(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-3302
(P2012-3302A)
(43)公開日　平成24年1月5日(2012.1.5)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 9/46 (2006.01)	G06F 9/46 350	

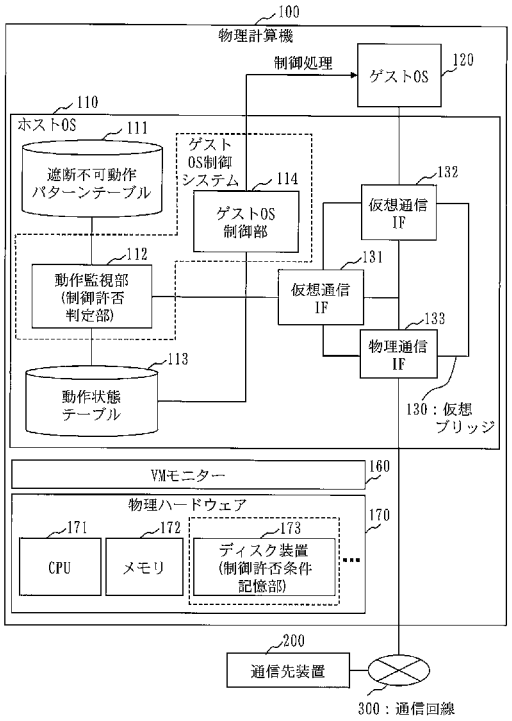
審査請求 未請求　請求項の数 5　ＯＬ　（全 16 頁）

(21)出願番号　特願2010-134826 (P2010-134826)
(22)出願日　平成22年6月14日 (2010.6.14)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100152881
弁理士　山地　博人
(72)発明者　扇谷　篤志
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　井上　淳
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　吉田　剛
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

(54)【発明の名称】ゲストＯＳ制御システム

(57)【要約】
【課題】ゲストＯＳの動作状態に応じて適切にゲストＯＳの制御が行う。
【解決手段】遮断不可動作パターンテーブル１１１には、ゲストＯＳ１２０の通信先装置２００のＩＰアドレスに対応付けて、遮断不可通信開始パターン、遮断不可通信終了パターンが記載される。遮断不可通信開始パターンはゲストＯＳ１２０に対する制御処理が許容されない遮断不可通信の開始を検知するためのビットパターンであり、遮断不可通信終了パターンは遮断不可通信の終了を検知するためのビットパターンであり、動作監視部１１２がゲストＯＳ１２０から通信先装置２００に送信するパケットにおいて遮断不可通信開始パターンを抽出した場合にはゲストＯＳ制御部１１４はゲストＯＳ１２０に対する制御処理を保留し、動作監視部１１２がパケットにおいて遮断不可通信開始パターンを抽出した後にゲストＯＳ１２０に対する制御処理を実行する。
【選択図】図１



【特許請求の範囲】
【請求項１】
仮想計算機上でゲストＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）が動作する物理計算機に含まれ、前記ゲストＯＳを制御するゲストＯＳ制御システムであって、
前記ゲストＯＳ外に構成され、前記ゲストＯＳに対する制御処理の実行許否の判定条件である制御許否条件を記憶する制御許否条件記憶部と、
前記ゲストＯＳ外に構成され、前記ゲストＯＳの動作状態を監視し、前記ゲストＯＳの動作状態の監視結果と前記制御許否条件とに基づき、前記ゲストＯＳに対する制御処理の実行許否を判定する制御許否判定部と、
前記ゲストＯＳ外に構成され、前記制御許否判定部により前記ゲストＯＳに対する制御処理を不許可とする判定がなされた場合に、前記制御許否判定部により前記ゲストＯＳに対する制御処理を許可する判定がなされるまで前記ゲストＯＳに対する制御処理の実行を保留するゲストＯＳ制御部とを有することを特徴とするゲストＯＳ制御システム。
【請求項２】
前記ゲストＯＳ制御部は、
前記制御許否判定部により前記ゲストＯＳに対する制御処理を不許可とする判定がなされてからの経過時間が所定の閾値を超えた場合は、前記制御許否判定部により前記ゲストＯＳに対する制御処理を許可する判定がなされなくても、前記ゲストＯＳに対する制御処理を実行することを特徴とする請求項１に記載のゲストＯＳ制御システム。
【請求項３】
前記制御許否条件記憶部は、
前記ゲストＯＳが通信データを送信又は受信する通信先装置の識別子に対応付けて、前記ゲストＯＳに対する制御処理が許容されない処理非許容状態の開始を示すビットパターンである処理非許容状態開始パターンと、前記処理非許容状態の終了を示すビットパターンである処理非許容状態終了パターンとが示される制御許否条件を記憶し、
前記制御許否判定部は、
前記ゲストＯＳが送信又は受信する通信データから当該通信データの通信先装置の識別子を抽出するとともに、抽出した通信先装置の識別子に対応する処理非許容状態開始パターン及び処理非許容状態終了パターンが前記通信データに出現するか否かを監視し、処理非許容状態開始パターンが出現してから処理非許容状態終了パターンが出現するまでは前記ゲストＯＳに対する制御処理を不許可とする判定を行い、処理非許容状態終了パターンが出現した後は前記ゲストＯＳに対する制御処理を許可する判定を行うことを特徴とする請求項１又は２に記載のゲストＯＳ制御システム。
【請求項４】
前記制御許否条件記憶部は、
前記ゲストＯＳが通信データを送信又は受信する通信先装置の識別子と通信先装置の動作環境との組合せに対応付けて、処理非許容状態開始パターンと処理非許容状態終了パターンとが示される制御許否条件を記憶し、
前記制御許否判定部は、
前記ゲストＯＳが通信データを送信又は受信する通信先装置の識別子を抽出するとともに、前記通信先装置の動作環境を判別し、抽出した通信先装置の識別子及び判別した動作環境の組合せに対応する処理非許容状態開始パターン及び処理非許容状態終了パターンが前記通信データに出現するか否かを監視することを特徴とする請求項３に記載のゲストＯＳ制御システム。
【請求項５】
前記制御許否条件記憶部は、
前記ゲストＯＳが利用する仮想ハードウェアの負荷レベルに対応付けられた制御許否条件を記憶し、
前記制御許否判定部は、
前記ゲストＯＳが利用する仮想ハードウェアの負荷レベルを監視し、前記仮想ハードウ

ェアの負荷レベルに対する監視結果と前記制御許否条件とに基づき、前記ゲストＯＳに対する制御処理の実行許否を判定することを特徴とする請求項１～４のいずれかに記載のゲストＯＳ制御システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、仮想化技術を適用したシステムにおいて、ホストＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）がゲストＯＳを制御する技術に関する。

【背景技術】

【０００２】

仮想化技術を適用したシステムにおいて、ホストＯＳがゲストＯＳに対し停止命令を出した際、ゲストＯＳが処理中であると、処理が途中で遮断されて不正終了してしまい、ゲストＯＳや通信先の計算機に悪影響が発生するという課題がある。

