(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2025-86620
(P2025-86620A)
(43)公開日　令和7年6月9日(2025.6.9)

(51)国際特許分類　FI

G06F 9/48 (2006.01)	G06F	9/48	300H
G06F 9/455(2018.01)	G06F	9/455	150
G06F 9/52 (2006.01)	G06F	9/52	120B

審査請求　未請求　請求項の数　14　ＯＬ　（全34頁）

(21)出願番号　特願2023-200713(P2023-200713)
(22)出願日　令和5年11月28日(2023.11.28)

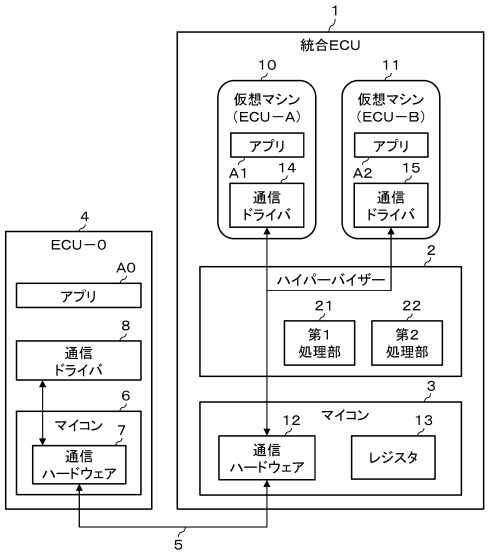
(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(71)出願人　501100881
イーソル株式会社
東京都中野区本町一丁目３２番２号
(74)代理人　110000567
弁理士法人サトー
(72)発明者　津田 大輝
愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内
(72)発明者　大井 学
東京都港区港南二丁目１６番２号 太陽生命品川ビル９階
(72)発明者　中山 大悟

最終頁に続く

(54)【発明の名称】　動作制御装置、動作制御プログラムおよび電子制御装置

(57)【要約】
【課題】連続して実行しなければならない処理が切り替え処理により中断されることを防止する。
【解決手段】第１処理部２１は、ＶＭ１０、ＶＭ１１のうち動作中のものである動作マシンを切り替える切り替え処理を実行することができる。動作マシンは、連続して実行しなければならない特定処理を開始する際に禁止要求を送信するとともに特定処理を完了した際に許可要求を送信する。第２処理部２２は、禁止要求を受信したとき、その時点から動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、判断処理の結果、残り時間が設定時間以上の時間である場合には切り替え処理の実行を禁止する禁止処理を実行するとともに残り時間が設定時間未満の時間である場合には禁止処理を実行せず、許可要求を受信したときに切り替え処理の実行を許可する許可処理を実行する。動作マシンは、禁止処理が実行されている禁止期間中に特定処理を実行する。
【選択図】図１

Fig.1



【特許請求の範囲】
【請求項１】
複数の仮想マシン（１０、１１）のそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置であって、
前記複数の仮想マシンのうち動作中のものを動作マシンとすると、
前記動作マシンを切り替える切り替え処理を実行することができる第１処理部（２１）と、
前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理部（２２）と、
を備え、
前記動作マシンは、連続して実行しなければならない処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっており、
前記第２処理部は、
前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、
前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっており、
前記許可要求を受信したとき、前記許可処理を実行するようになっており、
前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する動作制御装置。
【請求項２】
前記第１処理部は、前記禁止期間中、前記動作時間を所定のマージン時間だけ延長することができるようになっており、
前記第２処理部は、前記禁止要求を受信した時点から延長した前記動作時間が経過する時点までの時間を前記残り時間として前記判断処理を実行する請求項１に記載の動作制御装置。
【請求項３】
前記動作周期毎に使用可能時間が設定されており、
前記第１処理部は、前記使用可能時間から必要とする前記マージン時間を消費する形で前記動作時間の延長を行うようになっている請求項２に記載の動作制御装置。
【請求項４】
前記複数の仮想マシンのそれぞれ毎に使用可能時間が設定されており、
前記第１処理部は、前記動作マシンに対応する前記使用可能時間から必要とする前記マージン時間を消費する形で前記動作時間の延長を行うようになっている請求項２に記載の動作制御装置。
【請求項５】
前記第１処理部は、前記動作周期において最後に動作する前記動作マシンの動作が開始される際に前記使用可能時間に余りがある場合、その余りの少なくとも一部を最後に動作する前記動作マシンの前記動作時間に割り当てるようになっている請求項３に記載の動作制御装置。
【請求項６】
前記第１処理部は、前記禁止期間において前記動作時間が経過した時点で前記特定処理が完了していない場合、異常が発生したと判断して前記切り替え処理および前記異常を外部に通知する通知処理の一方または双方を実行する請求項１から５のいずれか一項に記載の動作制御装置。
【請求項７】
前記第１処理部は、前記禁止期間において前記動作時間が経過した時点で前記特定処理が完了していない場合、異常が発生したと判断して次回以降の前記動作周期において前記

許可要求を受信すると前記異常を外部に通知する通知処理を実行する請求項１から５のいずれか一項に記載の動作制御装置。
【請求項８】
前記設定時間は、前記複数の仮想マシンのそれぞれ毎に予め設定されている請求項１から５のいずれか一項に記載の動作制御装置。
【請求項９】
前記第２処理部は、前記禁止要求を受信したとき、前記禁止要求を送信した前記動作マシンが開始する前記特定処理に要する時間に基づいて前記設定時間を設定する請求項１から５のいずれか一項に記載の動作制御装置。
【請求項１０】
前記第１処理部は、前記動作マシンが前記禁止要求を送信した後に前記禁止処理が実行されなかった場合、前記禁止処理が実行されるまで前記動作マシンに前記禁止要求の送信を繰り返し実行させるようになっている請求項１から５のいずれか一項に記載の動作制御装置。
【請求項１１】
前記第１処理部は、前記動作マシンが前記禁止要求を送信した後に前記禁止処理が実行されなかった場合、前記切り替え処理が実行されるまでの期間、前記動作マシンを待機状態とする、または、前記動作マシンを前記特定処理とは異なる別の処理を実行可能な状態とするようになっている請求項１から５のいずれか一項に記載の動作制御装置。
【請求項１２】
前記第１処理部は、前記動作マシンが前記禁止要求を送信した後に前記禁止処理が実行されなかった場合、前記動作マシンに割り当てられた前記動作時間が経過する前に前記切り替え処理を実行する請求項１から５のいずれか一項に記載の動作制御装置。
【請求項１３】
複数の仮想マシン（ＶＭ１０、ＶＭ１１）のそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置（２）に実行させる動作制御プログラムであって、
前記複数の仮想マシンのうち動作中のものを動作マシンとすると、
前記動作マシンを切り替える切り替え処理を実行することができる第１処理と、
前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理と、
を含み、
前記動作マシンは、連続して実行しなければならない処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっており、
前記第２処理では、
前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、
前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっており、
前記許可要求を受信したとき、前記許可処理を実行するようになっており、
前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する動作制御プログラム。
【請求項１４】
コンピュータ（３）と、前記コンピュータ上で動作する複数の仮想マシン（ＶＭ１０、ＶＭ１１）と、前記複数の仮想マシンのそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置（２）と、を備えた電子制御装置であって、
前記複数の仮想マシンのうち動作中のものを動作マシンとすると、

前記動作制御装置は、
前記動作マシンを切り替える切り替え処理を実行することができる第１処理部（２１）と、
前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理部（２２）と、
を備え、
前記動作マシンは、連続して実行しなければならない処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっており、
前記第２処理部は、
前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、
前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっており、
前記許可要求を受信したとき、前記許可処理を実行するようになっており、
前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する電子制御装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、複数の仮想マシンのそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置、動作制御装置に実行させる動作制御プログラムおよび動作制御装置を備えた電子制御装置に関する。

【背景技術】

【０００２】

例えば自動車などの車両には複数の電子制御装置が搭載されており、それら複数の電子制御装置は、互いの間で通信を行い連携して各種の処理を行うようになっている。なお、本明細書では、電子制御装置のことをＥＣＵと省略することがある。近年、車両に搭載されるＥＣＵの数が増加する傾向であることから、複数のＥＣＵを１つに統合するという方法が実施されている。このように統合されたＥＣＵである統合ＥＣＵでは、従来単独で動作していた複数のＥＣＵの機能が、ハイパーバイザーを介して１つのマイクロコンピュータ上に複数の仮想マシンとして搭載されることになる。なお、本明細書では、マイクロコンピュータのことをマイコンと省略することがある。

【０００３】

従来のＥＣＵでは１つのマイコンのリソースを１つのＥＣＵの機能により占有可能であったが、統合ＥＣＵでは１つのマイコンのリソースを複数の仮想マシンのそれぞれが使用することになる。そのため、統合ＥＣＵでは、複数の仮想マシンに対して固定の動作時間を割り当てる時分割スケジューリングでの制御が行われる。時分割スケジューリングにより、複数の仮想マシンのそれぞれは、予め割り当てられた動作時間で個別に動作するため、各仮想マシン間で協調してリソースを割り振る必要がなくなる。

【０００４】

上記構成では、所定の仮想マシンが動作する際、動作時間が消費された段階で動作中の仮想マシンを切り替える切り替え処理が実行されることになる。つまり、上記構成では、動作中の処理が完了したか否かに関係なく切り替え処理が実行される可能性がある。そのため、上記構成では、連続して実行しなければならない処理、つまり中断不可能な処理またはアトミックな処理の実行中に切り替え処理が実行されてしまい、その結果、中断不可能な処理などが中断されてしまう、という課題が生じることになる。

【０００５】

このような課題に関連する従来技術として特許文献１、２に開示される技術を挙げるこ

とができる。まず、特許文献１には、タスクをいくつかのグループに分割し、それらグループの処理時間を適応的に時分割する方法が開示されている。続いて、特許文献２には、中断不可能な処理中に対して割り込みタスクが発生した場合、その割り込みタスクを検出して割り込みタスクを無効化し、中断不可能な処理が完了後に割り込みタスクを実行することで中断不可能な処理を保証する方法が開示されている。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】米国特許第９３６１１５６号明細書

【特許文献２】特開２００２－１５７１３２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかし、特許文献１に開示される従来技術では、中断不可能な処理について考慮されておらず、また、特許文献２に開示される従来技術では、動作中の仮想マシンを切り替える切り替え処理のような事前に割り込みが発生すると分かっている処理と中断不可能な処理が完了せずに割り込みタスクが実行されない可能性があることを考慮できていない。このようなことから、上記従来技術では、上記した課題を解決することが困難であった。

【０００８】

本発明は上記事情に鑑みてなされたものであり、その目的は、連続して実行しなければならない処理が切り替え処理により中断されることを防止することができる動作制御装置、動作制御プログラムおよび電子制御装置を提供することにある。

【課題を解決するための手段】

【０００９】

請求項１に記載の動作制御装置は、複数の仮想マシン（１０、１１）のそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う。この場合、前記複数の仮想マシンのうち動作中のものを動作マシンとする。前記動作制御装置は、前記動作マシンを切り替える切り替え処理を実行することができる第１処理部（２１）と、前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理部（２２）と、を備える。前記動作マシンは、連続して実行しなければならない処理、つまり中断不可能な処理またはアトミックな処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっている。

【００１０】

前記第２処理部は、前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行する。前記第２処理部は、前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっている。また、前記第２処理部は、前記許可要求を受信したとき、前記許可処理を実行するようになっている。前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する。

