

(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6月23日(23.06.2022)



(10) 国際公開番号

WO 2022/130699 A1

- (51) 国際特許分類:
B60R 16/02 (2006.01) *G06F 8/65* (2018.01)
- (21) 国際出願番号: PCT/JP2021/031847
- (22) 国際出願日: 2021年8月31日(31.08.2021)
- (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 2020-208372 2020年12月16日(16.12.2020) 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: 角屋 孝介(SUMIYA Kosuke); 〒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). 衣笠 駿

(KINUGASA Shun); 〒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). 阿部 雄介(ABE Yusuke); 〒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). 弘中 篤史(HIRONAKA Atsushi); 〒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).

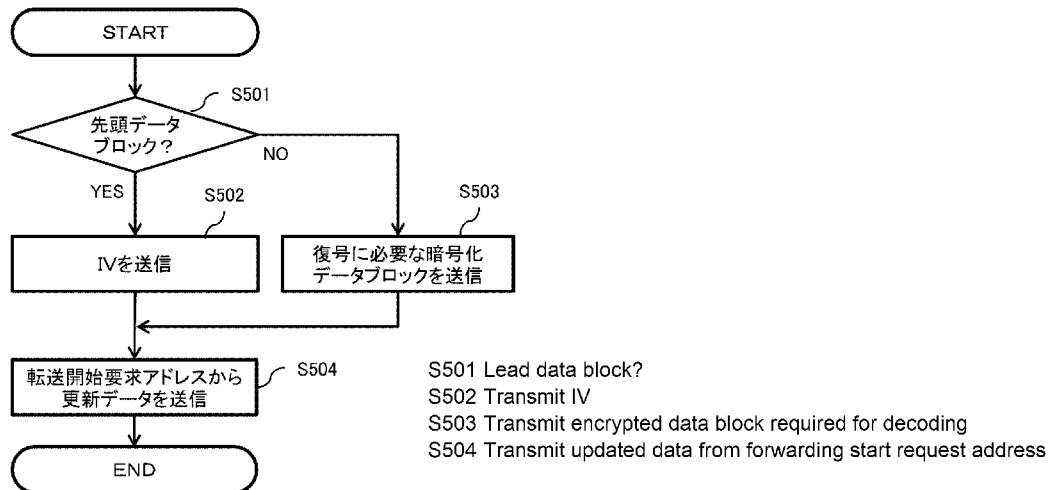
(74) 代理人: 特許業務法人平木国際特許事務所 (HIRAKI & ASSOCIATES); 〒1056232 東京都港区愛宕二丁目 5 - 1 愛宕グリーンヒルズ MORI タワー 3 2 階 Tokyo (JP).

(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,

(54) Title: ELECTRONIC CONTROL DEVICE

(54) 発明の名称: 電子制御装置

図 5



(57) Abstract: The purpose of the present invention is to provide a feature which, even when updated data to be written to an ECU is encrypted, is capable of appropriately resuming the writing processing when determined that the writing processing was interrupted while in progress. An electronic control device according to the present invention, wherein a first data block included in the updated data is encrypted by using a second data block, and when the writing processing for writing the first data block to the storage unit is interrupted while in progress, updated data which includes both the first data block and the second data block is reacquired, after which the first data block is decoded again by using the reacquired second data block.

HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, 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))

(57) 要約：本発明は、E C Uに対して書き込む更新版データが暗号化されている場合であっても、書き込み処理が途中中断したときその書き込み処理を適切に再開することができる技術を提供することを目的とする。本発明に係る電子制御装置において、更新データ内に含まれる第1データブロックは第2データブロックを用いて暗号化されており、前記第1データブロックを前記記憶部に対して書き込む書込処理が途中中断した場合は、前記第1データブロックと前記第2データブロックをともに含む前記更新データを再取得した上で、前記再取得した前記第2データブロックを用いて前記第1データブロックを再復号する。

明 細 書

発明の名称：電子制御装置

技術分野

[0001] 本発明は、車両に搭載される電子制御装置に関する。

背景技術

[0002] ECU (Electrical Control Unit) などの車載電子制御装置は、マイクロコンピュータ（以下、マイコン）により制御されている。マイコンには様々な機能が割り当てられており、さらにそれらに対応した外部回路が設けられている。ECUは、不揮発性メモリであるフラッシュROM (Read Only Memory) に記憶されている制御ソフトウェアを実行することにより、対象装置を制御する。自動車においては、例えば、エンジンの燃料噴射・点火を制御する。

[0003] ECUは一般に、ECUに搭載されているメモリに書き込まれている制御ソフトウェアを書き換える手段を有する。例えば以下のような手段がある：
(1) OBD (On-Board Diagnostic) コネクタを介して有線で診断ツールをECUへ接続し、CAN (Controller Area Network) などの信号によってフラッシュROMに書き込むデータを送信する方式（従来からの方式）；(2) OTA (Over-The-Air)：無線通信によって更新版データをECUへ送信する方式。

[0004] OTAによるソフトウェア書き換えにおいては、車両走行中に更新版データを受領することがある。この方式においては、実行中の他の制御に影響を与えないように、バックグラウンドで少しずつデータを転送する必要がある。このとき、ソフトウェア書き換えの時間が長くなり、例えばユーザによって電源供給が断たれてしまうなどの要因によって、プロセスが中断される可能性がある。このようなケースにおいて、ソフトウェア書き換えを中断しても途中から開始するリジューム機能が求められている。

[0005] 下記特許文献1は、ソフトウェア書き換えのリジューム機能について記載

している。同文献においては、ソフトウェア書き換え中断後にデータ転送元からECUへソフトウェア書き換え開始アドレスを要求する。

先行技術文献

特許文献

[0006] 特許文献1：特開2017-097576号公報

発明の概要

発明が解決しようとする課題

[0007] ECUのソフトウェア書き換えにおいては、診断ツールなどのデータ転送元と、書き換え対象のECUとの間で通信する。特にOTA方式においては、無線通信を用いてデータを転送するので、セキュリティの観点から転送データを暗号化することの重要性が高まっている。

[0008] 暗号化されていないデータを使ったソフトウェア書き換えをリジュームする場合、特許文献1のようにソフトウェア書き換え完了済みのデータ位置から再開すればよい。したがって、中断後はデータ転送元からの再開位置問い合わせメッセージに対して、書き換え完了済み位置の次のアドレスを開始アドレスとして返答すればよい。

[0009] 他方で更新版データが暗号化されている場合は、転送データをいくつかのデータブロックに分割してそのデータブロックごとに暗号化を施し、データブロックごとに順次ECUへ送信する。データを受け取ったECU側では、復号処理のために別の情報（例えば、転送開始データブロックの1つ前の暗号化データブロック）が必要になる。そうすると、特許文献1のように再送するデータアドレスを通知するのみでは、暗号化されたデータブロックをECU側において復号することができない。

[0010] 本発明は、上記のような課題に鑑みてなされたものであり、ECUに対して書き込む更新版データが暗号化されている場合であっても、書き込み処理が途中中断したときその書き込み処理を適切に再開することができる技術を提供することを目的とする。

課題を解決するための手段

[0011] 本発明に係る電子制御装置において、更新データ内に含まれる第1データブロックは第2データブロックを用いて暗号化されており、前記第1データブロックを前記記憶部に対して書き込む書込処理が途中中断した場合は、前記第1データブロックと前記第2データブロックをともに含む前記更新データを再取得した上で、前記再取得した前記第2データブロックを用いて前記第1データブロックを再復号する。

発明の効果

[0012] 本発明に係る電子制御装置によれば、ECUに対して書き込む更新版データが暗号化されている場合であっても、書き込み処理が途中中断したときその書き込み処理を適切に再開することができる。

図面の簡単な説明

- [0013] [図1]実施形態1に係る電子制御装置（ECU）1の構成図である。
[図2]更新データ3を暗号化する様子を示す模式図である。
[図3]グローバルヘッダ31の構成図である。
[図4]プログラム更新におけるリジューム処理を説明するフローチャートである。
[図5]更新データ送信部2が更新データ4を送信する処理を説明するフローチャートである。
[図6]S408の詳細を説明するフローチャートである。
[図7]S603の詳細を説明するフローチャートである。
[図8]実施形態2に係るECU1の構成図である。
[図9]実施形態3に係るECU1の構成図である。
[図10]実施形態4に係るECU1の構成図である。

発明を実施するための形態

[0014] <実施の形態1>

図1は、本発明の実施形態1に係る電子制御装置（ECU）1の構成図で

ある。ＥＣＵ１は、車両に搭載されている。ＥＣＵ１は、車両が搭載している機器を制御する。車載機器の例としては、エンジン、パワーステアリング装置、制御ブレーキ装置、などが挙げられる。ＥＣＵ１は、車載機器を制御する処理を実装した制御プログラムを実行することにより、これら機器を制御する。

[0015] ＥＣＵ１は、マイコン１１を備える。マイコン１１は、ソフトウェアを実行する少なくとも１つのＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｏｒ Ｕｎｉｔ）１２、少なくとも１つの揮発性ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１３、プログラムやデータを保持する少なくとも１つの不揮発性メモリ１５、少なくとも１つの通信部１４、を備える。通信部１４は、ＥＣＵ１の外部にある更新データ送信部２と接続されており、プログラム更新時には更新データ送信部２を介して更新データを受け取る。

[0016] 更新データ送信部２は、例えば、車両のデータ通信用コネクタに優先で接続されたプログラム更新用の端末であってもよいし、無線通信によってＥＣＵ１と通信するサーバコンピュータであってもよい。あるいは同じ車両が搭載している別のＥＣＵであってもよい。

