(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2010-211339
(P2010-211339A)
(43)公開日　平成22年9月24日(2010.9.24)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 9/46	(2006.01)	G06F	9/46	350	5B089
G06F 13/00	(2006.01)	G06F	13/00	351Z	

審査請求 未請求　請求項の数 6　ＯＬ　（全 15 頁）

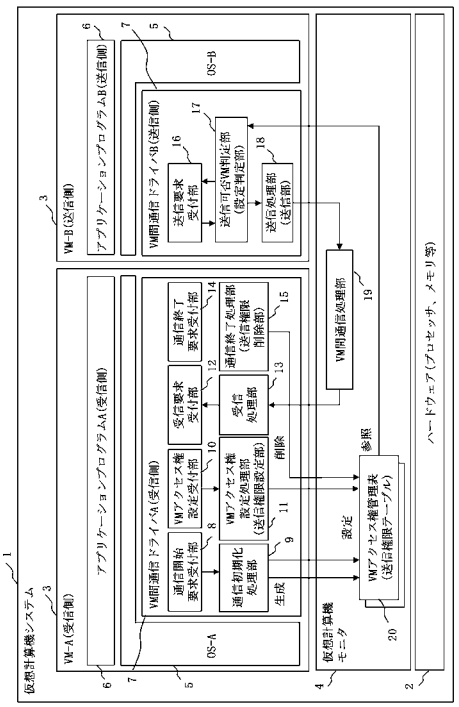
(21)出願番号　特願2009-54383(P2009-54383)
(22)出願日　平成21年3月9日(2009.3.9)

(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　100151220
弁理士　八巻　満隆
(72)発明者　片山　吉章
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

Ｆターム(参考)　5B089 KA17　KB13

(54)【発明の名称】仮想計算機システム、仮想計算機システムの通信制御プログラム及び仮想計算機システムの通信制御方法

(57)【要約】
【課題】仮想計算機システムにおいて、ＤｏＳ攻撃を回避可能なＶＭ間通信方式を実現することを目的とする。
【解決手段】仮想計算機システム１では、複数のＶＭ３（仮想計算機）が同時に動作し、各ＶＭ３は互いに仮想ネットワークを介して通信する。各ＶＭ３は、所定のＶＭ３から自己へのデータ送信を許可することを示す許可情報を、所定のＶＭ３が送信した送信データを受信する場合にVMアクセス権管理表２０に設定する。また、各ＶＭ３は、VMアクセス権管理表２０に自己から所定のＶＭ３へのデータ送信を許可することを示す許可情報が設定されているか否かを、前記所定のＶＭ３へ送信データを送信する場合に判定する。各ＶＭ３は、許可情報が設定されていると判定した場合に、前記所定のＶＭ３へ送信データを送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
１台の計算機において複数の仮想計算機が同時に動作し、前記複数の仮想計算機の各仮想計算機は互いに仮想ネットワークを介して通信する仮想計算機システムであり、
前記各仮想計算機は、
前記複数の仮想計算機の所定の仮想計算機から自己へのデータ送信を許可することを示す許可情報を、前記所定の仮想計算機が送信した送信データを受信する場合に送信権限テーブルに設定する送信権限設定部と、
前記送信権限テーブルに自己から所定の仮想計算機へのデータ送信を許可することを示す許可情報が、前記所定の仮想計算機の前記送信権限設定部により設定されているか否かを、前記所定の仮想計算機へ送信データを送信する場合に判定する設定判定部と、
前記許可情報が設定されていると前記設定判定部が判定した場合に、前記所定の仮想計算機へ送信データを送信する送信部と
を備えることを特徴とする仮想計算機システム。
【請求項２】
前記各仮想計算機は、さらに、
所定の仮想計算機の前記送信部が送信した送信データを受信する受信部と、
前記受信部が前記送信データの受信を完了した場合、前記送信権限テーブルに設定した前記所定の仮想計算機から自己へのデータ送信を許可することを示す許可情報を削除する送信権限削除部と
を備えることを特徴とする請求項１に記載の仮想計算機システム。
【請求項３】
前記送信権限設定部は、所定の仮想計算機が送信した送信データを受信する場合、前記所定の仮想計算機と共有する共有メモリに作成された前記送信権限テーブルに許可情報を設定する
ことを特徴とする請求項１又は２に記載の仮想計算機システム。
【請求項４】
前記送信権限設定部は、所定の仮想計算機の所定のプロトコルによる自己へのデータ送信を許可することを示す許可情報を、前記所定の仮想計算機が前記所定のプロトコルにより送信した送信データを受信する場合に送信権限テーブルに設定し、
前記設定判定部は、前記送信権限テーブルに自己の所定のプロトコルによる所定の仮想計算機へのデータ送信を許可することを示す許可情報が、前記所定の仮想計算機の前記送信権限設定部により設定されているか否かを、前記所定のプロトコルにより前記所定の仮想計算機へ送信データを送信する場合に判定する
ことを特徴とする請求項１から３までのいずれかに記載の仮想計算機システム。
【請求項５】
１台の計算機において複数の仮想計算機が同時に動作し、前記複数の仮想計算機の各仮想計算機は互いに仮想ネットワークを介して通信する仮想計算機システムの通信制御プログラムであり、
前記複数の仮想計算機の所定の仮想計算機から自己へのデータ送信を許可することを示す許可情報を、前記所定の仮想計算機が送信した送信データを受信する場合に送信権限テーブルに設定する送信権限設定処理と、
前記送信権限テーブルに自己から所定の仮想計算機へのデータ送信を許可することを示す許可情報が、前記所定の仮想計算機の前記送信権限設定処理で設定されているか否かを、前記所定の仮想計算機へ送信データを送信する場合に判定する設定判定処理と、
前記許可情報が設定されていると前記設定判定処理で判定した場合に、前記所定の仮想計算機へ送信データを送信する送信処理と
を各仮想計算機に実行させることを特徴とする仮想計算機システムの通信制御プログラム。
【請求項６】

１台の計算機において複数の仮想計算機が同時に動作し、前記複数の仮想計算機の各仮想計算機は互いに仮想ネットワークを介して通信する仮想計算機システムの通信制御方法であり、

前記各仮想計算機は、

前記複数の仮想計算機の所定の仮想計算機から自己へのデータ送信を許可することを示す許可情報を、前記所定の仮想計算機が送信した送信データを受信する場合に送信権限テーブルに設定する送信権限設定ステップと、

前記送信権限テーブルに自己から所定の仮想計算機へのデータ送信を許可することを示す許可情報が前記所定の仮想計算機の前記送信権限設定ステップで設定されているか否かを、前記所定の仮想計算機へ送信データを送信する場合に判定する設定判定ステップと、

前記許可情報が設定されていると前記設定判定ステップで判定した場合に、前記所定の仮想計算機へ送信データを送信する送信ステップと

を備えることを特徴とする仮想計算機システムの通信制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、１台の計算機において複数の仮想計算機が同時に動作する仮想計算機システムにおいて、各仮想計算機間の通信を制御する技術に関する。

【背景技術】

【０００２】

計算機の高性能化に伴い、単一もしくは複数のプロセッサを備える１つの計算機において複数の仮想計算機（ＶＭ：Ｖｉｒｔｕａｌ　Ｍａｃｈｉｎｅ）が実現される。各仮想計算機では、それぞれオペレーティングシステム（ＯＳ：Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）が動作する。

このような仮想計算機システムにおいては、各ＶＭは独立性が高く、あるゲストＯＳ（ＶＭで動作するＯＳのことを指す）での障害やウィルスなどの影響は、他のゲストＯＳに影響しない（非特許文献１，ｐ．１８参照）。また、各ゲストＯＳで動作するアプリケーションプログラム間の通信は、実在するネットワークアダプタをソフトウェアでエミュレートした仮想ネットワークアダプタを介して行うことができる（非特許文献１，ｐ．９８－１０４参照）。

