

2021年3月27日

**X線天文衛星「ひとみ」の大失敗と  
小惑星探査機「はやぶさ」の大成功  
～ 結果を左右したのは全体最適化の成否 ～**

澤田雅之技術士事務所(電気電子部門)所長  
元警察大学校警察情報通信研究センター所長

澤田 雅之

# はじめに

小惑星探査機「はやぶさ」の大成功は、今では感動的な伝説です。致命的なトラブルに幾度も見舞われ、満身創痍の瀕死状態に陥りながらも、的確かつ臨機応変なダメージコントロールで見事に乗り切り、2010年に奇跡の生還を果たしました。「はやぶさ」は宇宙航空研究開発機構(JAXA)の宇宙科学研究所が打ち上げ、その主製作者はNECです。

X線天文衛星「ひとみ」の大失敗(つまり、2016年に打ち上げには成功したが、プログラムのバグとデータ入力ミスにより衛星軌道上で空中分解してしまったこと)は、「ひとみ」が米国航空宇宙局や欧州宇宙機関等との国際協力ミッションであったため、X線天体観測がこの5年間にわたって世界的に停滞する事態を引き起こしてしまいました。「ひとみ」もJAXAの宇宙科学研究所が打ち上げ、その主製作者はNECです。

当事者はいずれも同じ(JAXAの宇宙科学研究所とNEC)であるのに、「はやぶさ」は大成功して「ひとみ」は大失敗した原因について分析しました。その結果、得られたキーフレーズですが、「はやぶさ」については、全体最適化、トップダウンによるプロジェクトマネジメント、事前の周到なリスクマネジメントの結果としての的確かつ臨機応変なダメージコントロール、「ひとみ」については、部分最適化、ボトムアップによるプロジェクトマネジメント、事前のリスクマネジメントの欠如によるマニュアルの不備、ソフトウェアが機能・性能を左右する場合には詳細設計審査(つまり、「仕様発注」の審査)ではなく要求性能審査(つまり、「性能発注」の審査)が必要、などでした。このようなキーフレーズとその意味するところは、様々な分野に応用できるのではないかと思いますので、「ひとみ」の大失敗と「はやぶさ」の大成功を題材として、わかりやすくご説明致します。

# I

**X線天文衛星「ひとみ」が  
軌道上で空中分解するまでの経緯**

# X線天文衛星「ひとみ」



出典 :<http://image.search.yahoo.co.jp/search?rkf=2&ei=UTF-8&p=X線天文衛星「ひとみ」>

宇宙からのX線は、大気に吸収されるため衛星による観測が欠かせない。

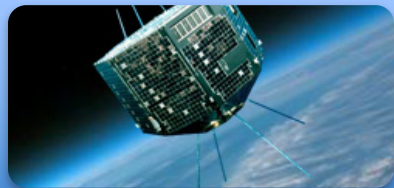


2016年に宇宙航空研究開発機構(JAXA)の宇宙科学研究所が打ち上げた「ひとみ」は、2005年に打ち上げ2015年まで運用したX線天文衛星「すざく」の後継 → 「ひとみ」は、「すざく」の数十倍の性能の観測機器を搭載。重量約2.7t



米航空宇宙局、欧州宇宙機関等が参加する国際協力ミッション。国内外51の大学や研究機関から約180名の研究者がミッションに参加。我が国の負担額は、衛星打ち上げを含めて約310億円。

# X線天文衛星は日本のお家芸



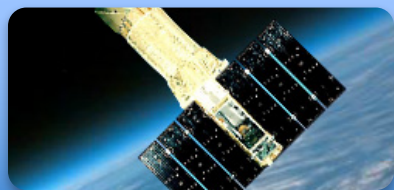
はくちょう 1979～1985 96Kg



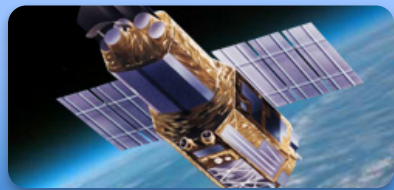
てんま 1983～1988 216Kg



ぎんが 1987～1991 420Kg



あすか 1993～2001 420Kg



すざく 2005～2015 1.7t

# 打ち上げ成功から空中分解までの経緯

2016年2月17日 衛星軌道への打ち上げに成功



2016年2月29日 衛星本体の基本機能確認や、ソーラーパネルと光学ベンチの伸展を行う「クリティカルフェーズ」が完了



2016年3月26日 全ての観測機器を立ち上げる「初期機能確認フェーズ」の期間中に、衛星異常回転が発生して空中分解



出典：X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書

# II

X線天文衛星「ひとみ」が大失敗した原因

資料28-2-2  
科学技術・学術審議会  
研究計画・評価分科会  
宇宙開発利用部会  
(第28回H28.6.14)

