宇宙システムにおける
検証戦略の共有と品質説明力の向上

～第1回DEOS協会オープンシンポジウム～

独立行政法人 宇宙航空研究開発機構
情報・計算工学センター
神戸 大輔

概要

第1部　宇宙システム開発の現状とIV&V

1. 宇宙システムの種類とソフトウェアの特徴
2. 安全性・信頼性確保のための取組み
3. IV&Vとは
4. IV&V活動の目的
5. IV&V活動の効果
6. IV&V活動の課題と対策
7. GSNに対する期待

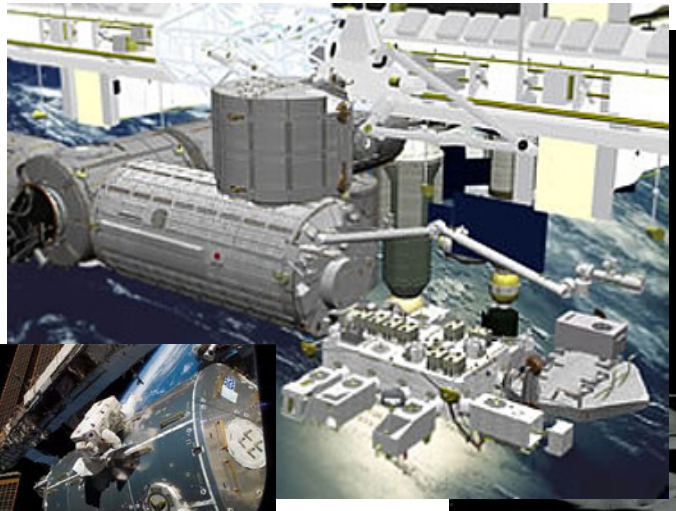
第2部　IV&Vにおけるディペンダビリティ技術～IV&Vケース～

1. IV&Vケースの概念（コンセプト）
2. IV&Vケースの工夫点
3. IV&Vケースの導入効果
4. IV&Vケースの課題と今後

まとめ

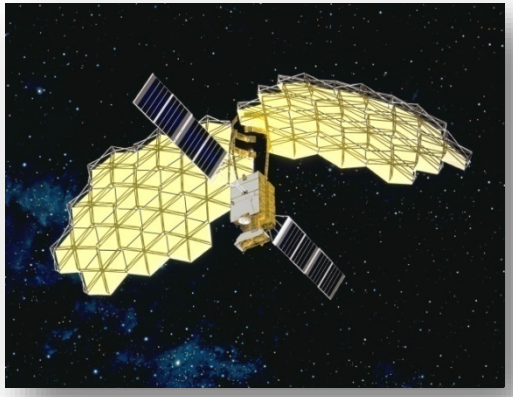
第1部
宇宙システム開発の現状とIV&V

宇宙システム



宇宙システムの種類とソフトウェアの特徴

人工衛星



- 姿勢制御系、データ処理系、ミッション系、センサ系など組込み系が中心
- 最近は書換可能なものもある
- 再利用／シリーズ化
- 放射線の影響

ロケット

- 航法誘導制御系など
- 高信頼性／多数決
- ハードリアルタイム

宇宙ステーション

- 管制システム、マニピュレータ、実験装置など、膨大な数のソフトウエア
- 高い安全要求（2故障でも安全に！）
- コマンド、データ、処理の独立性
- システム構成にクルーが入る

地上管制システム

- 管制システム等
- 信頼性

宇宙分野のソフトウェアの置かれる状況

- 組み込みソフトウェアとの共通課題
  - 上流工程の不確定さ(要求元は？決まらない？)
  - 機能要求の増加と複雑化による検証の限界
  - ハードウェア主体の文化
  - 開発の外注化の加速

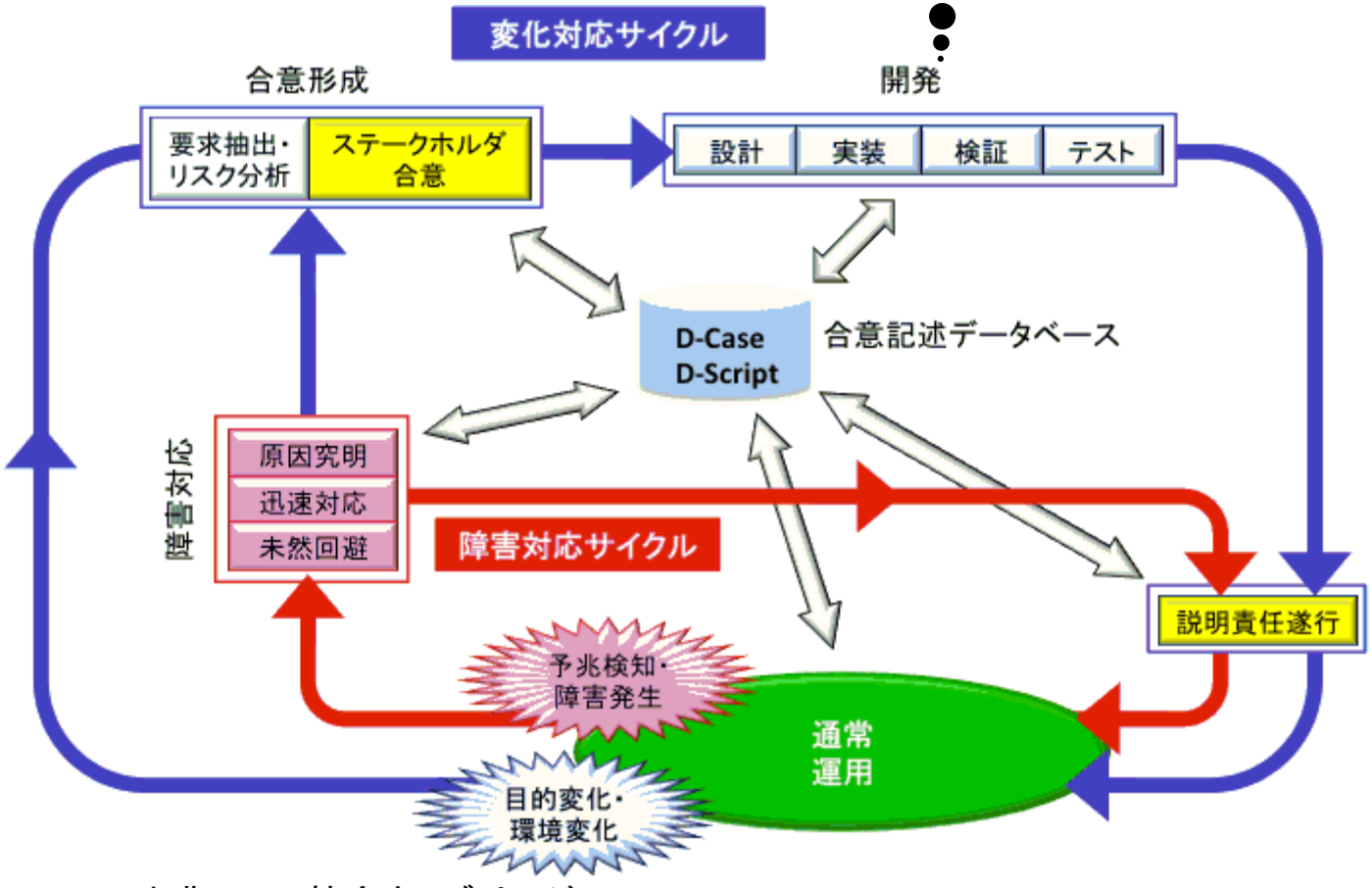
- 宇宙特有の問題
  - 容易に修理できない
  - 開発期間が長い
  - 製品が単発

