3Z－2 ナノカーネル方式による異種OS共存技術「DARMA」の実装

佐藤雅英*、関口知紀*、新井利明*、井上太郎*、宮崎義弘**、中橋晃文***、梅都利和****
*(株)日立製作所システム開発研究所、**同産業システム事業部、***同大みか制御本部、****同情報機器事業部

1. はじめに

標準的OS使用時のシステム構築上の制約（信頼性、拡張性）を緩和するための、マシン上に複数OSの同時実行を可能とするナノカーネル方式のインプリメンテーションに関して説明する。

2．ナノカーネル方式の実現

ナノカーネル機能は以下の機能の集合で実現する。

2．1 複数OS実行制御機能

複数のOSの起動および実行を制御する機能である。

（1） 資源分割機能

（a）メモリ分割機能

物理メモリを分割し、各OS、ナノカーネルおよび共用メモリ用に割付ける。各OSが使用する仮想空間も分離しているため、ユーザプロセスが他OSの領域を破壊する危険性はない。

（b）I/O分割機能

OS毎にI/O装置を占有させる機能。メモリと同様に、各OSは自分自身に割り付けられたI/O装置以外はハード的に搭載されていないものとして実行するため、OS障害時にも誤って他OSに割り付けられたI/O装置をアクセスする危険性は小さい。

（c）プロセッサ分割機能

プロセッサは時分割して各OSに割付ける。割付のアルゴリズムおよび優先順位は共存するOSの特性に応じて変更可能である。例えば、汎用的なOSとリアルタイムOSを共存させる場合には、リアルタイムOSを最優先させ、リアルタイムOSに対する割り込み事象が発生した場合には、汎用OSの処理を中断してリアルタイムOSに制御を移す。

（d）タイマ共用機能

タイマを仮想化し、OS間で共用する機能である。各OSからの割り込み発生要求を受取り、要求をマージして物理タイマにセットする。タイマ割り込みが発生した際には、該当するOSのタイマ割り込みハンドラルーチンへ制御をわたす。（第1図）

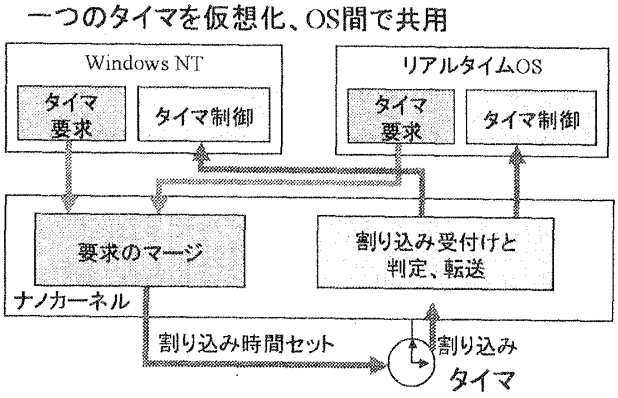

図1 タイマ共用機能

（2） OS間通信機能

OS間通信機能はOS間の連係機能を実現するために不可欠な機能である。（第2図）

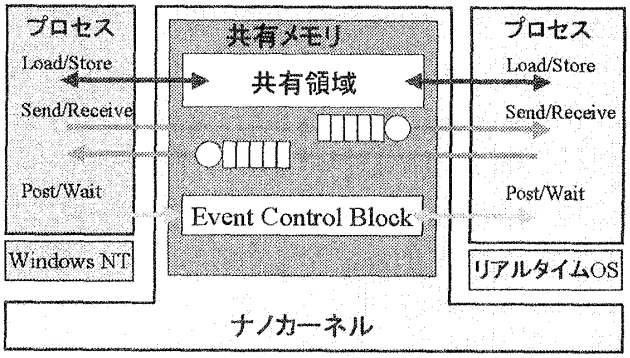

図2 OS間通信機能

（a）共用メモリ機能

OS間で共通に参照するメモリ領域を設定する機能である。プロテクション強化のため物理メモリを直接参照することは禁止し、仮想メモリ経由でのアクセスのみを許可する。

（b）OS間メッセージパシング機能

異なるOS上のプロセス間でメッセージパシングによってデータの共用、転送、プロセスの同期制御を実施する機能である。

（c）OS 間プロセス同期機能

異なる OS 上のプロセスの同期制御機能である。これにより、各 OS 上のプロセスは自 OS 上のプロセスと同様に、他 OS 上のプロセスと同期をとりながら処理を実施することが可能となる。

