータの破損を防止するための策 (例：チェックサム、リダンダンシ―) を識別している • 各モデルシリーズ又はコンフィギュレーションに対するバリアントの派生方法を記述している • ソフトウェアの動的振る舞い (スタートアップ、シャットダウン、ソフトウェア更新、エラー処理、復旧等) を記述している • どの状況下で、どのデータが持続的であるかを記述している • 以下を考慮している - 必要なあらゆるソフトウェア性能特性 - 必要なあらゆるソフトウェアインタフェース - 必要なあらゆるセキュリティ特性 - あらゆるデータベース設計要件
04-05	ソフトウェア 詳細設計書	• 詳細設計を提供している (プロトタイプ、フローチャート、ER 図、疑似コード等として表現できる) • インプット/アウトプットデータのフォーマットを提供している • CPU、ROM、RAM、EEPROM 及び Flash のニーズに対する仕様を提供している • 優先順位と共に割り込みを記述している • サイクルタイム及び優先順位と共にタスクを記

WP ID	作業成果物名	作業成果物特性
		述している • 必要なデータの命名規則を確立している • 必要なデータ構造のフォーマットを定義している • 必要な各データ要素のデータフィールド及び目的を定義している • プログラム構造の仕様を提供している
04-06	システム アーキテクチャ 設計書	• すべてのシステム設計の概要を提供している • システムエレメント間の相互関係を記述している • システムエレメントとソフトウェア間の関係を記述している • 必要な各システムエレメントの設計を明示しており、以下のような側面を考慮している - メモリ/容量要件 - ハードウェアインタフェース要件 - ユーザーインタフェース要件 - 外部システムインタフェース要件 - 性能要件 - コマンド構造 - セキュリティ/データ保護特性 - システムパラメータの設定 (アプリケーションパラメータ、グローバル変数等) - 手動運用 - 再利用可能なコンポーネント • システムエレメントに対する要件のマッピング • システムコンポーネントの運用モード (スタートアップ、シャットダウン、休止モード、診断モード等) の記述 • 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 • システム及びシステムコンポーネントの動的な振る舞いの記述
07-07	リスク測定項目	• リスク発生の確率を識別している • リスク発生の影響を識別している

WP ID	作業成果物名	作業成果物特性
		• 定義された各リスクに対する測定項目を確立している • リスクの状態変化を測定している
08-14	復旧計画書	• 復旧すべき対象を識別している - 復旧させるための手順/手法 - 復旧のスケジュール - 復旧に必要な時間 - 重要な依存性 - 復旧に必要なリソース - 保守対象のバックアップの一覧 - 復旧に責任のある要員及び役割の割当 - 必要な特殊器具 - 必要な作業成果物 - 必要な機器 - 必要な文書 - バックアップの場所及び保管 - 復旧について通知する相手の連絡先 - 検証手順 - 復旧のためのコスト見積り
08-19	リスク管理 計画書	• 識別され、優先順位が付けられたプロジェクトのリスク • リスクを追跡するための仕組み • 是正処置が必要になる時を識別するための閾値の基準 • リスクを低減するための提案方法 - リスク低減者 - 回避方法 - 是正処置の活動/タスク - 監視基準 - リスクを測定するための仕組み
08-20	リスク低減 計画書	• 計画されたリスク対応の活動及びタスク - 受容できないことが判明したリスク又はリスクの組合せに対して選定したリスク対応の

WP ID	作業成果物名	作業成果物特性
		詳細を記述している - 対応時に発生しうるあらゆる困難な点を記述している • 対応スケジュール • 対応のためのリソース及びそれらの割当 • 責任及び権限 - 対応の実施を保証する責任者及びその権限を記述している • 対応制御の測定項目 - リスク対応の有効性を評価するために使用する測定項目を定義している • 対応コスト • 関係者間の窓口 - 適切に対応するために、利害関係者間の調整またはプロジェクトのマスター計画との連携について記述している • 環境/インフラ - あらゆる環境要件、インフラ要件、又は影響を記述している (例：対応策が与えうる安全またはセキュリティへの影響) • リスク対応計画変更の手順及び履歴
08-50	テスト仕様書	• テスト設計仕様書 • テストケース仕様書 • テスト手順仕様書 • 回帰テスト用のテストケースの識別 • システム統合のための追加事項 - 必要なシステムエレメント (ハードウェアエレメント、配線エレメント、パラメータの設定〔アプリケーションパラメータ、グローバル変数等〕、データベース等) の識別 - システムエレメントを統合するために識別した必要なシーケンス又は順序