宇宙機搭載ソフトウェアの特徴

- ソフトウェアの誤動作により多大な損失が発生しうる
  - もしロケットの打ち上げが失敗した場合、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
  - 地球との通信が常に可能とは限らない
  - 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
  - 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

安全性・信頼性確保のための取組み

■独立検証及び有効性確認
（Independent Verification and Validation）



■出典：DEOS協会ウェブページ　http://deos.or.jp/technology/process-j.html

ソフトウエアIV&Vとは

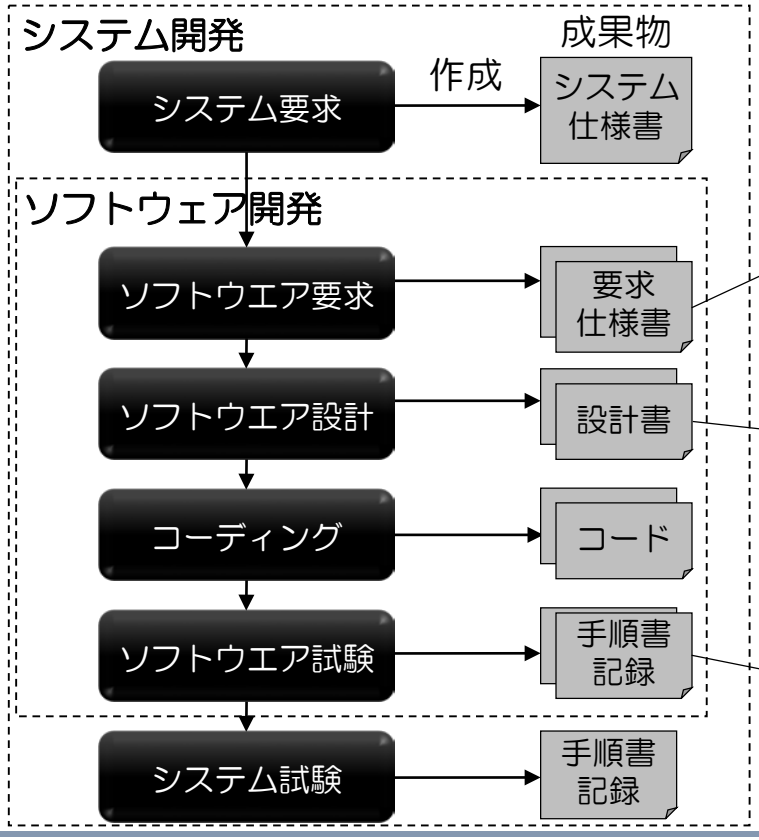
【定義】独立検証及び有効性確認（Independent Verification and Validation）

・Verification：各段階の開発成果物が、前工程からの入力情報に照らし、正しく作られているか

・Validation：各段階の開発成果物が、ユーザの期待する通りに作られているか

【目的】開発とは独立した組織が独立した観点・独立した技術によって、

開発側では気づきにくい、ソフトウエアに関連した重要課題や問題を洗い出すこと



IV&V：開発側とは独立した観点・技術（例）

上位仕様との整合性確認：
ソフトウェア要求仕様が、システム仕様から過不足なく、適切に展開されているか確認

仕様の一貫性確認：
ソフトウエアの振る舞いについて、不安定な(未定義な)状態となることがないか確認

検証網羅性確認：
仕様書で要求されている機能に対して、各試験ケースが適切に設定されているか確認

IV&V活動の目的

システムが致命的な状況（衛星喪失、ミッション喪失）に陥る可能性（リスク）を低減させる

→ ステークホルダーにソフトウェアが「安心」であることを示す

3つの問い：

- ソフトウエアは、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?
- ソフトウエアは、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?
- ソフトウエアは、不都合な事態に期待どおり振る舞うか？
  Will the system software respond as expected under adverse conditions?

