(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6083136号
(P6083136)

(45)発行日　平成29年2月22日(2017.2.22)　(24)登録日　平成29年2月3日(2017.2.3)

(51)Int.Cl.		F I		
G06F 11/07	(2006.01)	G06F	11/07	178
G06F 9/46	(2006.01)	G06F	11/07	140C
		G06F	11/07	140E
		G06F	9/46	350

請求項の数 11　(全 35 頁)

(21)出願番号　特願2012-141495 (P2012-141495)
(22)出願日　平成24年6月22日 (2012.6.22)
(65)公開番号　特開2014-6676 (P2014-6676A)
(43)公開日　平成26年1月16日 (2014.1.16)
審査請求日　平成27年3月19日 (2015.3.19)

前置審査

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(72)発明者　近藤　浩
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　岡野　憲司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】メモリダンプ機能を有する情報処理装置、メモリダンプ方法、およびメモリダンププログラム

(57)【特許請求の範囲】

【請求項１】

メモリと、

前記メモリに格納されたプログラムを実行することにより、仮想マシン、該仮想マシン上で稼動するオペレーティングシステム、および前記仮想マシンを制御するハイパーバイザを実行する処理部と、

前記メモリ及び前記処理部を含むシステムの制御を行なう制御部と、

を有し、

前記処理部は、

前記ハイパーバイザのエラーを検出したときに、前記オペレーティングシステムを停止し、

前記ハイパーバイザが使用している第１のメモリ領域を前記制御部に通知し、

前記ハイパーバイザを停止し、

前記ハイパーバイザが使用するメモリ領域を、前記制御部に通知された前記第１のメモリ領域とは異なる第２のメモリ領域に変更し、

前記第２のメモリ領域を使用領域として、前記ハイパーバイザを起動し、

前記第２のメモリ領域を使用領域として前記ハイパーバイザを起動した後、停止した前記オペレーティングシステムが使用するメモリ領域を、前記オペレーティングシステムのカーネルが使用していた第３のメモリ領域とは異なる第４のメモリ領域に変更し、

前記第４のメモリ領域を使用領域として、停止した前記オペレーティングシステムを

起動し、該オペレーティングシステム上で稼動する業務プログラムを再開し、
前記第１のメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す処理と、
前記第３のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す処理を実行する
ことを特徴とする情報処理装置。
【請求項２】
メモリと、
仮想マシン及び該仮想マシン上で稼動するオペレーティングシステムを実行する処理部と、
を有し、
前記処理部は、
実行中のオペレーティングシステムのエラーを検出したときに、前記エラーを検出したオペレーティングシステムを停止し、
停止したオペレーティングシステムが使用するメモリ領域を、前記停止したオペレーティングシステムのカーネルが使用していた第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記第２のメモリ領域を使用領域として、前記停止したオペレーティングシステムを起動して該オペレーティングシステム上で稼動する業務プログラムを再開し、
前記第１のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す処理と、
前記仮想マシンを制御するハイパーバイザを稼動させたまま、前記ハイパーバイザが使用するメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す処理を実行する
ことを特徴とする情報処理装置。
【請求項３】
メモリと、前記メモリに格納されたプログラムを実行することにより、仮想マシン、該仮想マシン上で稼動するオペレーティングシステムを実行する処理部とを各々有する複数の物理パーティションと、
前記複数の物理パーティションの制御を行なう制御部と、
を有し、
前記物理パーティションの各々に含まれる前記処理部は、
実行中のオペレーティングシステムのエラーを検出したときに、前記エラーを検出したオペレーティングシステムを停止し、
停止したオペレーティングシステムが使用するメモリ領域を、前記停止したオペレーティングシステムのカーネルが使用していた第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記第２のメモリ領域を使用領域として、前記停止したオペレーティングシステムを起動して該オペレーティングシステム上で稼動する業務プログラムを再開し、
前記第１のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す処理と、
前記仮想マシンを制御するハイパーバイザを稼動させたまま、前記ハイパーバイザが使用するメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す処理を実行する
ことを特徴とする情報処理装置。
【請求項４】
メモリと、前記メモリに格納されたプログラムを実行することにより、仮想マシン、該仮想マシン上で稼動するオペレーティングシステム、および前記仮想マシンを制御するハイパーバイザを実行する処理部とを各々有する複数の物理パーティションと、
前記複数の物理パーティションの制御を行なう制御部と、

を有し、
前記物理パーティションの各々では、複数の仮想マシンを実行し、
前記物理パーティションの各々に含まれる前記処理部は、
前記ハイパーバイザのエラーを検出したときに、複数の仮想マシンの各々で稼動するオペレーティングシステムを停止し、
前記ハイパーバイザが使用している第１のメモリ領域を前記制御部に通知し、
前記ハイパーバイザを停止し、
前記ハイパーバイザが使用するメモリ領域を、前記制御部に通知された前記第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記第２のメモリ領域を使用領域として、前記ハイパーバイザを起動し、
前記第２のメモリ領域を使用領域として前記ハイパーバイザを起動した後、停止した複数のオペレーティングシステムの各々が使用するメモリ領域を、前記停止した複数のオペレーティングシステムの各々のカーネルが使用していた複数の第３のメモリ領域とは異なり、各々重複しない複数の第４のメモリ領域に変更し、
前記複数の第４のメモリ領域の各々を使用領域として、各使用領域に対応する前記停止したオペレーティングシステムの各々を起動して、起動した各オペレーティングシステム上で稼動する業務プログラムを再開し、
前記第１のメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す処理と、
前記複数の第３のメモリ領域の各々データを読み出して、該データを前記複数のオペレーティングシステムのダンプファイルとしてファイルに書き出す処理を実行する
ことを特徴とする情報処理装置。
【請求項５】
少なくとも１つのメモリと、
プログラムを実行する少なくとも１つの処理部と、を有し、
前記メモリおよび前記処理部を用いて、オペレーティングシステムが稼動する仮想マシンを制御するハイパーバイザ、および前記メモリ及び前記処理部を含むシステムの制御を行なうファームウェアの処理が実行され、
前記ハイパーバイザは、
前記ハイパーバイザのエラーを検出したときに、前記オペレーティングシステムを停止し、
前記ハイパーバイザが使用している第１のメモリ領域を前記ファームウェアに通知し、
前記ハイパーバイザを停止し、
前記ファームウェアは、
前記ハイパーバイザが使用するメモリ領域を、前記第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記第２のメモリ領域を使用領域として、前記ハイパーバイザを起動させ、
起動した前記ハイパーバイザは、
停止した前記オペレーティングシステムが使用するメモリ領域を、前記オペレーティングシステムのカーネルが使用していた第３のメモリ領域とは異なる第４のメモリ領域に変更し、
前記第４のメモリ領域を使用領域として、停止した前記オペレーティングシステムを起動させ、
起動した前記オペレーティングシステムは、
業務プログラムを再開して、前記第１のメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出し、
前記第３のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す
処理を実行することを特徴とする情報処理装置。

【請求項６】
前記処理部は、前記ハイパーバイザのエラーを検出したときに、前記第１のメモリ領域を、ダンプ対象領域として前記ファームウェアに通知することを特徴とする、請求項５記載の情報処理装置。
【請求項７】
前記ファームウェアは、
前記ハイパーバイザを停止した後、前記第１のメモリ領域の内容を保持したまま、前記ハイパーバイザが使用するメモリ領域を前記第２のメモリ領域に変更し、少なくとも変更後の前記第２のメモリ領域を初期化した後に、前記ハイパーバイザを起動させる、ことを特徴とする請求項５または６に記載の情報処理装置。
【請求項８】
さらに、前記ファームウェアは、前記ハイパーバイザが使用していた領域のダンプを行うか否かを示すフラグ情報を設定し、
前記フラグ情報が、前記ハイパーバイザが使用していた領域のダンプを行うことを示す場合、前記オペレーティングシステムは、前記第１のメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す
ことを特徴とする請求項５乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
少なくとも１つのメモリと、
プログラムを実行する少なくとも１つのプロセッサと、を有し、
前記メモリおよび前記プロセッサを用いて、オペレーティングシステムが稼動する仮想マシンを制御するハイパーバイザ、および前記メモリ及び前記プロセッサを含むシステムの制御を行なうファームウェアの処理が実行され、
前記ハイパーバイザは、
実行中のオペレーティングシステムのエラーを検出したときに、前記エラーを検出したオペレーティングシステムを停止し、
前記ファームウェアは、
停止したオペレーティングシステムが使用するメモリ領域を、前記停止したオペレーティングシステムのカーネルが使用していた第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記ハイパーバイザは、
前記第２のメモリ領域を使用領域として、前記停止したオペレーティングシステムを起動させ、
起動したオペレーティングシステムは、
業務プログラムを再開し、
前記第１のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す処理と、
前記仮想マシンを制御するハイパーバイザが稼動した状態で、前記ハイパーバイザが使用するメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す処理を実行する
ことを特徴とする情報処理装置。
【請求項１０】
少なくとも１つのメモリと少なくとも１つのプロセッサを含む物理パーティションを有し、
前記物理パーティションは、
オペレーティングシステムが稼動する仮想マシンを制御するハイパーバイザ、および前記物理パーティションの制御を行なうファームウェアの処理を実行し、
前記ハイパーバイザは、
実行中のオペレーティングシステムのエラーを検出したときに、前記エラーを検出したオペレーティングシステムを停止し、

停止したオペレーティングシステムが使用するメモリ領域を、前記停止したオペレーティングシステムのカーネルが使用していた第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記第２のメモリ領域を使用領域として、前記停止したオペレーティングシステムを起動させ、
起動したオペレーティングシステムは、
業務プログラムを再開し、
前記第１のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す処理と、
前記仮想マシンを制御するハイパーバイザが稼動した状態で、前記ハイパーバイザが使用するメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す処理を実行する
ことを特徴とする情報処理装置。
【請求項１１】
少なくとも１つのメモリと少なくとも１つのプロセッサを含む物理パーティションを有し、
前記物理パーティションは、
オペレーティングシステムが稼動する仮想マシンを制御するハイパーバイザ、および前記物理パーティションの制御を行なうファームウェアの処理を実行し、
前記ハイパーバイザは、
複数の仮想マシンを制御し、
前記ハイパーバイザのエラーを検出したときに、複数の仮想マシンの各々で稼動するオペレーティングシステムを停止し、
前記ハイパーバイザが使用している第１のメモリ領域を前記ファームウェアに通知し、
前記ハイパーバイザを停止し、
前記ファームウェアは、
前記ハイパーバイザが使用するメモリ領域を、通知された前記第１のメモリ領域とは異なる第２のメモリ領域に変更し、
前記第２のメモリ領域を使用領域として前記ハイパーバイザを起動し、
起動した前記ハイパーバイザは、
停止した複数のオペレーティングシステムの各々が使用するメモリ領域を、前記停止した複数のオペレーティングシステムの各々のカーネルが使用していた複数の第３のメモリ領域とは異なり、各々重複しない複数の第４のメモリ領域に変更し、
前記複数の第４のメモリ領域の各々を使用領域として、各使用領域に対応する前記停止したオペレーティングシステムの各々を起動し、
起動した各オペレーティングシステムは、
業務プログラムを再開し、
前記複数の第３のメモリ領域の各々データを読み出して、該データを前記複数のオペレーティングシステムのダンプファイルとしてファイルに書き出し、
前記起動した各オペレーティングシステムのうちの１つは、
前記第１のメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す
処理を実行することを特徴とする情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、メモリダンプ機能を有する情報処理装置、メモリダンプ方法、およびメモリダンププログラムに関する。
【背景技術】

【０００２】
近年、UNIX（登録商標）サーバ、IAサーバが基幹システムに導入されるようになり、UNIX（登録商標）サーバ、IAサーバの高可用性が重要視されている。一般的に、システムに致命的なエラーが発生した場合はシステムを緊急停止（パニック）させて、その原因を調査するためにメモリダンプをディスクに保存している。
【０００３】
システムを停止している間は、システムを使用できないので、速やかにシステムを再起動することが重要な要件となる。
しかし、近年では、実装メモリの容量がテラバイト（TB）オーダのサーバが登場し、このようなシステムでは、メモリダンプを採取するのに非常に時間がかかり、速やかにシステムを再起動することができなくなっている。
【０００４】
また、メモリダンプをディスク上に保存せず、緊急停止時のメモリ内容を別のメモリ上に保存する方法や障害発生時のメモリ内容をダンプ格納領域に保存する際、メモリの一部を保存し、再起動後に保存していないメモリ内容をダンプファイルに変換する方法が知られている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開平１１－２１２８３６号公報
【特許文献２】特開２００１－２２９０５３号公報
【特許文献３】特開２００６－７２９３１号公報
【特許文献４】特開２００５－１２２３３４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、従来の方法では、異常発生時のメモリダンプを別のメモリやディスクに保存しているため、保存するメモリダンプのサイズが大きい場合は、メモリのコピーに時間がかかり、速やかにシステムを再起動することができないという問題があった。
【０００７】
また、オペレーティングシステムが致命的なエラーを検出して、システムを緊急停止する場合、異常を検出したオペレーティングシステムがダンプを採取するため、ダンプ採取処理中に再度異常を検出して、ハングアップが発生するなどの二次被害が発生することがあるという問題があった。
【０００８】
１つの側面では、本発明は、再起動が必要となる異常を検出した場合、速やかに業務を再開させて、原因調査のためのメモリダンプを採取することを課題とする。
【課題を解決するための手段】
【０００９】
１つの側面では、実施の形態の情報処理装置は、メモリと、前記メモリに格納されたプログラムを実行することにより、仮想マシン、該仮想マシン上で稼動するオペレーティングシステム、および前記仮想マシンを制御するハイパーバイザを実行する処理部と、前記メモリ及び前記処理部を含むシステムの制御を行なう制御部と、を有する。
【００１０】
前記処理部は、前記ハイパーバイザのエラーを検出したときに、前記オペレーティングシステムを停止し、前記ハイパーバイザが使用している第１のメモリ領域を前記制御部に通知する。
【００１１】
そして、前記処理部は、前記ハイパーバイザを停止し、前記ハイパーバイザが使用するメモリ領域を、前記制御部に通知された前記第１のメモリ領域とは異なる第２のメモリ領

