(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
2020年2月13日(13.02.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/032043 A1

(51) 国際特許分類:
G06F 8/65 (2018.01) *B60R 16/02* (2006.01)

(21) 国際出願番号： PCT/JP2019/030944

(22) 国際出願日： 2019年8月6日(06.08.2019)

(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 2018-151415 2018年8月10日(10.08.2018) JP
特願 2019-129956 2019年7月12日(12.07.2019) JP

(71) 出願人: 株式会社デンソー (**DENSO CORPORATION**) [JP/JP]; 〒4488661 愛知県刈谷市昭和町１丁目１番地 Aichi (JP).

(72) 発明者: 原田 雄三(**HARATA, Yuzo**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP). 上原 一浩(**UEHARA, Kazuhiro**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP). 河▲崎▼ 卓也(**KAWASAKI, Takuya**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP). 夏目 充啓(**NATSUME, Mitsuyoshi**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP).

(74) 代理人: 特許業務法人 サトー国際特許事務所 (**SATO INTERNATIONAL PATENT FIRM**); 〒4600008 愛知県名古屋市中区栄四丁目６番１５号 フォーティーンヒルズセンタービル Aichi (JP).

WO 2020/032043 A1

(54) **Title:** VEHICLE ELECTRONIC CONTROL SYSTEM, DOWNLOAD DETERMINATION METHOD FOR DISTRIBUTION PACKAGE, AND DOWNLOAD DETERMINATION PROGRAM FOR DISTRIBUTION PACKAGE

(54) 発明の名称： 車両用電子制御システム、配信パッケージのダウンロード判定方法及び配信パッケージのダウンロード判定プログラム

[図53]
Fig. 53

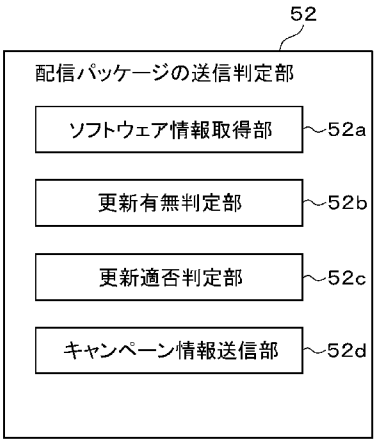


FIG. 53:
52 Transmission determination unit for distribution package
52a Software information acquisition unit
52b Update existence/nonexistence determination unit
52c Update appropriateness/inappropriateness determination unit
52d Campaign information transmission unit

(57) **Abstract:** A center device (3) acquires software information of an electronic control device from a vehicle side, determines existence or nonexistence of update data with respect to the vehicle on the basis of the acquired software information, and when it is determined that the vehicle is in a state appropriate to an update, transmits campaign information to a master device (11). Upon reception of the campaign information from the center device, when determining that the

［続葉有］

(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, 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, 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, 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:

— 国際調査報告(条約第21条(3))

vehicle is in a state in which the vehicle can download a distribution package, the master device downloads the distribution package from the center device.

(57) 要約:センター装置(3)は、車両側から電子制御装置のソフトウェア情報を取得し、その取得したソフトウェア情報に基づいて車両に対する更新データの有無を判定し、車両状態が更新に適する状態であると判定すると、キャンペーン情報をマスタ装置(11)に送信する。マスタ装置は、センター装置からキャンペーン情報を受信すると、車両状態が配信パッケージをダウンロード可能な状態であると判定すると、センター装置から配信パッケージをダウンロードする。

明　細　書

発明の名称 ：

車両用電子制御システム、配信パッケージのダウンロード判定方法及び配信パッケージのダウンロード判定プログラム

関連出願の相互参照

[0001] 本出願は、２０１８年８月１０日に出願された日本出願番号２０１８－１５１４１５号及び２０１９年７月１２日に出願された日本出願番号２０１９－１２９９５６号に基づくもので、ここにその記載内容を援用する。

技術分野

[0002] 本開示は、車両用電子制御システム、配信パッケージのダウンロード判定方法及び配信パッケージのダウンロード判定プログラムに関する。

背景技術

[0003] 近年、運転支援機能や自動運転機能等の車両制御の多様化に伴い、車両の電子制御装置（以下、ＥＣＵ（Electronic Control Unit）と称する）に搭載される車両制御や診断等のプログラムの規模が増大している。又、機能改善等によるバージョンアップに伴い、ＥＣＵのプログラムを書換える（リプログする）機会も増えつつある。一方、通信ネットワークの進展等に伴い、コネクッテッドカーの技術も普及している。このような事情から、例えば特許文献１には、車両側に中継装置としての車両用マスタ装置が設けられ、車両用マスタ装置がセンター装置から無線で受信した更新データを書換え対象ＥＣＵに配信することで、書換え対象ＥＣＵのプログラムをＯＴＡ（Over The Air）により書換える技術が提案されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１８－１００００２号公報

発明の概要

[0005] 特許文献１では、車両用マスタ装置は、例えばイグニッションオンの場合に、センター装置から更新データを含む配信パッケージをダウンロードする。車両用マスタ装置は、センター装置からの配信パッケージのダウンロードを完了すると、車両位置が予め登録されている所定範囲内であることを条件として、そのダウンロードした配信パッケージから更新データを抽出し、その抽出した更新データを書換え対象ＥＣＵにインストールする。

[0006] 車両用マスタ装置がセンター装置からの配信パッケージのダウンロードを無条件に開始してしまう構成では、車両状態が配信パッケージのダウンロードや更新データのインストールに適さない不適切な状態であるにも拘らず車両用マスタ装置がセンター装置からの配信パッケージのダウンロードを開始する虞がある。車両状態が不適切な状態で車両用マスタ装置がセンター装置からの配信パッケージのダウンロードを開始すると、配信パッケージのダウンロードや更新データのインストールを正常に完了することができない虞がある。

[0007] 本開示は、上記した事情に鑑みてなされたものであり、その目的は、車両用マスタ装置がセンター装置からの配信パッケージのダウンロードを適切に開始することができる車両用電子制御システム、配信パッケージのダウンロード判定方法及び配信パッケージのダウンロード判定プログラムを提供することにある。

[0008] 本開示の一態様によれば、センター装置において、ソフトウェア情報取得部は、車両側から電子制御装置のソフトウェア情報を取得する。更新有無判定部は、車両側から電子制御装置のソフトウェア情報がソフトウェア情報取得部により取得されると、その取得されたソフトウェア情報に基づいて、車両に対する更新データの有無を判定する。更新適否判定部は、車両に対する更新データが有ると更新有無判定部により判定されると、車両状態が更新に適する状態であるか否かを判定する。キャンペーン情報送信部は、車両状態が更新に適する状態であると更新適否判定部により判定されると、更新に関するキャンペーン情報を車両用マスタ装置に送信する。

[0009] 車両用マスタ装置において、キャンペーン情報受信部は、センター装置からキャンペーン情報を受信する。ダウンロード可能判定部は、キャンペーン情報がキャンペーン情報受信部により受信されると、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定する。ダウンロード実行部は、車両状態が配信パッケージをダウンロード可能な状態であるとダウンロード可能判定部により判定されると、センター装置から配信パッケージをダウンロードする。

[0010] センター装置において、車両に対する更新データが有ると判定し、車両状態が更新に適する状態であると判定すると、更新に関するキャンペーン情報を車両用マスタ装置に送信するようにした。車両用マスタ装置において、車両状態が配信パッケージをダウンロード可能な状態であると判定すると、センター装置から配信パッケージをダウンロードするようにした。このようなセンター装置による車両に対する更新データの有無の判定及び車両状態が更新に適する状態であるか否かの判定と、車両用マスタ装置による車両状態が配信パッケージをダウンロード可能な状態であるか否かの判定とを組み合わせて行うことで、車両用マスタ装置がセンター装置からの配信パッケージのダウンロードを適切に開始することができる。

図面の簡単な説明

[0011] 本開示についての上記目的及びその他の目的、特徴や利点は、添付の図面を参照しながら下記の詳細な記述により、より明確になる。その図面は、

[図1]図１は、一実施形態の全体構成を示す図であり、

[図2]図２は、ＣＧＷの電気的な構成を示す図であり、

[図3]図３は、ＤＣＭの電気的な構成を示す図であり、

[図4]図４は、ＥＣＵの電気的な構成を示す図であり、

[図5]図５は、電源ラインの接続態様を示す図であり、

[図6]図６は、リプログデータ及び配信諸元データをパッケージ化する態様を示す図であり、

[図7]図７は、ＤＣＭ用の書換え諸元データを示す図であり、

[図8]図８は、ＣＧＷ用の書換え諸元データを示す図であり、

[図9]図９は、配信諸元データを示す図であり、

[図10]図１０は、配信パッケージをアンパッケージ化する態様を示す図であり、

[図11]図１１は、組込み型の１面単独メモリにおける通常動作時の態様を示す図であり、

[図12]図１２は、組込み型の１面単独メモリにおける書換え動作時の態様を示す図であり、

[図13]図１３は、ダウンロード型の１面単独メモリにおける通常動作時の態様を示す図であり、

[図14]図１４は、ダウンロード型の１面単独メモリにおける書換え動作時の態様を示す図であり、

[図15]図１５は、組込み型の１面サスペンドメモリにおける通常動作時の態様を示す図であり、

[図16]図１６は、組込み型の１面サスペンドメモリにおける書換え動作時の態様を示す図であり、

[図17]図１７は、ダウンロード型の１面サスペンドメモリにおける通常動作時の態様を示す図であり、

[図18]図１８は、ダウンロード型の１面サスペンドメモリにおける書換え動作時の態様を示す図であり、

[図19]図１９は、組込み型の２面メモリにおける通常動作時の態様を示す図であり、

[図20]図２０は、組込み型の２面メモリにおける書換え動作時の態様を示す図であり、

[図21]図２１は、ダウンロード型の２面メモリにおける通常動作時の態様を示す図であり、

[図22]図２２は、ダウンロード型の２面メモリにおける書換え動作時の態様を示す図であり、

[図23]図２３は、アプリプログラムを書換える態様を示す図であり、

[図24]図２４は、アプリプログラムを書換える態様を示す図であり、

[図25]図２５は、アプリプログラムを書換える態様を示す図であり、

[図26]図２６は、電源制御によりアプリプログラムを書換える態様を示すタイミングチャートであり、

[図27]図２７は、電源制御によりアプリプログラムを書換える態様を示すタイミングチャートであり、

[図28]図２８は、電源自己保持によりアプリプログラムを書換える態様を示すタイミングチャートであり、

[図29]図２９は、電源自己保持によりアプリプログラムを書換える態様を示すタイミングチャートであり、

[図30]図３０は、フェーズを示す図であり、

[図31]図３１は、通常時の画面を示す図であり、

[図32]図３２は、キャンペーン通知発生時の画面を示す図であり、

[図33]図３３は、キャンペーン通知時の画面を示す図であり、

[図34]図３４は、ダウンロード承諾時の画面を示す図であり、

[図35]図３５は、ダウンロード承諾時の画面を示す図であり、

[図36]図３６は、ダウンロード実行中の画面を示す図であり、

[図37]図３７は、ダウンロード実行中の画面を示す図であり、

[図38]図３８は、ダウンロード完了時の画面を示す図であり、

[図39]図３９は、インストール承諾時の画面を示す図であり、

[図40]図４０は、インストール承諾時の画面を示す図であり、

[図41]図４１は、インストール実行中の画面を示す図であり、

[図42]図４２は、インストール実行中の画面を示す図であり、

[図43]図４３は、アクティベート承諾時の画面を示す図であり、

[図44]図４４は、ＩＧオン時の画面を示す図であり、

[図45]図４５は、確認操作時の画面を示す図であり、

[図46]図４６は、確認操作時の画面を示す図であり、

[図47]図４７は、センター装置の機能ブロック図であり、

[図48]図４８は、ＤＣＭの機能ブロック図であり、

[図49]図４９は、ＣＧＷの機能ブロック図であり、

[図50]図５０は、ＣＧＷの機能ブロック図であり、

[図51]図５１は、ＥＣＵの機能ブロック図であり、

[図52]図５２は、車載ディスプレイの機能ブロック図であり、

[図53]図５３は、配信パッケージの送信判定部の機能ブロック図であり、

[図54]図５４は、配信パッケージの送信判定処理を示すフローチャートであり、

[図55]図５５は、配信パッケージのダウンロード判定部の機能ブロック図であり、

[図56]図５６は、配信パッケージのダウンロード判定処理を示すフローチャートであり、

[図57]図５７は、書込みデータの転送判定部の機能ブロック図であり、

[図58]図５８は、書込みデータの転送判定処理を示すフローチャートであり、

[図59]図５９は、書込みデータの取得判定部の機能ブロック図であり、

[図60]図６０は、書込みデータの取得判定処理を示すフローチャートであり、

[図61]図６１は、インストールの指示判定部の機能ブロック図であり、

[図62]図６２は、インストールの指示判定処理を示すフローチャートであり、

[図63]図６３は、インストールを指示する態様を示す図であり、

[図64]図６４は、インストールを指示する態様を示す図であり、

[図65]図６５は、乱数値を生成する態様を示す図であり、

[図66]図６６は、セキュリティアクセス鍵の管理部の機能ブロック図であり、

[図67]図６７は、セキュリティアクセス鍵の生成処理を示すフローチャート

であり、

[図68]図６８は、セキュリティアクセス鍵を生成する態様を示す図であり、

[図69]図６９は、セキュリティアクセス鍵の消去処理を示すフローチャートであり、

[図70]図７０は、書込みデータの検証に関与する処理の流れを示す図であり、

[図71]図７１は、書込みデータの検証部の機能ブロック図であり、

[図72]図７２は、書込みデータの検証処理を示すフローチャートであり、

[図73]図７３は、書込みデータの検証に関与する処理を分散した態様を示す図であり、

[図74]図７４は、書込みデータの検証に関与する処理を分散した態様を示す図であり、

[図75]図７５は、書込みデータの検証に関与する処理を分散した態様を示す図であり、

[図76]図７６は、書込みデータの検証に関与する処理を分散した態様を示す図であり、

[図77]図７７は、書込みデータの検証及びアプリプログラムの書換えの流れを示す図であり、

[図78]図７８は、書込みデータの検証及びアプリプログラムの書換えの流れを示す図であり、

[図79]図７９は、データ格納面情報の送信制御部の機能ブロック図であり、

[図80]図８０は、データ格納面情報の送信制御処理を示すフローチャートであり、

[図81]図８１は、２面書換え情報を通知する態様を示すシーケンス図であり、

[図82]図８２は、非書換え対象の電源管理部の機能ブロック図であり、

[図83]図８３は、非書換え対象の電源管理処理を示すフローチャートであり、

[図84]図８４は、起動状態、停止状態、スリープ状態の遷移を示す図であり、

[図85]図８５は、起動状態、停止状態、スリープ状態の遷移を示す図であり、

[図86]図８６は、電源ラインの接続態様を示す図であり、

[図87]図８７は、バッテリ残量の監視処理を示すフローチャートであり、

[図88]図８８は、ファイルの転送制御部の機能ブロック図であり、

[図89]図８９は、ファイルの転送制御処理を示すフローチャートであり、

[図90]図９０は、ファイルを授受する態様を示す図であり、

[図91]図９１は、ファイルを授受する態様を示す図であり、

[図92]図９２は、分割ファイル及び書込みファイルを示す図であり、

[図93]図９３は、ＣＧＷが転送要求をＤＣＭに送信する態様を示す図であり、

[図94]図９４は、ＣＧＷが転送要求をＤＣＭに送信する態様を示す図であり、

[図95]図９５は、ＣＧＷが書込みデータを書換え対象ＥＣＵに配信する態様を示す図であり、

[図96]図９６は、ＣＧＷが書込みデータを書換え対象ＥＣＵに配信する態様を示す図であり、

[図97]図９７は、ＣＧＷが書込みデータを書換え対象ＥＣＵに配信する態様を示す図であり、

[図98]図９８は、ＥＣＵの接続態様を示す図であり、

[図99]図９９は、書込みデータの配信制御部の機能ブロック図であり、

[図100]図１００は、バス負荷テーブルを示す図であり、

[図101]図１０１は、書換え対象ＥＣＵ所属テーブルを示す図であり、

[図102]図１０２は、書込みデータの配信制御処理を示すフローチャートであり、

[図103]図１０３は、書込みデータを配信する態様を示す図であり、

[図104]図１０４は、書込みデータを配信する態様を示す図であり、

[図105]図１０５は、車両が走行中の書込みデータを配信する態様を示す図であり、

[図106]図１０６は、駐車中の書込みデータを配信する態様を示す図であり、

[図107]図１０７は、書込みデータの配信量を示す図であり、

[図108]図１０８は、書込みデータの配信量を示す図であり、

[図109]図１０９は、アクティベート要求の指示部の機能ブロック図であり、

[図110]図１１０は、アクティベート要求の指示処理を示すフローチャートであり、

[図111]図１１１は、アクティベート要求を指示する態様を示す図であり、

[図112]図１１２は、アクティベートの実行制御部の機能ブロック図であり、

[図113]図１１３は、書換え処理を示すフローチャートであり、

[図114]図１１４は、アクティベートの実行制御処理を示すフローチャートであり、

[図115]図１１５は、書換え対象のグループ化部の機能ブロック図であり、

[図116]図１１６は、書換え対象のグループ管理処理を示すフローチャートであり、

[図117]図１１７は、書換え対象のグループ管理処理を示すフローチャートであり、

[図118]図１１８は、書換え対象をグループ化する態様を示す図であり、

[図119]図１１９は、ロールバックの実行制御部の機能ブロック図であり、

[図120]図１２０は、ロールバック方法の特定処理を示すフローチャートであり、

[図121]図１２１は、キャンセル要求の判定処理を示すフローチャートであり、

[図122]図１２２は、キャンセル要求の判定処理を示すフローチャートであり、

[図123]図１２３は、キャンセル要求の判定処理を示すフローチャートであり

、

[図124]図１２４は、キャンセル要求の判定処理を示すフローチャートであり、

[図125]図１２５は、キャンセル要求の判定処理を示すフローチャートであり、

[図126]図１２６は、ロールバックを実行する態様を示す図であり、

[図127]図１２７は、ロールバックを実行する態様を示す図であり、

[図128]図１２８は、ロールバックを実行する態様を示す図であり、

[図129]図１２９は、ロールバックを実行する態様を示す図であり、

[図130]図１３０は、ロールバックを実行する態様を示す図であり、

[図131]図１３１は、書換え進捗状況の表示制御部の機能ブロック図であり、

[図132]図１３２は、書換え進捗状況の表示制御処理を示すフローチャートであり、

[図133]図１３３は、書換え進捗状況の表示制御処理を示すフローチャートであり、

[図134]図１３４は、書換え進捗状況の画面を示す図であり、

[図135]図１３５は、書換え進捗状況の画面を示す図であり、

[図136]図１３６は、書換え進捗状況の画面を示す図であり、

[図137]図１３７は、書換え進捗状況の画面を示す図であり、

[図138]図１３８は、書換え進捗状況の画面を示す図であり、

[図139]図１３９は、進捗グラフ表示の遷移を示す図であり、

[図140]図１４０は、進捗グラフ表示の遷移を示す図であり、

[図141]図１４１は、進捗グラフ表示の遷移を示す図であり、

[図142]図１４２は、進捗グラフ表示の遷移を示す図であり、

[図143]図１４３は、書換え進捗状況の画面を示す図であり、

[図144]図１４４は、差分データの整合性判定部の機能ブロック図であり、

[図145]図１４５は、差分データの整合性判定処理を示すフローチャートであり、

[図146]図１４６は、差分データの整合性を判定する態様を示す図であり、

[図147]図１４７は、差分データの整合性を判定する態様を示す図であり、

[図148]図１４８は、書換えの実行制御部の機能ブロック図であり、

[図149]図１４９は、通常動作処理を示すフローチャートであり、

[図150]図１５０は、書換え動作処理を示すフローチャートであり、

[図151]図１５１は、情報通知処理を示すフローチャートであり、

[図152]図１５２は、書換えプログラムの検証処理を示すフローチャートであり、

[図153]図１５３は、識別情報及び書込みデータを送信する態様を示す図であり、

[図154]図１５４は、識別情報及び書込みデータを送信する態様を示す図であり、

[図155]図１５５は、インストール指示処理を示すフローチャートであり、

[図156]図１５６は、セッションの確立部の機能ブロック図であり、

[図157]図１５７は、プログラムの構成を示す図であり、

[図158]図１５８は、状態遷移を示す図であり、

[図159]図１５９は、状態遷移を示す図であり、

[図160]図１６０は、状態遷移を示す図であり、

[図161]図１６１は、セッションの調停を示す図であり、

[図162]図１６２は、セッションの調停を示す図であり、

[図163]図１６３は、第１状態の状態遷移管理処理を示すフローチャートであり、

[図164]図１６４は、第１状態の状態遷移管理処理を示すフローチャートであり、

[図165]図１６５は、第１状態の状態遷移管理処理を示すフローチャートであり、

[図166]図１６６は、第２状態の状態遷移管理処理を示すフローチャートであり、

[図167]図１６７は、第２状態の状態遷移管理処理を示すフローチャートであり、

[図168]図１６８は、プログラムの構成を示す図であり、

[図169]図１６９は、状態遷移を示す図であり、

[図170]図１７０は、リトライポイントの特定部の機能ブロック図であり、

[図171]図１７１は、フラッシュメモリの構成を示す図であり、

[図172]図１７２は、処理フラグの設定処理を示すフローチャートであり、

[図173]図１７３は、処理フラグの判定処理を示すフローチャートであり、

[図174]図１７４は、処理フラグの判定処理を示すフローチャートであり、

[図175]図１７５は、進捗状態の同期制御部の機能ブロック図であり、

[図176]図１７６は、進捗状態の同期制御部の機能ブロック図であり、

[図177]図１７７は、進捗状態信号を送受信する態様を示す図であり、

[図178]図１７８は、進捗状態の同期制御処理を示すフローチャートであり、

[図179]図１７９は、進捗状態の同期制御処理を示すフローチャートであり、

[図180]図１８０は、進捗状態の表示処理を示すフローチャートであり、

[図181]図１８１は、表示制御情報の送信制御部の機能ブロック図であり、

[図182]図１８２は、表示制御情報の送信制御処理を示すフローチャートであり、

[図183]図１８３は、表示制御情報の受信制御部の機能ブロック図であり、

[図184]図１８４は、表示制御情報の受信制御処理を示すフローチャートであり、

[図185]図１８５は、配信諸元データに含まれる情報を示す図であり、

[図186]図１８６は、進捗表示の画面表示制御部の機能ブロック図であり、

[図187]図１８７は、書換え諸元データを示す図であり、

[図188]図１８８は、メニュー選択時の画面を示す図であり、

[図189]図１８９は、ユーザ選択時の画面を示す図であり、

[図190]図１９０は、ユーザ登録時の画面を示す図であり、

[図191]図１９１は、進捗表示の画面表示制御処理を示すフローチャートであ

り、

[図192]図１９２は、進捗表示の画面表示制御処理を示すフローチャートであり、

[図193]図１９３は、メッセージフレームを示す図であり、

[図194]図１９４は、アクティベート承諾時の画面を示す図であり、

[図195]図１９５は、項目の表示有無の設定を示す図であり、

[図196]図１９６は、項目の表示有無の設定を示す図であり、

[図197]図１９７は、アクティベート承諾時の画面を示す図であり、

[図198]図１９８は、データ通信の態様を示す図であり、

[図199]図１９９は、キャンペーン通知時のメッセージフレームを示す図であり、

[図200]図２００は、ダウンロード承諾時のメッセージフレームを示す図であり、

[図201]図２０１は、インストール承諾時のメッセージフレームを示す図であり、

[図202]図２０２は、アクティベート承諾時のメッセージフレームを示す図であり、

[図203]図２０３は、画面の遷移を示す図であり、

[図204]図２０４は、キャンペーン通知発生時の画面を示す図であり、

[図205]図２０５は、ダウンロード承諾時の画面を示す図であり、

[図206]図２０６は、ダウンロード承諾時の画面を示す図であり、

[図207]図２０７は、ダウンロード実行中の画面を示す図であり、

[図208]図２０８は、ダウンロード完了時の画面を示す図であり、

[図209]図２０９は、インストール承諾時の画面を示す図であり、

[図210]図２１０は、アクティベート承諾時の画面を示す図であり、

[図211]図２１１は、プログラム更新の報知制御部の機能ブロック図であり、

[図212]図２１２は、プログラム更新の報知制御処理を示すフローチャートであり、

[図213]図２１３は、インジケータの報知態様を示す図であり、

[図214]図２１４は、書換え対象が２面メモリの場合の報知態様の遷移を示す図であり、

[図215]図２１５は、書換え対象が１面サスペンドメモリの場合の報知態様の遷移を示す図であり、

[図216]図２１６は、書換え対象が１面単独メモリの場合の報知態様の遷移を示す図であり、

[図217]図２１７は、接続態様を示す図であり、

[図218]図２１８は、ＣＧＷにおける電源自己保持の実行制御部の機能ブロックであり、

[図219]図２１９は、ＥＣＵにおける電源自己保持の実行制御部の機能ブロックであり、

[図220]図２２０は、ＣＧＷにおける電源自己保持の実行制御処理を示すフローチャートであり、

[図221]図２２１は、ＥＣＵにおける電源自己保持の実行制御処理を示すフローチャートであり、

[図222]図２２２は、電源自己保持を必要とする期間を示す図であり、

[図223]図２２３は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図224]図２２４は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図225]図２２５は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図226]図２２６は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図227]図２２７は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図228]図２２８は、アプリプログラムを書換える態様を示す全体シーケンス

図であり、

[図229]図２２９は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図230]図２３０は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図231]図２３１は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図232]図２３２は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図233]図２３３は、アプリプログラムを書換える態様を示す全体シーケンス図であり、

[図234]図２３４は、第１実施形態において、車両情報通信システムの全体構成を示す図であり、

[図235]図２３５は、ＣＧＷの電気的な構成を示す図であり、

[図236]図２３６は、ＥＣＵの電気的な構成を示す図であり、

[図237]図２３７は、電源ラインの接続態様を示す図であり、

[図238]図２３８は、リプログデータ及び配信緒元データをパッケージ化する態様を示す図であり、

[図239]図２３９は、配信パッケージをアンパッケージ化する態様を示す図であり、

[図240]図２４０は、センター装置における主としてサーバの各機能に係る部分をブロック図化して示す図であり、

[図241]図２４１は、センター装置における処理の流れを示すイメージ図であり、

[図242]図２４２は、構成情報ＤＢに登録される車両の構成情報の一例を示す図であり、

[図243]図２４３は、ＥＣＵリプロデータＤＢに登録されるプログラムやデータの一例を示す図であり、

[図244]図２４４は、ＥＣＵメタデータＤＢに登録される諸元データの一例を示す図であり、

[図245]図２４５は、個車情報ＤＢに登録される車両の構成情報の一例を示す図であり、

[図246]図２４６は、パッケージＤＢに登録される配信パッケージデータの一例を示す図であり、

[図247]図２４７は、キャンペーンＤＢに登録されるキャンペーンデータの一例を示す図であり、

[図248]図２４８は、ＥＣＵリプロデータＤＢに登録されるプログラムやデータを生成する処理を示すフローチャートであり、

[図249]図２４９は、ＥＣＵメタデータＤＢに登録される諸元データの一例を生成する処理を示すフローチャートであり、

[図250]図２５０は、諸元データの一例を示す図であり、

[図251]図２５１は、バス負荷テーブルの一例を示す図であり、

[図252]図２５２は、パッケージＤＢに登録される配信パッケージを生成する処理を示すフローチャートであり、

[図253]図２５３は、パッケージファイルの内容をイメージ的に示す図であり、

[図254]図２５４は、第２実施形態において、センター装置と車両側システムとの間で実行される処理手順を示すシーケンス図であり、

[図255]図２５５は、センター装置が行う処理を示すフローチャートであり、

[図256]図２５６は、図２４８に示すフローチャートのステップＤ６，Ｄ７で行う処理内容をイメージ的に示す図であり、

[図257]図２５７は、車両側システムからセンター装置にハッシュ値を送信する場合の処理を示すフローチャートであり、

[図258]図２５８は、第３実施形態において、センター装置と車両側システムとの間で実行される処理手順を示すシーケンス図であり、

[図259]図２５９は、センター装置が行う処理を示すフローチャートであり、

[図260]図２６０は、センター装置がＳＭＳにより、ＥＶ車とコンベ車とにそれぞれ通知を行う状態を示すシーケンス図であり、

[図261]図２６１は、第４実施形態において、センター装置と車両側システムとの間で実行される処理手順を示すシーケンス図であり、

[図262]図２６２は、第５実施形態において、サプライヤ、センター装置、車両側システム間で行う処理をイメージ的に示す図であり、

[図263]図２６３は、サプライヤ、センター装置、車両側システム間で行う処理手順を示すシーケンス図（その１）であり、

[図264]図２６４は、サプライヤ、センター装置、車両側システム間で行う処理手順を示すシーケンス図（その２）であり、

[図265]図２６５は、サプライヤ、センター装置、車両側システム間で行う処理手順を示すシーケンス図（その３）であり、

[図266]図２６６は、第１実施形態の変形（その１）であり、１つのキャンペーンに複数のパッケージを対応させる場合のパッケージＤＢのデータフォーマットを示す図

[図267]図２６７は、１つのキャンペーンに複数のパッケージを対応させる場合のキャンペーンＤＢのデータフォーマットを示す図であり、

[図268]図２６８は、諸元データをグループ毎に生成する場合の図２４２相当図であり、

[図269]図２６９は、配信パッケージをグループ毎に生成する場合の図２４５相当図であり、

[図270]図２７０は、第１実施形態の変形（その２）であり、パッケージ生成ツールの処理内容を示す図である。

発明を実施するための形態

[0012] 以下、一実施形態について図面を参照して説明する。車両用プログラム書換えシステム（車両用電子制御システムに相当する）は、電子制御装置（以下、ＥＣＵ（Electronic Control Unit）と称する）に搭載されている車両制御や診断等のアプリプログラムをＯＴＡ（Over The Air）により書換え可能

なシステムである。本実施形態では、アプリプログラムを有線又は無線で書換える場合について説明するが、例えば地図アプリで使用される地図データ、ＥＣＵで使用される制御パラメータ等、各種アプリで使用されるデータを有線又は無線で書換える場合にも適用することができる。

[0013] 有線でのアプリプログラムの書換えは、アプリプログラムを車両外部から有線を介して取得して書換えることに加え、アプリプログラムが実行される際に使用される各種データを車両外部から有線を介して取得して書換えることも含む。無線でのアプリプログラムの書換えは、アプリプログラムを車両外部から無線を介して取得して書換えることに加え、アプリプログラムが実行される際に使用される各種データを車両外部から無線を介して取得して書換えることも含む。

[0014] 図１に示すように、車両用プログラム書換えシステム１は、通信ネットワーク２側のセンター装置３と、車両側の車両側システム４と、表示端末５とを有する。通信ネットワーク２は、例えば４Ｇ回線等による移動体通信ネットワーク、インターネット、ＷｉＦｉ（Wireless Fidelity）（登録商標）等を含んで構成される。尚、本実施形態では、主として車両側の構成について説明し、センター装置３の構成については図２３４から図２７０において詳述する。

[0015] 表示端末５は、ユーザからの操作入力を受付ける機能や各種画面を表示する機能を有する端末であり、例えばユーザが携帯可能なスマートフォンやタブレット等の携帯端末６、車室内に配置されている車載ディスプレイ７である。携帯端末６は、移動体通信ネットワークの通信圏内であれば、通信ネットワーク２を介してセンター装置３とデータ通信可能である。車載ディスプレイ７は、車両側システム４に接続されており、ナビゲーション機能を兼用する構成であっても良い。又、車載ディスプレイ７は、ＥＣＵの機能を有する車載ディスプレイＥＣＵであっても良し、センターディスプレイやメータディスプレイ等への表示を制御する機能を有していても良い。

[0016] ユーザは、車室外であって移動体通信ネットワークの通信圏内であれば、

アプリプログラムの書換えに関与する各種画面を携帯端末６により確認しながら操作入力を行い、アプリプログラムの書換えに関与する手続きを可能である。ユーザは、車室内では、アプリプログラムの書換えに関与する各種画面を車載ディスプレイ７により確認しながら操作入力を行い、アプリプログラムの書換えに関与する手続きを可能である。即ち、ユーザは、車室外と車室内で携帯端末６と車載ディスプレイ７を使い分け、アプリプログラムの書換えに関与する手続きを可能である。

[0017] センター装置３は、車両用プログラム書換えシステム１において通信ネットワーク２側のプログラム更新機能を統括し、ＯＴＡセンターとして機能する。センター装置３は、ファイルサーバ８と、ウェブサーバ９と、管理サーバ１０とを有し、各サーバ８～１０が相互にデータ通信可能に構成されている。即ち、センター装置３は、機能毎に異なる複数のサーバを含んで構成されている。

[0018] ファイルサーバ８は、センター装置３から車両側システム４に配信されるアプリプログラムのファイルを管理するサーバである。ファイルサーバ８は、センター装置３から車両側システム４に配信されるアプリプログラムの提供事業者であるサプライヤ等から提供される更新データ（以下、リプログデータ、書込みデータとも称する）、ＯＥＭ（Original Equipment Manufacturer）から提供される配信諸元データ、車両側システム４から取得する車両状態等を管理する。ファイルサーバ８は、通信ネットワーク２を介して車両側システム４との間でデータ通信可能であり、配信パッケージのダウンロード要求が発生すると、リプログデータと配信諸元データとが１つのファイルにパッケージ化された配信パッケージを車両側システム４に送信する。

[0019] ウェブサーバ９は、ウェブ情報を管理するサーバである。ウェブサーバ９は、携帯端末６等が有するウェブブラウザからの要求に応じて自己が管理するウェブデータを送信する。管理サーバ１０は、アプリプログラムの書換えのサービスに登録しているユーザの個人情報、車両毎のアプリプログラムの書換え履歴等を管理するサーバである。

[0020] 車両側システム４は、マスタ装置１１（車両用マスタ装置に相当する）を有する。マスタ装置１１は、ＤＣＭ（Data Communication Module）１２（車載通信機に相当する）と、ＣＧＷ（Central Gate Way）１３（車両用ゲートウェイ装置に相当する）とを有する。ＤＣＭ１２とＣＧＷ１３とは、第１バス１４を介してデータ通信可能に接続されている。ＤＣＭ１２は、センター装置３との間で通信ネットワーク２を介してデータ通信を行う。ＤＣＭ１２は、ファイルサーバ８から配信パッケージをダウンロードすると、そのダウンロードした配信パッケージから書込みデータを抽出し、その抽出した書込みデータをＣＧＷ１３に転送する。

[0021] ＣＧＷ１３は、データ中継機能を有し、ＤＣＭ１２から書込みデータを取得すると、その取得した書込みデータの書込みをアプリプログラムの書換え対象である書換え対象ＥＣＵに指示し、書込みデータを書換え対象ＥＣＵに配信する。又、ＣＧＷ１３は、書換え対象ＥＣＵにおいて書込みデータの書込みが完了し、アプリプログラムの書換えが完了すると、その書換え完了後のアプリプログラムを有効とするアクティベートを書換え対象ＥＣＵに指示する。

[0022] マスタ装置１１は、車両用プログラム書換えシステム１において車両側のプログラム更新機能を統括し、ＯＴＡマスタとして機能する。尚、図１では、ＤＣＭ１２と車載ディスプレイ７が同一の第１バス１４に接続されている構成を例示しているが、ＤＣＭ１２と車載ディスプレイ７とが別々のバスに接続されている構成でも良い。又、ＤＣＭ１２の機能の一部又は全体をＣＧＷ１３が有する構成でも良いし、ＣＧＷ１３の機能の一部又は全体をＤＣＭ１２が有する構成でも良い。即ち、マスタ装置１１において、ＤＣＭ１２とＣＧＷ１３との機能分担がどのように構成されていても良い。マスタ装置１１は、ＤＣＭ１２及びＣＧＷ１３の２つのＥＣＵから構成されても良いし、ＤＣＭ１２の機能とＣＧＷ１３の機能とを有する１つの統合ＥＣＵで構成されても良い。

[0023] ＣＧＷ１３には、第１バス１４に加え、第２バス１５と、第３バス１６と

、第４バス１７と、第５バス１８とが車内側のバスとして接続されており、バス１５～１７を介して各種ＥＣＵ１９が接続されていると共に、バス１８を介して電源管理ＥＣＵ２０が接続されている。

[0024] 第２バス１５は、例えばボディ系ネットワークのバスである。第２バス１５に接続されているＥＣＵ１９は、ボディ系の制御を行うＥＣＵである。ボディ系の制御を行うＥＣＵは、例えばドアのロック／アンロックを制御するドアＥＣＵ、メータディスプレイへの表示を制御するメータＥＣＵ、エアコンの駆動を制御するエアコンＥＣＵ、ウィンドウの開閉を制御するウィンドウＥＣＵ、車両の盗難防止のために駆動するセキュリティＥＣＵ等である。

[0025] 第３バス１６は、例えば走行系ネットワークのバスである。第３バス１６に接続されているＥＣＵ１９は、走行系の制御を行うＥＣＵである。走行系の制御を行うＥＣＵは、例えばエンジンの駆動を制御するエンジンＥＣＵ、ブレーキの駆動を制御するブレーキＥＣＵ、自動変速機の駆動を制御するＥＣＴ（Electronic Controlled Transmission）ＥＣＵ、パワーステアリングの駆動を制御するパワーステアリングＥＣＵ等である。

[0026] 第４バス１７は、例えばマルチメディア系ネットワークのバスである。第４バス１７に接続されているＥＣＵ１９は、マルチメディア系の制御を行うＥＣＵである。マルチメディア系の制御を行うＥＣＵは、例えばナビゲーションシステムを制御するためのナビゲーションＥＣＵ、電子式料金収受システム（ＥＴＣ（Electronic Toll Collection System、登録商標））を制御するＥＴＣＥＣＵ等である。バス１５～１７は、ボディ系ネットワークのバス、走行系ネットワークのバス、マルチメディア系ネットワークのバス以外の系統のバスであっても良い。又、バスの本数やＥＣＵ１９の個数は例示した構成に限らない。電源管理ＥＣＵ２０は、ＤＣＭ１２、ＣＧＷ１３、各種ＥＣＵ１９等に供給する電源を管理するＥＣＵである。

[0027] ＣＧＷ１３には、第６バス２１が車外側のバスとして接続されている。第６バス２１には、ツール２３（サービスツールに相当する）が着脱可能に接続されるＤＬＣ（Data Link Coupler）コネクタ２２が接続されている。車内

側のバス１４～１８及び車外側のバス２１は、例えばＣＡＮ（Controller Area Network、登録商標）バスにより構成されており、ＣＧＷ１３は、ＣＡＮのデータ通信規格や診断通信規格（ＵＤＳ（Unified Diagnosis Services）：ＩＳＯ１４２２９）にしたがってＤＣＭ１２と、各種ＥＣＵ１９と、ツール２３との間でデータ通信を行う。尚、ＤＣＭ１２とＣＧＷ１３とがイーサーネットにより接続されていても良いし、ＤＬＣコネクタ２２とＣＧＷ１３とがイーサーネットにより接続されても良い。

[0028] 書換え対象ＥＣＵ１９は、ＣＧＷ１３から書込みデータを受信すると、その受信した書込みデータをフラッシュメモリ（不揮発性メモリに相当する）に書込んでアプリプログラムを書換える。上記した構成では、ＣＧＷ１３は、書換え対象ＥＣＵ１９から書込みデータの取得要求を受信すると、書込みデータを書換え対象ＥＣＵ１９に配信するリプログマスタとして機能する。書換え対象ＥＣＵ１９は、ＣＧＷ１３から書込みデータを受信すると、その受信した書込みデータをフラッシュメモリに書込んでアプリプログラムを書換えるリプログスレーブとして機能する。

[0029] アプリプログラムを書換える態様としては、有線で書換える態様と、無線で書換える態様とがある。アプリプログラムを有線で書換える態様とは、車両外部から有線を介して取得したアプリプログラムを用いて書換え対象ＥＣＵ１９を書換える態様である。具体的には、ツール２３がＤＬＣコネクタ２２に接続されると、ツール２３は、書込みデータをＣＧＷ１３に転送する。ＣＧＷ１３は、ゲートウェイとして機能し、有線書換え要求を書換え対象ＥＣＵ１９に送信し、書込みデータの書込み（インストール）を書換え対象ＥＣＵ１９に指示し、ツール２３から転送された書込みデータを書換え対象ＥＣＵ１９に配信する。書込みデータを書換え対象ＥＣＵ１９に配信することは、書込みデータを中継することである。

[0030] アプリプログラムを無線で書換える態様とは、車両外部から無線を介して取得したアプリプログラムを用いて書換え対象ＥＣＵ１９を書換える態様である。具体的には、ＤＣＭ１２は、ファイルサーバ８から配信パッケージを

ダウンロードすると、そのダウンロードした配信パッケージから書込みデータを抽出し、その書込みデータをＣＧＷ１３に転送する。ＣＧＷ１３は、書換えツールとして機能し、書込みデータの書込み（インストール）を書換え対象ＥＣＵ１９に指示し、ＤＣＭ１２から転送された書込みデータを書換え対象ＥＣＵ１９に配信する。

[0031] ＥＣＵ１９を診断する態様としては、有線で診断する態様と、無線で診断する態様とがある。有線で診断する態様とは、車両外部から有線を介してＥＣＵ１９を診断する態様である。具体的には、ツール２３がＤＬＣコネクタ２２に接続されると、ツール２３は、診断要求をＣＧＷ１３に転送する。ＣＧＷ１３は、ゲートウェイとして機能し、診断要求を診断対象ＥＣＵ１９に送信し、ツール２３から転送された診断コマンドを診断対象ＥＣＵ１９に配信する。診断対象ＥＣＵ１９は、ＣＧＷ１３から受信した診断コマンドに応じた診断処理を行う。

[0032] 無線で診断する態様とは、車両外部から無線を介してＥＣＵ１９を診断する態様である。具体的には、センター装置３からＤＣＭ１２に診断要求として診断コマンドが送信されると、ＤＣＭ１２は、診断コマンドをＣＧＷ１３に転送する。ＣＧＷ１３は、ゲートウェイとして機能し、診断要求として診断コマンドを診断対象ＥＣＵ１９に配信する。診断対象ＥＣＵは、ＣＧＷ１３から受信した診断コマンドに応じた診断処理を行う。

[0033] 図２に示すように、ＣＧＷ１３は、電気的な機能ブロックとして、マイクロコンピュータ（以下、マイコンと称する）２４と、データ転送回路２５と、電源回路２６と、電源検出回路２７とを有する。マイコン２４は、ＣＰＵ（Central Processing Unit）２４ａと、ＲＯＭ（Read Only Memory）２４ｂと、ＲＡＭ（Random Access Memory）２４ｃと、フラッシュメモリ２４ｄとを有する。フラッシュメモリ２４ｄには、ＣＧＷ１３の外部から情報の読出しが不可であるセキュア領域が含まれる。マイコン２４は、非遷移的実体的記憶媒体に格納されている各種制御プログラムを実行して各種処理を行い、ＣＧＷ１３の動作を制御する。

[0034] データ転送回路２５は、バス１４～１８，２１との間のＣＡＮのデータ通信規格や診断通信規格に準拠したデータ通信を制御する。電源回路２６は、バッテリ電源（以下、＋Ｂ電源と称する）、アクセサリ電源（以下、ＡＣＣ電源と称する）、イグニッション電源（以下、ＩＧ電源と称する）を入力する。電源検出回路２７は、電源回路２６が入力する＋Ｂ電源の電圧値、ＡＣＣ電源の電圧値、ＩＧ電源の電圧値を検出し、これらの検出した電圧値を所定の電圧閾値と比較し、その比較結果をマイコン２４に出力する。マイコン２４は、電源検出回路２７から入力する比較結果により、外部からＣＧＷ１３に供給されている＋Ｂ電源、ＡＣＣ電源、ＩＧ電源が正常であるか異常であるかを判定する。

[0035] 図３に示すように、ＤＣＭ１２は、電気的な機能ブロックとして、マイコン２８と、無線回路２９と、データ転送回路３０と、電源回路３１と、電源検出回路３２とを有する。マイコン２８は、ＣＰＵ２８ａと、ＲＯＭ２８ｂと、ＲＡＭ２８ｃと、フラッシュメモリ２８ｄとを有する。フラッシュメモリ２８ｄには、ＤＣＭ１２の外部から情報の読出しが不可であるセキュア領域が含まれる。マイコン２８は、非遷移的実体的記憶媒体に格納されている各種制御プログラムを実行して各種処理を行い、ＤＣＭ１２の動作を制御する。センター装置３からダウンロードするデータを保存するためのフラッシュメモリは、ＣＧＷ１３に配置しても良い。

[0036] 無線回路２９は、センター装置３との通信ネットワーク２を介したデータ通信を制御する。データ転送回路３０は、バス１４とのＣＡＮのデータ通信規格に準拠したデータ通信を制御する。電源回路３１は、＋Ｂ電源、ＡＣＣ電源、ＩＧ電源を入力する。電源検出回路３２は、電源回路３１が入力する＋Ｂ電源の電圧値、ＡＣＣ電源の電圧値、ＩＧ電源の電圧値を検出し、これらの検出した電圧値を所定の電圧閾値と比較し、その比較結果をマイコン２８に出力する。マイコン２８は、電源検出回路３２から入力する比較結果により、外部からＤＣＭ１２に供給されている＋Ｂ電源、ＡＣＣ電源、ＩＧ電源が正常であるか異常であるかを判定する。

[0037] 又、ＤＣＭ１２は、例えばＧＰＳ（Global Positioning System）により車両位置を検出する車両位置検出機能を有する。ＤＣＭ１２のフラッシュメモリ２８ｄは、センター装置３からダウンロードした配信パッケージを記憶可能な十分なメモリ容量を有し、ＣＧＷ１３のフラッシュメモリ２４ｄよりも大きいメモリ容量を有する。即ち、ＤＣＭ１２のフラッシュメモリ２８ｄが十分なメモリ容量を有する構成であることにより、ＣＧＷ１３のフラッシュメモリ２４ｄが十分なメモリ容量を有する構成でなくても、マスタ装置１１において、センター装置３から配信パッケージをダウンロードし、そのダウンロードした配信パッケージをＤＣＭ１２に蓄積しておくことが可能である。

[0038] 図４に示すように、ＥＣＵ１９は、電気的な機能ブロックとして、マイコン３３と、データ転送回路３４と、電源回路３５と、電源検出回路３６とを有する。マイコン３３は、ＣＰＵ２８ａと、ＲＯＭ２８ｂと、ＲＡＭ３３ｃと、フラッシュメモリ２８ｄとを有する。フラッシュメモリ２８ｄには、ＥＣＵ１９の外部から情報の読出しが不可であるセキュア領域が含まれる。マイコン３３は、非遷移的実体的記憶媒体に格納されている各種制御プログラムを実行して各種処理を行い、ＥＣＵ１９の動作を制御する。

[0039] データ転送回路３４は、バス１５～１７との間のＣＡＮのデータ通信規格に準拠したデータ通信を制御する。電源回路３５は、＋Ｂ電源、ＡＣＣ電源、ＩＧ電源を入力する。電源検出回路３６は、電源回路３５が入力する＋Ｂ電源の電圧値、ＡＣＣ電源の電圧値、ＩＧ電源の電圧値を検出し、これらの検出した電圧値を所定の電圧閾値と比較し、その比較結果をマイコン３３に出力する。マイコン３３は、電源検出回路２７から入力する比較結果により、外部からＥＣＵ１９に供給されている＋Ｂ電源、ＡＣＣ電源、ＩＧ電源が正常であるか異常であるかを判定する。尚、ＥＣＵ１９は、自己が接続する例えばセンサやアクチュエータ等の負荷が異なり、基本的には同等の構成である。

[0040] 車載ディスプレイ７は、図４に示すＥＣＵ１９と同様の構成を有する。電

源管理ＥＣＵ２０は、図４に示すＥＣＵ１９と同様の構成を有する。電源管理ＥＣＵ２０は、後述する電源制御回路４３との間でデータ通信可能に接続される。

[0041] 図５に示すように、電源管理ＥＣＵ２０、ＣＧＷ１３、ＥＣＵ１９は、電源供給ラインである＋Ｂ電源ライン３７、ＡＣＣ電源ライン３８、ＩＧ電源ライン３９に接続されている。＋Ｂ電源ライン３７は、車両バッテリ４０の正極に接続されている。ＡＣＣ電源ライン３８は、ＡＣＣスイッチ４１を介して車両バッテリ４０の正極に接続されている。ユーザがＡＣＣ操作を行うと、ＡＣＣスイッチ４１がオフからオンに切替わり、車両バッテリ４０の出力電圧がＡＣＣ電源ライン３８に印加される。ＡＣＣ操作とは、例えばキーを差込口に挿入する型の車両であれば、キーを差込口に挿入して「ＯＦＦ」位置から「ＡＣＣ」位置に回動する操作であり、スタートボタンを押下する型の車両であれば、スタートボタンを１回押下する操作である。

[0042] ＩＧ電源ライン３９は、ＩＧスイッチ４２を介して車両バッテリ４０の正極に接続されている。ユーザがＩＧ操作を行うと、ＩＧスイッチ４２がオフからオンに切替わり、車両バッテリ４０の出力電圧がＩＧ電源ライン３９に印加される。ＩＧ操作とは、例えばキーを差込口に挿入する型の車両であれば、キーを差込口に挿入して「ＯＦＦ」位置から「ＯＮ」位置に回動する操作であり、スタートボタンを押下する型の車両であれば、スタートボタンを２回押下する操作である。車両バッテリ４０の負極は接地されている。

[0043] ＡＣＣスイッチ４１とＩＧスイッチ４２との両方がオフであるときには、＋Ｂ電源だけが車両側システム４に供給される。＋Ｂ電源だけが車両側システム４に供給されている状態を＋Ｂ電源状態と称する。ＡＣＣスイッチ４１がオンであり、ＩＧスイッチ４２がオフであるときには、ＡＣＣ電源と＋Ｂ電源とが車両側システム４に供給される。ＡＣＣ電源と＋Ｂ電源とが車両側システム４に供給されている状態をＡＣＣ電源状態と称する。ＡＣＣスイッチ４１とＩＧスイッチ４２との両方がオンであるときには、＋Ｂ電源とＡＣＣ電源とＩＧ電源とが車両側システム４に供給される。＋Ｂ電源とＡＣＣ電

源とＩＧ電源とが車両側システム４に供給されている状態をＩＧ電源状態と称する。又、上記した各電源状態に加え、無線によるプログラム更新に適した電源を与える電源状態等も考えられる。

[0044] ＥＣＵ１９は、電源状態に応じて起動条件が異なり、＋Ｂ電源状態で起動する＋Ｂ電源系ＥＣＵ、ＡＣＣ電源状態で起動するＡＣＣ系ＥＣＵ、ＩＧ電源状態で起動するＩＧ系ＥＣＵに区分される。例えば車両盗難等の用途で駆動するＥＣＵ１９は、＋Ｂ電源系ＥＣＵに区分される。例えばオーディオ等の非走行系の用途で駆動するＥＣＵ１９は、ＡＣＣ系ＥＣＵに区分される。例えばエンジン制御等の走行系の用途で駆動するＥＣＵ１９は、ＩＧ系ＥＣＵに区分される。

[0045] ＋Ｂ電源系ＥＣＵは、＋Ｂ電源ライン３７、ＡＣＣ電源ライン３８及びＩＧ電源ライン３９に接続され、＋Ｂ電源状態のときには＋Ｂ電源ライン３７を選択し、ＡＣＣ電源状態のときにはＡＣＣ電源ライン３８を選択し、ＩＧ電源状態のときにはＩＧ電源ライン３９を選択するように構成される。ＡＣＣ系ＥＣＵは、ＡＣＣ電源ライン３８及びＩＧ電源ライン３９に接続され、ＡＣＣ電源状態のときにはＡＣＣ電源ライン３８を選択し、ＩＧ電源状態のときにはＩＧ電源ライン３９を選択するように構成される。ＩＧ系ＥＣＵは、ＩＧ電源ライン３９に接続される。

[0046] ＣＧＷ１３は、スリープ状態にあるＥＣＵ１９に起動要求を送信することで、その起動要求の送信先のＥＣＵ１９をスリープ状態から起動状態に移行させる。又、ＣＧＷ１３は、起動状態にあるＥＣＵ１９にスリープ要求を送信することで、そのスリープ要求の送信先のＥＣＵ１９を起動状態からスリープ状態に移行させる。ＣＧＷ１３は、例えばバス１５～１７に送信する送信信号の波形を異ならせることで、特定のＥＣＵ１９を起動状態又はスリープ状態に移行させることが可能である。即ち、ＥＣＵ１９毎に起動要求波形及びスリープ要求波形が予め定められており、ＥＣＵ１９は、自己に適合する起動要求波形を受信すると、スリープ状態から起動状態に移行し、ＣＧＷ１３から自己に適合するスリープ要求波形を受信すると、起動状態からスリ

ープ状態に移行する。

[0047] ＣＧＷ１３は、例えばＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）が起動状態の場合に第１波形を送信することで、ＥＣＵ（ＩＤ１）を起動状態からスリープ状態に移行させ、ＥＣＵ（ＩＤ２）を起動状態に保持する。又、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）が起動状態の場合に第２波形を送信することで、ＥＣＵ（ＩＤ１）を起動状態に保持し、ＥＣＵ（ＩＤ２）を起動状態からスリープ状態に移行させる。

[0048] ＡＣＣスイッチ４１及びＩＧスイッチ４２に対して電源制御回路４３が並列接続されている。ＣＧＷ１３は、電源制御要求を電源管理ＥＣＵ２０に送信し、電源管理ＥＣＵ２０に電源制御回路４３を制御させる。即ち、ＣＧＷ１３は、電源制御要求として電源起動要求を電源管理ＥＣＵ２０に送信することで、ＡＣＣ電源ライン３８やＩＧ電源ライン３９と車両バッテリ４０の正極を電源制御回路４３の内部で接続させる。この状態では、ＡＣＣスイッチ４１やＩＧスイッチ４２がオフであってもＡＣＣ電源やＩＧ電源が車両側システム４に供給される。又、ＣＧＷ１３は、電源制御要求として電源停止要求を電源管理ＥＣＵ２０に送信することで、ＡＣＣ電源ライン３８やＩＧ電源ライン３９と車両バッテリ４０の正極を電源制御回路４３の内部で途絶させる。

[0049] ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９、電源管理ＥＣＵ２０は、それぞれ電源自己保持回路を有し、車両バッテリ４０からの電源供給を保持する電源自己保持機能を有する。即ち、ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９は、電源管理ＥＣＵ２０は、起動状態にあるときに車両電源がＡＣＣ電源又はＩＧ電源から＋Ｂ電源に切替わると、その切替わった直後に起動状態から停止状態又はスリープ状態に移行するのではなく、車両バッテリ４０からの電源供給により起動状態を所定時間（例えば数分間）に亘って継続して駆動電源を自己保持する。ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９、電源管理ＥＣＵ２０は、車両電源がＡＣＣ電源又はＩＧ電源から＋Ｂ電源に切替わった直後から所定時間が経過した後に起動状態から停止状態又はスリープ状態に移行する

。例えばエンジン制御系のＥＣＵ１９であれば、車両電源がＡＣＣ電源又はＩＧ電源から＋Ｂ電源に切替わった後に電源自己保持機能が作動することで、車両走行中に取得したエンジン制御に関する各種データをログとして記憶する。

[0050] 次に、センター装置３からマスタ装置１１に配信される配信パッケージについて説明する。図６に示すように、車両用プログラム書換えシステム１においては、アプリプログラムの提供事業者であるサプライヤから提供される書込みデータと、ＯＥＭから提供される書換え諸元データ（諸元データに相当する）とからリプログデータが生成される。書換え諸元データについては、センター装置３で生成しても良い。サプライヤから提供される書込みデータとしては、旧アプリプログラムと新アプリプログラムとの差分に相当する差分データと、新アプリプログラムの全体に相当する全データとがある。差分データや全データは周知のデータ圧縮技術により圧縮されていても良い。図６では、サプライヤＡ～Ｃから書込みデータとして差分データが提供され、サプライヤＡから提供されるＥＣＵ（ＩＤ１）の暗号済みの差分データと認証子、サプライヤＢから提供されるＥＣＵ（ＩＤ２）の暗号済みの差分データと認証子、サプライヤＣから提供されるＥＣＵ（ＩＤ３）の暗号済みの差分データと認証子、ＯＥＭから提供される書換え諸元データからリプログデータが生成されている場合を例示している。

[0051] 認証子は、差分データの完全性を検証するために書込みデータ毎に付与されるデータであり、例えばＥＣＵ（ＩＤ）と、そのＥＣＵ（ＩＤ）に紐付く鍵情報と、差分データとから生成される。ここで、アプリプログラムの書換えが途中でキャンセルされる場合に備え、旧バージョンへの書戻し（ロールバック）用の書込みデータがリプログデータに含まれていても良い。

[0052] ＯＥＭから提供される書換え諸元データは、アプリプログラムの書換えに関与する情報として、書換え対象ＥＣＵ１９を特定可能な情報、書換え対象ＥＣＵ１９が複数の場合の書換え順序を特定可能な情報、後述するロールバック方法を特定可能な情報等を含む。書換え諸元データは、ＤＣＭ１２、Ｃ

ＧＷ１３、書換え対象ＥＣＵ１９等における書換えに関与する動作を定義するデータである。書換え諸元データは、ＤＣＭ１２が使用するＤＣＭ用の書換え諸元データと、ＣＧＷ１３が使用するＣＧＷ用の書換え諸元データとに区分される。

[0053] 図７に示すように、ＤＣＭ用の書換え諸元データは、諸元データ情報と、ＥＣＵ情報とを含む。諸元データ情報は、アドレス情報と、ファイル名とを含む。ＥＣＵ情報は、各書換え対象ＥＣＵ１９の更新プログラム（書込みデータ）をＣＧＷ１３に送信する際に参照するアドレス情報等を書換え対象ＥＣＵ１９の個数分だけ含む。具体的には、ＥＣＵ情報は、ＥＣＵを識別するＩＤ（ＥＣＵ（ＩＤ））と、更新プログラムを取得する際の参照アドレス（更新プログラム取得アドレス）と、更新プログラムサイズと、ロールバックプログラムを取得する際の参照アドレス（ロールバックプログラム取得アドレス）と、ロールバックプログラムサイズとを少なくとも含む。ロールバックプログラムは、アプリプログラムの書換えが途中でキャンセルされた際に、アプリプログラムを元のバージョンに戻すためのプログラム（書込みデータ）である。

[0054] 図８に示すように、ＣＧＷ用の書換え諸元データは、グループ情報と、バス負荷テーブルと、バッテリ負荷と、書換え時の車両状態と、ＥＣＵ情報とを含む。ＣＧＷ用の書換え諸元データは、これらの他に、書き換え手順情報や表示のシーン情報等を含んでいても良い。グループ情報は、書換え対象ＥＣＵ１９の属するグループ及び書換え順序を示す情報であり、例えば第１グループ情報として、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）の順序でアプリプログラムを書換える旨、第２グループ情報として、ＥＣＵ（ＩＤ４）、ＥＣＵ（ＩＤ５）、ＥＣＵ（ＩＤ６）の順序でアプリプログラムを書換える旨が規定されている。バス負荷テーブルは、後述する図１００に示すテーブルであり、詳細については後述する。バッテリ負荷は、車両において許容可能な車両バッテリ４０のバッテリ残量の下限値を示す情報である。書換え時の車両状態は、車両状態がどのような場合に書換えを行うか

を示す情報である。

[0055] ＥＣＵ情報は、書換え対象ＥＣＵ１９に関する情報であり、ＥＣＵ＿ＩＤ（装置識別情報に相当する）と、接続バス（バス識別情報に相当する）と、接続電源と、セキュリティアクセス鍵情報と、メモリ種別と、書換え方法と、電源自己保持時間と、書換え面情報と、更新プログラムバージョンと、更新プログラム取得アドレスと、更新プログラムサイズと、ロールバックプログラムバージョンと、ロールバックプログラム取得アドレスと、ロールバックプログラムサイズと、書込みデータ種別とを少なくとも含む。

[0056] 接続バスは、ＥＣＵ１９が接続されるバスを示す。接続電源は、ＥＣＵ１９が接続される電源ラインを示す。セキュリティアクセス鍵情報は、ＣＧＷ１３が書換え対象ＥＣＵ１９にアクセスするための認証に用いる鍵情報を示し、乱数値又はユニークな情報、鍵パターン、復号演算パターンを含む。メモリ種別は、書換え対象ＥＣＵ１９に搭載されているメモリが１面単独メモリ、１面サスペンドメモリ（疑似２面メモリとも称する）、２面メモリの何れであるかを示す。書換え方法は、電源自己保持による書換え又は電源制御による書換えの何れであるかを示す。電源自己保持時間は、書換え方法が電源自己保持による書換えである場合に、電源自己保持を継続する時間を示す。書換え面情報は、何れの面が運用面であり、何れの面が非運用面であるかを示す。運用面は起動面とも称し、非運用面は書換え面とも称する。

[0057] 更新プログラムバージョンは、更新プログラムのバージョンを示す。更新プログラム取得アドレスは、更新プログラムのアドレスを示す。更新プログラムサイズは、更新プログラムのデータサイズを示す。ロールバックプログラムバージョンは、ロールバックプログラムのバージョンを示す。ロールバックプログラム取得アドレスは、ロールバックプログラムのアドレスを示す。ロールバックプログラムサイズは、ロールバックプログラムのデータサイズを示す。書込みデータ種別は、書込みデータが差分データ又は全データの何れの種別であるかを示す。尚、書換え諸元データには、これらの情報の他に、システムで独自に定義した情報を含むことが可能である。

[0058] ＤＣＭ１２は、ＤＣＭ用の書換え諸元データを取得すると、その取得したＤＣＭ用の書換え諸元データを解析する。ＤＣＭ１２は、ＤＣＭ用の書換え諸元データを解析すると、書換え対象ＥＣＵ１９の更新プログラムが格納されるアドレスから書込みデータを取得し、その取得した書込みデータをＣＧＷ１３に転送する等の書換えに関与する動作を制御する。

[0059] ＣＧＷ１３は、ＣＧＷ用の書換え諸元データを取得すると、その取得したＣＧＷ用の書換え諸元データを解析する。ＣＧＷ１３は、ＣＧＷ用の書換え諸元データを解析すると、その解析結果にしたがって書換え対象ＥＣＵ１９の更新プログラムの所定サイズ分の転送をＤＣＭ１２に要求したり、書込みデータを指定された順序で書換え対象ＥＣＵ１９に配信したりする等の書換えに関与する動作を制御する。

[0060] ファイルサーバ８には、上記したリプログデータが登録されると共に、ＯＥＭから提供される配信諸元データが登録される。ＯＥＭから提供される配信諸元データは、表示端末５における各種画面の表示に関与する動作を定義するデータである。図９に示すように、配信諸元データは、言語情報と、表示文言と、パッケージ情報と、画像データと、表示パターンと、表示制御プログラム等を含む。

[0061] 表示端末５は、ＣＧＷ１３から配信諸元データを取得すると、その取得した配信諸元データ解析し、その解析結果にしたがって各種画面の表示を制御する。表示端末５は、例えば予め保持している表示用フレームに対し、配信諸元データから取得した表示文言を重畳して表示したり、配信諸元データから取得した表示制御プログラムを実行したりする。尚、配信諸元データには、これらの情報の他に、システムで独自に定義した情報を含めることが可能である。

[0062] ファイルサーバ８は、リプログデータと配信諸元データとが登録されると、その登録されたリプログデータを暗号化し、パッケージを認証するためのパッケージ認証子と、暗号済みのリプログデータと、配信諸元データとを格納した配信パッケージを生成する。認証子は、リプログデータ及び配信諸元

データの完全性を検証するために付与されるデータであり、例えばＣＧＷ１３に紐付く鍵情報、リプログデータ及び配信諸元データから生成される。ファイルサーバ８は、外部から配信パッケージのダウンロード要求を受信すると、その配信パッケージをＤＣＭ１２に送信する。尚、ファイルサーバ８は、図６では、リプログデータと配信諸元データとを格納した配信パッケージを生成し、リプログデータと配信諸元データを１つのファイルとして同時にＤＣＭ１２に送信する場合を例示しているが、リプログデータと配信諸元データとを別々のファイルとしてＤＣＭ１２に送信しても良い。即ち、ファイルサーバ８は、先に配信諸元データをＤＣＭ１２に送信し、後からリプログデータをＤＣＭ１２に送信しても良い。その場合、配信諸元データ、リプログデータのそれぞれに対して認証子を付与すると良い。

[0063] 図１０に示すように、ＤＣＭ１２は、ファイルサーバ８から配信パッケージをダウンロードすると、そのダウンロードした配信パッケージに格納されているパッケージ認証子を用い、暗号済みのリプログデータの完全性を検証する。ＤＣＭ１２は、検証結果が正であると、暗号済みのリプログデータを復号化する。ＤＣＭ１２は、暗号済みのリプログデータを復号化すると、その復号化したリプログデータをアンパック（以下、アンパッケージングとも称する）し、暗号済みの差分データと認証子、ＤＣＭ用の書換え諸元データ、ＣＧＷ用の書換え諸元データに分割して抽出する。図１０では、ＥＣＵ（ＩＤ１）の暗号済みの差分データと認証子、ＥＣＵ（ＩＤ２）の暗号済みの差分データと認証子、ＥＣＵ（ＩＤ３）の暗号済みの差分データと認証子、ＤＣＭ用の書換え諸元データ、ＣＧＷ用の書換え諸元データに分割して抽出する場合を例示している。

[0064] 次に、ＥＣＵ１９のフラッシュメモリ３３ｄについて図１１から図２２を参照して説明する。ＥＣＵ１９のフラッシュメモリ３３ｄは、メモリ構成に応じて、フラッシュ面を１面で持つ１面単独メモリ、フラッシュ面を疑似的な２面で持つ１面サスペンドメモリ、フラッシュ面を実質的な２面で持つ２面メモリに区分される。これ以降、１面単独メモリを搭載するＥＣＵ１９を