[0017] 図２は、更新データ３を暗号化する様子を示す模式図である。更新データ３は、ＥＣＵ１が実行するプログラムなどの更新版を含むデータである。更新データ３は、例えばデータセンタなどからＥＣＵ１に対して無線通信によって送信される。更新データ３は、例えば不揮発性メモリ１５が格納するバイナリデータそのものとして構成されている。

[0018] 更新データ３は、グローバルヘッダ３１と、１以上のデータブロック（図２においてはデータブロック３２、３３、３Ｎを例示した）とによって構成されている。データブロックは、ローカルヘッダ部とボディ部によって構成されている（例えばデータブロック３２はローカルヘッダ３２１とボディ３２２によって構成されている）。各データブロックのサイズは同じであってもよいし異なってもよい。

[0019] データブロックのボディ部は、ＥＣＵ１に対して送信する前に圧縮される

。ローカルヘッダ部は圧縮されない。圧縮したボディ部に対してローカルヘッダが付与される。ローカルヘッダとボディのペアを連結して1つのデータを形成し、さらにグローバルヘッダ31を付与することにより、更新データ3が作成される。ローカルヘッダはデータブロックの付帯情報を記述しており、グローバルヘッダは更新データ3全体の付帯情報を記述している。これらヘッダの詳細については後述する。

[0020] 更新データ3は、ECU1に対して送信する前に暗号化され、更新データ4となる。更新データ4は、暗号化されたデータブロック（図2においてはデータブロック42、43、4Nを例示した）を有する。グローバルヘッダ31は暗号化されずにそのまま付与される。暗号アルゴリズムは、本実施形態においてはブロック暗号を用いるが、別のアルゴリズムでもよい。ブロック暗号アルゴリズムを使用する場合、更新データ4は、データブロックごとに暗号化した後、さらにある大きさのブロックごとに暗号化される。

[0021] ローカルヘッダは、暗号化してもよいしなくてもよい。すなわち、後述するように更新データ4内の各データブロックと、不揮発性メモリ15上の各データブロックの格納アドレスとの間の対応関係を特定することができればよい。換言すると、この対応関係はグローバルヘッダ31内に記述してもよいし、各ローカルヘッダ内に記述してもよい。前者の場合は、更新データ4内における各データブロックの開始アドレスをグローバルヘッダ31内に記述することにより、ECU1は更新データ4内の各データブロックと不揮発性メモリ15内の格納先アドレスとの間の対応関係を特定できるので、各ローカルヘッダを暗号化してもよい。後者の場合は、各ローカルヘッダは更新データ4内における次のローカルヘッダの位置を記述し、これを連続することによって更新データ4内の各データブロックの位置を特定する。データブロックのローカルヘッダは、不揮発性メモリ15内においてそのデータブロックを格納すべき位置（アドレス）を特定することができる情報を記述する。これによりECU1は、更新データ4内の各データブロックと不揮発性メモリ15内の格納先アドレスとの間の対応関係を特定できる。いずれの場

合においても、グローバルヘッダ 31 は暗号化されない。

[0022] ローカルヘッダは、必ずしもデータブロックの先頭に配置する必要はなく、例えばデータブロックの末尾に配置してもよいし、先頭と末尾との間の任意位置に配置してもよい。ローカルヘッダが次のデータブロックの位置を指定する方法としては、次のデータブロックのボディの先頭を指定してもよいし、次のデータブロックのローカルヘッダ（ただしローカルヘッダがデータブロックの先頭に配置されている場合に限る）を指定してもよい。

[0023] 図 3 は、グローバルヘッダ 31 の構成図である。グローバルヘッダ 31 は、ROM 情報 311、リジュームアドレス 312、IV (Initial Vector) 313 を有する。ここではグローバルヘッダ 31 内にデータブロックと不揮発性メモリ 15 内の格納先アドレスとの間の関係（すなわちリジュームアドレス 312）を格納する例を示した。

[0024] ROM 情報 311 は、更新データ 3 を構成するブロックの個数、更新データ 3 のサイズ、圧縮・暗号化アルゴリズムを示すコード、などの情報である。リジュームアドレス 312 は、更新データ 3 内の各データブロックの先頭アドレスと、不揮発性メモリ 15 内の当該データブロックを書き込むアドレスとの間の対応関係を記述している。不揮発性メモリ 15 内のアドレスそのものを記述してもよいし、不揮発性メモリ 15 内のアドレスを特定できる他の情報を記述してもよい。IV 313 は、ブロック暗号において最初の暗号化データブロック（図 2 においてはデータブロック 42）を復号するために必要となる情報である。ROM 情報 311 やリジュームアドレス 312 は、ローカルヘッダに含めてもよい。IV 313 はグローバルヘッダ 31 内に含めず、あらかじめ不揮発性メモリ 15 に保存しておいてもよい。

[0025] グローバルヘッダ 31 が記述している更新データ 3 内のアドレスは、更新データ 4 においても同じ値が用いられる（グローバルヘッダ 31 は更新データ 3 と 4 との間で共通であるため）。したがって、更新データ 3 を暗号化するとき、各データブロックのサイズを変えないことが望ましい。例えばデータブロックのサイズが変わらない暗号化アルゴリズムを用いることが望まし

い。ブロック暗号はその１例である。これに対して更新データ３を暗号化するとき、各データブロックのサイズが変化する場合は、その変化をリジュームアドレス３１２に対して反映する必要がある。

[0026] グローバルヘッダ３１内の各情報の一部またはすべては、更新データ送信部２を介してＥＣＵ１に対して送信された後、不揮発性メモリ１５内に保存される。本実施形態においては、ＥＣＵ１が更新データ４を受け取ったとき、リジュームアドレス３１２が不揮発性メモリ１５内に保存され、グローバルヘッダ３１内の他の情報は保存されないものとするが、これに代えてあるいはこれに加えて、例えばＩＶ３１３を不揮発性メモリ１５内に保存してもよい。

[0027] 図４は、プログラム更新におけるリジューム処理を説明するフローチャートである。以下図４の各ステップを説明する。

[0028] (図４：ステップＳ４０１)

リジューム処理がスタートすると、更新データ送信部２はＥＣＵ１に対して、更新データ４の転送開始アドレスを送信するように要求する。転送開始アドレスは、例えば更新データ４を不揮発性メモリ１５へ書き込む処理が途中中断された場合、更新データ４のうちどこからＥＣＵ１に対して再送するかを指定するアドレスである。途中中断していない場合は先頭アドレスを指定すればよい。

[0029] (図４：ステップＳ４０２)

ＣＰＵ１２は、不揮発性メモリ１５に対して最初に書き込むデータブロックが、更新データ４の先頭データブロックであるか否かを判定する。この判定は、後述する書き込み完了ブロック情報を参照することにより、実施できる。先頭データブロックをこれから書き込む場合はＳ４０３へ進み、先頭データブロック以外のデータブロックをこれから書き込む場合はＳ４０４へ進む。

[0030] (図４：ステップＳ４０３、Ｓ４０７)

ＣＰＵ１２は、転送開始要求アドレスを更新データ４の先頭にセットする

(S403)。CPU12は、転送開始要求アドレスを更新データ送信部2へ返答する(S407)。

[0031] (図4：ステップS404～S406、S407)

CPU12は、書き込み完了ブロック情報にしたがって、不揮発性メモリ15内のデータブロックを書き込み完了していない領域の先頭アドレスを特定する(S404)。CPU12は、特定したアドレスにしたがって、更新データ4内の対応するアドレスを特定する(S405)。このアドレスが更新データ4のリジュームアドレスとなる。不揮発性メモリ15内のアドレスと更新データ4内のアドレスとの間の対応関係は、例えばあらかじめ不揮発性メモリ15内に格納しておけばよい。あるいはこの対応関係を更新データ送信部2においてあらかじめ保持しておき、CPU12は不揮発性メモリ15内のアドレスをリジュームアドレスとして指定するとともに更新データ送信部2においてその対応関係にしたがって更新データ4内の対応するアドレスを特定してもよい。CPU12は、そのリジュームアドレスを転送開始要求アドレスとしてセットする(S406)。CPU12は、転送開始要求アドレスを更新データ送信部2へ返答する(S407)。

[0032] (図4：ステップS405：補足)

更新データ4内のデータブロックの位置は、更新データ4内のアドレスによって特定してもよいし、例えばデータブロックの番号などのようにアドレス以外の情報によって特定してもよい。すなわち、少なくとも更新データ4内のデータブロックと不揮発性メモリ15内の位置との間の対応関係を特定できる情報を、更新データ送信部2とECU1との間で共有できればよい。

[0033] (図4：ステップS408)

更新データ送信部2は、転送開始要求アドレスをECU1から受領すると、更新データ4の転送開始要求アドレス以降の部分をECU1に対して送信する。CPU12は、更新データ4を受け取って不揮発性メモリ15へ書き込む。本ステップの詳細は後述する。

[0034] 図5は、更新データ送信部2が更新データ4を送信する処理を説明するフ

ローチャートである。更新データ送信部 2 は、E C U 1 から転送開始要求アドレスを受信すると、本フローチャートを開始する。以下図 5 の各ステップを説明する。

[0035] (図 5 : ステップ S 5 0 1)

更新データ送信部 2 は、転送開始要求アドレスが更新データ 4 の先頭の暗号化データブロックであるか否かを判定する。先頭である場合は S 5 0 2 へ進み、先頭ではない場合は S 5 0 3 へ進む。

