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

特許第3886560号

(P3886560)

(45)発行日　平成19年2月28日(2007.2.28)　(24)登録日　平成18年12月1日(2006.12.1)

(51)Int.Cl.		F I		
G06F 12/14	(2006.01)	G06F	12/14	320B
G09C 1/00	(2006.01)	G06F	12/14	320C
H04L 9/10	(2006.01)	G09C	1/00	660A
H04L 9/32	(2006.01)	H04L	9/00	621A
		H04L	9/00	673E

請求項の数 1　(全 11 頁)

(21)出願番号　特願平8-123330
(22)出願日　平成8年5月17日(1996.5.17)
(65)公開番号　特開平9-34797
(43)公開日　平成9年2月7日(1997.2.7)
審査請求日　平成15年5月12日(2003.5.12)
(31)優先権主張番号　95410047.5
(32)優先日　平成7年5月18日(1995.5.18)
(33)優先権主張国　ドイツ(DE)

前置審査

(73)特許権者　398038580
ヒューレット・パッカード・カンパニー
HEWLETT-PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男
(72)発明者　ヴィカード・ドミニク
フランス国クロレス，ルー　アポリネール　24

最終頁に続く

(54)【発明の名称】機能用法制御付き集積回路デバイス

(57)【特許請求の範囲】

【請求項１】

集積回路デバイスの機能ブロックの動作の有効化を制御するために該集積回路デバイスの中に実装する標準セルであって、該標準セルが、

少なくとも１つの参照値を記憶するための記憶手段と、

入力を受信し、該入力を暗号解読処理にかけて第１の中間値を生成するための保全通信手段と、

前記第１の中間値を受信し、該第１の中間値について一方向機能を実行して第２の中間値を生成するための一方向手段と、

前記第２の中間値と前記少なくとも１つの参照値との一致を検出し、少なくとも１つの前記一致が検出されると有効信号を生成する比較手段と、

前記有効信号が生成されるまで、前記機能ブロックへの必要なクロック信号を遮断するための抑止手段と、

を備えている標準セル。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】

本願発明は機能の用法制御付き集積回路デバイスに関する。

【０００２】

【従来の技術】

コンピュータの機密保護の分野では、2つの要素、即ち、データアクセス制御と機能用法制御が特徴となる。これらの要素は相互に重複し且つからみ合っており－例えば、データアクセス制御はアクセス装置の用法の限定（機能用法制御）にしばしば左右され、一方、機能用法制御はしばしばパスワードの保全格納（データアクセス制御）に厳密に基づいている。

【０００３】

データアクセス制御に関しては、これは保全すべきデータを維持する概して安全な環境を設定し且つその上でデータアクセス装置の用法を制御するという形をとることができる。しかし、多くの場合、環境の保全を保証することは不可能であり且つそのような場合に保全すべきデータは改ざん（不正変更）防止パッケージ(tamper-proof package)で保持するかもしくは暗号形式で格納しなければならない。後者のアプローチは必ずしも可能でなくてもよく（マスタ暗号キーは明文で記憶の必要あり）、従って、例えば、パッケージを開けようとする何らかの試みがなされると内部に格納された重要なデータを破壊する改ざん防止パッケージの設計に多くの努力を払った。改ざん防止パッケージは少なくとも小回路基板を保持するよう設計されるが、改ざん防止の特徴はある種の"スマート・カード"チップにも備えられている。

【０００４】

さて、本願発明が関わる機能用法制御について考えれば、認可された人だけがコンピュータシステム及び他の電子機器のようなアイテムに操作上アクセスし得るということを保証するための様々な技法が知られている。例えば、コンピュータは、そのコンピュータの電源がオンされると又は（例えば、ユーザが一時的にそのコンピュータを離れる時の）パスワード保護の起動の後では、コンピュータの動作機能を復帰させる前に予め決めたパスワードを入力しなければならない。別の周知の機能用法制御技術は、自動窓口機(ATM)に関連した個人識別番号(PIN)の利用である。これらの両方の場合、ユーザは（形式はどうであれ、ATMを含む）有効なパスワードを覚えていなければならず、結果として、そのようなパスワードは、通常、短く従って極めて安全とは言えず、しばしば推測可能である。

【０００５】

代替アプローチとしては、有効パスワードを記憶する磁気層カード又は"スマート"カードのような携帯素子を用いることであり、この携帯素子は認可されたユーザが携えて当該機器を使用可能にするのに用いる。この場合、パスワードはかなり長くてもよく、従って比較的安全である。