【００１１】

上記構成によれば、動作マシンが特定処理を実行しているときに動作マシンを切り替える切り替え処理が発生することが防止される。このようにすれば、特定処理が完了するまで一貫した動作を保証することができる。また、上記構成によれば、第２処理部が判断処理を実行することにより、残り時間が設定時間未満の時間である場合、言い換えると、これから開始しようとする特定処理を動作時間が経過するまでに完了することができる可能性が極めて低い場合、禁止処理が実行されず、それに伴い、特定処理も実行されない。このようにすれば、その動作周期で完了する見込みのない特定処理を、次の動作周期にて実

行することができる。このように、上記構成によれば、連続して実行しなければならない処理である特定処理が切り替え処理により中断されることを防止することができるという優れた効果が得られる。

【図面の簡単な説明】

【００１２】

【図１】第１実施形態に係る統合ＥＣＵおよびＥＣＵの構成を模式的に示す図

【図２】比較例に係る第１比較動作例における各部の動作内容を表すタイミングチャート

【図３】比較例に係る第２比較動作例における各部の動作内容を表すタイミングチャート

【図４】第１実施形態に係る第１動作例における各部の動作内容を表すタイミングチャート

【図５】第１実施形態に係る第２動作例における各部の動作内容を表すタイミングチャート

【図６】第１実施形態に係る第３動作例における各部の動作内容を表すタイミングチャート

【図７】第１実施形態に係る第４動作例における各部の動作内容を表すタイミングチャート

【図８】第１実施形態に係る第５動作例における各部の動作内容を表すタイミングチャート

【図９】第１実施形態に係る第６動作例における各部の動作内容を表すタイミングチャート

【図１０】第１実施形態に係る第７動作例における各部の動作内容を表すタイミングチャート

【図１１】第１実施形態に係る第８動作例における各部の動作内容を表すタイミングチャート

【図１２】第１実施形態に係る第９動作例における各部の動作内容を表すタイミングチャート

【図１３】比較例に係る第３比較動作例における各部の動作内容を表すタイミングチャート

【図１４】第１実施形態に係る第１０動作例における各部の動作内容を表すタイミングチャート

【図１５】比較例に係る第４比較動作例における各部の動作内容を表すタイミングチャート

【図１６】比較例に係る第５比較動作例における各部の動作内容を表すタイミングチャート

【図１７】第１実施形態に係る第１１動作例における各部の動作内容を表すタイミングチャート

【図１８】第１実施形態に係る全体マージン時間の割り振りに関する具体例を示す図

【図１９】第１実施形態に係る禁止要求を受信したときに実行される各処理の具体的な内容の一例を模式的に示す図

【図２０】第１実施形態に係る禁止期間に実行される各処理の具体的な内容の一例を模式的に示す図

【図２１】変形例に係る動作時間が終了したときに実行される各処理の具体的な内容の一例を模式的に示す図

【図２２】第１実施形態に係る許可要求を受信したときに実行される各処理の具体的な内容の一例を模式的に示す図

【図２３】第２実施形態に係る第１２動作例における各部の動作内容を表すタイミングチャート

【図２４】第２実施形態に係る第１３動作例における各部の動作内容を表すタイミングチャート

【図２５】第２実施形態に係る第１４動作例における各部の動作内容を表すタイミングチ

ャート
【図２６】第３実施形態に係る第１５動作例における各部の動作内容を表すタイミングチャート
【発明を実施するための形態】
【００１３】
以下、本発明の複数の実施形態について図面を参照して説明する。なお、各実施形態において実質的に同一の構成には同一の符号を付して説明を省略する。
（第１実施形態）
以下、第１実施形態について図１～図２２を参照して説明する。
【００１４】
図１に示すように、本実施形態の統合ＥＣＵ１は、例えば自動車などの車両に搭載されるものであり、従来単独で動作していた複数のＥＣＵの機能がハイパーバイザー２を介して１つのマイコン３のチップ上に搭載されたものである。複数のＥＣＵの具体例としては、例えばエンジンＥＣＵ、エアコンＥＣＵ、セントラルゲートウェイＥＣＵおよびボデーＥＣＵなどを挙げることができる。この場合、複数のＥＣＵの機能は、仮想マシンという単位で搭載される。なお、本明細書では、ハイパーバイザーのことをＨＶと省略することがあるとともに、仮想マシンのことをＶＭと省略することがある。
【００１５】
統合ＥＣＵ１は、ＥＣＵ－ＡおよびＥＣＵ－Ｂという２つのＥＣＵに相当する機能を備えている。統合ＥＣＵ１は、３つ以上のＥＣＵに相当する機能を備えていてもよい。ＥＣＵ４は、統合ＥＣＵ１として統合されることなく、従来のＥＣＵと同様に独立して設けられている。統合ＥＣＵ１およびＥＣＵ４は、バス通信線５を介して接続されており、これにより互いの間で通信を行うことが可能となっている。
【００１６】
ＥＣＵ４は、マイコン６を備えている。マイコン６は、そのハードウェアとして図示しないＣＰＵ、各種の記憶装置、各種のペリフェラルなどを備えている。各種のペリフェラルには、通信を行うための通信ハードウェア７などが含まれる。なお、本明細書では、ハードウェアのことをＨＷと省略することがある。ＥＣＵ４は、その主たる機能を実現するためのＥＣＵ－０アプリケーションＡ０を備えている。なお、本明細書ではアプリケーションのことをアプリと省略することがある。また、以下の説明および図面では、ＥＣＵ－０アプリＡ０のことをアプリＡ０と省略することがある。
【００１７】
ＥＣＵ４は、通信ドライバ８を備えている。通信ドライバ８は通信ＨＷ７を制御して統合ＥＣＵ１を含む他のＥＣＵとの間でバス通信線５を介したデータ通信を行うものである。アプリＡ０および通信ドライバ８は、いずれもマイコン６が備えるＣＰＵが非遷移的実体的記憶媒体に格納されているコンピュータプログラムを実行してコンピュータプログラムに対応する処理を実行することにより実現されている、つまりソフトウェアにより実現されている。
【００１８】
統合ＥＣＵ１は、２つのＶＭ１０およびＶＭ１１を備えている。この場合、ＥＣＵ－Ａの機能はＶＭ１０により実現され、ＥＣＵ－Ｂの機能はＶＭ１１により実現される。ＶＭ１０は、ＥＣＵ－Ａの主たる機能を実現するためのＥＣＵ－ＡアプリケーションＡ１を備えている。ＶＭ１１は、ＥＣＵ－Ｂの主たる機能を実現するためのＥＣＵ－ＢアプリＡ２を備えている。なお、以下の説明および図面では、ＥＣＵ－ＡアプリＡ１およびＥＣＵ－ＢアプリＡ２のことを、それぞれアプリＡ１およびアプリＡ２と省略することがある。
【００１９】
ＨＶ２は、マイコン３上でＶＭ１０およびＶＭ１１を動作させるためのものである。マイコン３は、コンピュータの一例であり、そのハードウェアとして図示しないＣＰＵ、各種の記憶装置、各種のペリフェラルなどを備えている。各種のペリフェラルには、通信を行うための通信ＨＷ１２などが含まれる。各種の記憶装置には、レジスタ１３が含まれる

。レジスタ１３は、プロテクション対象のレジスタ、つまり書き込みに関する保護設定を行うことができるレジスタである。ＶＭ１０は、通信ドライバ１４を備えている。ＶＭ１１は、通信ドライバ１５を備えている。通信ドライバ１４、１５は、通信ＨＷ１２を制御してＥＣＵ４を含む他のＥＣＵとの間でバス通信線５を介したデータ通信を行うものである。

【００２０】

この場合、ＨＶ２は、複数のＶＭ１０およびＶＭ１１のそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置として機能する。つまり、統合ＥＣＵ１では、複数のＶＭ１０およびＶＭ１１に対して固定の動作時間を割り当てる時分割スケジューリングでの制御が行われる。また、この場合、統合ＥＣＵ１は、マイコン３と、マイコン３上で動作する複数のＶＭ１０およびＶＭ１１と、動作制御装置として機能するＨＶ２と、を備えた電子制御装置の一例である。なお、本明細書では、複数のＶＭ１０およびＶＭ１１のうち動作中のものを動作マシンと称することがある。

【００２１】

ＨＶ２、ＶＭ１０およびＶＭ１１は、いずれもマイコン３が備えるＣＰＵが非遷移的実体的記憶媒体に格納されているコンピュータプログラムを実行してコンピュータプログラムに対応する処理を実行することにより実現されている、つまりソフトウェアにより実現されている。なお、上記したコンピュータプログラムのうちＨＶ２が実行するプログラムは、動作制御プログラムに相当する。

【００２２】

ＨＶ２は、第１処理部２１および第２処理部２２といった２つの機能ブロックを備えている。第１処理部２１は、動作マシンを切り替える切り替え処理を実行することができる。第１処理部２１により実行される各処理は、第１処理に相当する。第２処理部２２は、切り替え処理の実行を禁止する禁止処理および切り替え処理の実行を許可する許可処理を実行することができる。第２処理部２２により実行される各処理は、第２処理に相当する。

【００２３】

この場合、動作マシンは、連続して実行しなければならない処理、つまり中断不可能な処理またはアトミックな処理である特定処理を開始する際に禁止要求を送信するとともに、特定処理を完了した際に許可要求を送信するようになっている。本明細書において、「連続して実行しなければならない処理」とは、連続して実行しなかった場合に処理が成立せずに失敗となるような処理だけでなく、連続して実行しなかった場合にユーザが所望するレベルの処理結果が得られないような処理、つまり連続して実行することが望ましいような処理をも含む。

【００２４】

第２処理部２２は、禁止要求を受信したとき、その時点から動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行する。第２処理部２２は、判断処理の結果、残り時間が設定時間以上の時間である場合には禁止処理を実行するとともに、残り時間が設定時間未満の時間である場合には禁止処理を実行しないようになっている。第２処理部２２は、許可要求を受信したとき、許可処理を実行するようになっている。動作マシンは、禁止処理が実行されている期間である禁止期間中に特定処理を実行するようになっている。

【００２５】

第１処理部２１は、禁止期間中、動作時間を所定のマージン時間だけ延長することができるようになっている。第１処理部２１により上記延長が行われる場合、第２処理部２２は、禁止要求を受信した時点から延長した動作時間が経過する時点までの時間を残り時間として判断処理を実行することになる。本実施形態では、動作周期毎にマージン時間として使用することができる使用可能時間が設定されている。第１処理部２１は、使用可能時間から必要とするマージン時間を消費する形で動作時間の延長を行うようになっている。

すなわち、マージン時間は、使用可能時間から割り当てられて使用されるようになっている。

【００２６】

第１処理部２１は、動作周期において最後に動作する動作マシンの動作が開始される際に使用可能時間に余りがある場合、その余りの少なくとも一部を最後に動作する動作マシンの動作時間に割り当てることができる。第１処理部２１は、禁止期間において動作時間が経過した時点で特定処理が完了していない場合、異常が発生したと判断して切り替え処理および異常を外部に通知する通知処理の一方または双方を実行することができる。第１処理部２１は、禁止期間において動作時間が経過した時点で特定処理が完了していない場合、異常が発生したと判断して次回以降の動作周期において許可要求を受信すると異常を外部に通知する通知処理を実行することができる。

【００２７】

第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、禁止処理が実行されるまで動作マシンに禁止要求の送信を繰り返し実行させることができる。第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、切り替え処理が実行されるまでの期間、動作マシンを待機状態とする、または、動作マシンを特定処理とは異なる別の処理を実行可能な状態とすることができる。第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、動作マシンに割り当てられた動作時間が経過する前に切り替え処理を実行することができる。

