宇宙科学研究報告
特集　第28号　1991年3月

「ひてん」OBCのフォールトトレランス実験

高野　忠・山田　隆弘・周東晃四郎
金川　信康*・田中　俊之*

Fault-Tolerance Experiments of the "Hiten" Onboard Computer

By

Tadashi Takano, Takahiro Yamada, Kohshiroh Shutoh,
Nobuyasu Kanekawa* and Toshiyuki Tanaka*

Abstract: In this paper, the authors report the results of experiments for the verification of fault-tolerance using an onboard computer which was loaded on "Hiten" launched on Jan. 24 1990. The experiment aims at observing (1) System behaviour in response to intentionally introduced faults, (2) SEU in space.

Tolerance against intentional faults was verified to satisfy the requirements.

The function to record faults occurence was added after the launch in order to collect the field data. Eight 1-bit errors in RAM due to SEU were observed from 14:16 5th Jul. to 10:05 3rd Aug. 1990 (UT). The SEU at 02:09:14 on 26th Jul. might be caused by the solar flare of importance 2N from 22:00 on 25th Jul. to 01:51 on 26th Jul. Other SEU's did not have any correlation with solar flare occurances, and were probably caused by galactic cosmic-rays.

概　要

1990年1月24日に打ち上げられた「ひてん」OBC（搭載コンピュータ）を用いたフォールトトレランス実験の概要及び結果について報告する．本実験は，(1) 人為的に発生させた誤りへのシステムの対応，(2) 軌道上での稼働状況を見るものである．

人為的に発生させた誤りに対してはシステムは設計仕様通り動作することを確認した．軌道上での稼働状況監視については，誤り発生を記録する

* ㈱日立製作所

機能を打ち上げ後にOBCへのリモートローディングにより追加した．この機能により7月5日14：16（UT）から8月3日10：05（UT）の28.86日間に，RAMでSEUによって8回の1ビット誤りが観測された．このうち7月26日02：09：14（UT）にCell Cで発生したSEUは，7月25日22：00～7月26日01：51（UT）に発生した重要度2Nの太陽フレアの影響と見られ，他のSEUは太陽フレアとの相関は認められず，銀河宇宙線に由来するものと考えられる．

重要語　フォールトトレランス（Fault-Tolerance），
シングルイベントアップセット（Single Event Upset），
宇宙機搭載用コンピュータ（Onboard Computer）

1．はじめに

宇宙線によるシングルイベントアップセット（SEU：Single Event Upset）やラッチアップ，そして部品の劣化[1]に対処するために，従来から採用されていた部品の耐環境性を強化するアプローチに加え，最近ではフォールトトレランス（FT：Fault-Tolerance）技術を用いてシステム的に耐環境性を強化するアプローチについても研究されている[2]－[6]．

FT技術によるシステム的な耐環境性強化が有効であることが実証されれば，宇宙用電子機器に使用する部品の制約を大幅に緩和でき，開発コストの削減，処理性能の向上，小型軽量化，低消費電力化が容易に可能となろう．

1990年1月24日に打ち上げられた「ひてん」には，FT技術によるシステム的な耐環境性強化の有効性を実証するためにフォールトトレランスコンピュータが搭載されている．

本報告では，「ひてん」OBC（Onboard Computer）を用いた軌道上でのフォールトトレランス技術の実証実験の概要と実験結果を報告する．

2．「ひてん」OBC

2．1　概要

本OBCは(1) FT技術の実証実験，(2) パケットによる高効率テレメトリデータ伝送実験のために「ひてん」に搭載されている．通常モードではパケットテレメトリ作成のためのアプリケーションタスクが稼働しており，アプリケーションタスクの高信頼度動作をFT機能がサポートしている．また本OBCには，パケットテレメトリ作成機能のほかにリモートローディング機能も備わっており，この機能により地上よりプログラムをロード，実行することができる．このリモートローディング機能は後述するように，今回の一連の実験で重要な役割を果たしている．