【０００６】

前述の構成における1つの潜在的弱点は、用法制御に供される装置は、ユーザの入力パスワードの比較のため有効パスワードのコピーを記憶している必要がある（データアクセス制御問題に帰着）。パスワードが明文で格納される場合、もしその装置が非認可のユーザ（ここでは"侵入者"と呼ぶ）によって内部的に物理的にアクセスされるとそのパスワードは見破られる可能性がある。この弱点を克服する1つの方法は、その装置のパスワードの識別特性(signature)だけを格納することであり、該識別特性は、パスワードが合法的ユーザによって入力される時にその装置がそのパスワードから識別特性を容易に作ることができるが、それからパスワードを引き出せないような種類のものである。前述のアプローチでは、パスワードから識別特性を引き出すために一方向ハッシュ機能のような機能が用いられる。

【０００７】

しかし、装置の物理的構造の故に侵入者がユーザによるその入力時にパスワードをキャッチできるか（これは例えパスワードが暗号形式で装置に通されたとしても可能であろう）、又は用法制御を巧みに免れて装置の機能素子に直接アクセスできれば、前述の精巧な技術でさえ無価値なものとなってしまう。

【０００８】

装置アイテムに対して侵入者が内部的物理的アクセスに成功するという可能性を克服するのに、装置ケースを物理的に施錠することが知られている。一般的には高度に感知可能な

データを保護するという情況においてであるが、それよりも精巧なアプローチ法も知られている；例えば、暗号化／暗号解読キーを格納している暗号化／暗号解読モジュールに対して改ざん防止の囲いを設けることが知られている。内部的物理的な不正侵入に対して防御壁を設けるというようなアプローチは、効果があるとはいえ、一般に非常に費用がかかり且つ感知可能データと密接に関連づけられない機能性の保護には適用されない。

【０００９】

【発明の目的】

本願発明の目的は、非認可のユーザにとって物理的にアクセス可能であるかも知れない電子機器に適していてしかも特別の改ざん防止格納装置を使わなくてもよい機能用法制御への一般的アプローチ法を提供することにある。

【００１０】

【発明の概要】

一般的に、本発明は、電子組立体を作り上げる集積回路デバイスのレベルで機能用法制御を設定することを考察するものであり、それによって、少なくとも1つの集積回路デバイスで設定される機能性を使用するには、先ず、そのデバイスが暗号形式の適当なパスワード（"チップ・キー"）を備える必要がある。そのような機能用法制御は、各デバイスに組み込まれたもので、その機能性へのアクセスに制御を要するロック回路セルによって実行される。そのような構成では、機器アイテムへの内部的物理的アクセスをする侵入者は、保護されたデバイスの機能性のロックを開けることができず、且つ当該デバイスを切り開けば必要とされている機能性が破壊されることになるので、その機能性に直接アクセスできない。

【００１１】

より正式には、本願発明によって、デバイスに所望の機能性を与えるための機能ブロックと、デバイスの外部からの、少なくとも1つの予め決めた暗号形式のチップ・キーの処理がロック回路機構になされるまでこの機能ブロックの動作を抑止するロック回路機構とを有して成る集積回路デバイスが提供され；該ロック回路機構は、

少なくとも1つの参照値を記憶するための記憶手段と；

デバイスの外部からの入力を受信し且つその入力を暗号解読処理にかけて第一の中間値を生成する保全通信手段であって、該暗号解読処理の特徴は、前記入力が暗号形式のようなキーである時、前記第一中間値が前記チップ・キーの明文形式に一致するようなものである保全通信手段と；

第一の中間値を受信し且つそれについて一方向機能を実行して第二の中間値を生成するための手段と；

第二の中間値と記憶した参照値との一致状況を検出し、且つ少なくとも1つの前述の一致が検出し終わった時に有効信号を生成するための比較手段と；

有効信号が生成されるまで前記機能ブロックの動作を禁止する抑止手段と

を備え；

前記機能ブロックの本来の目的は、外部アイテムの制御及び／又は外部供給データの処理と出力である。

【００１２】

例として、保全通信手段は、デバイスに前記入力を渡すのに用いられる一回限りの暗号キーでDiffie-Hellman Key Exchangeアルゴリズムを実行してよい。一方向機能は、Secure Hash Algorithmによって実行されるような一方向ハッシュ機能であってよい。

