(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 11 月 22 日(22.11.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/157166 A1

(51) 国際特許分類:
G06F 9/54 (2006.01) *G06F 9/46* (2006.01)

(21) 国際出願番号: PCT/JP2012/002229

(22) 国際出願日: 2012 年 3 月 30 日(30.03.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2011-109028 2011 年 5 月 16 日(16.05.2011) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 神山　輝壮 (KAMIYAMA, Teruo). 天野　克重 (AMANO, Katsushige). 齊藤　雅彦 (SAITO, Masahiko). 谷川　忠雄 (TANIKAWA, Tadao).

(74) 代理人: 小谷　悦司, 外 (KOTANI, Etsuji et al.); 〒5300005 大阪府大阪市北区中之島２丁目２番２号大阪中之島ビル２階 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS,

[続葉有]

(54) **Title**: VIRTUAL COMPUTER SYSTEM, CONTROL METHOD FOR VIRTUAL COMPUTER SYSTEM, CONTROL PROGRAM FOR VIRTUAL COMPUTER SYSTEM, AND INTEGRATED CIRCUIT

(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制御方法、仮想計算機システムの制御プログラム、及び集積回路

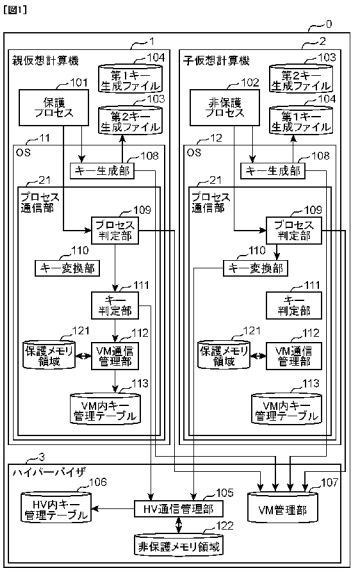


FIG. 1:
1 Parent virtual computer
2 Child virtual computer
3 Hypervisor
21 Process communication unit
101 Protected process
102 Unprotected process
103 Second key generation file
104 First key generation file
105 Hypervisor communication management unit
106 Intra-hypervisor key management table
107 VM management unit
108 Key generation unit
109 Process assessment unit
110 Key conversion unit
111 Key assessment unit
112 VM communication management unit
113 Intra-VM key management table
121 Protected memory area
122 Unprotected memory area

(57) **Abstract**: In the present invention, a key assessment unit (111) assesses whether an object key, which is a key generated by a key generation unit (108), is a key of a first or a second type on the basis of key conversion rules if a process has been assessed to be a protected process (101) by a process assessment unit (109). A VM communication management unit (112) notifies the process of the memory ID of a protected memory area (121) corresponding to the first type of key if the object key has been assessed to be a key of the first type by the key assessment unit (111). A key conversion unit (110) converts the object key from a key of the first type to a key of the second type on the basis of the key conversion rules if the process has been assessed to be an unprotected process (101) by the process assessment unit (109). A hypervisor communication management unit (105) notifies the process of the memory ID of an unprotected memory area (122) corresponding to the second type of key.

(57) 要約:

[続葉有]

WO 2012/157166 A1

LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

キー判定部１１１は、プロセス判定部１０９により、対象プロセスが保護プロセス１０１であると判定された場合、キー生成部１０８により生成されたキーである対象キーが、第１又は第２種のキーであるかをキー変換ルールに基づいて判定する。ＶＭ通信管理部１１２は、キー判定部１１１により、対象キーが第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域１２１のメモリＩＤを対象プロセスに通知する。キー変換部１１０は、プロセス判定部１０９により、対象プロセスが非保護プロセスであると判定された場合、キー変換ルールに基づき、対象キーを第１種のキーから第２種のキーに変換する。ＨＶ通信管理部１０５は、第２種のキーに対応する非保護メモリ領域１２２のメモリＩＤを対象プロセスに通知する。

明　細　書

発明の名称 ：

仮想計算機システム、仮想計算機システムの制御方法、仮想計算機システムの制御プログラム、及び集積回路

技術分野

[0001] 本発明は、複数の仮想計算機と仮想計算機を制御するハイパーバイザとを備える仮想計算機システムに関するものである。

背景技術

[0002] 情報処理装置の中には、個人情報や金銭を伴うサービスの情報、著作権物などを扱うアプリケーションを持つものがある。このようなアプリケーションは悪意のある別のアプリケーションからのアクセスや、コンピュータウィルスといった攻撃から保護しなければならない。

[0003] アプリケーションを保護する一つの手段として、仮想計算機の技術を適用できる。仮想計算機を用いた環境では、一つの物理的な計算機で複数の仮想計算機が動作する。そこで、特定の隔離したいアプリケーションを一般的な処理をさせる仮想計算機とは別の仮想計算機に処理させる。これにより、隔離したい悪意のあるアプリケーションが他のアプリケーションに影響を与えることを仮想計算機レベルで防止することができる。

[0004] 本発明に関連する従来技術としては、例えば、下記に示す特許文献１、２が知られている。特許文献１には、仮想計算機を制御するハイパーバイザに共有メモリのキー管理情報を持たせ、仮想計算機間の通信を実現させる技術が開示されている。

[0005] 特許文献２には、仮想計算機間の通信のセキュリティ面の問題を解決するために、ハイパーバイザ内に仮想計算機間の通信を許可するか否かを設定する通信許可テーブルを設け、受信側のアプリケーションがその通信許可テーブルに送信を許可する送信側のアプリケーションを設定し、送信側のアプリケーションがその通信許可テーブルを参照し、仮想計算機間の通信を制御す

る技術が開示されている。

[0006] しかしながら、特許文献１の技術では、キーさえ分かれば、仮想計算機内のプロセス間通信用の共有メモリを、仮想計算機間のプロセス間通信の共有メモリとして他の仮想計算機がアクセスできる。そのため、セキュリティ面の課題がある。

[0007] また、特許文献２の技術では、通信許可テーブルを設定する受信側のアプリケーションがウイルスに感染している場合、送信を許可する送信側のアプリケーションをウイルスに感染させてしまうという課題がある。

先行技術文献

特許文献

[0008] 特許文献1：特開平１１－８５５４６号公報

特許文献2：特開２０１０－２１１３３９号公報

発明の概要

[0009] 本発明の目的は、非保護プロセスを保護プロセスと別の仮想計算機で実行させる場合において、仮想計算機同士の通信を安全に行わせることができる技術を提供することである。

[0010] 本発明の一態様による仮想計算機システムは、保護プロセスを実行する第１仮想計算機と、非保護プロセスを実行する第２仮想計算機と、前記第１、第２仮想計算機を制御するハイパーバイザとを備える仮想計算機システムであって、前記第１、第２仮想計算機は、前記非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、第１種のキーが所定のキー変換ルールで変換された第２種のキーを生成し、他のプロセスから通信依頼が発行された場合、前記第１種のキーを生成するキー生成部と、前記通信依頼を発行したプロセスである対象プロセスが、前記保護プロセス又は前記非保護プロセスであるかを判定するプロセス判定部と、前記プロセス判定部により、前記対象プロセスが前記保護プロセスであると判定された場合、前記キー生成部により生成されたキーである対象キーが、前記第１種のキー又は前記第２種のキーであるかを判定するキー判定部と、前記キー判定部により、前記

対象キーが前記第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＶＭ通信管理部とを備え、前記ハイパーバイザは、前記キー判定部により、前記対象キーが前記第２種のキーと判定された場合、当該第２種のキーに対応する非保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＨＶ通信管理部を備え、前記第１、第２仮想計算機は、前記プロセス判定部により、前記対象プロセスが前記非保護プロセスであると判定された場合、前記キー変換ルールに基づき、前記対象キーを前記第１種のキーから前記第２種のキーに変換するキー変換部を更に備え、前記ＨＶ通信管理部は、前記キー変換部により変換された第２種のキーに対応する前記非保護メモリ領域のメモリＩＤを前記対象プロセスに通知する。

図面の簡単な説明

[0011] [図1]実施の形態による仮想計算機システムの機能ブロック図である。

[図2]本発明の実施の形態による仮想計算機システムの動作を示すフローチャートである。

[図3]（Ａ）は本発明の実施の形態による第１キー生成ファイルの一例を示した図である。（Ｂ）は本発明の実施の形態による第２キー生成ファイルの一例を示した図である。

[図4]本発明の実施の形態において、ＶＭ通信管理部に保護メモリ領域の使用依頼が通知された際の処理を示すフローチャートである。

[図5]（Ａ）はＶＭ内キー管理テーブルの一例を示した図である。（Ｂ）はＨＶ内キー管理テーブルの一例を示した図である。

[図6]本発明の実施の形態による仮想計算機システムにおいて、キーが生成されてからメモリＩＤが通知されるまでの処理の流れを示した図である。

[図7]ＶＭ管理情報の一例を示した図である。

[図8]本発明の実施の形態による仮想計算機システムのハードウェア構成を示すブロック図である。

[図9]本発明の実施の形態において、ＨＶ通信管理部に非保護メモリ領域の使

用依頼が通知された際の処理を示すフローチャートである。

発明を実施するための形態

[0012] （本発明の実施の形態を得るに至った経緯）

背景技術でも述べたように、個人情報や金銭を伴うサービスの情報、著作権物などを扱うアプリケーションは、悪意のある別のアプリケーションからのアクセスや、コンピュータウィルスといった攻撃から保護しなければならない。そして、それを解決するために、特定の隔離したいアプリケーションを一般的な処理をさせる仮想計算機とは別の仮想計算機に処理させることも背景技術で述べた。

[0013] ところで、仮想計算機を新たに生成する技術として、動作している仮想計算機を複製させて動的に生成させることが提案されている。このように、仮想計算機を複製して動的に生成することは“仮想計算機のフォーク”と呼ばれている。また、複製元の仮想計算機は“親仮想計算機”と呼ばれ、複製された仮想計算機は“子仮想計算機”と呼ばれている。

[0014] 隔離したいアプリケーションを起動する際に仮想計算機のフォークを実行して子仮想計算機を生成し、子仮想計算機上でそのアプリケーションを起動して処理させる。これにより、保護対象のアプリケーションは、隔離されたアプリケーションによる悪意のある攻撃から保護される。

[0015] 反対に親仮想計算機に危険なアプリケーションを起動させ、子仮想計算機に保護したいアプリケーションを起動させても、保護対象のアプリケーションを危険なアプリケーションから保護することができる。そして、子仮想計算機上でアプリケーションの処理が終わると、子仮想計算機は消滅され、隔離されたアプリケーションは消滅する。

[0016] 仮想計算機のフォークによって、子仮想計算機上に隔離されたアプリケーションのプロセスと複製元の親仮想計算機上で動作しているアプリケーションのプロセスとが通信する場合、仮想計算機間を跨いだプロセス間通信が行われる。

[0017] 一般的なプロセス間通信としては、共有メモリを用いるものが知られてい

る。この通信では、あるプロセスが共有メモリを生成し、別のプロセスがこの共有メモリを使用することによって、つまり、プロセス同士が共有メモリを共有することによってデータが送受される。共有メモリを生成する際にはキーが必要であり、キーによって共有メモリが識別される。通信するプロセス同士は、同じキーを提示することによって同じ共有メモリを共有し、通信することができる。

[0018] 従来の共有メモリを用いた仮想計算機間の通信として、仮想計算機を制御するハイパーバイザに共有メモリのキー管理情報を持たせ、仮想計算機間の通信を実現させる技術が知られている（特許文献１）。特許文献１は、従来、オペレーティングシステムによって行われていた共有メモリのキー管理を、ハイパーバイザに管理させることで、仮想計算機間の通信を実現している。

[0019] また、仮想計算機間の通信のセキュリティ面の問題を解決する方法として、ハイパーバイザ内に仮想計算機間の通信を許可するか否かを設定する通信許可テーブルを設け、受信側のアプリケーションがその通信許可テーブルに送信を許可する送信側のアプリケーションを設定し、送信側のアプリケーションがその通信許可テーブルを参照し、仮想計算機間の通信を制御する技術が知られている（特許文献２）。

[0020] しかしながら、特許文献１の技術では、仮想計算機間におけるプロセス間通信で使用される共有メモリと、仮想計算機内におけるプロセス間通信で使用される共有メモリとが区別されていない。そのため、キーさえ一致すれば、仮想計算機内のプロセス間通信用の共有メモリを、仮想計算機間のプロセス間通信の共有メモリとして他の仮想計算機がアクセスできる。従って、特許文献１の方法では、仮想計算機のフォークによって危険なアプリケーションを隔離したとしても、保護したい仮想計算機内のプロセス間通信に使用される共有メモリのキーさえ分かれば、隔離したアプリケーションは当該共有メモリにアクセスできるというセキュリティ面の課題がある。

[0021] また、特許文献２の方法では、通信許可テーブルを設定する受信側のアプ

リケーションがウイルスに感染している場合、送信を許可する送信側のアプリケーションをウイルスに感染させてしまうという課題がある。

[0022] 更に、従来の仮想計算機のフォークでは、仮想計算機内のプロセス同士で通信させることのみが想定され、仮想計算機間で通信を行うことは想定されていなかった。したがって、特許文献２の方法において仮想計算機のフォークを適用し、ダウンロードアプリケーションを別の仮想計算機から隔離した場合、ダウンロードアプリケーションは別の仮想計算機で実行されるアプリケーションと通信できないという課題がある。

[0023] 本実施の形態による仮想計算機システムの目的は、ある仮想計算機を複製して別の仮想計算機を生成する仮想計算機システムにおいて、仮想計算機同士の通信を安全に行わせることができる技術を提供することである。

[0024] 以下本発明の実施の形態について、図面を参照しながら説明する。

[0025] （実施の形態）

図１は、実施の形態による仮想計算機システム０の機能ブロック図である。仮想計算機システム０は、親仮想計算機１、子仮想計算機２、及びハイパーバイザ３を備える。子仮想計算機２は、親仮想計算機１を複製することで生成される。したがって、子仮想計算機２は、図１の各ブロックで示す親仮想計算機１の機能を全て備えている。以下の説明では、親仮想計算機１は保護プロセスを実行し、子仮想計算機２は非保護プロセスを実行するものとする。保護プロセスは、保護アプリケーションを実行することで発生するプロセスである。非保護プロセスは、非保護アプリケーションを実行することで発生するプロセスである。