本OBCではFT技術により最新の半導体技術が宇宙でどこまで実用になるかを実験するためにプロセッサなどには汎用のLSIにスクリーニングを施したものを使用している．またFT技術としては，次節で述べるSNV（Stepwise Negotiating Voting）方式を採用している．本OBCの仕様を表1に，外観を写真1に，衛星内での搭載位置を図1に示す．

表1．OBCの仕様

フォールトトレランス方　式	SNV方式
プロセッサ	HD68HC000ベース
オペレーティングシステム	HI68K(ITRON*仕様) +フォールトトレランス機能
メモリ容量	64Kbyte + ECC
冗長度	3重系(4重系構成まで可)
寸　法	260 x 210 x 76 (mm)
重　量	2.6 kg
消費電力	1.8 W　(5V D.C.)

*TRONはThe Realtime Operating System Nucleusの略である。

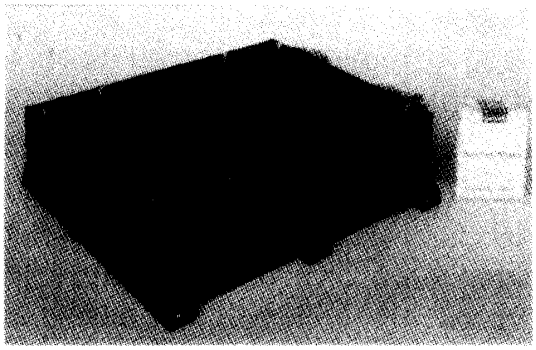

写真1　OBCの外観

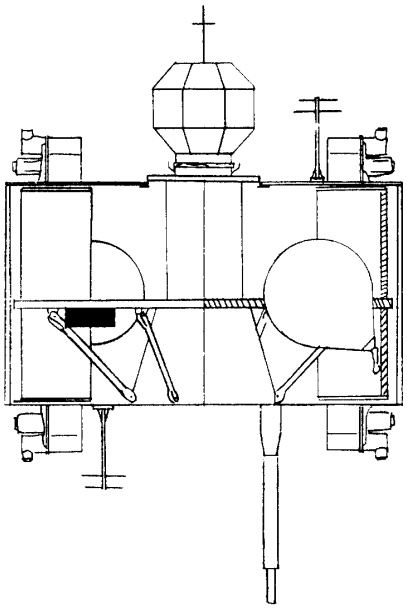

図1．衛星内でのOBCの搭載位置

2．2　SNV方式

先の述べたように，宇宙ではSEUと呼ばれる過渡フォールトが地上と比べて高い頻度で発生する．過渡フォールトは文字通り一過性のもので再現性がないために，検出が困難で検出漏れが多い．

また一旦打ち上げたあとの修理は極めて困難なため，OBC内で発生した固定フォールト（永久故障）は蓄積され多重フォールトとなる．従来から広く用いられていた多数決冗長方式は図2に示すように過半数のコンピュータモジュールが正常ならば，正常に動作することができる優れた方式である．しかし，固定フォールトが蓄積され過半数のコンピュータモジュールが異常となった場合には，原理的に多数決が成り立たないため正常な動作を継続できなくなる．

そこで筆者らは誤り検出，出力の比較照合（多数決）等の検査結果を組合せ，それぞれの検査の検出漏れの確率に基づき，コンピュータモジュールが「正常な確率」を推定し，「正常な確率」が最も高いコンピュータモジュールの出力を選択するSNV方式を提案した．簡単のために検査機能が誤り訂正符号による誤り検出機能と，処理結果の比較照合の2つであるとすると，各コンピュータモジュールが「正常な確率」は検査結果によって図3のように表される．本OBCでは検査結果として，この他に多重化データの比較照合結果等を用いている．なお本OBCでは，他のモジュールからの異常な通信を遮断する免疫機構をモジュールに持たせていることから，モジュールを生物の細胞に見立ててCellと呼んでいる．