【先行技術文献】

【非特許文献】

【０００３】

【非特許文献１】ＩＴｐｒｏ編「すべてわかる仮想化大全　ＶＭｗａｒｅ／Ｖｉｒｔｕａｌ　Ｓｅｒｖｅｒ」日経ＢＰ社、２００６年１０月３０日

【非特許文献２】Ｄａｖｉｄ　Ｃｈｉｓｎａｌｌ著、日本仮想化技術（株）監訳、渡邉了介訳「仮想化技術Ｘｅｎ－概念と内部構造」（株）毎日コミュニケーションズ、２００８年８月２０日

【非特許文献３】及川卓也、藤野衛、野坂昌己、上田英邦、森裕史著「ＷｉｎｄｏｗｓＮＴ　３．５１完全技術解説」日経ＢＰ社、１９９６年６月２０日

【非特許文献４】坂村健監修、高田広章編「μＩＴＲＯＮ４．０仕様Ｖｅｒ．４．００．００」（社）トロン協会　ＩＴＲＯＮ部会、１９９９年６月３０日

【発明の概要】

【発明が解決しようとする課題】

【０００４】

従来の仮想計算機システムのＶＭ間通信では、ＶＭをまたぐアプリケーションプログラムの通信には、仮想ネットワークアダプタを介した仮想ネットワーク機能を利用する。そのため、仮想ネットワーク機能を介してあるゲストＯＳにおけるアプリケーションプログラムから他のゲストＯＳに対し、ＤｏＳ（Ｄｅｎｉａｌ　Ｏｆ　Ｓｅｒｖｉｃｅ）攻撃を仕掛けることが可能であるという課題がある。

ＤｏＳ攻撃とはサーバなどの機器に対してネットワークを介した攻撃を行うことである。ＤｏＳ攻撃は、ネットワークトラフィックを増大させ、通信を処理している回線やサーバの機能（プロセッサやメモリ等のリソース）を占有する。これにより、サーバで実行しているサービスの提供が不能な状態になる。

非仮想計算機システムにおけるＤｏＳ攻撃の対策としては、例えば、物理ネットワークに物理的なルータを配置し、ＤｏＳ攻撃を実施してくる計算機からの通信を拒否する方法がある。しかし、仮想計算機システムにおいては、同一マシン内に存在するＶＭから攻撃されるため、物理的なルータを配置しＤｏＳ攻撃を実施してくるＶＭからの通信を拒否することができない。そのため、仮想計算機システムにおいて、ＤｏＳ攻撃を防ぐことは不可能である。

この発明は、仮想計算機システムにおいて、ＤｏＳ攻撃を回避可能なＶＭ間通信方式を実現することを目的とする。

【課題を解決するための手段】

【０００５】

この発明に係る仮想計算機システムは、例えば、

１台の計算機において複数の仮想計算機が同時に動作し、前記複数の仮想計算機の各仮想計算機は互いに仮想ネットワークを介して通信する仮想計算機システムであり、

前記各仮想計算機は、

前記複数の仮想計算機の所定の仮想計算機から自己へのデータ送信を許可することを示す許可情報を、前記所定の仮想計算機が送信した送信データを受信する場合に送信権限テーブルに設定する送信権限設定部と、

前記送信権限テーブルに自己から所定の仮想計算機へのデータ送信を許可することを示す許可情報が前記所定の仮想計算機の前記送信権限設定部により設定されているか否かを、前記所定の仮想計算機へ送信データを送信する場合に判定する設定判定部と、

前記許可情報が設定されていると前記設定判定部が判定した場合に、前記所定の仮想計算機へ送信データを送信する送信部と

を備えることを特徴とする。

【発明の効果】

【０００６】

この発明に係る仮想計算機システムでは、各仮想計算機は、データを受信する場合には許可情報を設定し、データを送信する場合には許可情報が設定されているときに限りデータを送信する。そのため、各仮想計算機は、不要なデータを受信することがなく、Ｄｏｓ攻撃を回避することができる。

【図面の簡単な説明】

【０００７】

【図１】実施の形態１に係る仮想計算機システム１の構成図。

【図２】ＶＭアクセス権管理表２０の一例を示す図。

【図３】実施の形態１に係るＶＭ３間通信方式の動作を示すフローチャート（１）。

【図４】実施の形態１に係るＶＭ３間通信方式の動作を示すフローチャート（２）。

【図５】実施の形態２に係る仮想計算機システム１の構成図。

【図６】プロトコルアクセス権管理表２４の一例を示す図。

【図７】実施の形態２に係るＶＭ３間通信方式の動作を示すフローチャート（１）。

【図８】実施の形態２に係るＶＭ３間通信方式の動作を示すフローチャート（２）。

【図９】ハードウェア２の構成の一例を示す図。

【発明を実施するための形態】

【０００８】

実施の形態１．

図１は、仮想計算機システム１の構成図である。

仮想計算機システム１は、単一もしくは複数のプロセッサ、メモリなどのハードウェア２を備える。そして、仮想計算機システム１は、複数の独立した仮想的なハードウェア環

境を提供するＶＭ３を実現する。ここでは、ＶＭ－ＡとＶＭ－ＢとのＶＭ３が実現されるものとする。また、ここでは、ＶＭ－Ａを受信側のＶＭ３とし、ＶＭ－Ｂを送信側のＶＭ３とする。また、仮想計算機システム１は、ＶＭ３で動作するＯＳ５などのプログラムの実行を制御する仮想計算機モニタ４を備える。

【０００９】

各ＶＭ３は、ＯＳ５（ＯＳ－Ａ、ＯＳ－Ｂ）を動作させる。また、各ＶＭ３は、ＯＳ５においてアプリケーションプログラム６を動作させる。さらに、各ＶＭ３は、他のＶＭ３との通信を制御するＶＭ間通信ドライバ７を動作させる。ＶＭ間通信ドライバ７は、ＯＳ５のデバイスドライバの１つとして実現される。

各ＶＭ３のＶＭ間通信ドライバ７は、通信開始要求受付部８、通信初期化処理部９、ＶＭアクセス権設定受付部１０、ＶＭアクセス権設定処理部１１（送信権限設定部）、受信要求受付部１２、受信処理部１３、通信終了要求受付部１４、通信終了処理部１５（送信権限削除部）、送信要求受付部１６、送信可否ＶＭ判定部１７（設定判定部）、送信処理部１８（送信部）を備える。なお、図１では、簡単のため、受信側のＶＭ－Ａには受信側で使用する機能のみを示し、送信側のＶＭ－Ｂには送信側で使用する機能のみを示す。

通信開始要求受付部８は、アプリケーションプログラム６からの通信開始（オープン）要求を受け付ける。通信初期化処理部９は、通信開始要求受付部８から実行され、通信の初期化処理を実行する。

ＶＭアクセス権設定受付部１０は、アプリケーションプログラム６からのＶＭアクセス権設定要求を受け付ける。ＶＭアクセス権設定処理部１１は、ＶＭアクセス権設定受付部１０から実行され、ＶＭアクセス権（許可情報）を後述するＶＭアクセス権管理表２０に設定する。

受信要求受付部１２は、アプリケーションプログラム６からの受信（リード）要求を受け付ける。受信処理部１３は、受信要求受付部１２から実行され、他のＶＭ３から送信された送信データを受信する。

通信終了要求受付部１４は、アプリケーションプログラム６からの通信終了（クローズ）要求を受け付ける。通信終了処理部１５は、通信終了要求受付部１４から実行され、通信の終了処理を実行する。

