ISSN 2433-2232(Online)
JAXA-SP-18-001
宇宙航空研究開発機構特別資料

IV&V ガイドブック

【導入編】

Ver2.1

発行：2018 年 6 月

はじめに

ここでは、本書の目的、想定する利用者と利用方法について説明します。

本書について

■ 本書の目的

ソフトウェアやシステム開発において高い信頼性を実現する取り組みの一つに、ソフトウェア独立検証と妥当性確認（Independent Verification and Validation：IV&V）があります。

JAXA では、1998 年から IV&V に取り組んでいます。

本書の目的は、JAXA がこれまでの取り組みから得られた知見を公開することで、IV&V を広く普及させることにあります。

■ 想定する利用者と利用方法

本書の想定読者は、以下の方です。

- ソフトウェアまたはシステムの品質要求を定める担当者（IV&V 発注者）
- 高い信頼性が要求されるソフトウェアやシステムの開発担当者（IV&V 発注者）
- 高い信頼性を要するソフトウェアを開発する企業の経営者やプロジェクトマネージャ（IV&V 発注者）
- IV&V を実行する企業の経営者及び担当者（IV&V 実施組織）

本書の利用方法は、以下の場合で手引きとして利用することなどを想定しています。

- 検証と妥当性確認（Verification & Validation：V&V）に基づいてソフトウェアやシステムを開発しているが、より高い信頼性を実現する開発プロセスを新たに検討する場合
- IV&V を聞いたことがあるが、自らが所属する組織、プロジェクトにおいて、どのように IV&V を実施または利用したらよいかを検討する場合
- IV&V の実行にあたり、IV&V に係る概念や用語の理解と共有を促進する場合

■ 免責

本ガイドブックは国立研究開発法人宇宙航空研究開発機構（JAXA）研究開発部門 第三研究ユニットで実施している IV&V の実績を基に構成しています。

本ガイドブックで提供した内容に関連して、ご利用される方が不利益などをこうむる事態が生じたとしても、JAXA は一切の責任を負いかねますので、ご了承ください。

なお、本ガイドブックに対するご意見などがございましたら、IVV_INFO@jaxa.jp までお寄せください。

JAXA について

■ 宇宙航空研究開発機構(JAXA)について

2003 年 10 月、宇宙科学研究所（ISAS)、航空宇宙技術研究所（NAL)、宇宙開発事業団（NASDA）が 1 つになり、宇宙航空分野の基礎研究から開発・利用に至るまで一貫して行うことのできる機関が誕生しました。

それが、国立研究開発法人 宇宙航空研究開発機構（JAXA）です。

JAXA は、「Explorer to Realize」というコーポレートスローガンの下、人類の平和と幸福のために役立てるよう、宇宙・航空が持つ大きな可能性を追求し、さまざまな研究開発に挑みます。

目　次

第1部
IV&V とは何か？

ここでは、ソフトウェア開発に関する基本的な考え方と、一般的に定義されているソフトウェア独立検証と妥当性確認（Independent Verification and Validation：IV&V）について説明します。

1-1 高信頼性ソフトウェア開発の課題

宇宙ステーション、人工衛星、ロケットなどの宇宙機等に搭載されるソフトウェア、または輸送、電力、ガス、水道、放送、金融、及び医療などの社会インフラとして利用されるようなシステムのソフトウェアには高い信頼性が求められます。

万一、ソフトウェアが要求された機能や性能を十分に満たさなかったり、要求された機能や性能が十分であっても不要な機能の混入、異常事態において正しく対応できないなどの欠陥を含んでいると、人工衛星を喪失したり、ミッションを達成できなくなったり、ロケットの打ち上げが失敗するという事故につながる心配があります。

また、社会インフラとして利用されている情報システムやソフトウェアが、何らかの事情から機能しなくなった場合、企業経営に多大な影響を与えるだけでなく、多数の顧客及びシステムの利用者に被害を及ぼし、多くの国民生活に支障をきたすような社会問題に発展する心配があります。

こうした背景の下、これまでソフトウェアを開発する組織において、品質向上に向けた様々な取り組みがなされてきましたが、開発者自身によるデバッグや検証では問題が見落とされる場合があるため、客観的に品質を担保する検証手段が求められています。

客観的に品質を担保する取り組みの一つに、**ソフトウェア独立検証と妥当性確認（Independent-Verification and Validation：IV&V）**があります（下図）。

IV&V とは、ソフトウェアを開発する組織から技術面、組織面、及び資金面で独立している体制で実施する、ソフトウェア検証及び妥当性確認（V&V）です。

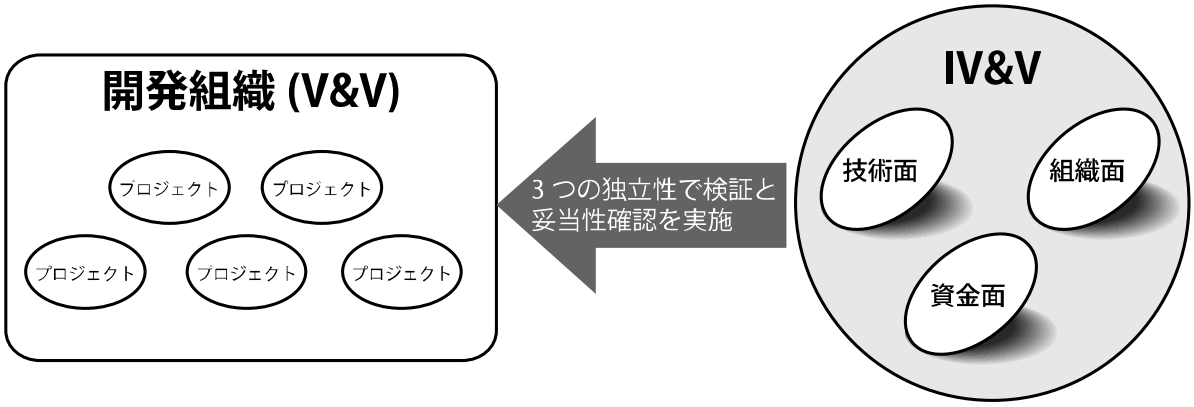


図 1-1　技術面、組織面、資金面独立のイメージ

*doi: 10.20637/JAXA-SP-18-001/0001

1-2 前提知識

ここでは、IV&V について理解するための前提知識として、一般的に定義されているソフトウェア開発プロセスモデルと V&V について説明します。

1-2-1 ソフトウェア開発プロセスモデル

ソフトウェア開発プロセスモデルとは、ソフトウェアを開発するための作業の進め方を定めたものです。

作業の進め方はモデル化されており、ウォータフォール型モデル、インクリメンタル型モデル、スパイラル型モデル、アジャイル型モデルなどがあります。

ここでは、ウォータフォール型モデルに属する V 字型モデルと W 字型モデルを取り上げます。

■ ウォータフォール型モデル

ウォータフォール型モデルでは、ソフトウェア開発は要件定義、基本設計、詳細設計、製作、テストの 5 つのプロセスから構成されます。[Royce 1970]

下図の通り、各プロセスの成果物（アウトプット）が次のプロセスのインプットとなって、開発が進行します。

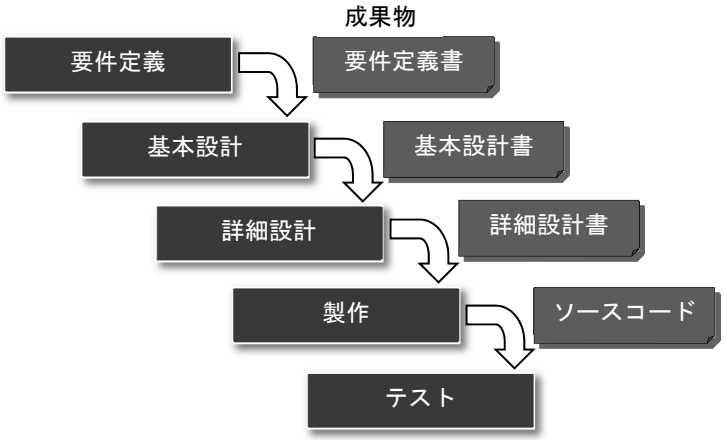


図 1-2　ウォータフォール型モデル

■ V 字型モデル

V 字型モデルは、ウォータフォール型モデルの表現を改良したモデルです。

下図の通り、ウォータフォール型モデルの要件定義、基本設計、詳細設計の各プロセスに対応させて試験プロセスを分割して表現したものが、V 字型モデルです。

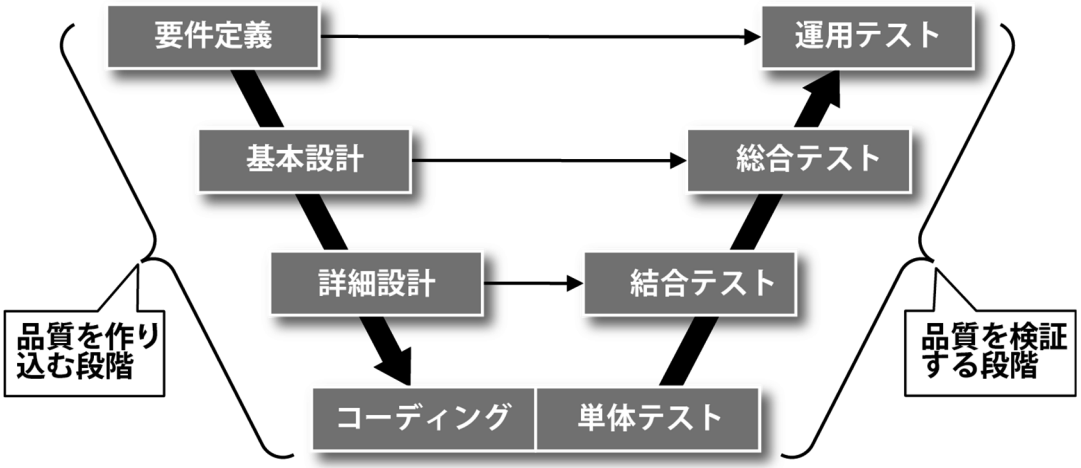


図 1-3 V 字型モデル

V 字型の左部分は「品質を作り込む段階」、右部分は「品質を検証する段階」と位置付けられ左右のプロセスが対応付けられます。

ウォータフォール型のメリットは、時間の流れとともに各プロセスが順番に進むことから、開発全体の進捗、コスト、品質を把握しやすく、マネジメントしやすいことです。また、プロセス単位で外部にも委託しやすく、大規模開発に向いています。

デメリットは、システムが複雑になるほど初期段階での確実な要件定義が難しくなり、後プロセスでの追加や変更による手戻りが発生しやすくなることです。要件定義からシステムをリリースするまでの期間も長くなり、途中で要件が変わってしまうことも少なくありません。

特に要件定義の段階における問題の混入は、開発の最終段階で実施される総合テストや運用時まで発見されることが無く、重大な問題となります。

また、システムの発注者は、一般に、総合テスト後半の段階になって初めてシステムに触れることが多く、要件を満たすシステムになっているか、その時に確認することになります。

この段階で要件に誤りがあると分かり、この誤りを修正しない限りシステムを利用することができないとなった場合、要件の見直しから行わなければなりません。これには、多大な手戻り工数が必要になります。場合によっては、システムリリースのスケジュールを見直さなければいけなくなります。その分、追加のコストも考慮しなければなりません。

■ W 字型モデル

V 字型モデルのデメリットを補えるモデルとして、W 字型モデルがあります。[Gerrard] [Spillner 2002]

下図の通り、W 字型モデルでは、V 字型モデルの右部分のテストプロセスで行われる作業のうち、テスト設計を左部分で行います。

このため、要件定義、基本設計、詳細設計等の各設計プロセスと、運用テスト設計、総合テスト設計、結合テスト設計等の各テストプロセスとが並行して行われることになります。

W 字型のメリットは、開発の初期段階でテスト設計を行うことで、要件や設計の抜け、漏れ、曖昧な点、矛盾点などを見つけることが可能になることです。設計プロセスから、より品質を高めることができます。

デメリットは、設計プロセスで仕様変更が発生した場合、同時にテスト設計の見直しも実施しなければいけなくなることです。V 字型モデルと比較して、見直しの必要な範囲が拡大する可能性があります。