この点、複数のＯＳを持ち、必要に応じてＯＳを切り替えるようなシステムにおいて、ゲストＯＳ上でゲストＯＳの通信を監視し、切り替え不可なイベント中は別のＯＳへの切り替えを禁止する方法が提案されている（特許文献１）。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００８－５２７１４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

特許文献１では、通信先の環境の違いを考慮していないため、例えば、通信先との通信シーケンスや通信先の機器のバージョンが異なり、監視対象である切り替え可否イベントの開始パターン、終了パターンが環境に応じて変化する場合にゲストＯＳを適切に制御できないという課題がある（課題１）。

つまり、ゲストＯＳの切り替えが可能な状態であるか否かを判別するための判別条件が、例えば通信先ごと、通信シーケンスごと、機器バージョンごとに異なっていても、特許文献１では、このような違いは考慮されていないため、通信先の属性、通信シーケンス、機器のバージョンの違い等に応じた適切なゲストＯＳの制御を行うことができない。

【０００５】

また、特許文献１ではゲストＯＳに機能を導入する必要があり、ゲストＯＳ改修不可の場合に動作しなかったり、切り替え可否イベントの管理テーブルの更新時、全てのゲストＯＳを修正しなくてはいけなかったりと運用上の課題がある（課題２）。

つまり、特許文献１では、ゲストＯＳがゲストＯＳの通信を監視するため、例えばゲストＯＳに不具合が生じた際にはＯＳ切り替え制御が適切に行われず、また、例えば、ゲストＯＳの切り替えが可能な状態であるか否かを判別するための判別条件の変更を行う場合には、ゲストＯＳごとに条件の変更作業を行なわればならず、多大な作業負担となる。

【０００６】

この発明は、上記のような課題を解決することを主な目的の一つとしており、ゲストＯＳの動作状態に応じて適切にゲストＯＳの制御が行え、また、ゲストＯＳの制御のための条件の変更等を容易に行える構成を実現することを主な目的とする。

【課題を解決するための手段】

【０００７】

本発明に係るゲストＯＳ制御システムは、

仮想計算機上でゲストＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）が動作する物理計算機に含まれ、前記ゲストＯＳを制御するゲストＯＳ制御システムであって、

前記ゲストＯＳ外に構成され、前記ゲストＯＳに対する制御処理の実行許否の判定条件である制御許否条件を記憶する制御許否条件記憶部と、

前記ゲストＯＳ外に構成され、前記ゲストＯＳの動作状態を監視し、前記ゲストＯＳの動作状態の監視結果と前記制御許否条件とに基づき、前記ゲストＯＳに対する制御処理の実行許否を判定する制御許否判定部と、

前記ゲストＯＳ外に構成され、前記制御許否判定部により前記ゲストＯＳに対する制御処理を不許可とする判定がなされた場合に、前記制御許否判定部により前記ゲストＯＳに対する制御処理を許可する判定がなされるまで前記ゲストＯＳに対する制御処理の実行を保留するゲストＯＳ制御部とを有することを特徴とする。

【発明の効果】

【０００８】

本発明によれば、ゲストＯＳの動作状態を監視し、ゲストＯＳの動作状態に基づいてゲストＯＳに対する制御処理の実行許否を判定するため、ゲストＯＳの動作状態に応じて適切にゲストＯＳの制御が行え、また、制御許否条件はゲストＯＳ外に配置されているため、制御許否条件の変更等をゲストＯＳごとに行う必要がなく、制御許否条件の変更等を容易に行える。

【図面の簡単な説明】

【０００９】

【図１】実施の形態１に係るシステム構成例を示す図。

【図２】実施の形態１に係る遮断不可動作パターンテーブル及び動作状態テーブルの例を示す図。

【図３】実施の形態１に係るＯＳ制御フロー図。

【図４】実施の形態１に係るゲストＯＳ監視フロー図。

【図５】実施の形態２に係るシステム構成例を示す図。

【図６】実施の形態２に係る遮断不可動作パターンテーブル及び動作状態テーブルの例を示す図。

【図７】実施の形態２に係るゲストＯＳ監視フロー図。

【図８】実施の形態２に係るタイムアウト監視フロー図。

【図９】実施の形態３に係るシステム構成例を示す図。

【図１０】実施の形態３に係る通信先リストの例を示す図。

【図１１】実施の形態３に係る動作環境検出フロー図。

【図１２】実施の形態１～３に係る物理計算機のハードウェア構成例を示す図。

【発明を実施するための形態】

【００１０】

実施の形態１～３では、仮想化技術を適用したシステムにおいて、ホストＯＳがゲストＯＳを制御したい場合に、ゲストＯＳの処理状態を監視して安全に制御処理を行うことで、ゲストＯＳが実施中の処理の不正終了を防止する方式を説明する。

ここで、ホストＯＳは物理計算機上で動作するＯＳであり、ゲストＯＳはホストＯＳ上に仮想化技術を適用して構築され、ホストＯＳの制御に基づいて動作するＯＳを指す。

また、制御処理とは、例えば、ホストＯＳがゲストＯＳを停止させる処理である。

なお、対象とする仮想化技術は、ホスト型の仮想化技術だけでなくハイパーバイザ型の仮想化技術も含む。

また、以下の説明では、ホストＯＳが監視するゲストＯＳの動作の一例として、通信（仮想ブリッジ）を監視することを想定したケースについて述べる。

ホストＯＳが監視するゲストＯＳの動作の他の例としては、ゲストＯＳの状態（故障、フリーズなど）、プロセス、サービス、仮想ハードウェアの負荷レベル（ＣＰＵ使用率、メモリ使用率、ディスク使用量、ディスク入出力量、ネットワーク入出力量など）などが挙げられ、監視対象に応じて後述の遮断不可動作パターンテーブルや動作状態テーブルの項目、動作監査部の監視対象が異なる。