域に変更し、前記第２のメモリ領域を使用領域として、前記ハイパーバイザを起動する。
【００１２】
さらに、前記処理部は、前記オペレーティングシステムを起動して該オペレーティングシステム上で稼動する業務プログラムを再開し、前記第１のメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出す。
【００１３】
他の１つの側面では、実施の形態の情報処理装置は、メモリと、オペレーティングシステムを実行、または、仮想マシン及び該仮想マシン上で稼動するオペレーティングシステムを実行する処理部と、を有する。
【００１４】
前記処理部は、実行中のオペレーティングシステムのエラーを検出したときに、前記エラーを検出したオペレーティングシステムを停止し、停止したオペレーティングシステムが使用するメモリ領域を、前記停止したオペレーティングシステムのカーネルが使用していた第１のメモリ領域とは異なる第２のメモリ領域に変更する。
【００１５】
そして、前記処理部は、前記第２のメモリ領域を使用領域として、前記停止したオペレーティングシステムを起動して該オペレーティングシステム上で稼動する業務プログラムを再開し、前記第１のメモリ領域のデータを読み出して、該データをオペレーティングシステムのダンプファイルとしてファイルに書き出す。
【発明の効果】
【００１６】
１つの実施の形態の情報処理装置によれば、再起動が必要となる異常を検出した場合、速やかに業務を再開させて、原因調査のためのメモリダンプを採取することができる。
【図面の簡単な説明】
【００１７】
【図１】実施の形態に係るサーバのハードウェア構成図である。
【図２】実施の形態に係るサーバと機能との対応関係を示す図である。
【図３】実施の形態に係る物理パーティションの機能ブロック図である。
【図４】実施の形態に係るファームウェアの構成図である。
【図５】実施の形態に係るハイパーバイザの構成図である。
【図６】実施の形態に係るOSの構成図である。
【図７Ａ】第１の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図７Ｂ】第１の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図７Ｃ】第１の実施の形態に係るメモリダンプ生成処理の変形例のフローチャートである。
【図８】HVダンプ対象領域情報の例である。
【図９Ａ】第２の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図９Ｂ】第２の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図９Ｃ】第２の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図１０】カーネルダンプ対象領域情報の例である。
【図１１】ダンプ採取用ドメインによるカーネルのメモリダンプ生成処理のフローチャートである。
【図１２】ダンプ採取用ドメインによるメモリダンプの採取を示す図である。
【図１３】ダンプ採取用ドメインによるメモリダンプの採取におけるPA-RAマッピング情報を示す図である。
【図１４】メモリDynamic Reconfiguration機能を用いたカーネルのメモリダンプ生成処理のフローチャートである。
【図１５】メモリDynamic Reconfiguration機能を用いたメモリダンプの採取を示す図である。
【図１６】メモリDynamic Reconfiguration機能を用いたメモリダンプの採取におけるPA-

RAマッピング情報を示す図である。
【図１７】第３の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図１８Ａ】第４の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図１８Ｂ】第４の実施の形態に係るメモリダンプ生成処理のフローチャートである。
【図１９】稼動中のハイパーバイザのメモリダンプ生成処理のフローチャートである。
【発明を実施するための形態】
【００１８】
以下、図面を参照しながら本発明の実施の形態を説明する。
図１は、実施の形態に係るサーバのハードウェア構成図である。
サーバ（情報処理装置）１０は、システムボード１１－ｉ（ｉ＝１～３）、サービスプロセッサ（ＳＰ）２１、ディスクユニット３１、および通信インタフェース４１を備える。
【００１９】
システムボード１１－ｉ、サービスプロセッサ２１、ディスクユニット３１、および通信インタフェース４１は、バス５１を介して接続されている。
システムボード１１－ｉは、Central Processing Unit（ＣＰＵ）１２－ｉ－ｋ（ｋ＝１、２）、不揮発性メモリ１４－ｉ、およびメモリ１３－ｉ－ｋを備える。
【００２０】
サービスプロセッサ２１は、サーバ１０の制御、サーバ１０内の物理パーティションの制御等を行う装置である。サービスプロセッサ２１は、ＣＰＵ２２およびメモリ２３を備える。サービスプロセッサ２１は、制御部の一例である。
【００２１】
ＣＰＵ２２は、サーバ１０の制御、サーバ１０内の物理パーティションの制御等の各種処理を行う。
メモリ２３は、サービスプロセッサ２１で用いられるデータを一時的に格納する。メモリ２３は、例えば、RAMである。
【００２２】
ディスクユニット３１は、ハードディスクドライブ（ＨＤＤ）３２－ｉ（ｉ＝１～３）を備える。
ＨＤＤ３２は、サーバ１０で使用されるデータを格納する装置である。ＨＤＤ３２は、記憶手段の一例である。
【００２３】
通信インタフェース４１は、サーバ１０と接続する装置と通信を行うインタフェースである。
【００２４】
図２は、実施の形態に係るサーバと機能との対応関係の一例を示す図である。
サーバ１０は、２つの物理パーティション６１－ｋ（ｋ＝１、２）に分割して運用されている。尚、明細書内において、物理パーティション６１－１、６１－２をそれぞれ物理パーティション＃０、物理パーティション＃１と表記する場合がある。
【００２５】
物理パーティション＃０、＃１は、サービスプロセッサ２１により制御される。物理パーティション＃０、＃１に含まれるＣＰＵは、処理部の一例である。
システムボード１１－１、１１－２から構成される物理パーティション＃０は、さらに物理パーティション＃０内で４つの論理ドメイン＃０～＃３に分割して、各論理ドメイン＃０～＃３で独立したオペレーティングシステム（OS）が稼動している。また、ハイパーバイザ（HV）＃０が、物理パーティション＃０内の物理リソースと各論理ドメイン＃０～＃３との対応関係を制御する。
【００２６】
システムボード１１－３から構成される物理パーティション＃１内では、論理ドメイン＃４でオペレーティングシステム（OS）が稼動している。またハイパーバイザ＃１が、物

理パーティション＃１内の物理リソースと論理ドメイン＃４との対応関係を制御する。
【００２７】
図３は、実施の形態に係る物理パーティションの機能ブロック図である。
物理パーティション６１－１は、論理ドメイン２０１－ｍ（ｍ＝１～４）、ファームウェア（ＦＷ）３１１、およびハイパーバイザ（HV）３５１を備える。
【００２８】
図３の物理パーティション６１－１は、図２の物理パーティション６１－１に対応する。
尚、論理ドメイン２０１－１～２０１－４は、それぞれ図２で示した各論理ドメイン＃０～＃３に対応する。
【００２９】
尚、明細書内において、論理ドメイン２０１－１は、制御ドメイン＃０と表記する場合がある。
また、明細書内において、論理ドメイン２０１－４は、ダンプ専用ドメイン＃３またはダンプ採取用ドメイン２０１－４と表記する場合がある。
【００３０】
以下、特に限定ない限り論理ドメインとは仮想マシンを示す。
論理ドメイン２０１－ｍは、ＣＰＵ２０２－ｍ－ｋ（ｋ＝１、２）、メモリ２０３－ｍ、およびディスク２０４－ｍを備える。以下、特に限定ない限りＣＰＵ２０２、メモリ２０３、およびディスク２０４は、それぞれ仮想ＣＰＵ、仮想メモリ、および仮想ディスクである。
【００３１】
ＣＰＵ２０２－ｍ－ｋは、各種処理を実行する。
メモリ２０３－ｍは、ディスク２０４－ｍから読み出された、各種プログラムやデータを格納する。
【００３２】
ファームウェア３１１は、サーバ１０全体（複数の物理パーティション６１－１、６１－２）の制御を行い、例えば、ハードウェアの初期化、メモリ診断、温度監視などを行う。ファームウェア３１１には、図１のサービスプロセッサ２１、およびシステムボード１１－１、１１－２の不揮発性メモリ１４－１、１４－２上に展開されるPower On Self Test（ＰＯＳＴ）が含まれる。ここで、Power On Self Test（ＰＯＳＴ）とは、システム起動時にハードウェアリソースの診断と初期化を実行するプログラムである。
【００３３】
ハイパーバイザ３５１は、論理ドメイン２０１－ｍ、および論理ドメイン２０１－ｍ上で稼動するオペレーティングシステム（OS）４０１－ｍを制御する。ハイパーバイザ３５１は、図１のシステムボード１１－１，１１－２のメモリ１３－１－１、１３－１－２、１３－２－１、１３－２－２上に展開されＣＰＵ１２－１－１、１２－１－２、１２－２－１、１２－２－２により実行される。
【００３４】
図３の下部は、物理パーティション６１－１内のソフトウェアを示す。
物理パーティション６１－１内の各論理ドメイン＃０～＃３で、OS４０１－ｍが稼動している。
OS４０１－１～４０１－４は、それぞれ論理ドメイン２０１－１～２０１－４のオペレーティングシステムに対応する。
【００３５】
図４は、実施の形態に係るファームウェアの詳細な構成図である。
ファームウェア３１１は、ダンプ対象領域情報/HVダンプフラグ格納処理部３１２、ダンプ対象領域情報/HVダンプフラグ格納領域３１３、HVダンプフラグ設定部３１４、メモリ初期化処理部３１５、HV使用領域変更部３１６、HV再起動命令部３１７、ダンプ対象領域情報/HVダンプフラグ通知部３１８、PA-RAマッピング通知部３１９、メモリ開放処理部

３２０、HVダンプフラグリセット処理部３２１を備える。
【００３６】
ダンプ対象領域情報/HVダンプフラグ格納処理部３１２は、ダンプ対象領域情報およびHVダンプフラグをダンプ対象領域情報/HVダンプフラグ格納領域３１３に格納する。
ダンプ対象領域情報/HVダンプフラグ格納領域３１３は、ダンプ対象領域情報およびHVダンプフラグが格納される領域である。ここでダンプ対象領域情報は、ダンプ対象領域を示す情報であり、ダンプ対象領域の開始アドレス（PA Base）およびサイズの情報を含む。HVダンプフラグは、ハイパーバイザが使用していたメモリ領域のダンプファイルを生成するか否かを示す制御情報である。また、HVダンプフラグは、稼動中のハイパーバイザのメモリダンプを採取するか否かを示す情報（HVライブダンプフラグ）を含むこともできる。
【００３７】
HVダンプフラグ設定部３１４は、HVダンプフラグの値を設定する。例えば、HVダンプフラグ設定部３１４は、HVダンプを行なう場合にHVダンプフラグをTRUEに設定する。
メモリ初期化処理部３１５は、メモリの初期化を行う。
【００３８】
HV使用領域変更部３１６は、ハイパーバイザ３５１が使用するメモリの領域を変更する。
HV再起動命令部３１７は、ハイパーバイザ３５１に再起動を指示する。
【００３９】
ダンプ対象領域情報/HVダンプフラグ通知部３１８は、ダンプ対象領域情報およびHVダンプフラグを通知する。
PA-RAマッピング通知部３１９は、OSの処理に必要なPA-RAマッピングをハイパーバイザ３５１へ通知し、ハイパーバイザ３５１のPA-RAマッピング処理部３６８は、通知されたPA-RAマッピングを用いて物理アドレス(PA)から実アドレス(RA)への、あるいは実アドレス(RA)から物理アドレス(PA)への変換を行う。
【００４０】
メモリ開放処理部３２０は、メモリの開放処理を行う。
HVダンプフラグリセット処理部３２１は、HVダンプフラグをリセットする。詳細には、HVダンプフラグリセット処理部３２１は、HVダンプフラグをFALSEに設定する。
【００４１】
図５は、実施の形態に係るハイパーバイザの詳細な構成図である。
ハイパーバイザ３５１は、ドメイン緊急停止指示部３５２、OSパニック指示部３５３、HVダンプ対象領域通知処理部３５４、HVダンプ対象領域情報/HVダンプフラグ格納処理部３５５、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６、HV再起動処理部３５７、OS再起動命令部３５８、HVメモリダンプフラグ読出・送信部３５９、HVダンプ対象領域読出処理部３６０、メモリ管理部３６１、メモリ開放処理部３６２、HVダンプフラグリセット処理部３６３、HVダンプフラグ通知部３６４、ダンプ専用ドメイン起動処理部３６５、カーネルダンプ対象領域情報/カーネルダンプフラグ格納処理部３６６、カーネルダンプ対象領域情報/カーネルダンプフラグ格納領域３６７、PA-RAマッピング処理部３６８、PA-RAマッピング情報格納域３６９、割り込み処理部３７０、メモリダンプ処理起動部３７１、メモリ初期化処理部３７２、およびカーネルダンプフラグリセット処理部３７３を備える。
【００４２】
ドメイン緊急停止指示部３５２は、ドメイン２０１に緊急停止を指示する。
OSパニック指示部３５３は、OS４０１に緊急停止（パニック）を指示する。
HVダンプ対象領域通知処理部３５４は、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６からHVダンプ対象領域情報を読み出して通知する。
【００４３】
HVダンプ対象領域情報/HVダンプフラグ格納処理部３５５は、HVダンプ対象領域情報お

よびHVダンプフラグをHVダンプ対象領域情報/HVダンプフラグ格納領域３５６に格納する。

【００４４】

HVダンプ対象領域情報/HVダンプフラグ格納領域３５６は、HVダンプ対象領域情報およびHVダンプフラグを格納する。HVダンプ対象領域情報は、ハイパーバイザ３５１が使用しているメモリ領域（HVダンプ対象領域）を示す情報であり、メモリ領域の開始アドレス（PA Base）およびサイズの情報を含む。HVダンプフラグは、ハイパーバイザが使用していたメモリ領域のダンプファイルを生成するか否かを示す制御情報である。