【００１３】

発明の好ましい実施例では、抑止手段は機能ブロックへの所要クロック信号を遮断し、それによって後者を操作上使えなくするというよりは内部的に稼働しなくする。

【００１４】

本発明の一実施例では、記憶手段は、前記機能ブロックに関して複数の参照値を記憶し、比較手段は、各記憶参照値について一致状態を検出した後でのみ前記有効信号を生成する。

【００１５】
別の実施例では、デバイスは、ぞれぞれが記憶手段に記憶された各参照値を有する複数の機能ブロックと、各機能ブロックに対するそれぞれの抑止手段との両方を備える；この場合、比較手段が第二の中間値と記憶参照値との間で一致を検出すると、それが一致した参照値と関連した機能ブロックの抑止手段へ有効信号を供給する。
【００１６】
前述の実施例のどちらにおいても、1つの機能ブロックの動作上の有効化が、対応する抑止手段による有効信号の受信と機能ブロックの別の1つの事前の有効化との両方を条件にするよう構成することもできる。
【００１７】
本願発明は、その全てが上記形式のロック回路機構を含む同一系列の集積回路デバイスを有するという概念に及び、該ロック回路機構は、好ましくは、必要に応じ新しい集積回路デバイスに組み込めるよう標準セルとして利用できるものである。
【００１８】
このように、本願発明の別の様相によって、集積回路デバイスに組み込んでそのデバイスの機能ブロックの動作上の有効化を制御できる標準セルが提供され、該標準セルは、
少なくとも1つの参照値を記憶するための記憶手段と；
入力を受信し且つそれを暗号解読処理にかけて第一の中間値を生成する保全通信手段と；
第一の中間値を受信し且つそれについて一方向機能を実行して第二の中間値を生成するための一方向手段と；
第二の中間値と記憶した参照値との一致状態を検出し、且つ少なくとも1つの一致が検出し終わった時に有効信号を生成するための比較手段と；
を備えて成るものである。
標準セルはさらに、前記有効信号が生成されるまで機能ブロックへの、クロック信号のような、所要信号を遮断するための抑止手段を有してよく、あるいは、その抑止手段は機能ブロックそのものの回路中に作り込んでもよい。
【００１９】
それ故、本願発明は、複数の標準セルに関する構成データのライブラリを設定する処理と、集積回路デバイスの製造に際して少なくとも1つの前述のセルに関する構成データを選択・利用する処理とを包含する集積回路製造法を考察するものであり、該ライブラリは前出のパラグラフで説明した方式の標準セルに関する構成データを含む。
【００２０】
【実施例】
図1に図解方式で示した集積回路デバイス10（以後、"チップ"）は、機能ブロック12の動作の有効化を制御するロック回路機構11を有する（図1は、回路機構11と機能ブロック12とによって占められる相対的チップ面積を正確に表現しようとするものではない）。機能ブロック12は、例えば、外部供給データを圧縮／伸長するためのデータ圧縮エンジン、又はディスク駆動コントローラの部分であってよい。
【００２１】
機能ブロック12は、外部のチップ接点（明確に示されていない）を通して外部データ、アドレス及びコントロールライン13、14、15に接続する。同ブロック12は、その作動にロック回路機構11からのライン16で信号が供給されなければならないことを除けば、標準の方法で動作する。この実施例では、ライン16上の所要信号は、コントロールライン17に乗せてロック回路機構11のうちのゲート回路18へ送られる外部クロック信号である。ゲート回路がライン19上の有効信号を供給されると、外部クロック信号がブロック12へ渡されその動作を実行可能にし；ライン19に有効信号が無い場合、ブロック12は内部的に非動作である。
【００２２】
ロック回路機構11のロックを外してブロック12を実行可能にするには、前もって決めたパスワード（チップ・キー）をチップ10の外部からロック回路機構11へ供給しなければなら

ない。このチップ・キーの機密性を確保するために2つの特異な対策が講じられる。第一は、チップ・キーを暗号形式でチップ10に渡し、その暗号化チップ・キーがロック回路機構11で解読される。この目的で、同ロック回路機構は、直列入力及び出力ライン21、22にのせて外界と通信する保全通信ブロック20を有する。ブロック20は、例えば、周知のDiffie-Hellman Key Exchangeアルゴリズムを実行し（例えば、"Network and Internetwork Security", p.342, William Stallings, Prentice Hall International,1995参照）；一回限りの暗号キーでこの公開キー・アルゴリズムを作動させることにより、繰返し攻撃に耐える機密の方法でチップ・キーをチップ20へ渡すことができる。

