

明 細 書

発明の名称： 多重系システムおよび多重系システム管理方法

技術分野

[0001] 本発明は、多重系システムおよび多重系システム管理方法に関する。

背景技術

[0002] 例えば金融機関の基幹システムなど安易なシステムダウンが許容されないミッションクリティカルなシステムは、クラスタ構成すなわち多重系システムであることが一般的である。こうした多重系システムでは、現用系と待機系の各装置が相互監視を行い、現用系に関する異常検知に応じて待機系を現用系に切替えるといった運用がなされる。

[0003] 上述のような多重系システムの監視、運用の技術としては、例えば以下のようなものが提案されている。すなわち、クライアント端末が、二重化されたネットワーク管理システムにアクセスしてシステム切替えを監視する監視プログラムを取得する過程と、取得した監視プログラムを起動する過程と、起動した監視プログラムにより二重化されたネットワーク管理システムに定期的にアクセスし、その応答によりネットワーク管理システムが切り替わったことを検出する過程を実行する技術（特許文献1参照）などである。

先行技術文献

特許文献

[0004] 特許文献1：特開2005-4404号公報

発明の概要

発明が解決しようとする課題

[0005] 現状、確かに現用系と待機系とでシステムの多重化が図られているが、一方で、異常検知およびそれに伴う系切替を担う機構は多重化されていない。そのため、該当機構に障害が発生すると、多重系システムにおける異常検知動作が行われなくなり、系切替動作の契機自体も発生せずにそのままサービス停止につながる場合も生じうる。つまり、異常検知と系切替の機構が単一

障害点となり、現用系と待機系からなるシステム多重化の効果を根本的に毀損する懸念が残されている。

[0006] そこで本発明の目的は、多重系システムにおける障害検知構成を多重化して、障害発生を的確に検知し、必要な系切替動作を確実に実行可能とする技術を提供することにある。

課題を解決するための手段

[0007] 上記課題を解決する本発明の多重系システムは、多重化された各コンピュータの電源機構が、当該電源機構の記憶装置に対する、他装置ないし該当コンピュータの他機構からの所定情報の書込処理を監視し、前記書込処理が所定規則に対応したものでなかった場合、電源の停止ないしリセットの動作を実行し、当該動作実行後、前記各コンピュータのうち他方のコンピュータに対して回復動作の指示を実行する演算装置を備えるものであることを特徴とする。なお、多重系システムで従来から備わっているクラスタリングソフトによる相互監視機能は、上述の各コンピュータにおいても当然備わっているものとする（以下同様）。

[0008] また、本発明の多重系システム管理方法は、多重化された各コンピュータの電源機構が、当該電源機構の記憶装置に対する、他装置ないし該当コンピュータの他機構からの所定情報の書込処理を監視し、前記書込処理が所定規則に対応したものでなかった場合、電源の停止ないしリセットの動作を実行し、当該動作実行後、前記各コンピュータのうち他方のコンピュータに対して回復動作の指示を実行することを特徴とする。

発明の効果

[0009] 本発明によれば、多重系システムで従来から備わっているクラスタリングソフトによる相互監視機能に加えて、電源機構での監視機能を更に備えることで、多重系システムにおける障害検知構成を多重化して、障害発生を的確に検知し、必要な系切替動作を確実に実行可能となる。

図面の簡単な説明

[0010] [図1]第1実施形態の多重系システムを含むネットワーク構成例を示す図であ

る。

[図2]第1実施形態のサーバの構成例を示す図である。

[図3]第1実施形態の電源機構の構成例を示す図である。

[図4]第1実施形態の監視テーブルの構成例を示す図である。

[図5]第1実施形態における多重系システム管理方法の処理手順例1を示すフロー図である。

[図6]第1実施形態における多重系システム管理方法の処理手順例2を示すフロー図である。

[図7]第2実施形態の多重系システムを含むネットワーク構成例を示す図である。

[図8]第2実施形態の監視用コンピュータの構成例を示す図である。

[図9]第2実施形態のサーバの構成例を示す図である。

[図10]第2実施形態における多重系システム管理方法の処理手順例1を示すフロー図である。

[図11]第2実施形態における多重系システム管理方法の処理手順例2を示すフロー図である。

発明を実施するための形態

[0011] 以下に本発明の実施形態について図面を用いて詳細に説明する。図1は第1実施形態の多重系システム10を含むネットワーク構成例を示す図である。図1に示す多重系システム10は、障害検知構成を多重化して、障害発生を的確に検知し、必要な系切替動作を確実に実行可能とするためのコンピュータシステムである。

[0012] ここで想定する多重系システム10としては、一例として金融機関で運用されている基幹システムを想定する。勿論、多重系システム10としては金融機関におけるシステムに限定されず、他業界における各種のサーバシステム（クラスタ構成され多重系を成している）を想定可能である。