[0036] (図 5 : ステップ S 5 0 2)

更新データ送信部 2 は、更新データ 4 の先頭の暗号化データブロックを復号するために用いる I V 3 1 3 を、E C U 1 に対して送信する。

[0037] (図 5 : ステップ S 5 0 3)

更新データ送信部 2 は、更新データ 4 のデータブロックを復号するために用いる別の暗号化データブロックを、E C U 1 に対して送信する。典型的には、データブロックを暗号化する際に、その 1 つ前の暗号化済データブロックを用いて暗号化を実施する。したがって更新データ送信部 2 は、転送開始要求アドレスが指定するデータブロックの 1 つ前の暗号化データブロックを、E C U 1 に対して送信する。

[0038] (図 5 : ステップ S 5 0 4)

更新データ送信部 2 は、転送開始要求アドレスが指定するデータブロックから順次、E C U 1 に対して送信する。E C U 1 は、最初に受信するデータブロックについては、S 5 0 2 または S 5 0 3 において受信するデータブロックを用いて、復号を実施できる。それ以後のデータブロックについては、1 つ前に受信したデータブロックを R A M 1 3 などに一時保存しておき、これを用いて復号を実施できる。1 つ前に受信したデータブロック以外のデータブロックを復号において用いる場合は、復号のために用いるデータブロックを R A M 1 3 などに一時保存しておけばよい。

[0039] 図 6 は、S 4 0 8 の詳細を説明するフローチャートである。以下図 6 の各ステップについて説明する。

[0040] (図6：ステップS601)

通信部14は、更新データ送信部2から更新データ4を受信する。CPU12は、更新データ4に含まれるグローバルヘッダ31（ROM情報311、リジュームアドレス312、IV313）を、RAM13または不揮発性メモリ15に格納する。

[0041] (図6：ステップS602)

CPU12は、暗号化データブロックを1つ以上受信したか否かを判定する。例えば更新データ送信部2から受信したデータが暗号化データブロックのサイズに達しているか否かに基づき、この判定を実施できる。暗号化データブロックを1つ以上受信した場合はS603へ進み、未受信である場合はS601へ戻って引き続きデータを受信する。

[0042] (図6：ステップS603)

CPU12は、受信した暗号化データブロックを復号する。復号したデータは、RAM13または不揮発性メモリ15に展開する。本ステップの復号処理の詳細については後述する。

[0043] (図6：ステップS604)

CPU12は、最後に復号した暗号化データブロックを、次の暗号化データブロックの復号に使用するために、RAM13または不揮発性メモリ15に保存しておく。

[0044] (図6：ステップS605)

CPU12は、復号したデータ内に圧縮データブロックが1つ以上含まれているか否かを判定する。例えば復号したデータサイズが圧縮データブロック1つ分に満たなければ、圧縮データブロックがないと判定することができる。圧縮データブロックが含まれていない場合は、S601へ戻って引き続きデータを受信する。圧縮データブロックが含まれている場合はS606へ進む。

[0045] (図6：ステップS606)

CPU12は、圧縮データブロックを解凍する。

[0046] (図6：ステップS607)

CPU12は、解凍したデータが不揮発性メモリ15の書き込みブロックサイズに達しているか否かを判定する。達していない場合は、ステップS601に戻って引き続きデータを受信する。達している場合はS608へ進む。

[0047] (図6：ステップS608～S609)

CPU12は、解凍したデータを不揮発性メモリ15に書き込む(S608)。CPU12は、当該データブロックを書き込み完了したことを表す書き込み完了データブロック情報を、不揮発性メモリ15に保存する(S609)。

[0048] (図6：ステップS609：補足)

書き込み完了データブロック情報は、書き込んだデータブロックの整合性チェックのために用いることもできる。例えば書き込み完了データブロック情報を用いて誤り訂正処理などを実施することにより、データブロックを正常に書き込み完了したか否かをCPU12が判断してもよい。

[0049] 図7は、S603の詳細を説明するフローチャートである。本実施形態において、暗号化処理および復号処理は、AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) モードを利用しているが、これに限らず、別のアルゴリズムを用いてもよい。以下図7の各ステップについて説明する。

[0050] (図7：ステップS701)

CPU12は、これから復号するデータブロックが更新データ4内の最初の暗号化データブロック(図2の例においてはデータブロック42)であるか否かを判定する。最初の暗号化データブロックをこれから復号する場合はS702へ進み、2つ目以降の暗号化データブロックをこれから復号する場合はS704へ進む。

[0051] (図7：ステップS702)

CPU12は、更新データ4内の最初の暗号化データブロックを復号する

。復号鍵は、例えば暗号化データブロックを生成するための暗号化処理において用いられたものと同じものを用いる。復号鍵は、あらかじめ不揮発性メモリ15に保存しておいてもよいし、別の安全な方法でECU1に対して送信するようにしてもよい。

[0052] (図7：ステップS703)

CPU12は、復号された暗号化データブロックと、図4のS408において不揮発性メモリ15に保存したIV313との排他的論理和(XOR)を取ることで、いわゆるプレーンテキストと呼ばれる平文ブロックを生成することができる。S702～S703をまとめて広義の復号処理とみなしてもよい。S704とS705についても同様である。

[0053] (図7：ステップS704)

CPU12は、更新データ4内の2つ目以降の暗号化データブロックを復号する。復号鍵についてはS702と同様である。

[0054] (図7：ステップS705)

CPU12は、復号された暗号化データブロックと、図6のS604において不揮発性メモリ15に保存した暗号化データブロックとのXORを取ることで、平文ブロックを生成することができる。

[0055] <実施の形態2>

図8は、本発明の実施形態2に係るECU1の構成図である。ECU1が更新データ4を更新データ送信部2から受け取る際に、データ中継ECU5が更新データ4を中継してもよい。例えばデータ中継ECU5は、ECU1と更新データ送信部2との間に配置されたゲートウェイ装置であり、ECU1と同じ車内ネットワーク内に搭載することができる。データ中継ECU5は、更新データ4を受け取ると、そのコピーをいったん保存する。データ中継ECU5は、更新データ4の復号や解凍を実施しない。

[0056] データ中継ECU5が、更新データ4の全てを滞りなく受信できた場合は、実施形態1における更新データ送信部2をデータ中継ECU5に置き換え、実施形態1と同様の方法でリジュームが実現できる。

[0057] データ中継ＥＣＵ５が更新データ４を保存している途中で異常が発生してしまった場合は、更新データ送信部２とデータ中継ＥＣＵ５との間で更新データ４を再送すればよい。データ中継ＥＣＵ５は更新データ４の復号や解凍をしないので、再送開始アドレスは、単純にデータ中継ＥＣＵ５に保存できたアドレス範囲の直後とすればよい。

[0058] ＜実施の形態３＞

図９は、本発明の実施形態３に係るＥＣＵ１の構成図である。更新データ４は、不揮発性メモリ１５に代えて、マイコン１１の外部に配置されたフラッシュメモリ１７などの不揮発性記憶装置へ格納してもよい。この場合はマイコン１１がシリアル通信部１６などのインターフェースを介してフラッシュメモリ１７へアクセスし、更新データ４を復号・解凍することによって得たデータブロックを書き込む。

[0059] ＜実施の形態４＞

図１０は、本発明の実施形態４に係るＥＣＵ１の構成図である。図１０のようにＥＣＵ１が２つ以上のマイコン１１を備える場合においても、本発明を適用することができる。具体的には、いずれかのマイコン１１が更新データ４を受信する。更新データ４から解凍・復号によって得たデータブロックを、マイコン間通信部１８を介してその他のマイコン１１が共有する。

[0060] ＜まとめ＞

本発明に係るＥＣＵ１は、車両に搭載される電子制御装置であって、前記車両が搭載している機器を制御する処理を実装したプログラムを実行する演算部、前記プログラムを更新するために用いる更新データを受信する通信部、前記プログラムを記憶する記憶部、を備え、前記更新データ内に含まれる第１データブロックは、前記更新データ内に含まれ前記第１データブロックとは異なる第２データブロックを用いて暗号化されており、前記演算部は、前記第２データブロックを用いて前記第１データブロックを復号することにより、前記更新データを復号し、前記演算部は、前記復号した前記第１データブロックを前記記憶部に対して書き込む書込処理が途中中断した場合は、

前記第1データブロックと前記第2データブロックをともに含む前記更新データを再取得した上で、前記再取得した前記第2データブロックを用いて前記第1データブロックを再復号する。例えば、電源の遮断等により書き込み処理が中断された場合、書き込み処理の対象データである復号データが消失する虞がある。よって、書き込み処理を再開する際には、再度、復号処理を行う必要があり、この復号処理には、復号するブロックだけでなく、復号のために用いる別のブロックも必要となる。そこで、書き込み処理の再開をする際、書き込み処理の対象となるブロックだけでなく、復号のために用いるブロックも併せて再送を指示する。これにより、適切に復号処理が行われ、書き込み処理を再開することができる。

[0061] このようなECU1において、前記第1データブロックは、前記更新データ内において前記第2データブロックの後に配置されており、前記演算部は、前記書き込み処理が途中中断した場合は、前記第1データブロックの開始アドレスと前記第2データブロックの開始アドレスとの間の差分を遡ったアドレスから前記更新データを再取得することにより、前記第1データブロックと前記第2データブロックをともに含む前記更新データを再取得する構成としてもよい。復号のために用いるブロックとして、復号対象ブロックの直前のデータブロックを用いることにより、暗号利用モードに準じた暗号化処理を適用することができる。

