

(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
2022年11月17日(17.11.2022)



(10) 国際公開番号

WO 2022/239331 A1

(51) 国際特許分類:
G06F 11/07 (2006.01) G06F 9/455 (2006.01)

(21) 国際出願番号: PCT/JP2022/004527

(22) 国際出願日: 2022年2月4日(04.02.2022)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

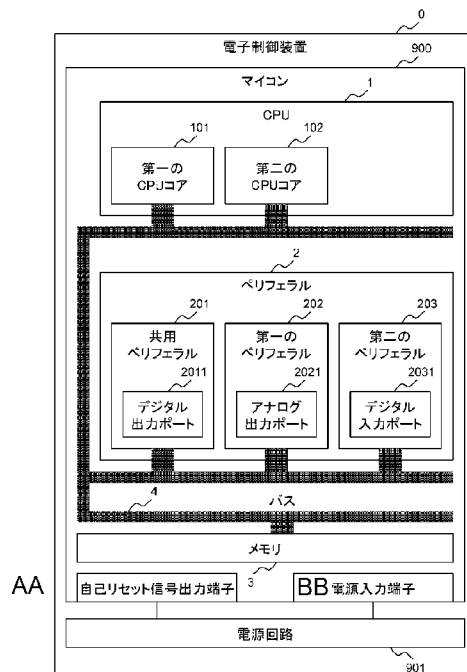
(30) 優先権データ:
特願 2021-080743 2021年5月12日(12.05.2021) JP

(71) 出願人: 日立 A s t e m o 株式会社(HITACHI
ASTEMO, LTD.) [JP/JP]; 〒3128503 茨城県ひ
たちなか市高場 2 5 2 0 番地 Ibaraki (JP).

(72) 発明者: 溝 口 将 史 (MIZOGUCHI Masashi);
〒1008280 東京都千代田区丸の内一丁目 6 番 6
号 株式会社日立製作所内 Tokyo (JP). 蛭 名 朋
仁(EBINA Tomohito); 〒3128503 茨城県ひたち
なか市高場 2 5 2 0 番地 日立 A s t e m o
株式会社内 Ibaraki (JP). 芹 沢 一(SERIZAWA
Kazuyoshi); 〒3128503 茨城県ひたちなか市高
場 2 5 2 0 番地 日立 A s t e m o 株式会
社内 Ibaraki (JP). 長 田 健 一(OSADA Kenichi);
〒3128503 茨城県ひたちなか市高場 2 5 2 0 番
地 日立 A s t e m o 株式会社内 Ibaraki (JP).
石 郷 岡 祐(ISHIGOOKA Tasuku); 〒1008280 東
京都千代田区丸の内一丁目 6 番 6 号 株式会
社日立製作所内 Tokyo (JP). 福 田 毅(FUKUDA

(54) Title: ELECTRONIC CONTROLLER AND ABNORMALITY DETERMINATION METHOD

(54) 発明の名称: 電子制御装置及び異常判定方法



- 0 Electronic controller
- 2 Peripheral devices
- 3 Memory
- 4 Bus
- 101 First CPU core
- 102 Second CPU core
- 201 Common peripheral device
- 202 First peripheral device
- 203 Second peripheral device
- 900 Computer
- 901 Power supply circuit
- 2011 Digital output port
- 2021 Analogue output port
- 2031 Digital input port
- AA Auto reset signal output terminal
- BB Power supply input terminal

(57) Abstract: This electronic controller is provided with: a virtual machine which accesses a first virtual driver and performs processing; a hypervisor which calls a first real driver of a first peripheral device on the basis of a peripheral access request received from the first virtual driver; an access recording unit which calls the first virtual driver and records the peripheral access request transmitted to the hypervisor; a state recording unit which calls the first real driver and records the register state in the first peripheral device; and a monitoring unit which monitors operation of the hypervisor.

Takeshi); 〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP).

(74) 代理人: 特許業務法人 藤央特許事務所 (**TOU-OU PATENT FIRM**); 〒1050001 東京都港区虎ノ門一丁目16番4号 アーバン虎ノ門ビル Tokyo (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

The monitoring unit determines abnormalities in the hypervisor on the basis of records of the access recording unit and records of the state recording unit.

(57) 要約: 電子制御装置であって、第一の仮想ドライバにアクセスして、処理を実行する仮想マシンと、前記第一の仮想ドライバから受信したペリフェラルアクセス要求に基づいて第一のペリフェラルの第一の実ドライバを呼び出すハイパーバイザと、前記第一の仮想ドライバを呼び出して、前記ハイパーバイザへ送信したペリフェラルアクセス要求を記録するアクセス記録部と、前記第一の実ドライバを呼び出して、前記第一のペリフェラルのレジスタの状態を記録する状態記録部と、前記ハイパーバイザの動作を監視する監視部とを備え、前記監視部は、前記アクセス記録部の記録と前記状態記録部の記録に基づいて、前記ハイパーバイザの異常を判定する。

明 細 書

発明の名称：電子制御装置及び異常判定方法

参照による取り込み

[0001] 本出願は、令和３年（２０２１年）５月１２日に出願された日本出願である特願２０２１－８０７４３の優先権を主張し、その内容を参照することにより、本出願に取り込む。

技術分野

[0002] 本発明は、電子制御装置に関する。

背景技術

[0003] ハイパーバイザを用いると、異なるＯＳ（Operating System）上で動作する複数の制御ソフトウェアアプリケーションを単一のマイコンに搭載できる。ハイパーバイザを監視する技術として、特開２０１９－１４４７８５（特許文献１）、特開２０１４－１０６５８７（特許文献２）に記載の技術がある。特許文献１には、仮想化ソフトウェア上に、仮想化ソフトウェアを含む複数の監視対象の監視に用いられる監視用の仮想マシンを配置し、所定間隔において監視用の仮想マシンによって実行された所定のテストの結果を取得し、取得したテストの結果から監視用の仮想マシンの異常有無を判定し、監視用の仮想マシンが異常である場合、複数の監視対象の所定の状態を取得し、監視用の仮想マシンの異常有無の判定結果と、複数の監視対象の所定の状態とを出力する監視プログラムが記載されている。

[0004] また、特許文献２には、ハイパバイザと第１のゲストＯＳがＩ／Ｏデバイスを共有する方法であって、Ｉ／Ｏデバイスは、物理機能と仮想機能を有し、ハイパバイザは、物理機能を利用する物理ドライバを有し、第１のゲストＯＳは、仮想機能を利用する仮想ドライバを有し、前記ハイパバイザが、物理ドライバを介してＩ／Ｏデバイスの状態を取得し、第１のゲストＯＳが、ハイパバイザを監視して所定の状態になったときには、Ｉ／Ｏデバイスを操作するサブ物理ドライバを起動し、前記第１のゲストＯＳは、メモリ上に予

め設定したキューを介して送受信を行う I/O デバイスの制御方法が記載されている。

発明の概要

発明が解決しようとする課題

[0005] 異なる OS 上で動作する複数の制御ソフトウェアアプリケーションを一つのマイコン（ハードウェア）に統合した電子制御装置においては、ハイパーバイザと呼称される仮想化ソフトウェアが用いられる。ハイパーバイザは、OS 及び制御ソフトウェアアプリケーションを動作させるための環境として、仮想マシンを提供する。仮想マシンとは、マイコン上の CPU（Central Processing Unit）、メモリ領域、及びマイコン上に搭載された CAN（Controller Area Network）コントローラや A/D（Analog/Digital）コンバータなどのペリフェラルに対するアクセス権を設定した単位である。各仮想マシン内のゲスト OS 及び制御ソフトウェアアプリケーションから見て、アクセス権限が付与されていない CPU、メモリ領域及びペリフェラルが別のマイコン上に存在することと論理的に等価である。一般に、電子制御装置の安全性や信頼性を確保するため、当該電子制御装置の動作中に、当該電子制御装置を構成するハードウェア及びソフトウェアが正常に動作しており、異常が発生していないことの監視が求められる。特に、ハイパーバイザを用いた電子制御装置において、ハイパーバイザの動作の監視が求められる。

[0006] 特許文献 1 によれば、仮想マシンとして監視用仮想マシンを設置し、該監視用仮想マシンが定期的にテストパターンを実行するとともに、ハイパーバイザの内部状態（正常・異常）を取得し、前記テストパターンの実行結果及び前記ハイパーバイザの内部状態の取得結果に基づき、電子制御装置に異常が発生しているか否か、及び異常が発生している場合に該異常による影響範囲を特定できる。しかし、特許文献 1 におけるハイパーバイザの監視は、ハイパーバイザ自身が判定する正常又は異常の状態を取得することにより実施されているため、ハイパーバイザに異常が発生することによってハイパーバ

イザによる異常状態が適切に判定されない場合が考慮されておらず、ハイパーバイザの正常動作が保証されない。また、ハイパーバイザの内部状態を取得する必要があるため、内部状態が公開されていないサードパーティ製のハイパーバイザに適用できない。

[0007] 特許文献2によれば、ハイパーバイザに対しカウンタ（ウォッチドッグタイマ）を設置し、当該カウンタを所定周期内にカウントアップ又はカウントダウンするよう要件を課し、当該カウンタが所定周期内に更新されない場合にハイパーバイザに異常が発生と判定する方法が記載されている。これにより、ハイパーバイザの予期しない停止や、ハイパーバイザに発生したデッドロックやライブロックを検出可能である。しかし、この方法を適用するためには、カウンタの更新に関する要件をハイパーバイザに課す必要がある。また、ウォッチドッグタイマのカウント更新処理は一般的に高優先度に設定されるため、ハイパーバイザ内部においてカウンタ更新処理の優先度がデッドロック又はライブロックを発生しているタスクの処理優先度より高い場合に、当該デッドロック及び当該ライブロックを検出できない。

[0008] そこで本発明では、サードパーティ製などの、内部ロジックが公開されていないハイパーバイザの入力及び出力のみに基づいた、当該ハイパーバイザの監視、当該ハイパーバイザに発生した異常の検知を目的とする。

課題を解決するための手段

[0009] 本願において開示される発明の代表的な一例を示せば以下の通りである。
すなわち、電子制御装置であって、第一の仮想ドライバにアクセスして、処理を実行する仮想マシンと、前記第一の仮想ドライバから受信したペリフェラルアクセス要求に基づいて第一のペリフェラルの第一の実ドライバを呼び出すハイパーバイザと、前記第一の仮想ドライバを呼び出して、前記ハイパーバイザへ送信したペリフェラルアクセス要求を記録するアクセス記録部と、前記第一の実ドライバを呼び出して、前記第一のペリフェラルのレジスタの状態を記録する状態記録部と、前記ハイパーバイザの動作を監視する監視部とを備え、前記監視部は、前記アクセス記録部の記録と前記状態記録部の

記録に基づいて、前記ハイパーバイザの異常を判定する。

発明の効果

[0010] 本発明の一態様によれば、ハイパーバイザの内部状態にアクセスせずに、ハイパーバイザの異常を検知できる。前述した以外の課題、構成及び効果は、以下の実施例の説明によって明らかにされる。

図面の簡単な説明

- [0011] [図1]第一の実施例の電子制御装置のハードウェア構成を示す図である。
- [図2]第一の実施例の電子制御装置のソフトウェア構成を示す図である。
- [図3]第一の実施例の第一の制御ソフトウェアアプリケーションが第一のペリフェラルを使用するときの処理フローの概要を表す図である。
- [図4]第一の実施例の第一の制御ソフトウェアアプリケーションが共有ペリフェラルを使用するときの処理フロー概要を示す図である。
- [図5]第一の実施例のペリフェラルアクセス要求情報の例を示す図である。
- [図6]第一の実施例のペリフェラルアクセス結果情報の例を示す図である。
- [図7]第一の実施例の第二の制御ソフトウェアアプリケーションが第二のペリフェラルを使用するときの処理フロー概要を示す図である。
- [図8]第一の実施例の第二の制御ソフトウェアアプリケーションが共有ペリフェラルを使用するときの処理フロー概要を示す図である。
- [図9]第一の実施例のペリフェラルアクセス記録情報の例を示す図である。
- [図10]第一の実施例のペリフェラル状態記録情報の例を示す図である。
- [図11]第一の実施例のハイパーバイザ監視プログラムの処理フロー概要を示す図である。
- [図12]第一の実施例のペリフェラル所望状態情報の例を示す図である。
- [図13]第一の実施例のハイパーバイザ監視プログラムのステップS 1におけるペリフェラル所望状態情報の生成処理を模式的に示す図である。
- [図14]第一の実施例のハイパーバイザ監視プログラムのステップS 1におけるペリフェラル所望状態情報の生成処理を模式的に示す図である。
- [図15]第二の実施例の電子制御装置のソフトウェア構成を示す図である。

[図16]第二の実施例のハイパーバイザ監視プログラムの処理フロー概要を示す図である。

[図17]第三の実施例の電子制御装置のハードウェア構成を示す図である。

[図18]第三の実施例の電子制御装置のソフトウェア構成を示す図である。

[図19]第三の実施例の第一の制御ソフトウェアアプリケーションが共有ペリフェラルであるCANコントローラを使用するときの処理フロー概要を示す図である。

[図20]第三の実施例のCAN台帳を示す図である。

[図21]第四の実施例の監視結果保存プログラムの処理フロー概要を示す図である。

[図22]第四の実施例のハイパーバイザ異常発生時刻情報の例を示す図である。

[図23]第四の実施例の監視結果保存プログラムのステップS7における処理の概要を模式的に示す図である。

発明を実施するための形態

[0012] 本実施例は、電子制御装置に関するものであって、特に、複数の制御ソフトウェアアプリケーションを一つのマイコン上に統合した電子制御装置に関する。

[0013] 以下、本発明に好適な実施形態の例（実施例）を説明する。説明のため本実施例においては、第一の制御ソフトウェアアプリケーションと第二の制御ソフトウェアアプリケーションの二つの制御ソフトウェアアプリケーションを一つの電子制御装置に統合する例を説明するが、これに限らず、第三の制御ソフトウェアアプリケーションや第四の制御ソフトウェアアプリケーションを一つの電子制御装置に統合するものでもよい。

実施例 1

[0014] <構成>

図1は、第一の実施例の電子制御装置のハードウェア構成を示す図である。

[0015] <電子制御装置0>

図1を参照して、本実施例の電子制御装置について説明する。電子制御装置0は、マイコン900と電源回路901を有する。マイコン900は、演算処理を行うCPU (Central Processing Unit) 1、電子制御装置0に搭載された周辺機器群であるペリフェラル2、ソフトウェアを格納するメモリ3、CPU1とペリフェラル2とメモリ3を接続しCPU1からペリフェラル2及びメモリ3へのアクセスを可能とするバス4で構成される。

