(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4388374号
(P4388374)
(45)発行日　平成21年12月24日(2009.12.24)　(24)登録日　平成21年10月9日(2009.10.9)

(51)Int.Cl.　F I
G06F 13/36 (2006.01)　G06F 13/36 310Z

請求項の数 19 (全 20 頁)

(21)出願番号	特願2003-540839 (P2003-540839)
(86)(22)出願日	平成14年9月12日 (2002.9.12)
(65)公表番号	特表2005-508049 (P2005-508049A)
(43)公表日	平成17年3月24日 (2005.3.24)
(86)国際出願番号	PCT/US2002/028980
(87)国際公開番号	WO2003/038646
(87)国際公開日	平成15年5月8日 (2003.5.8)
審査請求日	平成17年9月12日 (2005.9.12)
(31)優先権主張番号	10/033,142
(32)優先日	平成13年11月1日 (2001.11.1)
(33)優先権主張国	米国(US)

(73)特許権者　591016172
アドバンスト・マイクロ・ディバイシズ・インコーポレイテッド
ＡＤＶＡＮＣＥＤ　ＭＩＣＲＯ　ＤＥＶＩＣＥＳ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、９４０８８－３４５３　カリフォルニア州、サニィベイル、ピィ・オゥ・ボックス・３４５３、ワン・エイ・エム・ディ・プレイス、メイル・ストップ・６８（番地なし）
(74)代理人　100099324
弁理士　鈴木　正剛
(74)代理人　100111615
弁理士　佐野　良太

最終頁に続く

(54)【発明の名称】組み込みマイクロコントローラを備えたマイクロコンピュータ・ブリッジ・アーキテクチャ

(57)【特許請求の範囲】
【請求項１】
ブリッジとして構成された集積回路を有する装置であって、前記集積回路は、
内部バスと、
前記内部バスに結合され、当該内部バスのマスターとなって当該内部バスを制御するように構成されるとともに、アラート・スタンダード・フォーマット・スレーブとなるよう構成されたマイクロコントローラと、
前記内部バスに結合され、前記マイクロコントローラとこの内部バスを介してデータを交換するように構成されるとともに、アラート・スタンダード・フォーマット・メッセージを外部にあるアラート・スタンダード・フォーマット・マスターに中継するように構成されているイーサネット・コントローラと、
前記マイクロコントローラと前記イーサネット・コントローラとに結合され、前記データをバッファする複数のバッファと、を有する装置。
【請求項２】
前記複数のバッファは、前記内部バスと前記イーサネット・コントローラとに結合されたものである、請求項１記載の装置。
【請求項３】
前記マイクロコントローラはアラート・スタンダード・フォーマット・マスターとして構成されており、前記イーサネット・コントローラはアラート・スタンダード・フォーマット・メッセージを前記マイクロコントローラに中継するように構成されている請求項１

または２に記載の装置。
【請求項４】
前記マイクロコントローラは、組み込み８０５１マイクロコントローラとして構成されている、請求項１～３のいずれかに記載の装置。
【請求項５】
前記内部バスに結合されたリモート管理および制御プロトコル・セット命令ユニットをさらに有し、前記リモート管理および制御プロトコル・セット命令ユニットは、前記イーサネット・コントローラを介して外部の管理サーバーから受信したリモート管理および制御プロトコル命令を実行するように構成されている請求項１～４のいずれか１項に記載の装置。
【請求項６】
前記内部バスに結合されたシステム管理割り込み要求レジスタをさらに有し、前記システム管理割り込み要求レジスタは、前記システム管理割り込み要求レジスタにシステム管理割り込みベクタが書き込まれたことを受けてシステム管理割り込みに対する要求を発生させるように構成されており、前記マイクロコントローラは、前記システム管理割り込み要求レジスタに前記システム管理割り込みベクタを書き込むように構成されている請求項１～５のいずれか１項に記載の装置。
【請求項７】
前記内部バスに結合されたタイマをさらに有し、前記マイクロコントローラは、前記タイマが満了したことを受けて、前記システム管理割り込み要求レジスタに前記システム管理割り込みベクタを書き込むように構成可能である請求項６に記載の装置。
【請求項８】
前記内部バスに結合された割り込みレジスタをさらに有し、マイクロコントローラ割り込みベクタが前記割り込みレジスタに書き込まれたことを受けてマイクロコントローラ割り込みが生成される請求項１～５のいずれか１項に記載の装置。
【請求項９】
前記内部バスに結合されたデータ交換レジスタをさらに有し、前記データ交換レジスタは、前記マイクロコントローラからのデータまたは前記マイクロコントローラへのデータを記憶するように構成されており、前記マイクロコントローラは前記データ交換レジスタにデータを書き込むように構成されており、前記マイクロコントローラは前記データ交換レジスタからデータを読み出すように構成されている請求項１～５のいずれか１項に記載の装置。
【請求項１０】
前記内部バスに結合されたシステム管理割り込み要求レジスタをさらに有し、前記システム管理割り込み要求レジスタは、前記システム管理割り込み要求レジスタにシステム管理割り込みベクタが書き込まれたことを受けてシステム管理割り込みに対する要求を発生させるように構成されており、前記マイクロコントローラは、前記システム管理割り込み要求レジスタに前記システム管理割り込みベクタを書き込むように構成されている請求項８または９に記載の装置。
【請求項１１】
前記集積回路はコンピュータ・システムに組み込まれており、前記コンピュータ・システムは外部バスをさらに有し、前記集積回路は前記外部バスに結合されている請求項１～４のいずれかに記載の装置。
【請求項１２】
前記コンピュータ・システムは前記外部バスに結合されたプロセッサをさらに有し、前記プロセッサは前記集積回路内の前記イーサネット・コントローラによってネットワークを介して通信するように構成されている請求項１１に記載の装置。
【請求項１３】
前記コンピュータ・システムは前記外部バスに結合された少なくとも１つのセンサをさらに有し、前記イーサネット・コントローラは、ネットワークを介して前記センサからの

データを送信するように構成されている請求項１１または１２に記載の装置。
【請求項１４】
前記マイクロコントローラはアラート・スタンダード・フォーマット・マスターとして構成されており、前記イーサネット・コントローラはアラート・スタンダード・フォーマット・メッセージを前記マイクロコントローラに中継するように構成されている請求項１１～１３のいずれか１項に記載の装置。
【請求項１５】
前記コンピュータ・システムは、前記集積回路と前記プロセッサとに結合されたネットワーク・インタフェース・カードをさらに有し、前記ネットワーク・インタフェース・カードはアラート・スタンダード・フォーマット・マスターとして構成されており、前記マイクロコントローラはアラート・スタンダード・フォーマット・スレーブとして構成されており、前記イーサネット・コントローラは、アラート・スタンダード・フォーマット・メッセージを前記ネットワーク・インタフェース・カードに中継するように構成されている請求項１１～１３のいずれか１項に記載の装置。
【請求項１６】
アラート・スタンダード・フォーマット・サウス・ブリッジ内のイーサネット・コントローラにおいてアラート・スタンダード・フォーマット・メッセージを受信するステップと、
前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の内部バスを介して、前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記イーサネット・コントローラから前記アラート・スタンダード・フォーマット・サウス・ブリッジ内のマイクロコントローラに前記アラート・スタンダード・フォーマット・メッセージを送信するステップと、
前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラをアラート・スタンダード・フォーマット・スレーブ・モードで動作させている場合に、外部バスを介して前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラからアラート・スタンダード・フォーマット・ネットワーク・インタフェース・カードに前記アラート・スタンダード・フォーマット・メッセージを送信するステップと、
前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラをアラート・スタンダード・フォーマット・マスター・モードで動作させている場合に、前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラから前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記イーサネット・コントローラに、前記アラート・スタンダード・フォーマット・メッセージに対する肯定応答を送信するステップと、を有するコンピュータ・システムの動作方法。
【請求項１７】
前記アラート・スタンダード・フォーマット・メッセージに応答して複数のアラート・スタンダード・フォーマット・サウス・ブリッジ・レジスタのうちの少なくとも１つからデータを読み出すステップと、
前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラをアラート・スタンダード・フォーマット・スレーブ・モードで動作させている場合に、前記複数の外部アラート・スタンダード・フォーマット・サウス・ブリッジ・レジスタのうちの前記少なくとも１つから読み出した前記データを、前記外部バスを介して前記ネットワーク・インタフェース・カードから前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラに転送するステップと、
前記複数の外部アラート・スタンダード・フォーマット・サウス・ブリッジ・レジスタのうちの前記少なくとも１つから読み出した前記データを、前記内部バスを介して前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラから前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記イーサネッ

