(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-106950
(P2014-106950A)
(43)公開日　平成26年6月9日(2014.6.9)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/62 (2013.01)	G06F 21/24 162	

審査請求 未請求　請求項の数 18　ＯＬ　（全 19 頁）

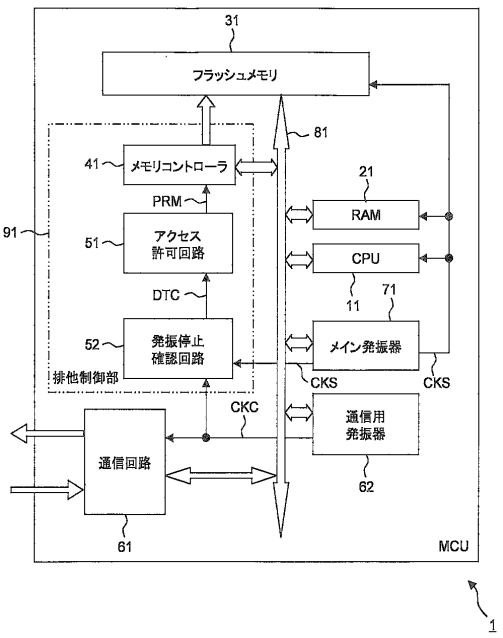
(21)出願番号　特願2012-262129 (P2012-262129)
(22)出願日　平成24年11月30日 (2012.11.30)

(71)出願人　302062931
ルネサスエレクトロニクス株式会社
神奈川県川崎市中原区下沼部１７５３番地
(74)代理人　100089071
弁理士　玉村　静世
(72)発明者　本泉　隆志
神奈川県川崎市中原区下沼部１７５３番地
ルネサスエレクトロニクス株式会社内

(54)【発明の名称】半導体装置及びアクセス制限方法

(57)【要約】
【課題】正規の通信動作中にバックグラウンドでその通信機能を経由して、不正機能が所定の記憶部にインストールされたり、さらには、所定の記憶部から秘匿情報が読み出されて盗み取られたりすることを防止する。
【解決手段】半導体装置に、その外部と通信可能な通信部による通信と所定の記憶部へのアクセスとの排他制御を行う排他制御部を採用する。例えば通信部が通信中か否かは通信クロックの活性／非活性に基づいて判別し、その判別結果を用いて排他制御を行う。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
外部と通信可能な通信部と、
所定の記憶部と、
前記通信部による通信と前記所定の記憶部へのアクセスとの排他制御を行う排他制御部と、を有する半導体装置。
【請求項２】
請求項１において、前記排他制御部は、前記通信部が通信に用いる通信クロックの状態を検出する検出回路を有し、前記検出回路による前記通信クロックの活性状態に応じて前記所定の記憶部へのアクセスを制限し、前記検出回路による前記通信クロックの非活性状態に応じて前記所定の記憶部へのアクセス制限を解除する、半導体装置。
【請求項３】
請求項１において、前記通信部が通信に用いる通信クロックを生成する通信クロック生成部を有し、
前記排他制御部は、前記通信部の通信クロックの状態を検出する検出回路を有し、前記検出回路による前記通信クロックの発振停止の検出に応じて前記所定の記憶部へのアクセス制限を解除し、前記検出回路による前記通信クロックの発振再開の検出に応じて前記所定の記憶部へのアクセスを制限する、半導体装置。
【請求項４】
請求項３において、前記通信クロックは通信レートを規定するクロック信号である、半導体装置。
【請求項５】
請求項１において、前記所定の記憶部へのアクセス制限は、前記所定の記憶部に対する書き込み動作の禁止であり、前記通信部がダウンロードしたデータを一時的に格納する一時記憶部を前記所定の記憶部とは別に有する、半導体装置。
【請求項６】
請求項１において、前記所定の記憶部へのアクセス制限は、前記所定　　の記憶部に対する読み出し動作の禁止である、半導体装置。
【請求項７】
請求項５又は６において、前記所定の記憶部は電気的に書換え可能な不揮発性メモリである、半導体装置。
【請求項８】
請求項５又は６において前記排他制御部は、アクセス要求に応答して前記所定の記憶部へのメモリインタフェース制御を行うメモリコントローラと、
前記通信クロックの状態を検出し、発振停止の状態を検出した場合には前記メモリコントローラのメモリインタフェース動作を可能とし、前記通信クロックの発振中の状態を検出した場合には前記メモリコントローラのメモリインタフェース動作を前記アクセス制限に従って不可能とする検出回路と、を有する半導体装置。
【請求項９】
請求項５又は６において前記排他制御部は、前記所定の記憶部のマッピングアドレスに対するメモリ保護機能を有するメモリマネージメントユニットと、
前記通信クロックの状態を検出し、発振停止の状態を検出した場合には前記メモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を可能とし、前記通信クロックの発振中の状態を検出した場合には前記メモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を前記アクセス制限に従って不可能とする検出回路と、を有する半導体装置。
【請求項１０】
外部と通信可能な通信部による通信動作中は所定の記憶部へのアクセスを制限し、前記通信部による通信動作の休止中は前記所定の記憶部へのアクセス制限を解除することによって、前記通信部による通信と前記所定の記憶部へのアクセスとの排他制御を行う、アク

セス制限方法。
【請求項１１】
請求項１０において、前記通信部が通信に用いる通信クロックの活性状態を検出回路で検出することに応じて前記所定の記憶部へのアクセスを制限し、前記通信クロックの非活性状態を前記検出回路で検出することに応じて前記所定の記憶部へのアクセス制限を解除する、アクセス制限方法。
【請求項１２】
請求項１０において、前記通信部が通信に用いる通信クロックを生成する通信クロック生成部における前記通信クロックの発振停止を検出回路で検出することに応じて前記所定の記憶部へのアクセス制限を解除し、前記通信クロックの発振再開を前記検出回路で検出することに応じて前記所定の記憶部へのアクセスを制限する、アクセス制限方法。
【請求項１３】
請求項１２において、前記通信クロックは通信レートを規定するクロック信号である、半導体装置。
【請求項１４】
請求項１０において、前記アクセス制限として前記所定の記憶部に対する書き込み動作が禁止されている最中に、前記通信部が一時記憶部にダウンロードしたデータを、前記所定の記憶部に対する書き込み動作の禁止が解除されてから前記所定の記憶部に書き込むアクセス制限方法。
【請求項１５】
請求項１０において、前記通信クロックの発振状態では前記アクセス制限として前記所定の記憶部に対する読み出し動作を禁止し、前記通信クロックの発振停止の状態で前記所定の記憶部に対する読み出し動作を可能にする、アクセス制限方法。
【請求項１６】
請求項１４又は１５において、前記所定の記憶部は電気的に書換え可能な不揮発性メモリである、アクセス制限方法。
【請求項１７】
請求項１４又は１５において、前記通信クロックの発振停止の状態を検出回路で検出した場合には、アクセス要求に応答して前記所定の記憶部へのメモリインタフェース制御を行うメモリコントローラのメモリインタフェース動作を可能とし、前記通信クロックの発振中の状態を前記検出回路で検出した場合には、前記メモリコントローラのメモリインタフェース動作を前記アクセス制限に従って不可能とする、アクセス制限方法。
【請求項１８】
請求項１４又は１５において、前記通信クロックの発振停止の状態を検出回路で検出した場合には、前記所定の記憶部のマッピングアドレスに対するメモリ保護機能を有するメモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を可能とし、前記通信クロックの発振中の状態を前記検出回路で検出した場合には、前記メモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を前記アクセス制限に従って不可能とする、アクセス制限方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電話やデータ通信のように加入者間を結ぶ通信ネットワークである外部の通信網と通信を行う通信部を介する記憶部への不正アクセスを防止するためのアクセス制限技術に関し、例えば通信機能を備えたマイクロコンピュータに適用して有効な技術に関する。
【背景技術】
【０００２】
特許文献１には、基地局側装置と、該基地局側装置に通信手段を介して接続された端末