# X線天文衛星ASTRO-H「ひとみ」 異常事象調査報告書

平成28(2016)年6月14日

国立研究開発法人

宇宙航空研究開発機構

本資料における時刻は注記のあるものを除いて全て日本時間(JST)で記述しております。



# X線天文衛星「ひとみ」が軌道上で分解



ソフトウェアのバグとデータ入力ミスが原因！

## 1 姿勢測定系のバグによる異常回転の開始

姿勢測定系のバグにより、実際には回転していない衛星がゆっくりと回転していると姿勢測定系が誤認 → 誤認した回転を止める方向に姿勢変更系が作動した結果、衛星はゆっくりと回転を開始

## 2 姿勢変更系のデータ入力ミスによる異常回転の加速

回転を始めた衛星は自動的に緊急対応モードとなり、ソーラーパネルを太陽に向けるため、姿勢変更系の事前入力データに基づき姿勢制御用スラスタを噴射 → データ入力ミスにより、スラスタの噴射が衛星の回転を加速させた結果、遠心力により衛星は分解



出典: 前掲

# 「ひとみ」の姿勢測定系と姿勢変更系

スタートラッカ(STT)  
[1/2]

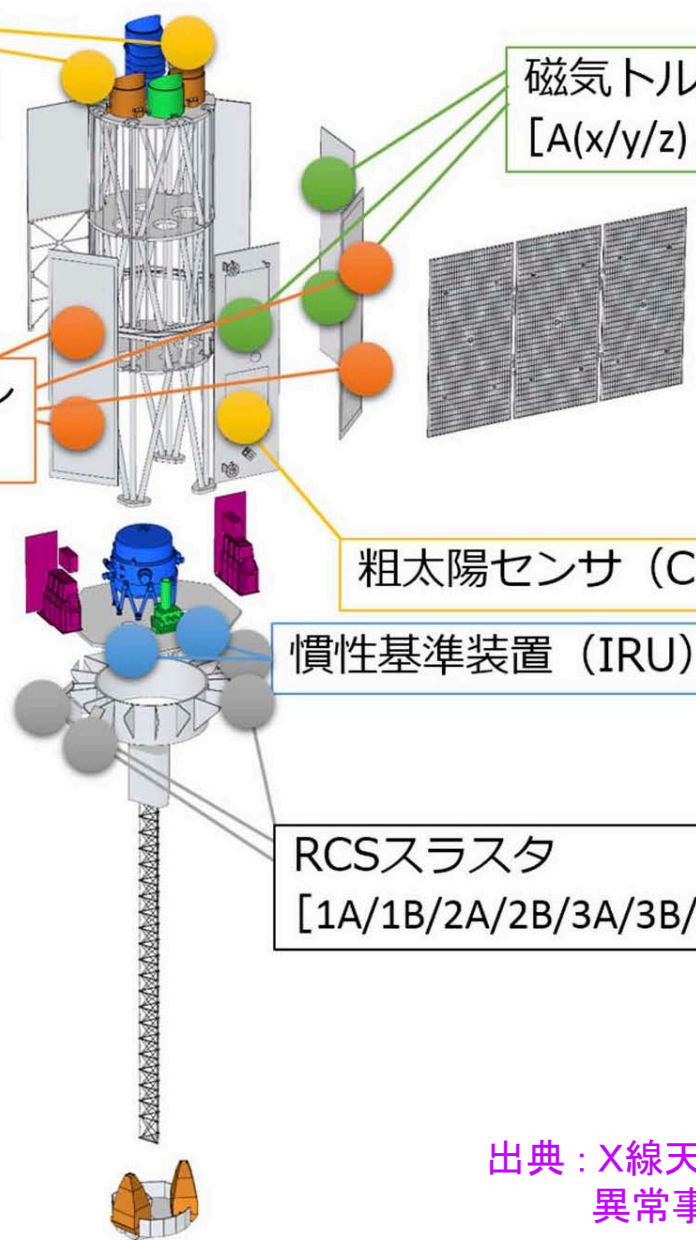
磁気トルカ (MTQ)  
[A(x/y/z) / B(x/y/z)]