図4に本方式を実現するためのシステム構成を示す．各々のCellでの処理結果はCell間で交換されて，比較照合される．また誤り検出符号等による自己検査の結果も同様に交換される．このようにして収集されたデータの比較照合結果や自己検査結果に基づき，各Cellの「正常な確率」が推定され，「正常な確率」が最も高いCellの出力が選択される．ここまでの確率推定，データ選択の動作は各Cellで行われ，さらにCellの故障による誤ったデータ選択を防ぐためにMV（Modoified Voter）と呼ばれる選択機能付き多数決回路でハード的にデータを選択している．MVには各Cellから出力信号と共に自分が正常とみなされているかどうかを表すステータス信号が入力され，ステータスが“正常”であるCellの出力

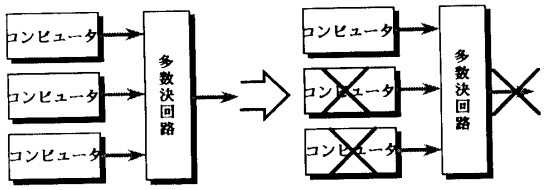

図2．多数決冗長方式

自己チェック	データ照合	Rd	グレースケール
正　常	一　致	$1-P_{\varepsilon}\cdot P_{a\varepsilon}\cdot P_{d\varepsilon}$	
誤り検出	一　致	$1-P_{\varepsilon}\cdot P_{a\varepsilon}$	
正　常	不一致	$1-P_{\varepsilon}\cdot P_{d\varepsilon}$	
誤り検出	不一致	——	

図3．SNV方式

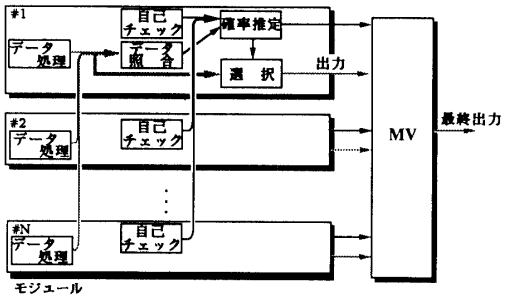

図4．SNV方式のシステム構成

信号の多数決を採る．

3．実験の方法及び結果

3．1　誤りの人為的な発生

誤りを人為的に発生させるプログラムを地上からリモートローディング機能を用いてロードし，動作させる事により人為的な誤りに対しての耐性を確認した．注入した誤りの種類は以下のとおりである．

(1)　他Cell異常の検出

他Cellからの通信異常を検出し，異常発生Cellとの通信路を遮断する機能を確認する．

異常発生の方法：通信データ種別コード書き替え

(2)　自己の異常出力抑制

SNV方式の確率推定により自己の異常を検出し，自己の出力を抑制し，さらにフォールトステータスを“Fault”にして自己の出力がMVで選択されないようにする機能を確認する．

異常発生の方法：処理結果データの書替

(3)　暴走検出

暴走を検出するための機能を確認する．

異常発生の方法：不正アドレスへのジャンプ

これら3つの実験においてOBCが正常に動作することが確認できた．なおこれらの実験試験は，打ち上げ前に地上試験としてすでに実施されていることは言うまでもなく，打ち上げ後に再度実施するのは軌道上での機能試験も兼ねるためである．

3．2　フィールドデータの採取

3．2．1　リアルタイムテレメトリデータによる方法

衛星各部の温度，電圧，電流などのハウスキーピングデータのほかにOBCなどの搭載機器の状態などがリアルタイムテレメトリデータとして衛星から地上に送られてくる．従って，衛星からのリアルタイムテレメトリデータをモニタすれば地上にいながらしてOBCの動作状況を時々刻々と知ることができる．表2にリアルタイムテレメトリデータの中のOBCについての情報を示す．

