

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5609333号  
(P5609333)

(45) 発行日 平成26年10月22日 (2014. 10. 22)

(24) 登録日 平成26年9月12日 (2014. 9. 12)

(51) Int. Cl.	F I				
<b>G06F</b>	<b>9/445</b>	<b>(2006.01)</b>	G06F	9/06	610K
<b>G06F</b>	<b>9/54</b>	<b>(2006.01)</b>	G06F	9/06	640B
<b>G06F</b>	<b>9/50</b>	<b>(2006.01)</b>	G06F	9/06	640H

請求項の数 8 (全 33 頁)

(21) 出願番号	特願2010-153190 (P2010-153190)	(73) 特許権者	000005223 富士通株式会社
(22) 出願日	平成22年7月5日 (2010. 7. 5)		神奈川県川崎市中原区上小田中4丁目1番1号
(65) 公開番号	特開2012-14637 (P2012-14637A)	(74) 代理人	100092978 弁理士 真田 有
(43) 公開日	平成24年1月19日 (2012. 1. 19)	(74) 代理人	100112678 弁理士 山本 雅久
審査請求日	平成25年5月7日 (2013. 5. 7)	(72) 発明者	田中 法美 石川県かほく市宇野気ヌ98番地の2 株式会社PFU内
		審査官	大塚 俊範

最終頁に続く

(54) 【発明の名称】 起動処理方法、情報処理装置、起動処理プログラム及び同プログラムを記録したコンピュータ読取可能な記録媒体

(57) 【特許請求の範囲】

【請求項1】

プロセッサをそなえた情報処理装置の起動処理方法であって、  
 該プロセッサにより実行されることにより当該情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードするステップと、  
 該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するステップと、  
 該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードするステップと、  
 該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得するステップとをそなえることを特徴とする、起動処理方法。

【請求項2】

該記憶領域に、2以上のモジュールにより共通に用いられる第2共通情報を格納する共通領域を形成するステップと、  
 該記憶領域に、該共通領域へアクセスするための共通領域アクセス情報を格納するステップと、  
 該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、アクセスした当該アクセス情報を用いて該第1共通情報にアクセスし、アクセスした当

該第 1 共通情報に基づいて該共通領域アクセス情報にアクセスし、アクセスした当該共通領域アクセス情報を用いて、該共通領域に格納された該第 2 共通情報を取得するステップとをそなえることを特徴とする、請求項 1 記載の起動処理方法。

【請求項 3】

該起動処理が複数のフェーズをそなえ、

該複数のフェーズのうち一のフェーズにおいて、該プロセッサのプロセッサキャッシュを該記憶領域として用い、

該情報処理装置の主記憶装置が使用可能な状態となった後に、該プロセッサキャッシュに格納されている該第 2 共通情報を該主記憶装置に複写するステップをそなえることを特徴とする、請求項 2 記載の起動処理方法。

10

【請求項 4】

プロセッサをそなえた情報処理装置であって、

起動処理時に、該プロセッサにより実行されることにより当該情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2 以上のモジュールにより共通に用いられる第 1 共通情報をそなえる第 1 モジュールをロードする第 1 モジュール設定部と、

起動処理時に、該情報処理装置にそなえられた記憶領域に、該第 1 共通情報へアクセスするためのアクセス情報を格納するアクセス情報設定部と、

起動処理時に、該アクセス情報にアクセスするためのインタフェース情報をそなえる第 2 モジュールをロードする第 2 モジュール設定部と、

該起動処理時に、該第 2 モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第 1 共通情報を取得する第 1 情報取得部とをそなえることを特徴とする、情報処理装置。

20

【請求項 5】

該起動処理時に、該記憶領域に、2 以上のモジュールにより共通に用いられる第 2 共通情報を格納する共通領域を形成する共通領域設定部と、

該起動処理時に、該記憶領域に、該共通領域へアクセスするための共通領域アクセス情報を格納する共通領域アクセス情報設定部と、

該起動処理時に、該第 2 モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、アクセスした当該アクセス情報を用いて該第 1 共通情報にアクセスし、アクセスした当該第 1 共通情報に基づいて該共通領域アクセス情報にアクセスし、アクセスした当該共通領域アクセス情報を用いて、該共通領域に格納された該第 2 共通情報を取得する第 2 情報取得部とをそなえることを特徴とする、請求項 4 記載の情報処理装置。

30

【請求項 6】

該起動処理が複数のフェーズをそなえ、

該複数のフェーズのうち一のフェーズにおいて、該プロセッサのプロセッサキャッシュを該記憶領域として用い、

該共通領域設定部が、該情報処理装置の主記憶装置が使用可能な状態となった後に、該プロセッサキャッシュに格納されている該第 2 共通情報を該主記憶装置に複写することを特徴とする、請求項 5 記載の情報処理装置。

【請求項 7】

起動処理をコンピュータに実行させるための起動処理プログラムであって、

該コンピュータに実行されることにより情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2 以上のモジュールにより共通に用いられる第 1 共通情報をそなえる第 1 モジュールをロードするステップと、

該情報処理装置にそなえられた記憶領域に、該第 1 共通情報へアクセスするためのアクセス情報を格納するステップと、

該アクセス情報にアクセスするためのインタフェース情報をそなえる第 2 モジュールをロードするステップと、

該第 2 モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第 1 共通情報を取得するステップとを、該コンピュータに実

40

50

行させることを特徴とする、起動処理プログラム。

【請求項 8】

起動処理をコンピュータに実行させるための起動処理プログラムを記録したコンピュータ読取可能な記録媒体であって、

該起動処理プログラムが、

該コンピュータに実行されることにより情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードするステップと、

該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するステップと、

該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードするステップと、

該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得するステップとを、該コンピュータに実行させることを特徴とする、起動処理プログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本件は、情報処理装置の起動処理を行なう技術に関する。

【背景技術】

【0002】

近年、P C (Personal Computer) の起動処理に、B I O S (Basic Input/Output System) に代えて、E F I (Extensible Firmware Interface) を用いる手法が知られている (下記特許文献1, 非特許文献1)。E F I は、B I O S に代わるプラットフォーム・ファームウェアであり、P C のハードウェアにO S (Operating System) を読み込む準備をさせる作業を行なう。マザーボードにE F I を組み込むことにより、P C の起動時間を短縮でき、ハードウェアの設計やソフトウェアの開発が容易になる。このE F I B I O S は、Unified EFI Forumによって規格の策定が進められている。

【0003】

E F I においては、O S が起動するまでに、主に、S E C (Security)、P E I (Pre-EFI Initialization)、D X E (Driver Execution Environment) 及びB D S (Boot Device Selection) の4つのフェーズをそなえ、各フェーズの処理オーダは、S E C、P E I、D X E、B D S の順となる。

また、各フェーズは、複数のモジュールから構成されており、P E I フェーズのモジュールをP E I モジュール (P E I M) という。又、D X E フェーズのモジュールとしては、D X E ドライバやE F I ドライバがある。

【0004】

各モジュールは、B I O S F l a s h から読み出され、C P U (Central Processing Unit) キャッシュやメモリ等の実行領域に展開 (ロード) された後、各モジュールが動作できる条件 (E F I ではプロトコルという) が整ったタイミングでそれぞれ実行される。なお、C P U キャッシュにおけるモジュールがロードされる領域のことを、C A R (Cache As Ram) 領域という。

【0005】

図26はE F I の各フェーズを説明するための図であり、各フェーズ (EFI Phase) について、プログラムロード動作領域、C P U モード及び開発言語を示している。又、図27は従来のE F I におけるモジュール構成を説明するための図、図28はE F I のフェーズ毎のプログラムロード領域を模式的に示す図である。

E F I においては、図26に示すように、E F I フェーズでC P U の動作モードが異なり、16ビット (bit)、32ビット、64ビット、32ビットのS M M (System Manage

10

20

30

40

50

ment Mode) 及び 64 ビットの SMM の各モードがある。又、図 26 ~ 図 28 に示すように、EFI においては、モジュールのプログラムがロードされ、このプログラムが動作する領域 (プログラムロード動作領域) も EFI フェーズで異なる。なお、プログラムロード実行領域としては、図 26 に示すように、BIOS Flash、CAR 及びメモリ (SMM を含む) がある。

【0006】

従来の EFI による PC の起動処理においては、まず、BIOS Flash 上にプログラムがロードされ CAR の機能を有効にする。すなわち、SEC フェーズにおいては、図 27 に示すように、BIOS Flash 上にプログラムがロードされる。

そして、PEI フェーズにおいては、この CAR 領域にプログラムがロードされ、この PEI において、メモリコントローラの初期化が行なわれ、メモリアクセスが有効になった後に、メモリ上にプログラムがロードされる。すなわち、PEI フェーズにおいては、その初期段階において CAR 領域にプログラムがロードされた後、メモリ上にプログラムがロードされる。

10

【0007】

その後、PEI の後半において、チップセットの設定等が行なわれ、DXE が動作できるための必要最小限のチップセット設定等が行なわれる。DXE フェーズにおいては、メモリ上にプログラムがロードされ、その後、BDS が読み出される。

また、使用されるプログラム言語もフェーズによって異なり、図 26 に示すように、SEC はアセンブラ言語であり、PEI、DXE、BDS は C 言語がメインとなる。

20

【0008】

そして、このような従来の EFI においては、画面表示やキーボード入力のような各モジュール間で共通に必要な機能はライブラリ化され、各モジュールにこれらの共通機能ライブラリをそれぞれ付加している。

すなわち、図 27 に示すように、従来の EFI においては、PEI 及び DXE (BDS) の各モジュールにそれぞれ共通機能ライブラリが付加されている。

【0009】

また、従来の EFI においては、異なるフェーズ間で、メモリサイズや CPU の種別等の情報を共有する手法として、HOB (Hand Of Block) 構造体を用いることが知られている。

30

具体的には、PEI フェーズにおいて構築した HOB 構造体と呼ばれる情報を、メモリを介して DXE フェーズに受け渡すことにより、PEI フェーズと DXE フェーズとの間での情報の共有を実現している。

【先行技術文献】

【特許文献】

【0010】

【特許文献 1】特開 2008 - 102906 号公報

【非特許文献】

【0011】

【非特許文献 1】Vincent Zimmer 著 「BIOS に代わるプラットフォーム・ファームウェアをあらゆるインテルシリコンに (日本語参考訳)」 (Technology@IntelMagazine) 2004 年 1 月 [http://download.intel.com/jp/developer/jpdoc/it01043\\_j.pdf](http://download.intel.com/jp/developer/jpdoc/it01043_j.pdf)

40

【発明の概要】

【発明が解決しようとする課題】

【0012】

しかしながら、このような従来の EFI においては、図 27 に示したように、各モジュールにそれぞれ共通機能ライブラリがそなえられているので、共通機能ライブラリのサイズが大きくなると、モジュール自身のサイズも大きくなる。これにより、EFI が使用するリソースサイズの肥大化が顕著となる。例えば、サーバや組込み系システムでは、必要とされる RAS (Reliability, Availability and Serviceability; 信頼性、可用性、保

50

守性)機能が多く、共通機能数が多くなるので、共通機能ライブラリのサイズが大きくなる。従って、サーバや組込み系システムではリソースサイズの肥大化が生じ易い。

【0013】

すなわち、従来のEFIにおいては、各モジュールにそれぞれ共通機能ライブラリがそなえられているので、モジュールのサイズが大きくなり、EFIを格納するBIOS Flashの領域やEFIが使用するプログラムロード動作領域のサイズも肥大化するという課題がある。

また、従来のEFIにおけるフェーズ間での情報共有手法に関し、PEIからDXEへのフェーズの切り替え時においては、32ビットから64ビットへのCPUモードの切り替え等、DXEフェーズが動作するためのモジュール(DXEコアという)が整うまではHOB構造体の参照を行なうことはできないという課題がある。

10

【0014】

例えば、ハードエラーが検出され、メモリ構成等を参照する必要がある場合等においては、PEIからDXEへのフェーズの切り替え時に、これらのフェーズ間での情報共有が必要になるケースが発生する。しかしながら、上述の如く、DXEコアの準備が完了するまで情報共有を行なうことができず、処理の遅滞をまねくおそれがある。

また、各モジュールにおいて、共通機能ライブラリが展開されるアドレスはモジュール毎に異なり、これらのモジュール間で共通機能ライブラリを共有することもできない。従って、従来のEFIにおいては、たとえ共通機能ライブラリに共有域を設けたとしても、この共有域の情報をモジュール間で共有することができず、又、フェーズ切り替え時における情報参照も行なうことができない。

20

【0015】

本件の目的の一つは、このような課題に鑑み創案されたもので、情報処理の起動処理にかかるプログラムサイズを小さくするとともに、起動処理過程におけるフェーズ間での情報を共有できるようにすることである。

なお、前記目的に限らず、後述する発明を実施するための形態に示す各構成により導かれる作用効果であって、従来の技術によっては得られない作用効果を奏することも本発明の他の目的の一つとして位置付けることができる。

【課題を解決するための手段】

【0016】

このため、この起動処理方法は、プロセッサをそなえた情報処理装置の起動処理方法であって、該プロセッサにより実行されることにより当該情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードするステップと、

該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するステップと、該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードするステップと、該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得するステップとをそなえる。