装置を含み、基地局側から端末装置へソフトウェアをダウンロードして端末装置側のソフトウェアのメンテナンスを行うシステムが記載されている。このソフトウェアのメンテナンスとは、ほとんどの場合、端末装置内の不揮発記憶領域に格納されたプログラムまたはデータの書き換えである。

【０００３】

特許文献２には、電子カメラ等の機器内にそのファームウェアと同一不揮発性メモリ内の通信サブルーチンを退避するための専用メモリを新たに設けなくてもよく（コスト低減）、しかも、書き換えデータの受信に並行してファームウェアの書換えを行わずに済む（通信異常によるハングアップ防止）ようにするために、ＰＣのような外部機器から送信されるファームウェア書き換え用データを前記機器内の第１メモリに格納した後、データ書き換え装置と外部機器との通信終了状態を検知したときに、第１メモリ内のファームウェア書き換え用データによって第２メモリに記憶されているファームウェアを書き換える制御手段を採用した技術が記載される。ファームウェアを書き換える制御手段における内部データ転送及び書き換え制御手順はプログラム又はハードウェアロジックの何れでもよいとする。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特許第３５９１２２９号

【特許文献２】特開２００４－２８０５５９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

特許文献１に代表されるようなシステムでは、端末装置のソフトウェアを書き換えることによって動作改善や不具合修正などのメンテナンスを行うことが可能である。しかし同時に、コンピュータウイルス、マルウェア等と呼ばれる不正なソフトウェアにより、通信機能を経由して不正機能のインストールが行われてしまう危険性が存在する。特に、特許文献１では、端末装置と基地局との自動的なバックグラウンド通信を行うことを特徴としているが、これは不正機能のダウンロードにも転用される危険性があり、かつ、これを使用者が事前に察知することは非常に困難である。またこのとき、前記特許に記載のあるユーザのインストール許可操作では、不正ソフトウェアによるインストール許可操作の迂回が行われてしまえば対策とならない。同様に「書き換えデータに特定の認証情報を付加する」、「書き換え時にユーザに承諾ボタンを押させる」等の対策であっても、あくまでソフトウェアによる対策であるため、さらなる不正ソフトウェアによる回避が可能となるなど根本的な対策とはならない。

【０００６】

一方、特許文献２は、外部機器との通信終了状態を検知して書き込みを行うようにしているが、これは、通信動作と書き換え動作を競合させないようにして通信時間を短縮し、且つ、通信異常によるＰＣのハングアップの発生の虞を低減させるためであり、通信機能を経由して不正機能のインストールが行われてしまう危険性からの回避とは着眼点が異なる。ファームウェアの書き換え対象はＰＣに接続されたカメラのような外部機器であり、必要に応じて通信網と通信可能にされた端末装置を想定するものではない。

【０００７】

上記並びにその他の課題と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。

【課題を解決するための手段】

【０００８】

本願において開示される代表的な実施の形態の概要を簡単に説明すれば下記の通りである。

【０００９】

すなわち、半導体装置に、その外部と通信可能な通信部による通信と所定の記憶部へのアクセスとの排他制御を行う排他制御部を採用する。例えば通信部が通信中か否かは通信クロックの活性／非活性に基づいて判別し、その判別結果を用いて排他制御を行う。

【発明の効果】

【００１０】

本願において開示される代表的な実施の形態によって得られる効果を簡単に説明すれば下記のとおりである。

【００１１】

すなわち、通信部による通信と所定の記憶部へのアクセスとが排他制御されるから、正規の通信動作中にバックグラウンドでその通信機能を経由して、不正機能が所定の記憶部にインストールされたり、さらには、所定の記憶部から秘匿情報が読み出されて盗み取られたりすることを防止することができる。

【図面の簡単な説明】

【００１２】

【図１】図１は半導体装置の一例であるマイクロコンピュータの概略的な構成を例示するブロック図である。

【図２】図２は通信回路の通信動作とフラッシュメモリに対する書き換え動作とのメモリコントローラによる排他制御に関する回路の接続関係を例示する説明図である。

【図３】図３はＣＰＵがフラッシュメモリの書換えを行おうとする場合の制御フローを例示するフローチャートである。

【図４】図４は通信回路の通信動作とフラッシュメモリに対する読み出し動作とのメモリコントローラによる排他制御に関する回路の接続関係を例示する説明図である。

【図５】図５はＣＰＵがフラッシュメモリの読み出しを行おうとする場合の制御フローを例示するフローチャートである。

【図６】図６は半導体装置の別の例であるマイクロコンピュータの概略的な構成を例示するブロック図である。

【図７】図７は通信回路の通信動作とフラッシュメモリに対する書き換え動作とのＭＭＵによる排他制御に関する回路の接続関係を例示する説明図である。

【図８】図８は通信回路の通信動作とフラッシュメモリに対する読み出し動作とのＭＭＵによる排他制御に関する回路の接続関係を例示する説明図である。

【図９】図９は通信回路の通信動作とＲＡＭに対する読み出し動作とのＭＭＵによる排他制御に関する回路の接続関係を例示する説明図である。

【発明を実施するための形態】

【００１３】

１．実施の形態の概要

先ず、本願において開示される実施の形態について概要を説明する。ここでの概要説明で括弧を付して参照する図面中の参照符号はそれが付された構成要素の概念に含まれるものを例示するに過ぎない。

【００１４】

〔１〕＜通信とメモリアクセスの排他制御＞

半導体装置（１，１Ａ）は、外部と通信可能な通信部（６１）と、所定の記憶部（３１，２１）と、前記通信部による通信と前記所定の記憶部へのアクセスとの排他制御を行う排他制御部（９１，９２）と、を有する。

【００１５】

これによれば、通信部による通信と所定の記憶部へのアクセスとが排他制御されるから、正規の通信動作中にバックグラウンドでその通信機能を経由して、不正機能が所定の記憶部にインストールされたり、さらには、所定の記憶部から秘匿情報が読み出されて盗み取られたりすることを防止することができる。

【００１６】

〔２〕＜通信クロックを用いた排他制御＞

項１において、前記排他制御部は、前記通信部が通信に用いる通信クロック（ＣＫＣ）の状態を検出する検出回路（５１，５２）を有し、前記検出回路による前記通信部の通信クロックの活性状態に応じて前記所定の記憶部へのアクセスを制限し、前記検出回路による前記通信部の通信クロックの非活性状態に応じて前記所定の記憶部へのアクセス制限を解除する。

【００１７】

これによれば、検出回路での通信クロックの活性／非活性というハードウェア面での状態に基づいて上記排他制御を行うので、通信中の不正アクセスに対するソフトウェア面での対策を補強するという意義を有する。

【００１８】

〔３〕＜通信クロックの発振、発振停止の判定＞

項２において、前記通信部が通信に用いる通信クロックを生成する通信クロック生成部（６２）を有する。前記排他制御部（９１，９２）は、前記通信部の通信クロックの状態を検出する検出回路（５１，５２）を有し、前記検出回路による前記通信クロックの発振停止の検出に応じて前記所定の記憶部へのアクセス制限を解除し、前記検出回路による前記通信クロックの発振再開の検出に応じて前記所定の記憶部へのアクセスを制限する。