【００２８】

設定時間は、以下の第１設定手法または第２設定手法により設定することができる。第１設定手法では、設定時間は、複数の仮想マシンのそれぞれ毎に予め設定される。この場合、設定時間は、その設定対象となる仮想マシンが実行する可能性がある特定処理に要する時間に基づいて設定することができる。設定時間は、仮想マシンが実行する可能性がある特定処理が１つである場合、その特定処理に要する時間に対応する時間に設定することができる。なお、特定処理に要する時間に対応する時間とは、特定処理に要する時間と同じ時間だけでなく、その時間に対して所定のマージンを持たせた時間をも含む。

【００２９】

また、設定時間は、仮想マシンが実行する可能性がある特定処理が複数ある場合、複数の特定処理のそれぞれに要する時間のうち最も長い時間に対応する時間に設定することができる。なお、複数の特定処理のそれぞれに要する時間のうち最も長い時間とは、複数の特定処理のそれぞれに要する時間のうち最も長い時間と同じ時間だけでなく、その時間に対して所定のマージンを持たせた時間をも含む。

【００３０】

第２手法では、第２処理部２２は、禁止要求を受信したとき、禁止要求を送信した動作マシンが開始する特定処理に要する時間に基づいて設定時間を設定する。設定時間は、禁止要求を送信した動作マシンが開始する特定処理に要する時間に対応する時間に設定することができる。なお、特定処理に要する時間に対応する時間とは、特定処理に要する時間と同じ時間だけでなく、その時間に対して所定のマージンを持たせた時間をも含む。

【００３１】

次に、上記構成の作用について、図２～図２１を参照して説明する。

以下の説明では、各用語について下記のように別の言い方をする場合がある。

特定処理　→　タスク

切り替え処理が開始されること　→　ＶＭ切り替え

動作周期　→　ＨＶ周期

使用可能時間　→　全体マージン時間

【００３２】

この場合、ＨＶ周期が１０００μ秒になっており、全体マージン時間が５０μ秒になっているものとする。図２～図１７などでは、動作マシンがＶＭ１０である期間を「ＶＭ１

０」と表し、動作マシンがＶＭ１１である期間を「ＶＭ１１」と表し、第１処理部２１が切り替え処理を実行している期間を「ＨＶ」と表し、動作マシンがタスクを実行している期間を「Task」と表し、マイコン３が消費電力を低減するモードに遷移している期間を「Halt」と表し、禁止処理が実行されている期間を「disable」と表している。

【００３３】

以下の説明では、本実施形態との比較のため、本実施形態による動作例の説明に加え、従来技術に相当する比較例による動作例である比較動作例の説明も行うこととする。なお、比較例は、本実施形態に対して第２処理部２２を省くとともに第２処理部２２により実行される各処理に関連する処理も省いたものとなっている。

【００３４】

［１－１］第１比較動作例

図２に示す第１比較動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともに、そのタスクを動作時間内に中断することなく完了することができた場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点においてタスクの実行を開始する。この場合、ＶＭ１０により実行されるタスクは、動作時間が終了する時点よりも前の時点において完了となっている。その後、ＶＭ１０に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。

【００３５】

［１－２］第２比較動作例

図３に示す第２比較動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともに、そのタスクを動作時間内に完了することができなかった場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点においてタスクの実行を開始する。この場合、ＶＭ１０により実行されるタスクは、ＶＭ１０に割り当てられた動作時間が経過した時点でも完了していないが、この時点において第１処理部２１により切り替え処理が行われることから、タスクが中断される。

【００３６】

このように中断されたタスクは、次のＨＶ周期において再開される。すなわち、次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点からタスクの実行を再開する。この場合、ＶＭ１０により実行されるタスクは、ＶＭ１０が動作マシンへと切り替えられた時点から所定時間が経過した時点において完了となっている。このように、比較例では、タスクの実行中にＶＭ切り替えが発生した場合、タスクが中断されてしまい、期待する機能が動作しないことが考えられる。これに対し、本実施形態では、タスクの実行中にＶＭ切り替えが発生しない機能を導入することにより、このような課題の解決を図るようになっている。

【００３７】

［２－１］第１動作例

図４に示す第１動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともにそのタスクを中断することなく完了することができた場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。

【００３８】

この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、タスクは、ＶＭ１０に割り当てられた当初の動作時間が経過した時点では完了しない。そのため、第１処理部２１は、ＶＭ１０により実行されているタスクが完了するまで動作時間を延長する。この場

合、全体マージン時間から２０μ秒だけ消費して動作時間の延長が行われる。
【００３９】
このような第１動作例によれば、ＶＭ１０は、その動作時間が２０μ秒だけ延長されることにより、中断不可能な処理であるタスクを連続して完了させることができる。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。これにより、第１処理部２１は、切り替え処理を実行する。このように、動作時間が延長された場合であっても、タスク完了後に直ちにＶＭ切り替えが行われることによりリアルタイム性を確保することができる。
【００４０】
［２－２］第２動作例
図５に示す第２動作例は、ＶＭ１０、ＶＭ１１が動作時間の途中においてタスクの実行を開始するとともにそのタスクを中断することなく完了することができた場合を想定したものである。この場合、ＶＭ１０の動作時間における動作は、第１動作例と同様である。そして、この場合、ＶＭ１１は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。
【００４１】
この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である３０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１１は、タスクの実行を開始する。この場合、タスクは、ＶＭ１１に割り当てられた当初の動作時間が経過した時点では完了しない。
【００４２】
そのため、第１処理部２１は、ＶＭ１１により実行されているタスクが完了するまで動作時間を延長する。この場合、全体マージン時間から１０μ秒だけ消費して動作時間の延長が行われる。このような第２動作例によれば、ＶＭ１１は、その動作時間が１０μ秒だけ延長されることにより、中断不可能な処理であるタスクを連続して完了させることができる。ＶＭ１１は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。これにより、第１処理部２１は、切り替え処理を実行する。
【００４３】
このように、動作時間が延長された場合であっても、タスク完了後に直ちにＶＭ切り替えが行われることによりリアルタイム性を確保することができる。第２動作例から分かるように、本実施形態の構成によれば、全体マージン時間に未だ使用されていない時間がある限り、複数のＶＭから要求された分だけマージン時間を割り当てることができる。本実施形態のように、ＨＶ周期全体でマージン時間を設定することで適応的にＶＭ毎に要求するマージン時間を分配することができる。
【００４４】
［２－３］第３動作例
図６に示す第３動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともにそのタスクが完了しなかった場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。
【００４５】
この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、タスクは、ＶＭ１０に割り当てられた当初の動作時間が経過した時点では完了しない。そのため、第１処理部２

１は、ＶＭ１０により実行されているタスクが完了するまで動作時間を延長する。
【００４６】
ただし、この場合、異常、故障などの何らかの理由により、全体マージン時間の全てである５０μ秒を消費して動作時間の延長が行われても、タスクが完了しなかったものとする。そうすると、第１処理部２１は、異常が発生したと判断し、通知処理を実行する。通知処理では、ＶＭ切り替えが禁止された状態である禁止期間が固着したことを検知した旨を表す固着エラーが発行される。また、このとき、第１処理部２１は、このようにＶＭ切り替えが禁止された状態のまま、切り替え処理を行う。
【００４７】
そして、この場合、ＶＭ１１は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。この場合、ＶＭ１０により全体マージン時間の全てが使用されたことに起因して、残り時間が設定時間より短いものであるとする。そのため、ＨＶ２が禁止処理を実行せず、その結果、ＶＭ１１は、このＨＶ周期においてタスクの実行を開始することができない。
【００４８】
このように、動作マシンであるＶＭ１１が禁止要求を送信した後に禁止処理が実行されなかった場合、第１処理部２１は、切り替え処理が実行されるまでの期間、動作マシンであるＶＭ１１を待機状態とする。なお、この場合、第１処理部２１は、切り替え処理が実行されるまでの期間、動作マシンであるＶＭ１１をタスクとは異なる別の処理を実行可能な状態とすることもできる。その後、ＶＭ１１に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。
【００４９】
次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点からタスクの実行を再開する。この場合、ＶＭ１０により実行されるタスクは、ＶＭ１０が動作マシンへと切り替えられた時点から所定時間が経過した時点において完了となっている。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。また、このとき、ＨＶ２は、通知処理を行い、これにより固着エラーが発行される。このようにすれば、統合ＥＣＵ１において、ＶＭの再起動や処理の中断などの判断を行うことができる。
【００５０】
その後、ＶＭ１０に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。ＶＭ１１は、自身が動作マシンへと切り替えられた時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１１は、タスクの実行を開始する。
【００５１】
この場合、ＶＭ１１により実行されるタスクは、ＶＭ１１が動作マシンへと切り替えられた時点から所定時間が経過した時点において完了となっている。ＶＭ１１は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。その後、ＶＭ１１に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。第３動作例から分かるように、本実施形態の構成によれば、優先度が高いＶＭをＨＶ周期の先頭から順に動作させるようにすることで、優先度が高いＶＭに対して優先的にマージン時間を割り当てることができる。
【００５２】
［２－４］第４動作例
図７に示す第４動作例は、第３動作例に対して次の点が異なっている。すなわち、第４

動作例では、動作マシンであるＶＭ１１が禁止要求を送信した後に禁止処理が実行されなかった場合、第１処理部２１は、禁止処理が実行されるまで動作マシンであるＶＭ１１に禁止要求の送信を繰り返し実行させるようになっている。なお、図７では、繰り返し送信される禁止要求について、単なる矢印により表している。

【００５３】

［２－５］第５動作例

図８に示す第５動作例は、第３動作例に対してＶＭ１１に関連する動作が異なっている。すなわち、第５動作例では、ＶＭ１１は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。この場合、ＶＭ１０により全体マージン時間の全てが使用されているためにＶＭ１１の動作時間の延長はできないものの、その時点から延長無しの動作時間が経過する時点までの残り時間が設定時間より短いものであるとする。

【００５４】

そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１１は、タスクの実行を開始する。この場合、ＶＭ１１により実行されるタスクは、禁止処理が開始された時点から所定時間が経過した時点において完了となっている。ＶＭ１１は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。その後、ＶＭ１１に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。

【００５５】

第５動作例から分かるように、本実施形態の構成によれば、全体マージン時間の全てが使用されており、マージン時間がない場合においても、タスクが完了するまでの時間を確保できる場合には禁止処理が行われるようになっており、その結果、当該動作時間中にタスクを連続して完了させることができる。

【００５６】

［２－６］第６動作例

図９に示す第６動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともに、動作時間を延長することなくそのタスクを中断することなく完了することができた場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。

【００５７】

この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、ＶＭ１０により実行されるタスクは、禁止処理が開始された時点から所定時間が経過した時点において完了となっている。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。その後、ＶＭ１０に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。

【００５８】

［２－７］第７動作例

図１０に示す第７動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始しようとしたものの、そのＨＶ周期における動作時間でのタスク実行ができずに次のＨＶ周期における動作時間でのタスク実行となる場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信

すると、判断処理を実行する。

【００５９】

この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも短いものであるとする。そのため、ＨＶ２が禁止処理を実行せず、その結果、ＶＭ１０は、このＨＶ周期においてタスクの実行を開始することができない。そして、次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点でＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。

【００６０】

そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、ＶＭ１０により実行されるタスクは、ＶＭ１０が動作マシンへと切り替えられた時点から所定時間が経過した時点において完了となっている。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。その後、ＶＭ１０に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。

【００６１】

第７動作例から分かるように、本実施形態の構成によれば、動作マシンからＨＶへ禁止要求禁止が送信されたとき、ＨＶ２は残り時間が設定時間未満の時間であると判断した場合、禁止処理を実行しないため、そのＨＶ周期における動作時間において完了する見込みのないタスクを次のＨＶ周期における動作時間において実施することができる。このように、本実施形態の構成によれば、事前にＶＭ切り替えまでの時間が分かるため、むやみに動作時間を延長したりすることなく、また他のＶＭへ影響を及ぼしたりすることなく、リアルタイム性を確保することができる。