30

【0017】

また、この情報処理装置は、プロセッサをそなえた情報処理装置であって、起動処理時に、該プロセッサにより実行されることにより情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードする第1モジュール設定部と、起動処理時に、該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するアクセス情報設定部と、起動処理時に、該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードする第2モジュール設定部と、該起動処理時に、該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得する第1情報取得部とをそなえる。

40

50

## 【 0 0 1 8 】

さらに、この起動処理プログラムは、起動処理をコンピュータに実行させるための起動処理プログラムであって、該コンピュータに実行されることにより情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードするステップと、該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するステップと、該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードするステップと、該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得するステップとを、該コンピュータに実行させる。又、このコンピュータ読取可能な記録媒体は、上述した起動処理プログラムを記録したものである。

10

## 【 発 明 の 効 果 】

## 【 0 0 1 9 】

開示の技術によれば、情報処理装置の起動処理において、第1モジュールにそなえられた第1共通情報を第2モジュールが取得して使用することができるので、複数のモジュール間で第1共通情報を共有することができる。これにより、情報処理装置の起動処理にかかるモジュールやプログラムのサイズを小さくすることができ、ロードされるメモリサイズやBIOS Flashの容量を小さく構成することができる。従って、処理速度の向上や製造コストを低減することができる。

## 【 図 面 の 簡 単 な 説 明 】

20

## 【 0 0 2 0 】

【 図 1 】 実施形態の一例としての情報処理装置のハードウェア構成を模式的に示す図である。

【 図 2 】 実施形態の一例としての情報処理装置のBIOS Flashに格納されたEFIのプログラムデータPを模式的に示す図である。

【 図 3 】 実施形態の一例としての情報処理装置におけるEFIのフェーズ毎のモジュールや各種情報のロード領域を模式的に示す図である。

【 図 4 】 実施形態の一例としての情報処理装置におけるデータ参照手法を模式的に示す図である。

【 図 5 】 実施形態の一例としての情報処理装置の起動時におけるEFIのフェーズの処理を説明するためのフローチャートである。

30

【 図 6 】 実施形態の一例としての情報処理装置におけるSECフェーズの処理を説明するためのフローチャートである。

【 図 7 】 実施形態の一例としての情報処理装置におけるPEIフェーズの処理を説明するためのフローチャートである。

【 図 8 】 実施形態の一例としての情報処理装置におけるDXE (BDS) フェーズの処理を説明するためのフローチャートである。

【 図 9 】 実施形態の一例としての情報処理装置におけるPEIフェーズ (CAR領域) での共通ライブラリSLの読み出し手法を説明するためのフローチャートである。

【 図 1 0 】 実施形態の一例としての情報処理装置におけるPEIフェーズ (CAR領域) での共通ライブラリSLへの参照経路を説明する図である。

40

【 図 1 1 】 実施形態の一例としての情報処理装置におけるPEIフェーズ (CAR領域) での共通領域に格納された共通領域情報の読み出し手法を説明するためのフローチャートである。

【 図 1 2 】 実施形態の一例としての情報処理装置におけるPEIフェーズ (CAR領域) での共通領域への参照経路を説明する図である。

【 図 1 3 】 実施形態の一例としての情報処理装置におけるPEIフェーズ (メモリ領域) での共通ライブラリSLの読み出し手法を説明するためのフローチャートである。

【 図 1 4 】 実施形態の一例としての情報処理装置におけるPEIフェーズ (メモリ領域) での共通ライブラリSLへの参照経路を説明する図である。

50

【図15】実施形態の一例としての情報処理装置におけるPEIフェーズ（メモリ領域）での共通領域に格納された共通領域情報の読み出し手法を説明するためのフローチャートである。

【図16】実施形態の一例としての情報処理装置におけるPEIフェーズ（メモリ領域）での共通領域への参照経路を説明する図である。

【図17】実施形態の一例としての情報処理装置におけるDXEフェーズ（メモリ領域）での共通ライブラリSLの読み出し手法を説明するためのフローチャートである。

【図18】実施形態の一例としての情報処理装置におけるDXEフェーズ（メモリ領域）での共通ライブラリSLへの参照経路を説明する図である。

【図19】実施形態の一例としての情報処理装置におけるDXEフェーズ（メモリ領域）での共通領域に格納された共通領域情報の読み出し手法を説明するためのフローチャートである。

10

【図20】実施形態の一例としての情報処理装置におけるDXEフェーズ（メモリ領域）での共通領域への参照経路を説明する図である。

【図21】実施形態の一例としての情報処理装置におけるSMMフェーズ（PEI, DXE）での共通ライブラリSLの読み出し手法を説明するためのフローチャートである。

【図22】実施形態の一例としての情報処理装置におけるSMMフェーズ（PEI）及びSMMフェーズ（DXE）での共通ライブラリSLへの参照経路を説明する図である。

【図23】実施形態の一例としての情報処理装置におけるSMMフェーズ（PEI, DXE）での共通領域に格納された共通領域情報の読み出し手法を説明するためのフローチャートである。

20

【図24】実施形態の一例としての情報処理装置におけるSMMフェーズ（PEI）での共通領域への参照経路を説明する図である。

【図25】実施形態の一例としての情報処理装置におけるSMMフェーズ（DXE）での共通領域への参照経路を説明する図である。

【図26】EFIの各フェーズを説明するための図である。

【図27】従来のEFIにおけるモジュール構成を説明するための図である。

【図28】EFIのフェーズ毎のプログラムロード領域を模式的に示す図である。

【発明を実施するための形態】

【0021】

30

以下、図面を参照して本起動処理方法、情報処理装置及び起動プログラムに係る実施の形態を説明する。

図1は実施形態の一例としての情報処理装置のハードウェア構成を模式的に示す図である。図2は実施形態の一例としての情報処理装置100のBIOS Flash 22に格納されたEFIのプログラムデータPを模式的に示す図である。図3は実施形態の一例としての情報処理装置におけるEFIのフェーズ毎のモジュールや各種情報のロード領域を模式的に示す図である。

【0022】

本情報処理装置100は、図1に示すように、CPU 10, RAM 20, ROM 21, BIOS Flash 22, ストレージ 23, ディスプレイ 24, キーボード 25 及びマウス 26 をそなえたコンピュータである。又、キーボード 25 及びマウス 26 は入力装置であり、オペレータはこれらのキーボード 25 やマウス 26 を操作して、本情報処理装置 100 の再起動指示を含む種々の指示や情報の入力操作を行なう。又、この情報処理装置 100 は、図示しない電源スイッチをそなえ、オペレータがこの電源スイッチを操作することにより電力投入が行なわれる。

40

【0023】

ストレージ 23 は、ハードディスクドライブ (Hard disk drive: HDD)、SSD (Solid State Drive) 等の記憶装置であって、OS や種々のプログラムやデータを格納するものである。

ディスプレイ 24 は、種々のデータやオペレータに対するメッセージ等の情報を表示す

50

る表示装置である。

【0024】

ROM 21は、CPU 10が実行するプログラムや種々のデータを格納する記憶装置である。

RAM 20は、種々のデータやプログラムを一時的に格納する主記憶装置であって、CPU 10がプログラムを実行する際に、データやプログラムを一時的に格納・展開して用いる。又、RAM 20は、本情報処理装置100の起動過程において、その所定の記憶領域が固有のメモリ領域201(図3参照)やSMM固定のメモリ領域211(図3参照)として機能する。固有のメモリ領域201には、管理域2001と共通領域202とが含まれ、管理域2001には、後述する共通ライブラリへのアドレス情報201と、同じく後述する共通領域へのアドレス情報203とが格納される。又、共通領域202の詳細についても後述する。

10

【0025】

BIOS Flash 22は、EFIのプログラムデータPを格納するメモリであり、例えば、フラッシュメモリ(フラッシュROM)である。

プログラムデータPは、図2に示すように、n個(nは自然数:図2に示す例ではn=3)のモジュールプログラムPn(図2に示す例ではP1~P3)や、起動処理を制御する制御プログラムP0をそなえる。モジュールプログラムPnは、後述するEFIの個々のモジュールを実現するプログラムであり、各モジュール毎にそなえられている。各モジュールプログラムPnは、それぞれヘッダ部Hと実行可能イメージPIをそなえている。

20

【0026】

制御プログラムP0は、後述するCPU 10に実行されることにより、モジュールプログラムPnを所定の順序でロードさせ、EFIの起動処理を実現させるプログラムである。本情報処理装置100の起動時において、CPU 10がこの制御プログラムP0に従い、BIOS Flash 22からモジュールプログラムPnの実行可能イメージPIを順次読み出し、情報処理装置100における所定のロード領域に展開(ロード)して実行することにより、起動処理が行なわれる。

【0027】

このように、情報処理装置100における所定の領域にロードされた各モジュールの実行可能イメージPIは、各モジュールとしての機能を実現する。

30

なお、図2に示す例においては、モジュールプログラムPnの例としてPEIモジュールにかかるモジュールプログラムP1、P2とDXEドライバにかかるモジュールプログラムP3とを示しているが、これに限定されるものではなく、SECモジュールや他の機能を実現するプログラムをモジュールプログラムに含めることを否定するものではなく、種々変形して実施することができる。

【0028】

また、本情報処理装置においては、BIOS Flash 22に格納された各モジュールプログラムP1の実行可能イメージPに、共有ライブラリSLや共有インタフェースライブラリSIが含まれている。

共通ライブラリSLは、例えば、ディスプレイ24への画面表示やキーボード25やマウス26の入力制御のような、複数のモジュールがそれぞれ使用しうる共通の情報(第1共通情報)である。この共通ライブラリSLは、これらの複数のモジュール間で共通に必要な機能をライブラリ化することにより、複数のモジュールが共通に使用できるようにしたものである。この共通ライブラリSLは、当該共通ライブラリSLをそなえるモジュールが使用できるとともに、後述する共通インタフェースライブラリSIをそなえる他のモジュールからも使用される。

40

【0029】

また、共通ライブラリSLは、後述するCAR領域101やRAM 20における所定の領域へアクセスするためのアクセス関数もそなえている。後述するCPU 10が、このアクセス関数を実行することにより、例えば、CAR領域101やRAM 20における所定

50



の領域へアクセスするためのアドレス演算が行なわれる。

これにより、例えば、P E IモジュールM 1 1の共通ライブラリS LからC A R領域1 0 1の共通領域へのアドレス情報1 0 3にアクセスすることができる。同様に、P E IモジュールM 2 1やP E IモジュールM 2 1の共通ライブラリS Lから固定のメモリ領域2 0 1の共通領域へのアドレス情報2 0 3へアクセスすることができる。又、D X EドライバD 1やD X EドライバD 3の共通ライブラリS Lから固定のメモリ領域2 0 1の共通領域へのアドレス情報2 0 3へアクセスすることができる。

【0030】

共通ライブラリS Lは、本情報処理装置1 0 0の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報として機能するのである。

10

なお、P E I、D X E、S M M ( D X E )の各フェーズにおいてロード領域が一致するグループ毎において、同一の共通ライブラリS Lが重複してそなえられることがないようにすることが望ましい。つまり、共通ライブラリS Lは、上記グループ毎に1つ構築される。これにより、共通ライブラリS Lの格納に要する容量を削減し、各モジュールのサイズを小さくすることができる。すなわち、B I O S F l a s h 2 2やこれらのモジュールをロードするプログラムロード動作領域を小さくすることができる。望ましくは、共通ライブラリS Lは、上記フェーズ毎に1つ構築される。

【0031】

図3に示す例においては、P E Iフェーズの初期段階においてC A R領域1 0 1に展開される2つのP E IモジュールM 1 1、M 1 2からなる第1のグループにおいては、P E IモジュールM 1 1に共有ライブラリS Lがそなえられている。なお、P E IモジュールM 1 1が、自身にそなえた共通ライブラリS Lを使用することは言うまでもない。以下、P E Iフェーズにおいて、モジュールのロード場所がC A R領域1 0 1の状態をP E Iフェーズ ( C A R領域 ) と表す場合がある。

20

【0032】

また、P E Iフェーズの途中からは、R A M 2 0が使用可となり、このR A M 2 0 ( メモリ領域 ) にモジュールが展開される。図3に示す例において、メモリ領域に展開される2つのP E IモジュールM 2 1、M 2 2からなる第2のグループにおいては、P E IモジュールM 2 1に共有ライブラリS Lがそなえられている。なお、P E IモジュールM 2 1が、自身にそなえた共通ライブラリS Lを使用することは言うまでもない。以下、P E Iフェーズにおいてモジュールのロード場所がR A M 2 0の状態をP E Iフェーズ ( メモリ領域 ) と表す場合がある。

30

【0033】

さらに、図3に示す例において、P E IフェーズにおいてS M M領域3 0 1に展開される2つのP E IモジュールM 2 3、M 2 4からなる第3のグループにおいては、P E IモジュールM 2 3に共有ライブラリS Lがそなえられている。なお、P E IモジュールM 2 3が、自身にそなえた共通ライブラリS Lを使用することは言うまでもない。そして、以下、P E Iフェーズにおいてモジュールのロード場所がS M Mの状態をS M Mフェーズ ( P E I ) と表す場合がある。