IV&V活動の効果


製品の顧客


経営者

Confidence（安心） を高める
ソフトウエアが顧客要望を満足しているのか
開発・運用のリスクを低減する
開発の後工程・運用中に検知される欠陥をより早く抽出する


プロジェクト
マネージャー


開発担当

IV&V活動
の効果

品質の
可視化

開発作業
品質の向上

技術的欠陥
の抽出

プロジェクト
マイルストーン

要求フェーズ → 設計フェーズ → 製造フェーズ → 試験フェーズ

IV&V活動
への期待

リスク

問題点の除去

より効果を上げるために・・・


IV&V
担当

プロジェクトに合わせた
データに基づくプランニング

観点・手法毎の
費用対効果の蓄積

対象製品の
特徴を分析

プロジェクト横断的
知見の活用

・検出した問題点に関する情報の蓄積

システム・運用視点
による検証観点

・ミッションや運用で重要な機能やシーンを特定し、検証観点を設定

開発活動とは異なる
検出技術の構築

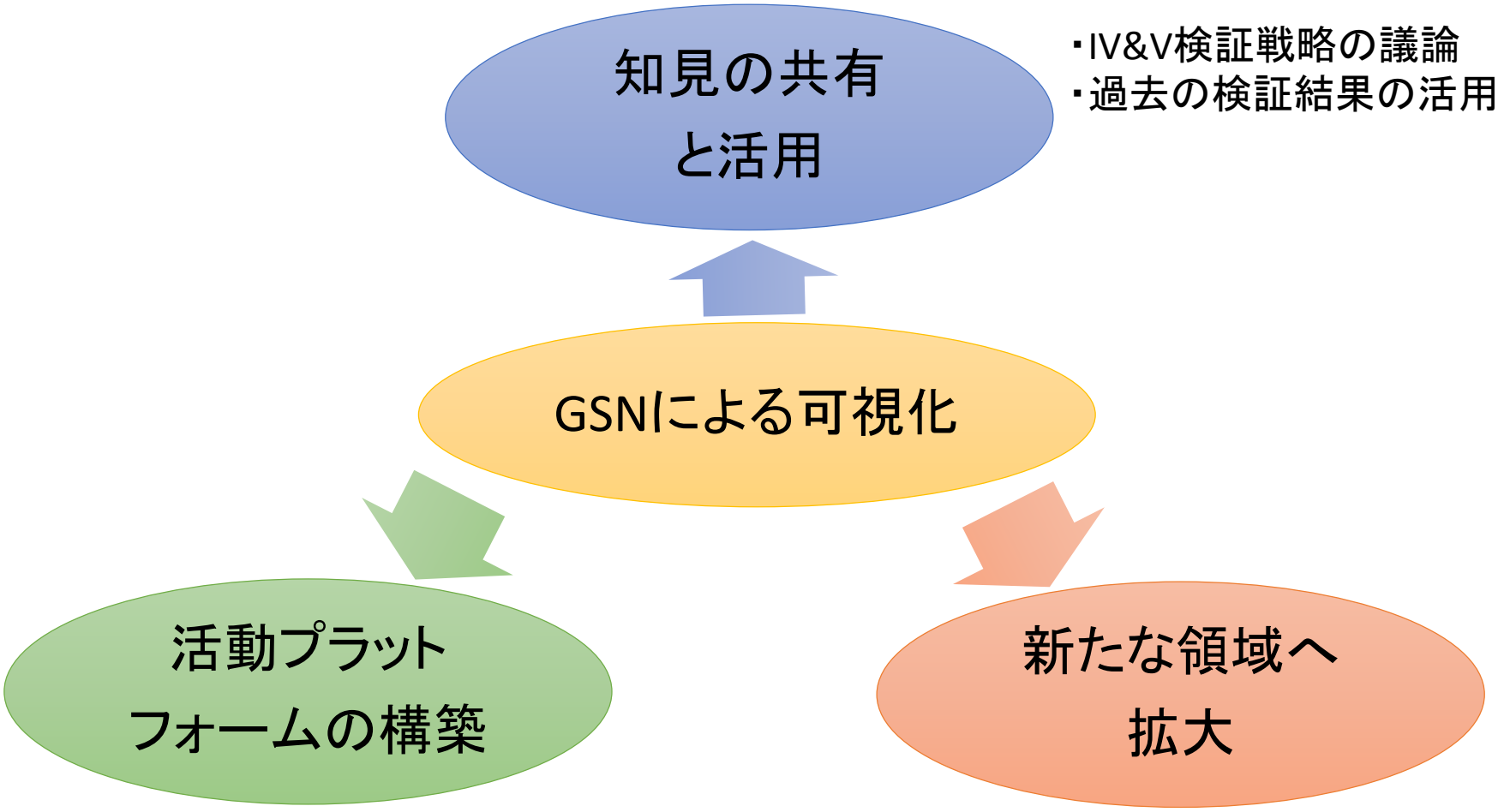
・IV&Vマニュアルの整備や
フォーマルメソッドの活用等。

IV&V活動の課題と対策

■課題	■対策
• ステークホルダーに対する説明責任が果たせておらず、IV&Vの価値が伝わっていない	• ステークホルダーに対して、IV&Vが確認した範囲と根拠を示す必要がある
• IV&Vの知見の蓄積と活用がされておらず、IV&Vの強み・独自性が出せていない	• IV&V活動において、何が価値のある知見なのか識別する必要がある
• IV&Vエンジニアの入れ替わりが激しく、組織としてIV&Vの品質を維持できていない	• IV&V初級エンジニアでも、一定レベルの品質でIV&Vを実施できる仕組みを作る必要がある