[0026] 親仮想計算機１は、保護プロセス１０１、オペレーティングシステム１１、第２キー生成ファイル１０３、及び第１キー生成ファイル１０４を備える。なお、図１では保護プロセス１０１は１つのみ記載したが、処理に応じて複数のプロセスが動作することもある。

[0027] 保護プロセス１０１は、個人情報、金銭情報、著作物データ、著作権管理情報等を取り扱う保護すべきプロセスであり、親仮想計算機１内で実行され

る。

[0028] オペレーティングシステム１１は、保護メモリ領域１２１を共有メモリに生成して管理する。ここで、共有メモリは、プロセス同士が通信する際に使用するメモリである。そして、オペレーティングシステム１１は、キー生成部１０８、及びプロセス通信部２１を備えている。プロセス通信部２１は、プロセス判定部１０９、キー変換部１１０、キー判定部１１１、ＶＭ通信管理部１１２、ＶＭ内キー管理テーブル１１３、及び保護メモリ領域１２１を備える。

[0029] キー生成部１０８は、非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、第１種のキーを所定のキー変換ルールで変換した第２種のキーを生成し、他のプロセスから通信依頼が発行された場合、第１種のキーを生成する。ここで、キー生成部１０８は、各プロセスのキーが割り付けられたキー生成ファイルを参照してキーを生成する。

[0030] キー生成ファイルには、第１キー生成ファイル１０４（図３（Ａ）参照）及び第２キー生成ファイル１０３（図３（Ｂ）参照）が存在する。第１キー生成ファイル１０４は、通信相手のプロセスと値が同じになるように各プロセスに第１種のキーが割り付けられたファイルである。

[0031] 第２キー生成ファイル１０３は、第１キー生成ファイル１０４を複製し、非保護プロセスと通信する保護プロセスに割り付けられた第１種のキーをキー変換ルールで第２種のキーに変換することで生成されたファイルである。第１、第２キー生成ファイル１０４、１０３の詳細については後述する。

[0032] 親仮想計算機１のキー生成部１０８は、第２キー生成ファイル１０３を参照してキーを生成する。一方、子仮想計算機２のキー生成部１０８は、第１キー生成ファイル１０４を参照してキーを生成する。

[0033] プロセス判定部１０９は、通信依頼を発行したプロセスである対象プロセスが、保護プロセス１０１又は非保護プロセス１０２であるかを判定する。ここで、プロセス判定部１０９は、ＶＭ管理部１０７により管理されるＶＭ管理情報に基づき、対象プロセスを実行する仮想計算機が親仮想計算機１又

は子仮想計算機２であるかを判定し、対象プロセスが親仮想計算機１で実行される場合、対象プロセスを保護プロセス１０１と判定し、対象プロセスが子仮想計算機２で実行される場合、対象プロセスを非保護プロセス１０２と判定する。

[0034] キー変換部１１０は、プロセス判定部１０９により、対象プロセスが非保護プロセスであると判定された場合、キー変換ルールに基づき、対象キーを第１種のキーから第２種のキーに変換する。本実施の形態においては、親仮想計算機１でキー変換部１１０は呼ばれることはない。

[0035] キー判定部１１１は、プロセス判定部１０９により、対象プロセスが保護プロセス１０１であると判定された場合、キー生成部１０８により生成されたキーである対象キーが、第１又は第２種のキーであるかをキー変換ルールに基づいて判定する。ここで、キー変換ルールとしては、第１種のキーに規定値を加算して第２種のキーに変換するというルールが採用される。したがって、キー判定部１１１は、対象キーが規定値未満の場合、第１種のキーと判定し、対象キーが規定値以上の場合、第２種のキーと判定する。

[0036] なお、キー変換ルールとして、第１種のキーに規定値を加算して第２種のキーに変換するというルールを採用したが、これに限定されず、第１種のキーと第２種のキーとを明確に区別することができるようなルールであれば、どのようなルールを採用してもよい。例えば、第１種のキーに対して数値を付与し、第２種のキーに対して各数値に対応する符号（例えばアルファベットや文字列）を割り付けるというルールを採用してもよい。具体的には、第１種のキーとして１、２、３というような数値を採用し、各数値がａ、ｂ、ｃというようなアルファベットに変換されるルールを採用してもよい。

[0037] ＶＭ通信管理部１１２は、親仮想計算機１内のプロセス間通信に使用される保護メモリ領域１２１を共有メモリに生成して管理する。具体的には、ＶＭ通信管理部１１２は、各保護メモリ領域１２１のメモリＩＤとキーと共有メモリアドレスとが対応付けられたＶＭ内キー管理テーブル１１３（図５（Ａ）参照）を生成して、保護メモリ領域１２１を管理する。

[0038] また、ＶＭ通信管理部１１２は、キー判定部１１１により、対象キーが第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域１２１のメモリＩＤをＶＭ内キー管理テーブル１１３から特定し、特定したメモリＩＤを対象プロセスに通知し、対象プロセスに他の保護プロセス１０１と通信させる。

[0039] すなわち、ＶＭ通信管理部１１２は、対象プロセスが保護プロセス１０１であり、その保護プロセス１０１が他の保護プロセス１０１と通信するプロセスである場合、両保護プロセス１０１を親仮想計算機１内で通信させる。これにより、保護プロセス１０１は親仮想計算機１内で通信することができ、保護プロセス１０１の情報が子仮想計算機２やハイパーバイザ３に漏洩することが防止される。

[0040] ＶＭ内キー管理テーブル１１３は、ＶＭ通信管理部１１２により生成され、各保護メモリ領域１２１のキーと共有メモリアドレスとメモリＩＤとを対応付けたテーブルである。

[0041] ここで、ＶＭ通信管理部１１２は、対象キーがＶＭ内キー管理テーブル１１３に存在すれば、当該対象キーに対応するメモリＩＤを対象プロセスに通知する。一方、ＶＭ通信管理部１１２は、対象キーがＶＭ内キー管理テーブル１１３に存在しなければ、共有メモリに新しく保護メモリ領域１２１を生成し、生成した保護メモリ領域１２１にメモリＩＤを付与し、対象キーとメモリＩＤと共有メモリアドレスとをＶＭ内キー管理テーブル１１３に登録し、メモリＩＤを対象プロセスに通知する。

[0042] 保護メモリ領域１２１は、例えば親仮想計算機１内に生成され、親仮想計算機１のみがアクセスすることができる共有メモリである。そして、保護メモリ領域１２１は、保護プロセス１０１同士が通信する場合に使用される。なお、保護メモリ領域１２１は、親仮想計算機１のみがアクセスできるという制限を設ければ、親仮想計算機１の外部に設けてもよい。

[0043] 子仮想計算機２は、親仮想計算機１を複製することで生成される。このような子仮想計算機２の生成は、例えば、非保護プロセス１０２により非保護

アプリケーションの起動命令が発行されたことを契機に行われる。そのため、図１に示すように、子仮想計算機２は、非保護プロセス１０２を備えている以外は、親仮想計算機１と同じ構成を備えている。但し、キー判定部１１１、ＶＭ通信管理部１１２、及びＶＭ内キー管理テーブル１１３は子仮想計算機２において呼ばれることはない。

[0044] 非保護アプリケーションとしては、例えば、インターネット上からダウンロードされたダウンロードアプリケーションが挙げられる。ダウンロードアプリケーションにはコンピュータウィルスやマルウェアなどが含まれる可能性がある。そこで、ダウンロードアプリケーションを子仮想計算機２に実行させる。これにより、ダウンロードアプリケーションは保護プロセス１０１から隔離され、保護プロセス１０１を保護することができる。

[0045] 子仮想計算機２のオペレーティングシステム１２は親仮想計算機１のオペレーティングシステム１１を複製して生成される。

[0046] ハイパーバイザ３は、親仮想計算機１を複製して子仮想計算機２を生成し、親仮想計算機１と子仮想計算機２とを制御する。そして、ハイパーバイザ３は、ＨＶ通信管理部１０５、ＨＶ内キー管理テーブル１０６、ＶＭ管理部１０７、及び非保護メモリ領域１２２を備えている。

[0047] ＨＶ通信管理部１０５は、子仮想計算機２内のプロセス間通信に使用され、且つ親仮想計算機１及び子仮想計算機２間のプロセス間通信に使用される非保護メモリ領域１２２を共有メモリに生成して管理する。具体的には、ＨＶ通信管理部１０５は、各非保護メモリ領域１２２のメモリＩＤとキーと共有メモリアドレスとが対応付けられたＨＶ内キー管理テーブル１０６（図５（Ｂ）参照）を生成することで、非保護メモリ領域１２２を管理する。

[0048] ＨＶ通信管理部１０５は、第２種のキーに対応する非保護メモリ領域１２２のメモリＩＤを対象プロセスに通知し、対象プロセスに非保護プロセスと通信させる。

[0049] すなわち、ＨＶ通信管理部１０５は、対象プロセスが保護プロセス１０１であり、その保護プロセス１０１が非保護プロセス１０２と通信するプロセ

スである場合、両プロセスに非保護メモリ領域１２２を用いて通信させる。

[0050] これにより、保護プロセス１０１は、非保護メモリ領域１２２を用いて非保護プロセス１０２と通信することができ、仮想計算機間のプロセス通信を実現することができる。保護プロセス１０１及び非保護プロセス１０２間の通信では、非保護メモリ領域１２２が使用されているため、保護メモリ領域１２１は非保護プロセス１０２によってアクセスされず、他の保護プロセス１０１の情報が子仮想計算機２に漏洩することを防止することができる。

[0051] また、ＨＶ通信管理部１０５は、対象プロセスが非保護プロセス１０２であり、その非保護プロセス１０２が子仮想計算機２内の別の非保護プロセス１０２又は別の子仮想計算機２の非保護プロセス１０２と通信するプロセスである場合、非保護メモリ領域１２２を用いて両非保護プロセス１０２を通信させる。非保護プロセス１０２同士の通信では、非保護メモリ領域１２２が用いられているため、保護メモリ領域１２１は非保護プロセス１０２によってアクセスされず、保護プロセス１０１の情報が非保護プロセス１０２に漏洩することを防止することができる。

[0052] ＨＶ内キー管理テーブル１０６は、ＨＶ通信管理部１０５により生成され、キーと共有メモリアドレスとメモリＩＤとが対応付けられたテーブルである（図５（Ｂ）参照）。

[0053] ここで、ＨＶ通信管理部１０５は、対象キーがＨＶ内キー管理テーブル１０６に存在すれば、当該対象キーに対応するメモリＩＤを対象プロセスに通知する。一方、ＨＶ通信管理部１０５は、対象キーがＨＶ内キー管理テーブル１０６に存在しなければ、共有メモリに新しく非保護メモリ領域１２２を生成し、生成した非保護メモリ領域１２２にメモリＩＤを付与し、対象キーとメモリＩＤと共有メモリアドレスとをＨＶ内キー管理テーブル１０６に登録し、メモリＩＤを対象プロセスに通知する。

[0054] 非保護メモリ領域１２２は、例えばハイパーバイザ３内に生成され、親仮想計算機１と子仮想計算機２とが共にアクセスすることができる共有メモリである。そして、非保護メモリ領域１２２は、非保護プロセス１０２同士が

通信する場合と、保護プロセス１０１及び非保護プロセス１０２が通信する場合とにおいて使用される。なお、非保護メモリ領域１２２は、ハイパーバイザ３の外部に設けてもよい。

[0055] ＶＭ管理部１０７は、各仮想計算機が親仮想計算機１又は子仮想計算機２に該当するかを管理するためのＶＭ管理情報を生成して管理する。また、ＶＭ管理部１０７は、親仮想計算機１を複製して子仮想計算機２を生成する際に、親仮想計算機１と子仮想計算機２との状態をＶＭ管理情報に登録する。

[0056] 図７は、ＶＭ管理情報の一例を示した図である。ＶＭ管理情報は、１つの仮想計算機に対して１つのレコードが割り付けられ、各レコードはＶＭＩＤ及び状態のフィールドを備えている。ＶＭＩＤは、各仮想計算機に個別に付与された識別情報である。ＶＭＩＤは親仮想計算機１と子仮想計算機２とが区別できるような記号列が用いられる。図７の例では、親仮想計算機１に対してはＶＭ＿Ｐの記号列が割り付けられ、子仮想計算機２に対してはＶＭ＿Ｃ１、ＶＭ＿Ｃ２、・・・の記号列が割り付けられ、“Ｐ”と“Ｃ”とによって親仮想計算機１か子仮想計算機２かが区別できる。

[0057] 状態は各仮想計算機の状態を示している。状態としては、“発行”及び“待機”が存在する。“発行”は仮想計算機内のいずれかのプロセスが通信依頼を発行した状態を示す。待機は仮想計算機内のプロセスが他のプロセスからの通信を待機している状態を示す。

[0058] 図７の例では、ＶＭＩＤ＝ＶＭ＿Ｐの親仮想計算機１の保護プロセス１０１が通信依頼を発行したため、状態が“発行”となっている。それ以外の子仮想計算機２の非保護プロセス１０２は通信依頼を発行していないため状態が“待機”となっている。

[0059] ＶＭ管理情報は、通信依頼を発行した対象プロセスが保護プロセス１０１であるか非保護プロセス１０２であるかを判定するために、キー生成部１０８及びプロセス判定部１０９によって参照される。具体的には、キー生成部１０８及びプロセス判定部１０９は、対象プロセスから通信依頼が発行されると、ＶＭ管理情報を参照し、状態のフィールドが“発行”であるレコード

を特定し、特定したレコードのＶＭＩＤが親仮想計算機１を示す場合、その対象プロセスは保護プロセス１０１と判定し、特定したレコードのＶＭＩＤが子仮想計算機２を示す場合、その対象プロセスは非保護プロセス１０２と判定する。

[0060] 図２は、本発明の実施の形態による仮想計算機システム０の動作を示すフローチャートである。以下、図２を用いて保護プロセス１０１又は非保護プロセス１０２が共有メモリのメモリＩＤを取得する際の処理を説明する。

[0061] まず、キー生成部１０８は、対象プロセスから通信依頼が発行されて呼び出されると、ＶＭ管理部１０７により管理されているＶＭ管理情報を参照し、対象プロセスが保護プロセス１０１又は非保護プロセス１０２であるかを判定する（Ｓ２００１）。

