(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
2006 年3 月2 日 (02.03.2006)

PCT

(10) 国際公開番号
WO 2006/022161 A1

(51) 国際特許分類[7]: G06F 12/14, 9/50, 9/54

(21) 国際出願番号: PCT/JP2005/014903

(22) 国際出願日: 2005 年8 月15 日 (15.08.2005)

(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2004-245731 2004 年8 月25 日 (25.08.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 井上 浩明 (INOUE, Hiroaki) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 酒井 淳嗣 (SAKAI, Junji) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 阿部 剛 (ABE, Tsuyoshi) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 枝廣 正人 (EDAHIRO, Masato) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

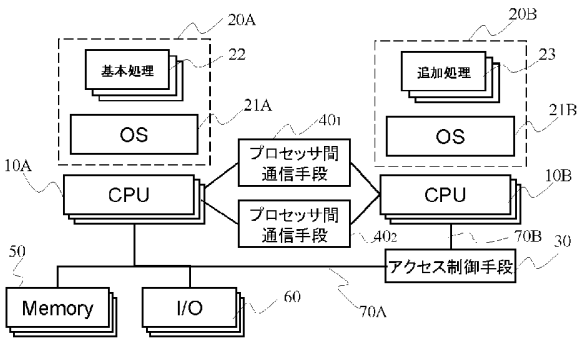
(74) 代理人: 加藤 朝道 (KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜３丁目２０番１２号 ダヴィンチ望星７階 加藤内外特許事務所 Kanagawa (JP).

(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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: INFORMATION COMMUNICATION DEVICE, AND PROGRAM EXECUTION ENVIRONMENT CONTROL METHOD

(54) 発明の名称: 情報通信装置及びプログラム実行環境制御方法



22... BASIC PROCESSING
40_1... INTER-PROCESSOR COMMUNICATION MEANS
40_2... INTER-PROCESSOR COMMUNICATION MEANS
23... ADDITIONAL PROCESSING
30... ACCESS CONTROL MEANS

(57) Abstract: An apparatus for and a method of making a high-speed processing possible and retaining the safety of a system at the time of adding an application or a driver. The apparatus comprises a first CPU group (10A) for executing a software (20A) composed of a basic processing (22) and an OS (21A), a second CPU group (10B) for executing a software (20B) composed of an additional processing (23) and an OS (21B) corresponding to an additional processing, inter-processor communication means (40_1 and 40_2) for communications between the first and second CPUs (10A and 10B), and access control means (30) for controlling the accesses to a memory (50) and/or an input/output device (60) by the second CPU (10B).

(57) 要約: 高速処理を可能とし、アプリケーション、ドライバ追加時に、システムの安全性を確保する装置及び方法の提供。 基本処理２２及びＯＳ２１Ａからなるソフトウエア２０Ａを実行する第１のＣＰＵ群１０Ａと、追加処理２３及び追加処理対応のＯＳ２１Ｂからなるソフトウエア２０Ｂを実行する第２のＣＰＵ群１０Ｂと、第１および第２のＣＰＵ１

[続葉有]

WO 2006/022161 A1

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, LS, MW, MZ, NA, 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 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

０Ａ、１０Ｂ間で通信を行うためのプロセッサ間通信手段４０$_1$、４０$_2$と、第２のＣＰＵ１０Ｂによるメモリ５０及び／又は入出力装置６０のアクセスを制御するアクセス制御手段３０を備えている。

明 細 書

情報通信装置及びプログラム実行環境制御方法

技術分野

[0001] 本発明は、情報処理装置に関し、特に、情報処理装置外部からダウンロードされた追加処理を実行する際のセキュリティ確保に好適とされる装置及び方法に関する。

背景技術

[0002] 携帯電話機(mobile phone)等の情報通信端末装置において、通常、該端末装置の基本機能を実現するための基本処理(例えば呼処理機能、インターネットアクセス用のブラウザ機能、電子メール機能、画面制御機能等)は、オペレーティングシステムとともに予めインストールされており、上記基本処理とは別の追加処理(プログラム)については、ユーザの操作等により、ネットワーク等外部から、該端末装置にダウンロードして実行、インストールが行われる。しかしながら、ダウンロードした追加処理を実行した場合、オペレーティングシステムや基本処理等は、該追加処理による攻撃に曝される可能性がある。

[0003] 図21は、ダウンロードされた追加処理を実行する情報通信端末装置の典型的な構成の一例を模式的に示す図である。図21には、よく知られた典型的な装置構成がブロック図にて模式的に例示されている。以下では、追加処理が、ネイティブコード(提供者側でコンパイル、またはアセンブル処理されたバイナリコード)で提供されるアプリケーションプログラムやデバイスドライバ(デバイスへのアクセス要求、デバイスからの割り込み処理を行うソフトウェアであり、「I/Oドライバ」ともいう)である場合について説明する。

[0004] 図21に示す構成において、追加処理23をダウンロードして実行したとき(追加処理23がデバイスドライバの場合には、オペレーティングシステムに組み込んで実行したとき)、基本処理22、オペレーティングシステム(「OS」という)21、CPU(Central Processing Unit)10、メモリ50、入出力デバイス(I/O)60に対して、追加処理23から、直接的に攻撃が行われる可能性がある。その理由は、基本処理22、CPU10、OS21、メモリ50、あるいは入出力デバイス(I/O)60に対する、追加処理23からの攻撃

を制限し、安全な実行環境を実現する手段が実装されていないためである。すなわち、図21に示す構成の場合、追加処理23は、基本処理22への処理要求、OS21への処理依頼、CPU10、メモリ50、及び入出力デバイス60への処理要求を任意に発行することができ、ハードウェア、ソフトウェアの各種資源へのアクセスも自在とされている。このため、悪意の追加処理23(あるいは、悪意はなくとも、ウイルス等に感染した追加処理)は、無防備なOS21、基本処理22等に対して攻撃自在とされる。

[0005] 追加デバイスドライバが、例えばレジデント(常駐型)ドライバとしてOS21のカーネル内に組み込まれる場合があり、該デバイスドライバの信頼性は、OS21の信頼性、及び性能にそのまま影響を及ぼすことになる。これは、デバイスドライバが、デバイスへの処理設定と、デバイスからの割り込み時にスケジューラから起動される割り込みサービスとを含み、割り込みサービスの実行時間(この間、再スケジュールは禁止される)は処理性能から特段に短い時間(例えばミリ秒以下)に制限されているという、デバイスドライバの特性からも、明らかである。つまり、追加デバイスドライバが仮に悪意のあるドライバである場合、情報処理装置の処理性能を容易に低下させることができる。これは、常駐型でなく、ローダブルドライバ(メモリに選択的にロード、アンロードされるドライバ)の場合も、同様である。このように、追加処理としてインストールされた悪意のドライバによって攻撃が行われた場合には、OS21のカーネルが直接攻撃されることになり、致命的ともなる(実質的に動作不能となる)。

[0006] そこで、ダウンロードされた追加処理の実行環境に制限を与え、基本処理等を保護する設計方式が、従来より、各種提案されている。以下、いくつかの典型例に即して概説しておく。

[0007] 図22は、ソフトウェアによる追加処理の実行保護環境を提供する構成の一典型例を示す図である。図22に示す例では、ネイティブコードの追加処理23は、仮想マシン24上で実行させる構成とされている。一例として、追加処理23が、JAVA(登録商標)バイトコードで記述されているものとすると、ダウンロードされたJAVA(登録商標)バイトコードは、仮想マシン24をなすJVM(JAVA(登録商標)仮想マシン)上で実行される。

[0008] かかる構成において、基本処理22やOS21等は、ソフト的に、追加処理23とは分

離され、その安全性が確保されることになる。すなわち、追加処理23は、仮想マシン24を介してのみ、OS21、CPU10、メモリ50、I／O60等へアクセスが行われる。仮想マシン24には、通常、OS21のカーネルモードでの実行（例えば特権的な命令の実行）等を行う権限が付与されていず、このため、追加処理23が、OS21を直接的に操作することはできない。また、仮想マシン24は、一般に、インタープリタ方式で追加処理23の命令コードを実行するため、追加処理23の命令・動作が適正であるか監視することが容易であり、例えば追加処理23からのハードウェア資源及びソフトウェア資源に対する不当なアクセス（例えば多量のデータをネットワーク上あるいは画面上に出力する等）を制限することで、仮想マシン24がソフト的な保護フィルタ、あるいは防護壁又は防護ゲートの役割を担うこともできる。このように、仮想マシン24を介して、基本処理22、OS21等は、追加処理23とは、ソフト的に分離されている。

[0009] しかしながら、図22に示した仮想マシン方式は、以下の問題点を有している。

[0010] ダウンロードされた追加処理23から、仮想マシン24の抜け（例えばセキュリティホール）への攻撃等がなされた場合、システムの安全性が損なわれることになる。

[0011] また、通常、JAVA（登録商標）仮想マシン等の仮想マシン24は、JAVA（登録商標）バイトコード等の命令コードを、一命令ずつ解釈実行するインタープリタ方式であるため、その実行速度が遅い。

[0012] さらに、仮想マシン24は、追加処理23を実行する時、システムコールを発行することで、OS21への処理依頼を行っているが、システムコールのオーバヘッドは大であることから、処理の実行は遅い。例えば仮想マシン24において、追加処理23の1つの命令に対応するシステムコールが1つ又は複数発行される。ユーザモードからのシステムコール発行によるシステムモードへのコンテクスト・スイッチング、OS21のシステムコールエントリ部におけるシステムコールのパケットデータのデコード、パラメータ等の正当性チェック（エラー検出処理）、処理の振分（ディスパッチ）、さらに、処理終了時の処理結果の引渡し及びコンテクスト・スイッチング、カーネル空間からユーザ空間への切り替え等、一連の制御が行われ、オーバヘッドが大きい。

[0013] そして、図22に示す構成の場合、追加処理23として、デバイスドライバをOS21に組み込むことはできない。図22からも明らかなように、仮想マシン24はOS21の上層

に位置している。仮想マシン24は、追加処理23のコードに基づき、OS21に対して処理依頼を行い、OS21から処理結果を受け取り、必要に応じて追加処理23に返す構成とされており、追加処理をデバイスドライバとしてOS21内に組み込もうとすると、追加処理の実行を制御する仮想マシンも、OS21内に組み込むことが必要となり、かかる構成は、図22に示す仮想マシン方式では、原理的に不可能であるためである。

[0014] ソフトウェアによる別のセキュリティ管理方式として、例えば図23に示すような構成も知られている。図23に示すように、追加処理23には、それが信頼できるものであることを証明するための証明書25が添付されて、端末(情報処理装置)にダウンロードされる。端末側では、添付された証明書25の内容をチェックし、添付された証明書25が正しい証明書であると認証された場合に、ダウンロードされた追加処理23のインストール、実行を許可する構成とされている。証明書25としては、ディジタル署名(ITU-T X509)を用いてもよい。例えば証明書25には、証明される機関とその公開鍵、CA(認証局)のデジタル署名(証明される機関や公開鍵などをCAの秘密鍵で暗号化したもの)が格納され、証明書の認証を行う場合には、CAのディジタル署名の部分を、CAの公開鍵で解読して証明書のデータの内容と一致するか否か確認し、一致する場合に、証明書のデータを信頼してもよいと判断される。あるいは、証明書25は、真正のベンダーを証明するものであれば、任意の証明書であってもよい。なお、デバイスドライバの署名機能(Driver Signing)は、例えばWindows(登録商標)2000等にも実装されている。

[0015] 図23に示した方式の場合、追加処理23はネイティブコードで提供することができ、図22に示した仮想マシン方式と比べて、高速実行が可能である。また、追加処理23として、アプリケーション、デバイスドライバの実行も可能である。しかしながら、システムの信頼性は、追加処理23の安全性に全面的に依拠している。つまり、追加処理23に事前に検知し得ない問題があると、システムに致命的損害をもたらす可能性もある。

[0016] 図24は、セキュリティ管理をハードウェアで行うプロセッサの構成を示す図である。図24を参照すると、CPU11は、安全(セキュア)モード12と、非安全(ノンセキュア)モード13を有し、ダウンロードされた追加処理23と該追加処理23に対応したOS21

Bは、もっぱらノンセキュアモード13で実行される。そして、メモリ管理ユニット14は、ノンセキュアモード13で実行されるメモリの領域(アドレス空間)を、セキュアモード12でアクセスされるメモリの領域と分離して管理し、ノンセキュアモード13からセキュアモード12のメモリ領域へのアクセスは禁止される。すなわち、メモリ管理ユニット14は、ノンセキュアモード13からのメモリのアクセス制御を行い、ノンセキュアモード13からセキュアモード12のメモリ領域へのアクセスを禁止する制御を行っている。

[0017] このように、図24に示す構成においては、基本処理22をセキュアモード12で実行し、仮想的に、追加処理23を実行するCPUと別CPUに分離することで、安全性の向上を図っている。

[0018] しかしながら、セキュアモードとノンセキュアモードは、CPU上で、時分割で実行されており、ノンセキュアモードから復帰しない場合には、セキュアモードでのシステムの動作は行われない。

[0019] また、ノンセキュアモードとセキュアモードを時分割処理しているため、その切替時、モード遷移等のオーバヘッドがかかる。

[0020] さらに、追加処理23をデバイスドライバとし、ノンセキュアモードのOS21B内に組み込む場合、ドライバに悪意があると、セキュアモードに復帰することができなくなる可能性があり、システムに致命的な損害をもたらす可能性がある。

[0021] なお、図24に示した構成と同様、システムメモリ中に分離域を設け、ノーマル実行モードと分離実行モードを備えたプロセッサとして、後記特許文献1の記載が参照される。特許文献1に記載の装置において、ノーマル実行モードは、プロセッサが非安全環境、すなわち分離実行モードによって提供されるセキュリティ機能がない通常の動作モードで動作するモードであり、ノーマル実行モードからは分離域へのアクセスが禁止され、分離実行モードでは、所定の分離命令の実行がサポートされる構成とされている。なお、かかる構成も、ノーマル実行モードと分離実行モードを時分割処理しているため、その切替時、モード遷移等のオーバヘッドがかかる。

[0022] また、2つのプロセッサユニットとスイッチユニットを備え、1つのプロセッサユニットが公共データ通信ネットワークと接続され、他方のプロセッサユニットは公共データ通信ネットワークと接続せず、データセキュリティ用ユニットとして機能する構成が開示され

ている(後記特許文献2参照)。特許文献2に記載されるシステムでは、公共データ通信ネットワークに接続されるプロセッサユニットと、データセキュリティ用ユニットをスイッチで分離しており、データセキュリティ用ユニットの安全性を確保している。しかしながら、公共データ通信ネットワークに接続されるプロセッサユニットが、前述した追加処理(ネットワーク等からダウンロードされた追加処理)の実行により、攻撃されることの対策に関しては、いささかも考慮されていない。データセキュリティ用ユニットは安全であっても、公共データ通信ネットワークに接続されるプロセッサユニットは追加処理による攻撃に対する有効なセキュリティ機構は具備していない。このため、公共データ通信ネットワークに接続されるプロセッサユニットにセキュリティ管理を実現する場合、前述したいずれかの方式を採用する必要がある。

[0023] さらに、プロセッサ上で分離された実行プログラムあるいはオペレーティングシステムを同時に実行するシステムにおいて、不正なプログラムの実行環境を保護するために、第1のプログラムが実行される間、第1のプログラムのみが利用するメモリ空間が設定され、第1のプログラムとコンピュータの実行環境との通信は、共有メモリ空間の利用、専用の割り込み、あるいは専用のI/Oポートを含む単一のリンクを介して行われ、第1のプログラムは、制限された実行環境において、設定されたメモリ空間と単一のリンクを除いてプロセッサ上のリソースのアクセスすることが制限されるようにした構成が特許文献3に記載されている。この特許文献3に記載された方法の場合、第1のプログラムは、設定されたメモリ空間と単一のリンク(共有メモリ空間の利用、専用の割り込み、あるいは専用のI/Oポート)を除いてプロセッサ上のリソースのアクセスすることが制限されるため、第1のプログラムを、デバイスドライバとして用いることはできず、デバイスドライバを含む追加処理に適用することはできない。

[0024] なお、後述される本発明で用いられるプロセッサ間通信手段に関連する技術を開示した刊行物として、後記特許文献4には、マルチプロセッサシステムにおけるCPU間通信方式が開示されている。この特許文献4には、マルチプロセッサが共通メモリを利用してCPU間通信を行うにあたり、CPU2がCPU1に割り込みを発生させる場合、CPU1に対する固定領域における自己用のCPU間通信情報書き込み領域に、通信情報を書き込んで割り込みを発生し、CPU1では、割り込みが発生すると、CP

U2に対応するCPU間通信情報書き込み領域をアクセスして割り込み処理を実行する構成がその従来技術として記載されており、さらに、共有メモリのアクセス回数を削減するようにした発明が記載されている。

[0025] 特許文献1:特表2004－500666号公報

特許文献2:特表2002－542537号公報

特許文献3:特表2002－533791号公報

特許文献4:特開平6－332864号公報

発明の開示

発明が解決しようとする課題

[0026] 上記したように、ダウンロードされた、悪意のある、もしくは過失の追加処理からの攻撃に対する安全性確保の対策を施した従来の装置は、処理性能の点、デバイスドライバの実行が不可である点、安全性確保に問題がある点等、実用上、各種課題が残されている。特に、図22、及び図24に示したように、情報処理装置に関して、装置外部から、追加デバイスドライバのダウンロードが不可である設計方式(アーキテクチャ)は、デバイスの追加、機能追加等が実質的に不可能であることを意味しており、この点で、可用性(availability)が制限される。一方、前述したように、追加デバイスドライバを例えばカーネルモードで動作させる場合には、OS、システムの信頼性に直接影響を及ぼすことから、特段の安全性確保、信頼性の向上が要請されている。

[0027] したがって、本発明の目的は、簡易な構成により高速処理を可能とし、アプリケーションプログラム及びデバイスドライバの追加時に安全性、信頼性を確保する装置及び方法を提供することにある。

課題を解決するための手段

[0028] 前記目的を達成する本発明は、その概略を述べれば以下の通りである。

[0029] 本発明の1つの側面(アスペクト)に係る装置は、複数のプロセッサを備え、実行する処理の信頼度に応じて、前記複数のプロセッサが、複数のドメインを構成し、異なるドメイン間のプロセッサ同士は、プロセッサ間通信手段を介して、相互に通信し、セキュリティの相対的に低い処理を実行するドメインに属するプロセッサによるセキュリティの相対的に高い処理を実行するドメインに属するメモリ及び／又は入出力装置への

アクセスを制御するアクセス制御手段を備えている。

[0030] 本発明の1つの側面に係るプログラム実行環境制御方法は、情報処理装置を構成する複数のプロセッサを、実行するプログラムの信頼度に応じて、複数のドメインに分け、異なるドメイン間のプロセッサ同士が、データ又はコマンドを、プロセッサ間通信手段を介して相互に送信する工程と、信頼度の相対的に低いプログラムを実行するドメインに属するプロセッサによる信頼度の相対的に高いプログラムを実行するドメインに属するメモリ及び／又は入出力装置へのアクセスをアクセス制御手段でチェックし、許可されたアクセスのみが実行される工程と、を含む。

[0031] 本発明の別の側面に係る装置は、予め定められた第1の類の処理を実行する、少なくとも1つのプロセッサ（「第1類プロセッサ」という）と、前記第1の類の処理と異なる予め定められた第2の類の処理を実行する、少なくとも1つのプロセッサ（「第2類プロセッサ」という）と、メモリ及び入出力装置と、前記第1類及び第2類プロセッサ間の通信を制御するプロセッサ間通信手段と、前記第2類のプロセッサによる前記メモリ及び／又は前記入出力装置のアクセスを制御するアクセス制御手段と、を備えている。

[0032] 本発明に係る装置において、前記第1の類の処理は、相対的に信頼度の高い処理を含み、前記第2の類の処理は、相対的に信頼度の低い処理を含む。本発明において、前記第1の類の処理は、ベンダー提供の基本処理を含み、前記第2の類の処理は、ネットワーク又は記憶媒体よりダウンロードされた追加処理を含む。本発明において、前記第2の処理は、前記第2類プロセッサで実行されるデバイスドライバ、及び／又はアプリケーション・プログラムを含む構成としてもよい。

[0033] 本発明に係る装置において、前記プロセッサ間通信手段として、前記第1類プロセッサ側から前記第2類プロセッサへ情報を受け渡すためのプロセッサ間の通信を行うプロセッサ間通信手段と、前記第2類プロセッサ側から前記第1類プロセッサへ情報を受け渡すためのプロセッサ間の通信を行うプロセッサ間通信手段と、を備えている。

[0034] 本発明に係る装置において、前記プロセッサ間通信手段は、好ましくは、情報の送り手側のプロセッサからの割り込み要求を受け、前記情報の受け手側のプロセッサに割り込みを発行する割り込み制御装置を備えている。本発明において、前記プロセッ

サ間通信手段は、好ましくは、割り込み先のプロセッサに対応させて、割り込み制御装置と、共有メモリと、を備え、前記割り込み制御装置は、割り込み要求元のプロセッサからの割り込み要求を受け付け、前記割り込み先のプロセッサに割り込み要求を行う割り込み指示部と、前記割り込み指示部での割り込み要求を保持する割り込み保持部と、前記割り込み先のプロセッサからの割り込み処理の完了通知を受けて割り込みを取り消す割り込み取り消し部と、を備え、前記共有メモリは、前記割り込み要求元のプロセッサから前記割り込み先のプロセッサに転送するデータを格納する通信領域と、前記通信領域の排他制御を行う排他制御領域と、を備えている。

[0035] 本発明に係る装置において、前記アクセス制御手段は、好ましくは、前記第2類プロセッサからの前記メモリ及び／又は前記入出力装置へのアクセスに関する情報を記憶するアクセス許可データを記憶する手段と、前記第2類プロセッサからの前記メモリ及び／又は前記入出力装置へのアクセスを監視し、前記アクセス許可データを参照して、前記アクセスの許可の有無を判別するアクセス許可手段と、を備えている。本発明において、前記アクセス許可データを記憶する手段は、前記第2類プロセッサに関して、アクセスを許可するプロセッサに対応させて、アクセスが許可されるアドレス範囲と、前記アドレス範囲に関する許可されたアクセス種別に関する情報を格納している。

[0036] 本発明のさらに別の側面の装置は、予め定められた第3類の処理を実行する、少なくとも1つのプロセッサ（「第3類プロセッサ」という）と、前記第2類及び第3類プロセッサ間で通信を行うプロセッサ間通信手段と、前記第3類のプロセッサによる前記第1類プロセッサに接続するメモリ及び／又は入出力装置のアクセスを制御する第2のアクセス制御手段と、をさらに備えている。

[0037] 本発明のさらに別の側面の装置は、予め定められた第3類の処理を実行する、少なくとも1つのプロセッサ（「第3類プロセッサ」という）と、前記第2類及び第3類プロセッサ間で通信を行うプロセッサ間通信手段と、を備え、前記第1類乃至第3類プロセッサの各々は、それぞれバスを介して、接続されるメモリ及び入出力装置を備え、前記第2類プロセッサによる、前記第1類プロセッサに接続する前記メモリ及び／又は前記入出力装置へのアクセスは、前記アクセス制御手段により制御され、前記第3類プ

ロセッサによる、前記第1類プロセッサに接続するメモリ及び／又は入出力装置、及び／又は、前記第2類プロセッサに接続する前記メモリ及び／又は前記入出力装置へのアクセスを制御する第2のアクセス制御手段をさらに、備えている。

[0038] 本発明の別の側面に係る装置は、(A)基本ソフトウエア環境と、外部デバイス、及び／又はファイルシステムと、オペレーティングシステムと、を備え、ダウンロードされたデータのセキュリティ情報を格納するセキュリティーデータベースと、ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、を備えた基本ドメインと、(B)ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、オペレーティングシステムと、を備え、前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたアプリケーション・プログラム(「信頼アプリケーション・プログラム」という)を実行し、前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたデバイスドライバ(「信頼ドライバ」という)を前記オペレーティングシステムにインストールし、前記信頼ドライバにより、予め用意された許可された外部デバイスにアクセスし、信頼できる追加処理を実行する信頼拡張ドメインと、(C)ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、オペレーティングシステムと、前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できないと判定された、ダウンロードされたアプリケーション・プログラム(「無信頼アプリケーション・プログラム」という)を実行し、前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できないと判定された、ダウンロードされたデバイスドライバ(「無信頼ドライバ」という)を前記オペレーティングシステムにインストールし、前記デバイスドライバにより予め用意された許可された外部デバイスにアクセスし、無信頼の追加処理を実行する無信頼拡張ドメインと、を備え、前記基本ドメイン、前記信頼拡張ドメイン、前記無信頼拡張ドメインは、それぞれ、前記第1類乃至第3類のプロセッサに実装される。

[0039] 本発明の別の側面に係る方法は、前記基本ドメインの外部デバイスからダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードアアプリケーション・プログラムと認識した場合、前記基本ドメインの前記ネイティブコードダ

ウンロード管理手段が、前記ダウンロードアプリケーション・プログラムの証明書をチェックする工程と、前記チェックの結果、正しい証明書と判定した場合、前記ダウンロードアアプリケーション・プログラムを、前記信頼拡張ドメインの前記ネイティブコードダウンロード管理手段にダウンロードデータを送信する工程と、を含む。

[0040] 本発明に係る方法において、前記基本ドメインの外部デバイスからダウンロードデータが入力される、前記基本機能が、前記ダウンロードデータをダウンロードドライバと認識した場合、前記ネイティブコードダウンロード管理手段が、ダウンロードドライバの証明書をチェックする工程と、前記チェックの結果、正しい証明書と判定した場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード管理手段にダウンロードドライバを送信する工程と、前記信頼拡張ドメインの前記ネイティブコードダウンロード管理手段は、前記ダウンロードドライバを、前記信頼拡張ドメインのオペレーティングシステムにインストールする工程と、を含むようにしてもよい。

[0041] 本発明に係る方法において、前記基本ドメインの外部デバイスからダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードアプリケーション・プログラムと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、ダウンロードアプリケーション・プログラムの証明書をチェックする工程と、前記チェックの結果、証明書がないか、証明書の内容が正しくない場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード管理手段を介して、前記無信頼拡張ドメインの前記ネイティブコードダウンロード管理手段にダウンロードデータを送信する工程と、を含むようにしてもよい。

[0042] 本発明に係る方法において、前記基本ドメインの外部デバイスから、ダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードドライバと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードドライバの証明書をチェックする工程と、前記チェックの結果、証明書がないか、証明書の内容が正しくない場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード管理手段を介して、前記無信頼拡張ドメインの前記ネイティブコードダウンロード管理手段にダウンロードドライバを送信する工程と、前記無信頼拡張ドメインの前記ネイティブコードダウンロード管理手段は、前記ダウンロードドライバを、

