特別論説

情報処理最前線

宇宙機搭載用フォールトトレラントコンピュータ†

檜原弘樹††　大塚　誠††　水島泰彦††
森里　司††　大島　武††　三好弘晃††
馬場研一††

1. 宇宙機搭載用オンボードコンピュータ (OBC) について

宇宙機搭載用オンボードコンピュータ (OBC) は，通常の計算機と比較するとその使用される環境において考慮されなければならないことが多い．

まず外部環境としては，宇宙空間特有の温度差や放射線環境を考慮する必要がある．温度差に関しては近年の衛星システム開発技術の進歩により運用中の衛星内部の温度変化を非常に緩やかにすることが可能となっている．しかしながら，輸送，打上げなども含めたライフサイクル全体を考慮した場合，コンポーネント単体として動作を保証する温度幅は依然として70度から90度にも達する．放射線環境としては惑星の近傍や太陽風などに含まれるγ線などの放射線，および銀河宇宙線などに含まれる重粒子イオンなどが存在する．前者は主として，その総線量によるデバイス特性の劣化を招き，後者はシングルイベントアップセット(データの反転など)，ないしはラッチアップ☆ などの過渡フォールトを引き起こす．こういった放射線の影響に対して耐性をもたせる必要がある．

さらに，打ち上げた後は保守を行うことがまず不可能であるため，MPU の暴走や他の機器のテレメトリ・ステータスエラーなどの機能レベルのエラーについても十分考慮する必要がある．特に衛星自体の運用にかかわるバス系と呼ばれる機器については故障が検出されても破局的な故障には至らず，最悪の場合においてもいったんミッションを中断し，マニュアル操作によってオペレーション／復帰ができるようなフェイル・セーフ機能が必要とされてきた．

近年の宇宙開発においてはロケットや人工衛星などの宇宙機自体の開発から，宇宙機の提供する機能，サービスの高度化へと重点が移ってきている．有人活動のサポートが要求される一方で，微小重力を必要とし，ごくわずかな振動さえも排除するために意図的に無人環境とするミッション要求もあり，無人機に対する要求も高度化してきている．また，有人活動を協調的に支援するための遠隔操作などの自動化技術も求められるようになってきた．

人工衛星／人工惑星に関してみれば，そのミッションは，通信衛星や放送衛星に代表される通信機能，および気象衛星や地球観測衛星，深宇宙プローブに代表されるセンサ機能が主である．特に後者のセンサを使用するミッション要求の高度化は顕著であり，ミッション機器のインテリジェント化が進み，MPU を内蔵したセンサが増えてきている．さらに個々のセンサを有機的に統合して運用する自動化・自律化運用を司るための OBC も求められるようになってきた．通信機能についても自動追尾・捕捉のための通信装置やアンテナ駆動装置のインテリジェント化が進んでおり，これらにも MPU が使われるようになってきた．

有人活動の支援，あるいは代替としての軌道上

† Fault Tolerant Computers for Spacecrafts by Hiroki HIHARA, Makoto OHTSUKA, Yasuhiko MIZUSHIMA, Tsukasa MORISATO, Takeshi OHSHIMA, Hiroaki MIYOSHI and Ken-ichi BABA (Sensors and Electronics Systems, Space Systems Development Division, NEC Corporation).

†† 日本電気(株)　宇宙開発事業部　搭載機器開発部

☆ 過度の電荷により CMOS デバイスなどの内部に存在する寄生ダイオードが活性化され，デバイス内部で短絡を起こす現象．

作業機に搭載されるロボットの運用も，これから重要性が増してくるミッションの一つである．

これらのミッション機器では従来のフェイル・セーフからさらに進み，異常・故障が生じてもミッションを継続するフェイル・オペラティブ機能が求められるようになってきている．

宇宙機自体の運用に用いられるバス系機器についても，宇宙往還機による物資の輸送や軌道上作業機による衛星・プラットフォームなどへの軌道上サービスの提供のためのランデブ・ドッキング技術の要求などにより，フェイル・オペラティブ機能が求められてきている．バス系機器は宇宙機の寿命や安全性を直接左右するものだけに，ここに求められるフェイル・オペラティブ機能は信頼性の高いものでなければならない．