リアクションホイール  
(RW) [1/2/3/4]

粗太陽センサ (CSAS) [1A/1B/2A/2B]

慣性基準装置 (IRU) [A/B]

RCSスラスタ  
[1A/1B/2A/2B/3A/3B/4A/4B]



出典 : X線天文衛星ASTRO-H「ひとみ」  
異常事象調査報告書

# 「ひとみ」の姿勢測定系

**スタートラッカ**：星々の配置を見て、姿勢を実測する機器

➡ 精度は高いが、撮像部が地球に向いている場合には姿勢を実測できない。

**粗太陽センサ**：太陽の方角を調べて、姿勢を実測する機器

➡ 測定できる視野範囲が狭い。

**慣性基準装置**：加速度の大きさと方向を調べて、姿勢を推測する機器

➡ 加速度を調べるため、一定速度での姿勢の変化は検知・推測できない。また、時間の経過とともに推測値の誤差が累積していくので、スタートラッカや粗太陽センサの実測値による補正を要する。

# 「ひとみ」の姿勢変更系

**リアクションホイール** : ホイールの回転を加速・減速させて、その反動で衛星を回転させる機器

➡ 同じ向きにばかり加速を続けた場合には、リアクションホイールでの姿勢制御が限界を迎え、セーフホールドモードに移行する。

**磁気トルカ** : 電磁石と地磁気の相互作用により、姿勢を変更する機器

**RCSスラスタ** : 小型のロケットエンジンを噴射して、姿勢を変更する機器

➡ RCSとは、Reaction Control Subsystemのこと。セーフホールドモード等で使用する。

## 姿勢測定系の誤認による異常回転の開始の経緯(3月26日)

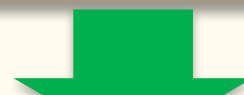
衛星の姿勢測定系は、加速度を調べて姿勢の変化を推測する慣性基準装置と、星空を見て衛星の姿勢を正確に実測するスタートラッカを用いており、慣性基準装置の推測値(時間とともに誤差が累積する。)を、スタートラッカの実測値で補正するように構成していた。 → スタートラッカは、現用・予備の2台を搭載していたが、切替時に発生する姿勢の微変動を避けるため、自動的に切り替えない設計としていた。また、慣性基準装置の推測値とスタートラッカの実測値に1度以上の角度の隔たりがある場合には、スタートラッカの実測値を棄却する設計としていた。



3時22分、望遠鏡の向きを変えるため、衛星の姿勢を変更した。



4時10分、地球に遮られていたスタートラッカの視野が開け、衛星の姿勢をスタートラッカが正確に実測した。しかし、この直後にスタートラッカが不意にリセットし、実測値を出力しなくなった。 → 姿勢制御系ソフトウェアは、4時10分時点での慣性基準装置に基づく推測値(誤差が累積)とスタートラッカの実測値(正確)との差異に基づき、1時間に21.7度の速度で衛星はゆっくりと回転していると誤認(実際には回転していない。)した。



次のページへ



姿勢制御系ソフトウェアは、誤認した回転を止めるため、リアクションホイールを作動させた結果、1時間間に21.7度の一定速度で衛星はゆっくりと回転し始めた。 → 一定速度の場合には、慣性基準装置では姿勢の変化を検知できないため、姿勢制御系ソフトウェアは回転を止めたと誤認(実際には回転している。)した。



4時14分、スタートラッカによる衛星の姿勢の正確な実測が再開した。 → 4時10分から4時14分の間、衛星は1度以上回転していたため、姿勢制御系ソフトウェアは、スタートラッカの異常と判断して、スタートラッカの出力を全て棄却した。



回転の継続により、地球の重力に対して衛星が直立した形にならないように姿勢を保つ機能に大きな負荷が掛かり、リアクションホイールの姿勢制御能力が限界に達した。 → 衛星は自動的にセーフホールドモードに移行した。

