(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5535547号
(P5535547)

(45)発行日　平成26年7月2日(2014.7.2)　(24)登録日　平成26年5月9日(2014.5.9)

(51)Int.Cl.　F I
G06F 12/16 (2006.01)　G06F 12/16 310B
G06F 12/16 310C

請求項の数 26　(全 23 頁)

(21)出願番号　特願2009-187810(P2009-187810)
(22)出願日　平成21年8月13日(2009.8.13)
(65)公開番号　特開2010-86523(P2010-86523A)
(43)公開日　平成22年4月15日(2010.4.15)
審査請求日　平成24年7月27日(2012.7.27)
(31)優先権主張番号　10-2008-0096574
(32)優先日　平成20年10月1日(2008.10.1)
(33)優先権主張国　韓国(KR)
(31)優先権主張番号　12/319,788
(32)優先日　平成21年1月12日(2009.1.12)
(33)優先権主張国　米国(US)

(73)特許権者　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市霊通区三星路１２９
１２９，Ｓａｍｓｕｎｇ－ｒｏ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆

最終頁に続く

(54)【発明の名称】セキュアメモリインターフェース

(57)【特許請求の範囲】
【請求項１】
セキュアモードが活性化された場合に、メモリ装置から受信された初期読出データからエラー検出コードを分離してデータプロセッシング部に送信される最終読出データを生成する読出部と、
前記データプロセッシング部からのメモリアクセス情報を使用して前記セキュアモードを活性化または非活性化させるモード選択部と、を含み、
前記最終読出データのデータ幅が１６ビットの場合には前記エラー検出コードは１６ビットであり、前記最終読出データのデータ幅が２４ビットの場合には前記エラー検出コードは８ビットである
ことを特徴とするセキュアメモリインターフェース。
【請求項２】
前記読出部は、
前記セキュアモードが非活性化された場合に、前記初期読出データから前記エラー検出コードを分離せず、前記最終読出データを生成することを特徴とする請求項１記載のセキュアメモリインターフェース。
【請求項３】
前記メモリアクセス情報は、命令語名称を含み、
前記モード選択部は、前記命令語名称がセキュア読出命令語に該当する場合に、前記セキュアモードを活性化させ、前記命令語名称が通常の読出命令語に該当する場合に、前記

セキュアモードを非活性化させる命令語デコーダーを含むことを特徴とする請求項２記載のセキュアメモリインターフェース。
【請求項４】
前記読出部及び前記命令語デコーダーは、中央処理装置ＣＰＵである前記データプロセッシング部の内部に配置されることを特徴とする請求項３記載のセキュアメモリインターフェース。
【請求項５】
前記メモリアクセス情報は、前記初期読出データのためにアクセスされる前記メモリ装置のアドレスを含み、
前記モード選択部は、前記アクセスされるメモリ装置のアドレスがセキュアアドレスである場合に、前記セキュアモードを活性化させ、前記アクセスされるメモリ装置のアドレスが非セキュアアドレスである場合に、前記セキュアモードを非活性化させるアドレスデコーダーを含むことを特徴とする請求項２記載のセキュアメモリインターフェース。
【請求項６】
前記アドレスデコーダーは、前記アクセスされるメモリ装置のアドレスを生成するＣＰＵである前記データプロセッシング部の外部に配置されることを特徴とする請求項５記載のセキュアメモリインターフェース。
【請求項７】
前記メモリアクセス情報はレジスタ名称を含み、
前記モード選択部は、前記レジスタ名称が前記セキュアモードの活性化または非活性化に相応するかの有無を示す各々のレジスタフラグを含むことを特徴とする請求項２記載のセキュアメモリインターフェース。
【請求項８】
前記読出部と前記各々のレジスタフラグは、ＣＰＵである前記データプロセッシング部の内部に配置されることを特徴とする請求項７記載のセキュアメモリインターフェース。
【請求項９】
前記読出部は、
前記セキュアモードが活性化された場合に、前記初期読出データから前記エラー検出コードを分離して最終読出データを生成し、前記セキュアモードが非活性化された場合に、前記初期読出データから前記エラー検出コードを分離せず前記最終読出データを生成するデミキサ（ｄｅｍｉｘｅｒ）と、
相応するアドレスまたは最終読出しデータのうち、少なくとも何れかの１つから予想エラー検出コードを生成するエンコーダーと、
前記初期読出データから分離された前記エラー検出コードと前記予想エラー検出コードを比較してエラー検出信号を生成する比較器と、
を含むことを特徴とする請求項１記載のセキュアメモリインターフェース。
【請求項１０】
前記読出部は、
前記メモリアクセス情報からメモリアドレス及び読出イネーブル信号を生成して前記メモリ装置から前記初期読出データを読み出す状態機械と、
少なくとも１つのデータ幅制御信号に従ったメモリデータ幅を有する前記初期読出データを読み出すように前記状態機械を制御する幅選択器と、をさらに含み、
前記少なくとも１つのデータ幅制御信号は、前記エンコーダーと前記デミキサの動作も制御することを特徴とする請求項９記載のセキュアメモリインターフェース。
【請求項１１】
前記メモリデータ幅は、前記メモリ装置に相応し、
前記少なくとも１つのデータ幅制御信号は、前記データプロセッシング部のプロセッシングデータ幅に相応することを特徴とする請求項１０記載のセキュアメモリインターフェース。
【請求項１２】

前記データプロセッシング部は、バスによって前記メモリ装置から分離されたＣＰＵであることを特徴とする請求項１１記載のセキュアメモリインターフェース。
【請求項１３】
前記データプロセッシング部及び前記メモリ装置は、１つの集積回路チップで製作されることを特徴とする請求項１２記載のセキュアメモリインターフェース。
【請求項１４】
前記データプロセッシング部及び前記メモリ装置は２つの分離された集積回路チップで製作されることを特徴とする請求項１２記載のセキュアメモリインターフェース。
【請求項１５】
セキュアモードが活性化された場合に、初期書込データ及び前記エラー検出コードから前記メモリ装置に書込まれるための最終書込データを生成し、前記セキュアモードが非活性化された場合に、前記エラー検出コード無しで前記初期書込データから前記最終書込データを生成する書込部をさらに含むことを特徴とする請求項１記載のセキュアメモリインターフェース。
【請求項１６】
前記書込部及び前記読出部は、ハードウェア論理ゲートで具現されることを特徴とする請求項１５記載のセキュアメモリインターフェース。
【請求項１７】
セキュアモードが活性化された場合に、初期書込データ及びエラー検出コードからメモリ装置に書込されるための最終書込データを生成する書込部と、
データプロセッシング部から生成されたメモリアクセス情報を使用して前記セキュアモードを活性化または非活性化させるモード選択部と、を含み、
前記初期書込データのデータ幅が１６ビットの場合には前記エラー検出コードは１６ビットであり、前記初期書込データのデータ幅が２４ビットの場合には前記エラー検出コードは８ビットである
ことを特徴とするセキュアメモリインターフェース。
【請求項１８】
前記書込部は、
前記セキュアモードが非活性化された場合に、前記エラー検出コード無しで前記初期書込データから前記最終書込データを生成することを特徴とする請求項１７記載のセキュアメモリインターフェース。
【請求項１９】
前記メモリアクセス情報は、命令語名称を含み、
前記モード選択部は、前記命令語名称がセキュア書込命令語に該当する場合に、前記セキュアモードを活性化させ、前記命令語名称が通常の書込命令語に該当する場合に、前記セキュアモードを非活性化させる命令語デコーダーを含むことを特徴とする請求項１８記載のセキュアメモリインターフェース。
【請求項２０】
前記メモリアクセス情報は、アクセスされる前記メモリ装置のアドレスを含み、
前記モード選択部は、前記アクセスされるメモリ装置のアドレスがセキュアアドレスである場合に、前記セキュアモードを活性化させ、前記アクセスされるメモリ装置のアドレスが非セキュアアドレスである場合に、前記セキュアモードを非活性化させるアドレスデコーダーを含むことを特徴とする請求項１８記載のセキュアメモリインターフェース。
【請求項２１】
前記メモリアクセス情報は、レジスタ名称を含み、
前記モード選択部は、前記レジスタ名称が前記セキュアモードの活性化または非活性化に相応するかの有無を示す各々のレジスタフラグを含むことを特徴とする請求項１８記載のセキュアメモリインターフェース。
【請求項２２】
前記書込部は、