【００４５】

HV再起動処理部３５７は、ハイパーバイザ３５１を停止させ、ハイパーバイザ３５１の再起動を行う。

OS再起動命令部３５８は、OS４０１に再起動を指示する。

【００４６】

HVメモリダンプフラグ読出・送信部３５９は、HVダンプフラグを読み出して送信する。

HVダンプ対象領域読出処理部３６０は、HVダンプ対象領域情報で示されるメモリ領域の内容を読み出し、送信する。または、HVダンプ対象領域読出処理部３６０は、現在のハイパーバイザ３５１が使用しているメモリ領域の内容を読み出し、送信する。

【００４７】

メモリ管理部３６１は、メモリを管理する。

メモリ開放処理部３６２は、メモリの開放処理を行う。

HVダンプフラグリセット処理部３６３は、HVダンプフラグをリセットする。詳細には、HVダンプフラグリセット処理部３６３は、例えば、HVダンプフラグをFALSEに設定する。

【００４８】

HVダンプフラグ通知部３６４は、HVダンプフラグを通知する。

ダンプ専用ドメイン起動処理部３６５は、ダンプ専用ドメインをファームウェアモードで起動する。ファームウェアモードとは、OSを起動しないモード、すなわちOSを起動する前に停止するモードである。

【００４９】

カーネルダンプ対象領域情報/カーネルダンプフラグ格納処理部３６６は、カーネルダンプ対象領域情報およびカーネルダンプフラグをカーネルダンプ対象領域情報/カーネルダンプフラグ格納領域３６７に格納する。

【００５０】

カーネルダンプ対象領域情報/カーネルダンプフラグ格納領域３６７は、カーネルダンプ対象領域情報およびカーネルダンプフラグを格納する。カーネルダンプ対象領域情報は、パニック時にOS４０１のカーネルが使用していたメモリ領域（カーネルダンプ対象領域）を示す情報であり、メモリ領域の開始アドレス（RA Base）およびサイズの情報を含む。カーネルダンプフラグは、OS４０１のカーネルのメモリダンプを実行するか否かを示す情報である。さらに、カーネルダンプフラグは、どのような方法でカーネルのメモリダンプを採取するかを示すこともできる。カーネルダンプフラグは、例えば、０：カーネルのメモリダンプを採取しない、１：ダンプ採取用ドメインで採取、または２：メモリDynamic Reconfiguration機能を用いて採取というような情報である。カーネルダンプフラグは、OS４０１から受信しても良いし、ハイパーバイザ３５１が予め設定して保持していても良い。

【００５１】

PA-RAマッピング処理部３６８は、物理アドレス（ＰＡ）とリアルアドレス（ＲＡ）間のマッピングを行う。ＰＡはメモリの物理アドレスであり、ＲＡはドメイン（オペレーティングシステム）上の実アドレスである。

【００５２】

PA-RAマッピング情報格納域３６９は、ＰＡとＲＡ間のマッピングの情報を格納する。

割り込み処理部３７０は、OS４０１のカーネルのメモリダンプをする場合にＳ４０１に

対して、割り込み処理させる。割り込み処理が受け付けられるとOS４０１のカーネルのメモリダンプが可能と判断されてOS４０１のカーネルのメモリダンプ処理に進み、受け付けられないと割り込み出来ないと判断してOS４０１のカーネルのメモリダンプ処理はせずに終了する。

【００５３】

メモリダンプ処理起動部３７１は、制御ドメイン２０１－１にハイパーバイザ３５１のメモリダンプ処理を起動させる。

メモリ初期化処理部３７２は、メモリの初期化を行う。

【００５４】

カーネルダンプフラグリセット処理部３７３は、カーネルダンプフラグをリセットする。例えば、カーネルダンプフラグリセット処理部３７３は、カーネルダンプフラグを削除または“０：カーネルのメモリダンプを採取しない”に設定する。

【００５５】

図６は、実施の形態に係るOSの詳細な構成図である。

OS４０１－mは、メモリ管理部４０２－m、ファイル管理部４０３－m、プロセス管理部４０４－m、割り込み処理部４０５－m、マッピング情報抽出・格納処理部４０６－m、マッピング情報格納領域４０７－m、HVメモリダンプ判断部４０８－m、OS起動処理部４０９－m、HVダンプ対象領域読出処理部の呼び出し部４１０－m、カーネルダンプ対象メモリ読出処理部４１１－m、HVダンプ採取処理部４１２－m、カーネルダンプ採取処理部４１３－m、パニック処理部４１４－m、カーネルダンプ対象領域通知処理部４１５－m、メモリDR組み込み処理部４１６－m、メモリDR切り離し処理部４１７－m、空きメモリ追加処理部４１８－m、ダンプ専用ドメイン停止処理部４１９－m、カーネルダンプフラグリセット処理部４２０－m、およびカーネルダンプフラグ通知部４２１－mを備える。

【００５６】

メモリ管理部４０２－mは、OS４０１－mが使用するメモリ２０３－mを割り当てる。

ファイル管理部４０３－mは、ディスク上に格納されたデータであるファイルを管理する。

【００５７】

プロセス管理部４０４－mは、OS４０１－mが実行するプログラムのプロセスを管理する。

割り込み処理部４０５－mは、割り込み処理を行う。

【００５８】

マッピング情報抽出・格納処理部４０６－mは、メモリ２０３－mのダンプを取得および解析するために必要な情報を、マッピング情報格納領域４０７－mに格納する。

マッピング情報格納領域４０７－mは、メモリ２０３－mのダンプを取得および解析するために必要な情報を格納する。マッピング情報格納領域４０７－mが格納する情報は、例えば、カーネルのテキスト域、データ域、ヒープ域、スタック域等、各セグメントのマッピング情報(論理アドレス、物理アドレス、サイズ等)やアドレス変換テーブル、ページテーブル等、各種制御テーブルのマッピング情報である。

【００５９】

HVメモリダンプ判断部４０８－mは、HVダンプフラグがTRUEまたはFALSEであるか判定し、ハイパーバイザのメモリダンプを行うか判断する。

OS起動処理部４０９－mは、OS４０１－mを再起動する。

【００６０】

HVダンプ対象領域読出処理部の呼び出し部４１０－mは、HVダンプ対象領域読出処理部３６０を呼び出す。

カーネルダンプ対象メモリ読出処理部４１１－mは、カーネルダンプ対象領域（パニック時にOS４０１－mのカーネルが使用していたメモリ領域）のメモリ内容を読み出す。

【００６１】

HVダンプ採取処理部４１２－ｍは、HVダンプ対象領域読出処理部３６０からHVダンプ対象領域読出処理部３６０が読み出したメモリ内容を受信し、ダンプファイルを生成する。
カーネルダンプ採取処理部４１３－ｍは、読み出したカーネルダンプ対象領域のメモリ内容をファイルに保存（ダンプファイルを生成）する。

【００６２】

パニック処理部４１４－ｍは、ドメイン２０１－ｍを緊急停止（パニック）させる。
カーネルダンプ対象領域通知処理部４１５－ｍは、パニック時にOS４０１－ｍのカーネルが使用しているメモリ領域をハイパーバイザ３５１に通知する。

【００６３】

メモリDR組み込み処理部４１６－ｍは、ドメイン２０１－ｍにメモリ領域を組み込む。
メモリDR切り離し処理部４１７－ｍは、ドメイン２０１－ｍからメモリ領域を切り離す。

【００６４】

空きメモリ追加処理部４１８－ｍは、メモリ管理部４０２－ｍにダンプ済みのメモリ領域を通知する。
ダンプ専用ドメイン停止処理部４１９－ｍは、ダンプを採取した後にダンプを採取するドメイン（ダンプ専用ドメイン）を停止する。

【００６５】

カーネルダンプフラグリセット処理部４２０－ｍは、ハイパーバイザ３５１にカーネルダンプフラグのリセットを指示する。
カーネルダンプフラグ通知部４２１－ｍは、ハイパーバイザ３５１にカーネルダンプフラグを通知する。カーネルダンプフラグ通知部４２１－ｍは、カーネルのメモリダンプを実行する必要がある場合にカーネルダンプフラグをハイパーバイザ３５１に通知する。例えば、カーネルダンプフラグ通知部４２１－ｍは、カーネルのメモリダンプを採取しない場合はカーネルダンプフラグの値を“０：カーネルのメモリダンプを採取しない”、ダンプ採取用ドメインでカーネルのメモリダンプを採取する場合にカーネルダンプフラグの値を“１：ダンプ採取用ドメインで採取”、メモリDynamic Reconfiguration機能を用いてカーネルのメモリダンプを採取する場合にカーネルダンプフラグの値を“２：メモリDynamic Reconfiguration機能を用いて採取”とする。

【００６６】

（第１の実施の形態）
第１の実施の形態では、制御ドメインを用いてハイパーバイザのメモリダンプを採取する。

【００６７】

図７Ａ、７Ｂは、第１の実施の形態に係るメモリダンプ生成処理のフローチャートである。
初期状態において、ドメイン２０１－１～２０１－３およびＯＳ４０１－１～４０１－３は、起動され運用状態となっており、ドメイン２０１－４およびＯＳ４０１－４は起動されていないものとする。

【００６８】

ステップＳ５０１において、ハイパーバイザ３５１は、致命的なエラーを検出する。
ステップＳ５０２において、ドメイン緊急停止指示部３５２は、運用状態の論理ドメイン、すなわち制御ドメイン２０１－１およびドメイン２０１－２、２０１－３に緊急停止を指示する。

【００６９】

ステップＳ５０３において、OS４０１－ｉ（ｉ＝１～３）は、緊急停止指示を受信し、OS４０１－ｉを緊急停止させる。
ステップＳ５０４において、HVダンプ対象領域通知処理部３５４は、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６からHVダンプ対象領域情報を読み出し、ファームウェア３１１に通知する。HVダンプ対象領域情報は、ハイパーバイザ３５１が使用している

メモリ領域（ダンプ対象領域）を示す情報であり、メモリ領域の開始アドレス（PA Base）およびサイズの情報を含む。HVダンプ対象領域情報は、図８に示すような形式であり、ブロックの番号、ブロックの物理メモリの開始アドレス（PA Base）、およびブロックのサイズが対応付けられている。また、HV再起動処理部３５７は、ハイパーバイザ３５１を停止する（HVアボート）。

【００７０】

ステップＳ５０６において、ダンプ対象領域情報/HVダンプフラグ格納処理部３１２は、HVダンプ対象領域情報を受信する。

ステップＳ５０７において、ダンプ対象領域情報/HVダンプフラグ格納処理部３１２は、受信したHVダンプ対象領域情報をダンプ対象領域情報として、ダンプ対象領域情報/HVダンプフラグ格納領域３１３に格納する。また、HVダンプフラグ設定部３１４は、HVダンプフラグをTUREに設定し、ダンプ対象領域情報/HVダンプフラグ格納領域３１３に格納する。

【００７１】

ステップＳ５０８において、ファームウェア３１１は、メモリの内容を保持したまま、物理パーティションの再起動処理を開始する。

ステップＳ５０９において、メモリ初期化処理部３１５は、メモリの初期化処理を開始する。先ず、例えば、メモリの先頭のアドレスを初期化処理対象の領域として設定する。

【００７２】

ステップＳ５１０において、メモリ初期化処理部３１５は、ダンプ対象領域情報を参照し、初期化処理対象の領域がダンプ対象領域情報で指定される領域、すなわちダンプ対象領域であるか否か判定する。初期化処理対象の領域がダンプ対象領域である場合、初期化処理対象の領域の内容を保持したまま、制御はステップＳ５１２に進み、ダンプ対象領域でない場合、制御はステップＳ５１１に進む。

【００７３】

ステップＳ５１１において、メモリ初期化処理部３１５は、初期化処理対象の領域を初期化する。

ステップＳ５１２において、メモリ初期化処理部３１５は、ダンプ対象領域以外のすべての領域に対する初期化処理を行ったか判定する。ダンプ対象領域以外のすべての領域に対する初期化処理を行った場合、制御はステップＳ５１３に進み、ダンプ対象領域以外のすべての領域に対する初期化処理を行っていない場合、未処理の領域（例えば、ダンプ対象領域であるかチェック済みの領域の次のアドレス）を初期化処理対象の領域とし、制御はステップＳ５１０に戻る。

【００７４】

ステップＳ５１３において、HV使用領域変更部３１６は、ハイパーバイザ３５１が使用する領域をダンプ対象領域情報で示される領域以外の領域に変更する。なお、初期化処理対象の領域として、少なくともハイパーバイザ３５１が使用する変更後の領域を初期化対象としてもよい。

【００７５】

ステップＳ５１４において、HV再起動命令部３１７は、ハイパーバイザ３５１に再起動を指示する。ダンプ対象領域情報/HVダンプフラグ通知部３１８は、ダンプ対象領域情報/HVダンプフラグ格納領域３１３からダンプ対象領域情報およびHVダンプフラグを読み出し、ハイパーバイザ３５１に通知する。

【００７６】

ステップＳ５１５において、HVダンプ対象領域情報/HVダンプフラグ格納処理部３５５は、ダンプ対象領域情報およびHVダンプフラグを受信し、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６に格納する。尚、HVダンプ対象領域情報/HVダンプフラグ格納処理部３５５は、受信したダンプ対象領域情報をHVダンプ対象領域情報として格納する。