１面単独メモリＥＣＵと称し、１面サスペンドメモリを搭載するＥＣＵ１９を１面サスペンドメモリＥＣＵと称し、２面メモリを搭載するＥＣＵ１９を２面メモリＥＣＵと称する。

[0065] １面単独メモリは、フラッシュ面を１面で持つ構成であるので、運用面及び非運用面と言う概念はなく、アプリプログラムを実行中にアプリプログラムを書換え不可である。一方、１面サスペンドメモリや２面メモリは、フラッシュ面を２面で持つ構成であるので、運用面及び非運用面と言う概念があり、運用面のアプリプログラムを実行中に非運用面のアプリプログラムを書換え可能である。２面メモリは、フラッシュ面を完全に分離した２面で持つ構成であるので、車両走行中等の任意のタイミングでアプリプログラムを書換え可能である。１面サスペンドメモリは、１面単独メモリを疑似的に２面で区切っている構成であるので、読出しや書込みを正常に行えるタイミングに制約があり、車両走行中でアプリプログラムを書換え不能であり、ＩＧ電源がオフされている駐車中にアプリプログラムを書換え可能である。

[0066] 又、１面単独メモリ、１面サスペンドメモリ、２面メモリは、それぞれリプログファームウェアが組込まれているリプログファームウェア組込み型（以下、組込み型と称する）と、リプログファームウェアを外部からダウンロードするリプログファームウェアダウンロード型（以下、ダウンロード型と称する）とがある。リプログファームウェアは、アプリプログラムを書換えるためのファームウェアである。

[0067] 以下、各フラッシュメモリの構成について順次説明する。

（Ａ）１面単独メモリ

（Ａ－１）組込み型の１面単独メモリ

組込み型の１面単独メモリについて図１１及び図１２を参照して説明する。組込み型の１面単独メモリは、差分エンジンワーク領域と、アプリプログラム領域と、ブートプログラム領域とを有する。アプリプログラム領域には、バージョン情報と、パラメータデータと、アプリプログラムと、ファームウェアと、通常時ベクタテーブルとが配置されている。ブート領域には、ブ

ートプログラムと、進捗状態ポイント２と、進捗状態ポイント１と、起動判定情報と、無線リプログファームウェアと、有線リプログファームウェアと、起動判定用プログラムと、ブート時ベクタテーブルとが配置されている。

[0068] 図１１に示すように、マイコン３３は、車両制御処理や診断処理等のアプリ処理を実行する通常動作時では、起動判定用プログラムを実行し、ブート時ベクタテーブルと通常時ベクタテーブルを参照して先頭アドレスを探索し、アプリプログラムの所定アドレスを実行する。

[0069] マイコン３３は、アプリプログラムの書換え処理を実行する書換え動作時では、アプリプログラムでなく無線又は有線リプログファームウェアを実行する。図１２は、更新プログラムとして差分データを用いてアプリプログラムを書換える動作を示す。図１２に示すように、マイコン３３は、アプリプログラムを旧データとして差分エンジンワーク領域に一旦退避させる。マイコン３３は、差分エンジンワーク領域に一旦退避させた旧データを読出し、組込んでいるリプログファームウェアに含まれる差分エンジンにより、その読出した旧データと、ＲＡＭ３３ｃに記憶した差分データとから新データを復元する。マイコン３３は、旧データと差分データから新データを生成すると、その新データをメモリの所定アドレスに書込んでアプリプログラムを書換える。

[0070] （Ａ－２）ダウンロード型の１面単独メモリ

ダウンロード型の１面単独メモリについて図１３及び図１４を参照して説明する。ダウンロード型は、上記した組込み型と比較し、無線リプログファームウェアや有線リプログファームウェアを外部からダウンロードし、アプリプログラムを書換えた後に、その無線リプログファームウェアや有線リプログファームウェアを削除する点で異なる。アプリプログラムを無線で更新する場合、例えば図６に示したリプログデータの中に、各ＥＣＵ１９で実行する無線リプログファームウェアを含めておく。ＥＣＵ１９は、ＣＧＷ１３から自ＥＣＵ向け無線リプログファームウェアを受信し、その受信した自ＥＣＵ向け無線リプログファームウェアをＲＡＭに保存する。

[0071] 図１３に示すように、マイコン３３は、車両制御処理や診断処理等のアプリ処理を実行する通常動作時では、組込み型と同様に、起動判定用プログラムを実行し、ブート時ベクタテーブルと通常時ベクタテーブルを参照して先頭アドレスを探索し、アプリプログラムの所定アドレスを実行する。

[0072] 図１４に示すように、マイコン３３は、アプリプログラムの書換え処理を実行する書換え動作時では、アプリプログラムを旧データとして差分エンジンワーク領域に一旦退避させる。マイコン３３は、差分エンジンワーク領域に一旦退避させた旧データを読出し、外部からダウンロードされたリプログファームウェアに含まれる差分エンジンにより、その読出した旧データと、ＲＡＭ３３ｃに記憶した差分データとから新データを復元する。マイコン３３は、旧データと差分データから新データを生成すると、その新データを書込んでアプリプログラムを書換える。

[0073] （Ｂ）１面サスペンドメモリ

（Ｂ－１）組込み型の１面サスペンドメモリ

組込み型の１面サスペンドメモリについて図１５及び図１６を参照して説明する。組込み型の１面サスペンドメモリは、差分エンジンワーク領域と、アプリプログラム領域と、ブートプログラム領域とを有する。プログラム更新を行うリプログファームウェアは、１面単独メモリと同様、ブートプログラム領域に配置され、プログラム更新の対象外である。プログラム更新の対象であるアプリプログラム領域は、Ａ面とＢ面を疑似的に有し、Ａ面とＢ面には、それぞれバージョン情報と、アプリプログラムと、通常時ベクタテーブルとが配置されている。ブート領域には、ブートプログラムと、リプログファームウェアと、リプログ時ベクタテーブルと、起動面判定機能と、起動面判定情報と、ブート時ベクタテーブルとが配置されている。

[0074] 図１５に示すように、マイコン３３は、車両制御処理や診断処理等のアプリ処理を実行する通常動作時では、ブートプログラムを実行して起動面判定機能によりＡ面とＢ面の各起動面判定情報からＡ面及びＢ面のうち何れが運用面であるかを判定する。マイコン３３は、Ａ面を運用面とすると判定する

と、Ａ面の通常時ベクタテーブルを参照して先頭アドレスを探索し、Ａ面のアプリプログラムを実行する。同様に、マイコン３３は、Ｂ面を運用面とすると判定すると、Ｂ面の通常時ベクタテーブルを参照して先頭アドレスを探索し、Ｂ面のアプリプログラムを実行する。尚、図１５では、リプログファームウェアをブートプログラム領域に配置したが、リプログファームウェアもプログラム更新の対象とし、Ａ面又はＢ面のそれぞれの領域に配置するように構成しても良い。

[0075] 図１６に示すように、マイコン３３は、非運用面のアプリプログラムの書換え処理を実行する書換え動作時では、非運用面のアプリプログラムを旧データとして差分エンジンワーク領域に一旦退避させる。マイコン３３は、差分エンジンワーク領域に一旦退避させた旧データを読出し、組込んでいるリプログファームウェア内の差分エンジンにより、その読出した旧データと、ＲＡＭ３３ｃに記憶した差分データとから新データを復元する。マイコン３３は、旧データと差分データから新データを生成すると、その新データを非運用面に書込んで非運用面のアプリプログラムを書換える。図１６では、Ａ面が運用面であり、Ｂ面が非運用面である場合を例示している。

[0076] （Ｂ－２）ダウンロード型の１面サスペンドメモリ

ダウンロード型の１面サスペンドメモリについて図１７及び図１８を参照して説明する。ダウンロード型は、上記した組込み型と比較し、リプログファームウェアとリプログ時ベクタテーブルを外部からダウンロードし、アプリプログラムを書換えた後に、そのリプログファームウェアとリプログ時ベクタテーブルを削除する点で異なる。

[0077] 図１７に示すように、マイコン３３は、車両制御処理や診断処理等のアプリ処理を実行する通常動作時では、組込み型と同様に、ブートプログラムを実行して起動面判定機能によりＡ面とＢ面の各起動面判定情報から新旧を判定し、Ａ面及びＢ面のうち何れが運用面であるかを判定する。マイコン３３は、Ａ面を運用面とすると判定すると、Ａ面の通常時ベクタテーブルを参照して先頭アドレスを探索し、Ａ面のアプリプログラムを実行する。同様に、

マイコン３３は、Ｂ面を運用面とすると判定すると、Ｂ面の通常時ベクタテーブルを参照して先頭アドレスを探索し、Ｂ面のアプリプログラムを実行する。

[0078] 図１８に示すように、マイコン３３は、アプリプログラムの書換え処理を実行する書換え動作時では、非運用面のアプリプログラムを旧データとして差分エンジンワーク領域に一旦退避させる。マイコン３３は、差分エンジンワーク領域に一旦退避させた旧データを読出し、外部からダウンロードされたリプログファームウェア内の差分エンジンにより、その読出した旧データと、ＲＡＭ３３ｃに記憶した差分データとから新データを復元する。マイコン３３は、旧データと差分データから新データを生成すると、その新データを書込んでアプリプログラムを書換える。図１８では、Ａ面が運用面であり、Ｂ面が非運用面である場合を例示している。このように１面サスペンドメモリでは、Ａ面のアプリプログラムを実行しつつ、Ｂ面のアプリプログラムの書換えをバックグラウンドで実行することができる。

[0079] （Ｃ）２面メモリ

（Ｃ－１）組込み型の２面メモリ

組込み型の２面メモリについて図１９及び図２０を参照して説明する。組込み型の１面単独メモリは、Ａ面のアプリプログラム領域及び書換えプログラム領域と、Ｂ面のアプリプログラム領域及び書換えプログラム領域と、ブートプログラム領域とを有する。ブート領域には、ブートプログラムが書換え不能として配置されている。ブートプログラムは、ブートスワップ機能と、ブート時ベクタテーブルを含む。各アプリプログラム領域には、バージョン情報と、パラメータデータと、アプリプログラムと、ファームウェアと、通常時ベクタテーブルとが配置されている。各書換えプログラム領域には、書換えを制御するプログラムと、リプログ進捗管理情報２と、リプログ進捗管理情報１と、起動面判定情報と、無線リプログファームウェアと、有線リプログファームウェアと、ブート時ベクタテーブルとが配置されている。ブート領域には、ブートプログラムと、ブートスワップ機能と、ブート時ベク

タテーブルとが配置されている。

[0080] 図１９に示すように、マイコン３３は、車両制御処理や診断処理等のアプリ処理を実行する通常動作時及び非運用面のアプリプログラムの書換え処理を実行する書換え動作時とも、ブートプログラムを実行してＡ面とＢ面の各起動面判定情報からブートスワップ機能により新旧を判定し、Ａ面及びＢ面の何れが運用面であるかを判定する。マイコン３３は、Ａ面を運用面とすると判定すると、Ａ面のブート時ベクタテーブルとＡ面の通常時ベクタテーブルを参照して先頭アドレスを探索し、Ａ面のアプリプログラムを実行する。同様に、マイコン３３は、Ｂ面を運用面とすると判定すると、Ｂ面のブート時ベクタテーブルとＢ面の通常時ベクタテーブルを参照して先頭アドレスを探索し、Ｂ面のアプリプログラムを実行する。

[0081] 図２０に示すように、マイコン３３は、非運用面のアプリプログラムの書換え処理を実行する書換え動作時では、非運用面のアプリプログラムを旧データとして差分エンジンワーク領域に一旦退避させる。マイコン３３は、差分エンジンワーク領域に一旦退避させた旧データを読出し、組込んでいるリプログファームウェア内の差分エンジンにより、その読出した旧データと、ＲＡＭ３３ｃに記憶した差分データとから新データを復元する。マイコン３３は、旧データと差分データから新データを生成すると、その新データを非運用面に書込んで非運用面のアプリプログラムを書換える。尚、差分エンジンワーク領域に一旦退避させる旧データは、運用面のアプリプログラムを対象としても良いし、非運用面のアプリプログラムを対象としても良い。この時、運用面のアプリプログラムを対象とする場合は、新データの書込み前に非運用面のデータを消去する。ここで、車両外部から取得したリプログデータが差分データでなく全データ（フルデータ）である場合、取得したリプログデータを新データとして非運用面に書込むこととなる。図２０では、Ａ面が運用面であり、Ｂ面が非運用面である場合を例示している。尚、差分エンジンワーク領域に一旦退避させる旧データは、運用面のアプリプログラムを対象としても良いし、非運用面のアプリプログラムを対象としても良い。ア

プリプログラムの実行アドレスを合致させる必要がある場合には、非運用面のアプリプログラムを旧データとして退避させる。

[0082] （Ｃ－２）ダウンロード型の２面メモリ

ダウンロード型の２面メモリについて図２１及び図２２を参照して説明する。ダウンロード型は、上記した組込み型と比較し、無線リプログファームウェアや有線リプログファームウェアを外部からダウンロードし、アプリプログラムを書換えた後に、その無線リプログファームウェアや有線リプログファームウェアを削除する点で異なる。

[0083] 図２１に示すように、マイコン３３は、車両制御処理等のアプリ処理や診断処理を実行する通常動作時及び非運用面のアプリプログラムの書換え処理を実行する書換え動作時とも、組込み型と同様に、ブートプログラムを実行してＡ面とＢ面の各起動面判定情報からブートスワップ機能により新旧を判定し、Ａ面及びＢ面の何れが運用面であるかを判定し、運用面のアプリプログラムを実行してアプリ処理を実行する。

[0084] 図２２に示すように、マイコン３３は、アプリプログラムの書換え処理を実行する書換え動作時では、非運用面のアプリプログラムを旧データとして差分エンジンワーク領域に一旦退避させる。マイコン３３は、差分エンジンワーク領域に一旦退避させた旧データを読出し、その読出した旧データと、外部からダウンロードされたリプログファームウェアによりＲＡＭ３３ｃに記憶した差分データとから新データを復元する。マイコン３３は、旧データと差分データから新データを生成すると、その新データを非運用面に書込んで非運用面のアプリプログラムを書換える。尚、差分エンジンワーク領域に一旦退避させる旧データは、運用面のアプリプログラムを対象としても良いし、非運用面のアプリプログラムを対象としても良い。この時、運用面のアプリプログラムを対象とする場合は、新データの書込み前に非運用面のデータを消去する。ここで、車両外部から取得したリプログデータが差分データでなく全データ（フルデータ）である場合、取得したリプログデータを新データとして非運用面に書込むこととなる。図２２では、Ａ面が運用面であり

、Ｂ面が非運用面の場合を例示している。尚、差分エンジンワーク領域に一旦退避させる旧データは、運用面のアプリプログラムを対象としても良いし、非運用面のアプリプログラムを対象としても良い。このように２面メモリでは、Ａ面のアプリプログラムを実行しつつ、Ｂ面のアプリプログラムの書換えをバックグラウンドで実行することができる。

[0085] 上記したように、組込み型及びダウンロード型の何れの構成でも、各アプリ領域に、アプリプログラムと、アプリプログラムを書換えるための書換えプログラムが配置されている。尚、図２０及び図２２では、アプリプログラムをリプログ対象として示したが、書換えプログラムもリプログ対象としても良い。又、書換えプログラムを書換え不能としたい場合には、書換えプログラムをブート領域に配置しても良い。例えばディーラー等においてツール２３を介した有線での書換えが確実に実施可能となるように有線書換えのためのプログラムをブート領域に配置して良い。

[0086] 次に、アプリプログラムを書換える全体シーケンスについて図２３から図２５を参照して説明する。尚、ここでは、ユーザが表示端末５として携帯端末６を操作して駐車中にアプリプログラムを書換える場合について説明するが、車載ディスプレイ７を操作して駐車中にアプリプログラムを書換える場合についても同様である。センター装置３からＤＣＭ１２に送信される配信パッケージには、１つ以上の書換え対象ＥＣＵ１９の書込みデータが格納される。即ち、配信パッケージには、書換え対象ＥＣＵ１９が１つであれば、その１つの書換え対象ＥＣＵ１９に向けた１つの書込みデータが格納され、書換え対象ＥＣＵ１９が複数であれば、その複数の書換え対象ＥＣＵ１９の個々に向けた複数の書込みデータが格納される。ここでは、書換え対象ＥＣＵ１９が２個であり、２つの書換え対象ＥＣＵ１９を書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）と称する。又、書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）以外のＥＣＵ１９を、その他のＥＣＵと称する。

[0087] 書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）は、それぞ

れ例えばバージョン通知信号の送信要求をマスタ装置１１から受信したと判定すると、バージョン通知信号の送信条件が成立したと判定する。書換え対象ＥＣＵ（ＩＤ１）は、バージョン通知信号の送信条件が成立すると、自己が記憶しているアプリプログラムのバージョン情報と自己を識別可能なＥＣＵ（ＩＤ）を含むバージョン通知信号をマスタ装置１１に送信する。マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ１）からバージョン通知信号を受信すると、その受信したバージョン通知信号をセンター装置３に送信する。同様に、書換え対象ＥＣＵ（ＩＤ２）は、バージョン通知信号の送信条件が成立すると、自己が記憶しているアプリプログラムのバージョンと自己を識別可能なＥＣＵ（ＩＤ）とを含むバージョン通知信号をマスタ装置１１に送信する。マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ２）からバージョン通知信号を受信すると、その受信したバージョン通知信号をセンター装置３に送信する。

[0088] センター装置３は、書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）からバージョン通知信号を受信すると、その受信したバージョン通知信号に含まれるアプリプログラムのバージョンとＥＣＵ（ＩＤ）を特定し、そのバージョン通知信号の送信元の書換え対象ＥＣＵ１９に配信すべき書込みデータの有無を判定する。センター装置３は、書換え対象から受信したバージョン通知信号から書換え対象ＥＣＵ１９の現在のアプリプログラムのバージョンを特定し、その現在のアプリプログラムのバージョンと、管理している最新のバージョンとを照合する。

[0089] センター装置３は、バージョン通知信号から特定したバージョンが、管理している最新のバージョンと同じ値であれば、そのバージョン通知信号の送信元の書換え対象ＥＣＵ１９に配信すべき書込みデータがなく、書換え対象ＥＣＵ１９に記憶されているアプリプログラムをアップデートする必要がないと判定する。一方、センター装置３は、バージョン通知信号から特定したバージョンが、管理している最新のバージョンよりも小さい値であれば、そのバージョン通知信号の送信元の書換え対象ＥＣＵ１９に配信すべき書込み

データがあり、書換え対象ＥＣＵ１９に記憶されているアプリプログラムをアップデートする必要があると判定する。

[0090] センター装置３は、書換え対象ＥＣＵ１９に記憶されているアプリプログラムをアップデートする必要があると判定すると、アップデートする必要がある旨を携帯端末６に通知する。携帯端末６は、アップデートする必要がある旨を通知されると、配信可否画面を表示する（Ａ１）。配信可否画面は、後述するキャンペーン通知画面と同等である。ユーザは、携帯端末６に表示される配信可否画面によりアップデートする必要がある旨を確認することができ、アップデートするか否かを選択することができる。

[0091] ユーザがアップデートする旨を携帯端末６において選択すると（Ａ２）、携帯端末６は、配信パッケージのダウンロード要求をセンター装置３に通知する。センター装置３は、携帯端末６から配信パッケージのダウンロード要求が通知されると、配信パッケージをマスタ装置１１に送信する。

[0092] マスタ装置１１は、センター装置３から配信パッケージをダウンロードすると、そのダウンロードした配信パッケージに対してパッケージ認証処理を開始する（Ｂ１）。マスタ装置１１は、配信パッケージを認証し、パッケージ認証処理を完了すると、書込みデータ抽出処理を開始する（Ｂ２）。マスタ装置１１は、配信パッケージから書込みデータを抽出し、書込みデータ抽出処理を完了すると、ダウンロード完了通知信号をセンター装置３に送信する。

[0093] センター装置３は、マスタ装置１１からダウンロード完了通知信号を受信すると、ダウンロードの完了を携帯端末６に通知する。携帯端末６は、センター装置３からダウンロードの完了が通知されると、ダウンロード完了通知画面を表示する（Ａ３）。ユーザは、携帯端末６に表示されるダウンロード完了通知画面によりダウンロードが完了した旨を確認することができ、車両側におけるアプリプログラムの書換え開始時刻を設定することができる。

[0094] ユーザが車両側におけるアプリプログラムの書換え開始時刻を携帯端末６において設定すると（Ａ４）、携帯端末６は、書換え開始時刻をセンター装

置３に通知する。センター装置３は、携帯端末６から書換え開始時刻が通知されると、そのユーザが設定した書換え開始時刻を設定開始時刻として記憶する。センター装置３は、現在時刻が設定開始時刻に到達すると（Ａ５）、書換え指示信号をマスタ装置１１に送信する。

[0095] マスタ装置１１は、センター装置３から書換え指示信号を受信すると、電源起動要求を電源管理ＥＣＵ２０に送信し、書換え対象ＥＣＵ（ＩＤ１）、書換え対象ＥＣＵ（ＩＤ２）、その他のＥＣＵを停止状態又はスリープ状態から起動状態に移行させる（Ｘ１）。

[0096] マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ１）への書込みデータの配信を開始し、書込みデータの書込みを書換え対象ＥＣＵ（ＩＤ１）に指示する。書換え対象ＥＣＵ（ＩＤ１）は、マスタ装置１１からの書込みデータの受信を開始し、書込みデータの書込みが指示されると、書込みデータの書込みを開始し、プログラム書換え処理を開始する（Ｃ１）。書換え対象ＥＣＵ（ＩＤ１）は、マスタ装置１１からの書込みデータの受信を完了し、書込みデータの書込みを完了し、プログラム書換え処理を完了すると、書換え完了通知信号をマスタ装置１１に送信する。

[0097] マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ１）から書換え完了通知信号を受信すると、書換え対象ＥＣＵ（ＩＤ２）への書込みデータの配信を開始し、書込みデータの書込みを書換え対象ＥＣＵ（ＩＤ２）に指示する。書換え対象ＥＣＵ（ＩＤ２）は、マスタ装置１１からの書込みデータの受信を開始し、書込みデータの書込みが指示されると、書込みデータの書込みを開始し、プログラム書換え処理を開始する（Ｄ１）。書換え対象ＥＣＵ（ＩＤ２）は、マスタ装置１１からの書込みデータの受信を完了し、書込みデータの書込みを完了し、プログラム書換え処理を完了すると、書換え完了通知信号をマスタ装置１１に送信する。マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ２）から書換え完了通知信号を受信すると、書換え完了通知信号をセンター装置３に送信する。

[0098] センター装置３は、マスタ装置１１から書換え完了通知信号を受信すると

、アプリプログラムの書換え完了を携帯端末６に通知する。携帯端末６は、センター装置３からアプリプログラムの書換え完了が通知されると、書換え完了通知画面を表示する（Ａ６）。ユーザは、携帯端末６に表示される書換え完了通知画面によりアプリプログラムの書換えが完了した旨を確認することができ、アクティベートとして同期の実施を設定することができる。

[0099] ユーザが同期の実施を携帯端末６において設定すると（Ａ７）、即ち、ユーザが新プログラムのアクティベートに対する承諾を設定すると、携帯端末６は、同期の実施をセンター装置３に通知する。センター装置３は、携帯端末６から同期の実施が通知されると、同期切替え指示信号をマスタ装置１１に送信する。マスタ装置１１は、センター装置３から同期切替え指示信号を受信すると、その受信した同期切替え指示信号を書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）に配信する。

[0100] 書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）は、それぞれマスタ装置１１から同期切替え指示信号を受信すると、次回に起動するアプリプログラムを旧アプリプログラムから新アプリプログラムに切替えるプログラム切替え処理を開始する（Ｃ２，Ｄ２）。書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）は、それぞれプログラム切替え処理を完了すると、切替え完了通知信号をマスタ装置１１に送信する。

[0101] マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）から切替え完了通知信号を受信すると、バージョン読出信号を書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）に配信する。書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）は、それぞれマスタ装置１１からバージョン読出信号を受信すると、これ以降に運用するアプリプログラムのバージョンを読出し（Ｃ３，Ｄ３）、その読出したバージョンを含む最新バージョン通知信号をマスタ装置１１に送信する。マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）からバージョン通知信号を受信することで、ソフトウェアのバージョンをチェックしたり、必要に応じてロールバックを行ったりする。

[0102] マスタ装置１１は、書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）からバージョン通知信号を受信すると、電源停止要求を電源管理ＥＣＵ２０に送信し、書換え対象ＥＣＵ（ＩＤ１）、書換え対象ＥＣＵ（ＩＤ２）、その他のＥＣＵを起動状態から停止状態又はスリープ状態に移行させる（Ｘ２）。

[0103] マスタ装置１１は、最新バージョン通知信号をセンター装置３に送信する。センター装置３は、マスタ装置１１から最新バージョン通知信号を受信すると、その受信した最新バージョン通知信号から書換え対象ＥＣＵ（ＩＤ１）及び書換え対象ＥＣＵ（ＩＤ２）のアプリプログラムの最新のバージョンを特定し、その特定した最新のバージョンを携帯端末６に通知する。携帯端末６は、センター装置３から最新のバージョンが通知されると、その通知された最新のバージョンを示す最新バージョン通知画面を携帯端末６において表示する（Ａ８）。ユーザは、携帯端末６に表示される最新バージョン通知画面により最新のバージョンを確認することができ、アクティベートが完了した旨を確認することができる。

[0104] 次に、アプリプログラムを書換える場合におけるＤＣＭ１２、ＣＧＷ１３、書換え対象ＥＣＵ１９の動作のタイミングチャートについて図２６から図２９を参照して説明する。尚、ここでは、ユーザ操作によりＩＧスイッチ４２がオンされている期間中、即ち、車両が走行可能中に２面メモリＥＣＵのアプリプログラムを書換え、ユーザ操作によりＩＧスイッチ４２がオフされた以降の駐車中に１面サスペンドメモリＥＣＵ及び１面単独メモリＥＣＵのアプリプログラムを書換える場合について説明する。又、電源制御によりアプリプログラムを書換える場合と、電源自己保持によりアプリプログラムを書換える場合とについて説明する。

[0105] （ア）電源制御によりアプリプログラムを書換える場合

電源制御によりアプリプログラムを書換える場合について図２６及び図２７を参照して説明する。電源制御によるアプリプログラムの書換えとは、電源自己保持回路を用いず、電源の切り替わりに応じて書換え動作を制御する

構成を意味する。ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、ＤＣＭ１２、ＣＧＷ１３、２面メモリＥＣＵ、１面サスペンドメモリＥＣＵ、１面単独メモリＥＣＵは、それぞれ通常動作を開始する（ｔ１）。

[0106] ＤＣＭ１２は、センター装置３からダウンロード開始が通知されると、通常動作からダウンロード動作に移行し、センター装置３からの配信パッケージのダウンロードを開始する（ｔ２）。ＤＣＭ１２は、通常動作を行いつつ、配信パッケージのダウンロードをバックグラウンドで行うと良い。ＤＣＭ１２は、センター装置３からの配信パッケージのダウンロードを完了すると、ダウンロード動作から通常動作に復帰する（ｔ３）。

[0107] ＤＣＭ１２は、センター装置３又はＣＧＷ１３から書換え指示信号（インストール指示信号）が通知されると、通常動作からデータ転送／センター通信動作に移行し、データ転送／センター通信動作を開始する（ｔ４）。即ち、ＤＣＭ１２は、配信パッケージから書込みデータを抽出し、ＣＧＷ１３への書込みデータの転送を開始すると共に、書換えの進捗状況をＣＧＷ１３から取得し、センター装置３への書換えの進捗状況の通知を開始する。

[0108] ＣＧＷ１３は、ＤＣＭ１２から書込みデータの取得を開始すると、通常動作からリプログマスタ動作に移行し、リプログマスタ動作を開始し、２面メモリＥＣＵへの書込みデータの配信を開始し、書込みデータの書込みを指示する。２面メモリＥＣＵは、ＣＧＷ１３からの書込みデータの受信を開始すると、通常動作においてプログラミングフェーズ（以下、インストールフェーズとも称する）を開始する。即ち、２面メモリＥＣＵは、通常動作を行いつつ、アプリプログラムのインストールをバックグラウンドで行う。２面メモリＥＣＵは、受信した書込みデータのフラッシュメモリへの書込みを開始し、アプリプログラムの書換えを開始する。

[0109] ２面メモリＥＣＵにおいてアプリプログラムの書換え中に、ユーザがＩＧスイッチオンからオフに切替えたことで車両電源がＩＧ電源から＋Ｂ電源に切替わると、ＤＣＭ１２は、データ転送／センター通信動作を中断し、ＣＧ

Ｗ１３は、リプログマスタ動作を中断し、２面メモリＥＣＵは、インストールフェーズを中断し、アプリプログラムの書換えを中断する（ｔ５）。

[0110] その後、ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、ＤＣＭ１２は、データ転送／センター通信動作を再開し、ＣＧＷ１３は、リプログマスタ動作を再開し、２面メモリＥＣＵは、インストールフェーズを再開し、アプリプログラムの書換えを再開する（ｔ６）。即ち、ユーザがＩＧスイッチオンからオフに切替えたことで車両電源がＩＧ電源から＋Ｂ電源に切替わり、その後、ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わり、トリップが発生する毎に、２面メモリＥＣＵは、アプリプログラムの書換えの中断と再開を繰返す（ｔ７，ｔ８）。

[0111] ２面メモリＥＣＵは、書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、インストールフェーズを終了し、通常動作からアクティベート待ちに移行する。即ち、２面メモリＥＣＵは、アクティベートフェーズを行っていない時点ではアプリプログラムを書換えた新面（Ｂ面）では起動せず、旧面（Ａ面）起動のままとする（ｔ９）。

[0112] ユーザがＩＧスイッチオンからオフに切替えたことで車両電源がＩＧ電源から＋Ｂ電源に切替わった後に（ｔ１０）、その時点で２面メモリＥＣＵがアプリプログラムの書換えを完了していると、ＣＧＷ１３が電源起動要求を電源管理ＥＣＵ２０に送信する。ＣＧＷ１３が電源起動要求を電源管理ＥＣＵ２０に送信したことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、ＤＣＭ１２は、データ転送／センター通信動作を再開し、ＣＧＷ１３は、リプログマスタ動作を再開し、１面サスペンドメモリＥＣＵ及び１面単独メモリＥＣＵへの書込みデータの配信を開始する。１面サスペンドメモリＥＣＵ及び１面単独メモリＥＣＵは、それぞれＣＧＷ１３からの書込みデータの受信を開始すると、通常動作からブート処理に移行し、ブート処理においてインストールフェーズを開始する（ｔ１１）。即ち、１面サスペンドメモリＥＣＵ及び１面単独メモリＥＣＵは、通常動作と並行してインストールを行うこ

とはなく、アプリプログラムが動作していないブート処理においてインストールを行う。

[0113] １面サスペンドメモリＥＣＵは、アプリプログラムの書換えを開始すると、アプリプログラムの書換えを完了する前にユーザ操作によりＩＧスイッチ４２がオフからオンに切替えられた場合には、アプリプログラムの書換えを中断する。１面サスペンドメモリＥＣＵは、アプリプログラムの書換えを中断した非運用面（Ｂ面）でなく、運用面（Ａ面）を起動面として復帰する。１面単独メモリＥＣＵは、アプリプログラムの書換えを開始すると、アプリプログラムの書換えを完了する前にユーザ操作によりＩＧスイッチ４２がオフからオンに切替えられたとしても、アプリプログラムの書換えを継続する。１面単独メモリＥＣＵは、アプリプログラムの書換え途中で中断してしまうと、通常動作として復帰不能であるからである。好ましくは、１面単独メモリＥＣＵのアプリプログラムの書換えを開始した以降は、アプリプログラムの書換えを完了するまでユーザによるＩＧスイッチ４２操作を無効とするのが良い。

[0114] １面サスペンドメモリＥＣＵは、書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、ブート処理においてインストールフェーズを終了し、ブート処理からアクティベート待ちに移行する。即ち、１面サスペンドメモリＥＣＵは、アクティベートフェーズを行っていない時点ではアプリプログラムを書換えた新面（Ｂ面）では起動せず、旧面（Ａ面）起動のままとする。１面単独メモリＥＣＵは、書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、ブート処理においてインストールフェーズを終了し、アクティベート待ちとする（ｔ１２）。

[0115] ＣＧＷ１３からのアクティベート指示により電源管理ＥＣＵ２０が車両電源をＩＧ電源から＋Ｂ電源に切替えると、２面メモリＥＣＵ及び１面サスペンドメモリＥＣＵは、それぞれ旧面から新面への切替えを行い、新面で起動し、新面起動においてポストプログラミングフェーズ（以下、アクティベートフェーズとも称する）を開始する。１面単独メモリＥＣＵは、再起動を開

始し、インストール完了後の再起動においてアクティベートフェーズを開始する（ｔ１３，ｔ１４）。アクティベートでは、新プログラムで正しく起動することの確認やＣＧＷ１３へのバージョン情報の通知等を行う。

[0116] アクティベートが完了し、ＣＧＷ１３からのアクティベート完了指示により電源管理ＥＣＵ２０が車両電源をＩＧ電源から＋Ｂ電源に切替えると、ＤＣＭ１２は、データ転送／センター通信動作からスリープ／停止動作に移行し、スリープ／停止動作を開始する。ＣＧＷ１３は、リプログマスタ動作からスリープ／停止動作に移行し、スリープ／停止動作を開始する。２面メモリＥＣＵ、１面サスペンドメモリＥＣＵ、１面単独メモリＥＣＵは、それぞれ新面起動からスリープ／停止動作に移行する（ｔ１５）。

[0117] これ以降、ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、２面メモリＥＣＵ及び１面サスペンドメモリＥＣＵは、それぞれ新面（Ｂ面）を起動面として新アプリプログラムを起動し、１面単独メモリＥＣＵは、新アプリプログラムを起動する（ｔ１６）。

[0118] （イ）電源自己保持によりアプリプログラムを書換える場合

電源自己保持によりアプリプログラムを書換える場合について図２８及び図２９を参照して説明する。電源自己保持によるアプリプログラムの書換えとは、電源自己保持回路を用いて、書換え動作を制御する構成を意味する。ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、ＤＣＭ１２、ＣＧＷ１３、２面メモリＥＣＵ、１面サスペンドメモリＥＣＵ、１面単独メモリＥＣＵは、それぞれ通常動作を開始する（ｔ２１）。

[0119] ＤＣＭ１２は、センター装置３からダウンロード開始が通知されると、即ち、新プログラムによる更新有りと通知されると、通常動作からダウンロード動作に移行し、センター装置３からの配信パッケージのダウンロードを開始する（ｔ２２）。ＤＣＭ１２は、センター装置３からの配信パッケージのダウンロードを完了すると、ダウンロード動作から通常動作に復帰する（ｔ

２３）。

[0120] ＤＣＭ１２は、センター装置３又はＣＧＷ１３から書換え指示信号（インストール指示信号）が通知されると、通常動作からデータ転送／センター通信動作に移行し、データ転送／センター通信動作を開始する（ｔ２４）。即ち、ＤＣＭ１２は、配信パッケージから書込みデータを抽出し、ＣＧＷ１３への書込みデータの転送を開始すると共に、書換えの進捗状況をＣＧＷ１３から取得し、センター装置３への書換えの進捗状況の通知を開始する。

[0121] ＣＧＷ１３は、ＤＣＭ１２から書込みデータの取得を開始すると、通常動作からリプログマスタ動作に移行し、リプログマスタ動作を開始し、２面メモリＥＣＵへの書込みデータの配信を開始し、書込みデータの書込みを指示する。２面メモリＥＣＵは、ＣＧＷ１３からの書込みデータの受信を開始すると、通常動作においてプログラミングフェーズ（以下、インストールフェーズとも称する）を開始する。即ち、２面メモリＥＣＵは、通常動作を行いつつ、アプリプログラムのインストールをバックグラウンドで行う。２面メモリＥＣＵは、受信した書込みデータのフラッシュメモリへの書込みを開始し、アプリプログラムの書換えを開始する。

[0122] ２面メモリＥＣＵにおいてアプリプログラムの書換え中に、ユーザがＩＧスイッチオンからオフに切替えたことで車両電源がＩＧ電源から＋Ｂ電源に切替わると（ｔ２５）、車両電源がＩＧ電源から＋Ｂ電源に切替わった直後では、ＤＣＭ１２は、データ転送／センター通信動作を継続し、ＣＧＷ１３は、リプログマスタ動作を継続し、２面メモリＥＣＵは、インストールフェーズを継続し、アプリプログラムの書換えを継続する。車両電源がＩＧ電源から＋Ｂ電源に切替わってから予め設定された時間である自己保持期間が経過すると、ＤＣＭ１２は、データ転送／センター通信動作を中断し、ＣＧＷ１３は、リプログマスタ動作を中断し、２面メモリＥＣＵは、インストールフェーズを中断し、アプリプログラムの書換えを中断する（ｔ２６）。即ち、ＩＧスイッチ４２がオフされてから所定時間が経過するまでは車両バッテリ４０からの電力供給によりインストールを継続する。

[0123] その後、ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、ＤＣＭ１２は、データ転送／センター通信動作を再開し、ＣＧＷ１３は、リプログマスタ動作を再開し、２面メモリＥＣＵは、インストールフェーズを再開し、アプリプログラムの書換えを再開する（ｔ２７）。即ち、ユーザがＩＧスイッチオンからオフに切替えたことで車両電源がＩＧ電源から＋Ｂ電源に切替わり、その後、ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わり、トリップが発生する毎に、２面メモリＥＣＵは、アプリプログラムの書換えの中断と再開を繰返す（ｔ２８～ｔ３０）。ただし、車両電源がＩＧ電源から＋Ｂ電源に切替わってから自己保持期間が経過するまでは、ＤＣＭ１２は、データ転送／センター通信動作を継続し、ＣＧＷ１３は、リプログマスタ動作を継続し、２面メモリＥＣＵは、インストールフェーズを継続し、アプリプログラムの書換えを継続する。

[0124] ２面メモリＥＣＵは、書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、インストールフェーズを終了し、通常動作からアクティベート待ちに移行する。即ち、２面メモリＥＣＵは、アクティベートフェーズを行っていない時点ではアプリプログラムを書換えた新面（Ｂ面）では起動せず、旧面（Ａ面）起動のままとする（ｔ３１）。

[0125] ユーザがＩＧスイッチオンからオフに切替えたことで車両電源がＩＧ電源から＋Ｂ電源に切替わり、その時点で２面メモリＥＣＵにおいてアプリプログラムの書換えを完了していると、１面サスペンドメモリＥＣＵ及び１面単独メモリＥＣＵは、それぞれ通常動作からブート処理に移行し、ブート処理を開始し、ブート処理においてインストールフェーズを開始する（ｔ３２）。

[0126] １面サスペンドメモリＥＣＵ及び単独メモリＥＣＵは、それぞれ書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、ブート処理においてインストールフェーズを終了する（ｔ３３）。ＣＧＷ１３が電源起動要求を電源管理ＥＣＵ２０に送信したことで車両電源が＋Ｂ電源からＩ

Ｇ電源に切替わると、ＤＣＭ１２は、データ転送／センター通信動作を再開する（ｔ３４）。

[0127] １面サスペンドメモリＥＣＵは、書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、ブート処理からアクティベート待ちに移行する。即ち、１面サスペンドメモリＥＣＵは、アクティベートフェーズを行っていない時点ではアプリプログラムを書換えた新面（Ｂ面）では起動せず、旧面（Ａ面）起動のままとする。１面単独メモリＥＣＵは、書込みデータの書込みを完了し、アプリプログラムの書換えを完了すると、ブート処理においてインストールフェーズを終了し、アクティベート待ちとする（ｔ３５）。

[0128] ＣＧＷ１３からのアクティベート指示により電源管理ＥＣＵ２０が車両電源をＩＧ電源から＋Ｂ電源に切替えると、２面メモリＥＣＵ及び１面サスペンドメモリＥＣＵは、それぞれ旧面から新面への切替えを行い、新面で起動し、新面起動においてアクティベートフェーズを開始する。１面単独メモリＥＣＵは、再起動を開始し、インストール完了後の再起動においてアクティベートフェーズを開始する（ｔ３６，ｔ３７）。

[0129] アクティベートが完了し、ＣＧＷ１３からのアクティベート完了指示により電源管理ＥＣＵ２０が車両電源をＩＧ電源から＋Ｂ電源に切替えると、ＤＣＭ１２は、データ転送／センター通信動作からスリープ／停止動作に移行し、スリープ／停止動作を開始する。ＣＧＷ１３は、リプログマスタ動作からスリープ／停止動作に移行し、スリープ／停止動作を開始する。２面メモリＥＣＵ、１面サスペンドメモリＥＣＵ及び１面単独メモリＥＣＵは、それぞれ新面起動からスリープ／停止動作に移行する（ｔ３８）。

[0130] これ以降、ユーザがＩＧスイッチオフからオンに切替えたことで車両電源が＋Ｂ電源からＩＧ電源に切替わると、２面メモリＥＣＵ及び１面サスペンドメモリＥＣＵは、それぞれ新面（Ｂ面）を起動面として新アプリプログラムを起動し、１面単独メモリＥＣＵは、新アプリプログラムを起動する（ｔ３９）。

[0131] ＣＧＷ１３は、センター装置３から配信パッケージをダウンロードする前、書込みデータの書換え対象ＥＣＵ１９に配信する前には、以下のチェックを行う。ＣＧＷ１３は、センター装置３から配信パッケージをダウンロードする前では、ダウンロードを正常に行えるように、電波環境、車両バッテリ４０のバッテリ残量、ＤＣＭ１２のメモリ容量のチェックを行う。ＣＧＷ１３は、書込みデータの書換え対象ＥＣＵ１９に配信する前には、書込みデータの配信を正常に行えるように、インストール環境を不安定にしないための有人環境のチェックとして、侵入センサの検知、ドアロックの検知、カーテンの検知、ＩＧオフの検知を行い、書換え対象ＥＣＵ１９が書込み可能であるか否かのチェックとして、バージョン、異常発生のチェックを行う。又、ＣＧＷ１３は、書換え対象ＥＣＵ１９に配信する書込みデータのチェックとして、インストールを開始する前には、改ざんチェック、アクセス認証、バージョンチェック等を行い、インストールを実行中には、通信途絶チェック、異常発生のチェック等を行い、インストールを完了後には、バージョンチェック、完全性チェック、ＤＴＣ（Diagnostic Trouble Code、エラーコード）チェック等を行う。

[0132] 次に、表示端末５が表示する画面について図３０から図４６を参照して説明する。図３０に示すように、書換え対象ＥＣＵ１９のアプリプログラムをＯＴＡにより書換える構成では、キャンペーン通知、ダウンロード、インストール、アクティベートのフェーズがある。キャンペーン通知とは、プログラム更新のお知らせである。例えばセンター装置３においてアプリプログラムの更新有りと判断されたことを受けて、配信諸元データ等をマスタ装置１１がダウンロードすることがキャンペーン通知である。表示端末５は、アプリプログラムの書換えが進行するにしたがって各フェーズにおいて画面を表示する。尚、ここでは、車載ディスプレイ７が表示する画面について説明する。

[0133] ＣＧＷ１３は、図３１に示すように、キャンペーン通知前の通常時では、例えばナビゲーション機能の１つである周知の経路案内画面等のナビゲーシ

ョン画面５０１を車載ディスプレイ７に表示させる。この状態からキャンペーン通知が発生すると、ＣＧＷ１３は、図３２に示すように、ナビゲーション画面５０１の右下にキャンペーン通知の発生を示すキャンペーン通知アイコン５０１ａを表示させる。ユーザは、キャンペーン通知アイコン５０１ａの表示を確認することで、アプリプログラムの更新に関するキャンペーン通知の発生を把握することができる。

[0134] この状態からユーザがキャンペーン通知アイコン５０１ａを操作すると、ＣＧＷ１３は、図３３に示すように、ナビゲーション画面５０１上にキャンペーン通知画面５０２をポップアップ表示させる。尚、ＣＧＷ１３は、キャンペーン通知画面５０２をポップアップ表示させることに限らず、他の表示態様を採用しても良い。ＣＧＷ１３は、キャンペーン通知画面５０２では、例えば「利用できるソフトウェア更新があります」のガイダンスを表示してキャンペーン通知の発生をユーザに知らせると共に、「確認する」ボタン５０２ａ、「後で」ボタン５０２ｂを表示させ、ユーザの操作を待機する。この場合、ユーザは、「確認する」ボタン５０２ａを操作することで、アプリプログラムの書換えを開始させるための次の画面へ進むことができる。尚、ＣＧＷ１３は、ユーザが「後で」ボタン５０２ｂを操作した場合には、キャンペーン通知画面５０２のポップアップ表示を消去させ、図３２に示すキャンペーン通知アイコン５０１ａを表示する画面に戻す。

[0135] この状態からユーザが「確認する」ボタン５０２ａを操作すると、ＣＧＷ１３は、図３４に示すように、ナビゲーション画面５０１からダウンロード承諾画面５０３に表示を切替え、ダウンロード承諾画面５０３を車載ディスプレイ７に表示させる。ＣＧＷ１３は、ダウンロード承諾画面５０３では、キャンペーンＩＤや更新名称をユーザに知らせると共に、「ダウンロード開始」ボタン５０３ａ、「詳細確認」ボタン５０３ｂ、「戻る」ボタン５０３ｃを表示させ、ユーザの操作を待機する。この場合、ユーザは、「ダウンロード開始」ボタン５０３ａを操作することで、ダウンロードを開始させることができ、「詳細確認」ボタン５０３ｂを操作することで、ダウンロードの

詳細を表示させることができ、「戻る」ボタン５０３ｃを表示させることで、ダウンロードを拒否し、前の画面に戻ることができる。「戻る」ボタン５０３ｃを操作した場合であって、ユーザは、キャンペーン通知アイコン５０１ａを操作することにより、ダウンロードを開始するための画面に進むことができる。

[0136] このダウンロード承諾画面５０３を表示させた状態からユーザが「詳細確認」ボタン５０３ｂを操作すると、ＣＧＷ１３は、図３５に示すように、ダウンロード承諾画面５０３の表示内容を切替え、ダウンロードの詳細を車載ディスプレイ７に表示させる。ＣＧＷ１３は、ダウンロードの詳細として、受信した配信諸元データを用いて、更新内容や、更新にかかる時間、更新に伴う車両機能の制約等を表示させる。又、ユーザが「ダウンロード開始」ボタン５０３ａを操作すると、ＣＧＷ１３は、ＤＣＭ１２を介して配信パッケージのダウンロードを開始する。ＣＧＷ１３は、配信パッケージのダウンロードを開始することと並行して、図３６に示すように、ダウンロード承諾画面５０３からナビゲーション画面５０１に表示を切替え、ナビゲーション画面５０１を車載ディスプレイ７に再度表示させ、ナビゲーション画面５０１の右下にダウンロード実行中を示すダウンロード実行中アイコン５０１ｂを表示させる。ユーザは、ダウンロード実行中アイコン５０１ｂの表示を確認することで、配信パッケージのダウンロード実行中を把握することができる。

[0137] この状態からユーザがダウンロード実行中アイコン５０１ｂを操作すると、ＣＧＷ１３は、図３７に示すように、ナビゲーション画面５０１からダウンロード実行中画面５０４に表示を切替え、ダウンロード実行中画面５０４を車載ディスプレイ７に表示させる。ＣＧＷ１３は、ダウンロード実行中画面５０４では、ダウンロードの実行中をユーザに知らせると共に、「詳細確認」ボタン５０４ａ、「戻る」ボタン５０４ｂ及び「キャンセル」ボタン５０４ｃを表示させ、ユーザの操作を待機する。この場合、ユーザは、「詳細確認」ボタン５０４ａを操作することで、ダウンロード実行中の詳細を表示

させることができ、「キャンセル」ボタン５０４ｃを操作させることで、ダウンロードを中断させることができる。

[0138] ＣＧＷ１３は、ダウンロードを完了すると、図３８に示すように、ナビゲーション画面５０１上にダウンロード完了通知画面５０５をポップアップ表示させる。ＣＧＷ１３は、ダウンロード完了通知画面５０５では、例えば「ダウンロードが完了しました　ソフトウェア更新ができます」のガイダンスを表示してダウンロードの完了をユーザに知らせると共に、「確認する」ボタン５０５ａ、「後で」ボタン５０５ｂを表示させ、ユーザの操作を待機する。この場合、ユーザは、「確認する」ボタン５０５ａを操作することで、インストールを開始するための画面に進むことができる。

[0139] この状態からユーザが「確認する」ボタン５０５ａを操作すると、ＣＧＷ１３は、図３９に示すように、ナビゲーション画面５０１からインストール承諾画面５０６に表示を切替え、インストール承諾画面５０６を車載ディスプレイ７に表示させる。ＣＧＷ１３は、インストール承諾画面５０６では、インストールに関する所要時間や制約事項及びスケジュールの設定をユーザに知らせると共に、「すぐ更新」ボタン５０６ａ、「予約して更新」ボタン５０６ｂ、「戻る」ボタン５０６ｃを表示させ、ユーザの操作を待機する。この場合、ユーザは、「すぐ更新」ボタン５０６ａを操作することで、インストールを直ぐに開始させることができる。又、ユーザは、インストールを実行したい時刻を設定し、「予約して更新」ボタン５０６ｂを操作することで、インストールを予約して開始させることができる。又、ユーザは、「戻る」ボタン５０６ｃを操作することで、インストールを拒否し、前の画面に戻ることができる。「戻る」ボタン５０６ｃを操作した場合であって、ユーザは、ダウンロード実行中アイコン５０１ｂを操作することにより、インストールを開始するための画面に進むことができる。

[0140] この状態からユーザが「すぐ更新」ボタン５０６ａを操作すると、ＣＧＷ１３は、図４０に示すように、インストール承諾画面５０６の表示内容を切替え、インストールの詳細を車載ディスプレイ７に表示させる。ＣＧＷ１３

は、ここでのインストール承諾画面５０６では、インストールの要求を受付け、インストールを開始する旨をユーザに知らせる。

[0141] ＣＧＷ１３は、インストールを開始すると、図４１に示すように、インストール承諾画面５０６からナビゲーション画面５０１に表示を切替え、ナビゲーション画面５０１を車載ディスプレイ７に再度表示させ、ナビゲーション画面５０１の右下にインストール実行中を示すインストール実行中アイコン５０１ｃを表示させる。ユーザは、インストール実行中アイコン５０１ｃの表示を確認することで、インストール実行中を把握することができる。

[0142] この状態からユーザがインストール実行中アイコン５０１ｃを操作すると、ＣＧＷ１３は、図４２に示すように、ナビゲーション画面５０１からインストール実行中画面５０７に表示を切替え、インストール実行中画面５０７を車載ディスプレイ７に表示させる。ＣＧＷ１３は、インストール実行中画面５０７では、インストールの実行中をユーザに知らせる。ＣＧＷ１３は、例えばインストールの所要残り時間や進捗パーセントをインストール実行中画面５０７に表示させても良い。

[0143] ＣＧＷ１３は、インストールを完了すると、図４３に示すように、ナビゲーション画面５０１からアクティベート承諾画面５０８に表示を切替え、アクティベート承諾画面５０８を車載ディスプレイ７に表示させる。ＣＧＷ１３は、アクティベート承諾画面５０８では、アクティベートの内容をユーザに知らせると共に、「戻る」ボタン５０８ａ及び「ＯＫ」ボタン５０８ｂを表示させ、ユーザの操作を待機する。この場合、ユーザは、「戻る」ボタン５０８ａを操作することで、アクティベートを拒否し、前の画面に戻ることができる。又、ユーザは、「ＯＫ」ボタン５０８ｂを操作することで、アクティベートを承諾することができる。尚、「戻る」ボタン５０８ａを操作した場合であって、ユーザは、インストール実行中アイコン５０１ｃを操作することにより、アクティベートを実行するための画面に進むことができる。尚、これらの表示や承諾については、ユーザの設定やプログラムのシーンにより表示させずに省略することも可能である。

[0144] ユーザが「ＯＫ」ボタン５０８ｂを操作した後の状態からユーザがＩＧ電源をオンすると、ＣＧＷ１３は、図４４に示すように、ナビゲーション画面５０１上にアクティベート完了通知画面５０９をポップアップ表示させる。ＣＧＷ１３は、アクティベート完了通知画面５０９では、例えば「ソフトウェア更新が完了しました」のガイダンスを表示してアクティベートの完了をユーザに知らせると共に、「ＯＫ」ボタン５０９ａ、「詳細確認」ボタン５０９ｂを表示させ、ユーザの操作を待機する。この場合、ユーザは、「ＯＫ」ボタン５０９ａを操作することで、アクティベート完了通知画面５０９のポップアップ表示を消去させることができ、「詳細確認」ボタン５０９ｂを操作することで、アクティベートの完了の詳細を表示させることができる。

[0145] この状態からユーザが「ＯＫ」ボタン５０９ａを操作すると、ＣＧＷ１３は、図４５に示すように、ナビゲーション画面５０１から確認操作画面５１０に表示を切替え、確認操作画面５１０を車載ディスプレイ７に表示させる。ＣＧＷ１３は、確認操作画面５１０では、アクティベートの完了をユーザに知らせると共に、「詳細確認」ボタン５１０ａ、「ＯＫ」ボタン５１０ｂを表示させ、ユーザの操作を待機する。この場合、ユーザは、「詳細確認」ボタン５１０ａを操作することで、アクティベートの完了の詳細を表示させることができる。

[0146] この状態からユーザが「詳細確認」ボタン５１０ａを操作すると、ＣＧＷ１３は、図４６に示すように、確認操作画面５１０の表示内容を切替え、アクティベートの完了の詳細を車載ディスプレイ７に表示させる。ＣＧＷ１３は、更新により追加された機能や変更された機能等を更新詳細として表示すると共に、「ＯＫ」ボタン５１０ｂを表示する。ＣＧＷ１３は、ユーザが「ＯＫ」ボタン５０９ａ、５１０ｂを操作したことをもって、ソフトウェア更新完了をユーザが確認したと判断する。

[0147] 以上に説明したように、車両側システム４は、キャンペーン通知、ダウンロード、インストール、アクティベート、更新完了という各動作フェーズを制御すると共に、各動作フェーズに合わせた表示をユーザへ提示する。尚、

上述した説明では、ＣＧＷ１３が表示の制御を行う構成としたが、車載ディスプレイ７がＣＧＷ１３から動作フェーズや配信諸元データを受信し、表示を行うように構成しても良い。

[0148] 次に、車両用プログラム書換えシステム１が行う特徴的な処理について図４７から図２３３を参照して説明する。車両用プログラム書換えシステム１は、以下に示す特徴的な処理を行う。

（１）配信パッケージの送信判定処理

（２）配信パッケージのダウンロード判定処理

（３）書込みデータの転送判定処理

（４）書込みデータの取得判定処理

（５）インストールの指示判定処理

（６）セキュリティアクセス鍵の管理処理

（７）書込みデータの検証処理

（８）データ格納面情報の送信制御処理

（９）非書換え対象の電源管理処理

（１０）ファイルの転送制御処理

（１１）書込みデータの配信制御処理

（１２）アクティベート要求の指示処理

（１３）アクティベートの実行制御処理

（１４）書換え対象のグループ管理処理

（１５）ロールバックの実行制御処理

（１６）書換え進捗状況の表示制御処理

（１７）差分データの整合性判定処理

（１８）書換えの実行制御処理

（１９）セッションの確立処理

（２０）リトライポイントの特定処理

（２１）進捗状態の同期制御処理

（２２）表示制御情報の送信制御処理

（２３）表示制御情報の受信制御処理

（２４）進捗表示の画面表示制御処理

（２５）プログラム更新の報知制御処理

（２６）電源自己保持の実行制御処理

[0149] センター装置３、ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９、車載ディスプレイ７は、それぞれ上記した（１）～（２６）の特徴的な処理を行う構成として以下の機能ブロックを有する。

[0150] 図４７に示すように、センター装置３は、配信パッケージ送信部５１を有する。配信パッケージ送信部５１は、ＤＣＭ１２から配信パッケージのダウンロード要求を受信すると、配信パッケージをＤＣＭ１２に送信する。センター装置３は、上記した構成に加え、特徴的な処理を行う構成として、配信パッケージの送信判定部５２と、進捗状態の同期制御部５３と、表示制御情報の送信制御部５４と、書込みデータ選定部５５（更新データ選定部に相当する）を有する。書込みデータ選定部５５（更新データ選定部に相当する）は、マスタ装置１１からデータ格納面情報を受信すると、その受信したデータ格納面情報により特定されるソフトウェアバージョン及び運用面に基づいて、非運用面に適合する書込みデータを選定する。即ち、配信パッケージ送信部５１は、書込みデータ選定部５５により選定された書込みデータを含む配信パッケージをＤＣＭ１２に送信する。特徴的な処理を行う機能ブロックについては後述する。

[0151] 図４８に示すように、ＤＣＭ１２は、ダウンロード要求送信部６１と、配信パッケージダウンロード部６２と、書込みデータ抽出部６３と、書込みデータ転送部６４と、書換え諸元データ抽出部６５と、書換え諸元データ転送部６６とを有する。ダウンロード要求送信部６１は、配信パッケージのダウンロード要求をセンター装置３に送信する。配信パッケージダウンロード部６２は、センター装置３から配信パッケージをダウンロードする。書込みデータ抽出部６３は、センター装置３から配信パッケージが配信パッケージダウンロード部６２によりダウンロードされると、そのダウンロードされた配

信パッケージから書込みデータを抽出する。

[0152] 書込みデータ転送部６４は、配信パッケージから書込みデータが書込みデータ抽出部６３により抽出されると、その抽出された書込みデータをＣＧＷ１３に転送する。書換え諸元データ抽出部６５は、センター装置３から配信パッケージが配信パッケージダウンロード部６２によりダウンロードされると、そのダウンロードされた配信パッケージから書換え諸元データを抽出する。書換え諸元データ転送部６６は、配信パッケージから書換え諸元データが書換え諸元データ抽出部５６により抽出されると、その抽出された書換え諸元データをＣＧＷ１３に転送する。ＤＣＭ１２は、上記した構成に加え、特徴的な処理を行う構成として、配信パッケージのダウンロード判定部６７と、書込みデータの転送判定部６８とを有する。特徴的な処理を行う機能ブロックについては後述する。

[0153] 図４９及び図５０に示すように、ＣＧＷ１３は、取得要求送信部７１と、書込みデータ取得部７２（更新データ記憶部に相当する）と、書込みデータ配信部７３（更新データ配信部に相当する）と、書換え諸元データ取得部７４と、書換え諸元データ解析部７５とを有する。書込みデータ取得部７２は、ＤＣＭ１２から書込みデータが転送されることで、ＤＣＭ１２から書込みデータを取得する。書込みデータ配信部７３は、書込みデータが書込みデータ取得部７２により取得されると、その書込みデータの配信タイミングになると、その取得された書込みデータを書換え対象ＥＣＵ１９に配信する。書換え諸元データ取得部７４は、ＤＣＭ１２から書換え諸元データが転送されることで、ＤＣＭ１２から書換え諸元データを取得する。書換え諸元データ解析部７５は、書換え諸元データが書換え諸元データ取得部７４により取得されると、その取得された書換え諸元データを解析する。

[0154] ＣＧＷ１３は、上記した構成に加え、特徴的な処理を行う構成として、書込みデータの取得判定部７６と、インストールの指示判定部７７と、セキュリティアクセス鍵の管理部７８と、書込みデータの検証部７９と、データ格納面情報の送信制御部８０と、非書換え対象の電源管理部８１と、ファイル

の転送制御部８２と、書込みデータの配信制御部８３と、アクティベート要求の指示部８４と、書換え対象のグループ管理部８５と、ロールバックの実行制御部８６と、書換え進捗状況の表示制御部８７と、進捗状態の同期制御部８８と、表示制御情報の受信制御部８９と、進捗表示の画面表示制御部９０と、プログラム更新の報知制御部９１と、電源自己保持の実行制御部９２とを有する。特徴的な処理を行う機能ブロックについては後述する。

[0155] 図５１に示すように、ＥＣＵ１９は、書込みデータ受信部１０１と、プログラム書換え部１０２とを有する。書込みデータ受信部１０１は、ＣＧＷ１３から書込みデータを受信する。プログラム書換え部１０２は、ＣＧＷ１３から書込みデータが書込みデータ受信部１０１により受信されると、その受信された書込みデータをフラッシュメモリに書込んでアプリプログラムを書換える。ＥＣＵ１９は、上記した構成に加え、特徴的な処理を行う構成として、差分データの整合性判定部１０３と、書換えの実行制御部１０４と、セッションの確立部１０５と、リトライポイントの特定部１０６と、アクティベートの実行制御部１０７と、電源自己保持の実行制御部１０８とを有する。特徴的な処理を行う機能ブロックについては後述する。

[0156] 図５２に示すように、車載ディスプレイ７は、配信諸元データの受信制御部１１１を有する。配信諸元データの受信制御部１１１は、配信諸元データの受信を制御する。

以下、上記した（１）～（２６）の各処理について順次説明する。

[0157] （１）配信パッケージの送信判定処理、（２）配信パッケージのダウンロード判定処理

センター装置３における配信パッケージの送信判定処理について図５３及び図５４を参照して説明し、マスタ装置１１における配信パッケージのダウンロード判定処理について図５５及び図５６を参照して説明する。

[0158] 図５３に示すように、センター装置３は、配信パッケージの送信判定部５２において、ソフトウェア情報取得部５２ａと、更新有無判定部５２ｂと、更新適否判定部５２ｃと、キャンペーン情報送信部５２ｄと有する。ソフト

ウェア情報取得部５２ａは、車両側から各ＥＣＵ１９のソフトウェア情報を取得する。具体的には、ソフトウェア情報取得部５２ａは、バージョンや書込み面等のソフトウェア情報とハードウェア情報とを含むＥＣＵ構成情報を車両側から取得する。ソフトウェア情報取得部５２ａは、これらＥＣＵ構成情報と合わせて、故障コード、盗難防止アラーム機能の設定、ライセンス契約情報等の車両状態情報を車両側から取得しても良い。

[0159] 更新有無判定部５２ｂは、ソフトウェア情報がソフトウェア情報取得部５２ａにより取得されると、その取得されたソフトウェア情報に基づいて、車両に対する更新データの有無を判定する。即ち、更新有無判定部５２ｂは、その取得されたソフトウェア情報のバージョンと自己の管理する最新のソフトウェア情報のバージョンとを比較し、両者が一致するか否かを判定し、車両に対する更新データの有無を判定する。更新有無判定部５２ｂは、両者が一致すると判定すると、車両に対する更新データが無いと判定し、両者が一致しないと判定すると、車両に対する更新データが有ると判定する。

[0160] 更新適否判定部５２ｃは、車両に対する更新データが有ることが更新有無判定部５２ｂにより判定されると、車両状態が配信パッケージを用いたプログラム等の更新に適する状態であるか否かを判定する。具体的には、更新適否判定部５２ｃは、ライセンス契約が成立しているか否か、車両位置がユーザにより予め登録された所定範囲内であるか否か、車両のアラーム機能の設定が有効化されているか否か、ＥＣＵ１９の故障情報が発生しているか否かを判定し、車両状態が配信パッケージのダウンロードに適する状態であるか否かを判定する。即ち、更新適否判定部５２ｃは、ユーザの意に反する更新となる可能性のある車両や、仮にダウンロードが成功したとしても、ダウンロード後のインストールで失敗する可能性のある車両であるか否かを判定する。

[0161] 更新適否判定部５２ｃは、ライセンス契約が成立しており、車両位置がユーザにより予め登録された所定範囲内であり、車両のアラーム機能の設定が有効化されており、ＥＣＵ１９の故障情報が発生していない状態であると判

定すると、車両状態が配信パッケージを用いたプログラム等の更新に適する状態であると判定する。更新適否判定部５２ｃは、ライセンス契約が成立していない、車両位置がユーザにより予め登録された所定範囲内でない、車両のアラーム機能の設定が有効化されていない、ＥＣＵ１９の故障情報が発生しているのうち少なくとも何れかであると判定すると、車両状態が配信パッケージを用いたプログラム等の更新に適する状態でないと判定する。

[0162] キャンペーン情報送信部５２ｄは、車両状態が配信パッケージを用いたプログラム等の更新に適する状態であると更新適否判定部５２ｃにより判定されると、キャンペーン情報をマスタ装置１１に送信する。キャンペーン情報送信部５２ｄは、車両状態が配信パッケージを用いたプログラム等の更新に適する状態でないと更新適否判定部５２ｃにより判定されると、キャンペーン情報をマスタ装置１１に送信しない。キャンペーン情報送信部５２ｄは、上記した判定を行うことで、キャンペーン情報をマスタ装置１１に送信しなかった車両に関する情報を記憶しておく。尚、センター装置３において、キャンペーン情報をマスタ装置１１に送信しなかった車両に関する情報を表示しても良い。

[0163] 次に、センター装置３における配信パッケージの送信判定部５２の作用について図５４を参照して説明する。センター装置３は、配信パッケージの送信判定プログラムを実行し、配信パッケージの送信判定処理を行う。

[0164] センター装置３は、配信パッケージの送信判定処理を開始すると、車両側からソフトウェア情報を取得する（Ｓ１０１、ソフトウェア情報取得手順に相当する）。即ち、センター装置３は、車両に対するソフトウェア更新があるか否かを判定する。センター装置３は、その取得したソフトウェア情報に基づいて車両に対する更新データの有無を判定する（Ｓ１０２、更新有無判定手順に相当する）。センター装置３は、車両に対する更新データが有ると判定すると（Ｓ１０２：ＹＥＳ）、車両状態が配信パッケージを用いたプログラム等の更新に適する状態であるか否かを判定する（Ｓ１０３、更新適否判定手順に相当する）。センター装置３は、車両状態が配信パッケージを用

いたプログラム等の更新に適する状態であると判定すると（Ｓ１０３：ＹＥＳ）、キャンペーン情報をマスタ装置１１に送信し（Ｓ１０４、キャンペーン情報送信手順に相当する）、配信パッケージの送信判定処理を終了する。