【００２３】

保全通信ブロック20が暗号化チップ・キーを供給されると、そのチップ・キーを解読し且つ第一中間値IV1としてそのチップ・キーを一時的に出力する。

【００２４】

チップ・キーの機密性を確保するために講じられる第二の対策は、チップ・キーのコピーが入力チップ・キーに対する比較用としてそれだけではチップ10に記憶されない、ということである。その代わりに、関連チップの正しいチップ・キーの識別特性がロック回路機構のレジスタ25に記憶され、この識別特性はチップ・キーの明文形式を一方向機能にかけることによって作られる値である。この一方向機能は、例えば、Secure Hash Algorithm SHA（前述の参考文献"Network and Internetwork Security"の276頁参照）で実行されるような一方向ハッシュ機能である。その内容が読み取られて侵入者がレジスタ25へのアクセスに成功できたとしても、レジスタ25に保持されたその識別特性からチップ・キーを決定することが計算上実行できないであろう故、このことでチップ・キーが危うくなるということはないであろう。

【００２５】

入力チップ・キーが当該特定チップ10のロックを開けるのに適切なものであるかどうかを確認するために、ロック回路機構はさらに一方向機能ブロック26を有し、これにより、チップ・キーの出力が、レジスタ25に保持されるチップ・キーの識別特性を形成するために用いる一方向機能（この場合、SHA）にブロック20からのIV1として当てられる。

【００２６】

その後、ブロック26によって得られる中間値IV2は、比較ブロック27でレジスタ25に格納された識別特性と比較され；もし一致が見られれば、比較ブロック27は、機能ブロック12の動作有効化を生じさせるべくライン19上に有効信号を出力する。いったんこの信号が発生されると、適当なIV2の値が除かれても、チップが消勢される（又は他のある種の条件が達成される）まで、それが存在し続けるという意味において、比較ブロック27は有効信号をラッチする。

【００２７】

レジスタ25に保持されるチップ・キーの識別特性は、製造時に永久的に設定するか又は、本実施例におけるように、連続して書込んでよい（この場合のレジスタは、例えば、Flash（フラッシュ）又はEEPROMメモリである）。この後者の処理を制御するために、チップ10は、データライン14とレジスタ25との間に挿入される書込み制御回路28を備える。レジスタ25に書込むために、必要となるチップ・キーの識別特性値がデータライン14に置かれ且つ書込み許可（ライト・イネイブル）信号がライン29にのせて書込み制御回路28へ渡される。加えて、書込み制御回路28は、その内容が（チップ・キーの識別特性が未だ何ら書込まれていないことを示す）全てゼロであるかもしくはロック回路機構が（例えば、比較ブロック27からのライン30上の信号の存在によって示されるような）そのロックが開けられた状態にあるかの何れかである場合のみ、レジスタ25への書込みを許可するよう構成される。

【００２８】

必要とされるチップ・キーの識別特性がいったんレジスタ25に書込まれてしまうと、それ以後のレジスタへの書込みは、書込み制御回路28に可溶連結（ライン31上に適当な外部信号が印加されると飛ばされる連結）を設けることで妨げられる。