[0062] ECU1において、前記演算部は、前記第1データブロックと前記第2データブロックを併せて再取得するとき、前記第1データブロックの位置を表すリジュームアドレスを指定した上で、前記再取得のリクエストを発信し、前記演算部は、前記再取得した前記更新データのうち前記リジュームアドレスに対応するアドレスから前記第1データブロックを取得するとともに、前記リジュームアドレスから前記差分だけ遡ったアドレスから前記第2データブロックを取得する構成としてもよい。復号対象ブロックのリジュームアドレスを指定すると、復号のために用いる別ブロックも併せて送信されるようにあらかじめ設定しておくことにより、復号対象ブロックと復号のために必

要な別ブロックの両方のリジュームアドレスを指定しなくともよい。これによりE C U 1 側における煩雑な処理を回避できる。

[0063] E C U 1 において、前記更新データは、圧縮処理を施された後に前記暗号化を施されており、前記演算部は、前記更新データに対して復号を実施した後に解凍処理を実施することにより、前記第1データブロックと前記第2データブロックを前記更新データから取得する構成としてもよい。暗号化処理の前に圧縮処理を行うことにより、より高い圧縮効果を得ることができる（圧縮率が高い）。また、圧縮⇒暗号化⇒データ転送⇒復号⇒解凍の順で処理を行うことにより、適切に復号処理および解凍処理を行うことができる。

[0064] E C U 1 において、前記電子制御装置はさらに、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを格納する初期化ベクトル記憶部を備え、前記演算部は、前記初期化ベクトル記憶部があらかじめ格納している前記初期化ベクトルを用いて、前記更新データ内の最初の暗号化されたデータブロックを復号する構成としてもよい。復号処理の際、初期化ベクトルを必要とする暗号化処理を行うことにより、より安全性の高いデータ転送を行うことができる。この初期化ベクトルを更新データに含める場合は、あらかじめ車両側に初期化ベクトルを持たせておく必要がなく、仕様毎に初期化ベクトルを変更する等、設定の変更が容易となる。初期化ベクトルを車両側にあらかじめ持たせる場合は、書き込み処理の中断理由が、電源の遮断のような場合であっても、送信された初期化ベクトルが消失することがない。

[0065] E C U 1 において、前記更新データは、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを含み、前記演算部は、前記初期化ベクトルを用いて、前記更新データ内の最初の暗号化されたデータブロックを復号する構成としてもよい。これにより、他のデータブロックを用いて復号を実施するアルゴリズムを用いる場合であっても、最初の暗号化データブロックを適切に復号できる。

[0066] E C U 1 において、前記初期化ベクトルは、前記更新データの先頭のヘッ

ダ部分に含まれており、前記演算部は、前記第2データブロックが前記更新データ内の最初の暗号化されたデータブロックである場合は、前記初期化ベクトルを用いて前記第2データブロックを復号する。初期化ベクトルがグローバルヘッダに含まれており、更新データの送信の際にこれが最初に送信されるので、最初に復号されるデータブロックの復号処理の際、確実に初期化ベクトルを使用することができる。

[0067] ECU1において、前記電子制御装置はさらに、前記演算部が前記更新データを復号する際に用いる前記第2データブロックを一時的に格納するメモリを備え、前記演算部は、前記第1データブロックを復号する前にあらかじめ前記第2データブロックを前記メモリへ格納し、前記演算部は、前記書込処理が途中中断した場合は、前記第1データブロックを再取得するとともに、前記メモリから前記第2データブロックを再取得する。復号のために用いる別ブロックがあらかじめメモリに記憶されているので、復号対象ブロックの復号処理を行う際、メモリに記憶された別ブロックを読み込むことにより、復号処理を行う構成としてもよい。例えば、車両に搭載される電子コントローラの製造時、この電子コントローラ内のメモリに初期化ベクトルを保存しておくことにより、更新データに初期化ベクトルを含めることなく、復号処理時に初期化ベクトルを使用することができる。

[0068] ECU1において、前記更新データは、前記第2データブロックの次に第1データブロックを含み、前記演算部は、前記第2データブロックを前記記憶部に対して書き込んだ後、前記第1データブロックを前記記憶部に対して書き込む処理が途中中断した場合は、前記更新データを前記記憶部に対して書き込む処理を前記第1データブロックから再開する構成としてもよい。書き込み処理が完了している第1データブロックの次の第2データブロックから書き込み処理を再開するので、データの送信や書き込みを最小限に抑えることができ、効率の良い書き込み処理を行うことができる。

[0069] ECU1において、前記電子制御装置はさらに、前記更新データのデータブロックを前記記憶部に対して書込完了したことを表す書込完了ブロック情

報を記憶するメモリを備え、前記演算部は、前記記憶部に対して前記更新データのデータブロックを書き込むごとに前記メモリに対してその書込完了したデータブロックに関する前記書込完了ブロック情報を格納し、前記演算部は、前記第1データブロックを前記記憶部に対して書込完了していない旨を前記書込完了ブロック情報が表している場合は、前記更新データを前記記憶部に対して書き込む処理を前記第1データブロックから再開する構成としてもよい。書き込み処理を再開するとき、データフラッシュにおける書き込み完了情報を参照することにより、どのデータブロックから書き込みの再開を行えばよいか、容易に特定することができる。

[0070] ECU1において、前記演算部は、前記書込完了ブロック情報にしたがって、前記更新データを前記記憶部に対して正常に書込完了したか否かを診断する構成としてもよい。書き込み処理の異常判断を行うことにより、より安全な書き込み処理、すなわち安全なプログラムデータの更新処理を行うことができる。

[0071] ECU1において、前記車両は、前記更新データを一時保存するとともに前記一時保存した前記更新データを前記電子制御装置に対して転送するゲートウェイ装置を搭載しており、前記通信部は、前記ゲートウェイ装置を介して前記更新データを受信し、前記演算部は、前記途中中断した書込処理を再開する場合は、前記ゲートウェイ装置が一時保存している前記更新データを再取得する構成としてもよい。更新データが一旦、ゲートウェイに保存された以降は、更新データ送信部2と車両との通信が不要となるので、通信状態に拘わらずプログラムデータの更新処理を行うことができる。また、書き込み処理の再開の際、ゲートウェイに保存された更新データを用いるので、改めて電子端末と車両の間の通信を行う必要が無い。

[0072] ECU1において、前記更新データは、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを含み、前記演算部は、前記第2データブロックが前記更新データ内の最初の暗号化されたデータブロックである場合は、前記第2データブロックと前記初期化ベク

トルを併せて取得することにより、前記第2データブロックを復号する構成としてもよい。最初の暗号化ブロックを書き込む場合、書き込み処理の前に行われる復号処理に必要な初期化ベクトルを併せて送信することにより、適切に復号処理を行うことができる。

[0073] ECU1において、前記更新データは、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを含み、前記第1データブロックは、前記更新データ内において前記第2データブロックの後に配置されており、前記演算部は、前記第1データブロックを復号する際には、前記第1データブロックと前記第2データブロックを併せて取得することにより、前記第1データブロックを復号する構成としてもよい。2つ目以降の暗号化ブロックを書き込む場合は、復号処理の際に別のブロックが必要となるので、このブロックも併せて送信することにより、適切に復号処理を行うことができる。

[0074] <本発明の変形例について>

本発明は上記実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上記実施形態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限定されるものではない。また、ある実施形態の構成の一部を他の実施形態の構成に置き換えることが可能であり、また、ある実施形態の構成に他の実施形態の構成を加えることも可能である。また、各実施形態の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

[0075] 以上の実施形態において、不揮発性メモリ15やフラッシュメモリ17へ書き込むデータは、圧縮したままであってもよい。この場合はCPU12が圧縮データを用いる際に動的に解凍してRAM13へ一時的に格納し、RAM13から解凍後データを読み出して実行すればよい。

[0076] 実施形態4において、更新データ4を最初に受信したマイコン11が更新データ4を復号した上で他のマイコン11へ復号データを送信してもよいし、更新データ4をそのまま他のマイコン11へ送信して各マイコン11が自

ら復号してもよい。

符号の説明

- [0077] 1 : ECU
- 1 1 : マイコン
- 1 2 : CPU
- 1 3 : RAM
- 1 4 : 通信部
- 1 5 : 不揮発性メモリ
- 1 6 : シリアル通信部
- 1 7 : フラッシュメモリ
- 1 8 : マイコン間通信部
- 2 : 更新データ送信部
- 3 : 更新データ
- 3 1 : グローバルヘッダ
- 3 2 1 ~ 3 N 1 : ローカルヘッダ
- 3 2 2 ~ 3 N 2 : ボディ
- 4 : 更新データ
- 4 2 ~ 4 N : 暗号化データブロック
- 5 : データ中継ECU

請求の範囲

[請求項1]

車両に搭載される電子制御装置であって、

前記車両が搭載している機器を制御する処理を実装したプログラムを実行する演算部、 前記プログラムを更新するために用いる更新データを受信する通信部、

前記プログラムを記憶する記憶部、
を備え、

前記更新データ内に含まれる第1データブロックは、前記更新データ内に含まれ前記第1データブロックとは異なる第2データブロックを用いて暗号化されており、

前記演算部は、前記第2データブロックを用いて前記第1データブロックを復号することにより、前記更新データを復号し、

前記演算部は、前記復号した前記第1データブロックを前記記憶部に対して書き込む書込処理が途中中断した場合は、前記第1データブロックと前記第2データブロックをともに含む前記更新データを再取得した上で、前記再取得した前記第2データブロックを用いて前記第1データブロックを再復号する