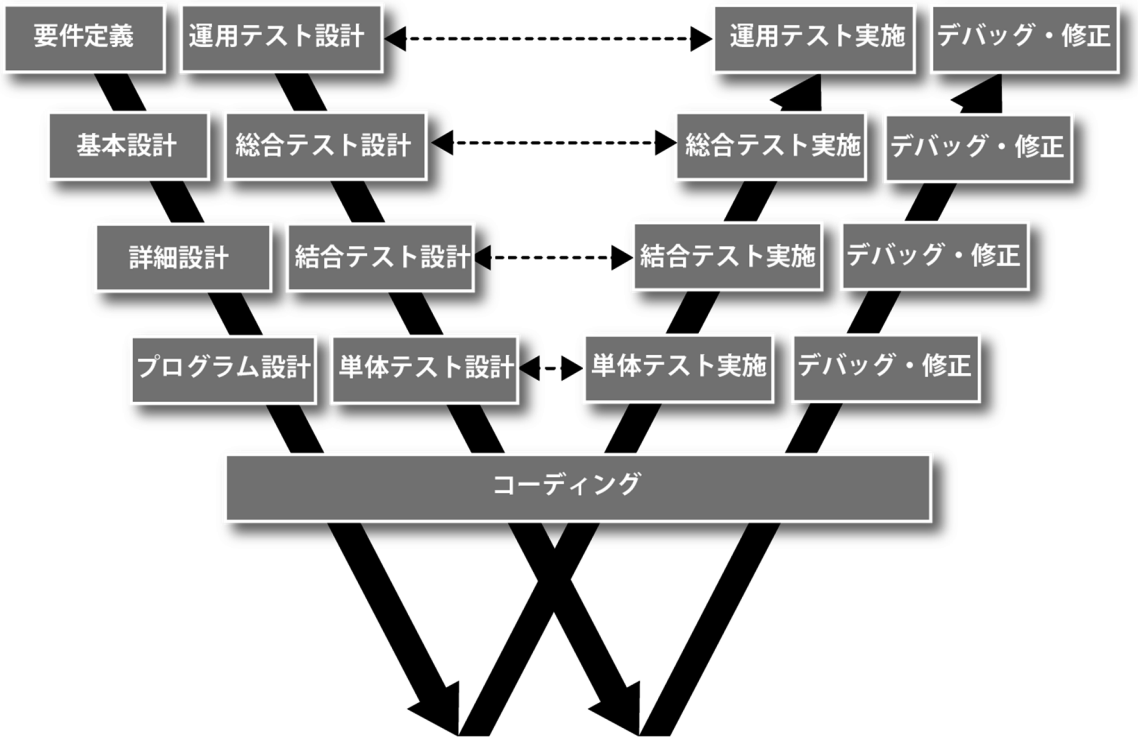


図 1-4　W 字型モデル

1-2-2 V&V とは何か

V&V（Verification and Validation）は、「検証と妥当性確認」と訳されます。

V&V は、製品やサービス、システムなどの品質保証における基本的な考え方の一つです。

要件定義、設計、製作などのプロセスが正しく行われていること、また各プロセスの成果物も正しく作られていることを、検証と妥当性確認という 2 つの視点から評価することです。

それでは検証と妥当性確認とは何か、一般的な概念を、SWEBOK Ver 3.0[SWEBOK 2013] に沿ってそれぞれ説明します。また、検証と妥当性確認の視点から評価される、ソフトウェア品質とは何かを説明します。

■ 検証の意味

検証とは、各プロセスの開発中間成果物が、前のプロセスからの入力情報に照らし、正しく作られているかを確認することです。バリー・ベーム（Barry W. Boehm）は、検証のことを「Are we building the product right?（正しくプロダクト（製品）を作っているか？）」と説明しています。[Boehm 1984]

本書では、Verification を「評価対象ソフトウェアのライフサイクルを通し、上流プロセスの成果物から下流プロセスの成果物への要求トレースが可能であり、それらが内容を含め整合していることを検証すること」と定義しています。

例えば、独立行政法人情報処理推進機構（IPA）が策定した『共通フレーム 2013』“第 3 部共通フレームとガイダンス 2.4.5.1 ソフトウェア構築”[共通フレーム 2013]というアクティビティを例に考えます。

下図の通り、このアクティビティのインプットは、この前の作業「ソフトウェア詳細設計」のアウトプットである『ソフトウェア詳細設計書』です。また、ソフトウェアコードの作成時に参照する『ソフトウェアコード作成標準』もインプットになります。

アクティビティ「ソフトウェア構築」のアウトプットは、「ソフトウェアコード」と「ソフトウェアテスト結果」です。

図 1-5　アクティビティ「ソフトウェア構築」のイメージ

このアクティビティに対して検証することは、次のとおりです。

・ソフトウェア詳細設計書の記述内容が、漏れなくソフトウェアコードに反映されていること。

・ソフトウェアテスト結果が、ソフトウェア詳細設計書の記述内容を網羅していること。

・ソフトウェアコードが、ソフトウェアコード作成標準に適合していること。

■ 妥当性確認の意味

妥当性確認とは、各プロセスの開発成果物がユーザの期待するとおりに作られていることを確認することです。バリー・ベームは、妥当性確認のことを「Are we building right product？（正しいプロダクト（製品）を開発しているか ?）」と説明しています。

本書は、Validation を「評価対象ソフトウェアが最上位要求であるミッション要求、安全要求、運用要求から求められる機能、性質及び品質を満足していることを確認すること」と定義します。

妥当性確認は、開発が完了したソフトウェア最終製品についてだけ行えばよいというものではありません。ソフトウェア要件定義やソフトウェア方式設計といった、より上流プロセスで埋め込まれた欠陥は、ソフトウェア最終製品に、より重大な品質問題を与えてしまいます。

その欠陥を取り除くためには、より上流プロセスで埋め込まれた欠陥であるほど、より多大な修正工数がかかります。

このため妥当性確認は、下図の通り、ソフトウェアライフサイクルの全般を通して、常にソフトウェア製品（中間成果物を含む）が最上位要求に合致しているかを評価することが望まれます。

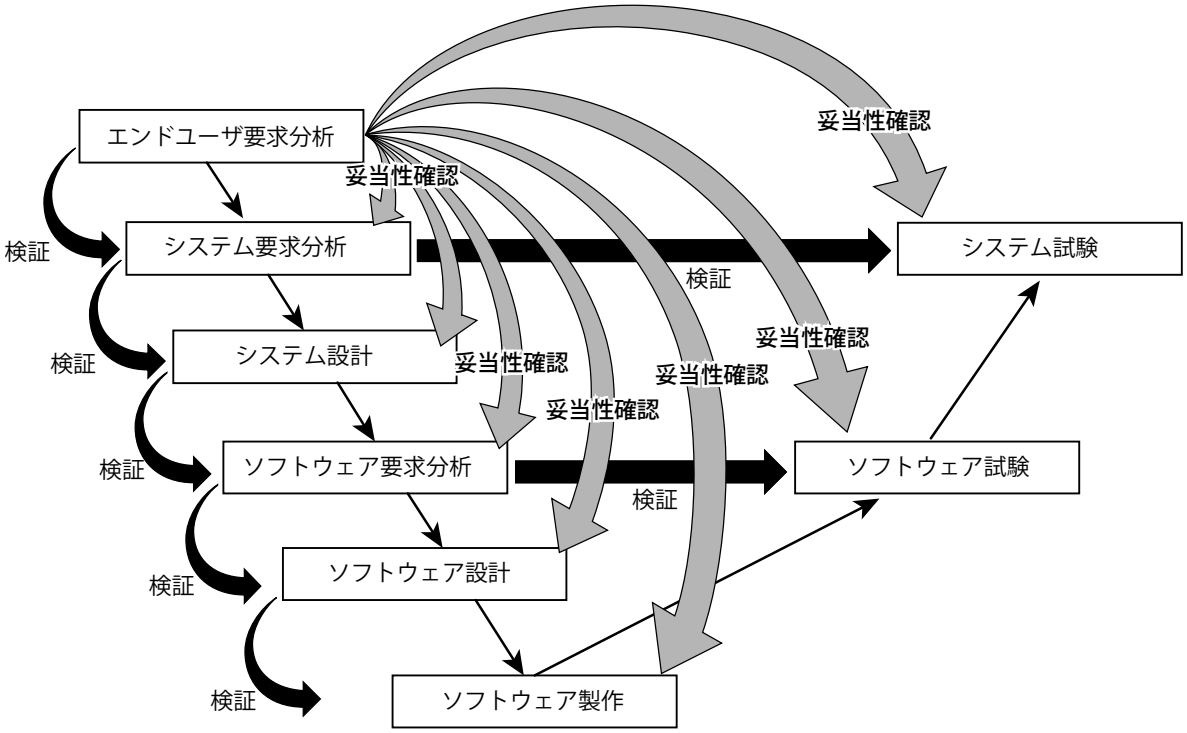


図 1-6　検証と妥当性確認（V&V）のイメージ

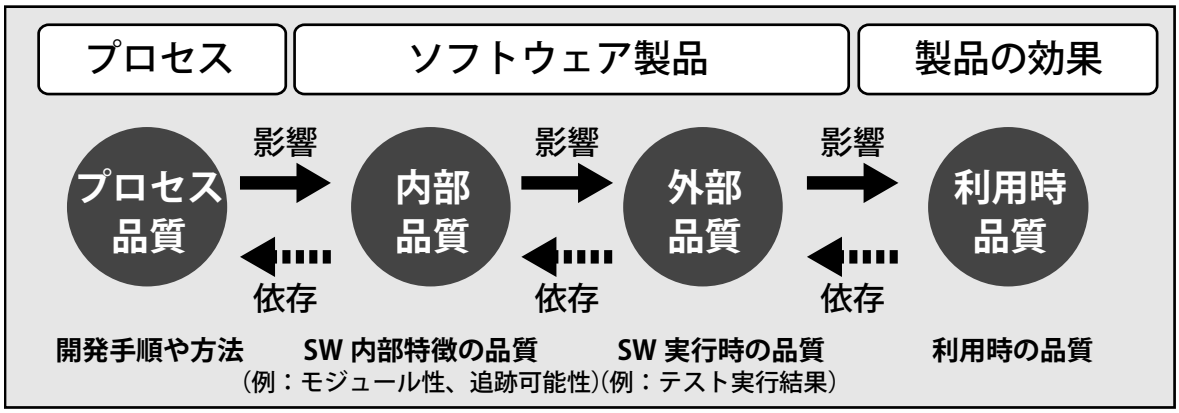
■ V&V の特質

開発の上流段階から V&V を実施することによって、比較的早い段階で欠陥を検出し、除去することができます。上流のプロセスで欠陥を除去することは、開発プロジェクトのリスク、費用、及びスケジュールへの影響を少なくすることができます。

V&V を実施するために必要な技術は、ソフトウェアの試験、レビュー、静的解析、あるいはモデル検査などが挙げられます。

■ ソフトウェア品質

JAXA IV&Vにおいて、ソフトウェアの品質はISO/IEC 25000シリーズ（Systems and software Quality Requirements and Evaluation: SQuaRE）のうち ISO/IEC25010 で定義されている「ライフサイクルでの品質」[ISO/IEC 25010:2011]としてとらえています。



※上図は、JIS-X-25010:2013 P.31 図 C.2 に基づき改変

図 1-7　ISO/IEC25010 ライフサイクルでの品質

上図の通り、ソフトウェアの品質は、プロセス品質、内部品質、外部品質、利用時品質から構成されており、隣接した品質は相互に影響または依存すると考えられています。例えば、プロセス品質（JIS-X-0160[ISO/IEC 12207:2008] で規定されたソフトウェアライフサイクルプロセスの品質等）を改善することは、ソフトウェア製品品質を改善することに貢献します。

先に紹介した V&V は、ソフトウェア製品品質を保証する活動の一つであると考えています。

1-3 IV&V の一般的な意味

IV&V（Independent Verification and Validation）は、「ソフトウェアの独立検証と妥当性確認」と訳されます。IV&V とは、開発プロジェクトから独立した組織が、独立した検証技術、及びソフトウェア開発組織の影響を受けない資金によって、ソフトウェアの課題や問題を洗い出し、潜在するリスクを軽減する活動です。

■ IV&V 活動の目的

IV&V 活動の目的は、システムが致命的な状況に陥る可能性（リスク）を低減させることにあります。すなわち、開発の後工程、もしくは、運用中に検知される欠陥を、より早い段階で抽出することで、開発・運用のリスクを低減させます。

また、ステークホルダー（システム発注者、エンドユーザ）の視点で説明すれば、ステークホルダーが懸念する次の「3 つの問い」に対して、IV&V 実施組織が根拠を示して答えることによって、ステークホルダーに安心を与えることです。以下の「3 つの問い」は米国航空宇宙局（NASA）の IV&V Facility において提唱されています。

3 つの問い：

- ソフトウェアは、意図どおりに正しく振る舞うか？
  Will the system software do what it is supposed to do?

- ソフトウェアは、意図しない振る舞いをしないか？
  Will the system software do what it is not supposed to do?

- ソフトウェアは、不都合な事態に対して、期待どおり振る舞うか？
  Will the system software respond as expected under adverse conditions.