[0016] マイコン900の電源入力端子は、電源回路901と接続されている。マイコン900は電源回路901から電源供給を受けると起動する。マイコン900は、自己リセット信号出力端子を有する。マイコン900が自己リセット信号出力端子からデジタル信号を出力することによって、電源回路901はマイコン900への電源供給を停止する。

[0017] <CPU1>

CPU1は、第一のCPUコア101と第二のCPUコア102の二つのコアを有する。なお、説明のためCPUコアは二つとしているが、これに限らず、例えば一つでも三つ以上でもよい。

[0018] <ペリフェラル2>

ペリフェラル2は、マイコン900の内部又は外部にデータ及び信号を入力出力するデバイスであり、第一の制御ソフトウェアアプリケーション10（すなわち第一のCPUコア101）及び第二の制御ソフトウェアアプリケーション15（すなわち第二のCPUコア102）の両方からアクセスされる共用ペリフェラル201と、第一の制御ソフトウェアアプリケーション10（すなわち第一のCPUコア101）のみからアクセスされる第一のペリフェラル202と、第二の制御ソフトウェアアプリケーション15（すなわち第二のCPUコア103）のみからアクセスされる第二のペリフェラル203とを含む。ペリフェラル2とは、マイコン900に搭載されるCPU1及びメモリ3以外の周辺回路の一般的な呼称であり、具体的には、マイコン900に搭載されたCAN (Controller Area Network) コントローラ、アナロ

グ・デジタル・コンバータ、ダイレクト・メモリ・アクセスコントローラ、G P I O (General Purpose Input/Output) などを含む。

[0019] <メモリ3>

メモリ3は、不揮発性の記憶素子であるR O M及び揮発性の記憶素子であるR A Mを含む。R O Mは、不変のプログラム（例えば、B I O S）などを格納する。R A Mは、D R A M (Dynamic Random Access Memory) のような高速かつ揮発性の記憶素子であり、C P U 1 が実行するプログラム及びプログラムの実行時に使用されるデータを格納する。

[0020] 簡単のため、本実施例においては、共用ペリフェラル2 0 1 がデジタル出力ポート2 0 1 1 を含み、第一のペリフェラル2 0 2 がアナログ出力ポート2 0 2 1 を含み、第二のペリフェラル2 0 3 がデジタル入力ポート2 0 3 1 を含むものとする。

[0021] 図2は、第一の実施例の電子制御装置のソフトウェア構成を示す図である。図2に示すソフトウェアはメモリ3に格納される。

[0022] <ソフトウェア構成>

以下の処理は、C P U 1 の第一のC P U コア1 0 1 又は第二のC P U コア1 0 2 のいずれかにおいて実行される。

[0023] ホストO S (Operating System) 5は、マイコン9 0 0 上に搭載される。ホストO S 5は、ハイパーバイザ6とハイパーバイザ監視プログラム1 7とレジスタ値取得プログラム1 8を起動する。ハイパーバイザ6は、ハイパーバイザ6によって定められる起動方法に従って起動される。ハイパーバイザ監視プログラム1 7とレジスタ値取得プログラム1 8は5ミリ秒周期で起動し、監視のための情報を取得する。なお、簡単のため本実施例では起動周期を5ミリ秒としたが、これに限らず、他のタイミングで起動してもよい。ハイパーバイザ6は、ホストO S 5上で実行されるソフトウェアで構成されても、マイコン9 0 0 に実装されるハードウェアで構成されてもよい。

[0024] ハイパーバイザ6は、ハイパーバイザ6によって定められる方法によって、第一の仮想マシン7と第二の仮想マシン8を構成し、それぞれを起動する

。なお、簡単のため本実施例では仮想マシンの数を2としたが、これに限らず、1又は3以上でもよい。

[0025] 第一の仮想マシン7では、第一のゲストOS9と、第一の制御ソフトウェアアプリケーション10と、仮想ドライバ11と、ペリフェラルアクセス要求記録プログラム19と、アナログ出力ポートドライバ12が実行される。第二の仮想マシン8では、第二のゲストOS13と、第二の制御ソフトウェアアプリケーション15と、仮想ドライバ11と、デジタル入力ポートドライバ14が実行される。ペリフェラルアクセス要求記録プログラム19は、第一の仮想マシン7上で実行されているが、第二の仮想マシン8上で実行されてもよい。すなわち、ペリフェラルアクセス要求記録プログラム19は、ハイパーバイザ6上で少なくとも一つ実行されていけばよい。

[0026] <第一の仮想マシン7>

第一の仮想マシン7におけるソフトウェアの動作について説明する。ハイパーバイザ6が第一の仮想マシン7を構成すると、第一の仮想マシン7は第一のゲストOS9を起動する。第一のゲストOS9は、第一の制御ソフトウェアアプリケーション10を起動する。第一の制御ソフトウェアアプリケーション10は、共用ペリフェラル201であるデジタル出力ポート2011と第一のペリフェラル202であるアナログ出力ポート2021を使用する。

[0027] 図3は、第一の制御ソフトウェアアプリケーション10が第一のペリフェラル202を使用するときの処理フローの概要を表す図である。

[0028] <第一の仮想マシン7から第一のペリフェラル202へのアクセス>

第一の制御ソフトウェアアプリケーション10から第一のペリフェラル202であるアナログ出力ポート2021にアクセスするためには、アナログ出力ポートドライバ12を用いる。すなわち、第一の制御ソフトウェアアプリケーション10がペリフェラルアクセス要求として、引数に5Vを指定してアナログ出力ポートドライバ12をコールすると、アナログ出力ポートドライバ12はアナログ出力ポート2021のレジスタにアクセスし、出力電

圧値を5 Vとするための値をマイコン900の所定のレジスタにセットし、第一の制御ソフトウェアアプリケーション10に正常終了をリターンする。

[0029] 図4は、第一の制御ソフトウェアアプリケーション10が共用ペリフェラル201を使用するときの処理フロー概要を示す図である。

[0030] <第一の仮想マシン7から共用ペリフェラル201へのアクセス>

第一の制御ソフトウェアアプリケーション10から共用ペリフェラル201であるデジタル出力ポート2011にアクセスするためには、ペリフェラルアクセス要求記録プログラム19と仮想ドライバ11とハイパーバイザ6とデジタル出力ポートドライバ16を用いる。すなわち、第一の制御ソフトウェアアプリケーション10は、ペリフェラルアクセス要求として、引数にHを指定してペリフェラルアクセス要求記録プログラム19をコールする。ペリフェラルアクセス要求記録プログラム19は、第一の制御ソフトウェアアプリケーション10によるペリフェラルアクセス要求情報51を記録し、引数にHを指定して仮想ドライバ11をコールする。仮想ドライバ11は、CPU1の処理コンテキストを第一の仮想マシン7からハイパーバイザ6に変更するための処理（一般にVME x i t と呼称される）を実行する。ハイパーバイザ6は、デジタル出力ポート2011の使用状況を確認する。すなわち、ハイパーバイザ6は、第二の仮想マシン8がデジタル出力ポート2011を使用中でなければ、引数をHとしてデジタル出力ポート2011にアクセスするためのデジタル出力ポートドライバ16をコールする。第二の仮想マシン8がデジタル出力ポート2011を使用中の場合は、ハイパーバイザ6の内部に準備されたバッファに引数Hを格納して待機し、第二の仮想マシン8によるデジタル出力ポート2011の使用終了後にバッファから引数Hを取り出し、取り出した引数を付してデジタル出力ポートドライバ16をコールする。

[0031] デジタル出力ポートドライバ16は、デジタル出力ポート2011のレジスタにアクセスし、出力値をH（High, 1）とするためのマイコン900の所定のレジスタに値をセットし、ハイパーバイザ6に正常終了をリター

ンする。ハイパーバイザ6は、デジタル出力ポートドライバ16から正常終了のリターンを受け取ると、CPU1の処理コンテキストをハイパーバイザ6から第一の仮想マシン7に変更するための処理（一般にVME n t r yと称される）を実行する。仮想ドライバ11は、ハイパーバイザ6から正常終了の情報を受け取ると、ペリフェラルアクセス要求記録プログラム19をコールする。ペリフェラルアクセス要求記録プログラム19は、第一の制御ソフトウェアアプリケーション10に対するペリフェラルアクセス結果情報52を記録し、第一の制御ソフトウェアアプリケーション10に正常終了をリターンする。

[0032] 図5は、第一の制御ソフトウェアアプリケーション10によるペリフェラルアクセス要求情報51の例を示す図である。

[0033] <第一の制御ソフトウェアアプリケーション10によるペリフェラルアクセス要求情報51>

第一の制御ソフトウェアアプリケーション10によるペリフェラルアクセス要求情報51は、第一の制御ソフトウェアアプリケーション10がペリフェラルアクセス要求記録プログラム19をコールした時刻と、当該コールによってアクセスを要求したペリフェラルと、当該コールにおいて付加した引数の情報を含む。

[0034] 図6は、第一の制御ソフトウェアアプリケーション10に対するペリフェラルアクセス結果情報52の例を示す図である。

[0035] <第一の制御ソフトウェアアプリケーション10に対するペリフェラルアクセス結果情報52>

第一の制御ソフトウェアアプリケーション10に対するペリフェラルアクセス結果情報52は、ハイパーバイザ6が仮想ドライバ11に対して正常処理済みである旨の情報を返信した時刻と、ハイパーバイザ6が処理を行ったペリフェラルの情報と、処理結果の情報を含む。

[0036] <第二の仮想マシン8>

第二の仮想マシン8におけるソフトウェアの動作について説明する。ハイ

パーバイザ6が第二の仮想マシン8を構成すると、第二の仮想マシン8は第二のゲストOS13を起動する。第二のゲストOS13は、第二の制御ソフトウェアアプリケーション15を起動する。第二の制御ソフトウェアアプリケーション15は、共用ペリフェラル201であるデジタル出力ポート2011と第二のペリフェラル203であるデジタル入力ポート2031を使用する。

[0037] 図7は、第二の制御ソフトウェアアプリケーション15が第二のペリフェラル203を使用するときの処理フロー概要を示す図である。

[0038] <第二の仮想マシン8から第二のペリフェラル203へのアクセス>

第二の制御ソフトウェアアプリケーション15から第二のペリフェラル203であるデジタル入力ポート2031にアクセスするためには、デジタル入力ポートドライバ14を用いる。すなわち、第二の制御ソフトウェアアプリケーション15がペリフェラルアクセス要求として、デジタル入力ポートドライバ14をコールすると、デジタル入力ポートドライバ14はデジタル入力ポート2031のレジスタにアクセスし、マイコン900の所定のレジスタの値を読み取り、該読み取りの結果を付して第二の制御ソフトウェアアプリケーション15にリターンする。

[0039] 図8は、第二の制御ソフトウェアアプリケーション15が共用ペリフェラル201を使用するときの処理フロー概要を示す図である。

[0040] <第二の仮想マシン8から共用ペリフェラル201へのアクセス>

第二の制御ソフトウェアアプリケーション15から共用ペリフェラル201であるデジタル出力ポート2011にアクセスするためには、仮想ドライバ11とハイパーバイザ6とデジタル出力ポートドライバ16を用いる。すなわち、第一の制御ソフトウェアアプリケーション10は、ペリフェラルアクセス要求として、引数にHを指定して仮想ドライバ11をコールする。仮想ドライバ11は、CPU1の処理コンテキストを第二の仮想マシン8からハイパーバイザ6に変更するための処理（一般にVMExitと呼称される）を実行する。ハイパーバイザ6は、デジタル出力ポート2011の使用状

況を確認する。すなわち、ハイパーバイザ6は、第一の仮想マシン7がデジタル出力ポート2011を使用中でなければ、引数をHとしてデジタル出力ポート2011にアクセスするためのデジタル出力ポートドライバ16をコールする。第一の仮想マシン7がデジタル出力ポート2011を使用中の場合は、ハイパーバイザ6の内部に準備されたバッファに引数Hを格納して待機し、第一の仮想マシン7によるデジタル出力ポート2011の使用終了後にバッファから引数Hを取り出し、取り出した引数を付してデジタル出力ポートドライバ16をコールする。

[0041] デジタル出力ポートドライバ16は、デジタル出力ポート2011のレジスタにアクセスし、出力値をH (High, 1) とするためのマイコン900の所定のレジスタに値をセットし、ハイパーバイザ6に正常終了をリターンする。ハイパーバイザ6は、デジタル出力ポートドライバ16から正常終了のリターンを受け取ると、CPU1の処理コンテキストをハイパーバイザ6から第一の仮想マシン7に変更するための処理（一般にVME n t r yと称される）を実行する。仮想ドライバ11は、ハイパーバイザ6から正常終了の情報を受け取ると、第一の制御ソフトウェアアプリケーション10に正常終了をリターンする。

[0042] <ペリフェラルアクセス要求記録プログラム19>

ペリフェラルアクセス要求記録プログラム19は、図4に示すように、第一の制御ソフトウェアアプリケーション10がペリフェラルアクセス要求を送出したときに、第一の制御ソフトウェアアプリケーション10によるペリフェラルアクセス要求情報51を生成する。また、ペリフェラルアクセス要求記録プログラム19は、図4に示すように、仮想ドライバ11がハイパーバイザ6から正常終了済みとの情報を受け取ったときに、第一の制御ソフトウェアアプリケーション10に対するペリフェラルアクセス結果情報52を生成する。さらに、ペリフェラルアクセス要求記録プログラム19は、第一のゲストOS9によって所定のタイミングで繰り返し（例えば100ミリ秒周期で）起動され、第一の制御ソフトウェアアプリケーション10によるペ

リフェラルアクセス要求情報 5 1 と第一の制御ソフトウェアアプリケーション 1 0 に対するペリフェラルアクセス結果情報 5 2 を統合したペリフェラルアクセス記録情報 5 3 を生成し、当該ペリフェラルアクセス記録情報 5 3 をハイパーバイザ監視プログラム 1 7 が参照可能なメモリ領域に書き込む。