40

【0034】

同様に、図3に示す例において、D X Eフェーズにおいてメモリ領域に展開される2つのD X EドライバD 1、D 2からなる第4のグループにおいては、D X EドライバD 1に共有ライブラリS Lがそなえられている。なお、D X EドライバD 1、D 3が、自身にそなえた共通ライブラリS Lを使用することは言うまでもない。又、D X EフェーズにおいてS M M領域3 0 2に展開される2つのD X EドライバD 3、D 4からなる第5のグループにおいては、D X EドライバD 3に共有ライブラリS Lがそなえられている。そして、以下、D X Eフェーズにおいてモジュールのロード場所がS M Mの状態をS M Mフェーズ ( D X E ) と表す場合がある。

【0035】

50

共通インタフェースライブラリ S I は、他のモジュールに含まれる共通ライブラリ S L や後述する共通領域 1 0 2 , 2 0 2 へアクセスするためのインタフェースであり、例えば、管理域 1 0 0 1 , 2 0 0 1 , 2 1 0 1 における所定のアドレスへのポインタをそなえる。

各モジュールは、この共通インタフェースライブラリ S I を介することで、後述する管理域 1 0 0 1 , 2 0 0 1 , 2 1 0 1 を経由し、共通ライブラリ S L や共通領域 1 0 2 , 2 0 2 にアクセスすることができる。すなわち、共通インタフェースライブラリ S I は、共通ライブラリ S L や共通領域 1 0 2 , 2 0 2 に格納された共通領域情報へアクセスするためのインタフェース情報として機能する。

【 0 0 3 6 】

また、BIOS Flash 2 2 には、後述する共通ライブラリへのアドレス情報 1 0 4 , 2 0 4 , 2 1 2 や共通領域へのアドレス情報 1 0 3 , 2 0 3 の他、共通領域 1 0 2 , 2 0 2 に格納する共通情報が格納されている。

CPU (プロセッサ) 1 0 は、種々の制御や演算を行なう処理装置であり、ストレージ 2 3 等に格納されたプログラムを実行することにより、種々の機能を実現する。又、CPU 1 0 は、図示しないキャッシュメモリ (プロセッサキャッシュ) をそなえている。このキャッシュメモリは、データや命令などの情報を一時的に格納する記憶領域であり、CPU 1 0 がアクセスしたいデータやそのアドレス、状態、設定など属性情報をコピーし保持する。なお、このキャッシュメモリは、PEI フェーズ (CAR 領域) においては、この PEI モジュールが展開 (ロード) され、PEI ジュールの実行領域となる。

【 0 0 3 7 】

そして、この CPU 1 0 は、本情報処理装置 1 0 0 の起動時において、BIOS Flash 2 2 に格納された E F I のプログラム P (制御プログラム P 0 ) を実行することにより、本情報処理部 1 0 0 の起動処理を行なう起動処理部 1 1 として機能する。以下、本情報処理装置 1 0 0 における起動処理について説明する。なお、この起動処理は、例えば、本情報処理装置 1 0 0 の電源投入時や再起動時に行なわれる。

【 0 0 3 8 】

この起動処理部 1 1 としての機能を実現するためのプログラム (起動処理プログラム) は、例えばフレキシブルディスク, CD (CD-ROM, CD-R, CD-RW 等), DVD (DVD-ROM, DVD-RAM, DVD-R, DVD+R, DVD-RW, DVD+RW, HD DVD 等), ブルーレイディスク, 磁気ディスク, 光ディスク, 光磁気ディスク等の、コンピュータ読取可能な記録媒体に記録された形態で提供される。そして、コンピュータはその記録媒体からプログラムを読み取って内部記憶装置または外部記憶装置に転送し格納して用いる。又、そのプログラムを、例えば磁気ディスク, 光ディスク, 光磁気ディスク等の記憶装置 (記録媒体) に記録しておき、その記憶装置から通信経路を介してコンピュータに提供するようにしてもよい。

【 0 0 3 9 】

起動処理部 1 1 としての機能を実現する際には、内部記憶装置 (本実施形態では RAM 2 0 や ROM 2 1 ) に格納されたプログラムがコンピュータのマイクロプロセッサ (本実施形態では CPU 1 0 ) によって実行される。このとき、記録媒体に記録されたプログラムをコンピュータが読み取って実行するようにしてもよい。

なお、本実施形態において、コンピュータとは、ハードウェアとオペレーティングシステムとを含む概念であり、オペレーティングシステムの制御の下で動作するハードウェアを意味している。又、オペレーティングシステムが不要でアプリケーションプログラム単独でハードウェアを動作させるような場合には、そのハードウェア自体がコンピュータに相当する。ハードウェアは、少なくとも、CPU 等のマイクロプロセッサと、記録媒体に記録されたコンピュータプログラムを読み取るための手段とをそなえており、本実施形態においては、情報処理装置 1 0 0 がコンピュータとしての機能を有しているのである。

【 0 0 4 0 】

起動処理部 1 1 は、本情報処理部 1 0 0 の起動処理を E F I の仕様に従って行なうもの

10

20

30

40

50

であり、本情報処理装置100の起動(電源投入)からOSへの制御の移行に至るまでのプラットフォームの初期化にかかる処理を実施する。

この起動処理部11は、SEC, PEI, DXE及びDXEの4つのフェーズを順次行なうことにより、EFIの仕様に沿った起動処理を実現する。EFIにおいては、各フェーズで利用可能なインフラストラクチャは中心となるフレームワークによって提供される。そして、プラットフォーム固有の機能は相互通信可能なモジュールを使って実装される。以下、PEIフェーズのモジュールをPEIモジュールという。又、DXEフェーズのモジュールとしては、DXEドライバやEFIドライバがある。

#### 【0041】

なお、図3に示す例においては、PEIモジュールに符号M11, M12, M21~M24を付して表し、又、DXEドライバに符号D1~D4を付して表す。又、以下、PEIモジュールを示す符号としては、複数のPEIモジュールのうち1つを特定する必要があるときには符号M11, M12, M21~M24を用いるが、任意のPEIモジュールを指すときには符号Mを用いる。同様に、以下、DXEドライバを示す符号としては、複数のDXEドライバのうち1つを特定する必要があるときには符号D1~D4を用いるが、任意のDXEドライバを指すときには符号Dを用いる。

#### 【0042】

起動処理部11は、図1に示すように、モジュール設定部111, アクセス情報設定部112, 共通領域アクセス情報設定部113, 共通領域設定部114及び情報取得部115をそなえ、これらの各部が機能することにより起動処理を実現する。

モジュール設定部111は、BIOS Flash 22から、各モジュールに対応するモジュールプログラムPnの実行可能イメージPIを読み出し、それぞれの所定の実行領域(プログラムロード動作領域, ロード領域)にロード(設定, 格納)するロードとして機能する。

#### 【0043】

以下、モジュールに対応するモジュールプログラムPnの実行可能イメージPIをロード領域にロードすることを、便宜上、単にモジュールをロードすると表現する。

モジュール設定部111は、SECフェーズにおいて、BIOS Flash 22にSECモジュール(図示省略)をロードする。そして、CPU10がBIOS Flash 22上のSECモジュールを実行することにより、CPU10のキャッシュが設定されCARの機能が有効になる。

#### 【0044】

また、PEIフェーズにおいては、CAR領域にPEIモジュールMがロードされ、このPEIにおいて、メモリコントローラの初期化が行なわれ、RAM20に対するメモリアクセスが有効になった後に、メモリ上に各モジュールの実行可能イメージP1がロードされるのである。

モジュール設定部111は、EFIの各フェーズを実行するためのPEIモジュールMやDXEドライバDのデータをBIOS Flash 22から読み出し、キャッシュメモリ12やRAM20等のそれぞれの所定の実行領域にロードする。

#### 【0045】

具体的には、モジュール設定部111は、PEIフェーズの初期段階においては、BIOS Flash 22から読み出したPEIモジュールMをCPU10のキャッシュメモリにおけるCAR領域101に展開する。又、モジュール設定部111は、PEIフェーズにおいて、CPU10がPEIモジュールMを実行することによりRAM20の初期設定が完了し、このRAM20が有効となり使用可能となった後においては、このRAM20上の固定のメモリ領域201もしくはSMM領域301にPEIモジュールMをロードする。

#### 【0046】

また、モジュール設定部111は、DXEフェーズにおいては、BIOS Flash 22から読み出したDXEドライバDを、RAM20もしくはRAM20におけるSMM

10

20

30

40

50

領域 3 1 1 上にロードする。

そして、このモジュール設定部 1 1 1 によってロードされるモジュールには、共通ライブラリ S L や共通インタフェースライブラリ S I をそなえるものも含まれる。すなわち、モジュール設定部 1 1 1 は、起動処理時に、2 以上のモジュールにより共通に用いられる共通ライブラリ S L をそなえるモジュールをロードする第 1 モジュール設定部として機能する。更に、モジュール設定部 1 1 1 は、起動処理時に、共通インタフェースライブラリ S I をそなえるモジュールをロードする第 2 モジュール設定部としても機能する。

【 0 0 4 7 】

共通領域設定部 1 1 4 は、C P U 1 0 のキャッシュメモリにおける C A R 領域 1 0 1 や R A M 2 0 における固有のメモリ領域 2 0 1 に、共通領域情報（第 2 共通情報）を格納する共通領域 1 0 2 , 2 0 2 を設定する。

10

ここで、共通領域情報は、例えば、メモリサイズや C P U 1 0 の種別等、E F I の複数のフェーズ間で共通に使用される情報である。このような共通領域情報は、例えば、P E I フェーズの P E I モジュール M と D X E フェーズの D X E ドライバ D とのよう、異なるフェーズのモジュールによって共通して使用される（共有される）。

【 0 0 4 8 】

共通領域設定部 1 1 4 は、P E I フェーズの初期段階において、C A R 領域 1 0 1 における所定位置に共通領域 1 0 2 を確保し、B I O S F l a s h 2 2 から共通領域情報を読み出して、この読み出した共通領域情報を共通領域 1 0 2 に格納する。ここで、共通領域 1 0 2 においては、同一の共通領域情報が重複することがないように格納することが望ましい。

20

【 0 0 4 9 】

また、共通領域設定部 1 1 4 は、P E I フェーズにおいて R A M 2 0 が有効となった後においては、R A M 2 0 の固定のメモリ領域 2 0 1 における所定位置に共通領域 2 0 2 を確保する。そして、共通領域設定部 1 1 4 は、C A R 領域 1 0 1 の共通領域 1 0 2 に格納されている共通領域情報を読み出して、この読み出した共通領域情報を共通領域 2 0 2 に格納する。すなわち、共通領域設定部 1 1 4 は、C A R 領域 1 0 1 の共通領域 1 0 2 の共通領域情報を固有のメモリ領域 2 0 1 の共通領域 2 0 2 にコピーする。

【 0 0 5 0 】

これにより、P E I フェーズ（C A R 領域）において使用されていた共通領域情報を、P E I フェーズ（メモリ領域）や D X E フェーズや S M M フェーズ（P E I）, S M M フェーズ（D X E）においても使用（共用）することができる。

30

アクセス情報設定部 1 1 2 は、C P U 1 0 のキャッシュメモリにおける C A R 領域 1 0 1 や、R A M 2 0 における固有のメモリ領域 2 0 1 , S M M 固定のメモリ領域 2 1 1 に、共通ライブラリへのアドレス情報 1 0 4 , 2 0 4 , 2 1 2 を格納（設定）する。

【 0 0 5 1 】

具体的には、アクセス情報設定部 1 1 2 は、P E I フェーズの初期段階において、B I O S F l a s h 2 2 から P E I 用 3 2 ビットの共通ライブラリへのアドレス情報を読み出して、この読み出した共通ライブラリへのアドレス情報を、C P U 1 0 のキャッシュメモリにおける C A R 領域 1 0 1 の所定の領域に格納する。

40

ここで、共通ライブラリへのアドレス情報 1 0 4 とは、モジュールにそなえられた共通ライブラリ S L へアクセスするためのアドレス情報であり、例えば、共通ライブラリ S L へのポインタを含む。又、この共通ライブラリ S L へのポインタとしては、単なるアドレスを示すポインタ（共有情報ポインタ）の他、関数ポインタが用いられる。

【 0 0 5 2 】

また、アクセス情報設定部 1 1 2 は、R A M 2 0 が有効となった後に、B I O S F l a s h 2 2 から P E I 用 3 2 ビットの共通ライブラリへのアドレス情報 2 0 4 を読み出し、この読み出した P E I 用 3 2 ビットの共通ライブラリへのアドレス情報 2 0 4 を R A M 2 0 上の固定のメモリ領域 2 0 1 に格納する。

さらに、アクセス情報設定部 1 1 2 は、R A M 2 0 における S M M (System Managemen

50

t Mode) 領域に対しても、その特定の領域である SMM 固定のメモリ領域 2 1 1 に共通ライブラリにアドレス情報 2 1 2 の設定を行なう。

【 0 0 5 3 】

アクセス情報設定部 1 1 2 は、PEI フェーズにおいて、BIOS Flash 2 2 から D X E 用 6 4 ビットの共通ライブラリへのアドレス情報 2 1 2 を読み出し、この読み出した D X E 用 6 4 ビットの共通ライブラリへのアドレス情報 2 1 2 を SMM 固定のメモリ領域 2 1 1 に格納する。