送信要求受付部１６は、アプリケーションプログラム６からの送信（ライト）要求を受け付ける。送信可否ＶＭ判定部１７は、送信要求受付部１６から実行され、他のＶＭ３へ送信データを送信することの可否を判定する。送信処理部１８は、送信可否ＶＭ判定部１７から実行され、他のＶＭ３へ送信データを送信する。

【００１０】

仮想計算機モニタ４は、ＶＭ間通信処理部１９、ＶＭアクセス権管理表２０（送信権限テーブル）を備える。

ＶＭ間通信処理部１９は、ＶＭ３間の通信を実現する仮想ネットワークである。

ＶＭアクセス権管理表２０は、ＶＭアクセス権が設定される。ＶＭアクセス権管理表２０は、通信初期化処理部９により生成され、ＶＭアクセス権設定処理部１１により設定される。また、ＶＭアクセス権管理表２０は、通信終了処理部１５により削除される。

図２は、ＶＭアクセス権管理表２０の一例を示す図である。ＶＭアクセス権管理表２０は、ＶＭ３の識別情報と、データ送信の許可又は拒否とが記憶される。図２では、ＶＭ－Ａへのデータ送信の許可と拒否とが、ＶＭ３毎に設定されている。図２は、ＶＭ－Ａ、ＶＭ－ＣからＶＭ－Ａへのデータ送信は拒否し、ＶＭ－ＢからＶＭ－Ａへのデータ送信は許可することを示す。

【００１１】

図３，４は、仮想計算機システム１におけるＶＭ３間通信方式の動作を示すフローチャートである。

まず、受信側のＶＭ３の動作を説明する。

異なるＶＭ３に存在するアプリケーションプログラム６同士がデータ通信を行う場合、最初に受信側のアプリケーションプログラム６がＯＳ５を介してＶＭ間通信ドライバ７に

対し、通信開始要求を出す（Ｓ１０１）。すると、ＯＳ５が持つドライバの管理機能により、ＶＭ間通信ドライバ７の通信開始要求受付部８が起動される（Ｓ１０２）。

通信開始要求受付部８は、通信初期化処理部９を呼び出す（Ｓ１０３）。通信初期化処理部９は、ＶＭ間通信処理部１９を利用するために必要な初期設定を行う。通信初期化処理部９は、例えば、通信データを格納するための共有メモリと、データ到着を通知するためのイベントチャネルの確保・設定を行う（Ｓ１０４）。ここで、共有メモリとは異なるＶＭ３間で共有可能なメモリ領域のことである。また、イベントチャネルとは、何等かの事象（イベント）が発生したことを他のＶＭ３に伝えるための手段である。共有メモリとイベントチャネルとについては非特許文献２に記載があるため、ここでは言及しない。次に、通信初期化処理部９は、ＶＭアクセス権管理表２０用の共有メモリを確保する（Ｓ１０５）。通信初期化処理部９は、他のＶＭ３に対してはリードオンリーで共有できるよう設定を行う（Ｓ１０６）。次に、通信初期化処理部９は、確保した共有メモリにＶＭアクセス権管理表２０を生成する（Ｓ１０７）。このとき、生成時のＶＭアクセス権管理表２０の初期内容は拒否でも許可でも構わない。ここでは安全のため、すべてのＶＭからの送信を拒否するよう設定しておくものとする。また、（Ｓ１０６）での設定により、ＶＭアクセス権管理表２０への書き込みは、共有メモリを設定したＶＭ３のみが行え、他のＶＭ３はＶＭアクセス権管理表２０からの読み込みのみ行える。

なお、通信開始要求受付部８および通信初期化処理部９の処理が成功すると、ＯＳ５はアプリケーションプログラム６に対し、以降の処理にてＶＭ間通信ドライバ７へアクセスする際に利用する識別子を返す。ここでは、識別子は、ＵＮＩＸ（登録商標）オペレーティングシステムを例とし、ファイルディスクリプタとする。

【００１２】

次に、受信側のアプリケーションプログラム６がＯＳ５を介してＶＭ間通信ドライバ７に対し、ＶＭ３を特定する識別子（ＩＤ）を指定してＶＭアクセス権設定要求を出す（Ｓ１０８）。ここでは、送信を許可するＶＭ３の識別子を指定する。なお、アプリケーションプログラム６は、通信開始要求を出した結果、返されたファイルディスクリプタを利用して、通信開始要求受付部８に対し、ＶＭアクセス権設定要求を出す。また、ＶＭ３を特定するＩＤとは、送信を許可するＶＭ３を一意に特定できるものであればよく、例えば整数（ＶＭ番号）や文字列（ＶＭ名）である。すると、ＯＳ５が持つドライバの管理機能により、ＶＭ間通信ドライバ７のＶＭアクセス権設定受付部１０が起動される（Ｓ１０９）。

ＶＭアクセス権設定受付部１０は、ＶＭアクセス権設定処理部１１を呼び出す（Ｓ１１０）。ＶＭアクセス権設定処理部１１は、ＶＭアクセス権管理表２０のうち、受信側のアプリケーションプログラム６が指定したＶＭ３に該当する部分の設定を許可に変更する（Ｓ１１１）。つまり、ＶＭアクセス権設定処理部１１は、アプリケーションプログラム６が指定したＶＭ３から自己へのデータ送信を許可するように、ＶＭアクセス権管理表２０の情報を変更する。

【００１３】

次に、受信側のアプリケーションプログラム６がＯＳ５を介してＶＭ間通信ドライバ７に対し、受信要求を出す（Ｓ１１２）。すると、ＯＳ５が持つドライバの管理機能により、ＶＭ間通信ドライバ７の受信要求受付部１２が起動される（Ｓ１１３）。

受信要求受付部１２は、受信処理部１３を呼び出す（Ｓ１１４）。受信処理部１３は、既に受信可能なデータが到着済みか判定する（Ｓ１１５）。受信処理部１３は、既にデータが到着していれば（Ｓ１１５でＹＥＳ）、（Ｓ１２７）へ処理を移す。一方、受信処理部１３は、まだデータが到着していなければ（Ｓ１１５でＮＯ）、ＶＭ間通信処理部１９からデータ到着の通知が来るまで待機する（Ｓ１１６）。ここで、ＯＳ５には通常、送受信が完了してから続きの処理を開始・継続する同期Ｉ／Ｏ（Ｉｎｐｕｔ／Ｏｕｔｐｕｔ）と、送受信が完了していなくても可能な処理を進める非同期Ｉ／Ｏとの２種類のＩ／Ｏ待ちの仕組みが存在する。しかし、ここでいう待機は、どちらの仕組みでも構わない。これらの仕組みについては非特許文献３に記載があるので、ここでは言及しない。また、待機

を行う際、あらかじめ指定された時間内に待機を解除する事象が発生しなかった場合にタイムアウトが発生したというエラーで呼び出し元にリターンしてもよい。この仕組みについては非特許文献４に記載があるので、ここでは言及しない。

また、（Ｓ１１５）の処理において、既にデータを受信している場合とは、受信側のアプリケーションプログラム６のＯＳ５への受信要求（Ｓ１１２）よりも先に送信側のアプリケーションプログラム６のＯＳ５への後述する送信要求（Ｓ１１７）の処理が行われた場合のことである。このように、（Ｓ１１２）から（Ｓ１１５）までの処理と、（Ｓ１１７）から（Ｓ１２３）までの処理の順序は問わない。

【００１４】

次に、送信側のＶＭ３の動作について説明する。

送信側のアプリケーションプログラム６も受信側のアプリケーションプログラム６と同様にファイルディスクリプタを利用する。そのため、送信側のアプリケーションプログラム６もＯＳ５を介してＶＭ間通信ドライバ７に対し、通信開始要求を出す。この処理は、（Ｓ１０１）から（Ｓ１０７）の処理と同様のため、ここでは説明を省略する。また、このとき、アプリケーションプログラム６がデータの送信処理しか行わない場合は、送信のみ実施することを指定して通信開始要求を行うことにより、（Ｓ１０３）から（Ｓ１０７）の処理を省略することができる。