[0043] 図 9 は、ペリフェラルアクセス記録情報 5 3 の例を示す図である。

[0044] <ペリフェラルアクセス記録情報 5 3>

ペリフェラルアクセス記録情報 5 3 は、第一の制御ソフトウェアアプリケーション 1 0 がペリフェラルアクセス要求記録プログラム 1 9 をコールした時刻と、当該要求によるアクセス要求先のペリフェラルと、当該要求において付加した引数の情報と、当該ペリフェラルアクセス要求に従ってハイパーバイザ 6 が仮想ドライバ 1 1 に対して正常処理済みとの情報を送信した時刻と、ハイパーバイザ 6 による処理結果の情報を含む。

[0045] <レジスタ値取得プログラム 1 8>

レジスタ値取得プログラム 1 8 は、ホスト OS 5 によって所定のタイミングで繰り返し（例えば 5 ミリ秒周期で）起動される。レジスタ値取得プログラム 1 8 は、起動毎にデジタル出力ポートドライバ 1 6 をコールして、共用ペリフェラル 2 0 1 であるデジタル出力ポート 2 0 1 1 の状態を表すマイコン 9 0 0 の所定のレジスタの値を取得し、ペリフェラル状態記録情報 5 4 を生成し、生成したペリフェラル状態記録情報 5 4 をハイパーバイザ監視プログラム 1 7 が参照可能なメモリ領域に書き込む。レジスタ値取得プログラム 1 8 は、ホスト OS 5 上で実行されているが、ハイパーバイザ 6 上で実行されてもよい。

[0046] 図 1 0 は、ペリフェラル状態記録情報 5 4 の例を示す図である。

[0047] <ペリフェラル状態記録情報 5 4>

ペリフェラル状態記録情報 5 4 は、レジスタ値取得プログラム 1 8 の処理対象のペリフェラルと、レジスタ値取得プログラム 1 8 がペリフェラル（デジタル出力ポートドライバ 1 6）をコールした時刻と、該コールにより取得したレジスタの値の情報を含む。

[0048] 図 1 1 は、ハイパーバイザ監視プログラム 1 7 の処理フロー概要を示す図である。

[0049] <ハイパーバイザ監視プログラム 1 7>

ハイパーバイザ監視プログラム 1 7 は、ペリフェラルアクセス記録情報 5 3 に基づいてレジスタ値が本来取るべき値を計算し、この本来取るべき値とペリフェラル状態記録情報 5 4 が一致していない場合に、ハイパーバイザ 6 に異常が発生したと判定する。

[0050] ステップ S 1 において、ハイパーバイザ監視プログラム 1 7 は、ペリフェラルアクセス記録情報 5 3 に含まれるすべての情報とペリフェラル状態記録情報 5 4 に含まれる状態確認時刻情報に基づいて、ペリフェラル所望状態情報 5 5 を生成する。

[0051] ステップ S 2 において、ハイパーバイザ監視プログラム 1 7 は、ペリフェラル状態記録情報 5 4 とペリフェラル所望状態情報 5 5 を比較し、ハイパーバイザ 6 の状態が正常であるか異常であるかを判定する。

[0052] 図 1 2 は、ペリフェラル所望状態情報 5 5 の例を示す図である。

[0053] <ペリフェラル所望状態情報 5 5>

ペリフェラル所望状態情報 5 5 は、レジスタ値取得プログラム 1 8 がデジタル出力ポートドライバ 1 6 をコールした時刻と、ペリフェラルアクセス記録情報 5 3 に基づいて計算された時刻におけるペリフェラルレジスタの値の情報を含む。

[0054] 図 1 3 は、ハイパーバイザ監視プログラム 1 7 のステップ S 1 におけるペリフェラル所望状態情報生成処理を模式的に示す図である。

[0055] <ステップ S 1>

本実施例では、レジスタの初期値は不定である。

[0056] ペリフェラルアクセス記録情報 5 3 によると、第一の制御ソフトウェアアプリケーション 1 0 は、時刻 1 0 : 0 0 に引数を H としてペリフェラルアクセス要求を送信している。第一の制御ソフトウェアアプリケーション 1 0 がペリフェラルアクセス要求を送信してから図 4 に示すフローに従ってデジタ

ル出力ポートドライバ16のレジスタの値が実際に操作されるまでの間にはオーバヘッドが存在する。当該オーバヘッドの長さは予測できないが、ペリフェラルアクセス記録情報53のハイパーバイザ返答時刻情報によって、時刻10:00と時刻16:00の間のいずれかの時刻でレジスタの値がHにセットされていると計算される。

[0057] 同様に、ペリフェラルアクセス記録情報53によると、第一の制御ソフトウェアアプリケーション10は、時刻25:00に引数をLとしてペリフェラルアクセス要求を送信している。第一の制御ソフトウェアアプリケーション10がペリフェラルアクセス要求を送信してから図4に示すフローに従ってデジタル出力ポートドライバ16のレジスタの値が実際に操作されるまでの間にはオーバヘッドが存在する。当該オーバヘッドの長さは予測できないが、ペリフェラルアクセス記録情報53のハイパーバイザ返答時刻情報によって、時刻25:00と時刻32:00の間のいずれかの時刻でレジスタの値がLにセットされていると計算される。

[0058] 従って、ペリフェラル所望状態情報55は、図12に示す通りに生成される。すなわち、時刻12:10においては不定値である初期値が維持されているか、時刻10:00に送信されたペリフェラルアクセス要求に従いHとなっているかのいずれかであり、レジスタの値はH又はLいずれも取り得る。時刻16:00より後の時刻17:10においては、レジスタの値はH、時刻22:10においては引き続きレジスタの値はHとなっている。また、時刻27:10においては、引き続きレジスタの値はHとなっているか、時刻25:00におけるペリフェラルアクセス要求に従ってLとなっているかのいずれかであり、レジスタの値はH又はLいずれも取り得る。時刻32:00より後の時刻32:10においては、レジスタの値はL、時刻37:10においては引き続きレジスタの値はLと計算される。

[0059] 図14は、ハイパーバイザ監視プログラム17のステップS1におけるペリフェラル所望状態情報生成処理を模式的に示す図である。

[0060] <ステップS2>

ステップS 2において、ハイパーバイザ監視プログラム17は、ペリフェラル所望状態情報55とペリフェラル状態記録情報54を比較し、ペリフェラル所望状態情報55で計算された各時刻におけるペリフェラルレジスタの値がペリフェラル状態記録情報54に記録されたレジスタの値と異なる場合に、ハイパーバイザ6の異常が発生したと判定する。すなわち、図14に示す場合、時刻32:10において、ペリフェラル所望状態情報55によるとレジスタの値はLであるべきだが、ペリフェラル状態記録情報54によると実際のレジスタの値はHとなっているため、ハイパーバイザ6の異常が検知される。これは、第一の制御ソフトウェアアプリケーション10が、デジタル出力ポート2011をLにするようペリフェラルアクセス要求を送信し、ハイパーバイザ6は正常に処理した旨を第一の制御ソフトウェアアプリケーション10に返答しているが、実際にはデジタル出力ポート2011の値がHのまま変更されていないことを表している。

[0061] 本実施例によれば、内部ロジックが公開されていないハイパーバイザ6であっても、ハイパーバイザ6が操作するマイコン900のレジスタの値の変化の記録によって、ハイパーバイザ6が仮想マシン7、8の内部の制御ソフトウェアアプリケーション10、15が要求した処理が正しく実行しているか否かをハイパーバイザ6の外部から監視する。このため、ハイパーバイザ6の内部状態にアクセスせずに、ハイパーバイザ6の入力及び出力に基づいて、ハイパーバイザ6の異常を検知できる。すなわち、ハイパーバイザ6が仮想マシン7、8に対して正常処理を返信している場合でも、実際に正常に処理が行われていなければハイパーバイザ6の異常を検出できる。

[0062] また、レジスタの実際の値と予定値の不整合によってハイパーバイザ6の異常を判定するので、テストパターンのような余分な処理が不要となり、本来の処理への影響を抑制できる。

実施例 2

[0063] 本発明の第二の実施例の電子制御装置及び方法について説明する。第二の実施例は、ソフトウェア構成に監視結果保存プログラム20が追加される点

で第一の実施例と異なる。なお、第一の実施例と同じ構成には、同じ符号を付して、その説明を省略する。

[0064] 図15は、第二の実施例の電子制御装置のソフトウェア構成を示す図である。図15に示すソフトウェアはメモリ3に格納される。

[0065] <ソフトウェア構成>

ホストOS5はマイコン900上に搭載される。ホストOS5は、ハイパーバイザ6とハイパーバイザ監視プログラム17とレジスタ値取得プログラム18を起動する。また、ホストOS5は、異常検知フラグ56の値を所定のタイミングで繰り返し（例えば5ミリ秒周期で）確認し、異常検知フラグ56がTrueであることを確認した場合、異常検知フラグ56をFalseに書き換えた後、監視結果保存プログラム20を起動する。

[0066] <異常検知フラグ56>

異常検知フラグ56はTrue、Falseの2値のいずれかをとり変数である。

[0067] 図16は、ハイパーバイザ監視プログラム17の処理フロー概要を示す図である。

[0068] <ステップS3>

ステップS3において、ハイパーバイザ監視プログラム17は、ステップS2における判定結果が正常であるか異常であるかに従って、処理を分岐する。すなわち、ステップS2における判定結果が正常である場合は何もせずに終了し、ステップS2における判定結果が異常である場合はステップS4に進む。

[0069] <ステップS4>

ステップS4において、ハイパーバイザ監視プログラム17は、異常検知フラグ56の値をTrueに変更し、処理を終了する。

[0070] <監視結果保存プログラム20>

監視結果保存プログラム20は、ペリフェラルアクセス記録情報53とペリフェラル状態記録情報54とペリフェラル所望状態情報55をマイコン9

00のメモリ3の内部の不揮発メモリ領域に保存する。

[0071] 本実施例によれば、不揮発メモリ領域の参照によって、ペリフェラルアクセス記録情報53とペリフェラル状態記録情報54とペリフェラル所望状態情報55を、ハイパーバイザ6に異常が検知された理由及びハイパーバイザ6に異常が発生する動作パターンを特定するデバッグのための情報として使用できる。

実施例 3

[0072] 本発明の第三の実施例の電子制御装置及び方法について説明する。第三の実施例は、ペリフェラルアクセス記録情報53を取り出すために別の仮想ドライバを使用する点で第一の実施例と異なる。なお、第一の実施例と同じ構成については、同じ符号を付して、その説明を省略する。

[0073] <構成>

図17は、第三の実施例の電子制御装置のハードウェア構成を示す図である。

[0074] <ペリフェラル2>

本実施例においては、共用ペリフェラル201にデジタル出力ポート2011及びCANコントローラ2012が含まれ、第一のペリフェラル202にアナログ出力ポート2021が含まれ、第二のペリフェラル203にデジタル入力ポート2031が含まれる。

[0075] 図18は、第三の実施例の電子制御装置のソフトウェア構成を示す図である。図18に示すソフトウェアはメモリ3に格納される。

[0076] <ソフトウェア構成>

第一の仮想マシン7は、第一のゲストOS9と、第一の制御ソフトウェアアプリケーション10と、仮想ドライバ11と、ペリフェラルアクセス要求記録プログラム19と、アナログ出力ポートドライバ12と、仮想CANDライバ21を含む。第二の仮想マシン8は、第二のゲストOS13と、第二の制御ソフトウェアアプリケーション15と、仮想ドライバ11と、デジタル入力ポートドライバ14と、仮想CANDライバ21を含む。

[0077] <第一の仮想マシン 7>

第一の仮想マシン 7 におけるソフトウェアの動作について説明する。ハイパーバイザ 6 が第一の仮想マシン 7 を構成すると、第一の仮想マシン 7 は第一のゲスト OS 9 を起動する。第一のゲスト OS 9 は、第一の制御ソフトウェアアプリケーション 10 を起動する。第一の制御ソフトウェアアプリケーション 10 は、共用ペリフェラル 201 であるデジタル出力ポート 2011 と CAN コントローラ 2012 と、第一のペリフェラル 202 であるアナログ出力ポート 2021 を使用する。

[0078] 図 19 は、第三の実施例の第一の制御ソフトウェアアプリケーション 10 が共用ペリフェラル 201 である CAN コントローラ 2012 を使用するときの処理フロー概要を示す図である。

[0079] <第一の仮想マシン 7 から CAN コントローラ 2012 へのアクセス>

第一の制御ソフトウェアアプリケーション 10 から共用ペリフェラル 201 である CAN コントローラ 2012 にアクセスするためには、仮想 CAN ドライバ 21 とハイパーバイザ 6 と CAN ドライバ 22 を用いる。すなわち、第一の制御ソフトウェアアプリケーション 10 は、ペリフェラルアクセス要求として、引数に CAN メッセージプロトコルで指定される ID 及び CAN フレームに送信するデータ *data* を指定して仮想 CAN ドライバ 21 をコールする。仮想 CAN ドライバ 21 は、CPU 1 の処理コンテキストを第一の仮想マシン 7 からハイパーバイザ 6 に変更するための処理（一般に VM *Exit* と呼称される）を実行する。ハイパーバイザ 6 は、CAN コントローラ 2012 の使用状況を確認する。すなわち、ハイパーバイザ 6 は、第二の仮想マシン 8 が CAN コントローラ 2012 を使用中でなければ、引数に ID と *data* を指定して CAN コントローラ 2012 にアクセスするための CAN ドライバ 22 をコールする。第二の仮想マシン 8 が CAN コントローラ 2012 を使用中の場合は、ハイパーバイザ 6 の内部に準備したバッファに引数 ID と *data* を格納して待機し、第二の仮想マシン 8 による CAN コントローラ 2012 の使用が終了した後に、前記バッファから引数 ID

と `data` を取り出し、前記取り出した引数をつけて `CAN` ドライバ 22 をコールする。

[0080] `CAN` ドライバ 22 は `CAN` コントローラ 2012 のレジスタにアクセスし、`CAN` 通信バスに対して `ID` と `data` を `CAN` フレームに格納して送信し、ハイパーバイザ 6 に対し、正常終了をリターンする。ハイパーバイザ 6 は、`CAN` ドライバ 22 から正常終了のリターンを受け取ると、`CPU` 1 の処理コンテキストをハイパーバイザ 6 から第一の仮想マシン 7 に変更するための処理（一般に `VME n t r y` と呼称される）を実行する。仮想 `CAN` ドライバ 21 は、ハイパーバイザ 6 から正常終了の情報を受け取ると、第一の制御ソフトウェアアプリケーション 10 に対し正常終了をリターンする。