【００６２】

［２－８］第８動作例

図１１に示す第８動作例は、ＨＶ周期において最後に動作する動作マシンの動作が開始される際に全体マージン時間に余りがある場合を想定したものである。この場合、ＶＭ１０およびＶＭ１１のいずれもタスクを実行しなかったことから、ＶＭ１１の動作が開始される際に全体マージン時間が消費されておらず５０μ秒そのまま残っているものとする。第１処理部２１は、このような全体マージン時間の余りの少なくとも一部を最後に動作する動作マシンであるＶＭ１１の動作時間に割り当てるようになっている。このようにすれば、マイコン３のリソースを有効活用し、何の処理も動作しない時間を無くすことができる。

【００６３】

［２－９］第９動作例

図１２に示す第９動作例は、第７動作例に対して次の点が異なっている。なお、図１２の上段には、各動作例の比較のため、第７動作例を説明する際に使用した図１０と同様の図も記載されている。すなわち、図１２の下段に示すように、第９動作例では、第１処理部２１は、動作マシンであるＶＭ１０が禁止要求を送信した後に禁止処理が実行されなかった場合、動作マシンであるＶＭ１０に割り当てられた動作時間が経過する前に切り替え処理を実行するようになっている。

【００６４】

このような第９動作例によれば、動作マシンであるＶＭ１０が禁止要求を送信した後に禁止処理が実行されなかった場合、ＶＭ１０に割り当てられた動作時間の残りの時間が、他のＶＭ１１に分け与えられる。このようにすれば、ＶＭ１０において他に動作可能な処理が存在しない場合にＶＭ１０で無駄な時間を消費することなく、その分の時間を他のＶＭ１１の動作時間として割り当てることが可能となり、その結果、マイコン３のリソース

を有効活用することができる。

【００６５】

［１－３］第３比較動作例

図１３に示す第３比較動作例は、第２比較動作例に対し、タスクの内容が具体化されている点が異なっている。この場合、統合ＥＣＵ１およびＥＣＵ４の間で行われる通信は、複数に分割されており、全ての通信データをＶＭ１０からＥＣＵ４へと例えば１００μ秒である所定時間以内に送信または受信する必要があるものとする。ＶＭ１０は、タスクとして、上記した通信を行うようになっている。ＶＭ１０が行う通信は、２回に分割されているものとする。

【００６６】

この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点においてＥＣＵ４に対する１回目の通信データの送信または受信を実行する。その後、ＶＭ１０がＥＣＵ４に対する２回目の通信データの送信または受信を実行するよりも前の時点においてＶＭ１０に割り当てられた動作時間が終了することから第１処理部２１により切り替え処理が行われる。つまり、この時点で、通信の処理が中断される。そして、次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点においてＥＣＵ４に対する２回目の通信データの送信または受信を実行する。

【００６７】

このように、第３比較動作例では、１回目の通信データの送信または受信の後にＶＭ切り替えが発生し、次のＨＶ周期で２回目の通信データの送信または受信が行われているため、１００μ秒以内に全ての通信データが送信または受信されていない。ただし、この場合、ＶＭ１０としては、通信の処理が正常に完了しているため、通信データの再送信または再受信を行うことがなく、統合ＥＣＵ１およびＥＣＵ４の間の通信が失敗したままになるおそれがある。

【００６８】

［２－１０］第１０動作例

図１４に示す第１０動作例は、第１動作例に対し、タスクの内容が具体化されている点が異なっている。タスクの具体的な内容は、第３比較動作例と同様である。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。

【００６９】

この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、ＥＣＵ４に対する１回目の通信データの送信または受信を実行する。この場合も、第３比較動作例と同様、ＶＭ１０がＥＣＵ４に対する２回目の通信データの送信または受信を実行するよりも前に時点においてＶＭ１０に割り当てられた当初の動作時間が終了する。ただし、この場合、第１処理部２１は、ＶＭ１０により実行されているタスクが完了するまで動作時間を延長する。

【００７０】

そのため、ＶＭ１０は、当該ＨＶ周期において、ＥＣＵ４に対する１回目の通信データの送信または受信を実行した後、それと連続してＥＣＵ４に対する２回目の通信データの送信または受信を実行することができる。このように、第１０動作例によれば、１００μ秒以内に全ての通信データを送信または受信することができる。つまり、第１０動作例によれば、通信の処理が、ＶＭ切り替えにより中断されることなく、連続して完了させることができる。

【００７１】

［１－４］第４比較動作例

図１５に示す第４比較動作例は、タスクの具体的な内容として、レジスタ１３に対する

書き込み制御を想定したものである。レジスタ１３に対する書き込み制御には、レジスタ１３の保護設定を解除する「保護解除」、レジスタ１３に対して書き込みを行う「書き込み」およびレジスタ１３の保護設定を再度行う「保護再設定」といった３つの処理が含まれる。

【００７２】

この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において書き込み制御を開始する。すなわち、ＶＭ１０は、まず保護解除の処理を行い、その後、書き込みの処理を開始する。その後、ＶＭ１０が書き込みの処理を完了するよりも前の時点においてＶＭ１０に割り当てられた動作時間が終了することから第１処理部２１により切り替え処理が行われる。つまり、この場合、書き込みの処理中にＶＭ切り替えが発生し、それにより書き込み制御が中断されている。

【００７３】

このとき、レジスタ１３の保護設定が解除されたままとなっている。そのため、この後に動作マシンへと切り替えられたＶＭ１１が、レジスタ１３に対する書き込みを行う可能性があり、そうすると、他のＶＭ１１によりレジスタ１３の内容が書き換えられてしまう。その後、次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点において書き込み処理を再開することになるが、前のＨＶ周期においてレジスタ１３の内容がＶＭ１１に書き換えられていることから、レジスタ１３の設定に誤りが生じるおそれがある。

【００７４】

［１－５］第５比較動作例

図１６に示す第５比較動作例は、第４比較動作例に対し、ＶＭ切り替えが発生するタイミングが異なっている。すなわち、第５比較動作例では、保護解除の処理の実行後であり且つ書き込みの処理の開始前の時点においてＶＭ１０に割り当てられた動作時間が終了することから第１処理部２１により切り替え処理が行われる。つまり、この場合、保護解除の処理の実行後にＶＭ切り替えが発生し、それにより書き込み制御が中断されている。

【００７５】

そして、この後に動作マシンへと切り替えられたＶＭ１１がレジスタ１３に対する書き込み制御を行う可能性があり、そうすると、他のＶＭ１１によりレジスタ１３に対して保護再設定が行われることになる。その後、次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点において書き込み処理を開始しようとするが、レジスタ１３が保護設定されているため、書き込みを行うことができなくなり、その結果、ＶＭ１０によるレジスタ１３の書き込み制御が正常に完了できなくなる。

【００７６】

［２－１１］第１１動作例

図１７に示す第１１動作例は、タスクの具体的な内容として、第４比較動作例および第５比較動作例と同様、レジスタ１３に対する書き込み制御を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。この場合、残り時間に対して全体マージン時間のうち未だ使用されていない時間である５０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。

【００７７】

禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、書き込み制御を開始する。すなわち、ＶＭ１０は、まず保護解除の処理を行い、その後、書き込みの処理を開始する。その後、ＶＭ１０が書き込みの処理を完了するよりも前の時点においてＶＭ１０に割り当てられた当初の動作時間が終了する。ただし、この場合、第１処理部２１は、ＶＭ１０により実行されているタスクが完了するまで動作時間を延長する。

【００７８】

そのため、ＶＭ１０は、当該ＨＶ周期において、書き込み制御における全ての処理を連続して実行することができる。このように、本実施形態の構成によれば、第４比較動作例および第５比較動作例において生じる問題が発生することなく、書き込み制御における一連の処理を正常に完了することができる。なお、第１１動作例でも、判断処理において、残り時間に対してマージン時間を加えた時間が設定時間よりも短いものであるとの結果が得られた場合には、第７動作例と同様、次のＨＶ周期における動作時間で書き込み制御が実行されることになる。

【００７９】

［３］全体マージン時間の割り振り

図１８に示すように、ＨＶ周期毎に設定された全体マージン時間がどのように各ＶＭ１０、ＶＭ１１に割り振られて消費されるのかは、図１８に示すように、様々なケースが考えられる。ケース１では、ＶＭ１０においてマージン時間として３０μ秒が消費されており、残りの２０μ秒が消費されずに余りとなっている。ケース２では、ＶＭ１０においてマージン時間として３０μ秒が消費されるとともにＶＭ１１においてマージン時間として２０μ秒が消費されている。つまり、ケース２は、ＶＭ１０とＶＭ１１とで全体マージン時間を分け合うとともに、全体マージン時間に余りが生じていないケースである。

【００８０】

ケース３では、ＶＭ１０においてマージン時間として２０μ秒が消費されるとともにＶＭ１１においてマージン時間として２５μ秒が消費されている。つまり、ケース２は、ＶＭ１０とＶＭ１１とで全体マージン時間を分け合うとともに、全体マージン時間に５μ秒の余りが生じているケースである。ケース４では、ＶＭ１０においてマージン時間として４０μ秒が消費されており、残りの１０μ秒が消費されずに余りとなっている。

【００８１】

ケース５では、ＶＭ１０においてマージン時間として５０μ秒が消費されており、全体マージン時間に余りが生じていない。ケース６では、ＶＭ１１においてマージン時間として５０μ秒が消費されており、全体マージン時間に余りが生じていない。ケース７では、ＶＭ１０、ＶＭ１１のいずれにおいてもマージン時間が消費されておらず、全体マージン時間の全てである５０μ秒の余りが生じている。このような全体マージン時間の割り振りに関するケースの数は、統合ＥＣＵ１に搭載されるＶＭの数に応じてさらに増加することになる。

【００８２】

［４－１］禁止要求を受信したときに実行される各処理の具体的な内容

ＨＶ２が禁止要求を受信したときに実行する各処理は、具体的には、図１９に示すような内容とすることができる。第２処理部２２は、禁止要求を受信するたびに、図１９に示すような内容の処理を実行するようになっている。ステップＳ１０１では、禁止要求を受信した時点から動作時間が経過する時点までの時間に対して使用可能なマージン時間を加えた時間Ｔ１が設定時間である時間Ｔ２以上であるか否かが判断される。

【００８３】

ここで、時間Ｔ１が時間Ｔ２以上である場合、ステップＳ１０１で「ＹＥＳ」となり、ステップＳ１０２に進む。ステップＳ１０２では、禁止処理が実行される。ステップＳ１０２の実行後、本処理が終了となる。一方、時間Ｔ１が時間Ｔ２未満である場合、ステップＳ１０１で「ＮＯ」となり、ステップＳ１０２の禁止処理が実行されることなく、本処理が終了となる。このような処理によれば、事前にＶＭ切り替えまでの時間が分かるため、むやみに動作時間を延長したりすることなく、また他のＶＭへ影響を及ぼしたりすることなく、リアルタイム性を確保することができる。

【００８４】

［４－２］禁止期間に実行される各処理の具体的な内容

禁止期間にＨＶ２の第１処理部２１により実行される各処理は、具体的には、図２０に示すような内容とすることができる。第１処理部２１は、禁止期間中、所定の周期毎に、図２０に示すような内容の処理を実行するようになっている。ステップＳ２０１では、禁