送信側のアプリケーションプログラム６がＯＳ５を介してＶＭ間通信ドライバ７に対し、送信先のＶＭ３を特定するＩＤを指定して送信要求を出す（Ｓ１１７）。すると、ＯＳ５が持つドライバの管理機能により、ＶＭ間通信ドライバ７の送信要求受付部１６が起動される（Ｓ１１８）。

送信要求受付部１６は、送信可否ＶＭ判定部１７を呼び出す（Ｓ１１９）。送信可否ＶＭ判定部１７はＶＭアクセス権管理表２０を参照して、送信側のアプリケーションプログラム６が指定したＶＭ３に該当する部分の設定を読み取る（Ｓ１２０）。送信可否ＶＭ判定部１７は、読み取った設定に従い、データ送信が許可されているか拒否されているかを判定する（Ｓ１２１）。ここで許可されていると判定した場合（Ｓ１２１で許可）、送信可否ＶＭ判定部１７は送信処理部１８を呼び出す（Ｓ１２２）。そして、送信処理部１８がＶＭ間通信処理部１９に対してデータを送信する（Ｓ１２３）。一方、拒否されていると判定した場合（Ｓ１２１で拒否）、送信可否ＶＭ判定部１７はアクセス違反を意味するエラー値を戻り値とし、送信要求受付部１６を介して送信側のアプリケーションプログラム６にエラーとして返す（Ｓ１２６）。

ＶＭ間通信処理部１９は（Ｓ１２３）で送信されたデータに対し、受信待ちをしているＶＭが存在するか判定する（Ｓ１２４）。受信待ちをしているＶＭが存在すれば（Ｓ１２４でＹＥＳ）、ＶＭ間通信ドライバ７は、データが到着したことを受信処理部１３に対し通知する（Ｓ１２５）。ここでの通知は例えば前記のイベントチャネルを用いて行うことができる。一方、受信待ちをしているＶＭが存在しなければ、ここでは通知処理を行わない。

【００１５】

ＶＭ間通信処理部１９からデータ到着の通知を受けると、受信処理部１３は、受信に関わる処理を再開し、データを受信する（Ｓ１２７）。データを受信すると、受信処理部１３は、受信成功を意味する値を戻り値とし、受信要求受付部１２を介して受信側のアプリケーションプログラム６に返す（Ｓ１２８）。

【００１６】

アプリケーションプログラム６がデータ通信を終えると、受信側のアプリケーションプログラム６からＯＳ５を介してＶＭ間通信ドライバ７に対し、終了処理要求を出す（Ｓ１２９）。すると、ＯＳ５が持つドライバの管理機能により、ＶＭ間通信ドライバ７の通信終了要求受付部１４が起動される（Ｓ１３０）。

通信終了要求受付部１４は、通信終了処理部１５を呼び出す（Ｓ１３１）。通信終了処理部１５は、ＶＭアクセス権管理表２０用に確保していたメモリを共有できないように設定する。さらに、その後、通信終了処理部１５は、そのメモリを解放することにより、Ｖ

Ｍアクセス権管理表２０を削除する（Ｓ１３２）。受信側のアプリケーションプログラム６と同様に送信側のアプリケーションプログラム６もデータ通信を終えた段階でＯＳ５を介してＶＭ間通信ドライバ７に対し、終了処理要求を出す。そして、（Ｓ１３１）、（Ｓ１３２）を実行する。しかし、上述したように、通信開始要求時に（Ｓ１０３）から（Ｓ１０７）の処理を省略した場合は、ＶＭアクセス権管理表２０の削除を行う必要がない。そのため、（Ｓ１３１）、（Ｓ１３２）の処理を省略できる。

【００１７】

以上のようにこの実施の形態に係る仮想計算機システム１は、データ送信前にＶＭアクセス権管理表２０を参照することにより、許可されていないデータ送信に関しては実際のデータ送信処理を避ける。そのため、悪意のあるプログラムがＤｏＳ攻撃を仕掛けても、送信先のＶＭ３の処理負荷には影響を与えない。

【００１８】

なお、上記説明では、仮想的なハードウェア環境を提供するシステムを仮想計算機システム１として説明した。しかし、仮想計算機システム１は、これに限らず、仮想的なハードウェア環境を提供しない、いわゆるマルチＯＳ環境であってもよい。いわゆるマルチＯＳ環境においても、同様の効果を得ることができる。

【００１９】

また、前記のようにＶＭアクセス権管理表２０をＶＭ３毎に備えるのではなく、システムに１つのみ備えるとしてもよい。この場合、（Ｓ１３２）では、ＶＭアクセス権管理表２０のうち、そのＶＭ３（ＶＭアクセス権管理表２０を操作しているＶＭ３）へのデータ送信の可否を示す情報のみを削除する。また、ＶＭアクセス権管理表２０をＶＭ３内のプロセス毎に具備してもよい。この場合、（Ｓ１１７）において送信要求を出す際に送信先のプロセスを一意に特定する識別子（例えば、プロセス番号やプロセス名など）を指定し、（Ｓ１２０）においてＶＭアクセス権管理表２０を参照する際に、送信先のプロセスに関連するＶＭアクセス権管理表２０を参照する。

【００２０】

また、上記説明では、受信側のアプリケーションプログラム６のＯＳ５へのＶＭアクセス権設定要求（Ｓ１０８）とＯＳ５への受信要求（Ｓ１１２）とを別々の処理とした。しかし、受信要求時に受信する特定のＶＭ３を指定し、ＶＭ間通信ドライバ７が（Ｓ１１４）の処理を行う前に（Ｓ１１０）、（Ｓ１１１）の処理を行うことにより、ＶＭアクセス権設定要求（Ｓ１０８）とＯＳ５への受信要求（Ｓ１１２）とをまとめて処理してもよい。

【００２１】

また、上記説明では、ＶＭ間通信ドライバ７が送信可否ＶＭ判定部１７を備える。しかし、ＶＭ間通信処理部１９が送信可否ＶＭ判定部１７を備えるとしてもよい。この場合、ＶＭ間通信ドライバ７は、（Ｓ１２０）から（Ｓ１２２）の処理は行わず、ＶＭ間通信処理部１９が備える送信可否ＶＭ判定部１７が（Ｓ１２３）の処理の後であって、（Ｓ１２４）の処理の前に（Ｓ１２０）、（Ｓ１２１）の処理を行う。（Ｓ１２１）での判定の結果、許可されていると判断した場合（Ｓ１２１でＹＥＳ）、送信可否ＶＭ判定部１７は（Ｓ１２４）の処理を行う。一方、（Ｓ１２１）での判定の結果、拒否されていると判断した場合（Ｓ１２１でＮＯ）、送信可否ＶＭ判定部１７は、アクセス違反を意味するエラー値を戻り値とし、送信要求受付部１６を介して送信側のアプリケーションプログラム６にエラーで返す（Ｓ１２６）。

【００２２】

また、上記説明では、受信側のアプリケーションプログラム６はＯＳ５へのＶＭアクセス権設定要求において許可要求を出すと説明した。しかし、アプリケーションプログラム６は、許可要求だけでなく、一旦許可したデータ送信を拒否できる拒否要求を出すことができるとしてもよい。この場合、（Ｓ１０９）から（Ｓ１１１）と原則として同様の処理を行う。但し、ＶＭアクセス権管理表２０の該当箇所の設定を許可ではなく、拒否に変更する部分のみ異なる。