[0081] 図 20 は、第三の実施例の `CAN` 台帳 57 を示す図である。

[0082] <`CAN` 台帳 57 >

`CAN` 台帳 57 は、`CAN` ドライバ 22 内部に保持され、各 `CAN` フレームを識別するためのメッセージ `ID` と当該 `CAN` フレームに含まれるデータの内容と当該 `CAN` フレームを送信処理するか受信処理するかの情報と当該 `CAN` フレームにおけるデータ長の情報を含む。本実施例では、`ID` 0 から 2000 までの `CAN` フレームは、通常の制御処理に使用され、`CAN` 通信バスに対し送信される又は `CAN` 通信バスから受信される。メッセージ `ID` 9900 の `CAN` フレームには、ペリフェラル状態記録情報 54 における状態確認時刻と処理対象とレジスタ値の組を 8 バイトのデータとして格納し、当該 `CAN` フレームの送信・受信の情報は監視部送信と記載する。

[0083] <`CAN` ドライバ 22 >

`CAN` ドライバ 22 は、`CAN` 台帳 57 に記述された情報に従って、`CAN` コントローラ 2012 のレジスタを操作する。すなわち、メッセージ `ID` 0 の 8 バイトデータについては `CAN` コントローラ 2012 のレジスタを操作して車両速度として `CAN` 通信バスから受信し、メッセージ `ID` 1 の 8 バイトデータについては `CAN` コントローラ 2012 のレジスタを操作してエンジン回転数として `CAN` 通信バスに送信し、メッセージ `ID` 2 の 8 バイト

データについてはCANコントローラ2012のレジスタを操作してスロットル開度としてCAN通信バスに送信する。

[0084] さらに、CANDライバ22は、CAN台帳57において送信・受信の種類が監視部送信となっているメッセージID9900のデータについては、CANコントローラ2012のレジスタを操作せず、ハイパーバイザ監視プログラム17が参照可能なメモリ領域に当該データを書き込む。CANDライバ22は第一の仮想マシン7及びハイパーバイザ6の外部に存在するため、ハイパーバイザ6によるメモリ領域の参照領域の制限の影響を受けない。また、ハイパーバイザ6の監視に使用するペリフェラル（デジタル出力ポート2011）と別のペリフェラル（CANコントローラ2012）を用いることによって、ハイパーバイザ6はデジタル出力ポート2011の操作において異常が発生している場合においても、ペリフェラルアクセス記録情報53をハイパーバイザ監視プログラム17が参照可能なメモリ領域に格納できる。

[0085] 本実施例によれば、ハイパーバイザ6が構成した仮想マシン内部から仮想マシン外部へのアクセスが禁止され、ペリフェラルアクセス要求記録プログラム19がペリフェラルアクセス記録情報53をハイパーバイザ監視プログラム17が参照可能なメモリ領域に書き込むことが不可能な場合でも、当該ペリフェラルアクセス記録情報53を第一の仮想マシン7の外部に取り出し、ハイパーバイザ監視プログラム17が参照可能なメモリ領域に書き込むことができる。

実施例 4

[0086] 本発明の第四の実施例の電子制御装置及び方法について説明する。第四の実施例は、ハイパーバイザ6の故障を所定の値以上の頻度で検出した場合に、電子制御装置をシャットダウンする点で第二の実施例と異なる。なお、第二の実施例と同じ構成については、同一の符号を付して、その説明を省略する。

[0087] 図21は、第四の実施例の監視結果保存プログラム20の処理フロー概要

を示す図である。

[0088] <監視結果保存プログラム20>

監視結果保存プログラム20は、ペリフェラルアクセス記録情報53とペリフェラル状態記録情報54とペリフェラル所望状態情報55をマイコン900のメモリ3の内部の不揮発メモリ領域に保存し、ハイパーバイザ6の異常発生頻度を計算し、計算された異常発生頻度が所定の閾値以上の場合に電子制御装置0をシャットダウンする。

[0089] <ステップS5>

ステップS5において、監視結果保存プログラム20は、ペリフェラルアクセス記録情報53とペリフェラル状態記録情報54とペリフェラル所望状態情報55をマイコン900のメモリ3の内部の不揮発メモリ領域に保存する。

[0090] <ステップS6>

ステップS6において、監視結果保存プログラム20は、ハイパーバイザ6に異常が発生した時刻を計算する。ハイパーバイザ6に実際に異常が発生した時刻をハイパーバイザ6の外部からの特定は困難であるため、異常が発生した時刻として、ハイパーバイザ監視プログラム17がハイパーバイザ6に異常が発生したと判定する根拠としたペリフェラル状態記録情報54とペリフェラル所望状態情報55に記載された時刻をハイパーバイザ6に異常が発生した時刻とする。すなわち、ペリフェラル状態記録情報54とペリフェラル所望状態情報55が図14に示すものがある場合、ハイパーバイザ6に異常が発生した時刻は、時刻00:32:10と計算される。監視結果保存プログラム20は、この時刻をハイパーバイザ異常発生時刻情報58に保存する。

[0091] 図22は、第四の実施例のハイパーバイザ異常発生時刻情報58の例を示す図である。

[0092] <ハイパーバイザ異常発生時刻情報58>

ハイパーバイザ異常発生時刻情報58は、第四の実施例の電子制御装置の

監視結果保存プログラム20のステップS6で計算された時刻の情報を格納する。

[0093] <ハイパーバイザ異常発生頻度要件59>

ハイパーバイザ異常発生頻度要件59は、電子制御装置0をシャットダウンするための条件である。本実施例では、時間10:00以内にハイパーバイザ6の異常を2回検出とする。

[0094] 図23は、第四の実施例の監視結果保存プログラム20のステップS7における処理の概要を模式的に示す図である。

[0095] <ステップS7>

監視結果保存プログラム20は、ステップS7において、ハイパーバイザ6に異常が発生した頻度を計算する。ハイパーバイザ異常発生頻度要件59によって時間10:00以内のハイパーバイザ6の異常発生頻度が条件となっているため、最新の異常発生時刻から遡って時間10:00以内に発生したハイパーバイザ異常発生時刻の記録回数を計算する。図23を用いて説明する。時刻50:25において、最新の異常発生時刻は47:10であり、この時刻から遡って時間10:00、すなわち時刻37:10から時刻47:10の間に発生した回数はハイパーバイザ異常発生時刻情報58によれば1回であるため、頻度は1回であると計算される。時刻54:35において、最新の異常発生時刻は52:10であり、この時刻から遡って時間10:00、すなわち時刻42:10から時刻52:10の間に発生した回数は、ハイパーバイザ異常発生時刻情報58によれば2回であるため、頻度は2回であると計算される。

[0096] <ステップS8>

ステップS8において、監視結果保存プログラム20は、ステップS7で計算した異常発生頻度がハイパーバイザ異常発生頻度要件59で規定した値以上であれば、ステップS9に進み、そうでなければステップS9をスキップしてこの処理を終了する。

[0097] <ステップS9>

ステップS 9において、監視結果保存プログラム20は、マイコン900の自己リセット出力端子からリセット信号を出力する。これにより、電源回路901はマイコン900への電源供給を停止し、電子制御装置0はシャットダウンする。電子制御装置0の停止範囲は、その一部でも全部でもよい。

[0098] 本実施例によれば、ハイパーバイザ6に異常を検知した頻度が低ければ、電子制御装置の動作を継続して、当該電子制御装置や当該電子制御装置が搭載された車両への影響を抑制し、ハイパーバイザ6に異常を検知した頻度が高ければ、電子制御装置をシャットダウンして、ハイパーバイザ6に発生した異常が当該電子制御装置や当該電子制御装置が搭載された車両の安全に与える影響を低減でき、可用性と安全性を両立できる。

[0099] なお、本発明は前述した実施例に限定されるものではなく、添付した特許請求の範囲の趣旨内における様々な変形例及び同等の構成が含まれる。例えば、前述した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに本発明は限定されない。また、ある実施例の構成の一部を他の実施例の構成に置き換えてもよい。また、ある実施例の構成に他の実施例の構成を加えてもよい。また、各実施例の構成の一部について、他の構成の追加・削除・置換をしてもよい。

[0100] また、前述した各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等により、ハードウェアで実現してもよく、プロセッサがそれぞれの機能を実現するプログラムを解釈し実行することにより、ソフトウェアで実現してもよい。

[0101] 各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリ、ハードディスク、SSD (Solid State Drive) 等の記憶装置、又は、ICカード、SDカード、DVD等の記録媒体に格納することができる。

[0102] また、制御線や情報線は説明上必要と考えられるものを示しており、実装上必要な全ての制御線や情報線を示しているとは限らない。実際には、ほとんど全ての構成が相互に接続されていると考えてよい。

請求の範囲

- [請求項1] 電子制御装置であって、
- 第一の仮想ドライバにアクセスして、処理を実行する仮想マシンと、
- 、
- 前記第一の仮想ドライバから受信したペリフェラルアクセス要求に基づいて第一のペリフェラルの第一の実ドライバを呼び出すハイパーバイザと、
- 前記第一の仮想ドライバを呼び出して、前記ハイパーバイザへ送信したペリフェラルアクセス要求を記録するアクセス記録部と、
- 前記第一の実ドライバを呼び出して、前記第一のペリフェラルのレジスタの状態を記録する状態記録部と、
- 前記ハイパーバイザの動作を監視する監視部とを備え、
- 前記監視部は、前記アクセス記録部の記録と前記状態記録部の記録に基づいて、前記ハイパーバイザの異常を判定する電子制御装置。
- [請求項2] 請求項1に記載の電子制御装置であって、
- 前記監視部は、前記アクセス記録部の記録と前記状態記録部の記録が整合しない場合、前記ハイパーバイザが異常であると判定する電子制御装置。
- [請求項3] 請求項2に記載の電子制御装置であって、
- 前記状態記録部は、所定のタイミングで繰り返し前記レジスタの状態を取得することを特徴とする電子制御装置。
- [請求項4] 請求項2に記載の電子制御装置であって、
- 前記監視部は、前記アクセス記録部にアクセス要求の記録があり、前記実ドライバの処理結果を前記仮想ドライバへ正常に返答した記録があり、かつ前記状態記録部のレジスタの状態が変化しない場合に、前記ハイパーバイザが異常であると判定する電子制御装置。
- [請求項5] 請求項1に記載の電子制御装置であって、
- 前記監視部が異常を判定した場合、前記アクセス記録部の記録及び

前記状態記録部の記録を不揮発に保存する監視結果保存部を備える電子制御装置。

[請求項6] 請求項5に記載の電子制御装置であって、
前記監視結果保存部は、前記ハイパーバイザが異常であると判定された頻度が所定の閾値以上である場合、前記電子制御装置の一部又は全部を停止する電子制御装置。

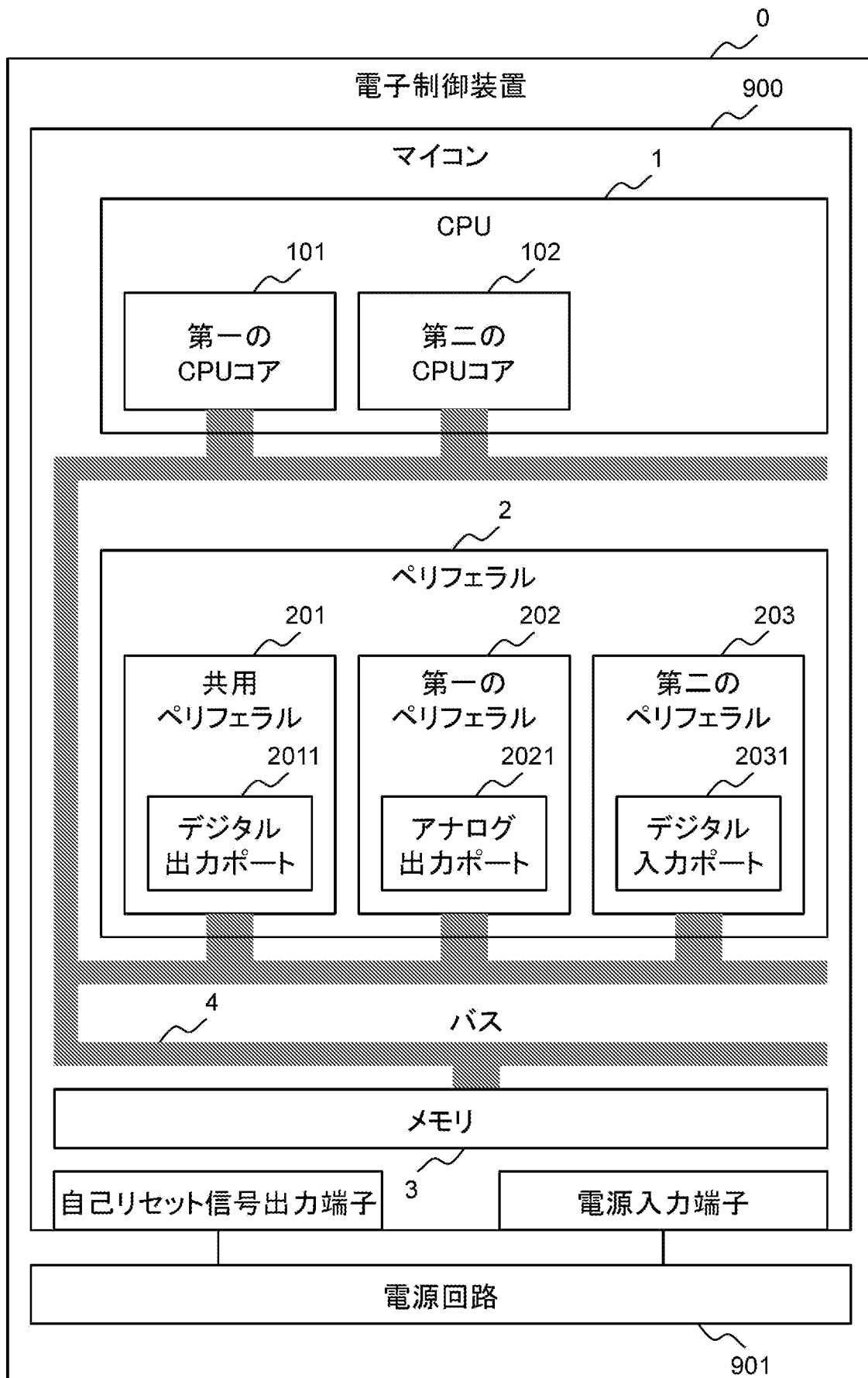
[請求項7] 請求項1に記載の電子制御装置であって、
前記第一のペリフェラルと異なる第二のペリフェラルと、
前記第二のペリフェラルを操作するための第二の実ドライバを備え、
前記第二のペリフェラルは、前記第二の実ドライバの指示に従って、
前記アクセス記録部の記録を前記仮想マシンの外部に出力し、
前記監視部は、前記仮想マシンの外部に出力された前記アクセス記録部の記録を参照する電子制御装置。