ト・コントローラに転送するステップと、をさらに有する請求項１６に記載の方法。
【請求項１８】
前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラの前記アラート・スタンダード・フォーマット・マスター・モードでの動作には、前記アラート・スタンダード・フォーマット・サウス・ブリッジにある前記マイクロコントローラが、アラート・スタンダード・フォーマット・センサ状態値を求めて前記コンピュータ・システム内のアラート・スタンダード・フォーマット・センサに対してポーリングを行うことと、前記アラート・スタンダード・フォーマット・センサ状態値を求める外部の管理サーバーからの要求に応じることと、が含まれる、請求項１７に記載の方法。
【請求項１９】
前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラの前記アラート・スタンダード・フォーマット・スレーブ・モードでの動作には、前記アラート・スタンダード・フォーマット・サウス・ブリッジ内の前記マイクロコントローラによって、前記アラート・スタンダード・フォーマット・ネットワーク・インタフェース・カードからのアラート・スタンダード・フォーマット要求に応答することが含まれる、請求項１７に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に演算システムに関し、より詳細にはパーソナル・コンピュータ・システム等用のリモート管理のためのチップセット・アーキテクチャに関する。
【背景技術】
【０００２】
図１Ａに、例示的なコンピュータ・システム１００を示す。コンピュータ・システム１００は、プロセッサ１０２、ノース・ブリッジ１０４、メモリ１０６、アドバンスド・グラフィックス・ポート（ＡＧＰ）デバイス１０８、ネットワーク・インタフェース・カード（ＮＩＣ）１０９、周辺機器相互接続（ＰＣＩ）バス１１０、ＰＣＩコネクタ１１１、サウス・ブリッジ１１２、バッテリ１１３、ＡＴアタッチメント（ＡＴＡ）インタフェース１１４（統合ドライブ機器［ＩＤＥ］インタフェースと呼ばれることが多い）、ＳＭＢｕｓ１１５、ユニバーサル・シリアル・バス（ＵＳＢ）インタフェース１１６、低ピンカウント（ＬＰＣ）バス１１８、入出力コントローラ・チップ（ＳｕｐｅｒＩ／Ｏ（登録商標））１２０、およびＢＩＯＳメモリ１２２を備える。ノース・ブリッジ１０４とサウス・ブリッジ１１２とは、１つのチップを有していても、複数のチップを有していてもよく、これらは総称して「チップセット」と呼ばれるという点が留意される。また、コンピュータ・システム１００には、キャッシュ、モデム、パラレル・インタフェース、シリアル・インタフェース、ＳＣＳＩインタフェースなどの他のバス、デバイス、またはサブシステムが必要に応じて含まれていてもよいという点も留意される。
【０００３】
プロセッサ１０２はノース・ブリッジ１０４に結合されている。ノース・ブリッジ１０４は、プロセッサ１０２、メモリ１０６、ＡＧＰデバイス１０８、およびＰＣＩバス１１０の間のインタフェースを提供している。サウス・ブリッジ１１２は、ＰＣＩバス１１０と、ＩＤＥインタフェース１１４、ＳＭＢｕｓ１１５、ＵＳＢインタフェース１１６、およびＬＰＣバス１１８に結合された周辺機器、デバイス、およびサブシステムとの間のインタフェースを提供している。バッテリ１１３は、サウス・ブリッジ１１２に結合されている。ＳｕｐｅｒＩ／Ｏチップ１２０はＬＰＣバス１１８に結合されている。
【０００４】
ノース・ブリッジ１０４は、プロセッサ１０２、メモリ１０６、ＡＧＰデバイス１０８、ＰＣＩバス１１０に結合されたデバイス、ならびにサウス・ブリッジ１１２に結合されたデバイスおよびサブシステムの間で通信を行えるようにする。通常は、取り外し可能な周辺機器が、本図でＰＣＩコネクタ１１１として示されるＰＣＩ「スロット」に挿入され

る。ＰＣＩ「スロット」は、ＰＣＩバス１１０に接続しており、コンピュータ・システム１００に結合される。別法として、マザーボードにあるデバイスがＰＣＩバス１１０に直接接続されてもよい。ＰＣＩコネクタ１１１のピンの一部をＳＭＢｕｓ１１５に使用することによって、ＳＭＢｕｓ１１５がＰＣＩバス１１０と「統合され」てもよい。

【０００５】

サウス・ブリッジ１１２は、ＰＣＩバス１１０と、モデム、プリンタ、キーボード、マウスなどの各種デバイスおよびサブシステムとの間のインタフェースを提供している。これらの機器は、通常はＬＰＣバス１１８か、あるいはＸ－バスや業界標準アーキテクチャ（ＩＳＡ）バスといったＬＰＣバスの前身のインタフェースを介してコンピュータ・システム１００に結合されている。サウス・ブリッジ１１２は、これらのデバイスを、ＩＤＥインタフェース１１４、ＵＳＢインタフェース１１６、およびＬＰＣバス１１８を介してコンピュータ・システム１００の他の部分とインタフェースするために使用されるロジックを有する。また、サウス・ブリッジ１１２は、二線式ＩＣ間（two-wire inter-IC bus）バス・プロトコルを拡張したＳＭＢｕｓ１１５を介してデバイスとインタフェースするロジックも有する。

【０００６】

図１Ｂは、バッテリ１１３による予備電力など、サウス・ブリッジ１１２の一部の態様を示すものであり、これは「ＲＴＣ（リアル・タイム・クロック）バッテリ・ウェル１２５に内蔵されている」と呼ばれる。サウス・ブリッジ１１２は、サウス・ブリッジ（ＳＢ）ＲＡＭ１２６とクロック回路１２８とを有し、これらはいずれもＲＴＣバッテリ・ウェル１２５に内蔵されている。ＳＢ　ＲＡＭ１２６は、ＣＭＯＳ　ＲＡＭ１２６ＡとＲＴＣ　ＲＡＭ１２６Ｂとを有する。ＲＴＣ　ＲＡＭ１２６Ｂは、クロック・データ１２９とチェックサム・データ１２７とを有する。また、サウス・ブリッジ１１２は、ＲＴＣバッテリ・ウェル１２５の外部に、ＣＰＵインタフェース１３２、電力およびシステム管理ユニット１３３、および各種バス・インタフェース・ロジック回路１３４を有する。

【０００７】

クロック回路１２８から送られた日時データは、クロック・データ１２９としてＲＴＣ　ＲＡＭ１２６Ｂに記憶される。ＲＴＣ　ＲＡＭ１２６Ｂにあるチェックサム・データ１２７は、下記に記載するブート処理中、例えば図２に示すブロック１４８などの間に、ＣＭＯＳ　ＲＡＭ１２６Ａのデータを基にＢＩＯＳによって計算されて記憶され得る。ＣＰＵインタフェース１３２は、割り込み信号コントローラとプロセッサ信号コントローラとを有し得る。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

図１Ｃに、コンピュータ・システム１００用の、先行技術によるリモート管理構成を示す。マザーボード１０１は、サウス・ブリッジ１１２、ＰＣＩバス１１０、ＰＣＩコネクタ１１１、ＳＭＢｕｓ１１５、およびセンサ１０３Ａ，１０３Ｂを構造的に支持していると共に、ベース電力を供給している。取り外し可能な増設カードであるＮＩＣ１０９は、ＰＣＩコネクタ１１１を介してマザーボード１０１、ＰＣＩバス１１０、およびＳＭＢｕｓ１１５に結合している。ＮＩＣ１０９は、イーサネット・コントローラ１０５とＡＳＦマイクロコントローラ１０７とを有する。イーサネット・コントローラ１０５はリモート管理サーバー９０と通信しており、ＡＳＦマイクロコントローラ１０７とリモート管理サーバー９０との間で管理データおよび命令の受け渡しを行っている。リモート管理サーバー９０は、コンピュータ・システム１００の外部にある。

【０００９】

アラート・スタンダード・フォーマット（Alert Standard Format：ＡＳＦ）仕様と一般に呼ばれている業界標準仕様は、リモート管理サーバー９０を使用した「システム管理」の一方式を規定している。ＡＳＦ仕様は、コンピュータ・システム１００などのクライアント・システムのオペレーティング・システムが機能しなくなった場合に動作すること

ができるリモート制御および警告発生インタフェースを規定している。一般に、リモート管理サーバー９０は、１台以上のクライアント・システムを監視および制御するように構成されている。ＡＳＦ警告発生インタフェースの典型的な動作では、クライアントからリモート管理サーバー９０に警告メッセージが送信され、リモート管理サーバー９０からクライアントにリモート制御命令が送信されて、クライアントからリモート管理サーバー９０に応答が送信され、クライアント固有の構成およびアセット（asset）が特定されてリモート管理サーバー９０に送信され、クライアントのオペレーティング・システムと対話することによってクライアントが構成および制御される。さらに、リモート管理サーバー９０は、ＡＳＦ　ＮＩＣ１０９と通信し、クライアントのＡＳＦ　ＮＩＣ１０９は、ローカル・クライアント・センサ１０３およびローカル・クライアント・ホスト・プロセッサと通信する。

【００１０】

ＡＣＰＩ対応のオペレーティング・システムがクライアントにおいて機能している場合、「成功した１回のブート」時にＡＳＦ　ＮＩＣ１０９用の構成ソフトウェアが実行されて、特定のＡＳＦデータ、ＡＣＰＩデータ、およびクライアントの構成データが記憶される。

【００１１】

クライアントからリモート管理サーバー９０に警告を送信するためにＡＳＦで使用される伝送プロトコルは、プラットフォーム・イベント・トラップ（Platform Event Trap：ＰＥＴ）である。ＰＥＴフレームは、複数のフィールドからなり、このフィールドには、ＧＵＩＤ（グローバル一意識別子）、シーケンス番号、時間、クライアントでのＰＥＴフレームの発信元、イベント・タイプ・コード、イベント・レベル、警告を発生させたセンサ・デバイス、イベント・データ、およびＩＤなどのフィールドがある。

【００１２】

警告の発生及び送信は、多くのイベントにより生じ得る。このようなイベントには、温度が設定値を上回ったか下回ったことや、電圧が設定値を上回ったか下回った、ファンの故障が実際に発生したか発生が予想される、ファンの回転速度が設定値を上回ったか下回った、コンピュータ・システムが物理的な侵入を受けたなどがある。システムの動作上のエラーが警告を発生させることもあり、この例としては、メモリ・エラー、データ・デバイスのエラー、データ・コントローラのエラーや、ＣＰＵの電気特性の不適合などが挙げられる。また、警告は、クライアントのいずれの部分のブート時または初期化時のＢＩＯＳまたはファームウェアの処理の進行状況（progression）に対応していることもある。また、オペレーティング・システム（ＯＳ）のブートの失敗またはＯＳのタイムアウトなど、ＯＳ関連のイベントが警告を発生させることがある。ＡＳＦ仕様は、クライアントが、自身の存在を示すメッセージである「ハートビート」を送信しなくなった場合に、プログラム可能な所定の間隔でハートビート警告を発生させる。この間隔は通常は１分であり、１０分を超えることはない。