GSN（Goal Structuring Notation）を活用した
”IV&Vケース”を考案し、IV&V活動に導入

GSNに対する期待



第2部
IV&Vにおけるディペンダビリティ技術
～IV&Vケース～

IV&Vケースの概念（コンセプト）（1/4）

リスクベース検証の可視化

- リスクに基づいた検証戦略

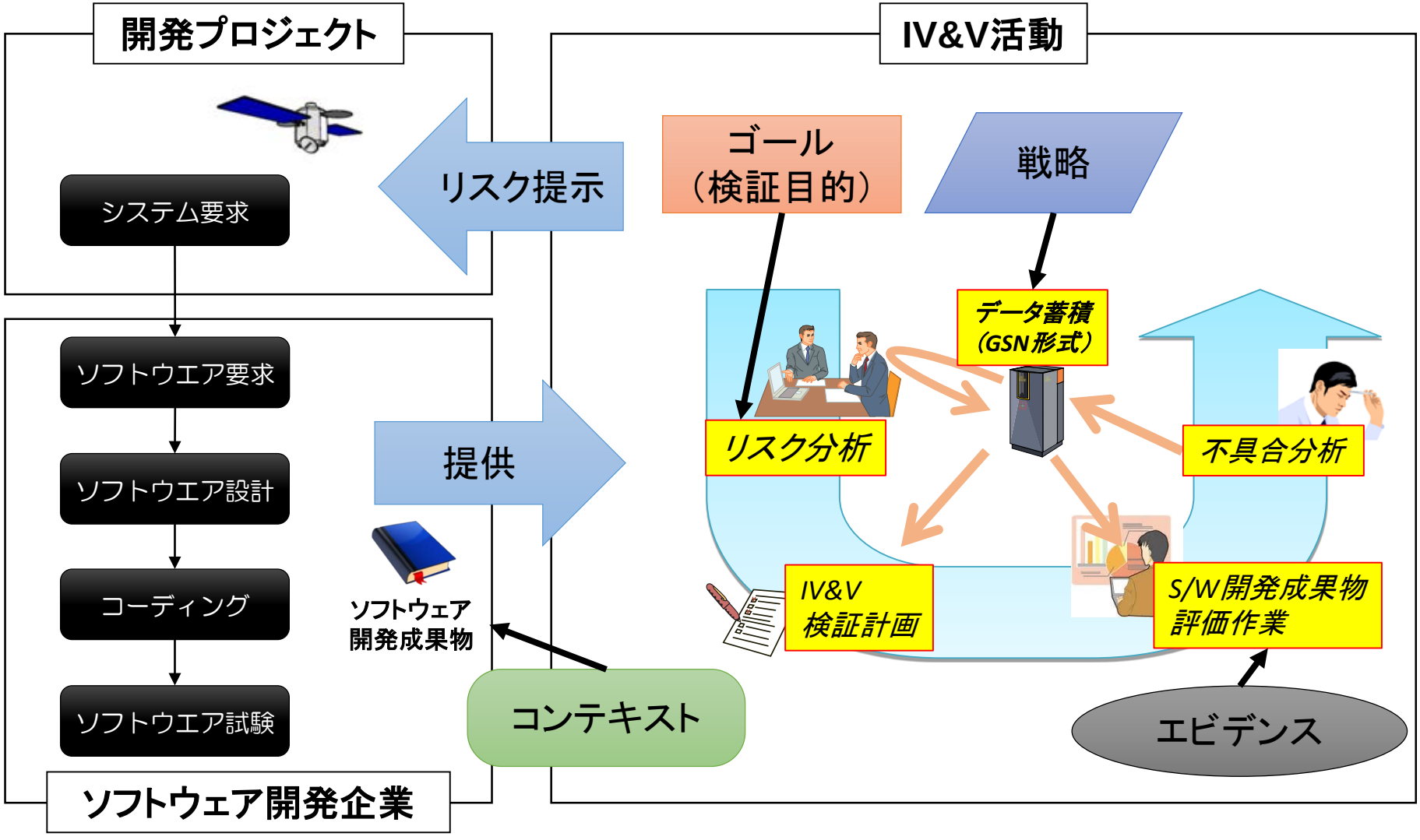
IV&V独自戦略

- プロジェクト横断的な情報（不具合情報等）を活用した、開発企業（V&V）と異なる戦略