[0165] センター装置３は、車両に対する更新データが無いと判定すると（Ｓ１０２：ＮＯ）、配信パッケージの送信対象でない旨、即ち、アプリプログラムの更新がない旨をマスタ装置１１に送信し（Ｓ１０５）、配信パッケージの送信判定処理を終了する。センター装置３は、車両状態が配信パッケージを用いたプログラム等の更新に適する状態でないと判定すると（Ｓ１０３：ＮＯ）、プログラム等の更新に適さない旨及びその理由をマスタ装置１１に送信し（Ｓ１０６）、配信パッケージの送信判定処理を終了する。この場合、マスタ装置１１は、プログラム等の更新に適さない旨及びその理由を車載ディスプレイ７に表示させる。マスタ装置１１は、例えばライセンス契約が成立していなければ、例えば「ライセンスが無効なためプログラム更新ができません。ディーラーへご相談下さい。」等を車載ディスプレイ７に表示させる。これにより、プログラム等の更新に適さない旨の理由をユーザに提示することができ、適切な情報をユーザに提示することができる。

[0166] 以上に説明したように、センター装置３は、マスタ装置１１への配信パッケージの送信前であり、キャンペーン情報の送信前に、配信パッケージの送信判定処理を行うことで、配信パッケージを用いたプログラム等の更新に適する状態であるか否かを判定することができる。そして、センター装置３は、配信パッケージを用いたプログラム等の更新に適する状態であると判定した場合に限って配信パッケージをマスタ装置１１に送信すべく、キャンペーン情報をマスタ装置１１に送信することができる。

[0167] センター装置３は、配信パッケージを用いたプログラム等の更新に適した場合として、ライセンス契約が成立しており、車両位置がユーザにより予め登録された所定範囲内であり、車両のアラーム機能の設定が有効化されており、ＥＣＵ１９の故障情報が発生していない場合に、キャンペーン情報をマスタ装置１１に送信することができる。即ち、センター装置３は、ライセン

ス契約が未成立であったり、車両位置が自宅から遠く離れた位置等の所定範囲外であったり、車両のアラーム機能の設定が無効化されていたり、ＥＣＵ１９の故障情報が発生していたりする場合に、キャンペーン情報をマスタ装置１１に送信する事態を回避することができる。このようにセンター装置３は、ユーザの意に反する更新となる可能性のある車両や、仮にダウンロードに成功したとしても、インストールで失敗する可能性のある車両に対し、キャンペーン情報をマスタ装置１１に送信しないようすることができる。

[0168] 尚、センター装置３は、配信パッケージの送信中に配信パッケージの送信判定処理を行っても良い。この場合、センター装置３は、配信パッケージの送信中に車両状態が配信パッケージを用いたプログラム等の更新に適する状態であると判定すると、配信パッケージの送信を継続するが、配信パッケージの送信中に車両状態が配信パッケージを用いたプログラム等の更新に適する状態でないと判定すると、配信パッケージの送信を中断する。即ち、センター装置３は、配信パッケージの送信中に例えばＥＣＵ１９の故障情報が発生すると、配信パッケージの送信を中断する。

[0169] 次に、センター装置３から送信されたキャンペーン情報を受信したマスタ装置１１の処理について説明する。マスタ装置１１における配信パッケージのダウンロード判定処理について図５５及び図５６を参照して説明する。車両用プログラム書換えシステム１は、マスタ装置１１において配信パッケージのダウンロード判定処理を行う。前述した（１）配信パッケージの送信判定処理は、センター装置３がダウンロードフェーズの前のキャンペーン通知フェーズで行う判定処理であるが、配信パッケージのダウンロード判定処理は、マスタ装置１１がダウンロードフェーズで行う判定処理である。尚、本実施形態ではマスタ装置１１において、ＤＣＭ１２が配信パッケージのダウンロード判定処理を行う場合を説明するが、ＣＧＷ１３がＤＣＭ１２の機能を有することで、ＣＧＷ１３が配信パッケージのダウンロード判定処理を行っても良い。

[0170] 図５５に示すように、ＤＣＭ１２は、配信パッケージのダウンロード判定

部６７において、キャンペーン情報受信部６７ａと、ダウンロード可能判定部６７ｂと、ダウンロード実行部６７ｃとを有する。キャンペーン情報受信部６７ａは、センター装置３からキャンペーン情報を受信する。尚、センター装置３からキャンペーン情報を受信すると、図３２に示したキャンペーン通知アイコン５０１ａが表示される。ダウンロード可能判定部６７ｂは、キャンペーン情報がキャンペーン情報受信部６７ａにより受信されると、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定する。即ち、ダウンロード可能判定部６７ｂは、センター装置３と通信するための電波環境が良好であるか否か、車両バッテリ４０のバッテリ残量が所定容量以上であるか否か、ＤＣＭ１２のメモリ空き容量が所定容量以上であるか否かを判定し、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定する。

[0171] ダウンロード可能判定部６７ｂは、電波環境が良好であり、車両バッテリ４０のバッテリ残量が所定容量以上であり、ＤＣＭ１２のメモリ空き容量が所定容量以上であると判定すると、車両状態が配信パッケージをダウンロード可能な状態であると判定する。ダウンロード可能判定部６７ｂは、電波環境が良好でなく、車両バッテリ４０のバッテリ残量が所定容量以上でなく、ＤＣＭ１２のメモリ空き容量が所定容量以上でないのうち少なくとも何れかを判定すると、車両状態が配信パッケージをダウンロード可能な状態でないと判定する。

[0172] このようにダウンロード可能判定部６７ｂは、ダウンロードを正常に完了することができない可能性があるか否かを判定する。尚、ダウンロード可能判定部６７ｂによる判定は、図３４及び図３５に示すダウンロード承諾画面５０３において、ユーザにより「ダウンロード開始」ボタン５０３ａを操作されたことを条件として行う。又、ダウンロード可能判定部６７ｂは、センター装置３における判定項目についても判定するように構成しても良い。即ち、ダウンロード可能判定部６７ｂは、例えば車両のアラーム機能の設定が有効化されている場合や、ＥＣＵ１９の故障情報が発生していない場合に、

ダウンロード可能な状態であると判定する。

[0173] ダウンロード実行部６７ｃは、車両状態が配信パッケージをダウンロード可能な状態であるとダウンロード可能判定部６７ｂにより判定されると、センター装置３から配信パッケージをダウンロードする。即ち、ダウンロード実行部６７ｃは、ダウンロードを正常に完了することができることを確認した上で、配信パッケージのダウンロードを実行する。

[0174] ダウンロード実行部６７ｃは、車両状態が配信パッケージをダウンロード可能な状態でないとダウンロード可能判定部６７ｂにより判定されると、センター装置３から配信パッケージをダウンロードしない。即ち、ダウンロード実行部６７ｃは、ダウンロードを正常に完了することができない可能性がある場合には、配信パッケージのダウンロードを実行しない。この場合、ダウンロード実行部６７ｃは、ナビゲーション画面５０１にダウンロードを開始できなかった旨及びその理由を示すポップアップ画面を表示するように車載ディスプレイ７に指示する。

[0175] 次に、マスタ装置１１における配信パッケージのダウンロード判定部６７の作用について図５６を参照して説明する。マスタ装置１１は、配信パッケージのダウンロード判定プログラムを実行し、配信パッケージのダウンロード判定処理を行う。

[0176] マスタ装置１１は、配信パッケージのダウンロード判定処理を開始すると、センター装置３からキャンペーン情報を受信する（Ｓ２０１、キャンペーン情報受信手順に相当する）。マスタ装置１１は、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定する（Ｓ２０２、ダウンロード可能判定手順に相当する）。マスタ装置１１は、車両状態が配信パッケージをダウンロード可能な状態であると判定すると（Ｓ２０２：ＹＥＳ）、センター装置３から当該キャンペーンに対応する配信パッケージをダウンロードし（Ｓ２０３、ダウンロード実行手順に相当する）、配信パッケージのダウンロード判定処理を終了する。マスタ装置１１は、車両状態が配信パッケージをダウンロード可能な状態でないと判定すると（Ｓ２０２：ＮＯ）、

センター装置３から配信パッケージをダウンロードせず、配信パッケージのダウンロード判定処理を終了する。

[0177] 以上に説明したように、マスタ装置１１は、センター装置３からの配信パッケージのダウンロード前に、配信パッケージのダウンロード判定処理を行うことで、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定することができる。そして、マスタ装置１１は、車両状態が配信パッケージをダウンロード可能な状態である場合に限って配信パッケージをダウンロードすることができる。

[0178] マスタ装置１１は、配信パッケージのダウンロードに適した場合として、電波環境が良好であり、車両バッテリ４０のバッテリ残量が所定容量以上であり、ＤＣＭ１２のメモリ空き容量が所定容量以上である場合に、センター装置３から配信パッケージをダウンロードすることができる。即ち、電波環境が良好でなかったり、車両バッテリ４０のバッテリ残量が所定容量未満であったり、ＤＣＭ１２のメモリ空き容量が所定容量未満であったりする場合に、センター装置３から配信パッケージをダウンロードする事態を回避することができる。

[0179] 尚、マスタ装置１１は、配信パッケージのダウンロード中に配信パッケージのダウンロード判定処理を行っても良い。この場合、マスタ装置１１は、配信パッケージのダウンロード中に車両状態が配信パッケージをダウンロード可能な状態であると判定すると、センター装置３からの配信パッケージのダウンロードを継続するが、配信パッケージのダウンロード中に車両状態が配信パッケージをダウンロード可能な状態でないと判定すると、センター装置３からの配信パッケージのダウンロードを中断する。即ち、マスタ装置１１は

、配信パッケージのダウンロード中に例えば電波環境が良好でなくなったり車両バッテリ４０のバッテリ残量が所定容量未満になったりＤＣＭ１２のメモリ空き容量が所定容量未満になったりすると、配信パッケージのダウンロードを中断する。

[0180] このようにセンター装置３において、ユーザの意に反する更新となる可能性のある車両や、インストールに失敗する可能性のある車両であるか否かを判定すると共に、マスタ装置１１において、ダウンロードに失敗する可能性があるか否かを判定することにより、センター装置３からマスタ装置１１への無用なキャンペーン情報や配信パッケージの送信を抑制することができる。

[0181] センター装置３は、以下の構成を有する。車両側から電子制御装置のソフトウェア情報を取得するソフトウェア情報取得部５２ａと、前記ソフトウェア情報取得部により取得されたソフトウェア情報に基づいて、車両に対する更新データの有無を判定する更新有無判定部５２ｂと、更新データが有ると前記更新有無判定部により判定された場合に、車両状態が更新に適する状態であるか否かを判定する更新適否判定部５２ｃと、車両状態が更新に適する状態であると前記更新適否判定部により判定された場合に、更新に関するキャンペーン情報を車両用マスタ装置に送信するキャンペーン情報送信部５２ｄと、を備える。

[0182] マスタ装置１１は、以下の構成を有する。センター装置からキャンペーン情報を受信するキャンペーン情報受信部６７ａと、キャンペーン情報が前記キャンペーン情報受信部により受信された場合に、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定するダウンロード可能判定部６７ｂと、車両状態が配信パッケージをダウンロード可能な状態であると前記ダウンロード可能判定部により判定された場合に、センター装置から配信パッケージをダウンロードするダウンロード実行部６７ｃと、を備える。

[0183] （３）書込みデータの転送判定処理、（４）書込みデータの取得判定処理、（５）インストールの指示判定処理

書込みデータの転送判定処理について図５７及び図５８を参照して説明し、書込みデータの取得判定処理について図５９及び図６０を参照して説明し、インストールの指示判定処理について図６１から図６４を参照して説明する。車両用プログラム書換えシステム１は、ＤＣＭ１２において書込みデー

タの転送判定処理を行う。ここでは、センター装置３からＤＣＭ１２に送信された配信パッケージがアンパッケージングされ、配信パッケージから書込みデータが抽出された状態とする。

[0184] 図５７に示すように、ＤＣＭ１２は、書込みデータの転送判定部６８において、取得要求受信部６８ａと、通信状態判定部６８ｂとを有する。取得要求受信部６８ａは、ＣＧＷ１３から書込みデータの取得要求を受信する。通信状態判定部６８ｂは、書込みデータの取得要求が取得要求受信部６８ａにより受信されると、例えばユーザが予め設定する転送可否判定フラグが第１所定値である場合に、センター装置３とＤＣＭ１２との間のデータ通信の状態を判定する。転送可否判定フラグとは、例えばインストールの際に所定条件をチェックする場合は１（第１所定値）、チェックを省略する場合は０（第２所定値）である。書込みデータ転送部６４は、センター装置３とＤＣＭ１２との間のデータ通信が接続状態であると通信状態判定部６８ｂにより判定されていることを条件として書込みデータをＣＧＷ１３に転送する。

[0185] 次に、ＤＣＭ１２における書込みデータの転送判定部６８の作用について図５８を参照して説明する。ＤＣＭ１２は、書込みデータの転送判定プログラムを実行し、書込みデータの転送判定処理を行う。ここでは、センター装置３からのインストール指示にしたがい、ＣＧＷ１３がＤＣＭ１２に対して書込みデータの取得を要求した場合の処理について説明する。

[0186] ＤＣＭ１２は、ＣＧＷ１３から書込みデータの取得要求を受信したと判定すると、書込みデータの転送判定処理を開始する。ＤＣＭ１２は、書込みデータの転送判定処理を開始すると、転送可否判定フラグを判定する（Ｓ３０１，Ｓ３０２）。ＤＣＭ１２は、転送可否判定フラグが第１所定値であると判定すると（Ｓ３０１：ＹＥＳ）、センター装置３と自己との間のデータ通信の状態を判定する（Ｓ３０３）。ＤＣＭ１２は、センター装置３と自己との間のデータ通信が接続状態であると判定すると（Ｓ３０３：ＹＥＳ）、書込みデータをＣＧＷ１３に転送し（Ｓ３０４）、書込みデータの転送判定処理を終了する。ＤＣＭ１２は、センター装置３と自己との間のデータ通信が

接続状態でなく途絶状態であると判定すると（Ｓ３０３：ＮＯ）、書込みデータをＣＧＷ１３に転送せず、書込みデータの転送判定処理を終了する。

[0187] 又、ＤＣＭ１２は、転送可否判定フラグが第２所定値であると判定すると（Ｓ３０２：ＹＥＳ）、センター装置３と自己との間のデータ通信の状態を判定せずに書込みデータをＣＧＷ１３に転送し、書込みデータの転送判定処理を終了する。

[0188] 以上に説明したように、ＤＣＭ１２は、ＣＧＷ１３への書込みデータの転送前に書込みデータの転送判定処理を行うことで、転送可否判定グラグが第１所定値の場合にセンター装置３と自己との間のデータ通信の状態を判定する。ＤＣＭ１２は、データ通信が接続状態であると判定すると、書込みデータの転送を開始し、データ通信が途絶状態であると判定すると、書込みデータの転送を開始せずに待機する。センター装置３とのデータ通信が可能な状況下において、書込みデータをＣＧＷ１３に転送することができ、書換え対象ＥＣＵ１９においてインストールを実行することができる。

[0189] 例えば書換え対象ＥＣＵ１９が複数であり、インストールに時間を要する場合に、インストールの進捗状況を車載側システム４からセンター装置３に通知することができ、携帯端末６にて進捗状況を逐一表示することができる。尚、ＤＣＭ１２は、書込みデータの転送中に書込みデータの転送判定処理を行っても良い。この場合、ＤＣＭ１２は、書込みデータの転送中にデータ通信が接続状態であると判定すると、書込みデータの転送を継続するが、書込みデータの転送中にデータ通信が途絶状態であると判定すると、書込みデータの転送を中断する。

[0190] 次に、書込みデータの取得判定処理について説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において書込みデータの取得判定処理を行う。前述した（３）書込みデータの転送判定処理は、インストールフェーズでＤＣＭ１２が行う判定処理であり、書込みデータの取得判定処理は、同じくインストールフェーズでＣＧＷ１３が行う判定処理である。

[0191] 図５９に示すように、ＣＧＷ１３は、書込みデータの取得判定部７６にお

いて、イベント発生判定部７６ａと、通信状態判定部７６ｂとを有する。イベント発生判定部７６ａは、センター装置３からの書込みデータの取得要求（インストール指示）のイベント発生を判定する。通信状態判定部７６ｂは、書込みデータの取得要求のイベント発生がイベント発生判定部７６ａにより判定されると、例えばユーザが予め設定する取得可否判定フラグが第１所定値である場合に、センター装置３とＤＣＭ１２との間のデータ通信の状態を判定する。取得可否判定フラグとは、例えばインストールの際に所定条件をチェックする場合は１（第１所定値）、チェックを省略する場合は０（第２所定値）である。ここで、イベント発生判定部７６ａは、ユーザがインストールを指示したことに基づいてイベント発生を判定しても良く、例えばユーザが車載ディスプレイ７にてインストールの指示操作（図３９参照）をした旨の通知を受けると、書込みデータの取得要求のイベントが発生したと判定する。

[0192] 次に、ＣＧＷ１３における書込みデータの取得判定部７６の作用について図６０を参照して説明する。ＣＧＷ１３は、書込みデータの取得判定プログラムを実行し、書込みデータの取得判定処理を行う。

[0193] ＣＧＷ１３は、書込みデータの取得要求のイベント発生を判定すると、書込みデータの取得判定処理を開始する。ＣＧＷ１３は、書込みデータの取得判定処理を開始すると、取得可否判定フラグを判定する（Ｓ４０１，Ｓ４０２）。ＣＧＷ１３は、取得可否判定フラグが第１所定値であると判定すると（Ｓ４０１：ＹＥＳ）、センター装置３とＤＣＭ１２との間のデータ通信の状態を判定する（Ｓ４０３：。ＣＧＷ１３は、センター装置３とＤＣＭ１２との間のデータ通信が接続であると判定すると（Ｓ４０３：ＹＥＳ）、書込みデータの取得要求をＤＣＭ１２に送信し（Ｓ４０４）、書込みデータの取得判定処理を終了する。これ以降、ＣＧＷ１３は、ＤＣＭ１２から書込みデータが転送されると、その転送された書込みデータを書換え対象ＥＣＵ１９に配信する。ＣＧＷ１３は、センター装置３とＤＣＭ１２との間のデータ通信が接続でなく途絶であると判定すると（Ｓ４０３：ＮＯ）、書込みデータ

の取得要求をＤＣＭ１２に送信せず、書込みデータの取得判定処理を終了する。

[0194] 又、ＣＧＷ１３は、取得可否判定フラグが第２所定値であると判定すると（Ｓ４０２：ＹＥＳ）、センター装置３とＤＣＭ１２との間のデータ通信の状態を判定せずに書込みデータの取得要求をＤＣＭ１２に送信し、書込みデータの取得判定処理を終了する。

[0195] 以上に説明したように、ＣＧＷ１３は、ＤＣＭ１２からの書込みデータの取得前に書込みデータの取得判定処理を行うことで、取得可否判定グラグが第１所定値の場合にセンター装置３とＤＣＭ１２との間のデータ通信の状態を判定する。ＣＧＷ１３は、データ通信が接続状態であると判定すると、書込みデータの取得を開始し、データ通信が途絶状態であると判定すると、書込みデータの取得を開始せずに待機する。センター装置３との通信が可能な状況下において、ＤＣＭ１２から書込みデータを取得することができ、書換え対象ＥＣＵ１９においてインストールを実行することができる。

[0196] 例えば書換え対象ＥＣＵ１９が複数であり、インストールに時間を要する場合に、インストールの進捗状況を車載側システム４からセンター装置３に通知することができ、携帯端末６にて進捗状況を逐一表示することができる。尚、ＣＧＷ１３は、書込みデータの取得中に書込みデータの取得判定処理を行っても良い。この場合、ＣＧＷ１３は、書込みデータの取得中にデータ通信が接続状態であると判定すると、書込みデータの取得を継続するが、書込みデータの取得中にデータ通信が途絶状態であると判定すると、書込みデータの取得を中断する。

[0197] 次に、前述した書込みデータの取得判定についてより詳細に説明する。書込みデータの取得は、インストールに関する処理の一つであり、ここでは、インストールの指示判定処理について図６１から図６４を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３においてインストールの指示判定処理を行う。前述した（１）配信パッケージの送信判定処理、（２）配信パッケージのダウンロード判定処理は、ダウンロードフェーズで行

う判定処理であり、（３）書込みデータの転送判定処理、（４）書込みデータの取得判定処理は、ダウンロード完了後のインストールフェーズで行う処理であり、（５）インストールの指示判定処理は、インストールフェーズ及びアクティベートフェーズで行う処理である。ここで、配信パッケージがＤＣＭ１２にダウンロードされ、図１０に示すように、書込み対象ＥＣＵ１９への書込みデータ（更新データ、差分データ）がアンパッケージングされた状態とする。

[0198] 図６１に示すように、ＣＧＷ１３は、インストールの指示判定部７７において、インストール条件判定部７７ａと、インストール指示部７７ｂと、車両状態情報取得部７７ｃと、アクティベート条件判定部７７ｄと、アクティベート指示部７７ｅとを有する。インストール条件判定部７７ａは、第１条件、第２条件、第３条件、第４条件、第５条件が成立しているか否かを判定する。第１条件は、インストールに関するユーザ承諾が得られている、という条件である。インストールに関するユーザ承諾とは、例えば図３９に示す画面において、インストールに対するユーザの承諾操作（例えば「すぐ更新」ボタン５０６ａを押下）を示す。又は、ダウンロードからアクティベートまでを一つの更新とみなし、更新に対するユーザの承諾操作としても良い。

[0199] 第２条件は、ＣＧＷ１３がセンター装置３とデータ通信可能である、という条件である。第３条件は、車両状態がインストール可能である、という条件である。第４条件は、書換え対象ＥＣＵ１９がインストール可能である、という条件である。ここで、第４条件は、インストール対象の書換え対象ＥＣＵ１９がインストール可能であることだけでなく、そのインストール対象の書換え対象ＥＣＵ１９と連携する書換え対象ＥＣＵ１９もインストール可能であることも含む。第５条件は、書込みデータが正常なデータである、という条件である。ここで、正常なデータとは、書換え対象ＥＣＵ１９に適したデータであること、改ざんされていないデータであること等を含む。

[0200] インストール指示部７７ｂは、第１条件、第２条件、第３条件、第４条件及び第５条件の全てが成立しているとインストール条件判定部７７ａにより

判定されると、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示する。即ち、インストール指示部７７ｂは、インストールに関するユーザ承諾が得られており、ＣＧＷ１３がセンター装置３とデータ通信可能であり、車両状態がインストール可能な状態であり、書換え対象ＥＣＵ１９がインストール可能な状態であり、書込みデータが正常なデータであるとインストール条件判定部７７ａにより判定されると、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示する。具体的には、インストール指示部７７ｂは、書込みデータをＤＣＭ１２から取得し、その取得した書込みデータを書換え対象ＥＣＵ１９に転送する。インストール指示部７７ｂは、第１条件、第２条件、第３条件、第４条件及び第５条件の少なくとも何れかが成立していないとインストール条件判定部７７ａにより判定されると、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示せず、待機又はインストールを開始することができない旨及びその理由をユーザに提示する。

[0201] 車両状態情報取得部７７ｃは、センター装置３から車両状態情報を取得する。アクティベート条件判定部７７ｄは、書換え対象ＥＣＵ１９の全てにおいてアプリプログラムのインストールが完了した場合に、第６条件、第７条件、第８条件が成立しているか否かを判定する。第６条件は、アクティベートに関するユーザ承諾が得られている、という条件である。アクティベートに関するユーザ承諾とは、例えば図４３に示す画面において、アクティベートに対するユーザの承諾操作（例えば「ＯＫ」ボタン５０８ｂを押下）を示す。又は、ダウンロードからアクティベートまでを一つの更新とみなし、更新に対するユーザの承諾操作としても良い。第７条件は、車両状態がアクティベート可能な状態である、という条件である。第８条件は、書換え対象ＥＣＵ１９がアクティベート可能な状態である、という条件である。

[0202] アクティベート指示部７７ｅは、第６条件、第７条件及び第８条件の全てが成立しているとアクティベート条件判定部７７ｄにより判定されると、アプリプログラムのアクティベートを書換え対象ＥＣＵ１９に指示する。具体的には、後述する（１２）アクティベート要求の指示処理において説明する

。即ち、アクティベート指示部７７ｅは、アクティベートに関するユーザ承諾が得られており、車両状態がアクティベート可能な状態であり、書換え対象ＥＣＵ１９がアクティベート可能な状態であるとアクティベート条件判定部７７ｄにより判定されると、アプリプログラムのアクティベートを書換え対象ＥＣＵ１９に指示する。アクティベートを行うことにより、書換え対象ＥＣＵ１９に書込まれた更新プログラムが有効化される。アクティベート指示部７７ｅは、第６条件、第７条件及び第８条件の少なくとも何れかが成立していないとアクティベート条件判定部７７ｄにより判定されると、アプリプログラムのアクティベートを書換え対象ＥＣＵ１９に指示せず、待機又はアクティベートを開始ことができない旨及びその理由をユーザに提示する。

[0203] 次に、ＣＧＷ１３におけるインストールの指示判定部７７の作用について図６２から図６４を参照して説明する。ＣＧＷ１３は、インストールの指示判定プログラムを実行し、インストールの指示判定処理を行う。

[0204] ＣＧＷ１３は、インストールの指示判定処理を開始すると、第１条件が成立しているか否かを判定し、インストールに関するユーザ承諾が得られているか否かを判定する（Ｓ５０１、インストール条件判定手順の一部に相当する）。ＣＧＷ１３は、インストールに関するユーザ承諾が得られていると判定すると（Ｓ５０１：ＹＥＳ）、第２条件が成立しているか否かを判定し、センター装置３とデータ通信可能であるか否かを判定する（Ｓ５０２、インストール条件判定手順の一部に相当する）。ＣＧＷ１３は、ＤＣＭ１２での通信電波状況に基づいて、センター装置３とデータ通信可能であるか否かを判定する。

[0205] ＣＧＷ１３は、センター装置３とデータ通信可能であると判定すると（Ｓ５０２：ＹＥＳ）、第３条件が成立しているか否かを判定し、車両状態がインストール可能であるか否かを判定する（Ｓ５０３、インストール条件判定手順の一部に相当する）。ＣＧＷ１３は、車両状態として、例えば車両バッテリ４０のバッテリ残量が所定容量以上であるか否か、書換え対象ＥＣＵ１９のメモリ構成が１面メモリの場合には車両が駐車状態（ＩＧオフ状態）で

あるか否か等を判定し、車両状態がインストール可能であるか否かを判定する。これら車両状態の条件は、受信した書換え諸元データ（図８参照）を参照する構成としても良い。ＣＧＷ１３は、例えば車両バッテリ４０のバッテリ残量が書換え諸元データで指定された所定容量以上であり、書換え諸元データで指定された車両状態（駐車状態のみ可、又は走行状態のみ可、又は駐車状態も走行状態も可）に合致する等の場合に、車両状態がインストール可能であると判定する。

[0206] ＣＧＷ１３は、車両状態がインストール可能であると判定すると（Ｓ５０３：ＹＥＳ）、第４条件が成立しているか否かを判定し、書換え対象ＥＣＵ１９がインストール可能であるか否かを判定する（Ｓ５０４、インストール条件判定手順の一部に相当する）。ＣＧＷ１３は、例えば書換え対象ＥＣＵ１９に故障コードが発生しておらず、書換え対象ＥＣＵ１９へのセキュリティアクセスに成功した等の場合に、書換え対象ＥＣＵ１９がインストール可能であると判定する。ここで、故障コードの発生有無は、書込みデータを書込む書換え対象ＥＣＵ１９に加え、その書換え対象ＥＣＵ１９と連携制御を行うＥＣＵ１９についても確認すると良い。即ち、ＣＧＷ１３は、書換え対象ＥＣＵ１９に対してだけでなく、その書換え対象ＥＣＵ１９と連携制御を行うＥＣＵ１９に対しても、故障コードが発生しているか否かを判定する。

[0207] ＣＧＷ１３は、書換え対象ＥＣＵ１９がインストール可能であると判定すると（Ｓ５０４：ＹＥＳ）、第５条件成立しているか否かを判定し、書込みデータが正常なデータであるか否かを判定する（Ｓ５０５、インストール条件判定手順の一部に相当する）。ＣＧＷ１３は、書換え対象ＥＣＵ１９の書込み面（非運用面）に合致する書込みデータであり、書込みデータに対する完全性の検証結果が正常である等の場合に、書込みデータが正常なデータであると判定する。ＣＧＷ１３は、書込みデータが正常なデータであると判定すると（Ｓ５０５：ＹＥＳ）、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示する（Ｓ５０６、インストール指示手順に相当する）、このようにＣＧＷ１３は、第１条件を満たしたことを条件として、第２条件

以降の判定を行う。又、ＣＧＷ１３は、最後に第５条件の判定を行う。ＣＧＷ１３は、第１条件から第５条件の全てが成立していると判定すると、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示する。

[0208] 一方、ＣＧＷ１３は、インストールに関するユーザ承諾が得られていないと判定すると（Ｓ５０１：ＮＯ）、センター装置３とデータ通信可能でないと判定すると（Ｓ５０２：ＮＯ）、車両状態がインストール可能でないと判定すると（Ｓ５０３：ＮＯ、書換え対象ＥＣＵ１９がインストール可能でないと判定すると（Ｓ５０４：ＮＯ）、書込みデータが正常なデータでないと判定すると（Ｓ５０５：ＮＯ）、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示しない。尚、上記した処理では、インストールに関するユーザ承諾が得られている条件を、他の条件よりも先に判定する構成を説明したが、他の条件よりも後に判定する構成でも良い。

[0209] ＣＧＷ１３は、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示すると、書込みデータを書換え対象ＥＣＵ１９に配信し（Ｓ５０７）、インストールを完了したか否かを判定する（Ｓ５０８）。ＣＧＷ１３は、インストールを完了したと判定すると（Ｓ５０８：ＹＥＳ）、第６条件が成立しているか否かを判定し、アクティベートに関するユーザ承諾が得られているか否かを判定する（Ｓ５０９）。ＣＧＷ１３は、アクティベートに関するユーザ承諾が得られていると判定すると（Ｓ５０９：ＹＥＳ）、第７条件が成立しているか否かを判定し、車両状態がアクティベート可能な状態であるか否かを判定する（Ｓ５１０）。

[0210] ＣＧＷ１３は、車両状態がアクティベート可能な状態であると判定すると（Ｓ５１０：ＹＥＳ）、第８条件が成立しているか否かを判定し、書換え対象ＥＣＵ１９がアクティベート可能な状態であるか否かを判定する（Ｓ５１１）。ＣＧＷ１３は、書換え対象ＥＣＵ１９がアクティベート可能な状態であると判定すると（Ｓ５１１：ＹＥＳ）、アクティベートを書換え対象ＥＣＵ１９に指示する（Ｓ５１２）、このようにＣＧＷ１３は、第６条件から第８条件の全てが成立していると判定すると、アクティベートを書換え対象Ｅ

ＣＵ１９に指示する。

[0211] 又、ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数の場合には、インストールを個別に指示しても良いし纏めて指示しても良い。書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）の場合、インストールを個別に指示する態様では、ＣＧＷ１３は、図６３に示すように、ＥＣＵ（ＩＤ１）についてインストール条件が成立するか否かを判定する。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）についてインストール条件が成立すると判定すると、インストールをＥＣＵ（ＩＤ１）に指示する。次いで、ＣＧＷ１３は、ＥＣＵ（ＩＤ２）についてインストール条件が成立するか否かを判定する。ここでは、ＣＧＷ１３は、インストール条件として、ＥＣＵ（ＩＤ２）について第４条件及び第５条件が成立するか否かを判定すれば良い。ＣＧＷ１３は、ＥＣＵ（ＩＤ２）についてインストール条件が成立すると判定すると、インストールをＥＣＵ（ＩＤ２）に指示する。

[0212] 書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）の場合、インストールを纏めて指示する態様では、ＣＧＷ１３は、図６４に示すように、ＥＣＵ（ＩＤ１）についてインストール条件が成立するか否かを判定する。即ち、ＣＧＷ１３は、第１条件から第３条件と、ＥＣＵ（ＩＤ１）についての第４条件及び第５条件を判定する。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）についてインストール条件が成立すると判定すると、ＥＣＵ（ＩＤ２）についてインストール条件が成立するか否かを判定する。即ち、ＣＧＷ１３は、ＥＣＵ（ＩＤ２）についての第４条件及び第５条件を判定する。ＣＧＷ１３は、ＥＣＵ（ＩＤ２）についてインストール条件が成立すると、インストールをＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）に指示する。ＣＧＷ１３は、例えばＥＣＵ（ＩＤ１）への書換えデータの転送と、ＥＣＵ（ＩＤ２）への書換えデータの転送とを同時に並行して行う。このようにＣＧＷ１３は、インストールを纏めて指示する態様では、第１条件から第３条件と、書換え対象ＥＣＵ全てについての第４条件及び第５条件を判定する。そして、ＣＧＷ１３は、これら全ての条件を満たした上で、インストールを指示する。

[0213] 以上に説明したように、ＣＧＷ１３は、インストールを書換え対象ＥＣＵ１９に指示する前に、インストール指示判定処理を行うことで、インストールに関するユーザ承諾が得られている第１条件、センター装置３とデータ通信可能である第２条件、車両状態がインストール可能な状態である第３条件、書換え対象ＥＣＵ１９がインストール可能な状態である第４条件、書込みデータが正常なデータである第５条件の全てが成立していると判定すると、アプリプログラムのインストールを書換え対象ＥＣＵ１９に指示するようにした。書換え対象ＥＣＵ１９に対してアプリプログラムのインストールを適切に指示することができる。

[0214] （６）セキュリティアクセス鍵の管理処理

セキュリティアクセス鍵の管理処理について図６５から図６９を参照して説明する。セキュリティアクセス鍵とは、ＣＧＷ１３が書込みデータのインストールを行う前に書換え対象ＥＣＵ１９にアクセスする際の機器認証を行うための鍵である。車両用プログラム書換えシステム１は、ＣＧＷ１３においてセキュリティアクセス鍵の管理処理を行う。ここでは、前述した（３）書込みデータの転送判定処理、又は（４）書込みデータの取得判定処理により、ＣＧＷ１３がＤＣＭ１２から書込みデータを取得可能な状態であることを前提として説明する。セキュリティアクセス鍵を用いた機器認証は、前述した（５）インストールの指示判定処理における第４条件（ステップＳ５０５）に相当する。

[0215] ＣＧＷ１３が書込みデータを書換え対象ＥＣＵ１９に配信する際には、ＣＧＷ１３が書換え対象ＥＣＵ１９との間でセキュリティアクセス鍵を用いてセキュリティアクセス（機器認証）を行う必要がある。この場合、ＣＧＷ１３において、乱数値の生成を書換え対象ＥＣＵ１９に要求し、書換え対象ＥＣＵ１９により生成された乱数値を書換え対象ＥＣＵ１９から取得し、その取得した乱数値を計算してセキュリティアクセス鍵を生成する手法が考えられる。しかしながら、このような手法では、アプリプログラムの書換えを行わないときでも書換え対象ＥＣＵ１９から乱数値を取得すれば、セキュリテ

ィアクセス鍵を保持可能となるので、セキュリティアクセス鍵の漏洩リスクが生じ得る。

[0216] 又、ＣＧＷ１３において、書換え対象ＥＣＵ１９から取得した乱数値をセンター装置３に送信し、センター装置３が乱数値を計算してセキュリティアクセス鍵を生成する構成とすれば、セキュリティアクセス鍵を保持しなくて済むので、セキュリティアクセス鍵の漏洩リスクを低減可能となる。しかしながら、センター装置３が乱数値を計算する構成では、書換え対象ＥＣＵ１９がセンター装置３から乱数値を取得するまでの待機時間が長くなり、ダイアグ通信の時間規定を満たすことが難しくなる。このような事情から、本実施形態では以下の構成を採用している。

[0217] 図６５に示すように、サプライヤは、書換え対象ＥＣＵ１９毎のセキュリティアクセス鍵を、セキュリティアクセス鍵の暗号・復号鍵を用いて暗号化して乱数値を生成する。ここでいう乱数値は、過去に使用した値と異なる値、過去に使用した値と同じ値の何れも含み、ランダムな値という意味である。乱数値は、暗号化されたセキュリティアクセス鍵である。サプライヤは、生成した乱数値をリプログデータと共に提供する。セキュリティアクセス鍵、セキュリティアクセス鍵の暗号・復号鍵、乱数値は、ＥＣＵ１９毎にユニークな鍵である。

[0218] ＯＥＭは、サプライヤからリプログデータと共に乱数値が提供されると、その提供された乱数値を、ＥＣＵ１９を識別するＥＣＵ（ＩＤ）と対応付け、図８に示したＣＧＷ用の書換え諸元データに格納する。又、ＯＥＭは、乱数値を復号化するために必要な鍵パターンや復号演算パターンについても、ＣＧＷ用の書換え諸元データに格納する。鍵パターンとしては、共通鍵／公開鍵等の方式や鍵長等を格納し、復号演算パターンとしては、復号演算に用いるアルゴリズムの種類等を格納する。ＯＥＭは、乱数値、鍵パターン及び復号演算パターンをＣＧＷ用の書換え諸元データに格納すると、その乱数値を格納したＣＧＷ用の書換え諸元データをリプログデータと共にセンター装置３に提供する。これらサプライヤから提供される情報は、後述するＥＣＵ

リプロデータＤＢ及びＥＣＵメタデータＤＢに保存される。

[0219] センター装置３は、ＯＥＭからリプログデータと共に書換え諸元データ（ＤＣＭ用の書換え諸元データ及びＣＧＷ用の書換え諸元データ）が提供されると、その提供された書換え諸元データとリプログデータとを含む配信パッケージをマスタ装置１１に送信する。マスタ装置１１において、ＤＣＭ１２は、センター装置３から配信パッケージをダウンロードすると、書換え諸元データと書込みデータをＣＧＷ１３に転送する。

[0220] 図６６に示すように、ＣＧＷ１３は、セキュリティアクセス鍵の管理部７８において、セキュア領域７８ａ（復号鍵記憶部に相当する）と、乱数値抽出部７８ｂ（鍵導出値抽出部に相当する）と、鍵パターン抽出部７８ｃと、復号演算パターン抽出部７８ｄと、鍵生成部７８ｅと、セキュリティアクセス実行部７８ｆと、セッション移行要求部７８ｇと、鍵消去部７８ｈとを有する。セキュア領域７８ａは、ＥＣＵ１９の外部から情報の読出しが不可であり、セキュリティアクセス鍵の暗号・復号鍵、復号演算アルゴリズムが配置されている。乱数値抽出部７８ｂは、ＣＧＷ用の書換え諸元データの解析結果から当該書換え諸元データに含まれている乱数値（鍵導出値）を抽出する。乱数値は、書換え対象ＥＣＵ１９のＥＣＵ（ＩＤ）に対応付けられて暗号化された値である。

[0221] 鍵パターン抽出部７８ｃは、ＣＧＷ用の書換え諸元データの解析結果から当該書換え諸元データに含まれている鍵パターンを抽出する。復号演算パターン抽出部７８ｄは、ＣＧＷ用の書換え諸元データの解析結果から当該書換え諸元データに含まれている復号演算パターンを抽出する。

[0222] 鍵生成部７８ｅは、乱数値が乱数値抽出部７８ｂにより抽出されると、セキュア領域７８ａを検索し、その抽出された乱数値を、セキュア領域７８ａに配置されているセキュリティアクセス鍵の復号鍵の束の中からＥＣＵ（ＩＤ）に対応する復号鍵を用いて復号化し、セキュリティアクセス鍵を生成する。この場合、鍵生成部７８ｅは、鍵導出値を、鍵パターン抽出部７８ｃにより抽出された鍵パターンにより特定される復号鍵を用い、復号演算パター

ン抽出部７８ｄにより抽出された復号演算パターンにより特定される復号演算方式にしたがって復号化する。即ち、複数の鍵パターン及び複数の復号演算パターンが用意されており、ＣＧＷ用の書換え諸元データにより鍵パターン及び復号演算パターンが指定されることで、鍵生成部７８ｅは、その鍵パターン及び復号演算パターンを用いてセキュリティアクセス鍵を生成する。

[0223] セキュリティアクセス実行部７８ｆは、セキュリティアクセス鍵が鍵生成部７８ｅにより生成されると、その生成されたセキュリティアクセス鍵を用いて書換え対象ＥＣＵ１９に対するセキュリティアクセスを実行する。具体的には、セキュリティアクセス実行部７８ｆは、例えばセキュリティアクセス鍵を用いてＥＣＵ（ＩＤ）を暗号化した暗号化データを送信し、書換え対象ＥＣＵ１９にアクセスを要求する。書換え対象ＥＣＵ１９は、暗号化データを受信すると、その受信した暗号化データを、自己が保持しているセキュリティアクセス鍵を用いて復号化する。そして、書換え対象ＥＣＵ１９は、復号化により生成した復号化データと自己のＥＣＵ（ＩＤ）とを比較し、両者が一致する場合には自己へのアクセスを許可し、両者が一致しない場合には自己へのアクセスを許可しない。

[0224] セッション移行要求部７８ｇは、書換えセッションへの移行を要求する。デフォルトセッションから書換えセッションへ移行した後に、セキュリティアクセス実行部７８ｆがセキュリティアクセスを実行する。尚、デフォルトセッション以外のセッション（例えば診断セッション）に移行した上でセキュリティアクセスを行い、その後、書換えセッションに移行しても良い。鍵消去部７８ｈは、書換え対象ＥＣＵ１９に対するセキュリティアクセスがセキュリティアクセス実行部７８ｆにより実行されて書換え対象ＥＣＵ１９のアプリプログラムの書換えが完了された後に、鍵生成部７８ｅにより生成されたセキュリティアクセス鍵を消去する。

[0225] 次に、ＣＧＷ１３におけるセキュリティアクセス鍵の管理部７８の作用について図６７から図６９を参照して説明する。ＣＧＷ１３は、セキュリティアクセス鍵の管理プログラムを実行し、セキュリティアクセス鍵の管理処理

を行う。ＣＧＷ１３は、セキュリティアクセス鍵の管理処理として、セキュリティアクセス鍵の生成処理、セキュリティアクセス鍵の消去処理を行う。以下、それぞれの処理について順次説明する。

[0226] （６－１）セキュリティアクセス鍵の生成処理

ＣＧＷ１３は、セキュリティアクセス鍵の生成処理を開始すると、ＤＣＭ１２から取得した書換え諸元データを解析し（Ｓ６０１、書換え諸元データ解析手順に相当する）、ＣＧW用の書換え諸元データから乱数値、鍵パターン、復号演算パターンを抽出する（Ｓ６０２、鍵導出値抽出手順に相当する）。

[0227] ＣＧＷ１３は、セキュア領域７８ａを検索し、ＣＧW用の書換え諸元データから抽出した乱数値を、セキュア領域７８ａに配置されているセキュリティアクセス鍵の復号鍵の束の中からＥＣＵ（ＩＤ）に対応する復号鍵を用いて復号化し、セキュリティアクセス鍵を生成する（Ｓ６０３、鍵生成手順に相当する）

[0228] ＣＧＷ１３は、図６８示すように、ＣＧW用の書換え諸元データからセキュリティアクセス鍵を生成する。ＣＧＷ１３は、書込みデータを書込み可能とする書換えセッションへのセッション移行要求を行い（Ｓ６０４）、セキュリティアクセス鍵を用い、書換え対象ＥＣＵ１９に対するセキュリティアクセスを実行する（Ｓ６０５）、ＣＧＷ１３は、セキュリティアクセスの実行を完了すると、書込みデータを書換え対象ＥＣＵ１９に配信し（Ｓ６０６）、セッション維持要求を行う（Ｓ６０７）。ＣＧＷ１３は、インストールを完了したと判定すると（Ｓ６０８：ＹＥＳ）、セキュリティアクセス鍵の生成処理を終了する。

[0229] （６－２）セキュリティアクセス鍵の消去処理

ＣＧＷ１３は、セキュリティアクセス鍵の消去処理を開始すると、書換え対象ＥＣＵ１９のアプリプログラムの書換えを完了したか否かを判定する（Ｓ６１１）。ＣＧＷ１３は、書換え対象ＥＣＵ１９のアプリプログラムの書換えを完了したと判定すると（Ｓ６１１：ＹＥＳ）、セキュリティアクセス

鍵の生成処理を実行して生成したセキュリティアクセス鍵を消去し（Ｓ６１２）、セキュリティアクセス鍵の消去処理を終了する。

[0230] 以上に説明したように、ＣＧＷ１３は、セキュリティアクセス鍵の管理処理を行うことで、書換え諸元データの解析結果から書換え対象ＥＣＵ１９に対応する乱数値を抽出し、その乱数値をセキュア領域７８ａに記憶されている書換え対象ＥＣＵ１９に対応する復号鍵を用いて復号化し、セキュリティアクセス鍵を生成するようにした。セキュリティアクセス鍵を外部から取得せず、セキュリティアクセス鍵をＣＧＷ１３において生成することで、セキュリティアクセス鍵の漏洩リスクを低減しつつ、書換え対象ＥＣＵ１９に対するセキュリティアクセスを適切に実行することができる。

[0231] 尚、ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数の場合には、それぞれの書込みデータのインストールを行う直前にセキュリティアクセス鍵の生成処理を行うことが望ましい。即ち、ＣＧＷ１３は、書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）の場合あれば、ＥＣＵ（ＩＤ１）のセキュリティアクセス鍵の生成処理、ＥＣＵ（ＩＤ１）への書込みデータのインストール、ＥＣＵ（ＩＤ２）のセキュリティアクセス鍵の生成処理、ＥＣＵ（ＩＤ２）への書込みデータのインストール、ＥＣＵ（ＩＤ３）のセキュリティアクセス鍵の生成処理、ＥＣＵ（ＩＤ３）への書込みデータのインストールの順序で行うことが望ましい。例えば図６３に示すように、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）に対するインストール条件が成立したか否かの一つとしてセキュリティアクセス処理を行い、正常にアクセスが許可された場合に、ＥＣＵ（ＩＤ１）に対してインストールを指示する。その後、ＣＧＷ１３は、ＥＣＵ（ＩＤ２）に対するインストール条件が成立したか否かの一つとしてセキュリティアクセス処理を行い、正常にアクセスが許可された場合に、ＥＣＵ（ＩＤ２）に対してインストールを指示する。

[0232] 又、書換え対象ＥＣＵ１９は、ＣＧＷ１３が自己へのセキュリティアクセスを行ったことで自己へのアクセスを許可すると、ＣＧＷ１３からセッション移行要求を受信することでセキュリティアクセスを解除し、書込みデータ

のフラッシュメモリに書込み可能な状態とする。セッション移行要求とは、例えば図１５５に示す第２状態の中の「書換えセッション移行要求」である。書換え対象ＥＣＵ１９は、自己へのアクセスを許可してから所定時間（例えば５秒）以内にＣＧＷ１３からセッション移行要求を受信しないと、タイムアウトになり、セキュリティアクセスをロックし、セッション移行要求の受信を受付けない。ＣＧＷ１３は、書換え対象ＥＣＵ１９へのアクセスの許可を特定してから所定時間以内にセッション移行要求を書換え対象ＥＣＵ１９に送信しない場合には、セッション維持要求を書換え対象ＥＣＵ１９に送信し、書換え対象ＥＣＵ１９がタイムアウトしないように保持し、セッション移行要求を書換え対象ＥＣＵ１９に送信する必要がある。

[0233] 又、例えば書換えの途中でキャンセル操作されたことで運用面にバージョン１．０のアプリプログラムが書込まれ、非運用面にバージョン２．０のアプリプログラムが書込まれており、その状態からバージョン２．０へのキャンペーン通知が発生すると、インストールを行わずにアクティベートだけを行えば良いので、セキュリティアクセス処理を省略しても良い。

[0234] （７）書込みデータの検証処理

書込みデータの検証処理について図７０から図７８を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において書込みデータの検証処理を行う。ＣＧＷ１３は、本実施形態で説明する書込みデータの検証処理を、前述した（６）セキュリティアクセス鍵の管理処理におけるアクセス許可を取得する前に行っても良いし、アクセス許可を取得した後に行っても良い。

[0235] 図７０に示すように、サプライヤやＯＥＭは、書込みデータを生成すると、その生成した書込みデータに対してデータ検証値算出アルゴリズムを適用してデータ検証値を生成する。ここで、書込みデータは、更新する新プログラムであっても良いし、旧プログラムから新プログラムへの差分データであっても良い。サプライヤやＯＥＭは、そのデータ検証値に対して所定の鍵（キー値）を用いた暗号化を適用して認証子を生成し、書込みデータと認証子

とを対応付けてセンター装置３に登録する。具体的には、後述するリプロデータＤＢにＥＣＵ１９毎にこれらのデータを記憶する。そして、センター装置３は、書込みデータと認証子とを含む配信パッケージを生成し、パッケージＤＢに記憶する。

[0236] センター装置３は、マスタ装置１１からの配信パッケージのダウンロード要求が発生すると、そのダウンロード要求にしたがって書込みデータと認証子とを含む配信パッケージをマスタ装置１１に送信する。この場合、センター装置３からマスタ装置１１に送信される書込みデータは暗文であり、センター装置３からマスタ装置１１に送信される認証子も暗文である。尚、センター装置３からマスタ装置１１に送信される認証子は平文であっても良い。センター装置３からマスタ装置１１に送信される認証子が平文である場合には、後述する復号処理は不要である。

[0237] マスタ装置１１は、センター装置３から配信パッケージをダウンロードすると、そのダウンロードした配信パッケージから書換え対象ＥＣＵ１９の書込みデータを抽出し、その書込みデータを書換え対象ＥＣＵ１９に配信する前に、その書込みデータの妥当性を検証する。即ち、マスタ装置１１は、復号処理、第１検証値算出処理、第２検証値算出処理、比較処理、判定処理を順次実行し、書込みデータを検証する。復号処理は、暗文で送信された認証子を復号する処理である。第１検証値算出処理は、復号した認証子から鍵（キー値）を用いて期待値である第１データ検証値を算出する処理である。第２検証値算出処理は、データ検証値算出アルゴリズムを用いて書込みデータから第２データ検証値を算出する処理である。比較処理は、第１データ検証値と第２データ検証値とを比較する処理である。判定処理は、比較処理の比較結果から書込みデータの妥当性を判定する処理である。

[0238] 図７１に示すように、ＣＧＷ１３は、書込みデータの検証部７９において、書込み可能判定部７９ａと、処理実行要求部７９ｂと、処理結果取得部７９ｃと、検証部７９ｄとを有する。書込み可能判定部７９ａは、書換え対象ＥＣＵ１９において書込みデータの書込みが可能であるか否かを判定する。

処理実行要求部７９ｂは、書換え対象ＥＣＵ１９において書込みデータの書込みが可能であると書込み可能判定部６９ａにより判定されると、処理実行要求をＤＣＭ１２に通知し、ＤＣＭ１２に対して処理の実行を要求する。処理実行要求部６８ｂは、復号処理、第１検証値算出処理、第２検証値算出処理、比較処理、判定処理のうち少なくとも何れかの処理実行要求をＤＣＭ１２に通知する。処理結果取得部６８ｃは、ＤＣＭ１２から処理結果が通知されることで、ＤＣＭ１２から処理結果を取得する。検証部７９ｄは、処理結果が処理結果取得部６８ｃにより取得されると、その処理結果を用いて書込みデータを検証する。即ち、上記した構成では、ＣＧＷ１３は第１装置及び第１機能部に相当し、ＤＣＭ１２は第２装置及び第２機能部に相当する。

[0239] 次に、ＣＧＷ１３における書込みデータの検証部７９の作用について図７２から図７７を参照して説明する。ＣＧＷ１３は、書込みデータの検証プログラムを実行し、書込みデータの検証処理を行う。

[0240] ＣＧＷ１３は、書込みデータの検証処理を開始すると、処理実行要求をＤＣＭ１２に通知し、ＤＣＭ１２に対して処理の実行を要求する（Ｓ７０１、処理実行要求手順に相当する）。ＣＧＷ１３は、上記した復号処理、第１検証値算出処理、第２検証値算出処理、比較処理、判定処理のうち少なくとも何れかの処理実行要求をＤＣＭ１２に通知する。ＣＧＷ１３は、ＤＣＭ１２から処理結果を取得すると（Ｓ７０２、処理結果取得手順に相当する）、その取得した処理結果を用いて書込みデータを検証する（Ｓ７０３、検証手順に相当する）。

[0241] 以下、ＣＧＷ１３が処理実行要求をＤＣＭ１２に通知する幾つかの場合を例示する。図７３の例示では、ＣＧＷ１３は、復号処理、第１検証値算出処理、第２検証値算出処理の処理実行要求をＤＣＭ１２に通知する。ＤＣＭ１２は、ＣＧＷ１３から復号処理、第１検証値算出処理、第２検証値算出処理の処理実行要求が通知されると、復号処理、第１検証値算出処理、第２検証値算出処理を順次実行する。ＤＣＭ１２は、処理結果通知処理を実行し、第１検証値算出処理により算出した第１データ検証値、第２検証値算出処理に

より算出した第２データ検証値を処理結果としてＣＧＷ１３に通知する。ＣＧＷ１３は、処理結果取得処理を実行し、ＤＣＭ１２から第１データ検証値、第２データ検証値を取得すると、その第１データ検証値、第２データ検証値を用い、比較処理、判定処理を順次実行する。ＣＧＷ１３は、判定処理の判定結果の正否により書込みデータを検証する。本例示では、第１データ検証値を算出するための鍵をＤＣＭ１２が保持している。

[0242] 図７４の例示では、ＣＧＷ１３は、復号処理、第２検証値算出処理の処理実行要求をＤＣＭ１２に通知する。ＤＣＭ１２は、ＣＧＷ１３から復号処理、第２検証値算出処理の処理実行要求が通知されると、復号処理、第２検証値算出処理を順次実行し、第２検証値算出処理により算出した第２データ検証値をＣＧＷ１３に通知する。ＣＧＷ１３は、処理結果取得処理を実行し、ＤＣＭ１２から第２データ検証値を取得すると、第１検証値算出処理を実行し、第１検証値算出処理により算出した第１データ検証値、その第２データ検証値を用い、比較処理、判定処理を順次実行する。ＣＧＷ１３は、判定処理の判定結果の正否により書込みデータを検証する。本例示では、第１データ検証値を算出するための鍵をＣＧＷ１３が保持している。

[0243] 図７５の例示では、ＣＧＷ１３は、復号処理、第１検証値算出処理、第２検証値算出処理、比較処理の処理実行要求をＤＣＭ１２に通知する。ＤＣＭ１２は、ＣＧＷ１３から復号処理、第１検証値算出処理、第２検証値算出処理、比較処理の処理実行要求が通知されると、復号処理、第１検証値算出処理、第２検証値算出処理、比較処理を順次実行する。ＤＣＭ１２は、処理結果通知処理を実行し、比較処理の比較結果を処理結果としてＣＧＷ１３に通知する。ＣＧＷ１３は、処理結果取得処理を実行し、ＤＣＭ１２から比較結果を取得すると、その比較結果を用い、判定処理を実行する。ＣＧＷ１３は、判定処理の判定結果の正否により書込みデータを検証する。本例示では、第１データ検証値を算出するための鍵をＤＣＭ１２が保持している。

[0244] 図７６の例示では、ＣＧＷ１３は、復号処理、第１検証値算出処理、第２検証値算出処理、比較処理、判定処理の処理実行要求をＤＣＭ１２に通知す

る。ＤＣＭ１２は、ＣＧＷ１３から復号処理、第１検証値算出処理、第２検証値算出処理、比較処理、判定処理の処理実行要求が通知されると、復号処理、第１検証値算出処理、第２検証値算出処理、比較処理、判定処理を順次実行する。ＤＣＭ１２は、処理結果通知処理を実行し、判定処理の判定結果を処理結果としてＣＧＷ１３に通知する。ＣＧＷ１３は、処理結果取得処理を実行し、ＤＣＭ１２から処理結果を取得すると、その処理結果により示される判定結果の正否により書込みデータを検証する。本例示では、第１データ検証値を算出するための鍵をＤＣＭ１２が保持している。

[0245] ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数の場合には、複数の書換え対象ＥＣＵ１９に対する書込みデータの検証処理を、以下のようにして行う。ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数の場合には、書込みデータを複数の書換え対象ＥＣＵ１９に対して纏めて検証する手法と、個別に検証する手法とがある。

[0246] ＣＧＷ１３は、書込みデータを複数の書換え対象ＥＣＵ１９に対して纏めて検証する手法では、図７７に示すように、例えばＥＣＵ（ＩＤ１）の書込みデータ、ＥＣＵ（ＩＤ２）の書込みデータ、ＥＣＵ（ＩＤ３）の書込みデータを纏めて検証し、ＥＣＵ（ＩＤ１）の書込みデータの書込え対象ＥＣＵ（ＩＤ１）に配信し、ＥＣＵ（ＩＤ２）の書込みデータの書込え対象ＥＣＵ（ＩＤ２）に配信し、ＥＣＵ（ＩＤ３）の書込みデータの書込え対象ＥＣＵ（ＩＤ３）に配信する。この場合、複数の書換え対象ＥＣＵ１９に対する書込みデータの検証を纏めることで、複数の書換え対象ＥＣＵ１９に対する書込みデータの検証の開始からプログラムの書換えの完了までに要する時間を短縮することができる。即ち、書込みデータを複数の書換え対象ＥＣＵ１９に対して個別に検証する構成よりも、複数の書換え対象ＥＣＵ１９に対する書込みデータの検証の開始からプログラムの書換えの完了までに要する時間を短縮することができる。

[0247] ＣＧＷ１３は、書込みデータを複数の書換え対象ＥＣＵ１９に対して個別に検証する手法では、図７８に示すように、例えばＥＣＵ（ＩＤ１）の書込

みデータを検証し、ＥＣＵ（ＩＤ１）の書込みデータの書込え対象ＥＣＵ（ＩＤ１）に配信し、ＥＣＵ（ＩＤ２）の書込みデータを検証し、ＥＣＵ（ＩＤ２）の書込みデータの書込え対象ＥＣＵ（ＩＤ２）に配信し、ＥＣＵ（ＩＤ３）の書込みデータを検証し、ＥＣＵ（ＩＤ３）の書込みデータの書込え対象ＥＣＵ（ＩＤ２）に配信する。この場合、書込みデータを配信する直前に書込みデータを検証することで、不正なアクセスを回避することができ、信頼性を高めることができる。即ち、書込みデータを複数の書換え対象ＥＣＵ１９に対して纏めて検証する構成では、書換え順序により検証を完了してから書込みデータを配信するまでの時間が書換え順序により異なり、検証を完了してから書込みデータを配信するまでの時間が長くなると、その間に不正なアクセスによる改ざんの危険性が発生することが懸念されるが、書込みデータを配信する直前に書込みデータを検証することで、そのような事態を回避することができる。

[0248] 以上に説明したように、ＣＧＷ１３は、書込みデータの検証処理を行うことで、書込みデータの検証に関与する処理のうち少なくとも一部を、センター装置３から配信パッケージをダウンロードするＤＣＭ１２に実行させるようにした。ＣＧＷ１３や書換え対象ＥＣＵ１９において、書込みデータを記憶するための領域が確保不能であったり、検証用の演算プログラムを搭載不能であったりしても、書込みデータを書換え対象ＥＣＵ１９にて書込む前に、書込みデータの検証を適切に行うことができる。

[0249] 図７４に例示したＣＧＷ１３が第１検証値算出処理を行う構成では、ＣＧＷ１３が鍵（キー値）を保持し、その鍵をＤＣＭ１２に送信することなく検証処理を行うので、ＤＣＭ１２が第１検証値算出処理を行う構成に比べ、セキュリティ性を高めることができる。又、書換え対象ＥＣＵ１９が複数の場合には、複数の書換え対象ＥＣＵ１９で共通する共通鍵（キー値）を用いて第１検証値算出処理を行っても良いし、複数の書換え対象ＥＣＵ１９で異なる個別鍵（キー値）を用いて第１検証値算出処理を行っても良い。

[0250] 尚、以上は、ＣＧＷ１３が処理実行要求をＤＣＭ１２に通知する構成を例

示したが、例えばＤＣＭ１２において処理負荷が増大して本来の処理に支障が発生するような場合には、ＤＣＭ１２に代えてナビゲーション装置や書換え対象ＥＣＵ１９以外のＥＣＵを用い、処理実行要求をナビゲーション装置や書換え対象ＥＣＵ１９以外のＥＣＵに通知しても良い。又、ＤＣＭ１２とＣＧＷ１３とが一体型の場合において、本来の処理に支障が発生せずに対応可能な場合は、処理実行要求を自身の処理実行部に要求しても良い。例えば同一ＥＣＵ内で異なるソフトコンポーネント間で行っても良い。又、ＤＣＭ１２及びＣＧＷ１３の機能を有する１つの統合ＥＣＵとして構成されるマスタ装置１１に対し、上述の構成を適用しても良い。例えば図７３から図７６において、ＣＧＷ１３における処理機能を第１機能部、ＤＣＭ１２における処理機能を第２機能部とし、第１機能部から第２機能部へ処理実行要求を通知し、第２機能部から第１機能部へ実行結果を返す。統合ＥＣＵとして構成されるマスタ装置１１において、処理負荷が増大して通信処理や中継処理に支障が発生するような場合には、第２機能部に代えて、ナビゲーション装置や書換え対象ＥＣＵ１９以外のＥＣＵに処理実行要求を通知しても良い。

[0251] 又、データ検証値は、アプリプログラム全体で１つの値を算出しても良いし、アプリプログラムのブロック単位で複数の値を算出しても良い。書込みデータが全データであれば、書込みデータの完了後に完全性検証で使うことができる。

[0252] 尚、セキュリティアクセスがＣＧＷ１３と書換え対象ＥＣＵ１９とが接続しても良いか否かを検証する手法であるのに対し、書込みデータの検証は、書込みデータの配信先であるセンター装置３が正規であること（ＴＬＳ通信による接続、相互認証）、センター装置３から書込みデータをダウンロードする通信路が正規であること（通信路の秘匿化、暗号化）、センター装置３からダウンロードした書込みデータが改ざんされていないこと（改ざん検知）、センター装置３からダウンロードした書込みデータが改ざん不能であること（暗号化）、という概念を含む。

[0253] 又、新プログラムの書換え時の書込みデータについて説明したが、旧プロ

グラムへ書き戻す際のロールバック時の書込みデータについても同様である。その場合、ＣＧＷ１３は、ロールバック時の書込みデータをセンター装置３からダウンロードした時点で検証しても良いが、書込みのキャンセル要求が発生したことでロールバック用の書込みデータを書換え対象ＥＣＵ１９に配信する直前に検証すると良い。

[0254] （８）データ格納面情報の送信制御処理

データ格納面情報の送信制御処理について図７９から図８１を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３においてデータ格納面情報の送信制御処理を行う。

[0255] 図７９に示すように、ＣＧＷ１３は、データ格納面情報の送信制御部８０において、データ格納面情報取得部８０ａと、データ格納面情報送信部８０ｂと、書換え方法特定部８０ｃと、書換え方法指示部８０ｄとを有する。データ格納面情報取得部８０ａは、ＥＣＵ構成情報として、各ＥＣＵ１９からハードウェア及びソフトウェアに関する情報を取得する。詳細には、データ格納面を複数面で持つ２面メモリＥＣＵ及び１面サスペンドメモリＥＣＵの場合、データ格納面それぞれのバージョン情報を含むソフトウェアＩＤ及び運用面を特定可能な情報を２面書換え情報（以下、面情報という）として取得する。

[0256] データ格納面情報送信部８０ｂは、面情報を含むＥＣＵ構成情報がデータ格納面情報取得部８０ａにより取得されると、その取得された面情報をＥＣＵ構成情報の一つとしてＤＣＭ１２からセンター装置３に送信させる。データ格納面情報送信部８０ｂは、ＩＧスイッチ４２のオンオフが切替わる度にＥＣＵ構成情報をセンター装置３に送信させても良いし、センター装置３からの要求に応じてＥＣＵ構成情報をセンター装置３に送信させても良い。又、データ格納面情報送信部８０ｂは、２面メモリＥＣＵ及び１面サスペンドメモリＥＣＵだけでなく、１面単独メモリＥＣＵについても面情報を含むＥＣＵ構成を合わせて送信しても良い。

[0257] 書換え方法特定部８０ｃは、ＣＧＷ１３用の書換え諸元データの解析結果

から書換え方法を特定する。書換え方法は、書換え対象ＥＣＵ１９におけるインストール時の電源切替え方法を示す。書換え方法指示部８０ｄは、書換え方法が書換え方法特定部８０ｃにより特定されると、その特定された書換え方法によるアプリプログラムの書換えを書換え対象ＥＣＵ１９に指示する。即ち、書換え方法指示部８０ｄは、電源自己保持による書換え方法が書換え方法特定部８０ｃにより特定されると、電源自己保持によるアプリプログラムの書換えを書換え対象ＥＣＵ１９に指示する。書換え方法指示部８０ｄは、電源制御による書換え方法が書換え方法特定部８０ｃにより特定されると、電源自己保持を用いずに電源制御によるアプリプログラムの書換えを書換え対象ＥＣＵ１９に指示する。

[0258] 次に、ＣＧＷ１３におけるデータ格納面情報の送信制御部８０の作用について図８０及び図８１を参照して説明する。ＣＧＷ１３は、データ格納面情報の送信制御プログラムを実行し、データ格納面情報の送信制御処理を行う。

[0259] ＣＧＷ１３は、データ格納面情報の送信制御処理を開始すると、面情報を含むＥＣＵ構成情報要求を全ＥＣＵ１９に送信し（Ｓ８０１）、全ＥＣＵ１９から面情報を含むＥＣＵ構成情報を取得する（Ｓ８０２、データ格納面情報取得手順に相当する）。ＣＧＷ１３は、各書換え対象ＥＣＵ１９からＥＣＵ構成情報を取得すると、その取得したＥＣＵ構成情報をＤＣＭ１２に送信し（Ｓ８０３、データ格納面情報送信手順に相当する）、ＤＣＭ１２からの書込みデータと書換え諸元データの取得を待機する（Ｓ８０４）。ここで、ＣＧＷ１３は、書換え対象ＥＣＵ１９が予め特定している場合は、その特定している書換え対象ＥＣＵ１９だけから面情報等を取得しても良い。