[0062] この場合、キー生成部１０８は、例えば、図７に示すＶＭ管理情報の状態のフィールドが“発行”のレコードを特定し、特定したレコードのＶＭＩＤが親仮想計算機１を示すものであれば、対象プロセスは保護プロセス１０１であると判定し、特定したレコードのＶＭＩＤが子仮想計算機２を示すものであれば、対象プロセスは非保護プロセス１０２と判定する。

[0063] そして、キー生成部１０８は、対象プロセスが保護プロセス１０１であると判定した場合（Ｓ２００２でＹ）、第２キー生成ファイル１０３を参照して、キーを生成する（Ｓ２００３）。一方、キー生成部１０８は、対象プロセスが非保護プロセス１０２であると判定した場合（Ｓ２００２でＮ）、第１キー生成ファイル１０４を参照して、キーを生成する（Ｓ２００４）。

[0064] 次に、第１、第２キー生成ファイル１０４、１０３の詳細について説明する。本実施の形態では、子仮想計算機２は、親仮想計算機１を複製することで生成されている。したがって、各仮想計算機は、親仮想計算機１又は子仮想計算機２になる可能性がある。そこで、本実施の形態では各仮想計算機が親仮想計算機１又は子仮想計算機２になっても、キー生成部１０８が保護プロセス１０１又は非保護プロセス１０２のキーが生成できるように、第２キー生成ファイル１０３及び第１キー生成ファイル１０４を各仮想計算機に設

けている。図３（Ａ）は、本発明の実施の形態による第１キー生成ファイル１０４の一例を示した図である。図３（Ｂ）は本発明の実施の形態による第２キー生成ファイル１０３の一例を示した図である。

[0065] 図３（Ａ）に示すように、第１キー生成ファイル１０４は、１つのプロセスにつき１つのレコードが割り付けられ、プロセス名を格納するフィールド３００１と、キーを格納するフィールド３００２とを備えている。また、図３（Ｂ）に示すように、第２キー生成ファイル１０３も、第１キー生成ファイル１０４と同じデータ構造を持つ。

[0066] フィールド３００１は、各プロセスに付与されたプロセス名を格納する。フィールド３００２は、各プロセスがプロセス間通信を行う際に使用する共有メモリを特定するためのキーを格納する。

[0067] 第２キー生成ファイル１０３は、第１キー生成ファイル１０４を複製し、非保護プロセス１０２と通信する保護プロセス１０１については、キーをキー変換ルールにしたがって第１種のキーから第２種のキーに変換することで生成される。ここで、キー変換ルールとしては、第１種のキーに規定値を加算して第１種のキーを第２種のキーに変換するルールが採用され、規定値としては、例えば１０００が採用されている。

[0068] 図３（Ｂ）の例では、プロセスＣ以外の各プロセスには図３（Ａ）の各プロセスと同じキーが割り付けられており、第２キー生成ファイル１０３は第１キー生成ファイル１０４を複製することで生成されていることが分かる。一方、プロセスＣは非保護プロセス１０２と通信する保護プロセス１０１である。そのため、プロセスＣには、図３（Ａ）で示すキー“２１”に１０００を加えて第２種のキーに変換されたキー“１０２１”が割り付けられている。

[0069] なお、第１、第２キー生成ファイル１０４、１０３は、システム設計者によって予め作成されている。作成方法としては、例えば、システム設計者が、各プロセスに対して１０００未満の数値を取るように第１種のキーを割り付けて第１キー生成ファイル１０４を生成する。次に、システム設計者は、

第１キー生成ファイル１０４を複製し、非保護プロセス１０２と通信する保護プロセス１０１のキーには１０００を加算し、第２キー生成ファイル１０３を生成すればよい。

[0070] 図２に戻り、キー生成部１０８は、対象プロセスが保護プロセス１０１であれば（Ｓ２００２でＹ）、対象プロセスのプロセス名から当該プロセスに対応するレコードを第２キー生成ファイル１０３から特定し、特定したレコードのフィールド３００２に格納されたキーを、対象プロセスのキーとして生成する（Ｓ２００３）。そして、キー生成部１０８は、生成したキーを対象プロセスに返す。

[0071] 一方、キー生成部１０８は、対象プロセスが非保護プロセス１０２であれば（Ｓ２００２でＮ）、第１キー生成ファイル１０４を参照し、Ｓ２００３と同様にしてキーを生成し（Ｓ２００４）、対象プロセスに返す。

[0072] なお、Ｓ２００３、Ｓ２００４では、キー生成部１０８が第２キー生成ファイル１０３、第１キー生成ファイル１０４を読み込んだが、本実施の形態ではこれに限定されない。例えば、Ｓ２００３において、保護プロセス１０１が第２キー生成ファイル１０３を読み込んで、キー生成部１０８に渡すようにしてもよい。また、Ｓ２００４において、非保護プロセス１０２が第１キー生成ファイル１０４を読み込んでキー生成部１０８に渡すようにしてもよい。

[0073] 次に、対象プロセスは、取得したキーを対象キーとし、対象キーを指定してプロセス判定部１０９を呼び出す（Ｓ２００５）。そして、プロセス判定部１０９は、ＶＭ管理部１０７が管理するＶＭ管理情報を参照し、対象プロセスが保護プロセス１０１又は非保護プロセス１０２であるかを判定する（Ｓ２００５）。

[0074] この場合、プロセス判定部１０９は、ＶＭ情報を参照し、状態のフィールドが“発行”のレコードを特定し、特定したレコードのＶＭＩＤが親仮想計算機１を示せば、対象プロセスは保護プロセス１０１であると判定する。一方、プロセス判定部１０９は、特定したレコードのＶＭＩＤが子仮想計算機

２を示せば、対象プロセスは非保護プロセス１０２と判定する。

[0075] そして、プロセス判定部１０９は、対象プロセスが保護プロセス１０１であると判定した場合（Ｓ２００６でＹ）、キー判定部１１１は、対象キーが第１種のキー又は第２種のキーであるかを判定する（Ｓ２００７）。

[0076] ここで、キー判定部１１１は、上述したキー変換ルールにしたがって、対象キーの種別を判定する。例えば、図３の（Ｂ）の例では、第１種のキーに１０００を加算して第１種のキーが第２種のキーに変換されている。よって、キー判定部１１１は、対象キーが１０００以上である場合、第２種のキーと判定し、対象キーが１０００未満である場合、第１種のキーと判定する。

[0077] なお、キー判定部１１１は、システム設計者がキー判定部１１１に予め登録しておいたキー変換ルールを用いて対象キーの種別を判定してもよい。或いは、キー判定部１１１は、第２キー生成ファイル１０３を読み取り、キー変換ルールを解読し、解読したキー変換ルールを用いて対象キーの種別を判定してもよい。キー変換ルールの解読手法としては、例えば、図３（Ｂ）の例では、キー判定部１１１は、下２桁が共通するキーを特定し、特定したキーが異なる数値であれば、両数値の差分をキー変換ルールの規定値として特定する手法を採用すればよい。

[0078] 次に、キー判定部１１１は、対象キーが第１種のキーであると判定した場合（Ｓ２００８でＹ）、対象キーを指定してＶＭ通信管理部１１２に保護メモリ領域１２１の使用依頼を通知する（Ｓ２００９）。一方、キー判定部１１１は、対象キーが第２種のキーであると判定した場合（Ｓ２００８でＮ）、対象キーを指定してＨＶ通信管理部１０５に非保護メモリ領域１２２の使用依頼を通知する（Ｓ２０１０）。

[0079] Ｓ２００６において、対象プロセスが非保護プロセス１０２であると判定された場合（Ｓ２００６でＮ）、キー変換部１１０は、対象キーを上記のキー変換ルールにしたがって第１種のキーから第２種のキーに変換する（Ｓ２０１１）。つまり、キー変換部１１０は、対象キーに規定値（＝１０００）を加算して第２種のキーに変換する。

[0080] 次に、キー変換部１１０は、Ｓ２０１１で第２種のキーに変換した対象キーを指定して、ＨＶ通信管理部１０５に非保護メモリ領域１２２の使用依頼を通知する（Ｓ２０１０）。

[0081] 以下、共有メモリを生成または共有する処理の詳細について説明する。本実施の形態では、対象プロセスが別の保護プロセス１０１と通信する保護プロセスである場合、ＶＭ通信管理部１１２に保護メモリ領域１２１の使用依頼が通知され（Ｓ２００９）、対象プロセスが非保護プロセス１０２と通信する保護プロセス１０１又は非保護プロセス１０２である場合、ＨＶ通信管理部１０５に非保護メモリ領域１２２の使用依頼が通知される（Ｓ２０１０）。

[0082] そこで、まず、ＶＭ通信管理部１１２に使用依頼が通知される際の処理について説明する。図４は、本発明の実施の形態において、ＶＭ通信管理部１１２に保護メモリ領域１２１の使用依頼が通知された際の処理を示すフローチャートである。まず、ＶＭ通信管理部１１２は、ＶＭ内キー管理テーブル１１３を参照し（Ｓ４００１）、ＶＭ内キー管理テーブル１１３に対象キーが登録されているか否かを判定する（Ｓ４００２）。

[0083] 図５（Ａ）はＶＭ内キー管理テーブル１１３の一例を示した図である。図５（Ａ）に示すようにＶＭ内キー管理テーブル１１３は、１つの保護メモリ領域１２１に対して１つのレコードが割り付けられ、各レコードは、キーのフィールド５００１、共有メモリアドレスのフィールド５００２、及びメモリＩＤのフィールド５００３を備えている。

[0084] 共有メモリアドレスは各保護メモリ領域１２１の開始アドレスである。メモリＩＤは各保護メモリ領域１２１に一意に付与された識別情報である。このように、ＶＭ内キー管理テーブル１１３は、各保護メモリ領域１２１における、キー、共有メモリアドレス、及びメモリＩＤを対応付けて記憶している。

[0085] したがって、ＶＭ通信管理部１１２は、キー判定部１１１により指定された対象キーがＶＭ内キー管理テーブル１１３に存在すれば、対象キーはＶＭ

内キー管理テーブル１１３に登録されていると判定し（Ｓ４００２でＹ）、対象キーがＶＭ内キー管理テーブル１１３に存在しなければ、対象キーはＶＭ内キー管理テーブル１１３に登録されていないと判定する（Ｓ４００２でＮ）。

[0086] 次に、ＶＭ通信管理部１１２は、対象キーを使用してプロセス通信部２１内に保護メモリ領域１２１を生成する（Ｓ４００３）。次に、ＶＭ通信管理部１１２は、生成した保護メモリ領域１２１をＶＭ内キー管理テーブル１１３に登録する（Ｓ４００４）。この場合、ＶＭ通信管理部１１２は、保護メモリ領域１２１を生成する際に使用した対象キーと、生成した保護メモリ領域１２１の開始アドレス及びメモリＩＤとをＶＭ内キー管理テーブル１１３に登録する。次に、ＶＭ通信管理部１１２は、生成した保護メモリ領域１２１のメモリＩＤを保護プロセス１０１に通知する（Ｓ４００５）。一方、対象キーがＶＭ内キー管理テーブル１１３に登録されている場合（Ｓ４００２でＹ）、ＶＭ通信管理部１１２は、対象キーに対応するメモリＩＤを保護プロセス１０１に通知する（Ｓ４００６）。

[0087] 以上により、他の保護プロセス１０１と通信する保護プロセス１０１に保護メモリ領域１２１のメモリＩＤが通知される。

[0088] 次に、ＨＶ通信管理部１０５に非保護メモリ領域１２２の使用依頼が通知された際の処理について説明する。図９は、本発明の実施の形態による仮想計算機システムにおいて、、ＨＶ通信管理部１０５に非保護メモリ領域１２２の使用依頼が通知された際の処理を示すフローチャートである。まず、ＨＶ通信管理部１０５は、ＨＶ内キー管理テーブル１０６を参照し（Ｓ９００１）、ＨＶ内キー管理テーブル１０６に対象キーが登録されているか否かを判定する（Ｓ９００２）。

[0089] 図５（Ｂ）はＨＶ内キー管理テーブル１０６の一例を示した図である。図５（Ｂ）に示すようにＨＶ内キー管理テーブル１０６は、１つの非保護メモリ領域１２２に対して１つのレコードが割り付けられ、各レコードは、キーのフィールド５００１、共有メモリアドレスのフィールド５００２、及びメ

モリＩＤのフィールド５００３を備えている。

[0090] 共有メモリアドレスは各非保護メモリ領域１２２の開始アドレスである。メモリＩＤは各非保護メモリ領域１２２に一意に付与された識別情報である。このように、ＨＶ内キー管理テーブル１０６は、各非保護メモリ領域１２２における、キー、共有メモリアドレス、及びメモリＩＤを対応付けて記憶している。

[0091] そして、ＨＶ通信管理部１０５は、対象キーがＨＶ内キー管理テーブル１０６に登録されていない場合（Ｓ９００２でＮ）、対象キーを使用してハイパーバイザ３内に非保護メモリ領域１２２を生成する（Ｓ９００３）。

[0092] 次に、ＨＶ通信管理部１１２は、Ｓ４００４と同様にして、生成した非保護メモリ領域１２２をＨＶ内キー管理テーブル１０６に登録する（Ｓ９００４）。次に、ＨＶ通信管理部１１２は、Ｓ４００５と同様にして、生成した非保護メモリ領域１２２のメモリＩＤを通信依頼を発行した保護プロセス１０１又は非保護プロセス１０２に通知する（Ｓ９００５）。一方、対象キーがＨＶ内キー管理テーブル１０６に登録されていない場合（Ｓ９００２でＹ）、ＨＶ通信管理部１０５は、対象キーに対応するメモリＩＤを通信依頼を発行した保護プロセス１０１又は非保護プロセス１０２に通知する（Ｓ９００６）。

[0093] 以上により非保護プロセス１０２と通信する保護プロセス１０１及び非保護プロセス１０２にメモリＩＤが通知される。

[0094] 次に、本発明の実施の形態の仮想計算機システム０にけるプロセス間通信の一例について説明する。図６は、本発明の実施の形態による仮想計算機システム０において、キーが生成されてからメモリＩＤが通知されるまでの処理の流れを示した図である。図６において、プロセスＡ、プロセスＢ、及びプロセスＣは保護プロセス１０１であり、プロセスＤ、プロセスＥ、及びプロセスＦは非保護プロセス１０２である。