しかし，当初予定していた本方法には以下のような問題点がある．

(1)　受信時間の制限

表2．リアルタイムテレメトリデータ

FW	機器	B	項　目	状態判別
*F4n・W26	OBC	B0	OBC	1:ON 0:OFF
		B1	OUT MODE	1:MSB 0:
		B2		1: 0:
		B3		1:LSB 0:
		B4	BPU-A	1:FAULT 0:
		B5	A/B	1:DISCON 0:
		B6	A/C	1:DISCON 0:
		B7	(予備)	1: 0:
*F4n+1・W26	OBC	B0	I/F	1:STOP 0:
		B1	SELECTOR MODE	1:MSB 0:
		B2		1: 0:
		B3		1:LSB 0:
		B4	BPU-B	1:FAULT 0:
		B5	B/C	1:DISCON 0:
		B6	B/A	1:DISCON 0:
		B7	(予備)	1: 0:
*F4n+2・W26	OBC	B0	A	1:DISAGR 0:
		B1	B	1:DISAGR 0:
		B2	C	1:DISAGR 0:
		B3	(予備)	1: 0:
		B4	BPU-C	1:FAULT 0:
		B5	C/A	1:DISCON 0:
		B6	C/B	1:DISCON 0:
		B7	(予備)	1: 0:
*F4n+3・W26	OBC	B0	(予備)	1: 0:
		B1	(予備)	1: 0:
		B2	(予備)	1: 0:
		B3	(予備)	1: 0:
		B4	(予備)	1: 0:
		B5	(予備)	1: 0:
		B6	(予備)	1: 0:
		B7	(予備)	1: 0:
*F4n・W27	OBC	B0	CELL-A	1:ON 0:OFF
		B1	〃	1:STOP 0:
		B2	〃	1:RES 0:
		B3	BPU-A	1:1 BIT ERROR 0:
		B4	〃	1:2 BIT ERROR 0:
		B5	BPU-A MODE	1:MSB 0:
		B6		1: 0:
		B7		1:LSB 0:
*F4n+1・W27	OBC	B0	CELL-B	1:ON 0:OFF
		B1	〃	1:STOP 0:
		B2	〃	1:RES 0:
		B3	BPU-B	1:1 BIT ERROR 0:
		B4	〃	1:2 BIT ERROR 0:
		B5	BPU-B MODE	1:MSB 0:
		B6		1: 0:
		B7		1:LSB 0:

FW	機器	B	項　目	状態判別
*F4n+2・W27	OBC	B0	CELL-C	1:ON 0:OFF
		B1	〃	1:STOP 0:
		B2	〃	1:RES 0:
		B3	BPU-C	1:1 BIT ERROR 0:
		B4	〃	1:2 BIT ERROR 0:
		B5	BPU-C MODE	1:MSB 0:
		B6		1: 0:
		B7		1:LSB 0:
*F4n+3・W27	OBC	B0	(予備)	1: 0:
		B1	(予備)	1: 0:
		B2	(予備)	1: 0:
		B3	(予備)	1: 0:
		B4	(予備)	1: 0:
		B5	(予備)	1: 0:
		B6	(予備)	1: 0:
		B7	(予備)	1: 0:
*F4n・W28	OBC	B0		1:MSB 0:
		B1		1: 0:
		B2		1: 0:
		B3	BPU-A DATA	1: 0:
		B4		1: 0:
		B5		1: 0:
		B6		1: 0:
		B7		1:LSB 0:
*F4n+1・W28	OBC	B0		1:MSB 0:
		B1		1: 0:
		B2		1: 0:
		B3	BPU-B DATA	1: 0:
		B4		1: 0:
		B5		1: 0:
		B6		1: 0:
		B7		1:LSB 0:
*F4n+2・W28	OBC	B0	(予備)	1: 0
		B1	(予備)	1: 0:
		B2	(予備)	1: 0:
		B3	BPU-C DATA	1: 0:
		B4	(予備)	1: 0:
		B5	(予備)	1: 0:
		B6	(予備)	1: 0:
		B7	(予備)	1: 0:
*F4n+3・W28	OBC	B0	(予備)	1: 0:
		B1	(予備)	1: 0:
		B2	(予備)	1: 0:
		B3	(予備)	1: 0:
		B4	(予備)	1: 0:
		B5	(予備)	1: 0:
		B6	(予備)	1: 0:
		B7	(予備)	1: 0:

＊　打上げモードを除く

衛星からのリアルタイムテレメトリデータを受信できるのは衛星が地球局から可視の時に限られる．「ひてん」の場合臼田からの可視時間は一日4時間程度である．更に可視であっても深宇宙局の運用の都合でリアルタイムテレメトリデータを受信できない場合もある．従ってこの方法では，ミッションタイムの一部しかOBCの動作状況をモニタすることができない．

(2)　伝送誤りの影響

雑音によりリアルタイムテレメトリデータの伝送途中に誤りが生じる．このためにデータの伝送誤りとOBCフォールトとの区別が困難である．特に一過性の過渡フォールトをデータの伝送誤りから区別するのは困難を極める．

3．2．2　フォールト記録機能による方法

上記のような問題点を解決するために，OBC自身にフォールト発生の時刻，種別を記録する機能を持たせ，図5のように記録していたデータを可視時に地上からのコマンドでダウ

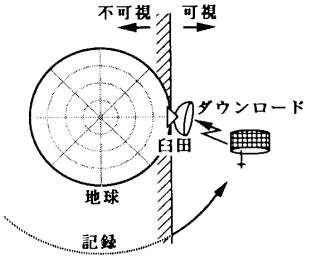

図5．フォールト記録機能

表3．OBCフォールト発生記録

「ひてん」OBC稼働記録（Cell A）

システムタイム	フォールトレジスタ		発生時刻	フォールト内容	発生原因
	アドレス	データ			
6F79EFB1	10CC81	04	7/ 5 14:39:25	ERR-GD Cell Z出力不選択	SEU
6F79EFB1	10CC7D	04	7/ 5 14:39:25	ERR-CK1 Cell Z 1 bit error	SEU
773BF37B	10CC77	02	7/13 04:16:29	CM2-ERR Cell Yチャンネル4エラー	SEU
780854B4	10CC77	10	7/13 22:57:54	CM2-ERR Cell Zチャンネル4エラー	SEU
7BD96564	10CC81	04	7/17 16:18:57	ERR-GD Cell Z出力不選択	SEU
7BD96564	10CC81	04	7/17 16:18:57	ERR-CK1 Cell Z 1 bit error	SEU
7C42B0F8	10CC81	04	7/18 01:56:42	ERR-GD Cell Z出力不選択	SEU
7C42B0F8	10CC7D	04	7/18 01:56:42	ERR-CK1 Cell Z 1 bit error	SEU
7CA89CD9	10CC79	01	7/18 11:15:42	ERR-REG Votoer出力不一致	不明
7D7E7CFF	10CC81	01	7/19 06:49:27	ERR-GD Cell X出力不選択	SEU
7D7E7CFF	10CC7D	01	7/19 06:49:27	ERR-CK1 Cell X 1 bit error	SEU
7DC6C63A	10CC77	01	7/19 13:26:04	CM2-ERR Cell Yチャンネル3エラー	SEU
7E0BEDC2	10CC81	04	7/19 19:45:31	ERR-GD Cell Z出力不選択	SEU
7E0BEDC2	10CC7D	04	7/19 19:45:31	ERR-CK1 Cell Z 1 bit error	SEU
7E6C91FE	10CC77	10	7/20 04:35:47	CM2-ERR Cell Zチヤンネル3エラー	SEU
7E83C2B6	10CC77	20	7/20 06:43:01	CM2-ERR Cell Zチャンネル4エラー	SEU
7FAD6E59	10CC77	20	7/21 09:56:19	CM2-ERR Cell Zチャンネル4エラー	SEU
81E6AE85	10CC77	20	7/23 13:59:44	CM2-ERR Cell Zチャンネル4エラー	SEU
82C16199	10CC77	40	7/24 09:59:43	CM2-ERR Cell Zサムチェックエラー	SEU
83203585	10CC77	10	7/24 18:40:02	CM2-ERR Cell Zチャンネル3エラー	SEU
84078DCC	10CC77	01	7/25 15:49:24	CM2-ERR Cell Yチャンネル3エラー	SEU
84788517	10CC81	04	7/26 02:09:14	ERR-GD Cell Z出力不選択	SEU
84788517	10CC7D	04	7/26 02:09:14	ERR-CK1 Cell Z 1 bit error	SEU