相応するアドレスまたは前記初期書込データのうち、少なくとも１つから前記エラー検出コードを生成するエンコーダーと、
前記セキュアモードが活性化された場合に、前記初期書込データ及び前記エラー検出コードから混合書込データを生成し、前記セキュアモードが非活性化された場合に、前記エラー検出コード無しで前記初期書込データから前記混合書込データを生成するミキサ（ｍｉｘｅｒ）を含み、
前記混合書込データは前記最終書込データを決めることを特徴とする請求項１８記載のセキュアメモリインターフェース。
【請求項２３】
前記書込部は、
前記混合書込データから前記最終書込データ、書込イネーブル信号及び前記最終書込データを保存する前記メモリ装置のメモリアドレスを生成する状態機械と、
少なくとも１つのデータ幅制御信号によるメモリデータ幅を有する前記最終書込データを生成するように前記状態機械を制御する幅選択器をさらに含み、
前記少なくとも１つのデータ幅制御信号は、前記データプロセッシング部のプロセッシングデータ幅に相応し、
前記少なくとも１つのデータ幅制御信号は、前記エンコーダーと前記ミキサの動作を制御することを特徴とする請求項２２記載のセキュアメモリインターフェース。
【請求項２４】
前記データプロセッシング部は、バスによって前記メモリ装置から分離されたＣＰＵであることを特徴とする請求項２３記載のセキュアメモリインターフェース。
【請求項２５】
前記データプロセッシング部及び前記メモリ装置は１つの集積回路チップで製作されることを特徴とする請求項２４記載のセキュアメモリインターフェース。
【請求項２６】
前記データプロセッシング部及び前記メモリ装置は、２つの分離された集積回路チップで製作されることを特徴とする請求項２４記載のセキュアメモリインターフェース。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、メモリ装置及びデータプロセッシング部を含む電子システムに関する。より詳しくは、データプロセッシング部を通じてメモリ装置へのセキュアアクセスまたは通常のアクセスを柔軟に制御する電子システムに関する。
【背景技術】
【０００２】
メモリ装置は、レーザーまたはレントゲンの使用などによる欠陥注入攻撃（ｆａｕｌｔ ｉｎｊｅｃｔｉｏｎ ａｔｔａｃｋ）を受けやすい。例えば、レーザーとレントゲンはメモリ装置内のビットの状態を変更させることができる精密な攻撃が可能である。特に、レーザーはレジスタ、ＲＡＭ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ）、ＥＥＰ（ｅｌｅｃｔｒｉｃａｌｌｙ ｅｒａｓａｂｌｅ ａｎｄ ｐｒｏｇｒａｍｍａｂｌｅ）、フラッシュメモリ装置などを欠陥注入するのに適している。このような欠陥注入は、永久的であるかまたは一時的であってもよい。
【０００３】
また、このような欠陥注入攻撃は、暗証番号を露出させるかまたはメモリに書込まれた内容を流出させるのに使用してもよい。メモリ装置に保存された情報の誤用または悪用を防ぐためにこのようなメモリ装置への欠陥注入（ｆａｕｌｔ ｉｎｊｅｃｔｉｏｎ）を検出することが必要である。
【０００４】
従来の技術において、レーザー光源を検出するためにレーザー検出器が使用された。しかし、レーザー検出器は、メモリ装置に対するレーザー攻撃を検出するのに適合ではない

。
【０００５】
また、他の従来技術においては、メモリ装置はエラー検出コードを保存して適応される。この場合、メモリ装置は前記メモリ装置内部の欠陥注入攻撃を検出する。しかし、メモリ装置内部に検出コードを実装するこのような方法は、メモリ装置のシリコン面積を増加させる。さらに、ビットの状態がメモリ装置外部のバスを通じて変更されると、エラー検出コードはこのようなメモリ装置の外部から発生した欠陥注入を検出できない可能性がある。
【０００６】
従来技術では、メモリ装置はメモリ装置内部で欠陥注入を検出するために余分のデータを保存するハードウェア冗長（ｒｅｄｕｎｄａｎｃｙ）を含むことができる。しかし、このような保存冗長によって特に大きなシリコン面積を有する高容量のメモリ装置において、シリコン面積が重複される結果が発生する。また、保存冗長のデータ検証によってメモリ装置の動作が遅くなることがあることがある。
【０００７】
また、別の従来技術において、メモリ装置にアクセスするＣＰＵ（ｃｅｎｔｒａｌ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ）のようなデータプロセッシング部はデータのインテグリティ（ｉｎｔｅｇｒｉｔｙ）を確認するソフトウェアを含む。しかし、メモリ装置に保存されたこのようなソフトウェアもやはり欠陥注入攻撃を受けやすい。さらに、ＣＰＵのソフトウェアに対するコードの大きさと実行時間が追加的データ検証機能によって増加する。
【０００８】
従って、メモリ装置の内部及びメモリ装置のバスにまたはバスからなどメモリ装置の外部の欠陥注入を検出するための効率的なメカニズムが要求される。
【発明の概要】
【発明が解決しようとする課題】
【０００９】
前述のような問題点を解決するために、本発明は欠陥注入を自動的に検出するように作動するセキュアメモリインターフェースを提供することを一目的とする。
【課題を解決するための手段】
【００１０】
前記目的を達成するために、本発明の一実施形態によるセキュアメモリインターフェースは、読出部及びモード選択部を含む。読出部はセキュアモードが活性化された場合、メモリ装置から受信された初期読出データからエラー検出コードを分離してデータプロセッシング部に送信される最終読出データを生成する。モード選択部は、前記データプロセッシング部から生成されたメモリアクセス情報を使用して前記セキュアモードを活性化または非活性化させる。
【００１１】
一実施形態において、前記読出部は前記セキュアモードが非活性化された場合、前記初期読出データから前記エラー検出コードを分離せずに前記最終読出データを生成することができる。
【００１２】
一実施形態において、前記メモリアクセス情報は、命令語名称を含んでもよい。この場合、前記モード選択部は、前記命令語名称がセキュア読出命令語に該当する場合、前記セキュアモードを活性化させ、前記命令語名称が通常の読出命令語に該当する場合、前記セキュアモードを非活性化させる命令語デコーダーを含んでもよい。前記読出部及び前記命令語デコーダーは、前記データプロセッシング部、即ち、中央処理装置（ＣＰＵ：Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）内部に配置されてもよい。
【００１３】
他の実施形態において、前記メモリアクセス情報は前記初期読出データのためにアクセ

スされる前記メモリ装置のアドレスを含んでもよい。この場合、前記モード選択部は、前記アクセスされるメモリ装置のアドレスがセキュアアドレスである場合、前記セキュアモードを活性化させ、前記アクセスされるメモリ装置のアドレスが非セキュアアドレスである場合、前記セキュアモードを非活性化させるアドレスデコーダーを含んでもよい。前記アドレスデコーダーは、前記アクセスされるメモリ装置のアドレスを生成するＣＰＵである前記データプロセッシング部の外部に配置されてもよい。

【００１４】

また他の実施形態において、前記メモリアクセス情報はレジスタ名称を含んでもよい。この場合、前記モード選択部は、前記レジスタ名称が前記セキュアモードの活性化または非活性化に相応するかを示す各々のレジスタフラグを含んでもよい。前記読出部と前記各々のレジスタフラグは、ＣＰＵである前記データプロセッシング部の内部に配置されることができる。

【００１５】

一実施形態において、前記読出部はデミキサ(demixer)、エンコーダー、及び比較器を含んでもよい。前記デミキサは、前記セキュアモードが活性化された場合、前記初期読出データから前記エラー検出コードを分離して前記最終読出データを生成し、前記セキュアモードが非活性化された場合、前記初期読出データから前記エラー検出コードを分離せずに前記最終読出データを生成する。前記エンコーダーは相応するアドレスまたは前記最終読出データのうち、少なくとも何れかの１つから予想エラー検出コードを生成する。前記比較器は前記初期読出データから分離された前記エラー検出コードと前記予想エラー検出コードを比較してエラー検出信号を生成する。

【００１６】

他の実施形態において、前記読出部は状態機械(state machine)及び幅選択器をさらに含むことができる。前記状態機械は、前記メモリアクセス情報からメモリアドレス及び読出イネーブル信号を生成して前記メモリ装置から前記初期読出データを読み出す。前記幅選択器は、前記エンコーダーと前記デミキサの動作を制御する、少なくとも１つのデータ幅制御信号によるメモリデータ幅を有する前記初期読出データを読み出すように前記状態機械を制御する。

【００１７】

一実施形態において、前記メモリデータ幅は前記メモリ装置に相応し、前記少なくとも１つのデータ幅制御信号は、前記データプロセッシング部のプロセッシングデータ幅に相応することができる。

【００１８】

一実施形態において、前記データプロセッシング部はバスによって前記メモリ装置から分離されたＣＰＵであってもよい。前記データプロセッシング部及び前記メモリ装置は、１つの集積回路チップで製作されてもよい。他の実施形態において、前記データプロセッシング部及び前記メモリ装置は２つの分離された集積回路チップで製作されてもよい。

【００１９】

他の実施形態において、前記セキュアメモリインターフェースは、前記セキュアモードが活性化された場合、初期書込データ及び前記エラー検出コードから前記メモリ装置に書込むための最終書込データを生成する書込部をさらに含んでもよい。前記書込部は、前記セキュアモードが非活性化された場合、前記エラー検出コードなしで前記初期書込データから前記最終書込データを生成する。

【００２０】

一実施形態において、前記書込部及び前記読出部は、ハードウェア論理ゲートで前記ＣＰＵ内に具現されることができる。

【００２１】

前記メモリアクセス情報が命令語名称を含む場合、前記命令語デコーダーは前記命令語名称がセキュア書込命令語に該当する場合、前記セキュアモードを活性化させ、前記命令語名称が通常の書込命令語に該当する場合、前記セキュアモードを非活性化させることが

できる。

【００２２】

一実施形態において、前記書込部はエンコーダー及びミキサを含んでもよい。前記エンコーダーは相応するアドレスまたは前記初期書込データのうち、少なくとも１つから前記エラー検出コードを生成する。前記ミキサは、前記セキュアモードが活性化された場合、前記初期書込データ及び前記エラー検出コードから混合書込データを生成し、前記セキュアモードが非活性化された場合、前記エラー検出コード無しで前記初期書込データから前記混合書込データを生成する。前記混合書込データは、前記最終書込データを決める。

【００２３】

他の実施形態において、前記書込部は状態機械及び幅選択器をさらに含んでもよい。前記状態機械は、前記混合書込データから前記最終書込データ、書込イネーブル信号、及び前記最終書込データを保存する前記メモリ装置のメモリアドレスを生成する。前記幅選択器は、前記エンコーダーと前記ミキサの動作を制御する少なくとも１つのデータ幅制御信号によるメモリデータ幅を有する前記最終書込データを生成するように前記状態機械を制御する。本発明の一実施形態に従った電子システムは、メモリ装置、データプロセッシング部、及びインターフェース部を含む。前記データプロセッシング部は、メモリ装置に対するアクセス種類を指定する少なくとも１つのアドレスビットまたはレジスタ名称を含むメモリアクセス情報を生成する。前記インターフェース部は、前記メモリアクセス方法によって指定された前記アクセス種類に基づいて前記メモリ装置にアクセスする。一実施形態において、前記アクセス種類は、セキュアアクセスまたは非セキュアアクセスを含んでもよい。前記データプロセッシング部から生成された前記少なくとも１つのアドレスビットは、前記メモリ装置に対する前記アクセス種類を決定することができる。他の実施形態において、前記データプロセッシング部から生成された前記レジスタ名称は前記メモリ装置に対する前記アクセス種類を決定することができる。