【００１３】

クライアント制御機能は、ユーザー・データグラム・プロトコル（ＵＤＰ）ベースのプロトコルであるリモート管理および制御プロトコル（ＲＭＣＰ）によって実装される。ＲＭＣＰは、クライアントがオペレーティング・システムを実行していない場合に使用される。リセット、電源投入、および電源切断の各サイクルの間に、ＲＭＣＰパケットが交換され、このメッセージのタイプはサイクルによって異なる。リモート管理サーバー９０は、存在確認要求（presence-ping-request）を使用したハンドシェーク・プロトコルによって、クライアントのＡＳＦ－ＲＭＣＰ機能を判定する。クライアントがこれに対して肯定応答を返し、続いて使用中のＡＳＦのバージョンを示す存在応答（presence-pong）を送信する。次に、リモート管理サーバー９０は、クライアントに対して、クライアントの構成を知らせるように求める要求を送信する。クライアントは肯定応答を返し、続いて「成功した１回のブート」中に不揮発メモリに記憶したクライアントの構成を示すメッセージを送る。ＲＭＣＰパケットには、コンテンツ・フィールド、タイプ・フィールド、オフ

セット・フィールド、および値フィールドが含まれる。

【００１４】

ＲＭＣＰメッセージ・トランザクションでは、リモート管理サーバー９０から要求を送信し、肯定応答の受信を所定の時間待機した後、応答の受信を所定の時間待機する。肯定応答の待機時間か応答の待機時間かのいずれかが経過すると、リモート管理サーバー９０は、パケットの一部をクライアントに再送する必要があるか、あるいはクライアントか通信リンクの障害によりクライアント側が接続できなくなったことを認識する。

【００１５】

ＡＳＦ　ＮＩＣ１０９は、オペレーティング・システムが関与しなくとも、自身のＩＰ（インターネット　プロトコル）アドレス（またはこれと同等のもの）を報告することができる。このため、ＡＳＦ　ＮＩＣ１０９は、オペレーティング・システムと共に、ＡＲＰ（アドレス解決プロトコル）要求を受信してこれに応答する必要があるほか、オペレーティング・システムが実行されているときはＡＲＰパケットに干渉せず、ＡＲＰパケットに応えて起動する（wake-up for）よう構成されている場合は、監視する必要がある。ＡＣＰＩには、標準の構成として、ＡＲＰパケットに応えた起動が含まれているという点に留意すべきである。

【００１６】

クライアントの構成を示す情報として、クライアントからリモート管理サーバー９０に送信される情報には、センサおよびその特性を識別するＡＣＰＩ記述テーブル、ＰＥＴメッセージのためのＡＳＦ機能およびシステム・タイプ、クライアントのＲＭＣＰへの対応情報および最後のＲＣＭＰ命令、オプションのオペレーティング・システム・ブート・ハング監視タイマのクライアントでの構成状況、ＰＥＴメッセージのためのＵＵＩＤ／ＧＵＩＤのＳＭＢＩＯＳ識別情報などがある。ＡＳＦオブジェクトは、ＡＣＰＩのＡＳＬ（ＡＳＦソフトウェア言語）命名規則に準拠している。

【００１７】

図２に、ＢＩＯＳ１２２に記憶されたコードを使用してコンピュータ・システムを初期化する従来の方法のフローチャートを示す。ブロック１３６において、電源の初期化時に、電源が電力良好信号を生成してノース・ブリッジ１０４に送る。ブロック１３８において、サウス・ブリッジ１１２（またはノース・ブリッジ１０４）は、電源から電力良好信号を受け取ると、プロセッサ１０２へのリセット信号のアサートを中止する。

【００１８】

ブロック１４０において、プロセッサ１０２は、初期化中にフォールト・ジャンプ位置を読み出す。メモリ内のフォールト・ジャンプ位置は、通常ＦＦＦＦ０ｈなどの所定の位置である。ブロック１４２において、プロセッサ１０２は、ＲＯＭ　ＢＩＯＳ１２２内の適切なＢＩＯＳコード位置（例えば、ＦＦＦＦ０ｈ）にジャンプして、ＢＩＯＳコードをＲＡＭメモリ１０６にコピーし、ＲＡＭメモリ１０６からＢＩＯＳコード命令の処理を開始する。ブロック１４４において、プロセッサ１０２によって処理されるＢＩＯＳコードが電源投入時自己診断（ＰＯＳＴ）を実行する。

【００１９】

次にＢＩＯＳコードは、ブロック１４６において、ビデオ・コントローラ、ＩＤＥコントローラ、ＳＣＳＩコントローラなどの追加のＢＩＯＳコードを探して、起動情報画面を表示する。例として挙げると、ビデオ・コントローラのＢＩＯＳはＣ０００ｈに存在することが多く、ＩＤＥコントローラのＢＩＯＳコードはＣ８００ｈに存在することが多い。ＢＩＯＳコードは、ブロック１４８において、ＲＡＭメモリ・カウントアップ・テスト、ＣＯＭ（シリアル）ポートやＬＰＴ（パラレル）ポートの識別といったシステム・インベントリの確認などの、追加のシステム診断を実行する。追加のシステム診断には、ＡＳＦの初期化とＡＣＰＩの初期化のほか、リモート管理サーバー９０との通信リンクの開始を含めたイーサネットの初期化がある。ＢＩＯＳコードは、ブロック１５０において、プラグアンドプレイ・デバイスやその他の類似するデバイスを識別し、識別されたデバイスの短い説明を示す画面を表示する。

【００２０】
ＢＩＯＳコードは、ブロック１５２において、ブート位置と、これに対応するブート・セクタとを識別する。このブート位置は、フロッピー・ドライブ、ハード・ドライブ、ＣＤ－ＲＯＭ、リモートの位置などに存在し得る。次にＢＩＯＳコードは、ブロック１５４において、ブート位置にあるブート・セクタ・コードを呼び出して、オペレーティング・システムを備えたコンピュータ・システムなどのコンピュータ・システムをブートする。
【００２１】
コールド・ブートすなわちハード・ブート（またはハード・リブート）では、ブロック１３６～１５４について説明した内容の全てもしくは大半が行われ得るという点が留意される。ウォーム・ブートすなわちソフト・ブート（またはソフト・リブート）では、通常はＢＩＯＳコードがブロック１４２からブロック１４８にジャンプし、ＰＯＳＴやメモリ・テストなどが省略される。
【００２２】
ＡＳＦなどのリモート管理技術は、オペレーティング・システムによってリモート管理ハードウェアおよび／またはファームウェアの初期化が監視されるように、オペレーティング・システムの「成功した１回のブート」の際にＮＩＣ１０９が取り付けられていることを前提としている。パーソナル・コンピュータのためのリモート管理が改善されたことで、リモート管理ハードウェアおよび／またはファームウェアの初期化が高速化され、オペレーティング・システムへの依存度が下がることが考えられる。ブートに時間がかかるコンピュータ・システム１００は生産性を低下させ、少なく見積もってもユーザーにストレスを与える。可能であればブート時間を短縮することが所望されている。
【課題を解決するための手段】
【００２３】
本発明の一態様においては、集積回路が開示される。この集積回路は、内部バスと、内部バスに接続されたマイクロコントローラとを有する。マイクロコントローラは、内部バスのマスターとなる、つまり、内部バスを制御あるいは支配するように構成されている。別の実施形態においては、集積回路は、内部バスに結合されたイーサネット・コントローラ、およびマイクロコントローラとイーサネット・コントローラとに結合され、マイクロコントローラとイーサネット・コントローラとの間でデータをバッファする複数のバッファを有する。イーサネット・コントローラとマイクロコントローラとは、内部バスを介してデータを交換するように構成されている。
【００２４】
本発明の別の態様においては、別の集積回路が開示される。この集積回路は、内部バス、内部バスに接続されたマイクロコントローラ、および内部バスに結合されたシステム管理割り込み要求レジスタを有する。マイクロコントローラは、内部バスのマスターとなるように構成されている。システム管理割り込み要求レジスタは、システム管理割り込み要求レジスタにシステム管理割り込みベクタが書き込まれたことを受けてシステム管理割り込みに対する要求を発生させるように構成されている。マイクロコントローラは、システム管理割り込み要求レジスタにシステム管理割り込みベクタを書き込むように構成されている。
【００２５】
本発明のさらに別の態様においては、さらに別の集積回路が開示される。この集積回路は、内部バス、内部バスに接続されたマイクロコントローラ、および内部バスに結合された割り込みレジスタを有する。マイクロコントローラは、内部バスのマスターとなるように構成されている。マイクロコントローラ割り込みベクタが割り込みレジスタに書き込まれたことを受けてマイクロコントローラ割り込みが生成される。
【００２６】
本発明の別の態様においては、コンピュータ・システムが開示される。このコンピュータ・システムは、外部バス、集積回路、および外部バスに結合されたプロセッサを有する。集積回路は、内部バス、内部バスに接続されたマイクロコントローラ、内部バスに結合

されたイーサネット・コントローラ、マイクロコントローラとイーサネット・コントローラとに結合され、データをバッファする複数のバッファ、および外部バスに接続されたバス・インタフェース・ロジックを有する。マイクロコントローラは、内部バスのマスターとなるように構成されている。イーサネット・コントローラとマイクロコントローラとは、内部バスを介してデータを交換するように構成されている。プロセッサは、イーサネット・コントローラによってネットワークを介して通信するように構成されている。

【００２７】

本発明のさらに別の態様においては、コンピュータ・システムの動作方法が開示される。この方法は、アラート・スタンダード・フォーマット・サウス・ブリッジ内のイーサネット・コントローラにおいてアラート・スタンダード・フォーマット・メッセージを受信するステップと、アラート・スタンダード・フォーマット・サウス・ブリッジ内の内部バスを介して、アラート・スタンダード・フォーマット・サウス・ブリッジ内のイーサネット・コントローラからアラート・スタンダード・フォーマット・サウス・ブリッジ内のマイクロコントローラにアラート・スタンダード・フォーマット・メッセージを送信するステップとを有する。この方法は、アラート・スタンダード・フォーマット・サウス・ブリッジ内のマイクロコントローラをアラート・スタンダード・フォーマット・スレーブ・モードで動作させている場合に、アラート・スタンダード・フォーマット・サウス・ブリッジ内のマイクロコントローラから外部バスを介してアラート・スタンダード・フォーマット・ネットワーク・インタフェース・カードにアラート・スタンダード・フォーマット・メッセージを送信するステップを有する。この方法は、アラート・スタンダード・フォーマット・サウス・ブリッジ内のマイクロコントローラをアラート・スタンダード・フォーマット・マスター・モードで動作させている場合に、アラート・スタンダード・フォーマット・サウス・ブリッジ内のマイクロコントローラからアラート・スタンダード・フォーマット・サウス・ブリッジ内のイーサネット・コントローラに、アラート・スタンダード・フォーマット・メッセージに対する肯定応答を送信するステップを有する。