以下、図面を参照して、ホストＯＳが、ゲストＯＳが送受信するメッセージを監視する例の詳細を説明する。

【００１１】

実施の形態１．
図１は、本実施の形態に係るシステム構成例を示す。
【００１２】
図１において、物理計算機１００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１７１、メモリ１７２、ディスク装置１７３等の物理ハードウェア１７０を有し、物理ハードウェア１７０上でＶＭ（Ｖｉｒｔｕａｌ Ｍａｃｈｉｎｅ）モニター１６０が動作し、更に、ＶＭモニター１６０上ではホストＯＳ１１０が動作している。
また、ホストＯＳ１１０が仮想化技術により構築したゲストＯＳ１２０が動作している。
ホストＯＳ１１０はＣＰＵ１７１により実行される。このため、ホストＯＳ１１０内のゲストＯＳ制御部１１４及び動作監視部１１２はＣＰＵ１７１により実行される。
ゲストＯＳ１２０は、ＶＭモニター１６０及びホストＯＳ１１０により提供される仮想ハードウェア（仮想ＣＰＵ、仮想メモリ、仮想ディスク、仮想Ｉ／Ｏ（Ｉｎｐｕｔ／Ｏｕｔｐｕｔ）デバイス等）を利用して動作する。
ゲストＯＳ１２０は複数あってもよい。
また、物理計算機１００及び通信先装置２００は通信回線３００に接続している。
また、ホストＯＳ１１０には、仮想ブリッジ１３０が含まれ、ゲストＯＳ１２０は仮想ブリッジ１３０を利用して通信先装置２００と通信可能である。
【００１３】
また、ホストＯＳ１１０において、遮断不可動作パターンテーブル１１１には、ゲストＯＳ１２０の遮断不可動作パターンが登録されている。
また、動作状態テーブル１１３には、ゲストＯＳ１２０の動作状態が登録されている。
なお、遮断不可動作パターンテーブル１１１及び動作状態テーブル１１３は、読み出される前はディスク装置１７３に格納されており、ホストＯＳ１１０が遮断不可動作パターンテーブル１１１及び動作状態テーブル１１３を利用する際に、ディスク装置１７３からメモリ１７２上のホストＯＳ１１０に割り当てられている領域にロードされ、ホストＯＳ１１０による利用が可能となる。
図１では、遮断不可動作パターンテーブル１１１及び動作状態テーブル１１３がメモリ１７２に展開されて、ホストＯＳ１１０による利用が可能な状態を示している。
なお、遮断不可動作パターンテーブル１１１及び動作状態テーブル１１３の詳細は図２を参照して後述するが、遮断不可動作パターンテーブル１１１は制御許否条件の例であり、遮断不可動作パターンテーブル１１１を格納しているディスク装置１７３は制御許否条件記憶部の例である。
【００１４】
動作監視部１１２は、ゲストＯＳ１２０の動作状態を監視し、ゲストＯＳ１２０の動作状態の監視結果と遮断不可動作パターンテーブル１１１に基づき、ゲストＯＳ１２０に対する制御処理の実行許否を判定する。
より具体的には、動作監視部１１２は、ゲストＯＳ１２０が送信又は受信するメッセージから当該メッセージの通信先装置の識別子を抽出するとともに、抽出した通信先装置の識別子に対応する遮断不可通信開始パターン及び遮断不可通信終了パターンがメッセージに出現するか否かを監視する。
そして、遮断不可通信開始パターンが出現してから遮断不可通信終了パターンが出現するまではゲストＯＳ１２０に対する制御処理を不許可とする判定を行い、遮断不可通信終了パターンが出現した後はゲストＯＳ１２０に対する制御処理を許可する判定を行う。
なお、遮断不可通信開始パターン及び遮断不可通信終了パターンは、遮断不可動作パターンテーブル１１１において定義されているビットパターンであり、遮断不可通信開始パターンはゲストＯＳ１２０に対する制御処理が許容されない状態（処理非許容状態）の開始を示すビットパターンであり、遮断不可通信終了パターンはゲストＯＳ１２０に対する制御処理が許容されない状態（処理非許容状態）の終了を示すビットパターンである。
また、動作監視部１１２は、判定結果を動作状態テーブル１１３に書き込む。

具体的には、制御処理を不許可とする場合は動作状態テーブル１１３に「通信中」と書き込み、制御処理を許可する場合は「待機中」と書き込む。

なお、動作監視部１１２は、制御許否判定部の例である。

【００１５】

ゲストＯＳ制御部１１４は、動作監視部１１２の判定結果に従って、ゲストＯＳ１２０に対する制御処理を実行する。

つまり、動作監視部１１２によりゲストＯＳ１２０に対する制御処理を許可する判定がなされている場合（動作状態テーブル１１３に「待機中」と書き込まれている場合）はゲストＯＳ１２０に対する制御処理を実行する。

一方、動作監視部１１２によりゲストＯＳ１２０に対する制御処理を不許可とする判定がなされている場合（動作状態テーブル１１３に「通信中」とある場合）は、動作監視部１１２により制御処理を許可する判定がなされるまで（動作状態テーブル１１３に「待機中」と書き込まれるまで）ゲストＯＳ１２０に対する制御処理の実行を保留する。

【００１６】

仮想ブリッジ１３０は、ホストＯＳ側の仮想通信ＩＦ（インタフェース）１３１、ゲストＯＳ側の仮想通信ＩＦ１３２と、物理計算機１００から外部に通信するために利用する物理通信ＩＦ１３３からなる。

物理通信ＩＦ１３３は、通信カード等の物理ハードウェアであり、物理ハードウェア１７０に分類されるものであり、正確には、ホストＯＳ１１０内の要素ではない。

しかし、仮想通信ＩＦ１３１及び仮想通信ＩＦ１３２と密接に関連しているため、仮想通信ＩＦ１３１及び仮想通信ＩＦ１３２の近傍に図示している。

【００１７】

なお、図１において、破線で囲まれている要素、つまり、動作監視部１１２、ゲストＯＳ制御部１１４及びディスク装置１７３がゲストＯＳ制御システムに対応する。

【００１８】

図２は、遮断不可動作パターンテーブル１１１、動作状態テーブル１１３の例を示す。

【００１９】

本実施の形態ではゲストＯＳ１２０の通信を監視するため、各テーブルのレコード項目は、通信パケットから得られる情報を利用する。

例えば、遮断不可動作パターンテーブル１１１のレコードには、送信元のゲストＯＳのＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレス、送信先となる通信先装置２００のＩＰアドレス、ポート番号、遮断不可通信開始パターン、遮断不可通信終了パターンが記載される。

前述のように、遮断不可通信開始パターンはゲストＯＳ１２０に対する制御処理が許容されない状態の開始を示すビットパターンであり、遮断不可通信終了パターンはゲストＯＳ１２０に対する制御処理が許容されない状態の終了を示すビットパターンである。

なお、図２の例では、ゲストＯＳ１２０から通信先装置２００にパケットを送信するケースに対応させた遮断不可動作パターンテーブルの例を示しているが、ゲストＯＳ１２０が通信先装置２００からパケットを受信するケースに対応させた遮断不可動作パターンテーブルを用意してもよい。

このように、遮断不可動作パターンテーブル１１１には、ゲストＯＳ１２０がメッセージを送信又は受信する通信先装置の識別子（ＩＰアドレス）に対応付けて、遮断不可通信開始パターンと遮断不可通信終了パターンが示される。

【００２０】

動作状態テーブル１１３のレコードには、送信元のＩＰアドレス、送信先のＩＰアドレス、ポート番号、状態が記載される。

動作状態テーブル１１３の状態には、遮断不可通信時（ゲストＯＳに対する制御処理が許可されない状態のとき）は「通信中」、遮断可能時（ゲストＯＳに対する制御処理が許可される状態のとき）は「待機中」が記載される。