[請求項8] 電子制御装置で動作するハイパーバイザの異常判定方法であって、
前記電子制御装置は、
第一の仮想ドライバにアクセスして、処理を実行する仮想マシンと、
前記第一の仮想ドライバから受信したペリフェラルアクセス要求に基づいて第一のペリフェラルの第一の実ドライバを呼び出すハイパーバイザと、
前記第一の仮想ドライバを呼び出して、前記ハイパーバイザへ送信したペリフェラルアクセス要求を記録するアクセス記録部と、
前記第一の実ドライバを呼び出して、前記第一のペリフェラルのレジスタの状態を記録する状態記録部と、
前記ハイパーバイザの動作を監視する監視部とを有し、
前記異常判定方法は、
前記状態記録部が、前記第一の実ドライバを呼び出して、前記第一

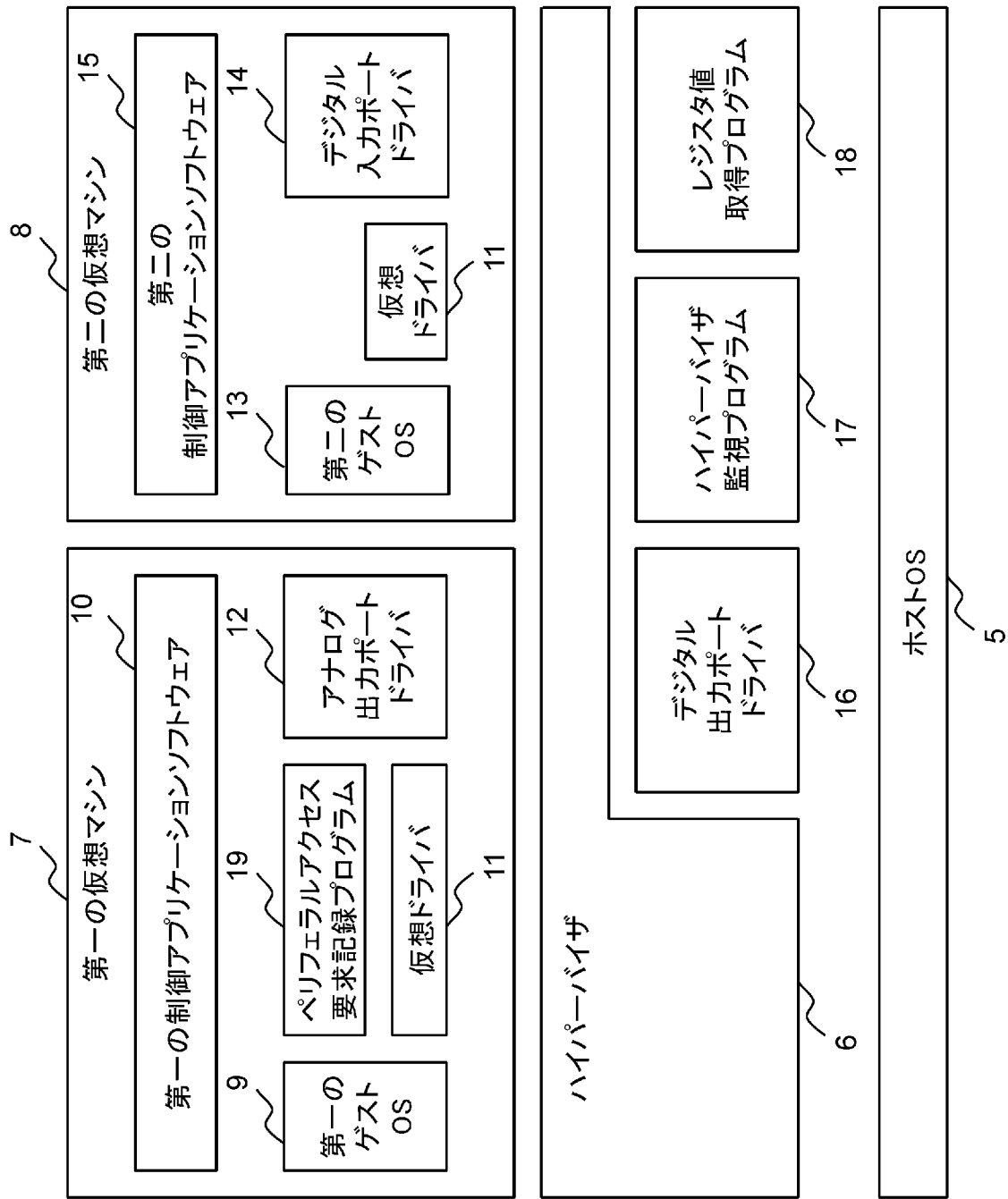
のペリフェラルのレジスタの状態を記録し、

前記監視部が、前記アクセス記録部の記録と前記状態記録部の記録に基づいて、前記ハイパーバイザの異常を判定する異常判定方法。

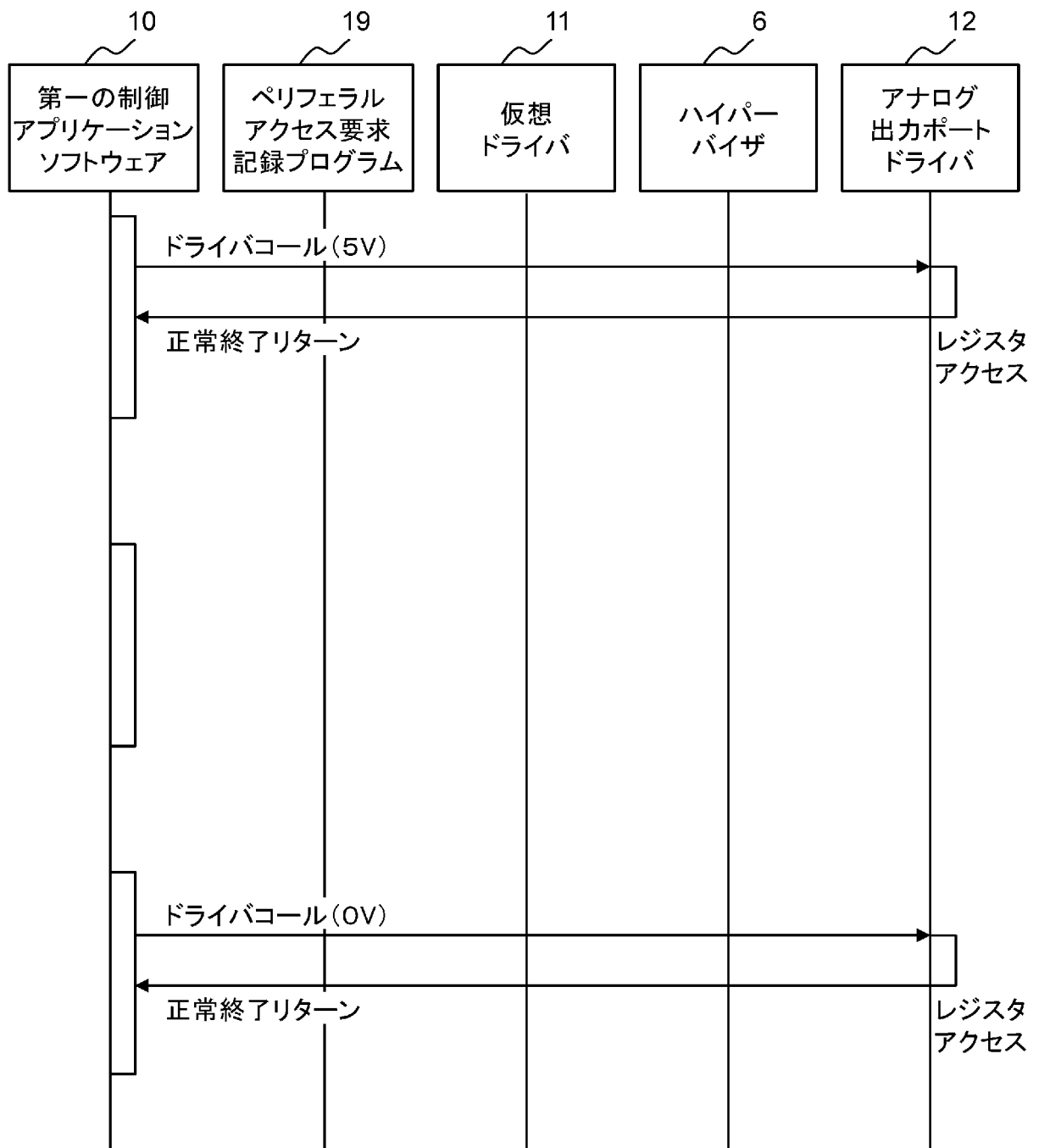
[図1]



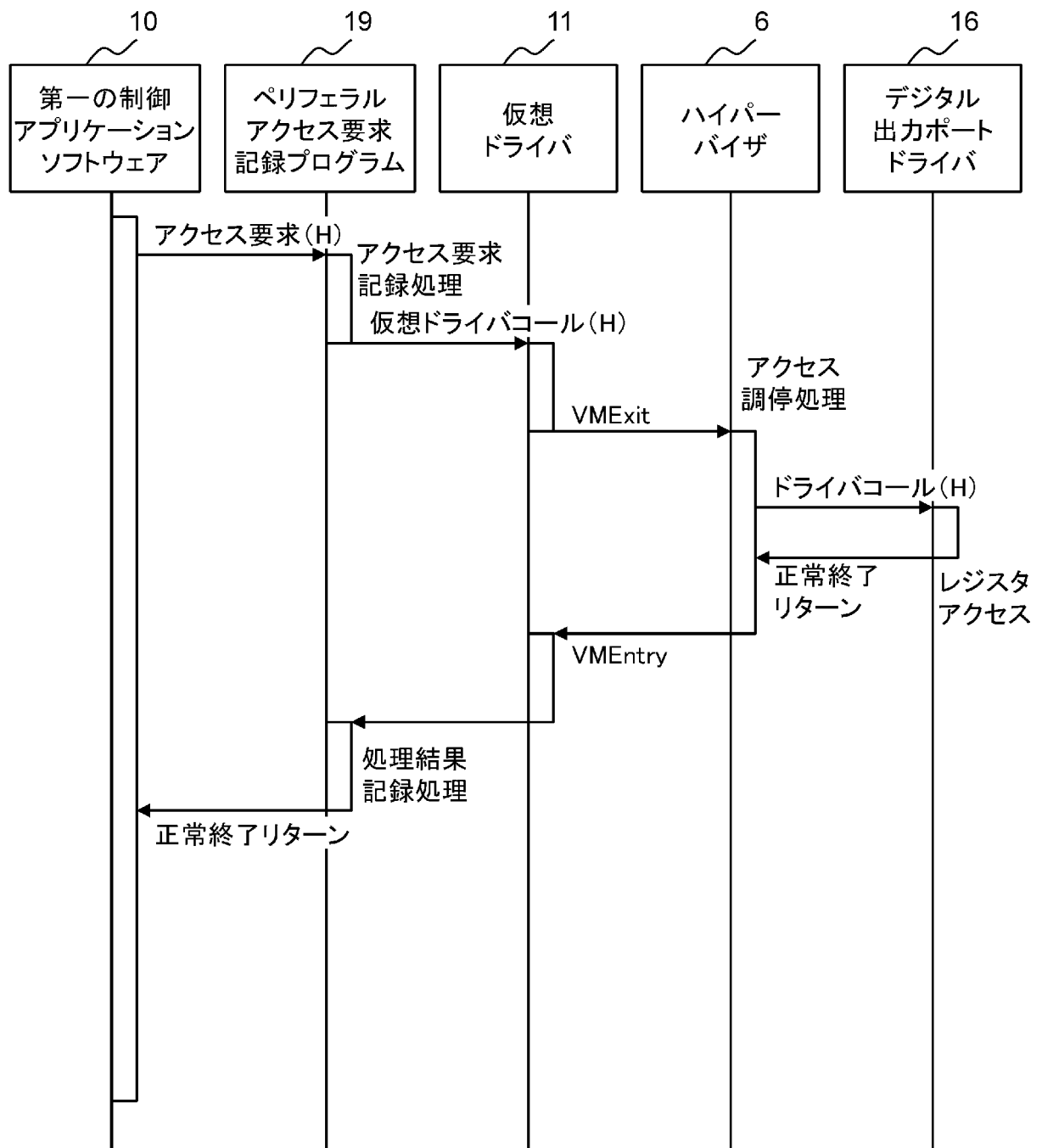
[図2]



[図3]



[図4]



[図5]