[0260] ＤＣＭ１２は、ＣＧＷ１３からＥＣＵ構成情報を受信すると、その受信したＥＣＵ構成情報を一時的に蓄積し、ＥＣＵ構成情報をセンター装置３に送信する（アップロードする）タイミングになると、そのＥＣＵ構成情報をセンター装置３に送信する。センター装置３は、ＤＣＭ１２からＥＣＵ構成情報を受信すると、その受信したＥＣＵ構成情報を保存し、解析する。

[0261] センター装置３は、面情報の送信元である各ＥＣＵ１９の各面のアプリプログラムのバージョン及び何れの面が運用面であるかを特定し、その特定した２面分のアプリプログラムのバージョン及び運用面に適合する書込みデータを特定する（更新データ選定手順に相当する）。センター装置３は、例えばＡ面が運用面であり、その運用面に格納されているアプリプログラムがバージョン２．０であり、Ｂ面が非運用面であり、その非運用面に格納されているアプリプログラムがバージョン１．０である場合には、書込みデータとしてＢ面用のバージョン３．０の書込みデータを特定する。センター装置３は、書込みデータが差分データである場合には、バージョン１．０からバージョン３．０に更新する差分データを特定する。センター装置３は、書込みデータを特定すると、その特定した書込みデータと書換え諸元データを含む配信パッケージをＤＣＭ１２に送信する（配信パッケージ送信手順に相当する）。

[0262] センター装置３は、ＤＣＭ１２に送信する配信パッケージを静的に選択しても良いし、動的に生成しても良い。センター装置３は、ＤＣＭ１２に送信する配信パッケージを静的に選択する場合には、書込みデータが格納されている配信パッケージを複数管理しており、非運用面に適合する書込みデータを選定し、その選定した書込みデータが格納されている配信パッケージを複数の配信パッケージの中から選択してＤＣＭ１２に送信する。センター装置３は、ＤＣＭ１２に送信する配信パッケージを動的に生成する場合には、非運用面に適合する書込みデータを特定すると、その特定した書込みデータを格納した配信パッケージを生成してＤＣＭ１２に送信する。

[0263] ＤＣＭ１２は、センター装置３から配信パッケージをダウンロードすると、そのダウンロードした配信パッケージから書込みデータと書換え諸元データを抽出し、その抽出した書込みデータと書換え諸元データをＣＧＷ１３に転送する。

[0264] ＣＧＷ１３は、ＤＣＭ１２から書込みデータと書換え諸元データを取得したと判定すると（Ｓ８０４：ＹＥＳ）、その取得した書換え諸元データを解

析し（Ｓ８０５）、その書換え諸元データの解析結果から書換え対象ＥＣＵ１９に対する書換え方法を判定する（Ｓ８０６，Ｓ８０７）。

[0265] ＣＧＷ１３は、書換え方法が電源自己保持による書換えであると判定すると（Ｓ８０６：ＹＥＳ）、インストール可能な車両状態であることを条件として書込みデータ取得要求をＤＣＭ１２に送信し、ＤＣＭ１２から書込みデータを取得し、その取得した書込みデータを書換え対象ＥＣＵ１９に配信し、アプリプログラムを電源自己保持により書換え（Ｓ８０８）、データ格納面情報の送信制御処理を終了する。アプリプログラムを電源自己保持により書換える方法については、前述した図２８及び図２９を用いて（イ）電源自己保持によりアプリプログラムを書換える場合において説明した通りである。

[0266] ＣＧＷ１３は、書換え方法が電源制御による書換えであると判定すると（Ｓ８０７：ＹＥＳ）、駐車中であることを条件として書込みデータ取得要求をＤＣＭ１２に送信し、ＤＣＭ１２から書込みデータを取得し、その取得した書込みデータを書換え対象ＥＣＵ１９に配信し、アプリプログラムを電源制御により書換え（Ｓ８０９）、データ格納面情報の送信制御処理を終了する。アプリプログラムを電源制御により書換える方法については、前述した図２６及び図２７を用いて（ア）電源制御によりアプリプログラムを書換える場合において説明した通りである。

[0267] 以上に説明したように、ＣＧＷ１３は、データ格納面情報の送信制御処理を行うことで、面情報を含むＥＣＵ構成情報をセンター装置３に通知し、ＥＣＵ構成情報に適合する書込みデータを含む配信パッケージをセンター装置３からＤＣＭ１２にダウンロードさせる。ＣＧＷ１３は、その面情報に適合する書込みデータをＤＣＭ１２から取得し、その書込みデータを書換え対象ＥＣＵ１９に配信する。データ格納面を２面で持つフラッシュメモリが搭載されているＥＣＵ１９を書換え対象とする場合に、アプリプログラムを適切に書換えることができる。

[0268] 尚、センター装置３が配信パッケージを配信する態様としては、以下に示

す第１配信態様から第３配信態様がある。第１配信態様では、センター装置３は、例えばＡ面用のバージョン２．０の書込みデータとＢ面用のバージョン２．０の書込みデータを格納した１つの配信パッケージを配信する。ＤＣＭ１２は、センター装置３からダウンロードした配信パッケージからＡ面用のバージョン２．０の書込みデータとＢ面用のバージョン２．０の書込みデータを抽出し、その抽出した書込みデータをＣＧＷ１３に転送する。ＣＧＷ１３は、ＤＣＭ１２からＡ面用のバージョン２．０の書込みデータとＢ面用のバージョン２．０の書込みデータが転送されると、そのうち何れかを選択して書換え対象ＥＣＵ１９に配信する。即ち、各データ格納面に対応する書込みデータが配信パッケージに含まれており、マスタ装置１１において書換え対象ＥＣＵ１９に適した書換えデータを選択する構成である。

[0269] 第２配信形態では、センター装置３は、例えばＡ面用のバージョン２．０の書込みデータを格納した配信パッケージ又はＢ面用のバージョン２．０の書込みデータを格納した配信パッケージのうち何れかを選択して配信する。ＤＣＭ１２は、センター装置３からダウンロードした配信パッケージから書込みデータを抽出し、その抽出した書込みデータをＣＧＷ１３に転送する。ＣＧＷ１３は、ＤＣＭ１２から転送された書込みデータを書換え対象ＥＣＵ１９に配信する。即ち、ＤＣＭ１２からアップロードされた面情報に基づいて、センター装置３が、非運用面用の書込みデータを含む配信パッケージを選択する構成である。

[0270] 第３配信態様では、センター装置３は、例えばＡ面用及びＢ面用で共有のバージョン２．０の書込みデータを格納した配信パッケージを配信する。ＤＣＭ１２は、センター装置３からダウンロードした配信パッケージからＡ面用及びＢ面用で共有のバージョン２．０の書込みデータを抽出し、その抽出した書込みデータをＣＧＷ１３に転送する。ＣＧＷ１３は、ＤＣＭ１２から転送されたＡ面用及びＢ面用で共有のバージョン２．０の書込みデータを書換え対象ＥＣＵ１９に配信する。書換え対象ＥＣＵ１９は、ＣＧＷ１３からＡ面用及びＢ面用で共有のバージョン２．０の書込みデータを受信すると、

その受信した書込みデータをＡ面又はＢ面の何れかに書込む。この場合、書換え対象ＥＣＵ１９において、アプリプログラムを実行する際に、マイコンのアドレス解決機能が働くことで、書込みデータをＡ面又はＢ面の何れに書込んでも適切に動作する。即ち、書込み対象ＥＣＵ１９のマイコンが面の違いに伴う実行アドレスの相違を解決することにより、センター装置３及びマスタ装置１１は、面を意識することなく動作することができる。

[0271] ＣＧＷ１３からＤＣＭ１２を介してセンター装置３に送信される面情報を含むＥＣＵ構成情報は、２面分のアプリプログラムのバージョン及び運用面を特定可能な情報に加え、車両特定情報、システム特定情報、ＥＣＵ特定情報、利用環境情報等が含まれていても良い。

[0272] 車両特定情報は、配信パッケージの配信先の車両を特定するためのユニークな情報であり、例えばＶＩＮ（Vehicle Identification Number）である。ＯＢＤ（On-board diagnostics）法規に該当する車両では、ＯＢＤ法規の規定によりＶＩＮを利用可能であるが、例えばＥＶ車両のようにＯＢＤ法規に該当しない車両であれば、ＶＩＮを利用可能でないので、ＶＩＮに代わる個車識別情報を採用すれば良い。

[0273] システム特定情報は、どのようなリプログシステムであるかを特定するためのユニークな情報である。ＣＧＷ１３は、自己が管理するダイアグ通信を利用した有線書換えを可能なシステムに対して無線書換え可能であるが、それ以外の独自方式のシステムに対して無線書換え不能である。即ち、有線を介して取得したプログラム更新の仕組みを利用し、無線を介して取得したプログラム更新を行うシステムだからである。そのため、センター装置３において、何れのシステムに何れの配信パッケージを配信すれば良いかを判定する必要があり、システム特定情報を使うことで車両にどのようなシステムが搭載されているかを管理することが可能である。センター装置３は、システム特定情報を判定することで、システム毎の書換え方式、複数のシステムを書換え対象とする場合の書換え順序等を判定可能となる。

[0274] ＥＣＵ特定情報は、書換え対象ＥＣＵ１９を特定するためのユニークな情

報であり、書換えＥＣＵと、当該書換え対象ＥＣＵ１９に書込まれているアプリプログラムとを一意に特定するためのソフトウェアバージョンと、ハードウェアバージョンとを含む情報である。ＥＣＵ特定情報は、ＥＣＵ品番にも相当する。最新のソフトウェアを全データで書込む場合には、ハードウェアバージョンだけでも良い。又、仕様バージョン、コンフィグレーションバージョン等のアプリプログラムが特定可能な情報を定義することも可能であり、更に、マイコンＩＤ、サブマイコンＩＤ、フラッシュＩＤ、ソフトウェア子バージョン、ソフトウェア孫バージョン等を定義することも可能である。

[0275] 利用環境情報は、ユーザが車両を利用する環境を特定するためのユニークな情報である。利用環境情報がＣＧＷ１３からＤＣＭ１２を介してセンター装置３に送信されることで、センター装置３は、ユーザが車両を利用する環境に適したアプリプログラムを配信することが可能となる。例えば停止時からの急加速運転を好むユーザには、加速に特化したアプリプログラムを配信し、エコ運転を好むユーザには、加速性能では劣るがエコ運転に特化したアプリプログラムを配信する等、ユーザが車両を利用する環境に適したアプリプログラムを配信することが可能となる。

[0276] 又、以上は、書換え対象ＥＣＵ１９のマイコンにフラッシュメモリが搭載されている場合について説明したが、書換え対象ＥＣＵ１９のマイコンに外付けメモリが接続されている場合は、外付けメモリを２面メモリと同等として処理を行い、外付けメモリの書込み領域を２つに区分して書込みデータを書込む。書換え対象ＥＣＵ１９のマイコンにフラッシュメモリが搭載されており、且つ外付けメモリが接続されている場合は、外付けメモリに格納されているプログラムをマイコンのメモリに一旦複製する（コピーする）処理を行う場合もある。外付けメモリは一般的にＥＣＵの動作ログの記憶領域として用いられることもあるので、外付けメモリへの書込みデータの書込みを開始した場合には、動作ログの記憶を中断し、外付けメモリへの書込みデータの書込みを完了した場合に、動作ログの記憶を再開することが望ましい。

[0277] アプリプログラムを書換える場合に限らず、例えば地図データ等の逐一更新される性質を有するデータについても、２面及びバージョンという概念があるので、地図データを書換える場合についても同様である。

[0278] （９）非書換え対象の電源管理処理

非書換え対象ＥＣＵ１９の電源管理処理について図８２から図８７を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において非書換え対象ＥＣＵ１９の電源管理処理を行う。本実施形態では、ＤＣＭ１２により配信パッケージのダウンロードが完了し、ＣＧＷ１３が書換え諸元データを取得し、車両が駐車状態においてＣＧＷ１３が書込みデータを書換え対象ＥＣＵ１９に配信する状況とする。ＣＧＷ１３は、書込みデータを書換え対象ＥＣＵ１９に配信する場合に、ＩＧ電源オンを電源管理ＥＣＵ２０に要求し、全てのＥＣＵ１９を起動状態とする。

[0279] 図８２に示すように、ＣＧＷ１３は、非書換え対象ＥＣＵ１９の電源管理部８１において、書換え対象特定部８１ａと、インストール可能判定部８１ｂと、状態移行制御部８１ｃと、書換え順序特定部８１ｄとを備える。書換え対象特定部８１ａは、書換え諸元データの解析結果から書換え対象ＥＣＵ１９及び非書換え対象ＥＣＵ１９を特定する。インストール可能判定部８１ｂは、書換え対象ＥＣＵ１９に対してインストール可能であるか否かを判定する。

[0280] 状態移行制御部８１ｃは、ＥＣＵ１９の状態を移行可能であり、停止状態又はスリープ状態のＥＣＵ１９を起動状態（ウェイクアップ状態）に移行させたり、起動状態のＥＣＵ１９を停止状態又はスリープ状態に移行させたりする。又、状態移行制御部８１ｃは、通常動作状態のＥＣＵ１９を省電力動作状態に移行させたり、省電力動作状態のＥＣＵ１９を通常動作状態に移行させたりする。状態移行制御部８１ｃは、インストールが可能であるとインストール可能判定部８１ｂにより判定されると、少なくとも一つ以上の非書換え対象ＥＣＵ１９を停止状態、スリープ状態又は省電力動作状態とするように制御する。書換え順序特定部８１ｄは、書換え諸元データの解析結果か

ら書換え対象ＥＣＵ１９の書換え順序を特定する。

[0281] 次に、ＣＧＷ１３における非書換え対象ＥＣＵ１９の電源管理部８１の作用について図８３から図８７を参照して説明する。ＣＧＷ１３は、非書換え対象の電源管理プログラムを実行し、非書換え対象の電源管理処理を行う。ここでは、ＣＧＷ１３が管理対象とする全てのＥＣＵ１９を起動状態とした場合について説明する。

[0282] ＣＧＷ１３は、非書換え対象ＥＣＵ１９の電源管理処理を開始すると、ＣＧＷ用の書換え諸元データの解析結果により書換え対象ＥＣＵ１９と非書換え対象ＥＣＵ１９を特定し（Ｓ９０１）、書換え諸元データの解析結果により一つ以上の書換え対象ＥＣＵ１９の書換え順序を特定する（Ｓ９０２）。ＣＧＷ１３は、書込みデータの書込みが可能であるか否かを判定し（Ｓ９０３、書込み可能判定手順に相当する）、書込みデータの書込みが可能であると判定すると（Ｓ９０３：ＹＥＳ）、電源オフ要求（停止要求）をＡＣＣ系の非書換え対象ＥＣＵ１９及びＩＧ系の非書換え対象ＥＣＵ１９に送信し、ＡＣＣ系の非書換え対象ＥＣＵ１９及びＩＧ系の非書換え対象ＥＣＵ１９を起動状態から停止状態に移行させる（Ｓ９０４、状態移行制御手順に相当する）。

[0283] ＣＧＷ１３は、電源オフ要求を該当する全てのＥＣＵ１９に送信完了したか否かを判定し（Ｓ９０５）、電源オフ要求を該当する全てのＥＣＵ１９に送信完了したと判定すると（Ｓ９０５：ＹＥＳ）、スリープ要求を＋Ｂ電源系の非書換え対象ＥＣＵ１９に送信し、＋Ｂ電源系の非書換え対象ＥＣＵ１９を起動状態からスリープ状態に移行させる（Ｓ９０６、状態移行制御手順に相当する）。

[0284] ＣＧＷ１３は、スリープ要求を該当する全てのＥＣＵ１９に送信完了したか否かを判定し（Ｓ９０７）、スリープ要求を該当する全てのＥＣＵ１９に送信完了したと判定すると（Ｓ９０７：ＹＥＳ）、全ての書換え対象ＥＣＵ１９についてアプリプログラムの書換えを完了したか否かを判定する（Ｓ９０８）。ＣＧＷ１３は、全ての書換え対象ＥＣＵ１９についてアプリプログ

ラムの書換えを完了したと判定すると（Ｓ９０８：ＹＥＳ）、非書換え対象ＥＣＵ１９の電源管理処理を終了する。ＣＧＷ１３は、全ての書換え対象ＥＣＵ１９についてアプリプログラムの書換えを完了していないと判定すると（Ｓ９０８：ＮＯ）、ステップＳ９０４に戻り、ステップＳ９０４以降を繰返す。

[0285] ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数の場合に、複数の書換え対象ＥＣＵ１９の状態を個別に移行させても良いし、複数の書換え対象ＥＣＵ１９の状態を纏めて移行させても良い。即ち、図８３では、非書換え対象ＥＣＵ１９に対し、ＣＧＷ１３が電源オフ要求又はスリープ要求を送信する処理について示している。次に示す図８４及び図８５では、非書換え対象ＥＣＵ１９に対する電源管理処理に加え、書換え対象ＥＣＵ１９に対する電源管理処理を行う場合について説明する。

[0286] まず、ＣＧＷ１３が複数の書換え対象ＥＣＵ１９の状態を個別に移行させる場合について図８４を用いて説明する。図８４に示すように、例えば書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）であり、書換え順序が早い方から順にＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）で指定されている書換え対象ＥＣＵ１９を駐車中に書換える場合について説明する。

[0287] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）の全てを停止状態又はスリープ状態から起動状態に移行させる。ＣＧＷ１３は、１番目に書き換えるＥＣＵ（ＩＤ１）を起動状態のまま保持し、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）を起動状態から停止状態又はスリープ状態に移行させ、書込みデータをＥＣＵ（ＩＤ１）に配信する。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）への書込みデータの配信を完了すると、ＥＣＵ（ＩＤ１）を起動状態から停止状態又はスリープ状態に移行させ、２番目に書き換えるＥＣＵ（ＩＤ２）を停止状態又はスリープ状態から起動状態に移行させ、ＥＣＵ（ＩＤ３）を停止状態又はスリープ状態のまま保持し、書込みデータをＥＣＵ（ＩＤ２）に配信する。

[0288] ＣＧＷ１３は、ＥＣＵ（ＩＤ２）への書込みデータの配信を完了すると、ＥＣＵ（ＩＤ１）を停止状態又はスリープ状態のまま保持し、ＥＣＵ（ＩＤ２）を起動状態から停止状態又はスリープ状態に移行させ、３番目に書き換えるＥＣＵ（ＩＤ３）を停止状態又はスリープ状態から起動状態に移行させ、書込みデータをＥＣＵ（ＩＤ３）に配信する。ＣＧＷ１３は、ＥＣＵ（ＩＤ３）への書込みデータの配信を完了すると、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）を停止状態又はスリープ状態のまま保持し、ＥＣＵ（ＩＤ３）を起動状態から停止状態又はスリープ状態に移行させる。このようにＣＧＷ１３は、複数の書換え対象ＥＣＵ１９のうち現在書換え中のＥＣＵ１９のみが起動状態となるように制御する。

[0289] 次に、ＣＧＷ１３が複数の書換え対象ＥＣＵ１９の状態を纏めて移行させる場合について図８５を用いて説明する。図８５に示すように、例えば書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）であり、書換え順序が早い方から順にＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）で指定されている書換え対象ＥＣＵ１９を駐車中に書換える場合について説明する。

[0290] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）の全てを停止状態又はスリープ状態から起動状態に移行させる。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）の全てを起動状態のまま保持し、書込みデータをＥＣＵ（ＩＤ１）に配信する。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）への書込みデータの配信を完了すると、書込みデータをＥＣＵ（ＩＤ２）に配信する。ＣＧＷ１３は、ＥＣＵ（ＩＤ２）への書込みデータの配信を完了すると、書込みデータをＥＣＵ（ＩＤ３）に配信する。ＣＧＷ１３は、ＥＣＵ（ＩＤ３）への書込みデータの配信を完了すると、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）の全てを起動状態から停止状態又はスリープ状態に移行させる。このようにＣＧＷ１３は、インストールが全て完了するまで、複数の書換え対象ＥＣＵ１９の全てを起動状態となるように制御する。ここで、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、

ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）への書込みデータの配信を同時並行で行っても良い。

[0291] 駐車中に書換え対象ＥＣＵ１９がアプリプログラムを書換える場合には、必ずしも書換え対象ＥＣＵ１９への供給電圧が安定した環境ではないので、アプリプログラムの書換え中に車両バッテリ４０がバッテリ上がりとなる事態が懸念される。特に書換え対象ＥＣＵ１９が複数であると、アプリプログラムの書換えに要する時間が長くなるので、アプリプログラムの書換え中に車両バッテリ４０がバッテリ上がりとなる可能性が高まる。この点に関し、上記したように非書換え対象ＥＣＵ１９を停止状態又はスリープ状態とすることで、プログラムの書換え中に車両バッテリ４０のバッテリ残量が不十分となる事態を未然に回避する。更に、書換え対象ＥＣＵ１９のうち現在書換え中でないＥＣＵ１９を停止状態又はスリープ状態とすることで、より消費電力を抑えることができる。

[0292] 以上は、駐車中に書換え対象ＥＣＵ１９のアプリプログラムを書換える場合について説明したが、車両走行中に書換え対象ＥＣＵ１９のアプリプログラムを書換える場合について説明する。車両走行中に書換え対象ＥＣＵ１９がアプリプログラムを書換える場合には、書換え対象ＥＣＵ１９への供給電圧が安定した環境にあるので、アプリプログラムの書換え中に車両バッテリ４０がバッテリ上がりとなる事態が懸念されることはないが、車両バッテリ４０のバッテリ残量が少ない場合もあり得る。このような事情から、車両走行中では、動作不要なＥＣＵ１９を停止状態又はスリープ状態に移行させておくことが望ましい。図８６に示すように、車両走行中に動作不要なＥＣＵ４４が＋Ｂ電源ライン３７に接続されているが、ＡＣＣ電源ライン３８及びＩＧ電源ライン３９に接続されていない構成である場合には、ＣＧＷ１３は、その車両走行中に動作不要なＥＣＵ４４を起動状態から停止状態又はスリープ状態に移行させる。ＥＣＵ４４は、例えば盗難防止等の機能を有するＥＣＵである。即ち、ＣＧＷ１３は、車両走行中では全てのＥＣＵ１９が起動状態にある中、動作不要であり且つ書換え対象でないＥＣＵ４４に対し、停

止状態又はスリープ状態に移行させる。これにより、車両走行中のインストールに伴う消費電力の増加を抑えることができる。

[0293] 又、ＣＧＷ１３は、車両バッテリ４０のバッテリ残量を監視し、上記した非書換え対象の電源管理処理を行う。ここで、バッテリ残量の監視処理について図８７を用いて説明する。ＣＧＷ１３は、バッテリ残量の監視処理を開始すると、書込みデータを書換え対象ＥＣＵ１９に配信中においてバッテリ残量を監視し（Ｓ９１１）、バッテリ残量が第１所定容量以上であるか、バッテリ残量が第１所定容量未満であり且つ第２所定容量以上であるか、バッテリ残量が第２所定容量未満であるかを判定する（Ｓ９１２～Ｓ９１４）。

[0294] ＣＧＷ１３は、バッテリ残量が第１所定容量以上であると判定すると（Ｓ９１２：ＹＥＳ）、非書換え対象ＥＣＵ１９を起動状態のまま保持し、書込みデータの書換え対象ＥＣＵ１９への配信を継続する（Ｓ９１５）。ＣＧＷ１３は、バッテリ残量が第１所定容量未満であり且つ第２所定容量以上であると判定すると（Ｓ９１３：ＹＥＳ）、非書換え対象ＥＣＵ１９のうち走行中に動作不要なＥＣＵを停止状態又はスリープ状態に移行させ、書込みデータの書換え対象ＥＣＵ１９への配信を継続する（Ｓ９１６）。ＣＧＷ１３は、バッテリ残量が第２所定容量未満であると判定すると（Ｓ９１４：ＹＥＳ）、書換えを中断可能であるか否かを判定する（Ｓ９１７）。

[0295] ＣＧＷ１３は、書換えを中断可能であると判定すると（Ｓ９１７：ＹＥＳ）、書込みデータの配信を中断する（Ｓ９１８）。ＣＧＷ１３は、書換えを中断可能でないと判定すると（Ｓ９１７：ＮＯ）、非書換え対象ＥＣＵ１９のうち停止状態又はスリープ状態に移行可能な全てのＥＣＵを停止状態又はスリープ状態に移行させる（Ｓ９１９）。

[0296] ＣＧＷ１３は、書換えを完了したか否かを判定し（Ｓ９２０）、書換えを完了していないと判定すると（Ｓ９２０：ＮＯ）、ステップＳ９１１に戻り、ステップＳ９１１以降を繰返す。ＣＧＷ１３は、書換えを完了したと判定すると（Ｓ９２０：ＹＥＳ）、停止状態又はスリープ状態の書換え対象ＥＣＵ１９を起動状態に移行させ（Ｓ９２１）、バッテリ残量の監視処理を終了

する。ここで、第１所定容量及び第２所定容量の値は、ＣＧＷ１３が予め保有していても良いし、書換え諸元データにより指定された値を用いても良い。

[0297] 又、ＣＧＷ１３は、ステップＳ９１９において、例えばアラーム機能等の特定の機能を有するＥＣＵ１９については停止状態又はスリープ状態に移行させる対象から除外し、特定の機能を有するＥＣＵ１９を除く非書換え対象ＥＣＵ１９を起動状態から停止状態又はスリープ状態に移行させても良い。ＣＧＷ１３は、書換え対象ＥＣＵ１９がアプリプログラムの書換え中にアプリ制御を実行可能である場合には、その書換え対象ＥＣＵ１９と通信可能なＥＣＵ１９を除く非書換え対象ＥＣＵ１９を停止状態又はスリープ状態としても良い。ＣＧＷ１３は、全てのＥＣＵ１９が停止状態又はスリープ状態にあるときに、例えば車両位置が所定位置になったり現在時刻が所定時刻になったりする等して書換え条件が成立すると、書換え対象ＥＣＵ１９を停止状態又はスリープ状態から起動状態に移行させても良い。

[0298] ＣＧＷ１３は、書換え対象ＥＣＵ１９又は非書換え対象ＥＣＵ１９を、起動電源（＋Ｂ電源系ＥＣＵ、ＡＣＣ系ＥＣＵ、ＩＧ系ＥＣＵ）、ドメイングループ（ボディ系、走行系、マルチメディア系）、同期タイミングの何れかを基準としてグループ化し、書換え対象ＥＣＵ１９をグループ単位で起動状態としたり、非書換え対象ＥＣＵ１９をグループ単位で停止状態又はスリープ状態としたりしても良い。

[0299] 又、ＣＧＷ１３は、バス単位で電源制御する構成でも良い。即ち、ＣＧＷ１３は、特定のバスに接続されている全てのＥＣＵ１９が非書換え対象ＥＣＵ１９であると判定すると、その特定のバスの電源をオフすることで、その特定のバスに接続されている全ての非書換え対象ＥＣＵ１９を停止状態又はスリープ状態に移行させても良い。

[0300] 以上に説明したように、ＣＧＷ１３は、非書換え対象の電源管理処理を行うことで、書換え対象ＥＣＵ１９に対してインストール可能であると判定すると、少なくとも一つ以上の非書換え対象ＥＣＵ１９を停止状態、スリープ

状態又は省電力動作状態とするようにした。アプリプログラムの書換え中に車両バッテリ４０のバッテリ残量が不十分となる事態を未然に回避することができる。又、非書換え対象ＥＣＵ１９が停止状態、スリープ状態又は省電力動作状態となることで、通信負荷の増大を抑えることができる。

[0301] （１０）ファイルの転送制御処理

ファイルの転送制御処理について図８８から図９７を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３においてファイルの転送制御処理を行う。本実施形態は、ＤＣＭ１２（第１装置が相当する）が保持している書換えデータを、ＣＧＷ１３（第２装置が相当する）を介して書換え対象ＥＣＵ１９（第３装置が相当する）に送信する際の処理である。

[0302] 図８８に示すように、ＣＧＷ１３は、ファイルの転送制御部８２において、転送対象ファイル特定部８２ａと、第１データサイズ特定部８２ｂと、取得情報特定部８２ｃと、第２データサイズ特定部８２ｄと、分割ファイル転送要求部８２ｅとを有する。転送対象ファイル特定部８２ａは、書換え諸元データの解析結果を用いて書換え対象ＥＣＵ１９に書込まれる書込みデータを含むファイルを転送対象ファイルとして特定する。転送対象ファイル特定部８２ａは、例えば書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）の場合、図８に示すＣＧＷ用の書換え諸元データからＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）のＥＣＵ情報を取得し、その取得したＥＣＵ情報から書込みデータを含むファイルを転送対象ファイルとして特定する。転送対象ファイルとして、そのファイルを取得する際のアドレスやインデックスを特定しても良いし、そのファイルのファイル名を特定しても良い。

[0303] 第１データサイズ特定部８２ｂは、転送対象ファイルが転送対象ファイル特定部８２ａにより特定されると、その転送対象ファイルを取得するための第１データサイズを特定する。取得情報特定部８２ｃは、転送対象ファイルが転送対象ファイル特定部８２ａにより特定されると、その転送対象ファイルを取得するための取得情報としてアドレスを特定する。尚、本実施形態で

は、転送対象ファイルを取得するための取得情報としてアドレスを特定するが、転送対象ファイルを取得するための取得情報であれば、アドレスに限らず、ファイル名称やＥＣＵ（ＩＤ）等であっても良い。第２データサイズ特定部８２ｄは、書込みデータを書換え対象ＥＣＵ１９に配信するための第２データサイズを特定する。即ち、第１データサイズは、ＤＣＭ１２からＣＧＷ１３へのデータ転送サイズであり、第２データサイズは、ＣＧＷ１３から書換え対象ＥＣＵ１９へのデータ転送サイズである。

[0304] 分割ファイル転送要求部８２ｅは、アドレスが取得情報特定部８２ｃにより特定され、第１データサイズが第１データサイズ特定部８２ｂにより特定されると、そのアドレス及び第１データサイズをＤＣＭ１２に指定し、分割ファイルの転送をＤＣＭ１２に要求する。分割ファイル転送要求部８２ｅは、例えばＥＣＵ（ＩＤ１）に配信すべき書込みファイルのデータ量が１Ｍバイトの場合、書込みデータをアドレス０ｘ１００００００から１ｋバイト毎に転送するように要求する。

[0305] 次に、ＣＧＷ１３におけるファイルの転送制御部８２の作用について図８９から図９７を参照して説明する。ＣＧＷ１３は、ファイルの転送制御プログラムを実行し、ファイルの転送制御処理を行う。

[0306] ＣＧＷ１３は、ＤＣＭ１２からアンパッケージング完了通知信号を受信したと判定すると、ファイルの転送制御処理を開始する。アンパッケージングとは、図１０に示すように、配信パッケージファイルをＥＣＵ毎のデータ及び各書換え諸元データに分ける処理である。ＣＧＷ１３は、ファイルの転送制御処理を開始すると、所定のアドレスをＤＣＭ１２に送信する（Ｓ１００１）。ＤＣＭ１２は、ＣＧＷ１３から所定のアドレスを受信すると、その所定のアドレスの受信を契機としてＣＧＷ用の書換え諸元データをＣＧＷ１３に転送する。ＣＧＷ１３は、ＤＣＭ１２からＣＧＷ用の書換え諸元データが転送されることで、ＣＧＷ用の書換え諸元データを取得する（Ｓ１００２）。

[0307] ＣＧＷ１３は、ＤＣＭ１２からＣＧＷ用の書換え諸元データを取得すると

、その取得したＣＧＷ用の書換え諸元データを解析し（Ｓ１００３）、書換え諸元データの解析結果から転送対象ファイルを特定する（Ｓ１００４、転送対象ファイル特定手順に相当する）。ＣＧＷ１３は、その転送対象ファイルに対応するアドレスを特定し（Ｓ１００５、取得情報特定手順に相当する）、その転送対象ファイルに対応する第１データサイズを特定する（Ｓ１００６、第１データサイズ特定手順に相当する）。ＣＧＷ１３は、その特定したアドレスとデータサイズをＳＩＤ（Service Identifier）３５の規定にしたがってＤＣＭ１２に送信し、そのアドレスとデータサイズをメモリ領域に指定し、分割ファイルの転送をＤＣＭ１２に要求する（Ｓ１００７）。

[0308] ＤＣＭ１２は、ＣＧＷ１３からアドレスとデータサイズを受信すると、ＤＣＭ用の書換え諸元データを解析し、そのアドレスとデータサイズに対応するファイルを分割ファイルとしてＣＧＷ１３に転送する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルが転送されることで分割ファイルを取得する（Ｓ１００８）。この場合、ＣＧＷ１３は、その取得したファイルをＲＡＭに記憶した後、フラッシュメモリに記憶してもよい。

[0309] ＣＧＷ１３は、取得すべき全ての分割ファイルの取得を完了したか否かを判定する（Ｓ１００９）。ＣＧＷ１３は、例えばＥＣＵ（ＩＤ１）に配信すべき書込みファイルのデータ量が１Ｍバイトの場合、１ｋバイト毎の分割ファイルを取得し、１ｋバイト毎の分割ファイルの取得を繰返して１Ｍバイトのデータ量を取得完了したか否かを判定する。ＣＧＷ１３は、取得すべき全ての分割ファイルの取得を完了していないと判定すると（Ｓ１００９：ＮＯ）、ステップＳ１００４に戻り、ステップＳ１００４以降を繰返す。ＣＧＷ１３は、取得すべき全てのファイルの取得を完了したと判定すると（Ｓ１００９：ＹＥＳ）、ファイルの転送制御処理を終了する。尚、ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数の場合には、上記したファイルの転送制御処理を各書換え対象ＥＣＵ１９に対して繰返す。

[0310] 即ち、ＣＧＷ１３は、例えば書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）の場合には、ＥＣＵ（ＩＤ１）への

書込みデータの配信が完了すると、ＥＣＵ（ＩＤ２）に対してファイルの転送制御処理を行い、ＥＣＵ（ＩＤ２）への書込みデータの配信が完了すると、ＥＣＵ（ＩＤ３）に対してファイルの転送制御処理を行う。尚、ＣＧＷ１３は、複数の書換え対象ＥＣＵ１９に対する転送制御処理を順次行っても良いし、並列して行っても良い。

[0311] 図９０では、ＤＣＭ１２のメモリ内に、例えばＥＣＵ（ＩＤ１）の書込みデータファイルがアドレス「１０００」～「３９９９」に記憶されており、ＥＣＵ（ＩＤ２）の書込みデータファイルがアドレス「４０００」～「６９９９」に記憶されており、ＥＣＵ（ＩＤ３）の書込みデータファイルがアドレス「７０００」～に記憶されている場合を示している。

[0312] この場合、ＣＧＷ１３は、図９１に示すように、ＤＣＭ１２からアンパッケージング完了通知信号を受信すると、アドレス「００００」をＤＣＭ１２に送信し、ＤＣＭ１２から書換え諸元データを取得する。即ち、ＤＣＭ１２は、アドレス「００００」の受信をＣＧＷ用の書換えデータの取得要求であると判定し、ＣＧＷ用の書換え諸元データをＣＧＷ１３に送信する。ＣＧＷ１３は、書込みデータの転送対象としてＥＣＵ（ＩＤ１）を指定し、アドレス「１０００」とデータサイズ「１ｋバイト」を指定し、アドレス「１０００」～「１９９９」に記憶されているＥＣＵ（ＩＤ１）の書込みデータを含む分割ファイルをＤＣＭ１２から取得する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルを取得すると、その分割ファイルに含まれる書込みデータをＥＣＵ（ＩＤ１）に配信する。

[0313] ＣＧＷ１３は、続いて書込みデータの転送対象として同じくＥＣＵ（ＩＤ１）を指定し、アドレス「２０００」とデータサイズ「１ｋバイト」を指定し、アドレス「２０００」～「２９９９」に記憶されているＥＣＵ（ＩＤ１）の書込みデータを含む分割ファイルをＤＣＭ１２から取得する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルを取得すると、その分割ファイルに含まれる書込みデータをＥＣＵ（ＩＤ１）に配信する。ＣＧＷ１３は、書込みデータのＥＣＵ（ＩＤ１）への書込みが全て完了するまで、ＤＣＭ１２からの

１ｋバイト毎に分割ファイルの取得を繰返し、その分割ファイルに含まれる書込みデータのＥＣＵ（ＩＤ１）への配信を繰返す。即ち、ＣＧＷ１３は、ＤＣＭ１２から１ｋバイトの書込みデータを取得すると、その１ｋバイトの書込みデータを書換え対象ＥＣＵ１９に送信し、書換え対象ＥＣＵ１９への送信が完了すると、次の１ｋバイトの書込みデータをＤＣＭ１２から取得する。これらの処理を書込みが全て完了するまでＣＧＷ１３が繰返す。

[0314] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）において書込みデータの書込みが正常に完了すると、書込みデータの転送対象としてＥＣＵ（ＩＤ２）を指定し、アドレス「４０００」とデータサイズ「１ｋバイト」を指定し、アドレス「４０００」～「４９９９」に記憶されているＥＣＵ（ＩＤ２）の書込みデータを含む分割ファイルをＤＣＭ１２から取得する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルを取得すると、その分割ファイルに含まれる書込みデータをＥＣＵ（ＩＤ２）に配信する。

[0315] ＣＧＷ１３は、ＥＣＵ（ＩＤ２）において書込みデータの書込みが正常に完了すると、書込みデータの転送対象としてＥＣＵ（ＩＤ３）を指定し、アドレス「７０００」とデータサイズ「１ｋバイト」を指定し、アドレス「７０００」～「７９９９」に記憶されているＥＣＵ（ＩＤ２）の書込みデータを含む分割ファイルをＤＣＭ１２から取得する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルを取得すると、その分割ファイルに含まれる書込みデータをＥＣＵ（ＩＤ２）に配信する。

[0316] 以上に説明したように、ＣＧＷ１３は、ファイルの転送制御処理を行うことで、書換え諸元データの解析結果から転送対象ファイルを特定し、その転送対象ファイルに対応するアドレスとデータサイズを特定する。ＣＧＷ１３は、そのアドレスとデータサイズをＤＣＭ１２に指定し、転送対象ファイルを分割した分割ファイルの転送をＤＣＭ１２に対して要求し、ＤＣＭ１２から分割ファイルを取得する。これにより、容量の大きい書込みデータをＤＣＭ１２のメモリで保持したまま、ＥＣＵ１９への書込みデータの配信を行うことができる。即ち、ＣＧＷ１３では容量の大きいファイルを記憶するため

のメモリを用意する必要がなくなり、ＣＧＷ１３のメモリ容量を削減することができる。

[0317] ここで、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量と、ＣＧＷ１３から書換え対象ＥＣＵ１９に配信される書込みファイルのデータ量との関係について説明する。上記した例示では、図９２に示すように、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量が１ｋバイトである場合を説明したが、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量と、ＣＧＷ１３から書換え対象ＥＣＵ１９に配信される書込みファイルのデータ量との関係は、どのようであっても良い。

[0318] 即ち、ＣＧＷ１３は、例えばＣＡＮ通信上の理由により書換え対象ＥＣＵ１９が書込みデータを４ｋバイトで受信する仕様であれば、書込みファイルのデータ量を４ｋバイト単位で書換え対象ＥＣＵ１９に配信する。この場合、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量が１ｋバイトであれば、ＣＧＷ１３は、分割ファイル４つ分をＤＣＭ１２から取得した後、書換え対象ＥＣＵ１９への４ｋバイトの配信を行う。即ち、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量は、ＣＧＷ１３から書換え対象ＥＣＵ１９に配信される書込みファイルのデータ量よりも小さくなる。このような関係では、ＣＧＷ１３において、メモリ容量の増大を抑えつつ、ＤＣＭ１２からの分割ファイルの取得と、書込みデータの書換え対象ＥＣＵ１９への配信とを並列して行うことができる。

[0319] 即ち、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量が４ｋバイトとすると、ＤＣＭ１２からの分割ファイルの取得と、書込みデータの書換え対象ＥＣＵ１９への配信とを並列して行うには、ＣＧＷ１３のメモリ容量を８ｋバイトにする必要がある。ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量が１ｋバイトとすることで、ＣＧＷ１３のメモリ容量を８ｋバイトにすることなく、ＤＣＭ１２からの分割ファイルの取得と、書込みデータの書換え対象ＥＣＵ１９への配信とを並列して行うことができる。例えばＣＧＷ１３のメモリ容量を５ｋバイト確保しておき、ＣＧ

Ｗ１３は、ＤＣＭ１２から取得し終わった４ｋバイトを書換え対象ＥＣＵ１９に配信すると共に、ＤＣＭ１２から次の１ｋバイトの取得を行う。そして、ＣＧＷ１３は、書換え対象ＥＣＵ１９への４ｋバイトの配信が完了した後、ＤＣＭ１２から更に次の１ｋバイトの取得を行う。

[0320] 一方、ＣＧＷ１３は、例えばＣＡＮ通信上の理由により書換え対象ＥＣＵ１９が書込みデータを１２８バイトで受信する仕様であれば、書込みデータを１２８バイトで書換え対象ＥＣＵ１９に配信する。この場合、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量が１ｋバイトであれば、ＣＧＷ１３は、分割ファイル１つ分をＤＣＭ１２から取得した後、書換え対象ＥＣＵ１９への１２８バイトずつの配信を行う。即ち、ＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量は、ＣＧＷ１３から書換え対象ＥＣＵ１９に配信される書込みファイルのデータ量よりも大きくなる。例えばＣＧＷ１３のメモリ容量を２ｋバイト確保しておき、ＣＧＷ１３は、ＤＣＭ１２から取得し終わった１ｋバイトを、１２８バイト単位で書換え対象ＥＣＵ１９に配信すると共に、ＤＣＭ１２から次の１ｋバイトの取得を行う。そして、ＣＧＷ１３は、書換え対象ＥＣＵ１９への１２８バイト×８回の配信が完了した後、ＤＣＭ１２から更に次の１ｋバイトの取得を行う。

[0321] このようにＤＣＭ１２からＣＧＷ１３に転送される分割ファイルのデータ量を固定値（例えば１ｋバイト）とし、ＣＧＷ１３から書換え対象ＥＣＵ１９に配信される書込みファイルのデータ量を書換え対象ＥＣＵ１９の仕様に応じて可変値とすれば良い。ＣＧＷ１３は、例えば書換え諸元データに指定される各ＥＣＵのデータ転送サイズを用いて、書換え対象ＥＣＵ１９に配信するデータ量を決定しても良い。

[0322] ＣＧＷ１３は、転送要求をＤＣＭ１２に送信し、分割ファイルの転送をＤＣＭ１２に要求するが、分割ファイルの転送をＤＣＭ１２に要求する態様として第１要求態様と第２要求態様がある。書換え対象ＥＣＵ１９は、書込みデータの受信を完了すると、書込みデータの受信を完了したことを示す受信完了通知をＣＧＷ１３に送信し、書込みデータの書込みを完了すると、書込

みデータの書込みを完了したことを示す書込み完了通知をＣＧＷ１３に送信する。

[0323] 第１配信態様について図９３を用いて説明する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルを取得すると、その取得した分割ファイルを書込みデータとして書換え対象ＥＣＵ１９に配信する。書換え対象ＥＣＵ１９は、書込みデータの受信を完了すると、受信完了通知をＣＧＷ１３に送信し、書込みデータの書込み処理を開始する。ＣＧＷ１３は、書換え対象ＥＣＵ１９から書込みデータの受信完了通知を受信すると、転送要求をＤＣＭ１２に送信し、次の分割ファイルの転送をＤＣＭ１２に要求する。ＣＧＷ１３は、ＤＣＭ１２から次の分割ファイルを取得すると、その取得した次の分割ファイルを書込みデータとして書換え対象ＥＣＵ１９に配信する。

[0324] このようにＣＧＷ１３は、第１配信態様では、書換え対象ＥＣＵ１９における書込みデータの書込み完了を待つことなく、次の書込みデータをＤＣＭ１２から取得し、書換え対象ＥＣＵ１９に配信する。そのため、第１配信態様では、ＣＧＷ１３において、書換え対象ＥＣＵ１９が書込みデータの書込みを完了していないと、次の分割ファイルをＤＣＭ１２から取得して次の書込みデータを書換え対象ＥＣＵ１９に配信しても、次の書込みデータを書換え対象ＥＣＵ１９が受信不能となる虞がある。しかしながら、書換え対象ＥＣＵ１９が書込みデータの書込みを完了していれば、次の分割ファイルをＤＣＭ１２から速やかに取得して次の書込みデータを書換え対象ＥＣＵ１９に速やかに配信することができる。

[0325] 第２配信態様について図９４を用いて説明する。ＣＧＷ１３は、ＤＣＭ１２から分割ファイルを取得すると、その取得した分割ファイルを書込みデータとして書換え対象ＥＣＵ１９に配信する。書換え対象ＥＣＵ１９は、書込みデータの受信を完了すると、受信完了通知をＣＧＷ１３に送信し、書込みデータの書込み処理を開始する。書換え対象ＥＣＵ１９は、書込みを完了すると、書込み完了通知をＣＧＷ１３に送信する。ＣＧＷ１３は、書換え対象ＥＣＵ１９から書込み完了通知を受信すると、転送要求をＤＣＭ１２に送信

し、次の分割ファイルの転送をＤＣＭ１２に要求する。ＣＧＷ１３は、ＤＣＭ１２から次の分割ファイルを取得すると、その取得した次の分割ファイルを書込みデータとして書換え対象ＥＣＵ１９に配信する。

[0326] このようにＣＧＷ１３は、第２配信態様では、書換え対象ＥＣＵ１９における書込みデータの書込み完了を待ってから、次の書込みデータをＤＣＭ１２から取得し、書換え対象ＥＣＵ１９に配信する。そのため、第２配信態様では、ＣＧＷ１３において、次の分割ファイルをＤＣＭ１２から取得するまでに時間を要するが、書換え対象ＥＣＵ１９が書込みデータの書込みを完了した状態で分割ファイルの転送をＤＣＭ１２に要求することができる。よって、次の分割ファイルをＤＣＭ１２から取得して次の書込みデータを書換え対象ＥＣＵ１９に配信すると、次の書込みデータを書換え対象ＥＣＵ１９に確実に配信することできる。

[0327] 又、ＣＧＷ１３は、書込みデータをＳＩＤ３４、３６、３７により書換え対象ＥＣＵ１９に配信するが、書込みデータを書換え対象ＥＣＵ１９に配信する態様として第１配信態様と第２配信態様がある。第１配信態様では、ＣＧＷ１３は、図９５に示すように、配信すべき書込みデータを所定のデータ量（例えば１ｋバイト）で分割して配信する。第２配信態様では、ＣＧＷ１３は、図９６に示すように、配信すべき書込みデータを分割せずに纏めて配信する。ＣＧＷ１３は、書換え対象ＥＣＵ１９に最初に配信するＳＩＤ３４により、第１配信態様又は第２配信態様の何れかを選択する。ＣＧＷ１３は、図９７に示すように、書換え対象ＥＣＵ１９に最後に配信するＳＩＤ３７に対するＡＣＫ（ＳＩＤ７４）を受信することにより、書換え対象ＥＣＵ１９における書込みデータの受信を特定する。このＳＩＤ３７に対するＡＣＫが、図９３及び図９４にて前述した書込みデータの受信完了通知に相当する。即ち、第１配信態様では、ＣＧＷ１３は、書換え対象ＥＣＵ１９に最後に配信するＳＩＤ３７に対するＡＣＫを受信すると、次の書込みデータのアドレスをインクリメントすることで、次の書込みデータを書換え対象ＥＣＵ１９に配信すると同時に、更に次の書込みデータをＤＣＭ１２から取得する。

[0328] 又、ＤＣＭ用の書換え諸元データではアドレスとファイルとが対応付けられているが、アドレスとファイルとが対応付けられる方法として、例えばフォルダ構成を工夫し、フォルダ１に諸元データを格納し、フォルダ２にファイル１を格納し、フォルダ３にファイル２を格納して管理しても良いし、ファイル名の順序で管理しても良い。例えば図１０に示すアンパッケージングにおいて、フォルダ１にＤＣＭ用の書換え諸元データ及びＣＧＷ用の書換え諸元データを格納し、フォルダ２にＥＣＵ（ＩＤ１）の認証子及び差分データを格納し、フォルダ３にＥＣＵ（ＩＤ２）の認証子及び差分データを格納して管理する。

[0329] 又、ＣＧＷ１３は、例えば通信途絶等の何らかの理由により書込みデータの書換え対象ＥＣＵ１９への配信を中断した場合には、書込みデータの書込みを完了したアドレスを特定可能な情報を書換え対象ＥＣＵ１９から取得し、その書込みを完了していない時点からの書込みデータを含む分割ファイルの転送をＤＣＭ１２に要求する。又は、ＣＧＷ１３は、先頭からの書込みデータを含む分割ファイルの転送をＤＣＭ１２に要求しても良い。

[0330] 以上に説明したように、ＣＧＷ１３は、ファイルの転送制御処理を行うことで、書換え対象ＥＣＵ１９に書込まれる書込みデータを含むファイルを転送対象ファイルとして特定し、転送対象ファイルを取得するためのアドレス及び第１データサイズを特定し、分割ファイルの転送をＤＣＭ１２に要求し、ＤＣＭ１２から分割ファイルが転送されると、書込みデータを書換え対ＥＣＵに配信する。ＤＣＭ１２からＣＧＷ１３への書込みデータの転送と、ＣＧＷ１３から書換え対象ＥＣＵ１９への書込みデータの配信を効率的に行うことができる。

[0331] （１１）書込みデータの配信制御処理

書込みデータの配信制御処理について図９８から図１０８を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において書込みデータの配信制御処理を行う。ＣＧＷ１３は、書込みデータを車両内のバスを介してＥＣＵ１９に送信するので、書込みデータを配信中のバス負荷が必要

以上に高くならないように書込みデータの配信制御処理を行う。

[0332] 図９８に示すように、＋Ｂ電源系ＥＣＵ、ＡＣＣ系ＥＣＵ、ＩＧ系ＥＣＵが同一バスに接続されている場合を想定する。この場合、＋Ｂ電源状態では、＋Ｂ電源系ＥＣＵのみが起動しており、ＡＣＣ系ＥＣＵとＩＧ系ＥＣＵが停止しているので、そのバスには＋Ｂ電源系ＥＣＵのみの車両制御データが伝送される。ＡＣＣ電源状態であるときには、＋Ｂ電源系ＥＣＵとＡＣＣ系ＥＣＵが起動しており、ＩＧ系ＥＣＵが停止しているので、そのバスには＋Ｂ電源系ＥＣＵとＡＣＣ系ＥＣＵの車両制御データが伝送される。ＩＧ電源状態であるときには、＋Ｂ電源系ＥＣＵとＡＣＣ系ＥＣＵとＩＧ系ＥＣＵが起動しているので、そのバスには＋Ｂ電源系ＥＣＵとＡＣＣ系ＥＣＵとＩＧ系ＥＣＵの車両制御データが伝送される。即ち、車両制御データの伝送量は、多い順にＩＧ電源状態、ＡＣＣ電源状態、＋Ｂ電源状態となる。

[0333] 図９９に示すように、ＣＧＷ１３は、書込みデータの配信制御部８３において、第１対応関係特定部８３ａと、第２対応関係特定部８３ｂと、伝送許容量特定部８３ｃと、配信頻度特定部８３ｄと、バス負荷計測部８３ｅと、配信制御部８３ｆとを有する。

[0334] 第１対応関係特定部８３ａは、書換え諸元データの解析結果から電源状態とバスの伝送許容量との関係を示す第１対応関係を特定し、図１００に示すバス負荷テーブルを特定する。伝送許容量とは、データの衝突や遅延が発生しない状況下でデータを送受信可能な伝送負荷の値である。バス負荷テーブルは、電源状態とバスの伝送許容量との対応関係を示すテーブルであり、バス毎に規定される。伝送許容量は、最大伝送許容量に対して伝送可能な車両制御データと書込みデータとの伝送量の合計である。

[0335] 図１００の例示では、第１バスについて、伝送許容量が最大伝送許容量に対して「８０％」であるので、ＣＧＷ１３は、ＩＧ電源状態では、車両制御データの伝送許容量として最大伝送許容量に対して「５０％」を許容し、書込みデータの伝送許容量として最大伝送許容量に対して「３０％」を許容する。又、第１バスについて、ＣＧＷ１３は、ＡＣＣ電源状態では、車両制御

データの伝送許容量として最大伝送許容量に対して「３０％」を許容し、書込みデータの伝送許容量として最大伝送許容量に対して「５０％」を許容する。又、第１バスについて、ＣＧＷ１３は、＋Ｂ電源状態では、車両制御データの伝送許容量として最大伝送許容量に対して「２０％」を許容し、書込みデータの伝送許容量として最大伝送許容量に対して「６０％」を許容する。図１００に示すように、第２バス及び第３バスについても同様に規定される。

[0336] 第２対応関係特定部８３ｂは、書換え諸元データの解析結果から書換え対象ＥＣＵ１９が所属するバスと電源系との関係を示す第２対応関係を特定し、図１０１に示す書換え対象ＥＣＵ所属テーブルを特定する。書換え対象ＥＣＵ所属テーブルは、書換え対象ＥＣＵ１９が所属するバスと電源系とを示すテーブルである。

[0337] 図１０１の例示では、ＣＧＷ１３は、第１書換え対象ＥＣＵ１９については、第１バスに接続されており、＋Ｂ電源状態、ＡＣＣ電源状態、ＩＧ電源状態の何れでも起動するので、＋Ｂ電源系ＥＣＵであると特定する。又、ＣＧＷ１３は、第２書換え対象ＥＣＵ１９については、第２バスに接続されており、＋Ｂ電源状態では停止するが、ＡＣＣ電源状態、ＩＧ電源状態で起動するので、ＡＣＣ系ＥＣＵであると特定する。又、ＣＧＷ１３は、第３書換え対象ＥＣＵ１９については、第３バスに接続されており、＋Ｂ電源状態、ＡＣＣ電源状態では停止するが、ＩＧ電源状態で起動するので、第３書換え対象ＥＣＵ１９をＩＧ系ＥＣＵであると特定する。

[0338] ＣＧＷ１３は、図８に示す書換え諸元データのうち、「接続バス」及び「接続電源」のデータを用いて、書換え対象ＥＣＵ１９が何れのバスに接続されており、何れの電源系であるかを特定する。尚、これらの情報が特定可能であれば、必ずしもテーブルの形で保有する必要はない。

[0339] 伝送許容量特定部８３ｃは、第１対応関係の特定結果及び第２対応関係の特定結果にしたがって書換え対象ＥＣＵ１９が属するバスの伝送許容量であって、プログラムの更新を行う際の車両の電源状態に対応する伝送許容量を

特定する。具体的に説明すると、伝送許容量特定部８３ｃは、第２対応関係である書換え対象ＥＣＵ所属テーブルを用いて、書換え対象ＥＣＵ１９が属するバスを特定し、第１対応関係であるバス負荷テーブルを用いて、その特定したバスについて電源状態毎の伝送許容量を特定する。

[0340] 配信頻度特定部８３ｄは、予め定められている電源状態と書込みデータの配信頻度との対応関係を用い、インストールする際の電源状態に対応する書込みデータの配信頻度を特定する。具体的に説明すると、配信頻度特定部８３ｄは、バス負荷テーブルを用いて、伝送許容量特定部８３ｃにより特定された伝送許容量のうち書込みデータを配信するために割当てられている伝送許容量を特定し、書込みデータの配信頻度を特定する。配信頻度特定部８３ｄは、例えば書換え対象ＥＣＵ１９が属するバスが第１バスであると特定し、インストールする際の電源状態がＩＧ電源状態であると特定すると、伝送許容量を「８０％」と特定し、そのうち書込みデータを配信するために割当てられている伝送許容量を「３０％」と特定することで、書込みデータの配信頻度を特定する。書込みデータを配信するために割当てられている伝送許容量が、伝送制約情報に相当する。

[0341] バス負荷計測部８３ｅは、書換え対象ＥＣＵ１９が属するバスのバス負荷を計測する。バス負荷計測部８３ｅは、例えば単位時間で受信したフレーム数又はビット数をカウントすることでバス負荷を計測する。配信制御部８３ｆは、配信頻度特定部８３ｄにより特定された配信頻度にしたがって書込みデータの配信を制御する。

[0342] 次に、ＣＧＷ１３における書込みデータの配信制御部８３の作用について図１０２から図１０８を参照して説明する。ＣＧＷ１３は、書込みデータの配信制御プログラムを実行し、書込みデータの配信制御処理を行う。

[0343] ＣＧＷ１３は、ＤＣＭ１２からアンパッケージング完了通知信号を受信すると、書込みデータの配信制御処理を開始する。ＣＧＷ１３は、ＤＣＭ１２からＣＧＷ用の書換え諸元データを取得し（Ｓ１１０１）、そのＣＧＷ用の書換え諸元データからバス負荷テーブル及び書換え対象ＥＣＵ所属テーブル

を特定する（Ｓ１１０２）。ＣＧＷ１３は、書換え対象ＥＣＵ１９が所属するバスを書換え対象ＥＣＵ所属テーブルから特定する（Ｓ１１０３）。ＣＧＷ１３は、その書換え対象ＥＣＵ１９が所属するバスであって、更新を行う際の車両の電源状態に対応する伝送許容量をバス負荷テーブルから特定する。そして、ＣＧＷ１３は、特定した伝送許容量を考慮し、書込みデータの配信頻度を特定する（Ｓ１１０４、配信頻度特定手順に相当する）。ＣＧＷ１３は、例えば第１書換え対象ＥＣＵ１９であるＥＣＵ（ＩＤ１）に対し、車両走行中に書込みデータを配信する場合、ＩＧ電源状態における第１バスの伝送許容量を参照する。図１００の例示では、ＩＧ電源状態における第１バスの伝送許容量は「８０％」であり、そのうち車両制御データで「５０％」の伝送が許容され、書込みデータで「３０％」の伝送が許容される。尚、伝送許容量は、あくまでも事例を示すための値であり、数値については、適用する通信の仕様にしたがった許容範囲内に設定される。

[0344] ＣＡＮの５００［ｋｂｐｓ］上での仕様では１フレーム２５０［μｓ］程度であるので、１秒間に割込みが４回発生すると、４個のフレームが発生し、バス負荷が１００％になる。ＣＧＷ１３は、バスで発生する割込みを判定することで、書込みデータの配信頻度を特定する。ＣＧＷ１３は、単位時間で受信したフレーム数の計測を開始し、バス負荷の計測を開始し（Ｓ１１０５）、その計測したバス負荷が伝送許容量を超えているか否かを判定し（Ｓ１１０６）、配信間隔を設定する。配信間隔とは、ＣＧＷ１３において、書込みデータを書換え対象ＥＣＵ１９に配信し、書換え対象ＥＣＵ１９から書込み完了通知（ＡＣＫ）を受信し、次の書込みデータを書換え対象ＥＣＵ１９に送信するまでの時間間隔である。

[0345] ＣＧＷ１３は、その計測したバス負荷が伝送許容量を超えていないと判定すると（Ｓ１１０６：ＮＯ）、書込みデータの配信間隔を予め設定されている最短間隔に設定し、図１０３に示すように、書込みデータの書換え対象ＥＣＵ１９への配信を開始する（Ｓ１１０７、配信制御手順に相当する）。即ち、ＣＧＷ１３は、ＣＡＮ上の１フレームの配信間隔を予め設定されている

最短間隔に設定し、書込みデータの書換え対象ＥＣＵ１９への配信を開始する。尚、ＣＡＮ上の１フレームは、データ量が８バイトの書込みデータを含む。尚、ＣＡＮ　ＦＤ（CAN with Flexible Data-Rate）上の１フレームは、データ量が６４バイトの書込みデータを含む。

[0346] 一方、ＣＧＷ１３は、その計測したバス負荷が伝送許容量を超えていると判定すると（Ｓ１１０６：ＹＥＳ）、バス負荷が伝送許容量を超えない間隔を計算し（Ｓ１１０８）、書込みデータの配信間隔を当該計算した間隔に設定し、図１０４に示すように、書込みデータの書換え対象ＥＣＵ１９への配信を開始する（Ｓ１１０９、配信制御手順に相当する）。

[0347] ＣＧＷ１３は、例えばＩＧ電源状態では第１バスに対してバス負荷が伝送許容量である「８０％」を超えているか否かを判定し、バス負荷が伝送許容量を超えていないと判定すると、書込みデータの伝送許容量が「３０％」となる配信間隔Ｔ１に設定する。即ち、図１００のバス負荷テーブルに示すように、ＣＧＷ１３は、ＩＧ電源状態で第１バスにおける書込みデータの伝送許容量である「３０％」を用いて、配信間隔Ｔ１を設定する。ＣＧＷ１３は、許容される最大伝送量となるように配信間隔Ｔ１を設定する。又、ＣＧＷ１３は、計測対象を書込みデータのフレームに絞ってバス負荷を計測し、書込みデータに依るバス負荷が書込みデータの伝送許容量「３０％」を超えているか否かを判定しても良い。ＣＧＷ１３は、バス負荷が伝送許容量を超えていると判定すると、そのバス負荷が伝送許容量を超えている量に応じて、バス負荷が伝送許容量を超えない配信間隔Ｔ２（＞Ｔ１）に変更する。このように、ＣＧＷ１３は、ＤＣＭ１２から書込みデータを取得した後に、設定した配信間隔に達するまで待機して書込みデータを書換え対象ＥＣＵ１９に配信する。

[0348] ＣＧＷ１３は、書込みデータの書換え対象ＥＣＵ１９への配信を開始すると、書込みデータの書換え対象ＥＣＵ１９への配信を完了したか否かを判定すると共に、その計測したバス負荷が伝送許容量を超えているか否かを継続して判定する（Ｓ１１１０，Ｓ１０１１）。ＣＧＷ１３は、その計測したバ

ス負荷が伝送許容量を超えていないと判定すると（Ｓ１１１１：ＮＯ）、書込みデータの配信間隔を予め設定されている最短間隔に設定し、書込みデータの書換え対象ＥＣＵ１９への配信間隔を変更する（Ｓ１１１２）。一方、ＣＧＷ１３は、その計測したバス負荷が伝送許容量を超えていると判定すると（Ｓ１１１１：ＹＥＳ）、バス負荷が伝送許容量を超えない間隔を計算し（Ｓ１１１３）、書込みデータの配信間隔を当該計算した間隔に設定し、書込みデータの書換え対象ＥＣＵ１９への配信間隔を変更する（Ｓ１１１４）。

[0349] ＣＧＷ１３は、書込みデータの書換え対象ＥＣＵ１９への配信を完了したと判定すると（Ｓ１１１０：ＹＥＳ）、単位時間で受信したフレーム数の計測を停止し、バス負荷の計測を停止し（Ｓ１１１５）、書込みデータの配信制御処理を終了する。ここで、ＣＧＷ１３は、書換え対象ＥＣＵ１９が複数ある場合、全ての書換え対象ＥＣＵ１９へのインストールに対して、書込みデータの配信制御処理を行う。

[0350] 以上に説明したように、ＣＧＷ１３は、書込みデータの配信制御処理を行うことで、予め定められている電源状態と書込みデータの配信頻度との対応関係を用い、書換え対象ＥＣＵ１９への書込みデータの配信頻度を特定し、その配信頻度にしたがって書込みデータの配信を制御する。インストールを行う際の、データの衝突や遅延等を抑制することができる。又、同一バスにおける車両制御データの配信を妨げることなく、書込みデータの配信を共存させることができる。

[0351] 尚、以上は、ＣＧＷ１３において、書換え諸元データの解析結果からバス負荷テーブルを特定する構成を例示したが、バス負荷テーブルを予め保持する構成でも良い。又、ＣＧＷ１３において、書換え諸元データの解析結果から書換え対象ＥＣＵ所属テーブルを特定する構成を例示したが、書換え対象ＥＣＵ所属テーブルを予め保持する構成でも良い。

[0352] 車両が走行中の電源状態では書込みデータの配信量を相対的に少なくし、駐車中の電源状態では書込みデータの配信量を相対的に多くしても良い。即

ち、ＣＧＷ１３は、図１０５に示すように、車両が走行中のＩＧ電源がオンでは、ＩＧ系ＥＣＵ、ＡＣＣ系ＥＣＵ、＋Ｂ電源系ＥＣＵがＣＡＮフレームを送信することにより、車両制御や診断等のアプリデータの伝送量が相対的に多くなるので、書込みデータの配信量を相対的に少なくする。又、ＣＧＷ１３は、図１０６に示すように、駐車中のＩＧ電源がオフでは、＋Ｂ電源系ＥＣＵのみがＣＡＮフレームを送信することにより、車両制御や診断等のアプリデータの伝送量が相対的に少なくなるので、書込みデータの配信量を相対的に多くする。即ち、ＣＧＷ１３は、車両制御や診断等のアプリデータの伝送を妨げない空き容量内で書込みデータの配信量を調整する。

[0353] 又、図１０７に示すように、ＣＧＷ１３において、書換え対象ＥＣＵ１９からイベントフレームが送信されている場合は、イベントフレームを受信することで割込みの頻度が高くなり、バス負荷が高くなるので、書込みデータの配信量を相対的に少なくし、書換え対象ＥＣＵ１９からイベントフレームが送信されなくなった場合に、書込みデータの配信量を相対的に多くしても良い。

[0354] 又、図１０８に示すように、車両システムにおいて、ＣＧＷ１３が書込みデータの配信中であることを特定した場合に、車両制御や診断等のアプリデータの送信間隔を、許容される最大間隔まで長くすることでバス負荷を低下させても良い。ＣＧＷ１３において、車両システムがアプリデータの送信間隔を長くしたことでバス負荷が低下されたことで、書込みデータの配信量を相対的に多くしても良い。

[0355] 書換え諸元データに組込まれるバス負荷テーブルは、例えば車両メーカが車種やグレード等に拘らず一律的に共通に設定される。例えば車種やグレード等によりＥＣＵの装備が大きく異なると、バス負荷が大きく異なり、車種やグレード等により個別に最適なバス負荷テーブルを設定してしまうと、その検証に工数を要する等の煩雑な手間を要してしまうので、そのような煩雑な手間を回避するためである。