【００２１】

次に動作について説明する。
実施の形態１は、ユーザあるいはプログラムによるゲストＯＳ制御操作を実行するための「ゲストＯＳ制御」と、ゲストＯＳの動作を監視する「ゲストＯＳ監視」により実現される。
【００２２】
図３は「ゲストＯＳ制御」のフロー図である。
まず、Ｓ０１において、ユーザあるいはプログラムがホストＯＳ１１０に対し、ゲストＯＳ１２０の制御操作を実行する。
次に、Ｓ０２において、ホストＯＳ１１０はゲストＯＳ制御部１１４に制御命令を発行する。
次に、Ｓ０３において、ゲストＯＳ制御部１１４は動作状態テーブル１１３を参照し、ゲストＯＳ１２０の動作状態を確認する。
ここで、動作状態テーブル１１３の状態が「通信中」であればＳ０４へ、「待機中」であればＳ０５へ遷移する。
Ｓ０４では、ゲストＯＳ制御部１１４はゲストＯＳ１２０が遮断不可動作中であるため、ゲストＯＳ１２０に対して制御処理を実行せず、次の動作状態テーブル監視タイミングまで一定時間待機し、Ｓ０３へ遷移する。
Ｓ０５では、ゲストＯＳ制御部１１４はゲストＯＳ１２０に対して制御処理を実施し、ゲストＯＳ制御処理を終了する。
【００２３】
図４は「ゲストＯＳ監視」のフロー図である。
まず、Ｓ０６において、動作監視部１１２は仮想ブリッジ１３０上を流れるパケットを捕捉するとともに、当該パケットの複製を取得する。
次に、Ｓ０７において、動作監視部１１２はパケットの情報（送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号）を元に、遮断不可動作パターンテーブル１１１を参照する。つまり、動作監視部１１２は、パケットの送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号と一致する送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号が記載されているレコードの遮断不可通信開始パターン、遮断不可通信終了パターンを取得する。
次に、Ｓ０８において、動作監視部１１２はパケットデータ内にＳ０７で取得した遮断不可通信開始パターンと一致するビットパターンが含まれているかどうか確認する。
Ｓ０８において遮断不可通信開始パターンと一致するビットパターンが確認された場合は、Ｓ０９において、動作監視部１１２は動作状態テーブル１１３を参照し、パケットの情報（送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号）と一致する動作状態テーブル１１３のレコードの状態を「通信中」に変更する。
一方、遮断不可通信開始パターンと一致するビットパターンが出現しない場合は、Ｓ１０において、パケットデータ内にＳ０７で取得した遮断不可通信終了パターンと一致するビットパターンが含まれているかどうか確認する。
Ｓ１０において遮断不可通信終了パターンと一致するビットパターンが確認された場合は、Ｓ１１において、動作監視部１１２は動作状態テーブル１１３を参照し、パケットの情報（送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号）と一致する動作状態テーブル１１３のレコードの状態を「待機中」に変更する。
また、Ｓ１２において、動作監視部１１２は仮想ブリッジ上のパケットの監視を継続する。
【００２４】
このように、本実施の形態では、ホストＯＳ上で「ゲストＯＳ制御」と「ゲストＯＳ監視」を実行することで、ゲストＯＳを改修することなくゲストＯＳの安全な制御が可能となる。
つまり、パケットの通信先ごとに固有の遮断不可通信の開始パターン、終了パターンを適用してゲストＯＳに対する制御処理の実行許否判定を行うため、通信先となる装置の属性、通信先となる装置との通信シーケンスに対応させてゲストＯＳを適切に制御できる。

また、ホストＯＳ内の動作監視部によりゲストＯＳに対する制御処理の実行許否判定が行われるため、ゲストＯＳが改修不可である場合や、遮断不可動作パターンテーブルの更新時もホストＯＳのみの変更でよい。

【００２５】

本実施の形態では、以下の要素を備え、ゲストＯＳを安全に制御することのできる、仮想マシンゲストＯＳ制御方式を説明した。

ゲストＯＳの動作を監視する動作監視部、

ゲストＯＳの遮断不可動作パターンを表す遮断不可動作パターンテーブル、

ゲストＯＳの動作状態を表す動作状態テーブル、

ゲストＯＳを制御するゲストＯＳ制御部。

【００２６】

実施の形態２．

以上の実施の形態１は、ホストＯＳがゲストＯＳを安全に制御できるようにしたものであるが、ゲストＯＳが遮断不可通信状態の際に、想定外の要因により遮断不可通信が完了できなくなった場合などに、ゲストＯＳの制御ができなくなってしまうことがある。

実施の形態２では、遮断不可動作パターンテーブルにタイムアウト値を設定し、遮断不可動作状態の持続時間がタイムアウト値を超えた場合、遮断不可動作状態を解除する方式を説明する。

【００２７】

図５は実施の形態２に係るシステム構成例を示す。

図５において、物理計算機１０１は、実施の形態１の物理計算機１００と同様の構成となっており、物理ハードウェア１７０及びＶＭモニター１６０上にホストＯＳ１４０と、ＶＭモニター１６０とホストＯＳ１４０が仮想化技術により構築したゲストＯＳ１２０が存在する。

ホストＯＳ１４０には、ゲストＯＳ１２０の遮断不可通信のタイムアウト値が追加された遮断不可動作パターンテーブル１４１と、ゲストＯＳ１２０の動作を監視する動作監視部１４２と、ゲストＯＳ１２０の遮断不可通信の開始時刻が追加された動作状態テーブル１４３と、遮断不可動作のタイムアウト監視機能が追加されたゲストＯＳ制御部１４４が含まれる。

【００２８】

本実施の形態では、動作監視部１４２は、ゲストＯＳ１２０のパケットデータに遮断不可通信開始パターンと一致するビットパターンが含まれていた場合には、ゲストＯＳ１２０に対する制御処理を不許可とする判定を行い、動作状態テーブル１４３に「通信中」と記述するとともに遮断不可通信の開始時刻を記述する。

また、ゲストＯＳ制御部１４４は、実施の形態１と同様に、ゲストＯＳ１２０に対する制御処理を不許可とする判定がなされている場合はゲストＯＳ１２０に対する制御処理を留保するが、不許可とする判定がなされてからの経過時間（動作状態テーブル１４３に記述されている開始時刻からの経過時間）が所定の閾値（遮断不可動作パターンテーブル１４１のタイムアウト値）を超えた場合は、動作監視部１４２によりゲストＯＳ１２０に対する制御処理を許可する判定がなされなくても、ゲストＯＳ１２０に対する制御処理を実行する。

【００２９】

また、図５の構成において、ゲストＯＳ１２０、仮想ブリッジ１３０、通信先装置２００、通信回線３００は実施の形態１と同様であるため、説明を省略する。

【００３０】

図６は、本実施の形態に係る遮断不可動作パターンテーブル１４１、動作状態テーブル１４３の例である。

図６の例では、実施の形態１の遮断不可動作パターンテーブル１１１のレコード項目にタイムアウト値を追加し、動作状態テーブル１１３のレコード項目に、停止要求有無、通信開始時刻を追加している。その他の項目に変更はない。