WP ID	作業成果物名	作業成果物特性
08-52	テスト計画書	• ISO/IEC/IEEE 29119-3 に従っているテスト計画書 • 背景 - プロジェクト/テストのサブプロセス - テストアイテム - テスト範囲 - 想定及び制約 - 利害関係者 - テスト情報の伝達 • テスト戦略 - 満足すべきニーズを識別している - ニーズを満足するために、選択肢及びアプローチを確立している (ブラックボックステスト及び/又はホワイトボックステスト、境界値クラステストの決定、回帰テスト戦略等) - 戦略的な選択肢を評価する対象のための評価基準を確立している - あらゆる制約/リスク、及びそれらの対処方法を識別している - テスト設計技法 - テスト完了基準 - テスト終了基準 - テスト開始、中断及び再開基準 - 収集対象のメトリクス - テストデータの要件 - 再テスト及び回帰テスト - 停止及び再開の基準 - 組織のテスト戦略からの逸脱 • テストデータの要件 • テスト環境要件 • テストのサブプロセス • テスト納入物 • テスト活動及び見積り

WP ID	作業成果物名	作業成果物特性
11-05	ソフトウェア ユニット	• (言語及び用途に適切な) 確立されたコーディング標準に従っている - コメントされている - 構造化、又は最適化されている - 意味のある命名規則 - 識別されたパラメータ情報 - 定義されたエラーコード - 説明的、かつ意味があるエラーメッセージ - フォーマット – インデント付き、階層構造 • (言語及び用途に適切な) データ定義標準に従っている - 定義された変数 - 定義されたデータの型 - 定義されたクラス及び継承構造 - 定義されたオブジェクト • 定義されたエンティティの関係 • データベースレイアウトが定義されている • ファイル構造及びブロックが定義されている • データ構造が定義されている • アルゴリズムが定義されている • 定義された機能的インタフェース
12-01	見積依頼書	• 要求仕様に言及している • サプライヤー選定基準を識別している • 以下のような適切な特性を識別している - システムアーキテクチャ、構成要件、又はサービス要件 (コンサルタント、保守等) - 品質基準、又は品質要件 - プロジェクトのスケジュール要件 - 納入/サービス予定日 - コスト/価格の期待事項 - 規制に関する標準規格/要件 • 提出に関する制約を識別している - 回答の再提出日

WP ID	作業成果物名	作業成果物特性
		- 回答のフォーマットに関する要件
13-01	検収記録	• 納入物の受領記録 • 受領日の識別 • 納入されたコンポーネントの識別 • 定義されたあらゆる顧客検収基準の検証を記録している • 受領した顧客によって署名されている
13-04	情報伝達記録	• 以下の内容を含む、要員間の情報伝達におけるすべての形式 - 手紙 - ファックス - E メール - 音声記録 - ポッドキャスト - ブログ - 映像 - フォーラム - ライブチャット - ウィキ - 写真プロトコル - 会議支援記録
13-14	進捗ステータス記録	• 以下のような計画に対するステータス記録 (計画に対する実績) - 計画したタスクに対する実際のタスクのステータス - 確立した目的/目標に対する実績のステータス - 計画したリソースに対する実際のリソース割当てのステータス - 予算見積りに対する実際のコストのステータス - 計画したスケジュールに対する実績のステータス

