高信頼PCサーバ ULTRASAVER$_{TM}$ MAGNIA$_{TM}$7010FR

ULTRASAVER$_{TM}$ MAGNIA$_{TM}$7010FR High-Reliability PC Server

小室　浩　KOMURO Hiroshi
申　承昊　SHIN Sung Ho

PCサーバは急激に市場規模を拡大し，ミッションクリティカルな事業領域(注1)にまで手を伸ばしつつある。この用途で使われるPCサーバの上位機では“信頼性”への要求が強い。

MAGNIA$_{TM}$7010FRは，当社独自のSFR(Super Fault Resilient)技術を搭載する高信頼性PCサーバである。SFRは，通常の計算機ではシステムダウンに至るソフトウェアのタイミングバグなどの一時的障害から自動的に回復し，処理を継続することを可能にする技術である。MAGNIA$_{TM}$7010FRは，最新のプロセッサに対応して処理能力を向上させると同時に，故障回避機能を搭載して，1ランク上の信頼性を提供している。

This paper describes the ULTRASAVER$_{TM}$ MAGNIA$_{TM}$7010FR, Toshiba's brand-new, high-reliability PC-based server. This server incorporates our new super fault resilient (SFR) technology, which enhances the reliability of the system by performing automatic recovery from failures caused by transient faults such as software timing bugs. This recovery technique employs the checkpoint rollback mechanism, typically taking 5 seconds, and no more than 30 seconds, to recover. We have also developed new features such as "hangup detection of application programs."

With these features, the MAGNIA$_{TM}$7010FR is expected to be widely used in emerging PC-based Internet system integration.

1 まえがき

インターネットの爆発的な普及は，一般家庭のコンピュータも巻き込み，全世界のコンピュータを結ぶ巨大なネットワークインフラを構築しつつある。その中でPCサーバは，ミドルクラスのコンピュータ市場で急激にシェアを拡大しており，ミッションクリティカルな事業領域まで脅かす存在となっている。この用途で使われるPCサーバは“信頼性”に対する要求が強い。そこで当社は，高信頼PCサーバMAGNIA$_{TM}$7010FR(図1，表1)を1999年9月に商品化した。MAGNIA$_{TM}$7010FRは，当社独自のSFR技術を搭載している。

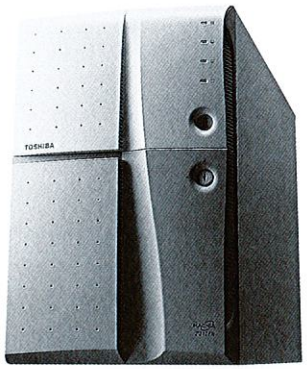

図1．MAGNIA$_{TM}$7010FR　SFR技術を搭載した高信頼PCサーバ。
ULTRASAVER$_{TM}$ MAGNIA$_{TM}$7010FR high-reliability server

表1．MAGNIA$_{TM}$7010FRの主な仕様
Main specifications of MAGNIA$_{TM}$7010FR

項　目	仕　様
プロセッサ	Pentium®III Xeon(注2) 550MHz
プロセッサ数	標準2 (最大3)
キャッシュ	1st (32Kバイト/CPU)，2nd (512Kバイト～2Mバイト/CPU)
メインメモリ	標準512Mバイト (最大4Gバイト)
HDD	最大216Gバイト (本体内蔵) ／1.08Tバイト (拡張時)
I/Oスロット	PCI＝6，PCI/ISA＝1
搭載OS	Microsoft®WindowsNT® (注3) SP5 (別売)
添付ソフトウェア	サーバ監視ソフトウェア，設定支援ソフトウェア
添付サービス	サーバ障害通知サービス

HDD：ハードディスク装置　PCI：Peripheral Component Interconnect
ISA：Industry Standard Architecture