【００３１】
次に動作について説明する。
実施の形態２は、実施の形態１で実施する「ゲストＯＳ制御」、「ゲストＯＳ監視」に、「タイムアウト監視」を加えたものである。
ここで、「ゲストＯＳ制御」については、実施の形態１と同様であるため、説明を省略する。
【００３２】
図７は「ゲストＯＳ監視」のフロー図である。
ここで、Ｓ０６、Ｓ０７、Ｓ０８、Ｓ１０、Ｓ１２については実施の形態１の「ゲストＯＳ監視」と同様の処理であるため、説明を省略する。
Ｓ０８においてゲストＯＳ１２０が送信または受信するパケットのデータ中に遮断不可通信開始パターンと一致するビットパターンが確認された場合は、Ｓ１３において、動作監視部１４２は動作状態テーブル１４３を参照し、パケットの情報（送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号）と一致する動作状態テーブル１４３のレコードの状態を「通信中」に変更し、通信開始時刻を「現在時刻」に変更する。
また、Ｓ１０においてパケットデータ中に遮断不可通信終了パターンと一致するビットパターンが確認された場合は、Ｓ１４において、動作監視部１４２は動作状態テーブル１４３を参照し、パケットの情報（送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号）と一致する動作状態テーブル１１３のレコードの状態を「待機中」に変更し、通信開始時刻を空欄に変更する。
【００３３】
図８は「タイムアウト監視」のフロー図である。
まず、Ｓ１５では、ゲストＯＳ制御部１４４が動作状態テーブル１４３で状態が「通信中」である全レコードに対して、現在時刻と通信開始時刻から動作時間（通信開始時刻からの経過時間）を計算する。
次に、Ｓ１６において、ゲストＯＳ制御部１４４は遮断不可動作パターンテーブル１４１を参照し、「通信中」であるレコードと同じ送信元ＩＰアドレス、送信先ＩＰアドレス、ポート番号が記述されているレコードに設定されているタイムアウト値と動作時間を比較する。
Ｓ１６において動作時間がタイムアウトしている場合、すなわち動作時間がタイムアウト値以上である場合は、Ｓ１７において、ゲストＯＳ制御部１４４は動作状態テーブル１４３を参照し、該当するレコードの状態を「待機中」に変更し、通信開始時刻を空欄に変更する。
また、Ｓ１８において、ゲストＯＳ制御部１４４は、動作状態テーブル１４３の停止要求有無を参照し、ゲストＯＳ１２０に対する制御命令が発行されていれば（停止要求が「有」であれば）、ゲストＯＳ１２０の制御処理を行う。
また、Ｓ１９において、ゲストＯＳ制御部１４４は定期的にタイムアウト監視を行い、一定時間後Ｓ１５へ遷移する。
【００３４】
以上のように「タイムアウト監視」を追加することで、異常時など、ゲストＯＳが遮断不可動作状態から待機中状態に復帰できなくなった場合に、それを検知し、ゲストＯＳを制御することができる。
【００３５】
本実施の形態では、実施の形態１の仮想マシンゲストＯＳ制御方式に、以下を加え、タイムアウト制御機能を追加した、仮想マシンゲストＯＳ制御方式を説明した。
タイムアウト情報を追加した遮断不可動作パターンテーブル、
タイムアウト判定のための動作開始時刻を追加した動作状態テーブル。
【００３６】
実施の形態３．
以上の実施の形態１および実施の形態２は、ホストＯＳ上がゲストＯＳを安全に制御で

きるようにしたものである。
実施の形態３では、通信先の環境の違いを考慮し、例えば、通信先の機器のバージョンが異なり、監視対象である遮断不可動作の開始、終了パターンが環境（通信先の機器のバージョン）に応じて変化する場合にゲストＯＳを適切に制御できるようにする。
実施の形態１、２の構成に動作環境検出部および通信先リストを追加し、通信先装置の動作環境に応じて適切な遮断不可動作パターンテーブルを切り替えることで、監視対象である遮断不可通信の開始、終了パターンが通信先装置の動作環境に応じて変化する場合でもゲストＯＳを適切に制御できる方式を実現する。
【００３７】
図９は実施の形態３に係るシステム構成例を示す。
図９において、物理計算機１０２は、実施の形態１の物理計算機１００と同様の構成となっており、物理ハードウェア１７０及びＶＭモニター１６０上にホストＯＳ１５０と、ＶＭモニター１６０及びホストＯＳ１５０が仮想化技術により構築したゲストＯＳ１２０が存在する。
ホストＯＳ１５０は実施の形態２の遮断不可動作パターンテーブル１４１、動作状態テーブル１４３、ゲストＯＳ制御部１４４と、通信先の動作環境を検出する動作環境検出部１５５と、通信先の情報を格納する通信先リスト１５６と、動作環境検出部１５５より検出した通信先の動作環境に応じて遮断不可動作パターンテーブルを切り変える動作監視部１５２からなる。
なお、遮断不可動作パターンテーブル１４１、動作状態テーブル１４３及び通信先リスト１５６は、読み出される前はディスク装置１７３に格納されており、ホストＯＳ１５０が遮断不可動作パターンテーブル１４１、動作状態テーブル１４３及び通信先リスト１５６を利用する際に、ディスク装置１７３からメモリ１７２上のホストＯＳ１５０に割り当てられている領域にロードされ、ホストＯＳ１５０による利用が可能となる。
本実施の形態では、動作監視部１５２及び動作環境検出部１５５が制御許否判定部の例となる。
また、本実施の形態では、動作環境検出部１５５を含めた破線で囲んだ範囲がゲストＯＳ制御システムに相当する。
なお、ゲストＯＳ１２０、仮想ブリッジ１３０、通信先装置２００、通信回線３００は実施の形態１、および実施の形態２と同様であるため、説明を省略する。
【００３８】
図１０は、通信先リスト１５６の例である。
レコード項目は、通信先の名前、ＩＰアドレス、通信先種別、バージョンからなる通信先を示す情報（これ以外の項目を含んでも良い）と、通信先装置の動作監視に対応させて選択する遮断不可動作パターンテーブル名が記載される。
なお、通信先の動作環境とは、例えば、通信先装置２００が含まれる通信システムのシステム種別や通信先装置２００のバージョン（例えば、通信先装置２００のＯＳのバージョン）である。
図１０の例では、通信先１のシステム種別及びバージョンを調査した結果、システム種別がシステムＡであり、バージョンが１．０であれば、遮断不可動作パターンテーブルＴａｂ１が選択される。
また、通信先１のシステム種別及びバージョンを調査した結果、システム種別がシステムＡであり、バージョンが１．１であれば、遮断不可動作パターンテーブルＴａｂ２が選択される。
【００３９】
次に動作について説明する。
実施の形態３は、実施の形態２で実施する「ゲストＯＳ制御」、「ゲストＯＳ監視」、「タイムアウト監視」に、「動作環境検出」を加えたものである。
ここで「ゲストＯＳ制御」、「ゲストＯＳ監視」、「タイムアウト監視」については、実施の形態２と同様であるため、説明を省略する。