【００２４】

このような方式で、ＣＰＵはセキュアアクセスのためにメモリ装置に保存されたデータの量と位置を柔軟に指定することができる。欠陥注入はハードウェアで具現された書込部と読出部を使用するＣＰＵで指定された前記データによって検出される。従って、書込部と読出部のシリコン面積の増加は、どの容量のメモリ装置においても大きな影響を及ぼさない。さらに、メモリ装置内またはＣＰＵとメモリ装置との間のバスで発生する欠陥注入が効率的に検出される。

【００２５】

本文に開示されている本発明の実施形態に対して、特定の構造的乃至は機能的説明は、単に本発明の実施形態を説明するための目的で例示されたもので、本発明の実施形態は多様な形態で実施することができ、本文に説明された実施形態に限定されることと解釈されてはいけない。

【００２６】

本発明は多様な変更を加えることができ、様々な形態を有することができるため、特定実施例を図面に例示し、本明細書に詳しく説明する。しかし、これは本発明を特定の開示形態に対して限定しようとすることではなく、本発明の思想及び技術範囲に含まれる全ての変更、均等物、ないしは代替物を含むことと理解されるべきである。各図面を説明しながら類似する参照符号を、類似する構成要素に対して使用した。

【００２７】

第１、第２などの用語は多様な構成要素を説明するにあたって使用することができるが、各構成要素は使用される用語によって限定されるものではない。各用語は１つの構成要素を他の構成要素と区別する目的で使用されるものであって、例えば、明細書中において、第１構成要素を第２構成要素に書き換えることも可能であり、同様に第２構成要素を第１構成要素とすることができる。

【００２８】

有る構成要素が他の構成要素に「連結されて」いるかまたは「接続されて」いると言及

された際には、その他の構成要素に直接的に連結されているかまたは接続されていることもあるが、中間に他の構成要素が存在することもあると理解するべきである。反面、有る構成要素が他の構成要素に「直接連結されて」いるかまたは「直接接続されて」いると言及された際には、中間に他の構成要素が存在しないことと理解するべきである。構成要素間の関係を説明する他の表現、即ち、「～間に」と「すぐ～間に」、または「～に隣接する」と「～に直接隣接する」なども同様に解釈するべきである。

【００２９】

本明細書で使用する用語は、「含む」または「有する」などの用語は、明細書上に記載された特徴、数字、段階、動作、構成要素、部分品、またはこれらを組み合わせたものが存在することを指定しようとすることであって、１つまたはそれ以上の別の特徴、数字、段階、動作、構成要素、部分品、またはこれらを組み合わせたものの存在または付加可能性を予め排除しないことと理解されるべきである。

【００３０】

また、別に定義しない限り、技術的或いは科学的用語を含んで、ここにおいて使用される全ての用語は本発明が属する技術分野で通常の知識を有する者であれば、一般的に理解されることと同一な意味を有する。一般的に使用される辞書において定義する用語と同じ用語は関連技術の文脈上に有する意味と一致する意味を有することと理解されるべきで、本明細書において明白に定義しない限り、理想的或いは形式的な意味として解釈しない。

【図面の簡単な説明】

【００３１】

【図１】本発明の一実施形態によるセキュアメモリインターフェースを含む電子システムのブロック図である。

【図２】本発明の一実施形態による図１のセキュアメモリインターフェースを示すブロック図である。

【図３】本発明の一実施形態による図２のセキュアメモリインターフェースに含まれた書込部を示すブロック図である。

【図４】本発明の一実施形態による図３の書込部に含まれた幅選択器を示す回路図である。

【図５】本発明の一実施形態による図３の書込部に含まれたエラー検出コードを生成するエンコーダーを示すブロック図である。

【図６】本発明の一実施形態による図２のセキュアメモリインターフェースに含まれた読出部を示すブロック図である。

【図７】本発明の一実施形態による図３及び図６の書込部及び／または読出部に含まれたモード選択部として命令語デコーダーを含むＣＰＵを示すブロック図である。

【図８】本発明の一実施形態による図３及び図６の書込部及び／または読出部に含まれたモード選択部としてアドレスデコーダーを含むＣＰＵを示すブロック図である。

【図９】本発明の他の実施形態によるＣＰＵの外部にモード選択部が配置された図８の変形例を示すブロック図である。

【図１０】本発明の一実施形態によるセキュアモードの活性化または非活性化を示すように使用されるＣＰＵアドレスビットを示した図である。

【図１１】本発明の一実施形態による図３及び図６の書込部及び／または読出部に含まれたモード選択部としてフラグレジスタを含むＣＰＵを示すブロック図である。

【図１２】本発明の一実施形態によるフラグレジスタ及びアドレスデコーダーがモード選択部のために使用される場合にセキュアモードの活性化または非活性化を示す表である。

【図１３】本発明の一実施形態によるＣＰＵとセキュアモードの活性化または非活性化によるメモリ装置のデータ幅を示す表である。

【図１４】本発明の一実施形態による図２のセキュアメモリインターフェースと図３の書込部動作による段階を示すフローチャートである。

【図１５】本発明の一実施形態による図２のセキュアメモリインターフェースと図６の読出部の動作による段階を示すフローチャートである。

【図１６】本発明の一実施形態による図５のエンコーダーに入力される入力値を示す表である。
【図１７】本発明の一実施形態による図５のエンコーダーから出力される出力値を示す表である。
【発明を実施するための最良の形態】
【００３２】
以下、添付図面を参照しつつ、本発明の望ましい実施形態をより詳しく説明する。図面上の同一構成要素に対しては同一参照符号を使用し、同一構成要素に対して重複される説明は省略する。
【００３３】
図１は、メモリ装置１０２、データプロセッシング部１０４、及びバス１０６を含む電子システム１００を示すブロック図である。本発明の一実施形態によると、電子システム１００は、スマートカード１１０に構成要素として含まれてもよい。しかし、本発明はこれに限定されず、電子システム１００は他のアプリケーションに適用されてもよい。本発明のメモリ装置１０２及びデータプロセッシング部１０４は１つの集積回路チップで製作されてもよく、２つの分離された集積回路チップで製作されてもよい。
【００３４】
メモリ装置１０２とデータプロセッシング部１０４は、バス１０６を通じて信号を交換する。本発明の実施形態によると、データプロセッシング部１０４は、セキュアメモリインターフェース１０８（即ち、インターフェース部）を含むＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）であってもよい。
【００３５】
図１及び図２を参照すると、セキュアメモリインターフェース１０８は、モード選択部１１２、書込部１１４、及び読出部１１６を含む。書込部１１４は、メモリ装置１０２の指定されたアドレスにデータを書込するためにＣＰＵ１０４からアドレス（ＣＰＵアドレス）とデータ（ＣＰＵデータ）を受信する。読出部１１６は、メモリ装置１０２の指定されたアドレスからデータを読み出すためにＣＰＵ１０４からアドレス（ＣＰＵアドレス）を受信する。
【００３６】
モード選択部１１２は、書込部１１４及び読出部１１６の動作に対するセキュアモードを活性化または非活性化させる。書込部１１４及び読出部１１６は、モード選択部１１２による前記セキュアモードの活性化または非活性化に従って各々セキュアモードまたは非セキュアモードで動作する。モード選択部１１２は前記セキュアモードの活性化または非活性化を示すセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）を生成する。
【００３７】
図３は、本発明の一実施形態に従った図２の書込部１１４を示すブロック図である。書込部１１４は、幅選択器２０２、エンコーダー２０４、ミキサ（ｍｉｘｅｒ）２０６、及びメモリ書込有限状態機械（ｍｅｍｏｒｙ ｗｒｉｔｅ ｆｉｎｉｔｅ ｓｔａｔｅ ｍａｃｈｉｎｅ）２０８を含む。
【００３８】
図１、図２、及び図３を参照すると、ＣＰＵ１０４は、ＣＰＵ１０４とメモリ装置１０２で処理されるビット数（即ち、ＣＰＵデータ幅またはさらに一般的にプロセッシングデータ幅）を示すＲｅｓｉｓｔｅｒ＿Ｗｉｄｔｈ信号である「２４」、「１６」、及び「８」のうち、何れかの１つを活性化させる。例えば、ＣＰＵ１０４は、１回に８ビット、１６ビット、または２４ビットのデータのうちの１つを生成してメモリ装置１０２に提供するかまたはメモリ装置１０２から８ビット、１６ビット、または２４ビットのデータのうちの１つを受信する。
【００３９】
図１３は、前記ＣＰＵデータ幅に従ってメモリ装置１０２を占有するデータビットを示す表である。第１列９０２は、８ビット、１６ビット、または２４ビットのようなＣＰＵ

データ幅の典型的な例を示す。第２列９０４は、前記セキュアモードが非活性化された場合、前記８ビット、１６ビット、または２４ビットのＣＰＵデータ幅の各々に相応するメモリ装置１０２に保存されたビット数を示す。第３列９０６は、前記セキュアモードが発生化された場合、前記８ビット、１６ビット、または２４ビットのＣＰＵデータ幅の各々に相応するメモリ装置１０２に保存されたビット数を示す。