【００２３】
実施の形態２．
実施の形態１では、ＶＭ３毎にデータ通信を許可するか否かを示すアクセス権の設定を行った。しかし、ネットワーク通信におけるトランスミッションコントロールプロトコル（ＴＣＰ：Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）やユーザデータプロトコル（ＵＤＰ：Ｕｓｅｒ Ｄａｔａ Ｐｒｏｔｏｃｏｌ）で定められたようなポート番号を用いてＶＭ３で動作している複数のプログラムのうちの１つのプログラムを通信相手として指定する場合もある。実施の形態１で説明した方法では、このような場合に、各ポート番号による通信を個別に許可や拒否することができない。実施の形態２では、ネットワークプロトコルを指定して、通信を許可や拒否する方法について説明する。
【００２４】
図５は、実施の形態２に係る仮想計算機システム１の構成図である。図５に示す仮想計算機システム１のうち、図１に示す仮想計算機システム１と同一の機能については、同一の符号を付し説明を省略する。
ＶＭ間通信ドライバ７は、ＶＭアクセス権設定受付部１０、ＶＭアクセス権設定処理部１１、送信可否ＶＭ判定部１７に代え、プロトコルアクセス権設定受付部２１、プロトコルアクセス権設定処理部２２（送信権限設定部）、送信可否プロトコル判定部２３を備える。プロトコルアクセス権設定受付部２１は、アプリケーションプログラム６からのプロトコルアクセス権設定要求を受け付ける。プロトコルアクセス権設定処理部２２は、プロトコルアクセス権設定受付部２１から実行され、プロトコル毎にプロトコルアクセス権（許可情報）を後述するプロトコルアクセス権管理表２４に設定する。送信可否プロトコル判定部２３は、送信要求受付部１６から実行され、他のＶＭ３へ所定のプロトコルにより送信データを送信することの可否を判定する。
仮想計算機モニタ４は、ＶＭアクセス権管理表２０に代え、プロトコルアクセス権管理表２４（送信権限設定テーブル）を備える。プロトコルアクセス権管理表２４は、プロトコル毎にプロトコルアクセス権が設定される。プロトコルアクセス権管理表２４は、通信初期化処理部９により生成され、プロトコルアクセス権設定処理部２２により設定される。また、プロトコルアクセス権管理表２４は、通信終了処理部１５により削除される。
図６は、プロトコルアクセス権管理表２４の一例を示す図である。プロトコルアクセス権管理表２４は、プロトコル名称、送信側アドレス、受信側アドレス、送信側ポート番号、受信側ポート番号等が記憶される。プロトコルアクセス権管理表２４に設定された情報と一致する情報を有する送信データのみ送信が許可され、その他の送信データは送信が拒否される。
【００２５】
図７，８は、仮想計算機システム１におけるＶＭ３間通信方式の動作を示すフローチャートである。なお、図３，４に示す実施の形態１に係る仮想計算機システム１におけるＶＭ３間通信方式の動作と同一の部分については説明を省略する。
（Ｓ２０１）から（Ｓ２０４）は、図３の（Ｓ１０１）から（Ｓ１０４）と同一である。（Ｓ２０４）に続き、通信初期化処理部９は、プロトコルアクセス権管理表２４用の共有メモリを確保する（Ｓ２０５）。そして、（Ｓ１０６）と同様に、リードオンリーで共有できるよう設定を行う（Ｓ２０６）。次に、通信初期化処理部９は、確保した共有メモリにプロトコルアクセス権管理表２４を生成する（Ｓ２０７）。このとき、生成時のプロトコルアクセス権管理表２４の初期内容は、所定のプロトコルについての情報が存在する状態であっても、存在しない状態であっても構わない。ここでは安全のため、１つのプロトコルについての情報も存在しない状態とする。つまりすべてのプロトコルについてＶＭ３へのデータ送信を拒否するよう設定しておくものとする。
次に、受信側のアプリケーションプログラム６がＯＳ５を介してＶＭ間通信ドライバ７に対し、自己に対する送信を許可するプロトコルを特定するパラメータを指定してプロトコルアクセス権設定要求を出す（Ｓ２０８）。なお、アプリケーションプログラム６は、通信開始要求を出した結果、返されたファイルディスクリプタを利用して、通信開始要求

受付部８に対し、ＶＭアクセス権設定要求を出す。プロトコルを特定するパラメータとは、許可するプロトコル内容を一意に特定できるものであればよく、例えば図５に示したような許可するプロトコル名称（ＴＣＰかＵＤＰかなど）、送信側アドレス（送信側インターネットプロトコルアドレス）、受信側アドレス（受信側インターネットプロトコルアドレス）、送信側ポート番号、受信側ポート番号などである。すると、ＯＳ５が持つドライバの管理機能により、ＶＭ間通信ドライバ７のプロトコルアクセス権設定受付部２１が起動される（Ｓ２０９）。

プロトコルアクセス権設定受付部２１はプロトコルアクセス権設定処理部２２を呼び出す（Ｓ２１０）。プロトコルアクセス権設定処理部２２は、プロトコルアクセス権管理表２４に、受信側のアプリケーションプログラム６が指定した許可するプロトコル内容を設定（表に追加）する（Ｓ２１１）。

（Ｓ２１２）から（Ｓ２１６）は、図４の（Ｓ１１２）から（Ｓ１１６）と同一である。

【００２６】

次に、送信側のＶＭ３の動作について説明する。

送信側のアプリケーションプログラム６も受信側のアプリケーションプログラム６と同様にファイルディスクリプタを利用する。そのため、送信側のアプリケーションプログラム６もＯＳ５を介してＶＭ間通信ドライバ７に対し、通信開始要求を出す。この処理は、（Ｓ２０１）から（Ｓ２０７）の処理と同様のため、ここでは説明を省略する。また、このとき、アプリケーションプログラム６がデータの送信処理しか行わない場合は、送信のみ実施することを指定して通信開始要求を行うことにより、（Ｓ２０３）から（Ｓ２０７）の処理を省略することができる。

（Ｓ２１７）から（Ｓ２１８）は、図４の（Ｓ１１７）から（Ｓ１１８）と同一である。

送信要求受付部１６は、送信可否プロトコル判定部２３を呼び出す（Ｓ２１９）。送信可否プロトコル判定部２３はプロトコルアクセス権管理表２４を参照して（Ｓ２２０）、送信側のアプリケーションプログラム６が利用するプロトコル内容に一致するものが存在するか否かを判定する（Ｓ２２１）。ここで存在すると判定した場合、許可されていると判断し（Ｓ２２１で許可）、送信可否プロトコル判定部２３は送信処理部１８を呼び出す（Ｓ２２２）。そして、送信処理部１８がＶＭ間通信処理部１９に対してデータを送信する（Ｓ２２３）。一方、存在しないと判定した場合、拒否されていると判断し（Ｓ２２１で拒否）、送信可否プロトコル判定部２３はアクセス違反を意味するエラー値を戻り値とし、送信要求受付部１６を介して送信側のアプリケーションプログラム６にエラーで返す（Ｓ２２６）。

（Ｓ２２４）から（Ｓ２２５）は、図４の（Ｓ１２４）から（Ｓ１２５）と同一である。また、（Ｓ２２７）から（Ｓ２３１）は、図４の（Ｓ１２７）から（Ｓ１３１）と同一である。そして、（Ｓ２３１）で呼び出された通信終了処理部１５は、プロトコルアクセス権管理表２４用に確保していたメモリを共有できないように設定する。さらに、その後、通信終了処理部１５は、そのメモリを解放することにより、プロトコルアクセス権管理表２４を削除する（Ｓ２３２）。受信側のアプリケーションプログラム６と同様に送信側のアプリケーションプログラム６もデータ通信を終えた段階でＯＳ５を介してＶＭ間通信ドライバ７に対し、終了処理要求を出す。そして、（Ｓ２３１）、（Ｓ２３２）を実行する。しかし、上述したように、通信開始要求時に（Ｓ２０３）から（Ｓ２０７）の処理を省略した場合は、ＶＭアクセス権管理表２０の削除を行う必要がない。そのため、（Ｓ２３１）、（Ｓ２３２）の処理を省略できる。

