

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 10 月 4 日(04.10.2012)



(10) 国際公開番号
WO 2012/132218 A1

- (51) 国際特許分類:
G06F 12/14 (2006.01)
- (21) 国際出願番号: PCT/JP2012/001284
- (22) 国際出願日: 2012 年 2 月 24 日(24.02.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2011-080479 2011 年 3 月 31 日(31.03.2011) JP
- (71) 出願人 (米国を除く全ての指定国について): ルネサスエレクトロニクス株式会社(Renesas Electronics Corporation) [JP/JP]; 〒2118668 神奈川県川崎市中原区下沼部 1 7 5 3 番地 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 金井 友明 (KANAI, Tomoaki) [JP/JP]; 〒2118668 神奈川県川崎市中原区下沼部 1 7 5 3 番地 ルネサスエレクトロニクス株式会社内 Kanagawa (JP).
- (74) 代理人: 家入 健(IEIRI, Takeshi); 〒2210835 神奈川県横浜市神奈川区鶴屋町三丁目 3 3 番 8 アサヒビルディング 10 階 響国際特許事務所 Kanagawa (JP).

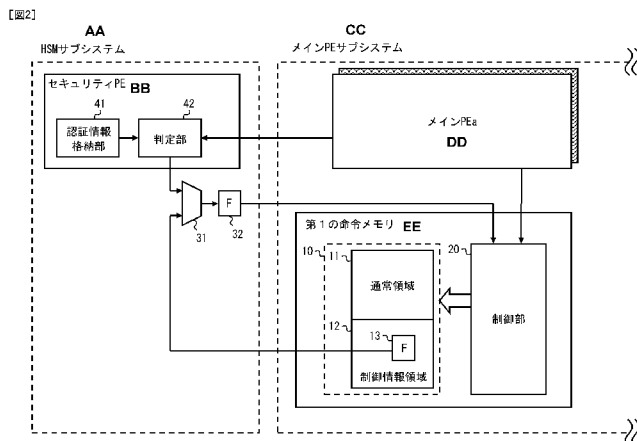
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ユーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告 (条約第 21 条(3))

(54) Title: PROCESSOR SYSTEM AND CONTROL METHOD THEREFOR

(54) 発明の名称: プロセッサシステム及びその制御方法



- 11 Normal area
12 Control information area
20 Control unit
41 Authentication information storage unit
42 Determination unit
AA HSM subsystem
BB Security PE
CC Main PE subsystem
DD Main PE
EE First command memory

(57) Abstract: This processor system is provided with: a storage unit (10); a control information area (12) for storing an access prohibit flag (13) which can be set to the prohibit side by switching from the permit side; a main PEa for issuing an access request and a copy register (32) rewrite request to the storage unit (10); a security PE for determining whether or not the copy register (32) rewrite request is authorized; the copy register (32) for storing a value corresponding to the permission if the access prohibit flag (13) is set to the permit side, or for storing a value corresponding to the determination result made by the security PE if the access prohibit flag (13) is set to the prohibit side; and an access control circuit (21) for either permitting or prohibiting access from the main PEa to the storage unit (10) on the basis of an output value from the copy register (32).

(57) 要約: 本発明にかかるプロセッサシステムは、記憶部 (10) と、許可側から禁止側に切り替えて設定可能なアクセス禁止フラグ (13) を格納する制御情報領域 (12) と、記憶部 (10) に対するアクセス要求と複写レジスタ (32) の書き換え要求とを発行するメインPEaと、複写レジスタ (32) の書き換え要求が正当であるか否かの判定を行うセキュリティPEと、アクセス禁止フラグ (13) が許可側に設定された場合に当該許可に応じた値を記憶し、アクセス禁止フラグ (13) が禁止側に設定された場合にセキュリティPEの判定結果

果に応じた値を記憶する複写レジスタ (32) と、複写レジスタ (32) の出力値に基づきメインPEaから記憶部 (10) に対するアクセスを許可するか否かを制御するアクセス制御回路 (21) と、を備える。

明 細 書

発明の名称： プロセッサシステム及びその制御方法

技術分野

[0001] 本発明は、プロセッサシステム及びその制御方法に関し、特にアクセス制御可能な半導体記憶回路を備えたプロセッサシステム及びその制御方法に関する。

背景技術

[0002] 特許文献 1 には、データの書き込みや消去に対するプロテクト機能を有する不揮発性の半導体記憶装置が開示されている。図 9 は、特許文献 1 が開示された不揮発性半導体記憶装置を示すブロック図である。図 9 に示すように、この不揮発性半導体記憶装置は、複数のメモリブロックから構成されるメモリセルアレイ 1、インタフェース 6、7、書き込み回路 2、3、4、5、8 及び読み出し回路 2、3、4、5、8 を備えている。上記メモリブロック中にはプロテクト・フラグが書き込まれている。上記書き込み回路は、上記インタフェースから書き込み命令が入力された場合に、プロテクト・フラグが第一の値になっている時は書き込み命令を履行し、第二の値になっている時は上記書き込み命令を履行しないことを特徴とする。

[0003] 特許文献 2 には、低コストで、コンピュータへの不正アクセス等の不正行為を防止することを目的としたプロセッサが開示されている。特許文献 2 が開示されたプロセッサは、演算手段と一体に形成され、第 1 メモリ認証用情報および第 2 メモリ認証用情報を保持するプロセッサ側メモリ認証用情報保持手段と、第 1 メモリから取得した第 1 メモリ認証用情報とプロセッサ側メモリ認証用情報保持手段が保持する第 1 メモリ認証用情報とを比較して第 1 メモリを認証し、さらに第 2 メモリから取得した第 2 メモリ認証用情報とプロセッサ側メモリ認証用情報保持手段が保持する第 2 メモリ認証用情報とを比較して第 2 メモリを認証するメモリ認証手段と、メモリ認証手段による認証結果に基づいて第 1 メモリおよび第 2 メモリへのアクセスを制御するアク

セス制御手段と、を備える。

先行技術文献

特許文献

[0004] 特許文献1：特開2005-108273号公報

特許文献2：特開2007-066201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に開示された不揮発性半導体記憶装置（半導体記憶回路）では、データの書き込みや消去を許可するか否かがプロテクト・フラグの値に応じて決定されている。しかし、特許文献1には、プロテクト・フラグ自体の書き換えの許可又は禁止をどのように制御するのかについて開示されていない。したがって、悪意のある第三者により、禁止側に設定されたプロテクト・フラグが許可側に書き換えられた後に、記憶されたデータが書き換えられ又は消去されてしまうという問題があった。

[0006] このような問題に対する解決策として、発明者は、プロテクト・フラグの書き込みを担うハードウェアの論理構成を、プロテクト・フラグを一度禁止側に設定すると二度と許可側に戻せない構成にすることを検討した。

[0007] しかし、この構成では、プロテクト・フラグを一度禁止側に設定すると、悪意のある第三者に限らず、不揮発性半導体記憶装置へのデータの書き込みや消去が不可能になってしまう。例えば、悪意のある第三者によるデータの書き込みや消去を防ぐためにメーカーがプロテクト・フラグを禁止側に設定すると、それ以降、メーカー自身もデータの書き込みや消去を行うことができなくなる。そのため、例えば、既に市場に出回っている不揮発性半導体記憶装置に記憶されたプログラムのアップデートを行うことができなくなる。このように、プロテクト・フラグを一度禁止側に設定すると二度と許可側に戻せない構成では、書き換え可能であるという不揮発性半導体記憶装置の利点が失われてしまう。

[0008] このように、関連する技術では、プロテクト・フラグによって半導体記憶回路へのアクセスが禁止されてしまうと、その後、当該半導体記憶回路へのアクセスを柔軟に制御できないという問題があった。

課題を解決するための手段

[0009] 本発明にかかるプロセッサシステムは、電氣的に書き換え可能な複数の不揮発性メモリセルにより構成される第1記憶部と、第1値から第2値に値を切り替え可能なアクセス禁止フラグを格納する第2記憶部と、前記第1記憶部に対するアクセス要求と、当該アクセス要求に対応する認証情報と、を発行する第1プロセッサと、前記第1プロセッサから発行された認証情報が正当であるか否かを判定する第2プロセッサと、前記アクセス禁止フラグの値が第1値の場合に当該第1値に応じた値を記憶し、前記アクセス禁止フラグの値が第2値の場合に第2プロセッサの判定結果に応じた値を記憶する複写レジスタと、前記複写レジスタに記憶された値に基づいて、前記第1プロセッサから前記第1記憶部に対するアクセスを許可するか否かを制御するアクセス制御回路と、を備える。

[0010] また、本発明にかかるプロセッサシステムの制御方法は、第1記憶部に対するアクセス要求と、当該アクセス要求に対応する認証情報と、を第1プロセッサから発行し、前記第1プロセッサから発行された認証情報が正当であるか否かの判定を第2プロセッサにより行い、第1値から第2値に値を切り替え可能なアクセス禁止フラグの値が第1値の場合に当該第1値に応じた値を複写レジスタに記憶し、前記アクセス禁止フラグの値が第2値の場合に第2プロセッサの判定結果に応じた値を複写レジスタに記憶し、前記複写レジスタに記憶された値に基づいて、前記第1プロセッサから前記第1記憶部に対するアクセスを許可するか否かを制御する。

[0011] 上述のような回路構成及び制御方法により、プロテクト・フラグによって半導体記憶回路へのアクセスが禁止された場合でも、その後の当該半導体記憶回路へのアクセスを柔軟に制御できる。

発明の効果

[0012] 本発明により、プロテクト・フラグによって半導体記憶回路へのアクセスが禁止された場合でも、その後の当該半導体記憶回路へのアクセスを柔軟に制御可能なプロセッサシステム及びその制御方法を提供することができる。

図面の簡単な説明

[0013] [図1]本発明が適用されるプロセッサシステムの概略図を示す。

[図2]本発明の実施の形態1にかかるプロセッサシステムの一部を示すブロック図である。

[図3A]本発明の実施の形態1にかかる制御部を示すブロック図である。

[図3B]本発明の実施の形態1にかかる制御部を示すブロック図である。

[図4]本発明の実施の形態1にかかるプロセッサシステムの動作を示すフローチャートである。

[図5]本発明の実施の形態1にかかるプロセッサシステムの動作を説明するための図である。

[図6]本発明の実施の形態1にかかるプロセッサシステムの変形例を示すブロック図である。

[図7]本発明の実施の形態2にかかるプロセッサシステムを示すブロック図である。

[図8A]本発明の実施の形態3にかかるプロセッサシステムを示すブロック図である。

[図8B]本発明の実施の形態3にかかるプロセッサシステムを示すブロック図である。

[図9]関連する技術の不揮発性半導体記憶装置を示すブロック図である。

発明を実施するための形態

[0014] 本発明の詳細な実施の形態を説明する前に、本発明が適用されるプロセッサシステム（情報処理装置）の概要について説明する。なお、本発明は、以下で説明するプロセッサシステムに適用されるものではあるが、説明するプロセッサシステムは一例であり、他のプロセッサシステムに本発明を適用することも可能である。

[0015] 本発明が適用されるプロセッサシステムの概略図を図1に示す。図1に示すように、本発明にかかるプロセッサシステムは、複数のPE (Processing Element) を用いることにより処理性能の向上を実現するものである。また、本発明にかかるプロセッサシステムでは、PEによる機能ブロックの分類とは別に3つのサブシステムによる機能の分類を行う。図1に示すように、本発明にかかるプロセッサシステムでは、メインPE (Processing Element) サブシステム、IO (Input Output) サブシステム、HSM (Hardware Security Module) サブシステムを有する。

[0016] メインPEサブシステムでは、予め内部に記憶されたプログラム又は外部から読み込んだプログラムに基づくプロセッサシステムに求められる具体的な処理を行う。IOサブシステムでは、メインPEサブシステム又はHSMサブシステムにより用いられる周辺装置が動作するための各種処理を行う。HSMサブシステムは、プロセッサシステムにおいて行われている処理のセキュリティ確認処理を行う。また、本発明にかかるプロセッサシステムでは、各サブシステムにクロック信号CLK a、CLK b、CLK c、CLK pが供給される。図1に示す例では、メインPEサブシステムにはクロック信号CLK aが供給され、IOサブシステムにはクロック信号CLK b、CLK pが供給され、HSMサブシステムにはクロック信号CLK cが供給される。これらのクロック信号CLK a、CLK b、CLK cは、システム全体構成の仕様に応じて、同一の周波数であっても、異なる周波数であっても良い。また、クロック信号CLK pは、周辺装置に与えられ、IOサブシステムに与えられるクロック信号CLK bとは非同期のクロック信号である。