[0013] こうした多重系システム10は、通常時に業務処理を実行する現用系サーバ150と、この現用系サーバ150に異常が生じた場合に当該現用系サー

サーバ１５０に成り代わる待機系サーバ１８０とを含んでいる。これら現用系サーバ１５０および待機系サーバ１８０は、ネットワーク２０を介して通信可能に結ばれ、既存のクラスタリングソフトにより多重系を構成している。また、これら現用系サーバ１５０および待機系サーバ１８０のそれぞれには、稼働用電源を供給する電源機構２００が付帯している。この電源機構２００は、所定電圧の電源供給や通信を行うためのコネクタで電源供給対象の現用系サーバ１５０および待機系サーバ１８０と接続されているものの、これらサーバ装置とは別構成のハードウェアとなっている。

[0014] 続いて、多重系システム１０を構成する現用系サーバ１５０および待機系サーバ１８０のハードウェア構成について説明する。以下、特に区別する必要が無い場合には、現用系サーバ１５０および待機系サーバ１８０を、サーバ１００と総称することとする。図２は、第１実施形態のサーバ１００の構成例を示す図である。

[0015] 多重系システム１０を構成するサーバ１００は、ハードディスクドライブなど適宜な不揮発性記憶装置で構成される記憶装置１０１、ＲＡＭなど揮発性記憶装置で構成されるメモリ１０４、記憶装置１０１に保持されるＯＳ（Operating System）１０２を起動し、適宜なプログラム１０３を読み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうＣＰＵなどの演算装置１０５、ネットワーク２０と接続し他装置との通信処理を担う通信装置１０６、可搬媒体の読み取りドライブ１０７を備える。

[0016] なお、記憶装置１０１内には、多重系システム１０を構成するサーバ１００として必要な機能を実装する為のＯＳ１０２およびプログラム１０３が記憶されている。このプログラム１０３としては、業務プログラム１１０、クラスタ監視プログラム１１１、および生存通知プログラム１１２が含まれる。このうち業務プログラム１１０は、例えば金融機関の所定業務に対応した処理を実行するためのプログラムである。また、クラスタ監視プログラム１１１は、現用系および待機系のサーバ間相互の異常監視を実行するための既

存プログラムであり、既存のクラスタリングソフトに含まれる。また、生存通知プログラム 112 は、電源機構 200 の記憶装置 201 に対する所定情報の書込処理を実行するためのプログラムである。

[0017] この場合、サーバ 100 の演算装置 105 が上述のクラスタ監視プログラム 111 を実行することで、クラスタ監視機能が実装される。クラスタ監視機能は、現用系サーバ 150 および待機系サーバ 180 の各々に常駐し、従来からのハートビートなどサーバ間で互いに死活監視を行う動作を実現する。

[0018] また、サーバ 100 の演算装置 105 が上述の生存通知プログラム 112 を実行することで、生存通知機能が実装される。生存通知機能は、現用系サーバ 150 および待機系サーバ 180 の各々に常駐し、所定情報として、例えば現在時刻情報すなわちタイムスタンプを一定時間間隔で OS 102 のクロック機能等から得て、これを内部信号線 30 を介して電源機構 200 に対し送信する動作を実現する。

[0019] なお、サーバ 100 の OS 102 や所定のプログラムが、上述の生存通知プログラム 112 による生存通知機能の稼働状況をモニタリングしておき、生存通知機能においてスローダウンあるいは停止といった何らかの不具合事象発生を検知した場合、所定時間内に生存通知プログラム 112 を再実行して生存通知機能の再起動を行うとすれば好適である。こうした運用を行うことにより、不具合を生じた生存通知機能を速やかに復旧して、速やかに書込処理を再開することができる。多重系システム 10 を成すサーバ 100 の本来機能（OS 102 や業務プログラム 110 による機能など）自体に不具合は発生していないにも関わらず、上述の書込処理の機能のみの不具合に由来する障害検知により系切替が実行される事態を的確に回避出来る。

[0020] 次に、上述のサーバ 100 すなわち、現用系サーバ 150 および待機系サーバ 180 のそれぞれに付帯し、稼働電源を供給する電源機構 200 のハードウェア構成は以下の如くとなる。図 3 は第 1 実施形態の電源機構 200 の構成例を示す図である。