前記無信頼拡張ドメインのオペレーティングシステムにインストールする工程と、を含むようにしてもよい。

[0043] 本発明に係る方法において、前記信頼拡張ドメインに、前記基本ドメインの基本ソフト環境の基本機能への要求を発行する処理群を、ライブラリとして含む基本機能ライブラリを設けておき、前記信頼拡張ドメインにダウンロードされたアプリケーション・プログラムからの要求を受けて、前記基本機能ライブラリは、前記アプリケーション・プログラムの証明書を用いて、前記基本ドメインの前記ネイティブコードダウンロード管理手段に要求を送信する工程と、前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインより受信した要求が、適正であるか(アプリケーション・プログラムの証明書と対応がとれたものであるか)確認し、前記要求が適正である場合、前記基本ソフト環境の基本機能へ処理を依頼する工程と、含むようにしてもよい。前記基本ドメインの前記基本機能は、要求を処理し、処理の完了を前記基本ドメインの前記ネイティブコードダウンロード管理手段に通知する工程と、前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインの基本機能ライブラリに完了を通知し、前記アプリケーション・プログラムに処理の完了が通知される工程と、を含むようにしてもよい。

[0044] 本発明に係る方法において、前記信頼拡張ドメインに、前記基本ドメインの基本ソフト環境の基本機能への要求を発行する処理群を、ライブラリとして含む基本機能ライブラリを設けておき、前記無信頼拡張ドメインにダウンロードされたアプリケーション・プログラムから、前記信頼拡張ドメインのアプリケーション・プログラムにデータを送信する工程と、前記信頼拡張ドメインの前記アプリケーション・プログラムは前記基本機能ライブラリに対して、前記無信頼拡張ドメインのダウンロードアプリケーション・プログラムからのデータを含む要求の処理要求を発行する工程と、前記信頼拡張ドメインからの要求を受けて、前記基本機能ライブラリは、前記基本ドメインの前記ネイティブコードダウンロード管理手段に要求を送信する工程と、前記基本ドメインの前記ネイティブコードダウンロード管理手段は、受信した要求が適正であるか(アプリケーション・プログラムの証明書と対応がとれたものであるか)確認する工程と、確認の結果、前記要求が適正である場合、ユーザに確認を求め、前記ユーザの確認結果が可の

場合、前記基本ソフト環境の基本機能へ処理を依頼する工程と、一方、前記ユーザの確認結果が不許可の場合、前記ネイティブコードダウンロード管理手段は、前記基本機能ライブラリに、不許可を通知する工程と、を含むようにしてもよい。

本発明において、基本機能は、要求を処理し、処理の完了を前記基本ドメインの前記ネイティブコードダウンロード管理手段に通知する工程と、前記基本ドメインの前記ネイティブコードダウンロード管理手段は前記信頼拡張ドメインの基本機能ライブラリに完了を通知する工程と、前記ダウンロードアプリケーション・プログラムに処理の完了が通知される工程と、前記ダウンロードアプリケーション・プログラムは、前記無信頼拡張ドメインの前記ダウンロードアプリケーション・プログラムに処理の完了を通知する工程と、

を含むようにしてもよい。

本発明に係る情報処理装置は、複数のプロセッサを備え、前記複数のプロセッサは、第1のドメインと、前記第1のドメインとは異なる第2のドメインを構成するプロセッサと、を構成し

前記第2のドメインは、前記第1のドメインに属するプロセッサが実行する処理よりも信頼度の低い処理を、少なくとも1以上有するプロセッサで構成され、

前記第1のドメインと前記第2のドメインのプロセッサ同士の通信を制御するプロセッサ間通信手段と、

前記第2のドメインに属するプロセッサによる前記第1のドメインに属するメモリ及び／又は入出力装置へのアクセスを、前記第2のドメインで実行される処理の信頼度に応じて制限するアクセス制御手段と、を備えている。

本発明に係る情報処理装置において、前記アクセス制御手段は、アクセス許可データを記憶する手段と、

前記第2のドメインに属するプロセッサからの前記メモリ及び／又は前記入出力装置へのアクセスを監視し、前記アクセス許可データを参照して、前記アクセスの許可の有無を判別するアクセス許可手段と、

を備えている。

本発明に係る情報処理装置において、前記アクセス制御手段は、前記アクセス許

可データを更新するアクセス許可データ更新手段を有する構成としてもよい。

本発明に係る情報処理装置において、前記アクセス制御手段は、前記第2のドメインに属するプロセッサによるアクセス情報を取得するアクセス監視手段と、前記アクセス情報を記憶する学習手段を有する構成としてもよい。

本発明に係る情報処理装置において、前記プロセッサ間通信手段は、情報の送り手側のプロセッサからの割り込み要求を受け、前記情報の受け手側のプロセッサに割り込みを発行する割り込み制御情報処理装置を備えた構成としてもよい。

本発明に係る携帯情報端末は、複数のプロセッサを備え、前記複数のプロセッサは、第1のドメインと、前記第1のドメインとは異なる第2のドメインを構成するプロセッサと、を構成し

前記第2のドメインは、前記第1のドメインに属するプロセッサが実行する処理よりも信頼度の低い処理を、少なくとも1以上有するプロセッサで構成され、

前記第1のドメインと前記第2のドメインのプロセッサ同士の通信を制御するプロセッサ間通信手段と、

前記第2のドメインに属するプロセッサによる前記第1のドメインに属するメモリ及び／又は入出力装置へのアクセスを、前記第2のドメインで実行される処理の信頼度に応じて制限するアクセス制御手段と、を備えている。

発明の効果

[0045] 本発明によれば、複数のプロセッサは、処理のセキュリティに応じたドメインを構成し、ドメイン間のプロセッサの通信を、プロセッサ間通信手段を介して行い、低セキュリティドメイン側のプロセッサが、高セキュリティドメイン側のメモリ及び入出力装置に対するアクセス許可の有無を制御するアクセス制御手段を備え、ダウンロードされたデバイスドライバ、アプリケーションを低セキュリティドメイン側で実行することで、安全性を確保している。

[0046] また、本発明によれば、高セキュリティと低セキュリティドメインでの処理は、各ドメインでのプロセッサによる並列処理が行われ、これにより、高速処理を可能としており、さらに、高セキュリティと低セキュリティドメインのプロセッサ間での同期、連携処理も可能としている。

図面の簡単な説明

[0047] [図1]本発明の一実施例のハードウェア構成を示す図である。

[図2]本発明の一実施例のプロセッサ間通信手段の構成を示す図である。

[図3]本発明の一実施例のプロセッサ間通信手段の動作を説明するための図である。

[図4]本発明の一実施例のアクセス制御手段の構成を示す図である。

[図5]本発明の一実施例のアクセス制御手段のアクセス許可データの例を示す図である。

[図6]本発明の一実施例のアクセス制御手段の動作を説明する図である。

[図7]本発明の別の実施例のハードウェア構成を示す図である。

[図8]本発明の別の実施例のハードウェア構成を示す図である。

[図9]本発明の一実施例のソフトウェア構成を示す図である。

[図10]本発明の一実施例の動作を説明するための図である。

[図11]本発明の一実施例の動作を説明するための図である。

[図12]本発明の一実施例の動作を説明するための図である。

[図13]本発明の一実施例の動作を説明するための図である。

[図14]本発明の一実施例の動作を説明するための図である。

[図15]本発明の一実施例の動作を説明するための図である。

[図16]本発明の一実施例の動作を説明するための図である。

[図17]本発明の一実施例の動作を説明するための図である。

[図18]本発明のさらに別の実施例の構成を示す図である。

[図19]本発明のさらに別の実施例の動作を説明するための図である。

[図20]本発明の一実施例の変形例を示す図である。

[図21]従来のシステム構成の一例を示す図である。

[図22]従来のシステム構成の別の例を示す図である。

[図23]従来のシステム構成の別の例を示す図である。

[図24]従来のシステム構成のさらに別の例を示す図である。

[図25]本発明の一実施例における信頼度の一例を示す図である。

[図26]本発明の一実施例における信頼度の一例を示す図である。

[図27]本発明の一実施例における信頼度の一例を示す図である。

[図28]本発明の一実施例における信頼度の一例を示す図である。

符号の説明

[0048] 10、10A、10B、10C CPU

11 CPU

12 セキュアモード

13 非セキュアモード

14 メモリ管理ユニット

15 分離手段

20、20A、20B、20C ソフトウェア

21、21A、21B、21C OS

22 基本処理

23、23B、23C 追加処理

24 仮想マシン

25 証明書

30 アクセス制御手段

31 アクセス許可手段

32 アクセス許可データ

40 プロセッサ間通信手段

41 割り込み制御装置

410～41n CPU＃0～CPU＃n用割り込み制御装置

42 共有メモリ

420～42n CPU＃0～CPU＃n用通信領域

50、50A、50B、50C メモリ

60、60A、60B、60C 入出力デバイス(I／O)

70A 基本側バス

70B 追加側バス

100A 基本ドメイン

100B Trusted拡張ドメイン

100C Untrusted拡張ドメイン

101A、101B、101C OS

102A 外部デバイス

102A' 仮想外部デバイス

102B、102C 許可された外部デバイス

102B'、102C' 許可された仮想外部デバイス

103 専用ファイルシステム

103' 仮想専用ファイルシステム

104A ネイティブコードダウンロード管理機能

104B、104C ネイティブコードダウンロード実行機能

105 セキュリティポリシーデータベース

110 基本ソフト環境

111 基本アプリケーション

112 基本機能

113 基本機能ライブラリ

120A、120B、120C ダウンロードアプリケーション

121B、121C ダウンロードドライバ

200A、200B、200C 仮想CPU

210A、210B、210C 仮想マシンモニタ

411 割り込み指示部

412 割り込み状態保持部

413 割り込み取り消し部

421 通信キュー

422 排他制御領域

発明を実施するための最良の形態

[0049] 本発明を実施するための最良の形態について説明する。本発明は、その好ましい

一実施の形態において、複数のCPUを備えたマルチCPU構成の情報処理装置において、複数のCPUを、実行するプログラム(処理)の信頼度に応じて、複数のドメイン(例えば基本ドメイン、信頼ドメイン、無信頼ドメイン等)に分け、各ドメインは、1つ又は複数のCPUを含み、異なるドメイン間でのCPUの通信を、プロセッサ間通信手段(例えば図1の40)を介して行うとともに、追加処理等の低セキュリティの処理を実行するドメインに属するCPUが、高セキュリティの処理を実行するドメインのメモリ及び入出力装置に対してアクセスする場合には、該アクセス要求は、アクセス制御手段(例えば図1の30)によって、アクセスの許可／非許可が判別され、許可されたアクセスのみが行われる構成とされる。

本明細書において、「信頼度」とは、処理ごとに付与されたセキュリティの度合いを示す電子証明書に基づき、あるセキュリティポリシーに従ってセキュリティレベルの段階ごとに設定されるものをいう。

例えば、デジタル署名が付与された処理ごとに、あるセキュリティポリシーに基づきセキュリティレベルが設定される。例えば図25に示すように、

レベルA:パスワードが必要、

レベルB:2度確認しない、

レベルC:実行ごとに確認、

レベルD:アクセスごとに確認、

といった具合に、実行する機能に応じたドメインにセキュリティレベルを付与する。

例えば、

基本ドメインには、レベルA、

信頼拡張ドメインには、レベルB、

無信頼ドメインには、レベルC

を配置するというように、1ドメインには、同種のセキュリティレベルのみを配置してもよいが、かかる構成に制限されるものではない。すなわち、1ドメインが複数種のセキュリティレベルを含むようにしてもよい。一例として、図25に示すように、

基本ドメインには、実行する機能の重要度によって、レベルA以上、レベルB以上、

信頼拡張ドメインにも、実行する機能によって、レベルB以上、レベルC以上

という配置としても良い。

このような設定が可能であれば、いかなる証明書やいかなるセキュリティポリシーに基づいて設定してもよく、実行する機能やドメイン数に応じて任意に設定することが可能である。

[0050] かかる構成の本発明の一実施の形態によれば、ダウンロードされた追加処理(デバイスドライバ、アプリケーション・プログラムを含む)を、高セキュリティ・ドメインとはハードウェア的に別構成の低セキュリティ・ドメイン側のCPUで実行することで、高セキュリティ・ドメインの安全性を確保している。

本明細書において、「ダウンロード」は、携帯電話のキャリアが用意するデータ通信網や一般的な無線LAN網等だけでなく、SDカードに代表される蓄積型メディア媒体、USBに代表される有線通信・媒体といった接続を経由した、情報装置へのダウンロードも含む。

[0051] そして、本発明の一実施の形態によれば、高セキュリティ・ドメインと低セキュリティ・ドメインのCPUを、スイッチ等で分離制御するのではなく、相互に通信可能とする、プロセッサ間通信手段を介して接続することで、安全性を保証しながら、高セキュリティ・ドメインと低セキュリティ・ドメインのCPU間の同期、協調動作も可能としている。

[0052] このプロセッサ間通信手段(図1の40)は、一のドメインのCPUから他のドメインのCPUへデータ(コマンド)の受け渡しを行うものであり、他のドメインのCPUへの直接的な攻撃等は行えない構成とされている。例えば低セキュリティ・ドメイン側のCPUから高セキュリティ・ドメインのCPU側へデータを多量に送信し続けることで、高セキュリティ・ドメインのCPUの性能劣化、バッファオーバフロー等を生じさせようとしても、プロセッサ間通信手段で抑止され、該データは、高セキュリティ・ドメインのCPUに伝達されない。

[0053] また、本発明の一実施の形態において、アクセス制御手段(図1の30)は、低セキュリティ・ドメイン側のCPUに対して、予め許可されたメモリ空間、入出力デバイス等へ予め許可された形態によるアクセスのみを許可するアクセス制御を行う。これにより、ダウンロードされた追加処理からの高セキュリティ・ドメインへの攻撃を防ぐことができる。あるいは、アクセス制御手段が、必要に応じて、帯域、流量制御等を行うことで、

ダウンロードされた追加処理からの高セキュリティ・ドメインへの各種攻撃を防ぐことができる。以下実施例に即して説明する。

実施例

[0054] 図1は、本発明の一実施例の構成を示す図である。図1を参照すると、基本処理22及びOS21Aからなるソフトウェア20Aを実行するCPU群10Aと、追加処理23及び追加処理対応のOS21Bからなるソフトウェア20Bを実行するCPU群10Bと、CPU群10A、10B間で通信を行うプロセッサ間通信手段401、402と、CPU群10Bによるメモリ50及び／又は入出力装置(I／O)60へのアクセスを制御するアクセス制御手段30と、を備えている。なお、図1には、CPU群10A、CPU群10Bは、それぞれ複数(3台)のCPUから成る構成として示されているが、各群とも1つのCPUであってもよいことは勿論である。また、CPU群10A、CPU群10Bにおいて、各群のCPUの台数は等しくなくてもよいことは勿論である。以下では、CPU群10A、CPU群10Bを、単に、CPU10A、CPU10Bという。本実施例において、ダウンロードされる追加処理23は、バイナリ形式のネイティブコードよりなる。なお、ダウンロードされたソースプログラムを、コンパイル処理(アセンブル処理)してバイナリ形式としたものであってもよい。

[0055] 本実施例によれば、追加処理23を実行するCPU10Bを、基本処理22を実行するCPU10Aと別に備え、CPU10A、10Bは、独立に動作可能であり、安全性を向上しながら、高速実行を可能とし、アプリケーションプログラム、デバイスドライバの実行を可能としている。なお、基本処理22を実行するCPU10Aをマスターとし、追加処理23を実行するCPU10Bをスレーブとして構成し、スレーブ側はマスターの監督下で動作する構成としてもよいことは勿論である。この場合、例えばCPU10Bによる追加処理23の実行は、CPU10Aからプロセッサ間通信手段402を介してコマンドを受け取って行われる。

[0056] プロセッサ間通信手段401、402は、CPU10AとCPU10B間でのデータの送受信を制御する。CPU10A、10Bは、独立に配設されていることから、それぞれの処理(プログラム)を並列に実行することが可能であるとともに、プロセッサ間通信手段401、402を介して、CPU10AとCPU10B間における、同期処理、連携(協調)処理も可

能としている。一例として、ユーザが表示装置の画面上から追加処理の実行を指示した場合、基本処理22を実行するCPU10Aから、プロセッサ間通信手段401を介して、追加処理23の起動要求が、CPU10Bに送信され、CPU10B上で追加処理23が実行され、実行結果が、CPU10Bから、プロセッサ間通信手段402を介して、CPU10Aに送信され、基本処理22を構成する画面制御ルーチン等が、追加処理23の実行結果を反映した情報をユーザに提示する、という具合である。

[0057] 本実施例では、CPU10Bで追加処理23を実行する際、メモリ50、入出力デバイス(I／O)60へのアクセス要求が行われた場合、アクセス制御手段30にて、当該アクセスに関する許諾の制御が行われ、許可されたアクセス要求のみが、メモリ50、入出力デバイス(I／O)60に対して実行される構成とされている。そして、CPU10Bにおいて、OS21B上で追加処理23を実行し、追加処理23からの、基本処理22あるいはOS21Aへの処理要求が発行された場合、該要求は、プロセッサ間通信手段401を介してCPU10Aに通知される。すなわち、追加処理23が、基本処理22を、直接操作することはできない。例えば、悪意のある追加処理23が、CPU10Aに要求を頻発して発行して負荷を与え、CPU10A側での基本処理の実行性能を著しく低下させようとしても、プロセッサ間通信手段401が、このような要求をCPU10A側に伝達しないように制御することで、上記攻撃からの防護が実現され、安全性が確保される。

[0058] なお、図1に示す例では、プロセッサ間通信手段401は、CPU10BからCPU10Aへの情報転送、プロセッサ間通信手段402は、CPU10AからCPU10Bへの情報転送を制御している。あるいは、一台のプロセッサ間通信装置で双方向のデータの受け渡しを行うようにしてもよいことは勿論である。本実施例において、基本処理22を実行する複数のCPU10A同士でCPU間の通信が必要な場合には、プロセッサ間通信手段40を用いることなく、CPU間の通信が行われる。また、追加処理23を実行する複数のCPU10Bについても同様である。ただし、後述するように、CPU群10Bを構成する複数のCPUのいくつかをCPU群10Aの要素としてダイナミックに切り替える場合、CPU群10Bは、論理的にはCPU群10Aに属するが、CPU間の通信は、プロセッサ間通信手段40を介して行うようにしてもよい。

[0059] 本実施例によれば、追加処理23として、アプリケーションプログラム、デバイスドライ

バのダウンロード、インストール、実行が可能とされている。追加されたデバイスドライバは、OS21Bに組み込まれ、CPU10B上で実行され、入出力デバイス60へのアクセス制御は、アクセス制御手段30の監視のもとで実行される。

[0060] なお、携帯電話機、PDA等の携帯型情報通信装置では、通常、図1における基本処理22、OS21Aは、図示されない書き換え可能な不揮発性メモリ(EEPROM;Electrically Programmable and Erasable ROM)に格納され、CPU10Aは、EEPROMから命令コードをフェッチしてデコードし実行する。同様にして、追加処理23、OS21Bも、CPU10A用とは別のEEPROMに格納され、CPU10Bは、EEPROMから命令コードをフェッチしてデコードし実行する。すなわち、基本処理22と追加処理23を実行するそれぞれのOS21A、21Bが格納されるメモリは、基本処理側と追加処理側で、ハードウェア的に分離されている。そして、基本処理、OS等の命令コードは、EEPROMに格納されたものが実行されるが、CPU10A、10Bで実行されるプログラムにより、初期化、参照、更新されるテーブル等のデータは、それぞれのOS起動時等に、DRAM(Dynamic RandomAccess Memory)よりなるメモリ50に展開される。そして、CPU10Bについて、リード/ライトするメモリ領域をアクセス制御手段30によって管理し、CPU10Aで参照されるメモリ領域へのアクセスを制限している。携帯型情報通信端末とは別の一般の情報処理装置においても、同様にして、基本処理22、OS21Aがロードされ CPU10Aが命令コードをフェッチするメモリと、追加処理23、OS21Bがロードされ CPU10Bが命令コードをフェッチするメモリとを別々に備えてもよいことは勿論である。あるいは、一般の情報処理装置において、メモリ50に、基本処理22、OS21Aがロードされる領域と、追加処理23、OS21Bがロードされる領域を分離して設け、CPU10Bのメモリ50へのリード/ライトアクセスをアクセス制御手段30によって管理するようにしてもよい。この場合、CPU10A、CPU10Bが参照のみするコードについては、共通のメモリ領域に格納し、アクセス制御手段30によって、共通のメモリ領域を、該CPU10Bがリードのみ可とするようにアクセス制御してもよい。

また、携帯型情報処理装置において、搭載する電池残量が少なくなってきた場合には、基本処理を実行するCPU以外を強制的にシャットダウンする、実行する処理の信頼度に応じてより信頼度の低い処理を実行するCPUを優先的にシャットダウン

することで電池残量の節約を行うことが可能である。これは、例えば、電池残量を検出する手段と、検出結果を通知する手段によって得られる電池残量に関する情報に基づき、基本処理を行うCPU上で判断を行ない、シャットダウンを実行する、といった処理により実現できる。

さらに、携帯型情報処理装置での資源、例えば外部との通信バンド幅や不揮発メモリ量等はより一層制限されているため、信頼度に応じて、資源を確保する相対的な割合を変更することも可能である。これは、例えば、基本処理を行うCPUにおいて、

・実行する処理の信頼度が高い場合には、優先的に資源の確保を許容する、

・実行する処理の信頼度が低い場合には、資源の制限をかける

等の判断をすることにより実現される。

[0061] 図2は、本発明の一実施例におけるプロセッサ間通信手段のハードウェア構成の一例を示す図である。図2を参照すると、左右両側のCPU(基本処理を実行するCPUと追加処理を実行するCPU)間に配設された、割り込み制御装置41と共有メモリ42の1セットで、図1のプロセッサ間通信手段401、402の全体を構成している。割り込み制御装置41としては、CPU＃0、CPU＃1、…CPU＃n用のn個の割り込み制御装置410～41nを備え、各割り込み制御装置は、割り込み指示部411と、割り込み状態保持部412と、割り込み取り消し部413とを備えている。また、共有メモリ42は、CPU＃0、CPU＃1、…CPU＃n用のn個の通信領域420～42nを備え、各通信領域は、送信情報(データ、メッセージ)をキューイング又はバッファリングする通信キュー421と、相互排他制御を行う排他制御領域422とを備えている。

[0062] 例えばCPU＃0とCPU＃1の2つの構成を想定すると、CPU＃1用の割り込み制御装置411と、CPU＃1用の通信領域421とが、CPU＃0からCPU＃1へプロセッサ間通信手段401を構成し、CPU＃0用の割り込み制御装置410とCPU＃0用の通信領域420とが、CPU＃1からCPU＃0へのプロセッサ間通信手段402を構成している。

[0063] 割り込み制御装置41と、共有メモリ42は、CPU＃0、CPU＃1、…CPU＃nと、バス接続する構成とされる。また、共有メモリ42の通信キュー421には、送信データそのものでなく、送信データを格納するバッファポインタ(例えばメモリ50上でのバッファ

領域のアドレス)を設定するようにしてもよい。

[0064] 本実施例では、共有メモリ42におけるCPU＃iの排他制御領域422iは、CPU＃iの通信領域42iを、あるCPUがすでに占有している場合、他のCPUがCPU＃iの通信領域42iを使用することがないようにする相互排他制御のために、設けられている。すなわち、CPU＃iの排他制御領域422iは、mutex等のセマフォア、フラグ等の同期管理情報の格納に用いられる。

[0065] 共有メモリ42に実装された相互排他制御機構により、送信CPUと受信CPU間におけるデータの整合性(consistency)が保証される。

[0066] また、相互排他制御機構により、送信側CPUは、排他制御領域422がロック状態のときは、送信CPUに対する割り込み要求を上げることができず、これにより、送信CPUから受信CPUへの頻繁なデータ送信等、不当な割り込み発生を防ぐことができる。

[0067] なお、排他制御領域422としては、キューへの繋ぎ(エンキュー)、キューからの取り外し(デキュー)のロック管理として用いてもよい。

[0068] 図2において、割り込み制御装置41を介して一つの受信CPUへの多重割り込みを許可する構成とした場合、共有メモリ42において、各CPUの通信領域における通信キュー421、排他制御領域422は、多重数分設けられることになる。

[0069] 特に制限されないが、共有メモリ42は、図1のメモリ50の所定のメモリ領域を共有メモリとして用いてもよいし、メモリ50とは別に、プロセッサ間通信手段40内に設ける構成としてもよい。また、図示されないが、割り込み制御装置410～41nからの割り込み要求(Interrupt Request)線は、パラレルに受信CPUに接続する構成としてもよいし(割り込み本数が増える)、あるいは、デイジーチェーン方式で接続する構成としてもよい。

[0070] 受信CPUは、割り込み制御装置41からの割り込み要求を受理すると、これを割り込み制御装置41に通知し、割り込み制御装置41は、図示されないデータ線に割り込み装置番号(割り込みベクター情報)を転送し、受信CPUは、割り込み装置番号から割り込みベクターを生成し、スケジューラを介して、受信CPUで実行される割り込みサービスルーチンが起動され、割り込みサービスルーチンが、対応する共有メモリ

42の通信キューからデータを取得し、排他制御領域のmutex等のセマフォアをリリース(アンロック)し、割り込みから復帰(Return From Interrupt)するという一連の制御が行われる。

[0071] 図3は、図2に示した本実施例のプロセッサ間通信手段の動作手順を説明するための図であり、CPU＃kからCPU＃0へデータを送信する場合の手順が示されている。図3において、矢線脇の数字は、ステップ番号を表している。

[0072] ステップ1:送信CPU＃kは、共有メモリ42のCPU＃0の通信領域の排他制御領域をロックする。なお、共有メモリ42のCPU＃0の通信領域の排他制御領域が他のCPUによりロックされていることを示している場合、例えば該ロックが解除されるまで、待機する。

[0073] ステップ2:送信CPU＃kは、共有メモリ42のCPU＃0の通信領域の排他制御領域をロックしたあと、共有メモリ42のCPU＃0用通信領域の通信キューに、送信CPU＃kに送信するデータを書き込む。

[0074] ステップ3:送信CPU＃kは、割り込み制御装置41のCPU＃0用割り込み制御装置の割り込み指示部に、割り込み要求を通知する。

[0075] ステップ4:CPU＃0用割り込み制御装置の割り込み指示部は、CPU＃0用割り込み制御装置の割り込み状態保持部を更新し、「割り込み要求あり」に設定する。