【発明を実施するための最良の形態】

【００２８】

添付の図面と併せて下記の説明を読めば、本発明を理解できるであろう。添付の図面においては、同一の参照符号は同じ要素を指している。

【００２９】

本発明は、種々の変形および代替形態を取り得るが、その特定の実施形態が、図面に例として図示され、ここに詳細に記載されているに過ぎない。しかし、この詳細な説明は、本発明を特定の実施形態に限定することを意図するものではなく、反対に、添付の特許請求の範囲によって規定される本発明の趣旨ならびに範囲に含まれる全ての変形例、均等物および代替例を含むことを理解すべきである。

【００３０】

本発明の例示的な実施形態を下記に記載する。簡潔を期すために、実際の実装の特徴を全て本明細書に記載することはしない。当然、実際の実施形態の開発においては、システム上の制約およびビジネス上の制約に適合させるなど、開発の具体的な目的を達するために、実装に固有の判断が数多く必要とされ、この判断は実装によって変わるということが理解される。さらに、この種の開発作業は複雑かつ時間がかかるものであるが、本開示による利益を受ける当業者にとって日常的な作業であるということが理解されよう。参照符号に文字が付加されている場合、参照符号が付されている項目の別の実施形態あるいは別例が存在するということを意味する。

【００３１】

下記の非特許文献は、その全てがここに記載されているものとして、何ら不利益を被ることなく、かつ無条件に、その全てが参照により援用される。

［ＡＳＦ］　アラート・スタンダード・フォーマット仕様、１．０３（２００１年６月２０日）、ＤＳＰ０１１４および以前のバージョン、http://www.dmtf.org/spec/asf.html

［ＡＣＰＩ］　アドバンスト・コンフィギュレーション電力管理インタフェース仕様、２

．０（２０００年７月２７日）および以前のバージョン、http://www.teleport.com/~acpi/spec.htm
［ＲＦＣ１１５７］簡易ネットワーク管理プロトコル、http://www.ietf.org/rfc/rfc1157.txt
［ＣＩＭ］　ＣＩＭ標準、http://www.dmtf.org/spec/cims.html
［ＩＰＭＩ］　インテリジェント・プラットフォーム管理インタフェース仕様ｖ１．０、ｒｅｖ　１．１（１９９９年８月２６日）および以前のバージョン、http://developer.intel.com/design/servers/ipmi/
［ＲＦＣ１１８８］　ＦＤＤＩネットワークでのＩＰおよびＡＲＰ、http://www.ietf.org/rfc/rfc1180.txt
［ＦＲＵ］　ＩＰＭ１フィールド・リプレーサブル・ユニット（ＦＲＵ）情報記憶定義、ｖ１．０、１６（１９９８年９月１６日）および以前のバージョン、ftp://download.intel.coaddesign/servers/ipmi/fru1010.pdf
［ＭＴＬＳ］　メトリアス（Ｍｅｔｏｌｉｏｕｓ）ＡＣＰＩ／管理機能、ｖ１．０（１９９９年４月３０日）、http://developer.intel.com/ial/metolious/index.htm
［ＮＤＣＰＭ］　ネットワーク・デバイス・クラス電力管理参考仕様、ｖ１．０ａ（１９９７年１１月２１日）、http://www.microsoft.com/hwdev/Specs/PMref/PMnetwork.htm
［ＰＥＴ］　プラットフォーム・イベント・トラップ仕様、ｖ１．０（１９９８年１２月７日）および以前のバージョン、ftp://download.intel.con/design/servers/ipmi/pet100.pdf
［ＳＣＭＩＳ］　ＳＭＢｕｓ制御方法インタフェース仕様、ｖ１．０（１９９９年１２月１０日）および以前のバージョン、http://www.smbus.org/specs/index.htm
［ＳＭＢＩＯＳ］　システム管理ＢＩＯＳ参考仕様、ｖ２．３．１（１９９９年3月１６日）および以前のバージョン、ftp://download.intel.com/ial/wfm/smbios.pdf
［ＳＭＢＵＳ＿２．０］　システム管理バス（ＳＭＢｕｓ）仕様、ｖ２．０（２０００年８月３日）および以前のバージョン、http://www.smbus.org/specs/index.html and
［ＲＦＣ＿ＵＤＰ］　ユーザー・ダイアグラム・プロトコル、ＲＦＣ　７６８、http://www.ietf.org/rfc/rfc0768.txt

【００３２】

図３Ａ，Ｂに、本発明の各種態様によるリモート管理構成を有するコンピュータ・システム２００Ａ，２００Ｂのブロック図を示す。図３Ａにおいて、ＡＳＦサウス・ブリッジ２１２には、リモート管理性を改善するためにＡＳＦ機能、ＡＣＰＩ機能および／またはイーサネット機能が統合されていてもよい。

【００３３】

図３Ａのコンピュータ・システム２００Ａは、プロセッサ２０２、ノース・ブリッジ２０４、メモリ２０６、アドバンスド・グラフィックス・ポート（ＡＧＰ）デバイス２０８、ＰＣＩバス２１０、ＰＣＩコネクタ２１１、ＡＳＦサウス・ブリッジ２１２、バッテリ２１３、ＡＴアタッチメント（ＡＴＡ）インタフェース２１４、ＳＭＢｕｓ２１５、ユニバーサル・シリアル・バス（ＵＳＢ）インタフェース２１６、低ピンカウント（ＬＰＣ）バス２１８、入出力コントローラ・チップ（ＳｕｐｅｒＩ／Ｏ（登録商標））２２０、および拡張ＢＩＯＳメモリ２２２を備え、このほか随意的に暗号プロセッサ２２４と保護記憶装置２３０とを備える。ノース・ブリッジ２０４とＡＳＦサウス・ブリッジ２１２とは、チップセットに１つのチップを有していても、複数のチップを有していてもよいという点が留意される。また、コンピュータ・システム２００Ａには、キャッシュ、モデム、パラレル・インタフェース、シリアル・インタフェース、ＳＣＳＩインタフェースなどの他のバス、デバイス、またはサブシステムが必要に応じて含まれていてもよいという点も留意される。

【００３４】

プロセッサ２０２はノース・ブリッジ２０４に結合されている。ノース・ブリッジ２０４は、プロセッサ２０２、メモリ２０６、ＡＧＰデバイス２０８、およびＰＣＩバス２１

０の間のインタフェースを提供している。ＡＳＦサウス・ブリッジ２１２は、ＰＣＩバス２１０と、ＩＤＥインタフェース２１４、ＳＭＢｕｓ２１５、ＵＳＢインタフェース２１６、およびＬＰＣバス２１８に結合された周辺機器、デバイス、およびサブシステムとの間のインタフェースを提供している。バッテリ２１３は、ＡＳＦサウス・ブリッジ２１２に結合されている。ＳｕｐｅｒＩ／Ｏ（登録商標）チップ２２０、拡張ＢＩＯＳ２２２、および暗号プロセッサ２２４は、ＬＰＣバス２１８に結合されている。保護記憶装置２３０は、暗号プロセッサ２２４を介して結合されている。

【００３５】

ノース・ブリッジ２０４は、プロセッサ２０２、メモリ２０６、ＡＧＰデバイス２０８、ＰＣＩバス２１０に結合されたデバイス、ならびにサウス・ブリッジ２１２に結合されたデバイスおよびサブシステムの間で通信を行えるようにする。通常は、取り外し可能な周辺機器が、本図でＰＣＩコネクタ２１１として示されるＰＣＩ「スロット」に挿入される。ＰＣＩ「スロット」は、ＰＣＩバス２１０に接続しており、コンピュータ・システム２００Ａに結合される。別法として、マザーボードにあるデバイスがＰＣＩバス２１０に直接接続されていてもよい。ＰＣＩコネクタ２１１のピンの一部をＳＭＢｕｓ２１５に使用することによって、ＳＭＢｕｓ２１５がＰＣＩバス２１０と「統合され」ている。

【００３６】

ＡＳＦサウス・ブリッジ２１２は、ＰＣＩバス２１０と、モデム、プリンタ、キーボード、マウスなどの各種デバイスおよびサブシステムとの間のインタフェースを提供している。これらの機器は、通常はＬＰＣバス２１８か、あるいはＸ－バスや業界標準アーキテクチャ（ＩＳＡ）バスといったＬＰＣバスの前身のインタフェースを介してコンピュータ・システム２００Ａに結合されている。ＡＳＦサウス・ブリッジ２１２は、これらのデバイスを、ＩＤＥインタフェース２１４、ＳＭＢｕｓ２１５、好ましくはＡＳＦサウス・ブリッジ２１２の外部にあるサポーティング・マスター（supporting master）、ＵＳＢインタフェース２１６、およびＬＰＣバス２１８を介してコンピュータ・システム２００Ａの他の部分とインタフェースするために使用されるロジックを有する。

【００３７】

ＬＰＣバス２１８の動作は、先行技術の低ピン・カウント・インタフェース仕様レビジョン１．０（１９９７年９月２９日）に対応していてもよいという点も留意される。ＬＰＣバス２１８の動作は、拡張ＬＰＣバス・トランザクション・メカニズムを使用していてもよい。拡張メモリ・アドレスにデコードする複数のＳＴＡＲＴ信号を使用することによって、ＬＰＣのアドレス範囲を超える追加のメモリ・アドレスを使用することができる。標準ＬＰＣバス・トランザクションでは複数のＳＴＡＲＴ値を使用することができるが、デコードされている値のほとんどは使用されない。

