ソフトウェア独立検証と有効性確認（IV&V）における観点の策定
- IV&Vガイドブックの紹介 -

宇宙航空研究開発機構
情報・計算工学センター
川口 真司

本発表の狙い

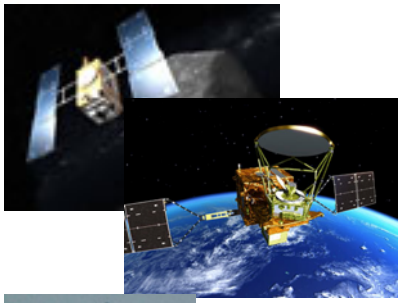
- ソフトウェアの信頼性・安全性を高める一つの手段として「ソフトウェア独立検証と有効性確認（ソフトウェアIV&V）」があることを知っていただき、IV&Vを皆さまのフィールドで活用・応用することを検討いただきたい。

- 世の中にIV&V技術を発表してフィードバックをいただくことで、当方の技術改善を図りたい。

このプレゼンテーションでは・・・

- IV&Vガイドブックを余すことなくご紹介・・・するには時間が足りない。
  チェックする価値があるかどうかを判断いただく情報を提供できれば。

宇宙機システムと搭載ソフトウェア

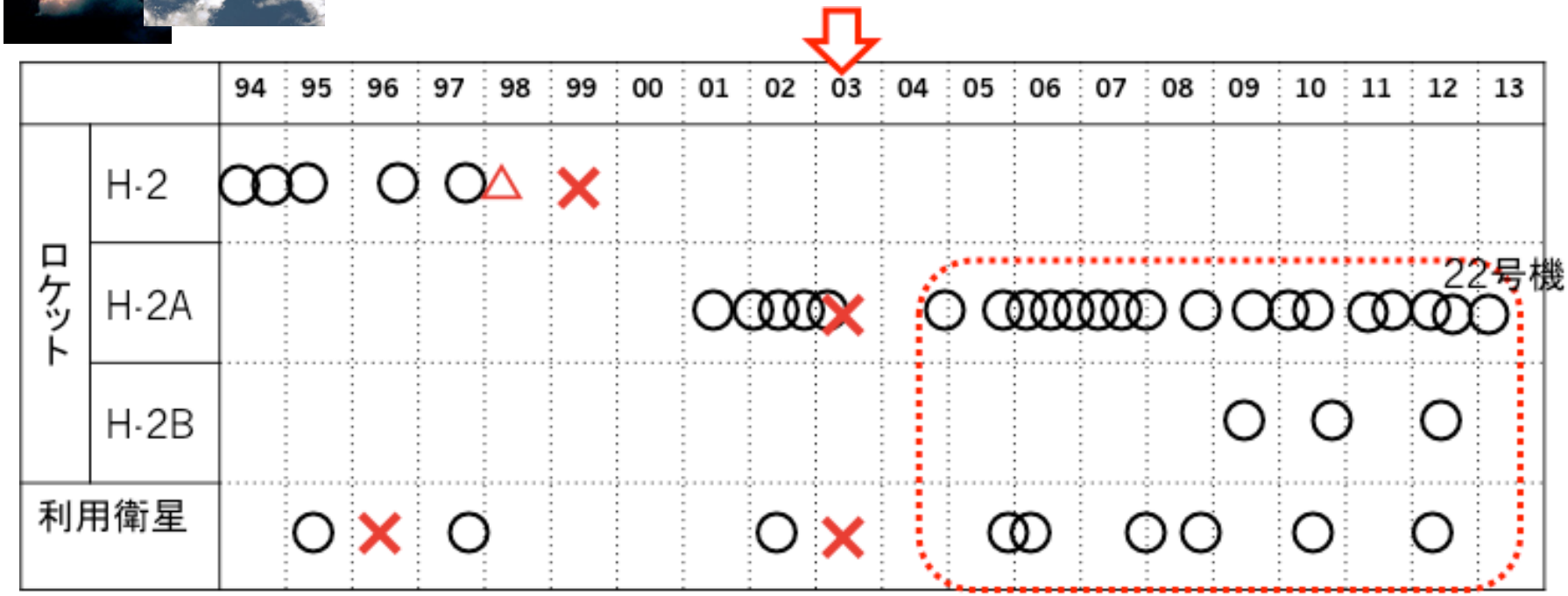


人工衛星（しずく、はやぶさ２、・・・）

バス系（姿勢制御、データ処理）　→　生き残るための安全化、故障検知回復機能
ミッション系（データ処理・装置制御）　→　社会インフラに必要なサービスの継続

輸送機（*H-IIA/B*、イプシロン、こうのとり）

航法誘導制御　→　飛んでいく方向を決める制御、多数決判断
→　衝突回避機能、故障検知・回復機能



宇宙機搭載ソフトウェアの特徴