【００１９】

これによれば、半導体装置が通信クロック生成部を備える場合には、前記クロック生成回路による通信クロックの発振／発振停止というハードウェア面での状態の検出結果に基づいて上記排他制御を行うので、通信中の不正アクセスに対するソフトウェア面での対策を補強するという意義を有する。

【００２０】

〔４〕＜通信レートを規定する通信クロック＞

項２又は３において、前記通信クロックは通信レートを規定するクロック信号（ＣＫＣ）である。

【００２１】

これによれば、通信レートを規定する通信クロックに対する発振停止／発振再開の検出は高精度に且つ短時間で行う事ができるので、通信クロックに対する検出誤りを防止することができ、上記通信とアクセスの排他制御に対する確実性を容易に保証することができる。

【００２２】

〔５〕＜通信時に書き込み禁止＞

項１において、前記所定の記憶部へのアクセス制限は、前記所定の記憶部（３１）に対する書き込み動作の禁止であり、前記通信部がダウンロードしたデータを一時的に格納する一時記憶部を前記所定の記憶部とは別に有する。

【００２３】

これによれば、通信部による一時記憶部へのダウンロード中にバックグラウンドでその通信機能を経由して不正プログラムなどが所定の記憶部にインストールされることはない。一時記憶部にダウンロードされたプログラムなどを所定の記憶部に書込むときは通信部の通信動作は不可能にされているから、その書き込みに乗じて通信部から不正なプログラムやデータが入り込んで一緒に格納され、或いはすりかえられて格納される事態の発生を抑制することができる。また、一時記憶部に不所望に入り込んだりした不正プログラムが、所定の記憶部に対する正規の書込み処理に乗じて、通信部から不正なプログラムやデータを取り込んで所定に記憶部に書き込むような所謂バックドア（Back Door）の操作を行おうとしてもその処理は阻まれる。要するに、不所望なバックドア操作による被害が通信中に拡大されることを防止することができる。更に具体的には、通信部による一時記憶部へのダウンロード中にバックグラウンドでその通信機能を経由して不正プログラムなどが一時記憶部に入り込んだとしても、ダウンロードと所定の記憶部への書込みとを２ステップで行うので、一時記憶部に入り込んだ不正プログラムそれ自体が所定の記憶部に格納されてしまうことは、ハッシュのようなデータチェックなどのその他のプロテクト手段を講

ずる時間的な余裕があるので、阻むことが容易になる。

【００２４】

〔６〕＜通信時に読み出し禁止＞

項１において、前記所定の記憶部へのアクセス制限は、前記所定の記憶部に対する読み出し動作の禁止である。

【００２５】

これによれば、所定の記憶部に対する読み出し動作中はこれに並行した通信部の通信動作は不可能にされているので、所定の記憶部から秘匿情報が読み出されても、これがそのまま不所望に通信部から外部に漏洩する事態の発生を防止することができる。

【００２６】

〔７〕＜不揮発性メモリ＞

項５又は６において、前記所定の記憶部は電気的に書換え可能な不揮発性メモリ（３１）である。

【００２７】

これによれば、揮発性メモリに不正なプログラムなどが入り込んでもシステムリセット又はメモリクリアされる限りでは、その影響は拡大し難い。一方、不揮発性メモリに不正プログラムなどが一旦入り込むと、その被害を累積的に拡大させるのが容易である。この点で、アクセス制限対象を書き換え可能な不揮発性メモリとすることの意義は大きい。

【００２８】

〔８〕＜メモリコントローラ＞

項５又は６において前記排他制御部（９１）は、アクセス要求に応答して前記所定の記憶部へのメモリインタフェース制御を行うメモリコントローラ（４１）と、前記通信クロックの状態を検出し、発振停止の状態を検出した場合には前記メモリコントローラのメモリインタフェース動作を可能とし、前記通信クロックの発振中の状態を検出した場合には前記メモリコントローラのメモリインタフェース動作を前記アクセス制限に従って不可能とする検出回路（５１，５２）と、を有する。

【００２９】

これによれば、メモリコントローラを流用して排他制御を行うことができる。

【００３０】

〔９〕＜メモリマネージメントユニット＞

項５又は６において前記排他制御部（９２）は、前記所定の記憶部のマッピングアドレスに対するメモリ保護機能を有するメモリマネージメントユニット（４２）と、前記通信クロックの状態を検出し、発振停止の状態を検出した場合には前記メモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を可能とし、前記通信クロックの発振中の状態を検出した場合には前記メモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を前記アクセス制限に従って不可能とする検出回路（５１，５２）と、を有する。

【００３１】

これによれば、メモリマネージメントユニットを流用して排他制御を行うことができる。

【００３２】

〔１０〕＜通信とメモリアクセスの排他制御によるアクセス制限方法＞

アクセス制限方法は、外部と通信可能な通信部による通信動作中は所定の記憶部へのアクセスを制限し、前記通信部による通信動作の休止中は前記所定の記憶部へのアクセス制限を解除することによって、前記通信部による通信と前記所定の記憶部へのアクセスとの排他制御を行う。

【００３３】

これによれば、項１と同様の効果を得る。

【００３４】

〔１１〕＜通信クロックを用いた排他制御＞

項１０において、前記通信部（６１）が通信に用いる通信クロック（ＣＫＣ）の活性状態を検出回路（５１，５２）で検出することに応じて前記所定の記憶部（３１，３２）へのアクセスを制限し、前記通信クロックの非活性状態を前記検出回路で検出することに応じて前記所定の記憶部へのアクセス制限を解除する。

【００３５】

これによれば、項２と同様の効果を得る。

【００３６】

〔１２〕＜通信クロックの発振、発振停止の判定＞

項１０において、前記通信部が通信に用いる通信クロックを生成する通信クロック生成部（６２）における前記通信クロックの発振停止を検出回路で検出することに応じて前記所定の記憶部へのアクセス制限を解除し、前記通信クロックの発振再開を前記検出回路で検出することに応じて前記所定の記憶部へのアクセスを制限する。

【００３７】

これによれば、項３と同様の効果を得る。

【００３８】

〔１３〕＜通信レートを規定する通信クロック＞

項１２において、前記通信クロックは通信レートを規定するクロック信号（ＣＫＣ）である。

【００３９】

これによれば、項４と同様の効果を得る。

【００４０】

〔１４〕＜通信時に書き込み禁止＞

項１０において、前記アクセス制限として前記所定の記憶部（３１）に対する書き込み動作が禁止されている最中に、前記通信部が一時記憶部にダウンロードしたデータを、前記所定の記憶部に対する書き込み動作の禁止が解除されてから前記所定の記憶部に書き込む。

【００４１】

これによれば、項５と同様の効果を得る。

【００４２】

〔１５〕＜通信時に読み出し禁止＞

項１０において、前記通信クロックの発振状態では前記アクセス制限として前記所定の記憶部（３１，２１）に対する読み出し動作を禁止し、前記通信クロックの発振停止の状態で前記所定の記憶部に対する読み出し動作を可能にする。

【００４３】

これによれば、項６と同様の効果を得る。

【００４４】

〔１６〕＜不揮発性メモリ＞

項１４又は１５において、前記所定の記憶部は電気的に書換え可能な不揮発性メモリ（３１）である。

【００４５】

これによれば、項７と同様の効果を得る。

【００４６】

〔１７〕＜メモリコントローラによるアクセス制限の制御＞

項１４又は１５において、前記通信クロックの発振停止の状態を検出回路で検出した場合には、アクセス要求に応答して前記所定の記憶部へのメモリインタフェース制御を行うメモリコントローラ（４１）のメモリインタフェース動作を可能とし、前記通信クロックの発振中の状態を前記検出回路で検出した場合には、前記メモリコントローラのメモリインタフェース動作を前記アクセス制限に従って不可能とする。