【００４０】
図１１は「動作環境検出」のフロー図である。
まず、Ｓ１９において、動作環境検出部１５５は通信先リスト１５６を参照し、通信先リストにあるアクセス方法情報（ＩＰアドレス、通信先種別、バージョン情報）を元に、通信先装置２００へアクセス（バージョンの確認など）を試みる。そして、通信先装置２００から正しい返信を得た際のアクセス方法情報に対応する環境（切り替えるべき遮断不可動作パターンテーブル名）を取得する。
次に、Ｓ２０において、動作環境検出部１５５は取得した動作環境（遮断不可動作パターンテーブル名）を動作監視部１５２に通知する。
次に、Ｓ２１において、動作監視部１５２は遮断不可動作パターンテーブル１４１を切り替える。
そして、Ｓ２２において、動作環境検出部１５５は定期的に動作環境の監視を行い、一定時間後、Ｓ１９へ遷移する。
【００４１】
このように、動作環境検出部１５５は、ゲストＯＳ１２０がパケットを送信又は受信する通信先装置にアクセスし、当該通信先装置の識別子を抽出するとともに、当該通信先装置の動作環境を判別する。
そして、動作環境検出部１５５は、抽出した通信先装置の識別子及び判別した動作環境の組合せに対応する遮断不可動作パターンテーブル１４１を選択し、選択した遮断不可動作パターンテーブル１４１を動作監視部１５２に通知する。
動作監視部１５２は、動作環境検出部１５５から通知された遮断不可動作パターンテーブル１４１に記述されている遮断不可通信開始パターン、遮断不可通信開始パターンと一致するビットパターンがパケットデータ内に存在しているかを確認する。
以降の動作は、実施の形態１又は実施の形態２で説明したものと同様である。
【００４２】
以上のように「動作環境検出」を追加することで、通信先に応じて適切な遮断不可動作パターンテーブルを切り替えることで、監視対象である遮断不可通信の開始、終了パターンが環境に応じて変化する場合でもゲストＯＳを適切に制御できる。
【００４３】
本実施の形態では、実施の形態１および実施の形態２の仮想マシンゲストＯＳ制御方式に、以下を加え、ゲストＯＳの通信先に応じて遮断不可動作パターンテーブルを適切に切り替えることのできる、仮想マシンゲストＯＳ制御方式を説明した。
ゲストＯＳの通信先の候補の情報の一覧を表す通信先リスト、
通信先リストを照会し、ゲストＯＳの通信先を検出する動作環境検出部。
【００４４】
最後に、実施の形態１～３に示した物理計算機１００、１０１、１０２のハードウェア構成例について説明する。
図１２は、実施の形態１～３に示す物理計算機１００、１０１、１０２のハードウェア資源の一例を示す図である。
なお、図１２の構成は、あくまでも物理計算機１００、１０１、１０２のハードウェア構成の一例を示すものであり、物理計算機１００、１０１、１０２のハードウェア構成は図１２に記載の構成に限らず、他の構成であってもよい。
【００４５】
図１２において、物理計算機１００、１０１、１０２は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。
ＣＰＵ９１１は、バス９１２を介して、例えば、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）９１３、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）９１４、通信ボード９１５、表示装置９０１、キーボード９０２、マウス９０３、磁気ディスク装置９２

０と接続され、これらのハードウェアデバイスを制御する。
更に、ＣＰＵ９１１は、ＦＤＤ９０４（Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ Ｄｒｉｖｅ）、コンパクトディスク装置９０５（ＣＤＤ）、プリンタ装置９０６、スキャナ装置９０７と接続していてもよい。また、磁気ディスク装置９２０の代わりに、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）、光ディスク装置、メモリカード（登録商標）読み書き装置などの記憶装置でもよい。
ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３、ＦＤＤ９０４、ＣＤＤ９０５、磁気ディスク装置９２０の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置の一例である。
通信ボード９１５、キーボード９０２、マウス９０３、スキャナ装置９０７、ＦＤＤ９０４などは、入力装置の一例である。
また、通信ボード９１５、表示装置９０１、プリンタ装置９０６などは、出力装置の一例である。

【００４６】
通信ボード９１５は、図１等に示すように、ネットワークに接続されている。例えば、通信ボード９１５は、ＬＡＮ（ローカルエリアネットワーク）、インターネット、ＷＡＮ（ワイドエリアネットワーク）などに接続されている。

【００４７】
磁気ディスク装置９２０には、ＶＭモニター９２１、ホストＯＳ９２２、プログラム群９２３、ファイル群９２４が記憶されている。
プログラム群９２３のプログラムには、ゲストＯＳやゲストＯＳで実行されるアプリケーションが含まれる。
プログラム群９２３のプログラムは、ＣＰＵ９１１、ＶＭモニター９２１、ホストＯＳ９２２により実行される。
また、ＶＭモニター９２１自身がホストＯＳ９２２の機能を含む場合や、ホストＯＳ９２２内にＶＭモニター９２１が存在する場合もある。

【００４８】
また、ＲＡＭ９１４には、ＣＰＵ９１１に実行させるＶＭモニター９２１、ホストＯＳ９２２、ゲストＯＳのプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。
また、ＲＡＭ９１４には、ＣＰＵ９１１による処理に必要な各種データが格納される。

【００４９】
また、ＲＯＭ９１３には、ＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）プログラムが格納され、磁気ディスク装置９２０にはブートプログラムが格納されている。
物理計算機１００、１０１、１０２の起動時には、ＲＯＭ９１３のＢＩＯＳプログラム及び磁気ディスク装置９２０のブートプログラムが実行され、ＢＩＯＳプログラム及びブートプログラムによりＶＭモニター９２１、ホストＯＳ９２２が起動される。

【００５０】
また、上記プログラム群９２３には、実施の形態１～３の説明において「～部」として説明している機能を実行するプログラムが記憶されている。
プログラムは、ＣＰＵ９１１により読み出され実行される。

【００５１】
ファイル群９２４には、実施の形態１～３の説明において、「～の入力」、「～の出力」、「～の判断」、「～の参照」、「～の生成」、「～の比較」、「～の取得」、「～の設定」、「～の登録」、「～の選択」等として説明している処理の結果を示す情報やデータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。
「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラ

メータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示などのＣＰＵの動作に用いられる。

抽出・検索・参照・比較・演算・計算・処理・編集・出力・印刷・表示のＣＰＵの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリ、レジスタ、キャッシュメモリ、バッファメモリ等に一時的に記憶される。

また、実施の形態１～３で説明しているフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、ＦＤＤ９０４のフレキシブルディスク、ＣＤＤ９０５のコンパクトディスク、磁気ディスク装置９２０の磁気ディスク、その他光ディスク、ミニディスク、ＤＶＤ等の記録媒体に記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【００５２】

また、実施の形態１～３の説明において「～部」として説明しているものは、「～ステップ」、「～手順」、「～処理」としても把握できる。

すなわち、実施の形態１～３で説明したフローチャートに示すステップ、手順、処理により、物理計算機１００、１０１、１０２における動作を方法として把握することができる。