【００２９】
典型的には、明文形式のチップ・キーは1Kビットの長さを有してよい。
【００３０】
図1ではチップ10はロック回路機構11で制御されるただ1個の機能ブロックで示されているが、多数の該ブロックは典型的には各々異なった機能性を有するものとして設けてよい。そのような構成を5個の機能ブロック12A～12Eについて図2に示す。この場合、それぞれのゲート回路18は各機能ブロックと関連し、且つレジスタ25は、機能ブロックのうちの特定なものと関連した複数の異なったチップ・キーに対する識別特性を格納するレジスタブロック35と置き換えられる。図2では、これらの識別特性は、チップ・キーK1～K6のハッシュに対応して、それぞれH(K1)～H(K6)と呼ぶ。中間値IV2が与えられると、比較ブロック27は、今度は、レジスタブロック35に格納された識別特性H(K1)～H(K6)の中から一致するものを探索し、いったん一致状態を見つけると関連機能ブロックに関して適当な作用をする。
【００３１】
図2の実施例では、機能ブロック12A、12B、12Cに関して、単一の各識別特性H(K1)、H(K2)、H(K3)がレジスタブロック35に格納され、そして信号IV2がいったん対応する値をとると、比較ブロック27は適当な機能ブロックへ有効信号を出力する。ブロック12A、12B及び12Cの機能性は、それ故、入力チップ・キーに従って選択的に許可され、このため個々のユーザにとって異なった機能性が利用できることになる。
【００３２】
ブロック12Dの有効化は、ブロック12A、B、Cに対するより以上に必要とされる。この場合、信号IV2は、ブロック12Dに関して格納した識別特性H(K4)に対応する正確な値を持たなければならないばかりでなく、ブロック12Cも最初に許可されていなければならない。これは、ブロック12Dだけに関連したゲート回路18が比較ブロック27とブロック12Cとの両方からの有効信号を受信して後者（ブロック12D）を実行可能にすることによって達成され、後者はそれ自身許可された時にだけそのような信号を供給する。この一般的構成によって、階層的アクセス方式が実施できるようになり、それによって各レベルが対応するチップ・キーを持ち、且つユーザは、それに対して彼らが正確なチップ・キーを有する階層のレベルまでの機能ブロックを実行可能にできるだけである。
【００３３】
機能ブロック12Eの有効化には、2つの暗号化チップ・キーK5、K6を（多分、直接連続して）入力する必要があり、レジスタブロック35は両チップ・キーの対応する識別特性H(K5)、H(K6)を記憶する。この場合、比較ブロック27は、チップ・キーの最初の1つについての一致を確認するとき、この事実を覚えていて且つ二番目のチップ・キーの一致を検出してから機能ブロック12Eに関連したゲート回路18へ有効信号を出力しなければならない。
【００３４】
ブロック12A-C、ブロック12D、及びブロック12Eを実行可能にするための上述の別アプローチ法は、必要に応じて任意の組合せで用いてよい、ということは明らかになるであろう。また、チップ10は、無条件で使用できるブロックのような、ロック回路機構11によって制御されない1つ以上の機能ブロックを備えてよいことも明らかになるであろう。
【００３５】
図3は、電子組立体の3個のチップ10について2通りの配置を説明するものである。明確にするため、図3においては、各チップ10のロック回路機構11への入力接続のみが示されており、この接続は1本のラインで表されている（一般的には、保全通信処理には両方向通信が必要故、図1に示すように2本になる）。再度、明確にするため、各チップは、ロック回路機構11で制御されるただ1個の主機能ブロック12を有するものとして示されている。
【００３６】
図3(a)は、3個のチップ10全てがそれらの機能性のロックを開けるのに暗号化チップ・キーを供給される配列を示しており、各チップは同一のチップ・キーの識別特性を記憶している。この配列は、チップがそれぞれ重要な機能性を含んでいるが、該機能性について認

可されたユーザがそのような機能性全てへのアクセスを必要とし且つ電子組立体の機能性の選択的有効化に対する実施上の要求がない場合に適している。

【００３７】

図3(b)は、3個のチップ10全てがそれらの機能性のロックを開けるのに別々に制御される配列を示しており、各チップは異なったチップ・キーの識別特性を記憶している。そのような配列は、チップ群によって設定される機能が独立して使われ且つ異なったユーザに別々の使用許可を与える場合に適している。

【００３８】

別々のチップ・キーが別々のチップに渡されることになる場合、これは、予定してないチップへチップ・キーを渡してもそのチップのロックが開けられないことを単に意味する故、同一の通信ラインにわたって行ってよい、ということが分かるであろう。

【００３９】

本願発明について記述した実施例に対しては種々修正を施してよい。さらに、前文より明らかになるように、ロック回路機構11は種々の異なった機能を有するチップに設けることができる。従って、該ロック回路機構は、安全な機能性を有するチップを設計するのに有用なビルディング・ブロックと考えることができる。この目的のため、該ロック回路機構に関する組立データは、標準セルのライブラリに保持してよく、更にまた、必要に応じ、その全てが該ロック回路機構によって設定された保全特性を示す同一系列のチップ群の設計と製造に用いてよい。

【００４０】

以上、本発明の実施例について詳述したが、以下、本発明の各実施態様の例を示す。

【００４１】

[実施態様１]

デバイスに所定の機能性を与えるための機能ブロックと、デバイスの外部から少なくとも1つの所定の暗号形式のチップ・キーがロック回路機構に供給されるまで前記機能ブロックの動作を抑止する前記ロック回路機構とを有し、