[0017] 続いて、より具体的に各サブシステムについて説明する。メインPEサブシステムは、メインPE a (第1プロセッサ)、メインPE b、第1の命令メモリ (半導体記憶回路)、データメモリ、システムバスを有する。メインPEサブシステムでは、メインPE a、メインPE b、命令メモリ及びデータメモリは、システムバスを介して互いに接続される。第1の命令メモリは、プログラムを格納する。データメモリは、外部から読み込んだプログラム

及びプロセッサシステム内で処理されたデータを一時的に記憶する。メイン P E a 及びメイン P E b は、それぞれ命令メモリ、データメモリ等を利用しながらプログラムを実行する。なお、メイン P E a は、冗長動作が可能なように構成される。冗長動作とは、ソフトウェア的には一つのプロセッサエレメントとして動作するが、ハードウェアとしては多重化された構成又は検査回路等が付加された構成により高信頼な動作を行う動作である。冗長動作の一例として、クロック毎に多重化された回路の出力結果が同一であるか否かを比較するロックステップ動作がある。

[0018] I O サブシステムは、周辺バス、I O P E、周辺装置を有する。I O P E は、周辺装置を利用する上で必要な処理を行う。なお、I O P E はメイン P E システムの第 1 の命令メモリに記憶されているプログラムに基づき動作しても良く、他の記憶領域に記憶されているプログラムに基づき動作しても良い。周辺バスは、I O P E 及び周辺装置を互いに接続する。

[0019] 図 1 では、周辺装置として、C A N ユニット、F L E X R A Y ユニット、S P I ユニット、U A R T ユニット、A D C ユニット、W D ユニット、タイマを例示した。C A N ユニットは、自動車の車内通信規格の一つである C A N (Controller Area Network) に基づく通信を行う。F L E X R A Y ユニットは、自動車の車内通信規格の一つである Flex Ray 規格に基づく通信を行う。S P I ユニットは、3 線又は 4 線のシリアル通信である S P I (System Packet Interface) 規格の通信を行う。U A R T (Universal Asynchronous Receiver Transmitter) ユニットは、調歩同期方式によるシリアル信号をパラレル信号に変換し、また、その逆方向の変換を行う。A D C (Analog to Digital Converter) ユニットは、センサ等から与えられるアナログ信号をデジタル信号に変換する。W D (Watch Dog) ユニットは、所定の期間が経過したことを検出するウォッチドックタイマ機能を提供する。タイマは、時間の計測、波形生成などを行う。図 1 の例では、上記ユニットを周辺装置としたが、他の機能を有するユニットを含むことも可能であり、また、一部のユニットのみを有する場合も考えられる。

[0020] HSMサブシステムは、セキュリティPE（第2プロセッサ）と、第2の命令メモリとを有する。セキュリティPEは、システムバスに接続される。セキュリティPEは、メインPEサブシステムで実行されているプログラムの正当性又はプログラムを実行して得られるデータの正当性を判断する。第2の命令メモリには、プログラムを格納する。また、第2の命令メモリは、セキュリティPEのみがアクセスできるメモリである。第2の命令メモリは、第1の命令メモリと共に1つの記憶領域として設けられていても良いが、セキュリティPEのみがアクセス可能な領域としてアクセス制御されていることが必要である。

[0021] 上記説明の通り、本発明が適用されるプロセッサシステムでは、複数のPEにより処理能力を向上させながら、予期しない故障、予期しないプログラムの改変等の不具合に対して高い耐性を実現するものである。なお、ここまでで説明したプロセッサシステムは、本発明が適用されるプロセッサシステムの一例を示したものであり、例えば、命令メモリ及びデータメモリの配置及びシステム中の個数は、そのシステムのアーキテクチャにより種々考えられる。また、メモリと各プロセッサエレメントとの接続は、例えば、複数のバスを介して接続される構成であっても良く、バスを介さずにプロセッサエレメントと接続される構成であっても良く、アーキテクチャの設計により種々の構成が考えられ得る。

[0022] 上記したプロセッサシステムの説明は、本発明が適用されるプロセッサシステムの全体的な構成を説明するためのものである。しかし、本発明の実施の形態の説明では、上記のプロセッサシステムの説明において説明しなかった構成要素についても適宜追加する。また、追加した当該構成要素についての説明も加える。

[0023] 以下、図面を参照しつつ、本発明の実施の形態について説明する。なお、図面は簡略的なものであるから、この図面の記載を根拠として本発明の技術的範囲を狭く解釈してはならない。また、同一の要素には、同一の符号を付し、重複する説明は省略する。

[0024] 実施の形態 1

図 2 は、本発明の実施の形態 1 にかかるプロセッサシステムの具体的な構成例を示すブロック図である。本実施の形態にかかるプロセッサシステムは、アクセス禁止フラグ（プロテクト・フラグ）によって記憶部 10 へのアクセスが禁止された場合でも、その後の記憶部 10 へのアクセスを柔軟に制御できることを特徴とする。以下、詳細に説明する。

[0025] 図 2 に示すプロセッサシステムにおいて、第 1 の命令メモリは、記憶部（第 1 記憶部）10 と、制御部 20 と、を備える。第 1 の命令メモリは、電氣的に書き換え可能な複数の不揮発性メモリセルによって構成されている。したがって、電力供給が停止した場合であっても、第 1 の命令メモリに記憶されているデータは消去されずに保持される。不揮発性の半導体メモリとしては、例えば、EEPROM やフラッシュ・メモリ等がある。

[0026] （記憶部 10）

記憶部 10 は、プログラムが格納される通常領域 11 と、アクセス禁止フラグ 13 が格納される制御情報領域（第 2 記憶部）12 と、を有する。なお、本実施の形態では、通常領域 11 と制御情報領域 12 とが一つの半導体メモリに構成された場合を例に説明しているが、これに限られない。通常領域 11 と制御情報領域 12 とが物理的に異なる半導体メモリにそれぞれ構成されても良い。したがって、例えば、通常領域 11 と制御情報領域 12 のうち一方の領域が第 1 の命令メモリに設けられ、他方の領域が第 1 の命令メモリとは異なるメモリに設けられても良い。

[0027] 制御情報領域 12 には、記憶部 10 に対するプログラムの書き込み、読み出し及び消去を許可するか禁止するかを設定するアクセス禁止フラグ 13 が格納される。アクセス禁止フラグ 13 が禁止側に設定されている場合、記憶部 10 に対するプログラムの書き込み、読み出し及び消去は禁止される。一方、アクセス禁止フラグ 13 が許可側に設定されている場合、記憶部 10 に対するプログラムの書き込み、読み出し及び消去は許可される。ここで、アクセス禁止フラグ 13 は、一度禁止側に設定されると二度と許可側に戻せな

いように制御情報領域 12 上に形成されている。以下では、アクセス禁止フラグ 13 が L レベル（第 2 値）の場合に禁止側に設定され、アクセス禁止フラグ 13 が H レベル（第 1 値）の場合に許可側に設定される場合を例に説明する。

[0028] （制御部 20）

図 3 A は、制御部 20 の詳細な回路構成を示すブロック図である。図 3 A に示すように、制御部 20 は、アクセス制御回路 21 と、リセット処理回路 22 と、リセット生成回路 23 と、を有する。また、アクセス制御回路 21 は、メモリコントローラ 211 と、ゲーティング回路 212 と、を有する。なお、本実施の形態では、ゲーティング回路 212 がビット毎に設けられた論理積回路（AND 回路）である場合を例に説明する。

[0029] アクセス制御回路 21 は、メイン P E a（第 1 プロセッサ）から発行された記憶部 10 に対するプログラムの書き込み、読み出し及び消去のいずれかの要求を受け取ると、後述するアクセス禁止フラグ複写レジスタ 32 の出力値に基づいて、当該要求に応じた処理を記憶部 10 に対して実行するか否かを制御する。以下、具体的に説明する。

[0030] ゲーティング回路 212 は、アクセス禁止フラグ複写レジスタ 32 の出力値に基づいて、メイン P E a（第 1 プロセッサ）から発行された記憶部 10 に対するプログラムの書き込み、読み出し及び消去のいずれかの要求をメモリコントローラ 211 に対して出力するか否かを制御する。

[0031] 例えば、アクセス禁止フラグ複写レジスタ 32 の出力値が許可側の値（例えば、H レベル）の場合、ゲーティング回路 212 は、メイン P E a から発行された記憶部 10 に対するアクセス要求を、後段のメモリコントローラ 211 に対してそのまま出力する。一方、アクセス禁止フラグ複写レジスタ 32 の出力値が禁止側の値（例えば、L レベル）の場合、ゲーティング回路 212 は、メイン P E a から発行された記憶部 10 に対するアクセス要求を出力しない。このとき、ゲーティング回路 212 は、例えば L レベルの固定信号をメモリコントローラ 211 に対して出力する。

- [0032] アクセス禁止フラグ複写レジスタ 32 の出力値が許可側の値である場合、メモリコントローラ 211 にはメイン P E a から発行された記憶部 10 に対するアクセス要求が伝達される。メモリコントローラ 211 は、メイン P E a から発行された記憶部 10 に対するアクセス要求に基づいて、ライトイネーブル信号 W E N、アドレス信号 A D D 及びデータ信号 D A T A を生成する。なお、データ信号 D A T A は、書き込み時に生成されるものであり、プログラムの一部を構成する。
- [0033] ここで、プログラムの読み出し時には、アドレス信号 A D D によって指定された通常領域 11 のメモリセルに記憶されたデータが読み出され、プログラムの書き込み時には、アドレス信号 A D D によって指定された通常領域 11 のメモリセルに対してデータ信号 D A T A が書き込まれる。なお、プログラムの書き込み、読み出し及び消去は、ライトイネーブル信号 W E N によって切り替えられる。このように、アクセス禁止フラグ複写レジスタ 32 の出力値が許可側の値である場合、アクセス制御回路 21 は、メイン P E a からの要求に応じた処理を実行する。
- [0034] 一方、アクセス禁止フラグ複写レジスタ 32 の出力値が禁止側の値である場合、メモリコントローラ 211 にはメイン P E a から発行された記憶部 10 に対するアクセス要求が伝達されない。そのため、メモリコントローラ 211 は、メイン P E a から発行された記憶部 10 に対するアクセス要求に応じた処理を実行しない。このように、アクセス禁止フラグ複写レジスタ 32 の出力値が禁止側の値である場合、アクセス制御回路 21 は、メイン P E a からの要求に応じた処理を実行しない。
- [0035] なお、本実施の形態では、メモリコントローラ 211 がライトイネーブル信号 W E N、アドレス信号 A D D 及びデータ信号 D A T A を出力する場合を例に説明しているが、これに限られない。メモリコントローラ 211 は、記憶部 10 の仕様に応じた信号を出力する回路構成に適宜変更可能である。例えば、メモリコントローラ 211 は、チップイネーブル信号 C E N 等の他の信号をさらに出力する回路構成に適宜変更可能である。

[0036] また、アクセス制御回路 21 は、図 3 A に示す構成のものに限定されない。例えば、アクセス制御回路 21 は、一例として、図 3 B に示す構成のものに適宜変更可能である。以下、図 3 B に示すアクセス制御回路 21 の構成及び動作について説明する。

[0037] 図 3 B において、アクセス制御回路 21 は、メモリコントローラ 211 と、ゲーティング回路 212-1 ~ 212-3 と、を有する。本実施の形態では、ゲーティング回路 212-1 ~ 212-3 がビット毎に設けられた論理積回路（AND 回路）である場合を例に説明する。

[0038] アクセス制御回路 21 は、メイン P E a（第 1 プロセッサ）から発行された記憶部 10 に対するプログラムの書き込み、読み出し及び消去のいずれかの要求を受け取ると、後述するアクセス禁止フラグ複写レジスタ 32 の出力値に基づいて、当該要求に応じた処理を記憶部 10 に対して実行するか否かを制御する。