ソフトウェアテストの観点から見た

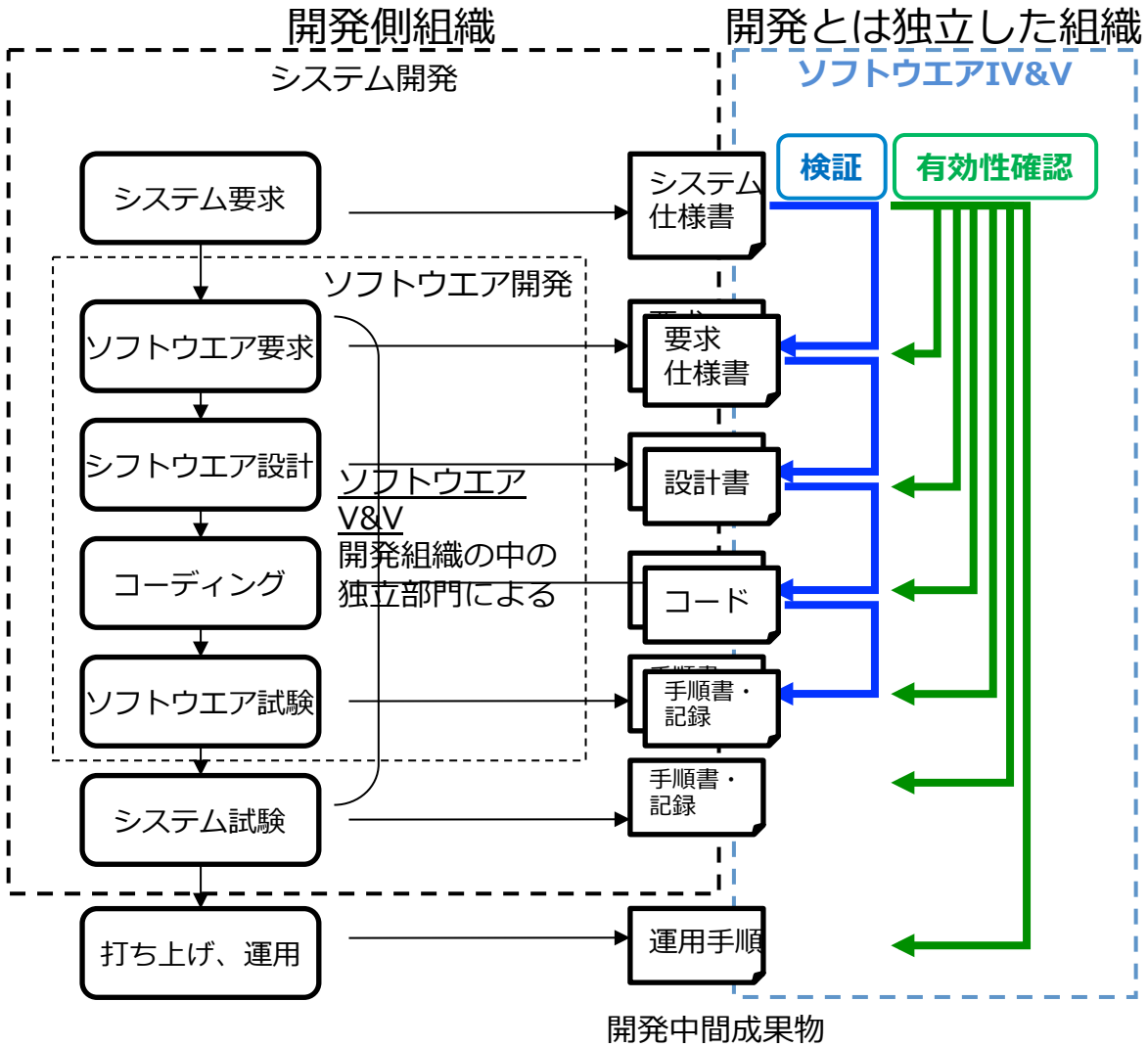
- ソフトウェアの誤動作により多大な損失が発生しうる。
  - もしロケットが打ち上げ失敗した場合、ロケットや搭載物（HTV、衛星等）の損失だけでなく、最悪の場合は環境の汚染や人命・財産の喪失にもつながりうる。

- システムの動作環境が過酷。
  - 太陽電池の電力で駆動するが、日陰のため発電できない時間帯が存在する。
    - 万一バッテリーが尽きたら。
  - 地球との通信が常に可能とは限らない。
    - 運用上の不可視帯、一時的な姿勢変更によるビットレート低下。
  - 放射線によるメモリ化けが発生する。

- 部品交換不可。
  - 基本的にハードウェアは予備（冗長系）を搭載している。
  - 故障対応が複雑。
- 故障対応も含めて自律的に動作“しなければならない”箇所がある。
  - 例：一時的に通信できない状況下で故障が発生したときの対応。

ソフトウェアIV&Vとは

製品の**正しさ及び品質**をライフサイクルを通して評価するための**システムエンジニアリングプロセス**



- 経済的、管理的、技術的独立性が必須
- IV&V活動は、ソフトウエアの開発工程（要求設定～試験）のすべての段階で実施
- 開発側が作成するソフトウエア中間成果物（文書、データ）を各開発工程において解析・評価