WP ID	作業成果物名	作業成果物特性
		- 計画した品質に対する実際の品質のステータス • 計画した活動からのあらゆる逸脱及びその理由の記録
13-16	変更依頼	• 変更の目的を識別している • 依頼のステータス (例: オープン、割当済、実施済、クローズ) を識別している • 依頼者の連絡先情報を識別している • 影響を受けるシステム • 定義された既存システムの運用に対する影響 • 定義された関連文書に対する影響 • 依頼の危機度及び期限
13-19	レビュー記録	• レビューについての背景情報を提供している - レビュー対象物 - 出席したレビュアの一覧 - レビューのステータス • レビュー範囲についての情報を提供している - チェックリスト - レビュー基準 - 要件 - 標準に対する適合性 • 以下についての情報を記録している - レビューに対する準備度合い - レビュー準備に費やした時間 - レビューで費やした時間 - レビュア、役割、及び専門性 • レビュー所見 - 不適合事項 - 改善提案 • 必要な是正処置を識別している - リスクの識別 - 検出した逸脱及び問題に対する優先順位

WP ID	作業成果物名	作業成果物特性
		の一覧 - 問題を是正するために実施すべき対策及びタスク - 是正処置の担当者 - 識別した問題のステータス及び終結目標期日
13-20	リスク対策依頼	• 着手日 • 範囲 • 対象 • 依頼者 • リスク管理プロセスの背景 - このセクションは、一度規定し、その後変更が生じなければ、対策依頼の発生時にそれを参照する - プロセスの範囲 - 利害関係者の見地 - リスクのカテゴリ - リスクの閾値 - プロジェクトの目標 - プロジェクトの想定 - プロジェクトの制約 • リスク - このセクションは、ユーザーの選択に応じて、1 つまたは複数のリスクを網羅してよい - 上記のすべての情報が、一連のリスク全体に当てはまる場合、1つの対策依頼で十分としてよい - 上記の情報がリスクによって異なる場合、各依頼は1つのリスク、または共通の情報を共有する複数のリスクを網羅してよい - リスクの記述 - リスクの確率 - リスクの値

WP ID	作業成果物名	作業成果物特性
		- リスクの影響 - リスクの予測タイミング • リスク対応の選択肢 - 選択したリスク対応オプション- 回避/低減/移転 - 選択肢の記述 - 推奨される選択肢 - 正当な理由 • リスク対策依頼の対応 - 各依頼は、受入、却下、または修正のいずれか、及びその決定に対する根拠について注釈を付けるべきである
13-22	トレーサビリティ記録	• すべての (顧客及び内部) 要件がトレースされている • ライフサイクル作業成果物に対する要件のマッピングを識別している • 作業成果物の分解過程 (すなわち、要件、設計コード、テスト、納入物等) に対する要件のリンクを提供している • ライフサイクルのすべてのフェーズを通して、要件と関連作業成果物との間の前方向及び後方向のマッピングを提供している *備考: トレーサビリティ記録は、他の定義した作業成果物の一機能として含めてもよい (例 : 設計分解のための CASE ツールは、その機能の一部として、マッピング機能を持っている場合がある)*
13-24	妥当性確認結果	• 妥当性確認チェックリスト • 妥当性確認で合格した項目 • 妥当性確認で不合格になった項目 • 妥当性確認で保留になった項目 • 妥当性確認中に識別された問題 • リスク分析

WP ID	作業成果物名	作業成果物特性
		• 対策の推奨 • 妥当性確認の結論 • 妥当性確認者の署名
13-25	検証結果	• 検証チェックリスト • 検証で合格した項目 • 検証で不合格になった項目 • 検証で保留になった項目 • 検証中に識別された問題 • リスク分析 • 対策の推奨 • 検証の結論 • 検証者の署名
13-50	テスト結果	• (該当テストフェーズの) テストログ • 異常報告書 • (該当テストフェーズの) テスト報告書 (要約) - 不合格になったテストケース - 実施しなかったテストケース - テスト実施に関する情報 (日付、テスト担当者名等) 追加事項 (必要に応じて) • (該当するテストフェーズの) 中間テストステータス報告書 • マスターテスト報告書 (要約)
14-02	是正処置登録	• 初期問題を識別している • 定義された対策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活動) を定義している • 開始日及び終結目標期日を識別している • ステータス指標が含まれている • 監査活動のフォローアップを識別している
14-05	サプライヤー候補登録	• 下請け、又はサプライヤーの経歴 • 下請け/サプライヤー候補の一覧