■ IV&V 活動の実施に関連する組織例

次に、IV&V 活動の実施に関連する組織とその相互関係の例を下図と下表で説明します。

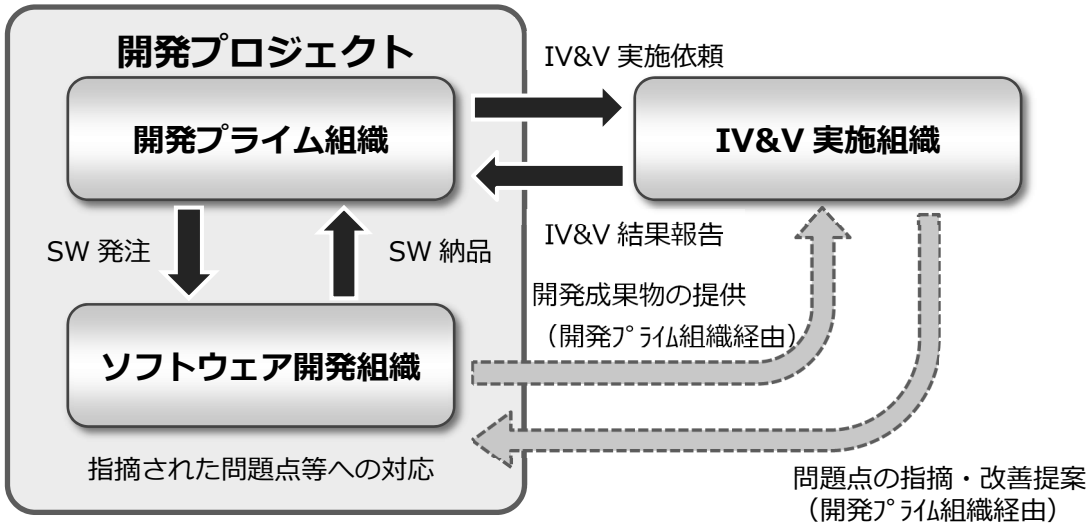


図 1-8　IV&V 活動の実施に関連する組織の関連図

各組織の役割例は下表のとおりです。

表 1-1　各組織の役割例

組織	役割
開発プライム組織	・ ソフトウェア開発の発注者であり IV&V 活動の発注者です。 ・ IV&V 実施組織とソフトウェア開発組織との間の調整窓口となります。 ・ IV&V 実施組織に対して、IV&V 活動に必要な資料や開発成果物（ソフトウェア要求仕様書など）を提供します。 ・ IV&V 活動から発見された問題点、改善提案などの処置に対する最終決定権を有します。
ソフトウェア開発組織	・ ソフトウェア開発の受注者であり、ソフトウェア開発に責任を有します。 ・ 開発プライム組織に対して、IV&V 活動に必要な開発成果物を提示します。 ・ IV&V 実施組織から提示された問題点、改善提案などに対して対処方法を検討して実行します。
開発プロジェクト	・ 開発プライム組織とソフトウェア開発組織を併せた組織体です。
IV&V 実施組織	・ IV&V 活動の受注者であり、IV&V 活動を計画し実施する責任を有します。 ・ 計画に基づき IV&V 評価を実施し、発見された問題点、改善提案などを精査し、開発プライム組織、ソフトウェア開発組織に提示します。

■ 独立（Independent）の意味

IV&V の I（Independent、独立）には、3 つの意味が含まれています。技術的独立、組織的独立、資金的独立です。それぞれの意味を、下表に記載します。

表 1-2　独立のタイプと内容

独立のタイプ	内容
技術的独立	ソフトウェアを評価する IV&V 技術は、ソフトウェア開発組織が使用する検証技術とは別の技術を選択します。
組織的独立	開発プロジェクトから独立した組織が、IV&V 実施組織として責任を持って活動し、開発プライム組織に対して結果を報告します。 IV&V 実施組織は、分析するソフトウェアの範囲、利用する IV&V 技術、活動スケジュール、及び焦点を置く技術的問題点を、独立的に選択します。 IV&V 活動を実施する作業量（工数）は、開発プロジェクトの作業工数から分離していることが重要です。
資金的独立	IV&V 活動を実施するために必要な資金（以下、IV&V 資金）は、開発プロジェクトから独立した組織によって提供されるべきものです。 通常、開発プロジェクトとは異なる組織（本社組織など）が、IV&V 資金の提供元となります。

ソフトウェア開発組織自らが行う V&V では、ソフトウェア発注者（開発プライム組織）の利益とソフトウェア開発組織の利益が一致しません。（利益相反）

なぜならば、ソフトウェア開発組織自らが行う V&V では、設計活動と V&V 活動との間で、人的リソースや資金的リソースの奪い合いが起こり易く、その結果、十分な V&V 活動の実施が妨げられる可能性があるためです。上表の 3 つの独立性のうち、組織的独立と資金的独立は、この利益相反による問題を防ぐために、特に重要な要素です。

なお一般的に、独立性を持った組織が実施する評価の意義としては、下記が挙げられます。

- 品質に対する説得力の向上
- 問題が発生した場合の、責任所在の明確化

■ 参考：IEEE による IV&V の定義について

IEEE1012:2012 Annex C「IV&V の定義」では、「IV&V は 3 つのパラメータ（技術的独立、組織的独立、資金的独立）によって定義される。」としています。[IEEE Std 1012-2012]

さらに、「3 つの独立性パラメータそれぞれの実現程度が、達成される独立性の度合を決定する。」として、「IV&V を実行する組織として、独立性の実現面で数多くの形態があり得る。」と記載しています。また、3 つの独立性の強弱によって区別した 5 種類の形態を記載しています。

表 1-3、表 1-4 を参照してください。

表 1-3　IV&V の 5 形態と独立性の達成度合

IV&V の形態		技術的独立	組織的独立	資金的独立
模範型 IV&V	Classical	◎：厳格	◎：厳格	◎：厳格
緩和型 IV&V	Modified	◎：厳格	○：条件付き	◎：厳格
統合型 IV&V	Integrated	○：条件付き	◎：厳格	◎：厳格
内部型 IV&V	Internal	○：条件付き	○：条件付き	○：条件付き
組込型（V&V）	Embedded	△：最小限	△：最小限	△：最小限

表 1-4　各形態の説明

IV&V の形態	説明
模範型 IV&V（Classical）	模範型 IV&V は、3 つすべての独立性を厳格に守ります。 IV&V の責任は、開発組織とは別の組織に帰属します。 IV&V の評価結果と提案が素早く開発プロセスに反映されるように、IV&V は開発組織と緊密な関係を築きます。 模範型 IV&V は、ソフトウェア完全性レベル 4（生命の損失、任務の喪失、重要な社会的または財政的な損失）を実現するために、通常必要とされます。
緩和型 IV&V（Modified）	開発プライム組織が選定されているような、数多くの大規模な開発プロジェクトでは、緩和型 IV&V が利用されます。 緩和型 IV&V では､元請インテグレータがシステム開発を支援するとともに､IV&V 実施組織を選択し、IV&V 活動結果の報告を受けます。このため、組織的独立性は低下します。 ただし、技術的独立性と資金的独立性は維持されます。 緩和型 IV&V は、ソフトウェア完全性レベル 3（重要な任務と目的）のシステムに適切です。
統合型 IV&V（Integrated）	統合型 IV&V は、開発プロセスに対して IV&V 結果を迅速にフィードバックすることに焦点を置いており､IV&V 実施組織が次のような活動を行うため､技術的独立性に影響を与えます。 ● ソフトウェア開発組織と隣同士で働く。 ● 暫定的な成果物をレビューする。 ● 開発スタッフによって実施されるインスペクションやウォークスルー､レビューを通して、IV&V のフィードバックを提供する。 ただし、独立に関する妥協を最小にするために、開発組織から資金的かつ組織的に独立している組織によって実行されます。
内部型 IV&V（Internal）	内部型 IV&V は、開発者が自組織内の要員（開発作業に直接関与していない要員が望ましい）を使って IV&V を実施する形態です。 当然のこととして、技術的、組織的、資金的な独立性は、低下します。 内部型 IV&V 活動のメリットは、システムとそのソフトウェアを知っているスタッフの存在です。 独立性の程度が明確に宣言されておらず、既存スタッフの知識による利益が、独立性確保による利益を上回る時に、この形態が使われます。
組込型（V&V）（Embedded）	組込型 V&V は、開発者が自組織内の要員を使って V&V を実施するという点で、内部型 IV&V と類似しています。 異なる点は､組込型 V&V が開発手順と開発プロセスへの適合に焦点を置いていることです。 組込型 V&V は、開発プロセスへの V&V 結果の迅速なフィードバックをもたらしますが、技術的、組織的、資金的な独立性は、大幅に低下します。

第2部
JAXA IV&V とは何か

ここでは、JAXA で定義する IV&V（以下、JAXA IV&V）について、説明します。

2-1 JAXA IV&V とは

宇宙機ソフトウェアとは、宇宙空間で利用する人工衛星、ロケット、国際宇宙ステーション等に搭載されているソフトウェア、及び宇宙空間で利用する機器を地上で制御するソフトウェアの総称です。

宇宙機ソフトウェアと同様に高い信頼性が必要な自動車ソフトウェアと、宇宙機ソフトウェアの特徴の比較を示したものを下図に示します。

	宇宙機ソフトウェア 	自動車ソフトウェア 
特徴① 開発サイクル	5年程度	1.5～2年程度
特徴② 開発量	基本1点もの	複数の車種分
特徴③ 開発プロセス	差分開発＋新規開発	差分開発
特徴④ 稼働機器数	1機	何十万台（量産）
特徴⑤ 利用者	訓練されたユーザ	不特定多数のユーザ

図 2-1　宇宙機ソフトウェアと自動車ソフトウェアの特徴の比較

宇宙機ソフトウェアの大きな特徴は、基本的に 1 機分だけを開発する点です。その際、過去の資産を利用した差分開発となる部分もありますが、個々のミッションに応じて新規に開発する部分も多くあります。

また、開発したソフトウェアが実際に稼働する機器数も、基本的に 1 機のみであり、自動車のように数十万台で稼働するソフトウェアとは大きな違いがあります。

これらのことから、宇宙機ソフトウェアの品質に係る特徴について、以下の 2 点が挙げられます。

- ソフトウェア開発過程において、ソフトウェア品質を計測可能な機会が少なく、量産製品がある産業で活用される品質管理尺度（例：欠陥除去率等）の適用効果が低い。

- ソフトウェア本稼働（リリース）後においても、他産業で活用される品質管理尺度（例：顧客満足度や平均故障時間等）の適用が難しい。

宇宙機ソフトウェアは他産業で開発されるソフトウェア（主に量産品）と比較し、品質を確かめることができる機会が少ないことが分かります。そこで、宇宙機ソフトウェアの高い信頼性を担保するために、ソフトウェア開発組織が通常実施する品質確認の機会（例：V&V、開発組織内の審査会等）に加えて、別に品質確認の機会を設けることが解決策としてあります。

宇宙機ソフトウェアの品質を確かめる機会として、様々な方法が適用されていますが、その一つが IV&V です。

2-1-1　JAXA IV&V の目的

JAXA IV&V 活動の目的を端的に言うと、IV&V 活動の発注者に対して、ソフトウェア開発組織が開発するソフトウェアの重要な部分の製品品質（ISO/ICE 25010 ライフサイクルでの品質における内部品質）に関するセカンドオピニオンを提示することから、システムが致命的な状況に陥る等のリスクを低減させることです。

一方で、ソフトウェア開発組織が実施する V&V 活動の主たる目的は、ソフトウェアの発注者に対して、ソフトウェアが要求（プロセスに対する要求及び製品に対する要求の両方）を充足していることを示し、リスクが十分低いことを示すことです。V&V における重要な視点は、「プロセス及び製品の要求に対してなるべく網羅的であること」になる性質があります。