SFR技術は，通常の計算機ではシステムダウンにいたる障害(ソフトウェアのタイミングバグやハードウェアの一時故障など)から，自動的に回復し処理の継続を可能にする技術[1]である。この故障回復機能は，通常のPCサーバ機をベースとして，最小限の専用モジュール(ハードウェアとソフトウェア)を付加することで実現している。このため，PCサーバのオープン性と低コストの特長を維持しつつ高信頼を達成することができた。また，SFRはPCサーバ単体の信頼性を向上させる技術であるが，当社のクラスタリング技術

(注1)　システムダウンが許されない基幹業務
(注2)　Pentium，Xeonは，米国Intel Corporationの商標。
(注3)　Microsoft，WindowsNTは，米国Microsoft Corporationの米国及びその他の国における登録商標。

“DNCWARE”ClusterPerfect™”（p.18参照）と組み合せることで，システム全体の耐障害性をいっそう高めることができる。

MAGNIA™7010FRは，最新プロセッサへの対応と，障害検出及び解析のための能力を強化させたことにより，1ランク上の処理能力と信頼性を提供している。

2 SFRによる高信頼化の原理

SFRは，障害時に自動的にリブート（システムの再起動）のダメージもなく短時間で障害検出前の状態に戻し，処理を再試行する技術である。

2.1 チェックポイント・ロールバック方式

SFRは，問題を解決して高信頼性を実現するために，チェックポイント・ロールバック方式[1]と呼ばれる手法を採用している。この方式の動作原理を図2を使って説明する。

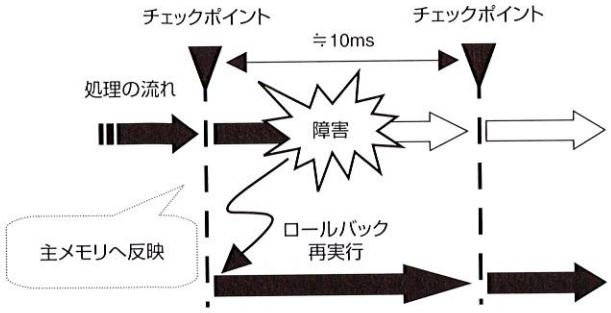

図2．チェックポイント・ロールバック方式　障害発生時，直前のチェックポイント時点にロールバックして処理を再実行する。
Checkpoint and rollback mechanism

まず，通常の処理を実行中，定期的にOS（Operating System）を含めたすべてのプログラムの状態を主メモリに反映させる（これを“チェックポイント”と呼ぶ）。チェックポイントは，プロセッサの状態と，プロセッサキャッシュ中の有効なデータを主メモリに書き戻す（ライトバック）処理で占められる。

万一，障害が発生した場合は，システム全体で障害発生直前のチェックポイント時点における主メモリ状態に戻って（これを“ロールバック”と呼ぶ），処理を再実行させる。もし，障害が一時故障などの一過性障害であれば，処理を再実行することで障害を回避し，ユーザーは故障を意識することなく処理を継続することができる。つまり，障害からリカバリできたことになる。

もちろん普段は，障害が発生しないためロールバックすることはないが，通常処理と並行してロールバックできるための機能が動作している。この機能の詳細は3章で述べる。

故障発生時に，SFRによるリカバリを行う場合と，リブートを行う場合の比較を，表2にまとめた。

表2．SFRによるリカバリとリブートの比較
Comparison of SFR recovery and reboot

項　目	SFRによるリカバリ	リブート
リカバリ時間	3〜30秒　典型的には5秒	数分
再初期化処理	I/Oのリセット	リブート
アプリケーション	障害発生に気づかない	再起動・回復処理