【００４７】

これによれば、項８と同様の効果を得る。

【００４８】
〔１８〕＜メモリマネージメントユニットによるアクセス制限の制御＞
項１４又は１５において、前記通信クロックの発振停止の状態を検出回路で検出した場合には、前記所定の記憶部のマッピングアドレスに対するメモリ保護機能を有するメモリマネージメントユニット（４２）に対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を可能とし、前記通信クロックの発振中の状態を前記検出回路で検出した場合には、前記メモリマネージメントユニットに対して前記所定の記憶部にマッピングされたアドレスに対するアドレス変換を前記アクセス制限に従って不可能とする。
【００４９】
これによれば、項９と同様の効果を得る。
【００５０】
２．実施の形態の詳細
実施の形態について更に詳述する。
【００５１】
《１．通信動作とメモリアクセス動作のメモリコントローラによる排他制御》
図１には半導体装置の一例であるマイクロコンピュータの概略的な構成が例示される。同図に示されるマイクロコンピュータ（ＭＣＵ）１は、特に制限されないが、ＣＭＯＳ半導体集積回路製造技術によって単結晶シリコンのような１個の半導体基板に形成される。
【００５２】
マイクロコンピュータ１は、ＣＰＵ（中央処理装置）１１、ＲＡＭ（Random Access Memory）２１、フラッシュメモリ３１、メモリコントローラ４１、アクセス許可回路５１、発振停止確認回路５２、通信回路６１、通信用発振器６２、メイン発振器７１、内部バス８１、及び図示を省略する割込みコントローラなどを有する。ＣＰＵ１１は内部バス８１を介してＲＡＭ２１、フラッシュメモリ３１、メモリコントローラ４１、及び通信回路６１をアクセスする。
【００５３】
ＣＰＵ１１は、フェッチした命令を解読して命令実行を制御する命令制御部及び命令制御部の制御に基づく演算処理を行う実行部とを有し、所定の命令セットを用いて記述されたプログラムを実行する。
【００５４】
ＲＡＭ２１はＣＰＵ１１のワーク領域又はデータ一時記憶領域などに用いられる揮発性メモリであり、例えばＳＲＡＭなどによって構成される。
【００５５】
通信回路６１はマイクロコンピュータ１の外部と通信可能な回路であって、例えば、ユニバーサルシリアルバス、シリアルコミュニケーションインタフェース、又はＩＩＣ（Inter Integrated Circuit）バスインタフェース、又はシリアルペリフェラルインタフェースなどの通信方式による外部インタフェース機能を有する。この通信回路６１における通信に用いるクロック、即ち、通信レートを規定する高精度のクロック信号（通信クロック）ＣＫＣは通信用発振器６２を用いて生成する。メイン発振器７１は上記通信クロックＣＫＣ以外のクロック信号を生成し、例えば内部同期用の基準クロック信号ＣＫＳを生成してマイクロコンピュータ１内のクロック同期回路にそれぞれ供給する。通信用発振器６２及びメイン発振器７１はマイクロコンピュータ１のパワーオンリセットによって発振動作を開始する。また、通信用発振器６２の発振動作はＣＰＵ１１によって停止と再開を制御することが可能にされる。通信回路６１の通信条件の設定、送信イネーブルの指示は例えばＣＰＵ１１が行い、受信データの処理は、例えば図示を省略する割込みコントローラへの受信割り込み要求を介してＣＰＵ１１の割込み処理に委ねる。
【００５６】
フラッシュメモリ３１はＣＰＵ１１が実行するプログラムやデータを書き換え可能に記憶する不揮発性記憶部の一例を成し、不揮発性記憶素子の電荷蓄積領域にトラップされる電子の量に応じて閾値電圧が決定される記憶形式を持つ。

【００５７】
メモリコントローラ４１はＣＰＵ１１からのフラッシュメモリ３１に対するアクセス要求に応答して、フラッシュメモリ３１に対する記憶情報の読み出し及び書き換えのためのメモリ制御を行う。読み出しのためのメモリ制御では、選択した不揮発性記憶素子から得られる読み出し情報を増幅して取得するための制御を行う。書き換えのためのメモリ制御は、プログラム処理とイレーズ処理である。例えばイレーズ処理では書き換え対象の不揮発性記憶素子に消去電圧を与えて閾値電圧の低い消去状態にする電圧印加及びタイミング制御を行う。プログラム処理では書き換え対象の不揮発性記憶素子に書込み電圧を与えて閾値電圧の高い書込み状態にする電圧印加及びタイミング制御を行う。更に、メモリコントローラ４１はアクセス許可回路５１及び発振停止確認回路５２と共に排他制御部９１を実現する。ここに示される排他制御部９１は、通信回路６１による通信とフラッシュメモリ３１へのアクセスとを排他制御する機能を実現する一例として位置付けられる。以下、排他制御部９１による排他制御について詳述する。
【００５８】
発振停止確認回路５２は通信クロックＣＫＣの状態を検出する回路であり、通信クロックが活性状態であるか又は非活性状態であるかを判別する。例えば、発振停止確認回路５２は通信クロックＣＫＣが発振停止したか、そして、通信クロックＣＫＣが発振再開したかを検出する。例えば発振停止確認回路５２は発振停止の検出で検出信号ＤＴＣをハイレベルからローレベルに変化させ、発振再開の検出で検出信号ＤＴＣをローレベルからハイレベルに変化させる。
【００５９】
アクセス許可回路５１は、特に制限されないが、検出信号ＤＴＣによる通信クロックＣＫＣの発振停止の検出に応じてメモリコントローラ４１へのアクセス許可信号ＰＲＭをイネーブルに反転してフラッシュメモリ３１へのアクセス制限を解除し、検出信号ＤＴＣによる通信クロックＣＫＣの発振再開の検出に応じてメモリコントローラ４１へのアクセス許可信号ＰＲＭをディスエーブルに反転してフラッシュメモリ３１へのアクセスを制限する。
【００６０】
メモリコントローラ４１は、ＣＰＵ１１からフラッシュメモリ３１の書き換え指示があった場合、アクセス許可信号ＰＲＭがイネーブルにされていることを条件に、フラッシュメモリ３１の書き換え動作を行うことができる。書き換え指示を受けたとき、アクセス許可信号ＰＲＭがディスエーブルにされている場合には、アクセス許可信号ＰＲＭがイネーブルにされているのを待って、フラッシュメモリ３１の書き換え動作を行うことができる。また、アクセス許可信号ＰＲＭがイネーブルにされている状態でフラッシュメモリ３１の書き換え動作を行っている最中に、アクセス許可信号ＰＲＭがディスエーブルにされたときは、これに応答して、書き換え動作を中断する。メモリコントローラ４１は、書き換え動作を中断した場合、例えば、その書き換え動作を途中から再開できるように必要な書き換え制御情報を自ら保持し、或いは、ＣＰＵ１１に書込みエラーを返す。
【００６１】
また、メモリコントローラ４１は、ＣＰＵ１１からフラッシュメモリ３１の読み出し指示があった場合、アクセス許可信号ＰＲＭがイネーブルにされていることを条件に、フラッシュメモリ３１の読み出し動作を行うことができる。読み出し指示を受けたとき、アクセス許可信号ＰＲＭがディスエーブルにされている場合には、アクセス許可信号ＰＲＭがイネーブルにされているのを待って、フラッシュメモリ３１の読み出し動作を行うことができる。また、アクセス許可信号ＰＲＭがイネーブルにされている状態でフラッシュメモリ３１の読み出し動作を行っている最中に、アクセス許可信号ＰＲＭがディスエーブルにされたときは、これに応答して、読み出し動作を中断する。メモリコントローラ４１は、読み出し動作を中断した場合、例えば、その読み出し動作を途中から再開できるように必要な読み出し制御情報を自ら保持し、或いは、ＣＰＵ１１に読み出しエラーを返す。
【００６２】