ことを特徴とする電子制御装置。

[請求項2]

前記第1データブロックは、前記更新データ内において前記第2データブロックの後に配置されており、

前記演算部は、前記書込処理が途中中断した場合は、前記第1データブロックの開始アドレスと前記第2データブロックの開始アドレスとの間の差分を遡ったアドレスから前記更新データを再取得することにより、前記第1データブロックと前記第2データブロックをともに含む前記更新データを再取得する

ことを特徴とする請求項1記載の電子制御装置。

[請求項3]

前記演算部は、前記第1データブロックと前記第2データブロックを併せて再取得するとき、前記第1データブロックの位置を表すリジ

ュームアドレスを指定した上で、前記再取得のリクエストを発信し、

前記演算部は、前記再取得した前記更新データのうち前記リジュームアドレスに対応するアドレスから前記第1データブロックを取得するとともに、前記リジュームアドレスから前記差分だけ遡ったアドレスから前記第2データブロックを取得する

ことを特徴とする請求項2記載の電子制御装置。

[請求項4] 前記更新データは、圧縮処理を施された後に前記暗号化を施されており、

前記演算部は、前記更新データに対して復号を実施した後に解凍処理を実施することにより、前記第1データブロックと前記第2データブロックを前記更新データから取得する ことを特徴とする請求項1記載の電子制御装置。

[請求項5] 前記電子制御装置はさらに、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを格納する初期化ベクトル記憶部を備え、

前記演算部は、前記初期化ベクトル記憶部があらかじめ格納している前記初期化ベクトルを用いて、前記更新データ内の最初の暗号化されたデータブロックを復号する

ことを特徴とする請求項1記載の電子制御装置。

[請求項6] 前記更新データは、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを含み、

前記演算部は、前記初期化ベクトルを用いて、前記更新データ内の最初の暗号化されたデータブロックを復号する

ことを特徴とする請求項1記載の電子制御装置。

[請求項7] 前記初期化ベクトルは、前記更新データの先頭のヘッダ部分に含まれており、

前記演算部は、前記第2データブロックが前記更新データ内の最初の暗号化されたデータブロックである場合は、前記初期化ベクトルを

用いて前記第2データブロックを復号する

ことを特徴とする請求項6記載の電子制御装置。

[請求項8] 前記電子制御装置はさらに、前記演算部が前記更新データを復号する際に用いる前記第2データブロックを一時的に格納するメモリを備え、

前記演算部は、前記第1データブロックを復号する前にあらかじめ前記第2データブロックを前記メモリへ格納し、

前記演算部は、前記書込処理が途中中断した場合は、前記第1データブロックを再取得するとともに、前記メモリから前記第2データブロックを再取得する

ことを特徴とする請求項1記載の電子制御装置。

[請求項9] 前記更新データは、前記第2データブロックの次に前記第1データブロックを含み、

前記演算部は、前記第2データブロックを前記記憶部に対して書き込んだ後、前記第1データブロックを前記記憶部に対して書き込む処理が途中中断した場合は、前記更新データを前記記憶部に対して書き込む処理を前記第1データブロックから再開する

ことを特徴とする請求項1記載の電子制御装置。

[請求項10] 前記電子制御装置はさらに、前記更新データのデータブロックを前記記憶部に対して書込完了したことを表す書込完了ブロック情報を記憶するメモリを備え、

前記演算部は、前記記憶部に対して前記更新データのデータブロックを書き込むごとに前記メモリに対してその書込完了したデータブロックに関する前記書込完了ブロック情報を格納し、

前記演算部は、前記第1データブロックを前記記憶部に対して書込完了していない旨を前記書込完了ブロック情報が表している場合は、前記更新データを前記記憶部に対して書き込む処理を前記第1データブロックから再開する

ことを特徴とする請求項 9 記載の電子制御装置。

[請求項11] 前記演算部は、前記書込完了ブロック情報にしたがって、前記更新データを前記記憶部に対して正常に書込完了したか否かを診断することを特徴とする請求項 10 記載の電子制御装置。

[請求項12] 前記車両は、前記更新データを一時保存するとともに前記一時保存した前記更新データを前記電子制御装置に対して転送するゲートウェイ装置を搭載しており、

前記通信部は、前記ゲートウェイ装置を介して前記更新データを受信し、

前記演算部は、前記途中中断した書込処理を再開する場合は、前記ゲートウェイ装置が一時保存している前記更新データを再取得することを特徴とする請求項 1 記載の電子制御装置。

[請求項13] 前記更新データは、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを含み、

前記演算部は、前記第 2 データブロックが前記更新データ内の最初の暗号化されたデータブロックである場合は、前記第 2 データブロックと前記初期化ベクトルを併せて取得することにより、前記第 2 データブロックを復号する

ことを特徴とする請求項 1 記載の電子制御装置。

[請求項14] 前記更新データは、前記更新データ内の最初の暗号化されたデータブロックを復号するために用いる初期化ベクトルを含み、

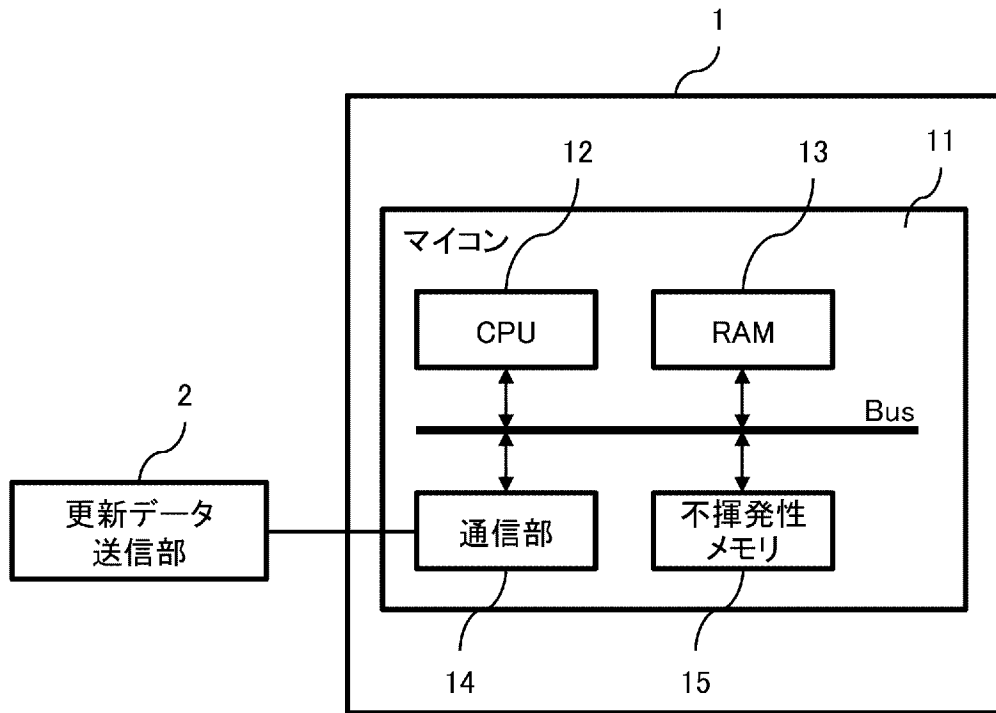
前記第 1 データブロックは、前記更新データ内において前記第 2 データブロックの後に配置されており、

前記演算部は、前記第 1 データブロックを復号する際には、前記第 1 データブロックと前記第 2 データブロックを併せて取得することにより、前記第 1 データブロックを復号する

ことを特徴とする請求項 1 記載の電子制御装置。

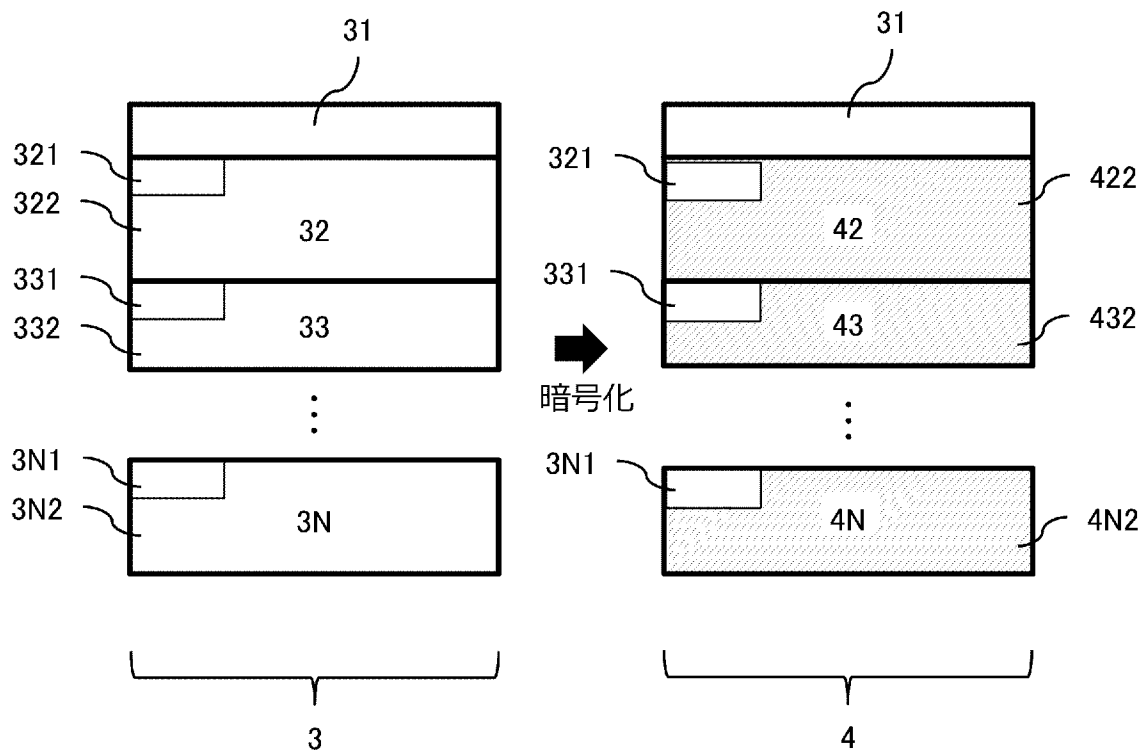
[図1]