[0039] より具体的には、アクセス制御回路 21 において、メモリコントローラ 211 は、メイン P E a から発行された記憶部 10 に対するプログラムの書き込み、読み出し及び消去のいずれかの要求に基づいて、ライトイネーブル信号 W E N、アドレス信号 A D D 及びデータ信号 D A T A を生成する。なお、データ信号 D A T A は、書き込み時に生成されるものであり、プログラムの一部を構成する。ゲーティング回路 212-1 ~ 212-3 は、アクセス禁止フラグ複写レジスタ 32 の出力値に基づいて、メモリコントローラ 211 によって生成されたライトイネーブル信号 W E N、アドレス信号 A D D 及びデータ信号 D A T A を記憶部 10 に対して出力するか否かを制御する。

[0040] 例えば、アクセス禁止フラグ複写レジスタ 32 の出力値が許可側の値（例えば、H レベル）の場合、ゲーティング回路 212-1 ~ 212-3 は、メモリコントローラ 211 からのライトイネーブル信号 W E N、アドレス信号 A D D 及びデータ信号 D A T A を記憶部 10 に対してそのまま出力する。ここで、プログラムの読み出し時には、アドレス信号 A D D によって指定された通常領域 11 のメモリセルに記憶されたデータが読み出され、プログラム

の書き込み時には、アドレス信号ADDによって指定された通常領域11のメモリセルに対してデータ信号DATAが書き込まれる。なお、プログラムの書き込み、読み出し及び消去は、ライトイネーブル信号WENによって切り替えられる。このように、アクセス禁止フラグ複写レジスタ32の出力値が許可側の値の場合、アクセス制御回路21は、メインPEaからの要求に応じた処理を実行する。

[0041] 一方、アクセス禁止フラグ複写レジスタ32の出力値が禁止側の値（例えば、Lレベル）の場合、ゲーティング回路212-1～212-3は、メモリコントローラ211からのライトイネーブル信号WEN、アドレス信号ADD及びデータ信号DATAを記憶部10に対して出力しない。このとき、ゲーティング回路212-1～212-3は、例えば何れもLレベルの固定信号を記憶部10に対して出力する。このように、アクセス禁止フラグ複写レジスタ32の出力値がLレベルの場合、アクセス制御回路21は、メインPEaからの要求に応じた処理を実行しない。

[0042] 図3Aに戻り、リセット生成回路23は、リセット信号RSTを生成する回路である。リセット生成回路23は、外部から供給されるリセット信号に基づいて当該リセット信号RSTを生成する回路構成であっても良いし、電源が起動したことに応じて当該リセット信号RSTを生成する、いわゆるパワーオンリセットの回路構成であっても良い。なお、本実施の形態では、リセット生成回路23が制御部20に備えられた場合を例に説明しているが、これに限られない。例えば、リセット生成回路23が図1に示すプロセッサシステムの外部に設けられていても良い。

[0043] リセット処理回路22は、リセット信号RSTによる初期化後に当該リセット信号が解除されたことを検知すると、アクセス禁止フラグ13の値をアクセス禁止フラグ複写レジスタ32（図3Aにおいて不図示）に転送する。それにより、アクセス禁止フラグ複写レジスタ32の値は、アクセス禁止フラグ13の値に書き換えられる。

[0044] 図2に戻り、メインPEaは、制御部20内に対して「記憶部10に対す

るプログラムの書き込み、読み出し及び消去のいずれかの要求」を発行する。さらに、HSMサブシステムに設けられたセキュリティPEに対して「アクセス禁止フラグ複写レジスタ32の書き換えの要求」を発行する。なお、「アクセス禁止フラグ複写レジスタ32の書き換えの要求」には認証情報が含まれている。

[0045] セキュリティPEは、「アクセス禁止フラグ複写レジスタ32の書き換えの要求」が正当であるか否かの判定を行う。言い換えると、セキュリティPEは、「アクセス禁止フラグ複写レジスタ32の書き換えの要求」に含まれる認証情報が正当であるか否かの判定を行う。

[0046] セキュリティPEは、例えば、予め所定の認証情報が格納されている認証情報格納部41と、認証情報格納部41に格納されている認証情報とメインPEaからの要求に含まれる認証情報と、を比較して当該要求が正当であるか否かを判定する判定部42と、を有する。判定部42は、例えば、これら認証情報が一致する場合にメインPEaからの要求が正当であると判定し、不一致の場合に不当であると判定する。なお、セキュリティPEは、図2に示す構成のものに限定されない。セキュリティPEは、メインPEaから発行された「アクセス禁止フラグ複写レジスタ32の書き換えの要求」が正当であるか否かを判定可能な構成に適宜変更可能である。

[0047] また、HSMサブシステムは、セキュリティPEに加え、セクタ回路31及びアクセス禁止フラグ複写レジスタ32をさらに備える。セクタ回路31及びアクセス禁止フラグ複写レジスタ32は、第2の命令メモリ（図2において不図示）とは異なる回路として設けられている。

[0048] セキュリティPEは、メインPEaから発行された「アクセス禁止フラグ複写レジスタ32の書き換えの要求」を受け取ると、まず、当該要求が正当なものであるか否かの判定を行う。具体的には、セキュリティPEにおいて、判定部42は、メインPEaから発行された「アクセス禁止フラグ複写レジスタ32の書き換えの要求」に含まれる認証情報と、認証情報格納部41に格納されている認証情報と、を比較して当該要求が正当なものであるか否

かを判定する。判定部42は、当該要求が正当なものであると判定した場合、当該要求に応じた固定信号をセクタ回路31の一方の入力端子に対して出力する。なお、セクタ回路31の他方の入力端子には、リセット信号RST解除時にアクセス禁止フラグ13の値が入力される。

[0049] セクタ回路31は、セキュリティPEから出力された固定信号と、リセット信号RST解除後のアクセス禁止フラグ13の値と、を選択的にアクセス禁止フラグ複写レジスタ32に対して出力する。より具体的には、セクタ回路31は、「アクセス禁止フラグ複写レジスタ32の書き換えの要求」がセキュリティPEにより正当なものであると判断された場合、セキュリティPEからの固定信号（Hレベル）を選択して出力する。また、セクタ回路31は、リセット信号RSTが解除された場合、制御情報領域12に格納されたアクセス禁止フラグ13の値を選択して出力する。それにより、アクセス禁止フラグ複写レジスタ32の値は書き換えられる。つまり、アクセス禁止フラグ複写レジスタ32の値は、リセット信号RST解除時には、アクセス禁止フラグ13の値に書き換えられ、それ以外の場合には、セキュリティPEからの固定信号によってのみ書き換えられる。

[0050] 例えば、メインPEaは、記憶部10に対するアクセス要求を発行する場合、同時に、アクセス禁止フラグ複写レジスタ32の値を禁止側から許可側（LレベルからHレベル）に書き換えるようにセキュリティPEに対して要求する。セキュリティPEは、当該要求が正当であるものと判定した場合、所定の固定信号（Hレベル）を出力する。そのため、アクセス禁止フラグ複写レジスタ32の値は禁止側から許可側（LレベルからHレベル）に書き換えられる。それにより、アクセス制御回路21は、上述のように、メインPEaからの要求に応じた処理を実行することができる。なお、アクセス禁止フラグ13が許可側に設定されている場合には、当然にアクセス禁止フラグ複写レジスタ32も許可側に設定されている。そのため、メインPEaは、アクセス禁止フラグ複写レジスタ32の書き換え要求が正当であるか否かに関わらず、記憶部10に対してアクセスすることが可能である。

[0051] 記憶部 10 に対するプログラムの書き込み、読み出し及び消去のいずれかが完了すると、メイン P E a は、アクセス禁止フラグ複写レジスタ 32 の値を許可側から禁止側（H レベルから L レベル）に書き換えるようにセキュリティ P E に対して要求する。このとき、セキュリティ P E は、所定の固定信号（L レベル）を出力する。そのため、アクセス禁止フラグ複写レジスタ 32 の値は許可側から禁止側（H レベルから L レベル）に書き換えられる。それにより、アクセス制御回路 21 は、メイン P E a からの要求に関わらず、記憶部 10 に対するプログラムの書き込み、読み出し及び消去を禁止する。

[0052] なお、アクセス禁止フラグ複写レジスタ 32 の値は、何らかの理由で禁止側（L レベル）に書き換えられなかった場合でも、リセット信号 R S T 解除時に、既に禁止側に設定されているアクセス禁止フラグ 13 の値が転送されることにより禁止側（L レベル）に書き換えられる。それにより、より確実に記憶部 10 へのアクセスを禁止することができるため、不正アクセスを防止することができる。

[0053] （フローチャート）

次に、本実施の形態にかかるプロセッサシステムの動作を、図 4 及び図 5 を用いて説明する。図 4 は、図 2 に示すプロセッサシステムの動作を示すフローチャートである。図 5 は、図 2 に示すプロセッサシステムの動作の流れを説明するための図である。

[0054] まず、製品出荷時等の初期状態では、アクセス禁止フラグ 13 は許可側に設定され、アクセス禁止フラグ複写レジスタ 32 も許可側に設定されている（図 4 のステップ S 100）。つまり、製品出荷時では、記憶部 10 に対してプログラムの書き込み等が可能である。

[0055] 記憶部 10 に対するプログラムの書き込み等が完了した後、アクセス禁止フラグ 13 は禁止側に設定される（図 4 のステップ S 101）。

[0056] その後、リセット信号 R S T が解除されると（図 4 のステップ S 102）、アクセス禁止フラグ 13 の値がアクセス禁止フラグ複写レジスタ 32 に転送される（図 4 のステップ S 103、図 5 の F 1）。それにより、アクセス

禁止フラグ複写レジスタ 32 は禁止側に書き換えられる。その結果、記憶部 10 に対するプログラムの書き込み等はできなくなる。

[0057] その後、記憶部 10 に対してプログラムの書き込み等を行いたい場合、メイン P E a は、アクセス禁止フラグ複写レジスタ 32 を禁止側から許可側に書き換えるようにセキュリティ P E に対して要求する（図 4 のステップ S 104、図 5 の F 2）。

[0058] セキュリティ P E は、メイン P E a から発行された「アクセス禁止フラグ複写レジスタ 32 の書き換えの要求」を受け取ると、まず、当該要求が正当なものであるか否かの判定を行う（図 4 のステップ S 105）。セキュリティ P E は、当該要求が正当なものであると判定した場合（図 4 のステップ S 105 の Y E S）、当該要求に応じた固定信号（例えば H レベル）を出力する。それにより、アクセス禁止フラグ複写レジスタ 32 は禁止側から許可側に書き換えられる（図 4 のステップ S 106、図 5 の F 3）。その結果、記憶部 10 に対するプログラムの書き込み等が一時的に可能になる。

[0059] なお、セキュリティ P E によりメイン P E a からの要求が不当なものであると判定された場合（図 4 のステップ S 105 の N O）、アクセス禁止フラグ複写レジスタ 32 の書き換えは行われない（図 4 のステップ S 111）。つまり、アクセス禁止フラグ複写レジスタ 32 は禁止側に設定されたままとなる。そのため、記憶部 10 に対してプログラムの書き込み等はできない。

[0060] メイン P E a からの要求（図 5 の F 4）に応じて記憶部 10 に対するプログラムの書き込み等が完了すると、メイン P E a は、アクセス禁止フラグ複写レジスタ 32 を許可側から禁止側に書き換えるようにセキュリティ P E に対して要求する（図 4 のステップ S 107）。このとき、セキュリティ P E は、固定信号（例えば L レベル）を出力する。それにより、アクセス禁止フラグ複写レジスタ 32 は許可側から禁止側に書き換えられる（図 4 のステップ S 108）。その結果、記憶部 10 に対してプログラムの書き込み等はできなくなる。

[0061] その後、リセット信号 R S T により初期化されると（ステップ S 109）

、既に禁止側に設定されているアクセス禁止フラグ13の値がアクセス禁止フラグ複写レジスタ32に転送される（図4のステップS110、図5のF5）。それにより、アクセス禁止フラグ複写レジスタ32は許可側から禁止側に書き換えられる。つまり、アクセス禁止フラグ複写レジスタ32は、何らかの理由で禁止側に書き換えられなかった場合でも、より確実に禁止側に書き換えられる。

[0062] このように、本実施の形態にかかるプロセッサシステムは、記憶部10へのアクセス要求とともに発行される認証情報の正当性を判定するセキュリティPEと、アクセス禁止フラグ13が禁止側に設定されている場合にセキュリティPEの判定結果に応じた固定値を記憶するアクセス禁止フラグ複写レジスタ32と、アクセス禁止フラグ複写レジスタ32の出力値に基づきメインPEaから記憶部10へのアクセスを許可するか否かを制御するアクセス制御回路21と、を備える。それにより、本実施の形態にかかるプロセッサシステムは、アクセス禁止フラグ13によって記憶部10へのアクセスが禁止された場合でも、認証情報を知る者によってアクセス禁止フラグ複写レジスタ32を書き換えることにより記憶部10へのアクセスが可能である。つまり、本実施の形態にかかるプロセッサシステムは、アクセス禁止フラグ13によって記憶部10へのアクセスが禁止された場合でも、その後の記憶部10へのアクセスを柔軟に制御可能である。