下図に JAXA IV&V と V&V の関係を示します。

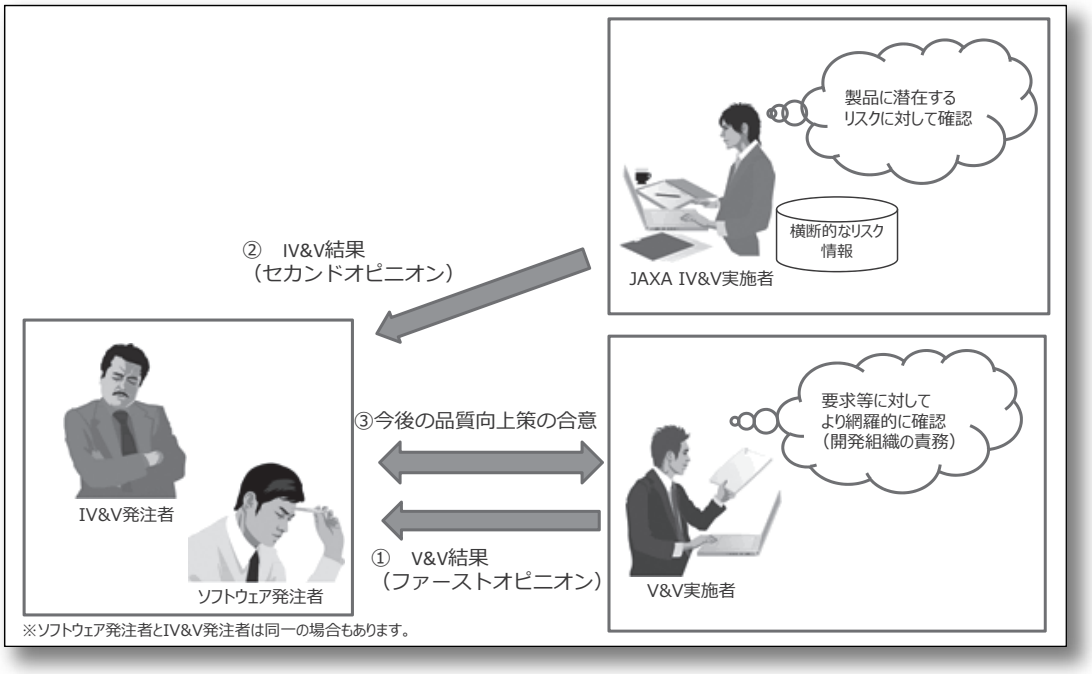


図 2-2　JAXA IV&V と V&V の関係

ソフトウェア開発組織は、開発しているソフトウェアの品質が確保されていることを立証することに責任を有しています。また、ソフトウェア発注者は、ソフトウェアが適切な品質であることを確認し、受け入れることに責任を有しています。

ソフトウェアがどのような品質であるかを開発中に確認する方法として V&V 結果の参照があります。しかし、V&V 結果の参照だけでは品質に対する確信が得られない場合、セカンドオピニオンとして IV&V の実施が一つの選択肢となります。

JAXA IV&V 活動は開発しているソフトウェア品質に対して責任は有しません。ただし、ソフトウェアやシステムが致命的な状況に陥る可能性がないか等のリスクに対して、将来問題が発生しそうか、しないのかを検証した結果に責任を有します。JAXA IV&V で確認した結果は IV&V 発注者に提示され、今後品質向上策が必要かどうかが IV&V 発注者またはソフトウェア発注者により判断され、合意されます。

JAXA IV&V は、セカンドオピニオンとして効果的な活動にするため、上述のようなリスクに基づいた評価（リスクベースドテスト）を実施しています。リスクに基づいた評価とは、問題が潜在する可能性が高い箇所に対してのみ評価を実施することです。つまり、JAXA IV&V では、評価対象ソフトウェアの特徴に応じて抽出した懸念や、過去評価で蓄積された懸念を起点とし、問題が潜在する可能性が高いと識別された特定の機能や処理に対してのみ評価を実施します。

従って、JAXA IV&V は全ての機能に対して検証と妥当性確認を網羅的に実施しているわけではありません。また、JAXA IV&V に限らず IV&V を実施するからといって、V&V が不要になるわけではないことに留意してください。ソフトウェア開発組織が説明責任を有する作業（例：ソフトウェアに対する要件が全て満たされていることの立証等）を、IV&V の作業結果のみを用いて完結させる等、ソフトウェア開発組織のリソース補完のため IV&V を利用することは避けるべきです。

2-1-2　その他の品質保証方法との比較

JAXA における IV&V とそれ以外の品質保証方法との違いを明確にするために一般的に実施されているソフトウェア品質保証方法の説明を下表に示します。

表 2-1　ソフトウェアに対する品質保証方法の説明

No.	品質保証方法	意味
1	アセスメント （一般的に）	・数値による見積もりや定量的評価 ・想定できる事態と影響などの評価 ・改善策を検討するための現状調査
2	アセスメント （ソフトウェア開発）	・ある開発組織のソフトウェア開発プロセスの強みと弱みを分析し、プロセス改善を行う方法、機会、及びリスクを特定した後、プロセス改善の実施に結び付けてゆく活動のこと。 ・分析において、ガイドラインに則っているか否かの判定は、（○/×）ではなくて、程度で判断する。 ・判定が×であっても、改善の実施、または対処の程度については開発組織が単独で判断する。
3	監査（一般的に）	・監督し検査を行うこと。 ・ある活動や業務の遂行方法と成果物が、遵守すべき規則に照らし合わせて、則っているかの証拠を収集し、収集結果から何らかの評価を行い、評価結果を活動組織の統率者に報告する任務のこと。 ・規則違反は（○/×）で判定し、違反は強制力をもって是正させる。
4	受入れテスト （ソフトウェア開発）	・システムが、ユーザのニーズ、要件、ビジネス・プロセスを満たしているかをチェックするための公式なテスト。 ・ユーザ、顧客、その他の認可団体がシステム及びソフトウェアを受入れるかどうかを判定する。
5	V&V （ソフトウェア開発）	・要件定義、設計、製作などの開発プロセスが正しく実施されていること、又プロセスごとの開発成果物が正しく作られていることを、検証と妥当性確認という視点で評価する。
6	JAXA IV&V （ソフトウェア開発）	・3 つの独立性（技術的、組織的、資金的）を伴った検証と妥当性確認のこと。 ・開発プロセス上流から開発成果物を分析して独自にリスクを抽出し、抽出したリスクに対して改良の要否を評価して改善案を提示する。 ・V&V に対するセカンドオピニオンの位置づけの活動。

2-2 JAXA IV&V の効果

2-2-1 JAXA IV&V が可能なこと

■ JAXA IV&V が可能なこと

前節で、JAXA IV&V は「網羅的なバグ出し」ではないこと等を説明しましたが、ここでは JAXA IV&V が可能なことをあらためて下記に示します。

- ソフトウェア製品の品質に関して、実運用時に重大な問題が発生するかもしれない等の不安を払拭すること。

- 標準等への適合の確認のため、ソフトウェアのある特定の機能が、特定条件下で必ず動作することを、論理上あり得ることを基に網羅的に確認すること。

■ JAXA IV&V 実施の前提

ただし、JAXA IV&V を効果的な活動にするためには、以下のような条件が前提として必要になります。

- 評価対象であるソフトウェアについて、一定のプロセス品質が確保されていること。

  【解説】前章では、ISO/IEC 25010[ISO/IEC 25010:2011]のライフサイクルでの品質において、ソフトウェアの製品の品質は、プロセス品質に影響されることを説明しました。JAXA IV&V の確認対象は製品品質であるため、プロセス品質がある程度保証されている必要があります。例として、JAXA が定めるソフトウェア開発標準等に準拠して開発が進められている等が実施の前提となります。

  なお、プロセス品質を確認する手段としては、ソフトウェアアセスメント活動等があります。

- 評価対象のソフトウェアが、ある程度クリティカルな性質であること。

  【解説】ソフトウェア製品の品質は、開発プロセスの管理及び V&V により、要求に対して充足していることはある程度保証されます。IV&V は、開発組織が実施するこれらの品質保証活動に上乗せして実施します。従って、費用対効果を考慮すると、人命やミッションの根幹に係わる等のクリティカルさがあるソフトウェア及びシステムに適用することが望まれます。

- IV&V で得たい期待効果が定められていること。

  【解説】ソフトウェアは、入力する可能性がある全てのパターンを検証し、品質を保証することは不可能な性質を持っています（JSTQB テスト 7 原則より）[JSTQB]。従って、どのようなことを保証したいのか、目標を設定することが重要になります。その目標に対して、V&V や IV&V 等の品質保証手段をアレンジすることが望まれます。

2-2-2　JAXA IV&V が有効な場面

2-2-1 項で示した JAXA IV&V が可能なことについて、JAXA IV&V が有効な活動になる具体的な場面を事例として下記に示します。なお、下記はあくまでも代表的な事例であり、この他にも、個々の開発プロジェクト状況に応じて、有効な場面があることに留意してください。

■ 事例 1

- 場面　：開発組織が実施した V&V の結果はあるが、ミッションの達成に対して現状のソフトウェア品質がどの程度なのか、悪影響はないのか確信が得られない場面。
- 例　：品質に確信が得られないとは、製品に何らかの不安が残っている状態です。
  例えば、類似システムで発生しているような問題が、当該システム及びソフトウェアで発生することがないのか等、製品に対する何らかの不安がある場合、JAXA IV&V のように第三者の目で当該問題が発生しないかを確認することが有効となります。

■ 事例 2

- 場面　：ある特定の利用シーンにおいて、ソフトウェアが必ず意図したとおりに動くことを担保しなければならない場面。
- 例　：ロケットがいかなる場合でも意図したタイミングで緊急停止できるか、人命に係わる装置がいかなる場合でも正しく動作する、または正しく止まるかを、開発組織でだけでなく、第三者が提示するエビデンスからも保証が必要な場合、JAXA IV&V のように第三者の目で当該問題が発生しないかを確認することが有効となります。

■ 事例 3

- 場面　：開発しているソフトウェアに不具合が発生した際、その不具合報告書や対策に関する信頼度が低い場面。
- 例　：開発しているソフトウェアに不具合が発生し、その不具合に対する処置をしたにも関わらず、再度不具合が発生する等があった場合、その開発組織の視点のみでは視点が不足していて、同じような問題を繰り返す可能性があります。そのような場合、JAXA IV&V のように第三者が独自に不具合分析や対処候補を提示することは、別の視点が入ることで改善が期待されます。

2-2-3 JAXA IV&V の限界

先の節では JAXA IV&V で可能なことを解説しました。ここでは IV&V で実施できないこと、IV&V の限界についてリソース、プロセス品質の側面から解説します。

■ リソースによる限界

- 繰り返しになりますが、ソフトウェアは全てのパターンを検証し、品質を保証することが不可能な性質であるため、IV&V ではより重要な箇所に対する、部分での確認が前提となります。
- 第三者がシステムやソフトウェアの前提を理解を要するためには、オーバーヘッドコストが必ず発生するため、IV&V は高コストという特性があります。システムやソフトウェアの前提理解のための一定コストがなければ、効果が発揮できないことが多いです。

■ プロセス品質による限界

- JAXA IV&V はプロセス品質ではなく、製品品質の確認をスコープとしています。プロセス品質がある程度確保されなければ、評価の実施ができません。例えば、ソフトウェア開発成果物がソースコード以外ない状態では、費用対効果を最大限に発揮することはできません。

2-3 JAXA IV&V のポイント

2-3-1　JAXA IV&V が満たすべき要件

■ 要員に係る要件

【要件】

全ての IV&V 要員は、対象ソフトウェアの開発を担当していないこと。また、所属する組織の直近の決裁権者が、対象ソフトウェア開発組織における末端の決裁権者と異なること。

【解説】

IV&V を実施する上で、IV&V 要員が評価対象ソフトウェアの問題を指摘した後、IV&V 発注者及び開発組織において適切な対応がとられる必要があります。例えば、IV&V 要員がソフトウェア開発組織と同じ組織にいることにより、問題を適切に受領してもらえない、対応してもらえない等の状況となることを避けるため、上記のような要件を設定しています。なお、決裁権者の権限は、人的リソース割当を決定する権限またはソフトウェアの設計内容の決定権限とします。

■ 技術に係る要件

【要件】

評価計画において評価対象、評価範囲、評価目的等を客観的に説明可能な手段を用いて明示すること。また、評価結果において、評価項目ごとに問題がないと判断された理由（あるいは問題がなかった理由）がエビデンスと共に明確であること。

【解説】

一般的に、第三者による評価を効果的なものにするためには、主観的な評価結果ではなく、客観的な評価結果を示すことが望まれます。JAXA IV&V では、評価対象、評価範囲、評価目的等の評価計画と、その結果を客観的に明示する手段の 1 つとして、GSN（Goal Structuring Notation）という手法を適用しています。手法の詳細は、JAXA 技術文書 「PEB-15042 IV&V 検証フレームワークにおける基準書（IV&V ガイドブック実践編にて掲載）」を参照してください。

2-3-2 開発フェーズごとでの留意事項

ソフトウェアの欠陥は、開発の早い段階で発見できれば、開発の後期段階で発見した場合と比較して、低コストで修正できます。JAXA IV&V をどのように、いつ利用するのか、マイルストンごとに見直し、効果的に活用することが重要です。

ここでは、宇宙機開発の各フェーズごと[JAXA 2007-1]に JAXA IV&V を企画、進行する上での留意事項を説明します。ソフトウェア開発フェーズのイメージを下図に示します。