検証精度の予測

- 計画時に想定の検証エビデンスを作成

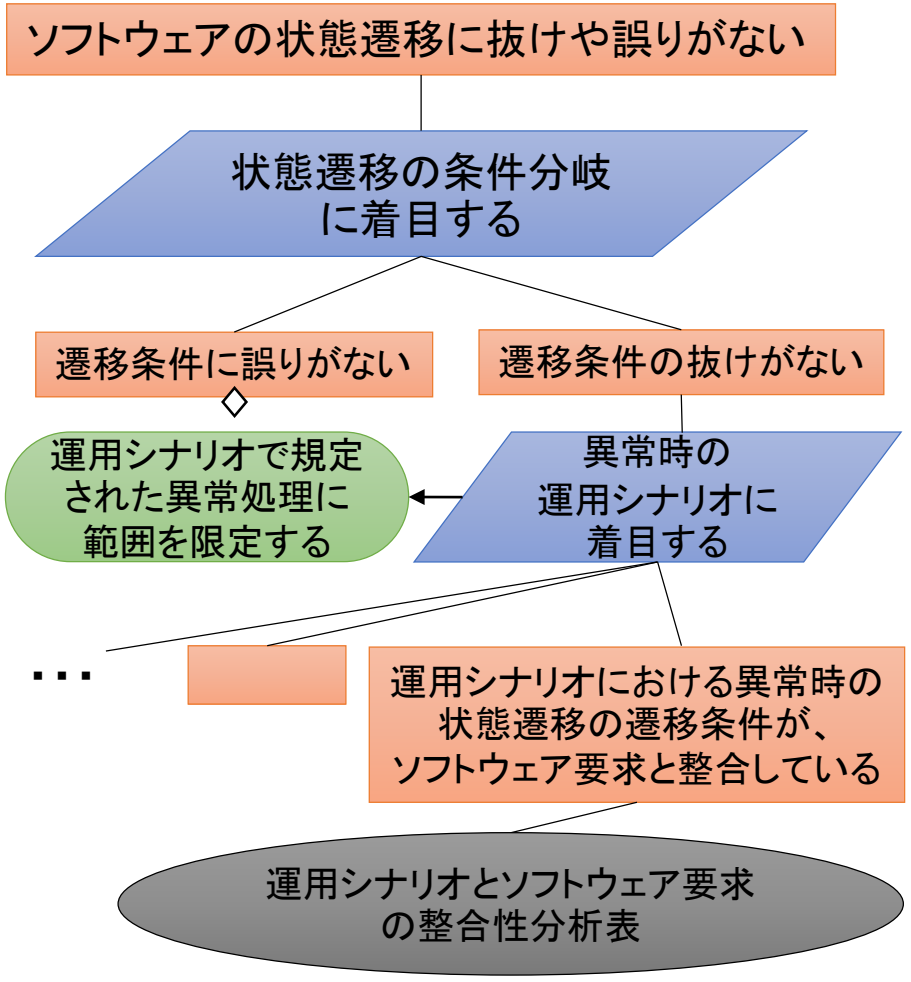
IV&Vケースの概念（コンセプト）（2/4）



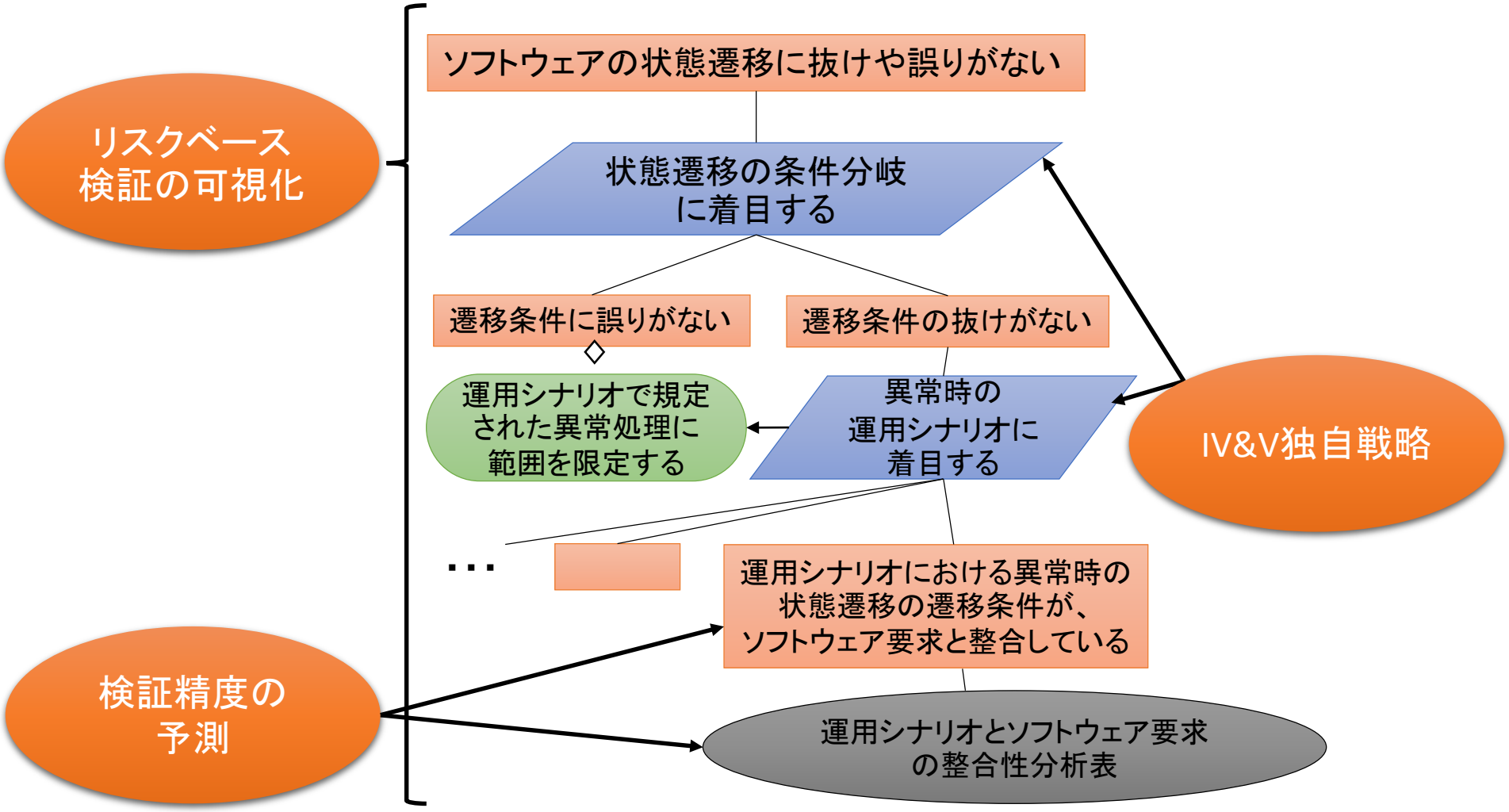
IV&Vケースの概念（コンセプト）（3/4）

■ノードの位置付け

ノード	IV&Vケースでの位置付け
ゴール	検証目的 （特定のリスクがないこと）
コンテキスト	仕様情報
戦略	検証観点 （検証目的を達成するための着眼点）
エビデンス	確認結果