【００３８】

拡張ＢＩＯＳ２２２は、ＢＩＯＳメモリ１２２内の記憶位置とは異なる追加の記憶位置を有するか、あるいはＢＩＯＳメモリ１２２内の記憶位置の他に追加の記憶位置を有する。追加の記憶位置は、特殊な読み出し／書き出し許可を有していても、安全な記憶位置であってもよく、この両方であってもよい。拡張ＢＩＯＳ２２２のメモリ・アドレス指定には、上記の拡張ＬＰＣバス・トランザクション・メカニズムが使用され得る。暗号プロセッサ２２４は、暗号プロセッサ２２４を介して保護記憶装置２３０にアクセスさせることによって、保護記憶装置２３０を保護し得る。

【００３９】

上記のように、ＡＳＦサウス・ブリッジ２１２には、本発明の各種態様によれば、ＡＳＦ機能、ＡＣＰＩ機能、および／またはイーサネット機能が統合されていてもよい。本発明の一態様によれば、コンピュータ・システム２００ＡにはＡＳＦ　ＮＩＣ１０９がないため、ＡＳＦサウス・ブリッジ２１２は、電源投入サイクル中に、自身がコンピュータ・システム２００Ａのマスター ＡＳＦコントローラとなる必要があることを認識する。ＡＳＦハードウェア、ＡＣＰＩハードウェア、および／またはイーサネット・ハードウェアは、ＢＩＯＳコードの記述前に知られているため、ＢＩＯＳのロードの主な部分においてＡ

ＳＦサウス・ブリッジ２１２内のＡＳＦアセットおよび／またはＡＣＰＩアセットを初期化することによって、コンピュータ・システム２００Ａがコンピュータ・システム１００よりも高速にブートするようになり有利である。その後、ＢＩＯＳコード自体が、ＡＳＦ、ＡＣＰＩ、および／またはイーサネットの初期化データおよび／またはファームウェアを含むように拡張され得る。下記に、本発明の各種実施形態の上記以外の詳細を記載する。

【００４０】

図３Ｂにおいて、コンピュータ・システム２００ＢがＰＣＩコネクタ２１１にＡＳＦ　ＮＩＣ１０９を有するという点で、コンピュータ・システム２００Ｂはコンピュータ・システム２００Ａとは異なる。コンピュータ・システム２００Ｂにおいて、本発明の一態様によるＡＳＦサウス・ブリッジ２１２は、自身がＡＳＦ　ＮＩＣ１０９に対するＡＳＦスレーブとなるべきことを認識する。

【００４１】

電力管理機能は、セキュア実行モード（ＳＥＭ）内で実行され得、これにはサウス・ブリッジに統合されているセキュリティ・ハードウェアを使用することが含まれる。電力管理および構成のための現行の標準の１つに、ＡＣＰＩ仕様がある。ＡＣＰＩ仕様では、命令の一種である制御メソッドにより、コンピュータ・システムに動作を実行させる。ＡＣＰＩ仕様は命令の実行方法には関知しない。ＡＣＰＩ仕様が規定しているのは命令の呼び出しであり、規定の方法に従って呼び出しを実行するようソフトウェアを記述する必要がある。ＡＣＰＩ仕様に規定されている方法は非常に厳格である。ハードウェアの一部のレジスタはアクセスができない。このようなレジスタにアクセスするには、ＳＭＩ＃（システム管理割り込み）を生成して、ＳＭＭに入り、これらのレジスタを読み出すことができる。動作限界を超えるまでプロセッサの電圧および動作周波数を上げてプロセッサが破壊されたり、動作限界を下回るまで電圧および動作周波数を下げてプロセッサが使用不能にされる（denial of service）など、電力管理が悪用される可能性があるため、ＡＣＰＩの呼び出しは、ＳＥＭの内部で行うなどの安全な方法によって行う必要がある。

【００４２】

ＳＥＭの内部では、安全な動作を保証するために、各ＡＣＰＩ要求が内部ルールと比較され得る。ＡＣＰＩ要求が「メールボックス」（サウス・ブリッジの一方向のみの記憶位置）の「受信ボックス」（サウス・ブリッジ内の受信専用の記憶位置）に格納され、受信ボックスからパラメータ値が読み出されて、受信ボックスのパラメータを使用して、ＡＣＰＩ要求が許容されるかどうかが評価され、この評価結果に基づいて要求に応じるかどうかが評価される必要がある。

【００４３】

システム管理モード（ＳＭＭ）は、電力を節約するために実装されたコンピュータ・システムの動作モードである。ＳＭＭは、ｘ８６プロセッサの第４世代のために策定されたものであり、ｘ８６動作モードとは異なる。これより新しい世代のｘ８６プロセッサが登場し、ＳＭＭはオペレーティング・システムからは比較的透過的なものとなった。換言すれば、コンピュータ・システムがＳＭＭに入ったりＳＭＭから復旧しても、オペレーティング・システムにほとんど影響を与えない。

【００４４】

図４に、本発明の各種態様によるＡＳＦサウス・ブリッジ２１２の一実施形態が示される。本図に示されるように、内部サウス・ブリッジ・バス３０２は、サウス・ブリッジ・レジスタ３０４と、イーサネット・コントローラ３４４の内部バス・インタフェース３３８と、ＬＰＣブリッジ３３０とを接続している。また、サウス・ブリッジ・レジスタ３０４は、ＳＭＩ要求レジスタ３０６、ＡＳＦ構成レジスタ３０８、監視タイマ（ＷＤＴ）３１、ＣＰＵ－ＭＣ（マイクロコントローラ）割り込みレジスタ３１２、ＣＰＵ－ＭＣデータ交換レジスタ３１４、ＡＣＰＩインタフェース３１６、ＡＳＦ状態レジスタ３１８、およびサウス・ブリッジ・レジスタ・ブリッジ３３４に結合している。さらに、サウス・ブリッジ・レジスタ・ブリッジ３３４は、ＭＣアドレス／データ（Ａ／Ｄ）バス３２２に結

合している。

【００４５】

ＭＣ　Ａ／Ｄバス３２２には、メモリ３２４、ＡＳＦ送信（Ｔｘ）バッファ３２６、ＡＳＦ受信（Ｒｘ）バッファ３２８、ＬＰＣブリッジ３３０、ＲＭＣＰセット命令ユニット３３６、および組み込みマイクロコントローラ３２０も結合している。また、ＭＣ３２０は、ＷＤＴ３１０に結合されていると共に、ＣＰＵ－ＭＣ割り込みレジスタ３１２およびＡＣＰＩインタフェース３１６に結合され、これら２つから割り込み（ＩＮＴ）を受信する。ＡＣＰＩインタフェース３１６はＳＣＩ割り込み要求も発生させる。ＡＳＦ状態レジスタ３１８は、割り込み要求も発生させる。組み込みイーサネット・コントローラは、ＡＳＦ　Ｒｘバッファ３２８に結合されたＲｘバッファ、ＡＳＦ　Ｔｘバッファ３２６に結合されたＴｘバッファ３４０、およびレジスタ３４６を備えたイーサネット・コア３４４も有する。イーサネット・コア３４４は、ＭＩＩ（マシン独立インタフェース）を介してＰＨｙ３４８に結合されている。ＰＨｙ３４８は、ＡＳＦサウス・ブリッジ２１２の外部にあってもよい。

【００４６】

ＭＣ３２０は、図示されていないＳＭＢｕｓ２１５に結合している。本発明の一態様によると、ＭＣ３２０は、ＡＣＰＩ仕様の第１３章に規定されていることからＡＣＰＩ仕様の「第１３章インタフェース」と呼ばれているインタフェースを使用して、ＳＭＢｕｓプロトコルのためにソフトウェアによって作動するＩ／Ｏポートを使用し得る。本実施形態および他の実施形態においては、プロセッサ（ＣＰＵ）２０２は、ＳＭＢｕｓ２１５のマスターとしてＳＭｂｕｓを制御することができる。ＢＩＯＳ　ＲＯＭ１２２または拡張ＢＩＯＳ２２２に記憶された、マザーボードに存在する従来の固定センサ・アドレスのほか、ＭＣ３２０は割り当て可能なアドレスをメモリ３２４に記憶し得る。ＡＳＦ　ＮＩＣ１０９が存在し、ＡＳＦサウス・ブリッジ２１２がスレーブ・モードで動作している場合、ＡＳＦサウス・ブリッジ２１２内のセンサが全てＡＳＦ　ＮＩＣ１０９によって認識可能となる。

【００４７】

イーサネット・コア３４４を備えた組み込みイーサネット・コントローラは、ブート時に、拡張ＢＩＯＳに記憶されているＢＩＯＳコードか、またはＭＣ３２０がＥＥＰＲＯＭ（図示なし）から値を読み出してレジスタ３４６に書き込むことによって構成され得る。レジスタ３４６は、複数の記憶位置を有していても、１つ以上の記憶位置を備えた複数のレジスタを有していてもよいという点が留意される。

【００４８】

ＭＣ３２０は、図示されていない汎用Ｉ／Ｏピンを何本か有していてもよい。入力ピンは、パニック割り込みを生成して、ＭＣ３２０に送信するために使用され得る。出力ピンは、プロセッサ２０２が「ハング」したときに必要とされるマザーボード機能を制御すると共に、ＡＳＦスレーブ・モード・パニックを生成するために使用され得る。ＡＳＦスレーブ・モード・パニックの生成は、センサ１０３の出力の「プッシュ」の代わりとして使用することができる。必要に応じて、汎用Ｉ／Ｏ入力が割り込みを生成してＭＣ３２０に送信しても、汎用Ｉ／Ｏ入力がＭＣ３２０によってポーリングされてもよい。