## 姿勢変更系の誤入力による異常回転の加速の経緯(3月26日)

スタートラッカや粗太陽センサが出力する実測値を用いず、慣性基準装置による推測値のみに依存することとなった姿勢制御系ソフトウェアでは、大きな推測誤差の発生を検知して補正することができず、衛星の実際の姿勢を把握できなくなった。 → 姿勢制御系ソフトウェアが推測した誤った姿勢に基づき、磁気トルカとリアクションホイールを動作させ続けたため、リアクションホイールの姿勢制御能力が限界に達した。



衛星は自動的にセーフホールドモードに移行し、粗太陽センサで捉えた太陽の方角に太陽電池パドルを向けるため、予め設定されたパラメータに基づき、RCSスラスタ(小型のロケットエンジン)を噴射した。 ← このパラメータは、光学ベンチの伸展に伴い、2月25日に設定値が変更されていた。



2月25日に設定変更されたパラメータに入力誤り(絶対値とすべきところをマイナス数値のまま入力)があったため、スラスタの噴射は衛星の回転を加速する方向に働き、高速回転による遠心力で衛星は分解した。

# 姿勢測定系が脆弱化した要因

## 【異常と判断したスタートラッカを測定系から排除する設定】

主目的は、精度の劣化を避け、安定姿勢でのX線天体観測時間を長く取るため

➡ 結果として、慣性基準装置の推測値に依存する設計

## 【予備のスタートラッカに自動的に切り替わらない設定】

主目的は、スタートラッカ切替時に発生する姿勢微変動を避け、安定姿勢でのX線天体観測時間を長く取るため

➡ 結果として、慣性基準装置の推測値に依存する設計

## 【粗太陽センサを姿勢測定に用いない設定】

主目的は、粗太陽センサの視野範囲の狭さから、不必要に緊急対応モードに移行した場合にX線天体観測が中断されるのを回避するため

➡ 結果として、慣性基準装置の推測値に依存する設計

つまり、



「X線天体観測」の部分最適化のみを追求した結果、  
「衛星の安全・信頼性」を含めた全体最適化に失敗



## 異常回転を引き起こした設計上の直接要因

### \*\* 発注側が X線天体観測の部分最適のみを追求 \*\*

姿勢変更に伴うX線観測時間のロスを減らすため、姿勢変更後の姿勢決定収束時間が短くなるよう、姿勢決定システムのリセット後のゲインを高く設定した。

スタートラッカ出力の単発的なノイズ変動による姿勢決定精度の劣化を避けるため、スタートラッカが出力する瞬時の姿勢情報と、慣性基準装置に基づき姿勢制御系ソフトウェアが継続的に計算している姿勢情報との間に1度以上の角度差がある場合は、スタートラッカを棄却して姿勢制御ソフトウェアの計算値を優先する設計とした。

スタートラッカ切替時に発生する姿勢微変動を避け、安定姿勢でのX線天体観測時間を長く取るため、2台搭載していたスタートラッカの片方が使用できない際には両方共に使用せず、慣性基準装置の出力に基づく姿勢制御系ソフトウェアの計算値に依存する設計とした。

ミッションの継続性を優先するASTRO-Hプロジェクトからの要求に基づき、視野範囲の狭さから不必要にセーフホールドに移行する可能性があった粗太陽センサについては、セーフホールド移行判断に用いず、姿勢制御系ソフトウェアの計算値を用いる設計とした。

## 異常回転を引き起こした設計上の背後要因 (1/3)

**\* 発注側の設計審査ではソフトウェアのバグを発見できない \***

受注企業による衛星の詳細設計は、『JAXAの設計審査会』で審査され、その結果に基づきJAXAから受注企業に製造が「仕様発注」された。

しかし、



今日では、ソフトウェアが衛星の安全・信頼性を決定的に左右するが、ソフトウェアの詳細設計の良し悪しについて、発注側の設計審査会で分析審査することは困難 ➡ 設計審査会でソフトウェアのバグを発見することは不可能