WP ID	作業成果物名	作業成果物特性
		• 資格情報 • 下請け/サプライヤー候補の資格証明 • 過去の経歴情報 (存在する場合)
14-08	追跡システム	• 顧客及びプロセス設計担当者の情報を記録する機能 • 関連するシステム構成情報を記録する機能 • 問題、又は必要な対策についての情報を記録する機能 - 開始日、及び終結目標期日 - 対象項目の重大度/危機度 - あらゆる問題又は必要な対策のステータス - 問題又は対策の担当者についての情報 - 問題解決の優先順位 • 解決策案、又は対応計画を記録する機能 • 管理ステータス情報を提供する機能 • 情報が、知る必要のある者すべてに利用可能である • 統合変更制御体系/記録
14-51	サイバー セキュリティ シナリオ登録	• 以下を識別している - 損害シナリオ o ID o タイトル o 記述 o 影響カテゴリ ▪ 安全 ▪ 金銭的 ▪ 運用 ▪ プライバシー ▪ 品質 - 脅威シナリオ o ID o 関連する資産 o セキュリティ属性 ▪ 機密性

WP ID	作業成果物名	作業成果物特性
		▪ 完全性 ▪ 可用性 o 攻撃実現可能性 (高い/中程度/低い/非常に低い)
14-52	資産ライブラリ	• 以下を識別している - タイトル - 記述 - セキュリティ属性 o 機密性 o 完全性 o 可用性 - 資産に関連する利害関係者
15-01	分析報告書	• 分析の対象 • 分析の実施者 • 使用した分析基準 - 使用した選定基準、又は優先順位体系 - 意思決定基準 - 品質基準 • 結果を記録している - 決定事項/選定事項 - 選定の理由 - 想定 - 潜在的リスク • 以下を含む、分析における正確性の側面 - 完全性 - 理解可能性 - テスト可能性 - 検証可能性 - 実現可能性 - 妥当性 - 一貫性 - 内容の十分性

WP ID	作業成果物名	作業成果物特性
15-08	リスク分析 報告書	• 分析したリスクを識別している - ID - 影響シナリオ (例：損害シナリオ) • 分析結果を記録している - リスクを低減するための可能な方法 - 選択したリスク対応オプション (例：サイバーセキュリティクレームとしてリスクを受容、又はリスク低減) - 想定 - 発生の確率 (例：攻撃実現可能性) - リスクの値 - 制約
15-09	リスクステータス 報告書	• 識別したリスクのステータスを示している - 関連するプロジェクト若しくは活動、又は製品若しくはサービス - リスクの記述 - 状態 - 影響度 - 優先順位の変更 - 低減策を開始した場合の低減期間 - 進行中のリスク低減活動 - 責任 - 制約
15-21	サプライヤー 評価報告書	• 評価の目的を記述する • 評価に用いられる手法及び手段 (チェックリスト、ツール) • 評価に用いられる要件 • 想定及び制約 • 背景及び必要な情報の範囲を識別する (例: 評価日、関係者) • 評価する要件の充足度
15-50	脆弱性分析 報告書	• 以下を識別している - ID

WP ID	作業成果物名	作業成果物特性
		- 記述 - 関連する攻撃経路 - 攻撃実現可能性 (例: CVSS〔共通脆弱性評価システム〕の評定)
17-11	ソフトウェア要件仕様書	• 使用すべき標準規格を識別している • ソフトウェア構造上のあらゆる考慮点/制約を識別している • 必要なソフトウェアエレメントを識別している • ソフトウェアエレメント間の関係を識別している • 以下を考慮している - 必要なあらゆるソフトウェア性能特性 - 必要なあらゆるソフトウェアインタフェース - 必要なあらゆるセキュリティ特性 - あらゆるデータベース設計要件 - 必要なあらゆるエラー取扱及び復旧属性 - 必要なあらゆるリソース消費特性 • サイバーセキュリティにおけるソフトウェアの機能要件及び非機能要件を含んでいる • 1つ以上のサイバーセキュリティゴールに関連している • サイバーセキュリティ要件が認識可能であり、サイバーセキュリティ要件として分類されている
17-12	システム要件仕様書	• システム要件は、「システムの機能及び能力」、「ビジネス、組織、及びユーザーに関する各種要件」、「安全、セキュリティ、人間工学、インタフェース、運用、及び保守に関する各種要件」、「設計上の制約及び適格性確認要件」を含む • 必要なシステム概要の識別 • システムエレメント間の相互関係におけるあらゆる考慮点/制約を識別している • システムエレメントとソフトウェア間の関係におけるあらゆる考慮点/制約を識別している • 必要な各システムエレメントに対して、以下を含