止期間中に消費されたマージン時間である時間Ｔ３が設定されたマージン時間である時間Ｔ４以上であるか否かが判断される。

【００８５】

ここで、時間Ｔ３が時間Ｔ４以上である場合、ステップＳ２０１で「ＹＥＳ」となり、ステップＳ２０２に進む。ステップＳ２０２では、固着エラーが発行されて通知される。ステップＳ２０２は、通知処理に対応している。ステップＳ２０２の実行後はステップＳ２０３に進み、固着エラーフラグが設定される。ステップＳ２０３の実行後はステップＳ２０４に進み、切り替え処理が行われる。ステップＳ２０４の実行後、本処理が終了となる。一方、時間Ｔ３が時間Ｔ４未満である場合、ステップＳ２０１で「ＮＯ」となり、ステップＳ２０２～Ｓ２０４の処理、つまり通知処理および切り替え処理などの処理が実行されることなく、本処理が終了となる。

【００８６】

このような処理によれば、消費されたマージン時間が設定されたマージン時間と同じになった場合に固着エラーを発行するとともに固着エラーフラグを設定し、その後にＶＭ切り替えを行うようになっているため、ＨＶ２全体でのリアルタイム性が保証される。また、上記処理によれば、固着エラーを発行することでＶＭに対して処理を再度実行させることや、ＶＭの再起動を行う判断材料とすることができる。

【００８７】

なお、第１処理部２１は、図２０に示した本実施形態に係る各処理に代えて、図２１に示すような内容の変形例に係る各処理を行うことができる。図２１に示す変形例による各処理は、ＶＭに割り当てられた当初の動作時間に設定されたマージン時間を加えた動作時間、つまりマージン込みの動作時間が終了したときに実行されるものであり、図２０に示した本実施形態による各処理に対し、ステップＳ２０１に代えてステップＳ２１１が設けられている点が異なっている。ステップＳ２１１では、切り替え処理の実行が禁止された禁止状態であるか否かが判断される。

【００８８】

ここで、禁止状態である場合、ステップＳ２１１で「ＹＥＳ」となり、ステップＳ２０２に進む。一方、禁止状態ではない場合、ステップＳ２１１で「ＮＯ」となり、ステップＳ２０４に進み、切り替え処理が行われた後に本処理が終了となる。このような変形例によれば、設定されたマージン時間を加えた動作時間が終了したときに切り替え処理の実行が禁止された禁止状態であれば、固着エラーフラグが設定される、つまりＶＭ固着と判断される。

【００８９】

［４－３］許可要求を受信したときに実行される各処理の具体的な内容

ＨＶ２が許可要求を受信したときに実行する各処理は、具体的には、図２２に示すような内容とすることができる。第２処理部２２は、許可要求を受信するたびに、図２２に示すような内容の処理を実行するようになっている。ステップＳ３０１では、固着エラーフラグが設定されているか、言い換えると固着エラーフラグが立っているか、が判断される。なお、図２２では、固着エラーフラグが立っていることをエラーフラグ「オン」と称している。ここで、固着エラーフラグが立っている場合、ステップＳ３０１で「ＹＥＳ」となり、ステップＳ３０２に進む。ステップＳ３０２では、固着エラーが発行されて通知される。

【００９０】

ステップＳ３０２は、通知処理に対応している。ステップＳ３０２の実行後はステップＳ３０３に進み、許可処理が実行される。ステップＳ３０３の実行後、本処理が終了となる。一方、固着エラーフラグが立っていない場合、ステップＳ３０１で「ＮＯ」となり、ステップＳ３０２の処理、つまり通知処理が実行されることなく、ステップＳ３０３に進み、許可処理が実行される。このような処理によれば、許可処理の実行時にも固着エラーを発行することにより、禁止期間の固着が生じたうえで特定処理の実行が終了したことを明確にすることができる。

【００９１】
以上説明した本実施形態によれば、次のような効果が得られる。
本実施形態の統合ＥＣＵ１が備えるＨＶ２は、複数のＶＭ１０、ＶＭ１１のそれぞれをＨＶ周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行うものであり、動作マシンを切り替える切り替え処理を実行することができる第１処理部２１と、切り替え処理の実行を禁止する禁止処理および切り替え処理の実行を許可する許可処理を実行することができる第２処理部２２と、を備える。ＶＭ１０、ＶＭ１１は、特定処理を開始する際に禁止要求を送信するとともに、特定処理を完了した際に許可要求を送信するようになっている。
【００９２】
第２処理部２２は、禁止要求を受信したとき、その時点から動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、その結果、残り時間が設定時間以上の時間である場合には禁止処理を実行するとともに残り時間が設定時間未満の時間である場合には禁止処理を実行しないようになっている。また、第２処理部２２は、許可要求を受信したとき、許可処理を実行するようになっている。動作マシンは、禁止処理が実行されている期間である禁止期間中に特定処理を実行する。
【００９３】
上記構成によれば、動作マシンが特定処理を実行しているときに動作マシンを切り替える切り替え処理が発生することが防止される。このようにすれば、特定処理が完了するまで一貫した動作を保証することができる。また、上記構成によれば、第２処理部２２が判断処理を実行することにより、残り時間が設定時間未満の時間である場合、言い換えると、これから開始しようとする特定処理を動作時間が経過するまでに完了することができる可能性が極めて低い場合、禁止処理が実行されず、それに伴い、特定処理も実行されない。このようにすれば、そのＨＶ周期で完了する見込みのない特定処理を、次のＨＶ周期にて実行することができる。このように、本実施形態の構成によれば、連続して実行しなければならない処理である特定処理が切り替え処理により中断されることを防止することができるという優れた効果が得られる。
【００９４】
本実施形態では、切り替え処理の実行が禁止された禁止期間では、元々設定されていた動作時間をマージン時間だけ延長することが可能となっており、そのように延長された動作時間が経過するまで動作マシンによる特定処理の実行が継続される。このようにすれば、より確実に、特定処理を中断することなく、連続して完了することができる。また、本実施形態では、延長された動作時間が経過するまでに特定処理が完了しない場合には、通知処理および切り替え処理が行われる。
【００９５】
このようにすれば、設定されたマージン時間を超えるような動作時間の延長が行われることがなく、特定のＶＭだけがむやみに長い時間動作するような事態の発生が防止され、他のＶＭの動作時間が減少するなどの悪影響が生じることがなくなりリアルタイム性を確保することができる。また、本実施形態によれば、固着エラーを通知する通知処理が行われることにより、特定処理が完了しなかった動作マシンに対して再起動や特定処理の再実行などを行うことができる。
【００９６】
本実施形態では、ＨＶ周期毎に全体マージン時間が設定されており、第１処理部２１は、全体マージン時間から必要とするマージン時間を消費する形で動作時間の延長を行うようになっている。このようにすれば、ＨＶ２全体でマージン時間を設定することができるため、その設定を簡易なものとすることができる。また、このようにすれば、ＨＶ周期の中で適応的に各ＶＭが要求するマージン時間を分配することができる。さらに、このようにすれば、複数のＶＭのうち優先度が高いＶＭをＨＶ周期の先頭から順に動作させることで、相対的に優先度の高いＶＭに対して優先的にマージン時間を与えることができる。

【００９７】
第１処理部２１は、ＨＶ周期において最後に動作する動作マシンの動作が開始される際に全体マージン時間に余りがある場合、その余りの少なくとも一部を最後に動作する動作マシンの動作時間に割り当てるようになっている。このようにすれば、無駄なマージン時間を無くすことができる。第１処理部２１は、禁止期間において動作時間が経過した時点で特定処理が完了していない場合、異常が発生したと判断して切り替え処理および異常を外部に通知する通知処理を実行する。このようにすれば、特定処理が正常に完了しない場合などにおいて、禁止処理が実行されたまま他のＶＭの動作時間に影響を与えてしまうことが防止されてリアルタイム性を確保することができるとともに、ＶＭの再起動や特定処理の中断の判断などを行うことができる。

【００９８】
第１処理部２１は、禁止期間において動作時間が経過した時点で特定処理が完了していない場合、異常が発生したと判断して次回以降のＨＶ周期において許可要求を受信すると異常を外部に通知する通知処理を実行する。このようにすれば、禁止期間が固着したまま動作し続けていることを通知処理により報知することで、ＶＭの再起動や特定処理の中断の判断などを行うことができる。

【００９９】
設定時間は、複数のＶＭ１０、ＶＭ１１のそれぞれ毎に予め設定することができる。このようにすれば、各ＶＭが動作する時間を一律に管理することができる。または、第２処理部２２が、禁止要求を受信したとき、禁止要求を送信した動作マシンが開始する特定処理に要する時間に基づいて設定時間を設定することができる。このようにすれば、何らかの理由により特定処理を正常に完了することができなかった場合などにおいて、動作時間を延長する時間を必要最小限に抑えることが可能となり、その結果、リアルタイム性を確保することができる。

【０１００】
第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、禁止処理が実行されるまで動作マシンに禁止要求の送信を繰り返し実行させることができる。このようにすれば、ＶＭ切り替えまでの時間をＨＶ２に要求することなく、ＶＭだけで完結して処理を行うことができる。第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、切り替え処理が実行されるまでの期間、動作マシンを待機状態とすることができる。このようにすれば、マイコン３をスリープなどに遷移させて消費電力を低減することができる。

【０１０１】
第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、切り替え処理が実行されるまでの期間、動作マシンを特定処理とは異なる別の処理を実行可能な状態とすることができる。このようにすれば、ＶＭ切り替えまでの時間で他の処理を実行することが可能となり、その結果、マイコン３のリソースを有効活用することができる。第１処理部２１は、動作マシンが禁止要求を送信した後に禁止処理が実行されなかった場合、動作マシンに割り当てられた動作時間が経過する前に切り替え処理を実行することができる。このようにすれば、動作マシンにおいて特定処理のほかに実行可能な処理がない場合、他のＶＭを動作させることが可能となり、その結果、マイコン３のリソースを有効活用することができる。

【０１０２】
（第２実施形態）
以下、第２実施形態について図２３～図２５を参照して説明する。
本実施形態は、第１実施形態に対し、使用可能時間の設定について変更が加えられたものである。本実施形態では、複数のＶＭ１０、ＶＭ１１のそれぞれ毎に使用可能時間が設定されている。そのうえで、第１処理部２１は、動作マシンに対応する使用可能時間から必要とするマージン時間を消費する形で動作時間の延長を行うようになっている。すなわち、マージン時間は、動作マシンに対応する使用可能時間から割り当てられて使用される

ようになっている。
【０１０３】
次に、上記構成の作用について説明する。
以下の説明では、使用可能時間のことをＶＭ毎マージン時間と称することがある。この場合、ＶＭ毎マージン時間は、ＶＭ１０、ＶＭ１１のいずれについても、２０μ秒になっているものとする。
【０１０４】
［２－１２］第１２動作例
図２３に示す第１２動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともにそのタスクを中断することなく完了することができた場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。
【０１０５】
この場合、残り時間に対してＶＭ１０に対応するＶＭ毎マージン時間である２０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、タスクは、ＶＭ１０に割り当てられた当初の動作時間が経過した時点では完了しない。そのため、第１処理部２１は、ＶＭ１０により実行されているタスクが完了するまで動作時間を延長する。この場合、ＶＭ毎マージン時間の全てである２０μ秒だけ消費して動作時間の延長が行われる。
【０１０６】
このような第１２動作例によれば、ＶＭ１０は、ＶＭ毎マージン時間まで、その動作時間を延長することができ、中断不可能な処理であるタスクを連続して完了させることができる。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。これにより、第１処理部２１は、切り替え処理を実行する。このように、動作時間が延長された場合であっても、タスク完了後に直ちにＶＭ切り替えが行われることによりリアルタイム性を確保することができる。
【０１０７】
［２－１３］第１３動作例
図２４に示す第１３動作例は、ＶＭ１０、ＶＭ１１が動作時間の途中においてタスクの実行を開始するとともにそのタスクを中断することなく完了することができた場合を想定したものである。この場合、ＶＭ１０の動作時間における動作は、第１２動作例と同様である。そして、この場合、ＶＭ１１は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。
【０１０８】
この場合、残り時間に対してＶＭ１１に対応するＶＭ毎マージン時間である２０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１１は、タスクの実行を開始する。この場合、タスクは、ＶＭ１１に割り当てられた当初の動作時間が経過した時点では完了しない。
【０１０９】
そのため、第１処理部２１は、ＶＭ１１により実行されているタスクが完了するまで動作時間を延長する。この場合、ＶＭ毎マージン時間の全てである２０μ秒だけ消費して動作時間の延長が行われる。このような第１３動作例によれば、ＶＭ１１は、ＶＭ毎マージン時間まで、その動作時間を延長することができ、中断不可能な処理であるタスクを連続して完了させることができる。ＶＭ１１は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。