そこで、



目に見えないソフトウェアが機能・性能を左右する発注では、受注者に実現を求める機能・性能の要求要件(衛星の安全・信頼性等)を発注仕様書に規定して、設計と製造を一括受注させる「性能発注」が効果的。 ➡ 設計審査会では、詳細設計の良し悪しを審査するのではなく、発注仕様書で規定した要求要件の妥当性と要求要件に過不足がないか否かを審査することが理想

## 異常回転を引き起こした設計上の背後要因 (2/3)

**\* 発注側に衛星の安全・信頼性を含めた全体最適の認識が欠如 \***

姿勢制御系(姿勢測定系と姿勢変更系)の設計に向けて、発注側であるASTRO-Hプロジェクトから受注企業への要求が偏っており、より良い観測条件を確保するための要求は詳細である一方、衛星の安全・信頼性に関する要求は殆ど無かった。

しかし、




発注側からの要求内容は、受注企業側には決定的と言えるほどの意味を持つ。


➡ 衛星の安全・信頼性に関する要求が殆ど無いままに、より良い観測条件を確保するための要求が詳細であれば、受注企業としては、より良い観測条件を確保するための要求を鵜呑みにして設計せざるを得ない。 ➡ X線天体観測の部分最適に行き着くことなり、衛星の安全・信頼性を含めた全体最適化を、受注企業側で行うことは困難

## 異常回転を引き起こした設計上の背後要因 (3/3)

### \* 全体を統括したプロジェクトマネジメントの不備 \*

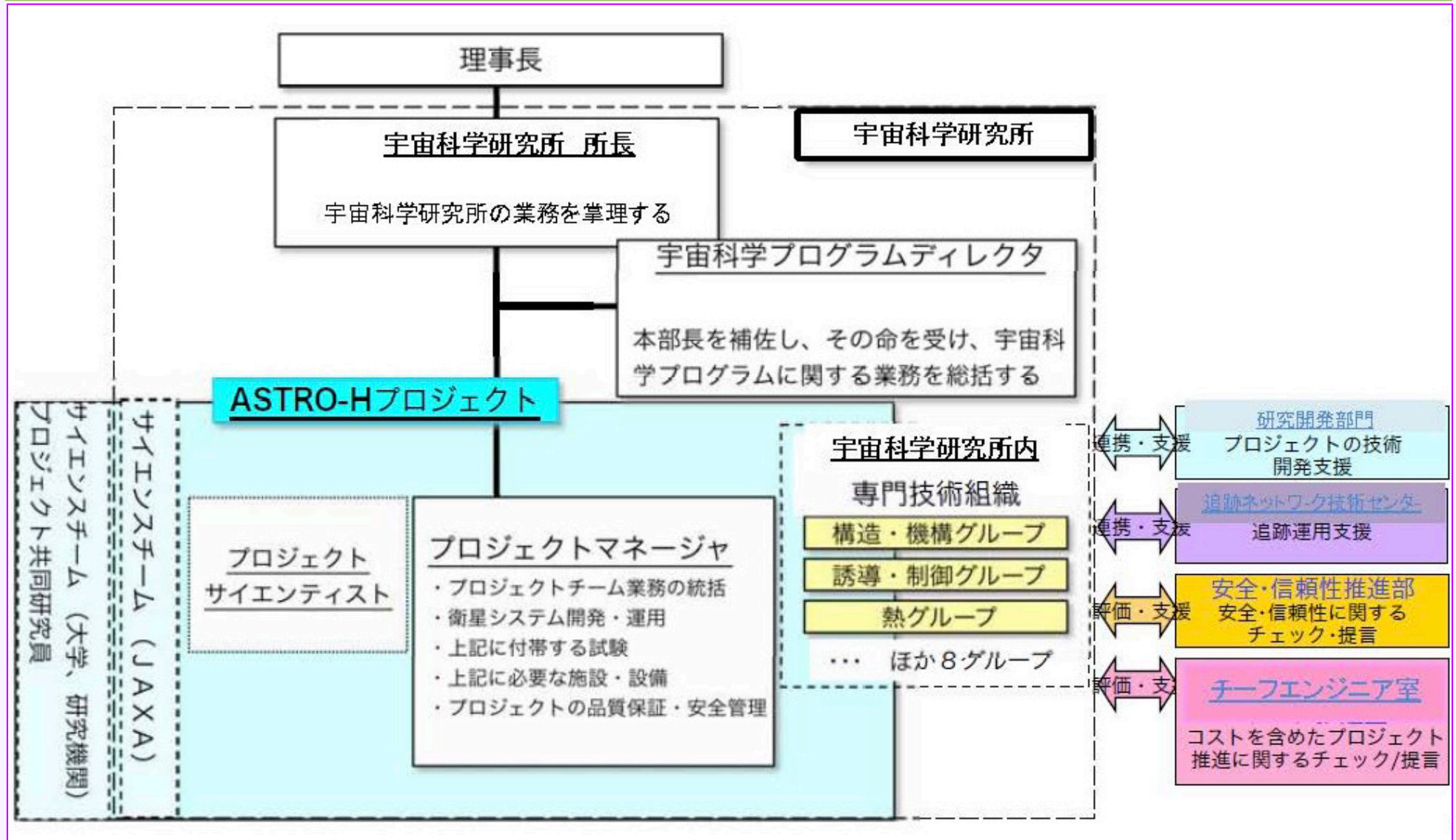
発注側のASTRO-Hプロジェクト全体を統括すべきプロジェクトマネージャは、高エネルギー宇宙物理学が専門の理学博士であり、衛星の工学的知見には乏しく、科学的成果創出面に専ら注力  プロジェクトマネージャは、衛星の安全・信頼性についてのプロジェクトマネジメントを事実上怠った。