[0356] 上述したように車両が走行中にインストールを行う場合と同様に、車両が

駐車中にインストールを行う場合についても、書込みデータの配信制御処理を行う。その場合、書換え対象ＥＣＵ１９が＋Ｂ電源系ＥＣＵであれば、＋Ｂ電源状態で更新を行うことも可能であるので、バス負荷テーブルにおける＋Ｂ電源状態の伝送許容量を参照する。一方、書換え対象ＥＣＵ１９がＩＧ系ＥＣＵの場合には、ＩＧ電源状態でインストールを行うので、バス負荷テーブルにおけるＩＧ電源状態の伝送許容量を参照する。ここで、例えば書換え対象ＥＣＵ１９がＡＣＣ系ＥＣＵの場合に、ＩＧ電源状態でインストールを行うことも可能である。この場合、バス負荷テーブルにおけるＩＧ電源状態の伝送許容量を参照する。尚、バス負荷テーブルと書換え対象ＥＣＵ所属テーブルを保持する構成を説明したが、電源状態毎の書込みデータの配信頻度を特定可能であれば、どのようなテーブルを保持する態様でも良い。

[0357] （１２）アクティベート要求の指示処理

アクティベート要求の指示処理について図１０９から図１１１を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３においてアクティベート要求の指示処理を行う。ＣＧＷ１３は、アプリプログラムの書換えを完了した複数の書換え対象ＥＣＵ１９に対し、その書換えたプログラムを有効にするためにアクティベート要求を行う。本実施形態において、ＣＧＷ１３は、ＣＧＷ用の書換え諸元データを解析することにより、書換え対象ＥＣＵ１９のグループを把握している状態とする。尚、ＣＧＷ１３は、駐車中においてのみアクティベート要求を行い、車両走行中ではアクティベート要求を行わない。

[0358] 図１０９に示すように、ＣＧＷ１３は、アクティベート要求の指示部８４において、書換え対象特定部８４ａと、書換え完了判定部８４ｂと、アクティベート実行可能判定部８４ｃと、アクティベート要求指示部８４ｄとを有する。書換え対象特定部８４ａは、連携制御する複数の書換え対象ＥＣＵ１９を対象とし、複数の書換え対象ＥＣＵ１９を特定する。書換え完了判定部８４ｂは、複数の書換え対象ＥＣＵ１９が書換え対象特定部８４ａにより特定されると、その特定された複数の書換え対象ＥＣＵ１９の全てにおいてプ

ログラムの書換えが完了したか否かを判定する。

[0359] アクティベート実行可能判定部８４ｃは、複数の書換え対象ＥＣＵ１９の全てにおいてプログラムの書換えが完了したと書換え完了判定部８４ｂにより判定されると、アクティベートを実行可能であるか否かを判定する。アクティベート実行可能判定部８４ｃは、ユーザによるアクティベート承諾が行われている場合であり、且つ車両が駐車状態の場合に、アクティベートを実行可能であると判定する。

[0360] アクティベート要求指示部８４ｄは、アクティベートを実行可能であるとアクティベート実行可能判定部８４ｃにより判定されると、アクティベート要求を指示する。具体的には、アクティベート要求指示部８４ｄは、新面への切替え要求を指示した後に、リセット要求を指示する、セッション移行タイムアウトを監視する、又は書換え対象ＥＣＵ１９の内部リセットを監視することで、アクティベート要求を指示する。２面メモリＥＣＵ又は１面サスペンドメモリＥＣＵでは、アプリプログラムを書込んだ新面（非運用面）で起動することにより、アプリプログラムをアクティベートする。一方、１面単独メモリＥＣＵでは、再起動によりアプリプログラムをアクティベートする。尚、書換え対象ＥＣＵ１９は、新面への切替え要求が指示された後、アクティベート要求に依らず、自身にてリセットする構成としても良い。

[0361] 次に、ＣＧＷ１３におけるアクティベート要求の指示部の作用について図１１０及び図１１１を参照して説明する。ＣＧＷ１３は、アクティベート要求の指示プログラムを実行し、アクティベート要求の指示処理を行う。

[0362] ＣＧＷ１３は、アクティベート要求の指示処理を開始すると、複数の書換え対象ＥＣＵ１９を特定する（Ｓ１２０１、書換え対象特定手順に相当する）。具体的には、ＣＧＷ１３は、書換え諸元データに記載されるＥＣＵ（ＩＤ）を参照することで、書換え対象ＥＣＵ１９を特定する。ＣＧＷ１３は、その特定した複数の書換え対象ＥＣＵ１９の全てにおいてアプリプログラムの書換えが完了したか否かを判定する（Ｓ１２０２、書換え完了判定手順に相当する）。ＣＧＷ１３は、例えば書換え諸元データに記載されるＥＣＵ（

ＩＤ）の順序にしたがって書換え対象ＥＣＵ１９に対するインストールを順番に行い、最後に記載されるＥＣＵ（ＩＤ）に対するインストールが完了したら全ての書換え対象ＥＣＵ１９において書込みが完了したと判定する。

[0363] ＣＧＷ１３は、その特定した複数の書換え対象ＥＣＵ１９の全てにおいてアプリプログラムの書換えが完了したと判定すると（Ｓ１２０２：ＹＥＳ）、アクティベートを実行可能であるか否かを判定する（Ｓ１２０３、アクティベート実行可能判定手順に相当する）。具体的には、ＣＧＷ１３は、これまでに更新に対するユーザ承諾を得ているか、車両が駐車状態であるか等を判定し、これらの条件を満たすと、アクティベートを実行可能であると判定する。ユーザ承諾は、更新処理全体に対する承諾でも良いし、アクティベートに対する承諾でも良い。ＣＧＷ１３は、アクティベートを実行可能であると判定すると（Ｓ１２０３：ＹＥＳ）、これ以降、アクティベート要求を複数の書換え対象ＥＣＵ１９に同時に指示する（アクティベート要求指示手順に相当する）。ここでは、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）が同一グループの書換え対象ＥＣＵ１９であるとして説明する。

[0364] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に対し、アクティベートを実行可能であると判定すると、アクティベート要求の指示処理を開始する。ＣＧＷ１３は、アクティベート要求の指示処理を開始すると、新面への切替え要求を書換え対象ＥＣＵ１９に指示する（Ｓ１２０４）。ＣＧＷ１３は、電源管理ＥＣＵ２０に対し、ＩＧ電源をオフからオンに切替えるように要求する（Ｓ１２０５）。ＣＧＷ１３は、車両が駐車状態であり、ＩＧスイッチ４２はオフの状態であるが、アクティベートを行うためにＩＧ電源をオフからオンに切替える。尚、ＣＧＷ１３は、インストールに引続いてアクティベートを行う場合には、ＩＧ電源がオン状態であるので、Ｓ１２０５は行わず、スリープ状態の書換え対象ＥＣＵ１９に対し、起動要求（ウェイクアップ要求）を行う。

[0365] ＣＧＷ１３は、ソフトウェアのリセット要求を書換え対象ＥＣＵ１９に送信し、ソフトウェアのリセット要求を書換え対象ＥＣＵ１９に指示する（Ｓ

１２０６）。書換え対象ＥＣＵ１９は、ソフトウェアのリセット要求に対応する仕様であれば、ＣＧＷ１３からソフトウェアのリセット要求を受信すると、ソフトウェアをリセットして再起動し、アプリプログラムをアクティベートする。書換え対象ＥＣＵ１９が１面単独メモリＥＣＵの場合には、書換え対象ＥＣＵ１９は、新アプリプログラムで再起動することで、旧アプリプログラムから新アプリプログラムに切替える。書換え対象ＥＣＵ１９が１面サスペンドメモリＥＣＵ又は２面メモリＥＣＵの場合には、書換え対象ＥＣＵ１９は、フラッシュメモリに記憶している運用面情報（Ａ面又はＢ面）を更新し、新アプリプロプログラムが書込まれた面を運用面に切替えることで、旧アプリプログラムから新アプリプログラムに切替える。

[0366] ＣＧＷ１３は、電源管理ＥＣＵ２０に対してＩＧ電源をオンからオフに切替え、ＩＧ電源をオフからオンに切替える旨を要求し、電源のリセット要求を書換え対象ＥＣＵ１９に指示し、再起動を書換え対象ＥＣＵ１９に指示する（Ｓ１２０７）。書換え対象ＥＣＵ１９は、ソフトウェアのリセット要求に対応していない仕様でも、ＩＧ電源がオンからオフに切替わり、ＩＧ電源がオフからオンに切替わると、自己をリセットして再起動し、アプリプログラムをアクティベートする。この場合も、書換え対象ＥＣＵ１９が１面単独メモリＥＣＵの場合には、書換え対象ＥＣＵ１９は、新アプリプログラムで再起動することで、旧アプリプログラムから新アプリプログラムに切替える。書換え対象ＥＣＵ１９が１面サスペンドメモリＥＣＵ又は２面メモリＥＣＵの場合には、書換え対象ＥＣＵ１９は、フラッシュメモリに記憶している運用面情報（Ａ面又はＢ面）を更新し、新アプリプロプログラムが書込まれた面を運用面に切替えることで、旧アプリプログラムから新アプリプログラムに切替える。又、ＣＧＷ１３は、セッション移行タイムアウトを監視し（Ｓ１２０８）、書換え対象ＥＣＵ１９の内部リセットの監視する（Ｓ１２０９）。

[0367] 即ち、ＣＧＷ１３は、書換え対象ＥＣＵ１９がソフトウェアのリセット要求に対応しない仕様であれば、ソフトウェアのリセット要求を書換え対象Ｅ

ＣＵ１９に送信してもアクティベートを指示することができないので、電源のリセット要求を書換え対象ＥＣＵ１９に指示することで、ソフトウェアのリセット要求に対応しない仕様の書換え対象ＥＣＵ１９のアクティベートを行う。例えばエンジンＥＣＵ等のＩＧ系ＥＣＵでは、電源オンオフで必ずリセットさせられる構成であるので、ソフトウェアのリセット要求に対応しない構成である場合が多い。書換え対象ＥＣＵ１９の観点では、ＣＧＷ１３からソフトウェアのリセット要求が指示されたこと、ＣＧＷ１３から電源のリセット要求が指示されたこと、セッション移行タイムアウト、内部リセットの何れかによりアクティベート（新プログラムでの起動）を行う。

[0368] ソフトウェアのリセット要求に対応する書換え対象ＥＣＵ１９は、ＣＧＷ１３からソフトウェアのリセット要求が指示されると、自己で強制的にリセットを行い、アクティベートを行う。ＡＣＣ系やＩＧ系ＥＣＵの書換え対象ＥＣＵ１９は、ＣＧＷ１３から電源のリセット要求が指示されると、電源が強制的に供給されなくなるので、次回の電源の供給時にリセットを行い、アクティベートを行う。＋Ｂ電源系ＥＣＵの書換え対象ＥＣＵ１９は、ＡＣＣ系やＩＧ系ＥＣＵの書換え対象ＥＣＵ１９とは異なり、電源が常時供給されているので、セッション移行タイムアウトや内部リセットにより、アクティベートを行う。尚、各書換え対象ＥＣＵ１９に対するアクティベートの方法は、書換え諸元データにより指定される。

[0369] ＣＧＷ１３は、全ての書換え対象ＥＣＵ１９から新アプリプログラムで正常起動した旨が通知されると、切替え完了通知をＤＣＭ１２に送信する（Ｓ１２１０）。ＤＣＭ１２は、更新プログラムのアクティベートが完了した旨をセンター装置３に通知する。ＣＧＷ１３は、電源管理ＥＣＵ２０に対してＩＧ電源をオンからオフに切替えるように要求し、アプリグラムのアクティベート同期指示処理を終了する。ＣＧＷ１３は、ユーザ操作によりＩＧ電源がオフからオンに切替えられると、各ＥＣＵのプログラムバージョン、起動面等をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３から受信した各ＥＣＵ１９の情報をセンター装置３に通知する。ここで、ＤＣＭ１２がアクテ

ィベート完了をセンター装置３に通知する際、各ＥＣＵのプログラムバージョン及び面情報を含むＥＣＵ構成情報をセンター装置３に送信しても良い。図１１１は、書換え対象ＥＣＵ１９が２面メモリＥＣＵ又は１面サスペンドメモリＥＣＵの場合を示している。

[0370] 以上に説明したように、ＣＧＷ１３は、アクティベート要求の指示処理を行うことで、アプリプログラムの書換えを完了した複数の書換え対象ＥＣＵ１９が旧プログラムから新プログラムへの切替えを独自のタイミングで行ってしまう事態を未然に回避し、その複数の書換え対象ＥＣＵ１９において旧プログラムから新プログラムへの切替えタイミングを適切に揃える。即ち、互いに連携し合う複数の書換え対象ＥＣＵ１９のプログラムバージョンが不整合な状態となり、連携した処理に不都合が生じることを回避する。

[0371] （１３）アクティベートの実行制御処理

アクティベートの実行制御処理について図１１２から図１１４を参照して説明する。アクティベートの実行制御処理は、ＣＧＷ１３が前述した（１２）アクティベート要求の指示処理を行うことに伴い、ＣＧＷ１３からアクティベート要求が指示された書換え対象ＥＣＵ１９が行う処理である。車両用プログラム書換えシステム１は、書換え対象ＥＣＵ１９においてアクティベートの実行制御処理を行う。ここで、書換え対象ＥＣＵ１９は、１面サスペンド方式メモリや２面メモリのように複数のデータ格納面を有する。書換え対象ＥＣＵ１９は、第１データ格納面と第２データ格納面とを有し、非運用面（新面）において書換えデータのインストールが完了している状態とする。

[0372] 図１１２に示すように、ＥＣＵ１９は、アクティベートの実行制御部１０７において、運用面情報更新部１０７ａと、実行条件判定部１０７ｂと、実行制御部１０７ｃと、通知部１０７ｄとを有する。運用面情報更新部１０７ａは、ＣＧＷ１３からアクティベート要求が指示されると、次回の再起動に向けてフラッシュメモリの起動面判定情報（運用面情報）を更新する。運用面情報更新部１０７ａは、例えば現在Ａ面で起動しており、Ｂ面に新プログ

ラムを書込んだ場合、運用面情報をＡ面からＢ面に更新する。

[0373] 実行条件判定部１０７ｂは、アクティベートの実行条件として、ＣＧＷ１３からソフトウェアのリセット要求が指示されたか否か、ＣＧＷ１３から電源管理ＥＣＵ２０へ電源のリセット要求が指示されたか否か、ＣＧＷ１３との通信途絶が所定時間継続したか否かを判定する。実行条件判定部１０７ｂは、何れか１つの条件を満たす場合に、アクティベートの実行条件が成立したと判定する。電源のリセット要求が指示されたか否かは、ＣＧＷ１３からの指示でなく、電源検出回路３６にて検出しても良い。実行制御部１０７ｃは、アクティベートの実行条件が成立したと実行条件判定部１０７ｂにより判定されると、運用面情報にしたがって起動面を旧面（現在運用している面）から新面（現在運用していない面）に切替える新面切替え（アクティベート）を行う。通知部１０７ｄは、運用面情報やバージョン情報等の通知情報をＣＧＷ１３に通知する。

[0374] 次に、書換え対象ＥＣＵ１９におけるアクティベートの実行制御部１０７の作用について図１１３及び図１１４を参照して説明する。書換え対象ＥＣＵ１９は、アクティベートの実行制御プログラムを実行し、アクティベートの実行制御処理を行う。

[0375] （１３－１）書換え処理

書換え対象ＥＣＵ１９は、書換え処理を開始すると、書換え前処理として品番読出しや認証等のメモリ消去の直前までの処理を行う（Ｓ１３０１）。書換え対象ＥＣＵ１９は、センター装置３から書換え面情報を受信したか否かを判定する（Ｓ１３０２）。書換え対象ＥＣＵ１９は、例えば配信パッケージに含まれる書換え諸元データに記載される書換え面情報をＣＧＷ１３から取得したか否かにより、書換え面情報を受信したか否かを判定する。書換え対象ＥＣＵ１９は、センター装置３から書換え面情報を受信したと判定すると（Ｓ１３０２：ＹＥＳ）、その書換え面情報と自己が管理している書換え面情報（運用面情報）とを照合し、両者が一致しているか否かを判定する（Ｓ１３０３）。ここで、書換え面情報は、例えばセンター装置３から送信

される書換え諸元データに記載されている。例えば自身が管理している書換え面情報が、運用面がＡ面であり且つ非運用面がＢ面である場合において、書換え諸元データに記載されている書換え面情報が、非運用面（Ｂ面）を示す場合には両者が一致すると判定し、諸元データに記載される書換え面情報が、運用面（Ａ面）を示す場合、両者は不一致と判定する。

[0376] 書換え対象ＥＣＵ１９は、両者が一致していると判定すると（Ｓ１３０３：ＹＥＳ）、書換え処理としてメモリ消去、書込みデータの書込み、ベリファイを行い（Ｓ１３０４）、書換え処理を終了する。ベリファイとは、例えばフラッシュメモリに書込んだデータの完全性検証である。書換え対象ＥＣＵ１９は、両者が一致していないと判定すると（Ｓ１３０３：ＮＯ）、否定応答をＣＧＷ１３に送信し（Ｓ１３０５）、書換え処理を終了する。

[0377] （１３－２）アクティベートの実行制御処理

書換え対象ＥＣＵ１９は、アクティベートの実行制御処理を開始すると、非運用面を書換え面とし、アプリプログラムの書換え面への書換えを完了したか否かを判定する（Ｓ１３１１）。書換え対象ＥＣＵ１９は、アプリプログラムの書換え面への書換えを完了したと判定すると（Ｓ１３１１：ＹＥＳ）、フラッシュメモリに書込まれたアプリプログラムの完全性を検証し、書換え後のデータ検証の正否を判定する（Ｓ１３１２）。書換え対象ＥＣＵ１９は、書換え後のデータ検証が正であると判定すると（Ｓ１３１２：ＹＥＳ）、新面の書換え完了フラグを「ＯＫ」に設定し記憶する（Ｓ１３１３）。

[0378] その後、書換え対象ＥＣＵ１９は、ＣＧＷ１３からアクティベート要求が指示されたか否かを判定する（Ｓ１３１４）。書換え対象ＥＣＵ１９は、アクティベート要求が指示されたと判定すると（Ｓ１３１４：ＹＥＳ）、新面の書換え完了フラグが「ＯＫ」であるか否かを判定し（Ｓ１３１５）、新面の書換え完了フラグが「ＯＫ」であると判定すると（Ｓ１３１５：ＹＥＳ）、運用面情報を更新する（Ｓ１３１６、運用面情報更新手順に相当する）。即ち、書換え対象ＥＣＵ１９は、例えば運用面がＡ面であり且つ非運用面がＢ面である場合にＢ面を書換え面としてアプリプログラムの書換え面への書

換えを完了した場合には、運用面がＡ面であり且つ非運用面がＢ面であることを示す運用面情報を、運用面がＢ面であり且つ非運用面がＡ面であることを示す運用面情報に更新する。

[0379] 書換え対象ＥＣＵ１９は、運用面情報に更新すると、ＣＧＷ１３からソフトウェアのリセット要求が受付けたか否か、ＣＧＷ１３から電源管理ＥＣＵ２０へ電源のリセット要求が指示されたか否か、ソフトウェアのリセット要求が指示されてからＣＧＷ１３との通信途絶が所定時間継続したか否かを判定し、アクティベートの実行条件が成立したか否かを判定する（Ｓ１３１７、実行条件判定手順に相当する）。ここで、書換え対象ＥＣＵ１９は、これらアクティベートの実行条件の何れが成立すると再起動するか、ＥＣＵそれぞれで再起動条件が定められている。

[0380] 書換え対象ＥＣＵ１９は、ＣＧＷ１３からソフトウェアのリセット要求が指示された、ＣＧＷ１３から電源管理ＥＣＵ２０へ電源のリセット要求が指示された、ソフトウェアのリセット要求が指示されてから所定時間が経過したことのうち何れかを判定し、アクティベートの実行条件が成立したと判定すると（Ｓ１３１７：ＹＥＳ）、再起動（リセット）を実行する。書換え対象ＥＣＵ１９は、再起動を実行したことで、更新された運用面情報にしたがって新面（Ｂ面）を起動面として起動し（Ｓ１３１８、起動制御手順に相当する）、アクティベートの実行制御処理を終了する。即ち、書換え対象ＥＣＵ１９は、再起動後は、アプリプログラムがインストールされたＢ面で起動する。

[0381] 書換え対象ＥＣＵ１９は、アプリプログラムの新面への書換えを完了していないと判定すると（Ｓ１３１１：ＮＯ）、又は書換え後のデータ検証が否であると判定すると（Ｓ１３１２：ＮＯ）、アクティベート要求が指示されたか否かを判定し（Ｓ１３１９）、アクティベート要求が指示されたと判定すると（Ｓ１３１９：ＹＥＳ）、否定応答をＣＧＷ１３に送信し（Ｓ１３２０）、ステップＳ１３１１に戻る。尚、書換え対象ＥＣＵ１９は、書換え後のデータ検証が否であると判定した場合には、アクティベートの実行制御処

理を終了し、ロールバック等の処理を行っても良い。又、書換え対象ＥＣＵ１９は、新面の書換え完了フラグが「ＯＫ」でないと判定すると（Ｓ１３１５：ＮＯ）、否定応答をＣＧＷ１３に送信し（Ｓ１３２１）、ステップＳ１３１１に戻る。

[0382] 以上に説明したように、書換え対象ＥＣＵ１９は、アクティベートの実行制御処理を行うことで、ＣＧＷ１３からアクティベート要求が指示されると、次回の再起動に向けて運用面情報を更新し、アクティベートの実行条件が成立すると、再起動後に運用面情報にしたがって起動面を旧面から新面に切替える新面切替えを行う。即ち、書換え対象ＥＣＵ１９は、更新プログラムのインストールが完了しても、ＣＧＷ１３からアクティベートを指示されない限り、更新プログラムで起動しない。例えばユーザがＩＧスイッチオフ４２をオフからオンに操作したことに伴い、書換え対象ＥＣＵ１９が再起動したとしても、ＣＧＷ１３からアクティベートを指示されていなければ、同じ運用面にて起動する。ＣＧＷ１３が複数の書換え対象ＥＣＵ１９へ同時にアクティベートを指示し、その後、ソフトウェアリセット、電源リセット又はセッションタイムアウトにより再起動が実行されることにより、複数の書換え対象ＥＣＵ１９の更新プログラムを同時に有効化することができる。尚、上述した説明ではデータ格納面が２面である場合について説明したが、データ格納面が３面以上ある場合についても同様である。

[0383] 尚、前述した（１２）ＣＧＷ１３におけるアクティベート要求の指示処理において、アプリプログラムの書換えを完了した複数の書換え対象ＥＣＵ１９に対してＣＧＷ１３がアクティベート要求の指示処理を行うことで、アプリプログラムの書換えを完了した複数の書換え対象ＥＣＵ１９が旧プログラムから新プログラムへの切替えを独自のタイミングで行ってしまう事態を未然に回避し、その複数の書換え対象ＥＣＵ１９において旧プログラムから新プログラムへの切替えタイミングを適切に揃えることができる。

[0384] （１４）書換え対象のグループ管理処理

書換え対象のグループ管理処理について図１１５から図１１８を参照して

説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において書換え対象のグループ管理処理を行う。ＣＧＷ１３は、同一グループに属する１以上の書換え対象ＥＣＵ１９に対し、アプリプログラムのアクティベートを同時に指示する。又、ＣＧＷ１３は、インストールからアクティベートまでの制御をグループ単位で行う。ここでは、ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）が第１グループの書換え対象ＥＣＵ１９であり、ＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）及びＥＣＵ（ＩＤ１３）が第２グループの書換え対象ＥＣＵ１９であるとして説明する。

[0385] 図１１５に示すように、ＣＧＷ１３は、書換え対象のグループ管理部８５において、グループ生成部８５ａと、指示実行部８５ｂとを有する。グループ生成部８５ａは、ＣＧＷ用の書換え諸元データの解析結果にしたがって同時にバージョンアップすべき書換え対象ＥＣＵ１９をグループ化してグループを生成する。指示実行部８５ｂは、グループがグループ生成部８５ａにより生成されると、そのグループを単位として所定の順番でインストールの指示を行い、インストールが完了すると、そのグループを単位としてアクティベートの指示を行う。

[0386] 次に、ＣＧＷ１３における書換え対象のグループ管理部８５の作用について図１１６から図１１８を参照して説明する。ＣＧＷ１３は、書換え対象のグループ化プログラムを実行し、書換え対象のグループ管理処理を行う。ＣＧＷ１３は、書換え対象のグループ管理処理を開始すると、ＤＣＭ１２からＣＧＷ用の書換え諸元データを取得し（Ｓ１４０１、書換え諸元データ取得手順に相当する）、その取得した書換え諸元データを解析し（Ｓ１４０２、書換え諸元データ解析手順に相当する）、今回の書換え対象ＥＣＵ１９の所属グループを判定する。ＣＧＷ１３は、例えば書換え諸元データのＥＣＵに関する情報を参照し、何れのグループに所属するかを特定しても良いし、書換え諸元データのグループに関する情報を参照し、当該グループに何れのＥＣＵが所属するかを特定しても良い。ＣＧＷ１３は、１つのグループに対し、最初の書換え対象ＥＣＵ１９の書換えであるか否かを判定し（Ｓ１４０３

）、前回の書換え対象ＥＣＵ１９と同じグループに属する書換え対象ＥＣＵ１９の書換えであるか否かを判定し（Ｓ１４０４）、前回の書換え対象ＥＣＵ１９と異なるグループに属する書換え対象ＥＣＵ１９の書換えであるか否かを判定する（Ｓ１４０５、グループ生成手順に相当する）。

[0387] ＣＧＷ１３は、最初の書換え対象ＥＣＵ１９の書換えであると判定すると（Ｓ１４０３：ＹＥＳ）、又は前回の書換え対象ＥＣＵ１９と同じグループに属する書換え対象ＥＣＵ１９の書換えであると判定すると（Ｓ１４０４：ＹＥＳ）、アプリプログラムの書換えを書換え対象ＥＣＵ１９に指示し、書換え対象ＥＣＵ１９のアプリプログラムの書換えを行う（Ｓ１４０６）。そして、ＣＧＷ１３は、次次の書換え対象ＥＣＵ１９が存在するか否かを判定する（Ｓ１４０７）。ＣＧＷ１３は、同一グループ内の次の書換え対象ＥＣＵ１９が存在すると判定すると（Ｓ１４０７：ＹＥＳ）、上記したステップＳ１４０３～Ｓ１４０５に戻り、Ｓ１４０３～Ｓ１４０５を繰返す。

[0388] ＣＧＷ１３は、前回の書換え対象ＥＣＵ１９と異なるグループに属する書換え対象ＥＣＵ１９の書換えであると判定すると（Ｓ１４０５：ＹＥＳ）、アクティベート要求の指示処理に移行する（Ｓ１４０８、指示実行手順に相当する）。

[0389] ＣＧＷ１３は、アクティベート要求の指示処理を開始すると、次の書換え対象ＥＣＵ１９が存在するか否かを判定する（Ｓ１４１１）。即ち、ＣＧＷ１３は、インストールが完了していないグループが存在するか否かを判定する。ＣＧＷ１３は、次の書換え対象ＥＣＵ１９が存在すると判定すると（Ｓ１４１１：ＹＥＳ）、書換えを完了したグループに属する書換え対象ＥＣＵ１９にアクティベート要求を指示する（Ｓ１４１２）。即ち、ＣＧＷ１３は、未だ第２グループに属する書換え対象ＥＣＵ１９に対するインストールを行っていない場合、既に書換えを完了した第１グループの書換え対象ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）に対してアクティベートを指示する。

[0390] ＣＧＷ１３は、ソフトウェアのリセット要求を書換え対象ＥＣＵ１９に指示し、電源管理ＥＣＵ２０を介して電源をオンからオフに切替え、オフから

オンに切替えることによる再起動を書換え対象ＥＣＵ１９に指示することで、書換え対象ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）のアプリプログラムを同時に起動させる。

[0391] ＣＧＷ１３は、次の書換え対象ＥＣＵ１９の書換えタイミングを判定する（Ｓ１４１３，Ｓ１３１４）。即ち、ＣＧＷ１３は、第２グループに属する書換え対象ＥＣＵ１９の書換えタイミングを判定する。ＣＧＷ１３は、次の書換え対象ＥＣＵ１９の書換えタイミングが次回のユーザ乗車から降車への切替え時であると判定すると（Ｓ１４１３：ＹＥＳ）、ＩＧ電源をオンからオフに切替え（Ｓ１４１５）、アクティベート要求の指示処理を終了し、書換え対象のグループ管理処理に戻る。ＣＧＷ１３は、例えばアプリプログラムの更新の実行を許容する時間帯をユーザが予め設定しており、その時間帯に第２グループに属する書換え対象ＥＣＵ１９へのインストールが完了しないと予測されるときは、次回の駐車状態にインストールを行うこととする。この場合、元の駐車状態に戻すべく、ＣＧＷ１３は、ＩＧ電源をオフするように電源管理ＥＣＵ２０に指示する。

[0392] ＣＧＷ１３は、次の書換え対象ＥＣＵ１９の書換えタイミングが今回の降車中（駐車状態）であると判定すると（Ｓ１４１４：ＹＥＳ）、車両バッテリ４０のバッテリ残量が閾値以上であるか否かを判定する（Ｓ１４１７）。ここで、閾値は、予め設定した値でも良いし、ＣＧＷ用の書換え諸元データから取得した値でも良い。ＣＧＷ１３は、車両バッテリ４０のバッテリ残量が閾値以上でないと判定すると（Ｓ１４１６：ＮＯ）、ＩＧ電源をオンからオフに切替えるように電源管理ＥＣＵ２０に指示し（Ｓ１４１５）、アクティベート要求の指示処理を終了し、書換え対象のグループ管理処理に戻る。ＣＧＷ１３は、車両バッテリ４０のバッテリ残量が閾値以上であると判定すると（Ｓ１４１６：ＹＥＳ）、ＩＧ電源のオンを継続し（Ｓ１４１７）、アクティベート要求の指示処理を終了し、書換え対象のグループ管理処理に戻る。ＣＧＷ１３は、図１１６に示した通り、第２グループに属する書換え対象ＥＣＵ１９のアプリプログラム書換えを行う。

[0393] ＣＧＷ１３は、次の書換え対象ＥＣＵ１９が存在しないと判定すると（Ｓ１４１１：ＮＯ）、書換えを完了したグループに属する書換え対象ＥＣＵ１９にアクティベート要求を指示し（Ｓ１４１８）、ＩＧ電源をオンからオフに切替え（Ｓ１４１９）、アクティベート要求の指示処理を終了し、書換え対象のグループ管理処理に戻る。例えば第２グループに属する書換え対象ＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）及びＥＣＵ（ＩＤ１３）の書換えを完了すると、次の書換え対象ＥＣＵ１９、即ち、次のグループは存在しない。この場合、ＣＧＷ１３は、ＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）及びＥＣＵ（ＩＤ１２）に対し、更新プログラムのアクティベートを指示し、アクティベート完了後、電源管理ＥＣＵ２０へＩＧ電源オフを指示する。

[0394] 図１１８に示すように、ＥＣＵ（ＩＤ１）からＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ１１）からＥＣＵ（ＩＤ１３）のアプリプログラムを書換える場合に、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）が連携制御する関係にあり、ＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）、ＥＣＵ（ＩＤ１３）が連携制御する関係にあれば、配信パッケージにおいて、第１グループとしてＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）が書換え対象ＥＣＵ１９として属し、第２グループとしてＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）及びＥＣＵ（ＩＤ１３）が、書換え対象ＥＣＵ１９として属することとなる。ＣＧＷ１３は、第１グループに属するＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）においてアプリプログラムの書換えを完了すると、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）に対し、同時にアクティベート要求を指示する。その後、ＣＧＷ１３は、第２グループに属するＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）及びＥＣＵ（ＩＤ１３）においてアプリプログラムの書換えを実行し、全て完了すると、ＥＣＵ（ＩＤ１１）、ＥＣＵ（ＩＤ１２）、ＥＣＵ（ＩＤ１３）に対し、アクティベート要求を指示する。尚、１面単独メモリである書換え対象ＥＣＵ１９に対しては、再起動を指示することで、アクティベート指示とする。

[0395] 以上に説明したように、ＣＧＷ１３は、アクティベート要求の書換え対象ＥＣＵ１９のグループ管理処理を行うことで、そのグループを単位としてア

クティベート要求を指示する。連携制御する関係にある複数のＥＣＵのバージョンアップを同時に行うことができる。即ち、連携制御する関係にある複数の書換え対象ＥＣＵ１９のアプリプログラムのバージョンが不整合な状態なって連携制御する処理に不都合が生じることを回避することができる。又、ＣＧＷ１３は、そのグループを単位として、所定の順番でインストールを行う。即ち、ＣＧＷ１３は、インストールからアクティベートまでをグループ単位で行うように制御する。

[0396] 尚、本実施形態では、第１グループに属する書換え対象ＥＣＵ１９のインストールを完了した後、第１グループに属する書換え対象ＥＣＵ１９のアクティベートを行い、続いて、第２グループに属する書換え対象ＥＣＵ１９のインストールを完了した後、第２グループに属する書換え対象ＥＣＵ１９のアクティベートを行う構成である。しかしながら、第１グループに属する書換え対象ＥＣＵ１９に対するアクティベートと、第２グループに属する書換え対象ＥＣＵ１９に対するアクティベートとを続けて行っても良い。即ち、第１グループに属する書換え対象ＥＣＵ１９のインストールを完了し、第２グループに属する書換え対象ＥＣＵ１９のインストールを完了し、その後、第１グループに属する書換え対象ＥＣＵ１９のアクティベートを行い、第２グループに属する書換え対象ＥＣＵ１９のアクティベートを行っても良い。この場合、第１グループ及び第２グループに属する書換え対象ＥＣＵ１９に対するアクティベートを同時に行っても良い。

[0397] 又、書換え対象ＥＣＵ１９に１面単独メモリＥＣＵが含まれている場合に、その１面単独メモリＥＣＵへのインストールの指示をグループ内の最後としても良い。インストールを連携動作する関係にある書換え対象ＥＣＵ１９に指示する場合に、先にデータの送信側として動作する書換え対象ＥＣＵ１９に対してインストールを指示し、後からデータの受信側として動作する書換え対象ＥＣＵに対してインストールを指示しても良い。

[0398] ＣＧＷ１３は、書換え諸元データのメモリ種別を参照し、書換え対象ＥＣＵ１９のメモリ種別に応じてインストール順序を決定する。例えば２面メモ

リ、１面サスペンドメモリ、１面単独メモリの順とする。又、ＣＧＷ１３は、連携動作する関係にあるＥＣＵ１９の情報としてデータ送信側及びデータ受信側の何れであるかを予め保有しており、その情報に基づいて書換え対象ＥＣＵ１９のインストール順序を決定する。

[0399] 又、複数のグループがある場合に、インストールする順序は、例えば緊急度、安全度、機能、時間等に基づいて決定しても良い。緊急度とは、直ちにインストールする必要があるか否かの指標であり、インストールせずに放置しておくと人災や事故等に繋がる可能性が比較的高い場合には緊急度が高く、インストールせずに放置しておいても人災や事故等に繋がる可能性が比較的低い場合には緊急度が低く、緊急度が高いグループを優先してインストールする。安全度とは、インストール時のマイコンの種類による制約の指標であり、制約が少ない順、即ち、２面メモリ、１面サスペンドメモリ、１面単独メモリの順序でインストールする。機能とは、ユーザにとっての利便性の指標であり、ユーザにとっての利便性が高いグループを優先してインストールする。時間とは、インストールに要する時間の指標であり、インストールに要する時間が短いグループを優先してインストールする

[0400] 又、ＣＧＷ１３は、インストールを同一グループに属する第１書換え対象ＥＣＵ１９及び第２書換え対象ＥＣＵ１９に指示する場合に、第１書換え対象ＥＣＵ１９においてインストールを成功し、第２書換え対象ＥＣＵ１９においてインストールを失敗した場合に、ロールバックを第２書換え対象ＥＣＵ１９に指示し、ロールバックを第１書換え対象ＥＣＵ１９に指示する。

[0401] 又、ＣＧＷ１３は、インストールを第１グループに属する書換え対象ＥＣＵ１９及び第２グループに属する書換え対象ＥＣＵ１９に指示する場合に、第１グループに属する書換え対象ＥＣＵ１９においてインストールを失敗した場合に、インストールを第２グループに属する書換え対象ＥＣＵ１９に指示する。ＣＧＷ１３は、例えば図１１６において、第１グループに属する書換え対象ＥＣＵ１９においてインストールを失敗した状態で、第２グループの書換えとなった場合（Ｓ１４０５；ＹＥＳ）、第１グループに対するアク

ティベート要求の指示処理（Ｓ１４０８）をスキップし、ステップＳ１４０７に進む。そして、ＣＧＷ１３は、ステップＳ１４０３に戻り、第２グループのインストールを開始し、インストールが完了した場合、第２グループに対してアクティベート要求の指示処理を行う（Ｓ１４０８）。即ち、ＣＧＷ１３は、第１グループに対する更新が失敗したとしても、第２グループに対する更新を実行する。

[0402] 尚、１つのキャンペーン（１つの配信パッケージ内）に２グループがある場合には、キャンペーンに対するユーザの承諾操作及びダウンロードに対するユーザの承諾操作を１回とし、インストールに対するユーザの承諾操作及びアクティベートに対するユーザの承諾操作をグループ毎に２回行わせる。即ち、更新により変更される機能がグループ毎に異なる場合には、その機能毎にインストールに対するユーザの承諾操作及びアクティベートに対するユーザの承諾操作を行うことが望ましい。尚、インストールに対するユーザの承諾操作及びアクティベートに対するユーザの承諾操作をグループ毎に行うことを煩雑に感じるユーザも想定されるので、インストールに対するユーザの承諾操作及びアクティベートに対するユーザの承諾操作をグループ全体で１回としても良い。

[0403] 書換え諸元データを利用して書換え対象ＥＣＵ１９の所属グループを判定する構成を例示したが、ＣＧＷ１３において、書換え対象ＥＣＵ１９の所属グループを記憶しておく構成でも良い。

[0404] （１５）ロールバックの実行制御処理

ロールバックの実行制御処理について図１１９から図１３０を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３においてロールバックの実行制御処理を行う。ロールバックとは、アプリプログラムの書換えを中断する場合に、アプリプログラムを元のバージョンに戻す等、書換え対象ＥＣＵ１９のメモリを所定状態に復帰させるための書込み又は書戻しであり、ユーザから見て書換え対象ＥＣＵ１９の状態を書込みデータの書込みが開始される前の状態に戻すことである。

[0405] 図１１９に示すように、ＣＧＷ１３は、ロールバックの実行制御部８６において、キャンセル要求判定部８６ａと、ロールバック方法特定部８６ｂと、ロールバック実行部８６ｃとを有する。キャンセル要求判定部８６ａは、アプリプログラムの書換え中に書換えのキャンセル要求が発生したか否かを判定する。例えばユーザが携帯端末６を操作し、プログラム書換えのキャンセルを選択すると、そのキャンセルの情報を取得したセンター装置３からＤＣＭ１２を介してＣＧＷ１３にプログラムの書換えのキャンセル要求が通知される。

[0406] 又、システムに異常が発生した場合に、システムの異常がセンター装置３に通知されると、センター装置３からＤＣＭ１２を介してＣＧＷ１３にプログラムの書換えのキャンセル要求が通知される。システムの異常とは、例えば一の書換え対象ＥＣＵ１９への書込みが成功したが、その一の書換え対象ＥＣＵ１９と連携制御する他の書換え対象ＥＣＵ１９への書込みに失敗した場合等である。このように連携制御する複数の書換え対象ＥＣＵ１９のうち１つでも書込みに失敗すると、システムの異常と判定し、書込みが成功した書換え対象ＥＣＵ１９に対し、センター装置３からＤＣＭ１２を介してＣＧＷ１３にプログラムの書換えのキャンセル要求が通知される。即ち、キャンセル要求が発生する要因には、ユーザによる操作と、システムの異常発生とが含まれる。

[0407] ロールバック方法特定部８６ｂは、書換え対象ＥＣＵ１９に搭載されているフラッシュメモリのメモリ種別と、新プログラム又は旧プログラムの書込みデータのデータ種別に応じて、書換え対象ＥＣＵ１９の状態を書込みデータの書込みが開始される前の状態に戻すためのロールバック方法を特定する。即ち、ロールバック方法特定部８６ｂは、書換え対象ＥＣＵ１９のメモリ種別として、フラッシュメモリが１面単独メモリ、１面サスペンドメモリ又は２面メモリのうち何れであるかを特定し、書込みデータのデータ種別として、書込みデータが全データ又は差分データのうち何れであるかを特定する。

[0408] そして、ロールバック方法特定部８６ｂは、これらメモリ種別及びデータ種別に応じて、第１ロールバック処理、第２ロールバック処理又は第３ロールバック処理を特定する。ロールバック実行部８６ｃは、ロールバック方法がロールバック方法特定部８６ｂにより特定されると、そのロールバック方法に応じたロールバックを書換え対象ＥＣＵ１９に指示し、書換え対象ＥＣＵ１９を旧プログラムで動作させる。即ち、ロールバック実行部８６ｃは、書換え対象ＥＣＵ１９の動作状態を、そのアプリプログラムの書換えを開始する前の状態に復帰させるロールバックを行う。

[0409] 次に、ＣＧＷ１３におけるロールバック実行制御部８６の作用について図１２０から図１３０を参照して説明する。ＣＧＷ１３は、ロールバック実行制御プログラムを実行し、ロールバック実行制御処理を行う。ＣＧＷ１３は、ロールバックの実行制御処理として、ロールバック方法の特定処理、キャンセル要求の判定処理を行う。以下、それぞれの処理について説明する。

[0410] （１５－１）ロールバック方法の特定処理

ＣＧＷ１３は、ロールバック方法の特定処理を開始すると、ＤＣＭ１２から取得したＣＧＷ用の書換え諸元データを解析し（Ｓ１５０１）、その解析結果からロールバック方法を特定し（Ｓ１５０２）、ロールバック方法の特定処理を終了する。ＣＧＷ１３は、図８に示す書換え諸元データからメモリ種別及びロールバックプログラムのデータ種別を取得し、ロールバック方法を特定する。データ種別が新プログラムも旧プログラム（ロールバックプログラム）も同じとする運用であるならば、新プログラムのデータ種別を用いて、ロールバック方法を特定しても良い。

[0411] 即ち、ＣＧＷ１３は、書換え対象ＥＣＵ１９のフラッシュメモリが１面単独メモリであり、且つ書込みデータが全データであれば、キャンセル要求が発生したときのロールバック方法として、全データの配信を即時中断し、書換え対象ＥＣＵ１９において旧アプリプログラムのデータを書換え領域に書込んで旧アプリプログラムに書換える方法（第１ロールバック処理）を特定する。１面単独メモリのための旧アプリプログラム（ロールバック用書換え

データ）は、更新プログラムと共に配信パッケージに含まれており、ＣＧＷ１３は、新アプリプログラムと同様の方法で旧アプリプログラムを書換え対象ＥＣＵ１９に配信する。

[0412] ＣＧＷ１３は、書換え対象ＥＣＵ１９のフラッシュメモリが１面単独メモリであり、且つ書込みデータが差分データであれば、キャンセル要求が発生したときのロールバック方法として、その差分データの配信を継続し、書換え対象ＥＣＵ１９において差分データを書換え領域に書込んで新アプリプログラムに書換えた後に、旧アプリプログラムの差分データを配信し、書換え対象ＥＣＵ１９において旧データを書換え領域に書込んで旧アプリプログラムに書換える方法（第２ロールバック処理）を特定する。

[0413] 書込みデータが差分データである場合、書換え対象ＥＣＵ１９は、フラッシュメモリに書込まれている現アプリプログラムとＣＧＷ１３から取得した差分データとを用いて新アプリプログラムを復元し、新アプリプログラムの書込みを行う。フラッシュメモリに異なるアプリプログラムが書込まれている状態では、書込み対象ＥＣＵ１９は、差分データから新アプリプログラムを復元することができない。そのため、１面単独メモリでは、一旦新アプリプログラムに書換える処理が必要となる。ここで、例えば、現アプリプログラムがバージョン１．０であり、新アプリプログラムがバージョン２．０であると、書換えプログラム（書換えデータ）はバージョン１．０をバージョン２．０に更新するための差分データであり、ロールバック用書換えデータは、バージョン２．０をバージョン１．０に更新するための差分データである。

[0414] ＣＧＷ１３は、書換え対象ＥＣＵ１９のフラッシュメモリが１面サスペンドメモリ又は２面メモリであれば、書込みデータの配信を継続し、書換え対象ＥＣＵ１９において運用面がＡ面であり、非運用面がＢ面であれば、書込みデータを非運用面であるＢ面に書込んで新アプリプログラムをインストールするが、Ａ面からＢ面への運用面の切替えを抑制する方法（第３ロールバック処理）を特定する。

[0415] （１５－２）キャンセル要求の判定処理

ＣＧＷ１３は、書換え対象ＥＣＵ１９においてアプリプログラムの書換えが開始されたと特定すると、キャンセル要求の判定処理を開始し、アプリプログラムの書換えが完了されたか否かを判定し（Ｓ１５１１）、キャンセル要求が発生したか否かを判定する（Ｓ１５１２）。即ち、ＣＧＷ１３は、上記したように、ユーザによる操作、システムの異常発生等によりキャンセル要求が発生したか否かを判定する。

[0416] ＣＧＷ１３は、アプリプログラムの書換えが完了される前にキャンセル要求が発生した、即ち、インストール中にキャンセル要求が発生したと判定すると（Ｓ１５１２：ＹＥＳ）、ロールバック対象の書換え対象ＥＣＵ１９を特定する（Ｓ１５１３）。同一グループに属する書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）であり、ＥＣＵ（ＩＤ１）が１面単独メモリ、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）が２面メモリであり、ＥＣＵ（ＩＤ１）へのインストールが完了し、ＥＣＵ（ＩＤ２）へのインストール途中でキャンセル要求が発生したとする。この場合、ＣＧＷ１３は、Ｓ１４１３において、第１グループに属する書換え対象ＥＣＵ１９全てについてロールバックの要否を判定する。

[0417] ＣＧＷ１３は、アプリプログラムの書換えが全部行われたＥＣＵ（ＩＤ１）及び一部行われたＥＣＵ（ＩＤ２）がロールバック対象であると特定する。ＣＧＷ１３は、その特定したロールバック対象の書換え対象ＥＣＵ１９のフラッシュメモリのメモリ種別を判定し、フラッシュメモリが１面単独メモリ、１面サスペンドメモリ及び２面メモリのうち何れであるかを判定する（Ｓ１５１４，Ｓ１５１５）。ＣＧＷ１３は、フラッシュメモリが１面単独メモリであると判定すると（Ｓ１５１４：ＹＥＳ）、ロールバックプログラムのデータ種別を判定し、ロールバック用書込みデータが全データ及び差分データのうち何れであるかを判定する（Ｓ１５１６，Ｓ１５１７）。

[0418] ＣＧＷ１３は、ロールバック用書込みデータが全データであると判定すると（Ｓ１５１６：ＹＥＳ）、第１ロールバック処理に移行する（Ｓ１５１８

、ロールバック実行手順に相当する）。ＣＧＷ１３は、第１ロールバック処理を開始すると、新プログラムである書込みデータの配信を即時中断する（Ｓ１５３１）。そして、ＣＧＷ１３は、ＤＣＭ１２から全データであるロールバック用書込みデータ（旧プログラム）を取得し、書換え対象ＥＣＵ１９に配信する。書換え対象ＥＣＵ１９は、ＣＧＷ１３から取得した旧アプリプログラムのデータをフラッシュメモリに書込んで旧アプリプログラムに書換え（Ｓ１５３２）、第１ロールバック処理を終了し、キャンセル要求の判定処理に戻る。

[0419] ＣＧＷ１３は、ロールバック用書込みデータが差分データであると判定すると（Ｓ１５１７：ＹＥＳ）、第２ロールバック処理に移行する（Ｓ１５１９、ロールバック実行手順に相当する）。ＣＧＷ１３は、第２ロールバック処理を開始すると、新プログラムである書込みデータの配信を継続し（Ｓ１５４１）、書換え対象ＥＣＵ１９において差分データを復元してフラッシュメモリに書込んで、新アプリプログラムに書換える（Ｓ１５４２）。ＣＧＷ１３は、新アプリプログラムへに書換え完了後に、ＤＣＭ１２から取得した旧アプリプログラムの書込みデータを書換え対象ＥＣＵ１９に配信する（Ｓ１５４３）。書換え対象ＥＣＵ１９において旧アプリプログラムの書込みデータである差分データを復元し、フラッシュメモリに書込んで旧アプリプログラムに書換え（Ｓ１５４４）、第２ロールバック処理を終了し、キャンセル要求の判定処理に戻る。

[0420] ＣＧＷ１３は、書換え対象ＥＣＵ１９が１面サスペンドメモリＥＣＵ又は２面メモリＥＣＵであると判定すると（Ｓ１５１５：ＹＥＳ）、第３ロールバック処理に移行する（Ｓ１５２０、ロールバック実行手順に相当する）。この場合、ＣＧＷ１３は、書換えデータ種別に依らず、第３ロールバック処理に移行する。ＣＧＷ１３は、第３ロールバック処理を開始すると、その書込みデータの配信を継続し（Ｓ１５５１）、書換え対象ＥＣＵ１９において書込みデータを非運用面（Ｂ面）に書込んで新アプリプログラムに書換える（Ｓ１５５２）。ＣＧＷ１３は、旧面（運用面：Ａ面）から新面（非運用面

：Ｂ面）への運用面の切替えを抑制し（Ｓ１５５３）、第３ロールバック処理を終了し、キャンセル要求の判定処理に戻る。尚、ＣＧＷ１３は、運用面の切替え抑制に加え、図１２６に示すように、バージョン２．０が書込まれている非運用面を新アプリプログラムに書換える前の状態（例えばバージョン１．０）に書き戻しても良い。

[0421] ＣＧＷ１３は、キャンセル要求の判定処理に戻ると、全てのロールバック対象の書換え対象ＥＣＵ１９についてロールバック処理を行ったか否かを判定する（Ｓ１５２１）。ＣＧＷ１３は、例えば前述した書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）の場合の例示では、まず、インストール途中であった１面単独メモリのＥＣＵ（ＩＤ１）に対し、ロールバック用データ種別に応じて、第１ロールバック処理又は第２ロールバック処理を行う。その後、ＣＧＷ１３は、インストールが完了していた２面メモリのＥＣＵ（ＩＤ２）に対し、第３ロールバック処理を行う。

[0422] 加えて、ＣＧＷ１３は、１面単独メモリであるＥＣＵ（ＩＤ１）に対し、書換えデータ種別に応じて、第１ロールバック処理又は第２ロールバック処理を行う。ＣＧＷ１３は、全てのロールバック対象の書換え対象ＥＣＵ１９についてロールバック処理を行っていない判定すると（Ｓ１５２１：ＮＯ）、ステップＳ１５１３に戻り、ステップＳ１５１３以降を繰返す。ＣＧＷ１３は、全てのロールバック対象の書換え対象ＥＣＵ１９についてロールバック処理を行ったと判定すると（Ｓ１５２１：ＹＥＳ）、キャンセル要求の判定処理を終了する。ＣＧＷ１３は、ロールバック処理を行った第１グループに属するＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に対し、旧アプリプログラムのアクティベートを同時に指示する。１面単独メモリであるＥＣＵ（ＩＤ１）は、再起動することにより、旧アプリプログラムへ切替える。２面メモリであるＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）は、更新プログラムが書込まれた非運用面（Ｂ面）でなく、これまでと同じ運用面（Ａ面）にて起動する。尚、ユーザの意向が変化し、やはりプログラム更新

を実行するとなった際は、ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ３）には新アプリプログラムを書込むが、ＥＣＵ（ＩＤ２）には、既に非運用面に新アプリプログラムがインストール済みであるため、書込みは省略される。

[0423] ＣＧＷ１３は、キャンセル要求が発生せずにアプリプログラムの書換えが完了されたと判定すると（Ｓ１５１１：ＹＥＳ）、アクティベートが完了されたか否かを判定し（Ｓ１５２２）、キャンセル要求が発生したか否かを判定する（Ｓ１５２３）。

[0424] ＣＧＷ１３は、アクティベートが完了される前にキャンセル要求が発生した、即ち、アクティベート中にキャンセル要求が発生したと判定すると（Ｓ１５２３：ＹＥＳ）、アクティベートの指示が書換え対象ＥＣＵ１９に到達されたか否かを判定し、運用面の切替えが完了したか否かを判定する（Ｓ１５２４）。

[0425] ＣＧＷ１３は、アクティベートの指示が書換え対象ＥＣＵ１９に到達されていないと判定し、運用面の切替えが完了していないと判定すると（Ｓ１５２４：ＮＯ）、第４ロールバック処理を行う（Ｓ１５２５）。ＣＧＷ１３は、第４ロールバック処理として、運用面を切替えないとする。又は、ＣＧＷ１３は、運用面を切替えずに非運用面を新アプリプログラムに書換える前の状態に戻しても良い。ＣＧＷ１３は、運用面を切替えない場合には、図１２７に示すように、バージョン１．０が書込まれている面を運用面のままとし、バージョン２．０が書込まれている面を非運用面のままとする。ＣＧＷ１３は、運用面を切替えずに非運用面を新アプリプログラムに書換える前の状態に戻す場合は、図１２８に示すように、バージョン１．０が書込まれている面を運用面のままとし、バージョン２．０が書込まれている面である非運用面を新アプリプログラムに書換える前の状態に（バージョン１．０）に書き戻す。

[0426] ＣＧＷ１３は、アクティベートの指示が書換え対象ＥＣＵ１９に到達されたと判定し、運用面の切替えが完了したと判定すると（Ｓ１５２４：ＹＥＳ）、第５ロールバック処理を行う。運用面の切替えが完了とは、図１２９に

示すように、バージョン２．０が書込まれた面が非運用面から運用面に切り替わり、バージョン１．０の面が運用面から非運用面に切り替わった状態を示す。ＣＧＷ１３は、第５ロールバック処理として、運用面を切替えるか、又は非運用面を新アプリプログラムに書換える前の状態に戻してから運用面を切替える。ＣＧＷ１３は、運用面を切替える場合には、図１２９に示すように、バージョン２．０が書込まれている面を運用面から非運用面に切替え、バージョン１．０が書込まれている面を非運用面から運用面に切替える。ＣＧＷ１３は、非運用面を新アプリプログラムに書換える前の状態に戻してから運用面を切替える場合には、図１３０に示すように、バージョン２．０が書込まれている面である運用面を新アプリプログラムに書換える前の状態（例えばバージョン１．０）に書き戻し、その新アプリプログラムに書換える前の状態に戻した面を運用面から非運用面に切替え、バージョン１．０が書込まれている面を非運用面から運用面に切替える。

[0427] 以上に説明したように、ＣＧＷ１３は、ロールバックの実行制御処理を行うことで、アプリプログラムの書換え中に書換えのキャンセル要求が発生すると、書換え対象ＥＣＵ１９の動作状態を、ユーザから見てそのアプリプログラムの書換えを開始する前の状態となるように復帰させる。これにより、同一グループに属する書換え対象ＥＣＵ１９全てを同時に、元のプログラムバージョンに戻すことができる。又、次のプログラム更新にて差分データを用いる場合であっても、正しく書込みデータを復元することができる。

[0428] （１６）書換え進捗状況の表示制御処理

書換え進捗状況の表示制御処理について図１３１から図１４３を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において書換え進捗状況の表示制御処理を行う。ユーザにアプリプログラムの書換えの進捗状況を伝えるため、表示端末５である携帯端末６や車載ディスプレイ７は、進捗状況を表示する。表示する進捗状況としては、プログラムを更新する場合だけでなく、例えばユーザのキャンセル操作や更新失敗等によりロールバックする場合も含む。

[0429] 図１３１に示すように、ＣＧＷ１３は、書換え進捗状況の表示制御部８７において、キャンセル検出部８７ａと、書込み指示部８７ｂと、報知指示部８７ｃとを有する。キャンセル検出部８７ａは、書換え対象ＥＣＵ１９に記憶されている第１書込みデータを、センター装置３から取得された第２書込みデータに書換えるプログラムの書換えに関し、キャンセルを検出する。キャンセル検出部８７ａは、例えばユーザによるキャンセル操作や、書換え対象ＥＣＵ１９への書込み失敗等の異常を検出する。キャンセル検出部８７ａは、書換え対象ＥＣＵ１９に不適合な書込みデータであった場合や、書込みデータに改ざんを検知した場合、書換え対象ＥＣＵ１９への書込みエラーが発生した場合など、所定の異常を検出した場合もロールバック処理が行われるため、これら異常の検出もキャンセルの検出とみなす。

[0430] 書込み指示部８７ｂは、第２書込みデータを書換え対象ＥＣＵ１９に配信し、第２書込みデータの書込みを指示する。報知指示部８７ｃは、アプリプログラムの書換えに関する進捗状況の報知を指示する。報知指示部８７ｃは、書込み指示部８７ｂにより第２書込みデータを配信中に、アプリプログラムの書換えに関する進捗状況を第１態様により報知するように指示し、キャンセル検出部８７ａによりキャンセルを検出すると、アプリプログラムの書換えに関する進捗状況を第２態様により報知するように指示する。書込み指示部８７ｂは、第２書込みデータを配信中に、キャンセル検出部８７ａによりキャンセルを検出すると、第２書込みデータの配信を継続する。

[0431] ＣＧＷ１３は、書換え対象ＥＣＵ１９の内部状態を特定すること、センター装置３からの指示を特定すること、ユーザ操作を特定することのうち何れかにより、書換え対象ＥＣＵ１９におけるアプリプログラムの書換えを特定する。ＣＧＷ１３は、アプリプログラムの書換えが特定されると、通常時の書換え（インストール）であるかロールバック時の書換え（アンインストール）であるかを判定する。ＣＧＷ１３は、書換え対象ＥＣＵ１９の内部状態を特定すること、センター装置３からの指示を特定すること、ユーザ操作を特定することのうち何れかにより、通常時の書換えであるかロールバック時

の書換えであるかを判定すると、その判定結果により通常時又はロールバック時の書換えの進捗状況を演算し、その演算した進捗状況の表示を表示端末５に指示する。

[0432] ＣＧＷ１３は、通常時の書換えかロールバック時の書換えかを示す書換え判定結果に応じて通常時の進捗状況又はロールバック時の進捗状況の表示を表示端末５に指示する。ＣＧＷ１３は、通常時の書換えの進捗状況を示す進捗表示と、ロールバック時の書換えの進捗状況を示す進捗表示とを区別するように表示を指示する。即ち、ＣＧＷ１３は、通常時の書換えの場合は第１の態様で進捗状況を表示し、ロールバック時の書換えの場合は、第１の態様と異なる第２の態様で進捗状況を表示する。ＣＧＷ１３は、進捗状況を表示させる際の表示に関する態様として、表示画面における文字、項目、色、数値、点滅等を通常時とロールバック時とで区別することで、通常時の進捗表示とロールバック時の進捗表示とを区別する。又、ＣＧＷ１３は、進捗表示を表示させる際の表示以外に関する態様として、音、振動等を通常時とロールバック時とで区別することで、通常時の進捗表示とロールバック時の進捗表示とを区別する。

[0433] 次に、ＣＧＷ１３の作用について図１３２から図１４３を参照して説明する。ＣＧＷ１３は、書換え進捗状況の表示制御プログラムを実行し、書換え進捗状況の表示制御処理を行う。

[0434] ＣＧＷ１３は、書換え対象ＥＣＵ１９においてプログラムの書換えが開始された旨を示す書換え開始信号を受信すると（書換え対象ＥＣＵ１９へのインストールが開始されると）、書換え進捗状況の表示制御処理を開始する。ＣＧＷ１３は、書換え進捗状況の表示制御処理を開始すると、ＣＧＷ用の書換え諸元データを解析し、書換え対象ＥＣＵ１９のフラッシュメモリのメモリ種別及び書込みデータ種別を特定し、通常時の書換え対象ＥＣＵ１９を特定する（Ｓ１６０１）。ＣＧＷ１３は、書換え対象ＥＣＵ１９のフラッシュメモリのメモリ種別、書込みデータ種別及び更新プログラムのサイズを特定すると（Ｓ１６０２）、その特定結果にしたがって通常時の書換え進捗状況

を演算し、その演算した通常時の書換え進捗状況の表示を指示する（Ｓ１６０３）。表示端末５は、ＣＧＷ１３からの指示にしたがって通常時の書換え表示態様で表示する。

[0435] ＣＧＷ１３は、アプリプログラムの書換えが完了されたか否かを判定し（Ｓ１６０４）、キャンセル要求が発生したか否かを判定する（Ｓ１６０５、キャンセル検出手順に相当する）。ＣＧＷ１３は、例えば書換え対象ＥＣＵ（ＩＤ１）へのインストール中において、Ｓ１６０４及びＳ１６０５を繰返し、進捗状況を随時更新して表示する。

[0436] ＣＧＷ１３は、書換え対象ＥＣＵ１９においてアプリプログラムの書換えが完了された旨を示す書換え完了信号を受信し、キャンセル要求が発生せずにアプリプログラムの書換えが完了されたと判定すると（Ｓ１６０４：ＹＥＳ）、通常時の書換え進捗状況の表示を終了し（Ｓ１６０６）、全ての書換え対象ＥＣＵ１９について書換えを完了したか否かを判定する（Ｓ１６０７）。ＣＧＷ１３は、例えば書換え対象ＥＣＵ（ＩＤ１）のインストールが完了した場合、ＥＣＵ（ＩＤ１）の進捗状況を１００％として表示しておく。ＣＧＷ１３は、全ての書換え対象ＥＣＵ１９について未だ書換えを完了していないと判定すると（Ｓ１６０７：ＮＯ）、ステップＳ１６０１に戻り、ステップＳ１６０１以降を繰返す。ＣＧＷ１３は、例えばＳ１６０１以降において、次にインストールする書換え対象ＥＣＵ（ＩＤ２）についての進捗表示を行う。

[0437] ＣＧＷ１３は、アプリプログラムの書換えが完了される前にキャンセル要求が発生したと判定すると（Ｓ１６０５：ＹＥＳ）、通常時の書換え進捗状況の表示を終了し（Ｓ１６０８）、ロールバック時の表示制御処理に移行する（Ｓ１６０９、報知指示手順に相当する）。ここで、キャンセル要求とは、ユーザによるキャンセル要求と、書換え対象ＥＣＵ１９への書込み失敗等に基づくシステムによるキャンセル要求とを含む。

[0438] ＣＧＷ１３は、ロールバック時の表示制御処理を開始すると、ロールバック時の書換え対象ＥＣＵ１９を特定し（Ｓ１６１１）、そのロールバック時

の書換え対象ＥＣＵ１９のフラッシュメモリのメモリ種別、ロールバックプログラムのデータ種別及びサイズを特定する（Ｓ１６１２）。ＣＧＷ１３は、例えば同一グループに属する書換え対象ＥＣＵ１９がＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）であり、ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）のインストールが完了し、ＥＣＵ（ＩＤ３）のインストール途中でキャンセル要求が発生したとする。この場合、ＣＧＷ１３は、各書換え対象ＥＣＵ１９のメモリ種別及び書込みデータ種別に応じて、ロールバックの要否及びロールバック方法を特定する。

[0439] ＣＧＷ１３は、ロールバック対象となる書換え対象ＥＣＵ１９のフラッシュメモリのメモリ種別及び書込みデータ種別を特定し、ロールバックの要否及びロールバック方法を特定する（前述したＳ１５１８の第１ロールバック処理、Ｓ１５１９の第２ロールバック処理、Ｓ１５２０の第３ロールバック処理）。ＣＧＷ１３は、その特定結果にしたがって進捗状況を演算し、進捗状況を表示すると共に、ロールバック時の書換え進捗状況の表示を指示する（Ｓ１６１３）。ＣＧＷ１３は、第１～第３ロールバック処理のそれぞれによりって、書込むデータ量が異なってくる。そのため、ＣＧＷ１３は、第１～第３ロールバック処理に応じて書込みデータ総量を決定し、書込んだデータ量との割合から進捗（何％書込んだか）を演算する。ＣＧＷ１３は、ロールバック処理としてのアプリプログラムの書換えが完了されたか否かを判定する（Ｓ１６１４）。

[0440] ＣＧＷ１３は、ロールバック処理としての書換えが完了するまで書換え対象ＥＣＵ１９へ書込みデータを配信すると共に、前述した進捗の演算と表示指示とを繰返す。ＣＧＷ１３は、Ｓ１６１３において、ロールバック時の表示態様にて、演算した進捗状況を表示する。ＣＧＷ１３は、Ｓ１６１４において、例えば書換え途中であったＥＣＵ（ＩＤ３）のロールバックが正常に完了したか否かを判定する。

[0441] ＣＧＷ１３は、ロールバック対象の書換え対象ＥＣＵ１９に対するロールバックが完了したと判定すると（Ｓ１６１４：ＹＥＳ）、ロールバック時の

書換え進捗状況の表示を終了する（Ｓ１６１５）。ＣＧＷ１３は、例えばＥＣＵ（ＩＤ３）についてはロールバックが１００％完了した旨の表示を継続する。

[0442] ＣＧＷ１３は、全てのロールバック対象ＥＣＵ１９について、ロールバック時の書換えが完了したか否かを判定する（Ｓ１６１６）。ＣＧＷ１３は、全てのロールバック対象ＥＣＵ１９について、ロールバック時の書換えが完了していないと判定すると（Ｓ１６１６：ＮＯ）、ステップＳ１６１１に戻り、ステップＳ１６１１以降を繰返す。

