

6J-6

## オペレーティングシステムの アベイラビリティ向上対策の一提案

向垣内岳弥, 花沢満

NTT 情報通信網研究所

### 1 はじめに

情報処理システムの適用範囲の拡大, サービス時間の延長等により, 計算機システムの24時間運転に対するニーズが高まっている。

24時間運転を阻害する要因は, 以下の2点に大きく分類することができる。

**非計画停止** ハードウェアの故障やソフトウェアのバグ等の不測の事態によるもの

**計画停止** ハードウェアのメンテナンスやソフトウェアの入れ換え等の保守によるもの

本稿では, 計画停止の中のソフトウェアの入れ換えに注目し, 常駐タスクとして動作するOSプログラムの入れ換えによるシステム停止時間の短縮をはかる方法の検討を行なう。

### 2 従来のOSプログラム入れ換え方式

従来のOSプログラム入れ換え方式は, 以下の2方式に分類することができる。

#### 2.1 単一計算機上での入れ換え

単一計算機上でのOSプログラムの入れ換え手順は以下の通りである。

- 1 該タスクの業務閉塞
- 2 旧タスクのアポート
- 3 新タスクの開始
- 4 業務閉塞の解除

この方式では, 業務閉塞というフェーズが入るため, システムのアベイラビリティが低下する。業務を閉塞する時間は, 数秒から数分である。

#### 2.2 予備系をもつ計算機上での入れ換え

予備系を持つ計算機上でのOSプログラムの入れ換え手順は以下の通りである。

- 1 新プログラムでの予備系の再立ち上げ。
- 2 現用系から予備系への切り替え

以上の操作を計算機台数回繰り返すことで, 全ての計算機上のOSプログラムの入れ換えが完了する。

この方式では, 業務の閉塞は行なわれない。しかし, 以下の問題点がある。(1) 予備系を使用するため, その期間信頼性が低下する。(2) ハードウェアが冗長化されている場合でも論理的に1台の計算機として動作する場合がある。

### 3 提案する入れ換え方式

業務の閉塞を行なわず, また, 予備系の存在を前提としない常駐タスクの入れ換え方式を提案する。常駐タスクの入れ換えは, (1) 新旧タスクの切り替えと (2) 新旧タスク間での制御表情報の引継とからなる。

#### 3.1 前提条件

検討を行なう上での前提条件を以下に示す。

- システム空間で走行するタスク(システムタスク)を対象とする。
- ユーザタスクからシステムタスクへの制御移行は, メッセージボックス通信を用いて行なわれる。
- 新旧タスク間で引き継ぐ制御表には変更はない。
- 予備系の存在を前提としない。

常駐タスクの実行モデルと, 常駐タスクが参照する制御表の位置を図1に示す。

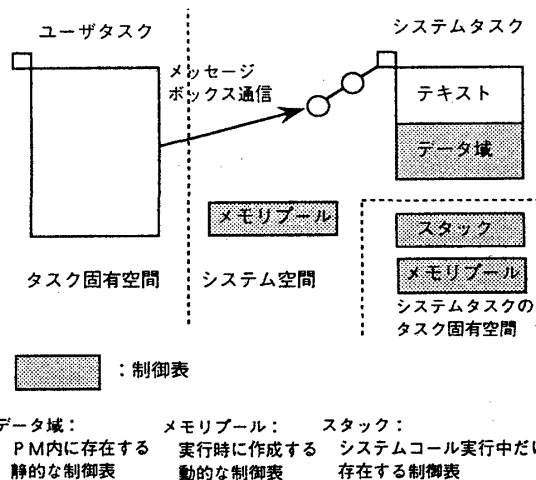


図1: OSの実行モデルと制御表の位置

### 3.2 タスク切り替え方式

すでにキューイングされているメッセージの処理を保証するために、旧タスクが用いていたキューを新タスクにつなぎ換えることでタスクの切替を実現する。具体的には、メッセージボックスのIDを新旧タスク間で引継ぎ、新タスクは旧タスクと同一キューを処理する。

キュー内のメッセージの順序を保証するため、新旧タスクは同時走行することができない。このため、新旧タスク間で同期をとる必要がある。

同期をとる契機として、入れ換え指示メッセージを旧タスクに送信する。入れ換え指示メッセージを受信した旧タスクは、新タスクに対して処理開始指示メッセージを送信する。このとき、メッセージボックスIDも同時に送信する。処理開始指示メッセージを受信した新タスクは、旧タスクに対して受信通知を送信する。この受信通知を受信した旧タスクはアポートする。一定時間内に受信通知を受信しなかったときは、旧タスクはタスク切替失敗を報告する。このときの処理フローを図2に示す。

入れ換え指示メッセージを処理する時間が、タスク切り替えによる処理の中断時間である。

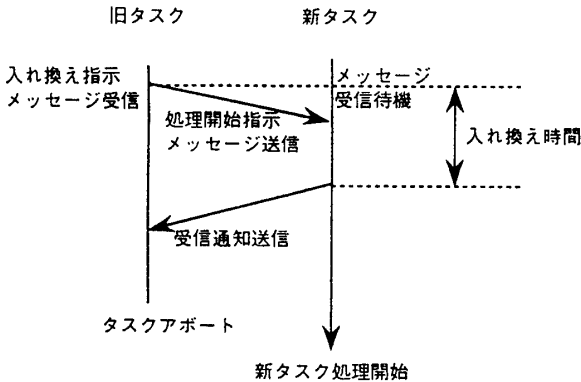


図2: タスク切り替えの処理フロー

### 3.3 制御表情報引継方式

処理の連続性を保つために、旧タスクから新タスクへ必要な制御表情報を引き継ぐ必要がある。図1に示した

それぞれの制御表の明示的な引継必要性およびその理由を表1に示す。

制御表の引継時間を最短にするために、新旧タスク間で同一制御表を共有する方式を採用する。すなわち、制御表の実体を全てシステム空間のメモリプール域に作成し、プログラムのデータ域にはメモリプールへのポインタだけを保持する。この方法を用いれば、制御表の引継はポインタ1個の引継で実現される。

新旧タスクは同時走行しないので、同時に制御表の更新を行なうことはない。このため、新旧タスク間で制御表の一貫性を保証するための新たなロジックの組み込みは不要である。

## 4 評価

今回提案した常駐タスク入れ換え方式を実際のOSに適用した。

測定の結果、タスク入れ換えに要する時間は約5msであった。これは、従来の単一計算機上でのタスク入れ換え時間と比較して約1000分の1の時間である。この時間は新旧タスク間の同期と完了通知とに費やされる。

## 5 おわりに

オペレーティングシステムのアベイラビリティ向上対策の一手法として、常駐タスクの入れ換え方式を提案した。これは、計算機システムの24時間運転を行なう際に有効な技術である。

今後は、入れ換え失敗時の切り戻し処理等の異常時処理や、制御表の構成等の変更を伴う入れ換え方式の検討を行い、適用範囲を拡大していく予定である。

## 参考文献

[1] J.Gray 他, フォールト・トレラント・システム, マグロウヒル株式会社

表1: 制御表の引継必要性

制御表の位置		明示的引継必要性	理由
システム空間	データ域	必要	すべての制御表の起点となる
	メモリプール	不要	システム空間のデータ域にある制御表の引継で自動的に引き継がれる
タスク固有空間	メモリプール	不要	システム空間のデータ域にある制御表の引継で自動的に引き継がれる
	スタック	不要	引継時にスタックは存在しない