なお、共有領域情報は、PEI 用 3 2 ビットと D X E 用 6 4 ビットとでそのまま共用可能である。

【 0 0 5 4 】

共通領域アクセス情報設定部 1 1 3 は、CPU 1 0 のキャッシュメモリにおける C A R 領域 1 0 1 や R A M 2 0 における固有のメモリ領域 2 0 1 に、共通領域へのアドレス情報 1 0 3 , 2 0 3 を格納する。

具体的には、共通領域アクセス情報設定部 1 1 3 は、PEI フェーズの初期段階において、CPU 1 0 のキャッシュメモリにおける C A R 領域 1 0 1 の所定の領域に、共通領域へのアドレス情報 1 0 3 を格納する。

【 0 0 5 5 】

ここで、共通領域へのアドレス情報 1 0 3 は、共通領域 1 0 2 へアクセスするための情報 ( 共有領域アクセス情報 ) であり、例えば、共通領域 1 0 2 における共通領域情報の格納位置を表すポインタ ( 共有情報ポインタ ) を含む。これにより、共通ライブラリ S L 1 0 3 にアクセスするモジュールは、共通領域 1 0 2 に格納された共通領域情報にアクセスすることが可能となる。

【 0 0 5 6 】

同様に、共通領域アクセス情報設定部 1 1 3 は、R A M 2 0 が使用可能となった後において、この R A M 2 0 の所定の領域に、共通領域へのアドレス情報 2 0 3 を格納する。

ここで、共通領域へのアドレス情報 2 0 3 は、共通領域 2 0 2 へアクセスするための情報である共有領域アクセス情報であり、例えば、共通領域 2 0 2 における共通領域情報の格納位置を表すポインタ ( 共有情報ポインタ ) を含む。これにより、共通ライブラリ S L 2 0 3 にアクセスするモジュールは、共通領域 2 0 2 に格納された共通領域情報にアクセスすることが可能となる。

【 0 0 5 7 】

なお、C A R 領域 1 0 1 における、共通ライブラリへのアドレス情報 1 0 4 及び共通領域へのアドレス情報 1 0 3 が格納される領域を管理領域 1 0 0 1 という場合がある。同様に、R A M 2 0 ( 固定のメモリ領域 2 0 1 ) における、共通ライブラリへのアドレス情報及び共通領域へのアドレス情報が格納される領域を管理域 2 0 0 1 という場合がある。又、R A M 2 0 の S M M ( 固定のメモリ領域 2 1 1 ) における、共通ライブラリへのアドレス情報が格納される領域を管理域 2 1 0 1 という場合がある。

【 0 0 5 8 】

情報取得部 1 1 5 は、本情報処理装置 1 0 0 の起動処理時において、PEI モジュール M や D X E ドライバ D 等のモジュールを実行する際に、共通ライブラリ S L や共通領域情報を参照・取得する。

この情報取得部 1 1 5 は、以下に詳述するように、共通インタフェースライブラリ S I や共通ライブラリへのアドレス情報 1 0 4 , 2 0 4 , 2 1 2 を用いて共通ライブラリ S L を取得する。すなわち、第 1 情報取得部として機能する。又、情報取得部 1 1 5 は、以下に詳述するように、共通インタフェースライブラリ S I や共通ライブラリへのアドレス情報 1 0 4 , 2 0 4 , 2 1 2、共通ライブラリ S L 及び共通領域へのアドレス情報 1 0 3 , 2 0 3 を用いて、共通領域 1 0 2 , 2 0 2 の共通領域情報を取得する。すなわち、第 2 情報取得部として機能する。

【 0 0 5 9 】

図 4 は実施形態の一例としての情報処理装置 1 0 0 におけるデータ参照手法を模式的に

10

20

30

40

50

示す図である。

起動処理部 11 は、共通インタフェースライブラリ S I をそなえるモジュールの実行に際して、各共通インタフェースライブラリ S I を介して、管理域 1001, 2001, 2101 にアクセスする。そして、これらの管理域 1001, 2001, 2101 に格納された共通ライブラリへのアドレス情報 104, 204, 212 や共通領域へのアドレス情報 103, 203 にアクセスする。起動処理部 11 は、これらの情報を用いて共通ライブラリ S L や共通領域情報にアクセスし、これらの情報を用いて本情報処理装置 100 の起動処理を実行する。

#### 【0060】

上述の如く構成された、実施形態の一例としての情報処理装置 100 の起動時における E F I のフェーズの処理を、図 5 に示すフローチャート（ステップ A 10 ~ A 30）に従って説明する。

本実施形態の一例としての情報処理装置 100 に電源投入（P O N : Power ON）が行なわれると、まず、S E C フェーズが行なわれた後（ステップ A 10）、P E I フェーズが行なわれ（ステップ A 20）、更に、D X E（B D S）フェーズ（ステップ A 30）が行なわれる。これらの E F I にかかる各フェーズの処理によりシステムの初期化が完了し、その後、O S ロードによる O S の起動処理が開始される。

#### 【0061】

次に、本実施形態の一例としての情報処理装置 100 における S E C フェーズの処理を、図 6 に示すフローチャート（ステップ A 101 ~ A 105）に従って説明する。

S E C フェーズにおいては、まず、C P U 10 の初期化を行なった後（ステップ A 101）、C A R 領域 101（C P U キャッシュ）の設定を行なう（ステップ A 102）。

そして、C A R 領域 101 のスタックポインタを予め規定された所定量ずらすことにより、共通ライブラリへのアドレス情報 104 や共通領域へのアドレス情報 103 及び共通領域 102 の領域を確保する（ステップ A 103）。なお、スタックポインタをずらす量は、共通ライブラリへのアドレス情報 104、共通領域へのアドレス情報 103 及び共通領域 102 のサイズに対応する。

#### 【0062】

その後、C A R 領域 101 の設定を行ない（ステップ A 104）、B I O S F l a s h 2 2 における P E I の開始アドレスを読み出し（ステップ A 105）、S E C フェーズを修了する。

次に、本実施形態の一例としての情報処理装置 100 における P E I フェーズの処理を、図 7 に示すフローチャート（ステップ A 201 ~ A 209）に従って説明する。

#### 【0063】

P E I フェーズにおいては、まず、アクセス情報設定部 112 及び共通領域アクセス情報設定部 113 が、C A R のスタック領域に P E I 用 32 ビットの共通ライブラリへのアドレス情報 104 及び共通領域へのアドレス情報 103 を設定する（ステップ A 201）。

次に、モジュール設定部 111 が、P E I モジュールを B I O S F l a s h 2 2 から読み出して C A R 領域 101 へロードし、これらの P E I モジュールをそれぞれ実行する（ステップ A 202）。これらの P E I モジュールにより R A M 20 の初期化が実行され（ステップ A 203）、R A M 20 が使用可能になる。

#### 【0064】

アクセス情報設定部 112 及び共通領域アクセス情報設定部 113 は、固定のメモリ領域 201 に、P E I 用 32 ビットの共通ライブラリへのアドレス情報 204 及び P E I 用 32 ビットの共通領域へのアドレス情報 203 を設定する（ステップ A 204）。

また、共通領域設定部 114 が、C A R 領域 101 の共通領域 102 に格納されている共通領域情報を固定のメモリ領域 201 の共通領域 202 にコピーする（ステップ A 205）。ここで、キャッシュが無効化される。

#### 【0065】

10

20

30

40

50

モジュール設定部 111 は、PEI モジュール M を RAM 20 (メモリ領域) にロードし、これらの PEI モジュール M の各処理を実行させる (ステップ A 206)。

次に、アクセス情報設定部 112 及び共通領域アクセス情報設定部 113 は、固定のメモリ領域 201 に、PEI 用 32 ビットの共通ライブラリへのアドレス情報 204 及び PEI 用 32 ビットの共通領域へのアドレス情報 203 を設定する (ステップ A 207)。

【0066】

その後、RAM 20 に D X E のメイン部分をロードし (ステップ A 208)、この RAM 20 上における D X E コアの開始アドレスを読み出して (ステップ A 209) 処理を修了する。

また、本実施形態の一例としての情報処理装置 100 における D X E (B D S) フェーズの処理を、図 8 に示すフローチャート (ステップ A 301 ~ A 302) に従って説明する。

10

【0067】

D X E (B D S) フェーズにおいては、先ず、アクセス情報設定部 112 及び共通領域アクセス情報設定部 113 が、固定のメモリ領域 201 に D X E 用 64 ビットの共通ライブラリへのアドレス情報 104 及び共通領域へのアドレス情報 103 を設定する (ステップ A 301)。

次に、モジュール設定部 111 が、D X E ドライバ D を BIOS Flash 22 から読み出して RAM 20 上にロードし、これらの各 D X E ドライバをそれぞれ実行することにより (ステップ A 302)、D X E (B D S) フェーズを完了させる。

20

【0068】

なお、図 7 に示す例においては、PEI フェーズの途中 (ステップ A 207 参照) において、固定のメモリ領域 201 に、PEI 用 32 ビットの共通ライブラリへのアドレス情報 204 及び PEI 用 32 ビットの共通領域へのアドレス情報 203 を設定しているが、これに限定されるものではない。

例えば、D X E (B D S) フェーズのステップ A 302 において D X E ドライバを RAM 20 上にロードし、これらの各 D X E ドライバをそれぞれ実行した後に行なってもよく、適宜変更して実施することができる。

【0069】

次に、本実施形態の一例としての情報処理装置 100 における PEI フェーズ (C A R 領域) での共通ライブラリ S L の読み出し手法を、図 10 を参照しながら、図 9 に示すフローチャート (ステップ B 10 ~ B 30 に従って説明する)。なお、図 10 は本情報処理装置 100 における PEI フェーズ (C A R 領域) での共通ライブラリ S L への参照経路を説明する図である。

30

【0070】

PEI フェーズ (C A R 領域) において、PEI モジュール M 12 (第 2 モジュール) が PEI モジュール M 11 (第 1 モジュール) の共通ライブラリ S L の関数を用いる例について説明する。

C A R 領域において、PEI モジュール M 12 は共通インタフェースライブラリ S I を呼び出し (ステップ B 10 : 図 10 の符号 P 01 参照)、C A R 領域 101 の共通ライブラリへのアドレス情報 104 を取得する (ステップ B 20 : 図 10 の符号 P 02 参照)。PEI モジュール M 12 は、この共通ライブラリへのアドレス情報 104 を用いて、PEI モジュール M 11 の共通ライブラリ S L の関数を呼び出す (ステップ B 30 : 図 10 の符号 P 03 参照)。

40

【0071】

このように、PEI フェーズ (C A R 領域) においては、PEI モジュール M 12 は、共通インタフェースライブラリ S I を用いて、C A R 領域 101 の共通ライブラリへのアドレス情報 104 を介して PEI モジュール M 11 の共通ライブラリ S L を読み出すことができる。又、PEI モジュール M 11 も自身がそなえる共通ライブラリ S L を用いることができる。

50

## 【 0 0 7 2 】

従って、P E I モジュール M 1 1 の共通ライブラリ S L を、P E I モジュール M 1 1 と P E I モジュール M 1 2 とによって共用することが可能となる。

次に、本実施形態の一例としての情報処理装置 1 0 0 における P E I フェーズ ( C A R 領域 ) での共通領域に格納された共通領域情報の読み出し手法を、図 1 2 を参照しながら、図 1 1 に示すフローチャート ( ステップ C 1 0 ~ C 5 0 に従って説明する ) 。なお、図 1 2 は本情報処理装置 1 0 0 における P E I フェーズ ( C A R 領域 ) での共通領域 1 0 2 への参照経路を説明する図である。

## 【 0 0 7 3 】

C A R 領域において、P E I モジュール M 1 2 ( 第 2 モジュール ) は共通インタフェースライブラリ S I を呼び出し ( ステップ C 1 0 : 図 1 2 の符号 P 1 1 参照 ) 、 C A R 領域 1 0 1 の共通ライブラリへのアドレス情報 1 0 4 を取得する ( ステップ C 2 0 : 図 1 2 の符号 P 1 2 参照 ) 。 P E I モジュール M 1 2 は、この共通ライブラリへのアドレス情報 1 0 4 を用いて、P E I モジュール M 1 1 ( 第 1 モジュール ) の共通ライブラリ S L の関数を呼び出す ( ステップ C 3 0 : 図 1 2 の符号 P 1 3 参照 ) 。

10

## 【 0 0 7 4 】

P E I モジュール M 1 2 は、この共通ライブラリ S L から、C A R 領域 1 0 1 の共通領域へのアドレス情報 1 0 3 へアクセスするための情報 ( 例えば、ポインタ ) を取得し、この情報に基づいて C A R 領域 1 0 1 の共通領域へのアドレス情報 1 0 3 を取得する ( ステップ C 4 0 : 図 1 2 の符号 P 1 4 参照 ) 。 P E I モジュール M 1 2 は、この共通領域へのアドレス情報 1 0 3 を用いて、C A R 領域 1 0 1 の共通領域 1 0 2 にアクセスし ( ステップ C 5 0 : 図 1 2 の符号 P 1 5 参照 ) 、この共通領域 1 0 2 に格納されている共通領域情報を取得する。