図２には通信回路６１の通信動作とフラッシュメモリ３１に対する書き換え動作との排他制御に関する回路の接続関係が例示される。ＣＰＵ１１が通信回路６１を設定して通信回路６１で受信した書き換えデータをＲＡＭ２１に格納する。通信回路６１の通信動作中は通信用発振器６２で生成される通信クロックＣＫＣに同期して通信動作が行われるから、発振停止確認回路５２で通信クロックＣＫＣのクロック変化が検出されることによって検出信号ＤＴＣがハイレベルにされ、これを受けるアクセス許可回路５１はアクセス許可信号ＰＲＭをディスエーブルとし、メモリコントローラ４１によるフラッシュメモリのアクセス制御が不可能にされている。したがって、通信回路６１によるダウンロードデータを直接フラッシュメモリ３１に書き込むことはできない。

【００６３】

ＣＰＵ１１は書き換えデータをＲＡＭ２１にダウンロードした後に、通信用発振器６２の発振動作を停止させる。これによって通信クロックＣＫＣのクロック変化が停止されると、検出信号ＤＴＣがローレベルにされ、これを受けるアクセス許可回路５１はアクセス許可信号ＰＲＭをイネーブルとし、メモリコントローラ４１によるフラッシュメモリのアクセス制御を可能にする。ＣＰＵ１１はＲＡＭ２１に格納された書き換えデータでフラッシュメモリ３１を書き換える指示を発行することにより、メモリコントローラ４１はその書き換え指示にしたがってフラッシュメモリ３１を書き換えることができる。書換えが行われているとき通信クロックＣＫＣは発振停止されているから通信回路６１による通信は不可能である。書き換え中に通信用発振器６２の発振動作が再開されたとしても、その時点でアクセス許可信号ＰＲＭがディスエーブルに反転されるので、書き換え動作それ自体が中断されることになる。

【００６４】

図３にはＣＰＵ１１がフラッシュメモリ３１の書換えを行おうとする場合の制御フローが例示される。ＣＰＵ１１が外部から書き換えデータをダウンロードしてフラッシュメモリ３１の書換えを行おうとする場合、先ず、通信用発振器６２の発振動作を開始させ（Ｓ１）、ＣＰU11が通信回路６１を用いて新しいプログラムやデータなどの書き換えデータをダウンロードして（Ｓ２）、ＲＡＭ２１の一時格納領域に格納する（Ｓ３）。ＣＰＵ１１は通信回路６１による受信完了の通知を割り込み要求などを介して受けることによって通信回路を終了し（Ｓ４）、通信用発振器６２の発振動作を停止させる（Ｓ５）。

【００６５】

発振停止確認回路５２は通信クロックＣＫＣの停止を確認すると（Ｓ６）、アクセス許可回路５１がメモリコントローラ４１に書換えを許可する（Ｓ７）。これによって、メモリコントローラ４１は、ＣＰＵ１１からの書き換え要求に基づいて、ＲＡＭ２１にダウンロードされた書き換えデータを用いてフラッシュメモリ３１を書き換える書き換え動作を制御する（Ｓ８）。

【００６６】

上記通信動作とフラッシュメモリの書き換え動作との排他制御によれば、以下の作用効果を奏する。

【００６７】

（１）発振停止確認回路５２での通信クロックＣＫＣの活性／非活性というハードウェア面での状態に基づいて通信回路６１による通信動作とメモリコントローラ４１によるフラッシュメモリ３１の書き換え動作とを排他制御するので、通信中の不正アクセスに対するソフトウェア面での対策（例えばデータサイズの検証、又はハッシュによる検証など）を補強することができる。

【００６８】

（２）通信レートを規定する通信クロックＣＫＣに対する発振停止／発振再開の検出は高精度に且つ短時間で行う事ができるので、通信クロックに対する検出誤りを防止することができ、上記通信とアクセスの排他制御に対する確実性を容易に保証することができる。即ち、通信と書き換えの排他動作を実現するためには、確実かつ容易な通信停止判定方法の実現が必要である。ここでは、通信機能ではボーレート生成のためにクロックが必須

であることに着目し、このクロック、即ち通信クロックＣＫＣを判定に用いる。一般的に、クロック停止判定に際しては、判定時間の長さ、および、対象クロックが不安定な場合の誤判定などが考慮される。例えば、クロック停止判定のために独立した発振器で生成した基準クロックを判定に用いる場合には、予め決められた基準クロックの複数サイクル期間で当該クロックの反転有無を検出しなければならない。これは、コストなどとの関係で当該基準クロックに過度な高精度を要求することができないからである。本実施の形態では、通信に必須な通信用クロックＣＫＣが高速かつ高精度であることを利用することにより、不安定なクロックに対する停止検出の時間的制約や検出精度低下という課題を残さないように解決している。換言すれば、通信動作の停止を通信クロックの停止というハードウェア面で検出することを容易且つ高精度に実現することができる。

【００６９】

（３）通信時にフラッシュメモリ３１に対する書き換え動作を禁止するというアクセス制限を行うことができるから、通信回路６１によるＲＡＭ２１へのダウンロード中にバックグラウンドでその通信動作を経由して不正プログラムなどがフラッシュメモリ３１にインストールされることはない。ＲＡＭ２１にダウンロードされたプログラムなどをフラッシュメモリ３１に書込むときは通信回路６１の通信動作は不可能にされているから、その書き込みに乗じて通信回路６１から不正なプログラムやデータが入り込んで一緒に格納され、或いはすりかえられて格納される事態の発生を抑制することができる。また、ＲＡＭ２１に不所望に入り込んだりした不正プログラムが、フラッシュメモリ３１に対する正規の書込み処理に乗じて、通信回路６１から不正なプログラムやデータを取り込んでフラッシュメモリ３１に書き込むような所謂バックドアの操作を行おうとしてもその処理は阻まれる。要するに、不所望なバックドア操作による被害が通信中に拡大されることを防止することができる。更に具体的には、通信回路６１によるＲＡＭ２１へのダウンロード中にバックグラウンドでその通信機能を経由して不正プログラムなどがＲＡＭ２１に入り込んだとしても、ダウンロードとフラッシュメモリ３１への書込みとを２ステップで行うので、ＲＡＭ２１に入り込んだ不正プログラムそれ自体がフラッシュメモリ３１に格納されてしまうことは、ハッシュのようなデータチェックなどのその他のプロテクト手段を講ずる時間的な余裕があるので、阻むことが容易になる。

【００７０】

図４には通信回路６１の通信動作とフラッシュメモリ３１に対する読み出し動作との排他制御に関する回路の接続関係が例示される。ＣＰＵ１１はフラッシュメモリ３１からデータを読み出すとき、予め通信用発振器６２の発振動作を停止させ、これを発振停止確認回路５２に検出させて許可信号ＰＲＭをイネーブルにする。これによってメモリコントローラ４１はＣＰＵ１１からのフラッシュメモリ３１に対する読み出しアクセスの要求に応答してフラッシュメモリ３１に対する読み出し動作を行う事ができる。フラッシュメモリ３１から読み出しが行われているとき通信クロックＣＫＣは発振停止されているから通信回路６１による通信は不可能である。読み出し中に通信用発振器６２の発振動作が再開されたとしても、その時点でアクセス許可信号ＰＲＭがディスエーブルに反転されるので、読み出し動作それ自体が中断されることになる。