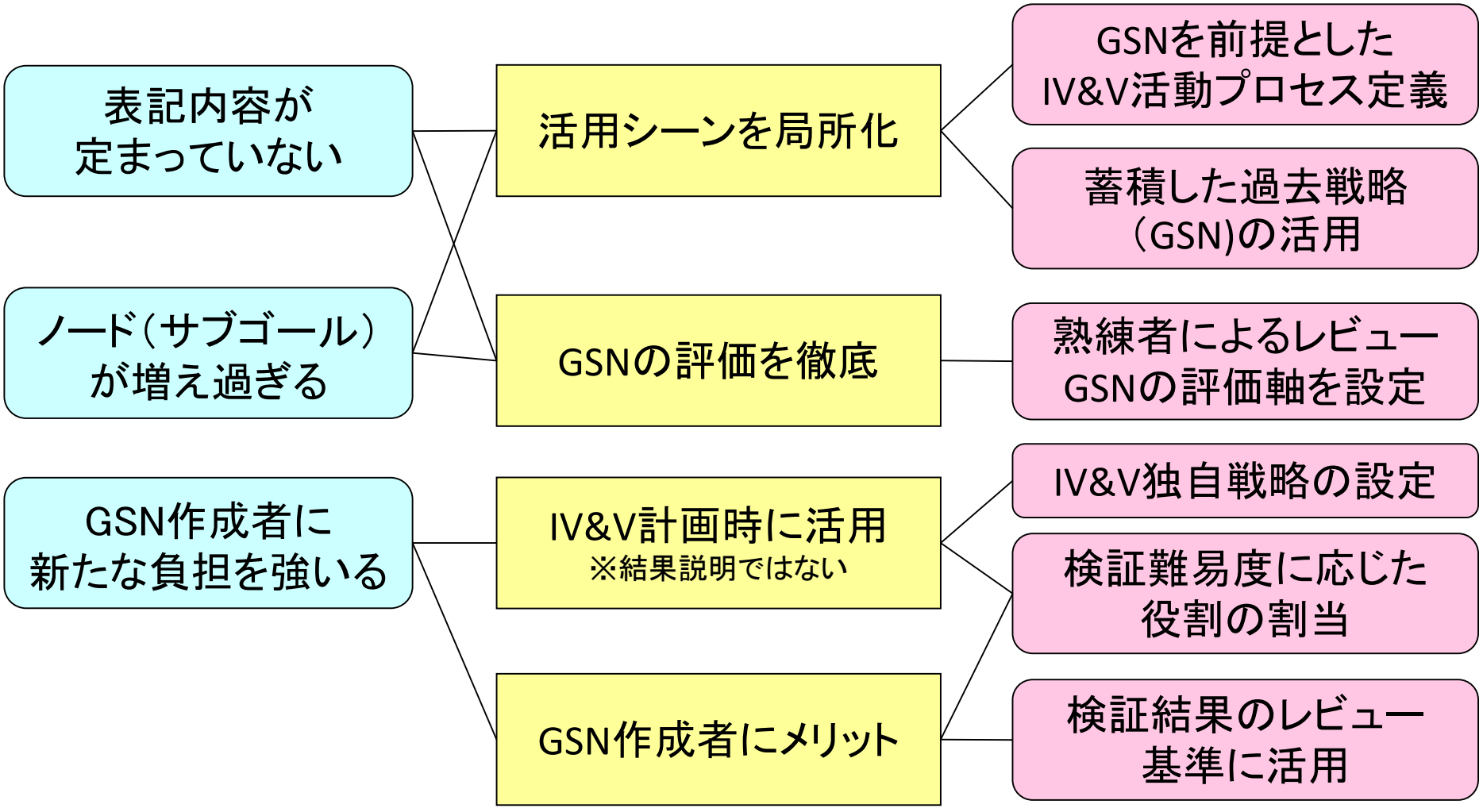


IV&Vケースの概念（コンセプト）（4/4）



IV&Vケースの工夫点(1/3)

GSN作成者にメリットを出すには



IV&Vケースの工夫点(2/3)

GSNの評価軸を設定する

GSNのレビュー方針(抜粋)