【００４０】

前記セキュアモードが非活性化された場合、ＣＰＵ１０４から生成された前記８ビットデータは、８ビットでメモリ装置１０２に保存される。これと類似に、前記セキュアモードが非活性化された場合、ＣＰＵ１０４から生成された前記１６ビットデータは、１６ビットでメモリ装置１０２に保存される。また、前記セキュアモードが非活性化された場合、ＣＰＵ１０４から生成された前記２４ビットデータは所定のビット値で設定された８ビットのデータが追加されて３２ビットでメモリ装置１０２に保存される。

【００４１】

前記セキュアモードが活性化された場合、ＣＰＵ１０４から生成された前記８ビットデータはエラー検出コードが追加されて１６ビットでメモリ装置１０２に保存される。これと類似に前記セキュアモードが活性化された場合、ＣＰＵ１０４から生成された前記１６ビットのエラー検出コードが追加されて３２ビットでメモリ装置１０２に保存される。また、前記セキュアモードが活性化された場合、ＣＰＵ１０４から生成された前記２４ビットデータは、８ビットのエラー検出コードが追加されて３２ビットでメモリ装置１０２に保存される。

【００４２】

図１３の表の第４例９０８は、前記セキュアモードが非活性化状態から活性化状態になった場合における、ＣＰＵ１０４から生成されたビット数（即ち、ＣＰＵデータ幅）に対するメモリ装置１０２に保存されたビット数（即ち、メモリデータ幅）の倍数（即ち、大きさ増加因子（ｓｉｚｅ　ｉｎｃｒｅａｓｅ　ｆａｃｔｏｒ））の増加比率を示す。前記ＣＰＵデータ幅が８ビットまたは１６ビットである場合、前記セキュアモードが活性化されると、前記ＣＰＵ１０４から生成されたビット数に対するメモリ装置１０２に保存されたビット数の倍数は２倍に増加する。前記ＣＰＵデータ幅が２４ビットである場合、前記セキュアモードが活性化されても前記ＣＰＵ１０４から生成されたビット数に対するメモリ装置１０２に保存されたビット数の倍数は１に維持される。

【００４３】

図１３の表の第５列９１０は、前記ＣＰＵデータ幅が８ビット、１６ビット、または２４ビットである場合、前記セキュアモードの活性化に従ったセキュア等級を示す。前記ＣＰＵデータ幅が８ビットまたは１６ビットである場合、前記エラー検出コードが結合されると、メモリ装置１０２に保存されるビット数が２倍に増加するため、前記セキュア等級（即ち、欠陥注入を検出する能力）は非常に高い。前記ＣＰＵデータ幅が２４ビットである場合、前記エラー検出コードが決合されると、メモリ装置１０２に保存されるビット数が２倍より少なく増加されるため、前記セキュア等級は高いが、前記ＣＰＵデータ幅が８ビットまたは１６ビットである場合よりは低い。

【００４４】

図３及び図１３を参照すると、幅選択器２０２は、メモリ書込有限状態機械２０８が８ビット、１６ビット、または３２ビットで前記メモリデータを生成するように前記メモリデータ幅信号「８」、「１６」、及び「３２」のうちの１つを活性化する。図４は、前記ＣＰＵデータ幅信号である「８」、「１６」、及び「２４」のうちの何れが活性化されたかに従って、また前記セキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）が活性化されたかに従って、前記メモリデータ幅信号である「８」、「１６」、及び「３２」のうちの１つを活性化する幅選択器２０２の一例を示す回路図である。

【００４５】

図４を参照すると、幅選択器２０２はインバーター２２０、第１～第４論理積ゲート（２２２，２２４，２２６，２２８）と第１及び第２論理和ゲート（２３２，２３４）を含

む。前記セキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）は、インバーター２２０、第１論理積ゲート２２２、及び第３論理積ゲート２２６に印加される。前記ＣＰＵデータ幅信号「２４」は、第１論理和ゲート２３２に印加され、前記ＣＰＵデータ幅信号「１６」は第１及び第２論理積ゲート（２２２，２２４）に印加され、前記ＣＰＵデータ幅信号「８」は、第３及び第４論理積ゲート（２２６，２２８）に印加される。

【００４６】

インバーター２２０、第１～第４論理積ゲート（２２２，２２４，２２６，２２８）及び第１及び第２論理和ゲート（２３２，２３４）は、図４に示したように接続される。第１論理和ゲート２３２は前記メモリデータ幅信号「３２」を出力し、第２論理和ゲート２３４は、前記メモリデータ幅信号「１６」を出力し、第４論理和ゲート２２８は、前記メモリデータ幅信号「８」を出力する。図４及び図１３を参照すると、図１３の第１列９０２及び第２列９０４に示したように、前記ＣＰＵデータ幅信号「８」、「１６」、及び「２４」のうちの１つが活性化され、前記セキュアモードが非活性化された場合、前記メモリデータ幅信号「８」、「１６」、及び「３２」のうち、相応する１つが活性化される。

【００４７】

他の実施形態において、図１３の第１列９０２及び第３列９０６に示したように、前記ＣＰＵデータ幅信号「８」、「１６」、及び「２４」のうちの１つが活性化され前記セキュアモードが活性化された場合、前記メモリデータ幅信号「１６」及び「３２」のうち、相応する１つが活性化される。図３を参照すると、前記メモリデータ幅信号「８」、「１６」、及び「３２」は前記メモリデータ幅信号「８」、「１６」、及び「３２」のうちの何れが活性化されるかによって８ビット、１６ビット、または３２ビットの前記メモリデータを生成するメモリ書込有限状態機械２０８に印加される。

【００４８】

図５は、前記セキュアモードが活性化された場合に使用される前記エラー検出コード（ＥＤＣ）を生成するエンコーダー２０４を示すブロック図である。図５に示した例示的なエンコーダー２０４は前記エラー検出コードを生成するためにＣＰＵ１０４から生成される前記ＣＰＵデータを使用する。しかし、本発明はＣＰＵ１０４から生成される前記ＣＰＵデータ及び前記ＣＰＵアドレスから前記エラー検出コードを生成するエンコーダーで具現されてもよい。この場合、セキュアメモリインターフェース１０８は、前記データ及び前記アドレス情報に対する欠陥注入を検出することができる。

【００４９】

図１６は、本発明の一実施形態に従って前記ＣＰＵデータ幅信号「８」、「１６」、及び「２４」各々を活性化するために図５のエンコーダー２０４に入力される値を示す表である。図１７は、本発明の一実施形態に従って前記ＣＰＵデータ幅信号「８」、「１６」、及び「２４」各々を活性化するために図５のエンコーダー２０４から出力される値を示す表である。

【００５０】

図５の実施形態を参照すると、エンコーダー２０４は８ビットの入力信号「Ｅ」２４２、８ビットの入力信号「Ｒｈ」２４４、及び８ビットの入力信号「Ｒｌ」２４８を含む。また、エンコーダー２０４は、８ビットの出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８及び８ビットの出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０を含む。

【００５１】

図５、図１６、及び図１７の実施形態を参照すると、前記ＣＰＵデータ幅が８ビットである場合、入力信号「Ｒｌ」２４８は前記ＣＰＵデータを含む反面、入力信号「Ｅ」２４２及び入力信号「Ｒｈ」２４４は定義されない（即ち、図１６のＸ）。またこの場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０は有効である反面、出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８は定義されない。従って、前記ＣＰＵデータ幅が８ビットである場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０はミキサ２０６で使用される前記８ビットのエラー検出コード（ＥＤＣ）を含む。

【００５２】

他の実施形態において、前記ＣＰＵデータ幅が１６ビットである場合、入力信号「Ｒｌ」２４８は前記ＣＰＵデータの下位バイトを含み、入力信号「Ｒｈ」２４４は前記ＣＰＵデータの上位バイトを含み、入力信号「Ｅ」２４２は「０」に固定される。またこの場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０及び出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８は有効である。従って、前記ＣＰＵデータ幅が１６ビットである場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０及び出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８はミキサ２０６で使用される前記１６ビットのエラー検出コード（ＥＤＣ）を含む。

【００５３】

前記ＣＰＵデータ幅が２４ビットである場合、入力信号「Ｒｌ」２４８は前記ＣＰＵデータの下位バイトを含み、入力信号「Ｒｈ」２４４は、前記ＣＰＵデータの中間バイトを含み、入力信号「Ｅ」２４２は、前記ＣＰＵデータの上位バイトを含む。またこの場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２６０は、有効である反面、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２５８は定義されない。従って、前記ＣＰＵデータ幅が２４ビットである場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２６０はミキサ２０６で使用される前記８ビットのエラー検出コード（ＥＤＣ）を含む。

【００５４】

また、本発明の一実施形態において、エンコーダー２０４は、前記ＣＰＵデータ幅信号「１６」であってもよい１ビットの制御信号である「Ｃｔｒｌ＿１６ｂｉｔｓ＿Ａｃｃｅｓｓ」２４６に従って動作する。また、エンコーダー２０４は予め決定されたデータレジスタ２５０、下位ビットコーダ２５２、上位ビットコーダ２５６、及びマルチプレクサ２５４を含む。「Ｃｔｒｌ＿１６ｂｉｔｓ＿Ａｃｃｅｓｓ」信号２４６は予め決定されたデータレジスタ２５０の出力または下位ビットコーダ２５２の出力のうちの１つを出力するマルチプレクサ２５４を制御する。

【００５５】

「Ｃｔｒｌ＿１６ｂｉｔｓ＿Ａｃｃｅｓｓ」信号２４６は、ＣＰＵ１０４が１６ビットのＣＰＵデータ幅を有する１６ビットデータを生成する場合、論理ハイ状態で活性化される。この場合、マルチプレクサ２５４は上位ビットコーダ２５６に入力される、予め決定されたビットパターンである前記予め決定されたデータレジスタ２５０の出力（例えば、０×００または０×ＦＦ）を選択する。