ンロードする方法に変更した．フォールト記録機能はリモートローディング機能により地上からプロクラムを送り，実行させることにより実現した．この機能により1日24時間のデータ採取が可能となり，しかも3つのCellから冗長なデータが送られてくるために伝送誤りの影響を受けることなくデータ収集が可能となる．

表3に本方式により採取したOBCの稼働状況の一例を示す．本方式によるデータ採取を始めた7月5日14：16（UT）から8月3日10：05（UT）の間のRAMのSEUの発生時刻を表4に示す．この28.86日間に8回の1ビット誤りが発生しているが，いずれの場合も誤りが発生したCellの出力は不採用となり，他の正常なCellの出力を選択することによりシステム全体は正常に動作したことがデータ選択状況の記録からわかった．なおこの間ラッチアップの発生は観測されなかった．

3．2．3　データの解析結果

(1) SEU発生回数

Cell CでのSEUが6回と最も多い．この原因としては，

(a) Cell Cが宇宙線の当たりやすい最上面に位置している（図6）

(b) Cell CのRAMがSEUに弱い

表4　SEU発生記録

7/ 5	14:39:25	Cell C 1bit 誤り
7/17	16:18:57	Cell C 1bit 誤り
7/18	01:56:42	Cell C 1bit 誤り
7/19	06:49:27	Cell A 1bit 誤り
7/19	19:45:31	Cell C 1bit 誤り
7/26	02:09:14	Cell C 1bit 誤り
7/27	14:26:21	Cell C 1bit 誤り
8/ 2	03:25:14	Cell A 1bit 誤り

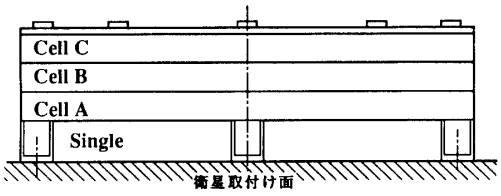

図6．OBCの構造

ことなどが考えられるが，断定するにはさらに解析が必要である．

この間のSEU発生率は，最多のCell Cでも

$Ru = 6[\text{upset}]/(28.86[\text{day}] \times 64[\text{Byte}] \times 8[\text{bit}])$

$= 2.88 \times 10^{-7}[\text{upset/bit/day}]$

と少ない値となる．なお，本OBCに使用しているSRAM（HM62256）の静止軌道上での誤り発生率（solar minimun＋90% worst case）は，照射試験の結果から3.1×10^{-5} [upset/bit/day] と推定されている[7]．推定値よりもRuが小さいのは，①太陽活動極大期で太陽風により銀河宇宙線が吹き払われている．②データ採取期間中大きな太陽フレアの発生が見られなかったからであろう．

(2)　太陽フレアの影響

7月26日02：09：14（UT）にCell Cで発生したSECは7月25日22：00～7月26日01：51（UT）に発生した重要度2Nクラスの太陽フレアの影響と見られる．今回の太陽フレアは規模が小さいためにSEUは1回発生しただけであり，SEUが連続発生するような大きな太陽フレアの発生はなかった．

他のSEUは太陽フレアとの相関が見られず，銀河宇宙線に由来するものと考えられる．

(3)　軌道との相関

軌道上でのSEU発生場所を図6に示す．この図をみると，月の軌道のやや遠方，地球から約40万Kmの地点でSEUが多発する傾向にあるが，まだサンプル数が少ないので軌道との相関を議論するためには更に多くのデータの蓄積が必要である．