20

## 【 0 0 7 5 】

このように、P E I フェーズ ( C A R 領域 ) においては、P E I モジュール M 1 2 は、共通インタフェースライブラリ S I を用いて、C A R 領域 1 0 1 の共通ライブラリへのアドレス情報 1 0 4 を介して P E I モジュール M 1 1 の共通ライブラリ S L を読み出す。更に、この共通ライブラリ S L を用いて C A R 領域 1 0 1 の共通領域へのアドレス情報 1 0 3 を取得し、この共通領域へのアドレス情報 1 0 3 を用いて共通領域情報を取得することができる。

30

## 【 0 0 7 6 】

また、P E I モジュール M 1 1 も自身がそなえる共通ライブラリ S L を用いて、C A R 領域 1 0 1 の共通領域へのアドレス情報 1 0 3 を取得し、この共通領域へのアドレス情報 1 0 3 を用いて共通領域情報を取得することができる。

従って、C A R 領域 1 0 1 の共通領域 1 0 2 の共通領域情報を、P E I モジュール M 1 1 と P E I モジュール M 1 2 とによって共用することが可能となる。

## 【 0 0 7 7 】

次に、本実施形態の一例としての情報処理装置 1 0 0 における P E I フェーズ ( メモリ領域 ) での共通ライブラリ S L の読み出し手法を、図 1 4 を参照しながら、図 1 3 に示すフローチャート ( ステップ D 1 0 ~ D 3 0 に従って説明する ) 。なお、図 1 4 は本情報処理装置 1 0 0 における P E I フェーズ ( メモリ領域 ) での共通ライブラリ S L への参照経路を説明する図である。

40

## 【 0 0 7 8 】

P E I フェーズ ( メモリ領域 ) において、P E I モジュール M 2 2 ( 第 2 モジュール ) が P E I モジュール M 2 1 ( 第 1 モジュール ) の共通ライブラリ S L の関数を用いる例について説明する。

メモリ領域において、P E I モジュール M 2 2 は共通インタフェースライブラリ S I を呼び出し ( ステップ D 1 0 : 図 1 4 の符号 P 3 1 参照 ) 、固有のメモリ領域 2 0 1 の共通ライブラリへのアドレス情報 2 0 4 を取得する ( ステップ D 2 0 : 図 1 4 の符号 P 3 2 参照 ) 。 P E I モジュール M 2 2 は、この共通ライブラリへのアドレス情報 2 0 4 を用いて

50



、 P E I モジュール M 2 1 の共通ライブラリ S L の関数を呼び出す（ステップ D 3 0 : 図 1 4 の符号 P 3 3 参照）。

【 0 0 7 9 】

このように、 P E I フェーズ（メモリ領域）においても、 P E I モジュール M 2 2 は、共通インタフェースライブラリ S I を用いて、固有のメモリ領域 2 0 1 の共通ライブラリへのアドレス情報 2 0 4 を介して P E I モジュール M 2 1 の共通ライブラリ S L を読み出すことができる。又、 P E I モジュール M 2 1 も自身がそなえる共通ライブラリ S L を用いることができる。

従って、 P E I モジュール M 2 1 の共通ライブラリ S L を、 P E I モジュール M 2 1 と P E I モジュール M 2 2 とによって共用することが可能となる。

10

【 0 0 8 0 】

次に、本実施形態の一例としての情報処理装置 1 0 0 における P E I フェーズ（メモリ領域）での共通領域 2 0 2 に格納された共通領域情報の読み出し手法を、図 1 6 を参照しながら、図 1 5 に示すフローチャート（ステップ E 1 0 ~ E 5 0 に従って説明する）。なお、図 1 6 は本情報処理装置 1 0 0 における P E I フェーズ（メモリ領域）での共通領域 2 0 2 への参照経路を説明する図である。

【 0 0 8 1 】

メモリ領域において、 P E I モジュール M 2 2 （第 2 モジュール）は共通インタフェースライブラリ S I を呼び出し（ステップ E 1 0 : 図 1 6 の符号 P 4 1 参照）、固有のメモリ領域 2 0 1 の共通ライブラリへのアドレス情報 2 0 4 を取得する（ステップ E 2 0 : 図 1 6 の符号 P 4 2 参照）。 P E I モジュール M 2 2 は、この共通ライブラリへのアドレス情報 2 0 4 を用いて、 P E I モジュール M 2 1 （第 1 モジュール）の共通ライブラリ S L を呼び出す（ステップ E 3 0 : 図 1 6 の符号 P 4 3 参照）。

20

【 0 0 8 2 】

P E I モジュール M 2 2 は、この共通ライブラリ S L から、固有のメモリ領域 2 0 1 の共通領域へのアドレス情報 2 0 3 へアクセスするための情報（例えば、ポインタ）を取得し、この情報に基づいて固定のメモリ領域 2 0 1 の共通領域へのアドレス情報 2 0 3 を取得する（ステップ E 4 0 : 図 1 6 の符号 P 4 4 参照）。 P E I モジュール M 2 2 は、この共通領域へのアドレス情報 2 0 3 を用いて、固有のメモリ領域 2 0 1 の共通領域 2 0 2 にアクセスし（ステップ E 5 0 : 図 1 6 の符号 P 4 5 参照）、この共通領域 2 0 2 に格納されている共通領域情報を取得する。

30

【 0 0 8 3 】

このように、 P E I フェーズ（メモリ領域）においても、 P E I モジュール M 2 2 は、共通インタフェースライブラリ S I を用いて、固有のメモリ領域 2 0 1 の共通ライブラリへのアドレス情報 2 0 4 を介して P E I モジュール M 2 1 の共通ライブラリ S L を読み出す。更に、この共通ライブラリ S L を用いて固有のメモリ領域 2 0 1 の共通領域へのアドレス情報 2 0 3 を取得し、この共通領域へのアドレス情報 2 0 3 を用いて共通領域情報を取得することができる。

【 0 0 8 4 】

また、 P E I モジュール M 2 1 も自身がそなえる共通ライブラリ S L を用いて、固有のメモリ領域 2 0 1 の共通領域へのアドレス情報 2 0 3 を取得し、この共通領域へのアドレス情報 2 0 3 を用いて共通領域情報を取得することができる。

40

従って、固有のメモリ領域 2 0 1 の共通領域 2 0 2 の共通領域情報を、 P E I モジュール M 2 1 と P E I モジュール M 2 2 とによって共用することが可能となる。

【 0 0 8 5 】

次に、本実施形態の一例としての情報処理装置 1 0 0 における D X E フェーズ（メモリ領域）での共通ライブラリ S L の読み出し手法を、図 1 8 を参照しながら、図 1 7 に示すフローチャート（ステップ F 1 0 ~ F 3 0 に従って説明する）。なお、図 1 8 は本情報処理装置 1 0 0 における D X E フェーズ（メモリ領域）での共通ライブラリ S L への参照経路を説明する図である。

50

## 【0086】

D X Eフェーズ（メモリ領域）において、D X EドライバD 2（第2モジュール）がD X EドライバD 1（第1モジュール）の共通ライブラリS Lの関数を用いる例について説明する。

メモリ領域において、D X EドライバD 2は共通インタフェースライブラリS Iを呼び出し（ステップF 10：図18の符号P 51参照）、固有のメモリ領域201の共通ライブラリへのアドレス情報204を取得する（ステップF 20：図18の符号P 52参照）。D X EドライバD 2は、この共通ライブラリへのアドレス情報204を用いて、D X EドライバD 1の共通ライブラリS Lの関数を呼び出す（ステップF 30：図18の符号P 53参照）。

10

## 【0087】

このように、D X Eフェーズ（メモリ領域）においても、D X EドライバD 2は、共通インタフェースライブラリS Iを用いて、固有のメモリ領域201の共通ライブラリへのアドレス情報204を介してD X EドライバD 1の共通ライブラリS Lを読み出すことができる。又、D X EドライバD 1も自身がそなえる共通ライブラリS Lを用いることができる。

従って、D X EドライバD 1の共通ライブラリS Lを、D X EドライバD 1とD X EドライバD 2とによって共用することが可能となる。

## 【0088】

次に、本実施形態の一例としての情報処理装置100におけるD X Eフェーズ（メモリ領域）での共通領域202に格納された共通領域情報の読み出し手法を、図20を参照しながら、図19に示すフローチャート（ステップG 10～G 50に従って説明する）。なお、図20は本情報処理装置100におけるD X Eフェーズ（メモリ領域）での共通領域202への参照経路を説明する図である。

20

## 【0089】

メモリ領域において、D X EドライバD 2（第2モジュール）は共通インタフェースライブラリS Iを呼び出し（ステップG 10：図20の符号P 61参照）、固有のメモリ領域201の共通ライブラリへのアドレス情報204を取得する（ステップG 20：図20の符号P 62参照）。D X EドライバD 2は、この共通ライブラリへのアドレス情報204を用いて、D X EドライバD 1（第1モジュール）の共通ライブラリS Lを呼び出す（ステップG 30：図20の符号P 63参照）。

30

## 【0090】

D X EドライバD 2は、この共通ライブラリS Lから、固有のメモリ領域201の共通領域へのアドレス情報203へアクセスするための情報（例えば、ポインタ）を取得し、この情報に基づいて固定のメモリ領域201の共通領域へのアドレス情報203を取得する（ステップG 40：図20の符号P 64参照）。D X EドライバD 2は、この共通領域へのアドレス情報203を用いて、固有のメモリ領域201の共通領域202にアクセスし（ステップG 50：図20の符号P 65参照）、この共通領域202に格納されている共通領域情報を取得する。

## 【0091】

このように、D X Eフェーズ（メモリ領域）においても、D X EドライバD 2は、共通インタフェースライブラリS Iを用いて、固有のメモリ領域201の共通ライブラリへのアドレス情報204を介してD X EドライバD 1の共通ライブラリS Lを読み出す。更に、この共通ライブラリS Lを用いて固有のメモリ領域201の共通領域へのアドレス情報203を取得し、この共通領域へのアドレス情報203を用いて共通領域情報を取得することができる。

40

## 【0092】

また、D X EドライバD 1も自身がそなえる共通ライブラリS Lを用いて、固有のメモリ領域201の共通領域へのアドレス情報203を取得し、この共通領域へのアドレス情報203を用いて共通領域情報を取得することができる。

50

従って、固有のメモリ領域 201 の共通領域 202 の共通領域情報を、D X Eドライバ D1 と D X Eドライバ D2 とによって共用することが可能となる。

【0093】

次に、本実施形態の一例としての情報処理装置 100 における SMM フェーズ ( P E I , D X E ) での共通ライブラリ S L の読み出し手法を、図 22 を参照しながら、図 21 に示すフローチャート ( ステップ H10 ~ H30 に従って説明する )。なお、図 22 は本情報処理装置 100 における SMM フェーズ ( P E I ) 及び SMM フェーズ ( D X E ) での共通ライブラリ S L への参照経路を説明する図である。

【0094】

ここでは、便宜上、SMM フェーズ ( P E I ) において、P E I モジュール M24 ( 第 2 モジュール ) が P E I モジュール M23 ( 第 1 モジュール ) の共通ライブラリ S L の関数を用いる例と、SMM フェーズ ( D X E ) において、D X Eドライバ D4 ( 第 2 モジュール ) が D X Eドライバ D3 ( 第 1 モジュール ) の共通ライブラリ S L の関数を用いる例とをまとめて説明する。

10

【0095】

SMM 領域において、P E I モジュール M24 は共通インタフェースライブラリ S I を呼び出し ( ステップ H10 : 図 22 の符号 P81 参照 )、SMM 固定のメモリ領域 211 の共通ライブラリへのアドレス情報 212 を取得する ( ステップ H20 : 図 22 の符号 P82 参照 )。P E I モジュール M24 は、この共通ライブラリへのアドレス情報 212 を用いて、P E I モジュール M23 の共通ライブラリ S L の関数を呼び出す ( ステップ H30 : 図 22 の符号 P83 参照 )。

20

【0096】

同様に、SMM 領域において、D X Eドライバ D4 は共通インタフェースライブラリ S I を呼び出し ( ステップ H10 : 図 22 の符号 P71 参照 )、SMM 固定のメモリ領域 211 の共通ライブラリへのアドレス情報 212 を取得する ( ステップ H20 : 図 22 の符号 P72 参照 )。D X Eドライバ D4 は、この共通ライブラリへのアドレス情報 212 を用いて、D X Eドライバ D3 の共通ライブラリ S L の関数を呼び出す ( ステップ H30 : 図 22 の符号 P73 参照 )。

【0097】

このように、SMM フェーズ ( P E I ) 及び SMM フェーズ ( D X E ) のいずれにおいても、P E I モジュール M24 や D X Eドライバ D4 は、共通インタフェースライブラリ S I を用いて、固有のメモリ領域 211 の共通ライブラリへのアドレス情報 212 を介して P E I モジュール M23 や D X Eドライバ D3 の共通ライブラリ S L を読み出すことができる。

30

【0098】

また、P E I モジュール M23 や D X Eドライバ D3 も自身がそなえる共通ライブラリ S L を用いることができる。

従って、P E I モジュール M23 の共通ライブラリ S L を、P E I モジュール M23 と P E I モジュール M24 とによって共用することが可能となり、又、D X Eドライバ D3 の共通ライブラリ S L を、D X Eドライバ D3 と D X Eドライバ D4 とによって共用することが可能となる。