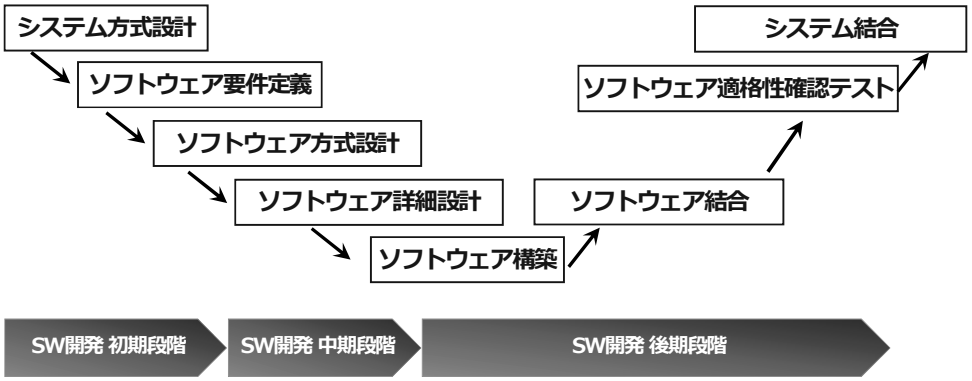


図 2-3 ソフトウェア開発フェーズのイメージ

■ ソフトウェア開発の初期段階（要件定義~方式設計周辺）

ここでのソフトウェア開発の初期段階とは、JAXA で定義する開発マイルストンのシステム PDR（基本設計審査）までのフェーズと位置付けます。

【留意事項】

- システム開発のごく初期段階では、どのソフトウェアを JAXA IV&V 実施の対象とするか、しないか理由が見いだせないため、全ソフトウェアが対象となりがちですが、確定していることが少ない開発初期段階では自然なことです。その後の開発マイルストンごとに、実施判断を繰り返す必要があります。
- ただし、ソフトウェアに関する大まかな情報がそろうシステム PDR の周辺までには、当該ソフトウェアの規模、過去の資産がある場合の流用量、複雑さ、システムにおける役割を識別する必要があります。そこから、求められる品質や、その保証がどの程度必要なのか想定する必要があります。

■ ソフトウェア開発の中期段階（詳細設計周辺）

ここでのソフトウェア開発の中期段階とは、JAXA で定義する開発マイルストンのシステム CDR（詳細設計審査）周辺のフェーズと位置付けます。

【留意事項】

- 遅くともソフトウェア詳細設計を開始する段階では、JAXA IV&V の実施要否判断が下り、実施する場合はその準備が進められている必要があります。
- JAXA IV&V は、IV&V が指摘した問題や改善案を開発組織が修正可能なタイミングまでに完了することが望まれます。

■ ソフトウェア開発の後期段階（構築（製造）～評価（試験））

ここでのソフトウェア開発の後期段階とは、システム引渡し前の試験を実施している状態を想定しています。

【留意事項】

- 開発の後期段階では、IV&V で識別された問題に対する適切な対処を開発組織がとりにくいため、開発後期での IV&V の効果は低い場合が多くなります。よって開発の中期段階で IV&V を実施することが望まれます。

2-3-3 IV&V 活動における組織対応の留意事項

IV&V 活動の実施に際して、IV&V 実施組織が留意すべき事項を説明します。

■ ソフトウェア開発組織への対応

- ソフトウェア開発組織（またはシステム開発組織）と IV&V 実施組織の秘密保持契約の締結や情報開示に係る調整等業務環境の整備に係る労力が必要なことに留意する。
- 開発組織には極力、負荷をかけないように留意する。
（開発組織に影響を与えると、品質が下がる恐れがある。）
- 開発成果物の開示について、方法、期間、場所、及びその他制約を実施以前によく調整する。
- IV&V 活動は開発活動の代行でないことを認識し合い、開発作業や V&V の品質が下がらないように注意する。
- IV&V で指摘した問題への対策は一つに固執せず、柔軟に調整すること。

■ IV&V 実施組織の内部

- 開発担当の負荷を軽減するよう心がけること。
（例：IV&V を行うために、開発者の負担を強いる資料作成を要求しない。）
- 評価対象システムの機能、特徴、運用方法について学習する。
- 時間的制約に対応するために、評価項目には優先順位をつけて、高順位項目から実施する。
- IV&V で指摘した問題に対して、可能な範囲で複数の対応策を提示すること。

■ 開発プライム組織への対応

- 下記のような IV&V に対するマネージャ層の理解とコミットメントが重要である。
「ソフトウェア開発組織の責務で実施しなくてはいけない作業の代替手段ではない。」
「開発プロセスの評価でなく、開発される製品の評価である。」
「バグ出しや問題を見つけるのみの作業ではなく、リスク回避及び安心のための作業。」

2-4 JAXA IV&V の流れ

2-4-1 JAXA IV&V 実行体制

JAXA IV&V 作業を実行するためには、具体的な体制を整備する必要があります。

下図に体制の一例を示します。

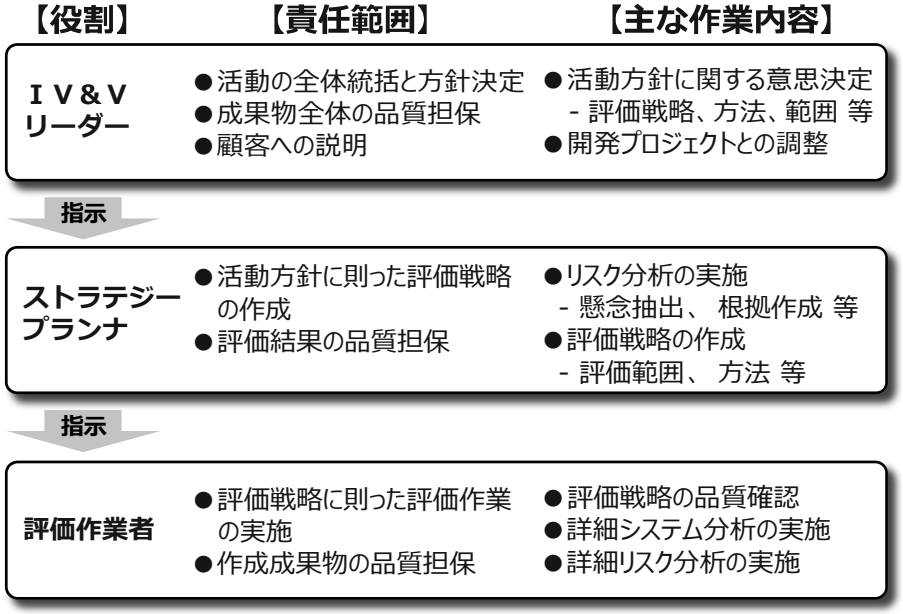


図 2-4　IV&V 作業の実行体制の例

IV&V 活動全体を統括する【IV&V リーダー】を筆頭に、リスク分析とシステム分析を行う

【ストラテジープランナ】、及び実際に評価作業を行う【評価作業者】を配置します。

【ストラテジープランナ】は、作業規模等に応じて、過去の不具合の分析による懸念抽出等のリスク分析を通して評価戦略を作成します。

【評価作業者】は【ストラテジープランナ】が作成した評価戦略の品質を確認するとともに、検証に必要な詳細なシステム分析やリスク分析を通して、指定された成果物を作成します。

各技術者の主な担当作業と必要なスキルは、下表のとおりです。

表 2-2　IV&V 実施技術者の種類と必要なスキル

技術者の種類	必要なスキル
IV&V リーダー	・プロセス管理 ・IV&V 見積もり ・計画策定
ストラテジープランナ	・システム分析 ・リスク識別 ・評価戦略策定
評価作業者	・各検証のノウハウ ・静的コード解析等

※必要なスキルの詳細については、「実践編」をご覧ください。

なお、図 2-4 で示した体制は理想的な体制であり、常にこのような体制を構築する必要があるわけではありません。

小規模な IV&V 活動では、IV&V リーダーとストラテジープランナが兼務するなど、少人数で実施体制を構築するのが現実的です。

なお、評価戦略の客観性担保のため、少なくともストラテジープランナと評価作業者は兼務しないことが望まれます。

2-4-2 IV&V プロセスの全体構成

IV&V 活動を PDCA サイクルで表現した時の全体構成、及び対応するプロセスを下図に示します。

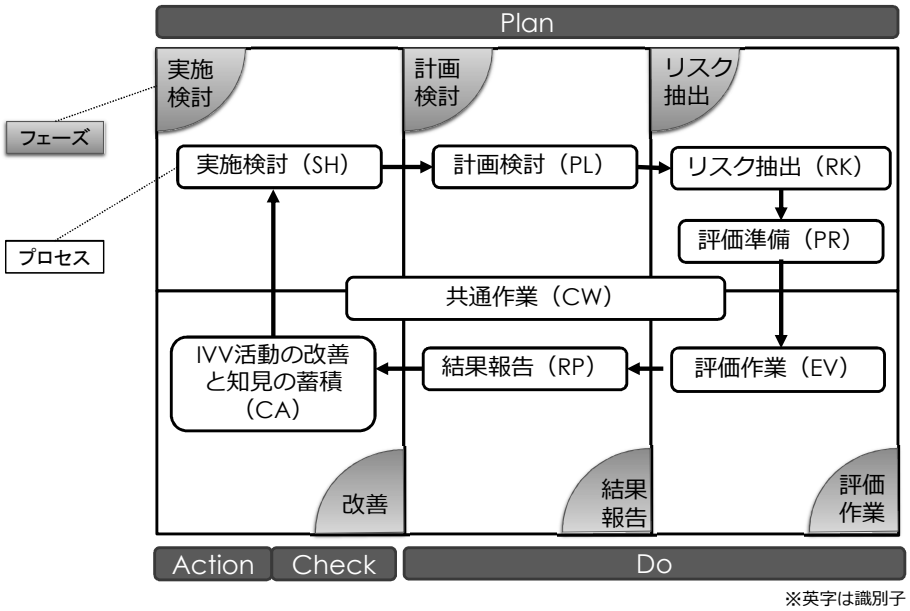


図 2-5　PDCA サイクルで表現した IV&V 活動のプロセス全体構成

上図に示すとおり、IV&V のフェーズは、Plan に対応する「実施検討」「計画検討」「リスク抽出」、Do に対応する「評価作業」「結果報告」、Check 及び Action に対応する「蓄積改善」の、6 つに分類できます。各フェーズには 1 つないしは 2 つの IV&V プロセス、また各フェーズによらない共通的な IV&V プロセスの、合計 8 つの IV&V プロセスが定義されています。

2-4-3 各プロセスの概要

ここでは、プロセスの概要を説明します（下表）。各プロセスや ID 等の詳細については、IV&V ガイドブック実践編を参照ください。

表 2-3 IV&V プロセスの概要

ID	プロセス名称	概要
SH	実施検討プロセス	当該開発プロジェクトにおいて、IV&V 活動を実施するか否かを検討、判断する。本プロセスは、IV&V 発注者によって実施される。
PL	計画検討プロセス	該当プロジェクトで IV&V 活動の対象とするソフトウェア成果物や、その実施規模を確定する。
RK	リスク抽出プロセス	IV&V 活動が検証する「リスク」を、開発プロジェクトの情報等から抽出し、IV&V 検証戦略を作成する。
PR	評価準備プロセス	リスク分析及びシステム分析によって抽出したリスクに対応して作成した「検証戦略」を基に、評価対処成果物の選定、評価観点の選択、体制の構築、及び環境（場所、パソコンなど）の手配を行う。
CW	共通作業プロセス	各フェーズに依存せずに実施する、進行管理を行う。
EV	評価作業プロセス	検証戦略に基づき、分析表やツールを用いて各懸念に対する評価作業を行う。
RP	結果報告プロセス	ステークホルダに対し、評価報告書の作成や報告会を開催し、IV&V 活動の結果を報告する。
CA	IV&V 活動の改善と知見の蓄積プロセス	IV&V 活動の価値を向上させるため、IV&V 活動で活用する不具合情報、実績情報の収集、及び IV&V 活動プロセスの改善を行う。

2-5 実施要否判断

2-5-1　実施要否判断で考慮すべき要素

ここでは、前述の実施検討（SH）プロセスにおいて行われる、JAXA IV&V を実施することが有意であるかの判断の際に考慮すべき要素を紹介します。実施要否を判断をする際には、当該開発プロジェクトで開発するソフトウェア各々に対し、これらの要素を組み合わせて考慮し、総合的に判断することが望まれます。なお、下記は IV&V を実施する上での有意性を判断する指標であり、プロセス品質が担保されているか等の実現性は別途考慮する必要があります。