51

アクセス要求時刻	送信対象	引数
00:10:00	デジタル出力ポート	H
00:25:00	デジタル出力ポート	L
00:41:00	デジタル出力ポート	L

ペリフェラルアクセス要求情報

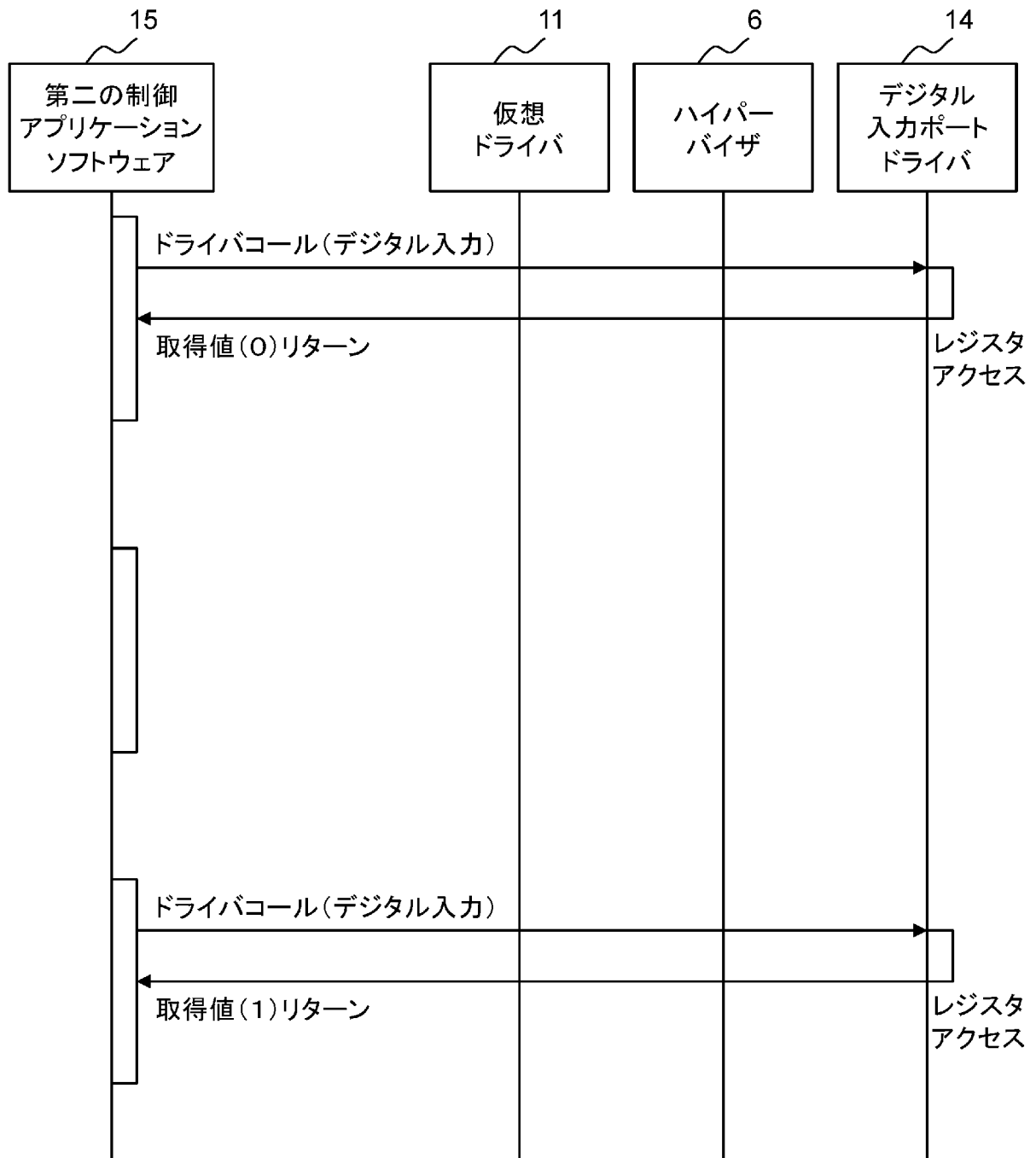
[図6]

52

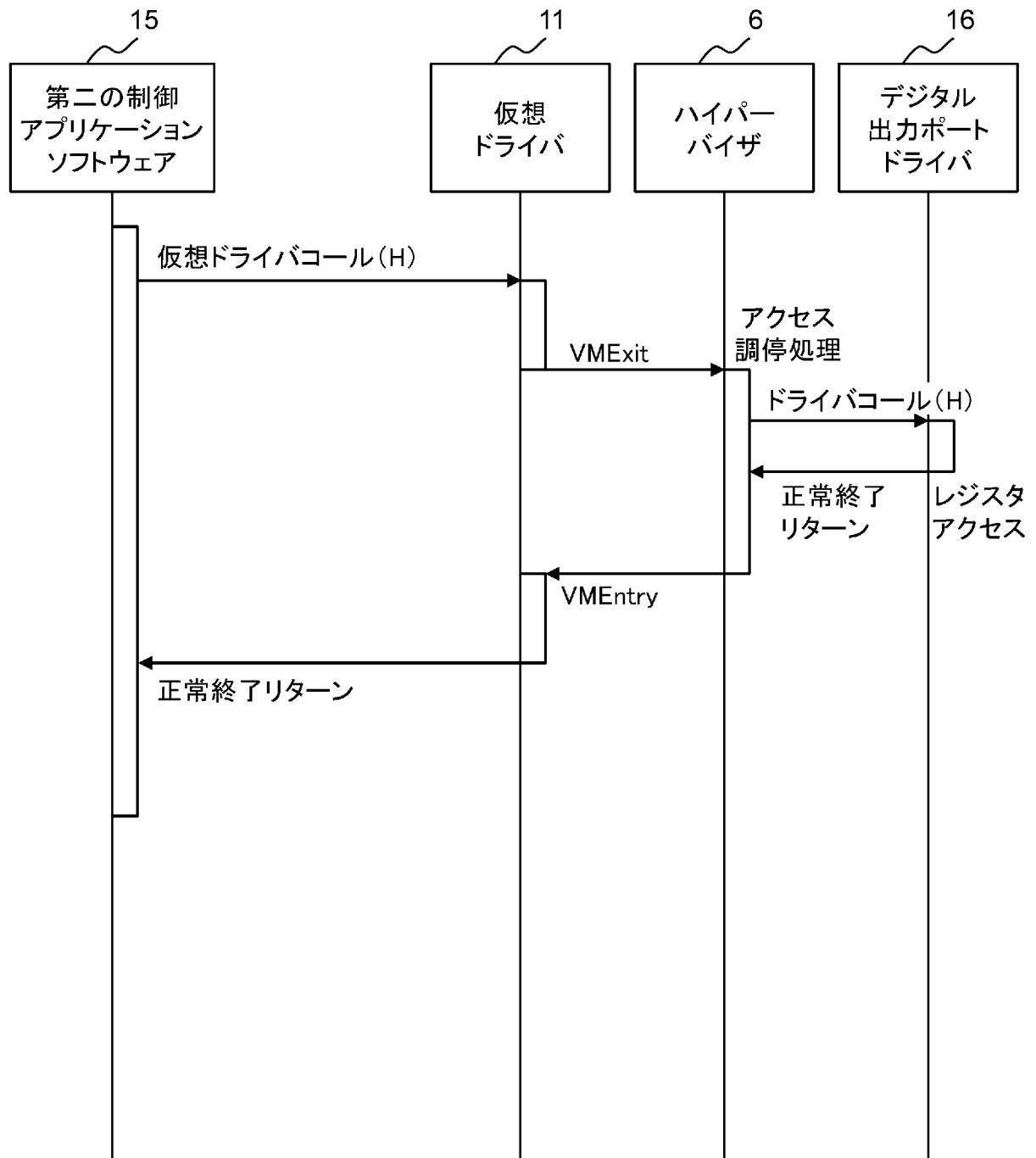
ハイパーバイザ 返答時刻	処理対象	処理結果
00:16:00	デジタル出力ポート	正常終了
00:32:00	デジタル出力ポート	正常終了

ペリフェラルアクセス結果情報

[図7]



[図8]



[図9]

53

アクセス 要求時刻	処理対象	引数	ハイパーバイザ 返答時刻	処理結果
00:10:00	デジタル 出力ポート	H	00:16:00	正常終了
00:25:00	デジタル 出力ポート	L	00:32:00	正常終了
00:41:00	デジタル 出力ポート	L		

ペリフェラルアクセス記録情報

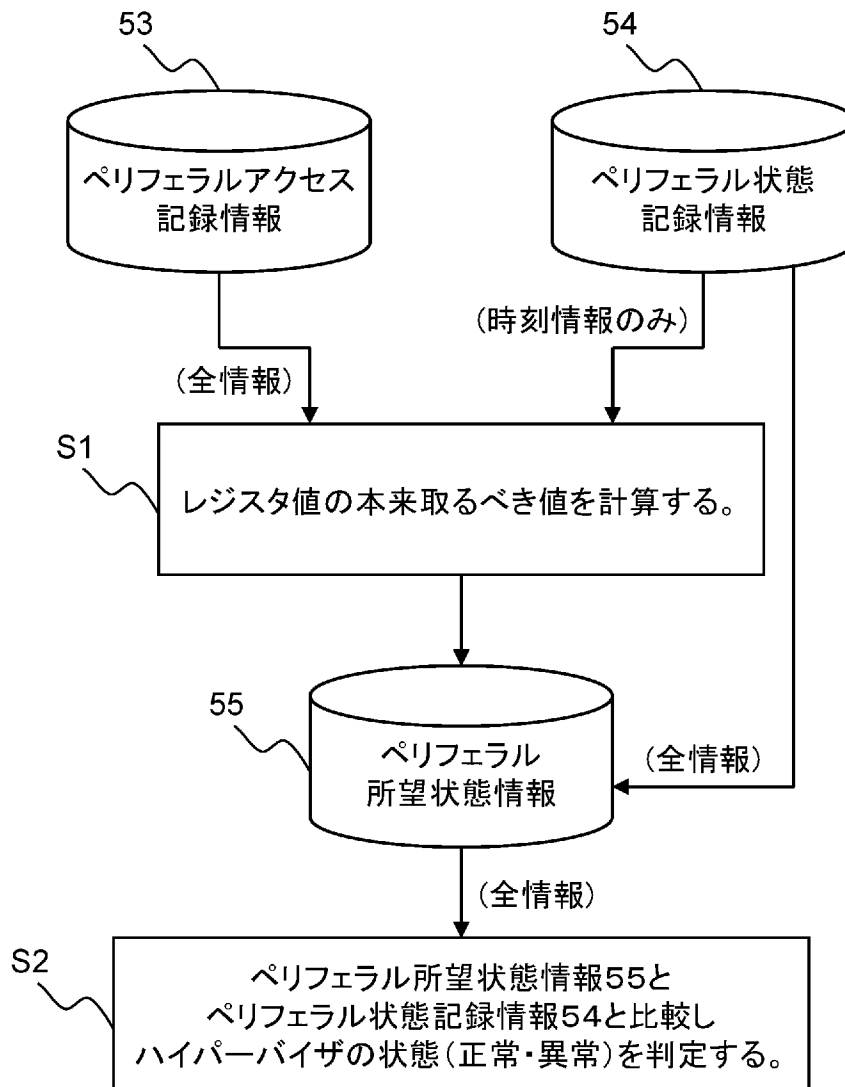
[図10]

54

状態確認時刻	処理対象	レジスタ値
00:12:10	デジタル出力ポート	H
00:17:10	デジタル出力ポート	H
00:22:10	デジタル出力ポート	H
00:27:10	デジタル出力ポート	H
00:32:10	デジタル出力ポート	H
00:37:10	デジタル出力ポート	H

ペリフェラル状態記録情報

[図11]



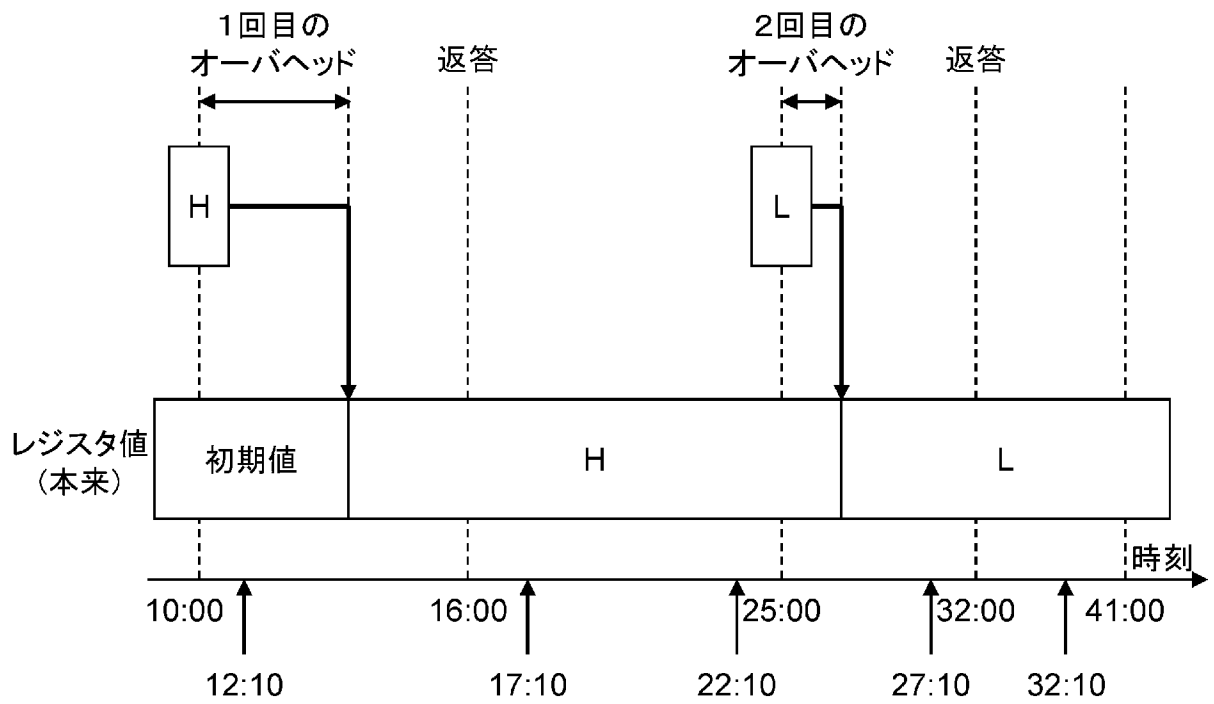
[図12]