【００７７】

ステップＳ５１６において、HV再起動処理部３５７は、ハイパーバイザ３５１を再起動

する。ただし、HVダンプ対象領域情報で指定されるメモリ領域は使用しない。
ステップＳ５１７において、OS再起動命令部３５８は、OS４０１－１～４０１－３に再起動を指示する。
【００７８】
ステップＳ５１８において、OS再起動処理部４０９－２、４０９－３は、それぞれOS４０１－２、４０１－３を再起動する。
ステップＳ５１９において、OS４０１－２、４０１－３は、業務を再開する。
【００７９】
ステップＳ５２０において、OS４０１－２、４０１－３は、通常の運用状態となる。
ステップＳ５２１において、OS再起動処理部４０９－１は、OS４０１－１を再起動する。
【００８０】
ステップＳ５２２において、OS４０１－１は、業務を再開する。
ステップＳ５２３において、HVメモリダンプ判断部４０８－１は、ハイパーバイザ３５１にHVダンプフラグの送信を要求する。
【００８１】
ステップＳ５２４において、HVメモリダンプフラグ読出・送信部３５９は、要求を受信すると、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６からHVダンプフラグを読み出し、OS４０１－１に送信する。
【００８２】
ステップＳ５２５において、HVメモリダンプ判断部４０８－１は、HVダンプフラグを受信し、HVダンプフラグがTRUEであるか否か判定する。HVダンプフラグがTRUEの場合、制御はステップＳ５２７に進み、FALSEの場合、制御はステップＳ５３１に進む。
【００８３】
ステップＳ５２６において、HVダンプ対象領域読出処理部の呼び出し部４１０－１は、HVダンプ対象領域読出処理部３６０を呼び出す。
ステップＳ５２７において、HVダンプ対象領域読出処理部３６０は、HVダンプ対象領域情報で示されるメモリ領域の内容を読み出し、制御ドメインに送信する。
【００８４】
ステップＳ５２８において、HVダンプ採取処理部４１２－１は、HVダンプ対象領域読出処理部３６０からHVダンプ対象領域読出処理部３６０が読み出したメモリ内容を受信し、受信したメモリ内容をファイルに書き出してダンプファイルを生成する。以下、ステップＳ５２９、Ｓ５３０とステップＳ５３１の処理が並列に実行される。
【００８５】
ステップＳ５２９において、メモリ開放処理部３６２は、HVダンプ対象領域情報で指定されるメモリ領域を開放する。また、HVダンプフラグリセット処理部３６３は、HVダンプフラグをリセット、すなわちFALSEに設定する。HVダンプフラグ通知部３６４は、ファームウェア３１１にHVダンプフラグを通知する。
【００８６】
ステップＳ５３０において、メモリ開放処理部３２０は、ダンプ対象領域情報をクリアする。また、HVダンプフラグリセット処理部３２１は、HVダンプフラグをリセット、すなわちFALSEに設定する。
【００８７】
ステップＳ５３１において、OS４０１－１は、通常の運用状態となる。
第１の実施の形態に係るメモリダンプ生成処理によれば、エラーを検出してハイパーバイザおよびオペレーティングシステムを再起動する場合、メモリダンプのサイズが大きい場合でも別のメモリ等にコピーを行っていないので、速やかにハイパーバイザおよびオペレーティングシステムを再起動できる。これにより、業務停止時間を短縮することができる。
【００８８】

ここで、第１の実施の形態に係るメモリダンプ生成処理の変形例について説明する。
変形例では、稼動中のハイパーバイザのメモリダンプの採取（ハイパーバイザのライブダンプと呼ぶ）が行われる。
【００８９】
図７Ｃは、第１の実施の形態に係るメモリダンプ生成処理の変形例のフローチャートである。
変形例のフローチャートは、図７Ａ、７Ｂの第１の実施の形態に係るメモリダンプ生成処理のフローチャートにステップＳ５３２、Ｓ５３３が追加され、ステップＳ５２５においてＮＯと判定された場合に、制御がステップＳ５３２に進むものである。
【００９０】
図７Ｃでは、図７Ａ、７Ｂに対する変更箇所について記載し、その他の部分については同様であるため記載は省略されている。
変形例において、例えば、HVダンプフラグのデータ構造を０：採取せず、１：異常時のHVダンプ、２：HVライブダンプのように変更することができる。HVメモリダンプ判断部４０８－１は、HVダンプフラグが１の場合、HVダンプフラグがTRUEと判定し、HVダンプフラグが０または２の場合、HVダンプフラグがFALSEと判定する。また、HVメモリダンプ判断部４０８－１は、HVダンプフラグが２の場合、HVダンプライブフラグがTRUEと判定する。
【００９１】
ステップＳ５３２において、HVメモリダンプ判断部４０８－１は、HVライブダンプフラグがTRUEであるか否か判定する。HVダンプフラグがTRUEの場合（すなわち、HVダンプフラグが２の場合）、制御はステップＳ５３３に進み、FALSEの場合、制御はステップＳ５３１に進む。
【００９２】
ステップＳ５３３において、HVライブダンプ処理が行われる。詳細には、HVダンプ対象領域読出処理部の呼び出し部４１０－１は、HVダンプ対象領域読出処理部３６０を呼び出す。HVダンプ対象領域読出処理部３６０は、稼動中のハイパーバイザ３５１が使用しているメモリ領域の内容を読み出し、制御ドメインに送信する。HVダンプ採取処理部４１２－１は、HVダンプ対象領域読出処理部３６０が読み出したメモリ内容を受信し、受信したメモリ内容をファイルに書き出してハイパーバイザのダンプファイルを生成する。
【００９３】
上記のように、稼動中のハイパーバイザのメモリダンプの採取では、ハイパーバイザを停止・再起動しないまま、ハイパーバイザが使用するメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出している。
【００９４】
（第２の実施の形態）
第２の実施の形態では、ハイパーバイザのメモリダンプに加えて、OSのカーネルのメモリダンプを行う。
【００９５】
図９Ａ、９Ｂ、９Ｃは、第２の実施の形態に係るメモリダンプ生成処理のフローチャートである。
初期状態において、ドメイン２０１－１～２０１－３およびＯＳ４０１－１～４０１－３は、起動され運用状態となっており、ドメイン２０１－４およびＯＳ４０１－４は起動されていないものとする。
【００９６】
ステップＳ６０１において、ハイパーバイザ３５１に致命的なエラーが発生する。
ステップＳ６０２において、ハイパーバイザ３５１は、致命的なエラーを検出する。
ステップＳ６０３において、割り込み処理部３７０は、運用状態のＯＳ、すなわちOS４０１－ｉ（ｉ＝１～３）に割り込み処理を通知し、OSパニック指示部３５３は、OS４０１－ｉにパニックを指示する。
【００９７】

ステップＳ６０４において、パニック処理部４１４－ｉは、パニック指示を受信し、OS４０１－ｉをパニックさせる。

ステップＳ６０５において、カーネルダンプ対象領域通知処理部４１５－ｉは、ハイパーバイザ３５１にカーネルダンプ対象領域情報を通知する。カーネルダンプ対象領域情報は、OS４０１－ｉのカーネルが使用しているメモリ領域（ダンプ対象領域）を示す情報であり、メモリ領域の開始アドレス（RA Base）およびサイズの情報を含む。カーネルダンプ対象領域情報は、図１０に示すような形式であり、ブロックの番号、ブロックのメモリの開始アドレス（RA Base）、およびブロックのサイズが対応付けられている。

【００９８】

尚、ステップＳ６０４およびＳ６０５は、パニック指示を受信した論理ドメインごとにそれぞれ実行される。

ステップＳ６０６において、PA-RAマッピング処理部３６８は、通知された開始アドレス（RA Base）をRA BaseからPA Baseの開始アドレス（PA Base）に変換するRA-PA変換を行う。

【００９９】

ステップＳ６０７において、HVダンプ対象領域通知処理部３５４は、ハイパーバイザ３５１が使用しているメモリ領域を示すHVダンプ対象領域情報をファームウェア３１１に通知する。さらに、HVダンプ対象領域通知処理部３５４は、OS４０１－ｉから受信したカーネルダンプ対象領域情報をファームウェア３１１に通知する。尚、通知されるカーネルダンプ対象領域情報は、RA BaseからPA Baseに変換された開始アドレス（PA Base）およびサイズを含む。実施の形態では、停止した論理ドメインに対応する３個のカーネルダンプ対象領域情報が通知される。

【０１００】

ステップＳ６０８において、ダンプ対象領域情報/HVダンプフラグ格納処理部３１２は、受信したHVダンプ対象領域情報および受信したカーネルダンプ対象領域情報をダンプ対象領域情報として、ダンプ対象領域情報/HVダンプフラグ格納領域３１３に格納する。また、HVダンプフラグ設定部３１４は、HVダンプフラグをTUREに設定し、ダンプ対象領域情報/HVダンプフラグ格納領域３１３に格納する。

【０１０１】

ステップＳ６０９において、HV再起動処理部３５７は、ハイパーバイザ３５１を停止する（HVアボート）。

ステップＳ６１０において、メモリ初期化処理部３１５は、ダンプ対象領域情報で示される領域以外のメモリ領域を初期化する。すなわち、メモリ初期化処理部３１５は、ハイパーバイザ３５１が使用していた領域とパニック時にOS４０１－ｉのカーネルが使用していた領域以外のメモリ領域を初期化する。

【０１０２】

ステップＳ６１１において、HV使用領域変更部３１６は、HV使用領域変更部３１６は、ハイパーバイザ３５１が使用する領域をダンプ対象領域情報で示される領域以外の領域に変更する。HV再起動命令部３１７は、ハイパーバイザ３５１に再起動を指示する。ダンプ対象領域情報/HVダンプフラグ通知部３１８は、ダンプ対象領域情報/HVダンプフラグ格納領域３１３からダンプ対象領域情報およびHVダンプフラグを読み出し、ハイパーバイザ３５１に通知する。ダンプ対象領域情報には、HVダンプ対象領域情報およびカーネルダンプ対象領域情報が含まれている。HVダンプ対象領域情報/HVダンプフラグ格納処理部３５５は、ダンプ対象領域情報の内のHVダンプ対象領域情報およびHVダンプフラグを受信し、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６に格納する。カーネルダンプ対象領域情報/カーネルダンプフラグ格納処理部３６６は、ダンプ対象領域情報の内のカーネルダンプ対象領域情報を受信し、カーネルダンプ対象領域情報/カーネルダンプフラグ格納領域３６７に格納する。

【０１０３】

ステップＳ６１２において、HV再起動処理部３５７は、ハイパーバイザ３５１を起動す

る。
ステップＳ６１３において、メモリ初期化処理部３７２は、カーネルダンプ対象領域情報で示される領域以外のメモリ領域を初期化する。
【０１０４】
ステップＳ６１４において、PA-RAマッピング処理部３６８、ＯＳ再起動命令部３５８、およびダンプ専用ドメイン起動処理部３６５は、カーネルダンプフラグの値をチェックする。以下、カーネルダンプフラグの値に応じた処理が実行される。例えばPA-RAマッピング処理部３６８は、カーネルダンプフラグが“１：ダンプ採取用ドメインで採取”の場合、パニック発生時にＯＳ４０１－１～４０１－３のカーネルが使用していたメモリのPAをダンプ採取用ドメイン２０４－４のRAに割り当てる。
【０１０５】
以下、ステップＳ６２１、ステップＳ６２２～Ｓ６２６、およびステップＳ６３２～Ｓ６３５の処理が別々に並列して実行される。
ただし、カーネルダンプフラグが“１：ダンプ採取用ドメインで採取”の場合、ステップＳ６２６、Ｓ６３５は実行されず、“２：メモリDynamic Reconfiguration機能を用いて採取”の場合、ステップＳ６２１は実行されない。
【０１０６】
ここでは、ステップＳ６２１は、ダンプ採取用ドメイン２０４－４に関する処理であり、ステップＳ６２２～Ｓ６２６は、制御ドメイン２０４－１に関する処理であり、ステップＳ６３２～Ｓ６３５は、論理ドメイン２０４－２、２０４－３に関する処理である。
【０１０７】
ステップＳ６２１において、ダンプ採取用ドメインによるカーネルのメモリダンプ生成処理が行われる。ダンプ採取用ドメインによるカーネルのメモリダンプ生成処理の詳細については後述する。
【０１０８】
ステップＳ６２２において、PA-RAマッピング処理部３６８は、ドメイン２０１－１の物理アドレス(PA)とリアルアドレス(RA)間のマッピングを以下の1)、2)のように変更する。それにより、OS４０１－１を再起動してもパニック時のカーネルおよびパニック時のハイパーバイザ３５１が使用していたメモリ領域のデータは上書きされなくなる。
1)パニック発生時にカーネルおよびハイパーバイザが使用していたメモリの物理アドレスは、再起動するドメインのリアルアドレスに割り当てないようにする。かつ、
2)再起動前後で、該当ドメインが使用できるメモリサイズがなるべく変化しないようにする。
【０１０９】
ただし、再起動するドメインに割り当て可能な物理メモリが所定値より不足する場合は、1)を優先する。
尚、パニック発生時にどの領域をカーネルおよびハイパーバイザ３５１が利用していたかは、HVダンプ対象領域情報およびカーネルダンプ対象領域情報を参照することにより判断される。
【０１１０】
ステップＳ６２３において、OS再起動命令部３５８は、OS４０１－１に再起動を指示する。また、OS再起動命令部３５８は、カーネルダンプフラグが“２：メモリDynamic Reconfiguration機能を用いて採取”の場合、メモリDR機能を用いたケーネルのメモリダンプ生成処理を行う旨を再起動指示に含める。指示を受信したOS起動処理部４０９－１は、OS４０１－１を起動する。
【０１１１】
ステップＳ６２４において、OS４０１－１は、業務を再開する。
ステップＳ６２５において、メモリDynamic Reconfiguration（DR）機能を用いたカーネルのメモリダンプ生成処理が行われる。メモリDR機能を用いたカーネルのメモリダンプ生成処理の詳細については後述する。　ステップＳ６２６において、ハイパーバイザのメ