[0443] ＣＧＷ１３は、例えばインストールが完了したＥＣＵ（ＩＤ１）が１面単独メモリの場合、ロールバック時の書換え進捗状況の表示を行う（Ｓ１６１３）。一方、例えばインストールが完了したＥＣＵ（ＩＤ２）が２面メモリでロールバックが不要な場合、ロールバック時の書換え対象からＥＣＵ（ＩＤ２）を除外する。ＣＧＷ１３は、ＥＣＵ（ＩＤ３）及びＥＣＵ（ＩＤ１）のロールバックが完了すると、全てのロールバック対象の書換え対象ＥＣＵ１９について書換え完了となり（Ｓ１６１６：ＹＥＳ）、ロールバック時の表示制御処理を終了する。

[0444] 尚、上述した説明では、ＣＧＷ１３がロールバック時の表示制御処理を行うこととしたが、ＣＧＷ１３から必要な情報を取得しつつ、車載ディスプレイＥＣＵ７やセンター装置３がロールバック時の表示制御処理を行うように構成しても良い。又、ロールバック時の書換えや進捗演算等をＣＧＷ１３で行い、ロールバック時の表示制御を車載ディスプレイＥＣＵ７やセンター装置３で行うよう構成しても良い。即ち、表示制御装置の機能をＣＧＷ１３だけが有する構成に限らず、表示制御装置の機能をＣＧＷ１３と車載ディスプレイＥＣＵ７とで分散して有する構成でも良いし、表示制御装置の機能をＣＧＷ１３とセンター装置３とで分散して有する構成でも良い。

[0445] 以下、書換え進捗状況の表示について図１３４から図１４２を参照して説明する。表示端末５は、通常時の書換え進捗状況の表示では、図１３４に示すように、全体進捗状況を「通常書換え」として表示し、通常時の書換え進

捗状況の表示であることをユーザに把握させる。「通常書換え」を「インストール」と表示しても良い。表示端末５は、第１態様として、通常時の書換え進捗状況の表示を行う。

[0446] 表示端末５は、アプリプログラムの書換えを完了し、更新プログラムをアクティベートする同期指示待ちの状態にある書換え対象ＥＣＵ１９については進捗状態を「同期指示待ち」として表示し、書換え中の状態にある書換え対象ＥＣＵ１９については進捗状態を「通常書換え中」として表示する。「同期待ち指示」を「アクティベート待ち」と表示しても良い。「通常書換え中」を「インストール中」と表示しても良い。図１３４は、ＥＣＵ（ＩＤ０００１）及びＥＣＵ（ＩＤ０００２）がアプリプログラムの書換えを完了して同期指示待ちの状態であり、ＥＣＵ（ＩＤ０００３）が通常書換え中の状態である場合を例示している。

[0447] 表示端末５は、この状態からキャンセル要求が発生すると、図１３５に示すように、例えば「キャンセルを受付けました。書換え前の状態に復元します。しばらくお待ちください。」というメッセージをポップアップ表示し、キャンセルを受付けたことをユーザに把握させる。表示端末５は、第２態様として、キャンセルを受付けた旨の表示を行う。

[0448] 表示端末５は、ＣＧＷ１３によりロールバック時の書換えの準備を完了すると、図１３６に示すように、全体進捗状況を「ロールバック書換え」として表示し、ロールバック時の書換え進捗状況の表示であることをユーザに把握させる。「ロールバック書換え」を「アンインストール」として表示しても良い。表示端末５は、全ての書換え対象ＥＣＵ１９について進捗状態を「ロールバック待ち」として表示し、書換え状況の進捗を示す進捗グラフの数値を「０％」として表示する。「ロールバック待ち」を「アンインストール待ち」と表示しても良い。ここでは、ＥＣＵ（ＩＤ０００１）及びＥＣＵ（ＩＤ０００２）が１面単独メモリＥＣＵ、ＥＣＵ（ＩＤ０００３）が２面メモリＥＣＵの例であり、書換え途中だったＥＣＵ（ＩＤ０００３）に加え、インストールが完了したＥＣＵ（ＩＤ０００１）及びＥＣＵ（ＩＤ０００２

）についてもロールバックが必要となる。図１３６では、全体進捗状況を１つ示すと共に、各書換え対象ＥＣＵ１９の進捗状況をそれぞれ表示する態様である。

[0449] ＣＧＷ１３は、ロールバック時の書換えを開始すると、図１３７に示すように、書換え中の状態にある書換え対象ＥＣＵ１９について進捗状態を「ロールバック書換え中（もしくはアンインストール中）」として表示する。表示端末５は、第３態様として、ロールバック時の書換え進捗状況の表示を行う。図１３７は、ＥＣＵ（ＩＤ０００３）がロールバック書換え中の状態にある場合を例示している。表示端末５は、書換え対象ＥＣＵ１９でのロールバックが完了すると、図１３８に示すように、書換えを完了した書換え対象ＥＣＵ１９について進捗状態を「ロールバック完了」として進捗状況を１００％で表示する。

[0450] 表示端末５は、ロールバック対象ＥＣＵ１９が１面単独メモリＥＣＵであり、全データの書換えである場合、図１３９に示すように、進捗グラフの表示を遷移させる。即ち、ロールバック対象ＥＣＵ１９が１面単独メモリＥＣＵであり、全データの書換えである場合には、全データの配信を即時中断し、書換え対象ＥＣＵ１９において旧アプリプログラムのデータをフラッシュメモリに書込んで旧アプリプログラムに書換える（第１ロールバック処理）。

[0451] 表示端末５は、例えば通常書換えが「５０％」まで完了した段階でキャンセル要求が発生すると（図１３９（ａ））、進捗グラフの数値を「０％」として表示し（図１３９（ｂ））、旧アプリプログラムのデータを書込む進捗に応じて進捗グラフの数値を増加させ、旧アプリプログラムに書換える（図１３９（ｃ）、（ｄ）、（ｅ））。表示端末５は、旧アプリプログラムへの書換えが１００％完了すると、その書換え対象ＥＣＵ１９が「ロールバック完了」した旨を表示する。尚、図１３９及び以降に説明する図１４０～１４２は、個々のＥＣＵの進捗表示を示すものである。

[0452] 表示端末５は、ロールバック対象ＥＣＵ１９が１面単独メモＥＣＵであり

、差分データの書換えである場合、図１４０又は図１４１に示すように、進捗グラフの表示を遷移させる。即ち、ロールバック対象ＥＣＵ１９が１面単独メモリであり、差分データの書換えである場合には、ＣＧＷ１３は差分データの配信を継続し、書換え対象ＥＣＵ１９において差分データをフラッシュメモリに書込んで新アプリプログラムに書換える。ＣＧＷ１３は、旧アプリプログラムのデータを書換え対象ＥＣＵ１９に配信し、書換え対象ＥＣＵ１９において旧データをフラッシュメモリに書込んで旧アプリプログラムに書換える（第２ロールバック処理）。

[0453] 表示端末５は、例えば通常書換え（インストール）が「５０％」まで完了した段階でキャンセル要求が発生すると（図１４０（ａ）、図１４１（ａ））、進捗グラフの数値を「０％」として表示する（図１４０（ｂ）、図１４１（ｂ））。書換え対象ＥＣＵ１９は、それまでに書込んでいた差分データを有効とし、ＣＧＷ１３から配信される差分データの書込みを引続き行う。即ち、「０％」の表示から、有効とされた「５０％」に相当する割合はインストールが完了しているという進捗表示に切替える（図１４０（ｃ）、図１４１（ｃ））。表示端末５は、ＣＧＷ１３から配信される新プログラムの差分データを書換え対象ＥＣＵ１９が書込む進捗に応じて進捗グラフの数値を増加させる（図１４０（ｄ）、（ｅ）、図１４１（ｄ）、（ｅ））。表示端末５は、書換え対象ＥＣＵ１９が新アプリプログラムの書換えを完了した後に引続いて、ＣＧＷ１３から配信される旧アプリプログラムの差分データを書換え対象ＥＣＵ１９が書込む進捗に応じて、進捗グラフの数値を増加させる（図１４０（ｆ）、（ｇ）、図１４１（ｆ）、（ｇ））。即ち、表示端末５は、ロールバック処理として、新プログラムの継続インストール及び旧プログラムのインストールが発生することに合わせ、新プログラム書込みの進捗状況と旧プログラム書込みの進捗状況とが分かるように表示する。

[0454] この場合、表示端末５は、図１４０に示すように、新アプリプログラムの書換え分として左側の進捗グラフを「１００％」と表示し、旧アプリプログラムの書換え分として右側の進捗グラフを「１００％」と表示することで、

進捗グラフの幅全体を「２００％」としても良い。この場合、表示端末５は、新アプリプログラムのファイルサイズと書込んだ新アプリプログラムの累積データサイズとから、新アプリプログラムの進捗パーセントを演算し、旧アプリプログラムのファイルサイズと書込んだ旧アプリプログラムの累積データサイズとから旧アプリプログラムの進捗パーセントを演算し、進捗状況を表示する。

[0455] 又、表示端末５は、図１４１に示すように、新アプリプログラムの書換え分を「５０％」とし、旧アプリプログラムの書換え分を「５０％」とすることで、進捗グラフの幅全体を「１００％」としても良い。この場合、表示端末５は、新アプリプログラムのファイルサイズと旧アプリプログラムのファイルサイズとの合算値と、書込んだ新アプリプログラムの累積データサイズと旧アプリプログラムの累積データサイズとの合算値とから、進捗パーセントを演算して表示する。

[0456] 表示端末５は、ロールバック対象ＥＣＵ１９が１面サスペンドメモリＥＣＵ又は２面メモリＥＣＵの書換えである場合、図１４２に示すように、進捗グラフの表示を遷移させる。即ち、ロールバック対象ＥＣＵ１９が１面サスペンドメモリＥＣＵ又は２面メモリＥＣＵの書換えである場合、ＣＧＷ１３は、書換え対象ＥＣＵ１９に書込みデータの配信を継続し、書換え対象ＥＣＵ１９において書込みデータを非運用面に書込んで新アプリプログラムに書換える（第３ロールバック処理）。

[0457] 表示端末５は、例えば通常書換え（インストール）が「５０％」まで完了した段階でキャンセル要求が発生すると（図１４２（ａ））、進捗グラフの数値を「０％」として表示する（図１４２（ｂ））。書換え対象ＥＣＵ１９は、それまでに書込んでいた差分データを有効とし、ＣＧＷ１３から配信される差分データの書込みを引続き行う。即ち、「０％」の表示から、有効とされた「５０％」に相当する割合はインストールが完了しているという進捗表示に切り替える（図１４２（ｃ））。表示端末５は、ＣＧＷ１３から配信される書込みデータを書換え対象ＥＣＵ１９が書込む進捗に応じて進捗グラ

フの数値を増加させる（図１４２（ｄ）、（ｅ））。尚、本実施形態では、ＣＧＷ１３が書換え進捗状況の表示制御処理を行う旨を説明したが、表示端末５が書換え進捗状況の表示制御処理を行う構成でも良い。

[0458] 以上に説明したように、表示端末５は、書換え進捗状況の表示制御処理を行うことで、ロールバック処理をふまえた上で、アプリプログラムの書換えが通常時の書換え（インストール）であるかロールバック時の書換え（アンインストール）であるかを区別した表示態様にて進捗状況を表示する。ユーザは、更新プログラムのキャンセルが受け付けられ、ロールバックが進行していることを把握することができる。尚、以上は、書換え対象ＥＣＵ１９毎に進捗状態を表示する構成を説明したが、図１４３に示すように、書換え対象ＥＣＵ１９を纏めて進捗状態を表示する構成でも良い。この場合、表示端末５は、３個の書換え対象ＥＣＵ１９に対する進捗表示を個別でなく１つの進捗状態として表示する。ＣＧＷ１３は、ロールバック処理として３個の書換え対象ＥＣＵ１９で発生する書込みデータ総量に対する書込み済みデータ量の割合から進捗を演算する。

[0459] （１７）差分データの整合性判定処理

差分データの整合性判定処理について図１４４から図１４７を参照して説明する。車両用プログラム書換えシステム１は、書換え対象ＥＣＵ１９においてインストールを開始する前に差分データの整合性判定処理を行う。

[0460] 図１４４に示すように、ＥＣＵ１９は、差分データの整合性判定部１０３において、差分データ取得部１０３ａと、整合性判定部１０３ｂと、書込みデータ復元部１０３ｃと、データ書込み部１０３ｄと、データ検証値算出部１０３ｅと、書換え諸元データ取得部１０３ｆと、データ識別情報取得部１０３ｇと、書換え面情報取得部１０３ｈとを有する。

[0461] 差分データ取得部１０３ａは、書換え対象ＥＣＵ１９の電子制御装置のデータ格納領域を書換えるためのデータであって旧データと新データとの差分を示す差分データを取得する。整合性判定部１０３ｂは、フラッシュメモリのデータ格納領域に記憶されている格納データに関する第１判定情報と、差

分データに紐づく形で取得された第２判定情報とに基づいて、差分データがデータ格納領域又は格納データに整合するか否かを判定する。例えば第１判定情報は格納データに対するデータ検証値であり、第２判定情報は旧データに対するデータ検証値又は新データに対するデータ検証値である。書込みデータ復元部１０３ｃは、差分データの整合性が正であると整合性判定部１０３ｂにより判定されると、差分データと格納データとを用いて書込みデータを復元し、差分データの整合性が否であると整合性判定部１０３ｂにより判定されると、書込みデータを復元しない。データ書込み部１０３ｄは、書込みデータが書込みデータ復元部１０３ｃにより復元されると、その復元された書込みデータをデータ格納領域に格納する。データ検証値算出部１０３ｅは、格納データを１以上に分割した各ブロックに対するデータ検証値を算出する。又、データ検証値算出部１０３ｅは、差分データと共に受信された各ブロックに対するデータ検証値を取得する。

[0462] 書換え諸元データ取得部１０３ｆは、ＣＧＷ１３からＣＧＷ用の書換え諸元データのうち自己に該当する書換え諸元データを取得する。データ識別情報取得部１０３ｇは、差分データに格納されているデータ識別情報と、旧データである旧アプリプログラムのデータ識別情報とを取得する。データ識別情報とは、差分データが自己のためのデータであるか否かを識別可能な情報であり、例えば旧データに所定のアルゴリズムを適用して算出したデータである。

[0463] 書換え面情報取得部１０３ｈは、ＣＧＷ１３から取得した書換え諸元データに格納されている書換え面情報と、旧データである旧アプリプログラムの書換え面情報とを取得する。書換え面情報とは、書込みデータである差分データがフラッシュメモリの何れの面に書込むためのデータであるかを示す情報であり、書換え対象ＥＣＵ１９が２面メモリ又は１面サスペンドメモリの場合に、Ａ面又はＢ面が指定される。書換え対象ＥＣＵ１９が１面単独メモリの場合には書換え面情報は使用しない。整合性判定部１０３ｂは、ＣＧＷ１３より配信される差分データが書込みデータ受信部１０１により受信され

ると、その差分データの整合性を、データ識別情報、データ検証値、書換え面情報の少なくとも何れか一つを用いて判定する。

[0464] 次に、書換え対象ＥＣＵ１９における差分データの整合性判定部１０３の作用について図１４５から図１４７を参照して説明する。書換え対象ＥＣＵ１９は、差分データの整合性判定プログラムを実行し、差分データの整合性判定処理を行う。書換え対象ＥＣＵ１９は、差分データの整合性判定処理を開始すると、差分データの整合性を判定するための第１判定情報として、差分データに関するデータ識別情報、データ検証値及び書換え面情報を取得する（Ｓ１７０１）。書換え対象ＥＣＵ１９は、第２判定情報として、データ識別情報、旧データのデータ検証値、新データのデータ検証値及び書換え面情報を取得する（Ｓ１７０２）。

[0465] 書換え対象ＥＣＵ１９は、第１判定情報のデータ識別情報と第２判定情報のデータ識別情報とが一致し、且つ第１判定情報の書換え面情報と第２判定情報の書換え面情報とが一致するか否かを判定する（Ｓ１７０３）。書換え対象ＥＣＵ１９は、第１判定情報のデータ識別情報と第２判定情報のデータ識別情報とが一致しない、又は第１判定情報の書換え面情報と第２判定情報の書換え面情報とが一致しないと判定すると（Ｓ１７０３：ＮＯ）、不適切な書込みデータであると判定し、エラー情報をＣＧＷ１３に通知し、差分データの整合性判定処理を終了する。

[0466] 書換え対象ＥＣＵ１９は、第１判定情報のデータ識別情報と第２判定情報のデータ識別情報とが一致し、且つ第１判定情報の書換え面情報と第２判定情報の書換え面情報とが一致すると判定すると（Ｓ１７０３：ＹＥＳ）、第１判定情報のデータ検証値と、第２判定情報の新データのデータ検証値とを照合し、両者が一致するか否かを判定する（Ｓ１７０４、整合性判定手順に相当する）。書換え対象ＥＣＵ１９は、両者が一致しないと判定すると（Ｓ１７０４：ＮＯ）、第１判定情報のデータ検証値と、第２判定情報の旧データのデータ検証値とを照合し、両者が一致するか否かを判定する（Ｓ１７０５、整合性判定手順に相当する）。

[0467] 書換え対象ＥＣＵ１９は、両者が一致すると判定すると（Ｓ１７０５：ＹＥＳ）、書込みデータを復元し（Ｓ１７０６、書込みデータを復元手順に相当する）、その復元した書込みデータをフラッシュメモリに書込み（Ｓ１７０７、データ書込み手順に相当する）、全ての書込みを完了したか否かを判定する（Ｓ１７０８）。書換え対象ＥＣＵ１９は、全ての書込みを完了していないと判定すると（Ｓ１７０８：ＮＯ）、ステップＳ１７０３に戻り、ステップＳ１７０３以降を繰返す。書換え対象ＥＣＵ１９は、全ての書込みを完了したと判定すると（Ｓ１７０８：ＹＥＳ）、差分データの整合性判定処理を終了する。

[0468] 書換え対象ＥＣＵ１９は、第１判定情報のデータ検証値と第２判定情報の新データのデータ検証値とが一致しないと判定し（Ｓ１７０４：ＮＯ）、且つ第１判定情報のデータ検証値と第２判定情報の旧データのデータ検証値とが一致しないと判定すると（Ｓ１７０５：ＮＯ）、１ブロック目に対する書込みであるか否かを判定する（Ｓ１７０９）。

[0469] 書換え対象ＥＣＵ１９は、１ブロック目に対する書込みであると判定すると（Ｓ１７０９：ＹＥＳ）、１ブロック目に対する書込みを完了していない状態であるので、全ての書込みを完了したか否かを判定する（Ｓ１７０８）。書換え対象ＥＣＵ１９は、１ブロック目に対する書込みでない、即ち、２ブロック目以降に対する書込みであると判定すると（Ｓ１７０９：ＮＯ）、書込みをリトライし（Ｓ１７１０）、全ての書込みを完了したか否かを判定する（Ｓ１７０８）。

[0470] 書換え対象ＥＣＵ１９が１面単独メモリＥＣＵの場合について図１４６を参照して説明する。ＣＧＷ１３から配信される差分データには、データ識別情報（旧）と、旧データのブロック毎に計算されたＣＲＣ値（データ検証値）とが添付されている。データ識別情報（旧）とは、旧データ（旧アプリプログラム）に所定のアルゴリズムを適用して算出したデータである。書換え対象ＥＣＵ１９は、データ識別情報を判定情報とする場合には、差分データに添付されているデータ識別情報（旧）と、フラッシュメモリに記憶されて

いるプログラム（旧データ）のデータ識別情報（旧）とを照合し、差分データの整合性を判定する。フラッシュメモリに記憶されているデータ識別情報（旧）は、書換え対象ＥＣＵ１９のフラッシュメモリにプログラムを書込む際に、合わせて記憶される情報である。又は、フラッシュメモリに書込まれたプログラムの先頭アドレスから所定ビット数をデータ識別情報（旧）とみなしても良い。

[0471] 書換え対象ＥＣＵ１９は、データ検証値を判定情報とする場合、フラッシュメモリに記憶されているプログラムのブロック毎のＣＲＣ値を計算し、受信した差分データに添付されている旧データに対するＣＲＣ値（ＣＲＣ（Ｂ１～Ｂｎ））及び新データに対するＣＲＣ値（ＣＲＣ（Ｂ１’～Ｂｎ’）と、その計算したＣＲＣ値とを照合し、差分データの整合性を判定する。フラッシュメモリに新プログラムが書込まれていない状態においては、全てのブロックにおいて受信したＣＲＣ値と計算したＣＲＣ値とが一致することとなる。書換え対象ＥＣＵ１９は、フラッシュメモリのｍ（＜ｎ）ブロックまで新プログラムが書込まれた状態において書込みが中断し、再開する場合においては、ブロック１～ｍまでは新データに対するＣＲＣ値（ＣＲＣ（Ｂ１’～Ｂｎ’）と一致するので、書込み処理（Ｓ１７０６，Ｓ１７０７）をスキップする。そして、書換え対象ＥＣＵ１９は、ブロックｍ＋１から、旧データに対するＣＲＣ値（ＣＲＣ（Ｂ１～Ｂｎ））との一致を見て書込み処理（Ｓ１７０６，Ｓ１７０７）を行う。

[0472] 尚、差分データには、新プログラム（新データ）のデータ識別情報（新）及びブロック毎のＣＲＣ値（ＣＲＣ（Ｂ１‘～Ｂｎ’））を添付しておいても良い。書換え対象ＥＣＵ１９は、差分データをフラッシュメモリに書込み、新プログラムのインストールが完了した際、合わせてデータ識別情報（新）も記憶しておき、次回のプログラム更新における整合性判定に用いる。又、書換え対象ＥＣＵ１９は、新プログラムのインストールが完了した際、フラッシュメモリに書込んだ新プログラムをブロック毎に読出してＣＲＣ値を計算し、差分データに添付されたＣＲＣ値と比較し、正しく書込まれたか否

かを検証する。

[0473] 書換え対象ＥＣＵ１９が２面メモリＥＣＵの場合について図１４７を参照して説明する。この場合も、書換え対象ＥＣＵ１９は、データ検証値を判定情報とする場合、フラッシュメモリに記憶されているプログラムのブロック毎のＣＲＣ値を計算し、受信した差分データに添付されている旧データに対するＣＲＣ値（ＣＲＣ（Ｂ１～Ｂｎ））及び新データに対するＣＲＣ値（ＣＲＣ（Ｂ１’～Ｂｎ’）と、その計算したＣＲＣ値とを照合し、差分データの整合性を判定する。フラッシュメモリに新プログラムが書込まれていない状態においては、全てのブロックにおいて受信したＣＲＣ値と計算したＣＲＣ値とが一致することとなる。書換え対象ＥＣＵ１９は、フラッシュメモリのｍ（＜ｎ）ブロックまで新プログラムが書込まれた状態において書込みが中断し、再開する場合においては、ブロック１～ｍまでは新データに対するＣＲＣ値（ＣＲＣ（Ｂ１’～Ｂｎ’）と一致するので、書込み処理（Ｓ１７０６，Ｓ１７０７）をスキップする。そして、書換え対象ＥＣＵ１９は、ブロックｍ＋１から、旧データに対するＣＲＣ値（ＣＲＣ（Ｂ１～Ｂｎ））との一致を見て書込み処理（Ｓ１７０６，Ｓ１７０７）を行う。

[0474] フラッシュメモリのＡ面が運用面且つバージョン２．０であり、Ｂ面が非運用面かつバージョン１．０であり、差分データはＢ面をバージョン３．０へ更新するための差分データ（バージョン１．０とバージョン３．０との差分データ）であるとする。ＣＧＷ１３から配信される差分データには、データ識別情報（旧（バージョン１．０）を示す情報）と、旧データ（旧プログラム（バージョン１．０））のブロック毎に計算されたＣＲＣ値及び新データ（新プログラム（バージョン３．０））のブロック毎に計算されたＣＲＣ値とが添付されている。

[0475] 又、書換え諸元データには、書換え対象ＥＣＵ１９に対する差分データがフラッシュメモリの何れの面に書込むデータかを示す書換え面情報が含まれている。書換え対象ＥＣＵ１９は、書換え面情報を判定情報とする場合、書換え諸元データから取得した書換え面情報と、書換え対象ＥＣＵ１９の非運

用面情報（Ｂ面）とを照合し、差分データの整合性を判定する。書換え対象ＥＣＵ１９は、データ識別情報を判定情報とする場合、差分データに添付されているデータ識別情報（旧（バージョン１．０））と、フラッシュメモリの非運用面（Ｂ面）に記憶されている旧プログラム（バージョン１．０）のデータ識別情報（旧）とを照合し、差分データの整合性を判定する。書換え対象ＥＣＵ１９は、データ検証値を判定情報とする場合、フラッシュメモリの非運用面（Ｂ面）に記憶されている旧プログラム（バージョン１．０）のブロック毎のＣＲＣ値を計算し、差分データに添付されているＣＲＣ値（ＣＲＣ（Ｂ１～Ｂｎ））と、その計算したＣＲＣ値とを照合し、差分データの整合性を判定する。

[0476] 上述した図１４３及び図１４４の例では、データ識別情報及びデータ検証値が差分データに添付されており、差分データと共にＣＧＷ１３から配信されると説明した。しかしながら、これらデータ識別情報及びデータ検証値が差分データのヘッダ情報として添付され、ＣＧＷ１３が差分データを書換え対象ＥＣＵ１９に配信する前に、ヘッダ情報を書換え対象ＥＣＵ１９に配信しても良い。書換え対象ＥＣＵ１９は、ヘッダ情報をＣＧＷ１３から受信した際、データ識別情報及びデータ検証値を用いて差分データの整合性を判定する。

[0477] 尚、図１４３及び図１４４では、書換えデータが差分データである場合を例に説明したが、全データである場合も同様である。又、書換え対象ＥＣＵ１９が１面単独メモリの場合において、ロールバック用の差分データを用いて元のバージョンに戻す際も同様の整合性判定を行う。

[0478] 以上に説明したように、書換え対象ＥＣＵ１９は、差分データの整合性判定処理を行うことで、差分データの整合性が正である場合に限って差分データに基づいて生成された書込みデータの書込みを実行し、差分データの整合性が否である場合に差分データに基づいて生成された書込みデータを書込んでしまう事態を未然に回避する。例えばフラッシュメモリのＢ面が非運用面である書換え対象ＥＣＵ１９に対し、Ａ面に書込むための差分データが配信

パッケージに含まれた場合に、差分データをフラッシュメモリに書込む前に不整合を検知することができる。又、他ＥＣＵ向けの差分データやバージョンが整合しない差分データが自己向けの差分データとして配信パッケージに含まれた場合に、差分データをフラッシュメモリに書込む前に不整合を検知することができる。

[0479] 尚、書換え対象ＥＣＵ１９は、書込みデータの書込みを中断した後に再開する場合には、フラッシュメモリの格納データに対するデータ検証値と、受信した差分データに付随する旧データのデータ検証値及び新データのデータ検証値に基づいて差分データの整合性を判定する。書換え対象ＥＣＵ１９は、格納データに対するデータ検証値と、受信した新データの検証値とに基づいて差分データの整合性を判定し、その判定結果が否であると判定された最終ブロックからは格納データに対するデータ検証値と受信した旧データのデータ検証値とに基づいて差分データの整合性を判定しても良い。

[0480] 又、書換え対象ＥＣＵ１９は、差分データの整合性が否であると判定された最終ブロックの少なくとも前段ブロックまでは書込みデータの書込みをスキップし、最終ブロック又は当該終ブロックの後段ブロックから書込みデータの書込みを再開する。ブロックサイズと、書込みデータの書込み領域のデータサイズとが等しい場合には、最終ブロックまでは書込みデータの書込みを完了しているので、最終ブロックまでの書込みをスキップし、最終ブロックの後段ブロックから書込みを再開すれば良い。一方、ブロックサイズと、書込みデータの書込み領域のデータサイズとが等しくない場合には、最終ブロックでは書込みデータの書込みが中断している可能性があるので、最終ブロックから書込みを再開する必要がある。

[0481] （１８）書換えの実行制御処理

書換えの実行制御処理について図１４８から図１５５を参照して説明する。車両用プログラム書換えシステム１は、ＥＣＵ１９において書換えの実行制御処理を行う。

[0482] 図１４８に示すように、ＥＣＵ１９は、書換えの実行制御部１０４におい

て、プログラム実行部１０４ａと、切替え要求受信部１０４ｂと、データ取得部１０４ｃと、面情報通知部１０４ｄと、ファームウェア取得部１０４ｅと、インストール実行部１０４ｆと、アクティベート実行部１０４ｇとを有する。プログラム実行部１０４ａは、運用面のアプリプログラムやパラメータデータを実行中に、運用面の書換えプログラムを実行して非運用面を書換える。切替え要求受信部１０４ｂは、ＣＧＷ１３からアクティベート要求を受信する。データ取得部１０４ｃは、非運用面のうち書換えを必要とする領域の書込みデータを外部から取得する。面情報通知部１０４ｄは、２面書換え情報（以下、面情報と称する）を外部に通知する。ファームウェア取得部１０４ｅは、外部から書換えプログラムのファームウェアを取得する。インストール実行部１０４ｆは、ＣＧＷ１３からインストールが指示されると、書込みデータをフラッシュメモリに書込み、インストールを実行する。アクティベート実行部１０４ｇは、ＣＧＷ１３からアクティベートが指示されると、再起動時に備えて運用面を切替えるアクティベートを実行する。

[0483] 次に、ＥＣＵ１９における書換えの実行制御部１０４の作用について図１４９から図１５５を参照して説明する。書換え対象ＥＣＵ１９は、書換えの実行制御プログラムを実行し、書換えの実行制御処理を行う。書換え対象ＥＣＵ１９は、書換えの実行制御処理として、通常動作処理、書換え動作処理、情報通知処理、アプリプログラムの検証処理を行う。以下、それぞれの処理について説明する。本実施形態では、書換え対象ＥＣＵ１９が２面メモリＥＣＵ又は１面サスペンドメモリＥＣＵの場合について説明する。

[0484] （１８－１）通常動作処理

書換え対象ＥＣＵ１９は、ＩＧ電源オン等に伴い、停止状態又はスリープ状態から起動状態に移行すると、通常動作処理を開始する。書換え対象ＥＣＵ１９は、通常動作処理を開始すると、Ａ面及びＢ面の起動面判定情報に基づいて起動面を特定し（Ｓ１８０１）、その起動面で起動する（Ｓ１８０２）。書換え対象ＥＣＵ１９は、起動面（運用面）に記憶されているプログラムの完全性を検証し、起動面が正であるか否かを判定する（Ｓ１８０３）。

[0485] 書換え対象ＥＣＵ１９は、起動面の完全性の検証結果が否であると判定し、起動面が否であると判定すると（Ｓ１８０３：ＮＯ）、起動面の完全性の検証結果が否である旨を示すエラー情報をＣＧＷ１３に送信し（Ｓ１８０４）、通常動作処理を終了する。ＣＧＷ１３は、書換え対象ＥＣＵ１９からエラー情報を受信すると、そのエラー情報をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３からエラー情報を受信すると、その受信したエラー情報をセンター装置３にアップロードする。即ち、書換え対象ＥＣＵ１９において起動面の完全性の検証結果が否であると判定すると、その旨がＣＧＷ１３、ＤＣＭ１２、センター装置３に通知される。

[0486] 書換え対象ＥＣＵ１９は、起動面の完全性の検証結果が正であると判定し、起動面が正であると判定すると（Ｓ１８０３：ＹＥＳ）、書換え面（非運用面）に記憶されているプログラムの完全性を検証し、書換え面が正であるか否かを判定する（Ｓ１８０５）。

[0487] 書換え対象ＥＣＵ１９は、書換え面の完全性の検証結果が否であると判定し、書換え面が否であると判定すると（Ｓ１８０５：ＮＯ）、書換え面の完全性の検証結果が否である旨を示すエラー情報をＣＧＷ１３に送信する（Ｓ１８０６）。ＣＧＷ１３は、書換え対象ＥＣＵ１９からエラー情報を受信すると、そのエラー情報をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３からエラー情報を受信すると、その受信したエラー情報をセンター装置３にアップロードする。即ち、書換え対象ＥＣＵ１９において書換え面の完全性の検証結果が否であると判定すると、その旨がＣＧＷ１３、ＤＣＭ１２、センター装置３に通知される。

[0488] 上述した完全性検証の処理は、アプリプログラムを実行する前にブートプログラムが実行する。書換え対象ＥＣＵ１９は、完全性検証を終了すると、ブートベクタテーブルの配置アドレスを特定し（Ｓ１８０７）、通常時ベクタテーブルの配置アドレスを特定し（Ｓ１８０８）、アプリプログラムの先頭アドレスを特定し（Ｓ１８０９）、アプリプログラムを実行し、通常動作処理を終了する。

[0489] （１８－２）書換え動作処理

書換え対象ＥＣＵ１９は、ＣＧＷ１３から書換え要求を受信すると、書換え動作処理を開始する。書換え対象ＥＣＵ１９は、書換え動作処理を開始すると、ＣＧＷ１３との間でセキュリティアクセス鍵を用いて認証を行う（Ｓ１８１１）。書換え対象ＥＣＵ１９は、認証結果が正であると判定すると（Ｓ１８１２：ＹＥＳ）、書込みデータの受信を待機する（Ｓ１８１３）。書換え対象ＥＣＵ１９は、ＣＧＷ１３から書込みデータを受信したと判定すると（Ｓ１８１３：ＹＥＳ）、起動面（運用面）に配置されているアプリプログラムを実行したまま、書換え面（非運用面）に配置されているアプリプログラムを書換える（Ｓ１８１４）。

[0490] 書換え対象ＥＣＵ１９は、アプリプログラムの書換えを完了したか否かを判定し（Ｓ１８１５）、アプリプログラムの書換えを完了したと判定すると（Ｓ１８１５：ＹＥＳ）、ベリファイが正であるか否かを判定する（Ｓ１８１６）。書換え対象ＥＣＵ１９は、ベリファイが正であると判定すると（Ｓ１８１６：ＹＥＳ）、書換え完了フラグを「ＯＫ」に設定する（Ｓ１８１７）。ベリファイとは、非運用面に書込んだアプリプログラムの完全性検証である。

[0491] 書換え対象ＥＣＵ１９は、ＣＧＷ１３からアクティベート要求を受信したか否かを判定する（Ｓ１８１８）。書換え対象ＥＣＵ１９は、ＣＧＷ１３からアクティベート要求を受信したと判定すると（Ｓ１８１８：ＹＥＳ）、例えば書換え面の起動面情報の数値をインクリメントし、書換え面の起動面情報を更新する（Ｓ１８１９）。即ち、これ以降はこの書換え面で起動することを示す情報に更新する。書換え対象ＥＣＵ１９は、ＣＧＷ１３からバージョン読出信号を受信したか否かを判定し（Ｓ１８２０）、バージョン読出信号を受信したと判定すると（Ｓ１８２０：ＹＥＳ）、運用面のバージョン情報、非運用面のバージョン情報、何れの面が運用面であるかを特定可能な識別情報をＣＧＷ１３に送信し（Ｓ１８２１）、書換え動作処理を終了する。ここで、書換え対象ＥＣＵ１９は、Ｓ１８１１からＳ１８２１までの全ての

処理を切替え前の運用面（旧面）のアプリプログラムが実行しても良い。又、書換え対象ＥＣＵ１９は、Ｓ１８１１からＳ１８１９までの処理を切替え前の運用面（旧面）のアプリプログラムが実行し、Ｓ１８１９を行った後に再起動することで、Ｓ１８２０からＳ１８２１までの処理を切替え後の運用面（新面）のアプリプログラムが実行しても良い。

[0492] （１８－３）情報通知処理

書換え対象ＥＣＵ１９は、停止状態又はスリープ状態から起動状態に移行する、又は例えばＩＧ電源がオンになったりＣＧＷ１３から通知要求を受信したりすると、情報通知処理を開始する。書換え対象ＥＣＵ１９は、情報通知処理を開始すると、運用面や非運用面に関するアプリプログラムやパラメータデータを一意に特定可能な識別情報と、運用面や非運用面のメモリ上の配置場所を一意に特定可能な識別情報とをＣＧＷ１３に通知する。即ち、書換え対象ＥＣＵ１９は、起動面に関する起動面情報を取得し（Ｓ１８３１）、その起動面情報をＣＧＷ１３に送信する（Ｓ１８３２）。書換え対象ＥＣＵ１９は、起動面情報として、Ａ面及びＢ面のうち何れの面が起動面であるかの情報及び起動面のバージョン情報等をＣＧＷ１３に送信する。

[0493] 書換え対象ＥＣＵ１９は、起動面情報のＣＧＷ１３への送信を完了すると、書換え面に関する書換え面情報（以下、面情報とも称する）を取得し（Ｓ１８３３）、その取得した書換え面情報をＣＧＷ１３に送信する（Ｓ１８３４）。書換え対象ＥＣＵ１９は、書換え面情報として、Ａ面及びＢ面のうち何れの面が書換え面であるかの情報及び書換え面のバージョン情報等をＣＧＷ１３に送信する。書換え対象ＥＣＵ１９は、書換え面情報のＣＧＷ１３への送信を完了すると、メモリ上の起動面及び書換え面の配置アドレスを特定可能な識別情報をＣＧＷ１３に送信し（Ｓ１８３５）、情報通知処理を終了する。書換え対象ＥＣＵ１９は、アドレスを特定可能な識別情報として例えばフラッシュメモリにおけるＡ面の開始アドレスと終了アドレス及びＢ面の開始アドレスと終了アドレスをＣＧＷ１３に送信する。

[0494] （１８－４）書換えプログラムの検証処理

書換え対象ＥＣＵ１９は、書換えプログラムの検証処理を開始すると、書換えプログラムを実行するためのアドレスを特定可能な識別情報を取得したか否かを判定する（Ｓ１８４１）。書換え対象ＥＣＵ１９は、書換えプログラムを実行するためのアドレスを特定可能な識別情報を取得したと判定すると（Ｓ１８４１：ＹＥＳ）、その識別情報と書換え対象ＥＣＵ１９の起動面情報とが一致しているか否かを判定する（Ｓ１８４２）。具体的には、書換え対象ＥＣＵ１９は、起動面情報のうちの起動面を示す面情報と、その識別情報とが一致しているか否かを判定する。

[0495] 書換え対象ＥＣＵ１９は、識別情報と書換え対象ＥＣＵ１９の起動面情報とが一致していると判定すると（Ｓ１８４２：ＹＥＳ）、書換えプログラムを取得し（Ｓ１８４３）、アプリプログラムの書換えを行うためのアドレスを特定可能な識別情報を取得したか否かを判定する（Ｓ１８４４）。ここで、書換え対象ＥＣＵ１９は、書換えプログラムが予めフラッシュメモリに組込まれている組込み型の構成であれば、Ｓ１８４３において、起動面の書込みプログラムをフラッシュメモリから取得してＲＡＭ上にて実行する。書換え対象ＥＣＵ１９は、書換えプログラムが予めフラッシュメモリに組込まれておらず、書換えプログラムを外部からダウンロードするダウンロード型の構成であれば、Ｓ１８４３において、書換えプログラムをＲＡＭにダウンロードして実行する。

[0496] 書換え対象ＥＣＵ１９は、アプリプログラムの書換えを行うためのアドレスを特定可能な識別情報を取得したと判定すると（Ｓ１８４４：ＹＥＳ）、その識別情報と書換え対象ＥＣＵ１９の起動面情報とが一致しているか否かを判定する（Ｓ１８４５）。具体的には、書換え対象ＥＣＵ１９は、起動面情報のうちの非起動面を示す面情報と、その識別情報とが一致しているか否かを判定する。書換え対象ＥＣＵ１９は、識別情報とＥＣＵ１９の起動面情報とが一致していると判定すると（Ｓ１８４５：ＹＥＳ）、アプリプログラムの書換えを行い（Ｓ１８４６）、書換えプログラムの検証処理を終了する。

[0497] 書換え対象ＥＣＵ１９は、識別情報とＥＣＵ１９の起動面情報が一致していないと判定すると（Ｓ１８４２：ＮＯ）、又は識別情報と書換え対象ＥＣＵ１９の起動面情報とが一致していないと判定すると（Ｓ１８４５：ＮＯ）、運用面や非運用面で実行可能なアプリプログラムやパラメータデータでないと判定し、否定応答をＣＧＷ１３に送信し（Ｓ１８４７）、書換えプログラムの検証処理を終了する。例えばフラッシュメモリのＡ面が運用面であり且つＢ面が非運用面である２面メモリＥＣＵの場合、書換えプログラムを実行するためのアドレスは運用面であるＡ面のアドレスであり、アプリプログラムの書換えを行うためのアドレスは非運用面であるＢ面のアドレスである。

[0498] 尚、書換え対象ＥＣＵ１９は、図１５０に示すように、ＣＧＷ１３から書込みデータを取得する前に、ＣＧＷ１３からアドレスを特定可能な識別情報を取得しても良い。又、書換え対象ＥＣＵ１９は、図１５１に示すように、ＣＧＷ１３から書込みデータを取得する際にアドレスを特定可能な識別情報を取得しても良い。書換え対象ＥＣＵ１９は、例えば書込みデータを取得する前にＣＧＷ１３から書換え諸元データを受信し、書換え面情報を取得する。書換え面情報には、何れの面が起動面であり、何れの面が書換え面であるかを識別可能なデータが含まれているので、その識別可能なデータを、アドレスを特定可能な識別情報として用いる。

[0499] 又、書換え対象ＥＣＵ１９は、ＣＧＷ１３がインストール指示処理を行うことに応じて前述した（１８－２）書換え動作処理を行う。ここで、ＣＧＷ１３が行うインストール指示処理について説明する。

[0500] ＣＧＷ１３は、インストール指示処理を開始すると、書換え諸元データを識別し（Ｓ１８５１）、書換え対象ＥＣＵ１９の全てについて駐車中のインストールが指定されているか、書換え対象ＥＣＵ１９の全てについて車両走行中のインストールが指定されているか、書換え対象ＥＣＵ１９のメモリ種別毎にインストールが指定されているか否かを判定する（Ｓ１８５２～Ｓ１８５４）。

[0501] ＣＧＷ１３は、書換え対象ＥＣＵ１９の全てについて駐車中のインストールが指定されていると判定すると（Ｓ１８５２：ＹＥＳ）、インストールの承諾が得られており、且つ駐車中であることを条件とし、インストールを書換え対象ＥＣＵ１９に指示する（Ｓ１８５５）。ＣＧＷ１３は、書換え対象ＥＣＵ１９の全てについて車両走行中のインストールが指定されていると判定すると（Ｓ１８５３：ＹＥＳ）、インストールの承諾が得られており、且つ車両走行中であることを条件とし、インストールを書換え対象ＥＣＵ１９に指示する（Ｓ１８５６）。

[0502] ＣＧＷ１３は、書換え対象ＥＣＵ１９のメモリ種別毎にインストールが指定されていると判定すると（Ｓ１８５４：ＹＥＳ）、書換え諸元データによりメモリ種別が２面メモリであるか、１面サスペンドメモリ又は１面単独メモリであるかを判定する（Ｓ１８５７，Ｓ１８５８）。

[0503] ＣＧＷ１３は、書換え対象ＥＣＵ１９のメモリ種別が２面メモリであり、第１所定条件を満たすと判定すると（Ｓ１８５７：ＹＥＳ）、インストールの承諾が得られており、且つ車両走行中であることを条件とし、インストールを書換え対象ＥＣＵ１９に指示する（Ｓ１８５９）。ＣＧＷ１３は、書換え対象ＥＣＵ１９のメモリ種別が１面サスペンドメモリ又は１面単独メモリであり、第２所定条件を満たすと判定すると（Ｓ１８５８：ＹＥＳ）、インストールの承諾が得られており、且つ駐車中であることを条件とし、インストールを書換え対象ＥＣＵ１９に指示する（Ｓ１８６０）。

[0504] ＣＧＷ１３は、全ての書換え対象ＥＣＵ１９においてインストールが完了したか否かを判定し（Ｓ１８６１）、全ての書換え対象ＥＣＵ１９においてインストールが完了していないと判定すると（Ｓ１８６１：ＮＯ）、ステップＳ１８５１に戻り、ステップＳ１８５１以降を繰返す。

[0505] 即ち、ＣＧＷ１３は、書換え対象ＥＣＵ１９が２面メモリＥＣＵであれば、車両が走行可能中にインストールを指示する。２面メモリＥＣＵは、車両が走行可能中にＣＧＷ１３からインストールが指示されることで、車両が走行可能中にインストールを行う（インストール実行手順に相当する）。ＣＧ

Ｗ１３は、書換え対象ＥＣＵ１９が１面サスペンドメモリＥＣＵや１面単独メモリＥＣＵであれば、駐車中にインストールを指示する。１面サスペンドメモリＥＣＵや１面単独メモリＥＣＵは、駐車中にＣＧＷ１３からインストールが指示されることで、駐車中にインストールを行う（インストール実行手順に相当する）。

[0506] ＣＧＷ１３は、全ての書換え対象ＥＣＵ１９においてインストールが完了したと判定すると（Ｓ１８６１：ＹＥＳ）、駐車中であるか否かを判定し（Ｓ１８６２）、駐車中であると判定すると（Ｓ１８６２：ＹＥＳ）、駐車中にアクティベートを書換え対象ＥＣＵ１９に指示し（Ｓ１８６３）、インストール指示処理を終了する。書換え対象ＥＣＵ１９は、駐車中にＣＧＷ１３からアクティベートが指示されることで、アクティベートを行う（アクティベート実行手順に相当する）。

[0507] 以上に説明したように、書換え対象ＥＣＵ１９は、書換えの実行制御処理を行うことで、データ格納面を複数面で持つ構成において、運用面のアプリプログラムを実行中に、運用面の書換えプログラムを実行して非運用面を書換える。アプリプログラムを書換え可能な期間が駐車状態に限定されず、車両走行中でもアプリプログラムを書換えることができる。書換え対象ＥＣＵ１９は、２面メモリＥＣＵであれば、車両が走行可能中にＣＧＷ１３からインストールが指示されることで、車両が走行可能中にインストールを行うことができる。書換え対象ＥＣＵ１９は、１面サスペンドメモリＥＣＵや１面単独メモリＥＣＵであれば、駐車中にＣＧＷ１３からインストールが指示されることで、駐車中にインストールを行うことができる。

[0508] （１９）セッションの確立処理

セッションの確立処理について図１５６から図１６９を参照して説明する。車両用プログラム書換えシステム１は、書換え対象ＥＣＵ１９においてセッションの確立処理を行う。

[0509] 図１５６に示すように、ＥＣＵ１９は、セッションの確立部１０５において、アプリ実行部１０５ａと、無線書換え要求特定部１０５ｂと、有線書換

え要求特定部１０５ｃとを有する。アプリ実行部１０５ａは、各プログラムの実行を調停する機能を有する。無線書換え要求特定部１０５ｂは、無線を介したプログラム書換え要求を特定する機能を有する。有線書換え要求特定部１０５ｃは、有線を介したプログラム書換え要求を特定する機能を有する。

[0510] 図１５７は、フラッシュメモリに記憶される各プログラムの構成を示す。車両制御プログラムは、ＥＣＵ１９自身に搭載されている車両制御機能（例えばステアリング制御機能）を実現するためのプログラムである。有線診断プログラムは、車両外部から有線を介してＥＣＵ１９自身の診断を行うためのプログラムである。無線診断プログラムは、車両外部から無線を介してＥＣＵ１９自身の診断を行うためのプログラムである。無線書換えプログラムは、車両外部から無線を介して取得されたプログラムの書換えを行うためのプログラムである。有線書換えプログラムは、車両外部から有線を介して取得されたプログラムの書換えを行うためのプログラムである。車両制御プログラムは、アプリ領域に第１プログラムとして配置される。有線診断プログラム及び有線書換えプログラムは、アプリ領域に第２プログラムとして配置される。無線診断プログラム及び無線書換えプログラムは、アプリ領域に第３プログラムとして配置される。換言すれば、第２プログラムは、車両制御以外の有線を介した特殊処理を行うプログラムであり、第３プログラムは、車両制御以外の無線を介した特殊処理を行うプログラムである。尚、有線書換えプログラムは、アプリ領域に配置せず、ブート領域に第４プログラムとして配置しても良い。

[0511] アプリ実行部１０５ａは、第１プログラムと、第２プログラムと、第３プログラムとを同時に実行可能となるように制御する（非排他制御する）。アプリ実行部１０５ａは、例えば車両制御プログラムと、有線診断プログラムと、無線診断プログラムとを同時に実行可能とする。即ち、アプリ実行部１０５ａは、車両制御と、有線でのＥＣＵ１９の診断と、無線でのＥＣＵ１９の診断とを同時に実行可能とする。同様に、アプリ実行部１０５ａは、車両

制御プログラムと、有線診断プログラムと、無線書換えプログラムとを同時に実行可能とし、車両制御プログラムと、有線書換えプログラムと、無線診断プログラムとを同時に実行可能とし、車両制御プログラムと、有線書換えプログラムと、無線書換えプログラムとを同時に実行可能とするように制御する。

[0512] 一方、アプリ実行部１０５ａは、第２プログラム内の各プログラムを同時に実行不能となるよう排他制御する。同様に、第３プログラム内の各プログラムを同時に実行不能となるよう排他制御する。アプリ実行部１０５ａは、例えば有線診断プログラムと、有線書換えプログラムとを排他制御し、無線診断プログラムと、無線書換えプログラムとを排他制御する。即ち、アプリ実行部１０５ａは、有線を介した特殊処理のうち一のプログラムのみを実行する。同様に、アプリ実行部１０５ａは、無線を介した特殊処理のうち一のプログラムのみを実行する。

[0513] 無線書換えプログラムは、換言すれば、無線診断プログラムの内部に配置されており、無線診断プログラムの一部として組込まれているとも言える。即ち、アプリ実行部１０５ａは、無線書換えプログラムが無線診断プログラムの内部に配置されている構成により、車両制御プログラム及び有線診断プログラムを実行中に後述するようにデフォルトセッション又は無線診断セッションから無線書換えセッションへ状態遷移されると、車両制御プログラム及び有線診断プログラムの実行を継続したまま、無線書換えプログラムを実行するように制御する。アプリ実行部１０５ａは、車両制御プログラム及び有線診断プログラムの実行を継続したまま、無線書換えプログラムの実行を開始することで、車両制御プログラムと、有線診断プログラムと、無線書換えプログラムとを同時に実行可能とする。即ち、アプリ実行部１０５ａは、車両制御と、有線でのＥＣＵ１９の診断と、無線でのアプリプログラムの書換えとを同時に実行可能となるように制御する。

[0514] ここで、診断処理や書換え処理の具体的な内容によっては、有線での診断と無線での診断及び有線での書換えと無線での書換えが同時に実行できない

状況が生じる。例えば有線での書換えと無線での書換えとが同じ領域を書換える場合、両者の処理が衝突する。そのため、アプリ実行部１０５ａは、処理や要求の具体内容に応じて有線診断プログラムと無線診断プログラムとを排他制御し、又、有線書換えプログラムと無線書換えプログラムとを排他制御する。又、診断処理の内容によっては、通常の車両制御が継続できない場合も生じ得る。例えばＥＣＵを動作させてその結果を読み出す診断処理の場合、通常の車両制御と同時に実行不能となる。その場合、アプリ実行部１０５ａは、車両制御プログラムを待機させ、有線又は無線診断プログラムを実行する、という調停制御を行う。

[0515] 一方、有線書換えプログラムをアプリ領域に配置せず、ブート領域に第４プログラムとして配置した場合、アプリ実行部１０５ａは、上述とは一部異なる調停制御を行う。有線書換えプログラムは、図１５７に破線で示すように、有線診断プログラムの外部に第４プログラムとして配置されており、有線診断プログラムの一部として組込まれていない。この場合、アプリ実行部１０５ａは、第４プログラムを実行する際は、第１～第３プログラムを終了するよう排他制御を行う。即ち、アプリ実行部１０５ａは、第１～第３プログラムを実行するモードから第４プログラムを実行する専用モードに切り替える。換言すれば、有線書換えプログラムは、有線書換えプログラムが有線診断プログラムの外部に配置されている構成により、車両制御プログラム及び無線診断プログラムを実行中に後述するように有線診断セッションから有線書換えセッションへ状態遷移されると、車両制御プログラム及び無線診断プログラムの実行を停止し、有線書換えプログラムの実行を開始するように制御する。アプリ実行部１０５ａは、車両制御プログラム及び無線診断プログラムの実行を停止し、有線書換えプログラムの実行を開始することで、車両制御プログラムと、無線診断プログラムと、有線書換えプログラムとを同時に実行可能とせず、有線書換えプログラムのみを実行可能とする。即ち、アプリ実行部１０５ａは、車両制御と、無線でのＥＣＵ１９の診断と、有線でのアプリプログラムの書換えとを同時に実行可能とせず、有線でのアプリ

プログラムの書換えのみを実行可能となるように制御する。

[0516] 図１５８に示すように、アプリ実行部１０５ａは、有線での特殊処理に関する第１状態として、デフォルトの状態（デフォルトセッション）、有線診断の状態（有線診断セッション）、有線書換えの状態（有線書換えセッション）を管理する。又、無線での特殊処理に関する第２状態として、デフォルトの状態（デフォルトセッション）、無線書換えの状態（無線書換えセッション）を管理し、動作の内部状態を管理している。

[0517] アプリ実行部１０５ａは、第１状態の状態遷移として、診断通信規格に準拠して車両制御を可能なデフォルトセッションと、車両外部から有線を介してＥＣＵ１９の診断を可能な有線診断セッションと、車両外部から有線を介して取得したアプリプログラムの書換えを可能な有線書換えセッションとを排他的に状態遷移させる。セッションを排他的に状態遷移させることは、セッションを同時に確立不能とすることであり、セッションを非排他的に状態遷移させることは、セッションを同時に確立可能とすることである。

[0518] 第１状態におけるデフォルトセッションとは、有線での特殊処理が行われていない状態を示すモードであり、車両制御を実行可能な状態である。デフォルトセッションは、車両制御に全く影響を与えない処理、例えば、車両制御に関わらない診断プログラムを実行しても良いモードであるとも言える。車両制御に関わらない診断プログラムとは、故障コード等の情報の読出し等を行うためのプログラムである。有線診断セッションは、ＥＣＵ１９の診断に関わる診断プログラムを実行するモードである。少なくとも、診断プログラムを実行することにより車両制御に影響を与え得る状態となる場合は、デフォルトセッションから有線診断セッションに移行させる。ＥＣＵ１９の診断に関わる診断プログラムとは、通信停止、ダイアグマスク、アクチュエータ駆動等を行うためのプログラムである。有線書換えセッションは、車両外部から有線を介して取得されたアプリプログラムの書換えを実行するモードである。

[0519] アプリ実行部１０５ａは、第１状態においてセッションの状態遷移を以下

のように行う。アプリ実行部１０５ａは、第１デフォルトセッションの状態で有線での診断要求が発生すると、診断セッション移行要求により第１デフォルトセッションから有線診断セッションに移行させ、有線での診断処理を実行する。アプリ実行部１０５ａは、有線診断セッションの状態でセッション復帰要求が発生する、タイムアウトが発生する、電源がオフになる又は法規サービスを受信すると、有線診断セッションから第１デフォルトセッションに移行させる。アプリ実行部１０５ａは、第１デフォルトセッションの状態で有線書換え要求が発生すると、診断セッション移行要求により第１デフォルトセッションから有線診断セッションに移行させた後に、書換えセッション移行要求により有線診断セッションから有線書換えセッションに移行させ、有線書換え処理を実行する。アプリ実行部１０５ａは、有線書換えセッションの状態でセッション復帰要求が発生する、タイムアウトが発生する、電源がオフになる又は法規サービスを受信すると、有線書換えセッションから第１デフォルトセッションに移行させる。又、アプリ実行部１０５ａは、セッション維持要求により現在のセッションを移行させずに維持させる。

[0520] アプリ実行部１０５ａは、第２状態の状態遷移として、診断通信規格に準拠して車両制御を可能なデフォルトセッションと、車両外部から無線を介して取得したアプリプログラムの書換えに関わる無線書換えセッションとを排他的に状態遷移させる。無線書換えセッションは、車両外部から無線を介して取得されたアプリプログラムの書換えを実行するモードである。

[0521] アプリ実行部１０５ａは、第２状態においてセッションの状態遷移を以下のように行う。アプリ実行部１０５ａは、第２デフォルトセッションの状態で無線書換え要求が発生すると、書換えセッション移行要求により第２デフォルトセッションから無線書換えセッションに移行させ、無線書換え処理を実行する。アプリ実行部１０５ａは、無線書換えセッションの状態でセッション復帰要求が発生する、タイムアウトが発生する又は電源がオフになると、無線書換えセッションから第２デフォルトセッションに移行させる。又、アプリ実行部１０５ａは、セッション維持要求により現在のセッションを移

行させずに維持させる。

[0522] アプリ実行部１０５ａは、第１プログラムとして車両制御プログラムを実行しつつ、有線での特殊処理に関する第１状態及び無線での特殊処理に関する第２状態を管理する。アプリ実行部１０５ａは、例えば第１状態及び第２状態ともにデフォルトセッションにおいて、有線診断要求が発生すると、車両制御プログラムを継続させたまま、第１状態を有線診断セッションに移行させ、有線診断プログラムの実行を開始する。この状態において、アプリ実行部１０５ａは、無線書換え要求が発生すると、車両制御プログラム及び有線診断プログラムの実行を継続させたまま、第２状態を無線書換えセッションに移行させ、無線書換えプログラムの実行を開始する。この状態において、アプリ実行部１０５ａは、有線書換え要求が発生すると、例えば無線書換えプログラムの実行を終了し、第２状態をデフォルトセッションに移行させる共に、有線診断プログラムの実行を終了し、第１状態を有線書換えセッションに移行させ、有線書換えプログラムの実行を開始する。アプリ実行部１０５ａは、同じメモリ領域への書込み処理が衝突するのを防ぐべく、第１状態の有線書換えセッションと、第２状態の無線書換えセッションとが、同時に確立しないよう排他的に状態遷移させる（排他的に制御する）。

[0523] 無線書換え要求特定部１０５ｂは、外部から受信した書換え要求の識別情報を判定し、無線書換え要求を特定する。即ち、センター装置３からＤＣＭ１２にリプログデータがダウンロードされ、ＣＧＷ１３がＤＣＭ１２から転送されたリプログデータを書換え対象ＥＣＵ１９に配信すると、無線書換え要求特定部１０５ｂは、ＣＧＷ１３からリプログデータと共に無線書換え要求を示す識別情報を受信することで、無線書換え要求を特定する。

[0524] 有線書換え要求特定部１０５ｃは、外部から受信した書換え要求の識別情報を判定し、有線書換え要求を特定する。即ち、ツール２３がＤＬＣコネクタ２２に接続され、ＣＧＷ１３がツール２３から転送されたリプログデータを書換え対象ＥＣＵ１９に配信すると、有線書換え要求特定部１０５ｃは、ＣＧＷ１３からリプログデータと共に有線書換え要求を示す識別情報を受信

することで、有線書換え要求を特定する。

[0525] 識別情報は、例えば有線書換え要求と無線書換え要求とで異なる識別ＩＤに該当する情報であっても良いし、有線書換え要求と無線書換え要求とで同じ識別ＩＤであるが異なるデータに該当する情報であっても良い。即ち、有線書換え要求と無線書換え要求とを識別可能であれば、どのような情報であっても良い。

[0526] アプリ実行部１０５ａにおいて、図１５８では、無線での特殊処理に関する第２状態として、デフォルトセッション、及び無線書換えセッションの２つの状態を管理する構成を説明したが、図１５９及び図１６０に示すように、第２状態として、デフォルトセッション、無線診断セッション及び無線書換えセッションの３つの状態を管理する構成でも良い。無線診断セッションは、車両外部から無線を介してＥＣＵ１９の診断を行うための無線診断プログラムを実行するモードである。少なくとも、車両制御に影響を与え得る無線診断プログラムを実行する場合は、無線診断セッションに移行させる。

[0527] 図１５９に示す構成の場合には、アプリ実行部１０５ａは、第２状態の状態遷移を以下のように行う。アプリ実行部１０５ａは、第２デフォルトセッションの状態で無線での診断要求が発生すると、診断セッション移行要求により第２デフォルトセッションから無線診断セッションに移行させ、無線診断処理を実行する。アプリ実行部１０５ａは、無線診断セッションの状態でセッション復帰要求が発生する、タイムアウトが発生する、電源がオフになると、無線診断セッションから第２デフォルトセッションに移行させる。アプリ実行部１０５ａは、第２デフォルトセッションの状態で無線書換え要求が発生すると、診断セッション移行要求により第２デフォルトセッションから無線診断セッションに移行させた後に、書換えセッション移行要求により無線診断セッションから無線書換えセッションに移行させ、無線書換え処理を実行する。アプリ実行部１０５ａは、無線書換えセッションの状態でセッション復帰要求が発生する、タイムアウトが発生する、電源がオフになると、無線書換えセッションから第２デフォルトセッションに移行させる。

[0528] 図１６０に示す構成の場合には、アプリ実行部１０５ａは、第２状態の状態遷移を以下のように行う。アプリ実行部１０５ａは、第２デフォルトセッションの状態で無線での診断要求が発生すると、診断セッション移行要求により第２デフォルトセッションから無線診断セッションに移行させ、無線診断処理を実行する。アプリ実行部１０５ａは、無線診断セッションの状態でセッション復帰要求が発生する、タイムアウトが発生する、電源がオフになると、無線診断セッションから第２デフォルトセッションに移行させる。アプリ実行部１０５ａは、第２デフォルトセッションの状態で無線書換え要求が発生すると、診断セッション移行要求により第２デフォルトセッションから無線診断セッションに移行させた後に、書換えセッション移行要求により無線診断セッションから無線書換えセッションに移行させるか、又は書換えセッション移行要求により第２デフォルトセッションから無線書換えセッションに移行させ、無線書換え処理を実行する。アプリ実行部１０５ａは、無線書換えセッションの状態でセッション復帰要求が発生する、タイムアウトが発生する、電源がオフになると、無線書換えセッションから第２デフォルトセッションに移行させる。

[0529] 尚、第１状態の有線診断セッションと第２状態の無線診断セッションとは、同じ診断プログラムを実行するものであっても良いし、異なる診断プログラムを実行するものであっても良い。第１状態の有線書換えセッションと第２状態の無線書換えセッションとは、同じ書換えプログラムを実行するものであっても良いし、異なる書換えプログラムを実行するものであっても良い。例えばメモリの消去や書込み等、共通する書換えプログラムを実行するものであっても良い。

[0530] 図１５９及び図１６０に示した構成において、第１状態の各セッションと第２状態の各セッションの調停について説明する。図１５７で説明したように、有線診断プログラムが第２プログラムとしてアプリ領域に配置され、無線診断プログラムと無線書換えプログラムとが第３プログラムとしてアプリ領域に配置され、有線診断プログラムが第４プログラムとしてブート領域に

配置される場合について説明する。換言すれば、無線書換えプログラムが無線診断プログラムの一部として組込まれている一方で有線書換えプログラムが有線診断プログラムの一部として組込まれていない構成についての説明である。この場合、第１状態及び第２状態の各セッションにおけるプログラム実行の調停は、図１６１に示す通りになる。

[0531] 第２状態が無線書換えセッションであり、且つ第１状態がデフォルトセッションの場合、アプリ実行部１０５ａは、車両制御プログラムを実行させつつ、無線書換えプログラムを実行させる。第２状態が無線書換えセッションであり、且つ第１状態が有線診断セッションの場合、アプリ実行部１０５ａは、車両制御プログラムを実行させつつ、無線書換えプログラム、及び有線診断プログラムを同時に実行させる。

[0532] 一方、第１状態が有線書換えセッションであり、且つ第２状態がデフォルトセッションの場合、アプリ実行部１０５ａは、車両制御プログラムを終了させ、有線書換えプログラムのみを実行させる。第１状態が有線書換えセッションであり、且つ第２状態が無線診断セッションの場合、アプリ実行部１０５ａは、無線診断プログラム及び車両制御プログラムを終了させ、有線書換えプログラムのみを実行させる。即ち、アプリ実行部１０５ａは、第４プログラムである有線書換えプログラムのみを実行する専用モードとして、第１～第３プログラムを排他制御する。

[0533] 尚、有線診断プログラム及び有線書換えプログラムが第２プログラムとしてアプリ領域に配置される構成では、各プログラムの調停が図１６１とは一部相異する。即ち、無線書換えプログラムが無線診断プログラムの一部として組込まれている共に有線書換えプログラムが有線診断プログラムの一部として組込まれている構成では、第１状態及び第２状態の各セッションにおけるプログラム実行の調停は、図１６２に示す通りになる。この場合において、第１状態が有線書換えセッションであり、且つ第２状態がデフォルトセッションの場合、アプリ実行部１０５ａは、車両制御プログラムを実行させつつ、有線書換えプログラムを実行させる。第１状態が有線書換えセッション

であり、且つ第２状態が無線診断セッションの場合、アプリ実行部１０５ａは、車両制御プログラムを実行させつつ、有線書換えプログラム及び無線診断プログラムを同時に実行させる。

[0534] 次に、上記した構成の作用について図１６３から図１６７を参照して説明する。ＥＣＵ１９において、マイコン３３は、セッションの確立プログラムを実行し、セッションの確立処理を行う。

[0535] マイコン３３は、電源投入を検知して起動すると、セッション確立プログラムを実行して状態遷移管理処理を行い、第１状態の状態遷移を管理する状態遷移管理処理と、第２状態の状態遷移を管理する状態遷移管理処理とを行う。以下、それぞれの状態遷移管理処理について説明する。尚、ここでは、アプリ実行部１０５ａが第２状態を図１５８に示す構成、即ち、無線診断セッションを有しない構成により管理する場合を説明する。

[0536] （１９－１）第１状態の状態遷移管理処理

マイコン３３は、電源投入を検知して起動し、第１状態の状態遷移管理処理を開始すると、書換え完了フラグを判定し、前回のアプリプログラムの書換えを正常に完了したか否かを判定する（Ｓ１９０１）。マイコン３３は、書換え完了フラグが正であると判定し、前回のアプリプログラムの書換えを正常に完了したと判定すると（Ｓ１９０１：ＹＥＳ）、第１状態をデフォルトセッションに移行させる（Ｓ１９０２）。即ち、マイコン３３は、第１状態をデフォルトセッションに移行させることで、車両制御処理を開始する。