【００５６】

結果的に、上位ビットコーダ２５６は、８ビットの出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８を生成するために８ビットの入力信号「Ｒｈ」２４４を使用する反面、入力信号「Ｅ」２４２はＣＰＵによって「０」に設定される。またこの場合、下位ビットコーダ２５２は、８ビットの出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０を生成するために８ビットの入力信号「Ｒｌ」２４８を使用する。図３及び図５を参照すると、前記１６ビットのＣＰＵデータ幅を有することによって、「Ｃｔｒｌ＿１６ｂｉｔｓ＿Ａｃｃｅｓｓ」信号２４６が活性化される場合に、出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８及び出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０を合算した総１６ビットの前記エラー検出信号がミキサ２０６で利用可能である。

【００５７】

「Ｃｔｒｌ＿１６ｂｉｔｓ＿Ａｃｃｅｓｓ」信号２４６は、ＣＰＵ１０４が前記８ビットまたは２４ビットのＣＰＵデータ幅を有する８ビットまたは２４ビットデータを生成する場合、論理ロー状態に非活性化される。前記２つの場合、下位ビットコーダ２５２は、ミキサ２０６及びマルチプレクサ２５４で利用可能な８ビットの出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０を生成するために８ビットの入力信号「Ｒｌ」２４８のみを使用する。前記２つの場合、マルチプレクサ２５４は上位ビットコーダ２５６に入力するように前記下位ビットコーダ２５２の出力を選択する。

【００５８】

前記ビットコーダ２５６は、ミキサ２０６で使用可能な８ビットのＥＤＣ出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８を生成するために入力信号「Ｒｈ」２４４、入力信号「Ｅ」２

４２、及び前記下位ビットコーダ２５２の出力を使用する。前記８ビットのＣＰＵデータ幅を有する場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０のみが有効でありミキサ２０６で使用され、出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８は無視される。前記２４ビットのＣＰＵデータ幅を有する場合、出力信号「ＥＤＣ＿ｏｕｔ＿Ｈ」２５８のみが有効でありミキサ２０６で使用され、出力信号「ＥＤＣ＿ｏｕｔ＿Ｌ」２６０は無視される。

【００５９】

図２及び図３を参照すると、ＣＰＵ１０４が書込動作のためにメモリ装置１０２にアクセスする場合、セキュアメモリインターフェース１０８及び書込部１１４は、図１４のフローチャートに従って動作する。ＣＰＵ１０４は、書込命令語名称、アクセスされるメモリ装置１０２のアドレスを示すＣＰＵアドレス及びメモリ装置１０２に書込まれるＣＰＵデータを含む書込コマンドのような書込メモリアクセス情報を生成する（図１４のステップＳ７０１）。前記ＣＰＵアドレスは前記ＣＰＵデータを保存するメモリ装置１０２の位置を示す。ＣＰＵ１０４は前記書込メモリアクセス情報の一部として前記ＣＰＵデータに保存する各々のレジスタ名称を生成することができる。

【００６０】

モード選択部１１２は、前記書込メモリアクセス情報から前記セキュアモードがＣＰＵによって活性化されたかの有無を判断する（図１４のステップＳ７０２）。本発明の一実施形態において、図７は、モード選択部１１２が命令語名称デコーダーに具現された場合を示す。この場合、ＣＰＵ１０４は相応する前記命令語名称を有する前記書込コマンドによって前記セキュアモードの活性化または非活性化を指定する。

【００６１】

例えば、前記書込コマンドは前記セキュアモードの非活性化を示す通常の書込命令語名称及び前記セキュアモードの活性化を示すセキュア書込命令語を含む。この場合、図７のモード選択部１１２は、前記命令語名称に従って前記セキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）の活性化または非活性化するように前記命令語名称を復号化する。図７の実施形態において、ＣＰＵ１０４は通常の読出命令語、セキュア読出命令語、通常の書込命令語及びセキュア書込命令語を含む追加的な命令語３つを実行することができる。各々の通常の書込命令語及び通常の読出命令語はセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）が非活性化されるようにし、各々のセキュア書込命令語及びセキュア読出命令語はセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）が活性化されるようにする。

【００６２】

図８は、本発明の他の実施形態に従ってアドレスデコーダー２６４に具現されたモード選択部１１２を示す。この場合、ＣＰＵ１０４は、ＣＰＵ１０４内のアドレス生成器２６２によって生成された前記ＣＰＵアドレスを有する前記書込コマンドによって前記セキュアモードの活性化または非活性化を指定する。図１０に示したように、ＣＰＵアドレスのビット数は１６メガバイトのメモリ容量を指定するのに充分である。しかし、実際にスマートカードのような装置に含まれた電子システム１００の全てのメモリ装置の総容量はアドレス可能なメモリ容量より充分に小さい。

【００６３】

従って、ＣＰＵ１０４から生成された前記ＣＰＵアドレスの一部ビットは、メモリ装置１０２のアドレスを指定するのに必要ではないために前記セキュアモードの活性化または非活性化を指定するのに使用してもよい。この場合、アドレスデコーダー２６４は、前記セキュアモードの活性化または非活性化を示すセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）を活性化または非活性化するために、アドレス生成器２６２から生成された前記ＣＰＵアドレスを復号化する。例えば、アドレスデコーダー２６４は、アドレス生成器２６２から生成された各々のＣＰＵアドレスが前記セキュアモードの活性化を示すセキュアアクセスであるかまたは前記セキュアモードの非活性化を示す非セキュアアドレスであるかを決定するアドレスフィルタを含む。

【００６４】

図９は、本発明の他の実施形態に従ってアドレスデコーダー２６５がＣＰＵ１０４の外部に具現される場合を示した図である。図９のアドレス生成器２６２は、図８のアドレス生成器２６２と類似に動作する。しかし、図９において、電子システム１００のＣＰＵ１０４の変更を最小化させるためにアドレスデコーダー２６５を有するモード選択部１１２は、ＣＰＵ１０４の外部に具現される。

【００６５】

図１１は、本発明の他の実施形態に従ってモード選択部１１２がＣＰＵ１０４の複数のデータレジスタ７６０に相応するフラグレジスタ７５０に具現される場合を示す。前記複数のデータレジスタ７６０各々は、ＣＰＵ１０４とメモリ装置１０２との間に処理される各々の前記ＣＰＵデータを保存する。書込／読出コマンドを生成する際、ＣＰＵ１０４は、前記ＣＰＵデータを保存する前記レジスタの各々の識別名（ｉｄｅｎｔｉｆｉｅｒ、即ち、相応するレジスタ名称）を指定する。

【００６６】

フラグレジスタ７５０は、複数のレジスタフラグを含み、前記レジスタフラグ各々は、複数のデータレジスタ７６０のうち、相応するデータレジスタに対する活性化または非活性化の有無を示すように設定される。例えば、レジスタフラグ＃１は、レジスタ＃１と相応し、レジスタフラグ＃２は、レジスタ＃２と相応する。図１１のモード選択部１１２は、レジスタマルチプレクサ７６２を通じて前記ＣＰＵデータを出力するようにデータレジスタ７６０のうち、Ｒｅｓｉｓｔｅｒ＿Ｓｅｌｅｃｔ信号によって選択された１つに相応するレジスタフラグを出力するフラグマルチプレクサ７５２を含む。

【００６７】

この場合、ＣＰＵ１０４は、前記ＣＰＵデータに相応する各々のレジスタ名称を含む書込／読出コマンドを生成する。フラグレジスタ７５０のうちの相応する１つ及びデータレジスタ７６０のうちの相応する１つに保存された前記ＣＰＵデータ出力するようにフラグマルチプレクサ７５２及びレジスタマルチプレクサ７６２を制御するために前記Ｒｅｓｉｓｔｅｒ＿Ｓｅｌｅｃｔ信号は、前記各々のレジスタ名称に従って生成される。フラグマルチプレクサ７５２から選択された前記レジスタフラグはセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）である。

【００６８】

図１１の実施形態において、フラグレジスタ７５０の各々のフラグはＣＰＵ１０４でプログラム可能である。図１１の実施形態は、スタック動作（ｓｔａｃｋ　ｏｐｅｒａｔｉｏｎ）における各々のポインタのためのメモリ装置１０２へのアクセスがセキュアかまたは非セキュアかを自動的に示すフラグレジスタ７５０によるＣＰＵ１０４のスタック動作に特に有用である。

【００６９】

図１２は、アドレスデコーダー（２６４または２６５）及びプレグレジスタ７５０を全て含むモード選択部１１２を有する本発明の他の実施形態を示す図である。この場合ＣＰＵ１０４から生成される前記メモリアクセス情報内の前記レジスタ名称及び前記ＣＰＵアドレスは図１２の表に従って前記セキュアモードの活性化または非活性化を決定することに使用される。

【００７０】

図１２の表の第１行７７１を参照すると、前記レジスタ名称のフラグは前記セキュアモードの非活性化を示し、前記ＣＰＵアドレスは前記セキュアモードの非活性化を示す。この場合、前記セキュアモードの非活性化のためにセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）は非活性化される。図１２の表の第２行７７２を参照すると、前記レジスタ名称のフラグは前記セキュアモードの非活性化を示すが、前記ＣＰＵアドレスは前記セキュアモードの活性化を示す。この場合、前記セキュアモードの活性化のためにセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）は活性化される。

【００７１】

図１２の表の第３行７７３を参照すると、前記レジスタ名称のフラグは前記セキュアモ

ードの活性化を示すが、前記ＣＰＵアドレスは、前記セキュアモードの非活性化を示す。この場合、前記セキュアモードの活性化のためにセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）は活性化される。図１２の表の第４行７７４を参照すると、前記レジスタ名称のフラグは前記セキュアモードの活性化を示し、前記ＣＰＵアドレスは前記セキュアモードの活性化を示す。この場合、前記セキュアモードの活性化のためにセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）は活性化される。図１２の方法において、前記レジスタ名称または前記ＣＰＵアドレスのうち、少なくとも１つが前記セキュアモードの活性化を示す場合、前記セキュアモードの活性化のためにセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）は活性化される。