WP ID	作業成果物名	作業成果物特性
		む設計上のあらゆる考慮点/制約を識別している - メモリ/容量要件 - ハードウェアインタフェース要件 - ユーザーインタフェース要件 - 外部システムインタフェース要件 - 性能要件 - コマンド構造 - セキュリティ/データ保護特性 - アプリケーションパラメータの設定 - 手動運用 - 再利用可能なコンポーネント • 運用能力を記述している • 環境能力を記述している • 文書化要件 • 信頼性要件 • ロジスティクス要件 • セキュリティ要件を記述している • 診断要件 • サイバーセキュリティにおけるシステムの機能要件及び非機能要件を含んでいる • 1つ以上のサイバーセキュリティゴールに関連している • サイバーセキュリティ要件が認識可能であり、サイバーセキュリティ要件として分類されている
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を保護するために必要な資産の属性を記述している • 1つ以上の脅威シナリオに関連している
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護、検出、又は低減するための技術的解決策 • 1つ以上のサイバーセキュリティ要件に関連している
18-50	サプライヤー 資格認定基準	• 適切な能力を保有するサプライヤーが満足すべき適合性に対する期待事項

WP ID	作業成果物名	作業成果物特性
		• 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件に対する適合性の証拠、又は取得組織が評価した要件に対する適合性の証拠 • 要件に対するテーラリング、又は例外事項の規定
19-10	検証戦略	• 検証手法、技法、及びツール • 検証対象の作業成果物、又はプロセス • 検証に対する独立性の度合い • 満足すべきニーズを識別している • ニーズを満足するために、選択肢及びアプローチを確立している • 戦略的な選択肢を評価する対象のための評価基準を確立している • あらゆる制約/リスク、及びそれらの対処方法を識別している • 検証終了基準 • 検証開始、中断、及び再開の基準
19-11	妥当性確認戦略	• 妥当性確認手法、技法、及びツール • 妥当性確認対象の作業成果物 • 妥当性確認に対する独立性の度合い • 満足すべきニーズを識別している • ニーズを満足するために、選択肢及びアプローチを確立している • 戦略的な選択肢を評価する対象のための評価基準を確立している • あらゆる制約/リスク、及びそれらの対処方法を識別している

付録 C　　用語集

Automotive SPICE では、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用語
b) ISO/IEC/IEEE 24765 及び ISO/IEC/IEEE 29119 の用語 (付録 C に記載)
c) Automotive SPICE で導入された用語 (付録 C に記載)
d) ISO/SAE 21434 のサイバーセキュリティ関連用語

付録 C は ISO/IEC/IEEE 24765 及び 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 で定義した固有の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	出典	説明
検収テスト	ISO/IEC/IEEE 24765	ユーザー、顧客、又は権限を与えられた実体がシステム又はコンポーネントを受理するか否かの判断をするための公式のテスト
アプリケーションパラメータ	Automotive SPICE V3.1	アプリケーションパラメータとは、システム又はソフトウェアの機能、振る舞い、又はプロパティに適用されるデータを含むパラメータのことである。アプリケーションパラメータの概念は 2 通りで表現される: 1 つ目は論理的仕様 (名称、記述、ユニット、バリュードメイン、閾値、特性曲線をそれぞれ含む) であり、2 つ目は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である。
アーキテクチャエレメント	Automotive SPICE V3.1	システム及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	ISO/SAE 21434	価値のある、又は価値に貢献する対象
攻撃経路	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	ISO/SAE 21434	対応する一連の行為を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	Automotive SPICE V3.1	テスト対象アイテムの内部構造、及び仕組みの知識がなくとも、テストを開発するための要件テスト手法
コードレビュー	Automotive SPICE V3.1	コードの使用目的に対する適合性の判断、並びに仕様及び標準との矛盾を識別するために行う、1 人以上の適格者によるコードのチェックのことである
コーディング	ISO/IEC/IEEE 24765	設計仕様 (設計記述) からプログラミング言語へ、ロジック及びデータを変換すること
一貫性	Automotive SPICE V3.1	一貫性とは、内容及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保証する。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ゴール	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件
サイバーセキュリティ属性	ISO/SAE 21434	守るべき属性
損害シナリオ	ISO/SAE 21434	車両又は車両の機能に関係し、道路利用者に影響を与える有害事象