これにより、第１処理部２１は、切り替え処理を実行する。
【０１１０】
このように、動作時間が延長された場合であっても、タスク完了後に直ちにＶＭ切り替えが行われることによりリアルタイム性を確保することができる。第１３動作例から分かるように、本実施形態の構成によれば、ＶＭ毎にマージン時間が与えられるため、優先度が相対的に高いＶＭがマージン時間を占有するようなことがなく、その結果、優先度が相対的に低いＶＭについても同程度にマージン時間を確保することができる。
【０１１１】
［２－１４］第１４動作例
図２５に示す第１４動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともにそのタスクが完了しなかった場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。
【０１１２】
この場合、残り時間に対してＶＭ１０に対応するＶＭ毎マージン時間である２０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、タスクは、ＶＭ１０に割り当てられた当初の動作時間が経過した時点では完了しない。そのため、第１処理部２１は、ＶＭ１０により実行されているタスクが完了するまで動作時間を延長する。
【０１１３】
ただし、この場合、異常、故障などの何らかの理由により、ＶＭ毎マージン時間の全てである２０μ秒を消費して動作時間の延長が行われても、タスクが完了しなかったものとする。そうすると、第１処理部２１は、異常が発生したと判断し、通知処理を実行する。通知処理では、ＶＭ切り替えが禁止された状態である禁止期間が固着したことを検知した旨を表す固着エラーが発行される。また、このとき、第１処理部２１は、このようにＶＭ切り替えが禁止された状態のまま、切り替え処理を行う。
【０１１４】
そして、この場合、ＶＭ１１は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。この場合、残り時間に対してＶＭ１１に対応するＶＭ毎マージン時間である２０μ秒を加えた時間が、設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１１は、タスクの実行を開始する。
【０１１５】
この場合、タスクは、ＶＭ１１に割り当てられた当初の動作時間が経過した時点では完了しない。そのため、第１処理部２１は、ＶＭ１１により実行されているタスクが完了するまで動作時間を延長する。この場合、ＶＭ毎マージン時間の全てである２０μ秒だけ消費して動作時間の延長が行われる。ＶＭ１１は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。これにより、第１処理部２１は、切り替え処理を実行する。
【０１１６】
次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点からタスクの実行を再開する。この場合、ＶＭ１０により実行されるタスクは、ＶＭ１０が動作マシンへと切り替えられた時点から所定時間が経過した時点において完了となっている。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。また、このとき、ＨＶ２は、通知処理を行い、これにより固着エラーが発行される。その後、ＶＭ１０に割り当てられた

動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。
【０１１７】
このような第１４動作例によれば、複数のＶＭ１０、ＶＭ１１のそれぞれ毎にＶＭ毎マージン時間が設定されていることから、ＶＭ１０およびＶＭ１１のうち一方がＶＭ毎マージン時間を消費したとしても、ＶＭ１０およびＶＭ１１のうち他方が禁止要求を送信した場合には、そのＶＭに割り当てられたＶＭ毎マージン時間の上限まで動作時間を延長して禁止処理を行うことができる。
【０１１８】
以上説明した本実施形態によれば、複数のＶＭ１０、ＶＭ１１のそれぞれ毎にＶＭ毎マージン時間が設定されており、第１処理部２１は、動作マシンに対応するＶＭ毎マージン時間から必要とするマージン時間を消費する形で動作時間の延長を行うようになっている。このようにすれば、優先度の高低に関係なく、全てのＶＭ１０、ＶＭ１１がいずれもＶＭ毎マージン時間である２０μ秒をマージン時間として使用することができる。つまり、本実施形態によれば、ＶＭ毎にマージン時間が与えられるため、優先度が相対的に高いＶＭがマージン時間を占有することなく、優先度が相対的に低いＶＭについてもマージン時間を確保することができる。
【０１１９】
（第３実施形態）
以下、第２実施形態について図２６を参照して説明する。
本実施形態は、第１実施形態に対し、第１処理部２１の処理内容について変更が加えられたものである。本実施形態では、第１処理部２１は、禁止期間中、動作時間の延長を行わないようになっている。つまり、本実施形態では、全体マージン時間またはＶＭ毎マージン時間といったマージン時間の設定が行われていない。
【０１２０】
次に、上記構成の作用について説明する。
［２－１５］第１５動作例
図２６に示す第１５動作例は、ＶＭ１０が動作時間の途中においてタスクの実行を開始するとともにそのタスクが完了しなかった場合を想定したものである。この場合、ＶＭ１０は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１０から送信された禁止要求を受信すると、判断処理を実行する。
【０１２１】
この場合、残り時間が設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１０は、タスクの実行を開始する。この場合、異常、故障などの何らかの理由により、ＶＭ１０に割り当てられた動作時間が経過した時点でもタスクが完了しなかったものとする。そうすると、第１処理部２１は、異常が発生したと判断し、通知処理を実行する。通知処理では、ＶＭ切り替えが禁止された状態である禁止期間が固着したことを検知した旨を表す固着エラーが発行される。また、このとき、第１処理部２１は、このようにＶＭ切り替えが禁止された状態のまま、切り替え処理を行う。
【０１２２】
そして、この場合、ＶＭ１１は、自身が動作マシンへと切り替えられた時点から所定時間が経過した時点において、ＨＶ２に対して禁止要求を送信する。ＨＶ２は、ＶＭ１１から送信された禁止要求を受信すると、判断処理を実行する。この場合、残り時間が設定時間よりも長いものであるとする。そうすると、ＨＶ２は、禁止要求を受信した時点において禁止処理を実行する。禁止処理の開始に合わせて、動作マシンであるＶＭ１１は、タスクの実行を開始する。この場合、タスクは、ＶＭ１１に割り当てられた動作時間が経過した時点よりも前の時点において完了となっている。ＶＭ１１は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。これにより、第１処理部２１は、切り替え処理を実行する。

【０１２３】
次のＨＶ周期において、ＶＭ１０は、自身が動作マシンへと切り替えられた時点からタスクの実行を再開する。この場合、ＶＭ１０により実行されるタスクは、ＶＭ１０が動作マシンへと切り替えられた時点から所定時間が経過した時点において完了となっている。ＶＭ１０は、タスクを完了した際に許可要求を送信する。ＨＶ２は、許可要求を受信した時点において、禁止処理を終了して許可処理を実行する。また、このとき、ＨＶ２は、通知処理を行い、これにより固着エラーが発行される。その後、ＶＭ１０に割り当てられた動作時間が経過した時点において、第１処理部２１は、切り替え処理を行う。
【０１２４】
以上説明した本実施形態によれば、全体マージン時間またはＶＭ毎マージン時間といったマージン時間の設定が行われていない。このような本実施形態によれば、マージン時間の設定を行う上記各実施形態に比べ、全てのＶＭ１０、ＶＭ１１に対してより多くの動作時間を割り振ることができる。上記各実施形態では、設定された全体マージン時間またはＶＭ毎マージン時間のうち使用されなかった時間が無駄な時間になるおそれがあったが、本実施形態では、このような無駄な時間を生じさせることがない。また、本実施形態によれば、上記各実施形態と同様、禁止期間の固着検出が可能であるとともに、完了する見込みのない特定処理を次のＨＶ周期で動作させることができる。
【０１２５】
（その他の実施形態）
なお、本発明は上記し且つ図面に記載した各実施形態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任意に変形、組み合わせ、あるいは拡張することができる。
上記各実施形態で示した数値などは例示であり、それに限定されるものではない。
【０１２６】
本発明は、車両に搭載される統合ＥＣＵ１を構成するマイコン３上で動作する複数のＶＭのそれぞれを時分割スケジューリングでの制御を行うＨＶ２に限らず、コンピュータ上で動作する複数のＶＭのそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置全般に適用することができる。
【０１２７】
本開示は、実施例に準拠して記述されたが、本開示は当該実施例や構造に限定されるものではないと理解される。本開示は、様々な変形例や均等範囲内の変形をも包含する。加えて、様々な組み合わせや形態、さらには、それらに一要素のみ、それ以上、あるいはそれ以下、を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。
【０１２８】
本開示に記載の制御部及びその手法は、コンピュータプログラムにより具体化された一つ乃至は複数の機能を実行するようにプログラムされたプロセッサ及びメモリーを構成することによって提供された専用コンピュータにより、実現されてもよい。あるいは、本開示に記載の制御部及びその手法は、一つ以上の専用ハードウェア論理回路によってプロセッサを構成することによって提供された専用コンピュータにより、実現されてもよい。もしくは、本開示に記載の制御部及びその手法は、一つ乃至は複数の機能を実行するようにプログラムされたプロセッサ及びメモリーと一つ以上のハードウェア論理回路によって構成されたプロセッサとの組み合わせにより構成された一つ以上の専用コンピュータにより、実現されてもよい。また、コンピュータプログラムは、コンピュータにより実行されるインストラクションとして、コンピュータ読み取り可能な非遷移有形記録媒体に記憶されていてもよい。
【０１２９】
本開示は、特許請求の範囲に記載の発明に加え、以下のような発明を含む。
［１］
複数の仮想マシン（１０、１１）のそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置であって、
前記複数の仮想マシンのうち動作中のものを動作マシンとすると、

前記動作マシンを切り替える切り替え処理を実行することができる第１処理部（２１）と、
前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理部（２２）と、
を備え、
前記動作マシンは、連続して実行しなければならない処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっており、
前記第２処理部は、
前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、
前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっており、
前記許可要求を受信したとき、前記許可処理を実行するようになっており、
前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する動作制御装置。
［２］
前記第１処理部は、前記禁止期間中、前記動作時間を所定のマージン時間だけ延長することができるようになっており、
前記第２処理部は、前記禁止要求を受信した時点から延長した前記動作時間が経過する時点までの時間を前記残り時間として前記判断処理を実行する［１］に記載の動作制御装置。
［３］
前記動作周期毎に使用可能時間が設定されており、
前記第１処理部は、前記使用可能時間から必要とする前記マージン時間を消費する形で前記動作時間の延長を行うようになっている［２］に記載の動作制御装置。
［４］
前記複数の仮想マシンのそれぞれ毎に使用可能時間が設定されており、
前記第１処理部は、前記動作マシンに対応する前記使用可能時間から必要とする前記マージン時間を消費する形で前記動作時間の延長を行うようになっている［２］に記載の動作制御装置。
［５］
前記第１処理部は、前記動作周期において最後に動作する前記動作マシンの動作が開始される際に前記使用可能時間に余りがある場合、その余りの少なくとも一部を最後に動作する前記動作マシンの前記動作時間に割り当てるようになっている［３］に記載の動作制御装置。
［６］
前記第１処理部は、前記禁止期間において前記動作時間が経過した時点で前記特定処理が完了していない場合、異常が発生したと判断して前記切り替え処理および前記異常を外部に通知する通知処理の一方または双方を実行する［１］から［５］のいずれか一項に記載の動作制御装置。
［７］
前記第１処理部は、前記禁止期間において前記動作時間が経過した時点で前記特定処理が完了していない場合、異常が発生したと判断して次回以降の前記動作周期において前記許可要求を受信すると前記異常を外部に通知する通知処理を実行する［１］から［６］のいずれか一項に記載の動作制御装置。
［８］
前記設定時間は、前記複数の仮想マシンのそれぞれ毎に予め設定されている［１］から［７］のいずれか一項に記載の動作制御装置。