したがって，これらのミッション機器，およびバス機器に使用される OBC への耐故障性の要求はますます高度化してきており，フェイル・セーフ，さらにフェイル・オペラティブ機能を実現するためのさまざまなアーキテクチャが開発されている．

2. MPU 多重化方式の比較と各方式の課題

宇宙機における MPU 多重化の目的は，単一点故障（シングル・ポイント・フェイリャ）を除去することである．すなわち，一部分の異常・故障によりシステム全体の機能が失われることを防止することを目的とする．

MPU の多重化方式はコールド・スタンバイ方式，およびホット・スタンバイ方式に大別される．前者は待機冗長方式に代表されるものであり，通常は一系統のみ運用しており，異常・故障が生じた場合には他系に切り替えて運用を再開するものである．我が国ではこの方式は科学衛星の姿勢軌道制御装置に早くから用いられている．衛星のミッション機器やアンテナを常に地上に向け地球を周回する地球指向制御の多い実用衛星に比べ，センサを地球を含めた各種天体に向けるために比較的任意な姿勢軌道制御を行う科学衛星の姿勢軌道制御装置は，バス系機器の中では最もインテリジェント化が進んだものと言える．

本方式はその性格上，主系から冗長系への切替に時間がかかるため，主としてフェイル・セーフ機能に重点が置かれたものである．

後者のホット・スタンバイ方式は多重構成系を同時に運用するものである．この方式には以下のようなものがあげられる．

多数決方式

各 MPU の入出力に多数決回路を設け，一つの MPU が異常・故障を起こしても，全体的には停止しないシステム．

しかし，本方式は，多数決回路自身の異常・故障には対応できていない．すなわち，MPU は多重化されているものの，通常は多数決回路で信号は一点に集中しており，多数決回路自身の異常・故障はシステムダウンにつながる．したがって，本システムでは，多数決回路自身が単一点故障（シングル・ポイント・フェイリャ）につながっている．

通常は，多数決回路として耐放射線性，および高信頼性を有する特殊なデバイスを用いることで対処しているが，これは，デバイスの故障率に依存した確率的な故障率低下を狙ったものであり，機能的な解決策とは異なる．

また，多数決回路自体を多重化する対応策もあるが，いずれにしても，入出力が一点に集まる点があり，システム的にも重量，消費電力などが増大する．

さらに，多重度を増すにあたり，たとえば，三重多数決を四重多数決に拡張する場合，多数決回路周りが新規設計となる．すなわち，多数決回路の存在が，システムの拡張性を阻んでいる．

一方でこの方式は最も早くから検討されており，使用実績も多く，さまざまな改良が施されている．

我が国における代表的なシステムとしては，平成6年度打上げ予定の技術試験衛星VI型（ETS—VI）に搭載される姿勢制御装置があげられる[1]．このシステムでは，システムバスの二重化，記憶部の三重多数決化などが用いられ，信頼度の高いシステムが構成されている．また，姿勢制御装置に対する要求を考慮することにより多数決回路に起因する単一点故障を排除する構成を実現している．これについては後で述べる．

ソフトウェア通信方式

これは，各 MPU が基本的には並行して処理を行い，あらかじめ決められたチェックポイントにおいて互いに通信を行い，データの照合を行いな

がら処理を進めていくものである．この方式は，異常・故障が起こった場合，故障の分離，システムの再構成，および再同期（正常な MPU にマスタ機能を移し，ロールバック処理などを行ってシステムの動作を続行する）が比較的容易に行える．

組み込まれるソフトウェアは常に通信・照合方式をインプリメントしなければならず，その結果，本方式が適用されるシステムは比較的大規模なシステムに限定される．

また，複数の MPU をシステムバスに接続する場合，やはり多数決回路などによって信号を一つにまとめる必要があり，このハードウェア自体は本方式にとって本質的でないにもかかわらず，単一故障点（シングル・フェイリャ・ポイント）を内在せざるをえないジレンマをもっている．

一方，本方式はソフトウェアによる通信を利用することから，既設計の計算機を流用することを可能にする．スペースシャトルに用いられているガイダンス・コンピュータは，この特徴をうまく利用している[2]．我が国では科学衛星「ひてん」に搭載された OBC が本方式を用いている[3]．この OBC はデバイスのハイブリッド化を行い，小型化を達成している．我が国の高度なデバイス技術の好例と言えよう．