■範囲や観点の設定が適切

■理解しやすい

■再利用性が高い

■不具合要因と対応付けができる

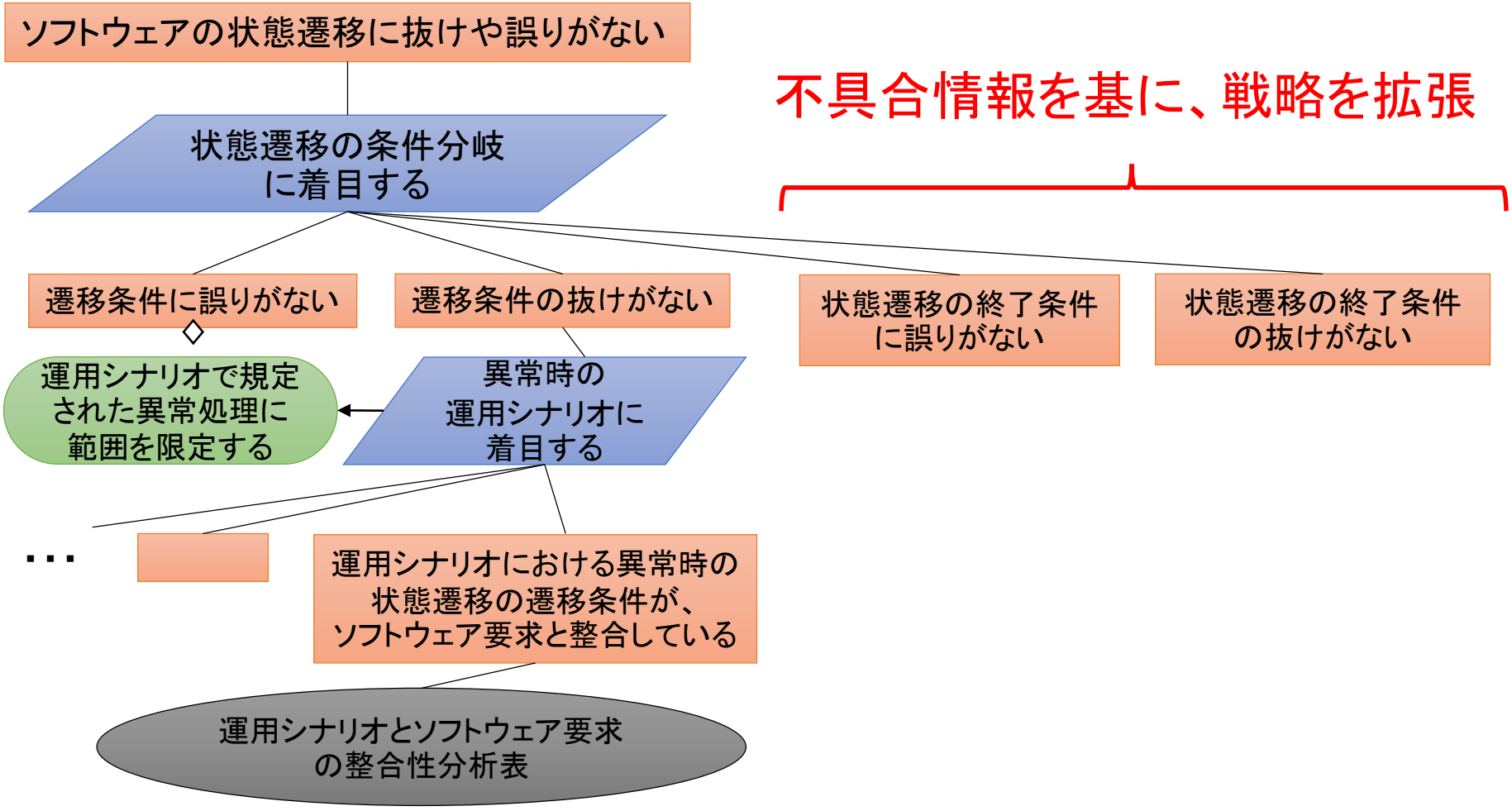
■論理性が高い

■手法や判断基準の設定が適切

■網羅性が高い

IV&Vケースの工夫点(3/3)

過去の不具合情報より、IV&V独自戦略を設定



IV&Vケースの導入効果(1/2)

IV&Vの需要向上

- ステークホルダーへの説明力の向上
  - 開発企業で行う検証と異なる、IV&V独自の検証内容が伝わり、より効果的にIV&V活動を行うことができる
  - ステークホルダーからの新たな要望に応えられる