【００７１】

図５にはＣＰＵ１１がフラッシュメモリ３１の読み出しを行おうとする場合の制御フローが例示される。ＣＰＵ１１は通信回路６１による通信処理を終了し（Ｓ１１）、通信用発振器６２の発振動作を停止させる（Ｓ１２）。発振停止確認回路５２は通信クロックＣＫＣの停止を確認すると（Ｓ１３）、アクセス許可回路５１がメモリコントローラ４１に書換えを許可する（Ｓ１４）。これによって、メモリコントローラ４１は、ＣＰＵ１１からの読み出し要求に基づいて、フラッシュメモリ３１の読み出し動作を制御する（Ｓ１５）。

【００７２】

上記通信動作とフラッシュメモリの読み出し動作との排他制御によれば、以下の作用効果を奏する。

【００７３】
（１）フラッシュメモリ３１に対する読み出し動作中はこれに並行した通信回路６１の通信動作は不可能にされているので、フラッシュメモリ３１から秘匿情報（例えばパスワード又は個人情報など）が読み出されても、これがそのまま不所望に通信回路６１を経由してから外部に漏洩する事態の発生を防止することができる。
【００７４】
（２）発振停止確認回路５２での通信クロックＣＫＣの活性／非活性というハードウェア面での状態に基づいて通信回路６１による通信動作とメモリコントローラ４１によるフラッシュメモリ３１の読み出し動作とを排他制御するので、通信中の不正アクセスに対するソフトウェア面での対策を補強することができる。
【００７５】
《２．通信動作とメモリアクセス動作とのＭＭＵによる排他制御》
図６には半導体装置の別の例であるマイクロコンピュータの概略的な構成が例示される。同図に示されるマイクロコンピュータ（ＭＣＵ）１Ａは、特に制限されないが、ＣＭＯＳ半導体集積回路製造技術によって単結晶シリコンのような１個の半導体基板に形成される。
【００７６】
図６のマイクロコンピュータ１Ａには仮想記憶が採用され、ＭＭＵ（メモリマネージメントユニット）４２により、ＣＰＵ１が出力する論理アドレスを物理アドレスに変換し、変換された物理アドレスがバス８７１に出力されることによってＲＡＭ２１やフラッシュメモリ３１などのアクセスアドレスが指定される。特に制限されないが、プログラム情報やデータ情報などのデータに関してはキャッシュメモリ（ＣＡＣＨＥ）４３が設けられている。ＭＭＵ４２は論理アドレスを物理アドレスに変換するために変換対を有し、更に変換対にはメモリ保護を行うための保護情報が設定される。保護情報は、当該アドレスのアクセスに必要なアクセス権（例えばユーザモードによるアクセス可能なユーザエリア、特権モードによるアクセス可能な特権エリアなど）の種別、当該アドレスのアクセスが許容されるアクセス種別（例えばリード又はライトなどの種別）を指定する情報などとされる。図６の例では、ＭＭＵ４２は、前記アクセス許可回路５１及び発振停止確認回路５２と共に排他制御部９２を実現する。ここに示される排他制御部９２は、通信回路６１による通信とフラッシュメモリ３１又はＲＡＭ２１へのアクセスとを排他制御する機能を実現する一例として位置付けられる。したがって、メモリコントローラ４１Ａには図１で説明した排他制御に特有の構成と機能、即ち、アクセス許可信号ＰＲＭに応じたアクセス制限機能が省略されている。その他、図１と同様に機能を有する回路ブロック及び信号には同じ参照符号を付してそれらの詳細な説明は省略する。以下、排他制御部９１による排他制御について詳述する。
【００７７】
ＭＭＵ４２はＣＰＵ１１がフラッシュメモリ３１又はＲＡＭ２１に割り当てられた特定の論理アドレスを出力したとき、アクセス許可信号ＰＲＭがイネーブルにされていることを条件に、当該特定論理アドレスに対する物理アドレスへのアドレス変換を行う。アクセス許可信号ＰＲＭがディスエーブルにされている場合には、アドレスエラーなどの例外処理をＣＰＵ１１に要求する。要するに、通信用発振器６２の発振状態において特定論理アドレスの物理アドレスへの変換が拒否され、結果として、このときはＣＰＵ１１によるフラッシュメモリ３１又はＲＡＭ２１のアクセスが拒否される。通信用発振器６２の発振停止状態では特定論理アドレスの物理アドレスへの変換が行われ、結果として、このときはＣＰＵ１１によるフラッシュメモリ３１又はＲＡＭ２１のアクセスが可能にされる。
【００７８】
ＭＭＵ４２は上記特定の論理アドレスに対するライト動作およびリード動作においてアクセス許可信号ＰＲＭのイネーブル／ディスエーブルの状態に従ってアドレス変換の制限／制限解除を行う。
【００７９】

図７には通信回路６１の通信動作とフラッシュメモリ３１に対する書き換え動作との排他制御に関する回路の接続関係が例示される。この例では上記特定の論理アドレスはフラッシュメモリ３１に割り当てられる論理アドレスとする。

【００８０】

ＣＰＵ１１が通信回路６１を設定して通信回路６１で受信した書き換えデータをＲＡＭ２１に格納する。通信回路６１の通信動作中は通信用発振器６２で生成される通信クロックＣＫＣに同期して通信動作が行われるから、発振停止確認回路５２で通信クロックＣＫＣのクロック変化が検出されることによって検出信号ＤＴＣがハイレベルにされ、これを受けるアクセス許可回路５１はアクセス許可信号ＰＲＭをディスエーブルとし、フラッシュメモリに割り当てられた論理アドレスに対するＭＭＵ４２でのアドレス変換が不可能にされ、結果として、通信回路６１による通信動作中にはメモリコントローラ４１によるフラッシュメモリ３１のアクセス制御が不可能になる。したがって、通信回路６１によるダウンロードデータを直接フラッシュメモリ３１に書き込むことはできない。

【００８１】

ＣＰＵ１１は書き換えデータをＲＡＭ２１にダウンロードした後に、通信用発振器６２の発振動作を停止させる。これによって通信クロックＣＫＣのクロック変化が停止されると、検出信号ＤＴＣがローレベルにされ、これを受けるアクセス許可回路５１はアクセス許可信号ＰＲＭをイネーブルとし、フラッシュメモリ３１に割り当てられた論理アドレスに対するＭＭＵ４２でのアドレス変換を可能にする。したがって、ＣＰＵ１１がＲＡＭ２１に格納された書き換えデータでフラッシュメモリ３１を書き換えるアクセス指示に対して、メモリコントローラ４１はその書き換え指示にしたがってフラッシュメモリ３１を書き換えることができる。書換えが行われているとき通信クロックＣＫＣは発振停止されているから通信回路６１による通信は不可能である。書き換え中に通信用発振器６２の発振動作が再開されたとしても、その時点でアクセス許可信号ＰＲＭがディスエーブルに反転されるので、ＣＰＵ１１が発行する新たなアクセスアドレスによるフラッシュメモリの書き換え動作はアドレスエラーによって阻まれることになる。

【００８２】

上記通信動作とフラッシュメモリの書き換え動作とのＭＭＵによる排他制御によれば、以下の作用効果を奏する。

【００８３】

（１）発振停止確認回路５２での通信クロックＣＫＣの活性／非活性というハードウェア面での状態に基づいて通信回路６１による通信動作中はＭＭＵ４２によるフラッシュメモリ３１のアクセス保護機能が働き、通信回路６１による通信動作とフラッシュメモリ３１の書き換え動作とを排他制御することができるので、通信中の不正アクセスに対するソフトウェア面での対策（例えばデータサイズの検証、又はハッシュによる検証など）を補強することができる。