[0537] マイコン３３は、車両制御プログラムを実行させて車両制御処理を開始すると、車両制御処理を実行中に、有線診断要求が発生したか否かを判定し（Ｓ１９０３）、有線書換え要求が発生したか否かを判定し（Ｓ１９０４）、状態遷移管理の完了条件の成立を判定する（Ｓ１９０５）。マイコン３３は、車両制御処理を実行中に、有線診断要求が発生したと判定すると（Ｓ１９０３：ＹＥＳ）、第１状態をデフォルトセッションから有線診断セッションに移行させ（Ｓ１９０６）、有線診断プログラムを実行させて有線診断処理を開始する（Ｓ１９０７）。マイコン３３は、有線診断処理の完了条件の成

立を判定し（Ｓ１９０８）、有線診断処理の完了条件が成立したと判定すると（Ｓ１９０８：ＹＥＳ）、有線診断プログラムを終了させて有線診断処理を終了し（Ｓ１９０９）、第１状態を有線診断セッションからデフォルトセッションに移行させる（Ｓ１９１０）。

[0538] マイコン３３は、車両制御処理を実行中に、有線書換え要求が発生したと判定すると（Ｓ１９０４：ＹＥＳ）、有線書換え要求発生時の書換え排他処理を開始する（Ｓ１９１１）。即ち、有線書換え処理と無線書換え処理とが衝突しないよう、排他制御を行うための処理である。マイコン３３は、有線書換え要求発生時の書換え排他処理を開始すると、第２状態において無線書換えセッションに移行中であるか否か、即ち、第２状態が無線書換えセッションであるか否かを判定する（Ｓ１９２１）。マイコン３３は、第２状態において無線書換えセッションに移行中でないと判定すると（Ｓ１９２１：ＮＯ）、第１状態を有線書換えセッションに移行可能であると特定する（Ｓ１９２２）。マイコン３３は、有線書換え要求発生時の書換え排他処理を終了し、第１状態の状態遷移管理処理に復帰する。

[0539] マイコン３３は、第２状態において無線書換えセッションに移行中であると判定すると（Ｓ１９２１：ＹＥＳ）、有線書換えセッション及び無線書換えセッションの何れを優先して排他制御を行うかを判定する。具体的には、マイコン３３は、有線書換えセッション優先条件、無線書換えセッション優先条件、移行中書換えセッション優先条件の何れが成立しているか否かを判定する（Ｓ１９２３～Ｓ１９２５）。有線書換えセッション優先条件は、有線書換えセッションを無線書換えセッションよりも優先する条件である。無線書換えセッション優先条件は、無線書換えセッションを有線書換えセッションよりも優先する条件である。移行中書換えセッション優先条件は、移行中の書換えセッションを優先する、即ち、先に移行していたセッションを優先する条件である。これらの優先条件のうち何れを採用するかは予め設定されており、例えば車両に対して優先条件フラグを設定しても良いし、書換えＥＣＵ毎に優先条件フラグを設定しても良い。

[0540] マイコン３３は、有線書換えセッション優先条件が成立していると判定すると（Ｓ１９２３：ＹＥＳ）、第２状態において無線書換えセッションをセッション復帰要求によりデフォルトセッションに移行させて無線書換えを中断させ（Ｓ１９２６）、第１状態を有線書換えセッションに移行可能であると特定する（Ｓ１９２２）。マイコン３３は、デフォルトセッション移行に伴い、無線書換えプログラムを終了させる。マイコン３３は、有線書換え要求発生時の書換え排他処理を終了し、第１状態の状態遷移管理処理に復帰する。

[0541] マイコン３３は、無線書換えセッション優先条件が成立していると判定すると（Ｓ１９２４：ＹＥＳ）、有線書換え要求を廃棄して無線書換えを継続させる（Ｓ１９２７）。即ち、マイコン３３は、第２状態を無線書換えセッションで維持し、無線書換えプログラムの実行を継続し、第１状態を有線書換えセッションに移行不能であると特定する（Ｓ１９２８）。マイコン３３は、有線書換え要求発生時の書換え排他処理を終了し、第１状態の状態遷移管理処理に復帰する。

[0542] マイコン３３は、移行中書換えセッション優先条件が成立していると判定すると（Ｓ１９２５：ＹＥＳ）、この場合も、有線書換え要求を廃棄して無線書換えを継続させる（Ｓ１９２７）。即ち、マイコン３３は、第２状態を無線書換えセッションで維持し、無線書換えプログラムの実行を継続し、第１状態を有線書換えセッションに移行不能であると特定する（Ｓ１９２８）。マイコン３３は、有線書換え要求発生時の書換え排他処理を終了し、第１状態の状態遷移管理処理に復帰する。マイコン３３は、このように有線書換え要求発生時の書換え排他処理を実行することで、有線書換えセッションと、無線書換えセッションとを排他的に制御し、同時にセッション確立しないようにする。

[0543] マイコン３３は、第１状態の状態遷移管理処理に復帰すると、有線書換え要求発生時の書換え排他処理の結果として有線書換えセッションに移行可能であるか否かを判定する（Ｓ１９１２）。マイコン３３は、有線書換え要求

発生時の書換え排他処理により有線書換えセッションに移行可能であると特定したことで、移行可能であると判定すると（Ｓ１９１２：ＹＥＳ）、第１状態をデフォルトセッションから有線診断セッションを介して有線書換えセッションに移行させ（Ｓ１９１３）、車両制御処理を中断して有線書換え処理を開始する（Ｓ１９１４）。マイコン３３は、有線書換えセッション移行に伴い、車両制御プログラムを終了させる。

[0544] マイコン３３は、有線書換え処理の完了条件の成立を判定し（Ｓ１９１５）、有線書換え処理の完了条件が成立したと判定すると（Ｓ１９１５：ＹＥＳ）、有線書換え処理を完了し（Ｓ１９１６）、第１状態を有線書換えセッションからデフォルトセッションに移行させる（Ｓ１９１７）。ここで、有線書換え処理の完了条件とは、例えばアプリプログラムの書込みが全て完了し、完全性検証が実行された場合等である。

[0545] マイコン３３は、有線書換え要求発生時の書換え排他処理により有線書換えセッションに移行不能であると特定したことで、移行可能でないと判定すると（Ｓ１９１２：ＮＯ）、第１状態をデフォルトセッションから有線診断セッションを介して有線書換えセッションに移行させない。即ち、マイコン３３は、第１状態をデフォルトセッションで維持する。マイコン３３は、状態遷移管理の完了条件が成立したと判定すると（Ｓ１９０５：ＹＥＳ）、第１状態の状態遷移管理処理を完了する。

[0546] 尚、以上は、マイコン３３は、有線書換え要求発生時の書換え排他処理において、第２状態において無線書換えセッションに移行中であると判定し、有線書換えセッション優先条件が成立していると判定すると、第２状態において無線書換えを中断させる場合を説明したが、無線書換えの未書換え残量に応じて無線書換えセッションを中断させるか否かを判定しても良い。

[0547] マイコン３３は、第２状態において無線書換えセッションに移行中であると判定し（Ｓ１９２１：ＹＥＳ）、有線書換えセッション優先条件が成立していると判定すると（Ｓ１９２３：ＹＥＳ）、その移行中の無線書換えセッションにおいて無線書換えの未書換え残量が所定量以上（例えば２０％以上

）であるか否かを判定する（Ｓ１９３１）。マイコン３３は、無線書換えの未書換え残量が所定量以上であると判定すると（Ｓ１９３１：ＹＥＳ）、第２状態を無線書換えセッションからデフォルトセッションに移行させて無線書換えを中断させる（Ｓ１９２６）。マイコン３３は、デフォルトセッションへの移行に伴い、無線書換えプログラムを終了させる。マイコン３３は、無線書換えの未書換え残量が所定量以上でないと判定すると（Ｓ１９３１：ＮＯ）、その有線書換え要求を廃棄して無線書換えを継続させる（Ｓ１９２７）。即ち、マイコン３３は、無線書換えを完了するまでの残り時間が比較的長ければ、無線書換えセッションを中断させるが、無線書換えを完了するまでの残り時間が比較的短ければ、無線書換えセッションを中断させずに継続させる。

[0548] （１９－２）第２状態の状態遷移管理処理

マイコン３３は、電源投入を検知して起動し、第２状態の状態遷移管理処理を開始すると、書換え完了フラグを判定し、前回のアプリプログラムの書換えを正常に完了したか否かを判定する（Ｓ１９４１）。マイコン３３は、書換え完了フラグが正であると判定し、前回のアプリプログラムの書換えを正常に完了したと判定すると（Ｓ１９４１：ＹＥＳ）、第２状態をデフォルトセッションに移行させる（Ｓ１９４２）。即ち、マイコン３３は、第２状態をデフォルトセッションに移行させることで、車両制御プログラムを実行し、車両制御処理を開始する。

[0549] マイコン３３は、車両制御処理を開始すると、無線書換え要求が発生したか否かを判定し（Ｓ１９４３）、状態遷移管理の完了条件の成立を判定する（Ｓ１９４４）。マイコン３３は、車両制御処理を実行中に、無線書換え要求が発生したと判定すると（Ｓ１９４３：ＹＥＳ）、無線書換え要求発生時の書換え排他処理を開始する（Ｓ１９４４）。マイコン３３は、無線書換え要求発生時の書換え排他処理を開始すると、第１状態において有線書換えセッションに移行中であるか否か、即ち、第１状態が有線書換えセッションであるか否かを判定する（Ｓ１９６１）。マイコン３３は、第１状態において

有線書換えセッションに移行中でないと判定すると（Ｓ１９６１：ＮＯ）、無線書換えセッションに移行可能であると特定する（Ｓ１９６２）。マイコン３３は、無線書換え要求発生時の書換え排他処理を終了し、第２状態の状態遷移管理処理に復帰する。

[0550] マイコン３３は、第１状態において有線書換えセッションに移行中であると判定すると（Ｓ１９６１：ＹＥＳ）、有線書換えセッション及び無線書換えセッションの何れを優先して排他制御を行うかを判定する。具体的には、マイコン３３は、無線書換えセッション優先条件、有線書換えセッション優先条件、移行中書換えセッション優先条件の何れが成立しているか否かを判定する（Ｓ１９６３～Ｓ１９６５）。

[0551] マイコン３３は、無線書換えセッション優先条件が成立していると判定すると（Ｓ１９６３：ＹＥＳ）、第１状態において有線書換えセッションをセッション復帰要求によりデフォルトセッションに移行させて有線書換えを中断させ（Ｓ１９６６）、第２状態を無線書換えセッションに移行可能であると特定する（Ｓ１９６２）。マイコン３３は、デフォルトセッションへの移行に伴い、有線書換えプログラムを終了させる。マイコン３３は、無線書換え要求発生時の書換え排他処理を終了し、第２状態の状態遷移管理処理に復帰する。

[0552] マイコン３３は、有線書換えセッション優先条件が成立していると判定すると（Ｓ１９６４：ＹＥＳ）、無線換え要求を廃棄して有線書換えを継続させる（Ｓ１９６７）。即ち、マイコン３３は、第１状態を有線書換えセッションで維持し、有線書換えプログラムの実行を継続させ、第２状態を無線書換えセッションに移行不能であると特定する（Ｓ１９６８）。マイコン３３は、無線書換え要求発生時の書換え排他処理を終了し、第２状態の状態遷移管理処理に復帰する。

[0553] マイコン３３は、移行中書換えセッション優先条件が成立していると判定すると（Ｓ１９６５：ＹＥＳ）、この場合も、無線換え要求を廃棄して有線書換えを継続させる（Ｓ１９６７）。即ち、マイコン３３は、第１状態を有

線書換えセッションで維持し、有線書換えプログラムの実行を継続させ、第２状態を無線書換えセッションに移行不能であると特定する（Ｓ１９６８）。マイコン３３は、無線書換え要求発生時の書換え排他処理を終了し、第２状態の状態遷移管理処理に復帰する。マイコン３３は、このように無線書換え要求発生時の書換え排他処理を実行することで、有線書換えセッションと、無線書換えセッションとを排他的に制御し、同時にセッション確立させない。

[0554] マイコン３３は、第２状態の状態遷移管理処理に復帰すると、無線書換え要求発生時の書換え排他処理の結果として無線書換えセッションに移行可能であるか否かを判定する（Ｓ１９４５）。マイコン３３は、無線書換え要求発生時の書換え排他処理により無線書換えセッションに移行可能であると特定したことで、移行可能であると判定すると（Ｓ１９４５：ＹＥＳ）、第２状態をデフォルトセッションから無線書換えセッションに移行させ（Ｓ１９４６）、無線書換えプログラムを実行させて無線書換え処理を開始する（Ｓ１８４７）。マイコン３３は、無線書換え処理の完了条件の成立を判定し（Ｓ１９４８）、無線書換え処理の完了条件が成立したと判定すると（Ｓ１９４８：ＹＥＳ）、無線書換え処理を終了し（Ｓ１９４９）、第２状態を無線書換えセッションからデフォルトセッションに移行させる（Ｓ１９５０）。マイコン３３は、デフォルトセッションへの移行に伴い、無線書換えプログラムを終了させる。ここで、無線書換え処理の完了条件とは、例えばアプリプログラムの書込みが全て完了し、完全性検証が実行された場合等である。

[0555] マイコン３３は、無線書換え要求発生時の書換え排他処理により無線書換えセッションに移行不能であると特定したことで、移行可能でないと判定すると（Ｓ１９４５：ＮＯ）、第２状態をデフォルトセッションから無線書換えセッションに移行させない。即ち、マイコン３３は、第２状態をデフォルトセッションで維持する。マイコン３３は、状態遷移管理の完了条件が成立したと判定すると（Ｓ１９５１：ＹＥＳ）、第２状態の状態遷移管理処理を終了する。

[0556] 以上は、アプリ実行部１０５ａにおいて、有線での特殊処理に関するプログラムと無線での特殊処理に関するプログラムとを独立して（同時に）実行可能である場合を説明したが、図１６５に示すように、有線診断プログラムと無線診断プログラムとを共通化する構成でも良い。車両制御プログラムを第１プログラムとしてアプリ領域に配置し、診断プログラム（有線診断プログラム及び無線診断プログラム）と、無線書換えプログラムとを第２プログラムとしてアプリ領域に配置する構成である。有線書換えプログラムは、第２プログラムとしてアプリ領域に配置しても良いし、第３プログラムとしてブート領域に配置しても良い。アプリ実行部１０５ａは、第１プログラムと、第２プログラムとを同時に実行させる。即ち、アプリ実行部１０５ａは、車両制御プログラムと、共通化した診断プログラムとを同時に実行可能となるように制御する。一方、アプリ実行部１０５ａは、第２プログラムを構成する各プログラムの実行を排他制御する。即ち、有線診断プログラム、無線診断プログラム、無線書換えプログラム及び有線書換えプログラムのうち何れか１つのみが動作するように制御する。

[0557] アプリ実行部１０５ａは、図１６６に示すように、状態として、デフォルトの状態（デフォルトセッション）、診断の状態（診断セッション）、有線書換えの状態（有線書換えセッション）、無線書換えの状態（無線書換えセッション）を管理し、動作の内部状態を管理することになる。ここで管理される状態は、有線と無線とで状態を独立して管理するものではなく、混在して１つの状態として管理するものである。

[0558] この構成においても、アプリ実行部１０５ａは、車両制御プログラムを実行しつつ、診断プログラムの実行を開始する。又、アプリ実行部１０５ａは、車両制御プログラムを実行しつつ、無線書換えプログラムや有線書換えプログラムの実行を開始する。一方、アプリ実行部１０５ａは、無線診断プログラム及び有線診断プログラムの実行を排他的に制御する。又、アプリ実行部１０５ａは、有線診断プログラム及び無線診断プログラムと、有線書換えプログラム及び無線書換えプログラムの実行も排他的に制御する。即ち、ア

プリ実行部１０５ａは、第２プログラムを構成する各プログラムの実行を排他的に制御する。

[0559] ここで、有線書換えプログラムが第３プログラムとしてブート領域に配置される場合、アプリ実行部１０５ａは、第３プログラムと、第１及び第２プログラムとを排他的に実行制御する。即ち、有線書換えプログラムを実行する場合、第１プログラム及び第２プログラムを終了させ、専用モードとして動作させる。

[0560] 図１６６に示すように、アプリ実行部１０５ａは、診断要求が発生すると、車両制御プログラムの実行を継続しつつ、診断セッションに移行させ、診断プログラムの実行を開始する。この状態において、アプリ実行部１０５ａは、無線書換え要求が発生すると、診断プログラムを終了させ、無線書換えセッションに移行すると共に、無線書換えプログラムの実行を開始する。車両制御プログラムの実行は継続したままである。一方、有線書換え要求が発生した場合は、アプリ実行部１０５ａは、診断プログラム及び車両制御プログラムを終了させ、有線書換えセッションに移行すると共に、有線書換えプログラムの実行を開始する。

[0561] アプリ実行部１０５ａは、無線書換えプログラムが診断プログラムの内部に配置されていても、車両制御プログラム及び診断プログラムを実行中に診断セッションから無線書換えセッションへ状態遷移されると、車両制御プログラム及び診断プログラムの実行を中断してから無線書換えプログラムの実行を開始する。尚、セッションを伴わない場合は処理を継続することが可能である。

[0562] アプリ実行部１０５ａは、有線書換えプログラムが診断プログラムの外部に配置されていれば、車両制御プログラム及び診断プログラムを実行中に診断セッションから有線書換えセッションに状態遷移されると、車両制御プログラム及び無線診断プログラムの実行を停止し、有線書換えプログラムが実行を開始する。即ち、アプリ実行部１０５ａは、車両制御と、有線又は無線でのＥＣＵ１９の診断と、有線でのアプリプログラムの書換えとを同時に実

行可能とならず、有線でのアプリプログラムの書換えのみを実行可能となる。

[0563] 以上に説明したように、ＥＣＵ１９は、セッションの確立処理を行うことで、第１状態の状態遷移管理処理と第２状態の状態遷移管理処理を実行し、第１状態と第２状態とおける各セッションの状態遷移を管理し、第１状態のデフォルトセッション又は有線診断セッションと、第２状態の無線書換えセッションとを非排他的に確立するようにした。車両制御又はＥＣＵ１９の診断と、無線でのプログラムの書換えとの要求に対し、車両制御プログラム又はＥＣＵ１９の診断プログラムと、無線書換えプログラムとを非排他的に実行するように制御し、外部からの各種要求に対して適切に調停することができる。

[0564] 又、ＥＣＵ１９において、有線書換えセッションと、無線書換えセッションとを排他的に確立するようにした。有線書換えプログラムと、無線書換えプログラムとを排他的に実行するように制御し、有線でのプログラムの書換えと、無線でのプログラムの書換えとを適切に調停することができる。

[0565] 又、ＥＣＵ１９において、有線書換えセッション優先条件が成立していると、有線書換えセッションを無線書換えセッションよりも優先するようにした。有線書換えセッション優先条件を設定しておくことで、有線でのプログラムの書換えを無線でのプログラムの書換えよりも優先して実行することができる。例えばディーラー等で整備者が指示する有線でのプログラムの書換えを、車両のユーザが指示する無線でのプログラムの書換えをよりも優先して実行することができる。

[0566] 又、ＥＣＵ１９において、無線書換えセッション優先条件が成立していると、無線書換えセッションを有線書換えセッションよりも優先するようにした。無線書換えセッション優先条件を設定しておくことで、無線でのプログラムの書換えを有線でのプログラムの書換えよりも優先して実行することができる。例えば車両のユーザが指示する無線でのプログラムの書換えを、ディーラー等で整備者が指示する有線でのプログラムの書換えよりも優先して

実行することができる。

[0567] 又、ＥＣＵ１９において、移行中書換えセッション優先条件が成立していると、移行中の書換えセッションを優先するようにした。移行中書換えセッション優先条件を設定しておくことで、移行中の書換えを優先して実行することができる。即ち、有線書換え及び無線書換えのうち先に開始した方を中断せず継続させることができる。

[0568] アプリ領域を２面で持つ構成において、各アプリ領域に車両制御プログラムと、診断プログラムと、無線書換えプログラムとが配置されている構成とし、車両制御プログラム又は診断プログラムと、無線書換えプログラムとを並列に（同時に）に実行するようにした。フラッシュメモリ３０ｄのメモリ構成を工夫することで、車両制御プログラム又は診断プログラムと、無線書換えプログラムとを並列に実行することができる。

[0569] 車両制御プログラム又は有線診断プログラムを実行中に無線書換え要求を特定すると、車両制御プログラム又は有線診断プログラムの実行を継続し、無線書換えプログラムを実行するようにした。車両制御プログラム又は有線診断プログラムを実行中に無線書換え要求が発生したときに、車両制御プログラム又は有線診断プログラムと、無線書換えプログラムとを並列に（同時に）実行することができる。

[0570] 無線書換えプログラムを実行中に車両制御要求又は有線診断要求を特定すると、無線書換えプログラムの実行を継続し、車両制御プログラム又は有線診断プログラムを実行するようにした。無線書換えプログラムを実行中に車両制御要求又は有線診断要求が発生したときに、無線書換えプログラムと、車両制御プログラム又は有線診断プログラムとを並列に（同時に）実行することができる。

[0571] 車両制御プログラム又は無線診断プログラムを実行中に有線書換え要求を特定すると、車両制御プログラム又は無線診断プログラムの実行を停止し、有線書換えプログラムを実行するようにした。車両制御プログラム又は無線診断プログラムを実行中に有線書換え要求が発生したときに、有線書換えプ

ログラムのみを排他的に実行することができる。

[0572] リプログファームウェアが組込まれているリプログファームウェア組込み型の場合に、アプリ領域に配置されているファームウェアを用い、書換えプログラムを実行するようにした。リプログファームウェアを外部からダウンロードすることなく、非運用面のアプリプログラムの書換え処理を実行することができる。

[0573] リプログファームウェアを外部からダウンロードするリプログファームウェアダウンロード型の場合に、外部からダウンロードされたファームウェアを用い、書換えプログラムを実行するようにした。アプリ領域における書換えプログラムの容量を低減した上で、非運用面のアプリプログラムの書換え処理を実行することができる。

[0574] アプリ領域を実質的な２面で持つ２面メモリについて説明したが、アプリ領域を疑似的な２面で持つ１面サスペンド方式メモリや外付けメモリについても適用することができる。

[0575] 旧データと差分リプログデータから新データを生成する差分書換えする場合について説明したが、旧データを削除して新データを書込む全書換えする場合についても適用することができる。

[0576] ＥＣＵ１９のアプリプログラムを書換える場合について説明したが、ＣＧＷ１３のアプリプログラムを書換える場合についても適用することができる。即ち、ＣＧＷ１３のフラッシュメモリ２６ｄを２面構成としてＥＣＵ１９のフラッシュメモリ３０ｄと同等の構成とし、マイコン２６にＥＣＵ１９のマイコン３３と同等の機能を持たせても良い。

[0577] （２０）リトライポイントの特定処理

リトライポイントの特定処理について図１７０から図１７４を参照して説明する。車両用プログラム書換えシステム１は、書換え対象ＥＣＵ１９においてリトライポイントの特定処理を行う。リトライポイントとは、書込みデータを複数回に分けて書込む場合において、書込みデータの書込みを中断した場合に、その中断した書込みデータの書込みを途中から再開するために、

どこまで処理を完了したかを示す情報である。書込みデータの書込みを中断する場合としては、例えばユーザ操作によるキャンセルが発生した場合、通信途絶等の異常が発生した場合、駐車状態においてイグニッションがオフからオンに切替わった場合等がある。

[0578] ＥＣＵ１９において、プログラム書換え部１０２は、アプリプログラムの書換えに関与する一連の処理を複数の書換えプログラムで分担する。プログラム書換え部１０２は、第１処理を行う第１書換えプログラムと、第２処理を行う第２書換えプログラムとを有し、それぞれの書換えプログラムを順次実行する。第１書換えプログラムが行う第１処理は、例えばフラッシュメモリのデータを消去するメモリ消去処理、書込みデータを書込むデータ書込み処理等である。第２書換えプログラムが行う第２処理は、例えばベリファイ処理、改ざんチェック処理等である。

[0579] 図１７０に示すように、ＥＣＵ１９は、リトライポイントの特定部１０６において、第１処理フラグ設定部１０６ａと、第２処理フラグ設定部１０６ｂと、リトライポイント特定部１０６ｃとを有する。第１処理フラグ設定部１０６ａは、プログラム書換え部１０２が第１書換えプログラムを実行すると、そのプログラム書換え部１０２が第１書換えプログラムにより第１処理を完了したか否かを判定し、その判定結果を示す第１処理フラグを設定する。第１処理フラグ設定部１０６ａは、プログラム書換え部１０２が第１処理を完了したと判定すると、第１処理フラグを「ＯＫ」に設定する。

[0580] 第２処理フラグ設定部１０６ｂは、プログラム書換え部１０２が第２書換えプログラムを実行すると、そのプログラム書換え部１０２が第２書換えプログラムにより第２処理を完了したか否かを判定し、その判定結果を示す第２処理フラグを設定する。第２処理フラグ設定部１０６ｂは、プログラム書換え部１０２が第２処理を完了したと判定すると、第２処理フラグを「ＯＫ」に設定する。

[0581] リトライポイント特定部１０６ｃは、プログラムの書換えに関与する処理の一部が中断された場合において、プログラム書換え部１０２がアプリプロ

グラムの書換えをリトライする際のリトライポイントを、第１処理フラグ及び第２処理フラグにしたがって特定する。又、リトライポイント特定部１０６ｃは、中断時までの更新データの書込み量を記憶しておき、プログラムの書換えに関与する処理を再開する場合において、その記憶している更新データの書込み量に基づく更新データの送信をＣＧＷ１３に要求する。図１７１に示すように、第１処理フラグと第２処理フラグは、書換え対象ＥＣＵ１９のフラッシュメモリの同一のブロック内に記憶されている。

[0582] 次に、書換え対象ＥＣＵ１９におけるリトライポイントの特定部１０６の作用について図１７２から図１７４を参照して説明する。書換え対象ＥＣＵ１９は、リトライポイントの特定プログラムを実行し、リトライポイントの特定処理を行う。書換え対象ＥＣＵ１９は、リトライポイントの特定処理として、処理フラグの設定処理、処理フラグの判定処理行う。以下、それぞれの処理について説明する。

[0583] （２０－１）処理フラグの設定処理

書換え対象ＥＣＵ１９は、処理フラグの設定処理を開始すると、アプリプログラムの書換え前の事前処理を完了しているか否かを判定する（Ｓ２００１）。書換え対象ＥＣＵ１９は、アプリプログラムの書換え前の事前処理を完了していると判定すると（Ｓ２００１：ＹＥＳ）、第１処理フラグを「ＮＧ」に設定し、第２処理フラグを「ＮＧ」に設定し、記憶する（Ｓ２００２、第１処理フラグ設定手順、第２処理フラグ設定手順に相当する）。

[0584] 書換え対象ＥＣＵ１９は、ＣＧＷ１３から書込みデータを受信すると、第１処理を開始し（Ｓ２００３）、第１処理を完了したか否かを判定する（Ｓ２００４）。書換え対象ＥＣＵ１９は、第１処理を完了したと判定すると（Ｓ２００４：ＹＥＳ）、第２処理フラグを「ＮＧ」に維持したまま、第１処理フラグを「ＯＫ」に設定し、記憶する（Ｓ２００５、第１処理フラグ設定手順、第２処理フラグ設定手順に相当する）。合わせて、書換え対象ＥＣＵ１９は、フラッシュメモリのどこまで書込みが完了したかを示す書込み完了アドレスを記憶する。

[0585] 書換え対象ＥＣＵ１９は、ＣＧＷ１３への書込み完了通知等の第２処理を開始し（Ｓ２００６）、第２処理を完了したか否かを判定する（Ｓ２００７）。書換え対象ＥＣＵ１９は、第２処理を完了したと判定すると（Ｓ２００７：ＹＥＳ）、第１処理フラグを「ＯＫ」に維持したまま、第２処理フラグを「ＯＫ」に設定して記憶し（Ｓ２００８、第１処理フラグ設定手順、第２処理フラグ設定手順に相当する）、処理フラグの設定処理を終了する。

[0586] （２０－２）処理フラグの判定処理

書換え対象ＥＣＵ１９は、スリープ又は停止状態から起動した際、処理フラグの判定処理を開始すると、ブートプログラムより起動し（Ｓ２０１１）、第１処理フラグ及び第２処理フラグをフラッシュメモリから読出して判定する（Ｓ２０１２～Ｓ２０１５）。

[0587] 書換え対象ＥＣＵ１９は、第１処理フラグが「ＮＧ」であり、且つ第２処理フラグが「ＮＧ」であると判定すると（Ｓ２０１２：ＹＥＳ）、リトライポイントを第１処理の先頭に特定し、第１処理の先頭からのリトライ要求をＣＧＷ１３に通知し（Ｓ２０１６、リトライポイント特定手順に相当する）、リトライポイントの特定処理を終了する。即ち、書換え対象ＥＣＵ１９は、書込みデータの配信をＣＧＷ１３に要求する。このとき、書換え対象ＥＣＵ１９がフラッシュメモリから読出した書込み完了アドレスもＣＧＷ１３に通知することで、ＣＧＷ１３は、分割して配信する書込みデータのうち何れを配信すれば良いか特定する。書換え対象ＥＣＵ１９は、第１処理フラグが「ＮＧ」であり、且つ第２処理フラグが「ＯＫ」であると判定すると（Ｓ２０１３：ＹＥＳ）、この場合も、リトライポイントを第１処理の先頭に特定し（Ｓ２０１６、リトライポイント特定手順に相当する）、第１処理の先頭からのリトライ要求をＣＧＷ１３に通知し（Ｓ２０１７）、処理フラグの判定処理を終了する。

[0588] 書換え対象ＥＣＵ１９は、第１処理フラグが「ＯＫ」であり、且つ第２処理フラグが「ＮＧ」であると判定すると（Ｓ２０１４：ＹＥＳ）、リトライポイントを第２処理の先頭に特定し（Ｓ２０１８、リトライポイント特定手

順に相当する）、第２処理の先頭からのリトライ要求をＣＧＷ１３に通知し（Ｓ２０１９）、処理フラグの判定処理を終了する。ＥＣＵ１９は、第２処理として例えば何れのアドレスまで書込みが完了したかをＣＧＷ１３に通知する。

[0589] 書換え対象ＥＣＵ１９は、第１処理フラグが「ＯＫ」であり、且つ第２処理フラグが「ＯＫ」であると判定すると（Ｓ２０１５：ＹＥＳ）、アプリプログラムの書換えに関与する処理の完了をＣＧＷ１３に通知し（Ｓ２０２０）、処理フラグの判定処理を終了する。尚、書換え対象ＥＣＵ１９は、ＣＧＷ１３が書込みデータを分割して配信する場合は、上述したリトライポイントの設定を分割された書込みデータ単位で行う。

[0590] 以上に説明したように、書換え対象ＥＣＵ１９は、リトライポイントの特定処理を行うことで、第１処理が完了したか否かを示す第１処理フラグを設定し、第２処理が完了したか否かを示す第２処理フラグを設定し、リトライポイントを第１処理フラグ及び第２処理フラグにしたがって特定する。例えば第１処理が完了し、且つ第２処理が完了していない状態で書換え対象ＥＣＵ１９が再起動された場合において、同じ書込みデータを再度書込むことを抑制することができる。

[0591] 尚、書換え対象ＥＣＵ１９は、書込みを完了した書込みデータのデータ量、即ち、書込みデータの書込みを何バイトまで完了したかを記憶しておき、書込みデータの書込みを再開する場合には、何バイト目の書込みデータから送信するようにＣＧＷ１３に対して要求する。書換え対象ＥＣＵ１９が書込みデータの書込みを何バイトまで完了したかを記憶しておき、再開する場合には、何バイト目の書込みデータから送信するようにＣＧＷ１３に対して要求することで、再開時において、ＣＧＷ１３は、送信済みの書込みデータを再送する無駄を回避することができ、書換え対象ＥＣＵ１９は、書込みデータの書込みを完了した次の書込み領域から書込みデータを書込むことができる。尚、このような書込みデータの書込みを何バイトまで完了したかを記憶する機能を有しない書換え対象ＥＣＵ１９は

、書込みデータの書込みを再開する場合には、先頭の書込みデータから送信するようにＣＧＷ１３に対して要求する。

[0592] （２１）進捗状態の同期制御処理

進捗状態の同期制御処理について図１７５から図１８０を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３及びセンター装置３において進捗状態の同期制御処理を行う。車両用プログラム書換えシステム１は、ユーザの入力操作が可能な表示端末５として、携帯端末６及び車載ディスプレイ７を有する。車載ディスプレイ７は、ＣＧＷ１３との連携により書換えの進捗を示す進捗画面を表示する。携帯端末６は、センター装置３に接続することで、センター装置３が提供する書換えの進捗を示す進捗画面を表示する。ＣＧＷ１３及びセンター装置３は、これら携帯端末６及び車載ディスプレイ７で表示される情報を同期させるべく進捗状態の同期制御処理を行う。

[0593] 前述した図３０に示したように、例えば書換え対象ＥＣＵ１９が２面メモリを搭載したＥＣＵ１９であれば、アプリプログラムの書換えを告知してユーザの承諾を得るキャンペーン通知フェーズ、センター装置３からＤＣＭ１２への書込みデータのダウンロードを実行させるダウンロードフェーズ、ＣＧＷ１３から書換え対象ＥＣＵ１９への書込みデータの配信を実行させるインストールフェーズ、次回起動時の起動面を旧面から新面に切替えるアクティベートフェーズにしたがい、アプリプログラムの書換えに関与する手順を行う。即ち、ユーザは、携帯端末６や車載ディスプレイ７を操作し、各フェーズの実行を承諾する等アプリプログラムの書換えに関与する一連の手順を進める。

[0594] 図１７５に示すように、ＣＧＷ１３は、進捗状態の同期制御部８８において、第１進捗状態判定部８８ａと、第１進捗状態送信部８８ｂと、第２進捗状態取得部８８ｃと、第１表示指示部８８ｄとを有する。第１進捗状態判定部８８ａは、プログラムの書換えに係る第１進捗状態を判定し、例えばキャンペーン通知フェーズ、ダウンロードフェーズ、インストールフェーズ、ア

クティベートフェーズという進捗状態を判定する。キャンペーン通知フェーズは、キャンペーンを受信し、図３２～図３３に示す画面を表示し、ユーザ承諾を得るまでのフェーズである。ダウンロードフェーズは、図３４～図３７に示す画面を表示し、ユーザ承諾を得てダウンロードを実行するフェーズである。インストールフェーズは、ダウンロードが完了し、図３８～図４２に示す画面を表示し、ユーザ承諾を得てインストールを実行するフェーズである。アクティベートフェーズとは、図４３に示す画面を表示し、ユーザの承諾を得てアクティベートを実行するフェーズである。

[0595] 第１進捗状態判定部８８ａは、ユーザが乗車中であり、ユーザが車載ディスプレイ７において「プログラム更新の実行を承諾する」を選択し、フェーズを次に進める操作を行うと、ユーザ操作信号が車載ディスプレイ７からＣＧＷ１３に送信されることで、ユーザが車載ディスプレイ７において行った操作を特定し、第１進捗状態を判定する。この場合、「プログラム更新の実行を承諾する」を選択することは、図３４に示す「ダウンロード開始」ボタン５０３ａ、図３９に示す「すぐ更新」ボタン５０６ａや「予約して更新」ボタン５０６ｂ、図４３に示す「ＯＫ」ボタン５０８ｂの何れかを操作することに該当する。第１進捗状態判定部８８ａは、第１進捗状態を判定すると、その判定した第１進捗状態を現在進捗状態として管理する。

[0596] 第１進捗状態送信部８８ｂは、第１進捗状態が第１進捗状態判定部８８ａにより判定されると、その判定された第１進捗状態をセンター装置３に送信すると共に、車載ディスプレイ７等の各車載表示機器に送信する。第２進捗状態取得部８８ｃは、プログラムの書換えに係る第２進捗状態をセンター装置３から取得する。第１表示指示部８８ｄは、第１進捗状態が第１進捗状態判定部８８ａにより判定され、第２進捗状態が第２進捗状態取得部により取得されると、その判定された第１進捗状態及び当該取得された第２進捗状態に基づいて車載ディスプレイ７において表示可能なコンテンツの作成を指示する。

[0597] ここで、第２進捗状態取得部８８ｃがセンター装置３から第２進捗状態を

取得した場合、第１進捗状態判定部８８ａは、第２進捗状態が現在進捗状態よりも先のフェーズであるならば、第２進捗状態を現在進捗状態として管理する。即ち、第１進捗状態を第２進捗状態の値で更新する。そして、第１進捗状態送信部８８ｂは、現在進捗状態である第１進捗状態をセンター装置３に送信する。例えば第１進捗状態が「ダウンロード待ちフェーズ」において、携帯端末６におけるユーザ承諾操作がなされた場合、第２進捗状態取得部８８ｃがセンター装置３から第２進捗状態として「ダウンロード実行中フェーズ」を取得する。第１進捗状態判定部８８ａは、センター装置３から取得した「ダウンロード実行中フェーズ」が現在進捗状態より先のフェーズであるため、現在進捗状態である第１進捗状態を第２進捗状態の値で更新すると共に、その更新した第１進捗状態をセンター装置３に送信すると共に、車載ディスプレイ７等の各種車載表示機器に送信する。第１進捗状態として「ダウンロード実行中フェーズ」に加え、ダウンロードの進捗の程度を示す「ダウンロード完了Ｘ％」を送信しても良い。

[0598] 第１表示指示部８８ｄは、車載ディスプレイ７においてユーザ操作信号が発生した場合、第１進捗状態判定部８８ａが判定した第１進捗状態に基づいて、コンテンツの作成を指示する。又、第１表示指示部８８ｄは、携帯端末６においてユーザ操作信号が発生した場合、第２進捗状態取得部８８ｃにより取得した第２進捗状態に基づいて、コンテンツの作成を指示する。尚、第１進捗状態判定部８８ａが判定する第１進捗状態が常に現在進捗状態となるように管理する構成、即ち、マスタ装置１１が現在進捗状態を管理する構成であれば、第１表示指示部８８ｄは、第１進捗状態に基づいてコンテンツの作成を指示すれば良い。

[0599] 図１７６に示すように、センター装置３は、進捗状態の同期制御部５３において、第２進捗状態判定部５３ａと、第２進捗状態送信部５３ｂと、第１進捗状態取得部５３ｃと、第２表示指示部５３ｄとを有する。第２進捗状態判定部５３ａは、プログラムの書換えに係る第２進捗状態を判定し、例えばキャンペーン通知フェーズ、ダウンロードフェーズ、インストールフェーズ

、アクティベートフェーズという進捗状態を判定する。第２進捗状態判定部５３ａは、ユーザが降車中（駐車中）であり、ユーザが携帯端末６において「プログラム更新の実行を承諾する」を選択し、フェーズを次に進める操作を行うと、携帯端末６とセンター装置３がデータ通信可能な環境であれば、携帯端末６から送信されるユーザ操作信号を受信する。

[0600] 第２進捗状態判定部５３ａは、これ以前に第１進捗状態取得部５３ｃによりマスタ装置１１から受信していた第１進捗状態である現在進捗状態と、ユーザ操作信号とに基づいて、第２進捗状態を判定する。第２進捗状態判定部５３ａは、例えば現在進捗状態が「インストール待ちフェーズ」であるときに、「承諾」を示すユーザ操作信号を受信すると、第２進捗状態として「インストール実行中フェーズ」と判定する。又、。第２進捗状態判定部５３ａは、「インストール待ちフェーズにおいてユーザ承諾あり」という判定でも良い。携帯端末６におけるユーザ操作信号は、センター装置３とＤＣＭ１２がデータ通信可能な環境であれば、センター装置３からＤＣＭ１２に送信される。そして、ＤＣＭ１２からＣＧＷ１３にユーザ操作信号が転送されることで、ＣＧＷ１３は、ユーザが携帯端末６において行った操作を判定し、進捗状態を判定することができる。

[0601] 第２進捗状態送信部５３ｂは、第２進捗状態が第２進捗状態判定部５３ａにより判定されると、その判定された第２進捗状態をマスタ装置１１に送信する。第１進捗状態取得部５３ｃは、プログラムの書換えに係る第１進捗状態をマスタ装置１１から取得し、現在進捗状態として管理する。現在進捗状態として第２進捗状態を第１進捗状態の値で更新しても良い。第２表示指示部５３ｄは、第２進捗状態が第２進捗状態判定部５３ａにより判定され、第１進捗状態が第１進捗状態取得部５３ｄにより取得されると、その判定された第２進捗状態及び当該取得された第１進捗状態に基づいて携帯端末６において表示可能なコンテンツの作成を指示する。

[0602] 例えば携帯端末６におけるユーザ操作信号だけであれば、第２進捗状態判定部５３ａにより判定される第２進捗状態と、第１進捗状態取得部５３ｄに

より取得される第１進捗状態とは同じ進捗状態を示すこととなる。そのため、第２表示指示部５３ｄは、第２進捗状態に基づいてコンテンツの作成を指示しても良い。その後、車載ディスプレイ７におけるユーザ操作信号が発生した場合は、第２表示指示部５３ｄは、取得した第１進捗状態に基づいてコンテンツの作成を指示する。

[0603] 携帯端末６は、例えばセンター装置３から進捗状態信号としてＳＭＳを受信すると、ＳＭＳに記載されるＵＲＬをユーザが選択することによりセンター装置３に接続し、センター装置３が提供する所定フェーズの画面を表示する。

[0604] 次に、ＣＧＷ１３における進捗状態の同期制御部８８及びセンター装置３における進捗状態の同期制御部５３が行う作用について図１７７から図１８０を参照して説明する。

[0605] 図１７７に示すように、マスタ装置１１とセンター装置３とは、第１進捗状態信号及び第２進捗状態信号を送受信することで、携帯端末６と車載ディスプレイ７におけるフェーズの進捗状態の表示を同期させる。即ち、マスタ装置１１は、現在進捗状態である第１進捗状態を更新すると、第１進捗状態信号をセンター装置３に送信すると共に、第１進捗状態信号を車載ディスプレイ７等の各種車載表示機器に送信する。センター装置３は、第１進捗状態信号を現在進捗状態として携帯端末６に送信する。これにより、携帯端末６がセンター装置３にアクセス可能であれば、携帯端末６と車載ディスプレイ７におけるフェーズの進捗状態の表示を同期させる。センター装置３は、携帯端末６におけるユーザ承諾操作に基づいて、第２進捗状態信号をマスタ装置１１に送信させることで、携帯端末６がセンター装置３にアクセス可能であれば、携帯端末６と車載ディスプレイ７におけるフェーズの進捗状態の表示を同期させる。

[0606] 第２進捗状態信号を取得したマスタ装置１１は、現在進捗状態である第１進捗状態を更新した後、第１進捗状態をセンター装置３及び車載ディスプレイ７等の各車載表示機器に送信しても良い。即ち、マスタ装置１１が現在進

捗状態をセンター装置３及び車載ディスプレイ７等の各車載表示機器に送信することで、フェーズの管理装置としての機能を果たす。ここで、携帯端末６、車載ディスプレイ７及びセンター装置３から送信される第２進捗状態信号は、何れかのフェーズを示す通知であっても良いが、ユーザ承諾操作があった旨を示す通知や操作されたボタンの意味を示す通知であっても良い。

[0607] ＣＧＷ１３は、進捗状態の同期制御処理を開始すると、配信諸元データを車載ディスプレイ７に送信する（Ｓ２１０１）。配信諸元データには、車載ディスプレイ７がユーザに向けて表示するテキストやコンテンツが含まれている。ＣＧＷ１３は、ユーザが車載ディスプレイ７又は携帯端末６において操作を行ったか否かを、車載ディスプレイ７又はセンター装置３からの通知に基づいて判定する（Ｓ２１０２）。ＣＧＷ１３は、ユーザが車載ディスプレイ７又は携帯端末６において操作を行ったと判定すると（Ｓ２１０２：ＹＥＳ）、第１進捗状態に基づき、その操作が何れのフェーズの操作であるかを判定する（Ｓ２１０３～Ｓ２１０６、第１進捗状態判定手順に相当する）。

[0608] ＣＧＷ１３は、キャンペーン通知フェーズであると判定すると（Ｓ２１０３：ＹＥＳ）、キャンペーン通知フェーズの処理を実施し（Ｓ２１０７）、そのキャンペーン通知フェーズの処理の進捗状態を示す第１進捗状態信号を車載ディスプレイ７及びセンター装置３に送信する（Ｓ２１１１）。キャンペーン通知フェーズの処理とは、車載ディスプレイ７又は携帯端末６に対するユーザの入力操作を取得すること等である。

[0609] ＣＧＷ１３は、例えば車載ディスプレイ７、又は携帯端末６からセンター装置３を介して、プログラムの更新に承諾又は不承諾の他、実行を許可する日時、場所等の条件等を取得する。ＣＧＷ１３は、携帯端末６にて承諾する旨のユーザの入力操作があったことをセンター装置３からＤＣＭ１２を介して取得すると、承諾が完了した旨の進捗を車載ディスプレイ７に通知する。一方、ＣＧＷ１３は、車載ディスプレイ７にて承諾する旨のユーザの入力操作があったことを車載ディスプレイ７から取得すると、承諾が完了した旨の

進捗をセンター装置３に通知する。

[0610] ＣＧＷ１３は、ダウンロードフェーズであると判定すると（Ｓ２１０４：ＹＥＳ）、ダウンロードフェーズの処理を実施し（Ｓ２１０８）、そのダウンロードフェーズの処理の進捗状態を示す第１進捗状態信号を車載ディスプレイ７及びセンター装置に送信する（Ｓ２１１１）。ダウンロードフェーズの処理とは、例えば配信パッケージのダウンロードが何％完了したか算出することである。

[0611] ＣＧＷ１３は、センター装置３からの通知に基づいてダウンロードが何％完了したか決定する。ＣＧＷ１３は、ダウンロードが何％完了したかを示す進捗を車載ディスプレイ７及びセンター装置３に通知する。ＣＧＷ１３は、これらの処理を配信パッケージのダウンロードが完了するまで繰返す。ＣＧＷ１３は、ダウンロードが完了すると、ダウンロードフェーズが完了した旨の進捗を車載ディスプレイ７及びセンター装置３に通知する。

[0612] ＣＧＷ１３は、インストールフェーズであると判定すると（Ｓ２１０４：ＹＥＳ）、インストールフェーズの処理を実施し（Ｓ２１０８）、そのインストールフェーズの処理の進捗状態を示す進捗状態信号を車載ディスプレイ７及びＤＣＭ１２に送信する（Ｓ２１１１）。インストールフェーズの処理とは、例えば書換え対象ＥＣＵ１９へのインストールが何％完了したかを算出することである。

[0613] ＣＧＷ１３は、書換え対象ＥＣＵ１９からの通知に基づいてインストールが何％完了したか決定する。ＣＧＷ１３は、インストールが何％完了したかを示す進捗を車載ディスプレイ７及びセンター装置３に通知する。ＣＧＷ１３は、これらの処理を全ての書換え対象ＥＣＵ１９に対するインストールが完了するまで繰返す。ＣＧＷ１３は、インストールが全て完了すると、インストールフェーズが完了した旨の進捗を車載ディスプレイ７及びセンター装置３に通知する。

[0614] ＣＧＷ１３は、アクティベートフェーズであると判定すると（Ｓ２１０４：ＹＥＳ）、アクティベートフェーズの処理を実施し（Ｓ２１０８）、その

アクティベートフェーズフェーズの処理の進捗状態を示す進捗状態信号を車載ディスプレイ７及びＤＣＭ１２に送信する（Ｓ２１１１、第１進捗状態送信手順に相当する）。アクティベートフェーズの処理とは、例えば同一グループに属する１以上の書換え対象ＥＣＵ１９のアクティベートが何％完了したかを算出することである。ＣＧＷ１３は、書換え対象ＥＣＵ１９からの通知に基づいてアクティベートが何％完了したか決定する。ＣＧＷ１３は、アクティベートが何％完了したかを示す進捗を車載ディスプレイ７及びセンター装置に通知する。

[0615] ＣＧＷ１３は、アクティベートフェーズを完了したか否かを判定し（Ｓ２１１２）、アクティベートフェーズを完了したと判定すると（Ｓ２１１２：ＹＥＳ）、進捗状態の同期制御処理を終了する。ＣＧＷ１３は、アクティベートフェーズを完了していないと判定すると（Ｓ２１１２：ＮＯ）、Ｓ２１０２に戻る。そして、ＣＧＷ１３は、各フェーズの処理を進めると共に、処理が何％完了したかを算出する（Ｓ２１０７～Ｓ２１１０）。ＣＧＷ１３は、第１進捗状態としてフェーズ及びＸ％完了した旨を定期的にセンター装置３に送信する（Ｓ２１１１）。

[0616] センター装置３は、配信諸元データを送信し、進捗状態の同期制御処理を開始すると、ＤＣＭ１２から送信される第１進捗状態信号の受信を監視する（Ｓ２１２１）。センター装置３は、ＤＣＭ１２から第１進捗状態信号を受信したと判定すると（Ｓ２１２１：ＹＥＳ）、携帯端末６からのアクセスを許可し（Ｓ２１２２）、第１進捗状態信号により特定されるフェーズが何れであるかを判定する（Ｓ２１２３～Ｓ２１２６）。

[0617] センター装置３は、キャンペーン通知フェーズであると判定すると（Ｓ２１２３：ＹＥＳ）、キャンペーン通知フェーズの処理を実施する（Ｓ２１２７）。即ち、センター装置３は、キャンペーン通知フェーズの画面を作成すると共に、このキャンペーン通知フェーズの画面の表示を指示する表示指示信号を携帯端末６に送信し、携帯端末６においてセンター装置３への接続によりキャンペーン通知フェーズの画面を表示させる。

[0618] センター装置３は、ダウンロードフェーズであると判定すると（Ｓ２１２４：ＹＥＳ）、ダウンロードフェーズの処理を実施する（Ｓ２１２８）。即ち、センター装置３は、ダウンロードフェーズの画面を作成すると共に、ダウンロードフェーズの画面の表示を指示する表示指示信号を携帯端末６に送信し、携帯端末６においてセンター装置３への接続によりダウンロードフェーズの画面を表示させる。センター装置３は、ＤＣＭ１２からダウンロードが何％完了したかを示す進捗を通知されると、ダウンロードフェーズの画面を更新する。

[0619] センター装置３は、インストールフェーズであると判定すると（Ｓ２１２５：ＹＥＳ）、インストールフェーズの処理を実施する（Ｓ２１２９）。即ち、センター装置３は、インストールフェーズの画面を作成すると共に、インストールフェーズの画面の表示を指示する表示指示信号を携帯端末６に送信し、携帯端末６においてセンター装置３への接続によりインストールフェーズの画面を表示させる。センター装置３は、ＤＣＭ１２からインストールが何％完了したかを示す進捗を通知されると、インストールフェーズの画面を更新する。

[0620] センター装置３は、アクティベートフェーズであると判定すると（Ｓ２１２６：ＹＥＳ）、アクティベートフェーズの処理を実施する（Ｓ２１３０）。即ち、センター装置３は、アクティベートフェーズの画面を作成すると共に、アクティベートフェーズの画面の表示を指示する表示指示信号を携帯端末６に送信し、携帯端末６においてセンター装置３への接続によりアクティベートフェーズの画面を表示させる。センター装置３は、ＤＣＭ１２からアクティベートが何％完了したかを示す進捗を通知されると、アクティベートフェーズの画面を更新する。センター装置３は、Ｓ２１２７～Ｓ２１３０において表示した画面に対し、ユーザ承諾等の操作が行われた場合、第２進捗状態信号をマスタ装置１１に送信し（Ｓ２１３１）、進捗状態の同期制御処理を終了する。

[0621] 車載ディスプレイ７は、ＣＧＷ１３から配信諸元データを受信すると、進

捗表示処理を開始し、ＣＧＷ１３から送信される進捗状態信号の受信を監視する（Ｓ２１４１）。車載ディスプレイ７は、ＣＧＷ１３から進捗状態信号を受信したと判定すると（Ｓ２１４１：ＹＥＳ）、車載ディスプレイ７におけるユーザ操作を許可し（Ｓ２１４２）、進捗状態信号により特定されるフェーズが何れであるかを判定する（Ｓ２１４３～Ｓ２１４６）。

[0622] 車載ディスプレイ７は、キャンペーン通知フェーズであると判定すると（Ｓ２１４３：ＹＥＳ）、配信諸元データに含まれるテキスト、コンテンツ等を用いてキャンペーン通知フェーズの画面を表示する（Ｓ２１４７）。車載ディスプレイ７は、ダウンロードフェーズであると判定すると（Ｓ２１４４：ＹＥＳ）、ダウンロードフェーズの画面を表示する（Ｓ２１４８）。車載ディスプレイ７は、ＣＧＷ１３からダウンロードが何％完了したかを示す進捗を通知されると、ダウンロードフェーズの画面を更新する。

[0623] 車載ディスプレイ７は、インストールフェーズであると判定すると（Ｓ２１４５：ＹＥＳ）、インストールフェーズの画面を表示する（Ｓ２１４９）。車載ディスプレイ７は、ＣＧＷ１３からインストールが何％完了したかを示す進捗を通知されると、インストールフェーズの画面を更新する。車載ディスプレイ７は、アクティベートフェーズであると判定すると（Ｓ２１４６：ＹＥＳ）、アクティベートフェーズの画面を表示する（Ｓ２１５０）。車載ディスプレイ７は、ＣＧＷ１３からアクティベートが何％完了したかを示す進捗を通知されると、アクティベートフェーズの画面を更新する。

[0624] 以上に説明したように、マスタ装置１１とセンター装置３との間で第１進捗状態及び第２進捗状態を送受信するようにした。例えば携帯端末６がセンター装置３にアクセス可能であり、車載ディスプレイ７がセンター装置３にアクセス不能である構成であっても、マスタ装置１１とセンター装置３との間で第１進捗状態及び第２進捗状態を送受信することで、アプリプログラムの書換えの進捗状態等を複数の表示端末で適切に同期させることができる。

[0625] （２２）表示制御情報の送信制御処理、（２３）表示制御情報の受信制御処理

センター装置３における表示制御情報の送信制御処理について図１８１及び図１８２を参照して説明し、マスタ装置１１における表示制御情報の受信制御処理について図１８３から図１８５を参照して説明する。

[0626] 図１８１に示すように、センター装置３は、表示制御情報の送信制御部５４において、書込みデータ記憶部５４ａ（更新データ記憶部に相当する）と、表示制御情報記憶部５４ｂと、情報送信部５４ｃとを有する。書込みデータ記憶部５４ａは、複数の書換え対象ＥＣＵ１９に対するアプリプログラムの書換えを一つのキャンペーンとし、複数の書換え対象ＥＣＵ１９に対する書込みデータを記憶する。表示制御情報記憶部５４ｂは、表示制御情報を含む配信緒元データを記憶する。表示制御情報は、書換え対象ＥＣＵ１９におけるアプリプログラムの書換えに関与する表示情報が車載ディスプレイ７において表示されるのに必要な情報であり、表示制御プログラムやプロパティ情報である。

[0627] 表示情報とは、アプリプログラムの書換えに関与する各種画面（キャンペーン通知画面、インストール画面等）を構成するデータである。表示制御プログラムは、ウェブブラウザと同等の機能を実現するプログラムである。プロパティ情報は、表示文字、表示位置、色等を規定する情報である。情報送信部５４ｃは、書込みデータ記憶部５４ａに記憶されている書込みデータと、表示制御情報記憶部５４ｂに記憶されている表示制御情報とをマスタ装置１１に送信する。情報送信部５４ｃは、複数の書換え対象ＥＣＵ１９に対する書込みデータを１つのパッケージとしてマスタ装置１１に送信する。ここで、表示制御情報として、何れのフェーズで表示する情報であるかを示すフェーズ識別情報を含めても良い。例えばキャンペーン通知フェーズ、ダウンロードフェーズ、インストールフェーズ、及びアクティベートフェーズのうち何れのフェーズで表示する情報であるかを示すフェーズ識別情報である。

[0628] 次に、センター装置３における表示制御情報の送信制御部５４が行う作用について図１８２を参照して説明する。センター装置３は、表示制御情報の送信制御プログラムを実行し、表示制御情報の送信制御処理を行う。

[0629] センター装置３は、表示制御情報の送信制御処理を開始すると、配信緒元データをＤＣＭ１２を介してＣＧＷ１３に送信し（Ｓ２２０１、制御情報送信手順に相当する）、書込みデータをＤＣＭ１２を介してＣＧＷ１３に送信する（Ｓ２２０２）。センター装置３は、表示情報をＤＣＭ１２を介してＣＧＷ１３に送信し（Ｓ２２０３、表示情報送信手順に相当する）、表示制御情報の送信制御処理を終了する。尚、センター装置３は、キャンペーン通知フェーズ、ダウンロードフェーズ、インストールフェーズ、アクティベートフェーズの各フェーズに対応する表示制御情報を送信する場合には、各フェーズに対応する表示制御情報を１つのファイルに纏めて車載ディスプレイ７に送信しても良いし、フェーズを終了する毎に次のフェーズに対応する表示制御情報を車載ディスプレイ７に送信しても良い。ここで、センター装置３が配信緒元データを送信するタイミングは、マスタ装置１１からの求めに応じて送信する構成とすると良い。

[0630] 図１８３に示すように、ＣＧＷ１３は、表示制御情報の受信制御部８９において、情報受信部８９ａと、書換え指示部８９ｂと、表示指示部８９ｃとを有する。情報受信部８９ａは、センター装置３から書込みデータと表示制御情報とを受信する。書換え指示部８９ｂは、センター装置３から書込みデータが情報受信部８９ａにより受信されると、その受信された書込みデータの書込みを書換え対象ＥＣＵ１９に指示する。表示指示部８９ｃは、書換え指示部８９ｂが書込みデータの書込みを書換え対象ＥＣＵ１９に指示する前に、表示制御情報を用いて、キャンペーンに関する情報を表示するように車載ディスプレイ７に指示する。尚、表示指示部８９ｃは、書込みデータの書込みが全て完了した後に、履歴情報としてキャンペーンに関する情報を表示するように指示しても良い。

[0631] 次に、ＣＧＷ１３における表示制御情報の受信制御部８９が行う作用について図１８４を参照して説明する。ＣＧＷ１３は、表示制御情報の受信制御プログラムを実行し、表示制御情報の受信制御処理を行う。これにより、表示端末として携帯端末６と車載ディスプレイ７とを有する場合に、これらの

表示形態を近づけることができ、ユーザの利便性を向上させることができる。

[0632] ＣＧＷ１３は、表示制御情報の受信制御処理を開始すると、センター装置３からＤＣＭ１２を介して配信緒元データを受信し（Ｓ２３０１、制御情報受信手順に相当する）。センター装置３からＤＣＭ１２を介して書込みデータを受信する（Ｓ２３０２）。ＣＧＷ１３は、センター装置３からＤＣＭ１２を介して表示情報を受信する（Ｓ２３０３、表示情報受信手順に相当する）。ＣＧＷ１３は、センター装置３から配信諸元データに含まれている表示制御情報を用いるか否かを判定する（Ｓ２３０４）。ＣＧＷ１３は、表示制御情報を用いると判定すると（Ｓ２３０４：ＹＥＳ）、表示制御情報を用いて表示情報を表示するように車載ディスプレイ７に指示する（Ｓ２３０５）。即ち、ＣＧＷ１３は、表示制御情報を用いてアプリプログラムの書換えに関与する画面を表示するように車載ディスプレイ７に指示する。車載ディスプレイ７は、ＣＧＷ１３からの指示にしたがい、表示制御情報を用いて表示情報を表示する。

[0633] ＣＧＷ１３は、表示制御情報を用いないと判定すると（Ｓ２３０４：ＮＯ）、予め保有するコンテンツを用いて表示情報を表示するように車載ディスプレイ７に指示する（Ｓ２３０６）。即ち、ＣＧＷ１３は、予め保有するコンテンツを用いてアプリプログラムの書換えに関与する画面を表示するように車載ディスプレイ７に指示する。車載ディスプレイ７は、ＣＧＷ１３からの指示にしたがい、予め保有するコンテンツを用いて表示情報を表示する。尚、車載ディスプレイ７は、キャンペーン通知フェーズ、ダウンロードフェーズ、インストールフェーズ、アクティベートフェーズの各フェーズに対応する表示情報を表示する場合には、各フェーズに対応する表示制御情報を纏めてセンター装置３から受信しても良いし、フェーズを終了する毎に次のフェーズに対応する表示制御情報をセンター装置３から受信しても良い。

[0634] 図１８５に示すように、車載ディスプレイ７がウェブブラウザの機能を有しておらず、センター装置３からＤＣＭ１２及びＣＧＷ１３を介して車載デ

ィスプレイ７に送信される配信諸元データにプロパティ情報は含まれているが表示制御プログラムが含まれていなければ、車載ディスプレイ７は、予め保持するコンテンツやフレームを用いて表示情報を簡易的な画面でプロパティ情報を表示する。プロパティ情報とは、テキスト等のデータ及びその表示位置、サイズ等であり、センター装置３が作成する画面で用いるプロパティ情報と同一である。即ち、車載ディスプレイ７が表示する画面イメージは、センター装置３が作成する画面イメージと背景やビットマップ等の相違はあるものの、表示内容はセンター装置３と同等となる。

[0635] 車載ディスプレイ７がウェブブラウザの機能を有しておらず、センター装置３からＤＣＭ１２及びＣＧＷ１３を介して車載ディスプレイ７に送信される配信諸元データに表示制御プログラムとプロパティ情報が含まれていれば、車載ディスプレイ７は、表示情報をセンター装置３と同等な画面で表示する。ここで、配信諸元データに含まれる表示制御プログラムとプロパティ情報は、センター装置３が作成する画面で用いるものと同一である。

[0636] 車載ディスプレイ７がウェブブラウザの機能を有していないが表示制御プログラムを保持しており、センター装置３から車載ディスプレイ７に送信される配信諸元データにプロパティ情報が含まれていれば、車載ディスプレイ７は、表示情報をセンター装置３と同等な画面で表示する。ここで、車載ディスプレイ７が保持している表示制御プログラムは、例えば、センター装置３が作成する画面で用いる表示制御プログラムとバージョン違いである。

[0637] 車載ディスプレイ７がウェブブラウザの機能を有していれば、車載ディスプレイ７は、センター装置へ接続することにより表示情報をセンター装置３と同一の画面で表示する。

[0638] 以上に説明したように、センター装置３は、表示制御情報の送信制御処理を行うことで、表示制御情報を車載ディスプレイ７に送信し、車載ディスプレイ７において表示情報を表示制御情報にしたがって表示させる。これにより、表示端末として携帯端末６と車載ディスプレイ７とを有する場合に、これらの表示形態を近づけることができ、ユーザの利便性を高めることができ

る。ＣＧＷ１３は、表示制御情報の受信制御処理を行うことで、表示制御情報をセンター装置３から受信し、表示情報をセンター装置３から受信し、表示情報を表示制御情報にしたがって表示する。

[0639] （２４）進捗表示の画面表示制御処理

進捗表示の画面表示制御処理について図１８６から図２１０を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３において進捗表示の画面表示制御処理を行う。

[0640] 図１８６に示すように、ＣＧＷ１３は、進捗表示の画面表示制御部９０において、モード判定部９０ａと、画面表示指示部９０ｂとを有する。

[0641] モード判定部９０ａは、ユーザのカスタマイズ操作によりカスタマイズモードが設定されているか否かを判定する。又、モード判定部９０ａは、外部からの外部モードが設定されているか否かを書換え諸元データに含まれるシーン情報により判定する。即ち、モード判定部９０ａは、図８に示す書換え諸元データに含まれるシーン情報を参照する。図８及び図１８７に示すように、書換え諸元データには、シーン情報、有効期限情報、位置情報が格納されている。シーン情報は、本更新のシーン（種類、場面等）を示すと同時に、本更新の画面表示を指定するものである。具体的には、リコールフラグ、ディーラーフラグ、工場用フラグ、機能更新通知フラグ、強制実行フラグがある。

[0642] リコールフラグは、リコールに応じてアプリプログラムの書換えを行う場合の画面表示を指定するフラグである。リコールとは、設計や製造上の過誤等により製品に欠陥があることが判明した場合に、法令の規定又は製造者や販売者の判断で無償修理や交換や回収等の措置を行うことである。

[0643] ディーラーフラグは、ディーラーにおいてアプリプログラムの書換えを行う場合の画面表示を指定するフラグである。工場用フラグは、工場においてアプリプログラムの書換えを行う場合の画面表示を指定するフラグである。機能更新通知フラグは、機能更新通知に応じてアプリプログラムの書換えを行う場合の画面表示を指定するフラグである。機能更新通知とは、特定の機

能を更新することである。例えば機能更新通知フラグは、新たな機能を有償（又は無償）で追加するためのプログラム更新における画面表示を指定するフラグである。

[0644] 強制実行フラグは、強制実行に応じてアプリプログラムの書換えを行う場合の画面表示を指定するフラグである。強制実行とは、キャンペーン通知を所定回数繰返しているが、そのアプリプログラムの書換えが行われないことにより、アプリプログラムの書換えを強制的に行うことである。例えば強制実行フラグは、プログラム更新を強制的に行う場合の画面表示を指定するフラグである。

[0645] これらシーン情報を示すフラグは、該当がない場合は全てが０（フラグ不成立）であり、該当がある場合は何れかが１（フラグ成立）となるよう設定される。モード判定部９０ａは、例えばリコールフラグが成立しているときには、リコールモードが設定されていると判定し、ディーラーフラグが成立しているときには、ディーラーモードが設定されていると判定し、工場フラグが成立しているときには、工場モードが設定されていると判定し、機能更新通知フラグが成立しているときには、機能更新モードが設定されていると判定し、強制実行フラグが成立しているときには、強制実行モードが設定されていると判定する。