FRM (Functional Redundancy Monitor) 方式

本方式は MPU に，自己の（アドレス，データ，ステータス）バス出力と外部のバス信号の内容とが一致しているか否かの比較監視機能をもたせるものである[4]．MPU は監視モード／通常モードの走行モードを指定できる．通常モード走行のプロセッサはこの比較回路を動作させずチップ内の処理結果をそのままバスに出力する．監視モードのプロセッサはチップ内の処理結果をバスに出力せず比較回路の入力とし，また外部バスからの信号を比較回路のもう一方の入力とする．したがって，各プロセッサのデータバス，アドレスバス，ステータス信号線はおのおの単純に Pin-to-Pin 接続するだけでプロセッサ間でお互いの処理内容の監視をすることができる．比較回路が不一致を検出すると監視モードのプロセッサは専用端子を通じて外部回路に対しこれを通知する．

この方式は，上記の 2 方式に対し，以下のような利点を有している．

- 比較・検出回路が各 MPU にそれぞれ内蔵されているため，多数決方式と異なり，これらの回路が単一故障点とならない．
- ソフトウェア通信方式と異なり，常時信号の比較が行われる．また，MPU 上のソフトウェアは，比較が行われていることを通常は意識する必要がない．

しかしながら，宇宙機搭載を考慮した場合，解決すべき問題は少なくない．主要なものとして，下記のものが上げられる．

- MPU 内蔵の機能であるため，使用する MPU が限定される．国産の宇宙機搭載用 MPU としては，宇宙開発事業団認定品として μPD 55040 B—028 (8 bit)，T 4915 (16 bit)，V 70 (32 bit) があり，また今後認定が予定されている H 32 (32 bit) がある．さらに，我が国初の宇宙機搭載用 16 bit MPU であり，搭載実績も豊富な μPD 55090 B—012 がある．しかしながら，FRM 機能を有するものは V 70 のみである．また，我が国で入手可能な海外製の宇宙機搭載可能な MPU でも FRM 機能を有するものはなく，実質的に本方式を用いることのできる MPU が限定されてしまう．
- 再構成を行うためには，多数決回路相当のものが必要となる．具体的には，N 重系を構成する各 MPU の出力する異常検出信号をまとめて判断し，正常な MPU を選択した上でバス上に信号を出力する権利をもつ MPU を指定する機能が必要となる．なぜなら，各 MPU が誤って異常検出信号を出力してくる可能性があるためである．

したがって，この異常検出量信号をとりまとめて判断する部分は，構成法によっては多数決回路のように単一故障点となり得る．

この方式を用いた代表的な OBC としては，宇宙ステーション日本実験モジュール (JEM) に搭載予定であり現在開発が進んでいる通信制御装置 (JCP) があげられる[5]．

3. 単一点故障回避のための具体的開発例

2. にあげた従来方式の課題を解決するために種種のアーキテクチャが開発されている．本章では特に，無人宇宙機向けに開発された代表例について述べる．

3.1 技術試験衛星 VI 型 (ETS—VI) 搭載用 ACE

ETS—VI 搭載用 ACE (姿勢制御電子回路) 内に実装された計算機は，ETS—VI の頭脳とも言えるもので，16 ビットの CPU モジュール 4 台を内蔵している．各 CPU モジュールにはそれぞれ 3 重多数決ローカル RAM をもち，システムバス，共有メモリモジュール，出力ポートなども 2 重化されており，さらに共有メモリモジュール内の RAM も 3 重多数決化されている．

上記のように各モジュール内の RAM が個々に 3 重多数決化されているが，一方，システムバス・インタフェースに関しては，Duplex 方式がとられている．計算機部をフォールトトレラント化する際に，2 CPU 並列運転 (Duplex) 方式と 3 重多数決方式の比較が行われているが，姿勢制御において数サイクルの制御の中断は許容可能なため，信頼度・消費電力の点から Duplex 方式が採用されている．

本方式は大規模なシステムであるが，多数決回路に起因する単一点故障を回避するとともに，システム要求の範囲内においてフェイル・オペラティブを実現し得るシステムと言える．

3.2 新しい MPU 多重化方式の開発

前項のようなシステム的アプローチに対し，フォールトトレラント計算機のもつ各機能（演算機能，故障検出機能，故障分離／再構成機能，および再同期機能）の分散化を図ることによって単一点故障を回避するアプローチがある．