このため、

衛星の安全・信頼性に関するリスクマネジメントが欠落し、その結果、『衛星の運用マニュアル』も不備となった。  姿勢変更系のデータ入力ミスを誘発した最大の原因。これでは、臨機応変のダメージコントロールなど不可能

  
\* 小惑星探査機「はやぶさ」のプロジェクトマネジメントとは真逆 \*

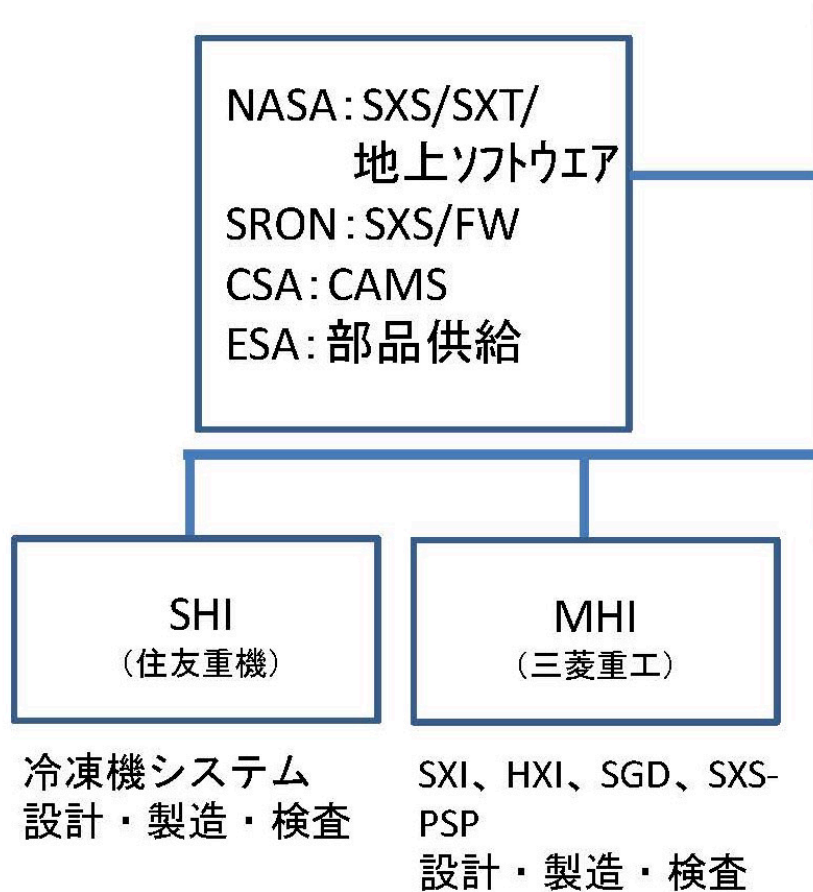
# X線天文衛星「ひとみ」の開発体制（JAXA内）



出典：X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書

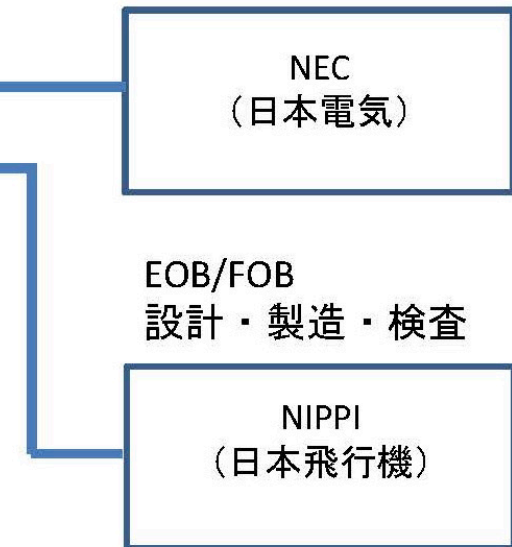
# X線天文衛星「ひとみ」の開発体制（他機関との関連）

## <ミッション機器関連>



## <衛星バス機器関連>

衛星バス機器(システム設計  
(姿勢系含む))  
設計・製造(調達)・検査



\* 大学共同利用システム研究員として、  
JAXA/ISASの一部をなす

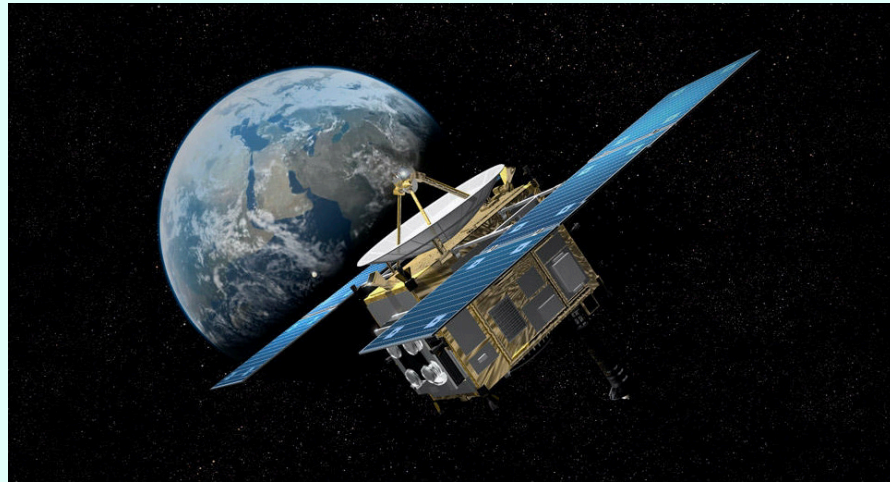
出典: X線天文衛星ASTRO-H「ひとみ」異常事象調査報告書