- [0021] この電源機構200は、コンピュータの電源ユニットとして一般的に備わるトランスやヒューズ、冷却ファン、ヒートシンクなどからなる電源装置230と、この電源装置230のオンオフ制御を行う電源制御装置240を備えている。
- [0022] このうち電源装置230は、上述のサーバ100におけるマザーボード上のコネクタや、記憶装置101や可搬媒体の読み取りドライブ107のコネクタと所定のケーブルで接続され、それらに所定電圧の直流を供給する装置となる。なお、上述のケーブルのうち1つの線は、微弱な待機電流が常に流れており、WOL (Wake-up On LAN) の信号など、電源供給対象のサーバ100のチップセット側からの制御信号を、電源制御装置240に伝達する信号線としての役割を担っている。本実施例では、この線を内部信号線30とする。
- [0023] また、電源制御装置240は、所定プロセッサを備えたシステム管理用コントローラであるBMC (Baseboard Management Controller) で構成されている。一般的にこのBMCは、電源装置230での供給電圧や冷却ファンの回転数、サーバ100のCPU (演算装置105) を含む各種パーツの温度といった各種事象について常時監視し、OS102に通知する機能を備えている。このBMCすなわち電源制御装置240は、サーバ本体が電源オフ状態であっても、商用電源等の適宜な電源ソースが電源装置230に接続されているかぎり電力が供給され、稼働が継続される。つまり電源制御装置240は、電源供給対象のサーバ100におけるOS102など上位ソフトウェアとは独立した構成となっている。
- [0024] 上述したBMCたる電源制御装置240は、ROMなど適宜な不揮発性記憶装置で構成される記憶装置201、RAMなど揮発性記憶装置で構成されるメモリ203、記憶装置201に保持されるプログラム202をメモリ203に読み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうプロセッサたる演算装置204、上述の内部信号線30を介して電源供給対象たるサーバ100のチップセットと接続し

、サーバ１００のＯＳ１０２との間で通信を行う通信装置２０５を備える。

[0025] こうした電源機構２００の記憶装置２０１内には、電源機構２００として必要な機能を実装する為のプログラム２０２と、監視テーブル２２５が記憶されている。このうちプログラム２０２としては、テーブル監視プログラム２１０、および電源制御プログラム２１１が含まれている。テーブル監視プログラム２１０は、上述のサーバ１００における生存通知機能から内部通信線３０を介し送信されてきた所定情報、例えばタイムスタンプを監視テーブル２２５に書込処理し、当該書込処理を実行する度に所定タイマーをリセットする動作を繰り返すと共に、監視テーブル２２５における情報更新が一定時間内にあったか否か繰り返し判定するためのプログラムである。また、電源制御プログラム２１１は、テーブル監視プログラム２１０からの通知を受けて、電源装置２３０に対する電源オフないしリセットの動作を実行し、当該動作実行後、待機系サーバ１８０に対して回復動作の指示を行うプログラムである。この電源制御プログラム２１１における電源オフないしリセットの機能は一般的なＢＭＣにおける電源制御機能と同様である。

[0026] 電源制御装置２４０の演算装置２０４が上述のテーブル監視プログラム２１０を実行することで、テーブル監視機能が実装される。また、電源制御装置２４０の演算装置２０４が上述の電源制御プログラム２１１を実行することで、電源制御機能が実装される。

[0027] この場合、テーブル監視機能は、電源機構２００に常駐し、例えば、サーバ１００の生存通知機能から送信されてくるのがタイムスタンプである場合、このタイムスタンプを内部信号線３０を介して受信する度に監視テーブル２２５に書き込んで更新し続けると共に、監視テーブル２２５におけるタイムスタンプの更新が一定時間内にあったか否か、タイムスタンプ更新ごとにタイマーを起動してモニタリングし、一定時間内のタイムスタンプ更新が継続されるべきとの規則に基づいた判定を実行する。この判定により、上述のタイムスタンプ更新が一定時間内になされなかった時点を検知した場合、テーブル監視機能は、サーバ１００すなわちＯＳ１０２側からの書込処理が滞

っていることを認識し、上述の電源制御機能に対し、電源装置 230 の電源オフないしリセットを指示する。

[0028] なお、上述の書込処理で監視テーブル 225 に書き込まれる情報として、図 4 に示すようにタイムスタンプの例をあげたが、その他にも、書込処理機会で変化しない特定の固定値、あるいは、書込処理機会ごとにインクリメントされる数値、など適宜な規則に応じた様々なものを採用することも出来る。

[0029] 書込処理機会で変化しない特定の固定値（例：1）を上述の生存通知機能から受信し、これを監視テーブル 225 に書き込む場合、テーブル監視機能は、固定値の書込を行う度に所定時間内に他の所定値（例：0）で上書き更新する。テーブル監視機能は、この上書き更新を行う度にタイマーを起動し、一定時間内に上書き更新が実行されるべきとの規則に基づいた判定を実行し、上述の上書き更新が一定時間内になされなかった時点を検知した場合、サーバ 100 すなわち OS 102 側からの書込処理が滞っていることを認識し、上述の電源制御機能に対し、電源装置 230 の電源オフないしリセットを指示する。