筆者らは後者のアプローチにより新しい MPU 多重化方式の開発を行った．本方式には，下記の特徴をもたせることを目標とした．

- 原理的に単一故障点を有しないこと．すなわち，一つのデバイスの故障によって，システムダウンにつながらないこと．
- どのようなデバイスにも適用可能であること．MPU の世代交代は速い．特定の MPU に依存した方式としたのでは，MPU の寿命とともに多重化方式の寿命も尽きてしまう．また，汎用の MPU ばかりではなく，デジタル・シグナル・プロセッサ (DSP)☆ などの特殊用途プロセッサや，周辺素子などにも拡大して適用できることが望ましい．
- 多重度を容易に高められること．たとえば，三重冗長システムから四重冗長システムへほとんどハードウェアの再設計を必要とせずに拡張できることが望ましい．
- ソフトウェアは原則として多重化されていることを意識せずに済むこと．宇宙機上の OBC に搭載されるソフトウェアは年々大規模になってきている．ソフトウェアを開発する場合に，なるべく負荷を少なくする必要がある．
- システムがリアルタイムで再構成されること．バスの制御権を有する MPU に異常が発見された場合，バスマスタの交代のためにシステムの動作を中断する時間を極力なくすものとする．

3.3 CRAFT システムの概要

前節の方針に基づき筆者らが開発した，CRAFT (Compare and Rational Abort for Fault-Tolerant) システムの概要について述べる．

図-1 は試作機 (OFD-1) の全体構成図であり，

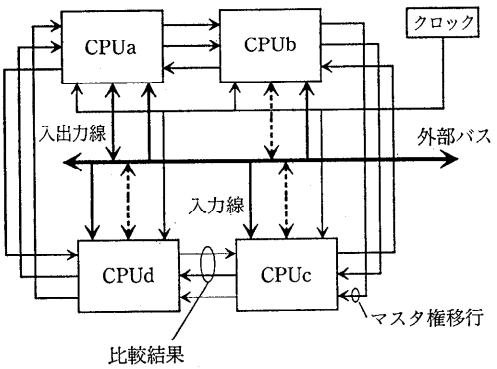


図-1 CRAFT システム構成

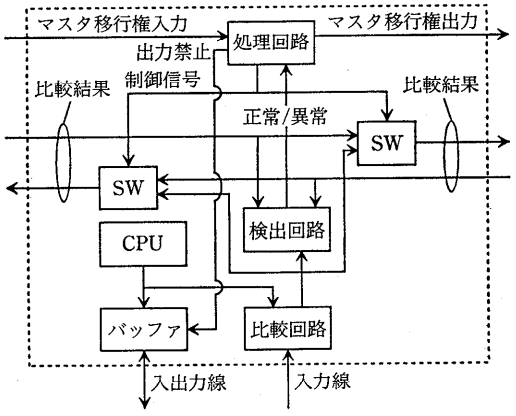


図-2 CPU モジュール構成

☆主としてフィルタリング処理や制御則の演算のために加算，乗算を高速に実行できるアーキテクチャをもつプロセッサ．行列演算機能をもつものなどのバリエーションがある．

各 CPU モジュールは異常検出ネットワークを構成している．**図-2** はそのうちの一つの CPU モジュール a の詳細図を示す．

（1） 異常検出ネットワーク

MPU および周辺回路からなる 4 個のおのおの独立した CPU モジュールは，それぞれ外部に出力を伝える外部バスに入出力線を介して接続されている．各 CPU モジュールは外部バスの内容と自モジュール内の MPU からの入出力とを比較回路で比較するために，外部バスの内容を取り込む入力線を有している．

これら 4 つの CPU モジュールは同一クロックで同期して動作しているが，外部入出力線に対する出力権はその中の一つの CPU モジュールにだけ与えられる．これをマスタ CPU と呼び，それ以外をチェッカ CPU と呼ぶ．図-1 では CPU モジュール a がマスタ CPU，それ以外はチェッカ CPU であり，チェッカ CPU は出力バッファにより外部バスへの出力が断たれているので入出力線が点線で表されている．

各 CPU モジュールは出力比較信号線を通じてリング状に接続され異常検出ネットワークを構成しており，各 CPU モジュール内部に設けられた比較回路の出力である比較結果と，両隣に接続された CPU モジュールから出力される比較結果との合計三つの信号とから自 CPU モジュールが正常か異常かを判断する検出回路をもつ．