[0076] ステップ5:CPU＃0用割り込み制御装置の割り込み指示部は、受信CPU＃0へ割り込みを行う。

[0077] ステップ6:受信CPU＃0は、CPU＃0用割り込み制御装置の割り込み指示部からの割り込みを受理し、共有メモリ42のCPU＃0用通信領域の通信キューから、データを取り出す。このとき、受信CPU＃0では、上記した割り込みサービスルーチンによる処理が行われる。

[0078] ステップ7:受信CPU＃0は、共有メモリ42のCPU＃0用通信領域の通信キューから、データを取得したのち、CPU＃0用割り込み制御装置の割り込み取り消し部に、割り込み処理完了を通知する。

[0079] ステップ8:受信CPU＃0からの割り込み処理完了通知を受けたCPU＃0用割り込み制御装置の割り込み指示部は、CPU＃0用割り込み制御装置の割り込み状態保

持部を更新する。

[0080] ステップ9:受信CPU＃0は、共有メモリ42のCPU＃0の通信領域の排他制御領域をアンロックする。

[0081] 本実施例において、特定の受信CPUへの割り込み要求の集中を認識した場合、受信CPUへの割り込み要求を抑制する等の流量制御、帯域制御を行うようにしてもよい。すなわち、割り込み制御装置41内に、送信CPU側から受信CPUに対して、連続・多発して割り込み要求を上げることがないように制限するQoS保証機能を備えてもよい。例えば、受信CPUへのデータの引渡しを伴わない割り込み要求は、排他制御の対象とされず、複数連続して発行することができる。そこで、受信CPU側で割り込み処理が完了しない状態において、送信CPU側からの割り込み要求が発生し、割り込み制御装置41の割り込み状態保持部の「割り込み要求あり」が所定数以上となった場合に、以降の送信CPU側から割り込み要求を不許可とする制御が行うようにしてもよい。かかる構成により、例えば送信CPUが、受信CPUへのデータの引渡しを伴わない割り込み要求を多量に発生することで、受信CPUの性能を低下させるといった類の攻撃を抑えることができる。

[0082] 図4は、図1に示した本発明の一実施例のアクセス制御手段30の構成を示す図である。図4を参照すると、このアクセス制御手段30は、基本側バス70Aを介して、基本処理(図1の22)を実行するCPU10Aに接続し、追加側バス70Bを介して追加処理(図1の23)を実行するCPU10Bに接続するアクセス許可手段31と、アクセス許可データ32を格納した記憶手段を備えている。

[0083] アクセス許可データ32は、CPU10Aから読み出し・書き込みが可能とされる。アクセス許可手段31からは読み出しのみが許可されている。そして、アクセス許可データ32は、CPU10Bからは読み出しも書き込みも不可とされる。すなわち、アクセス許可データ32とCPU10Bの間にはデータパスが存在しない。

[0084] アクセス許可手段31は、追加側バス70Bのアドレス信号線、制御信号線に転送される、メモリ50(図1参照)へのアクセスアドレス信号、及び、制御信号(アクセスコマンド)から、アクセスの種別(リード／ライト)を判別し、アクセス許可データ32の情報を参照して、当該アクセスが適正であるか否かを判別する。判別の結果、アクセスが不当

と判断された場合、アクセス許可手段31は、基本側バス70Aへのアクセスアドレス、制御信号(アクセスコマンド)の送出を行わず、これにより、CPU10B側から、基本側バス70Aへのアクセスは行われない。この場合、追加側バス70Bにアクセスアドレスを送出したCPU10B側では、バスエラー、あるいは、リード/ライトアクセスに対するメモリ50等からの不応答により、該アクセスが失敗したことを知る。

[0085] アクセス許可手段31は、入出力デバイス(I/O)60がメモリマップドI/Oである場合には、追加側バス70Bを監視し、アクセスアドレスが入出力デバイス対応のアドレスであることを検出し、データバス上に、I/Oコマンド(リード/ライト等)を検出した場合、該アクセスが適正であるかをアクセス許可データ32の情報を参照して決定する。入出力デバイスがメモリマップドI/Oでない場合も、追加側バス70Bに転送される入出力デバイスのデバイス番号、I/Oコマンドをデコードし、アクセス許可データ32の情報を参照して、アクセスの可否を決定する。

[0086] なお、本実施例において、アクセス制御手段30は、単位時間当りのデータ転送量の制御を行う帯域制約手段を備えてもよい。一例として、アクセス制御手段30は、CPU10Bがアクセス動作中に、CPU10Bから追加側バス70Bに転送されるデータ量を測定監視する手段を備え、例えば単位時間あたり予め定められた閾値を超えるバイト数のデータが転送される場合、CPU10BからCPU10Aへのデータ転送を打ち切る制御を行うようにしてもよい。その際、CPU10Bが、CPU10Aへのデータ転送がフェイルしたことを知ってリトライした場合にも、アクセス制御手段30は、CPU10Bからのデータを CPU10Aに転送することは行わない。あるいは、アクセス制御手段30は、バッファを備え、CPU10Bから追加側バス70Bに転送されるデータをバッファに蓄積し、CPU10Aに転送されるデータの流量を制御する構成としてもよい。

[0087] 図5は、本発明の一実施例におけるアクセス許可データ32の一例を示す図である。図5を参照すると、アクセス許可データは、追加処理を実行するCPU(図4の追加側バスに接続するCPU)と、アクセスが許可される範囲の始点アドレスと終点アドレスからなる許可範囲アドレスと、許可するアクセス種別(リード、リード/ライト、ライトの種別)がテーブル形式で格納されている。なお、許可範囲アドレスは、異なるCPUで重複してもよい。図5に示す例では、2行目のCPU#2、#3の許可範囲アドレスは、0x

C000000から0xF000000で、読み出し／書き込み可（R／W）あり、3行目のCPU＃3の許可範囲アドレスは、0xE000000から0xF000000であり、2行目と重複している。アドレス許可データの数、したがってテーブルのエントリ数は、その数が多いほど、きめ細かく、アクセス制御を行うことができる。なお、図5では、説明のため、R（読み出し可）、W（書き込み可）、R／W（読み出し／書き込み可）を例示したが、R（読み出し可）は、読み出しのみ可とし書き込みを不可とする情報であり、Wを書き込みを可とし（読み出しも可）とした場合には、R／Wは、不要とされる。また、読み出しが不可（書き込みも不可）のアドレス範囲は、アドレス許可データ32には格納されない。図5に示す例では、アクセス許可データとして、アクセスが許可されたCPUのそれぞれについて、アドレス範囲と、アクセス種別を有するが、アクセス許可データに、アクセス種別として、アクセス不可の情報をさらに設け、追加処理を実行するCPUについて、アクセス不可のアドレス範囲を格納するようにしてもよい。

[0088] 図4のアクセス許可手段31は、追加側のCPUからのアクセス要求（アドレス、読み書きコマンド）を受け取り、アクセス許可データ32の許可範囲アドレス、アクセス種別を参照して、許可されたアクセスの場合、該アクセスを許可する。一方、不許可の場合、アクセスを不許可とする。図5に示す例では、CPU＃4の場合、始点アドレス1000から終点アドレス2000（ヘキサデシマル）とされ、アクセス種別は読み出し（R）とされる。CPU＃2、＃3の場合、始点アドレス0xC000000から終点アドレス0xF000000（ヘキサデシマル）とされ、アクセス種別は読み出しと書き込み（R／W）とされる。CPU＃3の場合、始点アドレス0xE000000から終点アドレス0xF000000（ヘキサデシマル）のアクセス種別は書き込み（W）とされる。

[0089] 図6は、図4のアクセス制御手段30の動作の一例を説明するための図である。図6において、矢線脇の番号は、ステップ番号を表している。

[0090] ステップ1：基本処理を実行するCPU10Aは、アクセス制御手段30のアクセス許可データ32に、すべての追加処理を実行するCPU10Bが、あるアドレス範囲を読み出すことを禁止する。

[0091] ステップ2：CPU10Bが、追加処理23の実行等により、読み出しが禁止されたアドレス範囲への読み出し要求を発行したとする。

[0092] ステップ3:アクセス許可手段31は、アクセス許可データ32を読み出し、該アクセス要求の適否をチェックする。

[0093] ステップ4:アクセス許可手段31は、CPU10Bへエラーを返す。該アドレス範囲は、CPU10Bからの読み出しが禁止されているためである。

[0094] ステップ5:CPU10Bは、上記アドレス範囲とは別の範囲への読み出し要求を発行する。

[0095] ステップ6:アクセス許可手段31は、アクセス許可データ32を読み出してチェックする。

[0096] ステップ7:アクセス許可手段31は、CPU10Bの読み出しのアクセス要求を許可し、基本側バス70Aに読み出し要求として発行する。

[0097] なお、本実施例では、アクセス制御手段30の構成として、アクセス許可手段31と、アクセス許可データ32を備え、アクセス許可情報に基づき、アクセス制御を行う例について説明したが、本発明はかかる構成にのみ制限されるものでなく、アクセス許可のデータに変えて(反転し)、アクセス拒否データと、アクセス拒否手段を備えてもよい。この場合、アクセス拒否手段は、追加処理を実行するCPU10Bからのアクセスアドレスが、アクセス拒否データに、アクセス拒否が定義されたアドレス範囲に合致した場合に、アクセスを拒否する制御を行う。

[0098] 本実施例の変形例として、アクセス許可手段31に、キャッシュを備えてもよい。この場合、アクセス判定に用いたアクセスアドレス、アクセス許可データは、キャッシュに格納され、次回以降のアクセス制御の判定において、該当するアクセスアドレス(アドレス範囲)のアクセス許可データがキャッシュに存在するか判定し、キャッシュヒットした場合、アクセス判定の高速化を実現している。キャッシュには、アクセスアドレスの範囲に対応するタグアドレス、アクセス許可データを備え、追加側バス70Bのアクセスアドレスがキャッシュとヒットするか否か判定するキャッシュヒット判定回路を備えて構成される。

さらに、本実施例の変形例として、アクセス制御手段は、図26に示すように、新アクセス許可データ33と、アクセス許可データ更新手段34を備える構成としてもよい。図26を参照すると、アクセス制御手段30は、図4に示した実施例に加えて、基本側バ

ス70Aに接続するアクセス許可データ更新手段34と、新アクセス許可データ33を格納した記憶手段と、を備えている。この2つの手段の機能について詳細を説明する。

新アクセス許可データ33は、図4のアクセス許可データ32と同じ特徴を持つのに加え、アクセス許可データ更新手段34からのみの読み出しを許可する記憶手段である。

アクセス許可データ更新手段34は、基本側バス70Aを通じたCPU10Aからの要求によって、新アクセス許可データ33の内容をアトミックに新アクセス許可データ34に上書きする。

なお、本実施例において、アクセス許可データの更新ではなく、新アクセス許可データへの切替を行う手段を設けてもよい。

このような構成によれば、アクセス許可データ32の更新をCPUによりアトミックに書き換えることが可能となるため、アクセス制御手段による保護すべき領域、制限すべき領域を動的に変更することが可能である。

また、図27は本発明の一実施例のアクセス制御手段30の別の構成を示す図である。図27を参照すると、このアクセス制御手段30は、図4に示した実施例に加えて、追加側バス70Bに接続するアクセス監視手段35と学習手段36を備えている。この手段の機能について詳細を説明する。

アクセス監視手段35は、アクセス許可手段31と同様に、追加側バス70Bを通じたCPU10Bからのアクセス情報を取得する。

学習手段36は、前記アクセス監視手段35から提供されるアクセス情報を記憶する。そして、アクセス情報に基づき、その参照が適切かどうかを判断する。例えば、ユーザ保護データに対する参照回数をカウントしておき、もしあらかじめ指定された閾値を越えた場合には、異常事態と認定し、アクセス監視手段35にそのことを通知し、別途定められたルールに従ってアクセス許可データ32を動的に変更する。また、場合によっては、基本側バス70Aにつながるプロセッサ10Aに通知をし、異常時の処理を起動してもよい。

このような構成によれば、実際に参照されたパターンから信頼度が低いと思われるCPUの動作を履歴情報として蓄積することで自律的に制限できるため、実動作にお

けるCPUの動作状況に基づいたより安全な実行制御を行うことが可能となる。

また、アクセス制御手段の構成例としては、図4の構成に加えて、上記説明した新アクセス制御手段、アクセス許可更新手段、アクセス監視手段、学習手段のすべてを備える構成とすることも可能である。

[0099] 図7は、本発明の別の実施例の構成を示す図である。図7を参照すると、本実施例は、図1の構成に加えて、追加処理側のソフトウェアとOS、CPUをさらに1組追加したものである。すなわち、第2の追加処理側のCPU10Cは、プロセッサ間通信手段を介して、第1の追加処理用のCPU10Bと相互に通信する。また、第2の追加処理側のCPU10Cは、第2のアクセス制御手段302を介して、基本側バス70Aに接続される。

[0100] 各アクセス制御手段301、302の設定は、基本処理22を実行するCPU10Aが設定する。すなわち、基本処理22を実行するCPU10Aが、マスタープロセッサとして機能する。CPU10Aにより、メモリ50及び入出力デバイス(I／O)60の集中的な管理が行われる。

[0101] 第2の追加処理23Cを実行するCPU10Cは、第1の追加処理23Bを実行するCPU10Bに対してプロセッサ間通信手段403を介して通信(データ、コマンドの送信)を行い、第1の追加処理23Bを実行するCPU10Bは、基本処理22を実行するCPU10Aに対してプロセッサ間通信手段401を介して通信(データ、コマンドの送信)を行う。また、第2の追加処理23Cを実行するCPU10Cは、第2のアクセス制御手段302の監視の下、メモリ50、入出力デバイス(I／O)60に対して許可されたアクセスのみを行い、第1の追加処理23Bを実行するCPU10Bは、第1のアクセス制御手段301の監視の下、メモリ50、入出力デバイス(I／O)60に対して許可されたアクセスのみを行い、第1のアクセス制御手段301、第2のアクセス制御手段302のアクセス許可データの設定は、すべてCPU10Aによって行われる。かかる構成により、集中的な管理が行われ、また、プロセッサ間通信手段40により、CPU間で処理の受け渡しが行われる。本実施例においても、基本処理22を実行するCPU10Aに対する、追加処理23B、23Cからの直接的な攻撃等は回避される。すなわち、前記実施例と同様に、追加処理23B、23Cは、基本処理22を直接起動あるいはサブルーチン呼び出

しすることはできず、基本処理22の起動要求は、例えばCPU10CからCPU10Bを介して、CPU10Aに、プロセッサ間通信手段を介して伝達され、該要求を受け取ったCPU10Aでは、権限が付与されていないCPUからの要求である場合、該要求を受理しない(この詳細については、後述するソフトウェアの実施例で詳述する)。このように、追加処理側のCPUと基本処理側のCPUに権限の階層が設けられるほか、プロセッサ間通信手段40、及びアクセス制御手段30というハードウェア機構を介することで、基本処理等の直接的な攻撃は、回避される。本実施例におけるプロセッサ間通信手段401～404は、図2に示した前記実施例の構成と同様とされ、アクセス制御手段301、302も、図4に示した前記実施例の構成と同様とされるため、その詳細構成、動作の説明は省略する。

[0102] 図8は、本発明の別の実施例の構成を示す図である。図8を参照すると、本実施例は、図7に示した構成と同様に、図1の構成にさらに、追加処理側のCPU10Cと、アクセス制御手段302を追加したものである。本実施例は、図7に示した前記実施例と相違して、メモリと入出力デバイス(I／O)を、各組(ドメイン)のCPU群毎に用意している。第2の追加処理CPU10Cは、許可されたメモリ50C、入出力デバイス(I／O)60Cには、アクセス制限なく自在にアクセスすることができる。第1の追加処理CPU10Bは、許可されたメモリ50B、入出力デバイス(I／O)60Bには、アクセス制限なくアクセスすることができる。

[0103] 第2の追加処理側のCPU10Cからの、基本処理側のメモリ50A、入出力デバイス(I／O)60Aへのアクセスは、第2のアクセス制御手段302及び第1のアクセス制御手段301と2段構成にて、アクセス制御が行われる。

[0104] 第1の追加処理側のCPU10Bからの、基本処理側のメモリ50A、入出力デバイス(I／O)60Aへのアクセスは、第1のアクセス制御手段301により、アクセス許可が判定される。

[0105] 第1のアクセス制御手段301のアクセス許可データ、第2のアクセス制御手段302のアクセス許可データは、基本処理のCPU10Aが設定する。第2のアクセス制御手段302のアクセス許可データは第1の追加処理のCPU10Bが設定してもよい。この実施例によれば、メモリ、入出力デバイス(I／O)をドメイン単位に分離し、CPU間を

プロセッサ間通信手段40で多段に接続する構成としたことにより、追加処理による攻撃からの防護機能を高め、安全性を確保している。

図28は、図1に示した本発明の一実施例を2以上のチップにおいて適用した例である。図28を参照すると、本発明の一実施例のCPU10A、10B、10C、10Dとアクセス制御手段301の組み合わせを複数並べることに加えて、さらに個々のチップ間をアクセス制御手段303で結合する。

ある一チップ内における一部のCPUを基本処理実行用として設けることで、一チップ内のアクセス制御手段によりアクセス制限を行うこともできるし、各チップ内の少なくとも一部のCPUを基本処理実行用として設けることも可能である。

また、異なるチップにまたがってドメインを構成し、各チップ間のアクセス制御手段により実行を制御することも可能である。

いずれの場合でも、適切なアクセス制御手段の設定によって、複数のチップ間においても本発明における実行制御を行うことが可能となる。

[0106] 上記した実施例では、主に、本発明のハードウェア構成について説明したが、本発明のソフトウェア構成について以下に説明する。

[0107] 図9は、本発明を実施するソフトウェア構成の一例を示す図であり、基本ドメインと、Trusted(信頼)拡張ドメイン、Untrusted(無信頼)拡張ドメインを備えている。図9のハードウェア構成としては、3つの群のCPUを備えた、図8の構成等を用いることができる。この場合、基本処理を実行する実行環境である基本ドメインは、図8のソフト20A、OS21Aに対応し、Trusted拡張ドメインは、図8のソフト20B、OS21Bに対応し、Untrusted拡張ドメインは、図8のソフト20C、OS21Cに対応させることができる。

[0108] 図9を参照すると、基本ドメイン100Aは、基本アプリケーションプログラム(「基本アプリケーション」という)111と、基本機能112を含む基本ソフト110と、OS101Aと、専用ファイルシステム103と、外部デバイス102Aを備え、ネイティブコードダウンロード管理機能104Aと、セキュリティポリシーデータベース105を備えている。特に制限されないが、基本機能112は、例えば、本実施例の情報通信装置が携帯型情報通信端末である場合、発呼、着信処理等の呼処理、インターネットアクセス、画面処理

等の、携帯型情報通信端末の基本機能を実現するもので、図1の基本処理22に対応している。基本アプリケーション111は、基本機能112を呼び出して処理を行い、基本機能112は、OSを介してファイルシステム、外部デバイスへのアクセスを行う。外部デバイスは、ワイヤレス通信インタフェース等の通信インタフェース、表示装置のインタフェース、キー、ポインティングデバイス等の入力インタフェース、SD(Secure Digital)メモリカードインタフェース、サウンドインタフェース等を含む。

[0109] Trusted拡張ドメイン100Bは、ネイティブコードダウンロード実行機能104Bと、ダウンロードアプリケーションプログラム(「ダウンロードアプリケーション」という)120Bと、基本機能ライブラリ(ラッパー)113と、OS101Bと、許可された外部デバイス102Bを備えている。

[0110] OS101Bは、証明書付のダウンロードドライバ121Bを含む。証明書付ドライバ121Bは、許可された外部デバイス102Bの入出力制御を行う。

[0111] Untrusted拡張ドメイン100Cは、ネイティブコードダウンロード実行機能104Cと、ダウンロードアプリケーション120Cと、OS101Cと、許可された外部デバイス102Cを備えている。OS101Cに組み込まれるダウンロードドライバ121Cは、許可された外部デバイス102Cの入出力制御を行う。

[0112] 基本ドメイン100Aの外部デバイス102Aから入力され、ダウンロードされたファイルについて、ネイティブコードダウンロード管理機能104Aが、セキュリティポリシデータベース105の内容を参照することで、信頼できる(信頼できる電子証明書付)ネイティブコードのアプリケーションを、Trusted拡張ドメイン100Bへ転送し、信頼できる(信頼できる電子証明書付)ネイティブコードのダウンロードドライバ121BのOS101Bへの組み込みを行う。

[0113] また、ネイティブコードダウンロード管理機能104Aは、信頼できない(例えば電子証明書無しであるか、証明書の内容が正しくない場合等)アプリケーションを、Trusted拡張ドメイン100B経由で、Untrusted拡張ドメイン100Cへ転送し、信頼できない(証明書無し)ダウンロードドライバのUntrusted拡張ドメインのOS101Cへの組み込みを行う。

[0114] Trusted拡張ドメイン100Bからは、基本機能112の呼び出しは許可されるが、Unt

rusted拡張ドメイン100Cからの基本機能112の呼び出しは、許可されない。ただし、Untrusted拡張ドメイン100CとTrusted拡張ドメイン100Bとの協働作業は可能である。

[0115] 信頼できるドメインで動作するアプリケーションプログラムは、信頼できないドメインからのデータについて、ユーザの確認(OK)があった場合にのみ、基本機能112へ引き渡す。ユーザの確認なく、信頼できないドメインからのデータを、基本機能112に渡さない。なお、信頼できる拡張ドメイン100Bから、直接、基本ドメイン100Aの基本機能112へ、処理要求を発行することはできない。

[0116] 図10は、図9に示した本発明の一実施例の動作を説明するための図であり、基本アプリケーションの実行を示す図である。図10において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0117] ステップ1:基本ドメイン100Aの基本アプリケーション111は、基本機能112に、処理要求(例えば、アドレス帳の追加等)を発行する。

[0118] ステップ2:基本機能112は、OS101Aを利用して、該当要求を処理する。

[0119] ステップ3:基本機能112は、基本アプリケーション111に要求の成否を通知する。

[0120] 図11は、図9に示した本発明の一実施例の動作を説明するための図であり、信頼アプリケーションのダウンロードの実行の様子を示す図である。図11において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0121] ステップ1:基本ドメイン100A上の外部デバイス102A(ネットワーク又はSDメモリカード等)からOS101Aにダウンロードデータが到着する。

[0122] ステップ2:ダウンロードデータは、基本機能112にて、属性情報等の情報から、追加アプリケーション(ダウンロードアプリケーション)と認識される。

[0123] ステップ3:基本機能112は、追加アプリケーションを、ネイティブコードダウンロード管理機能104Aに渡し、ネイティブコードダウンロード管理機能104Aは、セキュリティポリシーデータベース105を参照して、追加アプリケーションに付随した電子証明書をチェックする。前述したように、例えば電子証明書には、公開鍵やデジタル署名(証明される機関や公開鍵などを秘密鍵で暗号化したもの)が格納され、ネイティブコードダウンロード管理機能104Aが、証明書の認証を行う場合には、ディジタル署名の

部分を、公開鍵で解読して、証明書のデータの内容と一致するか否か確認し、一致する場合に、証明書のデータを信頼してもよいと判断する。さらに、アプリケーションのダイジェストからなるデジタル署名を付随しておくことで、ダウンロードしたアプリケーションが改竄されていないかどうかをチェックすることができる。

[0124] ステップ4:ネイティブコードダウンロード管理機能104Aは、電子証明書とともに、ダウンロード情報を、セキュリティポリシーデータベース105に保存する。

[0125] ステップ5:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、電子証明書のチェックの結果、正しい場合、Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bに、ダウンロードアプリケーションを送信し、実行を要求する。基本ドメイン100Aのネイティブコードダウンロード管理機能104Aから、Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bのデータの送信は、図7又は図8のプロセッサ間通信手段40を用いて行われる。

[0126] ステップ6:Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bは、受け取ったダウンロードアプリケーションを実行するように制御する。

[0127] ステップ7:ダウンロードアプリケーションはTrusted拡張ドメイン上で実行される。

[0128] 図12は、図9に示した本発明の一実施例の動作を説明するための図であり、信頼ドライバのダウンロード実行を示す図である。信頼ドライバとは、例えばダウンロードされたドライバに添付される電子証明書の照合結果が正しいドライバをいう。図12において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0129] ステップ1:基本ドメイン100A上の外部デバイス102A(ネットワーク又はSDカード等)からOS101Aにダウンロードデータが到着する。

[0130] ステップ2:基本機能112にて、属性情報、自動インストール情報等から、ダウンロードデータは、追加デバイスドライバ(ダウンロードドライバ)であると認識する。

[0131] ステップ3:基本機能112は、受信したドライバを、ネイティブコードダウンロード管理機能104Aに渡す。ネイティブコードダウンロード管理機能104Aは、セキュリティポリシーデータベース105を参照して、ダウンロードデータに付随した電子証明書をチェックする。

[0132] ステップ4:ネイティブコードダウンロード管理機能104Aは、電子証明書とともに、ダウンロード情報をセキュリティポリシーデータベース105に保存する。

[0133] ステップ5:ネイティブコードダウンロード管理機能104Aは、Trusted拡張ドメインのネイティブコードダウンロード実行機能104Bに対して、ダウンロードドライバを送信し、インストールの実行を要求する。基本ドメイン100Aのネイティブコードダウンロード管理機能104Aから、Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bのデータの送信は、図7又は図8のプロセッサ間通信手段40を用いて行われる。

[0134] ステップ6:Trusted拡張ドメインのネイティブコードダウンロード実行機能104Bは、受け取ったダウンロードドライバを自動インストールする。特に制限されないが、この実施例において、ダウンロードドライバはインストールしたのちCPUを再起動してOS101Bのある領域に組み込むレジデント型のドライバであってもよい。

[0135] ステップ7:Trusted拡張ドメインのOS101Bは、ダウンロードドライバをインストールされたことを、既に実行済みのアプリケーションに通知するか、表示する。

[0136] ステップ8:Trusted拡張ドメインにおいて、既に実行済みのアプリケーション120Bは、インストールされたダウンロードドライバ121Bを参照する。

[0137] ステップ9:Trusted拡張ドメインのOS101Bにインストールされ、ロードされたダウンロードドライバ121Bは、許可された外部デバイス102Bをアクセスする。

[0138] ステップ10:ダウンロードドライバ121Bは、ダウンロードアプリケーション120Bに外部デバイス102Bからのデータを返す。

[0139] 図13は、図9に示した本発明の一実施例の動作を説明するための図であり、Trusted拡張ドメインの信頼アプリケーション(ダウンロードアプリケーション)が、基本ドメインの基本機能を利用する場合の動作を示す図である。図13において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0140] ステップ1:Trusted拡張ドメイン100Bにおいて、ダウンロードアプリケーション120Bが、基本機能ライブラリ113へ、基本ドメイン100Aの基本機能112の処理を要求する。基本機能ライブラリ113は、基本ドメイン100Aの基本機能112の処理を実行するためのルーチンを集めたライブラリであり、ダウンロードアプリケーション120Bか