■ ソフトウェア利用時の影響

システムやソフトウェアを利用している際、問題が発生した場合に与える影響の大きさを考慮します。なお、宇宙機システムのソフトウェアの場合、問題が発生した場合に与える影響が小さくなる事は稀です。

【判断要素の例】

- 宇宙機システムのミッション及び各サクセスクライテリアに与える影響の大きさ。
- システムやソフトウェアが安全に与える影響の大きさ。影響の大きさを分類する方法として、ソフトウェア安全リトマス試験基準（NASA-STD-8739.8 NASA Technical Standard: Software Assurance Standard Appendix 参照）等がある。[NASA-STD-8739.8]

■ 開発プロセスの特徴

ライフサイクルでの品質（ISO/IEC25010）のとおり、ソフトウェア製品の品質は、プロセスの品質に依存するため、開発プロセスの特徴を考慮します。

【判断要素の例】

- 開発組織の宇宙機開発の経験、プロダクトラインの成熟度合。
- 開発体制の複雑さ。複数の開発企業で開発を進める場合や、国外等に開発メンバーが分散している場合等が複雑な体制にあたる。
- 開発環境の充実度合い（例：検証のための環境シミュレータが充実）。

■ ソフトウェア製品の新規性とその規模

ソフトウェア製品に新規開発部分が多く含まれる場合、問題が混入する可能性が高くなります。また、レガシー部分に対して、新規開発部分の割合が低い場合でも、新規開発部分の規模が大きい場合は問題が入り込む可能性が高くなります。

【判断要素の例】

- 技術成熟度（TRL：Technology Readiness Level）。詳しくは、「JAXA 技術成熟度（TRL）運用ガイドライン」[JAXA 2007-2]や TRL に係る NASA ホワイトペーパーを参照すること。
- 新規開発部分のソースコード行数、またはレガシー部分に対する割合等。

■ ソフトウェアの品質確認機会

仮に、利用時の環境を模擬できる検証環境を開発組織において実現できる場合、IV&V ではなく検証環境を利用したテストを充実させる活動によりコストをかけることが望ましい場合もあります。

一方で、システムの本稼働まで実機での検証ができない性質がある場合、第三者による評価がより重要となります。

このように、どの程度検証しやすいソフトウェアであるかを考慮する必要があります。

【判断要素の例】

- V&V で利用する検証環境の有無や、模擬が可能な範囲。
- ソフトウェアが実際に稼働するまでに、実機で振る舞いを確認可能な手段の有無。

■ ソフトウェアの複雑さ

一般的に、ソフトウェアは複雑であるほど問題が入り込む可能性が高くなるとともに除去するのも難しくなります。

【判断要素の例】

- ソフトウェア製品としての複雑さ　：ソフトウェアの作りが複雑であるか。例えば、ソフトウェアの構造が複雑に作られており、サイクロマチック複雑度等の指標が水準よりも高い等が挙げられる。
- ソフトウェアの役割としての複雑さ　：システムを利用する際の、ソフトウェアの役割が複雑であるか。例えば、データを機器から機器へ通信する目的のソフトウェアは役割として単純だが、機器を操作するためにフィードバック制御を行いかつ異常を監視するようなソフトウェアは複雑な役割を担っている。

2-5-2　実施要否判断の事例

■ 事例：衛星システムの事例

ここでは、衛星システムに搭載する 2 つのソフトウェアのうち、どちらのソフトウェアに IV&V を適用すれば有意かを総合的に判断した事例を下表に示します。

この事例では、新規開発部分がより大きく、ソフトウェアの役割がより複雑な「姿勢制御ソフトウェア」を IV&V 実施対象としました。

なお、この姿勢制御ソフトウェアのように、検証環境で振る舞いを模擬できない部分がある特徴をもつソフトウェアの場合、IV&V では、動的テストが難しい部分の評価を、静的テスト手法（レビューやモデル検査等）を用いて、重点的に行います。

また、IV&V 実施対象外としたソフトウェアに対しても、IV&V は実施しないが、その他のどのような品質確認機会を利用してリスクを低減していくのかをプランニングすることが大切になります。

表 2-4　IV&V 実施要否判断のための総合評価

判断要素		姿勢制御 ソフトウェア	データ処理 ソフトウェア
要素 1	ソフトウェア利用時の 影響	**大** 問題が発生した時に、衛星喪失の可能性がある。	**大** 問題が発生した時に、衛星の状況を正確に把握できない場合がある。
要素 2	開発プロセスの特徴	**懸念低** 経験豊富なチームが開発。	**懸念低** 経験豊富なチームが開発。
要素 3	ソフトウェア製品の 新規性とその規模	**中** 新規開発部分は 2 割程度だが、新規コードが 2 万行を超える。	**小** 9 割以上がレガシー。
要素 4	ソフトウェアの 品質確認機会	**中** 検証環境の機器制約により確認できない振る舞いもある。	**大** 検証環境を用いて ソフトの振る舞いの確認が可能。
要素 5	ソフトウェアの複雑さ	**大** フィードバックループ制御により、機器を制御する。	**小** 入力データを指定のコンポーネントへ送信する。
総合判断		**IV&V 実施対象**	**IV&V 実施対象外** ※ただし、開発組織の試験ケースの設定の仕方を重点的に確認する活動を開発に組み込む。

第3部
JAXA IV&V 活動の事例

ここでは、JAXA IV&V 活動の流れを、事例を用いて説明します。

事例で紹介された作業は、IV&V ガイドブック実践編で詳細に定義しています。適宜ご参照ください。

3-1 姿勢軌道制御ソフトウェアの事例

ここでは､前章で IV&V の実施判断をした姿勢軌道制御ソフトウェアを事例に IV&V 作業の流れと、作業において特に重要な点（IV&V で評価するリスクと IV&V 活動の改善）を紹介します。

■ 衛星システムにおける姿勢軌道制御ソフトウェア

人工衛星の本体を「人」に例えると、姿勢軌道制御系は「目」の役割を担っていると言われています。

姿勢軌道制御系は自身の位置や向きを推定するセンサーを持ち（例：スタートラッカ)、目標とする姿勢、軌道へ動くためのアクチュエータを制御します（例：内蔵されているリアクションホイールやスラスタ)。衛星本体とセンサー等のイメージを下図に示します。

姿勢軌道制御系において、姿勢軌道制御ソフトウェアは、センサーからの入力情報を処理し、目標姿勢や軌道を計算し、アクチュエータへの指令値を出力することが一般的な役割です。また、衛星システムに異常が発生した際に、電力確保のために太陽方向へ向く等、安全な姿勢になるよう制御する役割もあります。

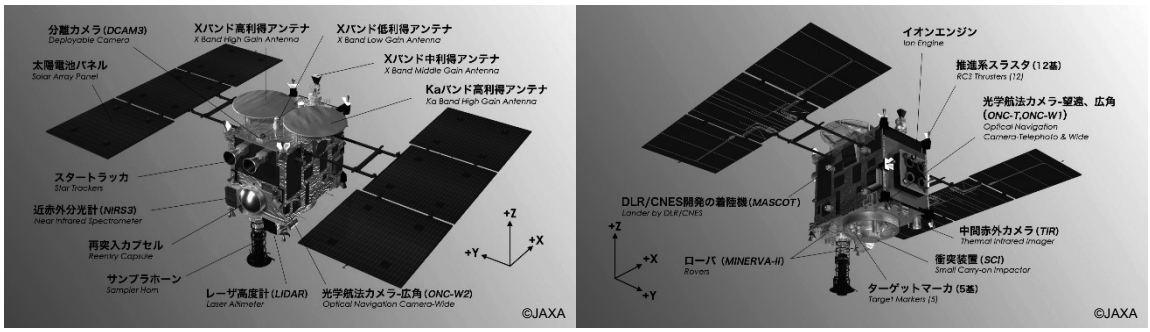


図 3-1　衛星本体と搭載機器のイメージ（はやぶさ 2 より）

■ 姿勢軌道制御ソフトウェアの特徴

- 人工衛星は地上から常に監視することが出来ないため、姿勢軌道制御はソフトウェアによって自律的に行われる部分がある。
- 目標姿勢の決定、推定、アクチュエータ駆動量の演算は、どの程度姿勢が動いているのかのトレンドデータ（前回値やカルマンフィルタ）を保持し、値の更新をすることが多い。
- センサーのキャリブレーション等のために、姿勢をダイナミックに動かす制御をすることがある。
- 目標姿勢・軌道に入るためにアクチュエータを駆動させる演算は、複数のセンサーからの値を入力とする。多くの大型人工衛星の場合、センサーの故障、値の欠損、ノイズの重畳が発生しても、代替手段等を用いて演算を継続する。
- 衛星システムに異常な状態が発生した時（例：発電量の低下等)、太陽方向等の安全な姿勢になるようにソフトウェアは制御し、安全な姿勢を保持する。

3-1-1　作業の流れ

ここでは、IV&V 作業の流れを概要で説明します。

作業は前章で紹介した IV&V プロセスに準じて進められます。ここでは実施判断（SH）は既に完了し、IV&V を実施すると判断された後の流れについて説明します。また、定常的に実施する進行管理である共通作業（CW）も本説明から除外しています。

以下の説明中に示される ID（例：PL-DPO-1000）は、IV&V プロセスではタスク ID と呼ばれ、詳細な手順は IV&V ガイドブック実践編で定義されています。適宜参照してください。

1. 計画検討（PL）

- IV&V をどのように実施するか、具体的な実施方針等の計画を定め、IV&V 実施組織は IV&V 発注者と合意します。実施方針には、情報の開示条件の調整も含みます。
- 姿勢軌道制御ソフトウェアの場合、当該衛星システムで重要なミッションは何か、ミッション失敗や衛星喪失に関わる姿勢制御ソフトウェアの役割があるかを分析し（PL-DPO-1000：IV&V 対象の選定）、実施方針を作成します（PL-DPO-2000：IV&V 実施方針の作成）。

2. リスク抽出（RK）

- IV&V において検証する「リスク」を開発成果物、参考資料、及び開発プロジェクト情報から抽出し、評価戦略を作成します。
- 姿勢制御ソフトウェアの場合、システム分析やリスク分析を実施し、抽出された懸念事項をリスク導出経緯とし（RK-RSK-4000：リスク導出経緯の作成）、懸念をどのように検証するかの計画を検証戦略として GSN 形式で作成します（RK-VSC-1000：リスクに対する検証戦略の作成）。

  【システム分析の例】センサー、アクチュエータ、ソフトウェアの関係をコンポーネント図として整理し、ソフトウェアに対する懸念点を抽出する（RK-SA2-2000：コンポーネント図の分析）

3. 評価準備（PR）

- IV&V を実施するための具体的な評価計画書を作成します（PR-EPL-1000：IV&V 実施計画書の作成）。

4. 評価作業（EV）

- リスク抽出（RK）または評価準備（PR）で作成した検証計画を基に、評価作業を実施します。続いて、IV&V 評価作業で識別した問題点（指摘及び申し送り事項）の一覧を整理した資料作成し、開発プライム組織とソフトウェア開発組織間で処置結果の確認を行います（EV-DPO-1000：指摘（問題点）の提示）。

5. 評価報告（RP）

- IV&V の評価・問題点の識別・処置結果の確認が終了した後、IV&V 活動全体を総括します（RP-R2S-1000：ステークホルダー向け評価報告会の開催）。

6. IV&V 活動の改善と知見の蓄積（CA）

- 今後の IV&V 活動をより良くするため、製品の特徴と懸念情報の蓄積を行います（CA-ACC：IV&V 知見の蓄積）。また、IV&V 終了後に製品に不具合が発生した場合、IV&V での見逃し分析等を行い、懸念情報の充実を図ります（CA-ANA-2000：IV&V 見逃し分析）。

3-1-2 IV&V で評価するリスクの例

前章で説明したとおり、宇宙機ソフトウェアにおいて、IV&V は品質確認の機会の一つとして利用します。従って、V&V 等の他の品質確認機会と同じ視点で評価するのではなく、なるべく異なる視点で評価を実施することにより、効果を発揮します。

異なる視点で、効果的な評価を実施するためには、より鋭い視点で製品の重要な部分や懸念を捉えることが必要です。では、より鋭い視点とはどのようなものなのでしょうか？

■ 製品特徴と懸念

製品の重要な部分を鋭く捉えるためには、当該製品が他製品と比較してユニークな部分を捉える必要があります。ここでは、製品のユニークな部分を「製品特徴」と呼んでいます。

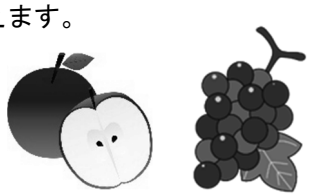
この製品特徴に対して、様々な角度から懸念を考えることにより、より鋭い視点で懸念を捉えることが可能になります。