図 1



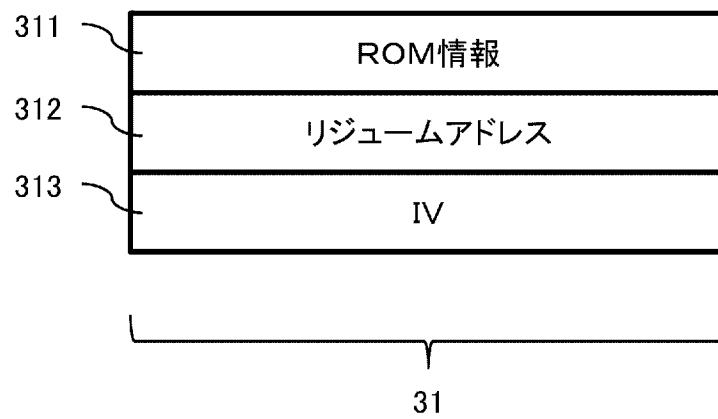
[図2]

図 2



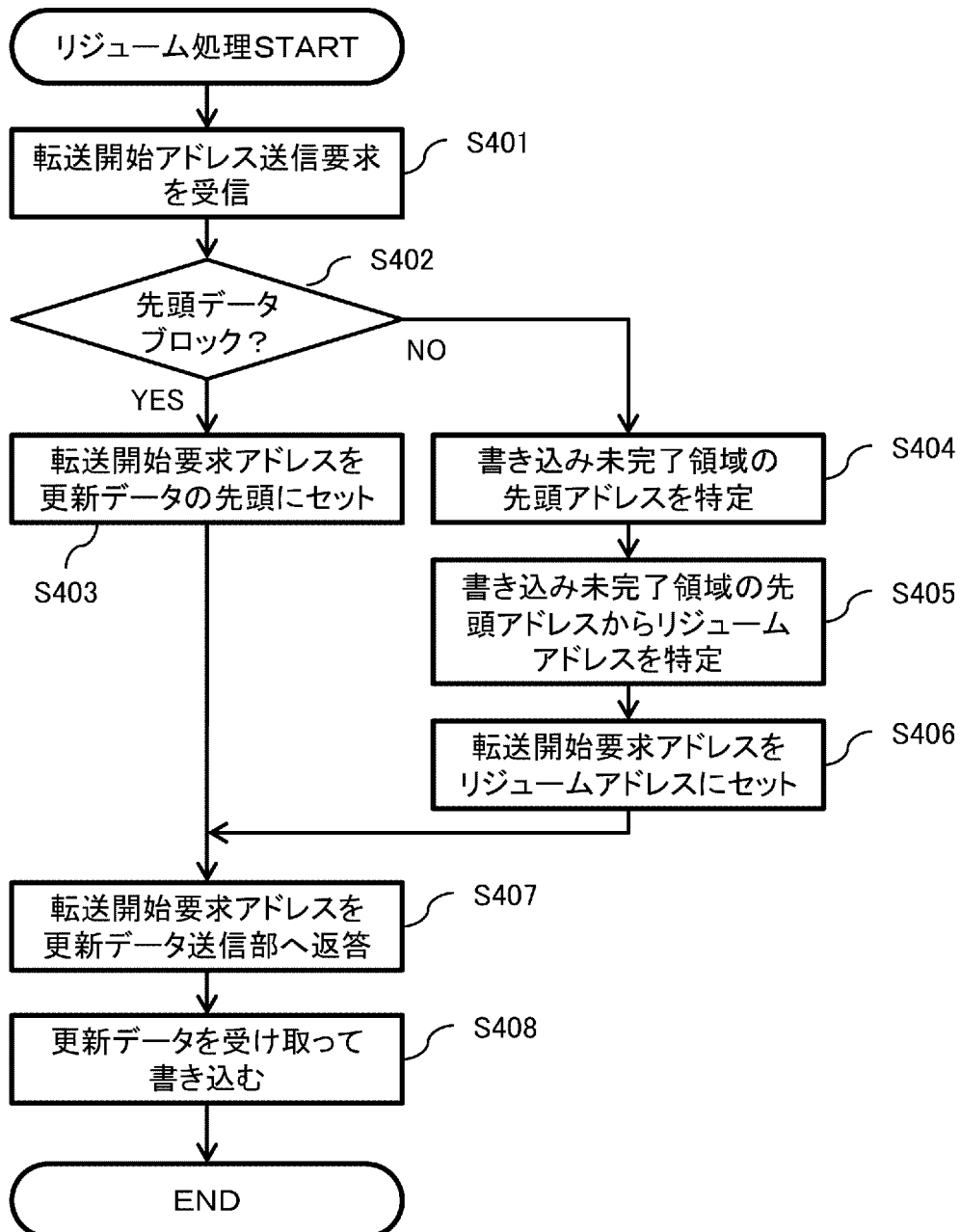
[図3]

図 3



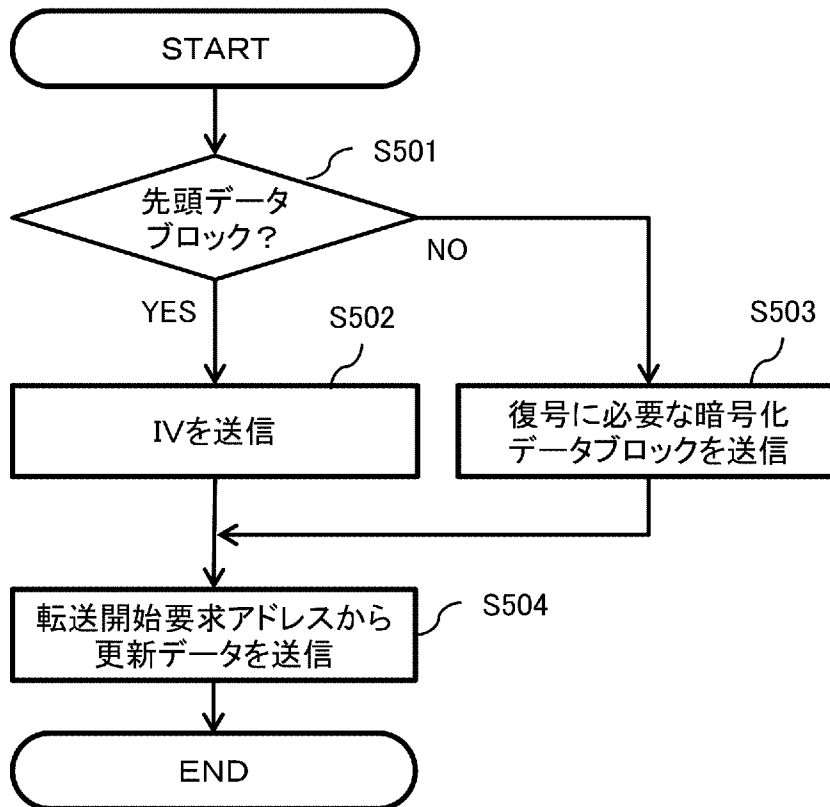
[図4]