ら起動される。

[0141] ステップ2:Trusted拡張ドメイン100Bの基本機能ライブラリ113は、ダウンロードアプリケーション120Bが保有する電子証明書の鍵(公開鍵等)を用いて、要求を暗号化し、暗号化した要求を、基本ドメイン100Aのネイティブコードダウンロード管理機能104Aへ送信する。Trusted拡張ドメイン100Bの基本機能ライブラリ113から基本ドメイン100Aのネイティブコードダウンロード管理機能104Aへの要求の送信は、図7又は図8のプロセッサ間通信手段40を介して行われる。

[0142] ステップ3:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、受け取った要求を復号し、該要求を、電子証明書を利用して、要求送信元が適正であるか否か等のチェックを行う。なお、この例では、要求の暗号化と復号を用いて、要求をチェックしているが、アプリケーションと電子証明書の対応がとれる方法であれば、任意の方法を用いてよいことは勿論である。

[0143] ステップ4:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、要求のチェックの結果、OKであれば、基本機能112へ要求を依頼する。

[0144] ステップ5:基本ドメイン100Aの基本機能112は、ネイティブコードダウンロード管理機能104Aから受け渡された該要求を処理し、処理完了後、基本ドメイン100Aのネイティブコードダウンロード管理機能104Aへ、処理完了を通知する。

[0145] ステップ6:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、Trusted拡張ドメイン100Bの基本機能ライブラリ113へ、処理の完了を通知する。基本ドメイン100Aのネイティブコードダウンロード管理機能104AからTrusted拡張ドメイン100Bの基本機能ライブラリ113への通知の送信は、図7又は図8のプロセッサ間通信手段40を介して行われる。

[0146] ステップ7:Trusted拡張ドメインの基本機能ライブラリ113は、ダウンロードアプリケーション120Bに、要求に対する応答として処理の完了を通知する。

[0147] 図14は、図9に示した本発明の一実施例の動作を説明するための図であり、Untrusted拡張ドメインの無信頼アプリケーションのダウンロードの実行手順を示す図である。図14において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0148] ステップ1:基本ドメイン100A上の外部デバイス102A(ネットワーク又はSDカード等)から、OS101Aにダウンロードデータが到着する。

[0149] ステップ2:基本ドメイン100Aの基本機能112では、属性情報等を解析し、ダウンロードデータをアプリケーション(ダウンロードアプリケーション)と認識する。

[0150] ステップ3:基本ドメイン100Aの基本機能112は、ダウンロードアプリケーションを、ネイティブコードダウンロード管理機能104Aに渡す。ネイティブコードダウンロード管理機能104Aでは、アプリケーションに、電子証明書が付随されていないか、あるいは電子証明書が正しくないと判別する。

[0151] ステップ4:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、セキュリティポリシーデータベース105に、ダウンロード情報を保存する。

[0152] ステップ5:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、Trusted拡張ドメインのネイティブコードダウンロード実行機能104Bに、ダウンロードされたアプリケーションを送信する。基本ドメイン100Aのネイティブコードダウンロード管理機能104AからTrusted拡張ドメインのネイティブコードダウンロード実行機能104Bへのアプリケーションの送信は、図7又は図8に示したプロセッサ間通信手段40を介して行われる。

[0153] ステップ6:Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bは、Untrusted拡張ドメイン100Cのネイティブコードダウンロード実行機能104Cにアプリケーションを送信し、実行を要求する。Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104BからUntrusted拡張ドメイン100Cのネイティブコードダウンロード実行機能104Cへのアプリケーションの送信は、図7又は図8に示したプロセッサ間通信手段40を介して行われる。

[0154] ステップ7:Untrusted拡張ドメインのネイティブコードダウンロード実行機能104Cは、受信したダウンロードアプリケーション120Cの起動を行う。

[0155] ステップ8:ダウンロードアプリケーション120Cは、Untrusted拡張ドメイン100Cで動作を開始する。この場合、Untrusted拡張ドメインのダウンロードアプリケーション120Cは、Untrusted拡張ドメインのOS101C上で動作し、許可された外部デバイス102Cへのアクセスのみが許可される。

[0156] 図15は、図9に示した本発明の一実施例の動作を説明するための図であり、無信頼ドライバのダウンロード実行の様子を示す図である。図15において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0157] ステップ1:基本ドメイン100A上の外部デバイス102A(ネットワーク又はSDカード等)からOS101Aにダウンロードデータが到着する。

[0158] ステップ2:基本機能112は、ダウンロードデータの到着で起動され、属性情報、インストール情報等のダウンロードデータを解析し、デバイスドライバ(ダウンロードドライバ)と認識する。

[0159] ステップ3:基本機能112は、ダウンロードドライバを、ネイティブコードダウンロード管理機能104Aに渡し、ネイティブコードダウンロード管理機能104Aは、ダウンロードドライバに電子証明書が添付されていないか、あるいは、電子証明書は添付されているが、電子証明書の内容が正しくないことがわかる。

[0160] ステップ4:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、ダウンロード情報のみをセキュリティポリシーデータベース105に保存する。

[0161] ステップ5:ネイティブコードダウンロード管理機能104Aは、Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bにダウンロードドライバを送信する。ネイティブコードダウンロード管理機能104AからTrusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bへのダウンロードドライバの送信は、図7又は図8に示したプロセッサ間通信手段40を介して行われる。

[0162] ステップ6:Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104Bは、受け取ったダウンロードドライバを、Untrusted拡張ドメイン100Cのネイティブコードダウンロード実行機能104Cに転送する。Trusted拡張ドメイン100Bのネイティブコードダウンロード実行機能104BからUntrusted拡張ドメイン100Cのネイティブコードダウンロード実行機能104Cへのダウンロードドライバの転送は、図7又は図8に示したプロセッサ間通信手段40を介して行われる。

[0163] ステップ7:Untrusted拡張ドメイン100Cのネイティブコードダウンロード実行機能104Cは、受信したダウンロードドライバ121Cをインストールする。

[0164] ステップ8:OS101Cは、ドライバ121Cがインストールされたことを、既に実行済み

のアプリケーション120Cへ通知するか、画面に表示する(ユーザに通知する)。

[0165] ステップ9:Untrusted拡張ドメイン100Cにおいて、既に実行済みのアプリケーション120Cは、インストールされたダウンロードドライバ121Cを参照する。

[0166] ステップ10:Untrusted拡張ドメイン100Cにおいて、インストールされたダウンロードドライバ121Cは、Untrusted拡張ドメインのOS101Cを介して、許可された外部デバイス102Cをアクセスする。

[0167] ステップ11:Untrusted拡張ドメイン100Cにおいて、ダウンロードドライバ121Cは、ダウンロードアプリケーション120Cに、外部デバイス102Cから取得したデータを返す。

[0168] 図16は、図9に示した本発明の一実施例の動作を説明するための図であり、信頼アプリケーションと無信頼アプリケーションの連携の様子を示す図である。図16において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0169] ステップ1:Untrusted拡張ドメイン100C上のダウンロードアプリケーション120Cは、Trusted拡張ドメイン100B上のダウンロードアプリケーション120Bへデータを送信する。このデータの送信は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0170] ステップ2:Trusted拡張ドメイン100B上のダウンロードアプリケーション120Bは、受け取ったデータによる処理を行い、基本機能ライブラリ113へ、Untrusted拡張ドメインと連携した情報を含む基本機能処理を要求する。

[0171] ステップ3:Trusted拡張ドメイン100B上の基本機能ライブラリ113は、アプリケーションが保有する電子証明書を用いて、要求を暗号化し、基本ドメイン100A上のネイティブコードダウンロード管理機能104Aへ送信する。この要求の送信は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0172] ステップ4:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、要求を復号し、該要求の完全性を、セキュリティポリシーデータベース105に格納された電子証明書を利用してチェックする。チェックの結果、要求が正しい場合、ネイティブコードダウンロード管理機能104Aは、基本アプリケーション111を介して、ユーザ

に確認を求める。基本アプリケーション111は、画面表示、入力のアプリケーションを含む。なお、この例では、要求の暗号化と復号を用いて、アプリケーションと電子証明書の対応をチェックしているが、アプリケーションと電子証明書との対応がとれる方法であれば、任意の方法を用いてよいことは勿論である。

[0173] ステップ5:ユーザからの確認として「NO」が入力されるとする。

[0174] ステップ6:ネイティブコードダウンロード管理機能104Aは、Trusted拡張ドメイン100Bの基本機能ライブラリ113へ不許可を通知する。この不許可の通知は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0175] ステップ7:基本機能ライブラリ113は、ダウンロードアプリケーション120Bへ不許可を通知する。

[0176] ステップ8:Trusted拡張ドメイン100B上のダウンロードアプリケーション120Bは、Untrusted拡張ドメイン100C上のダウンロードアプリケーション120Cに不許可を通知する。この不許可の通知は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0177] 図17は、図9に示した本発明の一実施例の動作を説明するための図であり、信頼アプリケーションと無信頼アプリケーションの連携を示す図である。図17において、各矢線に付された番号は、当該線を情報が転送されるステップ番号を表している。

[0178] ステップ1:Untrusted拡張ドメイン100C上のダウンロードアプリケーション120Cは、Trusted拡張ドメイン100B上のダウンロードアプリケーション120Bへデータを送信する。このデータの送信は、図7又は図8等のプロセッサ間通信手段によって行われる。

[0179] ステップ2:Trusted拡張ドメイン100B上のダウンロードアプリケーション120Bは、受け取ったデータによる処理を行い、基本機能ライブラリ113へ、Untrustedと連携した情報を含む基本機能処理を要求する。

[0180] ステップ3:Trusted拡張ドメイン100B上の基本機能ライブラリ113は、アプリケーション120Bが保有する電子証明書を用いて、要求を暗号化し、基本ドメイン100A上のネイティブコードダウンロード管理機能104Aへ送信する。この要求は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0181] ステップ4:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、要求を復号し、該要求の完全性を、セキュリティポリシーデータベース105に格納される電子証明書を利用してチェックする。チェックの結果、要求が正しい場合、ネイティブコードダウンロード管理機能104Aは、基本アプリケーション111を介してユーザに確認を求める。なお、この例では、要求の暗号化と復号を用いて、アプリケーションと電子証明書の対応をチェックしているが、アプリケーションと電子証明書との対応がとれる方法であれば、任意の方法を用いてもよいことは勿論である。

[0182] ステップ5:この場合、ユーザの確認として「Yes」が入力される。

[0183] ステップ6:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、基本機能112へ要求を依頼する。

[0184] ステップ7:基本機能112は、要求を処理し、ネイティブコードダウンロード管理機能104Aに処理完了を通知する。

[0185] ステップ8:基本ドメイン100Aのネイティブコードダウンロード管理機能104Aは、Trusted拡張ドメイン100Bの基本機能ライブラリ113に完了を通知する。この完了通知は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0186] ステップ9:Trusted拡張ドメイン100Bの基本機能ライブラリ113は、ダウンロードアプリケーション120Bに完了を通知する。

[0187] ステップ10:Trusted拡張ドメイン100Bのダウンロードアプリケーション120Bは、UnTrusted拡張ドメイン100Cのダウンロードアプリケーション120Cに完了を通知する。この完了通知は、通常、図7又は図8のプロセッサ間通信手段40によって行われる。

[0188] 図18は、本発明のさらに別の実施例の構成を示す図である。OSとCPU間に仮想マシンモニタ(OSとの間に設けられ、CPUで実行されるソフトウェア層)を備えている。これにより、CPU、I/O、メモリ資源を仮想化している。仮想マシンモニタは、OSとCPU間で、仮想ハードウェア(例えば仮想入出力デバイス)を、実際のハードウェアデバイスにマッピングする。基本ドメイン、Trusted拡張ドメイン、UnTrusted拡張ドメインのそれぞれについて、OSは、仮想の専用ファイルシステム、仮想外部デバイスとの入出力(I/O)制御を行い、OSとCPU間に、仮想CPU200A、200B、200C、仮

想マシンモニタ210A、210B、210Cを備え、仮想の専用ファイルシステム103'、仮想外部デバイス102A'、102B'、102C'を、対応する実ファイルシステム、実外部デバイスへマッピングする。

[0189] 本実施例によれば、図8のハードウェア構成、図9のソフトウェア構成と相違して、本実施例において、例えば基本ドメインに対応する仮想CPUは固定でなく、Trusted拡張ドメイン等のCPUを、基本ドメインの仮想CPUとしてマッピングすることができる。なお、仮想マシンモニタは、その実装において、既存のOS、アプリケーションプログラム、CPU等の修正等は不要とされる。本実施例によれば、各ドメインのCPUの個数は可変とされ、仮想CPUを構成する。ソフトウェア構成として、基本ドメイン、Trusted拡張ドメイン、Untrusted拡張ドメインの構成は、デバイス、ファイルシステムが仮想デバイス、仮想ファイルシステムであることを除いて、図9に示した構成と同様である。

[0190] 図19は、図18に示した実施例の処理手順の一例を示す図である。図19において、各矢線に付された番号は、ステップ番号を表している。

[0191] ステップ1:基本ドメイン100Aの仮想マシンモニタ210Aは、Trusted拡張ドメイン100B上の仮想マシンモニタ210Bに対してCPUの委譲を要求する。

[0192] ステップ2:Trusted拡張ドメイン100B上の仮想マシンモニタ210Bは、仮想CPU資源を減らす。

[0193] ステップ3:Trusted拡張ドメイン100B上の仮想マシンモニタ210Bは、基本ドメイン100A上のCPU上の仮想マシンモニタ210Aに委譲可能なCPUを通知する。

[0194] ステップ4:基本ドメイン100A上の仮想マシンモニタ210Aは、アクセス制御手段等の設定を行い、仮想CPUの数を増やす。

[0195] 本実施例によれば、別の群のCPUを、基本ドメインのCPUのように動作させることができる。なお、アプリケーションのダウンロード処理は、前記した実施例の処理動作(図10乃至図18)と同一であるため、その説明は省略する。

[0196] 本実施例と変形例として、仮想マシンモニタを、セキュアモードで動作させるようにしてもよい。このようにすることで、安全性をさらに向上させることができる。

[0197] 上記ソフトウェアの各実施例において、各ドメインのCPU群がマルチプロセッサとし

て動作する場合、キャッシュコヒーレンスを保つためのバス、仮想マルチプロセッサの無効化のために、TLB(Translation Lookaside Buffer;アドレス管理ユニット内に設けられるアドレス変換表)の全エントリをフラッシュするシュートダウン等、ハードウェアで協調動作するチャネルについては、すべて、基本ドメイン100Aから、制御できるように構成されている。また、図20に示すように、各ドメインのCPU群(例えば図1のマルチCPU構成のCPU群10A、10B)を、分離手段15を介して、複数に分離できる構成としてもよい。これにより、例えばあるドメインのCPUを他のドメインに委譲する際の制御が容易化し、さらに障害マルチプロセッサの分離(graceful degrading)等にも対応可能としている。

[0198] なお、前記各実施例では、ネットワーク等装置外部からネイティブコードの追加処理(アプリケーション、デバイスドライバ)をダウンロードして実行する情報通信端末装置を例に説明したが、本発明は、かかる情報通信端末装置に限定されるものでなく、任意の情報通信装置に適用可能である。以上、本発明を上記実施例に即して説明したが、本発明は、上記実施例の構成にのみ限定されるものでなく、本発明の範囲内で当業者であればなし得るであろう各種変形、修正を含むことは勿論である。

請求の範囲

[1] 複数のプロセッサを備え、

前記複数のプロセッサは、第1のドメインを構成するプロセッサと、前記第1のドメインとは異なる第2のドメインを構成するプロセッサと、を含み、

前記第2のドメインは、前記第1のドメインに属するプロセッサが実行する処理よりも信頼度の低い処理を少なくとも1以上有するプロセッサを含み、

前記第1のドメインと前記第2のドメインのプロセッサ同士の通信を制御するプロセッサ間通信手段と、

前記第2のドメインに属するプロセッサによる前記第1のドメインに属するメモリ及び／又は入出力装置へのアクセスを、前記第2のドメインに属するプロセッサで実行される処理の信頼度に応じて制限するアクセス制御手段と、

を備えている、ことを特徴とする情報処理装置。

[2] 前記アクセス制御手段は、アクセス許可データを記憶する手段と、

前記第2のドメインに属するプロセッサからの前記メモリ及び／又は前記入出力装置へのアクセスを監視し、前記アクセス許可データを参照して、前記アクセスの許可の有無を判別するアクセス許可手段と、

を備えている、ことを特徴とする請求項1記載の情報処理装置。

[3] 前記アクセス制御手段は、前記アクセス許可データを更新するアクセス許可データ更新手段を有することを特徴とする請求項2に記載の情報処理装置。

[4] 前記アクセス制御手段は、前記第2のドメインに属するプロセッサによるアクセス情報を取得するアクセス監視手段と、前記アクセス情報を記憶する学習手段を有することを特徴とする請求項2に記載の情報処理装置。

[5] 前記プロセッサ間通信手段は、情報の送り手側のプロセッサからの割り込み要求を受け、前記情報の受け手側のプロセッサに割り込みを発行する割り込み制御情報処理装置を備えている、ことを特徴とする請求項1記載の情報処理装置。

[6] 予め定められた第1の類の処理を実行する、少なくとも1つのプロセッサ（「第1類プロセッサ」という）と、

前記第1の類の処理とは異なる第2の類の処理を実行する少なくとも1つのプロセッ

サ(「第2類プロセッサ」という)と、

メモリ及び入出力装置と、

前記第1類及び第2類プロセッサ間の通信を制御するプロセッサ間通信手段と、

前記第2類プロセッサによる前記メモリ及び／又は前記入出力装置へのアクセスを、前記第2の類の処理の信頼度に応じて制限するアクセス制御手段と、

を備えている、ことを特徴とする情報処理装置。

[7] 前記第1類プロセッサを複数備え、前記第2類プロセッサを複数備えている、ことを特徴とする請求項6記載の情報処理装置。

[8] 前記第2類プロセッサは、前記第1類プロセッサが実行する前記第1の類の処理よりも信頼度の低い処理を少なくとも1以上実行する、ことを特徴とする請求項6に記載の情報処理装置。

[9] 前記第1の類の処理は、ベンダー提供の基本処理を含み、

前記第2の類の処理は、ネットワーク又は記憶媒体よりダウンロードされた追加処理を含む、ことを特徴とする請求項6記載の情報処理装置。

[10] 前記第2の類の処理は、前記第2類プロセッサで実行されるデバイスドライバ、及び／又はアプリケーション・プログラムを含む、ことを特徴とする請求項6記載の情報通信装置。

[11] 前記プロセッサ間通信手段として、前記第1類プロセッサ側から前記第2類プロセッサへ情報を受け渡すためのプロセッサ間の通信を行うプロセッサ間通信手段と、

前記第2類プロセッサ側から前記第1類プロセッサへ情報を受け渡すためのプロセッサ間の通信を行うプロセッサ間通信手段と、

を備えている、ことを特徴とする請求項6記載の情報処理装置。

[12] 前記プロセッサ間通信手段は、情報の送り手側のプロセッサからの割り込み要求を受け、前記情報の受け手側のプロセッサに割り込みを発行する割り込み制御情報処理装置を備えている、ことを特徴とする請求項6記載の情報処理装置。

[13] 前記プロセッサ間通信手段は、

割り込み先のプロセッサに対応させて、割り込み制御情報処理装置と、共有メモリと、

を備え、

前記割り込み制御情報処理装置は、割り込み要求元のプロセッサからの割り込み要求を受け付け、前記割り込み先のプロセッサに割り込み要求を行う割り込み指示部と、

前記割り込み指示部での割り込み要求を保持する割り込み保持部と、

前記割り込み先のプロセッサからの割り込み処理の完了通知を受けて割り込みを取り消す割り込み取り消し部と、

を備え、

前記共有メモリは、前記割り込み要求元のプロセッサから前記割り込み先のプロセッサに転送するデータを格納する通信領域と、

前記通信領域の排他制御を行う排他制御領域と、

を備えている、ことを特徴とする請求項6記載の情報処理装置。

[14] 前記アクセス制御手段は、アクセス許可データを記憶する手段と、

前記第2類プロセッサからの前記メモリ及び／又は前記入出力装置へのアクセスを監視し、前記アクセス許可データを参照して、前記アクセスの許可の有無を判別するアクセス許可手段と、

を備えている、ことを特徴とする請求項6記載の情報処理装置。

[15] 前記アクセス許可データを記憶する手段は、前記第2類プロセッサに関して、アクセスを許可するプロセッサに対応させて、アクセスが許可されるアドレス範囲と、前記アドレス範囲に対して許可されたアクセス種別に関する情報を格納している、ことを特徴とする請求項14記載の情報処理装置。

[16] 前記アクセス許可データを記憶する手段は、前記第2類プロセッサに関して、アクセスを不許可とするプロセッサに対応させて、アクセスが不許可されるアドレス範囲と、前記アドレス範囲に対して不許可とされるアクセス種別に関する情報を格納している、ことを特徴とする請求項14記載の情報処理装置。

[17] 前記第1類プロセッサによる前記アクセス許可データの書き込み及び読み出しは可とされ、

前記アクセス許可手段からは、前記アクセス許可データの読み出しのみが可とされ

、

前記第2類プロセッサによる前記アクセス許可データの読み出し及び書き込みは不可とされる、ことを特徴とする請求項14記載の情報処理装置。

[18] 前記アクセス制御手段が、前記第2類プロセッサのアクセスアドレスに関する情報とアクセス許可に関する情報とを対応して格納するキャッシュメモリを備えている、ことを特徴とする請求項14記載の情報処理装置。

[19] 前記アクセス制御手段は、アクセス許可データの更新を行うアクセス許可データ更新手段を有することを特徴とする請求項14に記載の情報処理装置。

[20] 予め定められた第3類の処理を実行する、少なくとも1つのプロセッサ(「第3類プロセッサ」という)と、

前記第2類及び第3類プロセッサ間で通信を行うプロセッサ間通信手段と、

前記第3類プロセッサによる前記第1類プロセッサに接続するメモリ及び／又は入出力情報処理装置へのアクセスを、前記第3の類の処理の信頼度に応じて制限する第2のアクセス制御手段と、

をさらに備えている、ことを特徴とする請求項6記載の情報処理装置。

[21] 予め定められた第3類の処理を実行する、少なくとも1つのプロセッサ(「第3類プロセッサ」という)と、

前記第2類及び第3類プロセッサ間で通信を行うプロセッサ間通信手段と、

を備え、

前記第1類乃至第3類プロセッサの各々は、それぞれバスを介して、接続されるメモリ及び入出力装置を備え、

前記第2類プロセッサによる前記第1類プロセッサに接続する前記メモリ及び／又は前記入出力装置へのアクセスは、前記アクセス制御手段により前記第2の類の処理の信頼度に応じて制限され、

前記第3類プロセッサによる前記第1類プロセッサに接続するメモリ及び／又は入出力情報処理装置へのアクセス、及び／又は、前記第2類プロセッサに接続する前記メモリ及び／又は前記入出力装置へのアクセスは、第2のアクセス制御手段により前記第3の類の処理の信頼度に応じて制限されることを特徴とする請求項6記載の

情報処理装置。

[22] 前記第3類プロセッサは、前記第2類プロセッサが実行する前記第2の類の処理よりも信頼度の低い処理を少なくとも1以上実行する、ことを特徴とする請求項20又は21に記載の情報処理装置。

[23] 請求項6に記載の情報処理装置を複数備える情報処理装置であって、前記情報処理装置のそれぞれが異なるチップ内に構成されていることを特徴とする情報処理装置。

[24] 請求項23に記載の情報処理装置であって、前記チップ間に構成され、メモリ/入出力装置へのアクセス許可を前記チップに構成された前記情報処理装置に属する処理の信頼度に応じて制限するアクセス制限手段を有することを特徴とする情報処理システム。

[25] 基本ソフトウエア環境と、

外部デバイス、及び／又はファイルシステムと、

オペレーティングシステムと、

を備え、

ダウンロードされたデータのセキュリティ情報を格納するセキュリティポリシーデータベースと、

ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、

を備えた基本ドメインと、

ネイティブコードのダウンロードプログラムの実行を制御するネイティブコードダウンロード実行手段と、

オペレーティングシステムと、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたアプリケーション・プログラム(「信頼アプリケーション・プログラム」という)を実行し、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたデバイスドライバ(「信頼ドライバ」という)を前記オペレーテ

ィングシステムにインストールし、前記信頼ドライバにより予め用意された許可された外部デバイスにアクセスし、信頼できる追加処理を実行する信頼拡張ドメインと、

を備え、

前記基本ドメインは前記第1類プロセッサに実装され、

前記信頼拡張ドメインは前記第2類プロセッサに実装される、ことを特徴とする請求項6記載の情報処理装置。

[26] 基本ソフトウエア環境と、

外部デバイス、及び／又はファイルシステムと、

オペレーティングシステムと、

を備え、

ダウンロードされたデータのセキュリティ情報を格納するセキュリティポリシーデータベースと、

ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、

を備えた基本ドメインと、

ネイティブコードのダウンロードプログラムの実行を制御するネイティブコードダウンロード実行手段と、

オペレーティングシステムと、

を備え、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたアプリケーション・プログラム(「信頼アプリケーション・プログラム」という)を実行し、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたデバイスドライバ(「信頼ドライバ」という)を前記オペレーティングシステムにインストールし、前記信頼ドライバにより、予め用意された許可された外部デバイスにアクセスし、信頼できる追加処理を実行する信頼拡張ドメインと、

ネイティブコードのダウンロードプログラムの実行を制御するネイティブコードダウンロード実行手段と、

オペレーティングシステムと、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できないと判定された、ダウンロードされたアプリケーション・プログラム(「無信頼アプリケーション・プログラム」という)を実行し、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できないと判定された、ダウンロードされたデバイスドライバ(「無信頼ドライバ」という)を前記オペレーティングシステムにインストールし、前記デバイスドライバにより予め用意された許可された外部デバイスにアクセスし、無信頼の追加処理を実行する無信頼拡張ドメインと、

を備え、

前記基本ドメインは前記第1類プロセッサに実装され、

前記信頼拡張ドメインは前記第2類プロセッサに実装され、

前記無信頼拡張ドメインは前記第3類プロセッサに実装される、ことを特徴とする請求項20又は21記載の情報処理装置。

[27] 前記基本ドメインの外部デバイスからダウンロードデータが入力されると、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードデータの証明書をチェックし、チェックの結果、正しい証明書であると判定した場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に、前記ダウンロードデータを送信し、