[0063] そのため、例えば、記憶部10に格納されているプログラムを悪意の第三者から保護するためにアクセス禁止フラグ13を禁止側に設定した後でも、認証情報を知るメーカ等は、アクセス禁止フラグ複写レジスタ32を書き換えることにより記憶部10へアクセスすることができる。したがって、市場におけるプログラムのアップデートに対応することが可能である。

[0064] さらに、本実施の形態にかかるプロセッサシステムでは、メインPEaとは異なるセキュリティPEによって認証情報の正当性が判定されている。そのため、本実施の形態にかかるプロセッサシステムは、メインPEaの脆弱性の影響を受けることなく高いセキュリティレベルを維持した状態で、当該認

証情報の正当性（複写レジスタの書き換え要求の正当性）を判定することができる。つまり、高いセキュリティレベルを維持した状態でアクセス禁止フラグ複写レジスタ 32 の書き換えを行うことができる。

[0065] さらに、本実施の形態にかかるプロセッサシステムでは、リセット信号 RST 解除時にアクセス禁止フラグ 13 の値がアクセス禁止フラグ複写レジスタ 32 に転送される。そのため、アクセス禁止フラグ複写レジスタ 32 は、メイン P E a からの要求により許可側に設定された場合でも、リセット信号 RST による初期化のたびに確実に禁止側に設定される。そのため、記憶部 10 へのアクセス可能期間を一定期間に制限とすることができ、不正アクセスを防止することができる。

[0066] なお、アクセス禁止フラグ 13 が許可側に設定されている場合には、当然にアクセス禁止フラグ複写レジスタ 32 も許可側に設定されているため、認証情報の正当性の判定を要することなく、記憶部 10 へのアクセスが可能である。つまり、アクセス禁止フラグ 13 が許可側に設定されている場合には、認証情報の正当性の判定に時間をかけることなく、記憶部 10 へのアクセスが可能である。

[0067] なお、本実施の形態では、セクタ回路 31 が設けられた場合を例に説明したが、これに限られない。例えば、図 6 に示すように、セクタ回路 31 部分をソフトウェアで実現しても構わない。

[0068] 実施の形態 2

図 7 は、本発明の実施の形態 2 にかかるプロセッサシステムを示すブロック図である。本実施の形態にかかるプロセッサシステムは、実施の形態 1 にかかるプロセッサシステムと比較して、制御情報領域 12 a に複数のアクセス禁止フラグ 13-1 ~ 13-3 を備え、HSM サブシステム内に複数のセクタ回路 31-1 ~ 31-3 及び複数のアクセス禁止フラグ複写レジスタ 32-1 ~ 32-3 を備える。

[0069] アクセス禁止フラグ 13-1 は、通常領域 11 に対するプログラムの書き込み、読み出し及び消去を許可するか否かを設定するフラグである。アクセ

ス禁止フラグ１３－２は、制御情報領域１２ aに対するプログラムの書き込み、読み出し及び消去を許可するか否かを設定するフラグである。アクセス禁止フラグ１３－３は、他のメモリ（不図示）に対するプログラムの書き込み、読み出し及び消去を許可するか否かを設定するフラグである。

[0070] アクセス禁止フラグ複写レジスタ３２－１～３２－３及び複数のセレクト回路３１－１～３１－３は、それぞれアクセス禁止フラグ１３－１～１３－３に対応して設けられている。それぞれの動作は、実施の形態１にて説明したアクセス禁止フラグ複写レジスタ３２及びセレクト回路３１の動作と同様であるため、説明を省略する。

[0071] このように、本実施の形態にかかるプロセッサシステムは、複数のアクセス禁止フラグ及び対応する複数のアクセス禁止フラグ複写レジスタを備えることにより、記憶領域ごとに個別にアクセス制御することが可能となる。

[0072] なお、本実施の形態では、アクセス禁止フラグ及びアクセス禁止フラグ複写レジスタがそれぞれ３個ずつ設けられた場合を例に説明したが、これに限られず、アクセス制御対象となる記憶領域の数に応じて任意の個数に変更することが可能である。

[0073] 実施の形態３

図８ Aは、本発明の実施の形態３にかかるプロセッサシステムを示すブロック図である。本実施の形態にかかるプロセッサシステムは、実施の形態１にかかるプロセッサシステムと比較して、制御情報領域１２ bにロック・フラグ１４をさらに備え、アクセス制御回路２１ bにゲーティング回路２１３をさらに備える。なお、本実施の形態では、ゲーティング回路２１３がビット毎に設けられた論理積回路（AND回路）である場合を例に説明する。

[0074] ロック・フラグ１４は、記憶部１０ bに対するプログラムの書き込み、読み出し及び消去を永久に禁止するか否かを設定するフラグである。ロック・フラグ１４が禁止側に設定されている場合、アクセス禁止フラグ複写レジスタ３２の出力値に関わらず、記憶部１０ bに対するプログラムの書き込み、読み出し及び消去は禁止される。一方、ロック・フラグ１４が許可側に設定

されている場合、記憶部 10b に対するプログラムの書き込み、読み出し及び消去が許可されるか否かは、アクセス禁止フラグ複写レジスタ 32 の出力値に依存する。つまり、ロック・フラグ 14 が許可側に設定されている場合、本実施の形態にかかるプロセッサシステムは、実施の形態 1 の場合と同様の動作を示す。

[0075] ここで、ロック・フラグ 14 は、一度禁止側に設定されると二度と許可側に戻せないように制御情報領域 12b 上に形成されている。したがって、ロック・フラグ 14 が禁止側に設定された場合、記憶部 10b に対するプログラムの書き込み、読み出し及び消去は永久に禁止されることとなる。

[0076] より具体的には、アクセス制御回路 21b において、ゲーティング回路 213 は、ロック・フラグ 14 の値に基づいて、ゲーティング回路 212 の出力信号をメモリコントローラ 211 に対して出力するか否かを制御する。以下では、アクセス禁止フラグ 13 が L レベルの場合に禁止側に設定され、アクセス禁止フラグ 13 が H レベルの場合に許可側に設定される場合を例に説明する。

[0077] 例えば、ロック・フラグ 14 の値が許可側（H レベル）の場合、ゲーティング回路 213 は、ゲーティング回路 212 の出力信号をそのままメモリコントローラ 211 に対して出力する。つまり、ロック・フラグ 14 の値が許可側（H レベル）の場合、アクセス制御回路 21b は、図 3A に示すアクセス制御回路 21 の場合と同様の動作を示す。

[0078] 一方、ロック・フラグ 14 の値が禁止側（L レベル）の場合、ゲーティング回路 213 は、ゲーティング回路 212 の出力信号をメモリコントローラ 211 に対して出力しない。このとき、ゲーティング回路 213 は、例えば L レベルの固定信号をメモリコントローラ 211 に対して出力する。このように、ロック・フラグ 14 の値が禁止側（L レベル）の場合、アクセス制御回路 21b は、アクセス禁止フラグ複写レジスタ 32 の出力値に関わらず、メイン P E a からの要求に応じた処理を実行しない。

[0079] このように、本実施の形態にかかるプロセッサシステムは、実施の形態 1

と同様の効果を奏することができることに加え、記憶部 10 へのアクセスを完全に禁止することができるため、不正アクセスの防止効果をさらに向上させることができる。

[0080] なお、アクセス制御回路 21b は、図 8A に示す構成のものに限定されない。例えば、アクセス制御回路 21b は、一例として、図 8B に示す構成のものに適宜変更可能である。以下、図 8B に示すアクセス制御回路 21b の構成及び動作について説明する。

[0081] 図 8B に示すアクセス制御回路 21b は、図 3B に示すアクセス制御回路 21 と比較して、ゲーティング回路 213-1 ~ 213-3 をさらに備える。なお、本実施の形態では、ゲーティング回路 213-1 ~ 213-3 がビット毎に設けられた論理積回路（AND 回路）である場合を例に説明する。

[0082] より具体的には、アクセス制御回路 21b において、ゲーティング回路 213-1 ~ 213-3 は、ロック・フラグ 14 の値に基づいて、それぞれゲーティング回路 212-1 ~ 212-3 の出力信号を記憶部 10b に対して出力するか否かを制御する。以下では、アクセス禁止フラグ 13 が L レベルの場合に禁止側に設定され、アクセス禁止フラグ 13 が H レベルの場合に許可側に設定される場合を例に説明する。

[0083] 例えば、ロック・フラグ 14 の値が許可側（H レベル）の場合、ゲーティング回路 213-1 ~ 213-3 は、ゲーティング回路 212-1 ~ 212-3 の出力信号をそのまま記憶部 10b に対して出力する。つまり、ロック・フラグ 14 の値が許可側（H レベル）の場合、アクセス制御回路 21b は、図 3B に示すアクセス制御回路 21 の場合と同様の動作を示す。

[0084] 一方、ロック・フラグ 14 の値が禁止側（L レベル）の場合、ゲーティング回路 213-1 ~ 213-3 は、ゲーティング回路 212-1 ~ 212-3 の出力信号を記憶部 10b に対して出力しない。このとき、ゲーティング回路 213-1 ~ 213-3 は、例えば何れも L レベルの固定信号を記憶部 10b に対して出力する。このように、ロック・フラグ 14 の値が L レベルの場合、アクセス制御回路 21b は、アクセス禁止フラグ複写レジスタ 32

の出力値に関わらず、メインPE aからの要求に応じた処理を実行しない。

[0085] なお、本発明は上記実施の形態1～3に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。上記実施の形態1～3では、プログラムの書き込み、読み出し及び消去の何れの要求に対してもアクセス制御可能な場合を例に説明したが、これに限られない。プログラムの書き込み、読み出し及び消去のうち少なくとも何れか一つの要求に対してアクセス制御可能な回路構成に適宜変更可能である。

[0086] また、上記実施の形態1～3では、ゲーティング回路212-1～212-1, 213-1～213-3がビット毎に設けられた論理積回路（AND回路）である場合を例に説明したが、これに限られず、同様の効果を得られる回路構成に適宜変更可能である。したがって、ゲーティング回路は、例えば、ラッチ回路及び論理積回路により構成される一般的な回路構成のものであっても良い。

[0087] また、上記実施の形態1～3では、アクセス禁止フラグ13の値及びアクセス禁止フラグ複写レジスタ32の出力値が1ビットである場合を例に説明したが、これに限られない。アクセス禁止フラグ13の値及びアクセス禁止フラグ複写レジスタ32の出力値は、それぞれ複数ビットで構成されるものであっても良い。あるいは、複数のアクセス禁止フラグ13が設けられ、これら複数のアクセス禁止フラグ13の値のうち多数を占める値によってアクセスの許可及び禁止が決定される構成であっても良い。同様に、複数のアクセス禁止フラグ複写レジスタ32が設けられ、これら複数のアクセス禁止フラグ複写レジスタ32の出力値のうち多数を占める値によって記憶部10に対するアクセスの許可及び禁止が決定される構成であってもよい。即ち、アクセス禁止フラグ13及びアクセス禁止フラグ複写レジスタ32が多重化された構成であっても良い。

[0088] なお、上記実施の形態1～3で説明したように、アクセス禁止フラグ13は一度禁止側に設定されると二度と許可側に戻せない。これは、たとえ認証システムを備えていたとしてもセキュリティの根幹をなすような制御情報領

域 1 2 を自由に変更できるのは好ましくないからである。また、通常領域 1 1 と制御情報領域 1 2 とが一体となっておりシングルポートでアクセス可能な構成となっている場合には、アクセス禁止フラグ 1 3 の値の読み出しと通常領域 1 1 に対するアクセスとを同時に行うことができないため、アクセス禁止フラグ 1 3 の値を別途記憶しているアクセス禁止フラグ複写レジスタ 3 2 を書き換える方が効率的だからである。

[0089] この出願は、2011年3月31日に提出された日本出願特願2011-080479を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