【００７２】

ＣＰＵ１０４から生成されるメモリアドレス情報は、次の例のように一連の読出／書込コマンドを含む。

【００７３】

ｗｒｉｔｅ＿８　Ｒ０　@０×１００
ｓｅｃｕｒｅ＿ｗｒｉｔｅ＿１６　Ａ８　@０×１０Ａ
ｒｅａｄ＿８　Ｒ１　@０×１０２
ｓｅｃｕｒｅ＿ｒｅａｄ＿２４　Ａ８　@０×１０Ａ

【００７４】

前記例示コマンド「ｗｒｉｔｅ＿８　Ｒ０　@０×１００」は、前記セキュアモードの非活性化及び８ビットのＣＰＵデータ幅を有する通常の書込を示す命令語名称「ｗｒｉｔｅ＿８」、メモリ装置１０２に書き込まれる前記ＣＰＵデータを含むレジスタ名称「Ｒ０」及び前記書込動作にアクセスされるためのメモリ装置１０２のアドレスを示すＣＰＵアドレス「０×１００」を含む。

【００７５】

前記例示コマンド「ｓｅｃｕｒｅ＿ｗｒｉｔｅ＿１６　Ａ８　@０×１０Ａ」は前記セキュアモードの活性化及び１６ビットのＣＰＵデータ幅を有するセキュア書込を示す命令語名称「ｓｅｃｕｒｅ＿ｗｒｉｔｅ＿１６」、メモリ装置１０２に書き込まれる前記ＣＰＵデータを含むレジスタ名称「Ａ８」及び前記書込み動作にアクセスされるためのメモリ装置１０２のアドレスを示すＣＰＵアドレス「０×１０Ａ」を含む。

【００７６】

前記例示コマンド「ｒｅａｄ＿８　Ｒ１　@０×１０２」は前記セキュアモードの非活性化及び８ビットのＣＰＵデータ幅を有する読出を示す命令語名称「ｒｅａｄ＿８」、メモリ装置１０２から読み出された前記データを受信するレジスタ名称「Ｒ１」及び前記読出動作にアクセスするためのメモリ装置１０２のアドレスを占めすＣＰＵアドレスである「０×１０２」を含む。

【００７７】

前記例示コマンド「ｓｅｃｕｒｅ＿ｒｅａｄ＿２４　Ａ８　@０×１０Ａ」は前記セキュアモードの活性化及び２４ビットのＣＰＵデータ幅を有するセキュア読出を示す命令語名称「ｓｅｃｕｒｅ＿ｒｅａｄ＿２４」、メモリ装置１０２から読み出された前記データを受信するレジスタ名称「Ａ８」及び前記読出動作にアクセスされるためのメモリ装置１０２のアドレスを示すＣＰＵアドレスである「０×１０Ａ」を含む。

【００７８】

再び、図３及び図１４を参照すると、前記セキュアモードがセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）に従って非活性化された場合（図１４のステップＳ７０３）、ミキサ２０６は前記ＣＰＵデータ（即ち、初期書込データ）として前記混合データをメモリ書込有限状態機械２０８に出力する（図１４のステップＳ７０４）。結果的に、メモリ書込有限状態機械２０８は前記書込みイネーブル信号の活性化に従ってメモリ装置１０２に前記メモリデータとして前記ＣＰＵデータ（即ち、初期記入データ）を伝達し、前記メモリアドレスとして前記ＣＰＵアドレスを伝達する（図１４のステップＳ７０７）。従って、前記メモリデータはメモリ装置１０２の前記メモリアドレスに書き込まれる。メ

モリ装置１０２に書き込まれた前記メモリデータの大きさは、図４及び図１３を参照して前述説明した幅選択器２０２の出力に従う。

【００７９】

他の実施形態において、前記セキュアモードがセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）に従って活性化された場合（図１４のステップＳ７０３）、エンコーダー２０４はＣＰＵ１０４から生成された前記ＣＰＵデータ（即ち、初期書込データ）及び／または相応する前記ＣＰＵアドレスを使用して前記エラー検出コード（ＥＤＣ）を生成する。前記エラー検出コード（ＥＤＣ）のビット数は、図５、図１６、及び図１７を参照して、前述説明した前記ＣＰＵデータ幅を従う（図１４のステップＳ７０５）。

【００８０】

前記エラー検出コード（ＥＤＣ）は前記請求項ＣＰＵデータ幅に従って多数のビットを有する混合書込データを生成するミキサ２０６によって前記ＣＰＵデータ（即ち、初期書込データ）と混合される（図１４のステップＳ７０６）。結果的に、書込み有限状態機械２０８は、前記混合書込データから前記メモリデータ（即ち、最終書込みデータ）及び前記メモリアドレスを生成する（図１４のステップＳ７０７）。前記メモリデータのビット数は図４及び図１３を参照して、前述説明した幅選択器２０２から生成された前記メモリデータ幅信号「８」、「１６」、及び「３２」に従う。メモリ装置１０２は、メモリ装置１０２の前記メモリアドレスに前記メモリデータを受信し、保存する。このような方式で、図１４のステップ７０７から前記セキュアモードが活性化された場合、セキュア書込み動作のためにメモリ装置１０２に保存された前記メモリデータは前記エラー検出コード（ＥＤＣ）と統合される。

【００８１】

図６は、本発明の実施形態に従う図２の読出部１１６を示すブロック図である。読出部１１６は、幅選択器２５２、エンコーダー２５４、デミキサ２５６、メモリ読出有限状態機械２５８、及び比較器２６０を含む。本発明の一実施形態に従うと、図６の読出部１１６の幅選択器２５２及びエンコーダー２５４は図３の書込部１１４の幅選択器２０２及びエンコーダー２０４と類似に具現される。図６の読出部１１６のデミキサ２５６は、前記データから前記エラー検出コード（ＥＤＣ）を分離するために、図３の書込部１１４のミキサ２０６と逆の動作をする。

【００８２】

図２及び図６を参照すると、セキュアメモリインターフェース１０８及び読出部１１６の前記構成要素である幅選択器２５２、エンコーダー２５４、デミキサ２５６、メモリ読出有限状態機械２５８、及び比較器２６０は、ＣＰＵ１０４が読出動作のためにメモリ装置１０２にアクセスする場合、図１５のフローチャートに従って動作する。ＣＰＵ１０４は読出命令語名称及びアクセスするためのメモリ装置１０２のアドレスを示すＣＰＵアドレスを含む読出コマンドのような読出メモリアクセス情報を生成する（図１５のステップＳ８０１）。前記ＣＰＵアドレスは、前記ＣＰＵデータが読み出されるメモリ装置１０２の位置を示す。

【００８３】

モード選択部１１２は、前記読出メモリアクセス情報から前記セキュアモードがＣＰＵによって活性化されたかの有無を判断する（図１５のステップＳ８０２）。モード選択器１１２は、前述説明した図７、８、９、１０、１１、及び１２の実施形態のうち、何れかの１つに従って具現されることができる。

【００８４】

さらに、メモリ読出有限状態機械２５８は、前記読出イネーブル信号の活性化に従ってメモリ装置１０２に前記メモリアドレスとして前記ＣＰＵアドレスを伝達する（図１５のステップＳ８０３）。結果的に、メモリ装置１０２は、メモリ装置１０２の前記メモリアドレスから前記メモリデータを初期読出データとしてメモリ読出有限状態機械２５８に伝送する（図１５のステップＳ８０４）。前記初期読出データのビット数は図４及び図１３を参照して、前述説明した幅選択器２５２から生成された前記メモリデータ幅信号「８」

、「１６」、及び「３２」に従う。
【００８５】
前記セキュアモードがセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）に従って非活性化された場合（図１５のステップＳ８０５）、デミキサ２５６は前記初期読出データからどのエラー検出コードも分離せず、前記初期読出データから最終読出データ（即ち、前記ＣＰＵデータ）を生成する（図１５のステップＳ８０６）。前記最終読出データ（即ち、ＣＰＵデータ）はＣＰＵ１０４に伝送され、活性化された前記ＣＰＵデータ幅信号「８」、「１６」、及び「２４」に相応する前記最終読出データのビット数を有する。
【００８６】
他の実施形態において、前記セキュアモードがセキュアモードイネーブル信号（ＳＭＩ＿Ｅｎａｂｌｅ）に従って活性化された場合（図１５のステップＳ８０５）、デミキサ２５６は前記初期読出データからエラー検出コードを分離して前記初期読出データから最終読出データ（即ち、ＣＰＵデータ）を生成する（図１５のステップＳ８０７）。結果的に、エンコーダー２５４は少なくとも１つの前記ＣＰＵアドレス及び前記最終読出データを使用する予想エラー検出コード（ＥＤＣ）を生成する（図１５のステップＳ８０８）。その後、比較器２６０は、エンコーダー２５４から生成された前記予想エラー検出コードとデミキサ２５６によって前記初期読出データから生成された計算されたエラー検出コード（ＥＤＣ）を比較してエラー検出信号（ＳＭＩ＿Ｅｒｒｏｒ）を生成する（図１５のステップＳ８０９）。
【００８７】
エンコーダー２５４から生成された前記予想エラー検出コードがデミキサ２５６によって前記初期読出データから生成された前記計算されたエラー検出コードＥＤＣと実質的に同じではないと、比較器２６０は、メモリ読出有限状態機械２５８から受信された前記初期読出データによって欠陥注入が検出されたことを示すためにエラー検出信号（ＳＭＩ＿Ｅｒｒｏｒ）を活性化する。電子システム１００に前記初期読出データに対する前記欠陥注入が通知される。
【００８８】
本発明の一実施形態において、書込部１１４と読出部１１６は、ＣＰＵ１０４内において、各々ハードウェア論理ゲートで具現されてもよい。前記追加的なハードウェア論理ゲートはＣＰＵ１０４内において相対的に小さいシリコン面積を占める。欠陥注入はＣＰＵ１０４によって指定された前記セキュアデータに対してＣＰＵ１０４のハードウェアに具現された書込部１１４と読出部１１６を使用して検出される。従って、書込部１１４と読出部１１６に従ってシリコン面積の増加は、高容量のメモリ装置１０２においても大きな影響は及ぼさない。
【００８９】
さらに、メモリ装置１０２内において、またはＣＰＵ１０４とメモリ装置１０２間のバス１０６で発生された欠陥注入が効率的に検出される。また、ＣＰＵ１０４はメモリ装置１０２の容量に関わらずメモリ装置に保存された前記セキュアデータの量と位置を柔軟に指定することができる。
【００９０】
前述説明した内容は、本発明の実施形態を示すのみで、本発明を限定しようとする意図ではない。従って、図示して説明した多数の構成要素は本発明の実施形態を示すのみである。さらに、本発明の一実施形態によると、ここの発明の詳細な説明に与えられた書込部１１４と読出部１１６の構成要素は、ハードウェア論理ゲートで具現されてもよい。しかし、書込部１１４と読出部１１６の構成要素はハードウェア及び／またはソフトウェアの組合せで具現されてもよい。
【００９１】
以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明はかかる例に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例ま