40

【0099】

次に、本実施形態の一例としての情報処理装置 100 における SMM フェーズ ( P E I , D X E ) での共通領域 202 に格納された共通領域情報の読み出し手法を、図 24 及び図 25 を参照しながら、図 23 に示すフローチャート ( ステップ J10 ~ J50 に従って説明する )。なお、図 24 は本情報処理装置 100 における SMM フェーズ ( P E I ) での共通領域 202 への参照経路を説明する図、図 25 は本情報処理装置 100 における SMM フェーズ ( D X E ) での共通領域 202 への参照経路を説明する図である。

【0100】

SMM 領域において、P E I モジュール M24 ( 第 2 モジュール ) や D X Eドライバ D

50

4 (第2モジュール)はそれぞれ共通インタフェースライブラリS Iを呼び出し(ステップJ 10:図24の符号P 91及び図25の符号P 101参照)、SMM固有のメモリ領域211の共通ライブラリへのアドレス情報212を取得する(ステップJ 20:図24の符号P 92及び図25の符号P 102参照)。

【0101】

PEIモジュールM 24やDXEドライバD 4は、この共通ライブラリへのアドレス情報212を用いて、PEIモジュールM 23(第1モジュール)やDXEドライバD 3(第1モジュール)の共通ライブラリS Lを呼び出す(ステップJ 30:図24の符号P 93及び図25の符号P 103参照)。

PEIモジュールM 24やDXEドライバD 4は、この共通ライブラリS Lから、固有のメモリ領域201の共通領域へのアドレス情報203へアクセスするための情報(例えば、ポインタ)を取得し、この情報に基づいて固有のメモリ領域201の共通領域へのアドレス情報203を取得する(ステップJ 40:図24の符号P 94及び図25の符号P 104参照)。PEIモジュールM 24やDXEドライバD 4は、この共通領域へのアドレス情報203を用いて、固有のメモリ領域201の共通領域202にアクセスし(ステップJ 50:図24の符号P 95及び図25の符号P 105参照)、この共通領域202に格納されている共通領域情報を取得する。

【0102】

このように、SMMフェーズ(PEI)やSMMフェーズ(DXE)においても、PEIモジュールM 24やDXEドライバD 4は、共通インタフェースライブラリS Iを用いて、固有のメモリ領域201の共通ライブラリへのアドレス情報204を介してPEIモジュールM 23やDXEドライバD 3の共通ライブラリS Lを読み出す。更に、この共通ライブラリS Lを用いて固有のメモリ領域201の共通領域へのアドレス情報203を取得し、この共通領域へのアドレス情報103を用いて共通領域情報を取得することができる。

【0103】

また、PEIモジュールM 23やDXEドライバD 3も、各自がそなえる共通ライブラリS Lを用いて、固有のメモリ領域201の共通領域へのアドレス情報203を取得し、この共通領域へのアドレス情報203を用いて、それぞれ共通領域情報を取得することができる。

従って、固有のメモリ領域201の共通領域202の共通領域情報を、PEIモジュールM 23とPEIモジュールM 24とや、DXEドライバD 3とDXEドライバD 4とで共有することが可能となる。

【0104】

なお、本実施形態においては、PEIモジュールM 12, M 22, M 24やDXEドライバD 2, D 4が、共通インタフェースライブラリS Iを用いて、共通ライブラリS Lや共通領域情報を取得している。すなわち、これらのPEIモジュールM 12, M 22, M 24やDXEドライバD 2, D 4を実行することにより、前述した情報取得部115としての機能が実現されるといえる。

【0105】

このように、実施形態の一例としての情報処理装置によれば、PEIモジュールM 11が自身がそなえる共通ライブラリS Lを用いることができる。その一方で、PEIモジュールM 12が、共通インタフェースライブラリS I及び共通ライブラリへのアドレス情報104を介して、PEIモジュールM 11の共通ライブラリS Lを用いることができる。

同様にして、PEIモジュールM 21, M 23やDXEドライバD 1, D 3が、それぞれがそなえる共通ライブラリS Lを使用できる。その一方で、PEIモジュールM 22がPEIモジュールM 21の共通ライブラリS Lを、又、PEIモジュールM 24がPEIモジュールM 23の共通ライブラリS Lを用いることができる。更に、DXEドライバD 2がDXEドライバD 3の共通ライブラリS Lを、又、DXEドライバD 4がDXEドライバD 3の共通ライブラリS Lをそれぞれ用いることができる。

## 【0106】

すなわち、共通インタフェースライブラリS Iをそなえるモジュールが、他のモジュールにそなえられた共通ライブラリS Lを使用することができ、共通ライブラリS Lを共用することができる。これにより、各モジュールやプログラムデータPのサイズを小さくすることができ、モジュールがロードされるプロセッサキャッシュやRAM 20のサイズや、プログラムデータPを格納するBIOS Flash 22の容量を小さく構成することができる。従って、処理速度の向上や製造コストを低減することができる。

## 【0107】

また、PEIモジュールM 11が自身がそなえる共通ライブラリS Lを用いて共通領域102の共通領域情報を用いることができる。その一方で、PEIモジュールM 12が、共通インタフェースライブラリS I、共通ライブラリS L及び共通領域へのアドレス情報103を用いて共通領域102の共通領域情報を用いることができる。

10

同様に、PEIモジュールM 21、M 23やDXEドライバD 1、D 3が、それぞれがそなえる共通ライブラリS Lを用いて、固定のメモリ領域201の共通領域へのアドレス情報203を介して共通領域202の共通領域情報を使用できる。その一方で、PEIモジュールM 22がPEIモジュールM 21の共通ライブラリS Lを、又、PEIモジュールM 24がPEIモジュールM 23の共通ライブラリS Lを用いて、固定のメモリ領域201の共通領域へのアドレス情報203を介して共通領域202の共通領域情報を使用できる。更に、DXEドライバD 2がDXEドライバD 3の共通ライブラリS Lを、又、DXEドライバD 4がDXEドライバD 3の共通ライブラリS Lをそれぞれ用いて、固定のメモリ領域201の共通領域へのアドレス情報203を介して共通領域202の共通領域情報を使用できる。

20

## 【0108】

従って、複数のモジュールが共通領域102や共通領域202の共通領域情報を使用することができ、これらの共通領域情報を共用することができる。これによっても、各モジュールやプログラムデータPのサイズを小さくすることができ、モジュールがロードされるプロセッサキャッシュやRAM 20のサイズや、プログラムデータPを格納するBIOS Flash 22の容量を小さく構成することができる。従って、処理速度の向上や製造コストを低減することができる。

## 【0109】

また、固定のメモリ領域201に共通領域情報を格納する共通領域202をそなえ、PEIモジュールM 21～M 24やDXEドライバD 1～D 4が、それぞれ、この共通領域202の共通領域情報を使用できる。これにより、PEIフェーズとDXEフェーズという異なるフェーズのモジュールで共通領域情報を共用することができ、処理速度の向上や製造コストを低減することができる他、利便性が向上する。

30

## 【0110】

また、共通領域設定部114が、CAR領域101の共通領域102に格納されている共通領域情報を固有のメモリ領域201の共通領域202にコピーすることにより、PEIフェーズ(CAR領域)において使用されていた共通領域情報を、PEIフェーズ(メモリ領域)やDXEフェーズやSMMフェーズ(PEI)、SMMフェーズ(DXE)においても使用(共用)することができ、利便性が向上する。

40

## 【0111】

そして、開示の技術は上述した実施形態に限定されるものではなく、本実施形態の趣旨を逸脱しない範囲で種々変形して実施することができる。

例えば、上述した実施形態においては、PEIモジュールM 11、M 21、M 23やDXEドライバD 1、D 3に共通ライブラリS Lをそなえ、PEIモジュールM 12、M 22、M 24やDXEドライバD 2、D 4に共通インタフェースライブラリS Iをそなえているが、これに限定されるものではない。すなわち、複数のモジュールのうち、どのモジュールに共通ライブラリS Lをそなえてもよく、又、同様に、どのモジュールに共通インタフェースライブラリS Iをそなえてもよい。又、同一のモジュールに共通ライブラリS

50

Lと他のモジュールの共通ライブラリSLを参照するための共通インタフェースライブラリSIとの両方をそなえてもよく、種々変形して実施することができる。

【0112】

また、上述した実施形態においては、PEIフェーズ(CAR領域)、PEIフェーズ(メモリ領域)、SMMフェーズ(PEI)及びSMMフェーズ(DXE)の各フェーズにおいて、それぞれ2つのモジュールで共通ライブラリSLや共通領域情報を共有する例を示しているが、これに限定されるものではない。すなわち、3以上のモジュールで共通ライブラリSLや共通領域情報を共有してもよく、各モジュールの数は適宜変更して実施することができる。

【0113】

さらに、上述した実施形態においては、プロセッサとしてCPU10をそなえ、このCPU10において起動処理部11としての各種機能を実現しているが、これに限定されるものではなく、例えば、MPU(Micro-Processing Unit)等、他のプロセッサを用いてもよい。

また、上述した開示により本実施形態を当業者によって実施・製造することが可能である。

【0114】

以上の実施形態に関し、更に以下の付記を開示する。

(付記1)

プロセッサをそなえた情報処理装置の起動処理方法であって、  
該プロセッサにより実行されることにより当該情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードするステップと、

該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するステップと、

該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードするステップと、

該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得するステップとをそなえることを特徴とする、起動処理方法。

【0115】

(付記2)

該記憶領域に、2以上のモジュールにより共通に用いられる第2共通情報を格納する共通領域を形成するステップと、

該記憶領域に、該共通領域へアクセスするための共通領域アクセス情報を格納するステップと、

該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、アクセスした当該アクセス情報を用いて該第1共通情報にアクセスし、アクセスした当該第1共通情報に基づいて該共通領域アクセス情報にアクセスし、アクセスした当該共通領域アクセス情報を用いて、該共通領域に格納された該第2共通情報を取得するステップとをそなえることを特徴とする、付記1記載の起動処理方法。

【0116】

(付記3)

該起動処理が複数のフェーズをそなえ、

該複数のフェーズのうち一のフェーズにおいて、該プロセッサのプロセッサキャッシュを該記憶領域として用い、

該情報処理装置の主記憶装置が使用可能な状態となった後に、該プロセッサキャッシュに格納されている該第2共通情報を該主記憶装置に複製するステップをそなえることを特徴とする、付記2記載の起動処理方法。

【0117】

## (付記4)

プロセッサをそなえた情報処理装置であって、

起動処理時に、該プロセッサにより実行されることにより当該情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードする第1モジュール設定部と、

起動処理時に、該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するアクセス情報設定部と、

起動処理時に、該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードする第2モジュール設定部と、

該起動処理時に、該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得する第1情報取得部とをそなえることを特徴とする、情報処理装置。

10

## 【0118】

## (付記5)

該起動処理時に、該記憶領域に、2以上のモジュールにより共通に用いられる第2共通情報を格納する共通領域を形成する共通領域設定部と、

該起動処理時に、該記憶領域に、該共通領域へアクセスするための共通領域アクセス情報を格納する共通領域アクセス情報設定部と、

該起動処理時に、該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、アクセスした当該アクセス情報を用いて該第1共通情報にアクセスし、アクセスした当該第1共通情報に基づいて該共通領域アクセス情報にアクセスし、アクセスした当該共通領域アクセス情報を用いて、該共通領域に格納された該第2共通情報を取得する第2情報取得部とをそなえることを特徴とする、付記4記載の情報処理装置。

20

## 【0119】

## (付記6)

該起動処理が複数のフェーズをそなえ、

該複数のフェーズのうち一のフェーズにおいて、該プロセッサのプロセッサキャッシュを該記憶領域として用い、

該共通領域設定部が、該情報処理装置の主記憶装置が使用可能な状態となった後に、該プロセッサキャッシュに格納されている該第2共通情報を該主記憶装置に複写することを特徴とする、付記5記載の情報処理装置。

30

## 【0120】

## (付記7)

起動処理をコンピュータに実行させるための起動処理プログラムであって、

該コンピュータに実行されることにより情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2以上のモジュールにより共通に用いられる第1共通情報をそなえる第1モジュールをロードするステップと、

該情報処理装置にそなえられた記憶領域に、該第1共通情報へアクセスするためのアクセス情報を格納するステップと、

該アクセス情報にアクセスするためのインタフェース情報をそなえる第2モジュールをロードするステップと、

該第2モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第1共通情報を取得するステップとを、該コンピュータに実行させることを特徴とする、起動処理プログラム。

40

## 【0121】

## (付記8)

該記憶領域に、2以上のモジュールにより共通に用いられる第2共通情報を格納する共通領域を形成するステップと、

該記憶領域に、該共通領域へアクセスするための共通領域アクセス情報を格納するステップと、

50

該第 2 モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、アクセスした当該アクセス情報を用いて該第 1 共通情報にアクセスし、アクセスした当該第 1 共通情報に基づいて該共通領域アクセス情報にアクセスし、アクセスした当該共通領域アクセス情報を用いて、該共通領域に格納された該第 2 共通情報を取得するステップとを、該コンピュータに実行させることを特徴とする、付記 7 記載の起動処理プログラム。

【 0 1 2 2 】

( 付記 9 )

