【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2005-515517(P2005-515517A)
【公表日】平成17年5月26日(2005.5.26)
【年通号数】公開・登録公報2005-020
【出願番号】特願2002-589945(P2002-589945)
【国際特許分類】
Ｇ０６Ｆ　21/02　　(2006.01)
Ｇ０６Ｆ　 9/46　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５１０Ｃ
Ｇ０６Ｆ　 9/46　　３６０Ｄ

【手続補正書】
【提出日】平成17年10月27日(2005.10.27)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
バスと、
前記バスに接続されたメモリであって、複数のメモリユニットに分割された複数の格納位置を含むメモリと、
前記バス経由で前記メモリにアクセスすべく接続されたデバイスとを含むコンピュータシステムであって、
前記デバイスは、コンピュータシステムがシステムマネージメントモード（ＳＭＭ）で動作しているかどうかを判定するように構成され、
コンピュータシステムがシステムマネージメントモード（ＳＭＭ）で動作しているかどうかの前記判定に基づいて、
前記複数のメモリユニットのうちの１以上に対するアクセスを制御するように構成可能に構成された１以上のロックを含む、コンピュータシステム。
【請求項２】
前記メモリがＲＯＭである、請求項１記載のコンピュータシステム。
【請求項３】
前記ＲＯＭがＢＩＯＳ　ＲＯＭである、請求項２記載のコンピュータシステム。
【請求項４】
前記ロックが複数のレジスタを含み、前記複数のレジスタのうちの１以上における１以上のエントリが、前記メモリユニットのうちの１以上に対するアクセス制御設定を示すものである、請求項１記載のコンピュータシステム。
【請求項５】
前記複数のレジスタのうちの少なくとも１つが前記メモリブロックのうちの１つに対する３つのロックビットを格納するように構成され、これらの３つのロックビットが、読み出しロックビット、書き込みロックビット、ロックダウンビットであり、前記ロックダウンビットが設定されている間は前記読み出しロックビットと前記書き込みロックビットとがリセットまで永続する、請求項４記載のコンピュータシステム。
【請求項６】

前記複数のレジスタのうちの少なくとも１つが、８ビットを格納するように構成され、これらの８ビットが、前記メモリブロックのうちの１つに対する３つのロックビットと、前記メモリブロックのうちの別の１つに対する別の３つのロックビットとを含み、これら３つのロックビットが、第１の読み出しロックビットと、第１の書き込みロックビットと、第１のロックダウンビットとを含み、前記第１のロックダウンビットが設定されている間は、前記第１の読み出しロックビットと前記第１の書き込みロックビットとがリセットまで永続し、前記別の３つのロックビットが、第２の読み出しロックビットと、第２の書き込みロックビットと、第２のロックダウンビットとを含み、前記第２のロックダウンビットが設定されている間は前記第２の読み出しロックビットと前記第２の書き込みロックビットとがリセットまで永続する、請求項４記載のコンピュータシステム。

【請求項７】

ＢＩＯＳデータが組み込まれた複数の第１の格納位置と、

複数の第２の格納位置であって、

ＳＭＭにおいてのみ読み取り可能な複数の第１のブロックと、

ＳＭＭならびにＳＭＭ以外の少なくとも１つの動作モードにおいて読み取り可能な複数の第２のブロックとを含む複数の第２の格納位置と、

を含むメモリ。

【請求項８】

前記複数の第１のブロックが、

書き込み１回ロックのあるブロックと、

消去不可ロックのあるブロックと、

ＳＭＭならびにＳＭＭ以外の少なくとも１つの動作モードで書き込み可能なブロックと、

のうちの少なくとも１つを含む、請求項７記載のメモリ。

【請求項９】

前記複数の第２のブロックが、

書き込み１回ロックのあるブロックと、

消去不可ロックのあるブロックと、

ＳＭＭならびにＳＭＭ以外の少なくとも１つの動作モードで書き込み可能なブロックと、

のうちの少なくとも１つを含む、請求項７記載のメモリ。

【請求項１０】

コンピュータシステムを動作させるための方法であって、

１以上のメモリアドレスに対するメモリトランザクションを要求する処理と、

前記１以上のメモリアドレスのロックステータスを判断する処理と、

前記１以上のメモリアドレスのロックステータスを返す処理と、

コンピュータシステムがシステムマネージメントモード（ＳＭＭ）で動作しているかどうかを判定する処理と、

コンピュータシステムがシステムマネージメントモード（ＳＭＭ）で動作しているかどうかの前記判定に基づいて、前記１以上のメモリアドレスに対するメモリトランザクションが許可されていないことが前記ロックステータスで示された場合に、前記１以上のメモリアドレスのロックステータスを変更可能であるか否かを判断する処理と、