# III

**X線天文衛星「ひとみ」が残した教訓**

**大成功した小惑星探査機「はやぶさ」との対比を含めて**

# 大成功した小惑星探査機「はやぶさ」



出典：JAXA宇宙科学研究所のHP

2003年に、文部科学省の宇宙科学研究所(同年にJAXAの宇宙科学研究所に改組)が打ち上げた小惑星探査機 ➡ プロジェクトマネージャは、宇宙航行システム工学が専門の工学博士 ➡ 2010年に、小惑星「イトカワ」からのサンプルリターン(世界初)に成功

「はやぶさ」が遭遇したトラブル ➡ 「イトカワ」への往路では、大規模な太陽フレアで太陽電池パネルが損傷して発電出力が低下。姿勢制御用3軸リアクションホイールのx軸が故障。「イトカワ」では、3軸リアクションホイールのy軸も故障。姿勢制御用スラスターの1つから燃料漏れが生じて全スラスターの推力が大幅に低下。通信が2ヶ月近く途絶。

➡ いずれも放置すれば「致命傷」となる重大なトラブルであったが、事前の周到なリスクマネジメントが功を奏して、臨機応変かつ的確なダメージコントロールにより、計画変更やプログラム修正を行って困難を乗り越えることができた。 ➡ 正に奇跡の生還!