[0030] また、監視テーブル 225 に対し、書込処理機会ごとにインクリメントされる数値を書き込む場合、テーブル監視機能は、上述の生存通知機能から受けた数値の書込を行う度にタイマーを起動し、一定時間内に更にインクリメントされた数値の書き込みが実行されるべきとの規則に基づいた判定を実行し、上述の数値の書き込みが一定時間内になされなかった時点を検知した場合、サーバ 100 すなわち OS 102 側からの書込処理が滞っていることを認識し、上述の電源制御機能に対し、電源装置 230 の電源オフないしリセットを指示する。

[0031] なお、上述のテーブル監視プログラム 210 によるテーブル監視機能と監視テーブル 225 の組み合わせは、いわゆるウォッチドッグタイマとみなすこともできる。

[0032] 以下、本実施形態における多重系システム管理方法の実際手順について図

に基づき説明する。以下で説明する多重系システム管理方法に対応する各種動作は、多重系システム 10 を構成する、上述のサーバ 100 および電源機構 200 が各々実行するプログラムによって実現される。そして各プログラムは、以下に説明される各種の動作を行うためのコードから構成されている。

[0033] 図 5 は、本実施形態における多重系システム管理方法の処理手順例 1 を示すフロー図である。ここで、多重系システム 10 における現用系サーバ 150 が、業務プログラム 110 により金融機関の所定業務処理を継続的に実行中であると共に、この現用系サーバ 150 と待機系サーバ 180 は、上述のクラスタ監視プログラム 111 によるクラスタ監視機能で従来からのハートビートによる死活監視を互いに行っている状況にあるとする。また、このクラスタ監視機能による従来の死活監視と平行し、現用系サーバ 150 および待機系サーバ 180 に常駐する上述の生存通知機能が、内部信号線 30 経由で電源機構 200 に対してタイムスタンプを一定時間毎に送信しているものとする。

[0034] こうした状況下において、現用系サーバ 150 は、自身に常駐している生存通知機能が発したタイムスタンプの値を、当該現用系サーバ 150 のマザーボード上のコネクタから内部信号線 30 を経由し、電源機構 200 における電源制御装置 240 に送信する (s 100)。

[0035] 一方、電源機構 200 における電源制御装置 240 は、上述の現用系サーバ 150 の生存通知機能から送信されてきたタイムスタンプを、記憶装置 201 の監視テーブル 225 に書込処理する (s 101) と共に、テーブル監視プログラム 210 によるテーブル監視機能によって、監視テーブル 225 へのタイムスタンプの書込処理タイミングを検知し、当該検知に応じて、所定時間でタイムアップするタイマーをリセットし、経時計測を開始する (s 102)。

[0036] 上述のタイマーが起動された状態における電源制御装置 240 は、上述のテーブル監視機能により、タイマーにおけるタイムアップまでの所定時間中

、監視テーブル２２５でのタイムスタンプの次なる書込処理、すなわち更新事象を監視する（ｓ１０３）。このタイムアップまでの監視中に、新たなタイムスタンプが生存通知機能から送られてきて、監視テーブル２２５でのタイムスタンプ更新を行った場合（ｓ１０４：ＯＫ）、電源制御装置２４０は、当該タイムスタンプ更新に応じて、処理をステップｓ１０２に戻し、上述のタイマーをリセットして経時計測を再度開始する。

[0037] 他方、このタイムアップまでの監視中に、新たなタイムスタンプを生存通知機能から受信出来ず、監視テーブル２２５でのタイムスタンプ更新が無かった場合（ｓ１０４：ＮＧ）、電源制御装置２４０のテーブル監視機能は、現用系サーバ１５０すなわちＯＳ１０２においてタイムスタンプ発行が出来ない何らかの障害が発生していると認識し、電源制御プログラム２１１による電源制御機能に対し、電源装置２３０の電源オフないしリセットを指示する（ｓ１０５）。この電源オフないしリセットの指示を受けた電源制御機能は、電源装置２３０を電源オフないしリセットさせる（ｓ１０６）。この電源装置２３０を電源オフないしリセットさせる動作は従来の電源制御動作と同様である。

[0038] 電源制御装置２４０は、電源制御機能により、上述の電源装置２３０での電源オフないしリセットの動作完了を検知し、内部信号線３０およびネットワーク２０を経由して、待機系サーバ１８０に対する回復動作の指示を実行する（ｓ１０７）。この指示を受けた待機系サーバ１８０は従来同様の手順で、現用系サーバ１５０から速やかに業務処理を受け継いで、新たな現用系として稼働を開始することとなる。