図 4



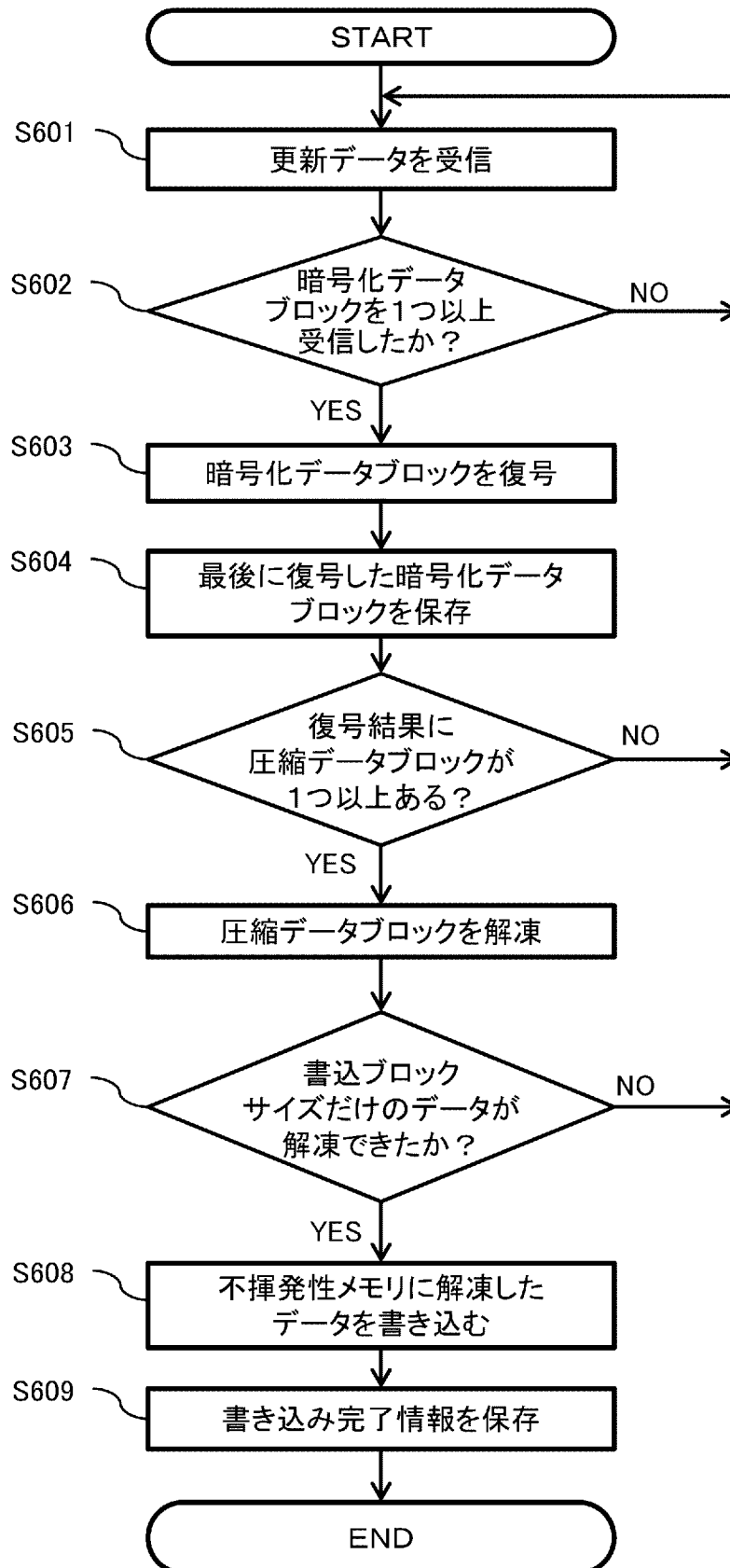
[図5]

図 5



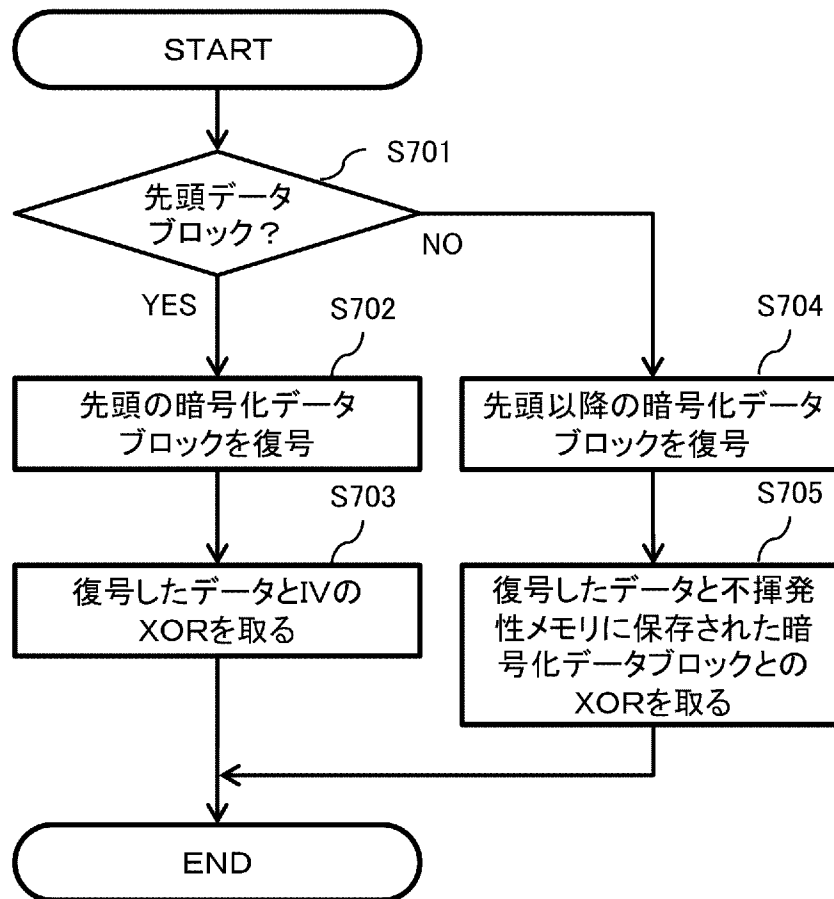
[図6]

図 6



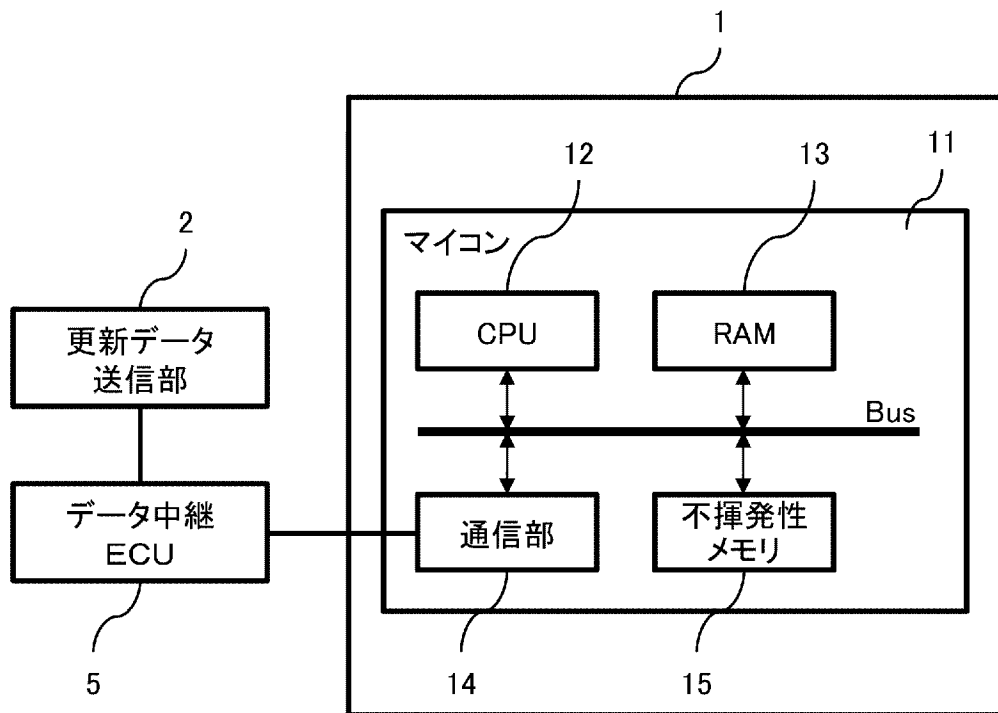
[図7]

図 7



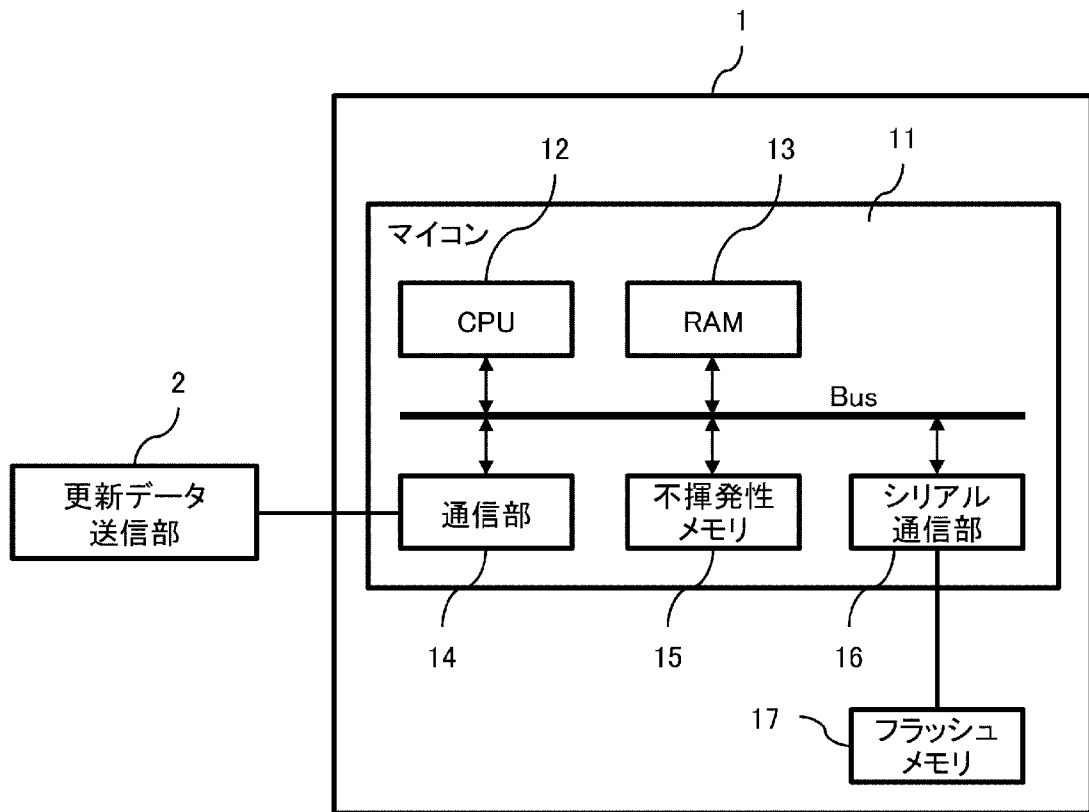
[図8]