モリダンプ生成処理が行われる。ステップＳ６２６は、図７Ｂのステップ５２３～Ｓ５３１の処理と同様であるため説明は省略する。

【０１１２】

ステップＳ６３２において、PA-RAマッピング処理部３６８は、ドメイン２０１－２，２０１－３の物理アドレス(PA)とリアルアドレス(RA)間のマッピングを以下の1)、2)のように変更する。それにより、OS４０１－１を再起動してもパニック時のカーネルおよびパニック時のハイパーバイザ３５１が使用していたメモリ領域のデータは上書きされなくなる。

1)パニック発生時にカーネルおよびハイパーバイザが使用していたメモリの物理アドレスは、再起動するドメインのリアルアドレスに割り当てないようにする。かつ、

2)再起動前後で、該当ドメインが使用できるメモリサイズがなるべく変化しないようにする。

【０１１３】

ただし、再起動するドメインに割り当て可能な物理メモリが所定値より不足する場合は、1)を優先する。

尚、パニック発生時にどの領域をカーネルおよびハイパーバイザ３５１が利用していたかは、HVダンプ対象領域情報およびカーネルダンプ対象領域情報を参照することにより判断される。

【０１１４】

ステップＳ６３３において、OS再起動命令部３５８は、OS４０１－２、４０１－３に再起動を指示する。また、OS再起動命令部３５８は、カーネルダンプフラグが“２：メモリDynamic Reconfiguration機能を用いて採取”の場合、メモリDR機能を用いたケーネルのメモリダンプ生成処理を行う旨を再起動指示に含める。指示を受信したOS起動処理部４０９－２、４０９－３は、OS４０１－２，４０１－３をそれぞれ起動する。

【０１１５】

ステップＳ６３４において、OS４０１－２，４０１－３は、それぞれ業務を再開する。

ステップＳ６３５において、メモリDR機能を用いたカーネルのメモリダンプ生成処理が行われる。

【０１１６】

以下、カーネルのメモリダンプ生成処理の詳細について説明する。

カーネルのメモリダンプ生成処理は、（１）ダンプ採取用ドメインによるメモリダンプを採取する方法（ステップＳ６２１）、または（２）メモリDynamic Reconfiguration機能を用いてメモリダンプを採取する方法（ステップＳ６２６、Ｓ６３５）のいずれかが用いられる。

【０１１７】

（１）ダンプ採取用ドメインでメモリダンプを採取する方法

ダンプ採取用ドメイン２０１－４は、複数のドメイン２０１が存在するシステムでも、それぞれの論理ドメイン毎に用意する必要はなく、システムで1つあれば良い。ダンプ採取用ドメイン２０１－４が1つの場合、複数の論理ドメイン２０１で同時にパニックが発生した場合は１ドメインずつメモリダンプを採取することになるが、ダンプ採取が完了しているかどうかにかかわらず、速やかに業務が再開できるため、業務への影響はない。

【０１１８】

ダンプ採取用ドメイン２０１－４では、パニックが発生した論理ドメインの業務を引き継ぐ必要はないため、メモリダンプを採取するために必要となる下記のハードウェア資源があれば良い。

・パニックが発生した論理ドメインのOSのカーネルがパニック時に使用していた物理メモリ領域
・1個以上のCPU
・ダンプファイルを格納するディスクとディスクを使用するために必要なI/O資源

【０１１９】

図１１は、ダンプ採取用ドメインによるカーネルのメモリダンプ生成処理のフローチャートである。
図１１は、図９Ｂのステップ６２１に対応する。
【０１２０】
ここでは、ＯＳ４０１－ｉのカーネルのメモリダンプ生成処理について説明する。
ステップＳ６５１において、ダンプ専用ドメイン起動処理部３６５は、ダンプ採取用ドメイン２０１－４をファームウェアモードで起動する。ファームウェアモードとは、OSを起動しないモード、すなわちOSを起動する前に停止するモードである。OSを起動しないことにより、ダンプ対象領域が書き換えられてしまうことを防ぐ。
【０１２１】
ステップＳ６５２において、カーネルダンプ対象メモリ読出処理部４１１－４は、パニック発生時にオペレーティングシステム４０１－ｉのカーネルが使用していたメモリ領域（カーネルダンプ対象領域）を読み出す。尚、カーネルダンプ対象領域の情報（開始アドレス（RA Base）やサイズ等）は、ファームウェア３１１またはハイパーバイザ３５１からの通知により得る。
【０１２２】
ステップＳ６５３において、カーネルダンプ採取処理部４１３－４は、読み出したメモリ内容をファイルに書き出してダンプファイルを生成する。
ステップＳ６５４において、ダンプ専用ドメイン停止処理部４１９－４は、ダンプ採取ドメイン２０１－４を停止する。そして、ダンプ専用ドメイン停止処理部４１９－４は、カーネルダンプ対象領域を使用可能な未使用のメモリ、すなわち空きメモリとするようにハイパーバイザ３５１のメモリ管理部３６１へ通知する。また、カーネルダンプフラグリセット処理部４２０－４は、ハイパーバイザ３５１にカーネルダンプフラグのリセットを指示する。リセット指示を受信したカーネルダンプフラグリセット処理部３７３は、カーネルダンプフラグをリセットする。
【０１２３】
ステップＳ６５５において、メモリ管理部３６１は、カーネルダンプ対象領域を他の論理ドメイン２０１－ｉからも使用可能な空きメモリとする。
【０１２４】
図１２は、ダンプ採取用ドメインによるメモリダンプの採取を示す図である。
図１２の左側は運用状態（およびパニック時）、真ん中は再起動時、右側はダンプ採取用ドメインによるメモリダンプの採取時を示す。
ここでは、論理ドメイン２０１－１の処理について記載している。尚、ドメイン２０１－２、２０１－３においても同様の処理が実行されるので、詳細は省略する。
【０１２５】
図１２の左側の運用状態において、ＰＡのある領域が論理ドメイン２０１－１のＲＡのある領域にマッピングされている。
OS４０１－１のパニック時にOS４０１－１のカーネルが使用していた領域はカーネルダンプ対象領域となる。
【０１２６】
OS４０１－１のパニック後、PA-RAマッピングの変更が行われ（ステップＳ６２２）、論理ドメイン２０１－１には、パニック時にOS４０１－１のカーネルが使用していた領域（カーネルダンプ対象領域）とは異なるＰＡの領域が割り当てられ、OS４０１－１は再起動する（図１２の真ん中）。
【０１２７】
図１２の右側のダンプ時において、ダンプ採取専用ドメイン２０１－４のＲＡには、パニック時にOS４０１－１のカーネルが使用していたＰＡの領域（カーネルダンプ対象領域）が割り当てられる。ダンプ採取専用ドメイン２０１－４は、カーネルダンプ対象領域を読み出して、ダンプファイルを生成する。
【０１２８】

図１３は、ダンプ採取用ドメインによるメモリダンプの採取におけるPA-RAマッピング情報を示す図である。
図１３の左側は運用状態（およびパニック時）、真ん中はダンプ時、右側はダンプ後を示す。

【０１２９】
ここでは、ドメイン２０１－１（制御ドメイン＃０）とダンプ採取専用ドメイン２０１－４（ダンプ採取専用ドメイン＃３）のPA-RAマッピングについて記載している。
PA-RAマッピング情報は、ドメイン、開始アドレス（PA Base）、サイズ、および開始アドレス（RA Base）が対応付けられて記載されている。

【０１３０】
図１３の左側のパニック時において、開始アドレス（PA Base）がxxxxx、サイズが８ＧＢである領域が制御ドメイン＃０の開始アドレス（RA Base）がaaaaaである領域にマッピングされている（図１２の左側に対応）。この領域がカーネルダンプ対象領域となる。

【０１３１】
OS４０１－１のパニック後、PA-RAマッピングの変更が行われ（ステップＳ６２２）、PA-RAマッピング情報は図１３の真ん中に示すようになる。
図１３の真ん中のダンプ時において、開始アドレス（PA Base）がxxxxx、サイズが８ＧＢである領域がダンプ採取専用ドメイン＃３の開始アドレス（RA Base）がaaaaaである領域にマッピングされている。すなわち、パニック時の制御ドメイン＃０のＰＡの領域がダンプ採取専用ドメイン＃３のＲＡにマッピングされている。また、開始アドレス（PA Base）がyyyyy、サイズが８ＧＢである領域が制御ドメイン＃０の開始アドレス（PA Base）がaaaaaである領域にマッピングされている。すなわち、新たなＰＡの領域が再起動後の制御ドメイン＃０に割り当てられている（図１２の右側に対応）。

【０１３２】
ダンプファイルの生成後、カーネルダンプ対象領域は他のドメインからも使用可能な空きメモリとなる（ステップＳ６５５）。
すなわち、図１３の右側のダンプ後において、ダンプ採取専用ドメイン＃３のマッピング情報は削除される。

【０１３３】
ダンプ採取用ドメインでメモリダンプを採取する方法によれば、異常を検出したドメインではなく、別のドメインでダンプを採取するため、ダンプ採取処理中に再度異常を検出してハングアップする等の二次被害が発生する可能性が低くなる。

【０１３４】
ダンプ採取用ドメインでメモリダンプを採取する方法によれば、Capacity on Demand (CoD)のような、ユーザが使用したハードウェア資源(CPU、メモリ、ディスク等)の量や時間に応じて課金を行うシステムにおいて、ダンプ採取のために使用するハードウェア資源に対する課金を行わないようにすることが容易に実現でき、料金の適正化を図ることができる。

【０１３５】
（２）メモリDynamic Reconfiguration機能を用いてメモリダンプを採取する方法
ここでは、論理ドメイン２０１－１の処理（ステップＳ６２５）について説明する。尚、論理ドメイン２０１－２、２０１－３の処理（ステップＳ６３５）も同様の処理が実行されるので、詳細は省略する。

【０１３６】
図１４は、メモリDynamic Reconfiguration機能を用いたカーネルのメモリダンプ生成処理のフローチャートである。
図１４は、図９Ｃのステップ６２５に対応する。

【０１３７】
ステップＳ６４１において、メモリDR組み込み処理部４１６－１は、メモリのDynamic Reconfiguration機能を使用して、パニック発生時にOS４０１－１のカーネルが使用して

いたメモリ領域（カーネルダンプ対象領域）をドメイン２０１－１に組み込む。なお、カーネルダンプ対象領域の情報（開始アドレス（RA Base）やサイズ等）は、ファームウェア３１１またはハイパーバイザ３５１からの通知により得る。

【０１３８】

ステップＳ６４２において、カーネルダンプ対象メモリ読出処理部４１１－１は、組み込んだメモリ領域を読み出す。

ステップＳ６４３において、カーネルダンプ採取処理部４１３－１は、読み出したメモリ内容をファイルに書き出してダンプファイルを生成する。

【０１３９】

ステップＳ６４４において、メモリDR切り離し処理部４１７－１は、メモリのDynamic Reconfiguration機能を使用して、パニック発生時にOS４０１－１のカーネルが使用していたメモリ領域をドメイン２０１－１から切り離して、切り離した領域を空きメモリとするようにメモリ管理部３６１に通知する。また、カーネルダンプフラグリセット処理部４２０－１は、ハイパーバイザ３５１にカーネルダンプフラグのリセットを指示する。リセット指示を受信したカーネルダンプフラグリセット処理部３７３は、カーネルダンプフラグをリセットする。

【０１４０】

ステップＳ６４５において、メモリ管理部３６１は、切り離した領域を他のドメイン２０１－２、２０１－３からも使用可能な空きメモリとする。

また、ステップＳ６４４およびＳ６４５の代わりに、空きメモリ追加処理部４１８－１は、パニック時にOS４０１－１のカーネルが使用していたメモリ領域(すなわち、ダンプ済み領域)を使用可能な未使用のメモリ、すなわち空きメモリとするようにメモリ管理部４０２－１へ通知し、メモリ管理部４０２－１はダンプ済み領域を空きメモリとする処理を行っても良い。

【０１４１】

図１５は、メモリDynamic Reconfiguration機能を用いたメモリダンプの採取を示す図である。

図１５の左側は運用状態（およびパニック時）、真ん中は再起動時、右側はダンプ採取用ドメインによるメモリダンプの採取時を示す。

ここでは、ドメイン２０１－１の処理について記載している。尚、ドメイン２０１－２、２０１－３においても同様の処理が実行されるので、詳細は省略する。

【０１４２】

図１５の左側の運用状態において、ＰＡのある領域がドメイン２０１－１のＲＡのある領域にマッピングされている。

【０１４３】

OS４０１－１のパニック時にOS４０１－１のカーネルが使用していた領域はカーネルダンプ対象領域となる。

OS４０１－１のパニック後、PA-RAマッピングの変更が行われ（ステップＳ６２２）、ドメイン２０１－１のＲＡには、パニック時にOS４０１－１のカーネルが使用していた領域（カーネルダンプ対象領域）とは異なるＰＡの領域が割り当てられ、OS４０１－１は再起動する（図１５の真ん中）。

【０１４４】

図１５の右側の再起動後のダンプ時において、ドメイン２０１－１のＲＡには、パニック時にOS４０１－１のカーネルが使用していた領域（カーネルダンプ対象領域）が組み込まれる。ドメイン２０１－１は、カーネルダンプ対象領域を読み出して、ダンプファイルを生成する。

【０１４５】

図１６は、メモリDynamic Reconfiguration機能を用いたメモリダンプの採取におけるPA-RAマッピング情報を示す図である。

図１６の左側は運用状態（およびパニック時）、真ん中はダンプ時、右側はダンプ後を

示す。

【０１４６】

ここでは、ドメイン２０１－１（制御ドメイン＃０）のPA-RAマッピングについて記載している。

PA-RAマッピング情報は、ドメイン、開始アドレス（PA Base）、サイズ、および開始アドレス（RA Base）が対応付けられて記載されている。

【０１４７】

図１６の左側のパニック時において、開始アドレス（PA Base）がxxxxx、サイズが８ＧＢである領域が制御ドメイン＃０の開始アドレス（RA Base）がaaaaaである領域にマッピングされている（図１５の左側に対応）。この領域がカーネルダンプ対象領域となる。