【００５３】

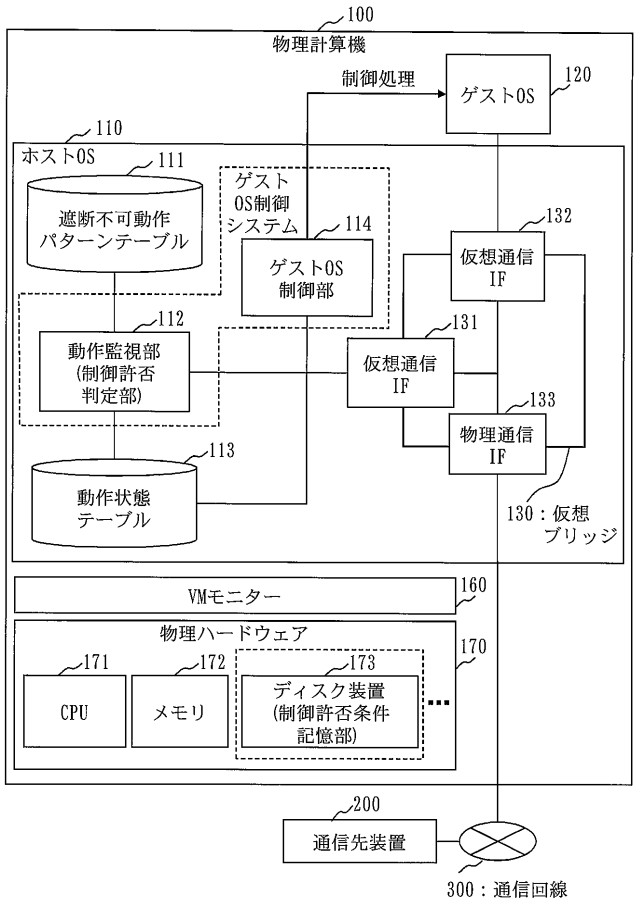
以上、実施の形態１～３に示す物理計算機１００、１０１、１０２は、処理装置たるＣＰＵ、記憶装置たるメモリ、磁気ディスク等、入力装置たるキーボード、マウス、通信ボード等、出力装置たる表示装置、通信ボード等を備えるコンピュータであり、上記したように「～部」として示された機能をこれら処理装置、記憶装置、入力装置、出力装置を用いて実現するものである。

【符号の説明】

【００５４】

１００　物理計算機、１０１　物理計算機、１０２　物理計算機、１１０　ホストＯＳ、１１１　遮断不可動作パターンテーブル、１１２　動作監視部、１１３　動作状態テーブル、１１４　ゲストＯＳ制御部、１２０　ゲストＯＳ、１３０　仮想ブリッジ、１３１　仮想通信ＩＦ、１３２　仮想通信ＩＦ、１３３　物理通信ＩＦ、１４０　ホストＯＳ、１４１　遮断不可動作パターンテーブル、１４２　動作監視部、１４３　動作状態テーブル、１４４　ゲストＯＳ制御部、１５０　ホストＯＳ、１５２　動作監視部、１５５　動作環境検出部、１５６　通信先リスト、１６０　ＶＭモニター、１７０　物理ハードウェア、１７１　ＣＰＵ、１７２　メモリ、１７３　ディスク装置、２００　通信先装置、３００　通信回線。

【図１】



【図２】

遮断不可動作パターンテーブル

111

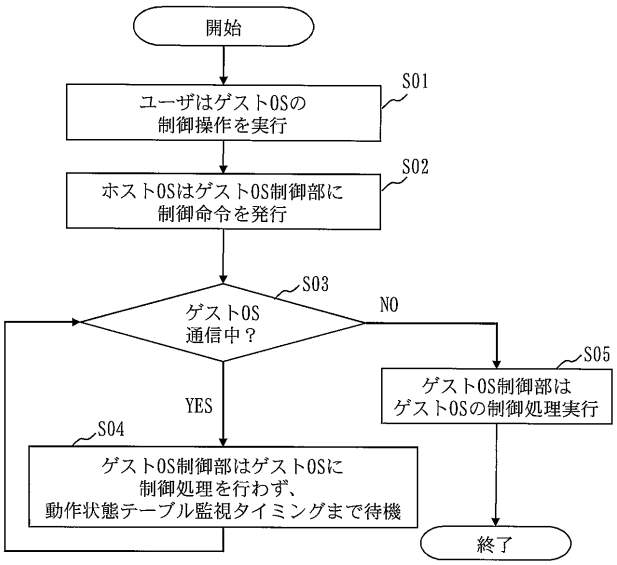
送信元	送信先	ポート	遮断不可通信 開始パターン	遮断不可通信 終了パターン
ゲストOS1	送信先1	5555	FFF9	FFCC
・・・	・・・	・・・	・・・	・・・