前記１以上のメモリアドレスのロックステータスが変更可能である場合に、前記１以上のメモリアドレスのロックステータスを変更して前記メモリトランザクションを許可する処理とを含む、方法。

【請求項１１】

前記ロックステータスを判断する処理が、第１のロックビットを読み出す処理を含み、前記ロックステータスを返す処理が、前記第１のロックビットの値を返す処理を含む、請求項１０記載の方法。

【請求項１２】

前記１以上のメモリアドレスのロックステータスを変更可能であるか否かを判断する処理が、第２のロックビットを読み出す処理を含む、請求項１１記載の方法。
【請求項１３】
前記１以上のメモリアドレスのロックステータスを変更してメモリトランザクションを許可する処理が、前記第１のロックビットの値を変更する処理を含む、請求項１２記載の方法。
【請求項１４】
いずれかの記憶位置に対するメモリトランザクションの要求を第１のデバイスから発行する処理と、
このメモリトランザクションの要求を、前記記憶位置あるいはその記憶位置の内容のコピーを含まない第２のデバイスで受信する処理と、
前記メモリトランザクションの要求を発行した第１のデバイスに前記第２のデバイスから応答を返す処理とを含む、コンピュータシステムを動作させる方法。
【請求項１５】
前記第２のデバイスから応答を返す処理が、前記メモリトランザクションを前記記憶位置に到達させることなく前記メモリトランザクションを終える処理を含む、請求項１４記載の方法。
【請求項１６】
前記メモリトランザクションの要求に記憶位置で答えることなく前記メモリトランザクションの要求を終える処理をさらに含む、請求項１４記載の方法。
【請求項１７】
前記第２のデバイスが、前記第１のデバイスと前記記憶位置との間に接続されたブリッジを含み、前記メモリトランザクションの要求を発行した第１のデバイスに第２のデバイスから前記応答を返す処理が、前記メモリトランザクションの要求を発行した第１のデバイスに前記ブリッジから応答を返す処理を含む、請求項１４記載の方法。
【請求項１８】
コンピュータシステムが第１の動作モードで動作している場合に、前記メモリトランザクションの要求を発行した第１のデバイスにブリッジから前記応答を返す処理が、前記記憶位置に対するメモリトランザクションの要求の受信時にあらかじめ定められた値を持つ前記ブリッジ内のアクセスフィルタから応答する処理を含む、請求項１７記載の方法。
【請求項１９】
前記記憶位置に対するメモリトランザクションの要求を前記第１のデバイスから発行する処理が、メモリ、ＲＯＭまたはフラッシュメモリ内の記憶位置に対するメモリトランザクションの要求を前記第１のデバイスから発行する処理を含む、請求項１８記載の方法。
【請求項２０】
前記第１のデバイスがセキュリティハードウェアを含み、前記メモリトランザクションの要求を前記記憶位置あるいはその記憶位置の内容のコピーを含まない第２のデバイスで受信する処理が、前記第１のデバイス内のセキュリティハードウェアで前記メモリトランザクションの要求を受信する処理を含み、前記メモリトランザクションの要求を発行した第１のデバイスに前記第２のデバイスから応答を返す処理が、メモリトランザクションの要求を発行した前記第１のデバイスに前記セキュリティハードウェアから応答を返す処理を含む、請求項１４記載の方法。
【請求項２１】
前記応答を返す前に前記第２のデバイス内の記憶位置から第１の値を読み出す処理をさらに含み、前記第２のデバイス内の前記記憶位置が前記メモリトランザクション用の記憶位置とは異なるものである、請求項１４記載の方法。