【０１４８】

OS４０１－１のパニック後、PA-RAマッピングの変更が行われ、さらにカーネルダンプ対象領域が制御ドメイン＃０に組み込まれ、PA-RAマッピング情報は図１６の真ん中に示すようになる。

【０１４９】

図１６の真ん中のダンプ時において、開始アドレス（PA Base）がyyyyy、サイズが８ＧＢである領域が制御ドメイン＃０のＲＡの開始アドレス（RA Base）がaaaaaである領域にマッピングされている。さらに、開始アドレス（PA Base）がxxxxx、サイズが８ＧＢである領域が制御ドメイン＃０の開始アドレス（RA Base）がbbbbbである領域にマッピングされている。

【０１５０】

すなわち、新たなＰＡの領域が再起動後の制御ドメイン＃０に割り当てられ、さらに制御ドメイン＃０の再起動後に、カーネルダンプ対象領域が制御ドメイン＃０に組み込まれる（図１５の右側に対応）。

【０１５１】

ダンプファイルの生成後、カーネルダンプ対象領域は他のドメインからも使用可能な空きメモリとなる（ステップＳ６４５）。

すなわち、図１６の右側のダンプ後において、カーネルダンプ対象領域のマッピング情報は削除される。

【０１５２】

メモリDynamic Reconfiguration機能を用いてメモリダンプを採取する方法によれば、異常を検出したオペレーティングシステムではなく、再起動後の新しいオペレーティングシステムがダンプを採取するため、ダンプ採取処理中に再度異常を検出してハングアップする等の二次被害が発生する可能性が低くなる。

【０１５３】

第２の実施の形態に係るメモリダンプ生成処理によれば、エラーを検出してハイパーバイザおよびオペレーティングシステムを再起動する場合、メモリダンプのサイズが大きい場合でも別のメモリ等にコピーを行っていないので、速やかにハイパーバイザおよびオペレーティングシステムを再起動できる。これにより、業務停止時間を短縮することができる。

【０１５４】

第２の実施の形態に係るメモリダンプ生成処理によれば、ハイパーバイザおよびカーネルのメモリダンプを採取することで、ハイパーバイザおよびドメインの両方に起因したエラーであっても、効果的にエラーの解析を行うことができる。

【０１５５】

（第３の実施の形態）

第３の実施の形態では、OSでエラーが検出され、カーネルのメモリダンプが行われる。

ここでは、OS４０１－１のカーネルのメモリダンプを生成する場合について説明する。

【０１５６】

図１７は、第３の実施の形態に係るメモリダンプ生成処理のフローチャートである。

先ず、メモリ管理部４０２－１は、OS４０１－１の起動時に、メモリ２０３－１の一番小さい(または一番大きい)リアルアドレス(RA)からカーネルが使用するメモリを割り当てる。このように、なるべくカーネルが使用するメモリ領域(ダンプ対象領域)のサイズが小さくなるようにする。また、マッピング情報抽出・格納処理部４０６－１は、カーネルが使用しているメモリのダンプを採取／解析するために必要となる情報（例えば、カーネルのテキスト域、データ域、ヒープ域、スタック域など、各セグメントのマッピング情報(論理アドレス、物理アドレス、サイズ等)、アドレス変換テーブル、ページテーブル、各種制御テーブルのマッピング情報）を、マッピング情報格納領域４０７－１に書き込む。また、ドメイン２０１－１～２０１－３およびＯＳ４０１－１～４０１－３は、起動され運用状態となっており、ドメイン２０１－４およびＯＳ４０１－４は起動されていないものとする。

【０１５７】

ステップＳ７０１において、OS４０１－１に致命的なエラーが発生する。

ステップＳ７０２において、OS４０１－１は、致命的なエラーを検出する。

ステップＳ７０３において、パニック処理部４１４－１は、OS４０１－１をパニック（緊急停止）させる。

【０１５８】

ステップＳ７０４において、カーネルダンプ対象領域通知処理部４１５－１は、緊急停止(パニック)時にOS４０１－１のカーネルが使用していたメモリ領域(カーネルダンプ対象領域)の情報(カーネルダンプ対象領域情報)をハイパーバイザ３５１に通知する。また、カーネルダンプフラグ通知部４２１－１は、カーネルダンプフラグをハイパーバイザ３５１に通知する。

【０１５９】

ステップＳ７０５において、カーネルダンプ対象領域情報/カーネルダンプフラグ格納処理部３６６は、受信したカーネルダンプ対象領域情報およびカーネルダンプフラグをカーネルダンプ対象領域情報/カーネルダンプフラグ格納領域３６７に格納する。

【０１６０】

ステップＳ７０６において、メモリ初期化部３７２は、カーネルダンプ対象領域情報で示される領域以外のメモリ領域を初期化する。すなわち、メモリ初期化部３７２は、パニック時にOS４０１－１のカーネルが使用していたメモリ領域の初期化処理を実施しない(すなわち、データを更新しない)ようにする。それにより、パニック時にOS４０１－１のカーネルが使用していたメモリ領域のデータはそのままの状態で残る。

【０１６１】

ステップＳ７０７において、PA-RAマッピング処理部３６８、ＯＳ再起動命令部３５８、およびダンプ専用ドメイン起動処理部３６５は、カーネルダンプフラグの値をチェックする。以下、カーネルダンプフラグの値に応じた処理が実行される。例えばPA-RAマッピング処理部３６８は、カーネルダンプフラグが“１：ダンプ採取用ドメインで採取”の場合、パニック発生時にＯＳ４０１－１～４０１－３のカーネルが使用していたメモリのPAをダンプ採取用ドメイン２０４－４のRAに割り当てる。

【０１６２】

以下、ステップＳ７０８とステップＳ７０９～Ｓ７１２の処理が別々に並列して実行される。

ただし、カーネルダンプフラグが“１：ダンプ採取用ドメインで採取”の場合はステップＳ７１２は実行されず、“２：メモリDynamic Reconfiguration機能を用いて採取”の場合はステップＳ７０８は実行されない。

【０１６３】

ステップＳ７０８において、ダンプ採取用ドメインによるカーネルのメモリダンプ生成処理が行われる。ステップＳ７０８は、図９Ｂのステップ６２１の処理と同様であるため説明は省略する。

【０１６４】

ステップＳ７０９において、PA-RAマッピング処理部３６８は、パニックしたドメイン２０１－１の物理アドレス(PA)とリアルアドレス(RA)間のマッピングを以下の1)、2)のように変更する。それにより、OS４０１－１を再起動してもパニック時にOS４０１－１のカーネルが使用していたメモリ領域のデータは上書きされなくなる。
1)パニック発生時にカーネルが使用していたメモリの物理アドレスは、再起動するドメインのリアルアドレスに割り当てないようにする。かつ、
2)再起動前後で、該当ドメインが使用できるメモリサイズがなるべく変化しないようにする。

【０１６５】

ただし、再起動するドメインに割り当て可能な物理メモリが所定値より不足する場合は、1)を優先する。

ステップＳ７１０において、OS再起動命令部３５８は、ドメイン２０１－１にOS４０１－１の再起動を指示する。また、OS再起動命令部３５８は、カーネルダンプフラグが“２：メモリDynamic Reconfiguration機能を用いて採取”の場合、メモリDR機能を用いたカーネルのメモリダンプ生成処理を行う旨を再起動指示に含める。OS起動処理部４０９－１は、カーネルが使用していたメモリのダンプをディスク等に書き出すことなく、OS４０１－１を再起動する。

【０１６６】

ステップＳ７１１において、OS４０１－１は、業務を再開する。

ステップＳ７１２において、カーネルのメモリダンプ生成処理が行われる。尚、ステップＳ７１２の処理は、上述のステップＳ６２５の処理と同様であるため説明は省略する。

【０１６７】

第３の実施の形態に係るメモリダンプ生成処理によれば、エラーを検出してオペレーティングシステムを緊急停止(パニック)する場合、メモリダンプのサイズが大きい場合でも別のメモリ等にコピーを行っていないので、速やかにオペレーティングシステムを再起動できる。これにより、業務停止時間を短縮することができる。

【０１６８】

（第４の実施の形態）

第４の実施の形態では、OSでエラーが検出され、カーネルのメモリダンプが行われ、さらに稼動中のハイパーバイザのメモリダンプの採取（ハイパーバイザのライブダンプと呼ぶ）が行われる。

ここでは、OS４０１－１のカーネルのメモリダンプを生成する場合について説明する。

【０１６９】

図１８Ａ、１８Ｂは、第４の実施の形態に係るメモリダンプ生成処理のフローチャートである。

ステップＳ８０１～ステップＳ８１１は、図１７のステップＳ７０１～Ｓ７１１とそれぞれ同様の処理であるため、説明は省略する。

【０１７０】

以下、ステップＳ８１２とステップＳ８１３は並列に実行される。

ステップＳ８１２において、カーネルのメモリダンプ生成処理が行われる。尚、ステップＳ８１２の処理は、上述のステップＳ６２５の処理と同様であるため説明は省略する。

ステップＳ８１３において、稼動中のハイパーバイザ３５１のメモリダンプ生成処理が制御ドメイン２０４－１で行われる。

【０１７１】

以下、稼動中のハイパーバイザ３５１のメモリダンプ生成処理の詳細について説明する。

図１９は、稼動中のハイパーバイザのメモリダンプ生成処理のフローチャートである。

【０１７２】

図１９は、図１８ＢのステップＳ８１３に対応する。

第４の実施の形態において、例えば、HVダンプフラグのデータ構造を０：採取せず、１

：異常時のHVダンプ、２：HVライブダンプのように変更することができる。HVメモリダンプ判断部４０８－１は、HVダンプフラグが０または１の場合、ＨＶのライブダンプを採取しないと判定し、HVダンプフラグが２の場合、ＨＶのライブダンプを採取すると判定する。

【０１７３】

ステップＳ８３１において、HVメモリダンプ判断部４０８－１は、ハイパーバイザ３５１にHVダンプフラグの送信を要求する。

ステップＳ８３２において、HVメモリダンプフラグ読出・送信部３５９は、要求を受信すると、HVダンプ対象領域情報/HVダンプフラグ格納領域３５６からHVダンプフラグを読み出し、OS４０１－１に送信する。

【０１７４】

ステップＳ８３３において、HVメモリダンプ判断部４０８－１は、受信したHVダンプフラグに基づいて、稼動中のハイパーバイザ３５１のライブダンプを採取するか否か判定する。稼動中のハイパーバイザ３５１のライブダンプを採取すると判定された場合、制御はステップＳ８３４に進み、採取しないと判定された場合の場合、処理は終了する。

【０１７５】

ステップＳ８３４において、HVダンプ対象領域読出処理部の呼び出し部４１０－１は、HVダンプ対象領域読出処理部３６０を呼び出す。

ステップＳ８３５において、HVダンプ対象領域読出処理部３６０は、現在、ハイパーバイザ３５１が使用しているメモリ領域を読み出し、読み出したメモリ内容を制御ドメイン２０４－１に送信する。

【０１７６】

ステップＳ８３６において、HVダンプ採取処理部４１２－１は、メモリ内容を受信し、受信したメモリ内容をファイルに書き出してハイパーバイザのダンプファイルを生成する。

【０１７７】

上記のように、稼動中のハイパーバイザのメモリダンプの生成処理では、ハイパーバイザを停止・再起動しないまま、ハイパーバイザが使用するメモリ領域のデータを読み出して、該データをハイパーバイザのダンプファイルとしてファイルに書き出している。

【０１７８】

第４の実施の形態に係るメモリダンプ生成処理によれば、エラーを検出してオペレーティングシステムを再起動する場合、メモリダンプのサイズが大きい場合でも別のメモリ等にコピーを行っていないので、速やかにオペレーティングシステムを再起動できる。これにより、業務停止時間を短縮することができる。

【０１７９】

第４の実施の形態に係るメモリダンプ生成処理によれば、ハイパーバイザおよびカーネルのメモリダンプを採取することで、ハイパーバイザおよびドメインの両方に起因したエラーであっても、効果的にエラーの解析を行うことができる。

【０１８０】

以上、複数の実施の形態を説明してきたが、実施の形態は装置および方法に限らず、プログラムとして構成することも出来るし、該プログラムを格納したコンピュータが読み取り可能な記録媒体として構成することも出来る。記録媒体としては、例えば、フレキシブルディスク（ＦＤ）、ハードディスクドライブ、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、磁気テープ、不揮発性のメモリーカード等が用いられる。

【０１８１】

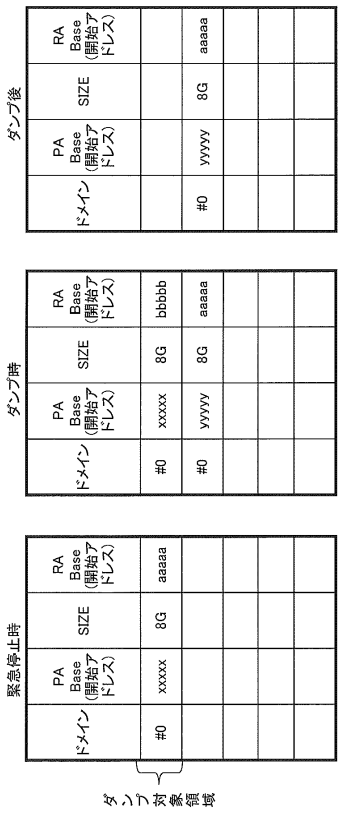
例えば、実施の形態のプログラムは、該プログラムを格納した記録媒体から読み出され、メモリ１３、２３や不揮発性メモリ１４に格納される。ＣＰＵ１２、２２は、メモリ１３、２３や不揮発性メモリ１４からプログラムを読み出して実行することにより、上述した実施の形態の各種処理を実行する。