該起動処理が複数のフェーズをそなえ、  
該複数のフェーズのうち一のフェーズにおいて、該プロセッサのプロセッサキャッシュを該記憶領域として用い、  
該情報処理装置の主記憶装置が使用可能な状態となった後に、該プロセッサキャッシュに格納されている該第 2 共通情報を該主記憶装置に複写するステップを該コンピュータに実行させることを特徴とする、付記 8 記載の起動処理プログラム。 10

【 0 1 2 3 】

( 付記 1 0 )

起動処理をコンピュータに実行させるための起動処理プログラムを記録したコンピュータ読取可能な記録媒体であって、  
該起動処理プログラムが、  
該コンピュータに実行されることにより情報処理装置の起動プロセスの一部を実現する複数のモジュールのうち、2 以上のモジュールにより共通に用いられる第 1 共通情報をそなえる第 1 モジュールをロードするステップと、  
該情報処理装置にそなえられた記憶領域に、該第 1 共通情報へアクセスするためのアクセス情報を格納するステップと、  
該アクセス情報にアクセスするためのインタフェース情報をそなえる第 2 モジュールをロードするステップと、  
該第 2 モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、該アクセス情報を介して該第 1 共通情報を取得するステップとを、該コンピュータに実行させることを特徴とする、起動処理プログラムを記録したコンピュータ読取可能な記録媒体。 20 30

【 0 1 2 4 】

( 付記 1 1 )

該起動処理プログラムが、  
該記憶領域に、2 以上のモジュールにより共通に用いられる第 2 共通情報を格納する共通領域を形成するステップと、  
該記憶領域に、該共通領域へアクセスするための共通領域アクセス情報を格納するステップと、  
該第 2 モジュールにより、該インタフェース情報によって該アクセス情報にアクセスし、アクセスした当該アクセス情報を用いて該第 1 共通情報にアクセスし、アクセスした当該第 1 共通情報に基づいて該共通領域アクセス情報にアクセスし、アクセスした当該共通領域アクセス情報を用いて、該共通領域に格納された該第 2 共通情報を取得するステップとを、該コンピュータに実行させることを特徴とする、付記 1 0 記載の起動処理プログラムを記録したコンピュータ読取可能な記録媒体。 40

【 0 1 2 5 】

( 付記 1 2 )

該起動処理が複数のフェーズをそなえ、  
該起動処理プログラムが、  
該複数のフェーズのうち一のフェーズにおいて、プロセッサキャッシュを該記憶領域として用い、  
該情報処理装置の主記憶装置が使用可能な状態となった後に、該プロセッサキャッシュ 50



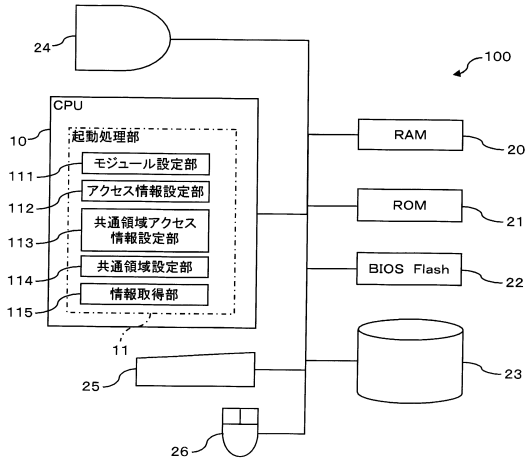
に格納されている該第2共通情報を該主記憶装置に複写するステップを該コンピュータに実行させることを特徴とする、付記1記載の起動処理プログラムを記録したコンピュータ読取可能な記録媒体。

【符号の説明】

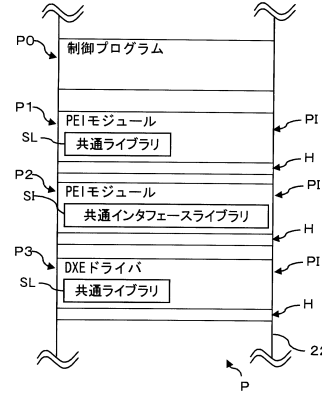
【0126】

10	CPU (プロセッサ)	
11	起動処理部	
20	RAM	
21	ROM	
22	BIOS Flash	10
23	ストレージ	
24	ディスプレイ	
100	情報処理装置	
101	CAR領域 (記憶領域)	
102	共通領域	
103, 203	共通領域へのアドレス情報 (共通領域アクセス情報)	
104, 204, 212	共通ライブラリへのアドレス情報 (アクセス情報)	
111	モジュール設定部 (第1モジュール設定部, 第2モジュール設定部)	
112	アクセス情報設定部	
113	共通領域アクセス情報設定部	20
114	共通領域設定部	
115	情報取得部 (第1情報取得部, 第2情報取得部)	
201	固定のメモリ領域 (記憶領域)	
211	SMM固定のメモリ領域	
301, 311	SMM領域	
1001, 2001, 2101	管理域	
D, D1~D4	DEXドライバ (モジュール)	
H	ヘッド	
M, M11, M12, M21~M24	PEIモジュール (モジュール)	
P	プログラムデータ	30
P1~P3	モジュールプログラム	
PI	実行可能イメージ	
SL	共通ライブラリ (第1共通情報)	
SI	共通インタフェースライブラリ (インタフェース情報)	