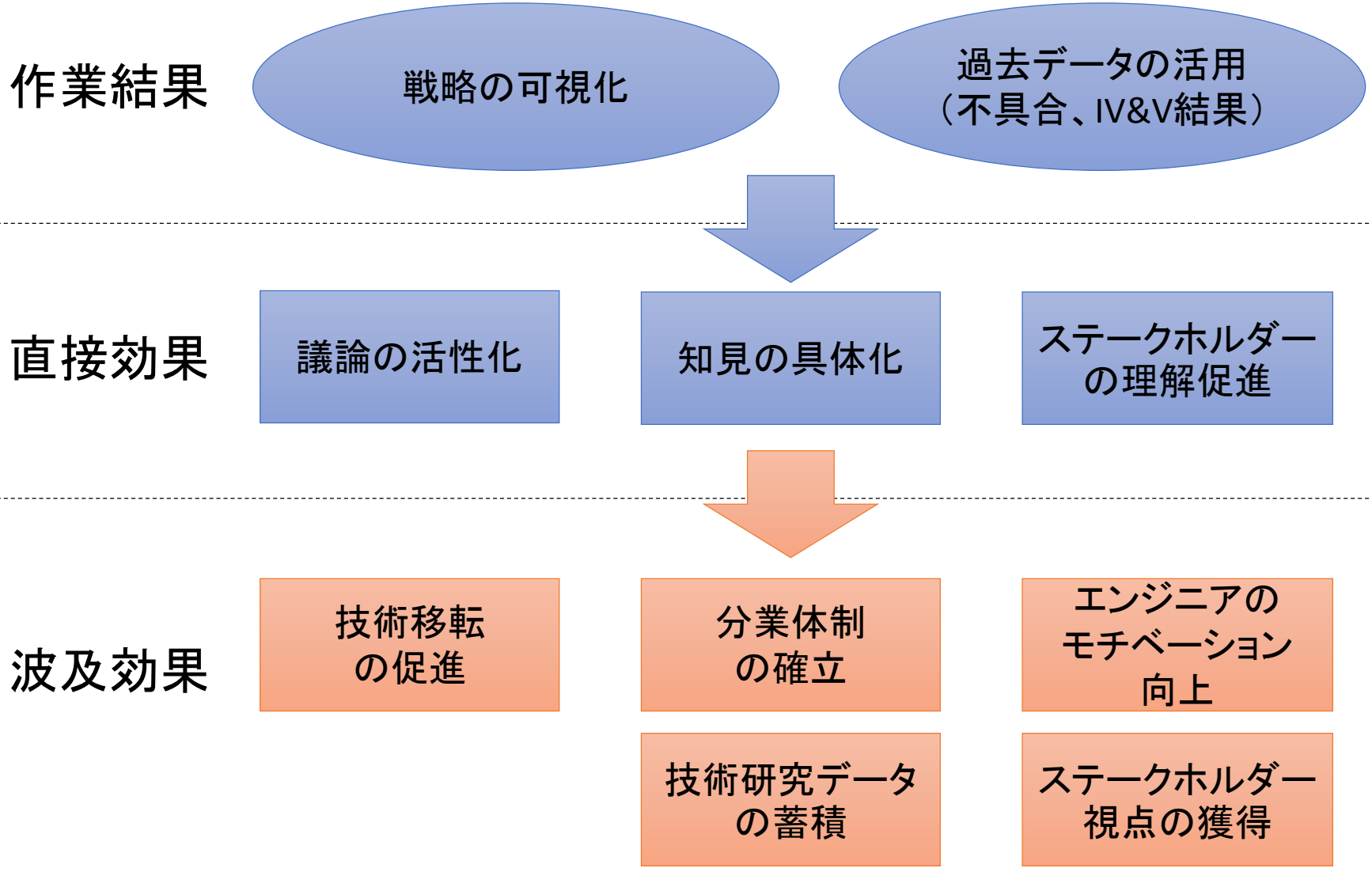
IV&Vの価値向上

- 価値ある知見の可視化
  - リスクベース検証に必要な知見が具体化され、不具合情報や過去のIV&V活動の結果を具体的に活用できるようになった

IV&Vの品質維持

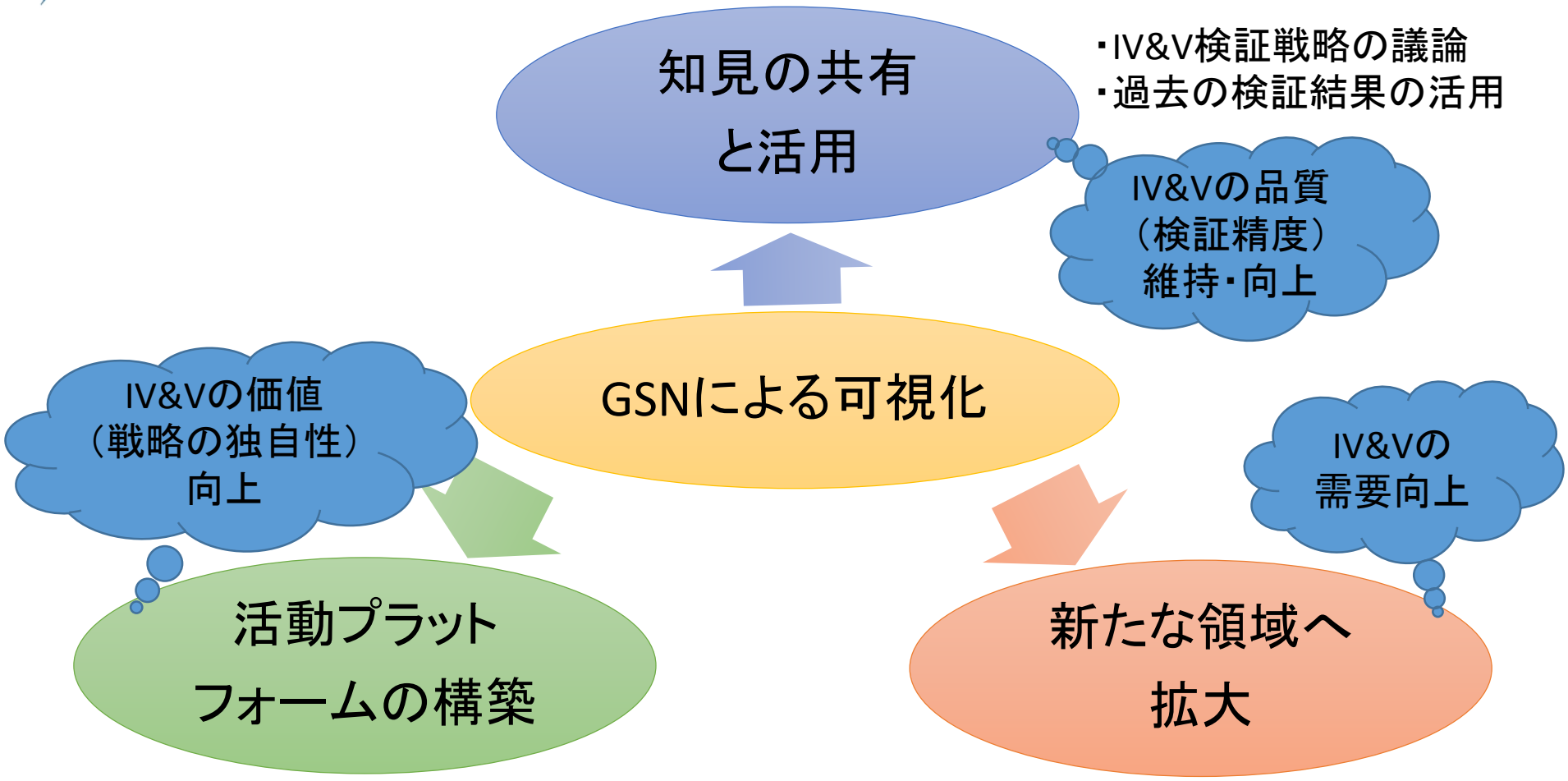
- 一定の品質のIV&V活動の確保
  - 計画時に検証内容が具体化され、エンジニアの能力に検証結果が左右されなくなった
  - 難易度が高い業務に、IV&V熟練エンジニアを投入する等の分業体制が確立した

IV&Vケースの導入効果(2/2)



まとめ

まとめ



JAXA

宇宙航空研究開発機構

Japan Aerospace Exploration Agency