【０１８２】
本発明は、以上に述べた実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内で種々の構成を取ることができる。例えば、論理ドメインの数は４つの限られるものでなく、任意の数にすることができる。
【符号の説明】
【０１８３】
１０　サーバ
１１　システムボード
１２　ＣＰＵ
１３　メモリ
１４　不揮発性メモリ
２１　サービスプロセッサ
２２　ＣＰＵ
２３　メモリ
３１　ディスクユニット
３２　ハードディスクドライブ
４１　通信インタフェース
５１　バス
６１　物理パーティション
２０１　論理ドメイン
２０２　ＣＰＵ
２０３　メモリ
２０４　ディスク
３１１　ファームウェア
３１２　ダンプ対象領域情報/HVダンプフラグ格納処理部
３１３　ダンプ対象領域情報/HVダンプフラグ格納領域
３１４　HVダンプフラグ設定部
３１５　メモリ初期化処理部
３１６　HV使用領域変更部
３１７　HV再起動命令部
３１８　ダンプ対象領域情報/HVダンプフラグ通知部
３１９　PA-RAマッピング通知部
３２０　メモリ開放処理部
３２１　HVダンプフラグリセット処理部
３５１　ハイパーバイザ
３５２　ドメイン緊急停止指示部
３５３　OSパニック指示部
３５４　HVダンプ対象領域通知処理部
３５５　HVダンプ対象領域情報/HVダンプフラグ格納処理部
３５６　HVダンプ対象領域情報/HVダンプフラグ格納領域
３５７　HV再起動処理部
３５８　OS再起動命令部
３５９　HVメモリダンプ読出・送信部
３６０　HVダンプ対象メモリ読出処理部
３６１　メモリ管理部
３６２　メモリ開放処理部
３６３　HVダンプフラグリセット処理部
３６４　HVダンプフラグ通知部
３６５　ダンプ専用ドメイン起動処理部
３６６　カーネルダンプ対象領域情報/カーネルダンプフラグ格納処理部

３６７　カーネルダンプ対象領域情報/カーネルダンプフラグ格納領域
３６８　PA-RAマッピング処理部
３６９　PA-RAマッピング情報格納域
３７０　割り込み処理部
３７１　メモリダンプ処理起動部
３７２　メモリ初期化処理部
３７３　カーネルダンプフラグリセット処理部
４０１　オペレーティングシステム
４０２　メモリ管理部
４０３　ファイル管理部
４０４　プロセス管理部
４０５　割り込み処理部
４０６　マッピング情報抽出・格納処理部
４０７　マッピング情報格納領域
４０８　HVメモリダンプ判断部
４０９　OS起動処理部
４１０　HVダンプ対象領域読出処理部の呼び出し部
４１１　カーネルダンプ対象メモリ読出処理部
４１２　HVダンプ採取処理部
４１３　カーネルダンプ採取処理部
４１４　パニック処理部
４１５　カーネルダンプ対象領域通知処理部
４１６　メモリDR組み込み処理部
４１７　メモリDR切り離し処理部
４１８　空きメモリ追加処理部
４１９　ダンプ専用ドメイン停止処理部
４２０　カーネルダンプフラグリセット処理部
４２１　カーネルダンプフラグ通知部

