

外94-36

早稲田大学大学院理工学研究科

## 博士論文概要

### 論文題目

知的分散システムにおける  
高信頼化手法に関する研究

申請者

関俊文

Toshibumi SEKI

1994年12月

技術革新に伴ってユーザニーズが多様化し、拡張性・信頼性・保守性・適応性に優れたシステムが求められている。分散システムは、これらの要求に応える能力を潜在的に持つ計算機システムアーキテクチャである。従来の分散システムは、集中管理機構を持ち、その集中機構によって分散された要素群（資源、プロセスなど）を制御している。よって個々の要素の動作が集中管理され、システム全体の運転効率の向上や高度な機能の実現が可能になっている。しかし、要素群を集中管理する部分に負荷や機能が集中することとなり、集中管理部の仕様決定や開発および修正に多大な時間を必要としている。さらに、システムの大規模化、複雑化に伴い、集中管理機構の故障の及ぼす影響が大きくなり、信頼性や処理能力のボトルネックとなることが明らかになっている。

このような問題を解決する分散システムアーキテクチャとして、集中管理機構を完全に排した「宣言型」の分散システム構造を提案する。そこでは、システムは要素の単なる集合からなり、それらの動作を管理する集中管理機構は存在しない。つまり個々の要素は各々独立でシステム内での予め決められた役割を持たない。要素の役割は、要素群が状況に応じて協力、協調することによって定まる。従って各要素は集中管理機構等の制約を受けることなく、常にその最大の能力を發揮することが可能となる。このような宣言型システムでは、個々の要素が関連要素の存在や位置、多重度に依存せず独立に動作する性質が重要となる。

本論文では、宣言型分散システムの実現として知的分散システムを提案し、その上で宣言型システムの性質を保存した高信頼分散システムを、要素の多重度によって実現する手法を提案する。アプリケーションレベルで要素の位置や多重度及び多重度要素制御方式の透過性を実現した高信頼化手法は既に提案されているが、本論文においてはオペレーティングシステム（OS）をはじめとするシステムレベルにおいても要素の透過性を実現している。

第2章では、従来の分散システムの問題点を述べ、それら問題点を解決するシステム・アーキテクチャが宣言型の分散システムである事を示す。そして、宣言型分散システムの構造を持つシステムの実現として、各要素をオブジェクトモデルに基づくオブジェクトとして記述し、各オブジェクト間の情報交換を放送通信を用いて行う知的分散システムを提案する。そこでシステムの高信頼化は、オブジェクトの多重度によって行う。オブジェクトモデルを導入することにより要素の自律性を実現し、放送通信を用いることにより要素の位置・多重度からの完全な透過性を実現する。これによって、知的分散システム構造が、宣言型分散システムの特徴である高い信頼性・適応性・拡張性等を実現できることを示す。

第3章では、自律的要素の動作を制御するOSとして知的分散OSを提案し、高信頼な知的分散システム実現をOSレベルで支援する機能について示す。高信頼な知的分散システムの実現を支援するOSは、そのOS機能自体も集中管理機構を保持せず要素群の協力・協調によって実現されなければならない。従来のOS

では、OS機能を核とプロセスに分離し、核の機能ができるだけ小さく抑える試みがされている。しかし、そこではOS機能の各々を専用のプロセスに割り当てる機能分散の形が採られており、全ての計算機からの要求が特定のプロセスに集中してしまい、宣言型システムの概念に合い入れない。よって知的分散OSでは、アプリケーションオブジェクト毎に必要とするOS機能を共通知識として分散させて持ち、OS機能はその実行時にOS核と関係するオブジェクト上の共通知識群の結合によって実現する。その結合は放送通信によるメッセージ交換によって実現する。このため、オブジェクト間で並列に進行する処理の同時実行制御、多重化されたオブジェクト間での状態の一貫性保証など、システム全体に渡る動作の全ての管理は、特定のオブジェクトによって実現するのではなく、オブジェクト群の共通知識部の結合によって実現する。

また、多重化オブジェクトの独立性を支援するOS機能としては、多重化オブジェクトが同一タイミングで送信するメッセージを識別するためのメッセージ識別子の発番機構と、同一メッセージ識別子の付加されたメッセージ中から正しいメッセージを選択するための多重化メッセージ選択機構を保持する。このメッセージ識別子の発番や選択機構においても、個々の要素の持つ情報のみによって実現する事によって宣言型分散システムの特徴を維持する。さらにオブジェクトの実行モード（稼動／待機モード）の透過性を支援するため、メッセージ宛先オブジェクトの実行モードに応じたオブジェクト駆動機構を保持する。即ち、宛先オブジェクトの実行モードが稼動状態なら即起動させ、待機状態の時はその受信メッセージをロールバック操作時に使用するために保存する。