[0095] なお、図６において、第２キー生成ファイル１０３としては図３（Ｂ）が採用され、第１キー生成ファイル１０４としては図３（Ａ）が採用されてい

る。

[0096] また、キー変換ルールとしては、１０００を加算して第１種のキーを第２種のキーに変換するルールを採用する。よって、プロセスＣのキーは、図３（Ａ）のプロセスＣのキー“２１”に１０００を加算した１０２１となっている。

[0097] 始めに、親仮想計算機１内のプロセス間通信について説明する。ここでは、プロセスＡの通信依頼によって保護メモリ領域１２１が生成され、プロセスＢが生成された保護メモリ領域１２１を用いてプロセスＡと通信する場合について説明する。

[0098] まず、プロセスＡはキー生成部１０８を呼ぶ。次に、キー生成部１０８は第２キー生成ファイル１０３を参照して、プロセスＡのキー“３８”をプロセスＡに返す。ここで、プロセスＡは親仮想計算機１で実行されているため、キー生成部１０８は、プロセスＡを保護プロセス１０１と判定する。そのため、キー生成部１０８は第２キー生成ファイル１０３を参照している。

[0099] 次に、プロセスＡはキー“３８”を指定してプロセス判定部１０９を呼ぶ。次に、プロセス判定部１０９は、プロセスＡが親仮想計算機１で実行されているため、プロセスＡを保護プロセス１０１と判定する。

[0100] 次に、キー判定部１１１は、プロセスＡのキー“３８”が１０００未満であるため、第１種のキーと判定する。次に、キー判定部１１１は、キー“３８”が第１種のキーであるため、キー“３８”を指定して保護メモリ領域１２１の使用依頼をＶＭ通信管理部１１２に通知する。

[0101] 次に、ＶＭ通信管理部１１２は、ＶＭ内キー管理テーブル１１３にキー“３８”が登録されているか否かを判定する。ここでは、ＶＭ内キー管理テーブル１１３にはキー“３８”がまだ登録されていない。そのため、ＶＭ通信管理部１１２は、キー“３８”を使用して保護メモリ領域１２１を生成する。

[0102] 次に、ＶＭ通信管理部１１２は、生成した保護メモリ領域１２１をＶＭ内キー管理テーブル１１３に登録し、当該保護メモリ領域１２１のメモリＩＤ

をプロセスＡに通知する。

[0103] 次に、プロセスＢがキー生成部１０８を呼ぶ。次に、キー生成部１０８は、第２キー生成ファイル１０３を参照して、プロセスＢのキー“３８”をプロセスＢに返す。ここで、プロセスＢは親仮想計算機１で実行されているため、キー生成部１０８は、プロセスＡを保護プロセス１０１と判定する。そのため、キー生成部１０８は第２キー生成ファイル１０３を参照している。

[0104] 次に、プロセスＢはキー“３８”を指定してプロセス判定部１０９を呼ぶ。次に、プロセス判定部１０９は、プロセスＢが親仮想計算機１で実行されているため、プロセスＢを保護プロセス１０１と判定する。

[0105] 次に、キー判定部１１１は、プロセスＢのキー“３８”が１０００未満であるため、キー“３８”が第１種のキーであると判定する。次に、キー判定部１１１は、キー“３８”が第１種のキーであるため、保護メモリ領域１２１の使用依頼をＶＭ通信管理部１１２に通知する。

[0106] 次に、ＶＭ通信管理部１１２はＶＭ内キー管理テーブル１１３にキー“３８”が登録されているか否かを判定する。ここでは、ＶＭ内キー管理テーブル１１３にキー“３８”の保護メモリ領域１２１が登録されているため、当該保護メモリ領域１２１のメモリＩＤをプロセスＢに通知する。

[0107] 以上の処理により、プロセスＡ、Ｂはキー“３８”で特定される保護メモリ領域１２１を使用して通信することができる。

[0108] 以上の説明と逆に、プロセスＢの通信依頼によって、キー“３８”の保護メモリ領域１２１が生成された場合も、プロセスＡにはキー“３８”の保護メモリ領域１２１のメモリＩＤが通知され、プロセスＡ、Ｂは通信することができる。これは、第２キー生成ファイル１０３においてプロセスＡ、Ｂには同じキー“３８”が割り付けられ、且つ両プロセスは保護プロセス１０１であるため、キー変換が行われないからである。

[0109] 次に、子仮想計算機２内のプロセス間通信について説明する。ここでは、プロセスＥの通信依頼によって非保護メモリ領域１２２が生成され、プロセスＦが生成された非保護メモリ領域１２２を用いてプロセスＥと通信する場

合について説明する。

[0110] まず、プロセスＥはキー生成部１０８を呼ぶ。次に、キー生成部１０８は第１キー生成ファイル１０４を参照してプロセスＥのキー“５７”をプロセスＥに返す。ここで、プロセスＥは子仮想計算機２で実行されているため、キー生成部１０８は、プロセスＥを非保護プロセス１０２と判定する。そのため、キー生成部１０８は第１キー生成ファイル１０４を参照している。

[0111] 次に、プロセスＥはキー“５７”を指定してプロセス判定部１０９を呼ぶ。次に、プロセス判定部１０９は、プロセスＥが子仮想計算機２で実行されているため、プロセスＥを非保護プロセス１０２と判定する。

[0112] 次に、プロセス判定部１０９は、プロセスＥが非保護プロセス１０２であるため、キー“５７”を指定してキー変換部１１０を呼ぶ。

[0113] 次に、キー変換部１１０は、キー“５７”に１０００を加算して、第１種のキーから第２種のキーに変換し、変換後のキー“１０５７”を指定して非保護メモリ領域１２２の使用依頼をＨＶ通信管理部１０５に通知する。

[0114] 次に、ＨＶ通信管理部１０５は、ＨＶ内キー管理テーブル１０６にキー“１０５７”が登録されているか否かを判定する。ここでは、ＨＶ内キー管理テーブル１０６にはキー“１０５７”がまだ登録されていない。そのため、ＨＶ通信管理部１０５は、キー“１０５７”を使用して非保護メモリ領域Ｂを生成する。

[0115] 次に、ＨＶ通信管理部１０５は、生成した非保護メモリ領域ＢをＨＶ内キー管理テーブル１０６に登録し、当該非保護メモリ領域Ｂのメモリ ＩＤをプロセスＥに通知する。

[0116] 次に、プロセスＦがキー生成部１０８を呼ぶ。次に、キー生成部１０８は、第１キー生成ファイル１０４を参照して、プロセスＦのキー“５７”をプロセスＦに返す。ここで、プロセスＦは子仮想計算機２で実行されているため、キー生成部１０８は、プロセスＦを非保護プロセス１０２と判定する。そのため、キー生成部１０８は第１キー生成ファイル１０４を参照している。

[0117] 次に、プロセスＦはキー“５７”を指定してプロセス判定部１０９を呼ぶ、次に、プロセスＦはキー“５７”を指定してプロセス判定部１０９を呼ぶ。次に、プロセス判定部１０９は、プロセスＦが子仮想計算機２で実行されているため、プロセスＦを非保護プロセス１０２と判定する。

[0118] 次に、プロセス判定部１０９は、プロセスＦが非保護プロセス１０２であるため、キー“５７”を指定してキー変換部１１０を呼ぶ。

[0119] 次に、キー変換部１１０は、キー“５７”に１０００を加算して、第１種のキーから第２種のキーに変換し、変換後のキー“１０５７”を指定して非保護メモリ領域１２２の使用依頼をＨＶ通信管理部１０５に通知する。

[0120] 次に、ＨＶ通信管理部１０５は、ＨＶ内キー管理テーブル１０６にキー“１０５７”が登録されているか否かを判定する。ここでは、ＨＶ内キー管理テーブル１０６にキー“１０５７”の非保護メモリ領域Ｂが既に登録されているため、当該非保護メモリ領域Ｂのメモリ ＩＤをプロセスＦに通知する。

[0121] 以上の処理により、プロセスＥ、Ｆはキー“１０５７”で特定される非保護メモリ領域Ｂを使用して通信することができる。

[0122] 以上の説明とは逆に、プロセスＦの通信依頼によって、キー“１０５７”の非保護メモリ領域Ｂが生成された場合も、プロセスＥにはキー“１０５７”の非保護メモリ領域Ｂのメモリ ＩＤが通知され、プロセスＥ、Ｆは通信することができる。これは、第１キー生成ファイル１０４においてプロセスＥ、Ｆには同じキー“５７”が割り付けられ、且つ両プロセスは非保護プロセス１０２であるため、同じキー変換ルールでキー“１０５７”に変換されるからである。

[0123] このように、非保護プロセス１０２により通信依頼が発行された際、キー変換部１１０により必ずキーが第１種のキーから第２種のキーに変換される。そのため、保護メモリ領域１２１は非保護プロセス１０２によりアクセスされず、保護プロセス１０１が非保護プロセス１０２によって改変されたり参照されたりすることが防止される。

[0124] 最後に、仮想計算機間のプロセス間通信について説明する。ここでは、プ

ロセスＤの通信依頼によって非保護メモリ領域Ａが生成され、プロセスＣが生成された非保護メモリ領域Ａを用いてプロセスＤと通信する場合について説明する。

[0125] まず、プロセスＤはキー生成部１０８を呼ぶ。次に、キー生成部１０８は第１キー生成ファイル１０４を参照して、プロセスＤのキー“２１”をプロセスＤに返す。ここで、プロセスＤは子仮想計算機２で実行されているため、キー生成部１０８は、プロセスＤを非保護プロセス１０２と判定する。そのため、キー生成部１０８は第１キー生成ファイル１０４を参照している。

[0126] 次に、プロセスＤはキー“２１”を指定してプロセス判定部１０９を呼ぶ。次に、プロセス判定部１０９は、プロセスＤが子仮想計算機２で実行されているため、プロセスＤを非保護プロセス１０２と判定する。

[0127] 次に、プロセス判定部１０９は、プロセスＤが非保護プロセス１０２であるため、キー“２１”を指定してキー変換部１１０を呼ぶ。

[0128] 次に、キー変換部１１０は、キー“２１”に１０００を加算して、第１種のキーから第２種のキーに変換し、変換後のキー“１０２１”を指定して非保護メモリ領域１２２の使用依頼をＨＶ通信管理部１０５に通知する。

[0129] 次に、ＨＶ通信管理部１０５は、ＨＶ内キー管理テーブル１０６にキー“１０２１”が登録されているか否かを判定する。ここでは、ＨＶ内キー管理テーブル１０６にはキー“１０２１”はまだ登録されていない。そのため、ＨＶ通信管理部１０５は、キー“１０２１”を使用して非保護メモリ領域Ａを生成する。

[0130] 次に、ＨＶ通信管理部１０５は、生成した非保護メモリ領域ＡをＨＶ内キー管理テーブル１０６に登録し、非保護メモリ領域Ａのメモリ ＩＤをプロセスＤに通知する。

[0131] 次に、プロセスＣがキー生成部１０８を呼ぶ。次に、キー生成部１０８は第２キー生成ファイル１０３を参照して、プロセスＣのキー“１０２１”をプロセスＣに返す。このキー“１０２１”は、キー変換ルールに則って、予め第１種のキー“２１”に１０００が加算されて第２種のキーに変換された

キーである。プロセスＣは親仮想計算機１で実行されているため、キー生成部１０８は、プロセスＣを保護プロセス１０１と判定する。そのため、キー生成部１０８は第２キー生成ファイル１０３を参照している。

[0132] 次に、プロセスＣはキー“１０２１”を指定してプロセス判定部１０９を呼ぶ。次に、プロセス判定部１０９は、プロセスＣが親仮想計算機１で実行されているため、プロセスＣを保護プロセス１０１と判定する。

[0133] 次に、キー判定部１１１は、プロセスＣのキー“１０２１”が１０００未満であるため、第２種のキーと判定する。次に、キー判定部１１１は、キー“１０２１”が第２種のキーであるため、キー“１０２１”を指定して非保護メモリ領域１２２の使用依頼をＨＶ通信管理部１０５に通知する。

[0134] 次に、ＨＶ通信管理部１０５は、ＨＶ内キー管理テーブル１０６にキー“１０２１”が登録されているか否かを判定する。ここでは、ＨＶ内キー管理テーブル１０６にはキー“１０２１”が既に登録されている。そのため、ＨＶ通信管理部１０５は、キー“１０２１”に対する非保護メモリ領域Ａのメモリ ＩＤをプロセスＣに返す。

[0135] 以上の処理により、プロセスＣ、Ｄはキー“１０２１”で特定される非保護メモリ領域Ａを用いて通信することができる。

[0136] 以上の説明とは逆に、プロセスＣの通信依頼によって、キー“１０２１”の非保護メモリ領域Ａが生成された場合も、プロセスＤにはキー“１０２１”の非保護メモリ領域Ａのメモリ ＩＤが通知され、プロセスＣ、Ｄは通信することができる。

[0137] これは、第２キー生成ファイル１０３に登録されているプロセスＣのキーは“１０２１”であり、プロセスＤのキー“２１”をキー変換するルールで変換すると“１０２１”となり、両キーが一致するからである。

[0138] つまり、プロセスＣ、Ｄが通信を行う際には、両プロセスのキーは最終的に同じ値になり、両プロセスには同じメモリ ＩＤが通知され、両プロセスは同じ非保護メモリ領域Ａを共有して通信することができる。

[0139] また、プロセスＣ、Ｄは非保護メモリ領域Ａを用いて通信するため、プロ

セスＤが保護メモリ領域１２１にアクセスすることがなくなり、親仮想計算機１内の他のプロセス（プロセスＡ、Ｂ）の取り扱う情報が親仮想計算機１の外部に漏洩することを防止することができる。

[0140] また、プロセスＤは、非保護プロセス１０２であるため、必ず第２種のキーに変換される。したがって、第２キー生成ファイル１０３においてプロセスＣのキーが第２種のキーに予め変換されていなければ、プロセスＤはプロセスＣとは通信することができない。そして、第２キー生成ファイル１０３におけるプロセスＣのキーの変換はシステム設計者の管理下で予め行われている。

[0141] よって、システム設計者の許可がなければ、プロセスＤはプロセスＣと通信することができず、保護プロセスであるプロセスＣが非保護プロセスであるプロセスＤから許可なく通信されることが防止される。その結果、プロセスＣの取り扱う情報がシステム設計者の管理外のプロセスに漏洩することを防止することができる。