[0039] なお、上述した、監視テーブル２２５でのタイムスタンプ更新を監視する動作フローとは別に、従来のクラスタ監視機能による死活監視で異常発生が検知された場合もステップｓ１０７と同様に、待機系サーバ１８０が現用系サーバ１５０に成り代わり、新たな現用系として稼働する動作フローが実行される。この処理については従来同様であるので説明を省略する。いずれにしても、異常発生を早く検知した方の動作フローが待機系サーバ１８０によ

る回復動作に至る処理を実行する。

[0040] また、現用系サーバ150および待機系サーバ180におけるOS102等の本来機能、およびそれを実現するハードウェアに異常は無く、生存通知プログラム112による生存通知機能にのみ不具合が生じた場合、特に対応動作を行わないと、上述のタイムスタンプの送信、それに伴う監視テーブル225でのタイムスタンプ更新が実行されないことになり、無意味な回復動作が実行される事態となる。

[0041] そこで、図6のフローにて示すように、現用系サーバ150および待機系サーバ180のOS102や所定のプログラムは、上述の生存通知プログラム112による生存通知機能の稼働状況を常にモニタリングし(s200)、生存通知機能においてスローダウンあるいは停止といった何らかの不具合事象発生を検知した場合(s201:Y)、所定時間内に生存通知プログラム112を再実行して生存通知機能の再起動を行う(s202)。この一連の処理は、上述のステップs100～s107の処理とは平行に実行されているものとする。

[0042] こうした運用を行うことにより、不具合を生じた生存通知機能を速やかに復旧して、速やかにタイムスタンプの発行と監視テーブル225でのタイムスタンプ更新の処理を再開することができる。

[0043] 続いて、第1実施形態とは異なり、図7に例示するように、ネットワーク20を介し現用系サーバ150および待機系サーバ180と通信可能な監視用コンピュータ300が生存通知機能を実装する第2実施形態について説明する。

[0044] この場合、監視用コンピュータ300のハードウェア構成は以下のようなものとなる。図8は第2実施形態の監視用コンピュータ300の構成例を示す図である。監視用コンピュータ300は、ハードディスクドライブなど適宜な不揮発性記憶装置で構成される記憶装置301、RAMなど揮発性記憶装置で構成されるメモリ304、記憶装置301に保持されるOS(Operating System)302を起動し、適宜なプログラム303を読

み出すなどして実行し装置自体の統括制御を行なうとともに各種判定、演算及び制御処理を行なうCPUなどの演算装置305、ネットワーク20と接続しサーバ100との通信処理を担う通信装置306を備える。

[0045] なお、上述のプログラム303としては生存通知プログラム310が含まれている。この生存通知プログラム310は、上述した電源機構200における監視テーブル225に対するタイムスタンプの書込要求を、現用系サーバ150および待機系サーバ180に対して所定間隔で繰り返し送信するプログラムである。

[0046] この場合、監視用コンピュータ300の演算装置305が上述の生存通知プログラム310を実行することで生存通知機能が実装される。生存通知機能は、監視用コンピュータ300に常駐し、所定情報として、例えば現在時刻情報すなわちタイムスタンプを一定時間間隔でOS302のクロック機能等から得て、これを含む書込要求をネットワーク20を介して現用系サーバ150および待機系サーバ180に対し送信する動作を実現する。

[0047] こうしたシステム構成における現用系サーバ150および待機系サーバ180は、監視用コンピュータ300からの書込要求を受けるごとに、当該書込要求を電源機構200に転送することになる。この書込要求の転送処理は、現用系サーバ150および待機系サーバ180における転送プログラム113により実行される。第2実施形態における現用系サーバ150および待機系サーバ180すなわちサーバ100のハードウェア構成については図9に示すとおりであるが、この転送プログラム113を保持する一方、生存通知プログラム112を保持しない構成となっている以外は第1実施形態と同様である。

[0048] また、第1実施形態と同様に、監視用コンピュータ300のOS302や所定のプログラムが、上述の生存通知プログラム310による生存通知機能の稼働状況をモニタリングしておき、生存通知機能においてスローダウンあるいは停止といった何らかの不具合事象発生を検知した場合、所定時間内に生存通知プログラム310を再実行して生存通知機能の再起動を行うとすれ

ば好適である。こうした運用を行うことにより、不具合を生じた生存通知機能を速やかに復旧して、速やかに書込処理を再開することができる。

[0049] 一方、第2実施形態における電源機構200のハードウェア構成は、第1実施形態での構成と同様であるため説明は省略する。

[0050] 続いて、当該第2実施形態における多重系システム管理方法について説明する。図10は第2実施形態における多重系システム管理方法の処理手順例1を示すフロー図である。ここで、多重系システム10における現用系サーバ150が、業務プログラム110により金融機関の所定業務処理を継続的に実行中であると共に、この現用系サーバ150と待機系サーバ180は、上述のクラスタ監視プログラム111によるクラスタ監視機能で従来からのハートビートによる死活監視を互いに行っている状況にあるとする。また、このクラスタ監視機能による従来の死活監視と平行し、監視用コンピュータ300に常駐する上述の生存通知機能が、ネットワーク20経由で上述の書込要求を現用系サーバ150に対して一定時間毎に送信しているものとする。