2.2 正しいリカバリを行うSFR

チェックポイント・ロールバック方式がうまく作用するためには，「チェックポイント時には問題が存在しなかった」という条件が必要である。一般的なチェックポイント・ロールバック方式による高信頼化では，チェックポイント時に保存する内容は，データベースのデータや，ファイル，計算の途中結果といった，フォーマットが決まったデータ群であるため，チェックポイント採取時に整合性のチェックを行い「保存されたデータは，正しいデータである」と保証できる。それに対し，SFRではチェックポイント時に保存する対象は，すべての物理メモリであるため，内容の正しさをチェックすることはできない。つまり，「チェックポイント時のメモリ内に潜在的なOSの不具合がない」ことは保証できない。チェックポイント時のメモリの内容の正しさの根拠としているのは，「そのときに，チェックポイント処理を行えるほど，システムは正常に動いていた」という事実である。チェックポイント処理は，OSの様々な機能を使って行うため，「チェックポイント処理ができた」ということから，「そのときOSは問題なく動いていた」と判断している。

計算機の動作には，割込みなど，非決定的な部分があり，一過性の障害については，障害が発生するかどうかは，これらの偶然に左右されている。したがって，正常に動作していたチェックポイント時点から処理をやり直せば，条件が変わるため一過性の問題は再発しなくなる可能性がある。

2.3 SFRによるリカバリ例

OSデッドロックが発生した場合にSFRは特に有効であり，その理由は次のとおりである。

SFR では，チェックポイントの時点では，「どのCPUもロックを保持していない，きれいな状態」となるようにしており，ロールバックして直前のチェックポイント時の状態に戻ると，すべてのロックが外れる。そこから再実行し，それぞれのCPU がロックを取り直すことにより，多くの場合はタイミングが変化し，ロックを取る順序が変わり，デッドロックが解消するのである。

3 SFRの実装

SFRは，QRM（Quick Rollback Mechanism）モジュール（図3）と呼ぶハードウェアと，それらを操作するためのSFR

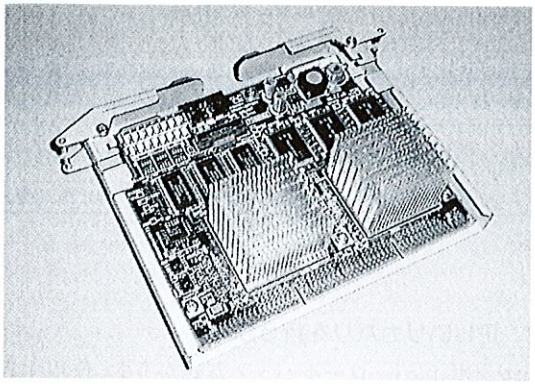

図3．QRMモジュール　SFRを実現するためのハードウェア。
Quick rollback mechanism (QRM) module

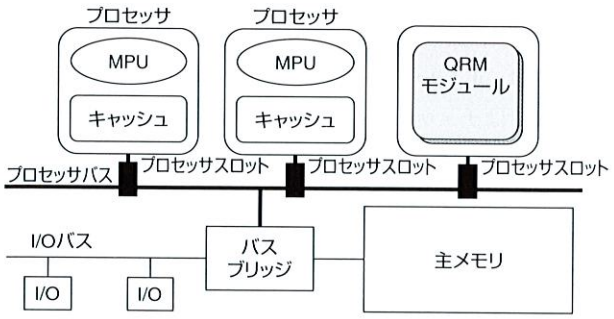

図4．SFRシステムの構成　SFRを搭載した計算機のハードウェア構成で，QRMモジュールはプロセッサバスに接続される。
Configuration of SFR system

ドライバモジュールと呼ぶソフトウェアで構成される。QRMモジュールは，図4のようにプロセッサバスに接続される。

3.1 QRMモジュールの機能

QRMモジュールは，専用ASIC（ゲートアレイ）を2品種（TC220G，270Kゲート，0.3 μmルール）と，DRAM・SRAMを複数実装し，周波数100MHzで動作している。ここではQRMモジュールに実装した機能を解説する。

3.1.1 ビフォアイメージ バックアップ機構　ビフォアイメージ バックアップ機構は，チェックポイント以降に主メモリを変更する（書き換える）トランザクションが発生した場合，変更前の主メモリの内容をBIB（Before Image Buffer）と呼ばれる退避用メモリに保存している。障害が発生した場合，BIBメモリに積まれたデータを主メモリに書き戻すことで直前のチェックポイントへ戻る機能を提供している。