- [0090] 10, 10a, 10b 記憶部
- 11 通常領域
- 12, 12a, 12b 制御情報領域
- 13 アクセス禁止フラグ
- 13-1~13-3 アクセス禁止フラグ
- 14 ロック・フラグ
- 20, 20b 制御部
- 21, 21b アクセス制御回路
- 22 リセット処理回路
- 23 リセット生成回路
- 31 セレクタ回路
- 31-1~31-3 セレクタ回路
- 32 アクセス禁止フラグ複写レジスタ
- 32-1~32-3 アクセス禁止フラグ複写レジスタ
- 41 認証情報格納部
- 42 判定部
- 211 メモリコントローラ
- 212 ゲーティング回路

2 1 2 - 1 ~ 2 1 2 - 3 ゲーティング回路

2 1 3 ゲーティング回路

2 1 3 - 1 ~ 2 1 3 - 3 ゲーティング回路

請求の範囲

- [請求項1] 電氣的に書き換え可能な複数の不揮発性メモリセルにより構成される第1記憶部と、
第1値から第2値に値を切り替え可能なアクセス禁止フラグを格納する第2記憶部と、
前記第1記憶部に対するアクセス要求と、当該アクセス要求に対応する認証情報と、を発行する第1プロセッサと、
前記第1プロセッサから発行された認証情報が正当であるか否かを判定する第2プロセッサと、
前記アクセス禁止フラグの値が第1値の場合に当該第1値に応じた値を記憶し、前記アクセス禁止フラグの値が第2値の場合に第2プロセッサの判定結果に応じた値を記憶する複写レジスタと、
前記複写レジスタに記憶された値に基づいて、前記第1プロセッサから前記第1記憶部に対するアクセスを許可するか否かを制御するアクセス制御回路と、を備えたプロセッサシステム。
- [請求項2] 前記アクセス制御回路は、
前記複写レジスタに記憶された値が第1値に対応する値の場合に前記第1記憶部に対するアクセスを許可し、前記複写レジスタに記憶された値が第2値に対応する値の場合に前記第1記憶部に対するアクセスを禁止することを特徴とする請求項1に記載のプロセッサシステム。
- [請求項3] 前記アクセス禁止フラグは、
第2値から第1値に切り替えられないように前記第2記憶部に格納されていることを特徴とする請求項1又は2に記載のプロセッサシステム。
- [請求項4] 前記第2プロセッサは、
所定の認証情報が格納された認証情報格納部と、
前記認証情報格納部に格納された認証情報と、前記第1プロセッサ

から発行された認証情報と、を比較し前記判定結果を出力する判定部と、を有する請求項 1 ～ 3 のいずれか一項に記載のプロセッサシステム。

[請求項5] 複数の前記第 1 記憶部と、
 複数の前記アクセス禁止フラグを格納する前記第 2 記憶部と、
 前記複数のアクセス禁止フラグに対応する複数の前記複写レジスタと、を備え、
 前記アクセス制御回路は、
 各複写レジスタに記憶された値に基づいて、前記第 1 プロセッサから対応する第 1 記憶部に対するアクセスを許可するか否かを制御することを特徴とする請求項 1 ～ 4 のいずれか一項に記載のプロセッサシステム。

[請求項6] 前記第 2 記憶部は、
 第 1 値から第 2 値に値を切り替え可能なロック・フラグをさらに格納し、
 前記アクセス制御回路は、
 前記複写レジスタに記憶された値及び前記ロック・フラグの値に基づいて、前記第 1 プロセッサから前記第 1 記憶部に対するアクセスを許可するか否かを制御することを特徴とする請求 1 ～ 5 の何れか一項に記載のプロセッサシステム。

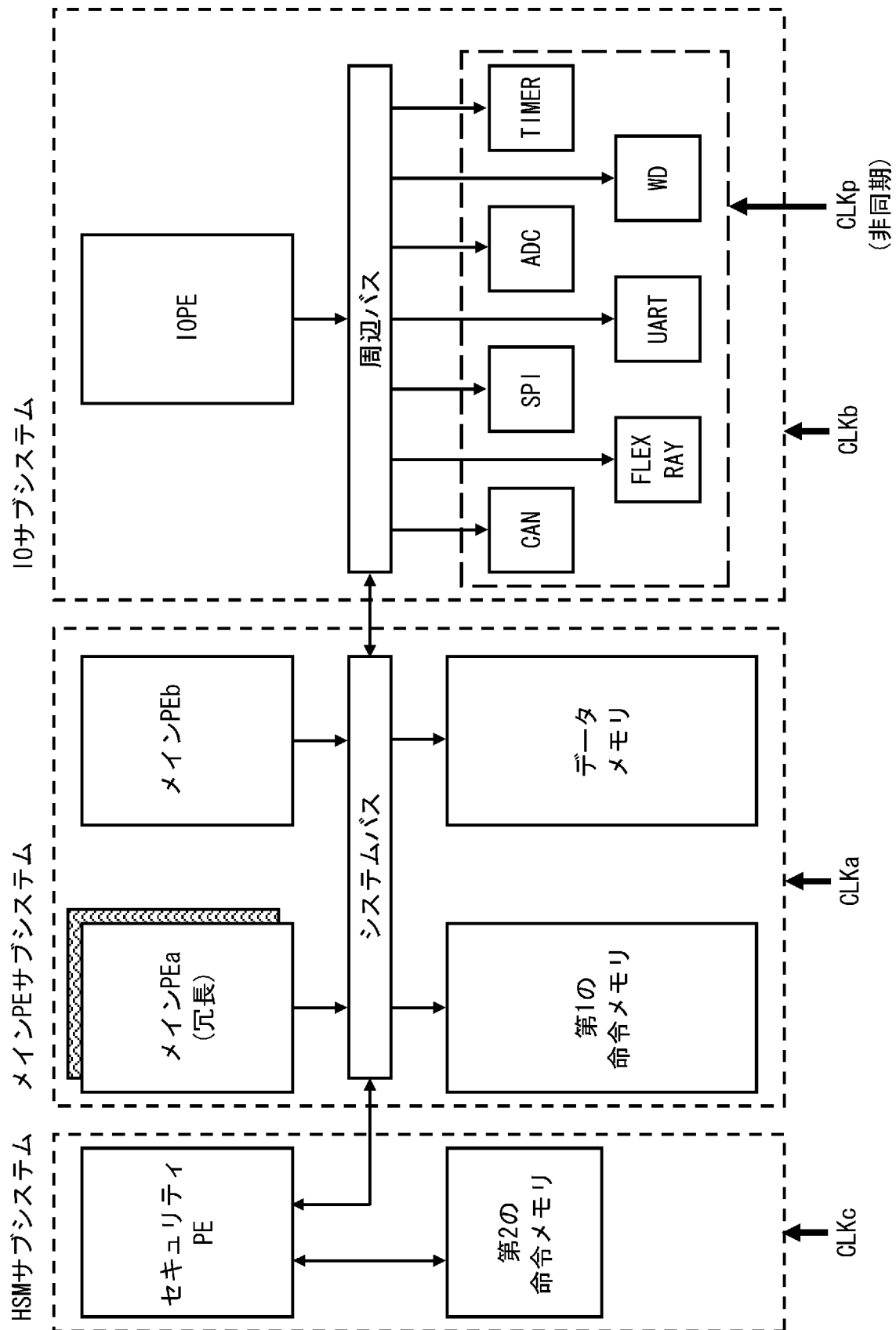
[請求項7] 前記アクセス制御回路は、
 前記ロック・フラグの値が第 2 値に対応する値の場合には、前記複写レジスタに記憶された値に関わらず前記第 1 記憶部に対するアクセスを禁止することを特徴とする請求項 6 に記載のプロセッサシステム。

[請求項8] 前記ロック・フラグは、
 第 2 値から第 1 値に切り替えられないように前記第 2 記憶部に格納されていることを特徴とする請求項 6 又は 7 に記載のプロセッサシス

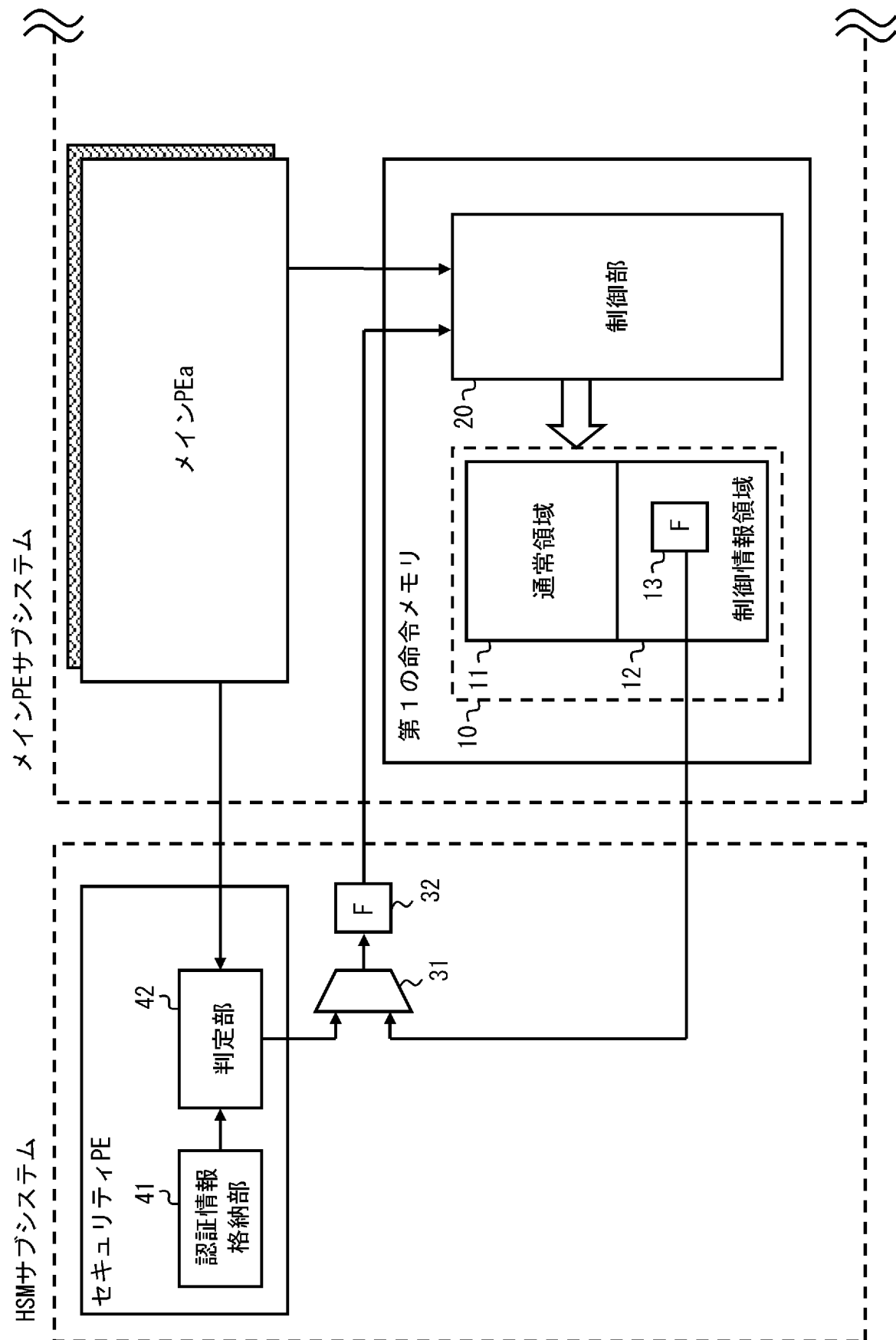
テム。

- [請求項9] 前記第2記憶部は、前記第1記憶部内に形成されていることを特徴とする請求項1～8のいずれか一項に記載のプロセッサシステム。
- [請求項10] リセット信号により初期化された場合には、前記判定結果に関わらず前記アクセス禁止フラグの値を前記複写レジスタに記憶させるリセット処理回路、をさらに備えた請求項1～9のいずれか一項に記載のプロセッサシステム。
- [請求項11] 前記リセット信号は、外部から供給されることを特徴とする請求項10に記載のプロセッサシステム。
- [請求項12] 前記リセット信号は、パワーオンリセット信号であることを特徴とする請求項10に記載のプロセッサシステム。
- [請求項13] 第1記憶部に対するアクセス要求と、当該アクセス要求に対応する認証情報と、を第1プロセッサから発行し、
前記第1プロセッサから発行された認証情報が正当であるか否かの判定を第2プロセッサにより行い、
第1値から第2値に値を切り替え可能なアクセス禁止フラグの値が第1値の場合に当該第1値に応じた値を複写レジスタに記憶し、
前記アクセス禁止フラグの値が第2値の場合に第2プロセッサの判定結果に応じた値を複写レジスタに記憶し、
前記複写レジスタに記憶された値に基づいて、前記第1プロセッサから前記第1記憶部に対するアクセスを許可するか否かを制御する、
プロセッサシステムの制御方法。
- [請求項14] 前記複写レジスタに記憶された値が第1値に対応する値の場合に前記第1記憶部に対するアクセスを許可し、前記複写レジスタに記憶された値が第2値に対応する値の場合に前記第1記憶部に対するアクセスを禁止することを特徴とする請求項13に記載のプロセッサシステムの制御方法。