該ロック回路機構が、

少なくとも1つの参照値を記憶するための記憶手段と、

前記デバイスの外部からの入力を受信し且つ該入力を暗号解読処理にかけて第一中間値を生成する保全通信手段であって、該暗号解読処理の特徴は、前記入力が暗号形式のようなキーである時、前記第一中間値が前記チップ・キーの明文形式に一致するようなものである保全通信手段と、

前記第一中間値を受信し且つそれについて一方向機能を実行して第二中間値を生成するための手段と、

第二中間値と前記少なくとも1つの参照値との一致状況を検出し、且つ前記少なくとも1つの一致が検出された時に有効信号を生成するための比較手段と、

前記有効信号が生成されるまで前記機能ブロックの動作を禁止する抑止手段と、

を備えて成り、

前記機能ブロックの本来の目的が、外部アイテムの制御及び／又は外部供給データの処理であることを特徴とする集積回路デバイス。

【００４２】

[実施態様２]

前記有効信号が生成されるまで前記抑止手段によって前記機能ブロックが内部的に失効にされることを特徴とする実施態様1記載の集積回路デバイス。

【００４３】

[実施態様３]

前記有効信号が生成されるまで前記抑止手段が作用して前記機能ブロックへの所要クロック信号を遮断することを特徴とする実施態様2記載の集積回路デバイス。

【００４４】

[実施態様４]

複数の集積回路デバイスがその中に組み込まれ、且つ少なくとも１つの前記デバイスが実施態様1に従う電子組立体。

【００４５】

[実施態様５]

前記記憶手段が前記機能ブロックに関して複数の前記参照値を記憶し、且つ前記比較手段が前記複数の参照値について前記一致を検出した後にだけ前記有効信号を生成することを特徴とする実施態様1記載のデバイス。

【００４６】

[実施態様６]

複数の前記機能ブロックが設けられ、且つ前記記憶手段が該各機能ブロックに関してそれぞれ前記参照値を記憶し、前記ロック回路機構が前記各機能ブロック用のそれぞれの前記抑止手段及び、前記第二中間値と前記参照値との間で一致を検出すると、その一致した参照値と関連した機能ブロックの抑止手段へ前記有効信号をもたらす比較手段を有することを特徴とする実施態様1記載のデバイス。

【００４７】

[実施態様７]

1つの前記機能ブロックの動作上の有効化が、対応する抑止手段による有効信号の受信と前記機能ブロックの別の1つの事前の有効化との両方を条件にすることを特徴とする実施態様6記載のデバイス。

【００４８】

[実施態様８]

前記機能ブロックによって設定される機能性が前記デバイス間で異なる実施態様1記載の同一系列の集積回路デバイス。

【００４９】

[実施態様９]

集積回路デバイスに組み込まれてそのデバイスの機能ブロックの動作の有効化を制御する標準セルであって、

少なくとも1つの参照値を記憶するための記憶手段と、

入力を受信し且つそれを暗号解読処理にかけて第一中間値を生成する保全通信手段と、

前記第一中間値を受信し且つそれについて一方向機能を実行して第二中間値を生成するための一方向手段と、

前記第二中間値と前記少なくとも1つの参照値との一致状態を検出し、且つ少なくとも1つの前記一致が検出された時に有効信号を生成するための比較手段と、

を備えて成る標準セル。

【００５０】

[実施態様１０]

さらに、前記有効信号が生成されるまで前記機能ブロックへの所要クロック信号を遮断するための抑止手段を有する実施態様9記載の標準セル。

【００５１】

[実施態様１１]

複数の標準セルについて組立データのライブラリを設定するステップと、集積回路デバイスの製造に際し少なくとも1つの該セルに関して前記組立データを選択し且つ利用するステップとを備えて成り、前記ライブラリが実施態様9又は実施態様10による標準セルについての組立データを有することを特徴とする集積回路の製造方法。