3.1.2 キャッシュ ライトバック高速化機構　定期的に行うチェックポイント処理は，前述したようにプロセッサキャッシュ中の有効なデータを主メモリに書き戻す機能が必要となる。プロセッサでもこの機能を実現することができるが，全キャッシュラインの状態を網羅的に調べているため効率的でない。

MAGNIA$_{TM}$7010FRでは，この処理をQRMモジュール上のMBT（Modified Block Table）と呼ばれる専用ハードウェアで実現している。MBTは，プロセッサが発行するバストランザクションを監視して，全プロセッサのキャッシュ状態遷移をライン単位で管理してMBTメモリへ保存している。このため，MBTメモリの状態を調べれば，書戻しの必要なデータを持っているプロセッサキャッシュを容易に判断できる。

MBTは，MBTメモリの内容を高速にサーチする機能と，有効なデータを書き戻させるトランザクションを発行する機能を持つことで，チェックポイントの高速化を実現している。

3.2 QRMモジュールの実装

QRMモジュールはプロセッサと等価な位置に実装するため，プロセッサ並みの性能・速度が要求される。ここでは，QRMモジュールに組み込まれた高度な実装技術を解説する。

3.2.1 高速化実装技術　各プロセッサは，プロセッサスロットのコネクタを介してバス接続している。QRMモジュールは，プロセッサバスで採用している低振幅かつ高速なAGTL＋（Assisted Gunning Transistor Logic Plus：改良型GTL）インタフェースを実装した。当社製ASICにAGTL＋準拠のI/O（入出力）ドライバを実装するため，シミュレーションと実チップによる評価を重ねて実現している。また，ASICに限らずPCB設計の制約条件も厳しく，コネクタからASICまでの配線長は5 cm以内としている。このため10層基板を採用し，最短配線によりルールを守り高速安定動作を保証している。

3.2.2 高密度化実装　QRMモジュールは，複数の多ピン素子（最大576ピン）で構成されており，プロセッサ並みにコンパクトな形状にするため，実装密度の高いBGA（Ball Grid Array）パッケージを積極的に採用した。

また，高密度実装と相反して冷却の問題が挙がってくる。ASICは，5 W程度の発熱があり，これを冷やすために高放熱の冷却フィンを開発し実装した。

3.3 SFRドライバモジュール

SFRドライバモジュール（ソフトウェア）は，通常のデバイスドライバとして実装しており，WindowsNT®のカーネル本体にはいっさい手を加えていない。そのため，WindowsNT®のバグフィックスなどによるバージョンアップに対する追随性が高い。

4 システム障害検出，解析機能

MAGNIA$_{TM}$7010FRでは，リカバリを行うという本来の機能に加えて，次の機能を提供している。

4.1 アプリケーション ハング検出機構

システムの障害のなかには，「OSは動いているのだが，そ

のシステムで本当に使いたいアプリケーション，例えば，データベースサーバなどが応答しなくなった（ハングアップした）」というパターンがある。このようなときのユーザーの被害の大きさは，OS全体がパニックしたときと同等か，自動的にリブートしないことを考えると，それ以上である。

この問題を解決するため，MAGNIA$_{TM}$7010FRでは，主要なアプリケーションと，ディスク，画面表示のハングアップを検出し，対策を実施する機能を追加した。対象とするアプリケーションは，ORACLE(注4)，Microsoft® SQL Server$_{TM}$(注5)，Microsoft® Exchange Server，Lotus(注6) Notes Domino Serverであり，ユーザーがプログラムを作成すれば，これ以外のアプリケーションについてもハングアップを検出可能である。

検出方法は，定期的に各サーバプログラムに対してリクエストを投げ，応答が返ってくるかを調べる，というもので，タイムアウトやリトライ回数などを指定して，より確実な判断を行うことができる。ハングアップ検出時の対策は，次の中から選択できる。