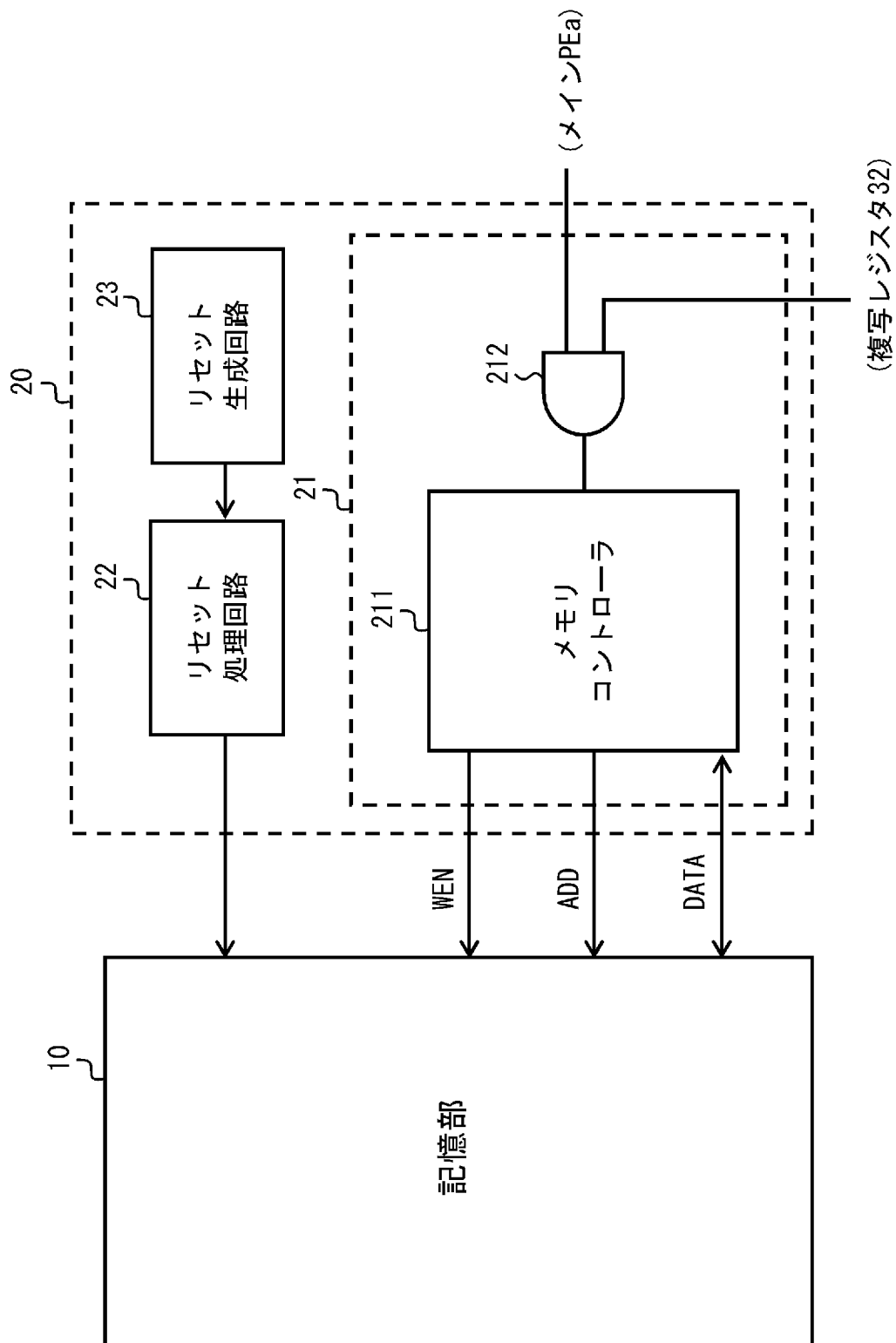
[図1]

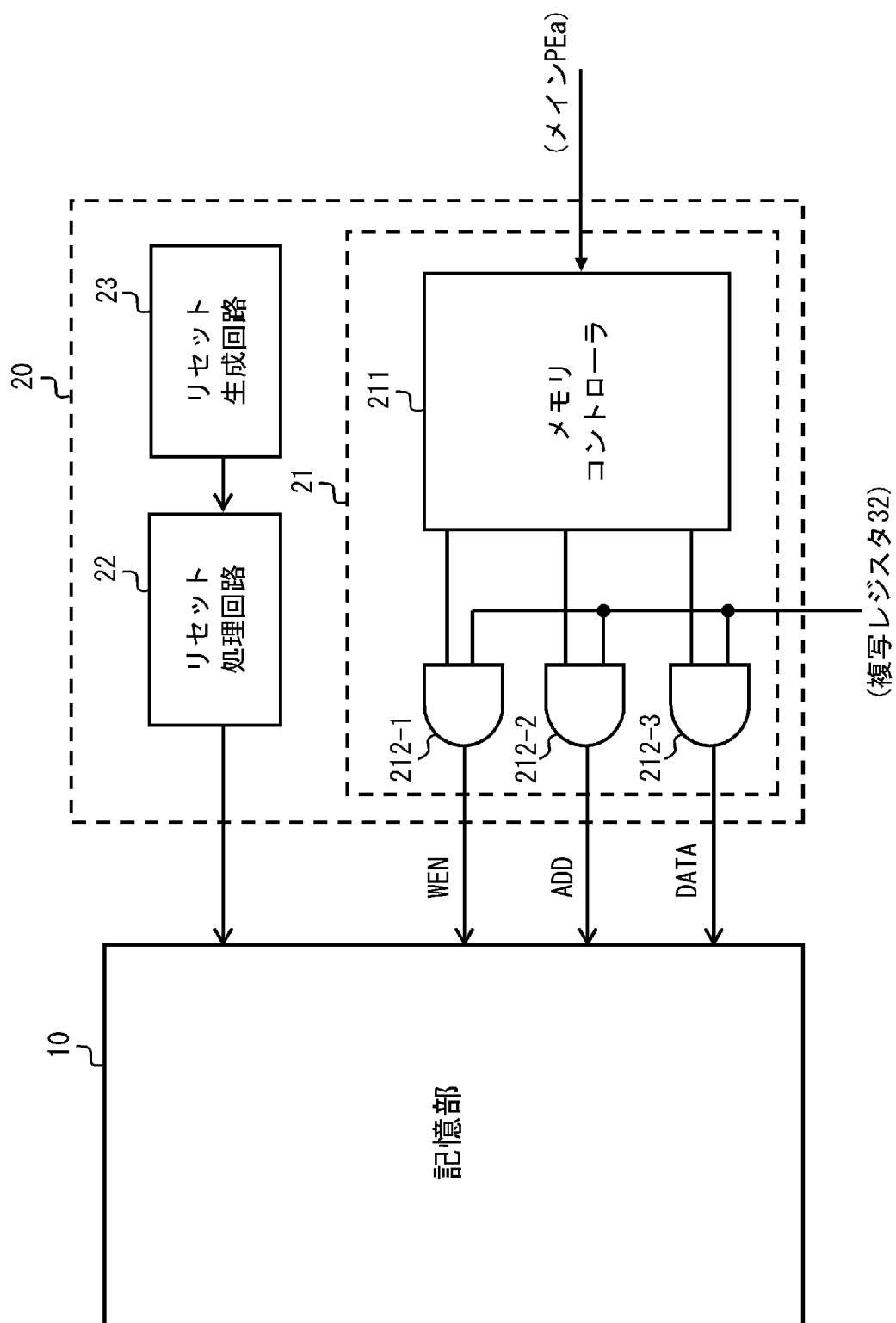


[図2]

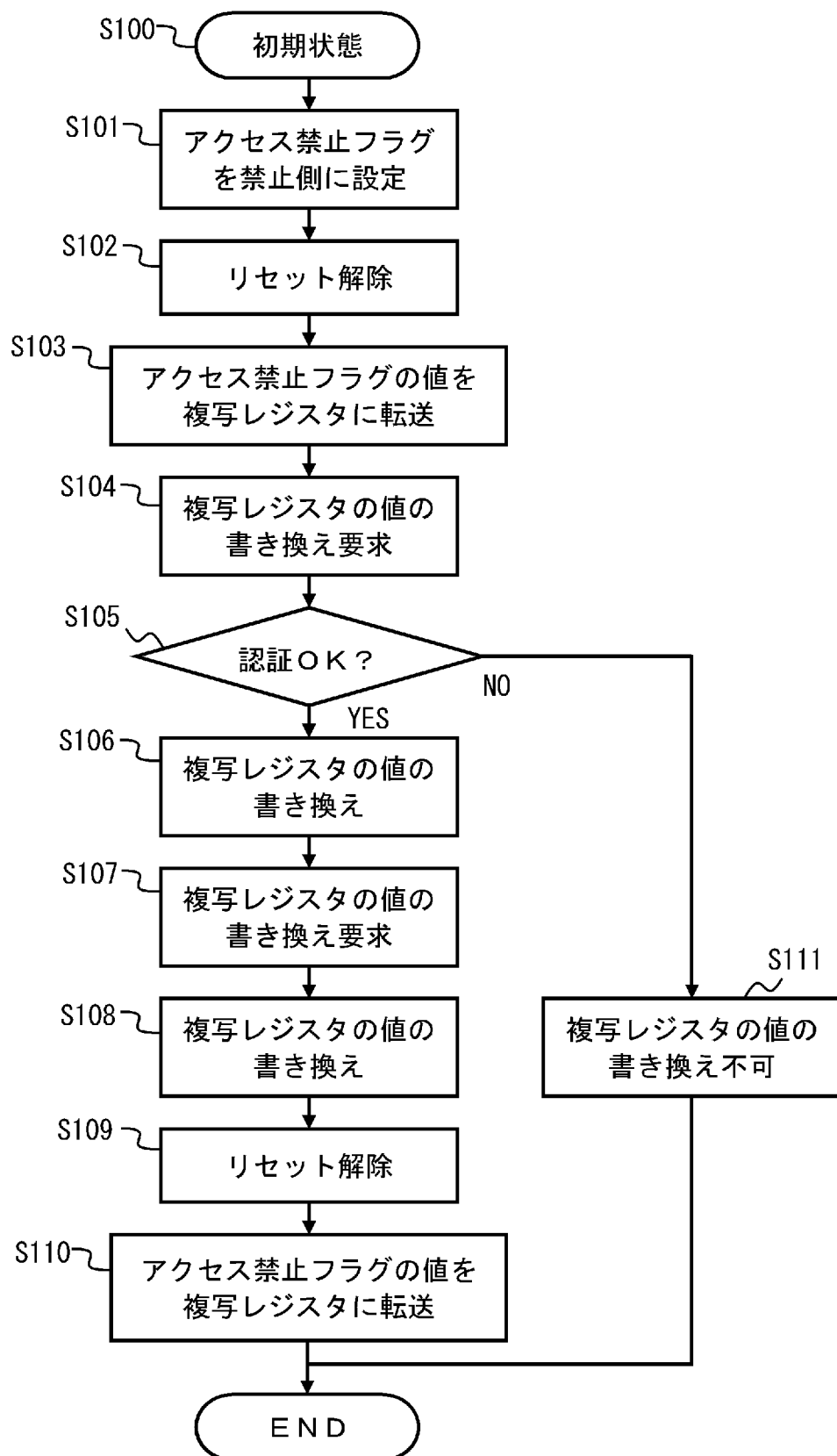


[図3A]