【００８４】

（２）通信レートを規定する通信クロックＣＫＣに対する発振停止／発振再開の検出は高精度に且つ短時間で行う事ができるので、通信クロックに対する検出誤りを防止することができ、上記通信とアクセスの排他制御に対する確実性を容易に保証することができる。

【００８５】

（３）通信時にフラッシュメモリ３１に対する書き換え動作を禁止するというアクセス制限をＭＭＵ４２を介して行うことができるから、通信回路６１によるＲＡＭ２１へのダウンロード中にバックグラウンドでその通信動作を経由して不正プログラムなどがフラッシュメモリ３１にインストールされることはない。ＲＡＭ２１にダウンロードされたプログラムなどをフラッシュメモリ３１に書込むときは通信回路６１の通信動作は不可能にされているから、その書き込みに乗じて通信回路６１から不正なプログラムやデータが入り込んで一緒に格納され、或いはすりかえられて格納される事態の発生を抑制することができる。また、ＲＡＭ２１に不所望に入り込んだりした不正プログラムが、フラッシュメモ

リ３１に対する正規の書込み処理に乗じて、通信回路６１から不正なプログラムやデータを取り込んでフラッシュメモリ３１に書き込むような所謂バックドアの操作を行おうとしてもその処理は阻まれる。要するに、不所望なバックドア操作による被害が通信中に拡大されることを防止することができる。

【００８６】

図８には通信回路６１の通信動作とフラッシュメモリ３１に対する読み出し動作との排他制御に関する回路の接続関係が例示される。この例では上記特定の論理アドレスはフラッシュメモリ３１に割り当てられる論理アドレスとする。

【００８７】

ＣＰＵ１１はフラッシュメモリ３１からデータを読み出すとき、予め通信用発振器６２の発振動作を停止させ、これを発振停止確認回路５２に検出させて許可信号ＰＲＭをイネーブルにする。これによってフラッシュメモリ３１に割り当てられた論理アドレスに対するＭＭＵ４２でのアドレス変換が可能にされ、変換された物理アドレスを用いてメモリコントローラ４１はＣＰＵ１１からのフラッシュメモリ３１に対する読み出しアクセスに応答してフラッシュメモリ３１に対する読み出し動作を行う事ができる。フラッシュメモリ３１から読み出しが行われているとき通信クロックＣＫＣは発振停止されているから通信回路６１による通信は不可能である。読み出し中に通信用発振器６２の発振動作が再開されたとしても、その時点でアクセス許可信号ＰＲＭがディスエーブルに反転されるので、ＣＰＵ１１が発行する新たなアクセスアドレスによるフラッシュメモリのリード動作はアドレスエラーによって阻まれることになる。

【００８８】

上記通信動作とフラッシュメモリ３１の読み出し動作とのＭＭＵ４１による排他制御によれば、以下の作用効果を奏する。

【００８９】

（１）フラッシュメモリ３１に対する読み出し動作中はこれに並行した通信回路６１の通信動作は不可能にされているので、フラッシュメモリ３１から秘匿情報（例えばパスワード又は個人情報など）が読み出されても、これがそのまま不所望に通信回路６１を経由してから外部に漏洩する事態の発生を防止することができる。

【００９０】

（２）発振停止確認回路５２での通信クロックＣＫＣの活性／非活性というハードウェア面での状態に基づいて通信回路６１による通信動作中はＭＭＵ４２によるフラッシュメモリ３１のアクセス保護機能が働き、通信回路６１による通信動作とフラッシュメモリ３１の読み出し動作とを排他制御することができるので、通信中の不正アクセスに対するソフトウェア面での対策（例えばデータサイズの検証、又はハッシュによる検証など）を補強することができる。

【００９１】

最後に、通信動作とメモリアクセス動作とのＭＭＵによる排他制御の対象をＲＡＭ２１とする場合の例を説明する。

【００９２】

図９には通信回路６１の通信動作とＲＡＭ２１に対する読み出し動作との排他制御に関する回路の接続関係が例示される。ここでは、許可信号ＰＲＭを参照して行われるＭＭＵ４２によるメモリ保護機能の対象が図７及び図８の場合と相違される。即ち、ここは上記特定の論理アドレスはＲＡＭ２１に割り当てられる論理アドレスとする。

【００９３】

通信用発振器６２の発振動作が行われているとき、これを発振停止確認回路５２が検出して許可信号ＰＲＭをイネーブルにすることにより、ＭＭＵ４２は、ＲＡＭ２１に割り当てられた論理アドレスに対してぶつ路アドレスへのアドレス変換を行わず、アドレスエラーを発行し、結果として、ＣＰＵ１１によるＲＡＭ２１のアクセスが不可能にされる。

【００９４】

ＣＰＵ１１はＲＡＭ２１をアクセスするとき、予め通信用発振器６２の発振動作を停止

させ、これを発振停止確認回路５２に検出させて許可信号ＰＲＭをイネーブルにする。これによって、ＲＡＭ２１に割り当てられた論理アドレスに対するＭＭＵ４２でのアドレス変換が可能にされ、結果として、変換された物理アドレスでＲＡＭ２１のアクセスが可能になる。ＲＡＭ２１に対するアクセス中は通信クロックＣＫＣの発振が停止されているから通信回路６１による通信は不可能である。ＲＡＭ２１のアクセス中に通信用発振器６２の発振動作が再開されたとしても、その時点でアクセス許可信号ＰＲＭがディスエーブルに反転されるので、ＣＰＵ１１がＲＡＭアクセスのために発行する新たなアクセスアドレスに対してはアドレスエラーが発生して、その後のＲＡＭ２１のアクセスが阻まれる。

【００９５】

通信回路６１の通信動作とＲＡＭ２１に対する読み出し動作とのＭＭＵ４２による排他制御についても、フラッシュメモリに対する場合と同様の作用効果を奏する。特にＲＡＭ２１に対する上記排他制御によるメモリ保護の場合は、フラッシュメモリ３１に対する不正書き込みや読み出しの前段階としての通信回路６１からＲＡＭ２１への不正なプログラムやデータの書込みを阻止する意味がある。

【００９６】

本発明は上記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【００９７】

例えば、発振停止の確認に基づくアクセス排他制御は高速クロックを検出して書き換えなどのアクセスを制限する機能を実現できればよく、上記実施の形態に制限されない。例えば、図１の排他制御部９１を、高速のクロックである通信クロックＣＫＣでは正常動作することができないメモリコントローラに置き換える例が考えられる。すなわち、メモリコントローラの制御対象をフラッシュメモリとすると、書き換えに用いる高電圧をチャージポンプで生成する構成において、その高速同期クロックが入力されているときはチャージポンプの昇圧動作を行わない構成とする。これにより、通信クロックが停止されている場合だけ昇圧電圧を用いた書換えが可能にされ

また、アクセス許可回路を省略して、発振停止の検出信号ＤＴＣをアクセス許可信号ＰＲＭに流用してもよい。

【００９８】

通信とアクセスとの排他制御の対象になる記憶部はフラッシュメモリ又はＲＡＭに限定されず、双方共に排他制御の対象としてもよいし、また、フラッシュメモリは誘電体メモリのアドのその他の不揮発性メモリであってもよい。

【００９９】

通信部は上記ユニバーサルシリアルバスなどの通信機能に限定されない。例えばアンテナに接続される高周波インタフェース部であってもよい。排他制御部にはＭＭＵやメモリコントローラを流用する場合に限定されず、物理的にアクセス経路を遮断するハードウェアを採用することも可能である。