[0142] 更に、システム設計者は、第１キー生成ファイル１０４において、非保護プロセス１０２と通信する保護プロセス１０１のキーを第２種のキーに変換して第２キー生成ファイル１０３を生成しさえすれば、保護プロセス１０１を非保護プロセス１０２と通信させることができる。そのため、システム設計者は、保護アプリケーションや非保護アプリケーションを改変しなくても、仮想計算機間のプロセス通信を実現することができる。

[0143] また、ＨＶ通信管理部１０５は、第２種のキーとメモリＩＤとを対応付けて非保護メモリ領域１２２を管理している。そして、非保護プロセス１０２から通信依頼が発行されると、ＨＶ通信管理部１０５にはキー変換部１１０によって変換された第２種のキーが通知される。また、非保護プロセス１０２と通信する保護プロセス１０１から通信依頼が発行された場合も、ＨＶ通信管理部１０５には第２種のキーが通知される。

[0144] そのため、非保護プロセス１０２と通信する保護プロセス１０１及び非保護プロセス１０２には、必ず非保護メモリ領域１２２のメモリＩＤが通知さ

れる。よって、非保護プロセス１０２が保護メモリ領域１２１にアクセスすることがなくなり、保護プロセス１０１を保護することができる。

[0145] また、ＶＭ通信管理部１１２は、第１種のキーとメモリＩＤとを対応付けて保護メモリ領域１２１を管理している。そして、他の保護プロセス１０１と通信する保護プロセス１０１から通信依頼が発行されると、ＶＭ通信管理部１０５には第１種のキーが通知される。

[0146] そのため、他の保護プロセス１０１と通信する保護プロセス１０１には、必ず保護メモリ領域１２１のメモリＩＤが通知される。よって、保護プロセス同士で通信する保護プロセス１０１は保護メモリ領域１２１のみを使用することになり、非保護プロセス１０２に保護プロセス１０１の情報が漏洩することを防止することができる。

[0147] なお、本実施の形態においては、親仮想計算機１において保護プロセス１０１を実行させ、子仮想計算機２において非保護プロセス１０２を実行させたが、親仮想計算機１において非保護プロセス１０２を実行させ、子仮想計算機２において保護プロセス１０１を実行させてもよい。

[0148] この場合、図１に示す親仮想計算機１の機能を子仮想計算機２に実行させ、図１に示す子仮想計算機２の機能を親仮想計算機１を実行させればよい。

[0149] また、本実施の形態において、保護メモリ領域１２１を親仮想計算機１に生成し、非保護メモリ領域１２２をハイパーバイザ３に生成したが、ハイパーバイザ３に保護メモリ領域１２１及び非保護メモリ領域１２２を生成してもよい。この場合、保護メモリ領域１２１は親仮想計算機１のみアクセス可能とすれば、保護プロセス１０１を非保護プロセス１０２から保護することができる。

[0150] 最後に本実施の形態における仮想計算機システム０のハードウェア構成について説明する図８は、本発明の実施の形態による仮想計算機システム０のハードウェア構成を示すブロック図である。

[0151] 仮想計算機システム０は、例えばコンピュータにより構成され、入力装置８０１、ＲＯＭ（リードオンリメモリ）８０２、ＣＰＵ（中央演算処理装置

）８０３、ＲＡＭ（ランダムアクセスメモリ）８０４、外部記憶装置８０５、表示装置８０６、記録媒体駆動装置８０７、及び通信装置８０８を備える。各ブロックは内部のバスに接続され、このバスを介して種々のデータ等が入出され、ＣＰＵ８０３の制御の下、種々の処理が実行される。

[0152] 入力装置８０１は、キーボード、マウス等から構成され、ユーザが種々のデータを入力するために使用される。ＲＯＭ８０２には、ＢＩＯＳ（Basic Input/Output System）等のシステムプログラムが記憶される。外部記憶装置８０５は、ハードディスクドライブ等から構成され、オペレーティングシステムや仮想計算機プログラム等を記憶する。ＣＰＵ８０３は、外部記憶装置８０５からオペレーティングシステムや仮想計算機プログラム等を読み出し、各ブロックの動作を制御する。ＲＡＭ８０４は、ＣＰＵ８０３の作業領域等として用いられる。

[0153] 表示装置８０６は、例えば液晶ディスプレイや有機ＥＬディスプレイにより構成され、ＣＰＵ８０３の制御の下に種々の画像を表示する。記録媒体駆動装置８０７は、ＣＤ－ＲＯＭドライブ、フレキシブルディスクドライブ等から構成される。

[0154] なお、仮想計算機プログラムは、ＣＤ－ＲＯＭ等のコンピュータ読み取り可能な記録媒体８０９に格納されてユーザに提供される。ユーザはこの記録媒体８０９を記録媒体駆動装置８０７に読み込ませることで、仮想計算機プログラムをコンピュータにインストールする。また、仮想計算機プログラムをインターネット上のサーバに格納し、このサーバからダウンロードすることで、仮想計算機プログラムをコンピュータにインストールしてもよい。

[0155] 通信装置８０８は、例えば、コンピュータをインターネットに接続するための通信装置により構成され、ＣＰＵ８０３の制御の下、インターネットを介して他の機器との間でデータを送受する。

[0156] なお、図１に示す第１、第２キー生成ファイル１０４、１０３、ＶＭ内キー管理テーブル１１３、ＨＶ内キー管理テーブル１０６、ＶＭ管理部１０７、及び保護メモリ領域１２１、及び非保護メモリ領域１２２は、例えばＲＯ

Ｍ８０２、ＲＡＭ８０４、及び外部記憶装置８０５等の記憶装置と、記憶装置を制御する仮想計算機プログラムに含まれるプログラムモジュールとにより構成される。また、図１に示す保護プロセス１０１、キー生成部１０８、プロセス判定部１０９、キー変換部１１０、キー判定部１１１、ＶＭ通信管理部１１２、及びＨＶ通信管理部１０５は、仮想計算機プログラムに含まれるプログラムモジュールであり、ＣＰＵ８０３により実行される。

[0157] 図１に示す仮想計算機システム０の各機能ブロックは、典型的にはプロセッサと外部メモリとの協同で処理されるプログラムとして実現されるが、集積回路であるＬＳＩで実現してもよい。これらの各機能ブロックは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化されても良い。ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ又はウルトラＬＳＩと呼称されることもある。

[0158] 仮想計算機システム０を集積回路で構成する場合、例えば、キー生成部１０８、プロセス判定部１０９、キー変換部１１０、キー判定部１１１、ＶＭ通信管理部１１２、ＨＶ通信管理部１０５を集積化すればよい。

[0159] また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

[0160] さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。

[0161] また、仮想計算機システム０は、プロセッサとタイマとを備えた計算処理装置であれば、あらゆる計算機、電子機器、情報機器、ＡＶ機器、通信機器及び家電機器にも適用可能であり、例えばＰＣ（パーソナルコンピュータ）、携帯情報端末（携帯電話、スマートフォン及びＰＤＡなど）、テレビ、ハーディスクレコーダー、ＤＶＤ及びブルーレイディスクなどを用いた各種デ

ィスクレコーダー、ＤＶＤ及びブルーレイディスクなどを用いた各種ディスクプレイヤー、及びカーナビゲーションシステムなどにも応用できる。

[0162] また、前述の説明はあらゆる点において本発明の例示に過ぎず、その範囲を限定しようとするものではない。本発明の範囲を逸脱することなく種々の改良や変形を行うことができることは言うまでもない。

[0163] （本発明の実施の形態のまとめ）

本発明の実施の形態による仮想計算機システムの技術的特徴は下記のようにまとめることができる。

[0164] （１）本実施の形態による仮想計算機システムは、保護プロセスを実行する第１仮想計算機と、非保護プロセスを実行する第２仮想計算機と、前記第１、第２仮想計算機を制御するハイパーバイザとを備える仮想計算機システムであって、前記第１、第２仮想計算機は、非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、第１種のキーが所定のキー変換ルールで変換された第２種のキーを生成し、他のプロセスから通信依頼が発行された場合、前記第１種のキーを生成するキー生成部と、前記通信依頼を発行したプロセスである対象プロセスが、前記保護プロセス又は前記非保護プロセスであるかを判定するプロセス判定部と、前記プロセス判定部により、前記対象プロセスが前記保護プロセスであると判定された場合、前記キー生成部により生成されたキーである対象キーが、前記第１種のキー又は前記第２種のキーであるかを判定するキー判定部と、前記キー判定部により、前記対象キーが前記第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＶＭ通信管理部とを備え、前記ハイパーバイザは、前記キー判定部により、前記対象キーが前記第２種のキーと判定された場合、当該第２種のキーに対応する非保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＨＶ通信管理部を備え、前記第１、第２仮想計算機は、前記プロセス判定部により、前記対象プロセスが前記非保護プロセスであると判定された場合、前記キー変換ルールに基づき、前記対象キーを前記第１種のキーから前記第２種のキーに

変換するキー変換部を更に備え、前記ＨＶ通信管理部は、前記キー変換部により変換された第２種のキーに対応する前記非保護メモリ領域のメモリＩＤを前記対象プロセスに通知する。

[0165] この構成によれば、非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、キー生成部により第２種のキーが生成され、他のプロセス（保護プロセス同士で通信する保護プロセス及び非保護プロセス）から通信依頼が発行された場合、キー生成部により第１種のキーが生成される。ここで、第２種のキーは所定のキー変換ルールで第１種のキーを変換して得られるものである。

[0166] そして、通信依頼を発行したプロセスである対象プロセスが保護プロセスであるとプロセス判定部により判定されると、キー生成部により生成されたキーである対象キーが第１種のキー又は第２種のキーであるかキー判定部により判定される。

[0167] そして、キー判定部により対象キーが第１種のキーであると判定されると、対象プロセスが他の保護プロセスと通信する保護プロセス、つまり、第１仮想計算機内で通信する保護プロセスであると判定され、当該保護プロセスに第１種のキーに対応する保護メモリ領域のメモリＩＤが通知される。

[0168] これにより、第１仮想計算機内で通信する保護プロセスは保護メモリ領域にアクセスして他の保護プロセスと通信することができる。

[0169] 一方、対象キーが第２種のキーであるとキー判定部により判定されると、対象プロセスは非保護プロセスと通信する保護プロセス、つまり、仮想計算機間で通信する保護プロセスと判定され、当該保護プロセスに非保護メモリ領域に対応するメモリＩＤが通知される。

[0170] これにより、非保護プロセスと通信する保護プロセスは非保護メモリ領域にアクセスして非保護プロセスと通信することができる。

[0171] このように、本構成では、保護メモリ領域と非保護メモリ領域とに分け、非保護メモリ領域において保護プロセス及び非保護プロセスの通信を行わせ、保護メモリ領域において、保護プロセス同士の通信を行わせている。その

ため、保護プロセスを非保護プロセスから保護すると同時に、仮想計算機間の通信を実現することができる。

[0172] また、対象プロセスが非保護プロセスとプロセス判定部により判定された場合、対象キーがキー変換部によって第１種のキーから第２種のキーに変換される。そのため、非保護プロセスには、非保護メモリ領域のメモリＩＤが通知される。よって、非保護プロセスは、非保護メモリ領域のみ使用して通信することになり、保護プロセスを非保護プロセスから保護することができる。

[0173] （２）上記仮想計算機システムは、例えば、前記キー生成部は、各プロセスについて予めキーが割り付けられたキー生成ファイルを参照してキーを生成する。

[0174] この構成によれば、各プロセスについてキーが予め割り付けられたキー生成ファイルを参照してキーが生成されるため、キーを高速に生成することができる。また、システム設計者は、キー生成ファイルを設定することで、あるプロセスを目的のプロセスと通信させることができる。そのため、システム設計者は、アプリケーションを変更することなく、プロセスを管理することができる。

[0175] （３）上記仮想計算機システムは、例えば、前記キー生成ファイルは、通信相手のプロセスと値が同じになるように各プロセスに第１種のキーが割り付けられた第１キー生成ファイルと、前記第１キー生成ファイルを複製し、前記非保護プロセスと通信する保護プロセスに割り付けられた第１種のキーを前記キー変換ルールで第２種のキーに変換することで生成された第２キー生成ファイルとを備え、前記キー生成部は、前記保護プロセスから前記通信依頼が発行された場合、前記第２キー生成ファイルを参照してキーを生成し、前記非保護プロセスから前記通信依頼が発行された場合、前記第１キー生成ファイルを参照してキーを生成する。

[0176] この構成によれば、保護プロセスから通信依頼が発行された場合、キー生成部は第２キー生成ファイルを参照してキーを生成する。ここで、第２キー

生成ファイルにおいて、非保護プロセスと通信する保護プロセスには第２種のキーが割り付けられ、他のプロセス（保護プロセス同士で通信する保護プロセス及び非保護プロセス）には第１種のキーが割り付けられている。そのため、キー生成部は、非保護プロセスと通信する保護プロセスに対して第２種のキーを生成する。

[0177] 一方、この保護プロセスと通信する非保護プロセスには第１キー生成ファイルを参照して第１種のキーが生成される。ここで、生成される第１種のキーは、通信相手の保護プロセスに対して生成された第２種のキーの変換前の第１種のキーと同じである。

[0178] そして、当該非保護プロセスに対して生成された第１種のキーはキー変換部によりキー変換ルールに則って第２種のキーに変換されるため、変換後の第２種のキーは、通信相手の保護プロセスに対して生成された第２種のキーと同じになる。

[0179] よって、非保護プロセスとその通信相手となる保護プロセスとは最終的に同じ第２種のキーを持つことになり、両プロセスには非保護メモリ領域の同じメモリＩＤが通知される。これにより、両プロセスは非保護メモリ領域を用いて通信することができる。

[0180] 一方、キー生成部は、保護プロセスと通信する保護プロセスに対しては、第２キー生成ファイルを参照して第１種のキーを生成する。ここで、第２キー生成ファイルにおいて、通信対象となる保護プロセス同士には同じ第１種のキーが割り付けられている。よって、両保護プロセスには、保護メモリ領域の同じメモリＩＤが通知される。これにより、両保護プロセスは、保護メモリ領域を用いて通信することができる。