[0051] こうした状況下において、監視用コンピュータ300は、自身に常駐している生存通知機能が発したタイムスタンプの値を、通信装置306を用いてネットワーク20経由で現用系サーバ150に送信する（s300）。

[0052] 一方、現用系サーバ150は、監視用コンピュータ300から書込要求を受信し、この書込要求を、上述の転送プログラム113による転送機能で、当該現用系サーバ150のマザーボード上のコネクタから内部信号線30を経由し、電源機構200における電源制御装置240に転送する（s301）。

[0053] 電源機構200における電源制御装置240は、上述の現用系サーバ150の転送機能から送信されてきた書込要求を受信し、この書込要求が示すタイムスタンプを、記憶装置201の監視テーブル225に書込処理する（s302）と共に、テーブル監視プログラム210によるテーブル監視機能によって、監視テーブル225へのタイムスタンプの書込処理タイミングを検

知し、当該検知に応じて、所定時間でタイムアップするタイマーをリセットし、経時計測を開始する（s 3 0 3）。

[0054] 上述のタイマーが起動された状態における電源制御装置 2 4 0 は、上述のテーブル監視機能により、タイマーにおけるタイムアップまでの所定時間中、監視テーブル 2 2 5 でのタイムスタンプの次なる書込処理、すなわち更新事象を監視する（s 3 0 4）。このタイムアップまでの監視中に、新たなタイムスタンプが転送機能から送られてきて、監視テーブル 2 2 5 でのタイムスタンプ更新を行った場合（s 3 0 5 : O K）、電源制御装置 2 4 0 は、当該タイムスタンプ更新に応じて、処理をステップ s 3 0 3 に戻し、上述のタイマーをリセットして経時計測を再度開始する。

[0055] 他方、このタイムアップまでの監視中に、新たなタイムスタンプを転送機能から受信出来ず、監視テーブル 2 2 5 でのタイムスタンプ更新が無かった場合（s 3 0 5 : N G）、電源制御装置 2 4 0 のテーブル監視機能は、現用系サーバ 1 5 0 すなわち O S 1 0 2 において監視用コンピュータ 3 0 0 からの書込要求を転送出来ない何らかの障害が発生していると認識し、電源制御プログラム 2 1 1 による電源制御機能に対し、電源装置 2 3 0 の電源オフないしリセットを指示する（s 3 0 6）。この電源オフないしリセットの指示を受けた電源制御機能は、電源装置 2 3 0 を電源オフないしリセットさせる（s 3 0 7）。この電源装置 2 3 0 を電源オフないしリセットさせる動作は従来の電源制御動作と同様である。

[0056] 電源制御装置 2 4 0 は、電源制御機能により、上述の電源装置 2 3 0 での電源オフないしリセットの動作完了を検知し、内部信号線 3 0 およびネットワーク 2 0 を経由して、待機系サーバ 1 8 0 に対する回復動作の指示を実行する（s 3 0 8）。この指示を受けた待機系サーバ 1 8 0 は従来同様の手順で、現用系サーバ 1 5 0 から速やかに業務処理を受け継いで、新たな現用系として稼働を開始することとなる。

[0057] また、現用系サーバ 1 5 0 および待機系サーバ 1 8 0 における O S 1 0 2 等の本来機能、およびそれを実現するハードウェアに異常は無く、転送プロ

グラム 1 1 3 による転送機能にのみ不具合が生じた場合、特に対応動作を行わないと、上述のタイムスタンプを含む書込要求の転送、それに伴う監視テーブル 2 2 5 でのタイムスタンプ更新が実行されないことになり、無意味な回復動作が実行される事態となる。

[0058] そこで、図 1 1 のフローにて示すように、監視用コンピュータ 3 0 0 の O S 3 0 2 や所定のプログラムは、上述の生存通知プログラム 3 1 0 による生存通知機能の稼働状況を常にモニタリングし (s 4 0 0) 、生存通知機能においてスローダウンあるいは停止といった何らかの不具合事象発生を検知した場合 (s 4 0 1 : Y) 、所定時間内に生存通知プログラム 3 1 0 を再実行して生存通知機能の再起動を行う (s 4 0 2) 。この一連の処理は、上述のステップ s 3 0 0 ~ s 3 0 8 の処理とは平行に実行されているものとする。