製品特徴のイメージを、「りんご」と「ぶどう」を例として説明します。

りんごもぶどうも同じ果実で、軸があり、果肉があります。しかし、腐っていないか等、食用としての基本的な要求以上のりんごの良さ／悪さ、またはぶどうの良さ／悪さを判断するためには、軸や果肉という果物一般に言える切り口のみでは難しいのが分かります。

例えば、ぶどうの良さを判断する要素として、果実の粒と粒同士の間隔があります。粒同士の隙間がない方が良いぶどうとされているそうです。ぶどうはりんごと比較して、房なりで粒が付くことがユニークであり、このユニークな点に着目することでより深い評価をすることが出来ます。

この、他のものと比較した時の差分を、ここでは「製品特徴」と呼んでいます。製品特徴とは、言い換えると、他の部分とは異なるユニークな保証が必要な部分とも言えます。



■ 姿勢軌道制御ソフトウェアの例

図 3-2 に姿勢軌道制御ソフトウェアのリスクの例を示します。

電力枯渇による衛星喪失を避けるためには、何らかの異常が発生した時に、姿勢軌道制御ソフトウェアでは電力を確保する姿勢を取るというのが共通的な価値観としてあります。

しかし、当該衛星システムでは、以下のような製品特徴があると仮定します。

- 姿勢軌道制御のうち、軌道制御がミッション達成において非常に重要な役割を担っている
- 軌道制御は高頻度で継続的に実行され、制御のためにソフトウェアが駆動させる機器は消費電力が大きい。

衛星システムの一般的な価値観や、これらの製品特徴を組み合わせながら懸念を検討すると、図 3-2 の SW リスク「バッテリ残量が少ない状態での運用中に、万が一何らかの異常が発生した時、姿勢制御ソフトウェアが要因で電力枯渇に至る懸念」等が抽出されます。

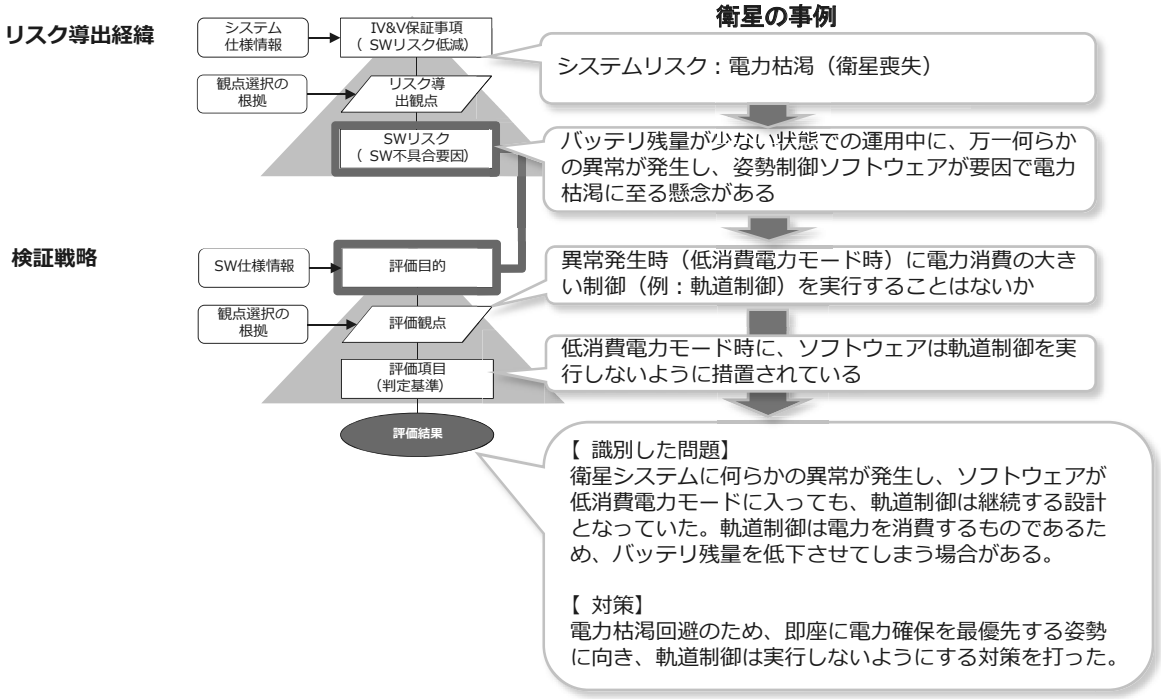


図 3-2　姿勢軌道制御ソフトウェアでのリスク例

なお、JAXA IV&V では、評価対象とする懸念や、懸念に対する検証計画は、図 3-2 のように各々リスク導出経緯と検証戦略で表現されます。リスク導出経緯と検証戦略は、GSN の形式で表現された図で、検証スコープを可視化し、客観性を担保する手段の 1 つとなります。

開発組織による V&V は、様々な要素を組み合わせた試験を、現実的なリソースの中で実施することが大変難しい性質があります。一方 IV&V は独立的な立場であるため、V&V で担保されていること以外の範囲で、製品にとって重要な特徴や懸念を組み合わせてサンプリングで評価することが出来ます。

図 3-2 の例では、電力確保も軌道制御もシステムとして重要な要素（特徴）であることが分かります。しかし、開発組織で双方の要素を組み合わせて試験する機会があったとしても、開発の終盤になってしまうことが予想されます。ソフトウェアの設計段階で、第三者の目で改めて電力確保と軌道制御どちらの方が優先されるべきなのか、実際の設計ではどちらが優先されているのかを明らかにすることにより、早い段階で問題を検出し、対処できる可能性があります。

3-1-3 IV&V 活動の改善の例

前節で説明したとおり、JAXA IV&V は製品特徴に着目し、懸念を抽出します。

ただし、製品特徴や懸念の抽出には一定の開発経験、あるいは IV&V での経験が必要となります。また、IV&V は組織的に実行する活動であるため、個人の経験だけでなく、組織的な知の蓄積により再現性を持つことが大切です。

そこで、IV&V 活動をより良くするため、継続的な製品特徴、懸念等の知見の蓄積が重要になります。継続的な知見の蓄積を行い IV&V 活動を改善することで、以前は視点として入っていなかった特徴や懸念が、次に IV&V を実施する時には考慮することが可能になります。

■ 姿勢軌道制御ソフトウェアの例

知見の蓄積のためにはまず、当該 IV&V 活動で評価した製品上の懸念や特徴を確実に把握することが必要です。例えば、前節の製品に関わる特徴や懸念は、下図のフレームワークを用いて整理することで、明確にすることが出来ます。下図のフレームワークを JAXA では保証構造図と呼んでいます。

保証構造図は、リスク導出経緯や検証戦略で表現された情報が、ソフトウェア製品の保証関係にどの程度貢献しているか表現している図です。IV&V は「開発プロセス」ではなく「開発成果物」を評価する活動であるため、保証構造図の基本的な構成はソフトウェアの入力、処理、出力の流れによって構成されています。入力、処理、出力に対して、負の事象（機器損失や情報の損失）を引き起こす阻害要因や変動要因（評価の視点）をマッピングし、保証関係を表現します。

これにより、IV&V 活動でソフトウェア製品に対して保証した範囲が表現できます。保証構造図の詳細は、IV&V ガイドブック実践編を参照してください。

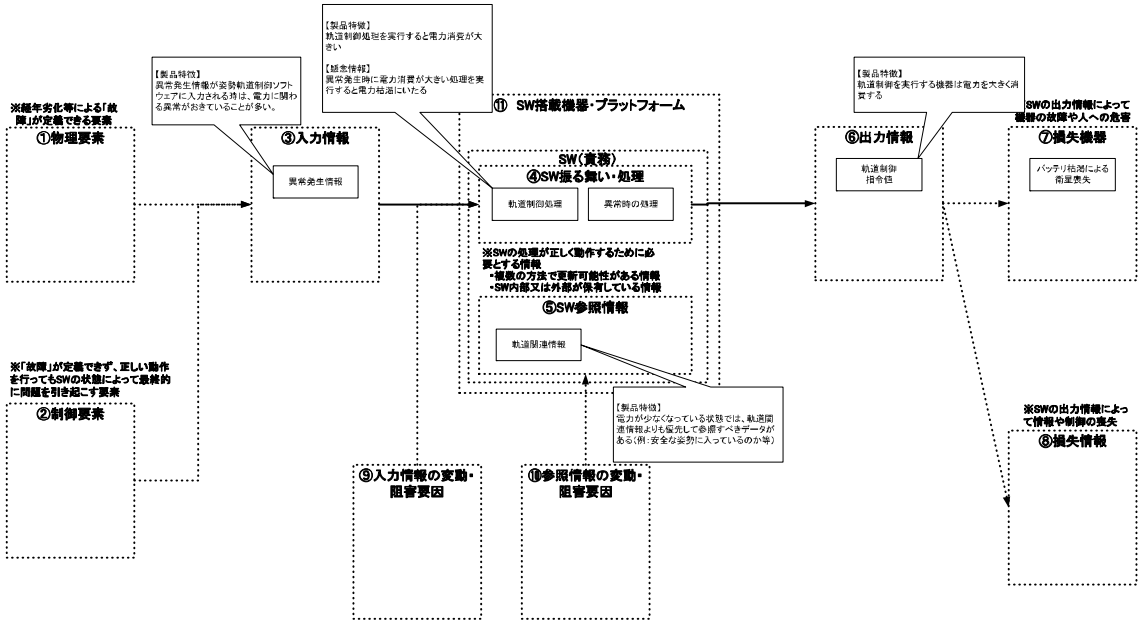


図 3-3 姿勢軌道制御ソフトウェアで評価した製品上の特徴と懸念（保証構造図）

また、IV&V が完了した後に実施した開発組織による試験で不具合が発生した時、なぜ IV&V で見つけることが出来なかったのか、どのような視点を持っていれば見つけられたのかを分析し、知見として加えることも重要です。

第4部
JAXA IV&V で利用する用語

ここでは、JAXA IV&V において独自に定義して利用している用語について説明します。JAXA IV&V で利用する用語の多くは、JSTQB（Japan Software Testing Qualifications Board : http://jstqb.jp/）において定義されている用語を参考にしていますので、あわせて参照ください。[JSTQB]

4-1 検証及び妥当性確認に係る用語

ここでは、検証及び妥当性確認に係る用語について、ソフトウェアテスト業界での一般的な定義（解釈）と対比しつつ、JAXA IV&V での定義（解釈）について解説します。

■ 欠陥及び故障の定義

JAXA IV&V の活動目的は、ソフトウェアの「故障」が顕在化する前に、「故障」の原因となる「欠陥」を取り除き、「故障」が発生する確率を十分低減させることです。

ここでの、「欠陥」と「故障」の意味は JSTQB [JSTQB]の定義に準じており、図式化すると下図のようになります。

「欠陥」とは、「コンポーネントまたはシステムに要求された機能が実現できない原因となる、コンポーネントまたはシステムに含まれる不備」と定義されています。

また、「故障」とは、「コンポーネントやシステムが、期待した機能、サービス、結果から逸脱すること。」と定義されています。

プログラムの実行中に「欠陥」に遭遇すると「故障」を引き起こします。

「欠陥」を取り除くためには、ソフトウェア詳細設計書等のソフトウェア開発成果物（テストベース）を基に、「テスト対象（テストしたいもの）」と「テスト条件（テストしたいこと）」を適切に抽出することが重要です。

「テスト条件」とは、「コンポーネントやシステムのアイテムやイベントで、テストケースより検証できるもの。たとえば、機能、トランザクション、フィーチャー、品質の属性、構造要素など。」と定義されています。