# 部分最適化ではなく全体最適化

X線天文衛星「ひとみ」のプロジェクト全体を統括するASTRO-Hプロジェクトの本来の役割は、プロジェクトの成功に向けて、「X線天体観測の精度と時間の確保」と「衛星の姿勢制御の信頼性の確保」の両立（全体最適化）を図ること

ところが、



ASTRO-Hプロジェクトは、「X線天体観測の精度と時間の確保」の最大化（X線天体観測の部分最適化）のみを追求 → 「X線天体観測の精度と時間の確保」と「衛星の姿勢制御の信頼性の確保」は、トレードオフの関係 → 「衛星の姿勢制御の信頼性の確保」の最小化に繋がった結果、空中分解事故が発生

このことから、



大規模なプロジェクトを運営して成功させるには、プロジェクト全体を「全体最適化」の視点で捉えることが極めて重要！ → ボトムアップではなく、トップダウンによるプロジェクト運営が欠かせない！

# トップダウンによるプロジェクトの全体最適化

**\* ボトムアップによる部分最適化の纏め上げでは失敗する！ \***

システムを構成する各部分ごとにそれぞれ最適化すれば、最適化された各部分を纏め上げた全体が最適化される？ → 各部分の間にトレードオフの関係があれば、全体最適化は不可能！ → プロジェクトの目的を見据えて、プロジェクトマネージャがトップダウンで全体最適化を図ることが重要



小惑星探査機「はやぶさ」のプロジェクトマネージャ → 宇宙航行システム工学が専門の工学博士で、衛星やロケットに関する豊富な経験と実績を有し、小惑星探査機の目的を踏まえた全体最適化に適任

X線天文衛星「ひとみ」のプロジェクトマネージャ → 高エネルギー宇宙物理学が専門の理学博士で、衛星の工学的知見に乏しく、「衛星の姿勢制御の信頼性に係る詳細設計」を含めた全体最適化には不適任 → 「衛星の姿勢制御の信頼性に係る要求性能」を含めた全体最適化であれば対処できたのでは！

# リスクマネジメントとダメージコントロール

## 【リスクマネジメント】

トラブルの発生に備えた事前対応であり、リスクマネジメントの結果を踏まえたマニュアルを作成

## 【ダメージコントロール】

トラブル発生時の事後対応であり、マニュアル化されていないトラブルにも迅速・的確に対応するには、事前のリスクマネジメントの徹底が肝要



X線天文衛星「ひとみ」 → 姿勢変更系データ誤入力の主因は、運用マニュアルの不備！ ← トラブルの発生に備えたリスクマネジメントが欠落！ → トラブル発生時の迅速・的確なダメージコントロールなど不可能！

小惑星探査機「はやぶさ」 → 事前に周到かつ徹底したリスクマネジメントを行って膨大なマニュアルを作成 → マニュアルでも想定外の幾多のトラブルに、迅速・的確なダメージコントロールで対処 → 奇跡の生還！

## 設計仕様の審査から要求性能の審査へ

### \* \* 設計審査会における審査の抜本的な見直しが必要 \* \*

今日では、ソフトウェアが衛星の安全・信頼性を大きく左右 → ソフトウェアの詳細設計の良し悪しについて、発注側の設計審査会で分析審査することは極めて困難  
→ 衛星の詳細設計を審査しようとする設計審査会では、ソフトウェアのバグを発見することもできない!



目に見えないソフトウェアが機能・性能を左右する発注では、実現したい機能・性能を要求要件として規定した発注仕様書を作成して、受注者に要求要件全ての達成を求めるのが効果的かつ現実的 → 設計審査会では、詳細設計の良し悪しの審査(つまり、設計仕様の審査)ではなく、発注仕様書に規定した要求要件の妥当性と要求要件に過不足がないか否かを審査(つまり、要求性能の審査)することが肝要 → 設計仕様の審査から要求性能の審査へ変えていかない限り、ソフトウェアが機能・性能を左右する案件の審査は形骸化する!

2021年3月27日

**X線天文衛星「ひとみ」の大失敗と  
小惑星探査機「はやぶさ」の大成功**  
～ 結果を左右したのは全体最適化の成否 ～

**終**

澤田雅之技術士事務所(電気電子部門)所長  
元警察大学校警察情報通信研究センター所長

澤田 雅之