[0059] こうした運用を行うことにより、不具合を生じた生存通知機能を速やかに復旧して、速やかにタイムスタンプの発行と、これを含む書込要求の送信、ならびに書込要求に伴う監視テーブル 2 2 5 でのタイムスタンプ更新の処理を再開することができる。

[0060] 以上、本発明を実施するための最良の形態などについて具体的に説明したが、本発明はこれに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

[0061] こうした本実施形態によれば、多重系システムで従来から備わっているクラスタリングソフトによる相互監視機能に加えて、電源機構での監視機能を更に備えることで、多重系システムにおける障害検知構成を多重化して、障害発生を的確に検知し、ひいては必要な系切替動作を確実に実行可能となる。

[0062] 本明細書の記載により、少なくとも次のことが明らかにされる。すなわち、本実施形態の多重系システムにおいて、前記多重化された各コンピュータが、前記書込処理を、前記電源機構の記憶装置に対して所定間隔で繰り返し実行する演算装置を備えるものであるとしてもよい。

[0063] これによれば、電源機構の記憶装置に対する書込処理が一定頻度で実行さ

れ、この書込処理の途絶事象等を所定規則に対応しない事象として迅速に検知出来ることになる。

[0064] また、本実施形態の多重系システムにおいて、前記多重化された各コンピュータの演算装置は、前記書込処理として、現在時刻情報を所定時間ごとに前記電源機構の記憶装置に対して書き込むものであり、前記電源機構の演算装置は、当該電源機構の記憶装置に書込処理された前記現在時刻情報を所定時間ごとに読み取り、前記現在時刻情報が所定時間以上更新されていなかった場合、電源の停止ないしリセットの動作を実行し、当該動作実行後、前記各コンピュータのうち他方のコンピュータに対して回復動作の指示を実行するものである、としてもよい。

[0065] これによれば、電源機構の記憶装置での現在時刻情報すなわちタイムスタンプの更新が一定時間内にあったか否かといった判定を行うことで、該当コンピュータが上述の書込処理を実行できない何らかの異常状態にあることを簡便かつ確実に検知出来ることになる。

[0066] また、本実施形態の多重系システムにおいて、前記多重化された各コンピュータの演算装置は、前記書込処理の実行機能を、所定事象の発生検知に応じて再起動するものであるとしてもよい。

[0067] これによれば、上述の書込処理を行う機能（生存通知プログラムにより実装される機能）自体に何らかの不具合が生じた場合に対応して当該機能を再起動し、迅速に書込処理を再開することが可能となる。そのため、多重系システムを成すコンピュータ自体に不具合は発生していないにも関わらず、上述の書込処理の機能のみの不具合に由来する障害検知により系切替が実行される事態を回避出来る。

[0068] また、本実施形態の多重系システムにおいて、前記多重化された各コンピュータと通信する通信装置と、前記電源機構の記憶装置に対する前記所定規則に対応した前記所定情報の書込要求を、前記各コンピュータに対して所定間隔で繰り返し送信する演算装置と、を備えた監視用コンピュータを更に含み、前記多重化された各コンピュータの演算装置は、前記監視用コンピュー

タからの前記書込要求を受けるごとに、当該書込要求が示す所定情報を、前記電源機構の記憶装置に対して書き込むものである、としてもよい。

[0069] これによれば、多重系システムを成す現用系及び待機系の各コンピュータとは完全に別体の装置すなわち監視用コンピュータから、上述の書込処理に対応した要求を行うことになり、現用系及び待機系での生存通知プログラム自体の破損、停止といった事態とは無関係に障害検知機能が維持されやすくなる。

[0070] また、本実施形態の多重系システムにおいて、前記監視用コンピュータの演算装置は、前記書込要求として、現在時刻情報を所定時間ごとに前記電源機構の記憶装置に対して書き込む要求を、前記各コンピュータに送信するものであり、前記多重化された各コンピュータの演算装置は、前記監視用コンピュータからの前記書込要求を受けるごとに、当該書込要求が示す現在時刻情報を、前記電源機構の記憶装置に対して書き込むものである、としてもよい。

[0071] これによれば、電源機構の記憶装置での現在時刻情報すなわちタイムスタンプの更新が一定時間内にあったか否かといった判定を行うことで、該当コンピュータが上述の監視用コンピュータ由来の書込要求に応じた書込処理を実行できない何らかの異常状態にあることを簡便かつ確実に検知出来ることになる。

[0072] また、本実施形態の多重系システムにおいて、前記監視用コンピュータの演算装置は、前記書込要求の実行機能を、所定事象の発生検知に応じて再起動するものであるとしてもよい。

[0073] これによれば、上述の書込要求を行う機能（生存通知プログラムにより実装される機能）自体に何らかの不具合が生じた場合に対応して当該機能を再起動し、迅速に書込処理を再開することが可能となる。そのため、多重系システムを成すコンピュータ自体に不具合は発生していないにも関わらず、監視用コンピュータにおける不具合に由来する障害検知により系切替が実行される事態を回避出来る。