エレメント	Automotive SPICE V3.1	エレメントとは、「V」字の左側におけるアーキテクチャ及び設計のレベルで定義されたすべての構造オブジェクトである。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又は設計をより詳細なサブエレメントへさらに分割できる
エラー	ISO/IEC/IEEE 24765	演算、観察、又は計測で得られた値/状態が、真値、規定値又は理論的正確値/状態と相違していること
障害	ISO/IEC/IEEE 24765	ソフトウェア内のエラーの兆候
機能要件	ISO/IEC/IEEE 24765	製品、又はプロセスが要求される振る舞い、及び/又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	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、蓄積、又は送信に使用される物理的な機器
統合	Automotive SPICE V3.1	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
品質保証	ISO/IEC/IEEE 24765	アイテム又は製品が確立された技術要件へ適合していることに対し、十分な確信を提供するために必要となる計画的及び体系的なすべての活動パターン
回帰テスト	Automotive SPICE V3.1	変更が意図しない影響を引き起こさないこと、及びシステム又はアイテムが依然としてその明示された要件に適合していることを検証するために、システム又はアイテムを選択的に再テストすること
要件	Automotive SPICE V3.1	システム、システムアイテム、製品、又はサービスが契約書、標準規格、仕様書、又は正式に課された文書を満足させるために、達

		成又は保有しなければならない特性、又は能力
要件仕様書	Automotive SPICE V3.1	機能要件、性能要件、インタフェース要件、設計要件、及び開発標準を含む、システム又はアイテムに対する要件を明示した文書
ソフトウェア	ISO/IEC/IEEE 24765	コンピュータプログラム、手順、並びに (場合によっては) コンピュータシステムの運用に関連する文書及びデータ
ソフトウェアコンポーネント	Automotive SPICE V3.1	Automotive SPICE V3.1 では、用語「ソフトウェアコンポーネント」は、最終的に詳細設計を定義するためのソフトウェアアーキテクチャにおける最下位レベルの「エレメント」として使用される。1つのソフトウェア「コンポーネント」は 1 つ以上のソフトウェア「ユニット」で構成される。 → [アーキテクチャエレメント]、[ユニット] を参照
ソフトウェアエレメント		→ [アーキテクチャエレメント] を参照
ソフトウェアユニット		→ [ユニット] を参照
静的解析	Automotive SPICE V3.1	アイテムの形式、構造、内容又は文書に基づいて、アイテムを評価するプロセス
システム	Automotive SPICE V3.1	特定の環境内において、特定の機能又は一連の機能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	Automotive SPICE V3.1	特定の条件の下にアイテム (システム、ハードウェア、又はソフトウェア) 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	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	ISO/IEC/IEEE 24765	開発プロセスの 2 つ以上の成果物間、特に、互いの前後関係又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	Automotive SPICE V3.1	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] を参照
ユニットテスト	Automotive SPICE V3.1	個々のソフトウェアユニット、又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	ISO/IEC/IEEE 29119	妥当性確認は、作業品目がユーザーの特定のタスクに使用できることを実証する
検証	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、明示された要件が所定の作業品目で満足していることを確認することである
ホワイトボックステスト	Automotive SPICE V3.1	テスト対象アイテムの内部構造及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	オートモーティブスパイス (Automotive SPICE)
ACSMS	自動車用サイバーセキュリティマネジメントシステム (Automotive Cybersecurity Management System)
ATA	アタックツリー分析 (Attack Tree Analysis)
BP	基本プラクティス (Base Practice)
CAN	コントローラエリアネットワーク (Controller Area Network)
CASE	コンピュータ支援ソフトウェア工学 (Computer-Aided Software Engineering)
CCB	変更制御委員会 (Change Control Board)
CFP	提案依頼 (Call For Proposals)