[0181] 更に、キー生成部は、非保護プロセス同士で通信する非保護プロセスから通信依頼が発行された場合、第１キー生成ファイルを参照して両非保護プロセスに対して同じ第１種のキーを生成する。そして、この第１種のキーはキー変換部によって第２種のキーに変換されるため、両非保護プロセスのキーは最終的に同じ第２種のキーとなる。よって、両非保護プロセスには非保護

メモリ領域の同じメモリＩＤが通知され、両非保護プロセスは非保護メモリ領域を用いて通信することができる。

[0182] （４）上記仮想計算機システムは、例えば、前記キー変換ルールは、前記第１種のキーに規定値を加算して前記第２種のキーに変換するというルールであり、前記キー判定部は、前記対象キーが前記規定値未満の場合、前記第１種のキーと判定し、前記対象キーが前記規定値以上の場合、前記第２種のキーと判定する。

[0183] この構成によれば、第１種のキーに規定値を加算すると第２種のキーになるという簡便なルールを用いて第１種、第２種のキーを区別することができる。

[0184] （５）上記仮想計算機システムは、例えば、前記キー判定部は、前記対象キーを前記第１種のキーと判定した場合、前記保護メモリ領域の使用依頼を前記ＶＭ通信管理部に通知し、前記対象キーを前記第２種のキーと判定した場合、前記非保護メモリ領域の使用依頼を前記ＨＶ通信管理部に通知する。

[0185] この構成によれば、キー判定部により対象キーが第１種のキーと判定された場合、他の保護プロセスと通信する保護プロセスから通信依頼が発行されたとして、保護メモリ領域の使用依頼がＶＭ通信管理部に通知される。よって、第１仮想計算機内で通信する保護プロセスには保護メモリ領域のメモリＩＤが通知されることになる。

[0186] 一方、キー判定部により対象キーが第２種のキーと判定された場合、非保護プロセスと通信するプロセスから通信依頼が発行されたとして、保護メモリ領域の使用依頼がＨＶ通信管理部に通知される。よって、非保護プロセスと通信する保護プロセスには非保護メモリ領域のメモリＩＤが通知されることになる。

[0187] （６）上記仮想計算機システムは、例えば、前記ハイパーバイザは、各仮想計算機が前記第１仮想計算機又は前記第２仮想計算機であるかを示すＶＭ管理情報を管理するＶＭ管理部を更に備え、前記プロセス判定部は、前記ＶＭ管理情報に基づき、前記対象プロセスを実行する仮想計算機が前記第１仮

想計算機又は前記第２仮想計算機に該当するかを判定し、前記第１仮想計算機に該当すると判定した場合、前記対象プロセスを前記保護プロセスと判定し、前記第２仮想計算機に該当すると判定した場合、前記対象プロセスを前記非保護プロセスと判定する。

[0188] ＶＭ管理情報は各仮想計算機が第１仮想計算機又は第２仮想計算機であるかを示す。一方、第１仮想計算機は保護プロセスを実行し、第２仮想計算機は非保護プロセスを実行する。よって、ＶＭ管理情報を用いることで対象プロセスが保護プロセス又は非保護プロセスであるかを正確に判定することができる。

[0189] （７）上記仮想計算機システムは、例えば、前記第１仮想計算機は、親仮想計算機であり、前記第２仮想計算機は、前記親仮想計算機を複製して生成された子仮想計算機である。

[0190] この構成によれば、第１仮想計算機を親仮想計算機、第２仮想計算機を子計算機とした場合において、保護プロセスを非保護プロセスから保護すると同時に、保護プロセス及び非保護プロセス間の通信を実現することができる。

[0191] （８）上記仮想計算機システムは、例えば、前記第２仮想計算機は、親仮想計算機であり、前記第１仮想計算機は、前記親仮想計算機を複製して生成された子仮想計算機である。

[0192] この構成によれば、第２仮想計算機を親仮想計算機、第１仮想計算機を子計算機とした場合において、保護プロセスを非保護プロセスから保護すると同時に、保護プロセス及び非保護プロセス間の通信を実現することができる。

[0193] （９）上記仮想計算機システムは、例えば、前記保護メモリ領域は、前記第１仮想計算機のみがアクセス可能な共有メモリに生成され、前記非保護メモリ領域は、前記第１及び第２仮想計算機がアクセス可能な共有メモリに生成されている。

[0194] この構成によれば、保護メモリ領域は第１仮想計算機のみアクセス可能で

あるため、保護メモリ領域の情報が第２仮想計算機に漏洩することが防止され、保護プロセスを保護することができる。

産業上の利用可能性

[0195] 本発明にかかる仮想計算機システムは、情報処理装置を用いるものであれば幅広い分野において有効である。例えば、大型コンピュータやパーソナルコンピュータのようなコンピュータのみならず、デジタルテレビや蓄積再生装置などの各種の家電機器、携帯電話などの通信機器、産業機器、制御機器、及び車載機器等でも利用可能である。

請求の範囲

［請求項1］ 保護プロセスを実行する第１仮想計算機と、非保護プロセスを実行する第２仮想計算機と、前記第１、第２仮想計算機を制御するハイパーバイザとを備える仮想計算機システムであって、

前記第１、第２仮想計算機は、

前記非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、第１種のキーが所定のキー変換ルールで変換された第２種のキーを生成し、他のプロセスから通信依頼が発行された場合、前記第１種のキーを生成するキー生成部と、

前記通信依頼を発行したプロセスである対象プロセスが、前記保護プロセス又は前記非保護プロセスであるかを判定するプロセス判定部と、

前記プロセス判定部により、前記対象プロセスが前記保護プロセスであると判定された場合、前記キー生成部により生成されたキーである対象キーが、前記第１種のキー又は前記第２種のキーであるかを判定するキー判定部と、

前記キー判定部により、前記対象キーが前記第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＶＭ通信管理部とを備え、

前記ハイパーバイザは、

前記キー判定部により、前記対象キーが前記第２種のキーと判定された場合、当該第２種のキーに対応する非保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＨＶ通信管理部を備え、

前記第１、第２仮想計算機は、

前記プロセス判定部により、前記対象プロセスが前記非保護プロセスであると判定された場合、前記キー変換ルールに基づき、前記対象キーを前記第１種のキーから前記第２種のキーに変換するキー変換部を更に備え、

前記ＨＶ通信管理部は、前記キー変換部により変換された第２種のキーに対応する前記非保護メモリ領域のメモリＩＤを前記対象プロセスに通知する仮想計算機システム。

［請求項2］ 前記キー生成部は、各プロセスについて予めキーが割り付けられたキー生成ファイルを参照してキーを生成する請求項１記載の仮想計算機システム。

［請求項3］ 前記キー生成ファイルは、

通信相手のプロセスと値が同じになるように各プロセスに第１種のキーが割り付けられた第１キー生成ファイルと、

前記第１キー生成ファイルを複製し、前記非保護プロセスと通信する保護プロセスに割り付けられた第１種のキーを前記キー変換ルールで第２種のキーに変換することで生成された第２キー生成ファイルとを備え、

前記キー生成部は、前記保護プロセスから前記通信依頼が発行された場合、前記第２キー生成ファイルを参照してキーを生成し、前記非保護プロセスから前記通信依頼が発行された場合、前記第１キー生成ファイルを参照してキーを生成する請求項２記載の仮想計算機システム。

［請求項4］ 前記キー変換ルールは、前記第１種のキーに規定値を加算して前記第２種のキーに変換するというルールであり、

前記キー判定部は、前記対象キーが前記規定値未満の場合、前記第１種のキーと判定し、前記対象キーが前記規定値以上の場合、前記第２種のキーと判定する請求項１～３のいずれかに記載の仮想計算機システム。

［請求項5］ 前記キー判定部は、前記対象キーを前記第１種のキーと判定した場合、前記保護メモリ領域の使用依頼を前記ＶＭ通信管理部に通知し、前記対象キーを前記第２種のキーと判定した場合、前記非保護メモリ領域の使用依頼を前記ＨＶ通信管理部に通知する請求項１～４のいず

れかに記載の仮想計算機システム。

[請求項6] 前記ハイパーバイザは、各仮想計算機が前記第１仮想計算機又は前記第２仮想計算機であるかを示すＶＭ管理情報を管理するＶＭ管理部を更に備え、

前記プロセス判定部は、前記ＶＭ管理情報に基づき、前記対象プロセスを実行する仮想計算機が前記第１仮想計算機又は前記第２仮想計算機に該当するかを判定し、前記第１仮想計算機に該当すると判定した場合、前記対象プロセスを前記保護プロセスと判定し、前記第２仮想計算機に該当すると判定した場合、前記対象プロセスを前記非保護プロセスと判定する請求項１～５のいずれかに記載の仮想計算機システム。

[請求項7] 前記第１仮想計算機は、親仮想計算機であり、

前記第２仮想計算機は、前記親仮想計算機を複製して生成された子仮想計算機である請求項１～６のいずれかに記載の仮想計算機システム。

[請求項8] 前記第２仮想計算機は、親仮想計算機であり、

前記第１仮想計算機は、前記親仮想計算機を複製して生成された子仮想計算機である請求項１～６のいずれかに記載の仮想計算機システム。

[請求項9] 前記保護メモリ領域は、前記第１仮想計算機のみがアクセス可能な共有メモリに生成され、

前記非保護メモリ領域は、前記第１及び第２仮想計算機がアクセス可能な共有メモリに生成されている請求項１～８のいずれかに記載の仮想計算機システム。

[請求項10] 保護プロセスを実行する第１仮想計算機と、非保護プロセスを実行する第２仮想計算機と、前記第１、第２仮想計算機を制御するハイパーバイザとを備える仮想計算機システムの制御方法であって、

前記非保護プロセスと通信する保護プロセスから通信依頼が発行さ

れた場合、第１種のキーが所定のキー変換ルールで変換された第２種のキーを前記第１仮想計算機のキー生成部が生成し、他のプロセスから通信依頼が発行された場合、前記第１種のキーを前記第２仮想計算機のキー生成部が生成するステップと、

前記通信依頼を発行したプロセスである対象プロセスが、前記保護プロセス又は前記非保護プロセスであるかを前記第１又は第２仮想計算機のプロセス判定部が判定するステップと、

前記プロセス判定部により、前記対象プロセスが前記保護プロセスであると判定された場合、前記キー生成部により生成されたキーである対象キーが、前記第１種のキー又は前記第２種のキーであるかを前記第１仮想計算機のキー判定部が判定するステップと、

前記キー判定部により、前記対象キーが前記第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域の識別情報を前記第１仮想計算機のＶＭ通信管理部が前記対象プロセスに通知するステップと、

前記キー判定部により、前記対象キーが前記第２種のキーと判定された場合、前記ハイパーバイザのＨＶ通信管理部が当該第２種のキーに対応する非保護メモリ領域のメモリＩＤを前記対象プロセスに通知するステップと、

前記第２仮想計算機の前記プロセス判定部により、前記対象プロセスが前記非保護プロセスであると判定された場合、前記キー変換ルールに基づき、前記対象キーを前記第１種のキーから前記第２種のキーに前記第２仮想計算機のキー変換部が変換するステップと、

前記キー変換部により変換された第２種のキーに対応する前記非保護メモリ領域のメモリＩＤを前記ＨＶ通信管理部が前記対象プロセスに通知するステップとを備える仮想計算機システムの制御方法。

［請求項11］ 保護プロセスを実行する第１仮想計算機と、非保護プロセスを実行する第２仮想計算機と、前記第１、第２仮想計算機を制御するハイパ

ーバイザとを備える仮想計算機システムの制御プログラムであって、

前記第１、第２仮想計算機を、

前記非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、第１種のキーが所定のキー変換ルールで変換された第２種のキーを生成し、他のプロセスから通信依頼が発行された場合、前記第１種のキーを生成するキー生成部と、

前記通信依頼を発行したプロセスである対象プロセスが、前記保護プロセス又は前記非保護プロセスであるかを判定するプロセス判定部と、

前記プロセス判定部により、前記対象プロセスが前記保護プロセスであると判定された場合、前記キー生成部により生成されたキーである対象キーが、前記第１種のキー又は前記第２種のキーであるかを判定するキー判定部と、

前記キー判定部により、前記対象キーが前記第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＶＭ通信管理部として機能させ、

前記ハイパーバイザを、

前記キー判定部により、前記対象キーが前記第２種のキーと判定された場合、当該第２種のキーに対応する非保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＨＶ通信管理部として機能させ、

前記第１、第２仮想計算機を、

前記プロセス判定部により、前記対象プロセスが前記非保護プロセスであると判定された場合、前記キー変換ルールに基づき、前記対象キーを前記第１種のキーから前記第２種のキーに変換するキー変換部として更に機能させ、

前記ＨＶ通信管理部は、前記キー変換部により変換された第２種のキーに対応する前記非保護メモリ領域のメモリＩＤを前記対象プロセ

スに通知する仮想計算機システムの制御プログラム。

［請求項12］ 保護プロセスを実行する第１仮想計算機と、非保護プロセスを実行する第２仮想計算機と、前記第１、第２仮想計算機を制御するハイパーバイザとを備える仮想計算機システムの集積回路であって、

前記第１、第２仮想計算機は、

前記非保護プロセスと通信する保護プロセスから通信依頼が発行された場合、第１種のキーが所定のキー変換ルールで変換された第２種のキーを生成し、他のプロセスから通信依頼が発行された場合、前記第１種のキーを生成するキー生成部と、

前記通信依頼を発行したプロセスである対象プロセスが、前記保護プロセス又は前記非保護プロセスであるかを判定するプロセス判定部と、

前記プロセス判定部により、前記対象プロセスが前記保護プロセスであると判定された場合、前記キー生成部により生成されたキーである対象キーが、前記第１種のキー又は前記第２種のキーであるかを判定するキー判定部と、

前記キー判定部により、前記対象キーが前記第１種のキーであると判定された場合、当該第１種のキーに対応する保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＶＭ通信管理部とを備え、