- 作業は以下の２つの観点からなる。

Verification(検証)

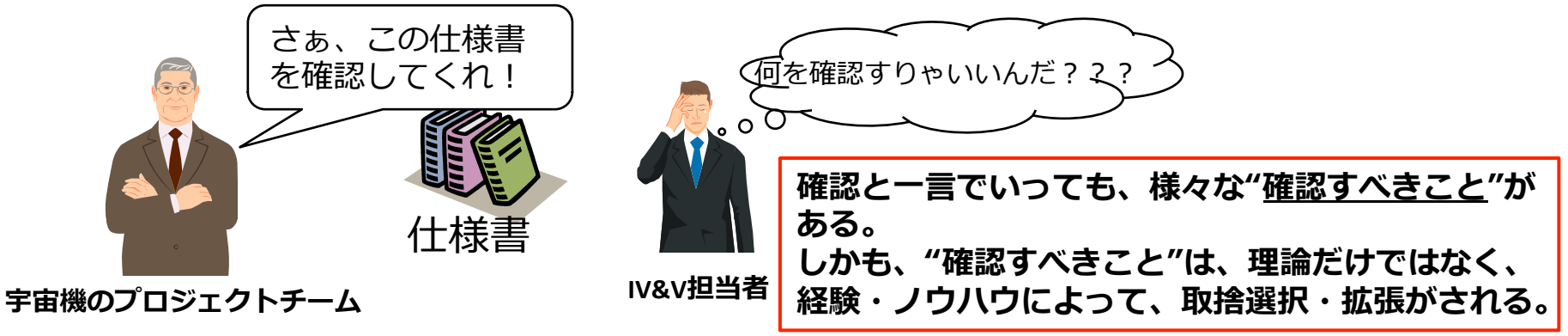
各段階の開発中間成果物が、**前の工程からの入力情報に照らし、正しく作られていること**を確認

Validation(有効性確認)

各段階の開発中間成果物が、**最上位要求通りに作られていること**を確認

IV&Vガイドブックを作成した動機

- IV&Vは「ソフトウェアの仕様書、ソースコードに問題がないか確認」をするが・・・



- そこで、“確認すべきこと”をまとめたIV&Vガイドブックを作成。

IV&Vガイドブックの概要

- 主に「IV&V評価観点」（What to check）と個々の「詳細観点の概要」（How to check）から構成される。

- IV&V評価観点は、指摘事項を見つけ出す時の「起点」として使うことを想定している。
  - 出てきた問題点は、複数の観点により発見されうるが、これはそういうものだと割り切る。（指摘が見つからないよりはダブるほうがずっといい。）

5観点の概要

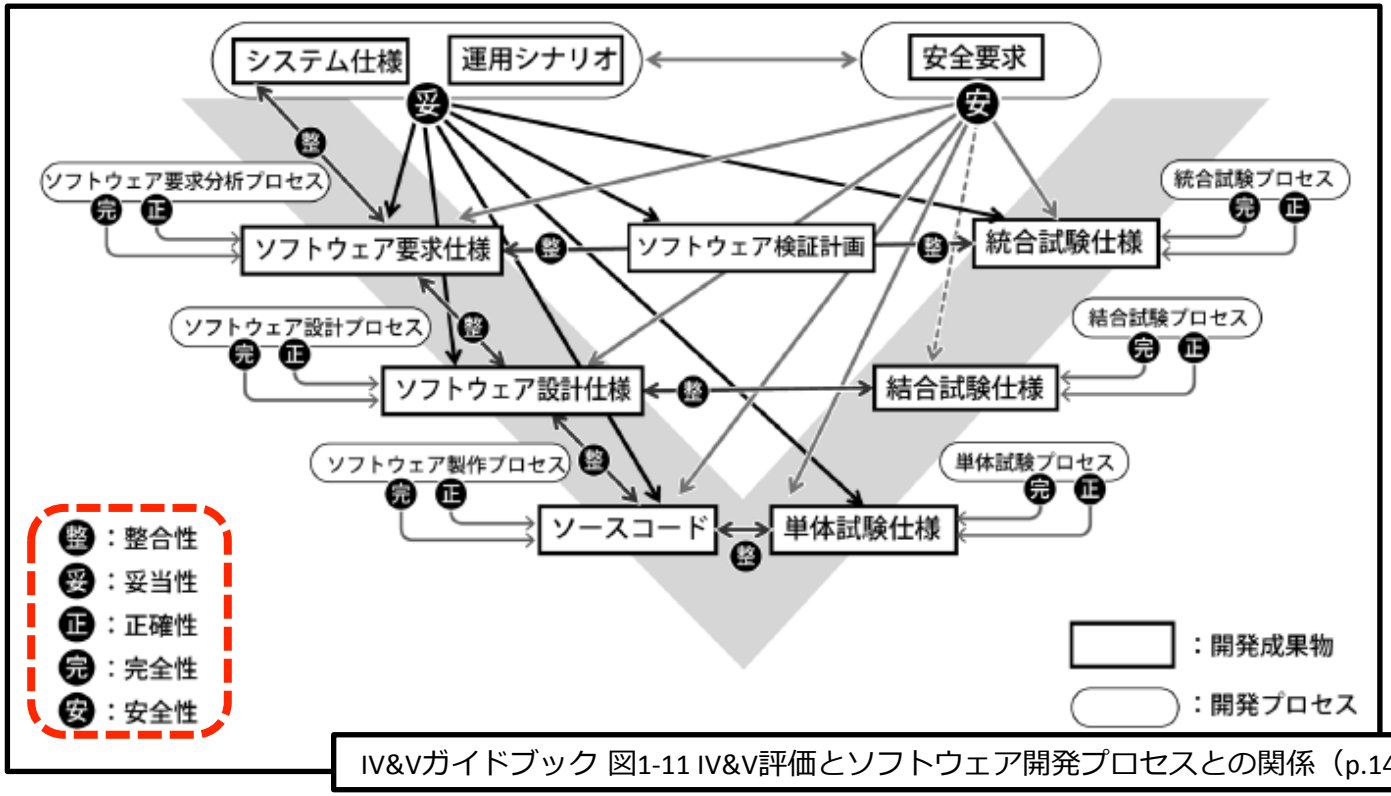
整合性 開発プロセスに沿って、ソフトウェアへの要求が漏れなく開発成果物に落としこまれているか？