【００４９】

また、ＭＣ３２０は、ＡＳＦ以外のＡＳＦサウス・ブリッジ２１２の機能を管理、制御、監視、および／または提供するように構成されてもよいという点に留意すべきである。他の機能には、ＳＥＭ機能などのセキュリティ、ＡＣＰＩなどのシステムのヘルス・チェック機能のほか、本明細書の教示と矛盾しない機能が含まれ得る。

【００５０】

ＳＭＩ要求レジスタ３０６は、ＳＭＩ要求レジスタ３０６に割り込みベクタが書き込まれると、ＳＭＩ割り込みを生成するように構成されている。割り込みベクタは、図示されていない割り込みコントローラに渡される。

【００５１】

メモリ３２４は、必要に応じてＲＯＭおよびＲＡＭの少なくともいずれかを有し得る。ＭＣ３２０は、メモリ３２４のＲＯＭから構成データ読み出して、この構成データをメモリ３２４のＲＡＭにシャドウイングしてコピーしてもよい。この構成データが拡張ＢＩＯＳ２２２に記憶されて、シャドウイングによるコピーをＲＡＭに作成してもよい。ＡＳＦサウス・ブリッジ２１２において、ＡＣＰＩインタフェース３１６は、図３の電源／システム管理コア２３３に接続されているという点に留意すべきである。

【００５２】

一実施形態においては、ＡＳＦ構成レジスタ３０８は、ＡＳＦ用に構成されたＭＣ３２０のためのプラグアンドプレイ構成レジスタである。ＡＳＦはオペレーティング・システムが存在しない（ブート時にオペレーティング・システムが未だロードされていない場合やハング時など）場合に主に使用されるが、ＡＳＦはオペレーティング・システムとも対話する。

【００５３】

一実施形態においては、ＭＣ３２０は、組み込み８０５１マイクロコントローラといった、従来からある市販のマイクロコントローラである。８０５１マイクロコントローラおよび関連のマイクロコントローラは当業界において公知の機能を有する。８０５１マイクロコントローラの代表的な機能としては、１ビット操作用に最適化されたブーリアン・プロセッサを有する中央処理装置、２つの外部レベルおよび２つの優先度レベルを有する５～６個の割り込み、２～３個のタイマあるいはカウンタ（１６ビットのことが多い）、タイマのうちの１つによってデータ・レートが定義されるプログラム可能な全二重シリアル・ポート、３２個のＩ／Ｏ線（４個の８ビット・ポート）、ＲＡＭ、およびオプションのＲＯＭがある。８０５１マイクロコントローラには数多くの変形例があることが知られており、すべての変形例が本明細書に包含される。他のマイクロコントローラおよびマイクロプロセッサの設計もＭＣ３２０であるとして考慮される。

【００５４】

図５に、本発明によるＡＳＦサウス・ブリッジ２１２のＲＴＣバッテリ・ウェル２２５を示す。ＲＴＣバッテリ・ウェル２２５は、ＣＭＯＳ　ＲＡＭ２２６ＡとＲＴＣ　ＲＡＭ２２６Ｂとに分けられているＳＢ　ＲＡＭ２２６を有するほか、クロック回路２２８、状態レジスタ２５０、およびイネーブル・レジスタ２５２を有する。ＲＴＣ　ＲＡＭ２２６Ｂは、チェックサム・データ２２７とクロック・データ２２９とを有する。バッテリ２１３は、ＲＴＣバッテリ・ウェル２２５に結合され、その内部に存在する要素に電力を供給している。状態レジスタ２５０は、コンピュータ・システム２００のＡＳＦ機能用の状態情報を記憶するように構成されている。イネーブル・レジスタ２５２は、マスター・ビットを記憶するように構成されている。このマスター・ビットがセットされている場合、ＡＳＦ　ＮＩＣ１０９がないことを示す。別法としてスレーブ・ビットを記憶してもよく、このスレーブ・ビットがセットされている場合、ＡＳＦ　ＮＩＣ１０９が存在することを示す。図５に示すＡＳＦレジスタ２５０，２５２は、複数の記憶位置を有していても、１つ以上の記憶位置を有する複数のレジスタを有していてもよいという点が留意される。

【００５５】

また、ＡＳＦサウス・ブリッジ２１２は、ＲＴＣバッテリ・ウェル２２５の外部に、ＣＰＵインタフェース２３２、電力およびシステム管理ユニット２３３、および各種バス・インタフェース・ロジック回路２３４を有する。クロック回路２２８から送られた日時データは、クロック・データ２２９としてＲＴＣ　ＲＡＭ２２６Ｂに記憶される。ＲＴＣ　ＲＡＭ２２６Ｂに格納されているチェックサム・データ２２７は、ブート処理中に、ＣＭＯＳ　ＲＡＭ２２６Ａのデータを基にＢＩＯＳコードによって計算されて記憶され得る。ＣＰＵインタフェース２３２は、割り込み信号コントローラとプロセッサ信号コントローラとを有し得る。電力およびシステム管理ユニット２３３は、ＡＣＰＩ（アドバンスト・コンフィギュレーション電力管理インタフェース）コントローラを有していてもよい。

【００５６】

図６は、ＡＳＦサウス・ブリッジを有するコンピュータ・システムの初期化方法の一実

施形態を示すフローチャートである。図２にあるステップのうち、図６には示されていないか、あるいは図６では置き換えられているステップも、図６に含まれているものとして考慮される。

【００５７】

プロセッサ２０２は、初期化中にフォールト・ジャンプ位置を読み出す。メモリ内のフォールト・ジャンプ位置は、通常ＦＦＦＦ０ｈなどの所定の位置である。ブロック４０５において、プロセッサ２０２は、ＲＯＭ　ＢＩＯＳ２２２内の適切なＢＩＯＳコード位置（例えば、ＦＦＦＦ０ｈ）にジャンプして、ＢＩＯＳコードをＲＡＭメモリ２０６にコピーし、ＲＡＭメモリ２０６からＢＩＯＳコード命令の処理を開始する。ＢＩＯＳコード命令の処理には、ＡＳＦ　ＮＩＣ１０９の有無の確認などがある。

【００５８】

判断ブロック４１０においてＡＳＦ　ＮＩＣ１０９が存在する場合、本方法はブロック４１５に移る。判断ブロック４１０においてＡＳＦ　ＮＩＣ１０９が存在しない場合、本方法はブロック４２０に移る。

【００５９】

ＡＳＦ　ＮＩＣ１０９が存在する場合、ＡＳＦサウス・ブリッジ２１２は、ブロック４１５においてＡＳＦ　ＮＩＣ１０９に対するスレーブとして構成される。ＡＳＦ　ＮＩＣ１０９が存在しない場合、ＡＳＦサウス・ブリッジ２１２は、ブロック４２０においてマスターＡＳＦデバイスとして構成される。ブロック４１５，４２０のいずれの場合も、次にブロック４２５が続く。

【００６０】

ブロック４２５において、プロセッサ２０２によって処理されるＢＩＯＳコードが電源投入時自己診断（ＰＯＳＴ）を実行する。次にＢＩＯＳコードは、ブロック４３０において、ビデオ・コントローラ、ＩＤＥコントローラ、ＳＣＳＩコントローラなどの追加のＢＩＯＳコードを探して、起動情報画面を表示する。ＢＩＯＳコードは、ブロック４３５において、ＲＡＭメモリ・カウントアップ・テスト、ＣＯＭ（シリアル）ポートやＬＰＴ（パラレル）ポートの識別といったシステム・インベントリの確認などの、追加のシステム診断を実行する。ＢＩＯＳコードは、ブロック４４０において、プラグアンドプレイ・デバイスやその他の類似するデバイスを識別し、識別されたデバイスの短い説明を示す画面を表示する。ＢＩＯＳコードは、ブロック４４５において、ブート位置と、これに対応するブート・セクタとを識別する。

【００６１】

ブロック４１５において、ＡＳＦサウス・ブリッジ２１２をＡＳＦ　ＮＩＣ１０９に対するスレーブとして構成する際には、スレーブ状態を示すビットが、ＡＳＦイネーブル・レジスタ２５２にセットされ得る。ブロック４２０において、ＡＳＦサウス・ブリッジ２１２をＡＳＦマスターとして構成する際には、マスター状態を示すビットが、ＡＳＦイネーブル・レジスタ２５２にセットされ得る。

【００６２】

図７Ａは、本発明の一態様による、スレーブ・モードのＡＳＦサウス・ブリッジ２１２を備えたコンピュータ・システムの動作方法５００の実施形態を示すフローチャートである。スレーブ・モードのＡＳＦサウス・ブリッジ２１２は、ブロック５０５において、ＡＳＦ　ＮＩＣ１０９による内部センサ状態の読み出しに応答する。スレーブ・モードのＡＳＦサウス・ブリッジ２１２は、ブロック５１０において、ＡＳＦ　ＮＩＣ１０９が発したＳＭＢｕｓ２１５のポーリングに応答する。スレーブ・モードのＡＳＦサウス・ブリッジ２１２は、ＡＳＦ　ＮＩＣ１０９に制御ポイントを与える。これにより、ＡＳＦ　ＮＩＣ１０９は、コンピュータ・システム２００を一旦リセットしてコンピュータ・システム２００への電力を再供給できるようになる。

【００６３】

図７Ｂは、本発明の一態様による、マスター・モードのＡＳＦサウス・ブリッジ２１２を備えたコンピュータ・システムの動作方法６００の実施形態を示すフローチャートであ

る。マスター・モードのＡＳＦサウス・ブリッジ２１２は、ブロック６０５において、プログラム可能なポーリング周期で、ＳＭＢｕｓ２１５に結合された外部センサを能動的にポーリングする。マスター・モードのＡＳＦサウス・ブリッジ２１２は、ブロック６１０において、内部センサの状態を能動的にポーリングするかまたは監視する。マスター・モードのＡＳＦサウス・ブリッジ２１２は、ブロック６１５において、割り込みを発生させるか、割り込みに応答するか、この両方を行う。ブロック６２０において、取得した外部センサの状態の値と内部的に監視したセンサ値とがまとめられて、ＡＳＦサウス・ブリッジ２１２のイーサネット・コア３４４を介してリモート管理サーバー９０に報告される。