（3） 障害監視、回復機能

ナノカーネル上では、ある OS の状態は他の OS に全く影響を与えない。これを実現するため、ナノカーネルは、メモリおよび I/O 装置を各 OS に占有させることで、OS 障害時に他 OS 用の資源を不正アクセスすることを防止している。また、プロセッサに関しても、障害発生をトラップし、障害が発生した OS に対してはプロセッサの割り当てを抑止して、障害が他の OS へ影響しないよう制御している。

さらに、ナノカーネルでは、異常終了した OS のみを、他 OS の実行は継続したまま、再起動することも可能としている。

5．「DARMA」ナノカーネルによる Windows NT(R)とリアルタイム OS の共存

ナノカーネルの有効性を検証するため、PC/AT ハード上に「DARMA(Dependable Autonomous Real-time Management)」ナノカーネルをインプリメントし、Windows NT(R)と独自リアルタイム OS を共存させた。その構成を第 3 図に示す。ここでは、汎用 OS である Windows NT を制御システムに適用することを目的に、共存する OS として高信頼なリアルタイム OS を選択した。

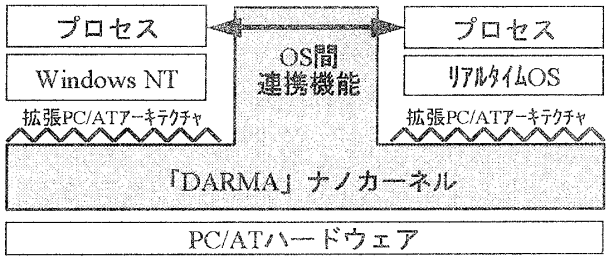

図３ 「DARMA」ナノカーネルの構成

（1） リアルタイム性強化

Windows NT のタイマ機構は 10 ミリ秒周期であり、これより短い周期の要求には対応不可能である。またネットワークに関する割込み処理が集中し、CPU の負荷が増加した場合には応答性が大幅に悪化する。

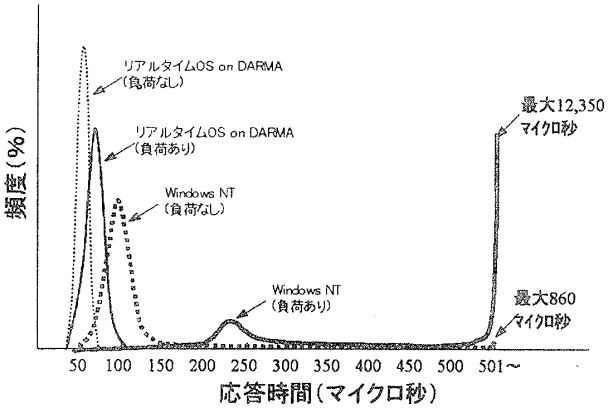

図4 DARMAの効果（応答時間比較）

「DARMA」ナノカーネル上にリアルタイム OS を搭載した場合の応答時間を図 4 に示す。ここでは、測定環境を高負荷状態とするため、応答時間測定対象タスクより優先度の低いディスクアクセスタスクを共存させている。DARMA 上のリアルタイム OS は安定した短い応答時間を保証している。一方、Windows NT では応答時間はバラツキが大きい。

（2） 信頼性向上

ナノカーネル方式の最大の特長は、Windows NT 障害時の監視／解析／回復機能である。Windows NT と、Windows NT の動作を監視する小規模な高信頼 OS を共存させ、万一 Windows NT に障害が発生した場合に、監視 OS が障害を検知する。監視 OS はナノカーネルを介して Windows NT の障害情報収集することができ、障害発生原因の解明を迅速に行うことが可能である。さらに、Windows NT のみの再起動も短時間で実施することが出来るため、障害の影響を最小限度に抑えることができる。

6．おわりに

PC システムの標準的 OS である Windows NT システムの機能強化、信頼性向上を可能とする「DARMA」ナノカーネル方式について説明した。