前記ハイパーバイザは、

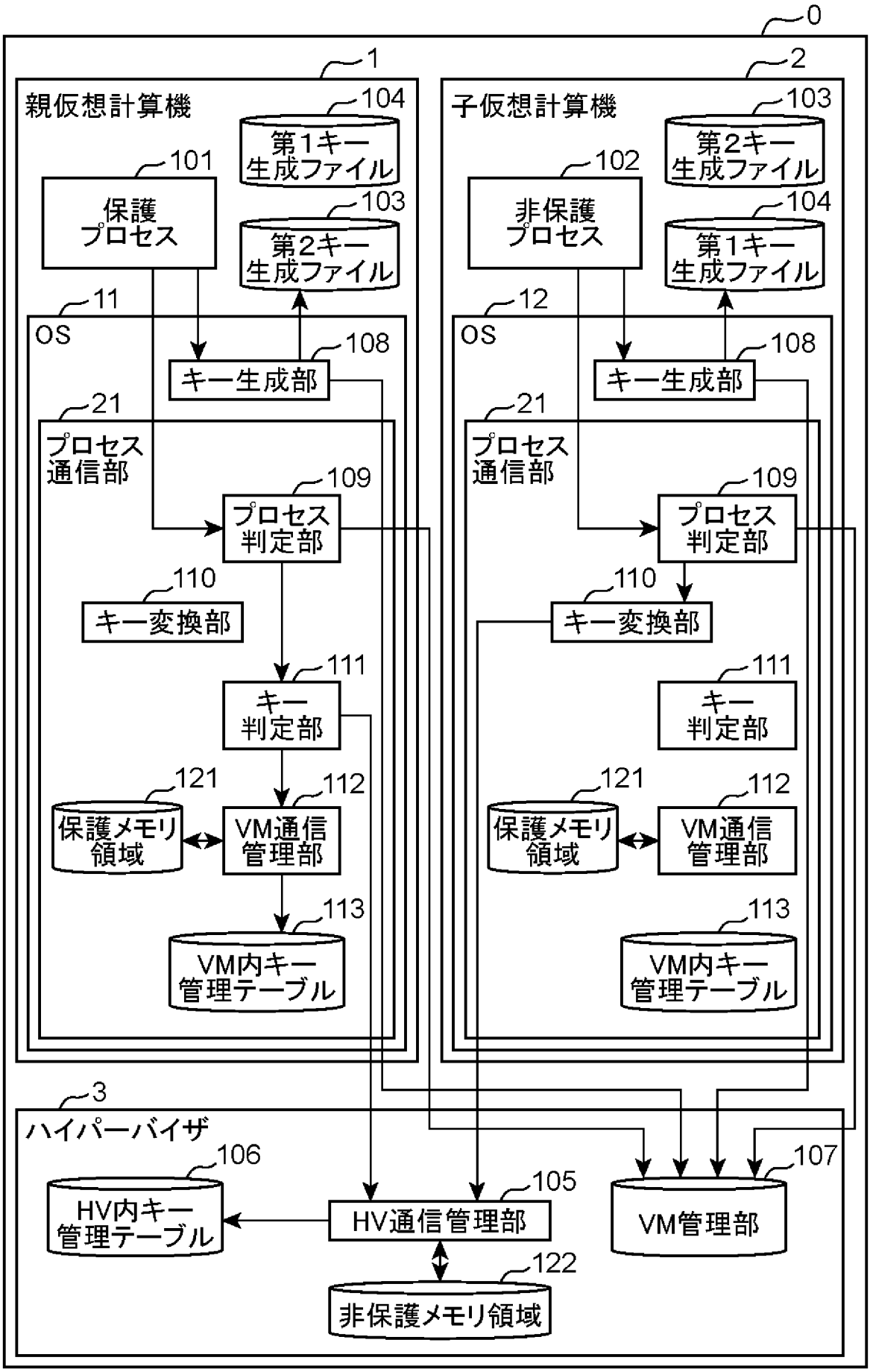
前記キー判定部により、前記対象キーが前記第２種のキーと判定された場合、当該第２種のキーに対応する非保護メモリ領域のメモリＩＤを前記対象プロセスに通知するＨＶ通信管理部を備え、

前記第１、第２仮想計算機は、

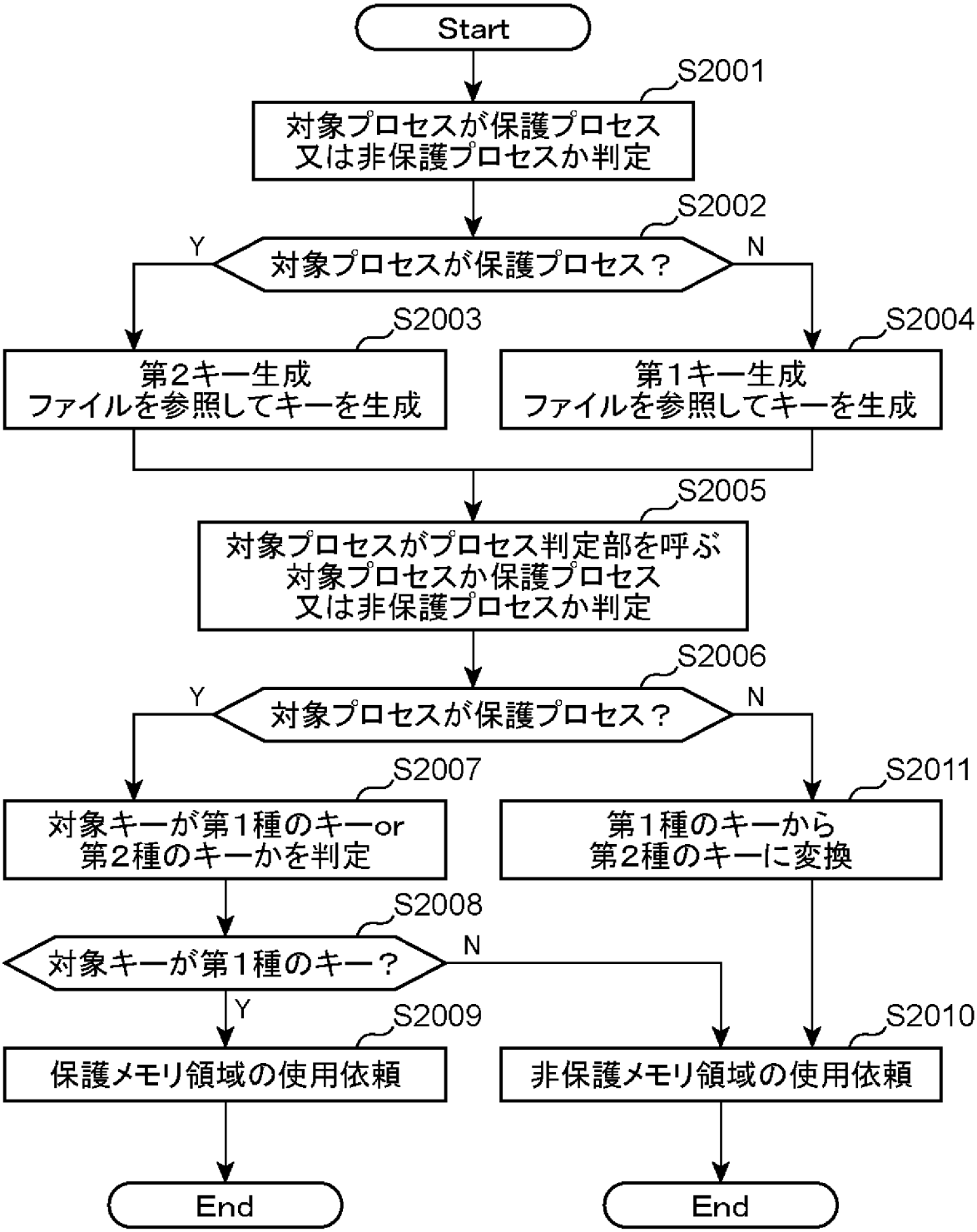
前記プロセス判定部により、前記対象プロセスが前記非保護プロセスであると判定された場合、前記キー変換ルールに基づき、前記対象キーを前記第１種のキーから前記第２種のキーに変換するキー変換部を更に備え、

前記ＨＶ通信管理部は、前記キー変換部により変換された第２種のキーに対応する前記非保護メモリ領域のメモリＩＤを前記対象プロセスに通知する集積回路。

[図1]


0
1
親仮想計算機
104
第1キー
生成ファイル
101
保護
プロセス
103
第2キー
生成ファイル
11
OS
108
キー生成部
21
プロセス
通信部
109
プロセス
判定部
110
キー変換部
111
キー
判定部
121
保護メモリ
領域
112
VM通信
管理部
113
VM内キー
管理テーブル
2
子仮想計算機
103
第2キー
生成ファイル
102
非保護
プロセス
104
第1キー
生成ファイル
12
OS
108
キー生成部
21
プロセス
通信部
109
プロセス
判定部
110
キー変換部
111
キー
判定部
121
保護メモリ
領域
112
VM通信
管理部
113
VM内キー
管理テーブル
3
ハイパーバイザ
106
HV内キー
管理テーブル
105
HV通信管理部
107
VM管理部
122
非保護メモリ領域

[図2]


Start
S2001
対象プロセスが保護プロセス
又は非保護プロセスか判定
S2002
対象プロセスが保護プロセス？
Y
N
S2003
第2キー生成
ファイルを参照してキーを生成
S2004
第1キー生成
ファイルを参照してキーを生成
S2005
対象プロセスがプロセス判定部を呼ぶ
対象プロセスか保護プロセス
又は非保護プロセスか判定
S2006
対象プロセスが保護プロセス？
Y
N
S2007
対象キーが第1種のキーor
第2種のキーかを判定
S2011
第1種のキーから
第2種のキーに変換
S2008
対象キーが第1種のキー？
N
Y
S2009
保護メモリ領域の使用依頼
S2010
非保護メモリ領域の使用依頼
End
End

[図3]

(A)

104

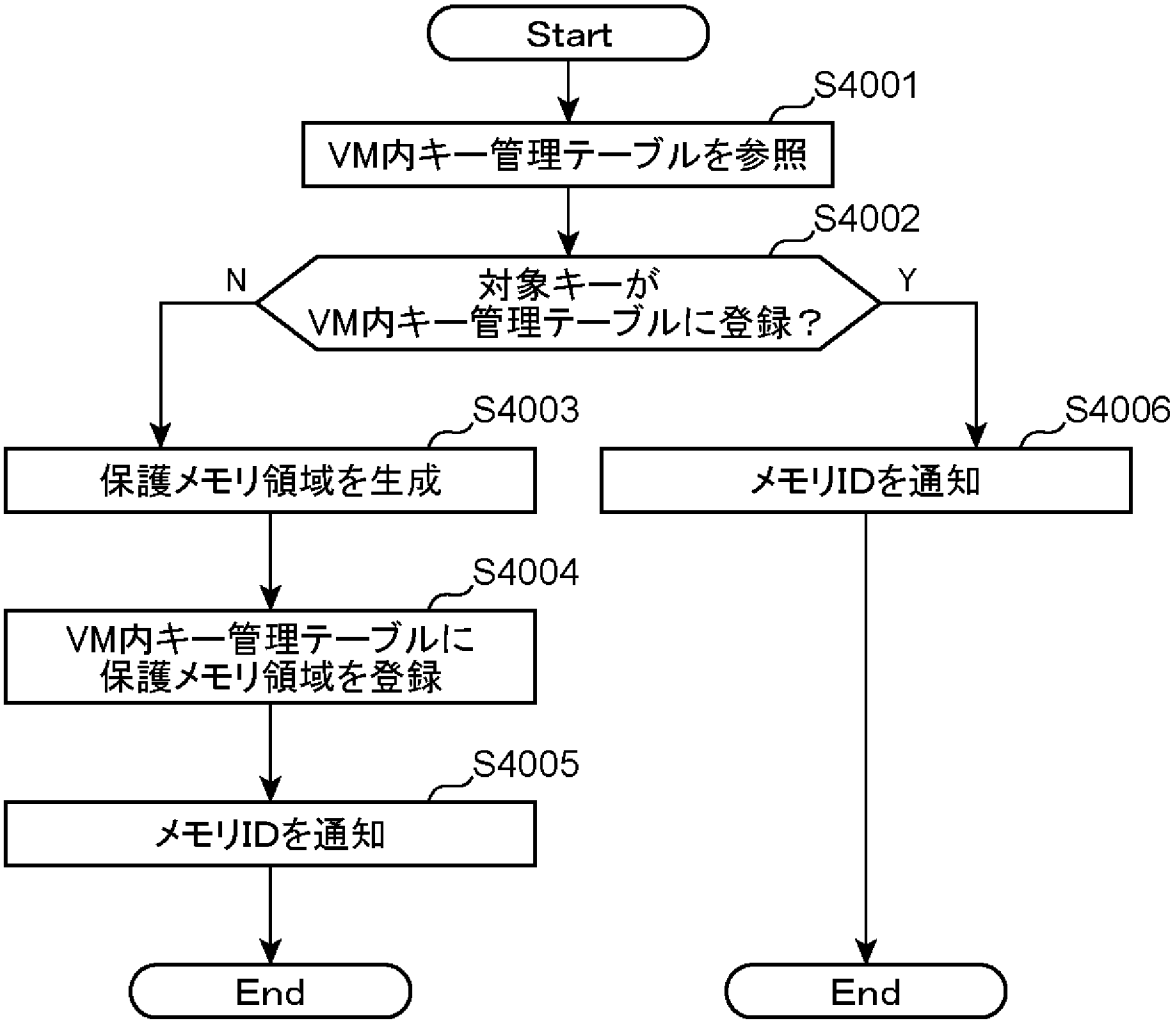
3001 プロセス名	3002 キー
プロセスA	38
プロセスB	38
プロセスC	21
プロセスD	21
プロセスE	57
プロセスF	57

(B)

103

3001 プロセス名	3002 キー
プロセスA	38
プロセスB	38
プロセスC	1021
プロセスD	21
プロセスE	57
プロセスF	57

[図4]


Start
S4001
VM内キー管理テーブルを参照
S4002
対象キーが
VM内キー管理テーブルに登録？
N
Y
S4003
保護メモリ領域を生成
S4004
VM内キー管理テーブルに
保護メモリ領域を登録
S4005
メモリIDを通知
End
S4006
メモリIDを通知
End

[図5]

(A)