妥当性 トップ要求に適合した開発成果物ができているか？

正確性 １つの開発成果物として正しい記述ができているか？（誤字・脱字がないか、等）

完全性 １つの開発成果物として必要な仕様（異常・故障への耐性も含む）が漏れなく考慮されているか？

安全性 ハザードが十分識別され、安全要求を満たす開発成果物ができているか？



IV&Vガイドブック 図1-11 IV&V評価とソフトウェア開発プロセスとの関係（p.14）

詳細観点の記述

開発工程に合わせて、**114個**の詳細観点としてまとめている。

各詳細観点の説明では、評価作業の目的、評価手順、使用できる技術等を記載している。

表 3-9　各開発プロセスのアウトプットに対する完全性の詳細観点一覧

観点：完全性

サブ観点	プロセス	詳細観点	詳細観点 ID
機能・処理の完全性	要求分析	入出力の完全性	完-要求-01
		実行内容の完全性	完-要求-02
	設計	入出力の完全性	完-設計-01
		実行内容の完全性	完-設計-02
	製作	入出力の完全性	完-製作-01
		実行内容の完全性	完-製作-02
	試験	—	—
	システム試験	—	—
設計値外の入力への耐性	要求分析	入力データへの耐性	完-要求-03
		入力タイミングへの耐性	完-要求-04
	設計	入力データへの耐性	完-設計-03
		入力タイミングへの耐性	完-設計-04
	製作	入力データへの耐性	完-製作-03
		入力タイミングへの耐性	完-製作-04
	試験	—	—
	システム試験	—	—
試験網羅性	要求分析	—	—
	設計	ソフトウェア要求仕様に対するソフトウェア試験仕様の網羅性	完-設計-05
	製作	—	—
	試験	ソフトウェア要求仕様に対するソフトウェア試験仕様（更新）の網羅性	完-試験-05
	システム試験	—	—