動作状態テーブル

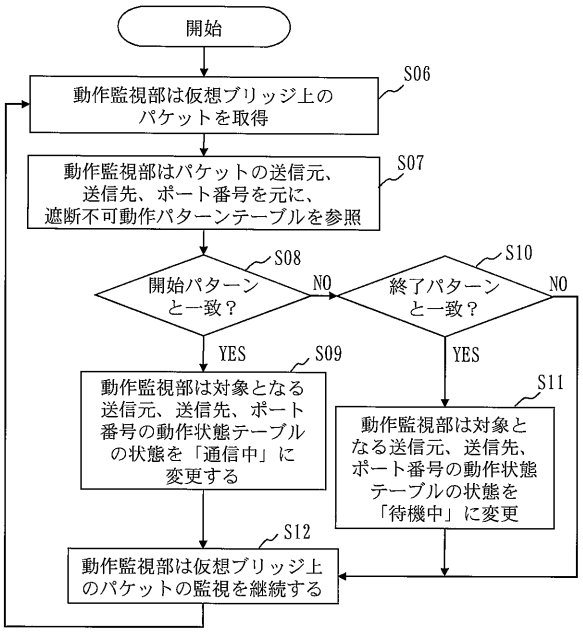
113

送信元	送信先	ポート	状態
ゲストOS1	送信先1	5555	通信中
・・・	・・・	・・・	・・・

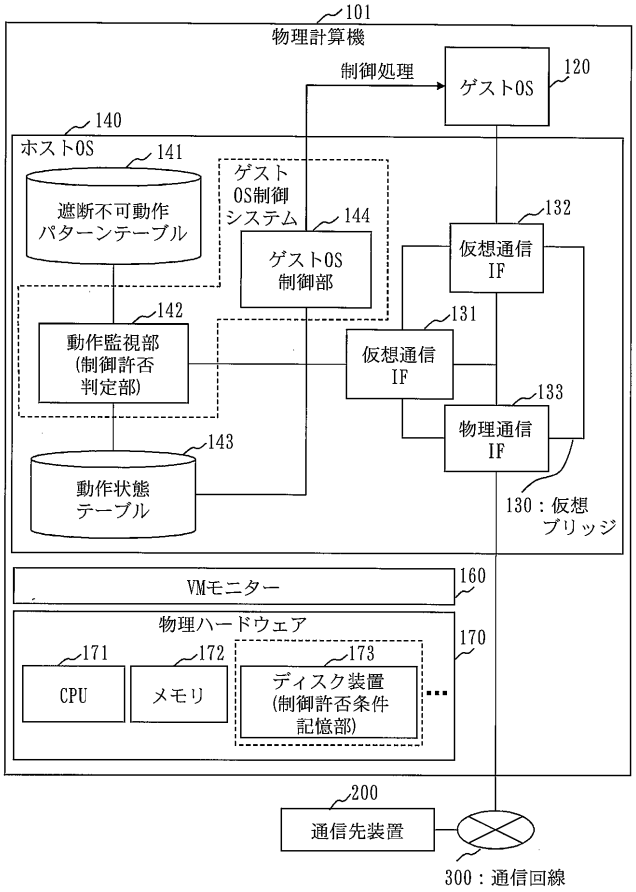
【図３】



【図４】



【図５】



【図６】

遮断不可動作パターンテーブル

141

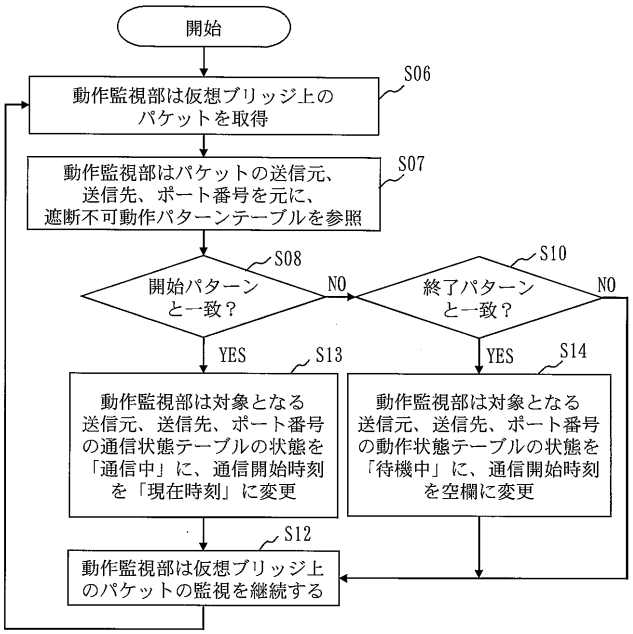
送信元	送信先	ポート	開始パターン	終了パターン	タイムアウト値
ゲストOS1	送信先1	5555	FFF9	FFCC	300
・・・	・・・	・・・	・・・	・・・	・・・

動作状態テーブル

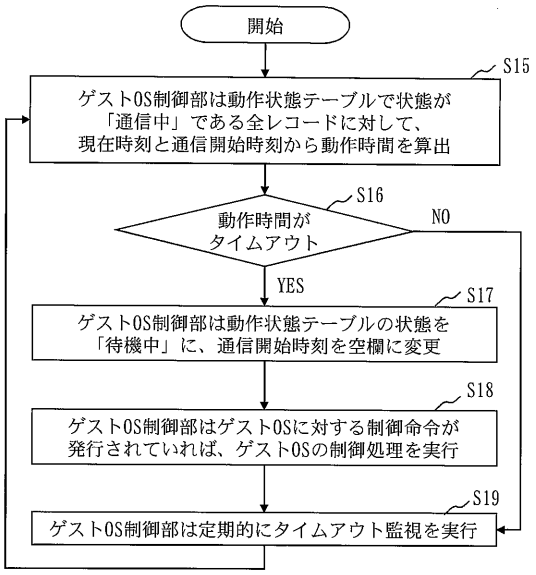
143

送信元	送信先	ポート	状態	停止要求有無	通信開始時刻
ゲストOS1	送信先1	5555	通信中	有	2010/1/1 12:00:00.000
・・・	・・・	・・・	・・・	・・・	・・・

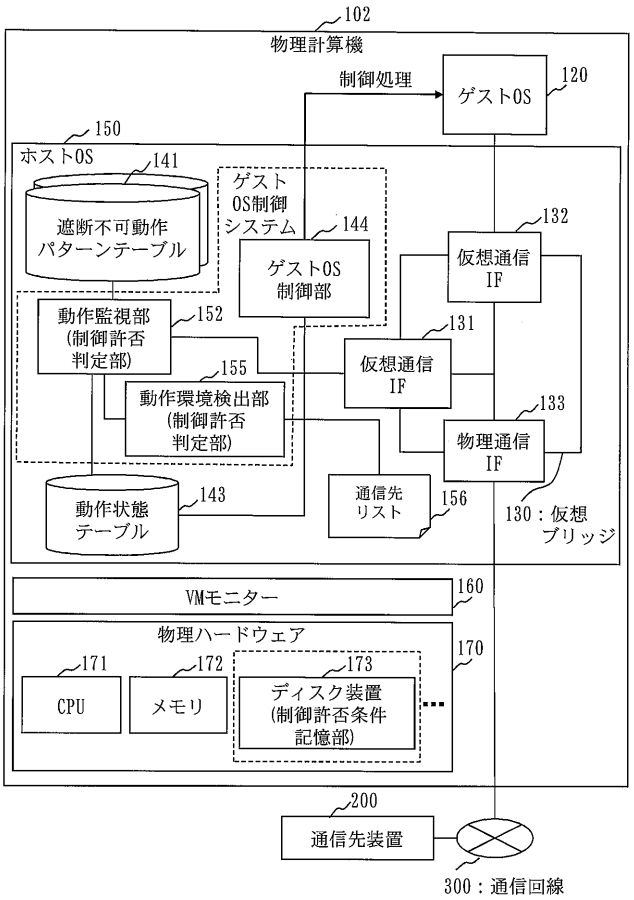
【図７】



【図８】



【図９】



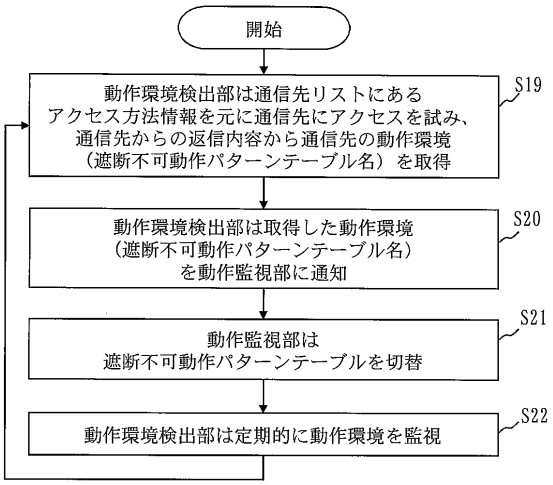
【図１０】

通信先リスト

156

通信先名	IPアドレス	通信先種別	バージョン	遮断不可動作パターンテーブル名
通信先１	192. xxx. xxx. xxx	システムA	1. 0	Tab1
通信先１	192. xxx. xxx. xxx	システムA	1. 1	Tab2
・・・	・・・	・・・	・・・	・・・

【図１１】



【図１２】