たは修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

【産業上の利用可能性】

【００９２】

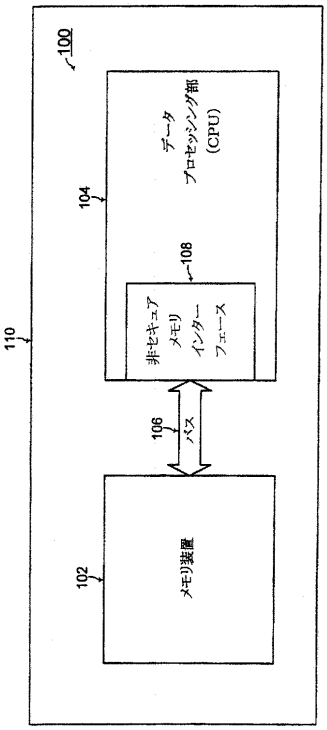
前述のような本発明の実施形態に従ったセキュアメモリインターフェースはＣＰＵ内において相対的に小さい面積を占める。さらに、メモリ装置内でまたはＣＰＵとメモリ装置と間のバスで発生する欠陥注入が効率的に検出される。また、ＣＰＵはメモリ装置の容量に関係なくメモリ装置に保存された前記セキュアデータの量と位置を柔軟に指定することができる。

【符号の説明】

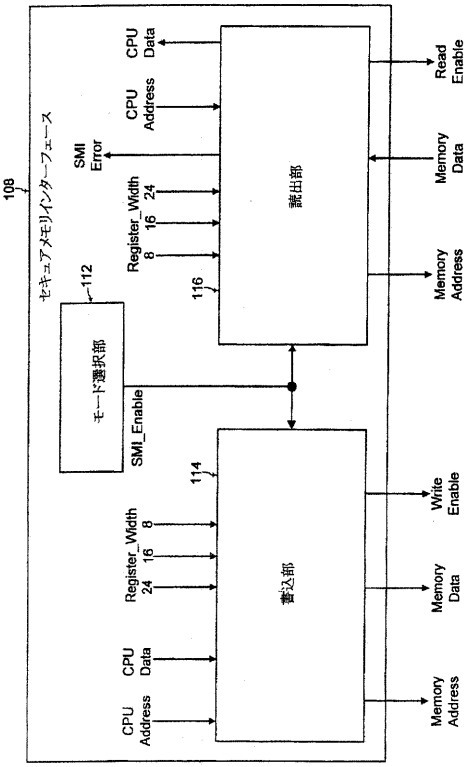
【００９３】

１００　　電子システム
１０２　　メモリ装置
１０４　　データプロセッシング部（ＣＰＵ）
１０６　　バス
１０８　　セキュアメモリインターフェース
１１０　　スマートカード
１１２　　モード選択部
１１４　　書込部
１１６　　読出部
２０２、２５２　　幅選択器
２０４、２５４　　エンコーダー
２０６　　ミキサ
２０８　　メモリ書込有限状態機械
２５６　　デミキサ
２５８　　メモリ読出有限状態機械
２６０　　比較器
２６４、２６５　　アドレス生成器
７５０　　フラグレジスタ
ＳＭＩ＿Ｅｎａｂｌｅ　　セキュアモードイネーブル信号
ＳＭＩ＿Ｅｒｒｏｒ　　エラー検出信号
ＥＤＣ　　エラー検出コード

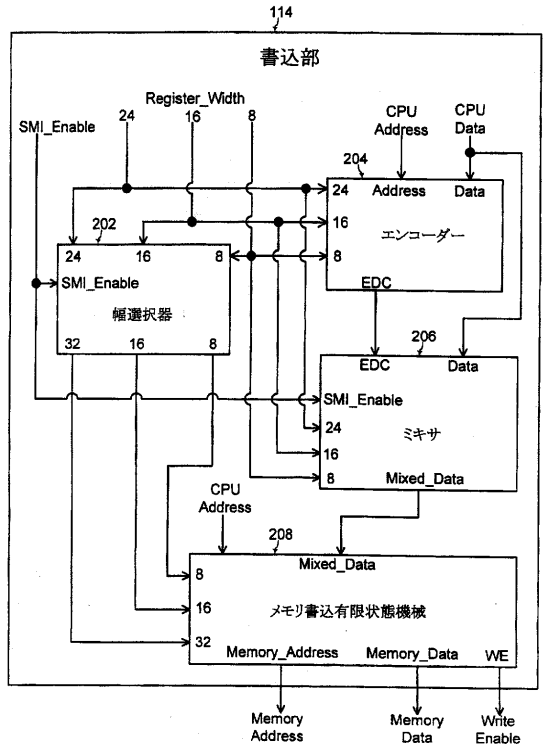
【図１】


100
データプロセッシング部 (CPU)
104
108
非セキュアメモリインターフェース
110
106
バス
メモリ装置
102

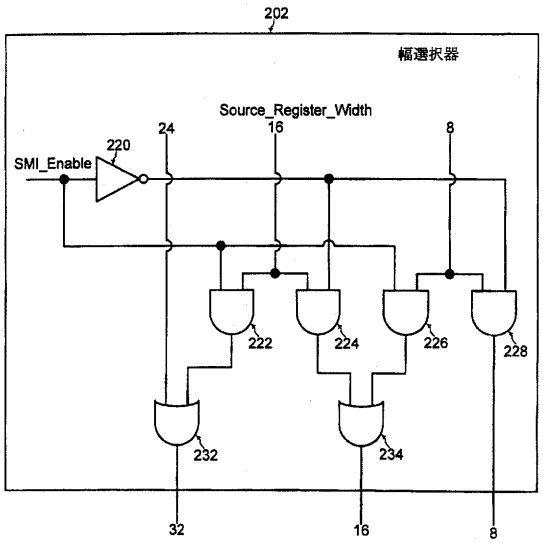
【図２】


108
セキュアメモリインターフェース
CPU Data
CPU Address
SMI Error
Register_Width 24 16 8
116
読出部
Read Enable
Memory Data
Memory Address
112
モード選択部
SMI_Enable
114
書込部
Write Enable
Memory Data
Memory Address

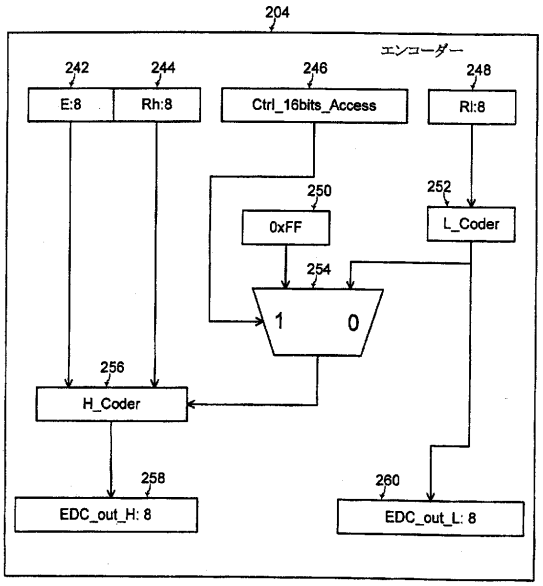
【図３】


114
書込部
Register_Width
SMI_Enable
24 16 8
CPU Address
CPU Data
204
24 Address Data
16
8
エンコーダー
EDC
202
24 16 8
SMI_Enable
幅選択器
32 16 8
206
EDC Data
SMI_Enable
24
16
8
ミキサ
Mixed_Data
CPU Address
208
Mixed_Data
8
16
32
メモリ書込有限状態機械
Memory_Address
Memory_Data
WE
Memory Address
Memory Data
Write Enable