5観点(1) – 整合性

整合性　開発プロセスに沿って、ソフトウェアへの要求が漏れなく開発成果物に落としこまれているか？

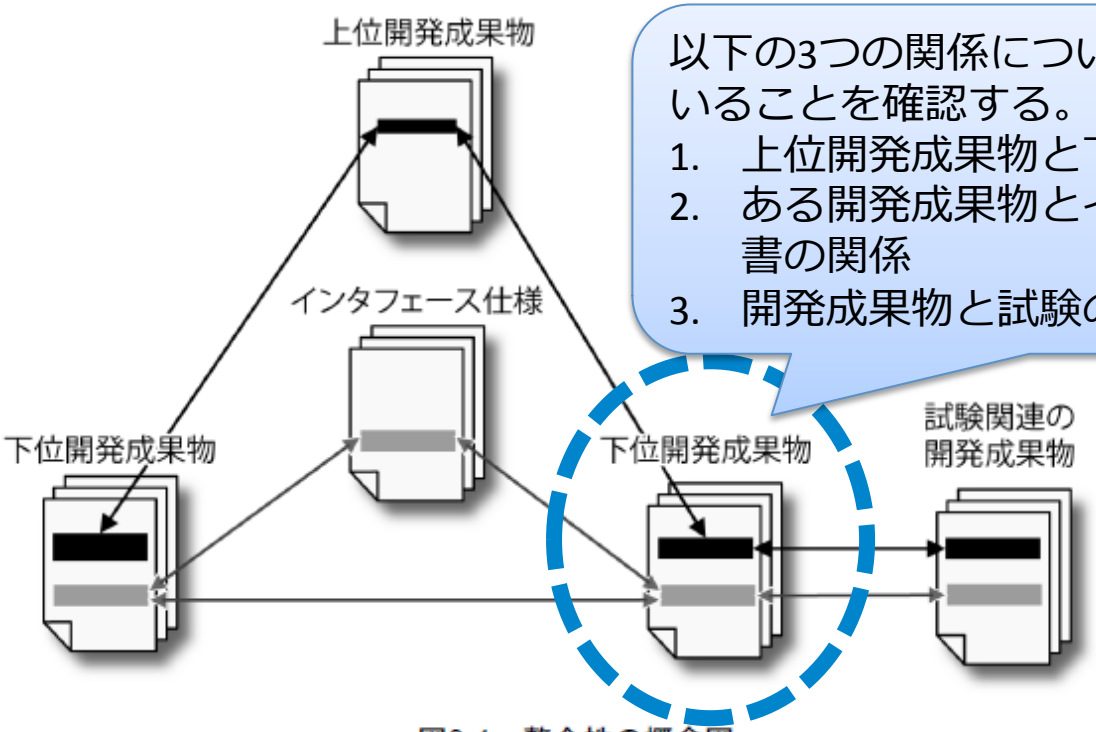


図3-1　整合性の概念図

以下の3つの関係について、整合性が保たれていることを確認する。
1. 上位開発成果物と下位開発成果物の関係
2. ある開発成果物とインタフェース関連文書の関係
3. 開発成果物と試験の関係

「整合性」といったときに、追跡可能性にある概念と、等価性にある概念の両方が、解釈としてありえる。

それぞれ単語を定義して、明確に区別できるようにしている。

IV&Vガイドブックでは、「整合性」を二つの概念で構成している。
- **追跡可能性（トレーサビリティ）**
  仕様書内の節・項レベルで追跡ができること。
- **等価性**
  節・項に記述されている内容が一致している、または上位仕様の内容を矛盾なく詳細化していること。