55

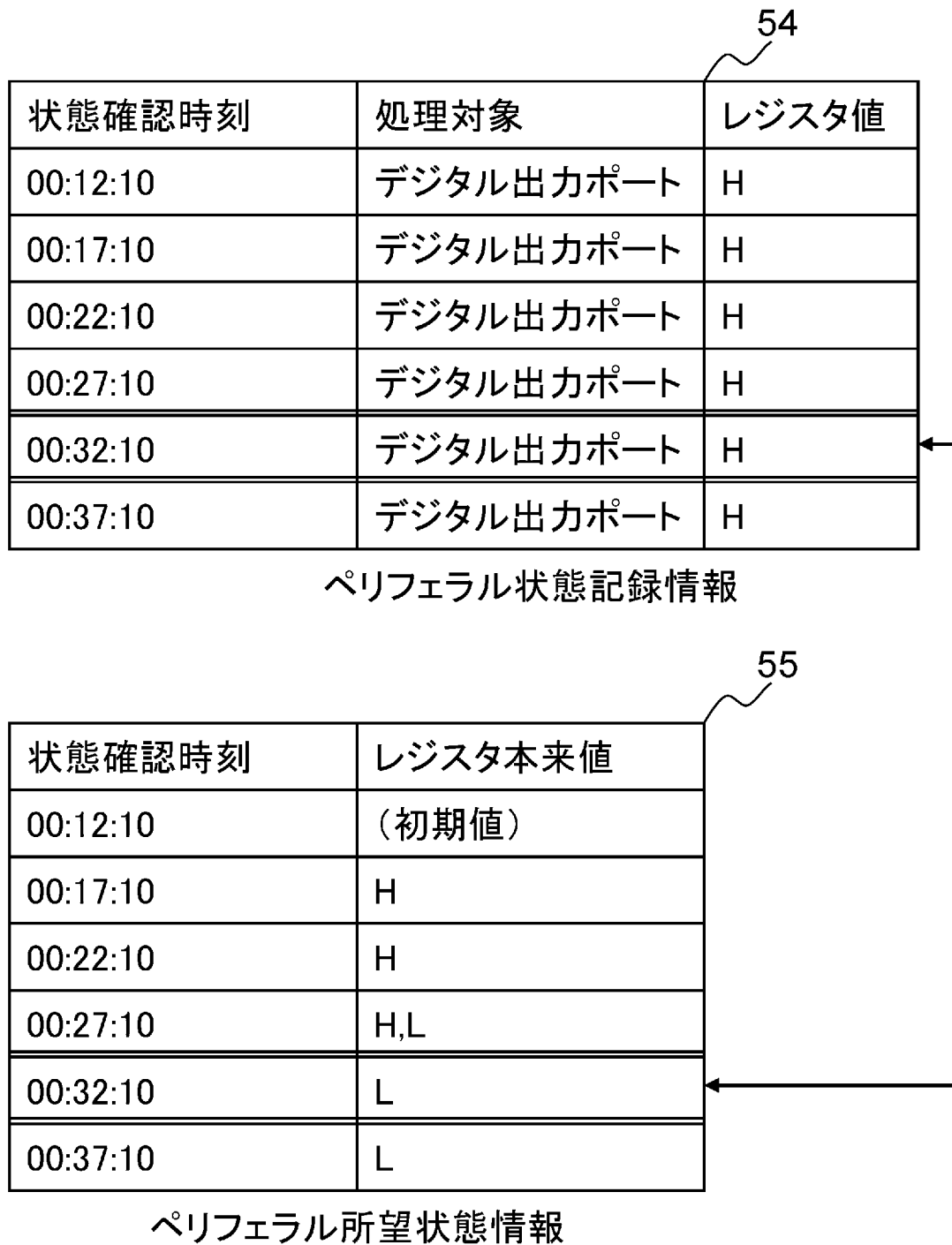
状態確認時刻	レジスタ本来値
00:12:10	(初期値)
00:17:10	H
00:22:10	H
00:27:10	H,L
00:32:10	L
00:37:10	L

ペリフェラル所望状態情報

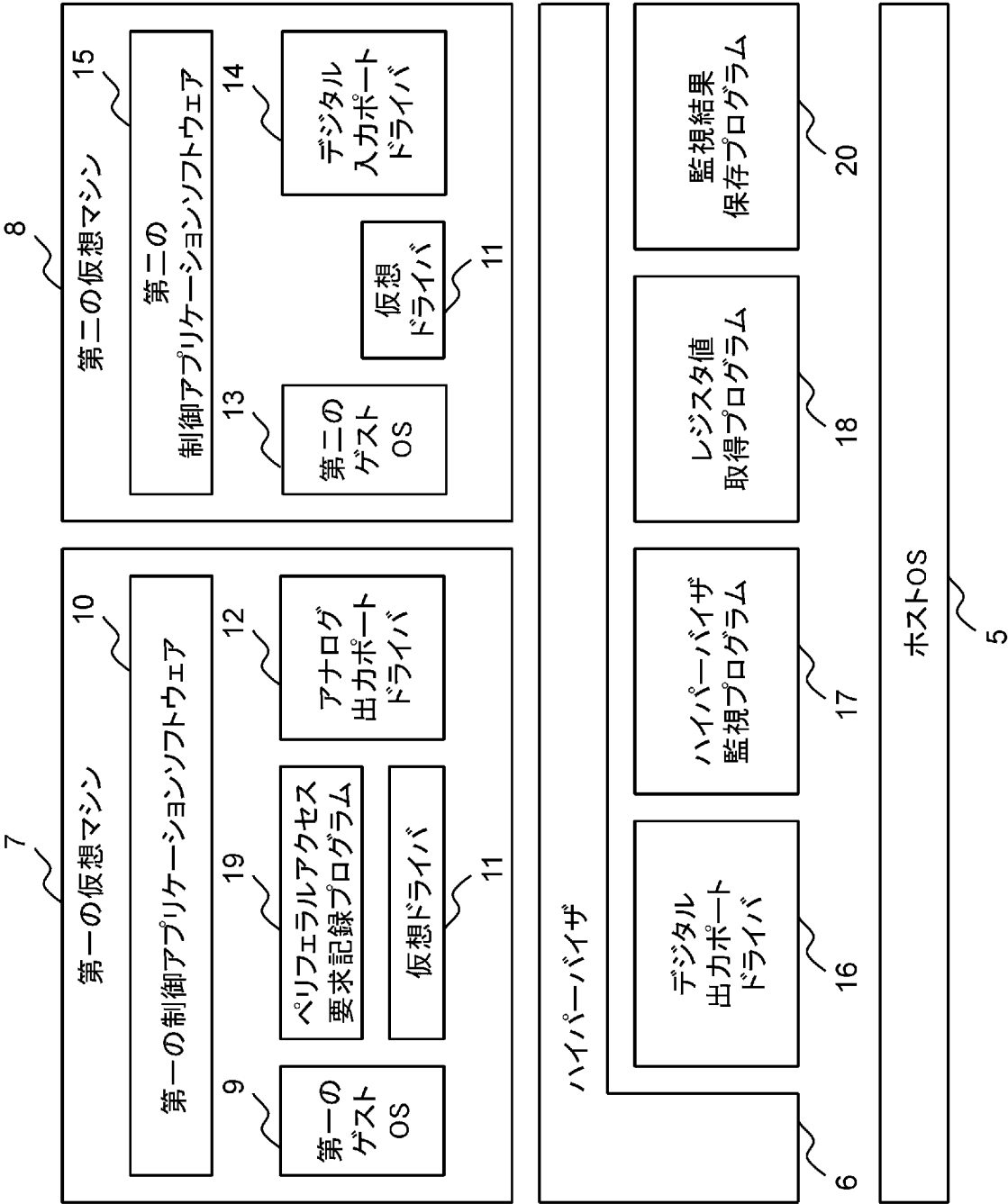
[図13]



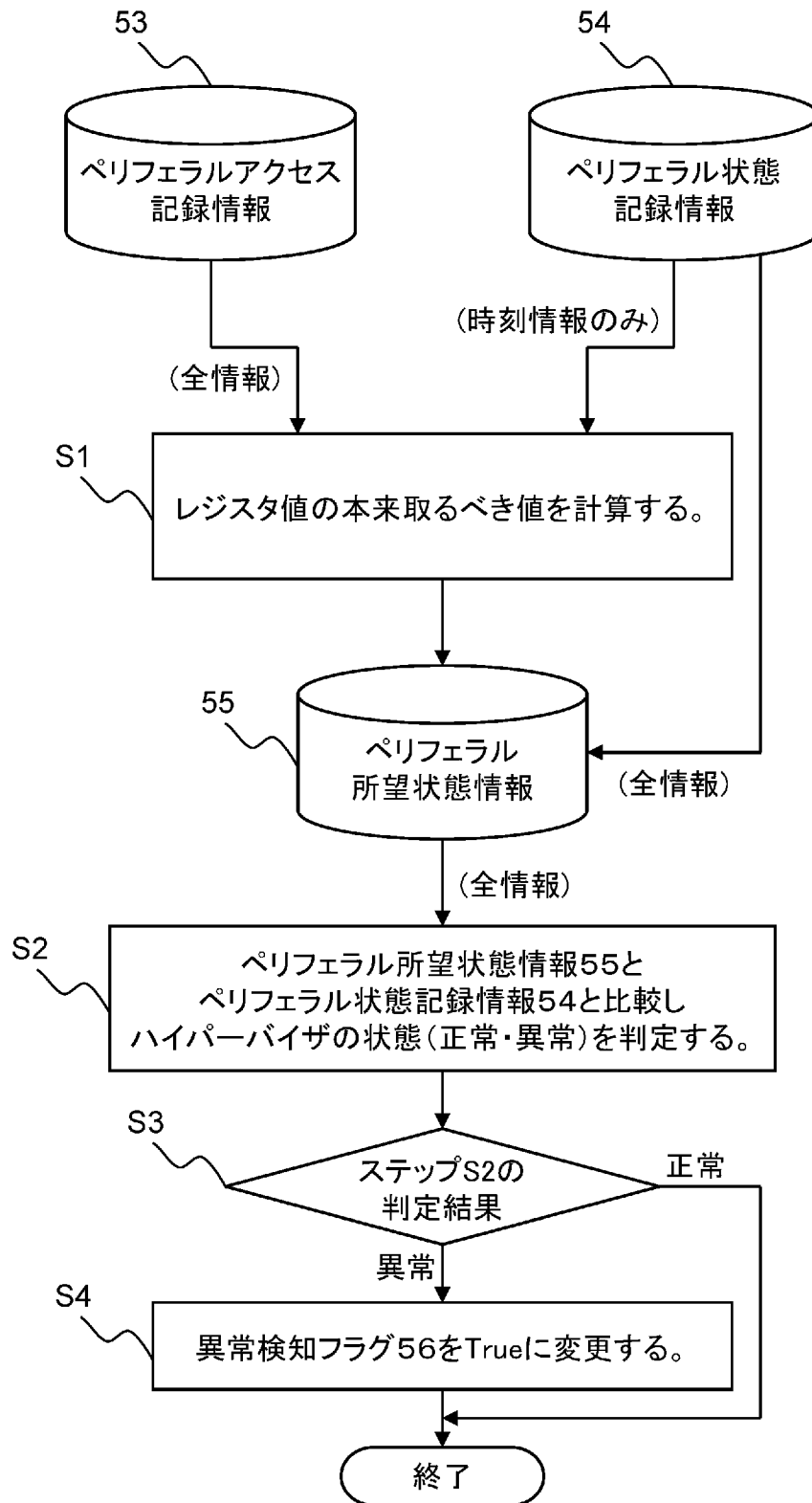
[図14]



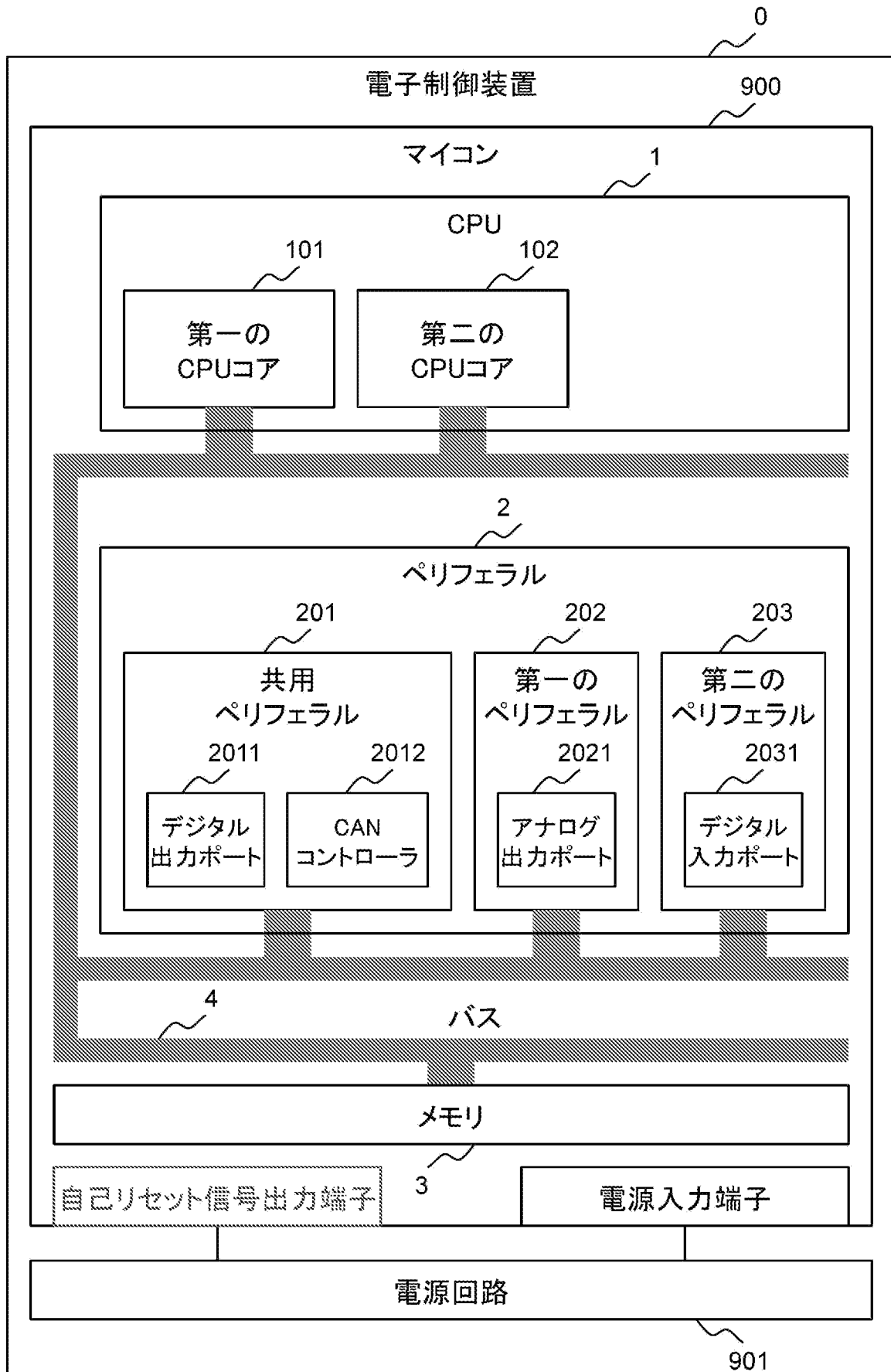
[図15]