【００５２】

【発明の効果】

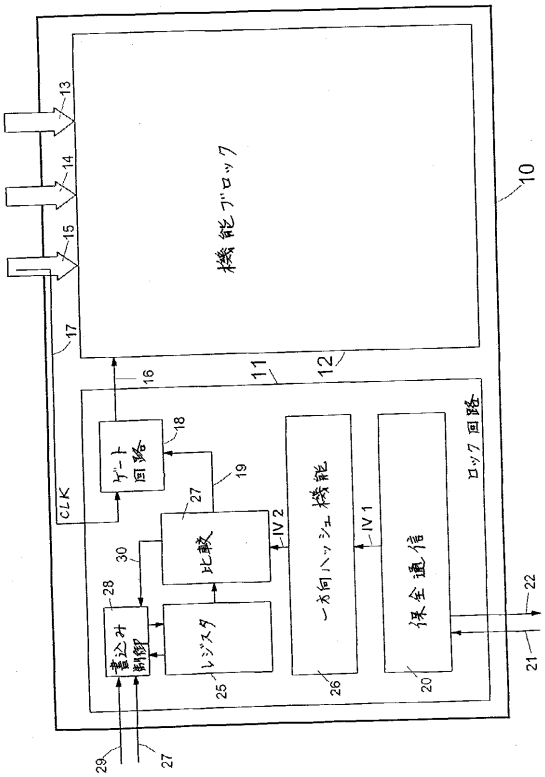
以上説明したように、本発明を用いることにより、特別の改ざん防止格納装置を使わなくてもよい機能用法制御を提供することができる。

【図面の簡単な説明】

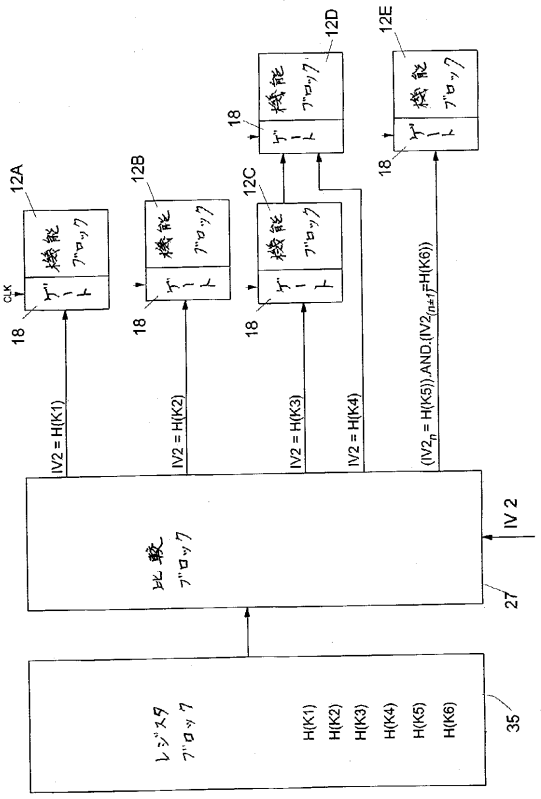
【図１】デバイスの機能ブロックの有効化を制御するためのロック回路機構を示す集積回

路デバイスのブロック図である。
【図２】同じ集積回路デバイスに設けられた種々の機能ブロックを実行可能にするための様々の構成を図解する線図である。
【図３ａ】ロック回路機構を設けた3個の集積回路デバイスの第一の構成を示す図である。
【図３ｂ】ロック回路機構を設けた3個の集積回路デバイスの第二の構成を示す図である。
【符号の説明】
１０：集積回路チップ
１１：ロック回路機構
１２：機能ブロック

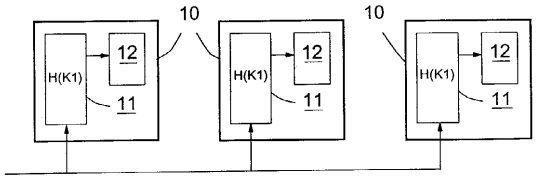
【図１】



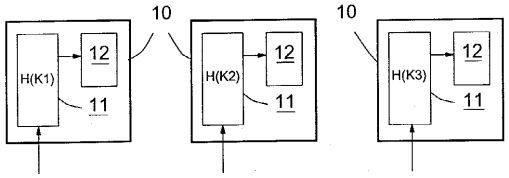
【図２】



【図３ａ】


10
10
12
H(K1)
11
12
H(K1)
11
12
H(K1)
11

【図３ｂ】


10
10
12
H(K1)
11
12
H(K2)
11
12
H(K3)
11

フロントページの続き

審査官　石川　正二

(56)参考文献　特開平０５－２０４４８６（ＪＰ，Ａ）
特開平０７－０５６７９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 12/14　320
G09C　1/00
H04L　9/10
H04L　9/32