第4章では、高信頼な知的分散システム構築のために要求される高信頼な放送通信機構について示す。即ち、オブジェクトの位置や多重度に関わらず、多重化オブジェクトが同一順序で同一メッセージの受信を保証する放送通信機構を提案する。従来より放送通信は便利なものと認識されているが、信頼性に問題があるため実システムに利用することは現実的でなかった。つまり放送通信では、受信相手の計算機が不特定多数な為、受信確認を幾つ待つべきか判断できないことが多く、受信確認メッセージを得ることが難しいためである。たとえ判断できたとしても、多数の計算機から受信確認メッセージを受信するオーバーヘッドが非常に大きい。既に提案されている高信頼な放送通信の実現法では、集中管理機構が存在したり多重度を意識した方法となっており、宣言型分散システムの概念に合い入れる方式ではない。よって、受信確認を必要とせず、かつ集中管理機構がなく、全計算機で同一順序で同一メッセージの受信を保証する高信頼な放送通信機構としてフェイル・ストップ放送通信機構を提案する。提案する放送通信機構では、通信エラーが生じた時その原因となった計算機を検出し、その回復処理（受信ミスマッチの再送など）を行うが、回復処理ができない場合は故障計算機を切り離し(Fail-Stop)、フォールトが他の計算機やオブジェクトに波及しないよ

うにする。このことにより正常に動作している全計算機が、同一順序で同一メッセージを受信する事を保証する。このような全順序を保証する放送通信機構の実現は、第5章で示す多重化オブジェクトの一貫性制御等を容易にする。

第5章では、高信頼な知的分散システム実現のため多重化されたオブジェクトの状態一貫性を保証する方法を示す。各オブジェクトに要求される信頼度や故障時に要求される復旧時間は、オブジェクト毎に異なっているので、オブジェクト毎に多重度と多重化要素制御方式として並列多重処理方式や待機冗長処理方式、及びその混在型の多重処理方式を自由に選択できることが望まれる。よって、オブジェクト毎にその要求に応じて多重度や多重化要素制御方式を選択可能とし、しかも要求の変更に動的に対応可能な方式を提案する。

並列多重処理方式では、各多重化オブジェクトはそれぞれ独自に処理結果をメッセージとして関連オブジェクトに放送する。この時、放送通信を用いるため関連オブジェクトの位置・多重度・実行モードを意識しない。受信側オブジェクトは、知的分散OSの支援機構（メッセージ識別子発番機構と多重化メッセージ選択機構）とフェイル・ストップ放送通信機構によって、多重化オブジェクトから送られてくるメッセージ中から正しいメッセージを選択受信することができる。よって多重化オブジェクトの決定的動作が仮定され同一初期状態が与えられたならば、多重化オブジェクトは同一処理を行い、少なくとも多重化オブジェクト中の1オブジェクトが正常動作している限り無停止で処理を継続することができる。

待機冗長処理方式では、稼動系オブジェクト故障時にその処理を待機系オブジェクトが引き継ぐため、チェックポイントにて稼働系オブジェクトの状態を待機系オブジェクトにコピーする必要がある。このチェックポイント機構として、宣言型システムの特徴を維持するため、オブジェクトの位置と多重度独立性だけでなくアプリケーションプログラムから独立な方式を提案する。即ち、プログラム中でチェックポイントを明記することは、待機冗長処理方式を意識する事になりその多重化オブジェクトを他の多重化要素制御方式で動作させる事を不可能にする。さらに、稼動系オブジェクト故障時の処理引継のための新稼動オブジェクト選択処理においても、稼動系や待機系オブジェクトの位置や多重度に依存せず、かつできる限り短時間で処理を引継ぐアルゴリズムを提案する。この時、多重化要素間の状態一貫性も保証されていることを示す。

第6章では、前章までに提案した高信頼な知的分散システム実現のための知的分散OS、フェイル・ストップ放送通信機構、多重化オブジェクトによる高信頼化機構の適用例として列車運行管理システムを探り上げる。そして、そのシミュレーションシステムの実現と評価を通して、提案する高信頼化手法の導入により対象システムの信頼性・拡張性・適応性等の向上が確認できたことを示す。

最後に第7章では、以上の知見より得られた結論をまとめ、今後の課題を述べる。