【００２７】

以上のようにこの実施の形態に係る仮想計算機システム１は、自己に対してＶＭ３毎に送信許可するのではなく、指定したネットワークプロトコル名称、送信側アドレス、受信側アドレス、送信側ポート番号、受信側ポート番号が一致するもののみ送信許可する。そのため、ＶＭ３間で通信可能なアプリケーションプログラムを限定することができ、シス

テムの安全性を高めることができる。

【００２８】

また、上記説明では、受信側アプリケーションプログラム６はＯＳ５へのプロトコルアクセス権設定要求において許可要求を出すと説明した。しかし、アプリケーションプログラム６は、許可要求だけでなく、一旦許可したデータ送信を拒否できる拒否要求を出すことができるとしてもよい。この場合、（Ｓ２０９）から（Ｓ２１１）と原則として同様の処理を行う。但し、（Ｓ２１１）において、指定したプロトコル内容を追加するのではなく、削除する部分のみ異なる。

【００２９】

また、上記説明では、プロトコルアクセス権管理表２４には送信を許可するネットワークプロトコル名称、送信側アドレス、受信側アドレス、送信側ポート番号、受信側ポート番号などのリストを記憶すると説明した。しかし、送信を拒否するネットワークプロトコル名称、送信側アドレス、受信側アドレス、送信側ポート番号、受信側ポート番号などのリストを記憶してもよい。この場合、（Ｓ２０７）でプロトコルアクセス権管理表２４を生成した際に初期内容が存在しないとすると、すべてのプロトコルにおいて自己への送信を許可する設定になる。そのため、（Ｓ２０８）では自己への送信を拒否するプロトコルを特定するパラメータを指定してプロトコルアクセス権設定要求を出すことになる。さらに、（Ｓ２２１）で存在しないと判定した場合、許可されていると判断し（Ｓ２２１で許可）、（Ｓ２２２）、（Ｓ２２３）を実行する。一方、（Ｓ２２１）で存在すると判定した場合、拒否されていると判断し（Ｓ２２１で拒否）、送信可否プロトコル判定部２３はアクセス違反を意味するエラー値を戻り値とし、送信要求受付部１６を介して送信側のアプリケーションプログラム６にエラーで返す（Ｓ２２６）。

【００３０】

また、上記説明では、実施の形態１で説明したＶＭ３毎に自己への送信を許可することについて述べていないが、プロトコルアクセス権設定受付部２１、プロトコルアクセス権設定処理部２２、送信可否プロトコル判定部２３、プロトコルアクセス権管理表２４とを、ＶＭアクセス権設定受付部１０、ＶＭアクセス権設定処理部１１、送信可否ＶＭ判定部１７、ＶＭアクセス権管理表２０と併用することも可能である。つまり、ＶＭ３毎、かつプロトコル毎に送信の可否が判断される。この場合、（Ｓ２０５）から（Ｓ２０７）において、ＶＭアクセス権管理表２０とプロトコルアクセス権管理表２４とを生成する。（Ｓ２２０）においてＶＭアクセス権管理表２０とプロトコルアクセス権管理表２４とを参照して、許可か拒否かを判定する。（Ｓ２３２）において、ＶＭアクセス権管理表２０とプロトコルアクセス権管理表２４と用に確保していたメモリを共有できないように設定して、解放する。これにより、送信可能なＶＭ３を限定しつつ、送信可能なプロトコルを限定することができるため、単独で実施した場合よりも安全性を高められる。

【００３１】

次に、実施の形態における仮想計算機システム１のハードウェア２の構成について説明する。

図９は、仮想計算機システム１のハードウェア２の構成の一例を示す図である。

図９に示すように、ハードウェア２は、プログラムを実行するＣＰＵ９１１（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ＲＯＭ９１３、ＲＡＭ９１４、ＬＣＤ９０１（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）、キーボード９０２（Ｋ／Ｂ）、通信ボード９１５、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０（固定ディスク装置）の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。磁気ディスク装置９２０は、所定の固定ディスクインタフェースを介して接続される。

【００３２】

ＲＯＭ９１３、磁気ディスク装置９２０は、不揮発性メモリの一例である。ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３とＲＡＭ９１４と磁気ディスク装置９２

０とは、メモリ（記憶装置）の一例である。また、キーボード９０２、通信ボード９１５は、入力装置の一例である。

【００３３】

磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、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のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

【００３４】

仮想計算機システム１は、以上のハードウェアを用いて、複数のＶＭ３を実現する。つまり、ＶＭ３毎にＲＡＭ９１４の領域を割り当て、ＶＭ３毎にＣＰＵ９１１を例えばタイムシェアリングにより割り当て、ＶＭ３毎にＯＳを起動させる。そして、仮想計算機システム１は、ＶＭ３毎に、割り当てたハードウェア資源を利用して、アプリケーションプログラム６やＶＭ間通信ドライバ７等のプログラムを実行する。

【００３５】

つまり、プログラム群９２３には、上記の説明において「仮想計算機モニタ４」（「ＶＭ間通信処理部１９」）、「アプリケーションプログラム６」、「通信開始要求受付部８」（「ＶＭアクセス権設定処理部１１」、「受信要求受付部１２」、「受信処理部１３」、「通信終了要求受付部１４」、「通信終了処理部１５」、「送信要求受付部１６」、「送信可否ＶＭ判定部１７」、「送信処理部１８」、「プロトコルアクセス権設定受付部２１」、「プロトコルアクセス権設定処理部２２」、「送信可否プロトコル判定部２３」）等として説明した機能を実行するソフトウェアやプログラムやその他の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。

ファイル群９２４には、上記の説明において「ＶＭアクセス権管理表２０」、「プロトコルアクセス権管理表２４」等の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・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１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、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

【００３６】

なお、上記の説明におけ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、その他光ディスク等の記録媒体やＩＣチップに記録される。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や電波によりオンライン伝送される。

また、上記の説明において「～部」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。また、「～装置」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。さらに、「～処理」として説明するものは「～ステップ」であっても構わない。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、ＲＯＭ９１３等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、上記で述べた「～部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた「～部」の手順や方法をコンピュータ