【００６４】

本開示のために、ＲＯＭに関して言及した箇所は、フラッシュ・メモリやその他の実質的な不揮発メモリにも適用されるものと解釈される。本明細書に記載した本発明の方法をフローチャートとして示したが、各種の実施形態においては、フローチャートの種々の要素が省略されても、異なる順序で実行されてもよいという点に留意すべきである。また、本明細書に記載した本発明の方法は、実装時に変形され得る。

【００６５】

上記に開示した本発明の態様の一部は、ハードウェアで実装されても、ソフトウェアで実装されてもよい。このため、本明細書の詳細な説明には、ハードウェアによって実装される処理として記載されたものもあれば、演算システムまたは演算装置のメモリ内のデータ・ビットの操作の記号的表記を含む、ソフトウェアによって実装される処理として記載されたものもある。このような記述および表現は、当業者が、ハードウェアおよびソフトウェアを用いた、自身の作業の内容を他の当業者に効率的に伝えるために用いられているものである。この処理および操作は、いずれも物理量の物理的な操作を必要とする。ソフトウェアにおいては、この物理量は通常、記憶、転送、結合、比較などの操作が可能な電気信号、磁気信号、または光学信号の形を取るが、必ずしもこれらに限定されない。主に公共の利用に供するという理由で、これらの信号を、ビット、値、要素、記号、文字、語（term）、数字などとして参照すれば、時として利便性が高いことが知られている。

【００６６】

しかし、上記の全用語ならびに類似の用語は、適切な物理量に関連付けられており、この物理量を表す簡便な標識に過ぎないという点を留意すべきである。特段の断りのない限り、もしくはそうではないことが自明ではない限り、本開示の全てにおいて、その記載内容は、電子装置の記憶領域内で物理（電子的、磁気的、または光学的な）量として表されるデータを、記憶装置、伝送装置または表示装置内で同様に物理量として表される他のデータへと操作および変換する電子装置の動作および処理を指す。このような内容を示す表現としては「処理」、「演算」、「計算」、「判定」、「表示」などがあるが、これらに限定されない。

【００６７】

ソフトウェアによって実装する本発明の態様は、典型的には、ある種のプログラム記憶媒体に符号化されているか、ある種の伝送媒体を介して実装されるという点に留意すべきである。プログラム記憶媒体は、磁気を利用したもの（例えば、フロッピー・ドライブやハード・ドライブ）でも、光学を利用したもの（例えば、コンパクト・ディスクの読み取り専用記憶装置、すなわち「ＣＤ－ＲＯＭ」）でもよく、読み取り専用であっても、ランダム・アクセス可能なものであってもよい。同様に、伝送媒体は、より線対、同軸ケーブル、ファイバのほか、当業界に公知の伝送媒体であってもよい。本発明は、いずれの特定の実装の態様にも限定されない。

【００６８】

上記に記載した特定の実施形態は例に過ぎず、本発明は、本開示の教示から利益を得る当業者にとって自明の、同等の別法によって変更および実施されてもよい。さらに、ここに記載した構成または設計の詳細が、添付の特許請求の範囲以外によって制限を受けることはない。このため、上記に記載した特定の実施形態を変形または変更することが可能であり、この種の変形例の全てが本発明の範囲ならびに趣旨に含まれることが意図されるこ

とが明らかである。したがって、ここに保護を請求する対象は、添付の特許請求の範囲に記載したとおりである。

【図面の簡単な説明】

【００６９】

【図１Ａ】先行技術によるコンピュータ・システムのブロック図である。

【図１Ｂ】先行技術によるサウス・ブリッジのブロック図である。

【図１Ｃ】先行技術によるリモート管理構成を示す図である。

【図２】従来技術による、ＲＯＭに記憶されたコードを使用してコンピュータ・システムを初期化する方法のフローチャートである。

【図３Ａ】本発明の各種態様によるリモート管理構成を備えたコンピュータ・システムの実施形態のブロック図である。

【図３Ｂ】本発明の各種態様によるリモート管理構成を備えたコンピュータ・システムの実施形態のブロック図である。

【図４】本発明の各種態様による、ＡＳＦ機能、ＡＣＰＩ機能、および／またはイーサネット機能が統合されたＡＳＦサウス・ブリッジの一実施形態のブロック図である。

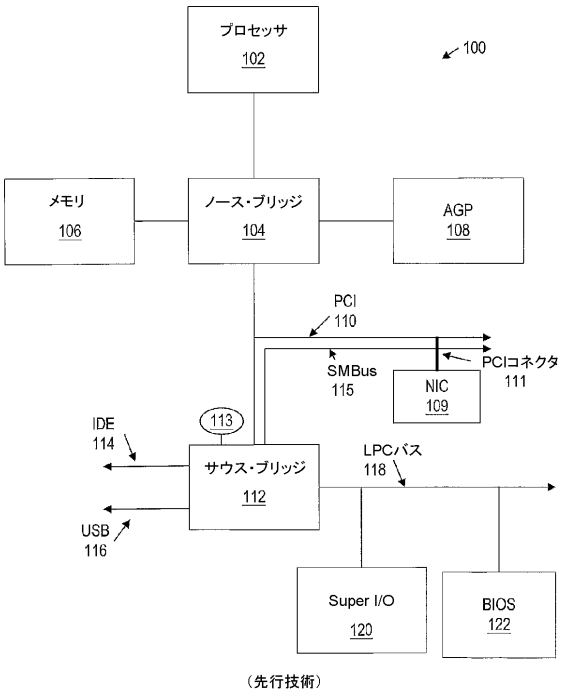
【図５】本発明の各種態様による、ＡＳＦサウス・ブリッジのＲＴＣバッテリ・ウェル内にＡＳＦレジスタを有するＡＳＦサウス・ブリッジの一実施形態のブロック図である。

【図６】本発明の一態様による図４のＡＳＦサウス・ブリッジを備えたコンピュータ・システムのブート方法の一実施形態を示すフローチャートである。

【図７Ａ】本発明の各種態様による図４のＡＳＦサウス・ブリッジを備えたコンピュータ・システムの動作方法の実施形態を示すフローチャートである。

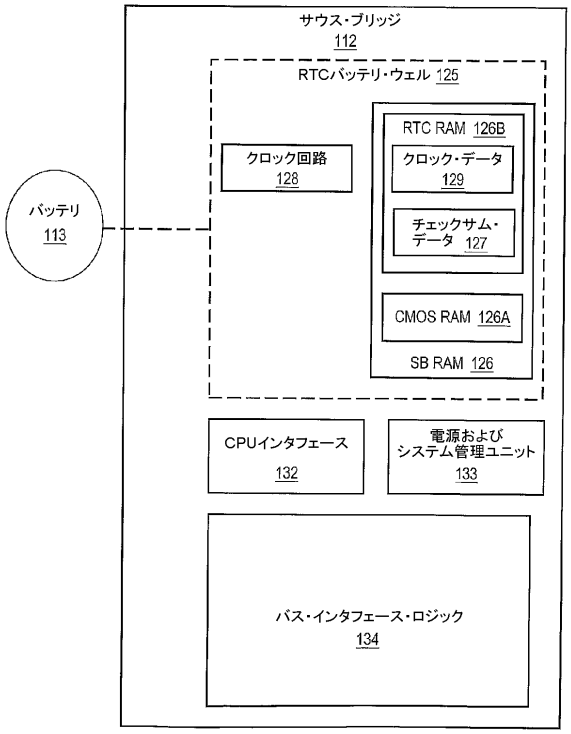
【図７Ｂ】本発明の各種態様による図４のＡＳＦサウス・ブリッジを備えたコンピュータ・システムの動作方法の実施形態を示すフローチャートである。