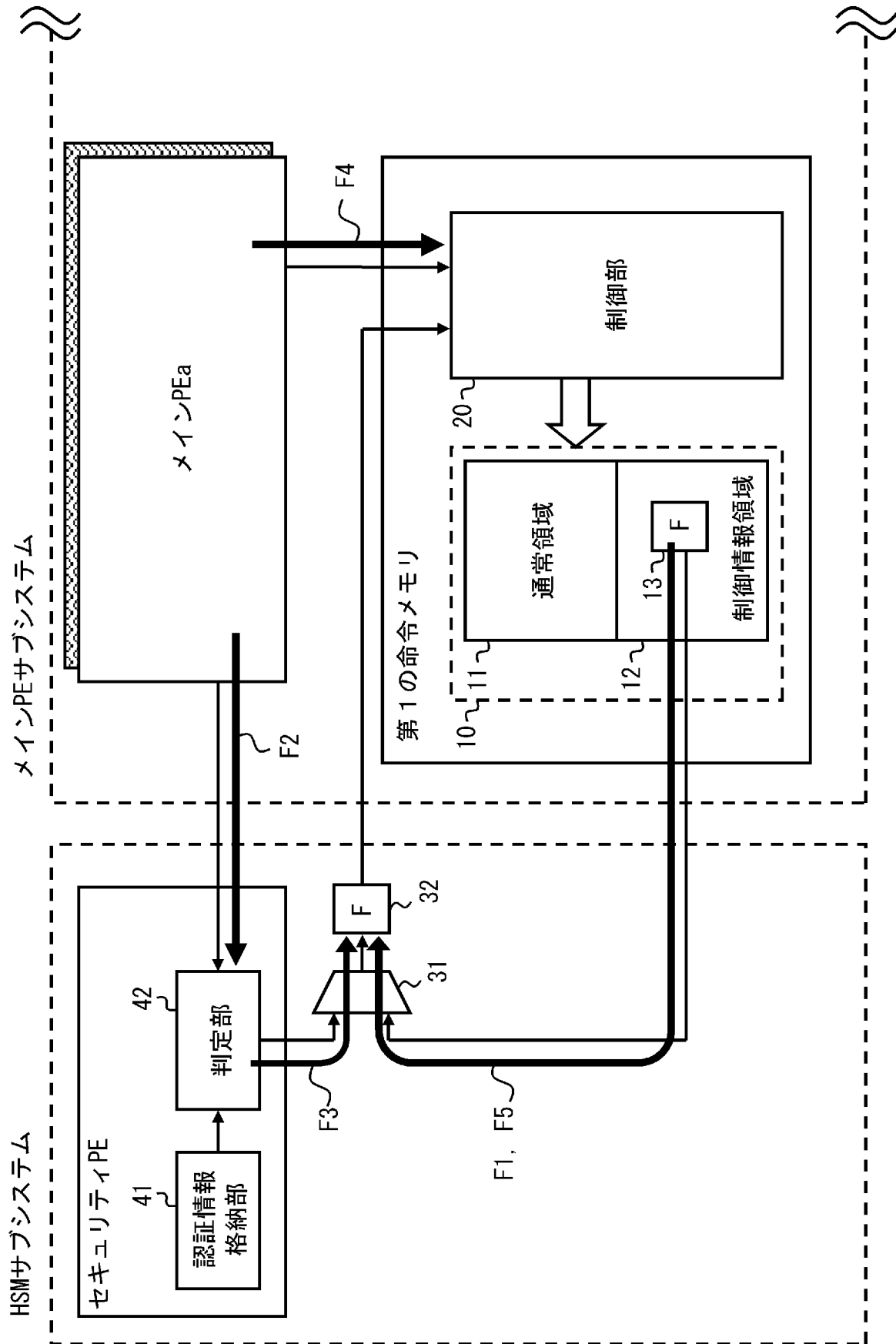




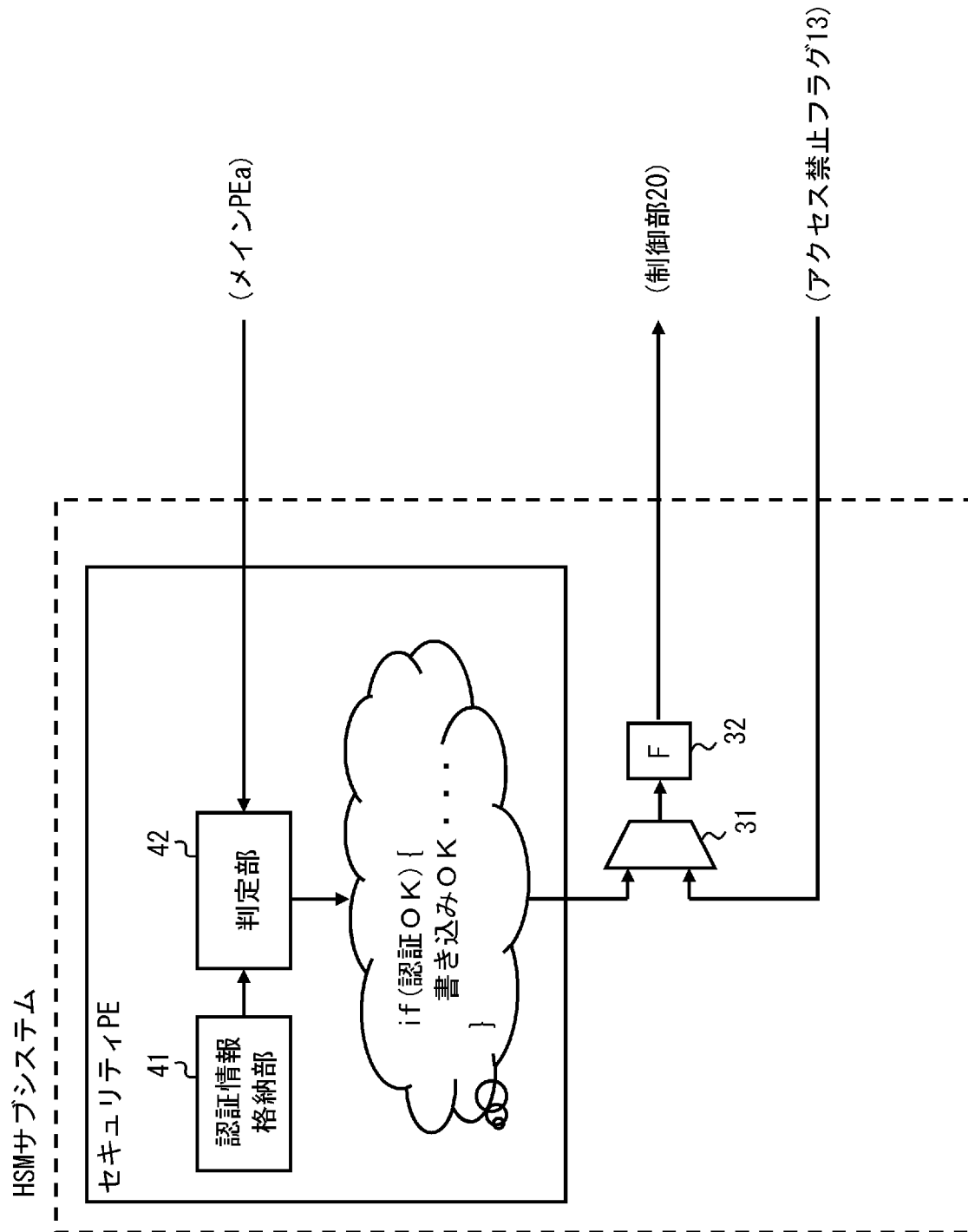
[図4]



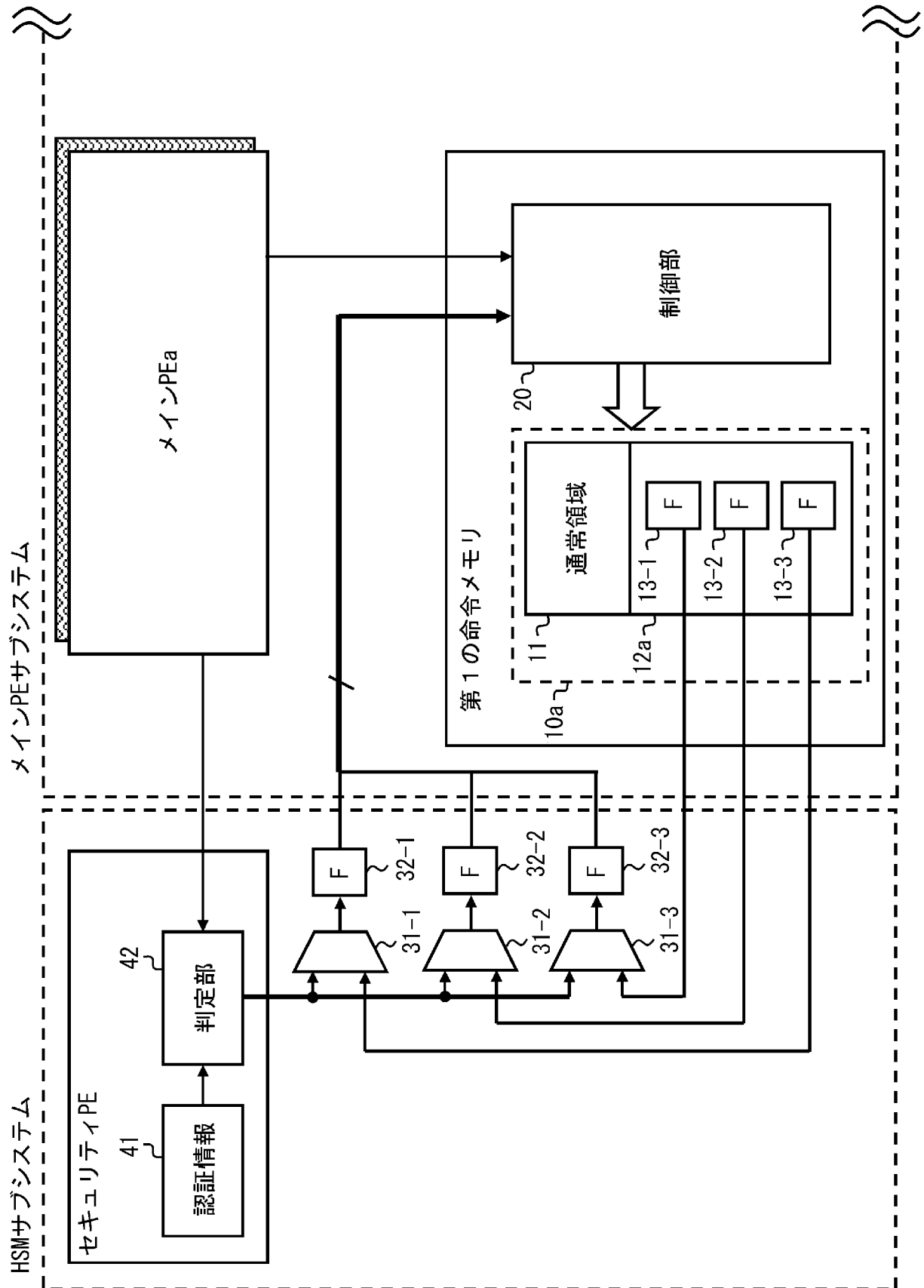
[図5]