(1) SFRによるリカバリ
(2) ユーザーによって指定されたコマンドの実行
(3) システムのリセット

また，システム全体が完全にハングアップした場合も，ウォッチドッグタイマ機能により，リセット，リブートさせるため，マシンが長時間使用不能状態になることはない。

4.2 障害解析機能

リカバリに成功した場合でも，障害の原因を特定しておくことは重要である。MAGNIA$_{TM}$7010FRでは，障害発生時に詳細な情報を収集し，ログファイルとして保存しており，この情報を予防保守に役立てることができる。一回の障害発生に関して採取する情報の量は20Kバイト程度であり，その内容は次のとおりである。

(1) 障害発生時の命令アドレス
(2) CPUのレジスタの値
(3) スレッド，プロセス情報
(4) スタックの内容
(5) チップセットのエラーレジスタの値
(6) OSパニック時のブルー画面の表示内容

これらの情報は不揮発性のメモリ上に保存しており，万一ディスクに書けないような障害の場合でも，リブート後に回収して確実にファイルとして保存できるようにしている。

保存したログファイルを，メールで自動的に保守センターに送付する“サーバ障害通知サービス”という保守サービスも用意している。保守センターに，客先と同じソフトウェアをインストールしたマシンか，客先マシンの以前のクラッシュダンプイメージのいずれかがあれば，メールで送付された障害ログファイルの内容から，詳細な解析を行うことが可能である。例えば，メールで送られてきたスタックの内容を調べて関数コールの流れを追っていけば，どのデバイスドライバがOSパニックに関係しているのか，を特定できる。WindowsNT®のようなオープンなOSで発生する障害は，他社製のデバイスドライバのバグが原因であることが多く，そのドライバを特定することは重要である。従来は，数十から数百メガバイトに及ぶクラッシュダンプを入手して実施してきた解析のかなりの部分を，メールから得た情報だけで行うことができる。

クラッシュダンプを入手できた場合は，SFRの機能により，より効果的な解析を行うことができる。SFRマシンのクラッシュダンプイメージの中には，メモリ変更の履歴（過去のチェックポイントイメージ），スレッド切換えの履歴，及び割込みの履歴が含まれており，例えばある不正なメモリの値に着目し，その値がいつ変更されており，変更前の値は何であったかを調べることができる。言い換えれば，OSパニックに至る経緯を知ることができ，より詳細に障害を解析することができる。その結果，デバイスドライバにおけるバグの位置を特定できることがある。実際，SFRでの障害解析によって，あるウイルスチェックソフトウェアの，OSパニックを引き起こすバグを特定することができた。

保存されている履歴の期間はシステムの負荷によるが，過去1～30秒である。

5 あとがき

MAGNIA$_{TM}$7010FR は，リカバリによる信頼性の向上だけでなく，障害解析を効率的に行えるというPCサーバを使ううえで有効な特長を備えている。サーバ障害通知サービスと連携して迅速な対応を行うことで顧客満足にもつながる。

文 献

(1) 増渕美生，他．新しい高信頼サーバ計算機技術－設計思想と方式．東芝レビュー．52，8，1997，p35-39.

(注4) ORACLEは，Oracle Corporationの登録商標。
(注5) SQL Severは，米国Microsoft Corporationの米国及びその他の国における商標。
(注6) Lotus は，Lotus Development社の商標。

小室　浩　KOMURO Hiroshi
デジタルメディア機器社 コンピュータ＆ネットワーク開発センター 開発第一部主務。コンピュータの高信頼化・高性能化の研究・開発に従事。情報処理学会会員。
Computer & Network Development Center

申　承昊　SHIN Sung Ho
デジタルメディア機器社 コンピュータ＆ネットワーク開発センター 開発第一部主務。コンピュータの高信頼化・高性能化の研究・開発に従事。
Computer & Network Development Center