【図１Ａ】



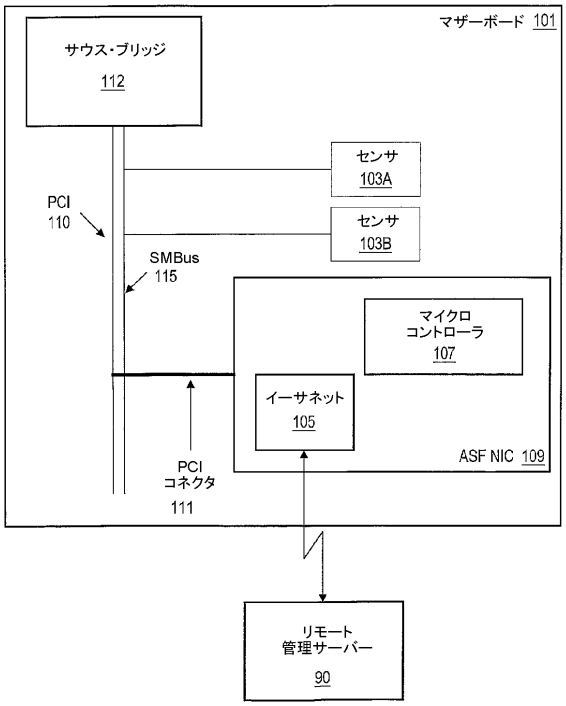
（先行技術）

【図１Ｂ】



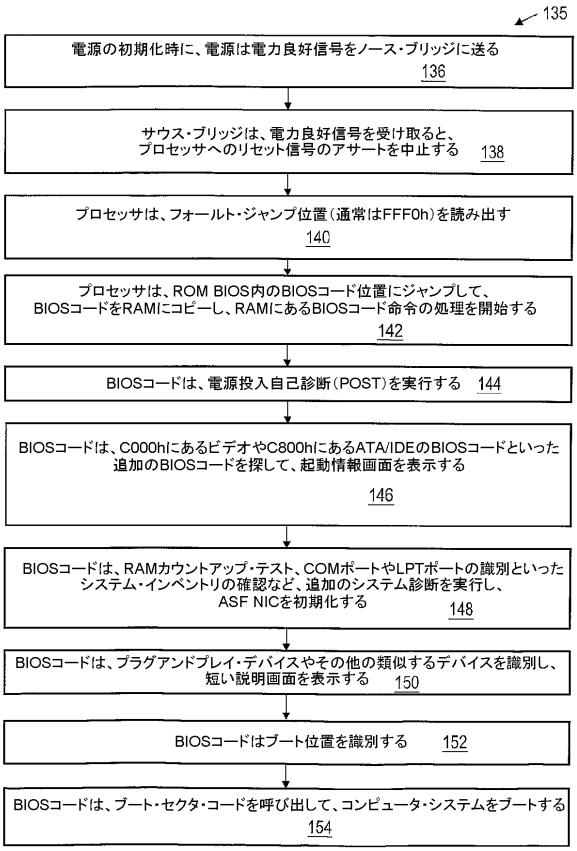
（先行技術）

【図１Ｃ】



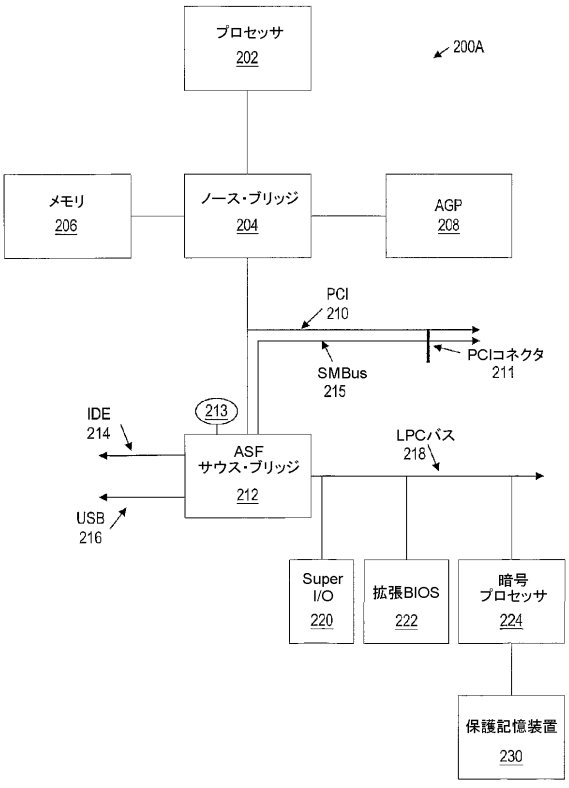
（先行技術）

【図２】

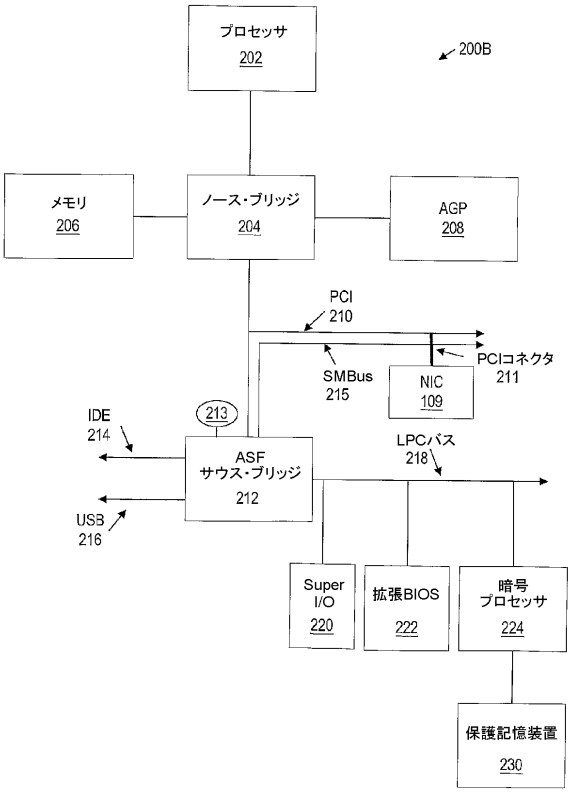


（先行技術）

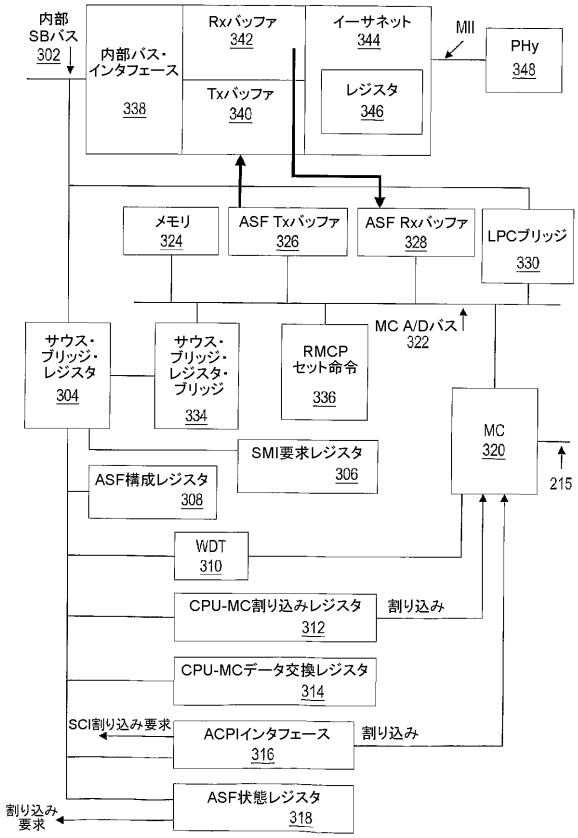
【図３Ａ】



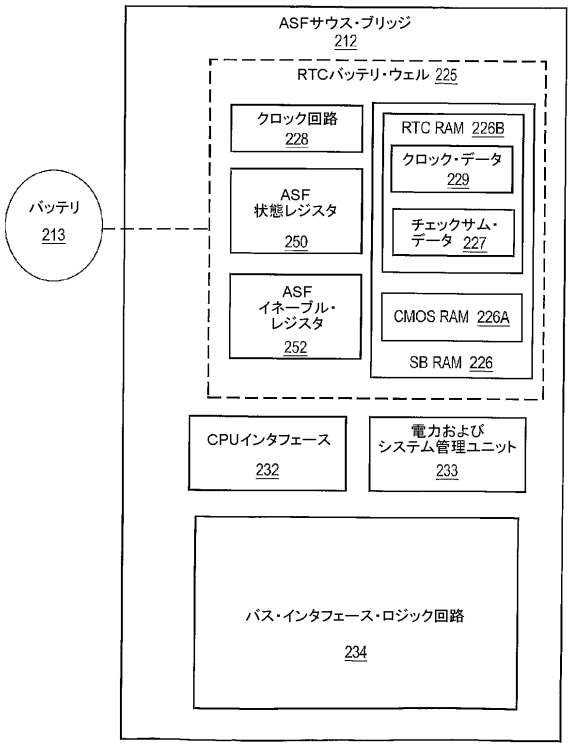
【図３Ｂ】



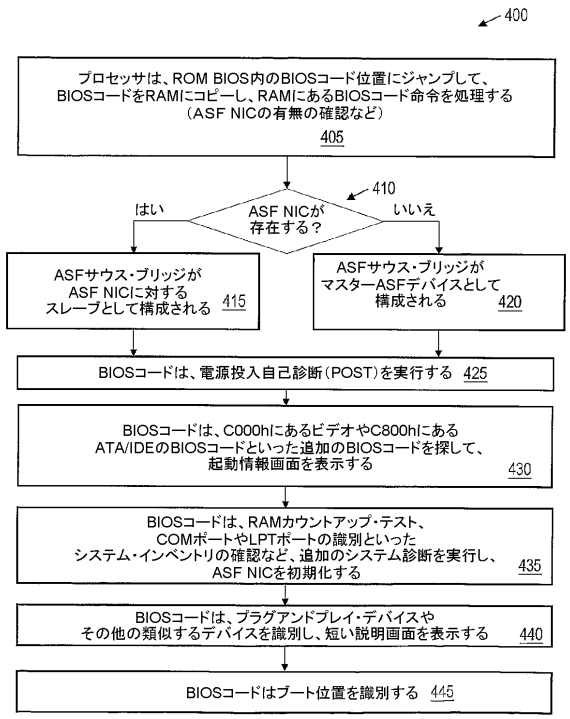
【図４】



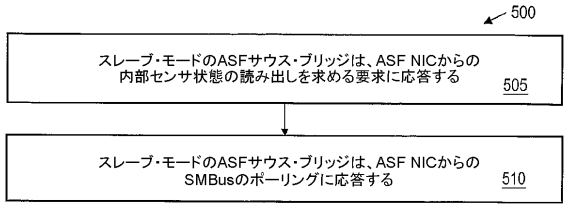
【図５】



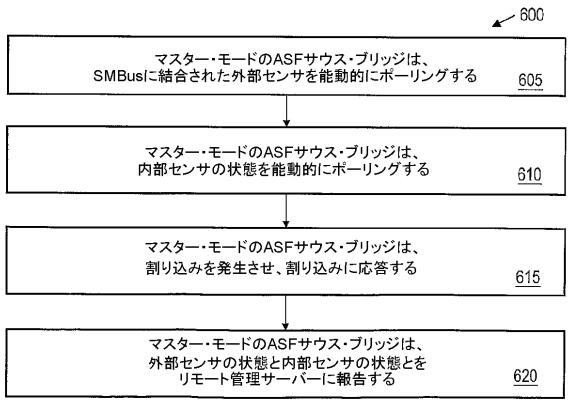
【図６】



【図７Ａ】



【図７Ｂ】



フロントページの続き

(74)代理人 100108604
弁理士 村松 義人
(72)発明者 デイル イー. ガリック
アメリカ合衆国、テキサス州 ７８７３８、オースティン、アストリア ドライブ １１７１５

審査官 須藤 竜也

(56)参考文献 特開平１１－１４９４３３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/36