［９］
前記第２処理部は、前記禁止要求を受信したとき、前記禁止要求を送信した前記動作マシンが開始する前記特定処理に要する時間に基づいて前記設定時間を設定する［１］から［７］のいずれか一項に記載の動作制御装置。
［１０］
前記第１処理部は、前記動作マシンが前記禁止要求を送信した後に前記禁止処理が実行されなかった場合、前記禁止処理が実行されるまで前記動作マシンに前記禁止要求の送信を繰り返し実行させるようになっている［１］から［９］のいずれか一項に記載の動作制御装置。
［１１］
前記第１処理部は、前記動作マシンが前記禁止要求を送信した後に前記禁止処理が実行されなかった場合、前記切り替え処理が実行されるまでの期間、前記動作マシンを待機状態とする、または、前記動作マシンを前記特定処理とは異なる別の処理を実行可能な状態とするようになっている［１］から［９］のいずれか一項に記載の動作制御装置。
［１２］
前記第１処理部は、前記動作マシンが前記禁止要求を送信した後に前記禁止処理が実行されなかった場合、前記動作マシンに割り当てられた前記動作時間が経過する前に前記切り替え処理を実行する［１］から［９］のいずれか一項に記載の動作制御装置。
［１３］
複数の仮想マシン（ＶＭ１０、ＶＭ１１）のそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置（２）に実行させる動作制御プログラムであって、
前記複数の仮想マシンのうち動作中のものを動作マシンとすると、
前記動作マシンを切り替える切り替え処理を実行することができる第１処理と、
前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理と、
を含み、
前記動作マシンは、連続して実行しなければならない処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっており、
前記第２処理では、
前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、
前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっており、
前記許可要求を受信したとき、前記許可処理を実行するようになっており、
前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する動作制御プログラム。
［１４］
コンピュータ（３）と、前記コンピュータ上で動作する複数の仮想マシン（ＶＭ１０、ＶＭ１１）と、前記複数の仮想マシンのそれぞれを動作周期毎に予め割り当てられた動作時間ずつ時分割で動作させるための制御を行う動作制御装置（２）と、を備えた電子制御装置であって、
前記複数の仮想マシンのうち動作中のものを動作マシンとすると、
前記動作制御装置は、
前記動作マシンを切り替える切り替え処理を実行することができる第１処理部（２１）と、
前記切り替え処理の実行を禁止する禁止処理および前記切り替え処理の実行を許可する許可処理を実行することができる第２処理部（２２）と、

を備え、
前記動作マシンは、連続して実行しなければならない処理である特定処理を開始する際に禁止要求を送信するとともに、前記特定処理を完了した際に許可要求を送信するようになっており、
前記第２処理部は、
前記禁止要求を受信したとき、その時点から前記動作時間が経過する時点までの時間である残り時間が所定の設定時間以上の時間であるか否かを判断する判断処理を実行し、
前記判断処理の結果、前記残り時間が前記設定時間以上の時間である場合には前記禁止処理を実行するとともに、前記残り時間が前記設定時間未満の時間である場合には前記禁止処理を実行しないようになっており、
前記許可要求を受信したとき、前記許可処理を実行するようになっており、
前記動作マシンは、前記禁止処理が実行されている期間である禁止期間中に前記特定処理を実行する電子制御装置。