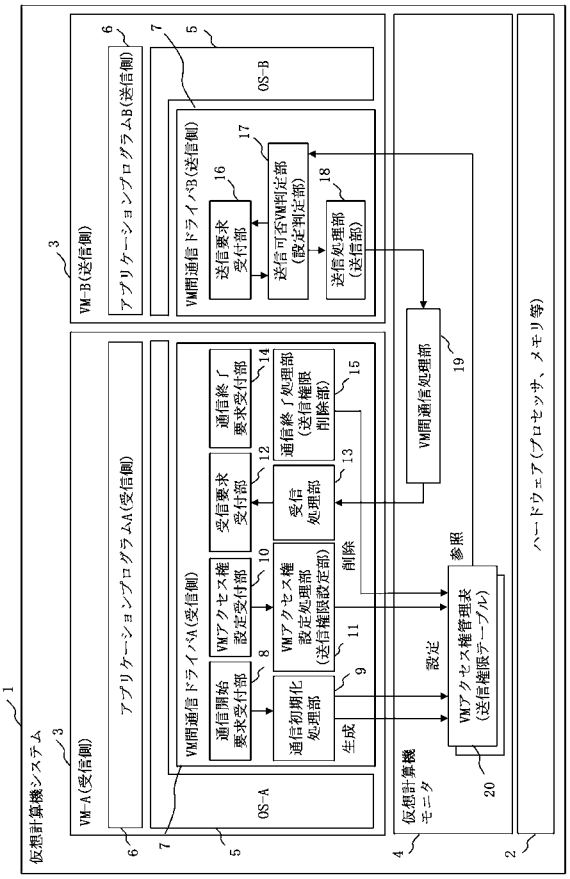
等に実行させるものである。

【符号の説明】

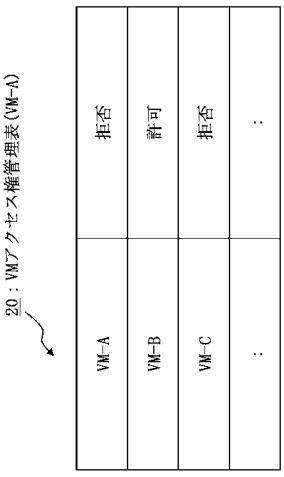
【００３７】

１　仮想計算機システム、２　ハードウェア、３　ＶＭ、４　仮想計算機モニタ、５　ＯＳ、６　アプリケーションプログラム、７　ＶＭ間通信ドライバ、８　通信開始要求受付部、９　通信初期化処理部、１０　ＶＭアクセス権設定受付部、１１　ＶＭアクセス権設定処理部、１２　受信要求受付部、１３　受信処理部、１４　通信終了要求受付部、１５　通信終了処理部、１６　送信要求受付部、１７　送信可否ＶＭ判定部、１８　送信処理部、１９　ＶＭ間通信処理部、２０　ＶＭアクセス権管理表、２１　プロトコルアクセス権設定受付部、２２　プロトコルアクセス権設定処理部、２３　送信可否プロトコル判定部、２４　プロトコルアクセス権管理表。