【符号の説明】

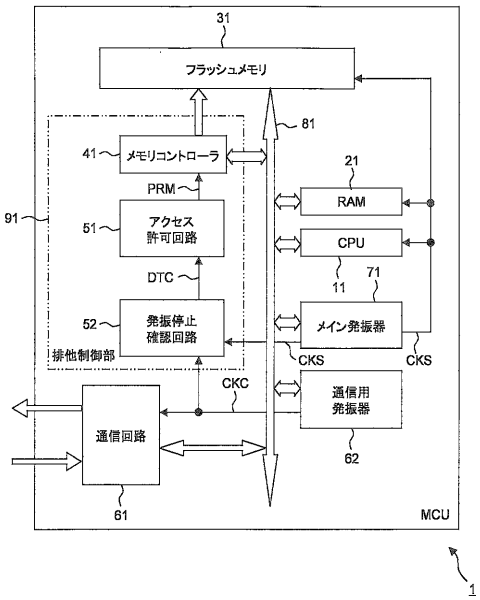
【０１００】

１　マイクロコンピュータ（ＭＣＵ）
１Ａ　マイクロコンピュータ
１１　ＣＰＵ（中央処理装置）
２１　ＲＡＭ
３１　フラッシュメモリ
４１　メモリコントローラ
４２　ＭＭＵ（メモリマネージメントユニット）
４３　キャッシュメモリ（ＣＡＣＨＥ）
５１　アクセス許可回路
５２　発振停止確認回路
６１　通信回路

６２　通信用発振器
７１　メイン発振器
８１　内部バス
９１　排他制御部
９２　排他制御部
ＣＫＣ　通信クロック
ＣＫＳ　基準クロック信号
ＤＴＣ　検出信号
ＰＲＭ　アクセス許可信号

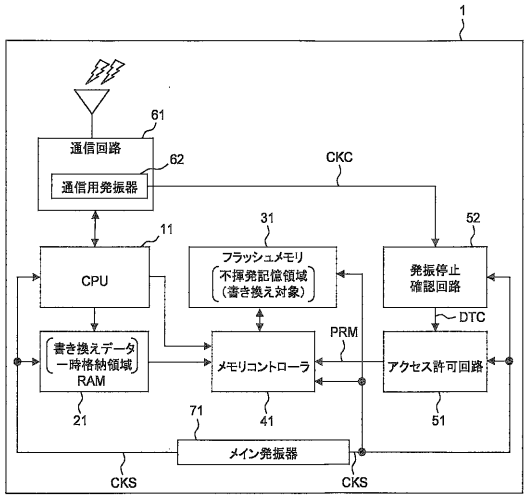
【図１】

図1



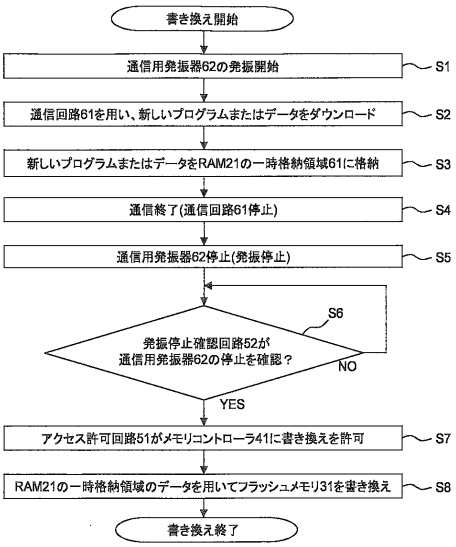
【図２】

図2



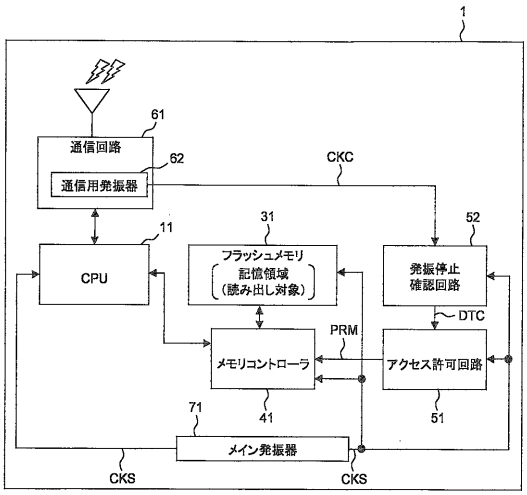
【図３】

図3



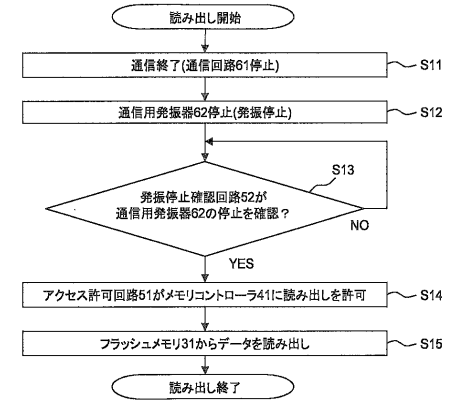
【図４】

図4



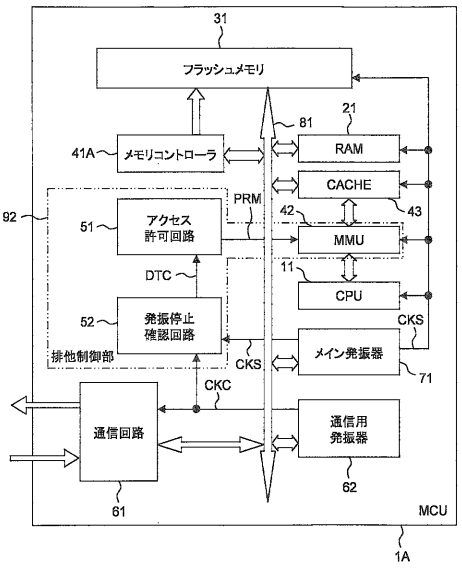
【図５】

図5



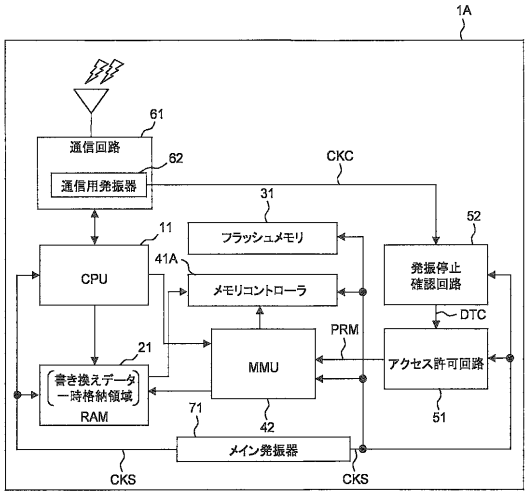
【図６】

図6



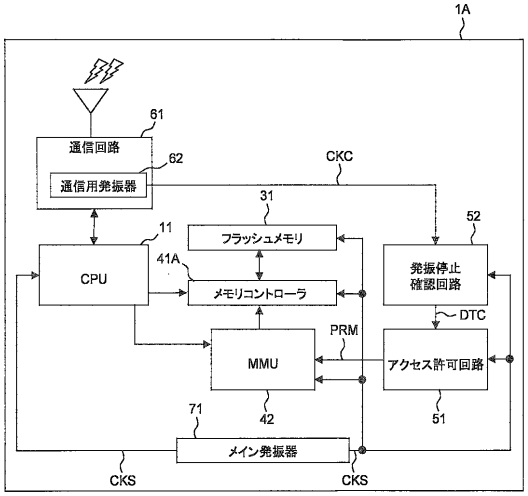
【図７】

図7



【図８】

図8



【図９】

図9