一方、前記チェックの結果、証明書がないか、あるいは証明書の内容が正しくない場合には、前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に、前記ダウンロードデータを送信する、ことを特徴とする請求項26記載の情報処理装置。

[28] 前記基本ドメインの外部デバイスからダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードアプリケーション・プログラムと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードアプリケーション・プログラムの証明書をチェックし、チェックの結果、正しい証明書と判定した場合、前記ダウンロードアプリケーション・プログラムを、前記信頼拡

張ドメインの前記ネイティブコードダウンロード実行手段に送信する、ことを特徴とする請求項25又は26記載の情報処理装置。

[29] 前記基本ドメインの外部デバイスからダウンロードデータが入力される、前記基本機能が、前記ダウンロードデータをダウンロードドライバと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードドライバの証明書をチェックし、チェックの結果、正しい証明書と判定した場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に前記ダウンロードドライバを送信し、

前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段は、前記ダウンロードドライバを、前記信頼拡張ドメインのオペレーティングシステムにインストールする、ことを特徴とする請求項25又は26記載の情報処理装置。

[30] 前記基本ドメインの外部デバイスからダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードアプリケーション・プログラムと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードアプリケーション・プログラムの証明書をチェックし、チェックの結果、証明書がないか、証明書の内容が正しくない場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段を介して、前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に、前記アプリケーション・プログラムを送信する、ことを特徴とする請求項26記載の情報処理装置。

[31] 前記基本ドメインの外部デバイスから、ダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードドライバと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードドライバの証明書をチェックし、チェックの結果、証明書がないか、証明書の内容が正しくない場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段を介して、前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に、前記ダウンロードドライバを送信し、

前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段は、前記ダウンロードドライバを、前記無信頼拡張ドメインのオペレーティングシステムにインストー

ルする、ことを特徴とする請求項26記載の情報処理装置。

[32] 前記信頼拡張ドメインが、前記基本ドメインの基本ソフトウェア環境の基本機能への要求を発行する処理群をライブラリとして含む基本機能ライブラリを備え、

前記信頼拡張ドメインにダウンロードされたアプリケーション・プログラムからの要求を受けて、前記信頼拡張ドメインの前記基本機能ライブラリは、前記基本ドメインの前記ネイティブコードダウンロード管理手段に要求を送信し、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインより受信した要求が適正であるか確認し、要求が正しい場合、前記基本ソフトウェア環境の基本機能へ処理を依頼する、ことを特徴とする請求項25又は26記載の情報処理装置。

[33] 前記基本ドメインの前記基本機能は、要求を処理し、処理の完了を前記基本ドメインの前記ネイティブコードダウンロード管理手段に通知し、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインの基本機能ライブラリに完了を通知し、前記基本機能ライブラリから前記アプリケーション・プログラムに処理の完了が通知される、ことを特徴とする請求項32記載の情報通信情報処理装置。

[34] 前記信頼拡張ドメインが、前記基本ドメインの基本ソフトウェア環境の基本機能への要求を発行する処理群をライブラリとして含む基本機能ライブラリを備え、

前記無信頼拡張ドメインにダウンロードされたアプリケーション・プログラムから、前記信頼拡張ドメインのアプリケーション・プログラムにデータを送信し、

前記信頼拡張ドメインの前記アプリケーション・プログラムは、前記基本機能ライブラリに対して、前記無信頼拡張ドメインのダウンロードアプリケーション・プログラムからのデータを含む要求を発行し、

前記基本機能ライブラリは、前記信頼拡張ドメインの前記アプリケーション・プログラムからの要求を受けて、前記基本ドメインの前記ネイティブコードダウンロード管理手段に対して要求を送信し、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、受信した要求が適正であるか確認し、前記要求が適正な場合、ユーザに確認を求め、前記ユーザの

確認結果が可の場合、前記基本ソフトウェア環境の基本機能へ処理を依頼し、

一方、前記ユーザの確認結果が不許可の場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記基本機能ライブラリに、不許可を通知する、ことを特徴とする請求項26記載の情報処理装置。

[35] 前記基本機能は、要求を処理し、処理の完了を前記基本ドメインの前記ネイティブコードダウンロード管理手段に通知し、前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインの基本機能ライブラリに完了を通知し、前記基本機能ライブラリから前記ダウンロードアプリケーション・プログラムに処理の完了が通知され、前記ダウンロードアプリケーション・プログラムは、前記無信頼拡張ドメインの前記ダウンロードアプリケーション・プログラムに処理の完了を通知する、ことを特徴とする請求項34記載の情報処理装置。

[36] 前記基本ドメイン及び前記信頼拡張ドメインが、仮想デバイスを、実ハードウエアデバイスにマッピングする仮想マシンモニタを備え、ファイルシステム、デバイス、CPUが仮想化されている、ことを特徴とする請求項25記載の情報処理装置。

[37] 前記基本ドメイン、前記信頼拡張ドメイン、前記無信頼拡張ドメインが、仮想デバイスを、実ハードウエアデバイスにマッピングする仮想マシンモニタを備え、ファイルシステム、デバイス、CPUが仮想化されている、ことを特徴とする請求項26記載の情報通信情報処理装置。

[38] 前記基本ドメインの仮想マシンモニタが、前記信頼拡張ドメイン又は前記無信頼拡張ドメインの仮想マシンモニタに、CPU資源の委譲を要求し、

前記信頼拡張ドメイン又は前記無信頼拡張ドメインの仮想マシンモニタは、前記基本ドメインの仮想マシンモニタに委譲できるCPUを通知し、

前記基本ドメインの仮想マシンモニタは、前記基本ドメインの仮想CPUの資源を増やす、ことを特徴とする請求項36又は37記載の情報処理装置。

[39] 前記ドメインのプロセッサのそれぞれの群において、分離手段を介して、複数に分離可能とされている、ことを特徴とする請求項25又は26記載の情報処理装置。

[40] 前記基本ドメインのプロセッサが、他のドメインのプロセッサを管理する、ことを特徴とする請求項25又は26記載の情報処理装置。

[41] 実行するプログラムの信頼度に応じて複数のドメインに分けられ、異なるドメインに属するプロセッサ同士が、データ又はコマンドを、プロセッサ間通信手段を介して相互に送信する工程と、

一定の信頼度より低いプログラムを少なくとも1以上実行するドメインに属するプロセッサによる前記一定の信頼度以上のプログラムを実行するドメインに属するメモリ及び／又は入出力装置へのアクセスを、一定の信頼度より低いプログラムを少なくとも1以上実行するドメインの信頼度に従って制限する工程と、を含むことを特徴とするプログラム実行制御方法。

[42] 基本ソフトウエア環境と、

外部デバイス、及び／又はファイルシステムと、

オペレーティングシステムと、

を備え、

ダウンロードされたデータのセキュリティ情報を格納するセキュリティポリシーデータベースと、

ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、

を備えた基本ドメインと、

ネイティブコードのダウンロードプログラムの実行を制御するネイティブコードダウンロード実行手段と、

オペレーティングシステムと、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたアプリケーション・プログラム（「信頼アプリケーション・プログラム」という）を実行し、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたデバイスドライバ（「信頼ドライバ」という）を前記オペレーティングシステムにインストールし、前記信頼ドライバにより予め用意された許可された外部デバイスにアクセスし、信頼できる追加処理を実行する信頼拡張ドメインと、

を有する情報処理システムによるプログラム実行環境制御方法であって、

基本ドメインと信頼拡張ドメイン間のプロセッサ同士は、プロセッサ間通信手段を介して、相互に通信する工程と、

前記信頼拡張ドメインに属するプロセッサによる前記基本ドメインのメモリ及び／又は入出力装置へのアクセスを、アクセス制御手段によって、制限する工程と、

を含む、ことを特徴とするプログラム実行環境制御方法。

[43] 基本ソフトウエア環境と、

外部デバイス、及び／又はファイルシステムと、

オペレーティングシステムと、

を備え、

ダウンロードされたデータのセキュリティ情報を格納するセキュリティポリシーデータベースと、

ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、

を備えた基本ドメインと、

ネイティブコードのダウンロードプログラムの実行を制御するネイティブコードダウンロード実行手段と、

オペレーティングシステムと、

を備え、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたアプリケーション・プログラム（「信頼アプリケーション・プログラム」という）を実行し、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できると判定された、ダウンロードされたデバイスドライバ（「信頼ドライバ」という）を前記オペレーティングシステムにインストールし、前記信頼ドライバにより、予め用意された許可された外部デバイスにアクセスし、信頼できる追加処理を実行する信頼拡張ドメインと、

ネイティブコードのダウンロードプログラムの実行を制御するネイティブコードダウンロード実行手段と、

オペレーティングシステムと、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できないと判定された、ダウンロードされたアプリケーション・プログラム(「無信頼アプリケーション・プログラム」という)を実行し、

前記基本ドメインのネイティブコードダウンロード管理手段により、信頼できないと判定された、ダウンロードされたデバイスドライバ(「無信頼ドライバ」という)を前記オペレーティングシステムにインストールし、前記デバイスドライバにより予め用意された許可された外部デバイスにアクセスし、無信頼の追加処理を実行する無信頼拡張ドメインと、

を有する情報処理システムによるプログラム実行環境制御方法であって、

前記基本ドメインと、前記信頼拡張ドメインと、無信頼拡張ドメインの各ドメイン間のプロセッサ同士は、プロセッサ間通信手段を介して、相互に通信する工程と、

前記信頼拡張ドメインに属するプロセッサによる前記基本ドメインのメモリ及び／又は入出力装置へのアクセスを、第1のアクセス制御手段によって、制限する工程と、

前記無信頼拡張ドメインに属するプロセッサによる前記基本ドメインのメモリ及び／又は入出力装置へのアクセスを、第2のアクセス制御手段によって、制限する工程と、

を含む、ことを特徴とするプログラム実行環境制御方法。

[44] 前記基本ドメインの外部デバイスからダウンロードデータが入力されると、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードデータの証明書をチェックする工程と、

チェックの結果、正しい証明書であると判定した場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段にダウンロードデータを送信する工程と、

を含む、ことを特徴とする請求項42記載のプログラム実行環境制御方法。

[45] 前記基本ドメインの外部デバイスからダウンロードデータが入力されると、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードデータの証明書をチェックする工程と、

前記チェックの結果、正しい証明書であると判定した場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に前記ダウンロードデータを送信する工

程と、

前記チェックの結果、証明書がないか、あるいは証明書の内容が正しくない場合には、前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に、前記ダウンロードデータを送信する工程と、

を含む、ことを特徴とする請求項42記載のプログラム実行環境制御方法。

[46] 前記基本ドメインの外部デバイスからダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードアプリケーション・プログラムと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードアプリケーション・プログラムの証明書をチェックする工程と、

前記チェックの結果、正しい証明書と判定した場合、前記ダウンロードアプリケーション・プログラムを、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に前記ダウンロードアプリケーション・プログラムを送信する工程と、

を含む、ことを特徴とする請求項42又は43記載のプログラム実行環境制御方法。

[47] 前記基本ドメインの外部デバイスからダウンロードデータが入力される、前記基本機能が、前記ダウンロードデータをダウンロードドライバと認識した場合、前記ネイティブコードダウンロード管理手段が、ダウンロードドライバの証明書をチェックする工程と、

前記チェックの結果、正しい証明書と判定した場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段にダウンロードドライバを送信する工程と、

前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段は、前記ダウンロードドライバを、前記信頼拡張ドメインのオペレーティングシステムにインストールする工程と、

を含む、ことを特徴とする請求項42又は43記載のプログラム実行環境制御方法。

[48] 前記基本ドメインの外部デバイスからダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードアプリケーション・プログラムと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、ダウンロードアプリケーション・プログラムの証明書をチェックする工程と、

前記チェックの結果、証明書がないか、証明書の内容が正しくない場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段を介して、前記無信頼拡張

ドメインの前記ネイティブコードダウンロード実行手段に、前記ダウンロードアプリケーション・プログラムを送信する工程と、

を含む、ことを特徴とする請求項43記載のプログラム実行環境制御方法。

[49] 前記基本ドメインの外部デバイスから、ダウンロードデータが入力され、前記基本機能が、前記ダウンロードデータをダウンロードドライバと認識した場合、前記基本ドメインの前記ネイティブコードダウンロード管理手段が、前記ダウンロードドライバの証明書をチェックする工程と、

前記チェックの結果、証明書がないか、証明書の内容が正しくない場合、前記信頼拡張ドメインの前記ネイティブコードダウンロード実行手段を介して、前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段に、前記ダウンロードドライバを送信する工程と、

前記無信頼拡張ドメインの前記ネイティブコードダウンロード実行手段は、前記ダウンロードドライバを、前記無信頼拡張ドメインのオペレーティングシステムにインストールする工程と、

を含む、ことを特徴とする請求項43記載のプログラム実行環境制御方法。

[50] 前記信頼拡張ドメインに、前記基本ドメインの基本ソフトウェア環境の基本機能への要求を発行する処理群を、ライブラリとして含む基本機能ライブラリを設けておき、

前記信頼拡張ドメインにダウンロードされたアプリケーション・プログラムからの要求を受けて、前記基本機能ライブラリは、前記基本ドメインの前記ネイティブコードダウンロード管理手段に対して要求を送信する工程と、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインより受信した要求が適正であるか確認し、前記要求が適正である場合、前記基本ソフトウェア環境の基本機能へ処理を依頼する工程と、

を含む、ことを特徴とする請求項42又は43記載のプログラム実行環境制御方法。

[51] 前記基本ドメインの前記基本機能は、要求を処理し、処理の完了を前記基本ドメインの前記ネイティブコードダウンロード管理手段に通知する工程と、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインの基本機能ライブラリに完了を通知し、前記基本機能ライブラリから前記アプリ

ケーション・プログラムに処理の完了が通知される工程と、

を含む、ことを特徴とする請求項50記載のプログラム実行環境制御方法。

[52] 前記信頼拡張ドメインに、前記基本ドメインの基本ソフトウェア環境の基本機能への要求を発行する処理群を、ライブラリとして含む基本機能ライブラリを設けておき、

前記無信頼拡張ドメインにダウンロードされたアプリケーション・プログラムから、前記信頼拡張ドメインのアプリケーション・プログラムにデータを送信する工程と、

前記信頼拡張ドメインの前記アプリケーション・プログラムは、前記基本機能ライブラリに対して、前記無信頼拡張ドメインのダウンロードアプリケーション・プログラムからのデータを含む要求を発行する工程と、

前記信頼拡張ドメインの前記アプリケーション・プログラムからの前記要求を受け、前記基本機能ライブラリは、前記基本ドメインの前記ネイティブコードダウンロード管理手段に要求を送信する工程と、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、受信した要求が適正であるか確認する工程と、

前記確認の結果、前記要求が適正である場合、ユーザに確認を求め、前記ユーザの確認結果が可の場合、前記基本ソフトウェア環境の基本機能へ処理を依頼する工程と、

一方、前記ユーザの確認結果が不許可の場合、前記ネイティブコードダウンロード管理手段は、前記基本機能ライブラリに、不許可を通知する工程と、

を含む、ことを特徴とする請求項43記載のプログラム実行環境制御方法。

[53] 基本機能は、要求を処理し、処理の完了を前記基本ドメインの前記ネイティブコードダウンロード管理手段に通知する工程と、

前記基本ドメインの前記ネイティブコードダウンロード管理手段は、前記信頼拡張ドメインの基本機能ライブラリに完了を通知する工程と、

前記基本機能ライブラリから前記ダウンロードアプリケーション・プログラムに処理の完了が通知される工程と、

前記ダウンロードアプリケーション・プログラムは、前記無信頼拡張ドメインの前記ダウンロードアプリケーション・プログラムに処理の完了を通知する工程と、

を含む、ことを特徴とする請求項52記載のプログラム実行環境制御方法。

[54] 前記基本ドメイン及び前記信頼拡張ドメインが、仮想デバイスを、実ハードウエアデバイスにマッピングする仮想マシンモニタにより、ファイルシステム、デバイス、CPUが仮想化されている、ことを特徴とする請求項42記載のプログラム実行環境制御方法。

[55] 前記基本ドメイン、前記信頼拡張ドメイン、前記無信頼拡張ドメインが、仮想デバイスを、実ハードウエアデバイスにマッピングする仮想マシンモニタを備え、ファイルシステム、デバイス、CPUが仮想化されている、ことを特徴とする請求項43記載のプログラム実行環境制御方法。

[56] 前記基本ドメインの仮想マシンモニタが、前記信頼拡張ドメインの仮想マシンモニタに、CPU資源の委譲を要求する工程と、

前記信頼拡張ドメインの仮想マシンモニタは、前記基本ドメインの仮想マシンモニタに委譲できるCPUを通知する工程と、

を含み、

前記基本ドメインの仮想マシンモニタは、前記基本ドメインの仮想CPUの資源を増やす、ことを特徴とする請求項54又は55記載のプログラム実行環境制御方法。

[57] 前記基本ドメインの仮想マシンモニタが、前記信頼拡張ドメイン及び／又は前記無信頼拡張ドメインの仮想マシンモニタに、CPU資源の委譲を要求する工程と、

前記信頼拡張ドメイン及び／又は前記無信頼拡張ドメインの仮想マシンモニタは、前記基本ドメインの仮想マシンモニタに委譲できるCPUを通知する工程と、

を含み、

前記基本ドメインの仮想マシンモニタは、前記基本ドメインの仮想CPUの資源を増やす、ことを特徴とする請求項55記載のプログラム実行環境制御方法。

[58] 基本ソフトウエア環境と、

外部デバイス、及び／又はファイルシステムと、

オペレーティングシステムと、

を備え、

ダウンロードされたデータのセキュリティ情報を格納するセキュリティポリシーデータベースと、

ネイティブコードのダウンロードデータのダウンロードを制御するネイティブコードダウンロード管理手段と、

を備え、

前記ネイティブコードダウンロード管理手段は、ダウンロードされたプログラムの証明書に基づき、前記ダウンロードされたプログラムの信頼度を判別し、前記判別結果に基づき、実行するプログラムの信頼度により定められた1又は複数のドメインへの要求の可否、又は要求内容を判断する、ことを特徴とするプログラム実行環境制御情報処理装置。

[59] 複数のプロセッサを備え、

前記複数のプロセッサは、第1のドメインを構成するプロセッサと、前記第1のドメインとは異なる第2のドメインを構成するプロセッサと、を含み、

前記第2のドメインは、前記第1のドメインに属するプロセッサが実行する処理よりも信頼度の低い処理を、少なくとも1以上有するプロセッサを含み、

前記第1のドメインと前記第2のドメインのプロセッサ同士の通信を制御するプロセッサ間通信手段と、

前記第2のドメインに属するプロセッサによる前記第1のドメインに属するメモリ及び／又は入出力装置へのアクセスを、前記第2のドメインで実行される処理の信頼度に応じて制限するアクセス制御手段と、

を備えている、ことを特徴とする携帯情報端末。

[60] 複数のプロセッサを備え、

実行する処理の信頼度に応じて、前記複数のプロセッサが、複数のドメインを構成し、

異なるドメイン間のプロセッサ同士は、プロセッサ間通信手段を介して、相互に通信し、

セキュリティの相対的に低い処理を実行するドメインに属するプロセッサによるセキュリティの相対的に高い処理を実行するドメインに属するメモリ及び／又は入出力装置へのアクセスを制御するアクセス制御手段を備えている、ことを特徴とする情報通信装置。

[61] 予め定められた第1の類の処理を実行する、少なくとも1つのプロセッサ(「第1類プロセッサ」という)と、

前記第1の類の処理と異なる予め定められた第2の類の処理を実行する、少なくとも1つのプロセッサ(「第2類プロセッサ」という)と、

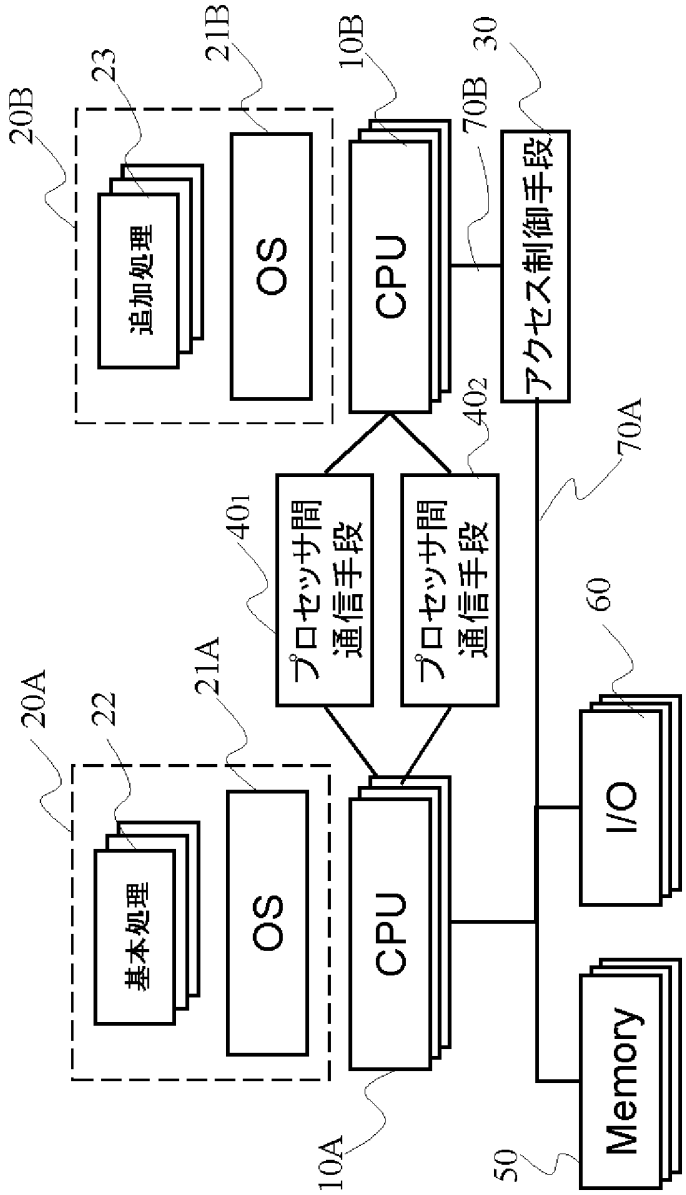
メモリ及び入出力装置と、

前記第1類及び第2類プロセッサ間の通信を制御するプロセッサ間通信手段と、

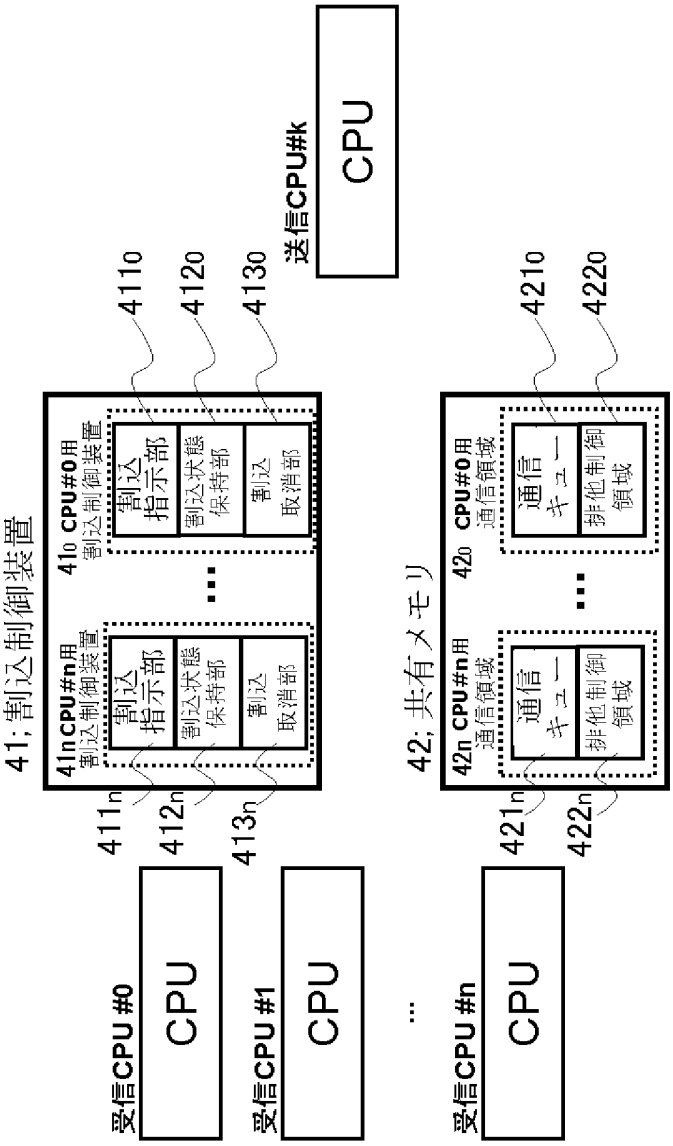
前記第2類プロセッサによる前記メモリ及び／又は前記入出力装置へのアクセスを制御するアクセス制御手段と、

を備えている、ことを特徴とする情報通信装置。

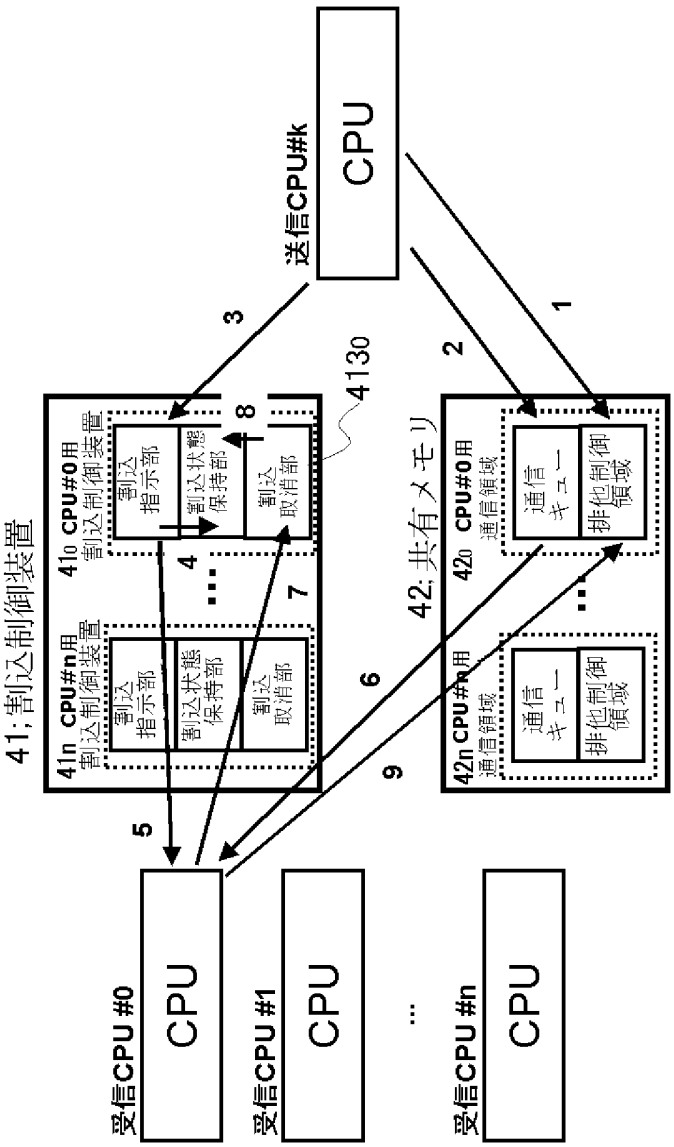
[図1]