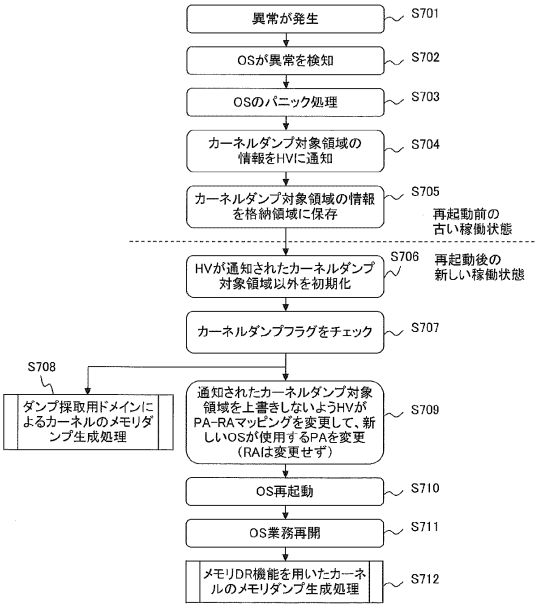
【図１６】

メモリDynamic Reconfiguration機能を用いた
メモリダンプの採取におけるPA-RAマッピング情報を示す図



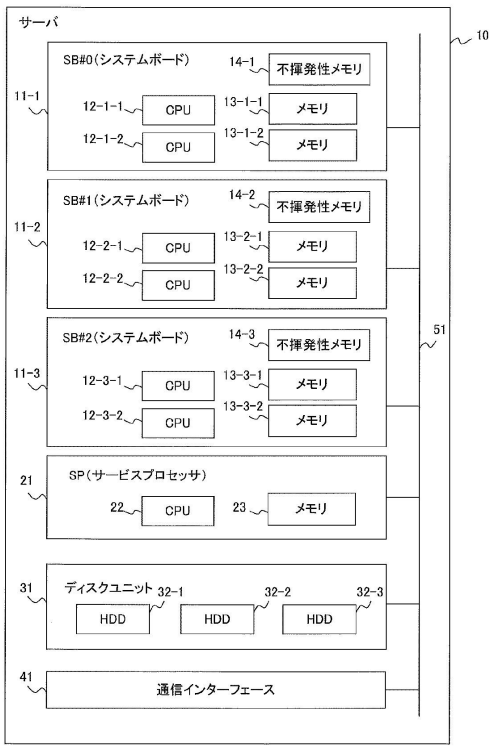
【図１７】

第3の実施の形態に係るメモリダンプ生成処理のフローチャート



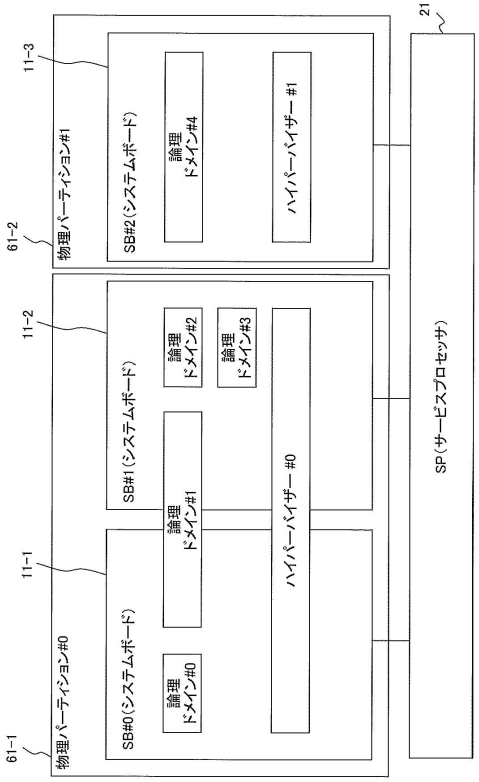
【図１】

実施の形態に係るサーバのハードウェア構成図



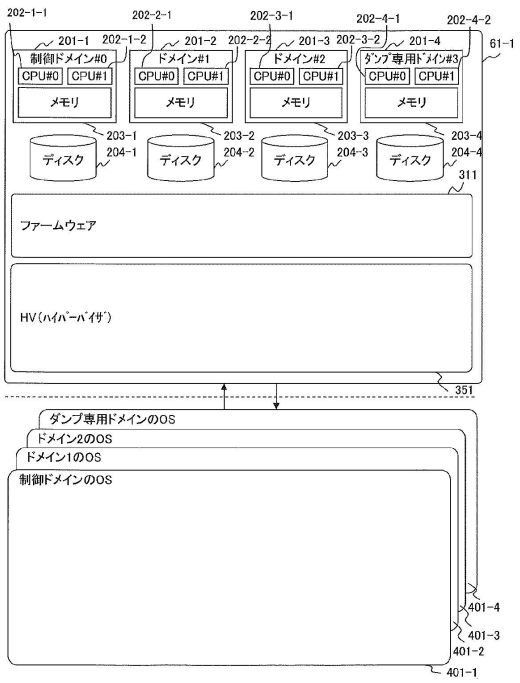
【図２】

実施の形態に係るサーバと機能との対応関係を示す図



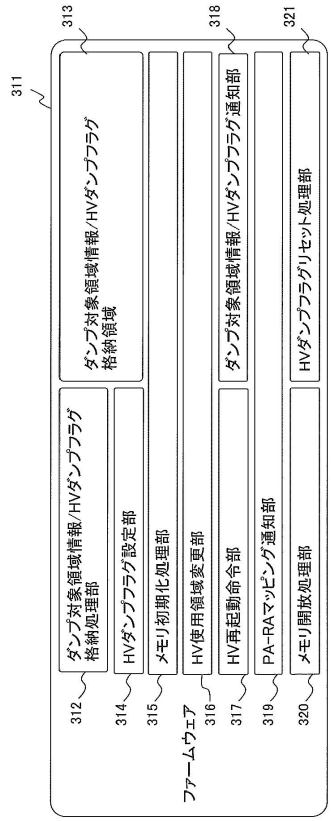
【図３】

実施の形態に係る物理パーティションの機能ブロック図



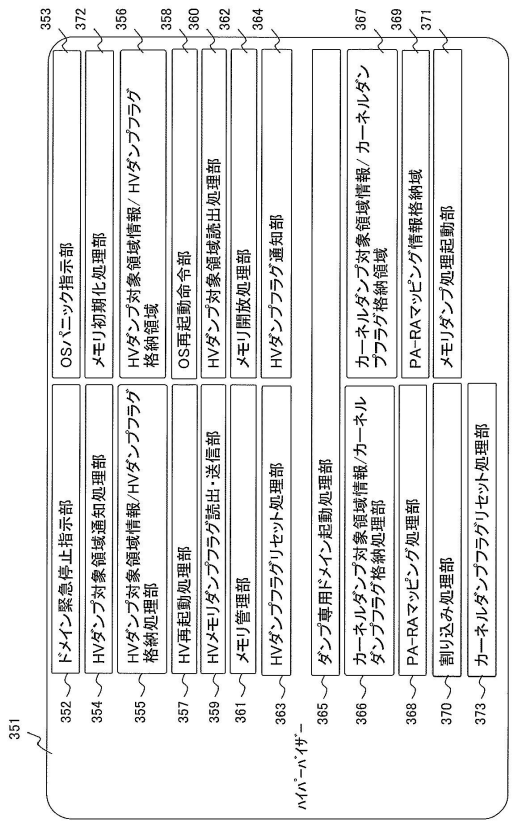
【図４】

実施の形態に係るファームウェアの構成図



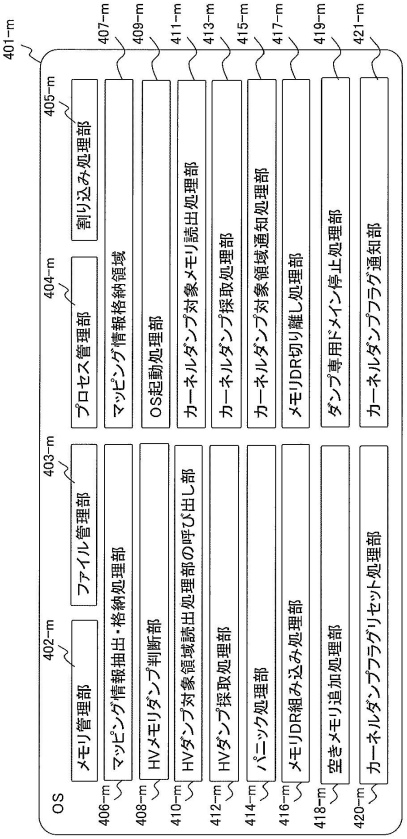
【図５】

実施の形態に係るハイパーバイザの構成図



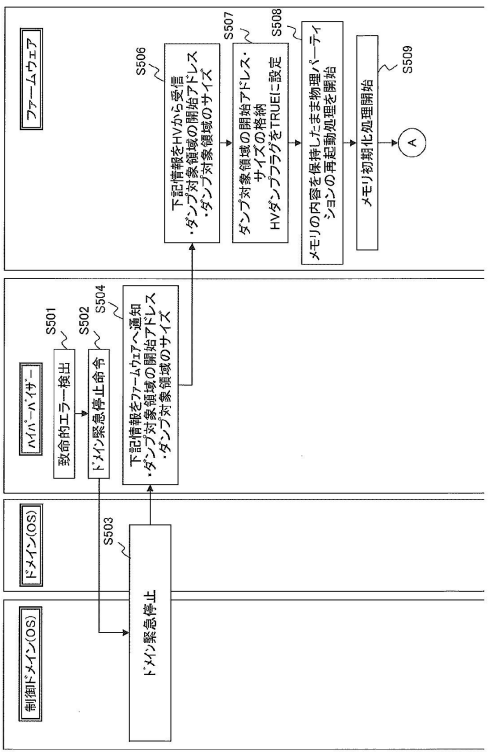
【図６】

実施の形態に係るOSの構成図



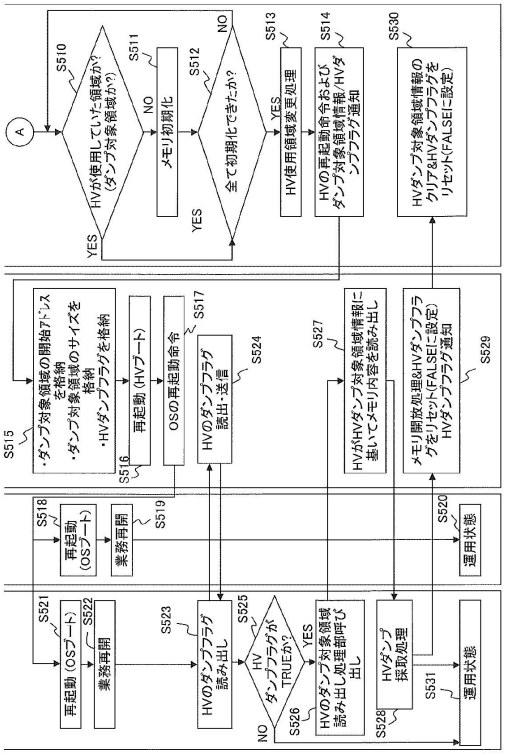
【図７Ａ】

第1の実施の形態に係るメモリダンプ生成処理のフローチャート



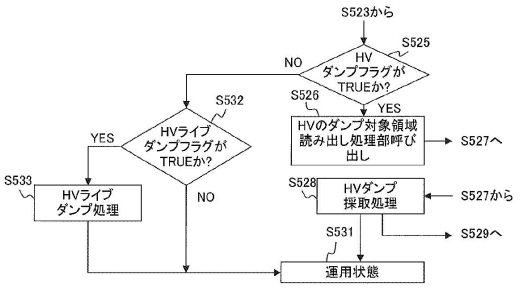
【図７Ｂ】

第1の実施の形態に係るメモリダンプ生成処理のフローチャート



【図７Ｃ】

第1の実施の形態に係るメモリダンプ生成処理の
変形例のフローチャート



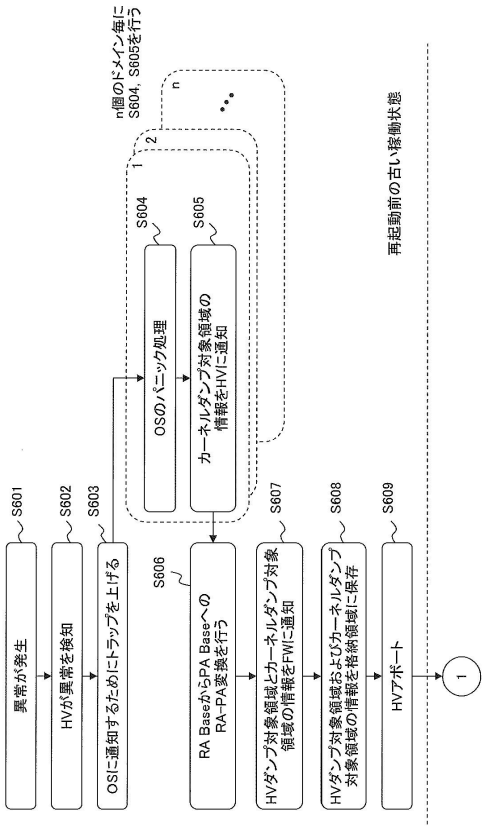
【図８】

HVダンプ対象領域情報の例

Block	PA Base (開始アドレス)	SIZE
0	xxxxxxx	1.5G
1	yyyyyyy	1.0G
N	zzzzzzz	512M

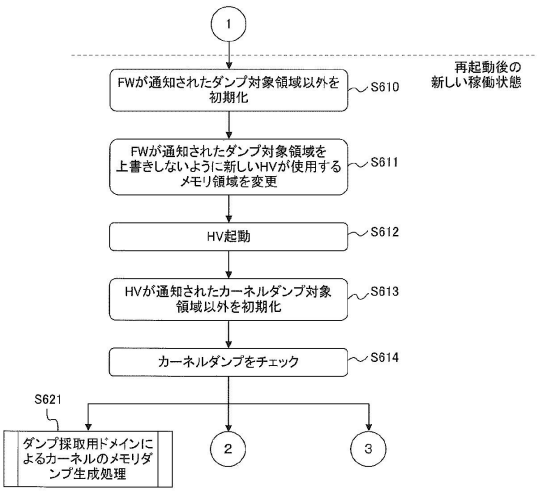
【図９Ａ】

第2の実施の形態に係るメモリダンプ生成処理のフローチャート



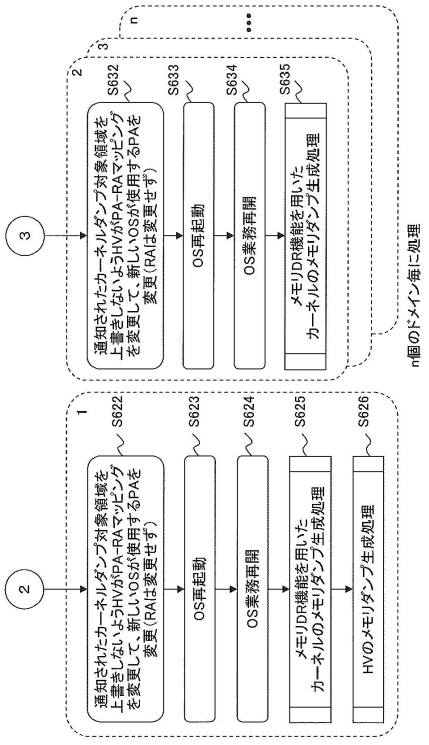
【図９Ｂ】

第2の実施の形態に係るメモリダンプ生成処理のフローチャート



【図９Ｃ】

第2の実施の形態に係るメモリダンプ生成処理のフローチャート



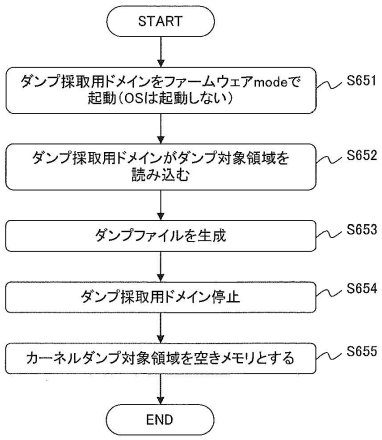
【図１０】

カーネルダンプ対象領域情報の例

Block	RA Base （開始アドレス）	SIZE
0	aaaaaaa	1.5G
N	ccccccc	512M

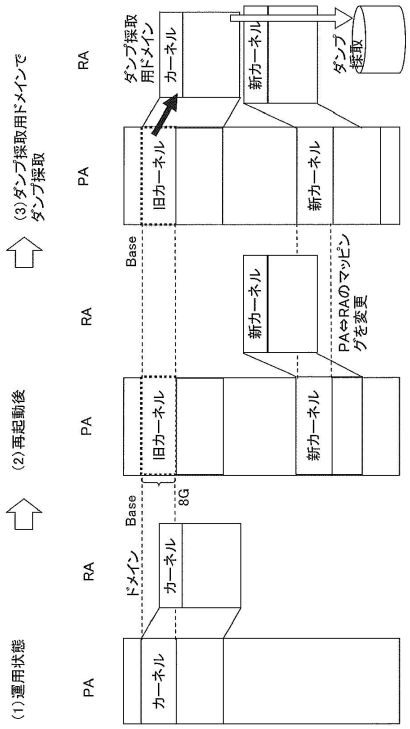
【図１１】

ダンプ採取用ドメインによるカーネルの
メモリダンプ生成処理のフローチャート



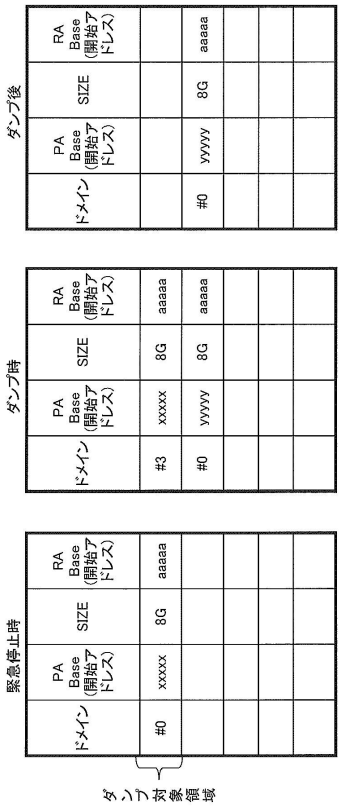
【図１２】

ダンプ採取用ドメインによるメモリダンプの採取を示す図



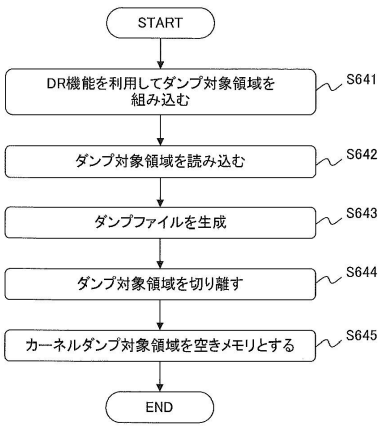
【図１３】

ダンプ採取用ドメインによるメモリダンプの採取における
PA-RAマッピング情報を示す図



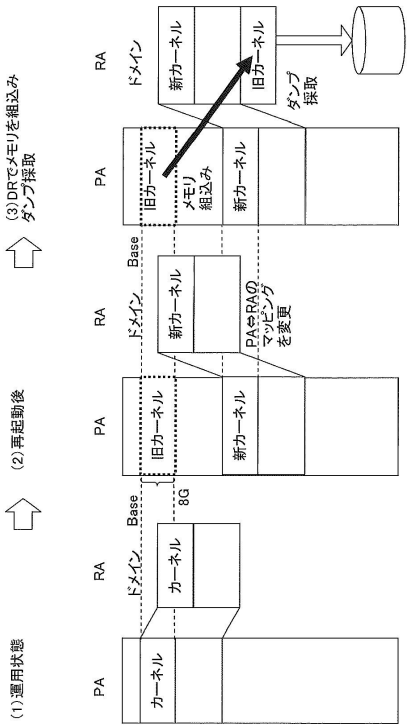
【図１４】

メモリDynamic Reconfiguration機能を用いた
カーネルのメモリダンプ生成処理のフローチャート



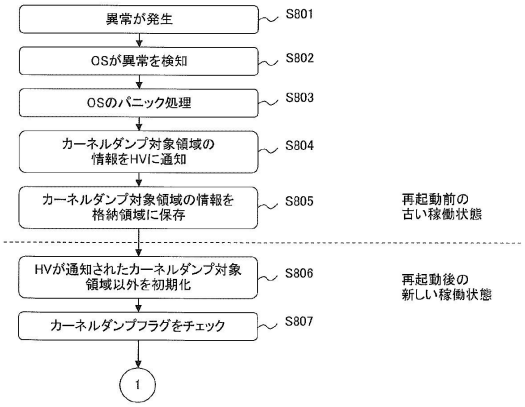
【図１５】

メモリDynamic Reconfiguration機能を用いた
メモリダンプの採取を示す図



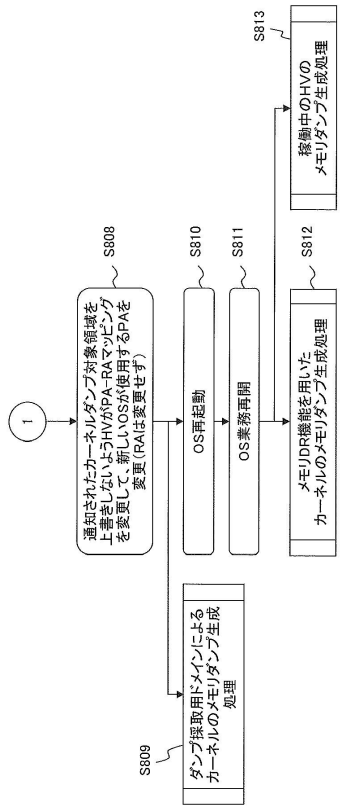
【図１８Ａ】

第4の実施の形態に係るメモリダンプ生成処理のフローチャート



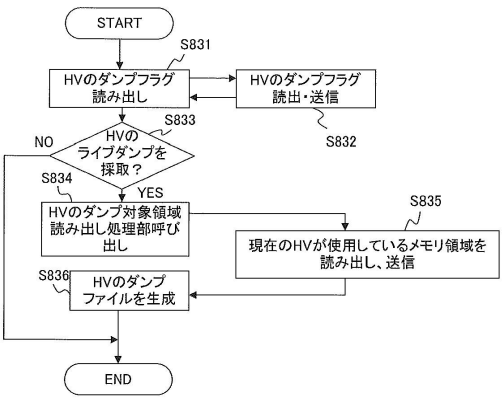
【図１８Ｂ】

第4の実施の形態に係るメモリダンプ生成処理のフローチャート



【図１９】

稼働中のハイパーバイザのメモリダンプ生成処理フローチャート



フロントページの続き

審査官　坂庭　剛史

(56)参考文献　国際公開第２０１１／００４４４１（WO，Ａ1）
国際公開第２００８／１１４３９５（WO，Ａ1）
特開２０１１－２２７７６６（ＪＰ，Ａ）
特開２０１１－２４３０１２（ＪＰ，Ａ）
米国特許出願公開第２０１１／０２２５４５８（ＵＳ，Ａ1）
特開２００６－１７２１００（ＪＰ，Ａ）
特開２００５－１２２３３４（ＪＰ，Ａ）
特開平０５－０１２０４５（ＪＰ，Ａ）
小口芳彦、山本 哲，“サーバ仮想化技術とその最新動向”，ＦＵＪＩＴＳＵ，日本，富士通株式会社，２００７年　9月10日，Ｖｏｌ．５８，Ｎｏ．５（通巻３４２号），ｐｐ．４２６－４３０，ISSN 0016-2515
岩田 恵、渡邊信彦，“総力特集 カーネルから見る最新ＵＮＩＸ：ＡＩＸ システム連続稼働を支えるＩＢＭのカーネル”，ＵＮＩＸ ｍａｇａｚｉｎｅ，日本，株式会社アスキー・メディアワークス，２００８年　7月　1日，第２３巻，第3号（通巻２４３号），ｐｐ．４０－４７

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１１／０７
Ｇ０６Ｆ　　９／４６
Ｇ０６Ｆ　１１／３４