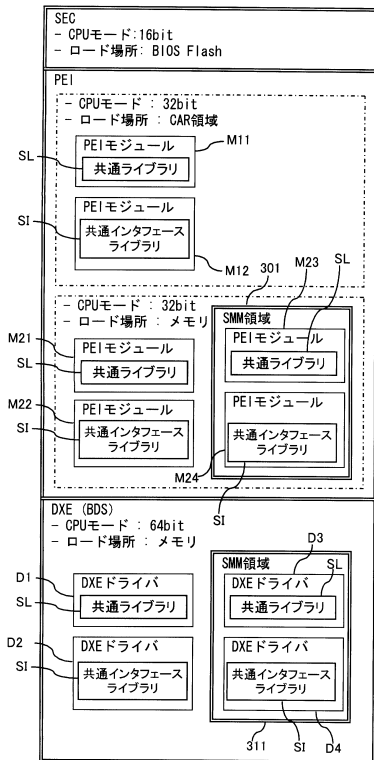
【図1】



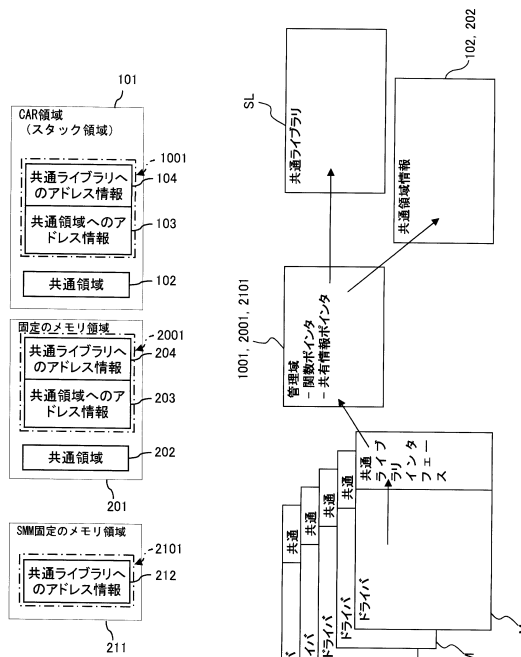
【図2】



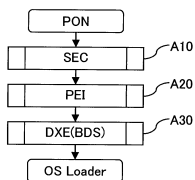
【図3】



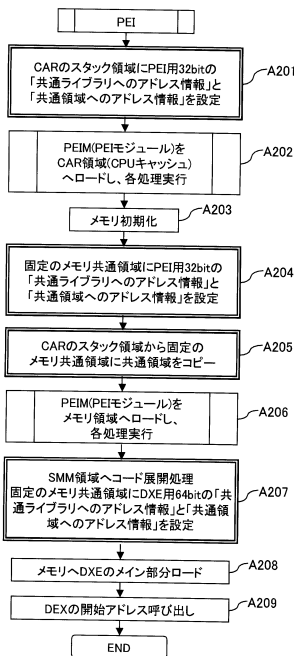
【図4】



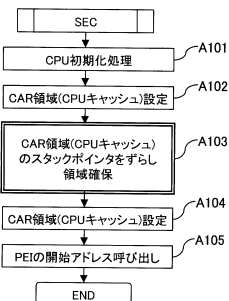
【図5】



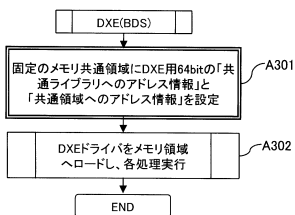
【図7】



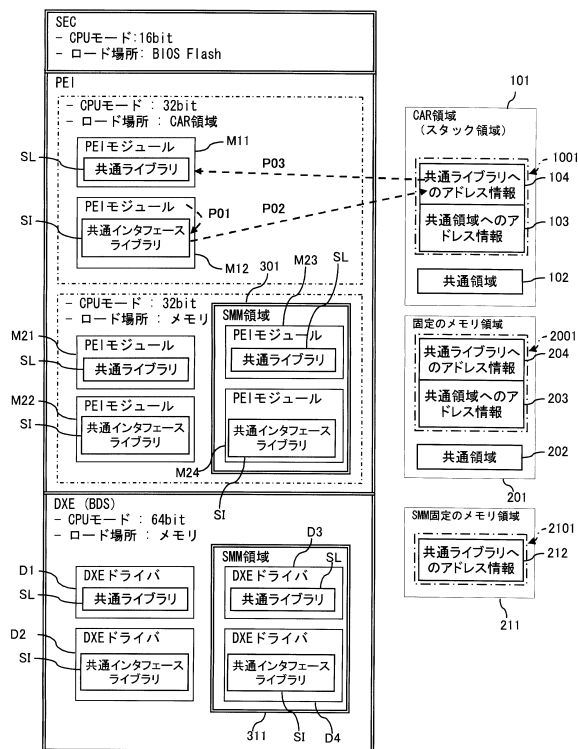
【図6】



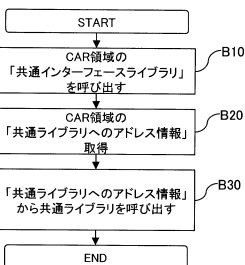
【図8】



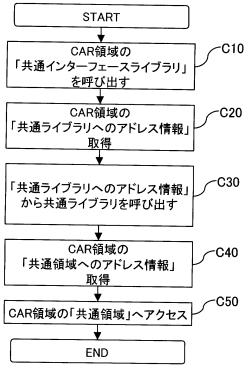
【図10】



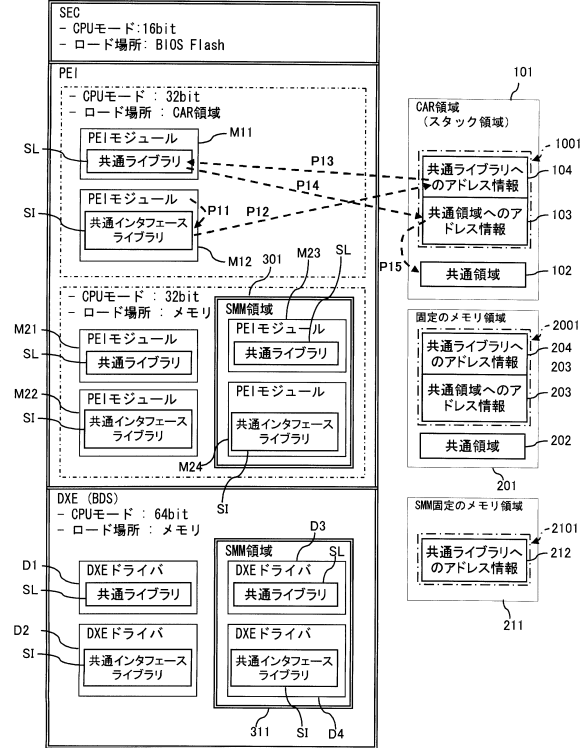
【図9】



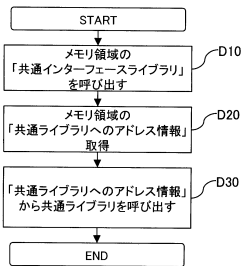
【図 1 1】



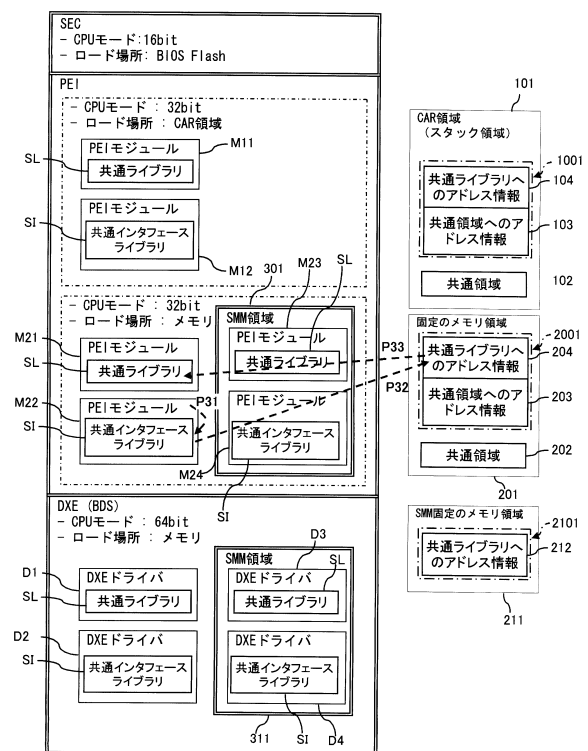
【図 1 2】



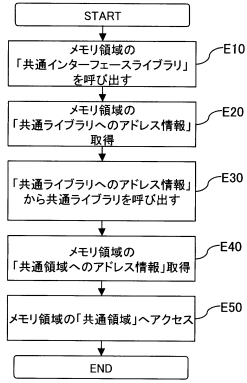
【図 1 3】



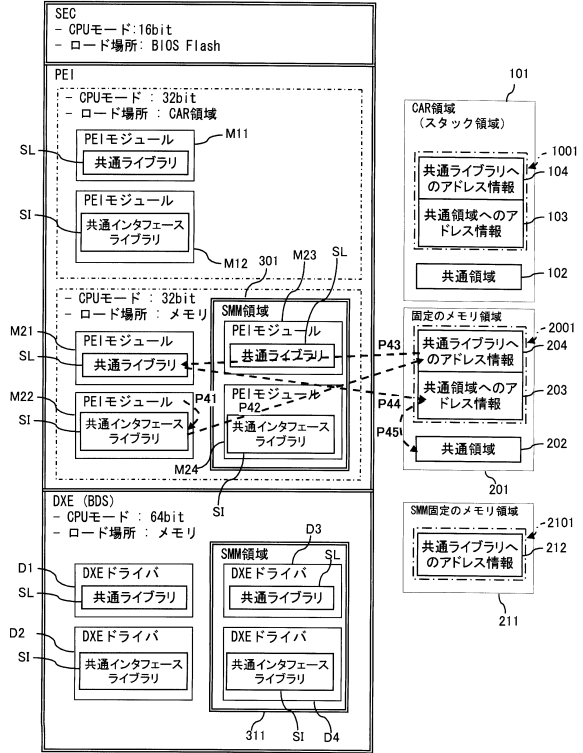
【図 1 4】



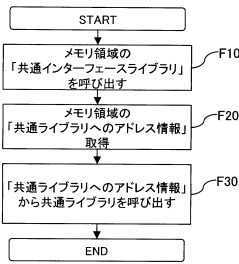
【図15】



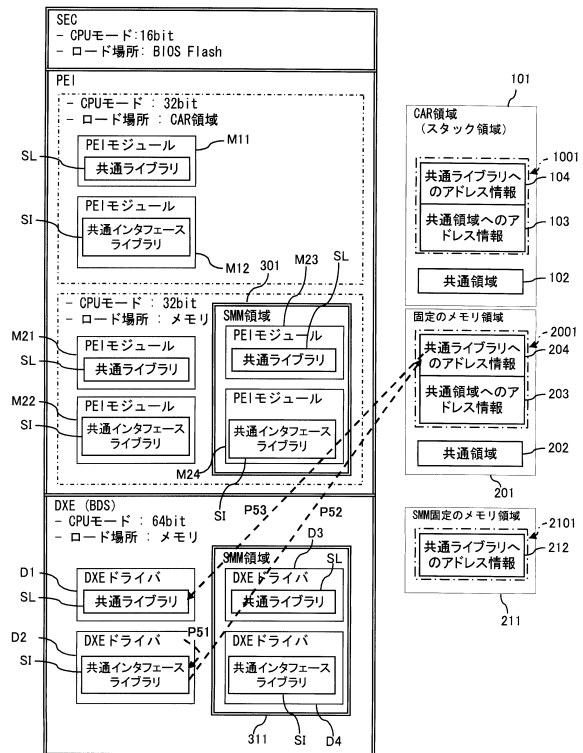
【図16】



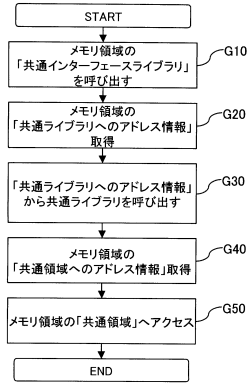
【図17】



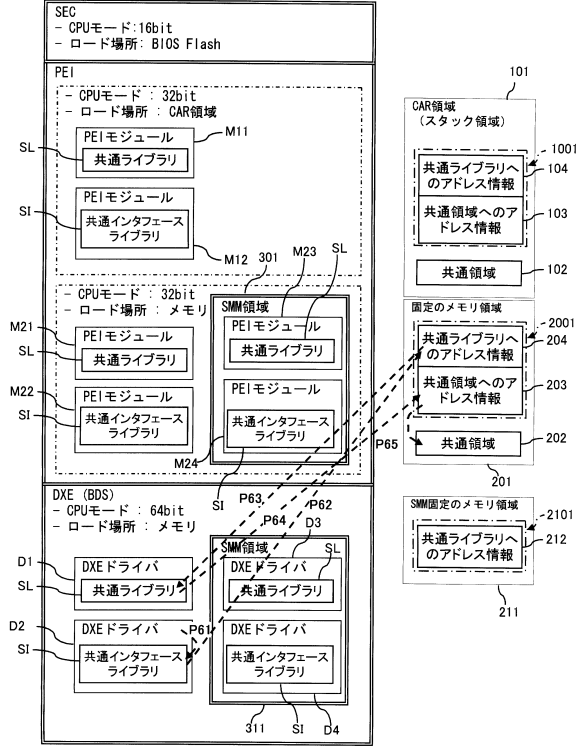
【図18】



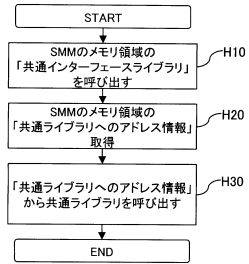
【図19】



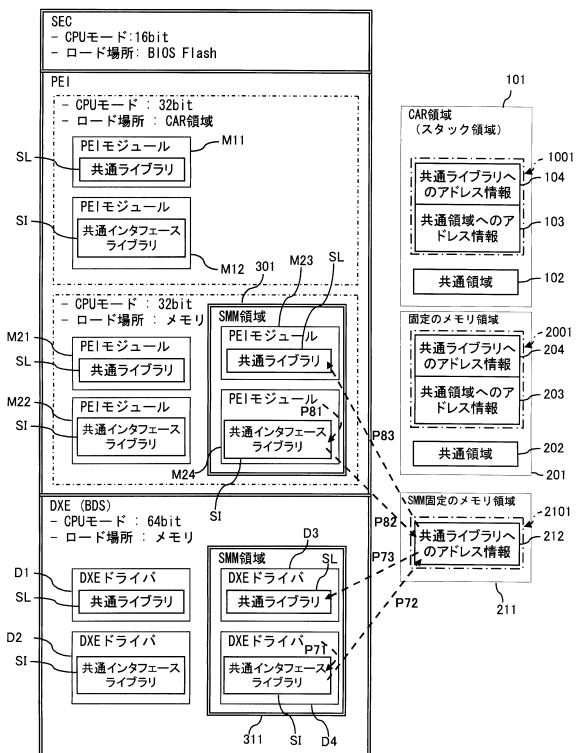
【図20】



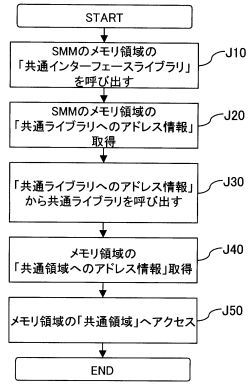
【図21】



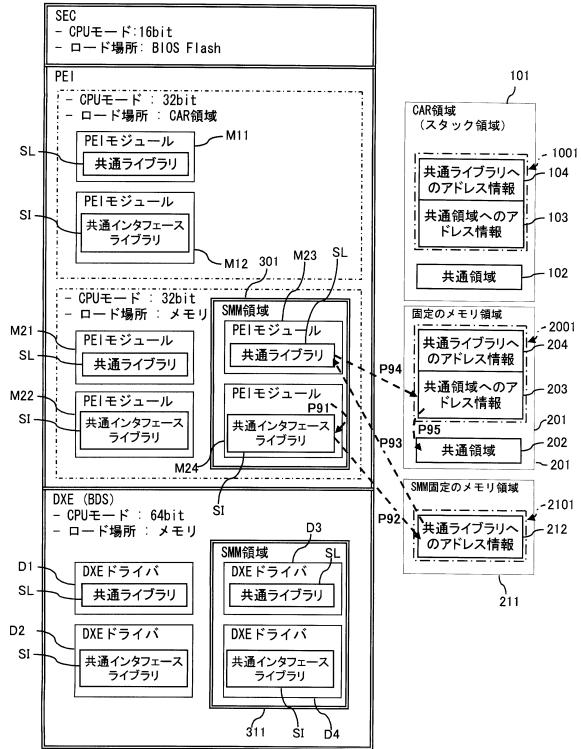
【図22】



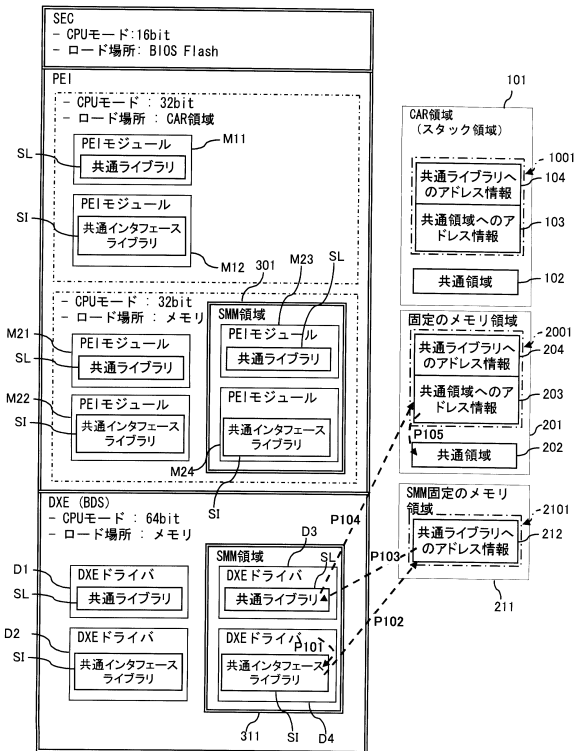
【図 23】



【図 24】



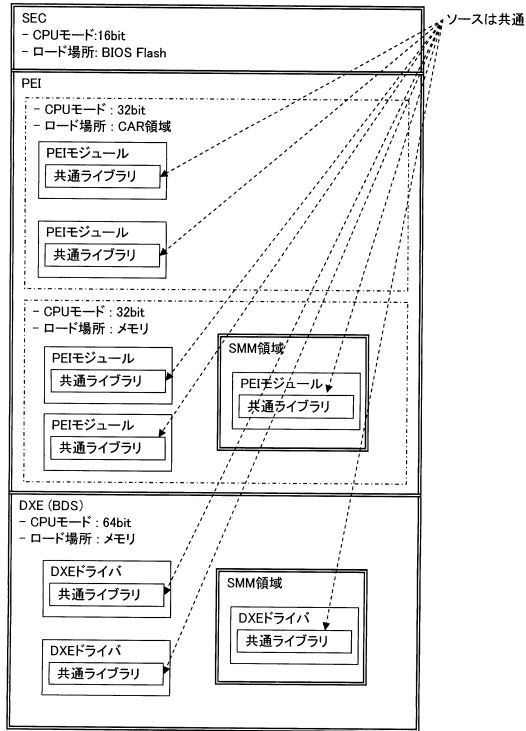
【図 25】



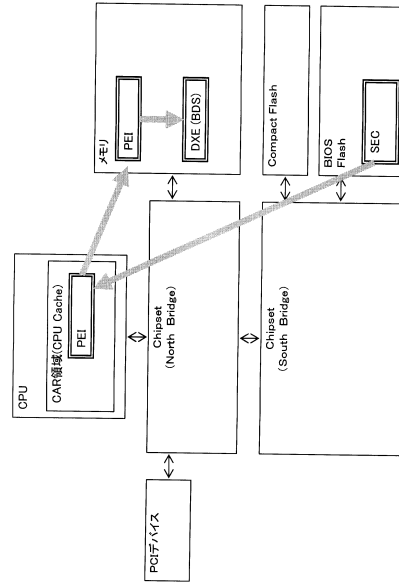
【図 26】

EFI Phase	プログラムロード動作領域	CPUモード	閉読言語
SEC	BIOS Flash	16bit	アセンブラ
PEI	CAR領域(CPU Cache)	32bit	C言語
	メモリ	32bit	C言語
	メモリ(SMM領域)	SMM, 32bit	C言語
DXE (BDS)	メモリ	64bit	C言語
	メモリ(SMM領域)	SMM, 64bit	C言語

【図 27】



【図 28】





---

フロントページの続き

- (56)参考文献 特開2005-196286(JP,A)  
特開平06-332675(JP,A)  
特開2006-139795(JP,A)  
米国特許第07512719(US,B1)  
米国特許出願公開第2011/0283098(US,A1)

(58)調査した分野(Int.Cl., DB名)

G06F 9/445  
G06F 9/50  
G06F 9/54