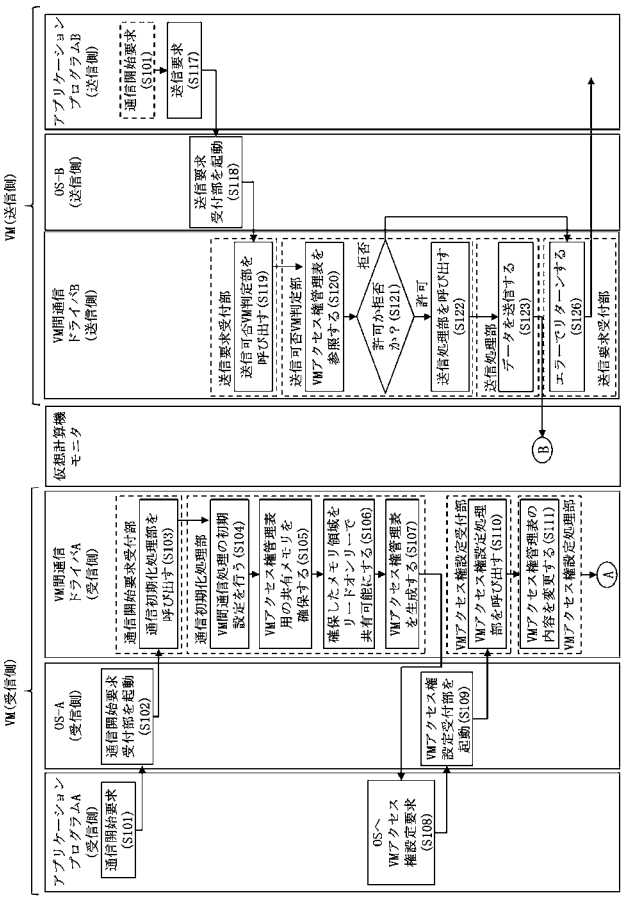
【図１】



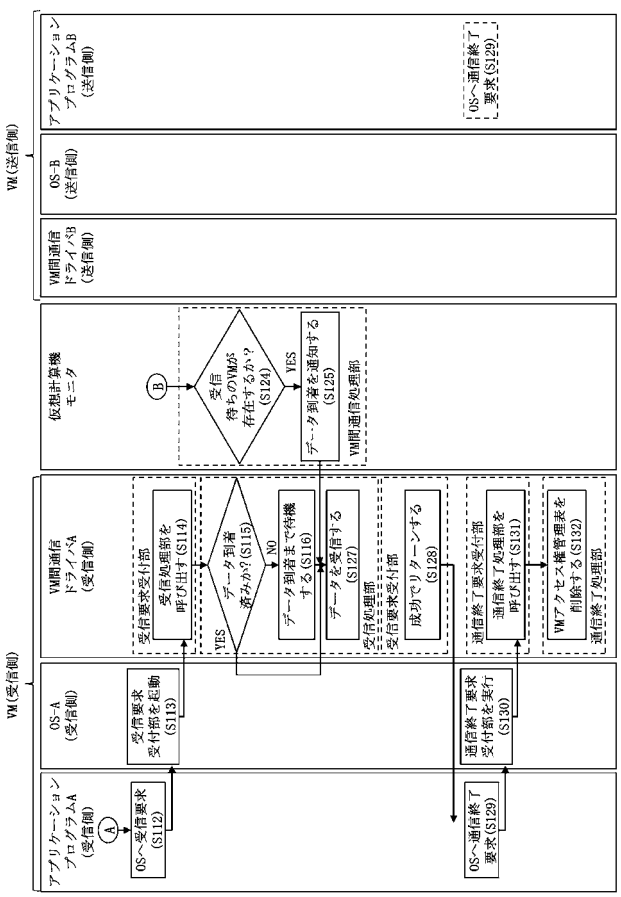
【図２】



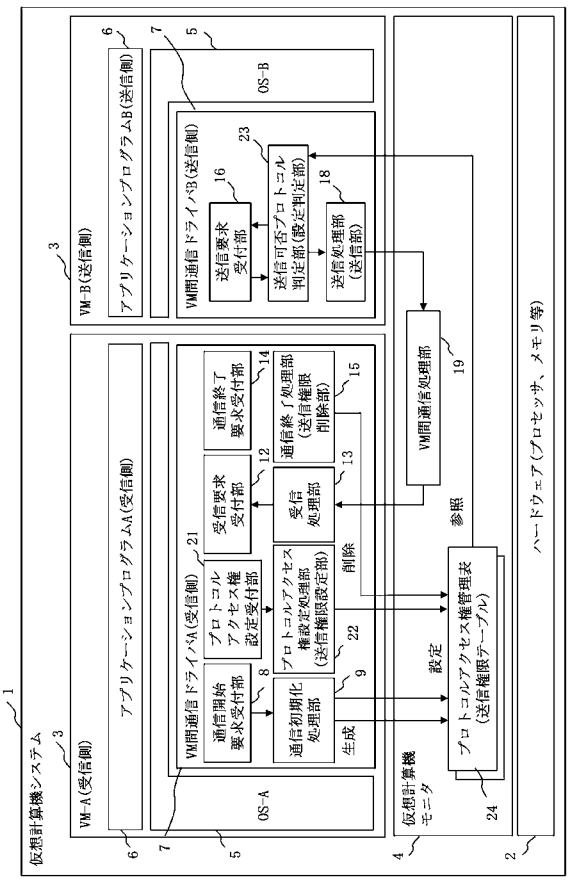
【図３】



【図４】



【図５】

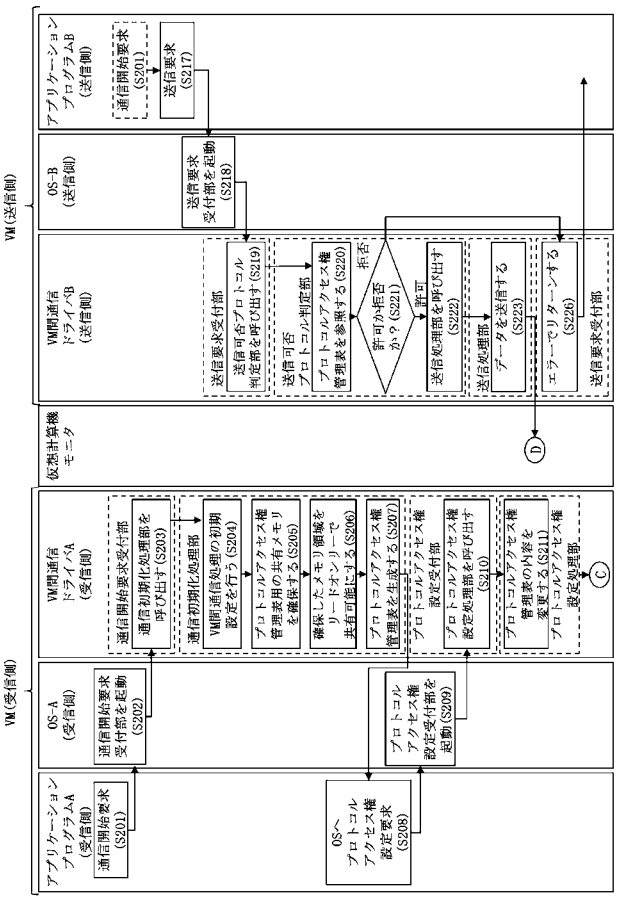


【図６】

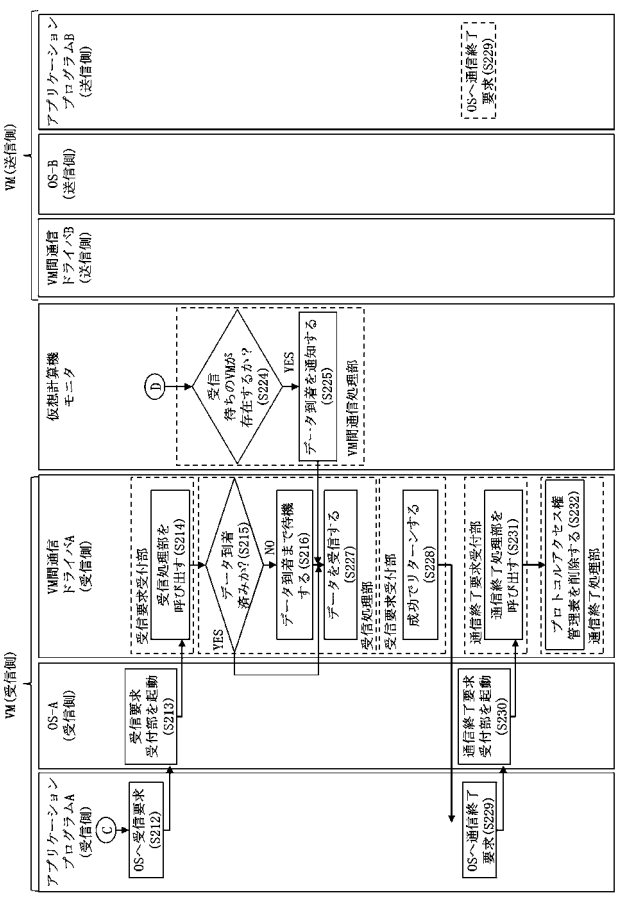
24：プロトコルアクセス権管理表(VM-A)

プロトコル名称	送信側アドレス	受信側アドレス	送信側ポート番号	受信側ポート番号	…
:	:	:	:	:	:

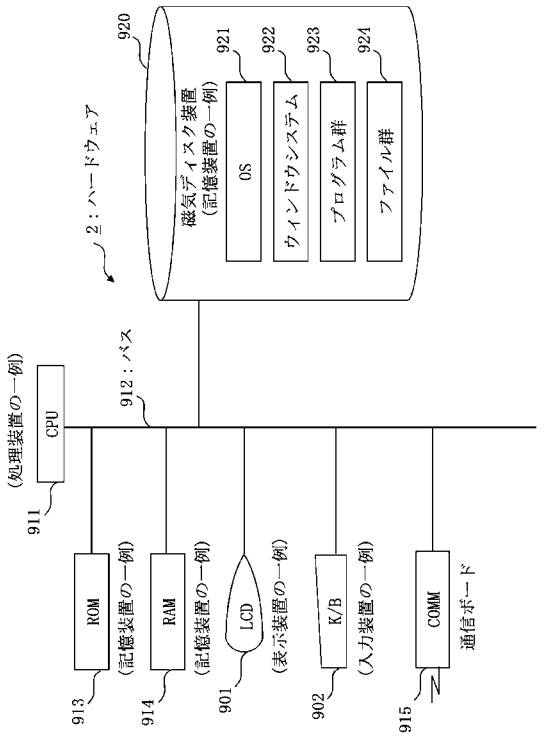
【図７】


VM(送信側)
VM(受信側)
アプリケーションプログラムAA (受信側)
OS-A (受信側)
VM間通信ドライバA (受信側)
仮想計算機モニタ
VM間通信ドライバB (送信側)
OS-B (送信側)
アプリケーションプログラムB (送信側)
通信開始要求 (S201)
通信開始要求受付部
通信初期化処理部を呼び出す (S203)
通信初期化処理部
VM間通信処理の初期設定を行う (S204)
プロトコルアクセス権管理表用の共有メモリを確保する (S205)
確保したメモリ領域をリードオンリーで共有可能にする (S206)
プロトコルアクセス権管理表を生成する (S207)
プロトコルアクセス権設定受付部
プロトコルアクセス権設定処理部を呼び出す (S210)
プロトコルアクセス権設定処理部
管理表の内容を変更する (S211)
プロトコルアクセス権設定処理部
通信開始要求受付部を起動 (S202)
プロトコルアクセス権設定受付部を起動 (S209)
OSへプロトコルアクセス権設定要求 (S208)
送信要求 (S217)
送信要求受付部を起動 (S218)
送信要求受付部
送信可否プロトコル判定部を呼び出す (S219)
送信可否プロトコル判定部
プロトコルアクセス権管理表を参照する (S220)
許可か拒否か？ (S221)
拒否
許可
送信処理部を呼び出す (S222)
送信処理部
データを送信する (S223)
エラーでリターンする (S226)
送信要求受付部
D
C

【図８】


VM(送信側)
VM(受信側)
アプリケーションプログラムAA (受信側)
OS-A (受信側)
VM間通信ドライバA (受信側)
仮想計算機モニタ
VM間通信ドライバB (送信側)
OS-B (送信側)
アプリケーションプログラムB (送信側)
OS～通信終了要求 (S229)
OS～受信要求 (S212)
受信要求受付部
受信処理部を呼び出す (S214)
受信要求受付部を起動 (S213)
受信待ちのVMが存在するか？ (S224)
YES
NO
データ到着済みか？ (S215)
データ到着まで待機する (S216)
データを受信する (S227)
受信処理部
受信要求受付部
成功でリターンする (S228)
データ到着を通知する (S225)
VM間通信処理部
通信終了要求受付部
通信終了処理部を呼び出す (S231)
通信終了要求受付部を起動 (S230)
プロトコルアクセス権管理表を削除する (S232)
通信終了処理部
OS～通信終了要求 (S229)
C
D

【図９】


2：ハードウェア
920
磁気ディスク装置（記憶装置の一例）
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
912：バス
911
CPU
（処理装置の一例）
913
ROM
（記憶装置の一例）
914
RAM
（記憶装置の一例）
901
LCD
（表示装置の一例）
902
K/B
（入力装置の一例）
915
COMM
通信ボード