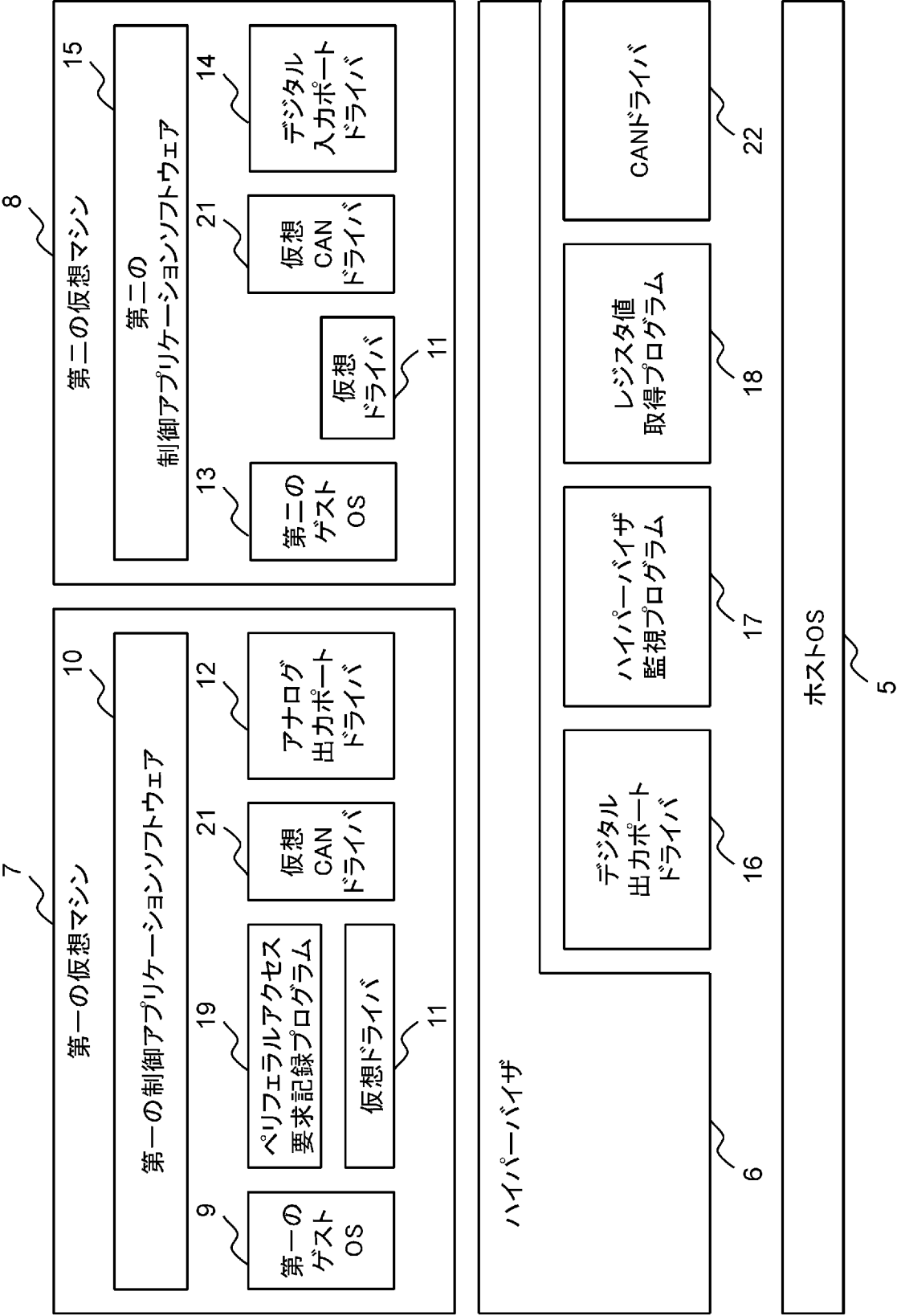
[図16]



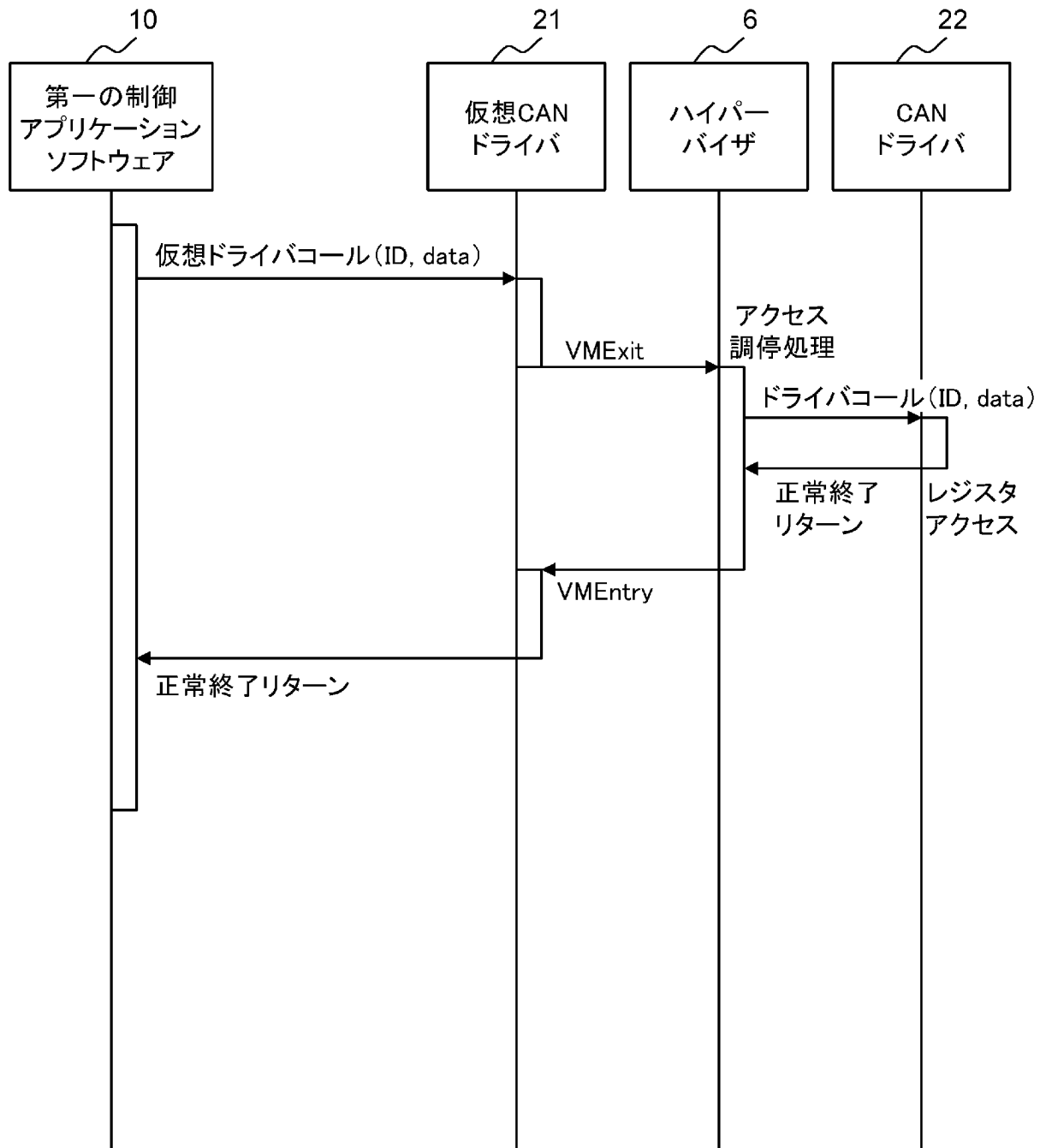
[図17]



[図18]



[図19]



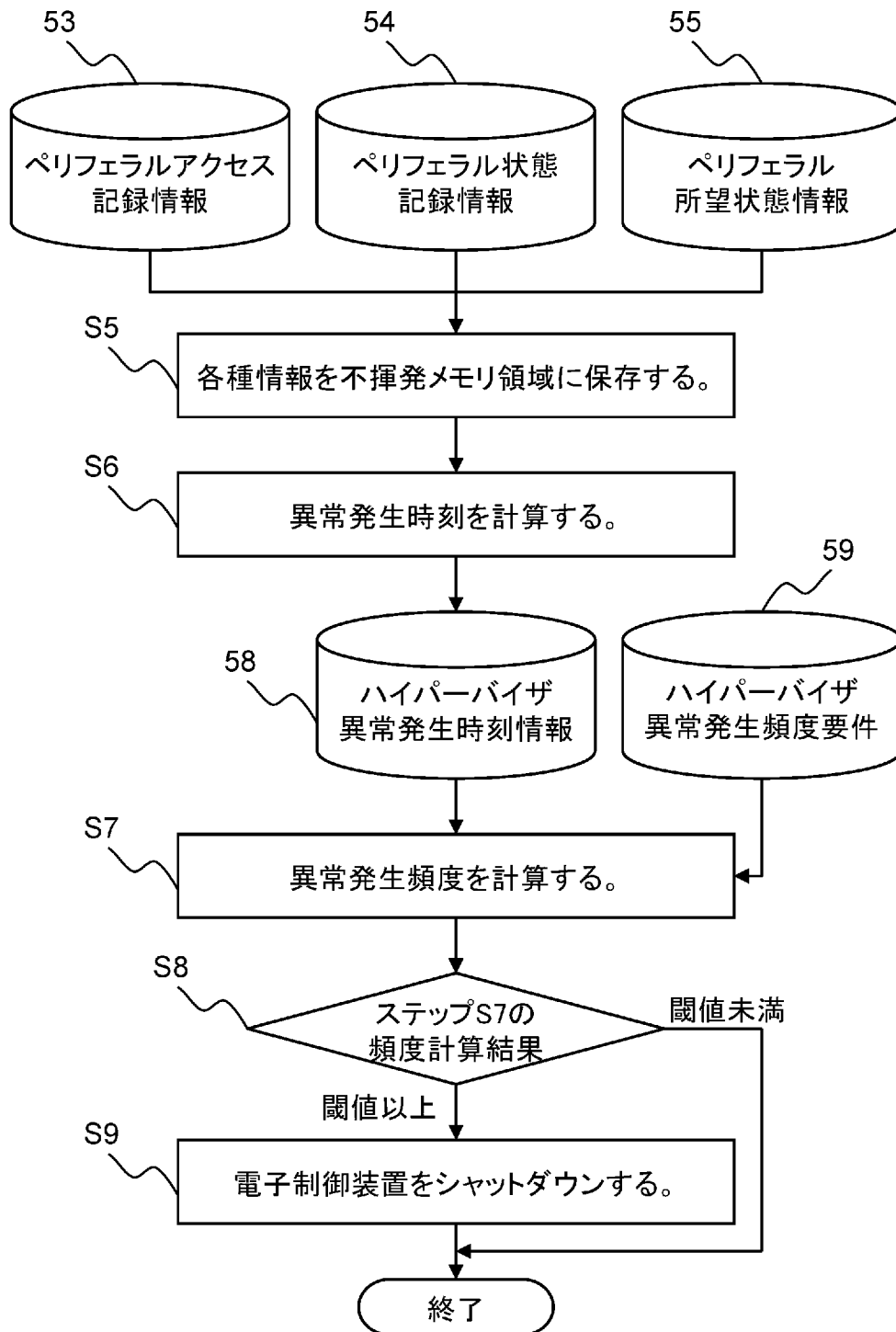
[図20]

57

メッセージ ID	データの内容	送信・受信	データ長
0	車両速度	受信	8バイト
1	エンジン回転数	送信	8バイト
2	スロットル開度	送信	8バイト
...	...		...
2000	ステアリング角度	受信	8バイト
9900	ペリフェラル状態記録 情報54における状態 確認時刻と処理対象と レジスタ値の組	監視部送信	8バイト

CAN台帳

[図21]



[図22]

58

異常発生時刻
00:32:10

[図23]

現在時刻 00:50:25	異常発生時刻 00:32:10 00:47:10
-------------------------------------	---

58

現在時刻 00:54:35	異常発生時刻 00:32:10 00:47:10 00:52:10
-------------------------------------	---

58

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2022/004527

A. CLASSIFICATION OF SUBJECT MATTER**G06F 11/07**(2006.01)i; **G06F 9/455**(2006.01)i

FI: G06F11/07 151; G06F11/07 140C; G06F9/455 150

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)

G06F11/07; G06F9/455

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2022

Registered utility model specifications of Japan 1996-2022

Published registered utility model applications of Japan 1994-2022

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 2006-268687 A (MITSUBISHI ELECTRIC CORP.) 05 October 2006 (2006-10-05) paragraphs [0013]-[0016]	1-8
A	JP 2014-178975 A (NEC CORP.) 25 September 2014 (2014-09-25) paragraphs [0019]-[0023]	1-8
A	JP 2019-144785 A (FUJITSU LTD.) 29 August 2019 (2019-08-29) paragraphs [0011]-[0023]	1-8
A	JP 2010-122736 A (RICOH CO., LTD.) 03 June 2010 (2010-06-03) abstract	1-8

☐ 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

12 April 2022

Date of mailing of the international search report

19 April 2022

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2022/004527

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2006-268687	A	05 October 2006	(Family: none)	
JP	2014-178975	A	25 September 2014	(Family: none)	
JP	2019-144785	A	29 August 2019	(Family: none)	
JP	2010-122736	A	03 June 2010	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 11/07(2006.01)i; G06F 9/455(2006.01)i FI: G06F11/07 151; G06F11/07 140C; G06F9/455 150														
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（IPC）） G06F11/07; G06F9/455														
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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2022年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2022年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2022年</td> </tr> </table>			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2022年	日本国実用新案登録公報	1996 - 2022年	日本国登録実用新案公報	1994 - 2022年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2022年													
日本国実用新案登録公報	1996 - 2022年													
日本国登録実用新案公報	1994 - 2022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 2006-268687 A（三菱電機株式会社）05.10.2006（2006 - 10 - 05） paras. [0013]-[0016]	1-8												
A	JP 2014-178975 A（日本電気株式会社）25.09.2014（2014 - 09 - 25） paras. [0019]-[0023]	1-8												
A	JP 2019-144785 A（富士通株式会社）29.08.2019（2019 - 08 - 29） paras. [0011]-[0023]	1-8												
A	JP 2010-122736 A（株式会社リコー）03.06.2010（2010 - 06 - 03） abstract	1-8												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 12.04.2022	国際調査報告の発送日 19.04.2022													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 金木 陽一 5B 4876 電話番号 03-3581-1101 内線 3545													

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2022/004527

引用文献			公表日	パテントファミリー文献	公表日
JP	2006-268687	A	05.10.2006	(ファミリーなし)	
JP	2014-178975	A	25.09.2014	(ファミリーなし)	
JP	2019-144785	A	29.08.2019	(ファミリーなし)	
JP	2010-122736	A	03.06.2010	(ファミリーなし)	