符号の説明

- [0074] 1 0 多重系システム
- 2 0 ネットワーク
- 3 0 内部信号線
- 1 0 0 サーバ（コンピュータ）
- 1 0 1 記憶装置
- 1 0 2 OS（Operating System）
- 1 0 3 プログラム
- 1 0 4 メモリ
- 1 0 5 演算装置
- 1 0 6 通信装置
- 1 0 7 ドライブ
- 1 1 0 業務プログラム
- 1 1 1 クラスタ監視プログラム
- 1 1 2 生存通知プログラム
- 1 1 3 転送プログラム
- 1 5 0 現用系サーバ
- 1 8 0 待機系サーバ
- 2 0 0 電源機構
- 2 0 1 記憶装置
- 2 0 2 プログラム
- 2 0 3 メモリ
- 2 0 4 演算装置
- 2 0 5 通信装置
- 2 1 0 テーブル監視プログラム
- 2 1 1 電源制御プログラム
- 2 2 5 監視テーブル
- 2 3 0 電源装置

- 2 4 0 電源制御装置
- 3 0 0 監視用コンピュータ
- 3 0 1 記憶装置
- 3 0 2 OS (Operating System)
- 3 0 3 プログラム
- 3 0 4 メモリ
- 3 0 5 演算装置
- 3 0 6 通信装置
- 3 1 0 生存通知プログラム

請求の範囲

[請求項1]

多重化された各コンピュータの電源機構が、

当該電源機構の記憶装置に対する、他装置ないし該当コンピュータの他機構からの所定情報の書込処理を監視し、前記書込処理が所定規則に対応したものでなかった場合、電源の停止ないしリセットの動作を実行し、当該動作実行後、前記各コンピュータのうち他方のコンピュータに対して回復動作の指示を実行する演算装置を備えるものである、

ことを特徴とする多重系システム。

[請求項2]

前記多重化された各コンピュータが、

前記書込処理を、前記電源機構の記憶装置に対して所定間隔で繰り返し実行する演算装置を備えるものであることを特徴とする請求項1に記載の多重系システム。

[請求項3]

前記多重化された各コンピュータの演算装置は、

前記書込処理として、現在時刻情報を所定時間ごとに前記電源機構の記憶装置に対して書き込むものであり、

前記電源機構の演算装置は、

当該電源機構の記憶装置に書込処理された前記現在時刻情報を所定時間ごとに読み取り、前記現在時刻情報が所定時間以上更新されていなかった場合、電源の停止ないしリセットの動作を実行し、当該動作実行後、前記各コンピュータのうち他方のコンピュータに対して回復動作の指示を実行するものである、

ことを特徴とする請求項2に記載の多重系システム。

[請求項4]

前記多重化された各コンピュータの演算装置は、

前記書込処理の実行機能を、所定事象の発生検知に応じて再起動するものであることを特徴とする請求項3に記載の多重系システム。

[請求項5]

前記多重化された各コンピュータと通信する通信装置と、

前記電源機構の記憶装置に対する前記所定規則に対応した前記所定

情報の書込要求を、前記各コンピュータに対して所定間隔で繰り返し送信する演算装置と、

を備えた監視用コンピュータを更に含み、

前記多重化された各コンピュータの演算装置は、

前記監視用コンピュータからの前記書込要求を受けるごとに、当該書込要求が示す所定情報を、前記電源機構の記憶装置に対して書き込むものである、

ことを特徴とする請求項 1 に記載の多重系システム。

[請求項6]

前記監視用コンピュータの演算装置は、

前記書込要求として、現在時刻情報を所定時間ごとに前記電源機構の記憶装置に対して書き込む要求を、前記各コンピュータに送信するものであり、

前記多重化された各コンピュータの演算装置は、

前記監視用コンピュータからの前記書込要求を受けるごとに、当該書込要求が示す現在時刻情報を、前記電源機構の記憶装置に対して書き込むものである、

ことを特徴とする請求項 5 に記載の多重系システム。

[請求項7]

前記監視用コンピュータの演算装置は、

前記書込要求の実行機能を、所定事象の発生検知に応じて再起動するものであることを特徴とする請求項 6 に記載の多重系システム。

[請求項8]

多重化された各コンピュータの電源機構が、

当該電源機構の記憶装置に対する、他装置ないし該当コンピュータの他機構からの所定情報の書込処理を監視し、前記書込処理が所定規則に対応したものでなかった場合、電源の停止ないしリセットの動作を実行し、当該動作実行後、前記各コンピュータのうち他方のコンピュータに対して回復動作の指示を実行する、

ことを特徴とする多重系システム管理方法。