（2） 故障検出，および再構成機能

各検出回路は自 CPU モジュールが異常と判断した場合，自身をネットワークから論理的に切り離し，マスタ権を隣接した CPU モジュールに移管し，自モジュールの比較結果と隣接 CPU モジュールからの比較結果入力とを切り換えて（すなわちバイパスして）隣接 CPU モジュールに出力する回路を有している．

各 CPU モジュールはバスサイクルごとに比較回路により自モジュール出力と外部バスに出力されているマスタ CPU モジュール出力との比較を行い，自モジュールの比較結果と両隣接モジュールからの比較結果を検出回路に取り込む．両隣接モジュールと自身の比較結果から自身の正常／異常は完全に判定できる．そしてもし自モジュールが異常と判断された場合は処理回路からのコントロール信号によりスイッチが切り換えられ隣接 CPU モジュールからの比較結果入力が異常 CPU モジュールをバイパスして隣接 CPU モジュールへ出力される．これにより異常な CPU モジュールはシステムから隔離され，4 個の CPU モジュールから構成されていたシステムから 3 個の CPU モジュールから構成される縮退システムへの再構成が瞬時に行われる．

マスタ MPU に異常が発生した場合は，処理回路からの出力禁止信号により出力バッファが出力禁止状態となり，マスタ MPU としての機能は取り除かれる．その後，処理回路からのマスタ移行出力信号により隣接 CPU モジュールが制御権を得，マスタとして機能するようになる．隣接 CPU モジュールからのマスタ移行入力信号により外部出力線への出力権が得られた場合は処理回路からの出力禁止信号を解除することによってマスタ CPU モジュールとなる．これらの動作により本システムでは異常出力はマスクされ，常に正常な出力が期待できる．

（3） 本方式の特徴

本方式では多数決方式における多数決回路のような外部共通回路を必要とせず，単一故障点をシステムから排除することが可能である．さらに各モジュールとも同一構成にて実現可能であるため，3 モジュール以上であれば理論的に N 重 ($N \geqq 3$) まで回路の変更なしに拡張可能であり，システム冗長性要求の変化に対して容易に対応可能である．また本方式は対象となるモジュールが MPU である必要はなく，DSP や I/O プロセッサなど他の機能デバイスにも応用可能である．

縮退モードへの遷移がソフトエラーによるものであった場合，隔離モジュールを再同期させることにより初期状態への復帰が可能である．この操作は障害発生モジュールの再同期，およびそれがソフトエラーか永久故障かを判断するためのチェックシーケンスを含むため，処理の複雑化が予想される反面，縮退モードでの運転による処理能力の低下はないので本シーケンス起動に対する時間的制約は低い．ゆえに再同期処理はハードウェア的に処理されるのではなく，ソフトウェアの処理負荷の低いタイミングを見計らって起動されるべきものと考えられ，オペレーティングシステムのシステムコールとして実現するのも適当であろう．

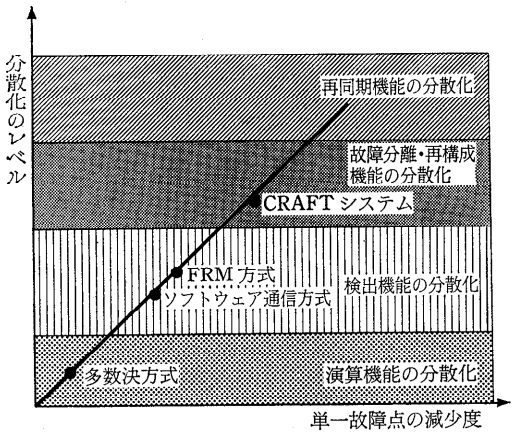


図-3 フォールトトレラント OBC 開発トレンド（フォールトトレラント性の各機能に着目した場合）

（4） CRAFT 方式の応用，および開発計画

今回の試作機（OFD-1）は汎用 MPU をターゲットとして開発された方式であるが，プロセッサ・アーキテクチャに依存しない方式であることから，視覚センサなどへの適用が期待される DSP，および近年高度化している I/O プロセッサなどへの応用も可能である．