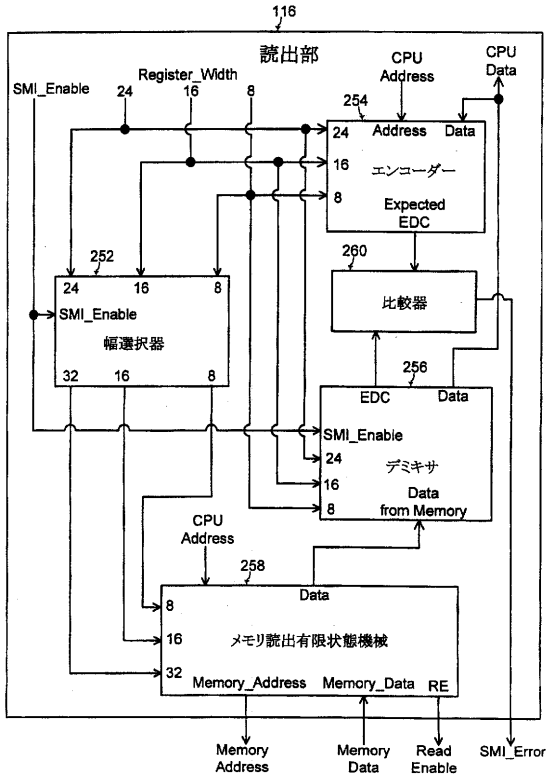
【図４】


202
幅選択器
Source_Register_Width
24 16 8
SMI_Enable
220
222
224
226
228
232
234
32
16
8

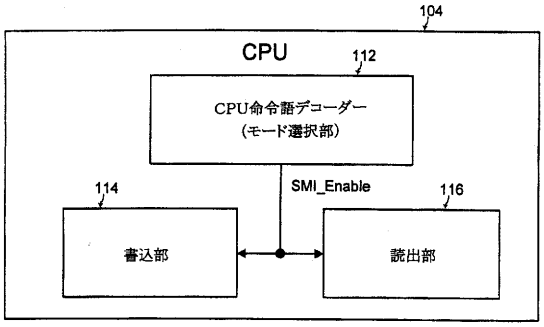
【図５】



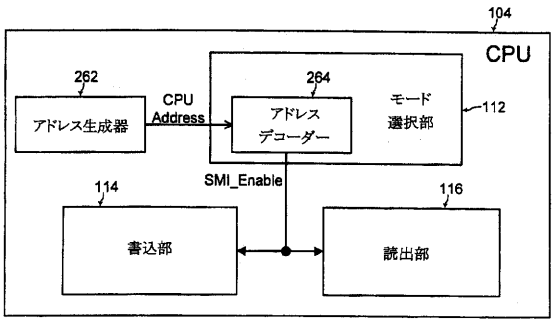
【図６】



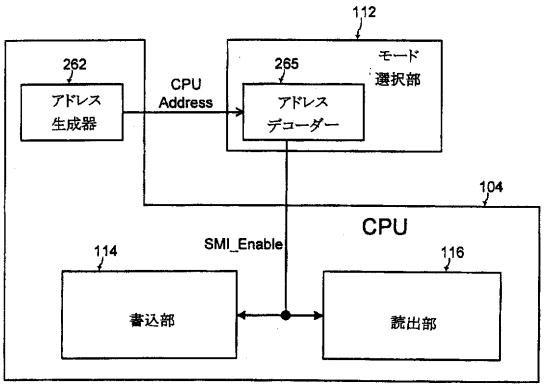
【図７】



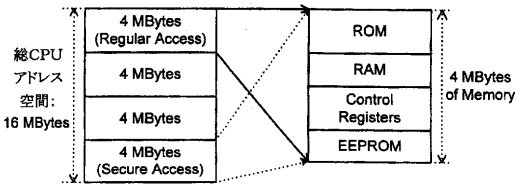
【図８】



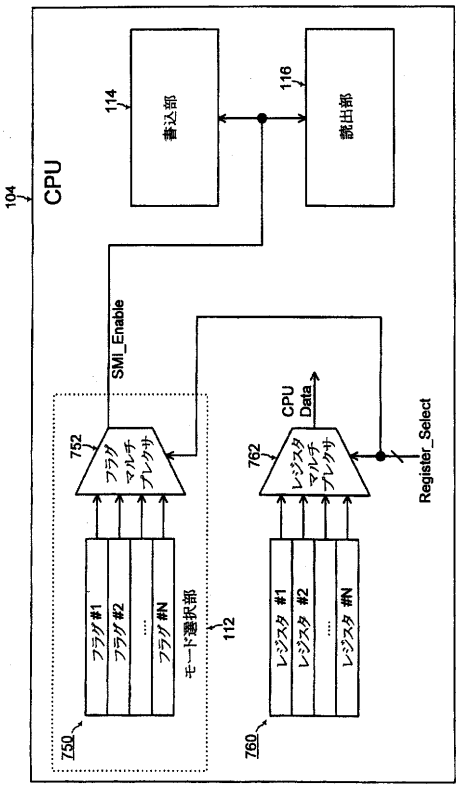
【図９】



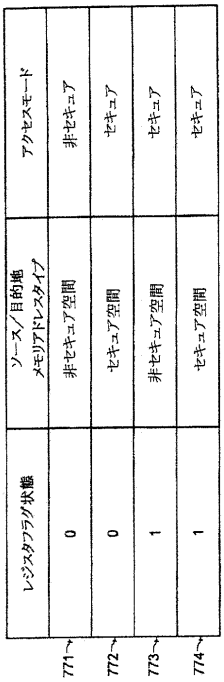
【図１０】



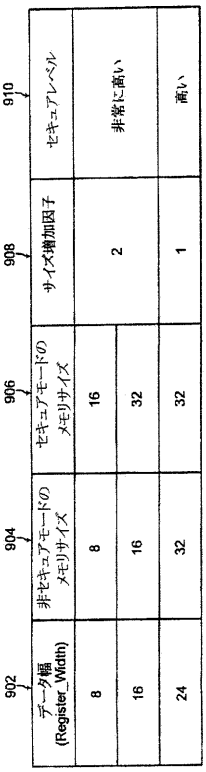
【図１１】



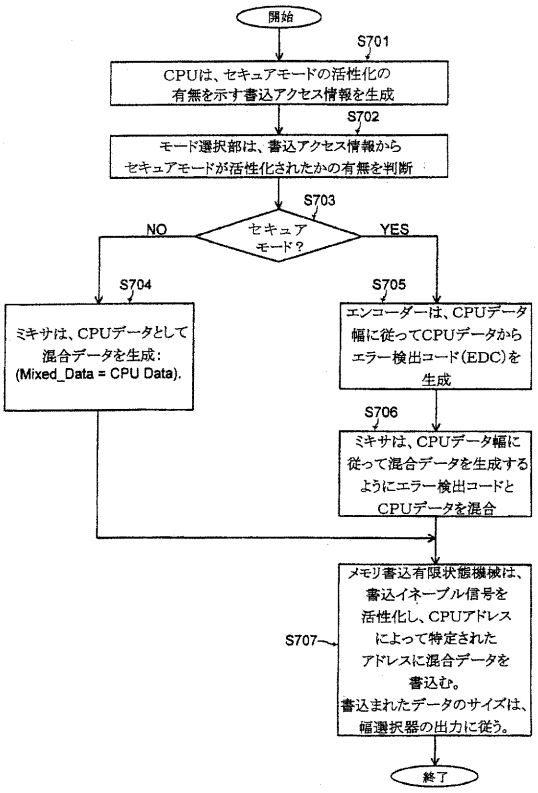
【図１２】



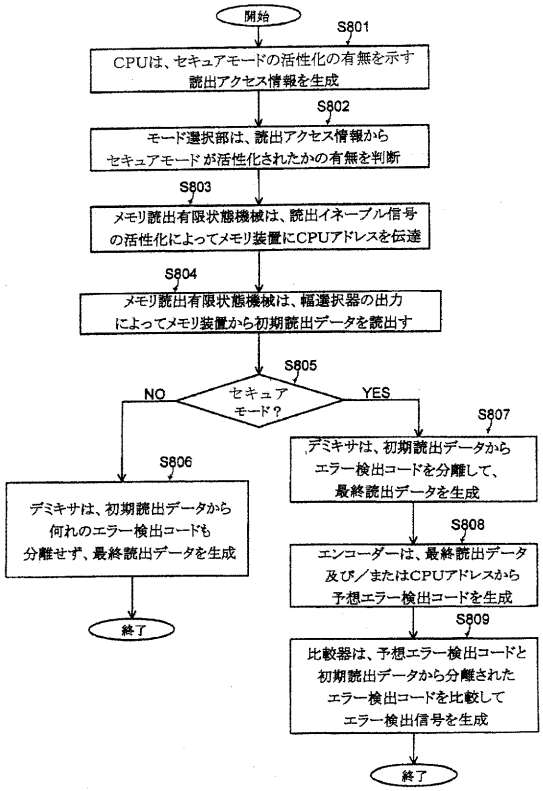
【図１３】



【図１４】



【図１５】



【図１６】

	エンコーダー入力		
活性化されたCPUデータ幅信号	E	Rh	Rl
8 bits	X	X	Data
16 bits	0x00	Data MSB	Data LSB
24 bits	Data MSB	Data Middle Byte	Data LSB

【図１７】

	エンコーダー出力	
活性化されたCPUデータ幅信号	EDC_out_H	EDC_out_L
8 bits	Undefined	EDC8
16 bits	EDC16H	EDC16L
24 bits	EDC24	Undefined

フロントページの続き

(74)代理人 100110364
弁理士 実広 信哉
(72)発明者 セバスチャン・リウ
大韓民国京畿道城南市盆唐区亭子洞（番地なし） 斗山ウィーブパビリオンビー棟８２６号

審査官 園田 康弘

(56)参考文献 特開平０１－２０９５５２（ＪＰ，Ａ）
特開平０３－２６３１４８（ＪＰ，Ａ）
特表２００１－５０３１８１（ＪＰ，Ａ）
特開平０５－３１４０２１（ＪＰ，Ａ）
特開平０６－０１２２７０（ＪＰ，Ａ）
特開平０５－２８２８８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １２／１６