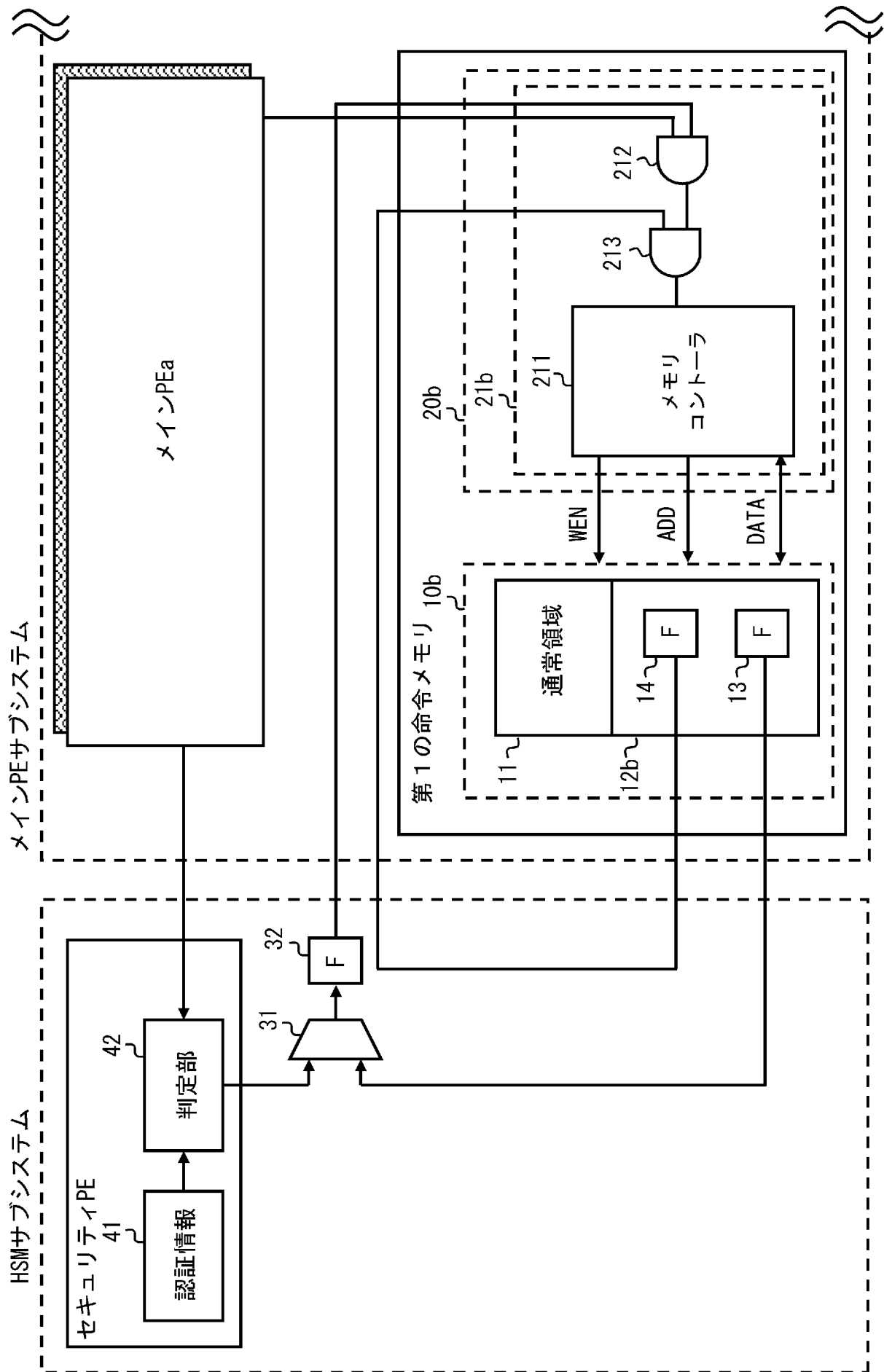
[図6]



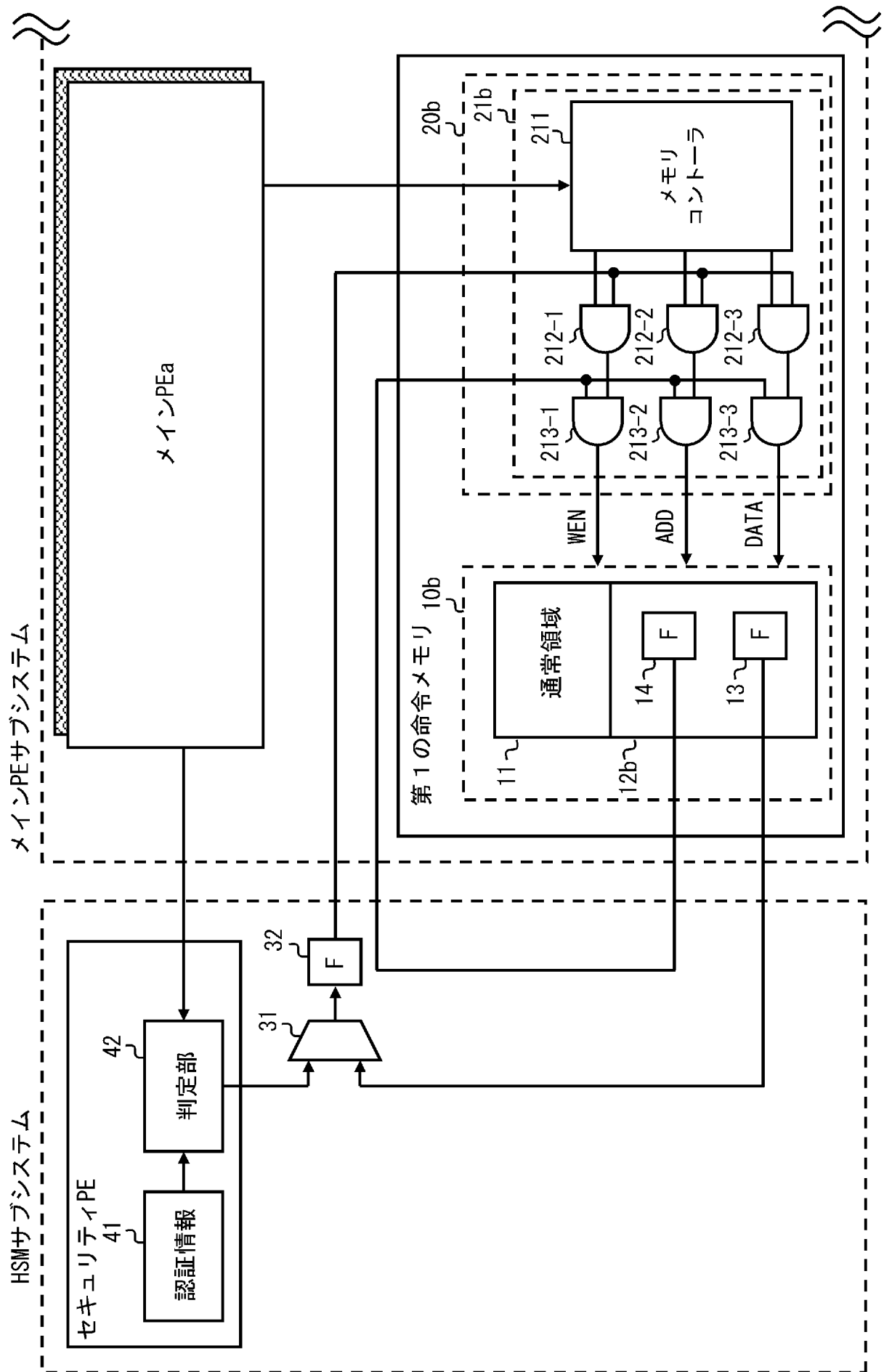
[図7]



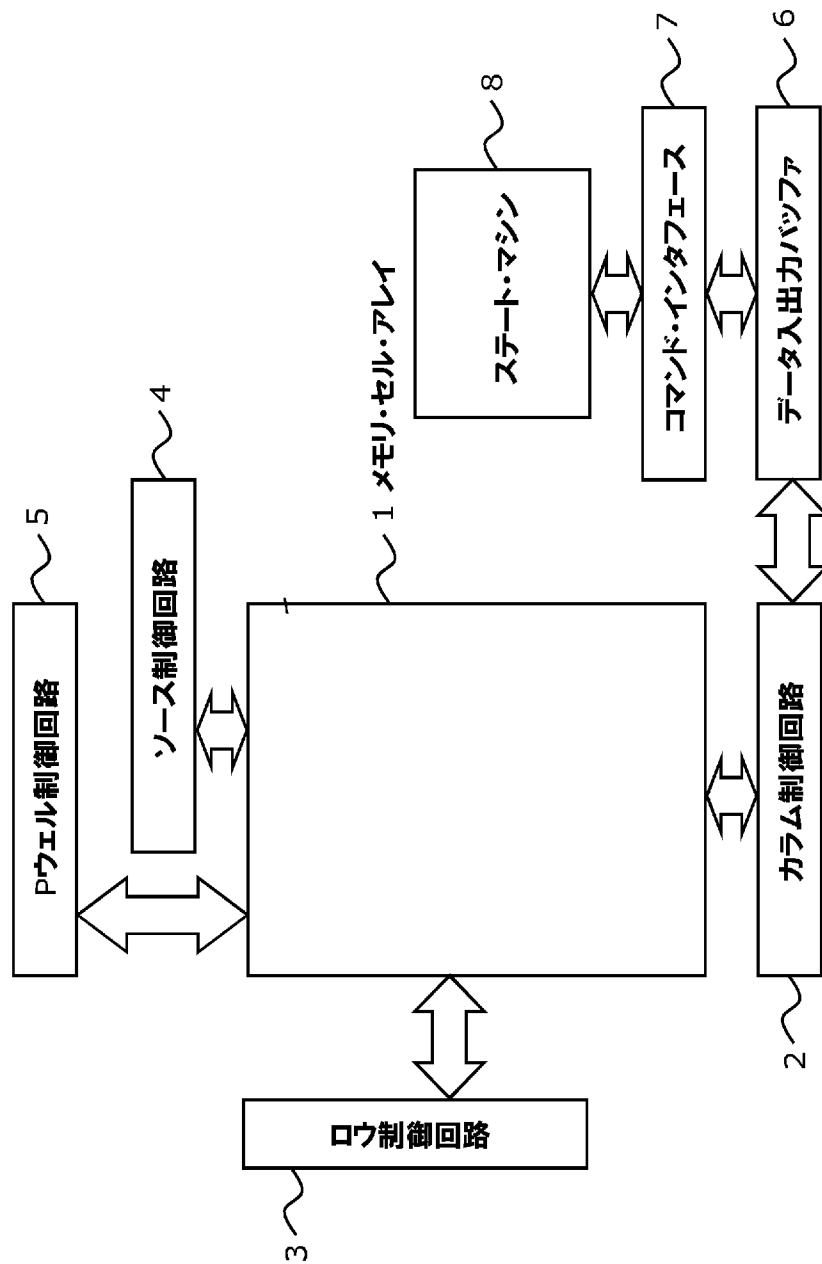
[図8A]



[図8B]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/001284

A. CLASSIFICATION OF SUBJECT MATTER

G06F12/14 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-350885 A (Renesas Technology Corp.), 28 December 2006 (28.12.2006), entire text; all drawings & US 2006/0285398 A1 & US 2008/0288735 A1 & US 2011/0010492 A1	1-14
A	JP 2004-259385 A (Fujitsu Ltd.), 16 September 2004 (16.09.2004), entire text; all drawings & US 2004/0179401 A1 & CN 1558423 A	1-14
A	JP 2001-51904 A (Hitachi, Ltd.), 23 February 2001 (23.02.2001), entire text; all drawings & US 7054990 B1 & WO 2001/013214 A1 & TW 484057 B	1-14

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
07 March, 2012 (07.03.12)

Date of mailing of the international search report
19 March, 2012 (19.03.12)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/001284

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-302416 A (Sharp Corp.), 02 November 2006 (02.11.2006), entire text; all drawings & US 2006/0242425 A1 & KR 10-2006-0110796 A	1-14
A	JP 2005-108273 A (Toshiba Corp.), 21 April 2005 (21.04.2005), entire text; all drawings & US 2006/0164886 A1 & US 2008/0205143 A1 & US 2010/0296339 A1 & EP 1665283 A1 & WO 2005/031754 A1 & TW 266326 B & KR 10-2006-0086364 A & CN 1856841 A	1-14

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F12/14(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2012年
日本国実用新案登録公報	1996-2012年
日本国登録実用新案公報	1994-2012年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2006-350885 A（株式会社ルネサステクノロジ） 2006.12.28, 全文, 全図 & US 2006/0285398 A1 & US 2008/0288735 A1 & US 2011/0010492 A1	1-14
A	JP 2004-259385 A（富士通株式会社） 2004.09.16, 全文, 全図 & US 2004/0179401 A1 & CN 1558423 A	1-14

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

07.03.2012

国際調査報告の発送日

19.03.2012

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

市川 武宜

5 S

4056

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2001-51904 A (株式会社日立製作所) 2001.02.23, 全文, 全図 & US 7054990 B1 & WO 2001/013214 A1 & TW 484057 B	1-14
A	JP 2006-302416 A (シャープ株式会社) 2006.11.02, 全文, 全図 & US 2006/0242425 A1 & KR 10-2006-0110796 A	1-14
A	JP 2005-108273 A (株式会社東芝) 2005.04.21, 全文, 全図 & US 2006/0164886 A1 & US 2008/0205143 A1 & US 2010/0296339 A1 & EP 1665283 A1 & WO 2005/031754 A1 & TW 266326 B & KR 10-2006-0086364 A & CN 1856841 A	1-14