CPU	中央処理装置 (Central Processing Unit)
ECU	電子制御ユニット (Electronic Control Unit)
EEPROM	電気的消去可能プログラマブルリードオンリーメモリ (Electrically Erasable Programmable Read-Only Memory)
FMEA	故障モード及び影響分析 (Failure Mode and Effects Analysis)
FTA	欠陥の木分析 (Fault Tree Analysis)
GP	共通プラクティス (Generic Practice)
GR	共通リソース (Generic Resource)
HARA	ハザード分析及びリスク評価 (Hazard Analysis and Risk Assessment)
IEC	国際電気標準会議 (International Electrotechnical Commission)
IEEE	アイトリプルイー (Institute of Electrical and Electronics Engineers)
I/O	インプット/アウトプット (Input/Output)
ISO	国際標準化機構 (International Organization for Standardization)
MISRA	ミスラ (Motor Industry Software Reliability Association)
PA	プロセス属性 (Process Attribute)
PAM	プロセスアセスメントモデル (Process Assessment Model)
PRM	プロセス参照モデル (Process Reference Model)
RAM	ランダムアクセスメモリ (Random Access Memory)
RC	推奨事項 (Recommendation)
RL	ルール (Rule)
ROM	リードオンメモリ (Read Only Memory)
SPICE	ソフトウェアプロセス改善及び能力判定 (Software Process Improvement and Capability dEtermination)
TARA	脅威分析及びリスク評価 (Threat Analyses and Risk Assessment)
UNECE	国際連合欧州経済委員会 (United Nations Economic Commission for Europe)
VDA	ドイツ自動車工業会 (Verband Der Automobilindustrie)
WP	作業成果物 (Work Product)
WPC	作業成果物特性 (Work Product Characteristic)

付録 E　　トレーサビリティ及び一貫性

トレーサビリティ及び一貫性は、Automotive SPICE 3.1 PAM と同様に、サイバーセキュリティのための Automotive SPICE において、2 つの別個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、又は作業成果物間のリンクを指し、カバレッジ、影響分析、要件の実装状況の追跡等に役立てられる。それとは対照的に、一貫性は内容及び意味について扱う。

さらに、双方向トレーサビリティは、以下の間で明確に定義された。

- 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件/アーキテクチャ設計/ソフトウェア詳細設計と、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
- テストケースと検証結果の間

双方向トレーサビリティ及び一貫性の概要を、次図に示す。

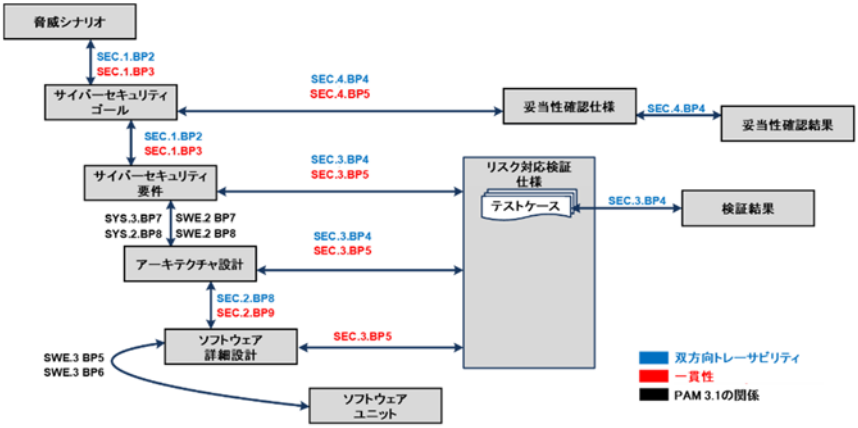

図 5 — 双方向トレーサビリティ及び一貫性