5観点(2) – 妥当性

妥当性　トップ要求に適合した開発成果物ができているか？

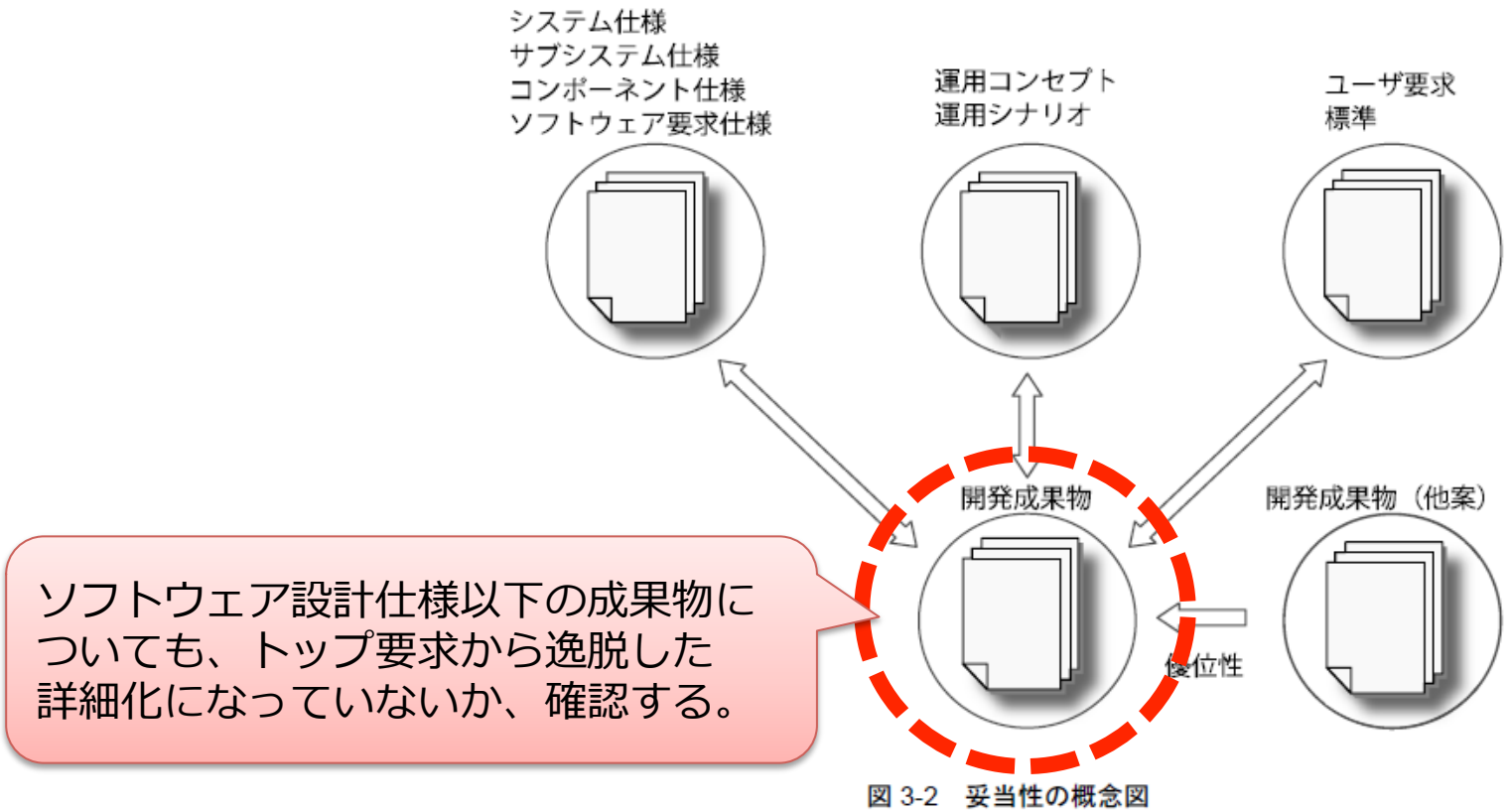


図 3-2　妥当性の概念図

ソフトウェア設計仕様以下の成果物についても、トップ要求から逸脱した詳細化になっていないか、確認する。

実際にはトップ要求とソフトウェア設計仕様・ソースコードは直接の対応関係になく、記述内容にギャップが大きい。そのため、評価は容易ではない。

⇒　評価作業の指針となるよう、詳細観点を細かく設定している。（他観点の約1.5倍）

5観点(3) – 正確性

正確性

１つの開発成果物として正しい記述ができているか？
（誤字・脱字がないか、等）

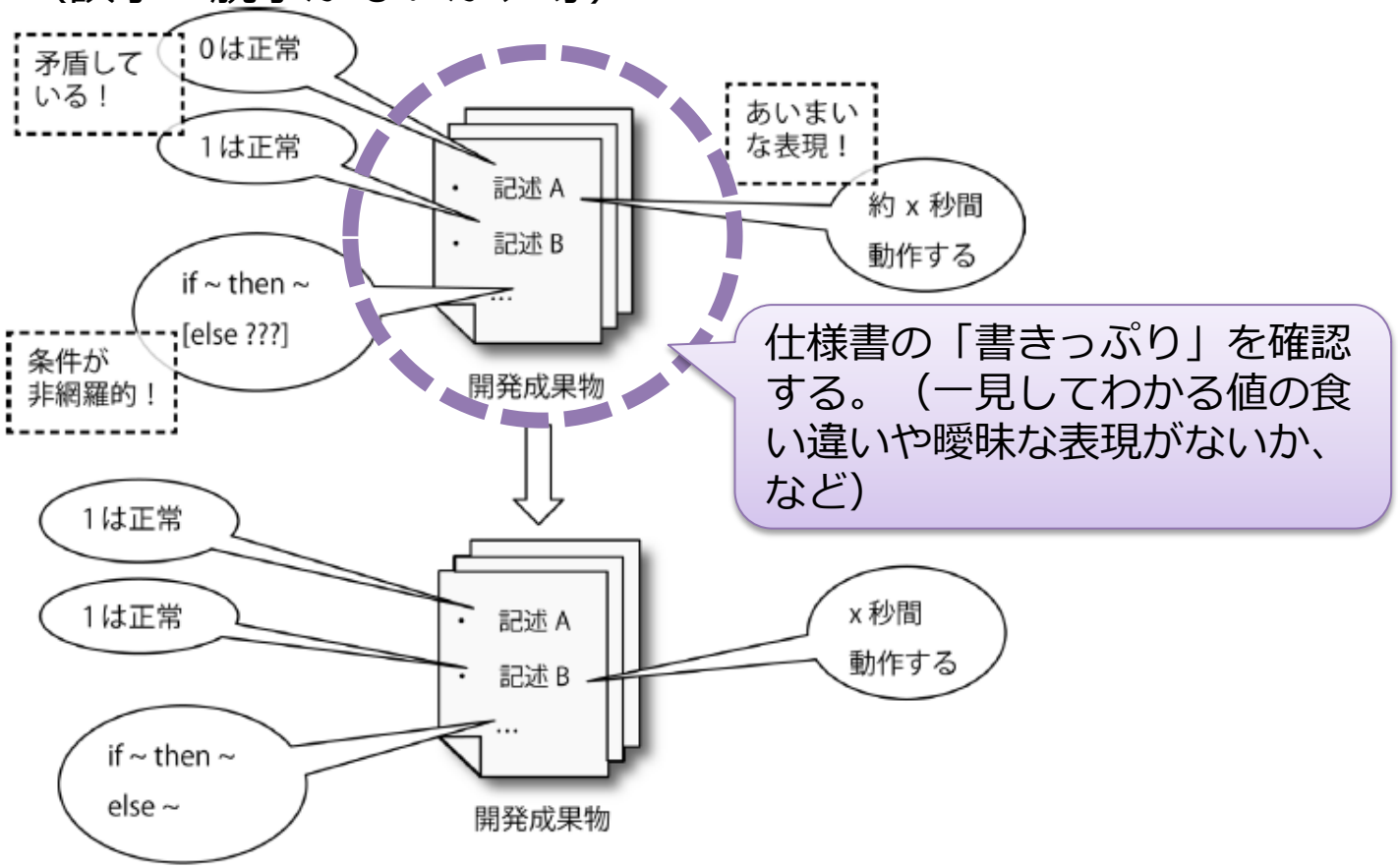