20B
23
21B
10B
30
70B
追加処理
OS
CPU
アクセス制御手段
401
402
70A
プロセッサ間通信手段
プロセッサ間通信手段
60
20A
22
21A
基本処理
OS
CPU
I/O
10A
50
Memory

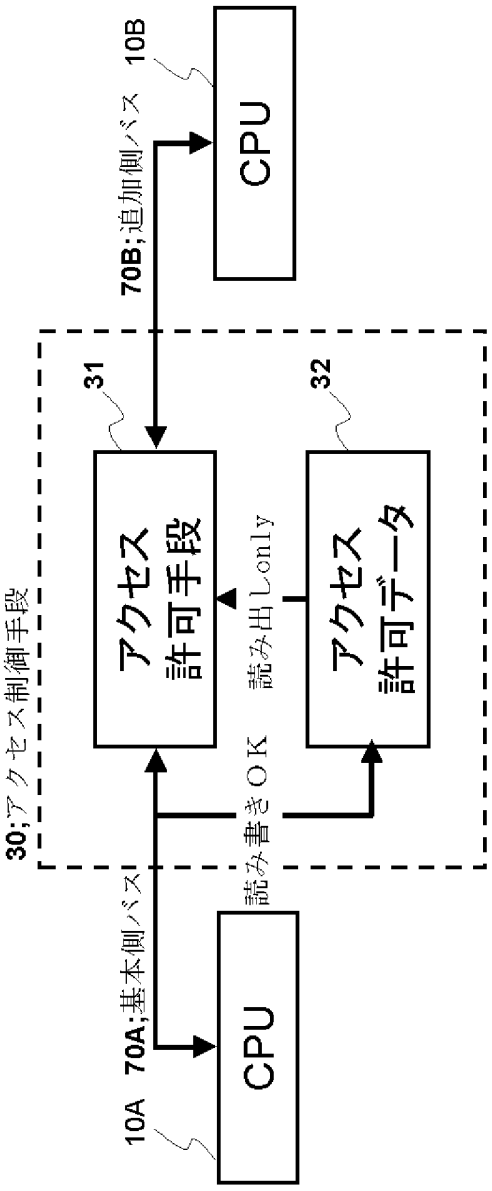
[図2]


41; 割込制御装置
41n CPU#n用 割込制御装置
41₀ CPU#0用 割込制御装置
割込 指示部
割込状態 保持部
割込 取消部
411n
412n
413n
411₀
412₀
413₀
42; 共有メモリ
42n CPU#n用 通信領域
42₀ CPU#0用 通信領域
通信 キュー
排他制御 領域
421n
422n
421₀
422₀
受信CPU #0
受信CPU #1
受信CPU #n
送信CPU#k
CPU

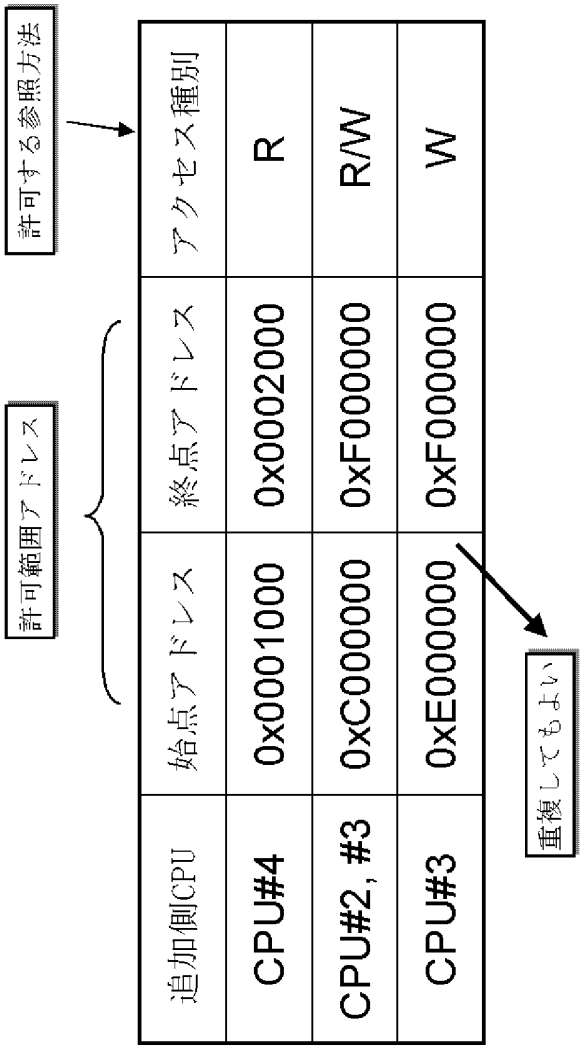
[図3]


41; 割込制御装置
41n CPU#n用 割込制御装置
割込 指示部
割込状態 保持部
割込 取消部
41₀ CPU#0用 割込制御装置
割込 指示部
割込状態 保持部
割込 取消部
4130
42; 共有メモリ
42n CPU#n用 通信領域
通信 キュー
排他制御 領域
42₀ CPU#0用 通信領域
通信 キュー
排他制御 領域
送信CPU#k
CPU
受信CPU #0
CPU
受信CPU #1
CPU
受信CPU #n
CPU
1
2
3
4
5
6
7
8
9

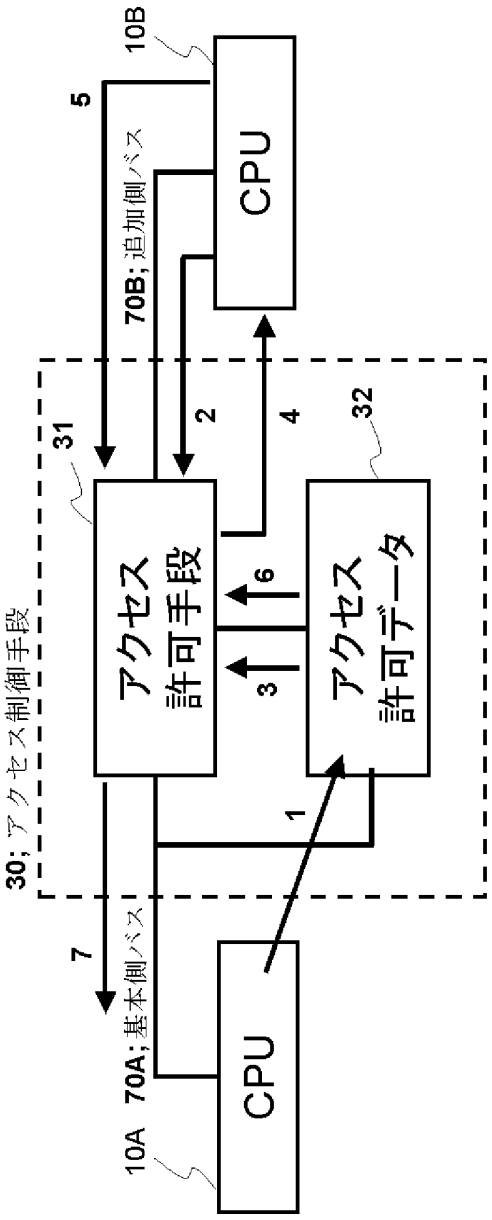
[図4]


10B
CPU
70B;追加側バス
31
32
アクセス
許可手段
読み出しOnly
アクセス
許可データ
30;アクセス制御手段
読み書きOK
70A;基本側バス
10A
CPU

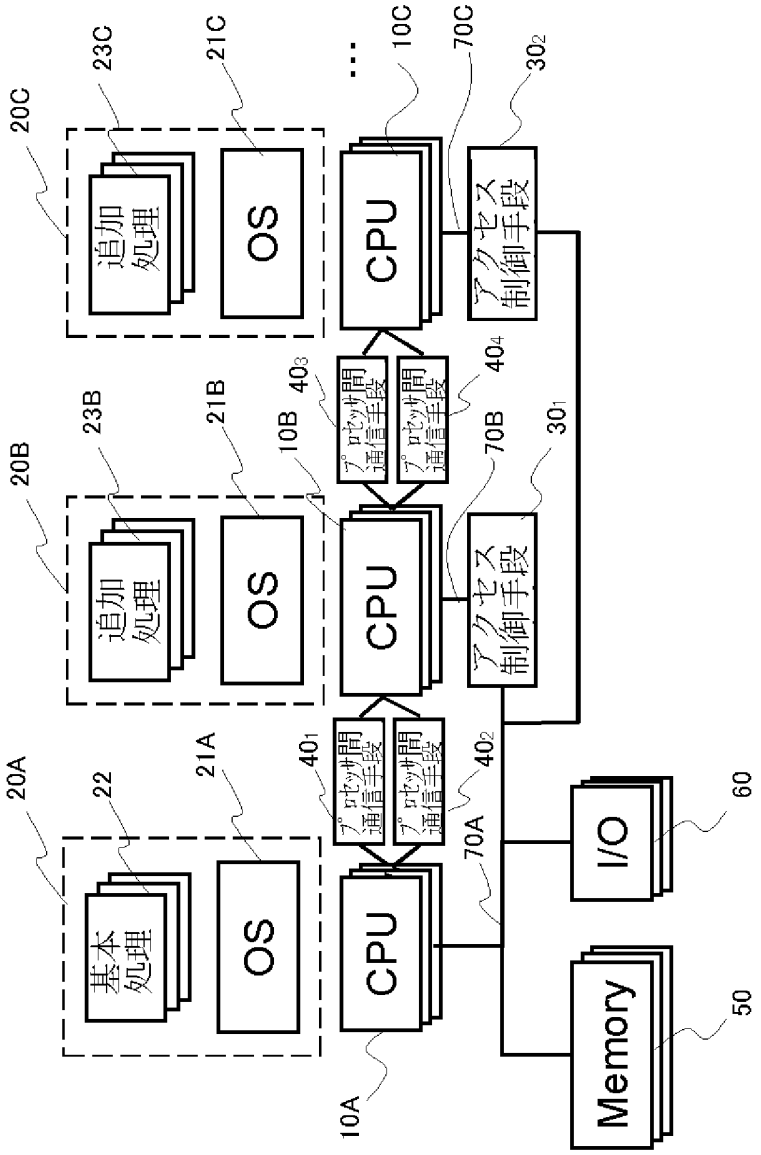
[図5]


許可する参照方法
許可範囲アドレス
追加側CPU
始点アドレス
終点アドレス
アクセス種別
CPU#4
0x0001000
0x0002000
R
CPU#2, #3
0xC000000
0xF000000
R/W
CPU#3
0xE000000
0xF000000
W
重複してもよい

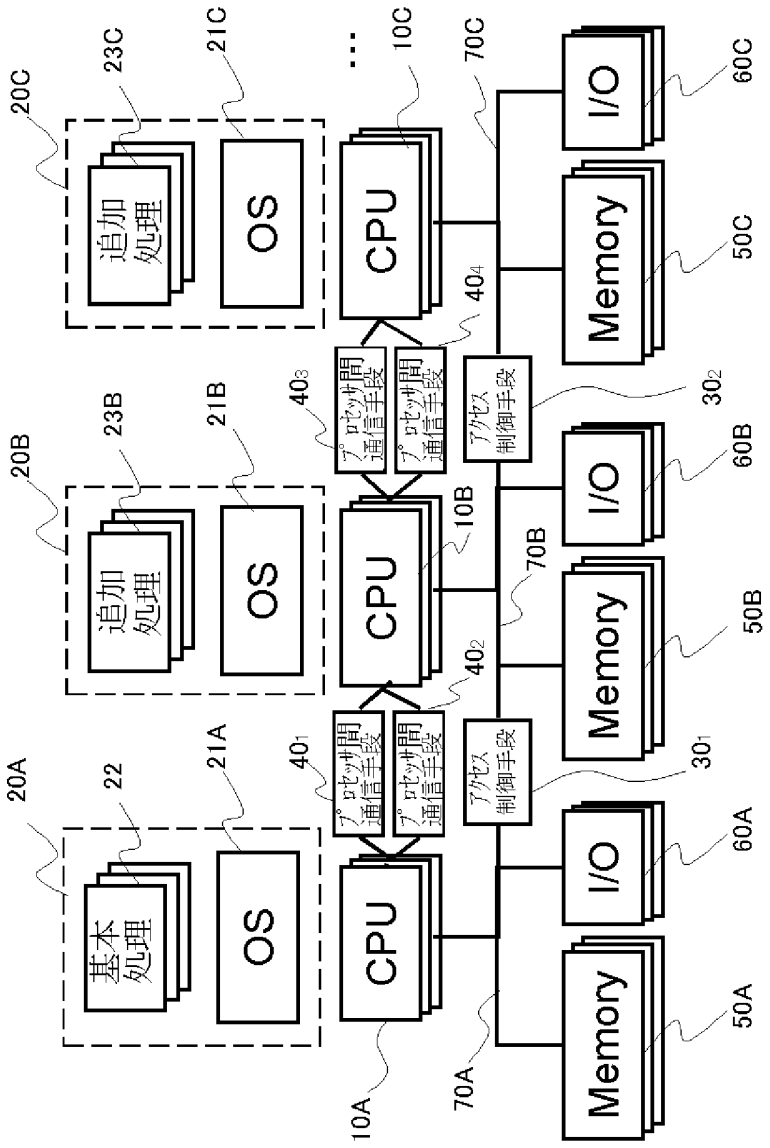
[図6]


10B
CPU
5
70B; 追加側バス
2
4
31
32
30; アクセス制御手段
アクセス
許可手段
6
3
アクセス
許可データ
1
7
70A; 基本側バス
10A
CPU

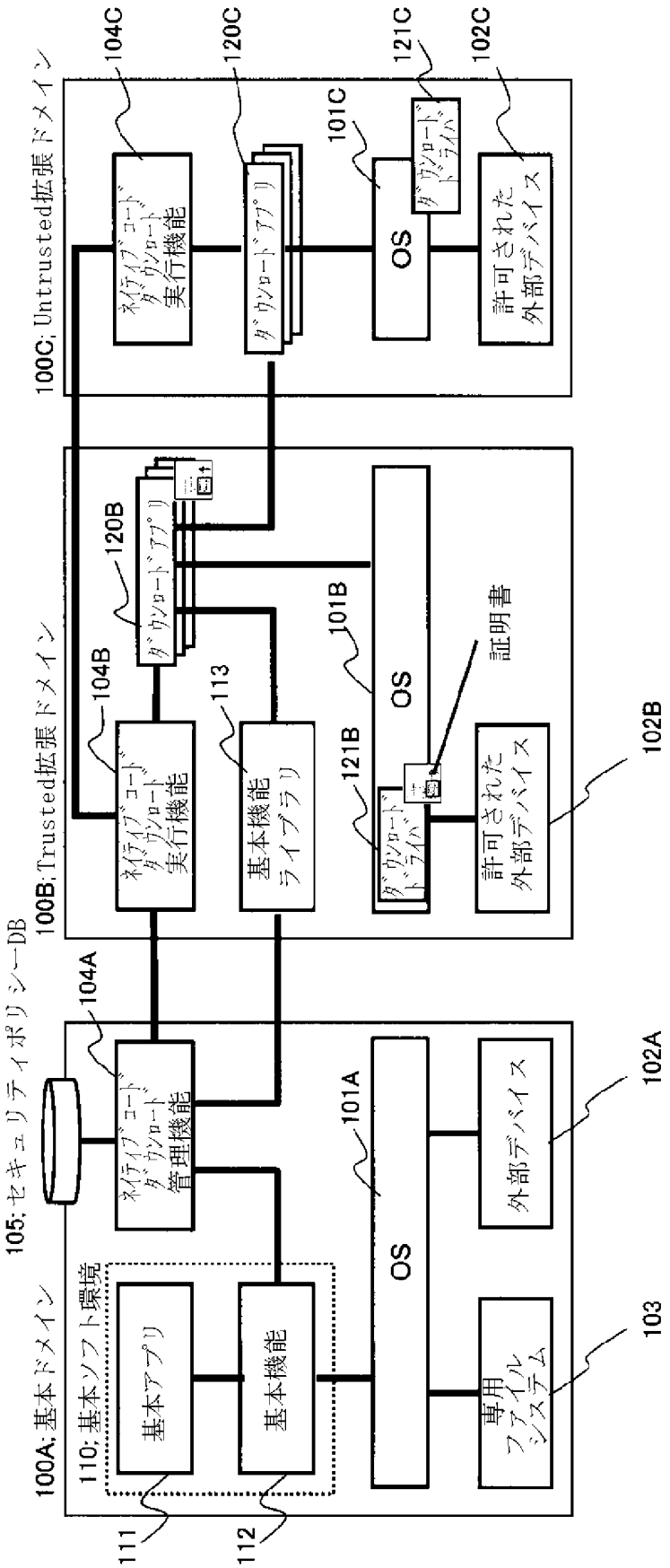
[図7]


20C
23C
21C
追加処理
OS
CPU
10C
70C
30₂
アクセス制御手段
40₃
40₄
20B
23B
21B
10B
追加処理
OS
CPU
70B
30₁
アクセス制御手段
20A
22
21A
40₁
40₂
基本処理
OS
CPU
70A
I/O
60
10A
Memory
50

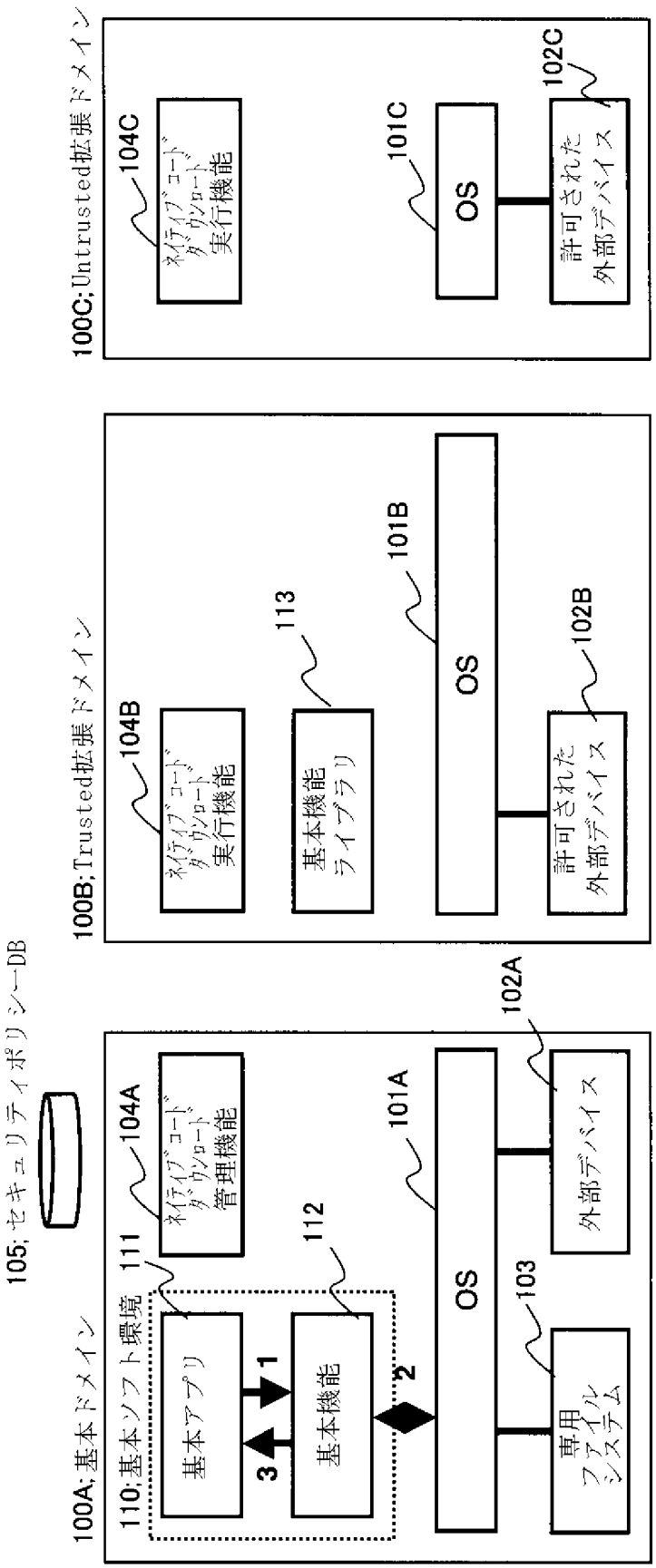
[図8]


20C
23C
21C
追加処理
OS
CPU
10C
70C
I/O
60C
Memory
50C
40₄
プロセッサ間通信手段
40₃
アクセス制御手段
30₂
20B
23B
21B
追加処理
OS
CPU
10B
70B
I/O
60B
Memory
50B
40₂
プロセッサ間通信手段
20A
22
21A
基本処理
OS
CPU
40₁
30₁
I/O
60A
Memory
50A
10A
70A

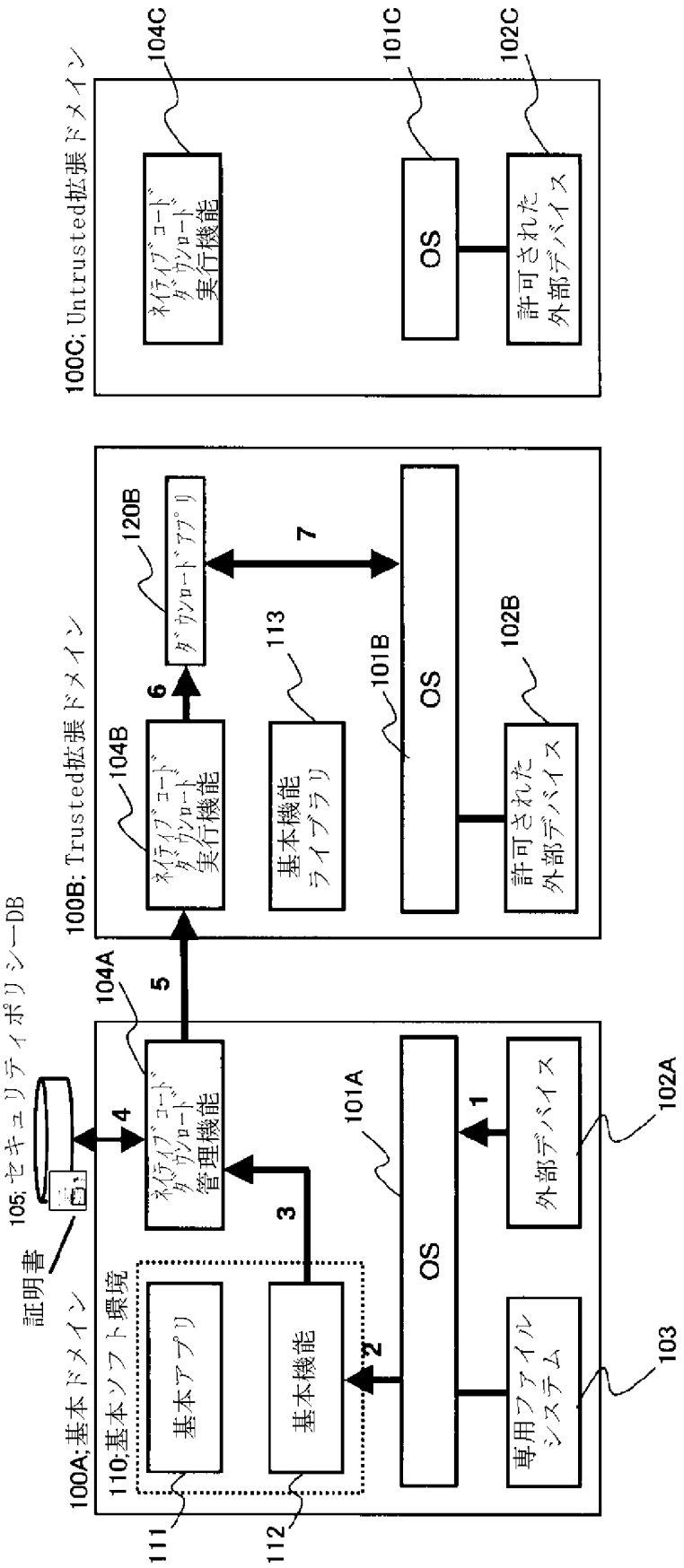
[図9]


100A; 基本ドメイン
110; 基本ソフト環境
基本アプリ
基本機能
111
112
ネイティブコード ダウンロード 管理機能
104A
OS
101A
外部デバイス
102A
専用 ファイル システム
103
105; セキュリティポリシーDB
100B; Trusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104B
ダウンロードアプリ
120B
基本機能 ライブラリ
113
OS
101B
ダウンロード ドライバ
121B
証明書
許可された 外部デバイス
102B
100C; Untrusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104C
ダウンロードアプリ
120C
OS
101C
ダウンロード ドライバ
121C
許可された 外部デバイス
102C