JAXA IV&V のテスト条件は「リスク」であり、リスクを捉える視点として、検証の視点と妥当性確認の視点を使い分けています（次項）。

なお、「リスク」については、次節において解説します。

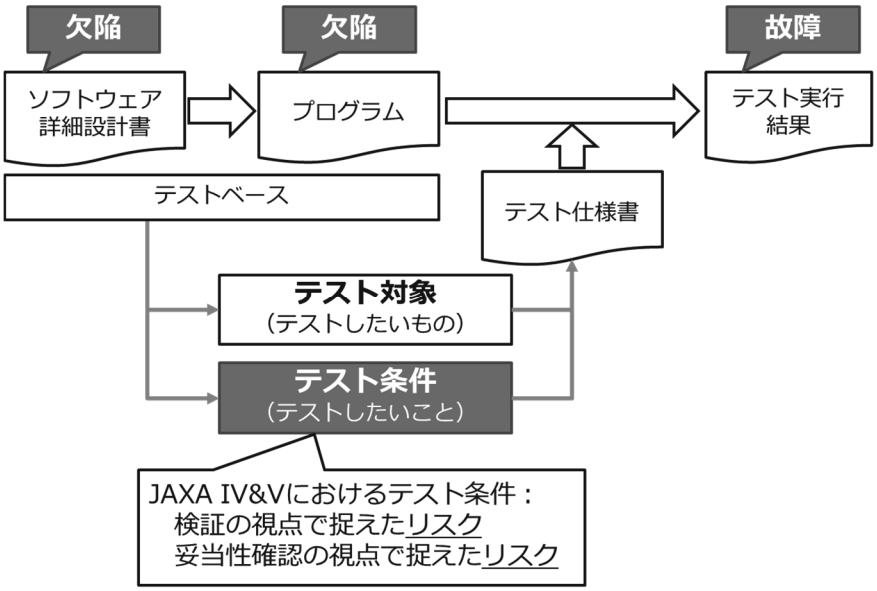


図 4-1　欠陥、故障、テスト条件の対応関係

■ JAXA IV&V における検証及び妥当性確認の定義

「検証」と「妥当性確認」の一般的な定義は、前章に示しています。ここでは、JAXA IV&V における定義（解釈）を解説します。

JAXA IV&V における検証と妥当性確認の解釈を図式化したものを下図に示します。「検証」と「妥当性確認」は、テスト条件を抽出する際の視点であると JAXA IV&V では捉えています。

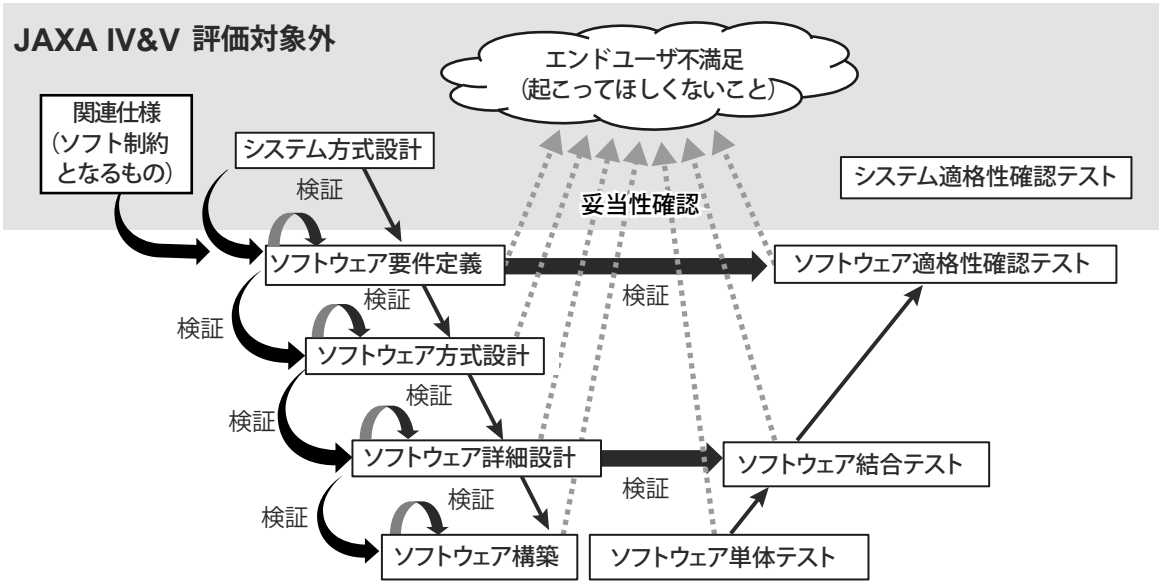


図 4-2　JAXA IV&V における検証と妥当性確認の解釈

●検証

一般的な定義と同様、各プロセスの開発中間成果物が、前のプロセスからの入力情報に照らし、正しく作られているかを確認する行為としています。ただし、JAXA IV&V では、ソフトウェア要件定義の前プロセス（システム方式設計）だけではなく、ソフトウェアに対する制約となり得る関連情報や仕様も評価の起点として利用します。また、ソフトウェアに対する制約の中には、JAXA IV&V において独自に抽出したリスクが含まれます。

●妥当性確認

一般的に、妥当性確認とは、各プロセスの開発成果物がユーザの期待するとおりに作られていることを確認することと定義されています。しかし、IV&V を実施する組織は独立組織であるため、開発組織と比較してユーザ要求に関する情報の入手が難しいことが多いという特徴があります。

また、JAXA における宇宙機開発では、開発期間が長期にわたることが多いため、開発当初に分析していたユーザ要求が変わっている場合があります。このような不確かな情報を起点とし、妥当性確認を実施しても、効果的な活動にならない可能性が高くなります。

そこで、JAXA IV&V では、IV&V 活動を通して得た検証結果やソフトウェア仕様等の確かな情報を評価の起点とし、ソフトウェアがエンドユーザの不満足を引き起こす問題を含んでいないか確認することを妥当性確認と解釈しています。

ただし、システムに対する安全要求等、万人にとって確かなエンドユーザ要求が存在する場合、一般的に定義されている妥当性確認の考え方を用いて評価することで、十分効果的な活動が可能です。

4-2 リスクに係る用語

前章で、JAXA IV&V はリスクに基づいた検証及び妥当性確認の活動を行っていると説明しましたが、「リスク」という言葉は様々な用途で利用されています。ここでは、「リスク」の一般的な定義と、JAXA IV&V におけるリスクの意味合い、また関連する用語について解説します。

■ リスクの一般的な定義

「リスク」は様々な標準等で定義されていますが、主なものを以下に挙げます。

- ISO 31000：2009（JIS Q 31000：2010） [ISO 31000：2009]
  ：「目的に対する不確かの影響」
- JSTQB ソフトウェアテスト標準用語集 日本語版 Version2.3.J01 [JSTQB]
  ：「将来、否定的な結果を生む要素。通常、影響度と発生可能性として表現する。」

■ JAXA IV&V におけるリスクの意味合い

JAXA IV&V における「リスク」とは、「将来、製品の問題となる可能性があること」を意味します。

しかしながら、上述したように、「リスク」という用語には様々な定義があり、用途や聞き手によって様々な解釈がなされ、誤解が生じる可能性があることから、JAXA IV&V では、IV&V の進行（IV&V ライフサイクル）及び問題が発生する可能性の確度に応じて、呼び方を変えています（図 4-3）。

このことは、IV&V で扱う問題の確度の状況を共有し、作業を円滑にするためという目的もあります。

IV&V ライフサイクルの各段階での「リスク」の呼称について、次節で説明します。

■ JAXA IV&V におけるリスクに関連する用語

●評価前

この段階でのリスクは「懸念候補」と呼びます。

この時点でのリスクの確度は最も低く、プロジェクトのミッションや構成品目から発生し得るあらゆるリスクを想定している状況を表します。

●評価時

リスクは「懸念」と呼びます。

この時点でのリスクは、「懸念候補」に対し、実際のシステム仕様やソフトウェア仕様を確認した結果、起こり得る可能性が十分想定できる状況を表します。

●評価結果作成時

リスクは「問題」と呼びます。

「懸念」であったものが、IV&V での評価を行ったことにより、是正処置をしない限り、確実に将来不具合になることが分かっている状況であることを表します。

●評価報告時

リスクは「指摘」または「提言」と呼びます。

IV&V 発注者に説明する際、是正処置の優先度を高く設定する必要がある「問題」を「指摘」、当該ソフトウェアに是正処置は不要と判断されたが、改めてシステム視点での再確認や、確実な運用準備を推奨する「問題」を「提言」として提示します。なお、IV&V プロセス上「提言」は「申し送り事項」と表現しています。

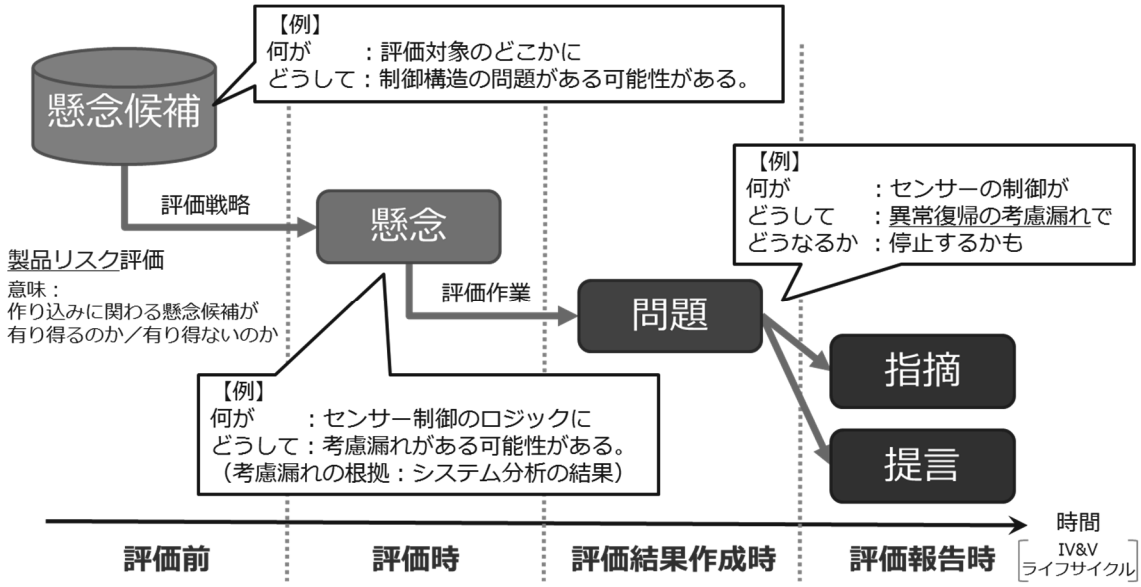


図 4-3　IV&V ライフサイクルでの「リスク」の呼び方の違い

参考文献

［Royce 1970］ Winston Royce, Managing the Development of Large Software Systems, Proc. of IEEE WESCON, 1970

［Gerrard］ Paul Gerrard, Introducing the W - Model, http://www.gerrardconsulting.com/?Q=node/531

［Spillner 2002］ Andreas Spillner, The W - MODEL - Strengthening the Bond Between Development and Test, STAREAST, 2002

［SWEBOK 2013］ SWEBOK V3.0, Guide to the Software Engineering Body of Knowledge, IEEE Computer Society, 2013

［Boehm 1984］ Barry W. Boehm, Verifying and Validating Software Requirements and Design Specifications, IEEE Software, 1(1984), pp. 75–88.

［共通フレーム 2013］ 独立行政法人情報処理推進機構 共通フレーム 2013～経営者、業務部門とともに取組む「使える」システムの実現～ 2013 年

［ISO/IEC 12207:2008］ ISO/IEC 12207:2008 Systems and software engineering - Software life cycle processes (JIS X 0160:2012 ソフトウェアライフサイクルプロセス)

［IEEE Std 1012-2012］ IEEE Std 1012-2012 IEEE Standard for System and Software Verification and Validation

［ISO/IEC 25010:2011］ ISO/IEC 25010:2011 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models (JIS X 25010:2013 システム及びソフトウェア製品の品質要求及び評価 (SQuaRE) - システム及びソフトウェア品質モデル)

［JSTQB］ JSTQB (Japan Software Testing Qualifications Board), JSTQB テスト技術者資格認定,ソフトウェア標準用語集 (日本語版) Version 2.3.J01 http://jstqb.jp/index.html

［JAXA 2007-1］ (JAXA 社内文書) BDB-06007B システムズエンジニアリングの基本的な考え方 2007 年

［NASA-STD-8739.8］ NASA (National Aeronautics and Space Administration), NASA-STD-8739.8, NASA Technical Standards System (NTSS), https://standards.nasa.gov/standard/nasa/nasa-std-87398

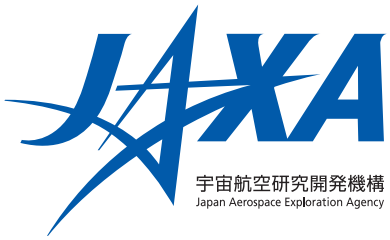
［JAXA 2007-2］ (JAXA 社内文書)BDB-06005A JAXA 技術成熟度 (TRL) 運用ガイドライン 2008 年

［ISO 31000：2009］ ISO 31000：2009 Risk management -- Principles and guidelines

宇宙航空研究開発機構特別資料　JAXA-SP-18-001
JAXA Special Publication

M&V ガイドブック　【導入編】　Ver2.1

発　　行　　国立研究開発法人 宇宙航空研究開発機構（JAXA）
〒182-8522　東京都調布市深大寺東町7-44-1
URL: http://www.jaxa.jp/
発　行　日　　平成30年6月29日
電子出版制作　　松枝印刷株式会社


JAXA
宇宙航空研究開発機構
Japan Aerospace Exploration Agency