図 3-3　正確性の概念図

他の仕様書と見比べることなく、発見可能な問題点をみつける観点の１つめ。
「正確性」の見方と他の観点（特に「完全性」）とを区別するために、定義している。

5観点(4) – 完全性

完全性　１つの開発成果物として必要な仕様（異常・故障への耐性も含む）が漏れなく考慮されているか？

仕様書・ソースコードの「記述内容」について、論理的な矛盾や欠落がないことを評価する。

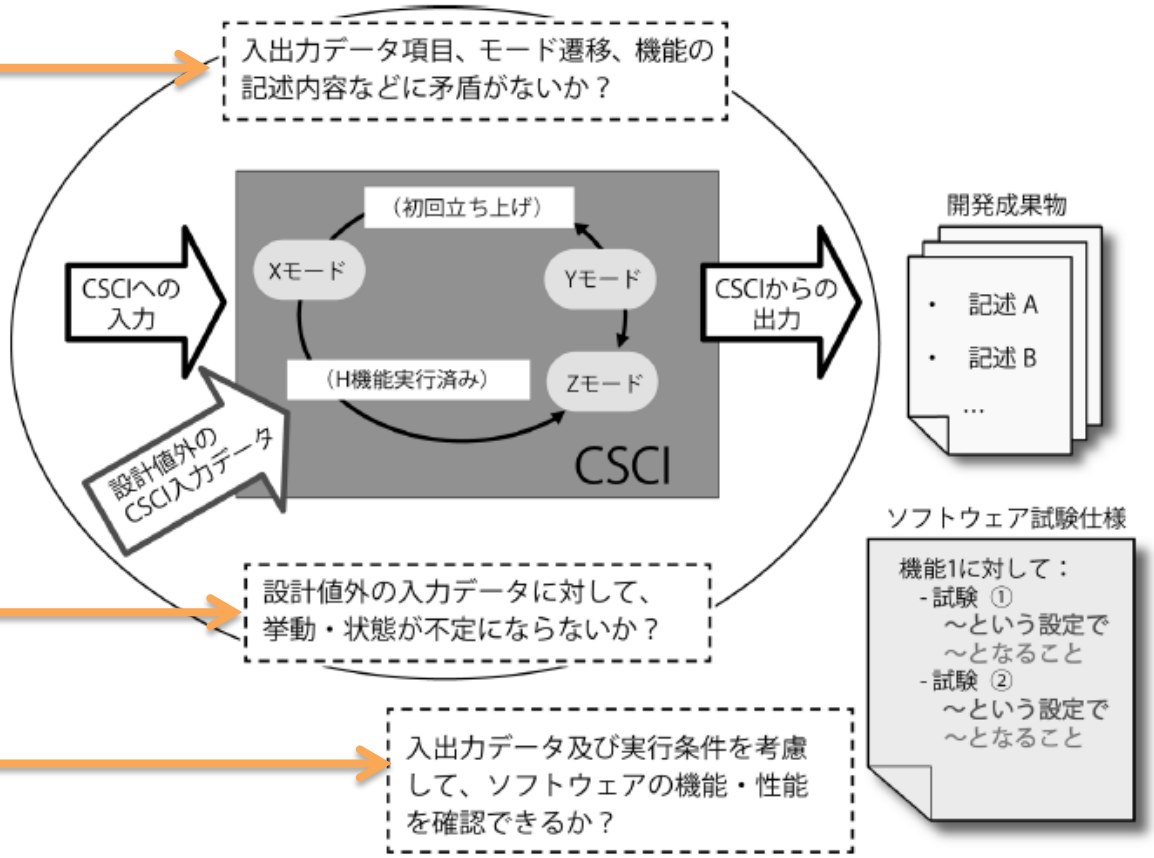


図 3-4　完全性の概念図

他の仕様書と見比べることなく、発見可能な問題点をみつける観点の2つめ。
「正確性」は表記に着目するが、「完全性」は内容に着目して論理的な矛盾や欠落がないかを評価する。