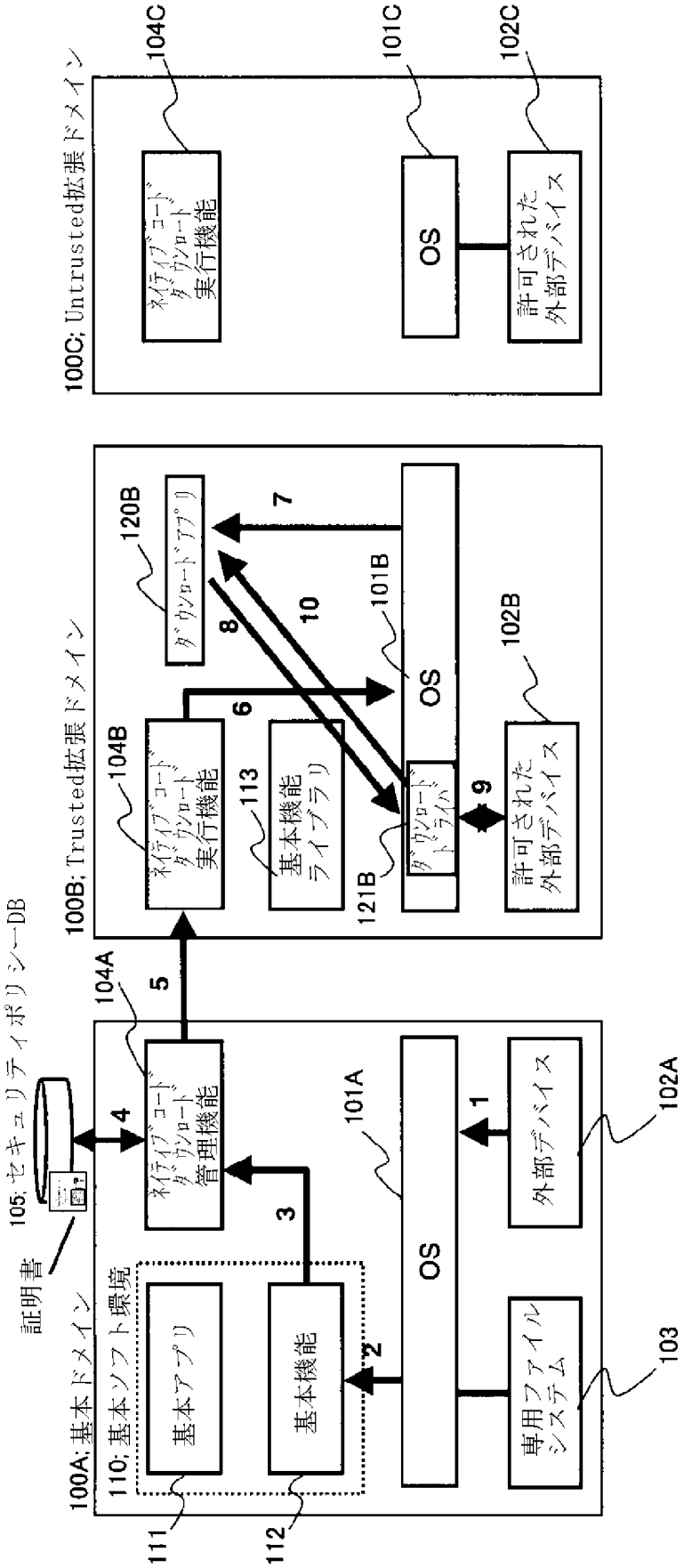
[図10]


105;セキュリティポリシーDB
100A;基本ドメイン
110;基本ソフト環境
111
基本アプリ
1
3
基本機能
112
2
104A
ネイティブコード
ダウンロード
管理機能
101A
OS
103
専用
ファイル
システム
102A
外部デバイス
100B;Trusted拡張ドメイン
104B
ネイティブコード
ダウンロード
実行機能
113
基本機能
ライブラリ
101B
OS
102B
許可された
外部デバイス
100C;Untrusted拡張ドメイン
104C
ネイティブコード
ダウンロード
実行機能
101C
OS
102C
許可された
外部デバイス

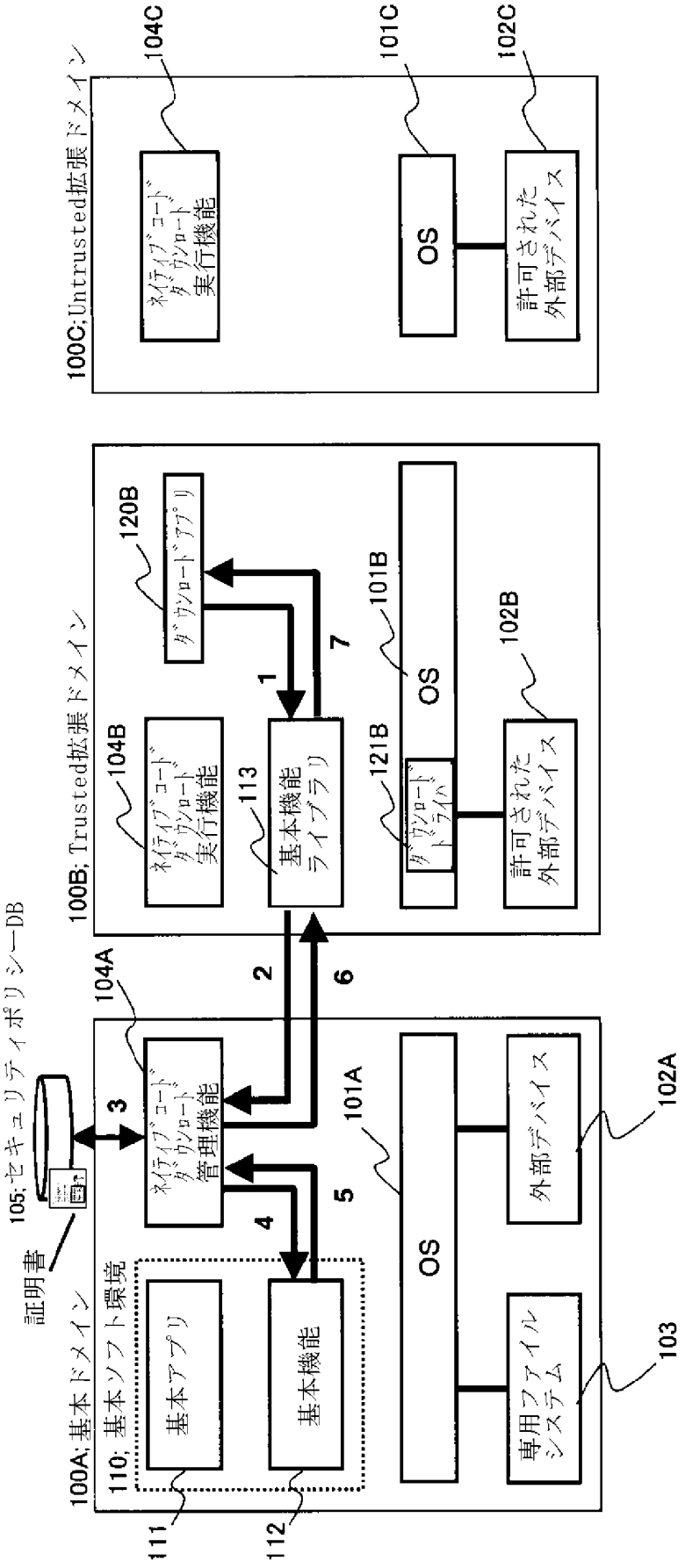
[図11]


100C; Untrusted拡張ドメイン
104C
ネイティブコード ダウンロード 実行機能
101C
OS
102C
許可された 外部デバイス
100B; Trusted拡張ドメイン
120B
ダウンロードアプリ
7
6
104B
ネイティブコード ダウンロード 実行機能
113
基本機能 ライブラリ
101B
OS
102B
許可された 外部デバイス
105; セキュリティポリシーDB
証明書
100A; 基本ドメイン
110; 基本ソフト環境
104A
5
4
ネイティブコード ダウンロード 管理機能
3
基本アプリ
基本機能
2
101A
OS
1
外部デバイス
102A
専用ファイル システム
103
111
112

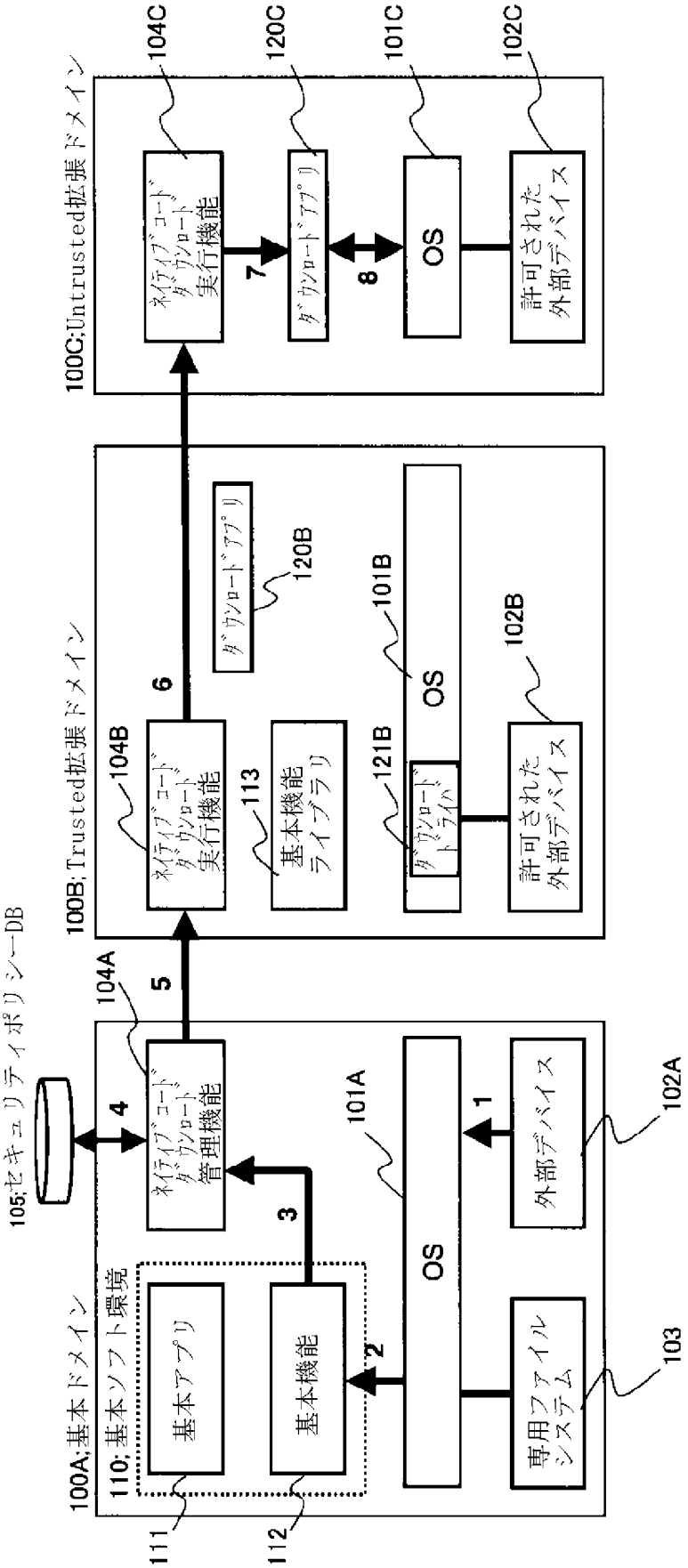
[図12]


100C; Untrusted拡張ドメイン
104C
ネイティブコード ダウンロード 実行機能
101C
OS
102C
許可された 外部デバイス
100B; Trusted拡張ドメイン
120B
ダウンロードアプリ
7
8
10
101B
OS
102B
6
104B
ネイティブコード ダウンロード 実行機能
113
基本機能 ライブラリ
121B
ダウンロード ドライバ
9
許可された 外部デバイス
105; セキュリティポリシーDB
5
104A
4
ネイティブコード ダウンロード 管理機能
3
101A
OS
1
外部デバイス
102A
証明書
100A; 基本ドメイン
110; 基本ソフト環境
基本アプリ
基本機能
2
専用ファイル システム
103
111
112

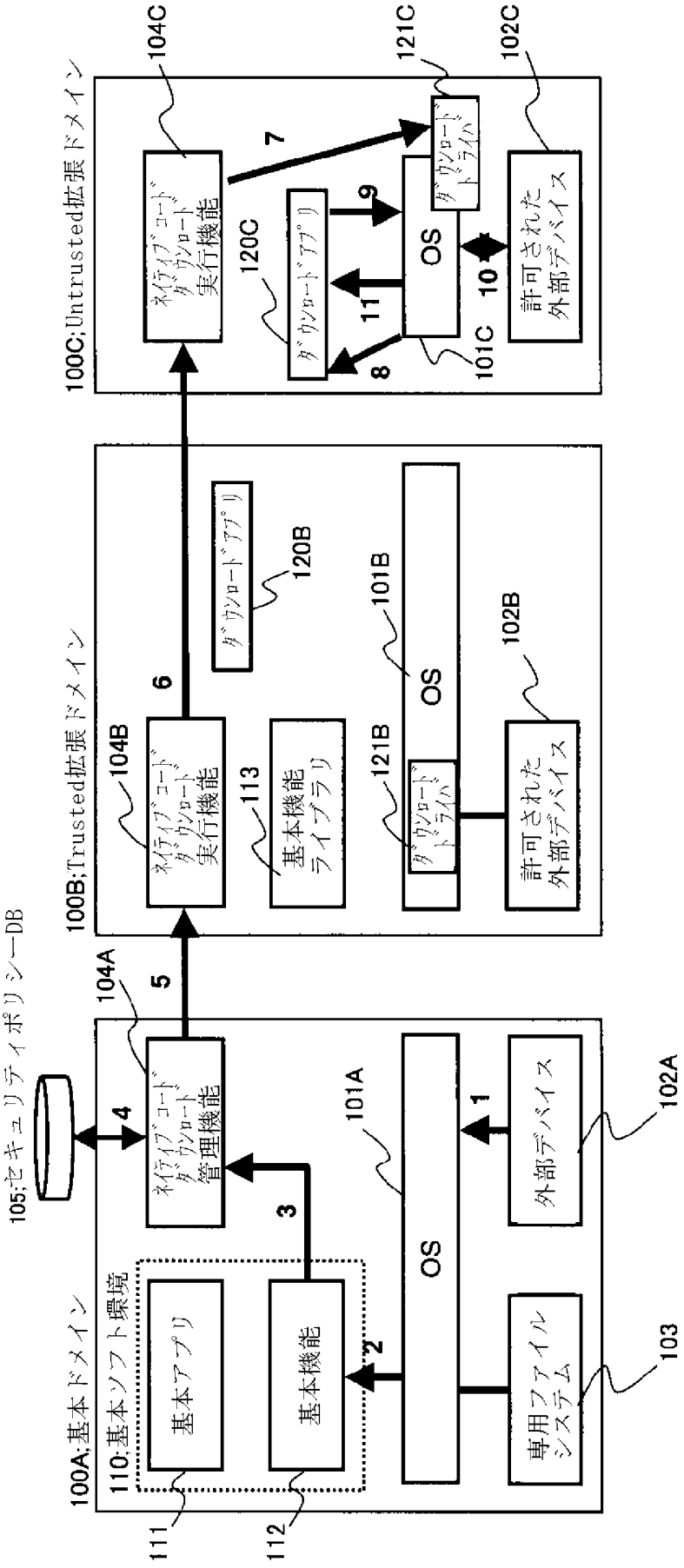
[図13]


100C;Untrusted拡張ドメイン
104C
ネイティブコード ダウンロード 実行機能
101C
OS
102C
許可された 外部デバイス
100B; Trusted拡張ドメイン
120B
ダウンロードアプリ
104B
ネイティブコード ダウンロード 実行機能
113
基本機能 ライブラリ
101B
OS
121B
ダウンロード ドライバ
102B
許可された 外部デバイス
1
2
3
4
5
6
7
105;セキュリティポリシーDB
証明書
100A; 基本ドメイン
104A
ネイティブコード ダウンロード 管理機能
110; 基本ソフト環境
基本アプリ
基本機能
111
112
101A
OS
外部デバイス
102A
専用ファイル システム
103

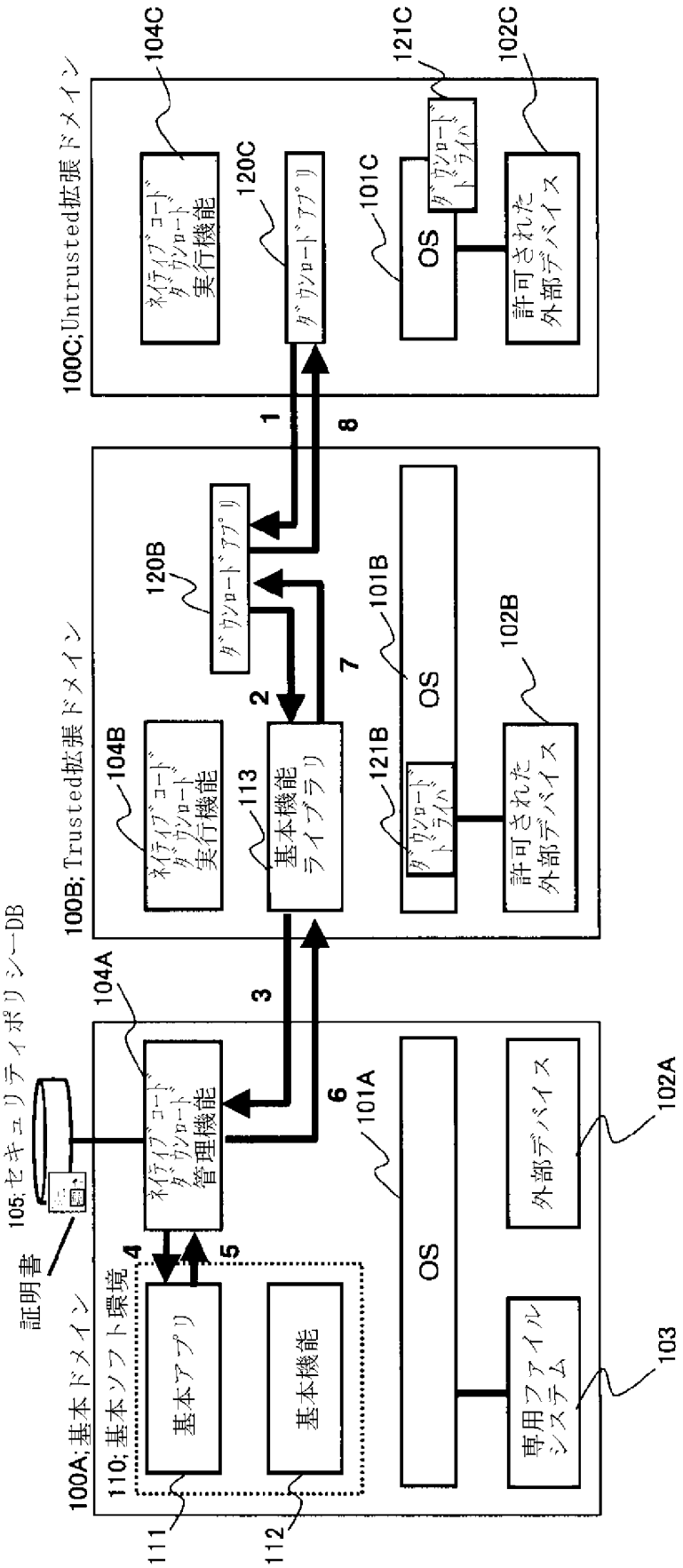
[図14]


100A;基本ドメイン
110;基本ソフト環境
基本アプリ
基本機能
111
112
ネイティブコード ダウンロード 管理機能
104A
OS
101A
外部デバイス
102A
専用ファイル システム
103
105;セキュリティポリシーDB
100B;Trusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104B
基本機能 ライブラリ
113
ダウンロードアプリ
120B
OS
101B
ダウンロード ライブラリ
121B
許可された 外部デバイス
102B
100C;Untrusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104C
ダウンロードアプリ
120C
OS
101C
許可された 外部デバイス
102C
1
2
3
4
5
6
7
8

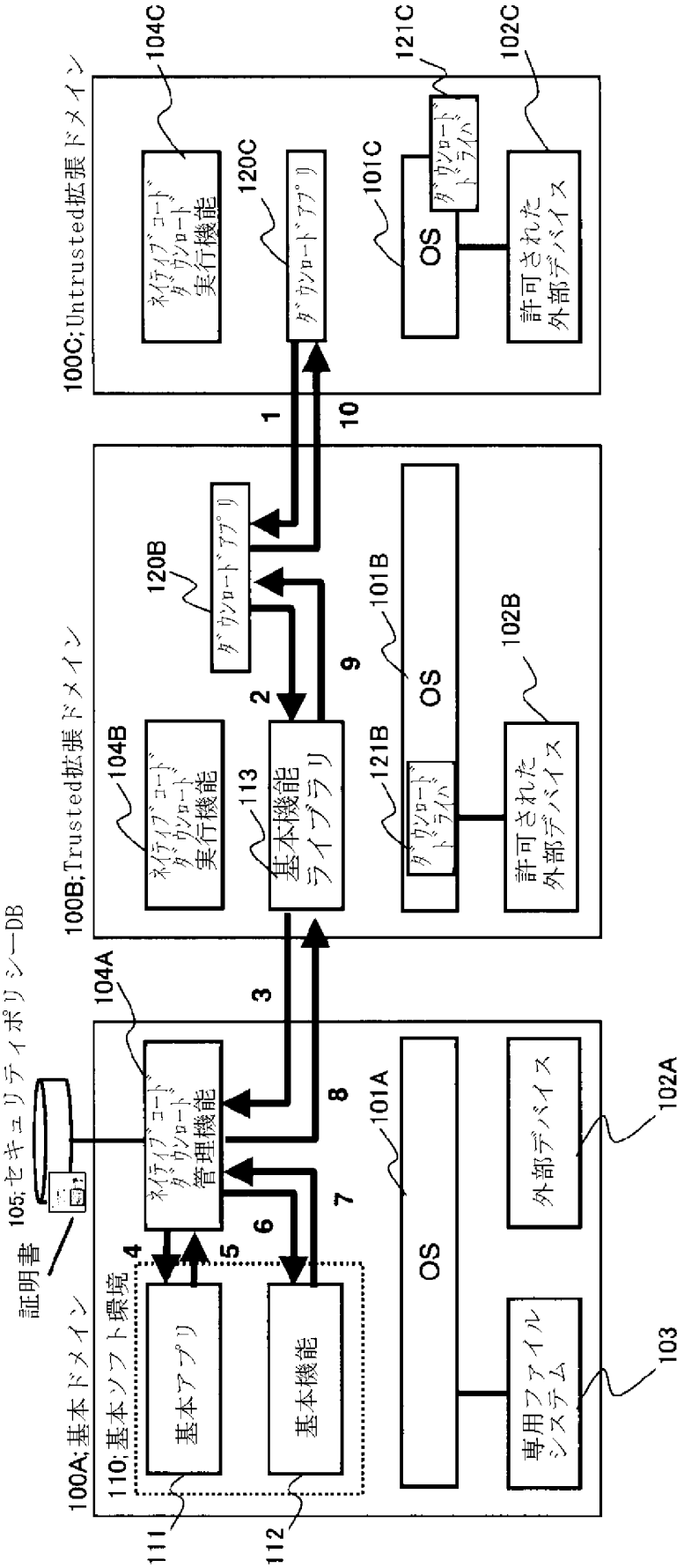
[図15]


100A;基本ドメイン
110;基本ソフト環境
基本アプリ
基本機能
111
112
ネイティブコード
ダウンロード
管理機能
104A
105;セキュリティポリシーDB
OS
101A
専用ファイル
システム
103
外部デバイス
102A
100B;Trusted拡張ドメイン
ネイティブコード
ダウンロード
実行機能
104B
基本機能
ライブラリ
113
ダウンロードアプリ
120B
OS
101B
ダウンロード
ドライバ
121B
許可された
外部デバイス
102B
100C;Untrusted拡張ドメイン
ネイティブコード
ダウンロード
実行機能
104C
ダウンロードアプリ
120C
OS
101C
ダウンロード
ドライバ
121C
許可された
外部デバイス
102C
1
2
3
4
5
6
7
8
9
10
11

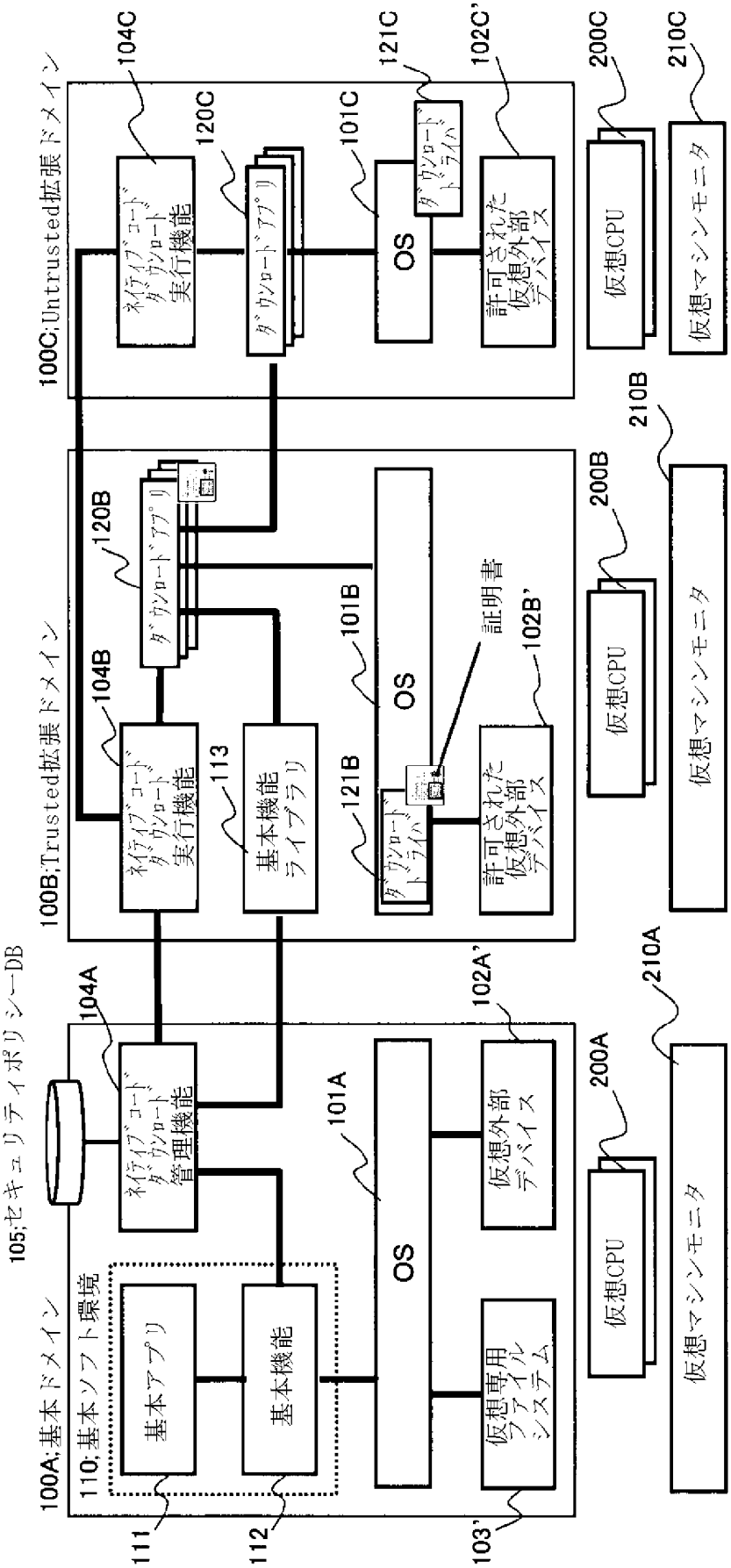
[図16]