【符号の説明】

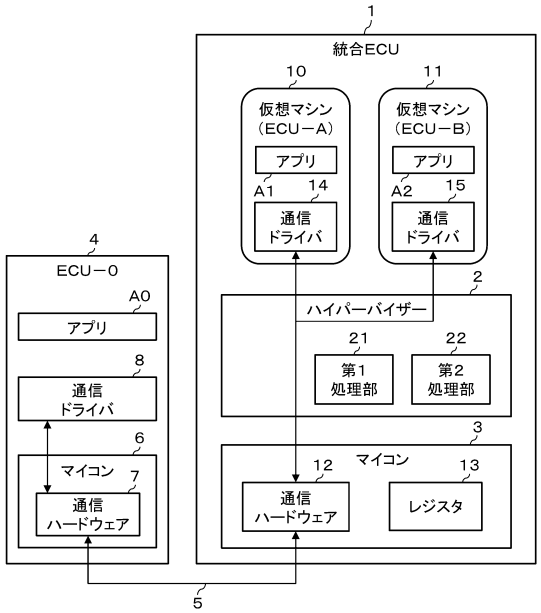
【０１３０】

１…統合ＥＣＵ、２…ハイパーバイザー、３…マイクロコンピュータ、１０、１１…仮想マシン、２１…第１処理部、２２…第２処理部。

【図面】

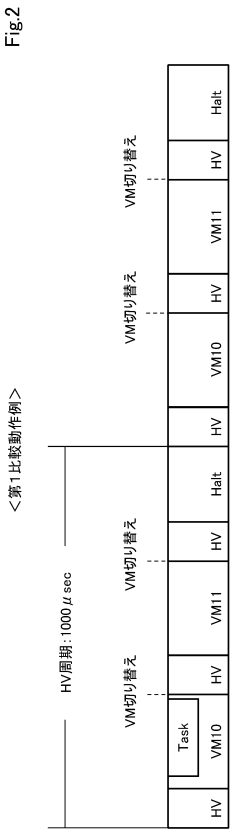
【図１】

Fig.1



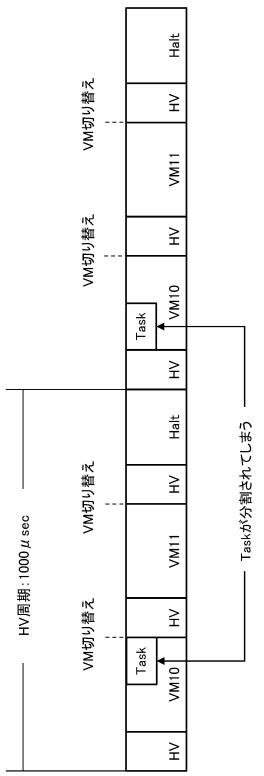
【図２】

Fig.2



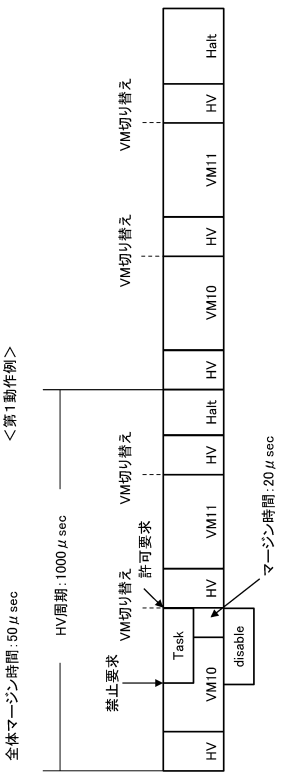
【図３】

Fig.3



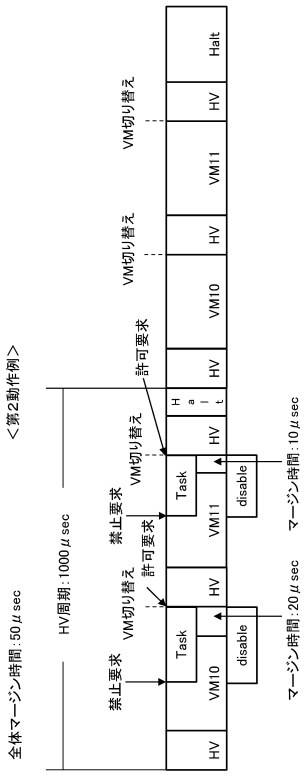
【図４】

Fig.4



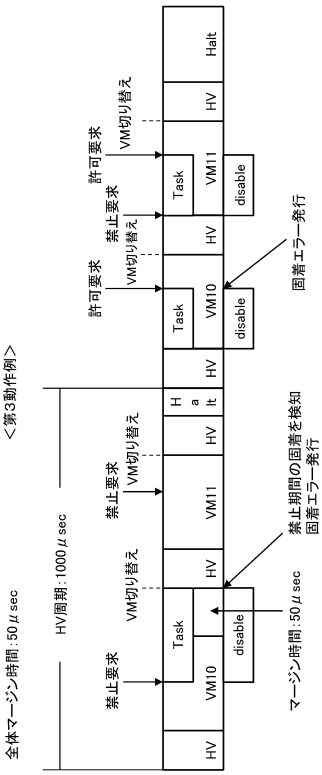
【図５】

Fig.5



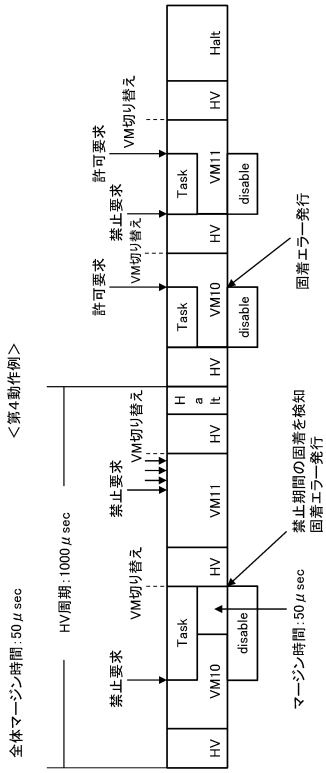
【図６】

Fig.6



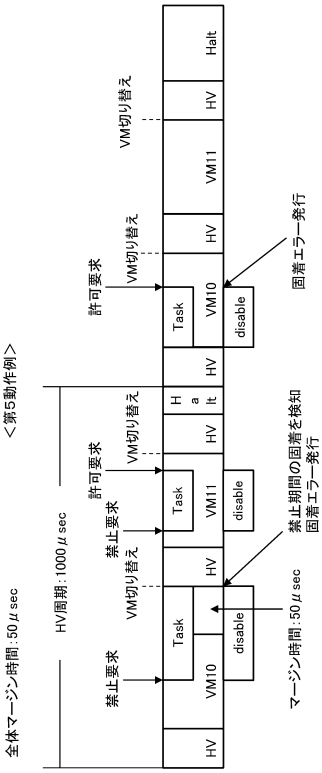
【図７】

Fig.7



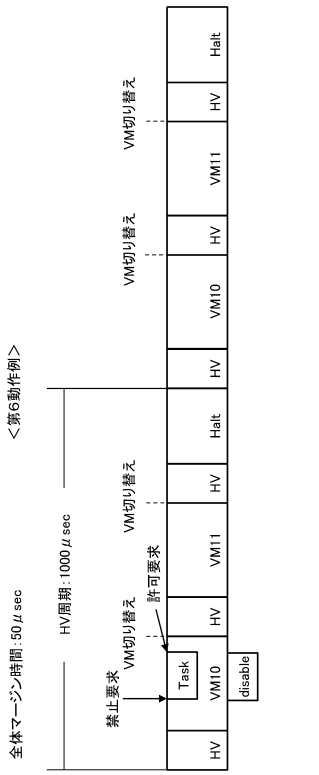
【図８】

Fig.8



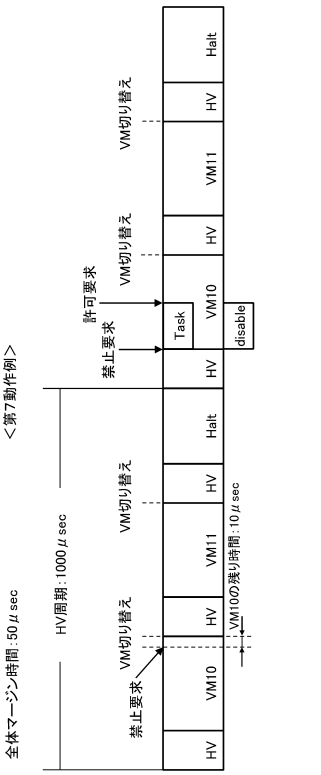
【図９】

Fig.9



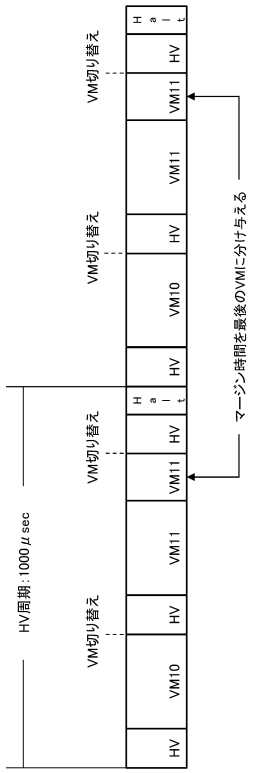
【図１０】

Fig.10



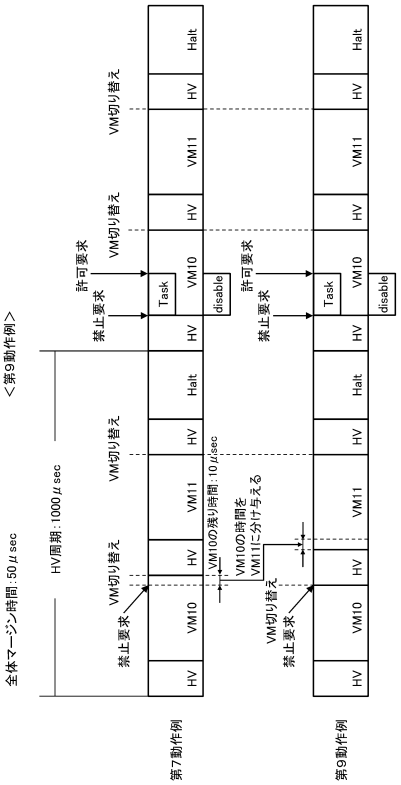
【図１１】

Fig.11



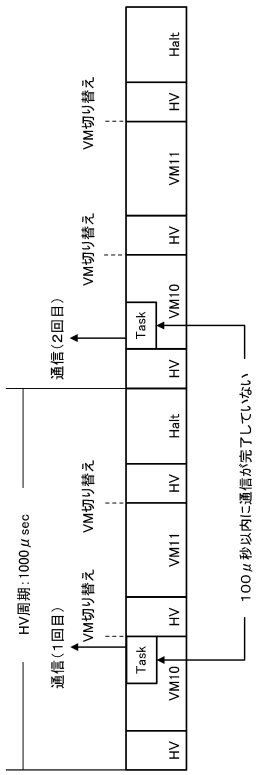
【図１２】

Fig.12



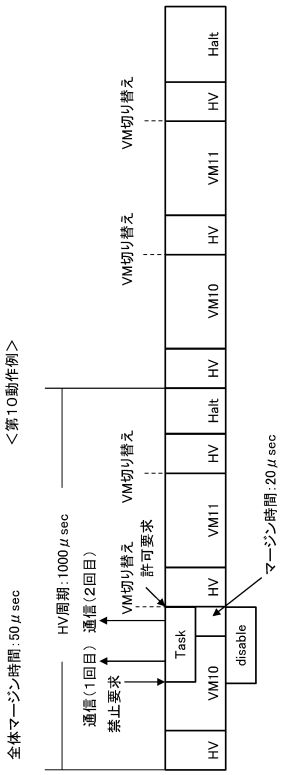
【図１３】

Fig.13



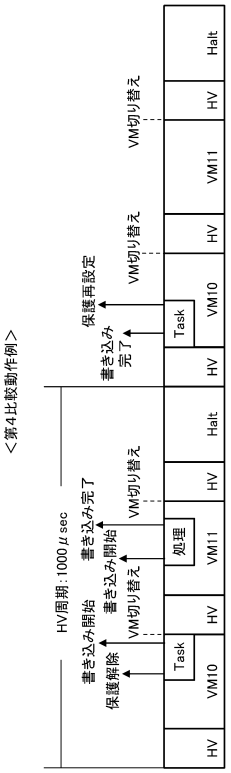
【図１４】

Fig.14



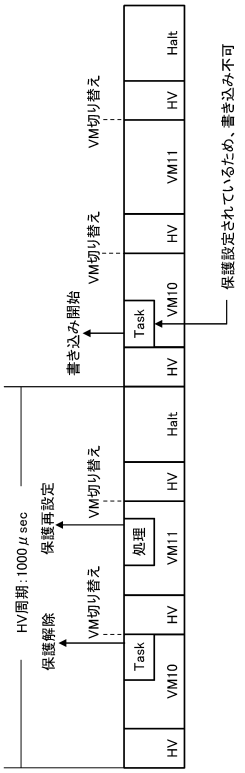
【図１５】

Fig.15



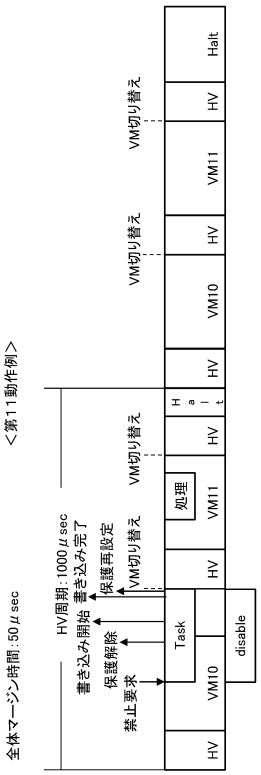
【図１６】

Fig.16



【図１７】

Fig.17



【図１８】

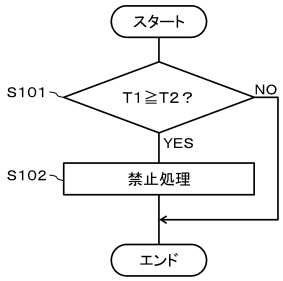
Fig.18



【図１９】

Fig.19

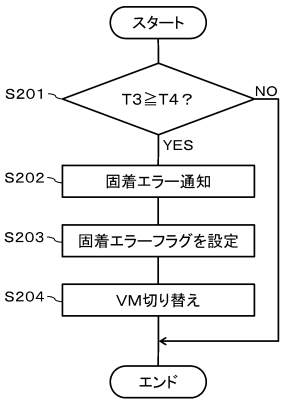
＜HV2が禁止要求を受信したときに実行する各処理＞



【図２０】

Fig.20

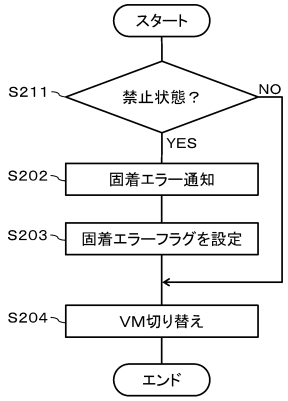
＜禁止期間にHV2の第1処理部21により実行される各処理＞



【図２１】

Fig.21

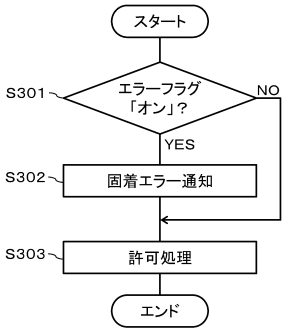
＜動作時間終了時にHV2の第1処理部21により実行される各処理＞



【図２２】

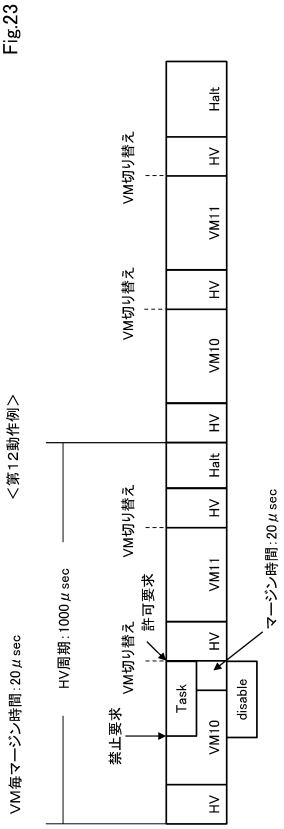
Fig.22

＜HV2が許可要求を受信したときに実行する各処理＞



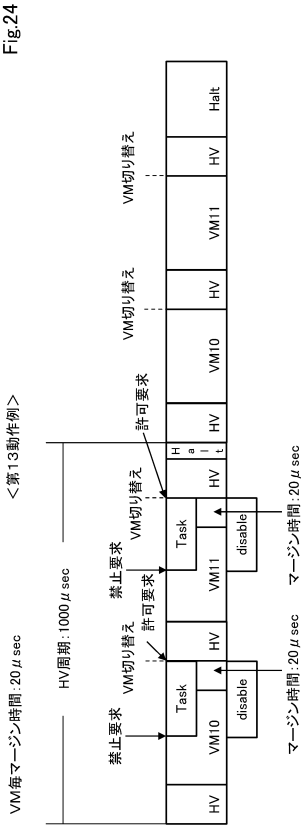
【図２３】

Fig.23



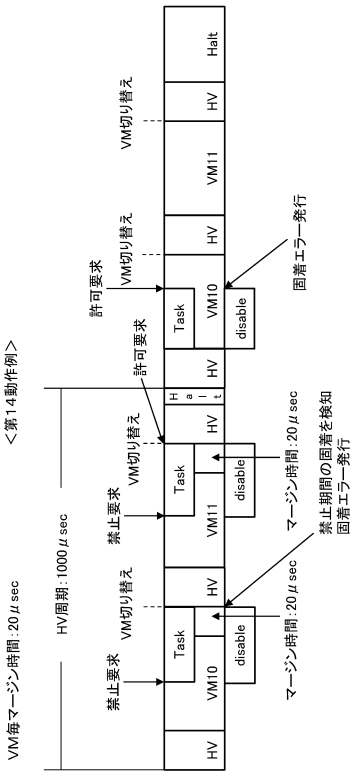
【図２４】

Fig.24



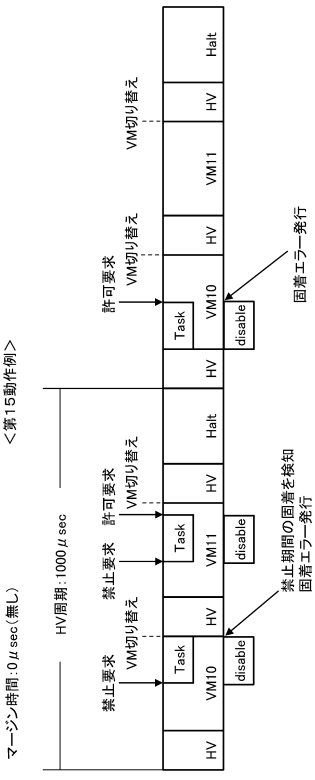
【図２５】

Fig.25



【図２６】

Fig.26



フロントページの続き

東京都中野区本町１－３２－２　ハーモニータワー
(72)発明者　西條　洸介
東京都中野区本町１－３２－２　ハーモニータワー