図 8



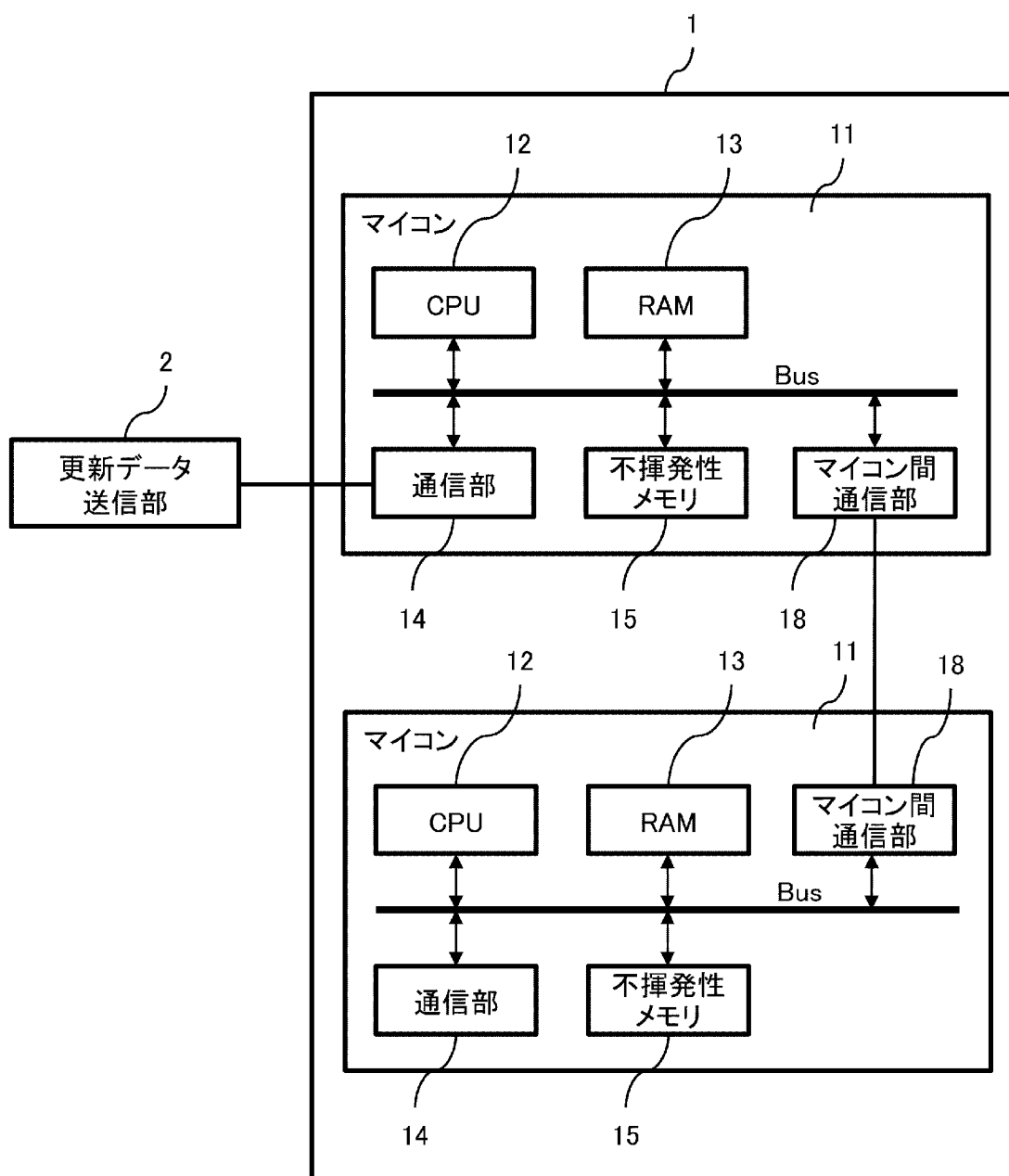
[図9]

図 9



[図10]

図 10



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/031847

A. CLASSIFICATION OF SUBJECT MATTER**B60R 16/02**(2006.01)i; **G06F 8/65**(2018.01)i

FI: G06F8/65; B60R16/02 660U

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)

B60R16/02; G09C1/00-5/00; G06F8/65-8/658; G06F21/00-21/88; H04L9/00-9/38

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 1971-2021

Registered utility model specifications of Japan 1996-2021

Published registered utility model applications of Japan 1994-2021

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	WO 2018/070156 A1 (HITACHI AUTOMOTIVE SYSTEMS LTD) 19 April 2018 (2018-04-19) paragraphs [0010]-[0013], [0033]-[0038], [0058]-[0061], [0115]-[0122], fig. 1, 6, 12	1-14
A	US 2020/0034134 A1 (FORD GLOBAL TECHNOLOGIES, LLC) 30 January 2020 (2020-01-30) entire text, all drawings	1-14
A	CN 108170455 A (AMLOGIC SEMICONDUCTOR (SHANGHAI) CO., LTD.) 15 June 2018 (2018-06-15) entire text, all drawings	1-14
A	JP 2019-519829 A (SQUARE, INC) 11 July 2019 (2019-07-11) paragraphs [0004], [0017]-[0019], [0070], [0127]-[0133], fig. 6	1-14
A	JP 2020-187184 A (DENSO CORP) 19 November 2020 (2020-11-19) paragraphs [0002]-[0003], [0021]-[0040], fig. 1-5	1-14
A	JP 2006-298261 A (DENSO CORP) 02 November 2006 (2006-11-02) paragraphs [0041]-[0048], fig. 9-12	10-11



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

11 November 2021

Date of mailing of the international search report

22 November 2021

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/JP2021/031847

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO	2018/070156	A1	19 April 2018	EP 3528118 A1 paragraphs [0014]-[0020], [0058]-[0069], [0101]-[0108], [0184]-[0195], fig. 1, 6, 12	
				US 2020/0225930 A1	
				CN 109804355 A	
US	2020/0034134	A1	30 January 2020	DE 102019120445 A1	
				CN 110780896 A	
CN	108170455	A	15 June 2018	(Family: none)	
JP	2019-519829	A	11 July 2019	WO 2017/172953 A1 paragraphs [0004], [0017]- [0019], [0070], [0127]-[0133], fig. 6	
				US 2017/0286085 A1	
				US 2017/0286093 A1	
JP	2020-187184	A	19 November 2020	(Family: none)	
JP	2006-298261	A	02 November 2006	US 2006/0259207 A1 paragraphs [0138]-[0145], fig. 19-22	

A. 発明の属する分野の分類（国際特許分類（IPC）） B60R 16/02(2006.01)i; G06F 8/65(2018.01)i FI: G06F8/65; B60R16/02 660U														
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）） B60R16/02; G09C1/00-5/00; G06F8/65-8/658; G06F21/00-21/88; H04L9/00-9/38 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>1971-2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2021年</td> </tr> </table> 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）			日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2021年	日本国実用新案登録公報	1996-2021年	日本国登録実用新案公報	1994-2021年				
日本国実用新案公報	1922-1996年													
日本国公開実用新案公報	1971-2021年													
日本国実用新案登録公報	1996-2021年													
日本国登録実用新案公報	1994-2021年													
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	WO 2018/070156 A1（日立オートモティブシステムズ株式会社）19.04.2018（2018-04-19） 段落[0010]-[0013], [0033]-[0038], [0058]-[0061], [0115]-[0122], 図1, 6, 12	1-14												
A	US 2020/0034134 A1（FORD GLOBAL TECHNOLOGIES, LLC）30.01.2020（2020-01-30） 全文, 全図	1-14												
A	CN 108170455 A（AMLOGIC SEMICONDUCTOR（SHANGHAI）CO., LTD.）15.06.2018（2018-06-15） 全文, 全図	1-14												
A	JP 2019-519829 A（スクエア、インコーポレイテッド）11.07.2019（2019-07-11） 段落[0004], [0017]-[0019], [0070], [0127]-[0133], 図6	1-14												
A	JP 2020-187184 A（株式会社デンソー）19.11.2020（2020-11-19） 段落[0002]-[0003], [0021]-[0040], 図1-5	1-14												
A	JP 2006-298261 A（株式会社デンソー）02.11.2006（2006-11-02） 段落[0041]-[0048], 図9-12	10-11												
☐ 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 11.11.2021	国際調査報告の発送日 22.11.2021													
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） 多賀 実 5B 9367 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/JP2021/031847

引用文献			公表日	パテントファミリー文献	公表日
WO	2018/070156	A1	19.04.2018	EP 3528118 A1 段落[0014]-[0020], [0058]-[0069], [0101]- [0108], [0184]-[0195], 図 1, 6, 12 US 2020/0225930 A1 CN 109804355 A	
US	2020/0034134	A1	30.01.2020	DE 102019120445 A1 CN 110780896 A	
CN	108170455	A	15.06.2018	(ファミリーなし)	
JP	2019-519829	A	11.07.2019	WO 2017/172953 A1 段落[0004], [0017]-[0019], [0070], [0127]-[0133], 図6 US 2017/0286085 A1 US 2017/0286093 A1	
JP	2020-187184	A	19.11.2020	(ファミリーなし)	
JP	2006-298261	A	02.11.2006	US 2006/0259207 A1 段落[0138]-[0145], 図19- 22	