本方式の開発に際しては，フォールトトレラントコンピュータの各機能に着目したアプローチがとられたが，その開発トレンドに関しては**図-3**に示すように今回は再構成機能までが分散化されている．したがって今後は，再同期処理の分散化の開発検討がなされることになろう．

また，実際の宇宙機搭載用モデルの開発も進められているが，これにあたっては**3.1**に示されたようなシステム的アプローチも併用されることになる．

4. ま と め

近年，宇宙機搭載用機器はますますインテリジェント化している．本稿ではこれらの機器に用いられるフォールトトレラントコンピュータが単一点故障を防ぐことを主目的として開発されていることを述べ，まず耐故障性を実現する各方式について実際の開発例を含めて概説した．さらに，単一点故障を回避するための具体的な開発例としてシステム的な多重度を最適化するアプローチによるもの，および耐故障性を実現するために必要な各機能の分散化を高めるアプローチによるものを紹介した．

H—Ⅱ ロケットの打上げ成功により，我が国の宇宙開発はより主体性を要求される新たな時代を迎えた．宇宙機搭載用フォールトトレラントコンピュータの分野においても今後は諸外国の技術開発動向を参考にするとともに，独自のニーズに基づいたアーキテクチャの研究開発もさらに重要性を増すものと考えられる．

謝辞　本稿をまとめるにあたり，適切な助言をしていただいた，NEC C&C 研究所コンピュータ・システム研究部の中田登志之氏に感謝します．

参 考 文 献

1) 川田恭裕，石毛康夫：人工衛星姿勢制御用コンピュータシステム，信学誌，Vol. 73, No. 11, pp. 1215-1221 (1990).
2) Sklaroff, J. R.: Redundancy Management Technique for Space Shuttle Computers, IBM J. R&D, 20, 1, p. 20 (1976).
3) 金川信康，井原廣一：宇宙機搭載用コンピュータ—汎用 LSI によるシステム構成—，信学誌，Vol. 73, No. 11, pp. 1209-1214 (1990).
4) 古城　隆，矢野陽一：汎用マイクロプロセッサチップ，信学誌，Vol. 73, No. 11, pp. 1222-1227 (1990).
5) Yamazaki, K., Hosaka, K., Morita, N., Ishii, S., Kikuchi, T. and Nakamura, T.: Development Model of Main Processing Controller for Japanese Experiment Module, NEC R&D, Vol. 34, No. 3, pp. 385-395 (1993).

（平成 6 年 1 月 5 日受付）

檜原　弘樹

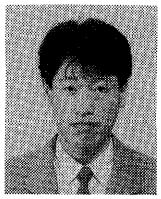
1962 年生．1986 年大阪大学大学院工学研究科電子工学専攻前期課程修了．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部主任．宇宙機搭載用計算機，インテリジェント・センサ，および画像処理装置の開発に従事．応用物理学会会員，および IEEE Member.

大塚　誠

1956 年生．1980 年慶應義塾大学工学部計測工学科卒業．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部技術課長．衛星搭載用電子機器の開発，およびデータ処理系サブシステムの開発に従事．

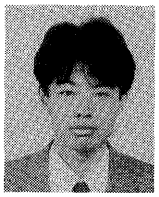
水島 泰彦

1958 年生．1981 年横浜国立大学工学部情報工学科卒業．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部主任．衛星搭載用各種電子機器の開発に従事．



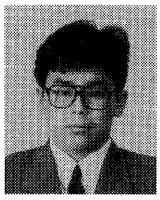
森里 司

1964 年生．1987 年三重大学工学部電子工学科卒業．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部勤務．衛星搭載用データバスの開発に従事．



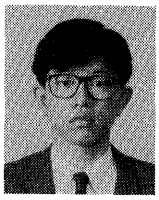
大島 武

1966 年生．1990 年東京大学大学院工学系研究科電子工学修士課程修了．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部勤務．衛星搭載用実験系制御装置の開発に従事．電子情報通信学会会員．



三好 弘晃

1967 年生．1991 年東京大学大学院工学系研究科航空学修士課程修了．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部勤務．衛星搭載用計算機，および電気推進の開発に従事．



馬場 研一

1965 年生．1991 年東京大学大学院工学系研究科航空学修士課程修了．同年，日本電気(株)入社．現在，宇宙開発事業部搭載機器開発部勤務．衛星搭載用メカトロニクス，および制御系機器の開発に従事．