113

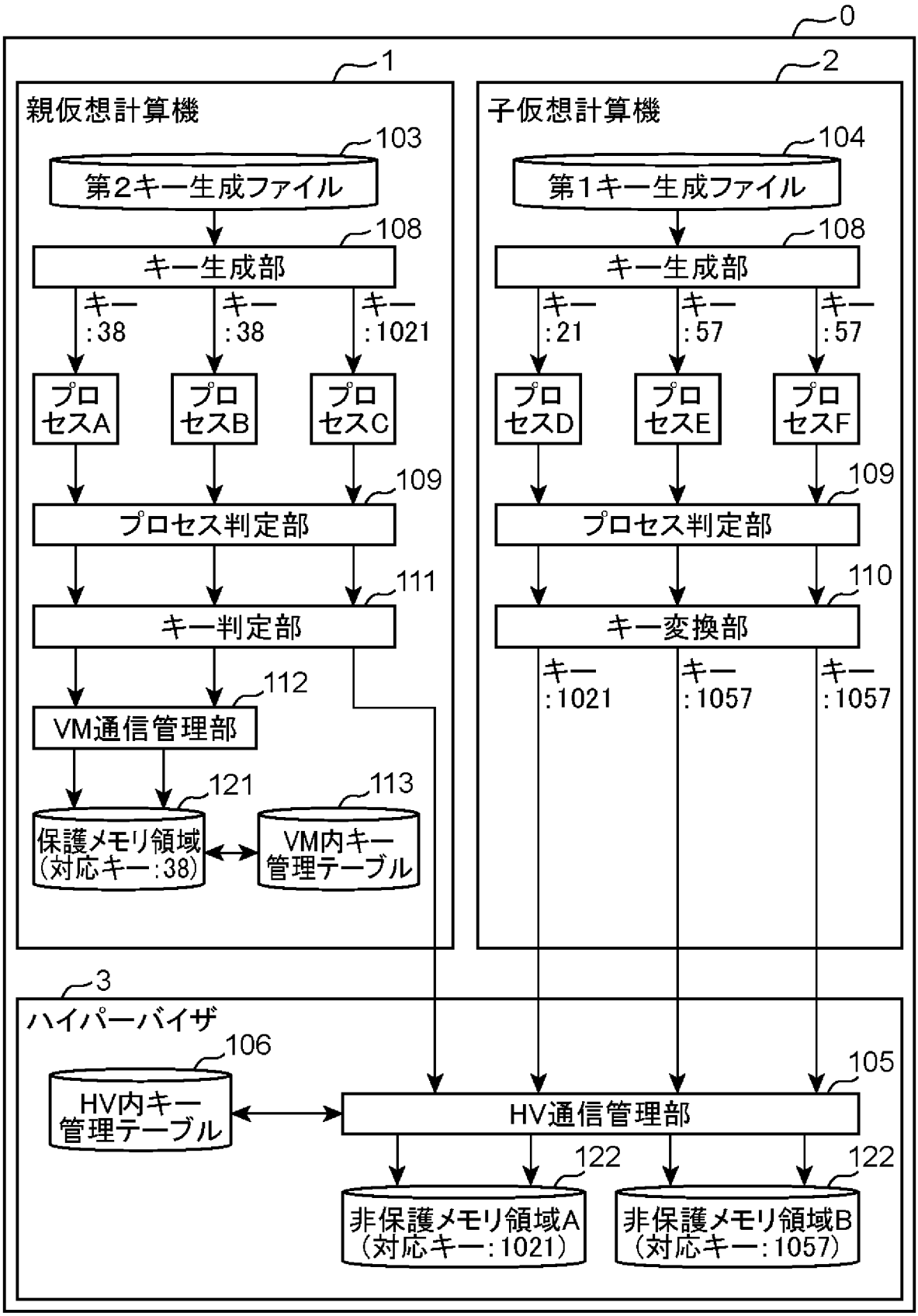
5001 キー	5002 共有メモリアドレス	5003 メモリID
38	0x20004000	3313
21	0x20008000	4243
57	0x20016000	7459

(B)

106

5001 キー	5002 共有メモリアドレス	5003 メモリID
1038	0x80004000	3891
1021	0x80008000	2998
1057	0x80012000	9701

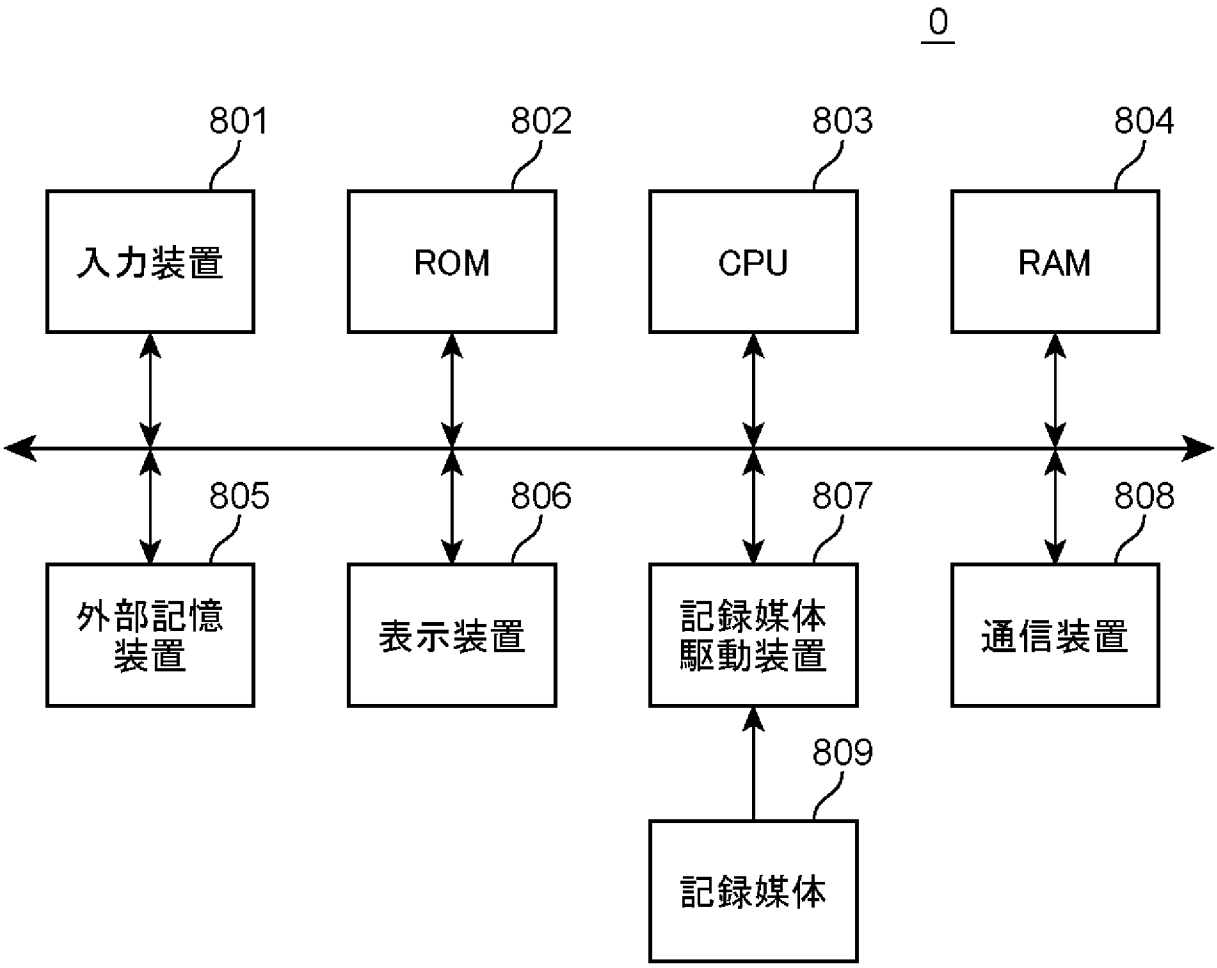
[図6]


0
1
親仮想計算機
103
第2キー生成ファイル
108
キー生成部
キー:38
キー:38
キー:1021
プロセスA
プロセスB
プロセスC
109
プロセス判定部
111
キー判定部
112
VM通信管理部
121
保護メモリ領域(対応キー:38)
113
VM内キー管理テーブル
2
子仮想計算機
104
第1キー生成ファイル
108
キー生成部
キー:21
キー:57
キー:57
プロセスD
プロセスE
プロセスF
109
プロセス判定部
110
キー変換部
キー:1021
キー:1057
キー:1057
3
ハイパーバイザ
106
HV内キー管理テーブル
105
HV通信管理部
122
非保護メモリ領域A(対応キー:1021)
122
非保護メモリ領域B(対応キー:1057)

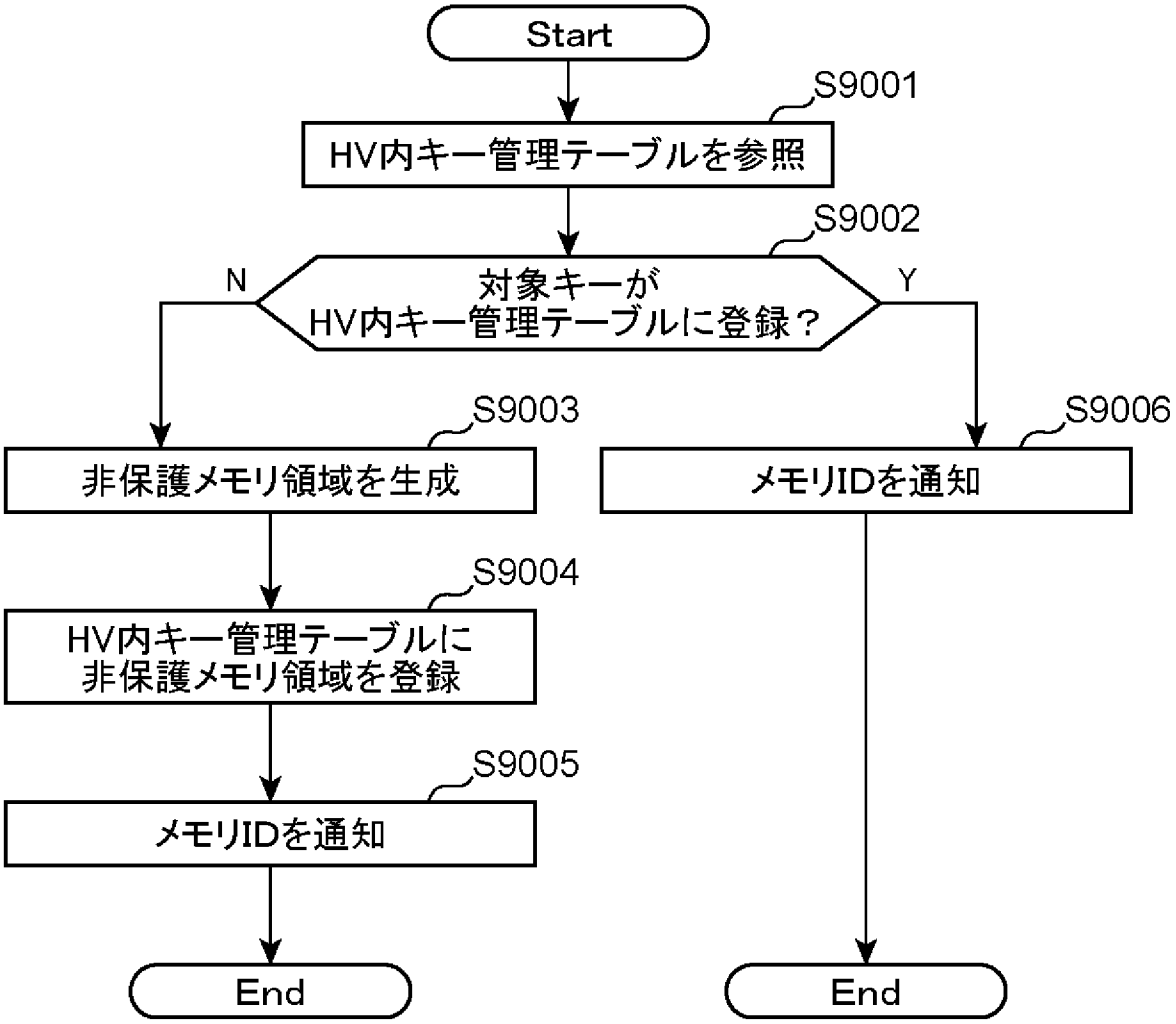
[図7]

VMID	状態
VM_P	発行
VM_C1	待機
VM_C2	待機
・・・	・・・

[図8]



[図9]


Start
S9001
HV内キー管理テーブルを参照
S9002
対象キーが
HV内キー管理テーブルに登録？
N
Y
S9003
非保護メモリ領域を生成
S9004
HV内キー管理テーブルに
非保護メモリ領域を登録
S9005
メモリIDを通知
End
S9006
メモリIDを通知
End

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/002229

A. CLASSIFICATION OF SUBJECT MATTER
G06F9/54(2006.01)i, *G06F9/46*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F9/54, G06F9/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2010-211339 A (Mitsubishi Electric Corp.), 24 September 2010 (24.09.2010), entire text; all drawings (Family: none)	1-12
A	WO 2006/101194 A1 (NEC Corp.), 28 September 2006 (28.09.2006), entire text; all drawings & US 2009/0055840 A1 & EP 1873678 A1	1-12
A	JP 2004-334893 A (Sun Microsystems, Inc.), 25 November 2004 (25.11.2004), entire text; all drawings & US 2004/0226023 A1 & EP 1475703 A2 & CN 1584843 A	1-12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 May, 2012 (22.05.12)	05 June, 2012 (05.06.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/002229

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-345654 A (Hitachi, Ltd.), 05 December 2003 (05.12.2003), entire text; all drawings & US 2003/0221115 A1 & EP 1365306 A2	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／００２２２９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F9/54(2006.01)i, G06F9/46(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F9/54, G06F9/46

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2010-211339 A (三菱電機株式会社) 2010.09.24, 全文, 全図 (ファミリーなし)	1-12
A	WO 2006/101194 A1 (日本電気株式会社) 2006.09.28, 全文, 全図 & US 2009/0055840 A1 & EP 1873678 A1	1-12
A	JP 2004-334893 A (サン・マイクロシステムズ・インコーポレイテッド) 2004.11.25, 全文, 全図 & US 2004/0226023 A1 & EP 1475703 A2 & CN 1584843 A	1-12
A	JP 2003-345654 A (株式会社日立製作所) 2003.12.05, 全文, 全図 & US 2003/0221115 A1 & EP 1365306 A2	1-12

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２２．０５．２０１２	０５．０６．２０１２

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｂ　３５６０
鈴木　修治
電話番号　０３－３５８１－１１０１　内線　３５４５