4．まとめ

打ち上げ後，OBC内で人為的に誤りを発生させる実験の結果，OBCが誤りにたいして設計仕様通りの動作をし，機能が正常であることが確認できた．

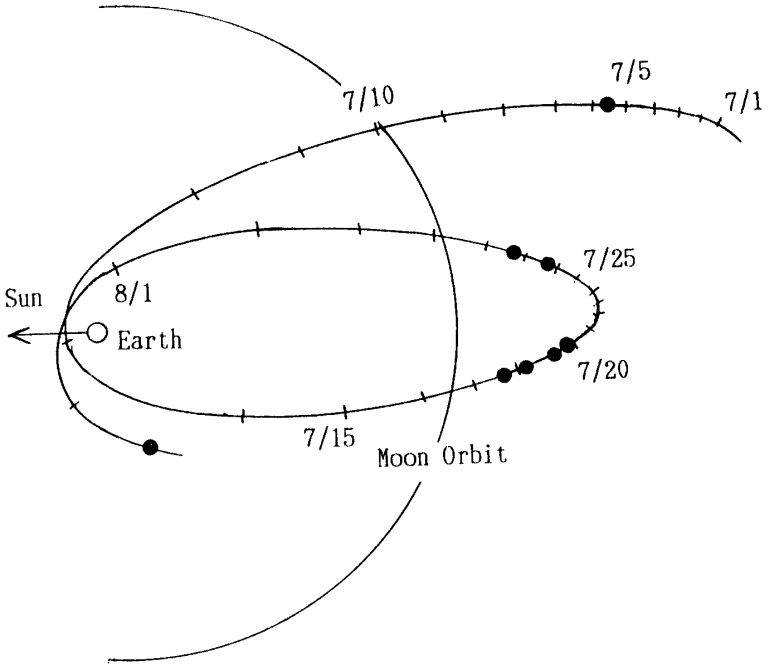

図7．軌道上でのSEU発生箇所

又，リモートローディングによりOBCにフォールト記録機能を追加し，1日24時間の動作状況のモニタが可能になった．この機能により7月5日14：16（UT）から8月3日10：05（UT）の28.86日間に，RAMでSEUによって8回の1ビット誤りが観測された．このうち7月26日02：09：14（UT）にCell Cで発生したSEUは，7月25日22：00～7月26日01：51（UT）に発生した重要度2Nクラスの太陽フレアの影響と見られ，他のSEUは太陽フレアとの相関は認められず，銀河宇宙線に由来するもと考えられる．

また，地球から約40万Kmの地点でSEUが多発する傾向にあるが，サンプル数が少ないので，結論を出すためにはさらにデータの蓄積が必要である．

稼働状況を常時モニタできるようになってまだ日が浅いが今後日を追うごとにデータが蓄積されて，有益な知見か得られよう．

謝　辞

「ひてん」OBCのフィールドデータの解析に当たり，太陽フレア発生のデータを提供してくださった郵政省通信総合研究所関東支所平磯宇宙環境センターに厚く感謝致します．

参考文献

[1] 山田弘善ほか;電子機器に対する宇宙環境，信学誌，66，3，PP. 254–258 1983

[2] 高野　忠ほか：耐故障性を有する人工衛星搭載用コンピュータの開発，信学技報，SANE–，PP. 25–30 1986

[3] 姉川　弘ほか：32ビットMPUのシングルイベント試験とJEM搭載用計算機の研究試作，信学技報，SANE87–38，PP. 23–30 1987

[4] T. Takno et al.,: Fault-Tolerant Onboard Computers, Proc. of th Int'l Symp. Space Tech. and Sci., ISTS-16, Sapporo, PP. 1097–1100 1988–06

[5] N. Kanekawa et al., "Dependable Onboard Computer Systems with a New Method - Stepwise Negotiating Voting, "Proc. 19th Fault-Tolerant Computing Symp., FTCS-19, PP. 13–19 1989

[6] 金川信康，前島英雄，加藤肇彦，井原廣一："新しい多数決方式によるフォールトトレラントコンピュータシステム" 信学論，J73-D-I, 2, pp .109–116 1990

[7] R. Koga, et al: "SEU test technique for 256K static RAMs and comparisons of upsets induced by heavy ions and protons, "IEEE Trans, Nuclear Sic., NS-35, 6, PP. 1638–1643 1988