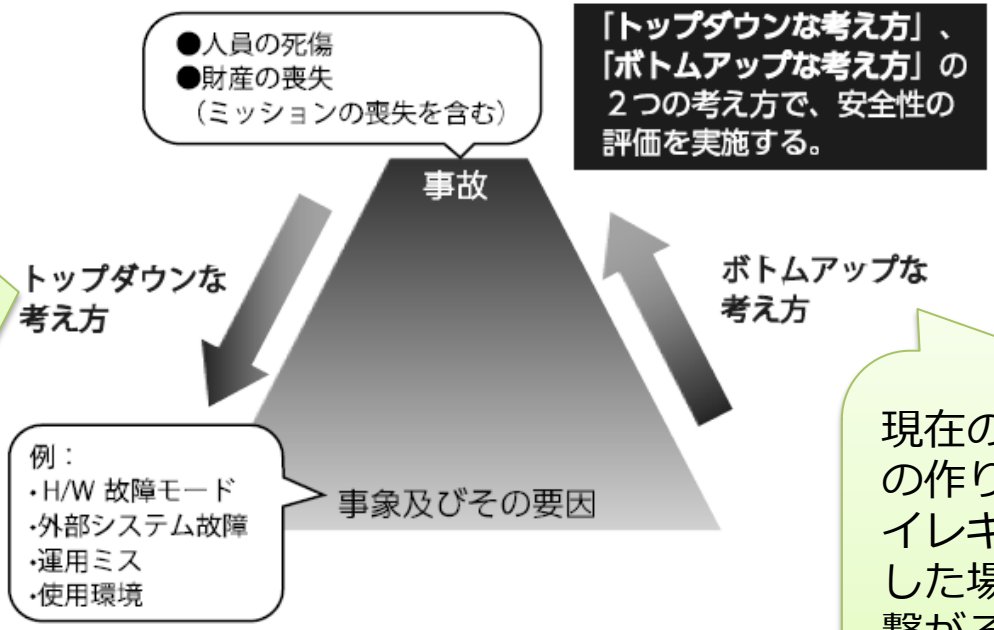
5観点(5) – 安全性

安全性

ハザードが十分識別され、安全要求を満たす開発成果物ができているか？

安全性では「**人員の死傷及び財産の喪失（ミッションの喪失を含む）を未然に防ぐために必要な対処があること**」を評価する。

最終的に防ぎたい「人員の死傷及び財産の喪失」から逆算して、そのような事故を誘発させる要因がないかを確認する。



「トップダウンな考え方」、「ボトムアップな考え方」の２つの考え方で、安全性の評価を実施する。

図 3-5　安全性の概念図

現在のソフトウェアの作りから、様々なイレギュラーが発生した場合に、事故に繋がることがないかを確認する。

「安全性」の評価では、必要に応じてシステム全体についても問題がないかどうか評価する。
（純粋にソフトウェアのみでは事故は起こらない（起こせない））

導入の効果

- 技術移転に有効
  - 新しく入ってきた人に読んでもらう。（5名ほど）
  - インターンシップの大学生・大学院生にも。（6名ほど）

おおむね好評。ただし記述が難解との指摘は少々あり。

- IV&V経験者にとっても有用
  - IV&V作業内容が明確になった。
  - IV&V作業者間の作業内容に関する議論が円滑になった。
  - 新規技術の導入を検討するとき、IV&V観点について適用可否を検討することで、適用先を網羅的に検討することができる。

いわゆる“辞書”としての有用性がある。

IV&Vガイドブックに書いてないこと

- 書いてないこと１：**各観点をいつ、どこに適用するか**
  - すべての詳細観点を全仕様・全モジュールに対して適用することは非現実的。
  - 実際の作業では、対象システムに対してリスク分析を実施し、その結果から適用する詳細観点や評価対象を決定している。（作業の流れは“2-2 IV&V実施の検討”で触れている。）

⇒ 今後、別の文書として制定する予定

- 書いてないこと２：**宇宙機で考慮する必要がない事項**
  - 不特定多数のユーザの利用
    - ユーザは訓練を積んだ要員のみ。故意に壊そうとするなど、悪意を持った使い方は想定しない。
    - セキュリティに関する要求は（今のところ）ない。
  - 不特定多数の計算機環境上での実行
    - 計算機が運用中に入れ替わることはない。
    - 多様なハードウェア上で実行するよう考慮する必要性は薄い。
  - 不特定多数の外部システムとの相互作用
    - 不特定多数のシステムと直接やりとりするようなことはない。
    - 衛星であれば、それぞれ固有の地上管制用システムが整備される。

⇒ 今後も取り扱い予定なし

まとめ

- ソフトウェア独立検証と有効性確認（ソフトウェアIV&V）を実施するとき、評価する観点をベースにIV&Vガイドブックを制定した。

- 今後の課題・展望
  - よりわかりやすい、平易な記述に更新する。（現状は記述の厳密さを優先している）
  - 定期的に更新し、陳腐化を防ぐ。

- IV&Vガイドブック配っています。
  お問い合わせ先：
  Tel: **050-3362-4385**
  email: **IVV_INFO@jaxa.jp**

- IV&V専門セミナー、開催しています。
  - 第一弾を1/15（水）に開催。（満員御礼）
  - 第二弾を近日中に開催予定。