100C;Untrusted拡張ドメイン
104C
ネイティブコード ダウンロード 実行機能
120C
ダウンロードアプリ
101C
OS
121C
ダウンロード ドライバ
102C
許可された 外部デバイス
1
8
100B; Trusted拡張ドメイン
120B
ダウンロードアプリ
2
7
101B
OS
104B
ネイティブコード ダウンロード 実行機能
113
基本機能 ライブラリ
121B
ダウンロード ドライバ
102B
許可された 外部デバイス
3
6
105;セキュリティポリシーDB
104A
ネイティブコード ダウンロード 管理機能
101A
OS
外部デバイス
102A
証明書
4
5
100A;基本ドメイン
110; 基本ソフト環境
基本アプリ
基本機能
専用ファイル システム
103
111
112

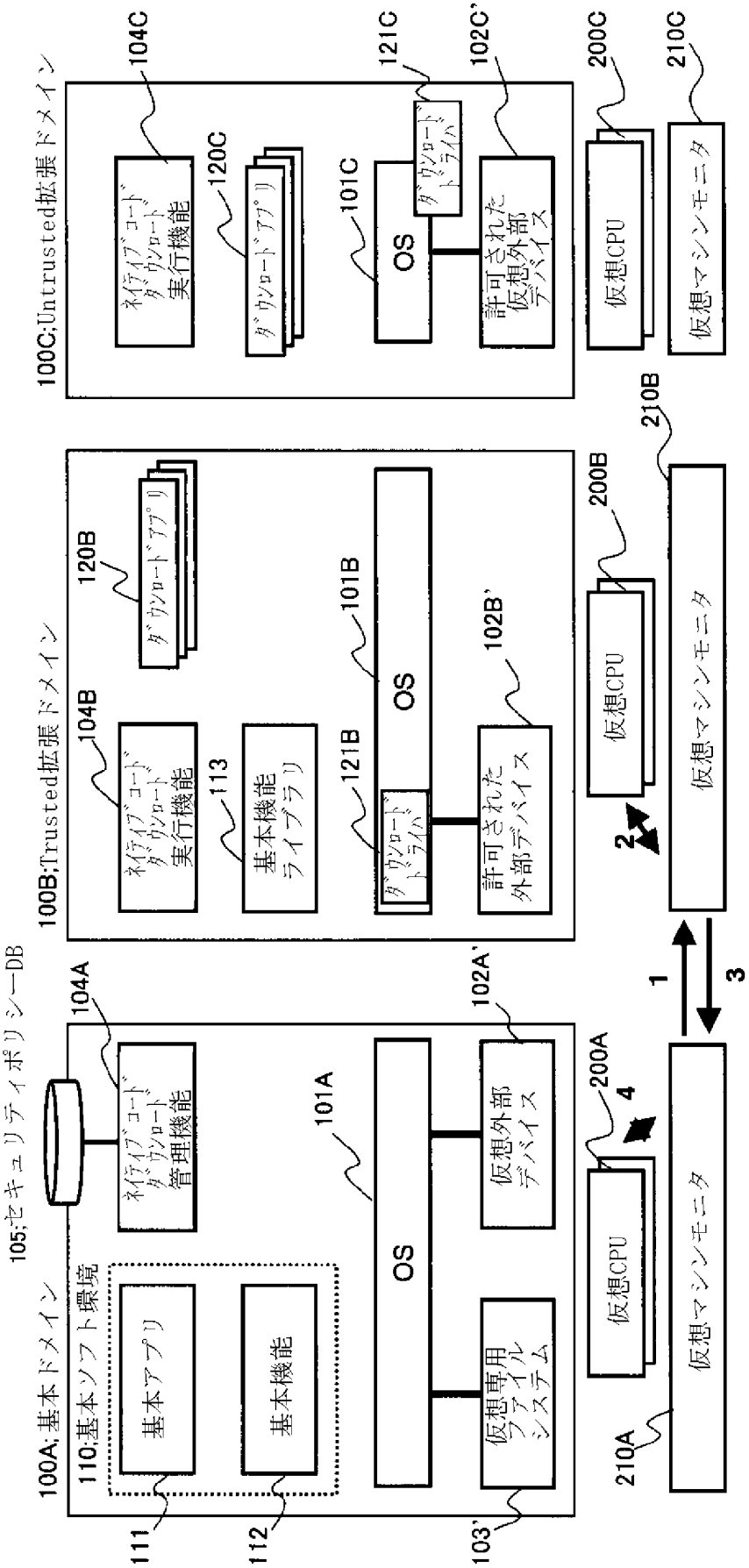
[図17]


100C;Untrusted拡張ドメイン
104C
ネイティブコード
ダウンロード
実行機能
120C
ダウンロードアプリ
101C
OS
121C
ダウンロード
ドライバ
102C
許可された
外部デバイス
100B;Trusted拡張ドメイン
104B
ネイティブコード
ダウンロード
実行機能
113
基本機能
ライブラリ
120B
ダウンロードアプリ
101B
OS
121B
ダウンロード
ドライバ
102B
許可された
外部デバイス
100A;基本ドメイン
110;基本ソフト環境
基本アプリ
基本機能
104A
ネイティブコード
ダウンロード
管理機能
101A
OS
外部デバイス
102A
専用ファイル
システム
103
105;セキュリティポリシーDB
証明書
111
112
1
2
3
4
5
6
7
8
9
10

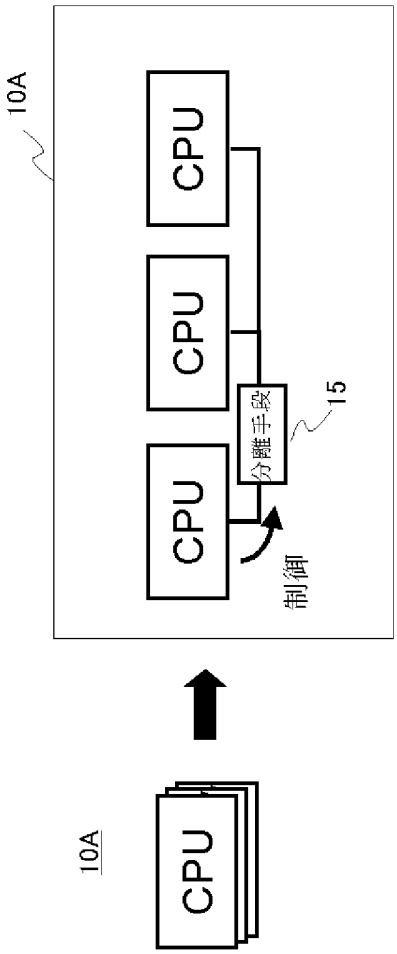
[図18]


100A;基本ドメイン
110;基本ソフト環境
基本アプリ
基本機能
111
112
ネイティブコード ダウンロード 管理機能
104A
OS
101A
仮想外部 デバイス
102A'
仮想専用 ファイル システム
103'
105;セキュリティポリシーDB
100B;Trusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104B
基本機能 ライブラリ
113
ダウンロードアプリ
120B
OS
101B
ダウンロード ドライバ
121B
許可された 仮想外部 デバイス
102B'
証明書
仮想CPU
200B
仮想マシンモニタ
210B
100C;Untrusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104C
ダウンロードアプリ
120C
OS
101C
ダウンロード ドライバ
121C
許可された 仮想外部 デバイス
102C'
仮想CPU
200C
仮想マシンモニタ
210C
仮想CPU
200A
仮想マシンモニタ
210A

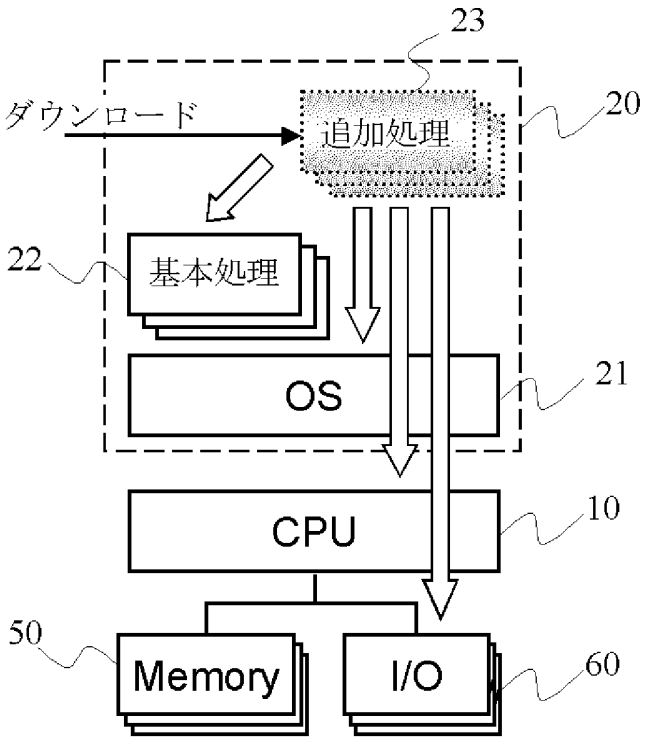
[図19]


100A;基本ドメイン
110;基本ソフト環境
基本アプリ
基本機能
111
112
ネイティブコード ダウンロード 管理機能
104A
105;セキュリティポリシーDB
OS
101A
仮想専用 ファイル システム
103'
仮想外部 デバイス
102A'
仮想CPU
200A
仮想マシンモニタ
210A
100B;Trusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104B
基本機能 ライブラリ
113
ダウンロードアプリ
120B
OS
101B
ダウンロード ドライバ
121B
許可された 外部デバイス
102B'
仮想CPU
200B
仮想マシンモニタ
210B
100C;Untrusted拡張ドメイン
ネイティブコード ダウンロード 実行機能
104C
ダウンロードアプリ
120C
OS
101C
ダウンロード ドライバ
121C
許可された 仮想外部 デバイス
102C'
仮想CPU
200C
仮想マシンモニタ
210C
1
2
3
4

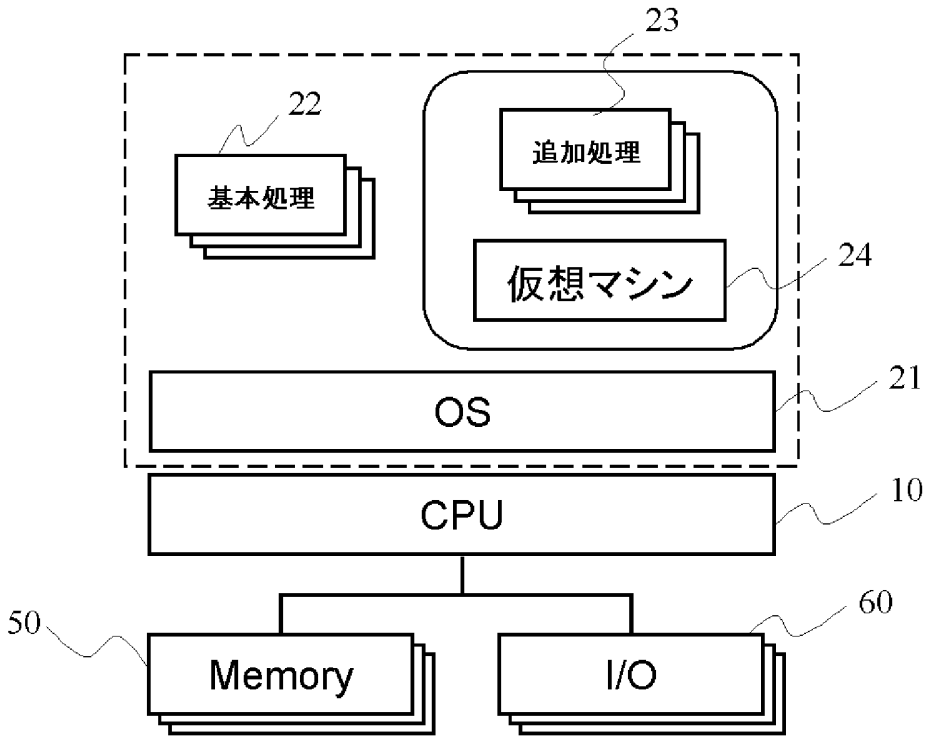
[図20]



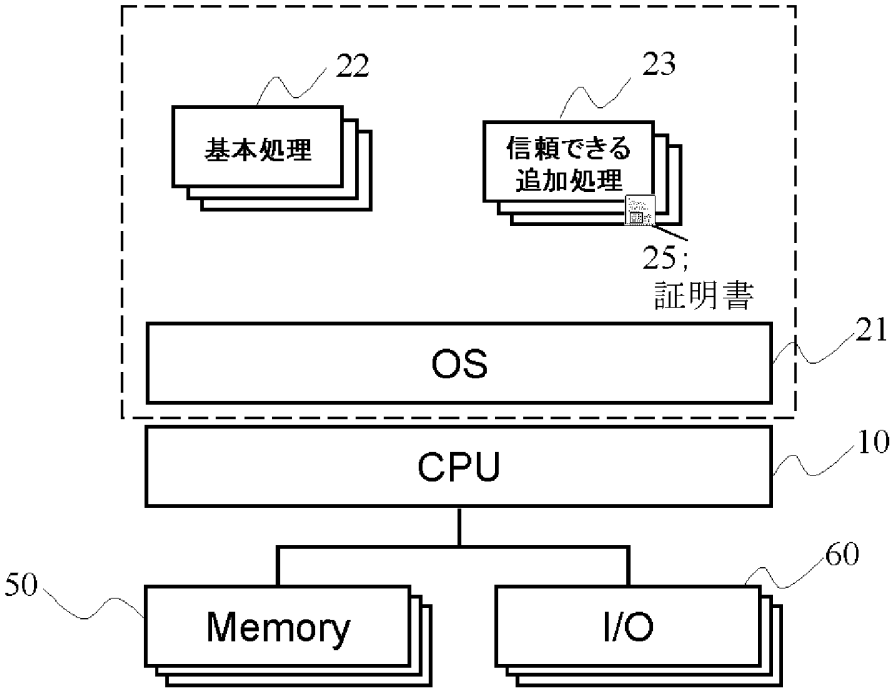
[図21]


23
ダウンロード
追加処理
20
22
基本処理
OS
21
CPU
10
50
Memory
I/O
60

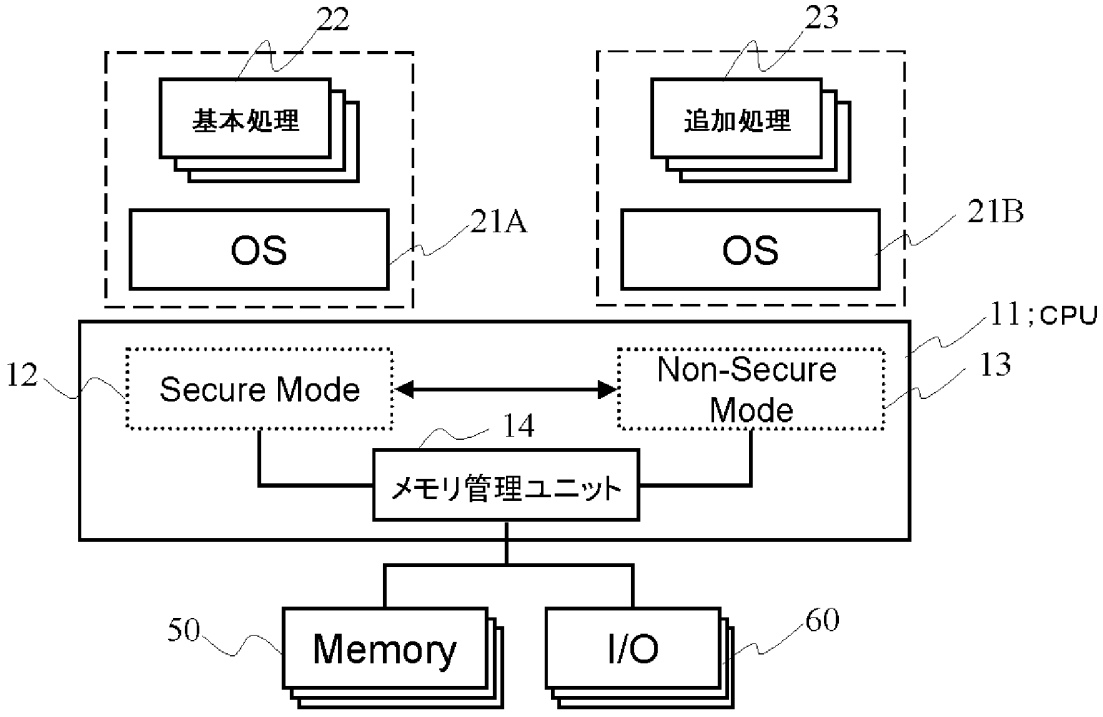
[図22]


23
22
基本処理
追加処理
仮想マシン
24
OS
21
CPU
10
50
Memory
I/O
60

[図23]


22
23
基本処理
信頼できる
追加処理
25;
証明書
OS
21
CPU
10
50
Memory
I/O
60

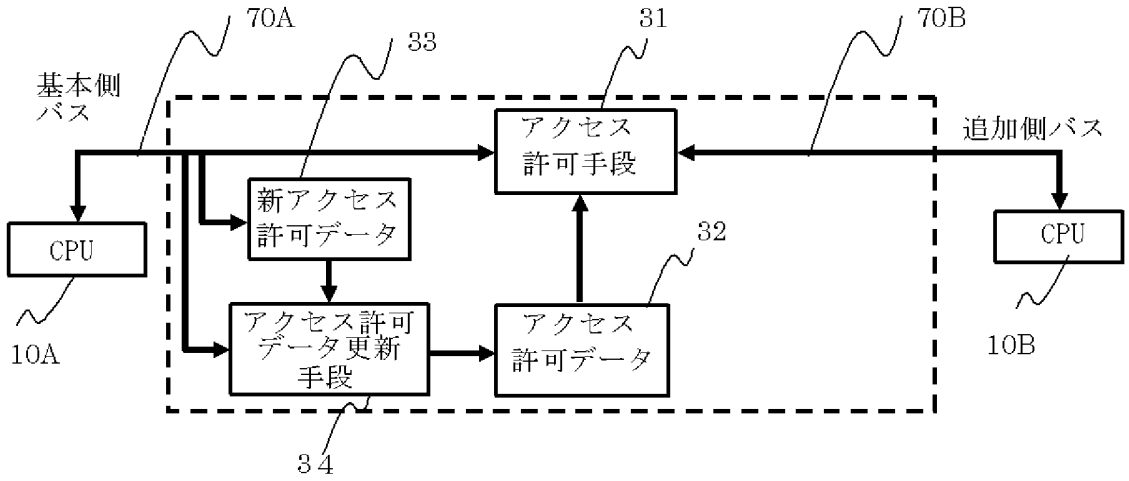
[図24]


22
23
基本処理
追加処理
OS
21A
OS
21B
11;CPU
12
Secure Mode
Non-Secure
Mode
13
14
メモリ管理ユニット
50
Memory
I/O
60

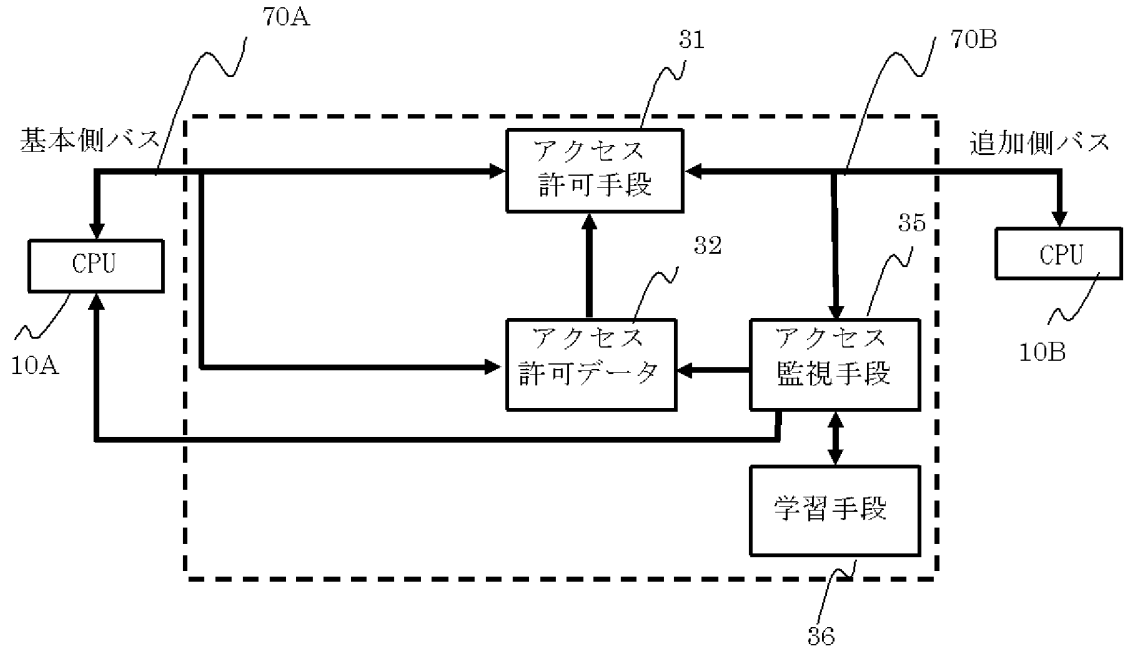
[図25]

	基本ドメイン	信頼拡張ドメイン	無信頼ドメイン
機能１	レベルＡ	―――	―――
機能２	レベルＡ	レベルＢ	―――
機能３	レベルＡ、レベルＢ	レベルＡ，レベルＢ	―――
機能４	レベルＡ、レベルＢ	レベルＡ，レベルＢ	レベルＣ
機能５	レベルＡ、レベルＢ	レベルＡ，レベルＢ、レベルＣ	レベルＣ、レベルＤ

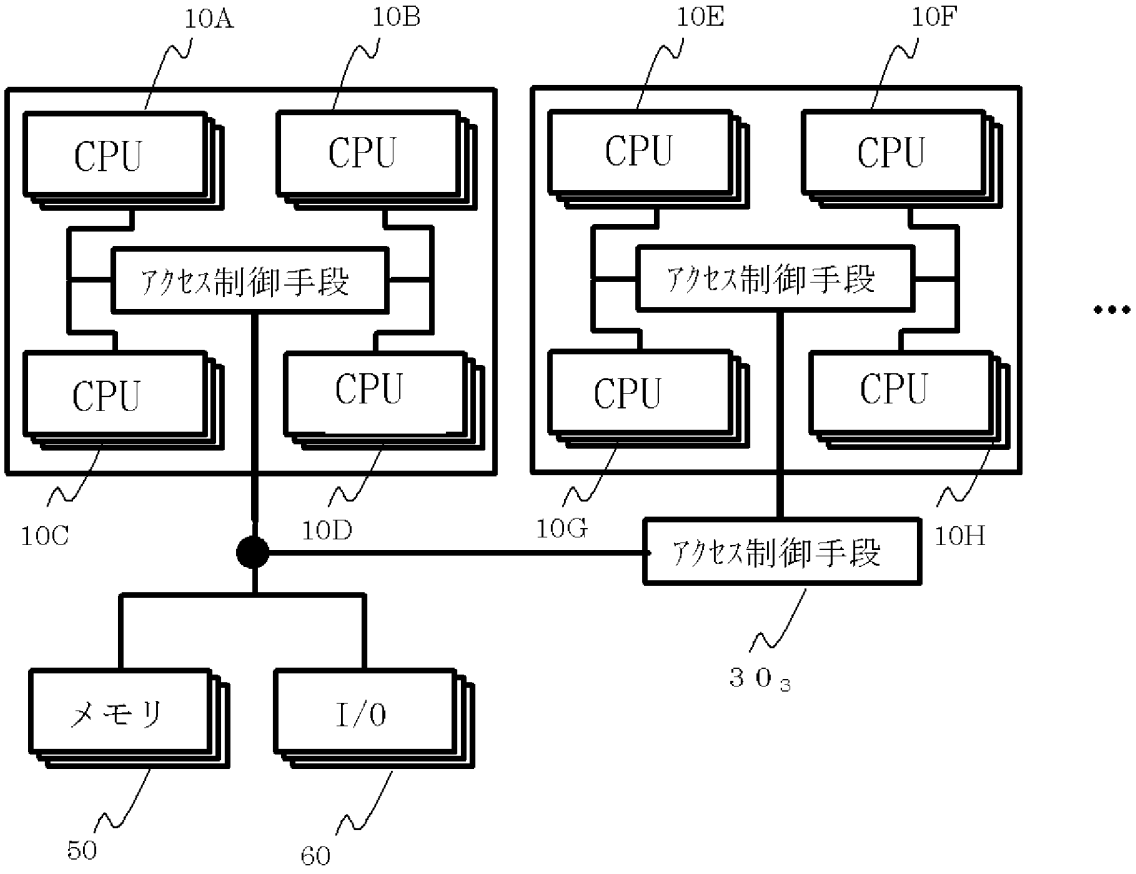
[図26]



[図27]



[図28]


10A
10B
10E
10F
CPU
CPU
CPU
CPU
アクセス制御手段
アクセス制御手段
CPU
CPU
CPU
CPU
10C
10D
10G
10H
アクセス制御手段
30 3
メモリ
I/O
50
60

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/014903

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, 9/50, 9/54

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)
Int.Cl[7] G06F12/14, 9/50, 9/54

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 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

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 X	JP 2002-351854 A (Omron Corp.), 06 December, 2002 (06.12.02), Full text; all drawings & US 2002/0184289 A1	1-60 61
A	JP 56-72754 A (Casio Computer Co., Ltd.), 17 June, 1981 (17.06.81), Full text; all drawings (Family: none)	1-61

☐ 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
05 September, 2005 (05.09.05)	20 September, 2005 (20.09.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号 PCT／JP2005／014903

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] G06F12/14, 9/50, 9/54

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.[7] G06F12/14, 9/50, 9/54

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	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005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	関連する請求の範囲の番号
A X	JP 2002-351854 A (オムロン株式会社) 2002.12.06, 全文、全図 & US 2002/0184289 A1	1-60 61
A	JP 56-72754 A (カシオ計算機株式会社) 1981.06.17, 全文、全図 (ファミリーなし)	1-61

☐ 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 05. 09. 2005	国際調査報告の発送日 20. 9. 2005
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） 5S 9071 平井 誠 電話番号 03－3581－1101 内線 3546