[0646] 有効期限情報は、有効期限を示す情報であり、アプリプログラムの書換えを実行するか否かの判定基準となる情報である。ＣＧＷ１３は、現在時刻が有効期限情報により示される有効期限内であれば、アプリプログラムの書換えを実行し、現在時刻が有効期限情報により示される有効期限外であれば、アプリプログラムの書換えを実行しない。即ち、ＣＧＷ１３は、配信パッケージをダウンロードした後、プログラムのインストールを行う際に有効期限情報を参照し、仮に現在時刻が有効期限外であれば、プログラムのインストールを実行せず、配信パッケージを破棄する。

[0647] 位置情報は、位置を示す情報であり、アプリプログラムの書換えを実行するか否かの判定基準となる情報であり、許可エリアと禁止エリアがある。Ｃ

ＧＷ１３は、位置情報として許可エリアが指定されている場合には、車両の現在位置が位置情報により示される許可エリア内であれば、アプリプログラムの書換えを実行し、車両の現在位置が位置情報により示される許可エリア外であれば、アプリプログラムの書換えを実行しない。ＣＧＷ１３は、位置情報として禁止エリアが指定されている場合には、車両の現在位置が位置情報により示される禁止エリア外であれば、アプリプログラムの書換えを実行し、車両の現在位置が位置情報により示される禁止エリア内であれば、アプリプログラムの書換えを実行しない。即ち、ＣＧＷ１３は、配信パッケージをダウンロードした後、プログラムのインストールを行う際に位置情報を参照し、仮に現在位置が許可エリア外であれば、プログラムのインストールを実行せず、許可エリア内となるまでインストールを待機する。

[0648] 画面表示指示部９０ｂは、アプリプログラムの書換えに応じた画面表示を表示端末５に指示する。画面表示指示部９０ｂは、アプリプログラムの書換えのフェーズに対応する画面の表示有無を指示すること、画面の項目の表示有無を指示すること、画面の項目の表示内容の変更を指示することにより、画面表示を表示端末５に指示する。

[0649] ユーザのカスタマイズ操作について説明する。尚、ここでは、車載ディスプレイ７が表示する画面について説明するが、携帯端末６が表示する画面についても同様である。尚、後述する画面において、ボタンの個数や配置等のレイアウトは例示した以外であっても良い。ユーザが車載ディスプレイ７においてメニュー画面の表示操作を行うと、ＣＧＷ１３は、図１８８に示すように、メニュー選択画面５１１を車載ディスプレイ７に表示させる。ＣＧＷ１３は、メニュー選択画面５１１では、「ソフトウェアップデート」ボタン５１１ａ、「アップデート結果確認」ボタン５１１ｂ、「ソフトウェアバージョン一覧」ボタン５１１ｃ、「更新履歴」ボタン５１１ｄ、「ユーザ情報登録」ボタン５１１ｅを表示させ、ユーザの操作を待機する。

[0650] この状態からユーザが「ユーザ情報登録」ボタン５１１ｅを操作すると、ＣＧＷ１３は、図１８９に示すように、ユーザ選択画面５１２を車載ディス

プレイ７に表示させる。ＣＧＷ１３は、ユーザ選択画面５１２では、「ユーザ」ボタン５１２ａ～５１２ｃを表示させ、ユーザの操作を待機する。

[0651] この状態からユーザが「ユーザ」ボタン５１２ａを操作すると、ＣＧＷ１３は、図１９０に示すように、ユーザ登録画面５１３を車載ディスプレイ７に表示させる。ＣＧＷ１３は、ユーザ登録画面５１３では、個人情報登録としてメールアドレス及びＶＩＮ情報（個車識別情報）の入力欄を表示させ、課金情報登録としてクレジットカード番号及び有効期限の入力欄を表示させ、アプリプログラムの書換え設定として、キャンペーン通知、ダウンロード、インストール、アクティベートの「オンオフ」ボタン５１３ａ～５１３ｄを表示させ、「詳細情報」ボタン５１３ｅを表示させ、ユーザの操作を待機する。

[0652] キャンペーン通知、ダウンロード、インストール、アクティベートの「オンオフ」ボタン５１３ａ～５１３ｄは、キャンペーン通知、ダウンロード、インストール、アクティベートについて画面表示を行うか否かを選択するボタンである。具体的には、キャンペーン通知を受信した際、ダウンロードを開始する際、インストールを開始する際、アクティベートを開始する際に、ユーザ承諾を求めるコンテンツ表示を行うか否かを、ユーザに予め選択させるボタンである。「詳細情報」ボタン５１３ｅは、上記した有効期限情報及び位置情報を登録するボタンである。これらユーザが設定した情報は、ＤＣＭ１２を介してセンター装置３に送信される。尚、これらの情報をユーザが携帯端末６で設定した場合、ＣＧＷ１３は、これらの情報をＤＣＭ１２を介してセンター装置３から取得する。

[0653] ユーザは、キャンペーン通知、ダウンロード、インストール、アクティベートについて、画面を煩わしいと感じる場合であれば、該当する「オンオフ」ボタン５１３ａ～５１３ｄをオフに設定すれば良い。オフに設定することにより、ユーザ承諾を求めるコンテンツの表示は省略されることとなる。ユーザは、例えばキャンペーン通知やアクティベートの画面表示を煩わしくないが、ダウンロードやインストールの画面表示を煩わしいと感じる場合であ

れば、キャンペーン通知を「オンオフ」ボタン５１３ａによりオンに設定し、ダウンロードを「オンオフ」ボタン５１３ｂによりオフに設定し、インストールを「オンオフ」ボタン５１３ｃによりオフに設定し、アクティベートを「オンオフ」ボタン５１３ｄによりオンに設定すれば良い。

[0654] この場合、表示端末５は、例えばキャンペーン通知がオン、ダウンロードがオフ、インストールがオフ、アクティベートがオンに設定されていれば、アプリプログラムの書換えフェーズに応じて、キャンペーン通知画面を表示し、ダウンロード承諾画面及びダウンロード実行中画面を表示せず、インストール承諾画面及びインストール実行中画面を表示せず、アクティベート画面を表示する。即ち、ユーザは、キャンペーン通知、ダウンロード、インストール、アクティベートのフェーズにおいて、オンに設定すれば、そのオンに設定したフェーズの画面表示が行われ、オフに設定すれば、そのオフに設定したフェーズの画面表示が行われず、画面表示をカスタマイズすることができる。このような画面表示のオンオフの設定は、フェーズ毎に個別に設定可能でも良いし、全てのフェーズを一括して一度に設定可能でも良い。

[0655] 又、ユーザは、有効期限、許可エリア、禁止エリアを登録したい場合であれば、「詳細情報」ボタン５１３ｅを操作し、有効期限、許可エリア、禁止エリアを設定すれば良い。ユーザは、有効期限情報としてアプリプログラムの書換えを許可する有効期限をカスタマイズすることができ、位置情報としてアプリプログラムの書換えを許可する許可エリアや禁止する禁止エリアをカスタマイズすることができる。

[0656] 次に、上記した構成の作用について図１９１から図２１４を参照して説明する。ＣＧＷ１３は、進捗表示の画面表示制御プログラムを実行し、進捗表示の画面表示制御処理を行う。

[0657] ＣＧＷ１３は、進捗表示の画面表示制御処理を開始すると、書換え諸元データに有効期限情報が格納されている否か、及びカスタマイズ情報に有効期限情報が設定されているか否かを判定する（Ｓ２４０１）。ＣＧＷ１３は、書換え諸元データに有効期限情報が格納されていると判定すると（Ｓ２４０

１：ＹＥＳ）、現在時刻が有効期限情報を満たしているか否かを判定する（Ｓ２４０２）。ＣＧＷ１３は、書換え諸元データに格納された有効期限情報と、カスタマイズ情報として設定された有効期限情報とが存在する場合に、両方を満たしているか否かを判定する。ＣＧＷ１３は、現在時刻が有効期限情報により示される有効期限外であり、現在時刻が有効期限情報を満たしていないと判定すると（Ｓ２４０２：ＮＯ）、進捗表示の画面表示制御処理を終了する。

[0658] ＣＧＷ１３は、現在時刻が有効期限情報により示される有効期限内であり、現在時刻が有効期限情報を満たしていると判定すると（Ｓ２４０２：ＹＥＳ）、書換え諸元データにシーン情報が格納されている否かを判定する（Ｓ２４０３）。ＣＧＷ１３は、書換え諸元データにシーン情報が格納されていると判定すると（Ｓ２４０３：ＹＥＳ）、外部モードが設定されていると判定し、そのシーン情報の設定内容にしたがう表示指示処理に移行し（Ｓ２４０４）、アプリプログラムの書換えに応じた画面表示を、その成立しているフラグのモードにしたがって行うように車載ディスプレイ７に指示する。ＣＧＷ１３は、例えばリコールフラグが成立していれば、アプリプログラムの書換え中に応じた画面表示を、リコールモードにしたがって行うように車載ディスプレイ７に指示する。ＣＧＷ１３は、例えばディーラーフラグが成立していれば、アプリプログラムの書換え中に応じた画面表示を、ディーラーモードにしたがって行うように車載ディスプレイ７に指示する。

[0659] ＣＧＷ１３は、書換え諸元データにシーン情報が格納されていないと判定すると（Ｓ２４０３：ＮＯ）、ユーザのカスタマイズ操作によりカスタマイズモードが設定されているか否かを判定する（Ｓ２４０５、カスタマイズモード判定手順に相当する）。ＣＧＷ１３は、カスタマイズモードが設定されていると判定すると（Ｓ２４０５：ＹＥＳ）、カスタマイズ操作の設定内容にしたがう表示指示処理に移行し（Ｓ２４０６、画面表示指示手順に相当する）、アプリプログラムの書換えに応じた画面表示を、カスタマイズモードにしたがって行うように車載ディスプレイ７に指示する。

[0660] ＣＧＷ１３は、カスタマイズモードが設定されていないと判定すると（Ｓ２４０５：ＮＯ）、初期設定の設定内容にしたがう表示指示処理に移行し（Ｓ２４０７、画面表示指示手順に相当する）、アプリプログラムの書換えに応じた画面表示を、カスタマイズモードにしたがって行うように車載ディスプレイ７に指示する。即ち、ＣＧＷ１３は、書換え諸元データに格納されたシーン情報を優先して適用し、シーン情報が格納されていないときに、カスタマイズモードを適用する。シーン情報及びカスタマイズモードのいずれも存在しない場合には、初期設定を適用する。ここで、初期設定とは、予め設定された値であり、例えばキャンペーン通知、ダウンロード、インストール及びアクティベートのいずれの設定もオンとする設定を初期設定とする。

[0661] 続いて、図１９２を用いて、Ｓ２４０４、Ｓ２４０６及びＳ２４０７の画面表示指示処理について説明する。ここでは、インストールフェーズにおける画面表示指示処理について例示するが、他のフェーズについても同様である。ＣＧＷ１３は、表示指示処理に移行すると、画面の表示有無を設定し（Ｓ２４１１）、画面の項目の表示有無を設定し（Ｓ２４１２）、画面の項目の表示内容の変更を指示する（Ｓ２４１３）。ＣＧＷ１３は、画面表示要求通知をＤＣＭ１２に送信し、画面表示要求をＤＣＭ１２から車載ディスプレイ７に送信させ（Ｓ２４１４）、ＤＣＭ１２からの操作結果情報の受信を待機する（Ｓ２４１５）。操作結果情報とは、ユーザがいずれのボタンを操作したかを示す情報である。尚、ＣＧＷ１３が画面表示要求通知を車載ディスプレイ７に直接送信し、操作結果情報を受信するようにしても良い。

[0662] ＣＧＷ１３は、車載ディスプレイ７からＤＣＭ１２に操作結果が送信されたことで、ＤＣＭ１２からの操作結果情報の受信を判定すると（Ｓ２４１５：ＹＥＳ）、その操作結果情報に基づいて承諾確認を行い、ユーザがアプリプログラムの書換えを承諾したか否かを判定する（Ｓ２４１６）。

[0663] ＣＧＷ１３は、ユーザがアプリプログラムの書換えを承諾したと判定すると（Ｓ２４１６：ＹＥＳ）、書換え諸元データに位置情報が格納されている否かを判定する（Ｓ２４１７）。ＣＧＷ１３は、書換え諸元データに位置情

報が格納されていると判定すると（Ｓ２４１７：ＹＥＳ）、車両の現在位置が位置情報を満たしているか否かを判定する（Ｓ２４１８）。尚、インストールフェーズ以外では、Ｓ２４１７及びＳ２４１８を省略しても良い。ＣＧＷ１３は、位置情報が許可エリアである場合、車両の現在位置が許可エリア内であれば、車両の現在位置が位置情報を満たしていると判定し（Ｓ２４１８：ＹＥＳ）、アプリプログラムの書換えを継続する（Ｓ２４１９）。

[0664] 一方、ＣＧＷ１３は、車両の現在位置が許可エリア外であれば、車両の現在位置が位置情報を満たしていないと判定し、アプリプログラムの書換えを継続せずに中止し、画面表示指示処理を終了する。ＣＧＷ１３は、位置情報が禁止エリアである場合、車両の現在位置が禁止エリア外であれば、車両の現在位置が位置情報を満たしていると判定し（Ｓ２４１８：ＹＥＳ）、アプリプログラムの書換えを継続し（Ｓ２４１９）、画面表示指示処理を終了する。ＣＧＷ１３は、車両の現在位置が禁止エリア内であれば、車両の現在位置が位置情報を満たしていないと判定し、アプリプログラムの書換えを継続せずに中止し、表示指示処理を終了する。

[0665] ＣＧＷ１３からＤＣＭ１２に送信される画面表示要求通知、ＤＣＭ１２からＣＧＷ１３に送信される操作結果情報について説明する。図１９３に示すように、ＣＧＷ１３からＤＣＭ１２に送信される画面表示要求通知には、フェーズＩＤ、シーンＩＤ、画面構成情報が含まれる。フェーズＩＤとは、キャンペーン通知、ダウンロード、インストール、アクティベートという各フェーズを識別するＩＤである。シーンＩＤとは、図１８７に示すシーン情報を識別するＩＤである。ＤＣＭ１２からＣＧＷ１３に送信される操作結果情報には、送信元情報、フェーズＩＤ、シーンＩＤ、操作結果、追加情報が含まれる。ＣＧＷ１３は、画面表示要求通知に格納されているフェーズＩＤ及びシーンＩＤと、操作結果情報に格納されているフェーズＩＤ及びシーンＩＤとを照合し、乖離や調停の確認を行う。

[0666] 即ち、ＣＧＷ１３は、ＤＣＭ１２に送信した画面表示要求通知に格納されているフェーズＩＤ及びシーンＩＤと、ＤＣＭ１２から受信した操作結果情

報に格納されているフェーズＩＤ及びシーンＩＤとが一致していれば、画面表示要求通知と操作結果情報とが整合しており、画面表示要求通知と操作結果情報とが乖離しておらず、調停を行う必要がないと判定する。一方、ＣＧＷ１３は、ＤＣＭ１２に送信した画面表示要求通知に格納されているフェーズＩＤ及びシーンＩＤと、ＤＣＭ１２から受信した操作結果情報に格納されているフェーズＩＤ及びシーンＩＤとが一致していなければ、画面表示要求通知と操作結果情報とが整合しておらず、画面表示要求通知と操作結果情報とが乖離しており、調停を行う必要があると判定する。ＣＧＷ１３は、ＤＣＭ１２から受信した操作結果情報にしたがって処理を行うか否かの調停を行う。

[0667] 画面構成情報は、画面の構成要素を示す情報であり、図１９４に示すように、例えばアクティベート承諾画面５１４では、「キャンペーンＩＤ…」ボタン５１４ａ、「更新名称Ａ…」ボタン５１４ｂ、「更新名称Ｂ…」ボタン５１４ｃ、「詳細確認」ボタン５１４ｄ、「戻る」ボタン５１４ｅ、「ＯＫ」ボタン５１４ｆの６項目がある。この場合、図１９５に示すように、画面構成情報の６項目の全てが「表示」に設定されていれば、図１９４に示したように、アクティベート承諾画面５１４に６項目の全てが表示される。即ち、ユーザは、「キャンペーンＩＤ…」ボタン５１４ａ、「更新名称Ａ…」ボタン５１４ｂ、「更新名称Ｂ…」ボタン５１４ｃ、「詳細確認」ボタン５１４ｄ、「戻る」ボタン５１４ｅ、「ＯＫ」ボタン５１４ｆの何れかを操作可能である。

[0668] 一方、図１９６に示すように、画面構成情報の６項目のうち「キャンペーンＩＤ…」ボタン５１４ａ、「更新名称Ａ…」ボタン５１４ｂ、「更新名称Ｂ…」ボタン５１４ｃ、「詳細情報」ボタン５１４ｄ、「ＯＫ」ボタン５１４ｆが「表示」に設定され、「戻る」ボタン５１４ｅが非表示に設定されていれば、図１９７に示すように、アクティベート承諾画面５１４に「キャンペーンＩＤ…」ボタン５１４ａ、「更新名称Ａ…」ボタン５１４ｂ、「更新名称Ｂ…」ボタン５１４ｃ、「詳細情報」ボタン５１４ｄ、「ＯＫ」ボタン

５１４ｆが表示される一方で、「戻る」ボタン５１４ｅが表示されない。即ち、ユーザは、「キャンペーンＩＤ…」ボタン５１４ａ、「更新名称Ａ…」ボタン５１４ｂ、「更新名称Ｂ…」ボタン５１４ｃ、「詳細確認」ボタン５１４ｄ、「ＯＫ」ボタン５１４ｆの何れかを操作可能であるが、「戻る」ボタン５１４ｅが表示されていないので、「戻る」ボタン５１４ｅを操作不能である。例えばリコール等による重要度や緊急度が比較的高いアプリプログラムの書換えについては、そのアクティベートを拒否することが望ましくないので、上記したように「戻る」ボタン５１４ｅを操作不能とすることで、そのアクティベートを拒否することがないように設定可能となる。この場合、ユーザが「ＯＫ」ボタン５１４ｆを操作することで、アクティベートを承諾したこととなる。

[0669] ＣＧＷ１３、ＤＣＭ１２、車載ディスプレイ７、センター装置３、メータ装置４５との間で送受信される画面表示、ユーザ操作に関するメッセージフレームワークについて説明する。図１９８に示すように、ＣＧＷ１３とＤＣＭ１２はＣＡＮやイーサーネットで接続されており、ＤＣＭ１２と車載ディスプレイ７はＵＳＢで接続されている。

[0670] ＣＧＷ１３は、ＤＣＭ１２を介してセンター装置３との間でデータ通信を行う。ＣＧＷ１３からダイアグ通信により送信されたデータは、ＤＣＭ１２でプロトコル変換され、ＤＣＭ１２からＨＴＴＰ通信によりセンター装置３に受信される。例えばＣＧＷ１３は、現在のフェーズや進捗割合等の現在進捗状態を示すデータを、ＤＣＭ１２を介してセンター装置３に送信する。センター装置３からＨＴＴＰ通信により送信されたデータは、ＤＣＭ１２でプロトコル変換され、ＤＣＭ１２からダイアグ通信によりＣＧＷ１３に受信される。

[0671] ＣＧＷ１３は、ＤＣＭ１２を介して車載ディスプレイ７との間でデータ通信を行う。ＣＧＷ１３からダイアグ通信により送信されたデータは、ＤＣＭ１２でプロトコル変換され、ＤＣＭ１２からＵＳＢ通信により車載ディスプレイ７に受信される。車載ディスプレイ７からＵＳＢ通信により送信された

データは、ＤＣＭ１２でプロトコル変換され、ＤＣＭ１２からダイアグ通信によりＣＧＷ１３に受信される。例えばＣＧＷ１３は、車載ディスプレイ７におけるユーザ操作に関する情報を、ＤＣＭ１２を介して取得する。このように車両用プログラム書換えシステム１では、ＤＣＭ１２にプロトコル変換機能を持たせ、携帯端末６と車載ディスプレイ７とをＣＧＷ１３が同様に扱えるよう構成する。又、ユーザ操作に関する情報をＣＧＷ１３へ集約することにより、ＣＧＷ１３が複数の操作端末におけるユーザ操作結果を調停し、現在進捗状態を管理できるようにしている。

[0672] ＣＧＷ１３、ＤＣＭ１２、車載ディスプレイ７との間で送受信されるメッセージフレームのシーケンスについて説明する。図１９９から図２０６に示すように、ＣＧＷ１３からＤＣＭ１２に送信される画面表示要求通知、ＤＣＭ１２からＣＧＷ１３に送信される操作結果情報において、キャンペーン通知ではフェーズＩＤを「０３」とし、ダウンロードではフェーズＩＤを「０４」とし、インストールではフェーズＩＤを「０５」とし、アクティベートではフェーズＩＤを「０６」としている。キャンペーン通知、ダウンロード、インストール及びアクティベートの各フェーズにおいて、メッセージフレームの送受信の順序は同じとし、フェーズＩＤを異ならせることで、フェーズを区分している。

[0673] 図１９９では、キャンペーン通知フェーズを例示している。ＣＧＷ１３は、現在進捗状態を管理しており、フェーズＩＤ、シーンＩＤ及び画面構成情報を指定し、画面表示要求通知をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３から画面表示要求通知を受信すると、画面表示要求を車載ディスプレイ７に送信する。車載ディスプレイ７は、ＤＣＭ１２から画面表示要求を受信すると、キャンペーン通知時の画面を表示し、ユーザがキャンペーン通知の確認操作を行うと、その操作結果をＤＣＭ１２に送信する。ＤＣＭ１２は、車載ディスプレイ７から操作結果を受信すると、操作結果情報をＣＧＷ１３に送信する。ＣＧＷ１３に受信される操作結果情報には、送信元情報、フェーズＩＤ、シーンＩＤ、操作結果及び追加情報が指定されている。ＣＧ

Ｗ１３は、ＤＣＭ１２から受信した操作結果情報に基づいて現在進捗状態を更新する。ここでは、ＣＧＷ１３は、キャンペーン通知フェーズにて承諾操作があった場合、現在進捗状態をダウンロードフェーズに更新する。

する。

[0674] 図２００では、ダウンロードフェーズを例示している。ＣＧＷ１３は、現在進捗状態を管理しており、フェーズＩＤ、シーンＩＤ及び画面構成情報を指定し、画面表示要求通知をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３から画面表示要求通知を受信すると、画面表示要求を車載ディスプレイ７に送信する。車載ディスプレイ７は、ＤＣＭ１２から画面表示要求を受信すると、ダウンロード承諾時の画面を表示し、ユーザがダウンロードの承諾操作を行うと、その操作結果をＤＣＭ１２に送信する。ＤＣＭ１２は、車載ディスプレイ７から操作結果を受信すると、操作結果情報をＣＧＷ１３に送信する。ＣＧＷ１３に受信される操作結果情報には、送信元情報、フェーズＩＤ、シーンＩＤ、操作結果及び追加情報が指定されている。ＣＧＷ１３は、ＤＣＭ１２から受信した操作結果情報に基づいて現在進捗状態を更新する。ここでは、ＣＧＷ１３は、ダウンロードフェーズにて承諾操作があった場合、現在進捗状態をインストールフェーズに更新する。

[0675] 図２０１では、インストールフェーズを例示している。ＣＧＷ１３は、現在進捗状態を管理しており、フェーズＩＤ、シーンＩＤ及び画面構成情報を指定し、画面表示要求通知をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３から画面表示要求通知を受信すると、画面表示要求を車載ディスプレイ７に送信する。車載ディスプレイ７は、ＤＣＭ１２から画面表示要求を受信すると、インストール承諾時の画面を表示し、ユーザがインストールの承諾操作を行うと、その操作結果をＤＣＭ１２に送信する。ＤＣＭ１２は、車載ディスプレイ７から操作結果を受信すると、操作結果情報をＣＧＷ１３に送信する。ＣＧＷ１３に受信される操作結果情報には、送信元情報、フェーズＩＤ、シーンＩＤ、操作結果及び追加情報が指定されている。ＣＧＷ１３は、ＤＣＭ１２から受信した操作結果情報に基づいて現在進捗状態を更新する

。ここでは、ＣＧＷ１３は、インストールフェーズにて承諾操作があった場合、現在進捗状態をアクティベートフェーズに更新する。

[0676] 図２０２では、アクティベートフェーズを例示している。ＣＧＷ１３は、現在進捗状態を管理しており、フェーズＩＤ、シーンＩＤ及び画面構成情報を指定し、画面表示要求通知をＤＣＭ１２に送信する。ＤＣＭ１２は、ＣＧＷ１３から画面表示要求通知を受信すると、画面表示要求を車載ディスプレイ７に送信する。車載ディスプレイ７は、ＤＣＭ１２から画面表示要求を受信すると、アクティベート承諾時の画面を表示し、ユーザがアクティベートの承諾操作を行うと、その操作結果をＤＣＭ１２に送信する。ＤＣＭ１２は、車載ディスプレイ７から操作結果を受信すると、操作結果情報をＣＧＷ１３に送信する。ＣＧＷ１３に受信される操作結果情報には、送信元情報、フェーズＩＤ、シーンＩＤ、操作結果及び追加情報が指定されている。ＣＧＷ１３は、ＤＣＭ１２から受信した操作結果情報に基づいて現在進捗状態を更新する。

[0677] 画面表示について図２０３から図２１０を参照して説明する。ＣＧＷ１３は、カスタマイズモードが設定されておらず、書換え諸元データのシーン情報に何れのフラグも設定されていない場合には、アプリプログラムの書換えに応じた画面表示を、初期設定の内容にしたがって表示端末５に指示する（Ｓ２４０７）。ＣＧＷ１３は、初期設定が、キャンペーン通知、ダウンロード、インストール、アクティベートの全てをオンする設定であれば、ＣＧＷ１３は、前述した図３１から図４６に示したように、ナビゲーション画面５０１、キャンペーン通知画面５０２、ダウンロード承諾画面５０３、ダウンロード実行中画面５０４、ダウンロード完了通知画面５０５、インストール承諾画面５０６、インストール実行中画面５０７、アクティベート承諾画面５０８、アクティベート完了通知画面５０９、確認操作画面５１０を順次表示するように、画面表示を表示端末５に指示する。このとき、キャンペーン通知画面５０２、ダウンロード承諾画面５０３、インストール承諾画面５０６、アクティベート承諾画面５０８、確認操作画面５１０では、ユーザの承

諾（ＯＫ）を得るためのコンテンツを表示する。

[0678] ＣＧＷ１３は、ユーザのカスタマイズモードが設定されている場合には、アプリプログラムの書換えに応じた画面表示を、カスタマイズモードの内容にしたがって表示端末５に指示する（Ｓ２４０６）。ただし、シーン情報が指定されていない場合に限る。ＣＧＷ１３は、例えばカスタマイズモードにおいてキャンペーン通知がオン、ダウンロードがオフ、インストールがオフ、アクティベートがオンに設定されていれば、キャンペーン通知画面５０２を表示した後に、ダウンロード承諾画面５０３、ダウンロード実行中画面５０４、ダウンロード完了通知画面５０５、インストール承諾画面５０６及びインストール実行中画面５０７を表示せず、アクティベート承諾画面５０８を表示するように、画面表示を表示端末５に指示する。

[0679] ＣＧＷ１３は、書換え諸元データのシーン情報にリコールフラグが設定されている場合には、アプリプログラムの書換えに応じた画面表示を、リコールモードの内容にしたがって表示端末５に指示する（Ｓ２４０４）。この場合、ＣＧＷ１３は、図２０４に示すように、キャンペーン通知画面５０２では、「後で」ボタン５０２ａを非表示とする。又、ＣＧＷ１３は、図２０５及び図２０６に示すように、ダウンロード承諾画面５０３では、「戻る」ボタン５０３ｃを非表示とする。又、ＣＧＷ１３は、図２０７に示すように、ダウンロード実行中画面５０４では、「戻る」ボタン５０４ｂを非表示とする。又、ＣＧＷ１３は、図２０８及び図２０９に示すように、インストール承諾画面５０５では、「戻る」ボタン５０５ｂを非表示とする。又、ＣＧＷ１３は、図２１０に示すように、アクティベート承諾画面５１８では、「戻る」ボタンを非表示とする。

[0680] 即ち、書換え諸元データのシーン情報にリコールフラグが設定されている場合には、上記したように「後で」ボタンや「戻る」ボタンが非表示に設定されることで、「後で」ボタンや「戻る」ボタンを表示しないようにすれば良い。又は、キャンペーン通知画面５０２を表示し、ダウンロード承諾画面５０３においてユーザの承諾を得た後は、インストール承諾画面５０５、ア

クティベート承諾画面５１８の表示を省略しても良い。以上は、書換え諸元データのシーン情報にリコールフラグが設定されている場合について説明したが、書換え諸元データのシーン情報にディーラーフラグ、工場用フラグ、機能更新通知フラグ、強制実行フラグが設定されている場合も同様であり、アプリプログラムの書換えを行う状況に応じてフェーズに対応する画面の表示有無、画面の項目の表示有無、画面の項目の表示内容の変更を指示すれば良い。

[0681] 具体的に説明すると、書換え諸元データのシーン情報にディーラーフラグが設定されている場合には、ディーラー環境において修理工程での専用の画面表示が必要となるので、ユーザ用の画面ではなく、ディーラー用の専用の画面を表示すれば良い。即ち、ユーザがアプリプログラムの書換えに関する操作を行うのではなく、ディーラーの作業者がアプリプログラムの書換えに関する操作を行うので、ディーラーの作業用に「後で」ボタンや「戻る」ボタンが表示に設定されることで、「後で」ボタンや「戻る」ボタンを表示するようにすれば良い。尚、例えば「ディーラーでの書換えを実施してください」等のガイダンスを表示し、ディーラーへの車両の入庫を促しても良い。

[0682] 書換え諸元データのシーン情報に工場用フラグが設定されている場合には、工場環境での製造工程では画面表示を必要としないので、画面を表示しないようにすれば良い。

[0683] 書換え諸元データのシーン情報に機能更新通知フラグが設定されている場合には、ユーザがカスタマイズで表示不要の設定をしていても、ユーザへ確実に変更内容を通知するための画面表示が必要となるので、カスタマイズの設定に拘らずユーザ向けの画面を表示すれば良い。即ち、ユーザが承諾を不要と判断している場合でも、承諾を強制的に実施させ、承諾画面を強制的に表示するようにすれば良いので、上記したように「後で」ボタンや「戻る」ボタンが表示に設定されることで、「後で」ボタンや「戻る」ボタンを表示するようにすれば良い。

[0684] 書換え諸元データのシーン情報に強制実行フラグが設定されている場合に

は、ユーザがカスタマイズで表示必要の設定をしており、ユーザが承諾を行わない場合でも、車両のソフトウェア更新を確実に実施するための強制実行が必要となるので、カスタマイズの設定に拘らずユーザ向けの画面を表示すれば良い。即ち、ユーザが承諾必要と判断していながら承諾不要でもアプリプログラムの書換えを実施するので、上記したように「後で」ボタンや「戻る」ボタンが非表示に設定されることで、「後で」ボタンや「戻る」ボタンを表示しないようにすれば良い。又、承諾をすることを前提とした機能となるので、画面自体を表示せず承諾を得たものとして書換えを実行しても良い。

[0685] 以上に説明したように、ＣＧＷ１３は、進捗表示の画面表示制御処理を行うことで、カスタマイズモードが設定されている場合に、カスタマイズモードの設定内容に応じた画面表示を表示端末５に指示するようにした。書換えの進捗に応じた画面表示をユーザがカスタマイズすることができる。

[0686] （２５）プログラム更新の報知制御処理

プログラム更新の報知制御処理について図２１１から図２１７を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３においてプログラム更新の報知制御処理を行う。

[0687] 図２１１に示すように、ＣＧＷ１３は、プログラム更新の報知制御部９１において、フェーズ特定部９１ａと、表示指示部９１ｂと、インジケータ表示制御部９１ｃと、アイコン表示制御部９１ｄと、詳細情報表示制御部９１ｅと、無効化指示部９１ｆと、を備える。フェーズ特定部９１ａは、プログラム更新の進捗状況としてのフェーズを特定する。フェーズ特定部９１ａは、プログラム更新のフェーズとして、キャンペーン通知、ダウンロード承諾、ダウンロード実行中、インストール承諾、インストール実行中、アクティベート承諾、アクティベート実行中及び更新完了を特定する。

[0688] 表示指示部９１ｂは、プログラム更新のフェーズがフェーズ特定部９１ａにより特定されると、その特定されたプログラム更新のフェーズに応じた態様でインジケータを表示するように指示する。インジケータ表示制御部９１

ｃは、表示指示部９１からインジケータを表示するように指示されると、その指示にしたがってインジケータを表示制御する。具体的には、インジケータ表示制御部９１ｃは、メータ装置４５においてインジケータ４６を点灯制御する。

[0689] アイコン表示制御部９１ｄは、インジケータ表示制御部９１ｃがインジケータを表示制御することに追従し、車載ディスプレイ７においてアイコンを表示制御する。詳細情報表示制御部９１ｅは、インジケータ表示制御部９１ｃがインジケータを表示制御することに追従し、車載ディスプレイ７又は携帯端末６においてプログラム更新に係るアイコン及び詳細情報を表示制御する。アイコンとは、図３２に示すキャンペーン通知アイコン５０１ａであり、詳細情報とは、例えば図３３に示すポップアップ表示されるキャンペーン通知画面５０２や、図３４及び図３５に示すダウンロード承諾画面等である。詳細情報表示制御部９１ｅは、フェーズ特定部９１ａにより特定されたプログラム更新のフェーズに応じた態様でアイコンを表示するように指示したり、フェーズ及びユーザ操作に応じた詳細情報画面を表示するように指示したりする。

[0690] 無効化指示部９１ｆは、駐車中にプログラム更新が行われることで電源管理ＥＣＵ２０が電源制御を行う場合であってもユーザ操作の受付の無効化を電源管理ＥＣＵ２０やユーザ操作に関わる各ＥＣＵ１９に指示する。例えばエンジンＥＣＵ４７（図２１７参照）にユーザ操作の受付の無効化を指示しておくことで、書換え対象ＥＣＵ１９のメモリ構造が１面メモリであり、駐車中にインストールを行う場合、ユーザがエンジンを始動させる操作を行ったとしても、受付を無効化し、エンジンが始動しないように抑制する。又、電源管理ＥＣＵ２０にユーザ操作の無効化を指示しておくことで、書換え対象ＥＣＵ１９のメモリ構造が１面メモリであり、駐車中にＩＧ電源オンしてインストールを行う場合、ユーザがＩＧ電源をオフする操作を行ったとしても、受付を無効化し、ＩＧ電源がオフされないように抑制する。このとき、無効化指示部９１ｆは、車載ディスプレイ７にユーザ操作の受付が無効化さ

れている旨の報知を行うように指示すると良い。

[0691] 次に、上記した構成の作用について図２１２から図２１７を参照して説明する。ＣＧＷ１３は、プログラム更新の報知制御プログラムを実行し、プログラム更新の報知制御処理を実行する。

[0692] ＣＧＷ１３は、プログラム更新の報知制御処理を開始すると、プログラム更新のキャンペーンが発生しているか否かを判定する（Ｓ２５０１）。ＣＧＷ１３は、プログラム更新のキャンペーンが発生していると判定すると（Ｓ２５０１：ＹＥＳ）、プログラム更新のフェーズ及びメモリ構成を特定する（Ｓ２５０２、フェーズ特定手順に相当する）。ＣＧＷ１３は、その特定したプログラム更新のフェーズに応じた態様でインジケータ４６を表示するようにメータ装置４５に指示し（Ｓ２５０３、表示指示手順に相当する）。その特定したプログラム更新のフェーズに応じたアイコンを表示するように車載ディスプレイ７に指示する（Ｓ２５０４）。

[0693] ＣＧＷ１３は、詳細表示要求の有無を判定し（Ｓ２５０５）、詳細表示要求の有りを判定すると（Ｓ２５０５：ＹＥＳ）、車載ディスプレイ７とデータ通信可能であるか否かを判定する（Ｓ２５０６）。ＣＧＷ１３は、例えば図３２に示すキャンペーン通知アイコン５０１ａ、図３３に示す「確認する」ボタン５０２ａ、図３４に示す「詳細確認」ボタン５０３ｂ等をユーザが押下した場合に、詳細表示要求有りと判定する。ＣＧＷ１３は、車載ディスプレイ７とデータ通信可能であると判定すると（Ｓ２５０６：ＹＥＳ）、詳細情報を取得し（Ｓ２５０７）、詳細情報を表示するように車載ディスプレイ７に指示し（Ｓ２５０８）、詳細情報を表示するようにセンター装置３に指示する（Ｓ２５０９）。

[0694] ＣＧＷ１３は、キャンペーン通知と共に受信した報知内容や、配信諸元データの報知内容を取得し、車載ディスプレイ７に通知して詳細情報表示を指示する。又、ＣＧＷ１３は、車載ディスプレイ７と同様の内容が携帯端末６にも表示されるようにセンター装置３へ詳細情報の表示指示としてフェーズ及びユーザの操作内容を通知する。

[0695] ＣＧＷ１３は、プログラム更新のイベントが終了したか否かを判定する（Ｓ２５１０）。

ＣＧＷ１３は、例えばアクティベートが完了し、プログラム更新が完了したことをユーザが確認したら、イベント終了と判定する。ＣＧＷ１３は、プログラム更新のイベントが終了していないと判定すると（Ｓ２５１０：ＮＯ）、ステップＳ２５０２に戻り、ステップＳ２５０２以降を繰り返す。ＣＧＷ１３は、キャンペーン通知、ダウンロード承諾、ダウンロード実行中、インストール承諾、インストール実行中、アクティベート承諾、アクティベート実行中及び更新完了の各フェーズにおいて、ステップＳ２５０２以降を繰り返す。

ＣＧＷ１３は、プログラム更新のイベントが終了したと判定すると（Ｓ２５１０：ＹＥＳ）、プログラム更新の報知制御処理を終了する。

[0696] メータ装置４５は、ユーザが確認可能な所定位置にインジケータ４６が配置されており、ＣＧＷ１３から報知要求通知を受信すると、アプリプログラムの書換え中の報知としてインジケータ４６を点灯又は点滅させる。ここで、点滅に代えて、インジケータ４６の色を変えたり輝度を挙げたりする等の通常の点灯表示よりも強調される点灯表示としても良い。即ち、通常の表示よりも強調される表示であれば良い。尚、プログラム更新に関するインジケータ４６は一つであり、一の意匠で構成される。

[0697] 図２１３に示すように、メータ装置４５は、アプリプログラムの書換え対象が２面メモリの場合、１面サスペンドメモリの場合、１面単独メモリの場合で、各フェーズにおけるインジケータの報知態様を異ならせる。具体的には、メータ装置４５は、ＣＧＷ１３から指定されたフェーズ及びメモリ構成に応じて、インジケータ４６の報知態様を特定し、その特定した報知態様にしたがって報知する。又、メータ装置４５に代えて、インジケータ表示制御部９１ｃがインジケータ４６の報知態様を制御しても良く、インジケータ表示制御部９１ｃがインジケータ４６の報知態様を特定し、その報知態様でインジケータ４６を点灯制御するようにメータ装置４５へ指示しても良い。

[0698] インジケータ表示制御部９１ｃは、図２１３に示すように、インストールやアクティベート等の車両の走行に制約が生じ得るフェーズにおいて、インジケータ４６を例えば緑色で点滅表示する。インジケータ表示制御部９１ｃは、書換え対象ＥＣＵ１９が２面メモリの場合、アクティベート実行中のフェーズのみで点滅表示する。インジケータ表示制御部９１ｃは、書換え対象ＥＣＵ１９が１面サスペンドメモリの場合、ＩＧオフ中のインストール実行中のフェーズ、アクティベート承諾のフェーズ及びアクティベート実行中のフェーズで点滅表示する。インジケータ表示制御部９１ｃは、書換え対象ＥＣＵ１９が１面メモリの場合、インストール実行中のフェーズ、アクティベート承諾のフェーズ、及びアクティベート実行中のフェーズで点滅表示する。即ち、キャンペーン通知フェーズ、ダウンロードフェーズ及びアクティベート完了後のフェーズ（ＩＧオフ時、ＩＧオン時、確認操作時）におけるインジケータ４６の表示は、メモリ構成に依らず共通であるが、インストールフェーズ及びアクティベートフェーズにおけるインジケータ４６の表示は、メモリ構成に依って異なる表示態様となる。ここで、図２１３に示すＩＧオフ時とは、駐車中にアクティベートが実行され、アクティベート完了に伴いＩＧ電源をオフした際の表示態様であり、ＩＧ電源オフに伴いインジケータ４６を消灯させる。その後、ユーザ操作によりＩＧ電源オンされた際は、インジケータ４６を点灯させる。これは、プログラム更新が全て完了したことをユーザに報知するためである。そして、図４５に示す確認操作画面５１０において、ユーザが「ＯＫ」ボタン５１０ｂを押下すると、確認操作が行われたと判断し、インジケータ４６を消灯させる。

[0699] 以下、メータ装置４５がインジケータ４６の報知態様を制御する場合を説明するが、上記したようにインジケータ表示制御部９１ｃがインジケータ４６の報知態様を制御しても良い。図２１４には、書換え対象ＥＣＵ１９のメモリ種別が２面メモリの場合におけるインジケータの報知態様を示す。ＣＧＷ１３からの指示に基づき、メータ装置４５は、キャンペーン通知からアクティベート承諾までのフェーズではインジケータ４６を点灯させ、アクティ

ベート実行中のフェーズではインジケータ４６を点滅させる。メータ装置４５は、その後、ＩＧオフではインジケータ４６を消灯させ、ＩＧオンではインジケータ４６を点灯させ、ユーザが更新完了に対する確認操作を行うと、インジケータ４６を消灯させる。即ち、２面メモリの場合、車両の走行に制約が生じる可能性があるのは、アクティベート実行中だけである。アクティベートの実行だけは、車両が駐車状態において行うため、車両を走行させることができない期間となる。そのため、メータ装置４５は、アクティベート実行中のフェーズではインジケータ４６を点滅させる。尚、ここでのインジケータは、所定の意匠であり、正常に進捗している場合は緑色で表示する。

[0700] 図２１５には、書換え対象ＥＣＵ１９のメモリ種別が１面サスペンドメモリの場合におけるインジケータの報知態様を示す。ＣＧＷ１３からの指示に基づき、メータ装置４５は、アプリプログラムの書換え対象が１面サスペンドメモリの場合には、キャンペーン通知からインストール承諾までのフェーズではインジケータ４６を点灯させ、インストール実行中ではＩＧオンでインジケータ４６を点灯させ、ＩＧオフでインジケータ４６を点滅させる。即ち、メータ装置４５は、ＩＧオン状態では１面サスペンドメモリＥＣＵのフラッシュメモリへの書込みが実行されないため、インジケータ４６を点灯させるが、ＩＧオフ状態ではフラッシュメモリへの書込みが実行されているため、インジケータ４６を点滅させる。メータ装置４５は、アクティベート承諾からアクティベート実行中までのフェーズではインジケータ４６を点滅させる。その後、ＩＧオフではインジケータ４６を消灯させ、ＩＧオンではインジケータ４６を点灯させ、ユーザが更新完了に対する確認操作を行うと、インジケータ４６を消灯させる。即ち、１面サスペンドメモリの場合、車両の走行に制約が生じる可能性があるのは、ＩＧオフでのインストール実行中からアクティベート実行中までである。そのため、メータ装置４５は、これらのフェーズではインジケータ４６を点滅させる。ここで、１面サスペンドメモリの場合、非運用面へのインストール実行中であっても、そのインストールを中断することで、運用面を起動して車両を走行制御することが可能で

ある。そのため、２面メモリの場合と同様、車両を走行させることができないアクティベート実行中のみを点滅表示としても良い。

[0701] 図２１６には、書換え対象ＥＣＵ１９のメモリ種別が１面メモリの場合におけるインジケータの報知態様を示す。ＣＧＷ１３からの指示に基づき、メータ装置４５は、アプリプログラムの書換え対象が１面単独メモリの場合には、キャンペーン通知からインストール承諾までのフェーズではインジケータ４６を点灯させ、インストール実行中からアクティベート実行中までのフェーズではインジケータ４６を点滅させる。その後、ＩＧオフではインジケータ４６を消灯させ、ＩＧオンではインジケータ４６を点灯させ、ユーザが更新完了に対する確認操作を行うと、インジケータ４６を消灯させる。即ち、１面メモリの場合、車両の走行に制約が生じる可能性があるのは、インストール実行中からアクティベート実行中までである。そのため、メータ装置４５は、これらのフェーズではインジケータ４６を点滅させる。

[0702] 又、メータ装置４５は、１回のキャンペーン通知でプログラムの書換え対象ＥＣＵ１９として２面メモリ、１面サスペンドメモリ、１面単独メモリのＥＣＵ１９が含まれる場合には、２面メモリ、１面サスペンドメモリ、１面単独メモリの順序にしたがってＥＣＵ１９のアプリプログラムの書換えを行う。ＣＧＷ１３は、キャンペーン通知後に、２面メモリのＥＣＵ１９に対するダウンロード承諾からインストール実行中までを行い、メータ装置４５は、この期間でインジケータ４６を点灯させる。ＣＧＷ１３は、２面メモリのＥＣＵ１９に対するインストール実行中のフェーズを終えると、１面サスペンドメモリのＥＣＵ１９に対するダウンロード承諾からインストール実行中までを行い、メータ装置４５は、この期間でインジケータ４６を点灯させる。ＣＧＷ１３は、１面サスペンドメモリのＥＣＵ１９に対するインストール実行中のフェーズを終えると、１面単独メモリのＥＣＵ１９に対するダウンロード承諾からインストール承諾までを行い、メータ装置４５は、この期間でインジケータ４６を点灯させる。

[0703] メータ装置４５は、１面単独メモリのインストール実行中から、これらの

メモリ種別が異なる３種のＥＣＵ１９に対するアクティベート実行中まではインジケータ４６を点滅させる。メータ装置４５は、その後のＩＧオフではインジケータ４６を消灯させ、ＩＧオンではインジケータ４６を点灯させ、ユーザが更新完了に対する確認操作を行うと、インジケータ４６を消灯させる。

[0704] 又、メータ装置４５は、１回のキャンペーン通知でプログラムの書換え対象ＥＣＵ１９として２面メモリ、１面サスペンドメモリ、１面単独メモリのＥＣＵ１９が含まれる場合に、以下のように制御しても良い。メータ装置４５は、２面メモリ、１面サスペンドメモリ、１面単独メモリの順序にしたがってＥＣＵ１９のアプリプログラムの書換えを行う。ＣＧＷ１３は、キャンペーン通知後に、これら書換え対象ＥＣＵ１９の更新データが含まれる配信パッケージのダウンロード承諾及びダウンロード実行中のインジケータ４６として、緑色の所定意匠を点灯させるように指示する。その後、ＣＧＷ１３は、インストール承諾のインジケータ４６として、緑色の所定意匠を点灯させるように指示する。尚、ここでのインストール承諾は、１面単独メモリのＥＣＵ１９が含まれている都合上、アクティベート承諾も兼ねる。インストールに対するユーザの承諾が得られると、ＣＧＷ１３は、１番目として２面メモリのＥＣＵ１９へのインストールを実行する。２面メモリのＥＣＵ１９へのインストールを実行する間、メータ装置４５は、インジケータ４６を点灯させる。ＣＧＷ１３は、２面メモリのＥＣＵ１９に対するインストール実行中のフェーズを終えると、１面サスペンドメモリのＥＣＵ１９へのインストールを実行する。１面サスペンドメモリのＥＣＵ１９へのインストールを実行する間、メータ装置４５は、インジケータ４６を点灯させる。ＣＧＷ１３は、１面サスペンドメモリのＥＣＵ１９に対するインストール実行中のフェーズを終えると、１面単独メモリのＥＣＵ１９に対するインストールを実行する。１面サスペンドメモリのＥＣＵ１９へのインストールを実行する間、メータ装置４５は、インジケータ４６を点滅させる。ＣＧＷ１３は、これら書換え対象ＥＣＵ１９のインストールが全て完了すると、インジケータ４

６の点滅を継続させたまま、アクティベートを実行する。ＣＧＷ１３は、その後のＩＧオフではインジケータ４６を消灯させるようメータ装置４５へ指示し、ＩＧオンではインジケータ４６を点灯させるようメータ装置４５へ指示し、ユーザが更新完了に対する確認操作を行うと、インジケータ４６を消灯させるようにメータ装置４６へ指示する。

[0705] 図２１４～図２１６に示した各フェーズにおいて、ＣＧＷ１３は、車載ディスプレイ７へアイコン表示の指示も行う。ＣＧＷ１３は、キャンペーン通知フェーズでは、図３２に示すキャンペーン通知アイコン５０１ａを表示するように指示する。ＣＧＷ１３は、ダウンロード承諾フェーズでも、このキャンペーン通知アイコン５０１ａの表示を継続する。ＣＧＷ１３は、ダウンロード実行中フェーズでは、図３６に示すダウンロード実行中アイコン５０１ｂを表示するように指示する。ＣＧＷ１３は、インストール承諾フェーズでは、このダウンロード実行中アイコン５０１ｂの表示を継続しても良いし、キャンペーン通知アイコン５０１ａを再度表示するように指示しても良い。ＣＧＷ１３は、インストール実行中フェーズでは、図４１に示すインストール実行中アイコン５０１ｃを表示するように指示する。ＣＧＷ１３は、アクティベート承諾フェーズでは、このインストール実行中アイコン５０１ｃの表示を継続しても良いし、キャンペーン通知アイコン５０１ａを再度表示するように指示しても良い。ＣＧＷ１３は、アクティベート実行中フェーズ及びその後のＩＧオフ時では、アイコン表示を行わない。ＣＧＷ１３は、ＩＧオン時には、キャンペーン通知アイコン５０１ａを再度表示するように指示しても良いし、図４４に示すようにアクティベート完了通知画面５０９をポップアップ表示させても良い。ＣＧＷ１３は、ユーザが更新完了に対する確認操作を行うと、アイコン表示を行わない。尚、プログラム更新に関するアイコン表示は一つであり、各フェーズに応じた意匠で構成される。

[0706] ＣＧＷ１３は、上記したようにアプリプログラムの書換え中の報知をインジケータ４６に指示する際に、アプリプログラムの書換え中に異常が発生したときには、正常時とは異なる報知態様とする。ＣＧＷ１３は、アプリプロ

グラムの書換えが正常に進んでいるときには、例えば緑色で点灯表示や点滅表示を指示し、異常が発生したときには、例えば黄色や赤色で点灯表示や点滅表示を指示する。ＣＧＷ１３は、異常の程度に応じて色を異ならせても良く、例えば異常の程度が比較的大きいときには赤色で点灯表示や点滅表示を指示し、異常の程度が比較的小さいときには黄色で点灯表示や点滅表示を指示しても良い。ここでいう、異常とは、配信パッケージをダウンロード不能な状態、書込みデータをインストール不能な状態、書換え対象ＥＣＵ１９において書込みデータを書込み不能な状態、書込みデータが不正な状態等を含む。

[0707] 車載ディスプレイ７は、詳細表示として、前述したキャンペーン通知画面５０２、ダウンロード承諾画面５０３、ダウンロード実行中画面５０４、ダウンロード完了通知画面５０５、インストール承諾５０６、インストール実行中画面５０７、アクティベート承諾画面５０８、ＩＧオン時画面５０９、更新完了に対する確認操作時画面５１０を、ユーザの操作に基づいて順次表示する。車載ディスプレイ７と同様の詳細表示は、センター装置３と通信可能に接続された携帯端末６でも表示可能である。例えば車載ディスプレイ７が搭載されていない車両では、ハンドルスイッチの操作等によりユーザが詳細表示を要求した場合、ＣＧＷ１３は、ＤＣＭ１２を介してセンター装置３に詳細表示を要求する。センター装置３は、詳細表示のコンテンツを作成し、そのコンテンツを携帯端末６が表示することで、ユーザは携帯端末６にて詳細情報を確認することができる。

[0708] 図２１７に示すように、ＣＧＷ１３は、駐車中にＩＧ系ＥＣＵやＡＣＣ系ＥＣＵの１面サスペンドメモリや１面単独メモリのアプリプログラムを書換える場合には、電源管理ＥＣＵ２０を強制的に起動し、車両電源をオンの状態とする。この場合、電源管理ＥＣＵ２０が強制的に起動すると、電源管理ＥＣＵ２０の動作によりメータ装置４５や車載ディスプレイ７が起動することになる。そのため、ＣＧＷ１３は、プログラム更新に関する報知の抑制をメータ装置４５や車載ディスプレイ７に指示する。メータ装置４５は、ＣＧ

Ｗ１３からプログラム更新の報知の抑制が指示されると、前述したインジケータ４６の点灯や点滅を行わない。車載ディスプレイ７は、ＣＧＷ１３からプログラム更新の報知の抑制が指示されると、前述した詳細表示を行わない。即ち、駐車中に行うインストールやアクティベートにおいて、ユーザが乗車していない状況の場合は、プログラム更新に関する報知は不要であるため、報知が行われないように制御する。

[0709] 又、電源管理ＥＣＵ２０が強制的に起動し、車両電源をオンの状態とすると、ユーザからのプッシュスイッチの操作を受付けてエンジン制御を可能となるが、ＣＧＷ１３は、ユーザ操作の受付の無効化を電源管理ＥＣＵ２０に指示し、ユーザ操作の受付の無効化の報知をメータ装置４５や車載ディスプレイ７及びユーザ操作に関わるＥＣＵ１９に指示する。メータ装置４５は、ＣＧＷ１３からユーザ操作の受付の無効化が指示されると、ユーザがメータ装置４５にて操作を行っても、その操作の受付を無効化する。同様に、車載ディスプレイ７は、ＣＧＷ１３からユーザ操作の受付の無効化が指示されると、ユーザが車載ディスプレイ７にて操作を行っても、その操作の受付を無効化する。又、エンジンＥＣＵ４７は、ＣＧＷ１３からユーザ操作の受付の無効化が指示されると、ユーザがプッシュスイッチによりエンジンを始動させる操作を行っても、その操作の受付を無効化し、エンジンが始動しないように抑制する。

[0710] 以上に説明したように、ＣＧＷ１３は、プログラム更新の報知制御処理を行うことで、アプリプログラムの書換え中の報知をメータ装置４５に指示するようにした。アプリプログラムの書換え中を携帯端末６や車載ディスプレイ７によりユーザに知らせることができない状況でも、アプリプログラムの書換え中をメータ装置４５によりユーザに知らせることで、アプリプログラムの書換え中をユーザに適切に知らせることができる。尚、ＣＧＷ１３は、アプリプログラムの書換えの進捗状況に応じて報知態様を変化させても良い。

[0711] （２６）電源自己保持の実行制御処理

電源自己保持の実行制御処理について図２１８から図２２２を参照して説明する。車両用プログラム書換えシステム１は、ＣＧＷ１３、ＥＣＵ１９、車載ディスプレイ７、電源管理ＥＣＵ２０において電源自己保持の実行制御処理を行う。この場合、ＣＧＷ１３がＥＣＵ１９、車載ディスプレイ７、電源管理ＥＣＵ２０に対して電源自己保持を指示する。即ち、ＣＧＷ１３が車両用マスタ装置に対応し、ＥＣＵ１９、車載ディスプレイ７、電源管理ＥＣＵ２０が車両用スレーブ装置に対応する。ＣＧＷ１３は、第２電源自己保持回路を有しており、車両用スレーブ装置は、第１電源自己保持回路を有している。

[0712] 図２１８に示すように、ＣＧＷ１３は、電源自己保持の実行制御部９２において、車両電源判定部９２ａと、書換え中判定部９２ｂと、第１電源自己保持判定部９２ｃと、電源自己保持指示部９２ｄと、第２電源自己保持判定部９２ｅと、第２電源自己保持有効化部９２ｆと、第２停止条件成立判定部９２ｇと、第２電源自己保持停止部９２ｈとを有する。

[0713] 車両電源判定部９２ａは、車両電源のオンオフを判定する。書換え中判定部９２ｂは、アプリプログラムの書換え中であるか否かを判定する。書換え中判定部９５ｂは、どの書換え対象ＥＣＵ１９が書換え中であるかも判定する。第１電源自己保持有効化部９２ｃは、車両電源がオフであると車両電源判定部９２ａにより判定され、プログラムの書換え中であると書換え中判定部９２ｂにより判定されると、車両用スレーブ装置において電源を自己保持する必要性を判定する。即ち、第１電源自己保持有効化部９２ｃは、図８に示す書換え諸元データを参照し、書換え対象ＥＣＵ１９のＥＣＵ情報の書換え方法が電源自己保持に指定されていれば、電源を自己保持する必要性が有ると判定し、電源制御に指定されていれば、電源を自己保持する必要性が無いと判定する。

[0714] 電源自己保持指示部９２ｄは、車両用スレーブ装置において電源を自己保持する必要が有ると第１電源自己保持判定部９２ｃにより判定されると、第１電源自己保持回路の有効化を車両用スレーブ装置に指示する。電源自己保

持指示部９２ｄは、第１電源自己保持回路の有効化を指示する態様として、電源自己保持の完了時刻を指定する態様、電源自己保持の延長時間を指示する態様、自己保持要求を車両用スレーブ装置に定期的に出力し続ける態様がある。電源自己保持指示部９２ｄは、図８に示す書換え諸元データを参照し、書換え対象ＥＣＵ１９のＥＣＵ情報の電源自己保持時間で指定されている時間にしたがい、第１電源自己保持回路の有効化を車両用スレーブ装置に指示する。

[0715] 即ち、電源自己保持指示部９２ｄは、電源自己保持の完了時刻を指定する態様であれば、現在時刻から書換え諸元データで指定されている時間を加算した時刻を完了時刻として指定する。電源自己保持指示部９２ｄは、電源自己保持の延長時間を指定する態様であれば、書換え諸元データで指定されている時間を延長時間として指定する。電源自己保持指示部９２ｄは、自己保持要求を車両用スレーブ装置に定期的に出力し続ける態様があれば、書換え諸元データで指定されている時間が経過するまで自己保持要求を車両用スレーブ装置に定期的に出力し続ける。

[0716] 第２電源自己保持判定部９２ｅは、車両電源がオフであると車両電源判定部９２ａにより判定され、プログラムの書換え中であると書換え中判定部９２ｂにより判定されると、自己において電源を自己保持する必要性を判定する。即ち、ＣＧＷ１３がＩＧ電源系又はＡＣＣ電源系である構成を考慮し、電源を自己保持する必要性を判定する。第２電源自己保持有効化部９２ｆは、自己において電源を自己保持する必要が有ると第２電源自己保持判定部９２ｅにより判定されると、第２電源自己保持回路の有効化する。

[0717] この場合、第２電源自己保持有効化部９２ｆは、第２電源自己保持回路が停止中の場合には、第２電源自己保持回路を起動することで、第２電源自己保持回路を有効化する。第２電源自己保持有効化部９２ｆは、第２電源自己保持回路が起動中の場合には、第２電源自己保持回路の動作期間を延長することで、電源自己保持回路を有効化する。

[0718] 第２停止条件成立判定部９２ｇは、第２電源自己保持回路の電源自己保持

の停止条件が成立したか否かを判定する。具体的には、第２停止条件成立判定部９２ｇは、車両バッテリ４０のバッテリ残量、タイムアウトの発生、書換え対象ＥＣＵ１９における書換え完了を監視し、車両バッテリ４０のバッテリ残量が所定容量未満になったり、タイムアウトが発生したり、書換え対象ＥＣＵ１９が書換えを完了したと判定すると、第２電源自己保持回路の電源自己保持の停止条件が成立したと判定する。第２電源自己保持停止部９２ｈは、第２電源自己保持回路の電源自己保持の停止条件が成立したと第２停止条件成立判定部９２ｇにより判定されると、第２電源自己保持回路を停止させる。

[0719] 図２１９に示すように、ＥＣＵ１９は、電源自己保持の実行制御部１０８において、指示判定部１０８ａと、第１電源自己保持有効化部１０８ｂと、第１停止条件成立判定部１０８ｃと、第１電源自己保持停止部１０８ｄとを有する。指示判定部１０８ａは、ＣＧＷ１３から第１電源自己保持回路の有効化が指示されたか否かを判定する。

[0720] 第１電源自己保持有効化部１０８ｂは、第１電源自己保持回路の有効化が指示されたと指示判定部１０８ａにより判定されると、第１電源自己保持回路を有効化する。第１電源自己保持有効化部１０８ｂは、電源自己保持の完了時刻が指定された場合には、その指定された完了時刻まで第１電源自己保持回路を有効化する。第１電源自己保持有効化部１０８ｂは、電源自己保持の延長時間が指定された場合には、現在時刻から当該指定された延長時間が経過するまで第１電源自己保持回路を有効化する。第１電源自己保持有効化部１０８ｂは、ＣＧＷ１３から自己保持要求を入力する場合には、自己保持要求を入力し続けている限り第１電源自己保持回路を有効化する。

[0721] この場合、第１電源自己保持有効化部１０８ｂは、第１電源自己保持回路が停止中の場合には、第１電源自己保持回路を起動することで、第１電源自己保持回路を有効化する。第１電源自己保持有効化部１０８ｂは、第１電源自己保持回路が起動中の場合には、第１電源自己保持回路の動作期間を延長することで、第１電源自己保持回路を有効化する。尚、第１電源自己保持有

効化部１０８ｂは、デフォルトの電源自己保持時間を保持しており、第１電源自己保持回路の有効化が指示されなくても、そのデフォルトの電源自己保持時間だけ第１電源自己保持回路を有効化する。即ち、第１電源自己保持有効化部１０８ｂは、第１電源自己保持回路の有効化が指示されると、デフォルトの電源自己保持時間と、ＣＧＷ１３からの指示による電源自己保持時間とのうち長い方を優先して第１電源自己保持回路を有効化する。

[0722] 第１停止条件成立判定部１０８ｃは、第１電源自己保持回路の電源自己保持の停止条件が成立したか否かを判定する。具体的には、第１停止条件成立判定部１０８ｃは、電源自己保持の対象が書換え対象ＥＣＵ１９であれば、タイムアウトの発生、ＣＧＷ１３からの停止指示を監視し、タイムアウトが発生したり、ＣＧＷ１３からの停止指示を受信したりしたと判定すると、第１電源自己保持回路の電源自己保持の停止条件が成立したと判定する。第１停止条件成立判定部１０８ｃは、電源自己保持の対象が車載ディスプレイ７であれば、タイムアウトの発生、ユーザの降車、ＣＧＷ１３からの停止指示を監視し、タイムアウトが発生したり、ユーザの降車を判定したり、ＣＧＷ１３からの停止指示を受信したりしたと判定すると、第１電源自己保持回路の電源自己保持の停止条件が成立したと判定する。第１停止条件成立判定部１０８ｃは、電源自己保持の対象が電源管理ＥＣＵ２０であれば、ＣＧＷ１３からの停止指示を監視し、ＣＧＷ１３からの停止指示を受信したと判定すると、第１電源自己保持回路の電源自己保持の停止条件が成立したと判定する。第１電源自己保持停止部１０８ｄは、第１電源自己保持回路の電源自己保持の停止条件が成立したと第２停止条件成立判定部１０８ｃにより判定されると、第１電源自己保持回路を停止させる。

[0723] 次に、上記した構成の作用について図２２０から図２２２を参照して説明する。ここでは、車両用スレーブ装置が書換え対象ＥＣＵ１９の場合を説明する。ＣＧＷ１３及び書換え対象ＥＣＵ１９は、それぞれ電源自己保持の実行制御プログラムを実行し、電源自己保持の実行制御処理を行う。

[0724] ＣＧＷ１３は、電源自己保持の実行制御処理を開始すると、車両電源がオ

フであるか否かを判定する（Ｓ２６０１、車両電源判定手順に相当する）。ＣＧＷ１３は、車両電源がオフであると判定すると（Ｓ２６０１：ＹＥＳ）、アプリプログラムの書換え中であるか否かを判定する（Ｓ２６０２、書換え中判定手順に相当する）。ＣＧＷ１３は、アプリプログラムの書換え中であると判定すると（Ｓ２６０２：ＹＥＳ）、第２電源自己保持回路を起動し（Ｓ２６０３、第２電源自己保持有効化手順に相当する）、書換え対象ＥＣＵ１９において電源を自己保持する必要性を判定する（Ｓ２６０４、電源自己保持判定手順に相当する）。

[0725] ＣＧＷ１３は、書換え対象ＥＣＵ１９において電源自己を保持する必要が有ると判定すると（Ｓ２６０４：ＹＥＳ）、第１電源自己保持回路の有効化を書換え対象ＥＣＵ１９に指示する（Ｓ２６０５、電源自己保持指示手順に相当する）。ＣＧＷ１３は、電源自己保持の停止条件が成立したか否かを判定し（Ｓ２６０６）、電源自己保持の停止条件が成立したと判定すると（Ｓ２６０６：ＹＥＳ）、第２電源自己保持回路を停止させ（Ｓ２６０７）、電源自己保持の実行制御処理を終了する。

[0726] 以上は、ＣＧＷ１３は、アプリプログラムの書換え中であると判定した場合に電源自己保持回路を起動する構成であるが、車両電源がオフであると判定すると、電源自己保持回路を起動し、アプリプログラムの書換え中であると判定すると、その起動中の電源自己保持回路の動作時間を延長する構成でも良い。

[0727] 書換え対象ＥＣＵ１９は、電源自己保持の実行制御処理を開始すると、車両電源がオフであるか否かを判定する（Ｓ２６１１）。書換え対象ＥＣＵ１９は、車両電源がオフであると判定すると（Ｓ２６１１：ＹＥＳ）、自己保持回路を起動し（Ｓ２６１２）、電源自己保持の停止条件が成立したか否かを判定し（Ｓ２６１３）、ＣＧＷ１３から電源自己保持回路の有効化が指示されたか否かを判定する（Ｓ２６１４）。書換え対象ＥＣＵ１９は、ＣＧＷ１３から電源自己保持回路の有効化が指示されたと判定すると（Ｓ２６１４：ＹＥＳ）、その起動中の電源自己保持回路の動作期間を延長する（Ｓ２６

１５）。書換え対象ＥＣＵ１９は、電源自己保持の停止条件が成立したと判定すると（Ｓ２６１３：ＹＥＳ）、電源自己保持回路を停止させ（Ｓ２６１６）、電源自己保持の実行制御処理を終了する。

[0728] 以上は、書換え対象ＥＣＵ１９は、車両電源がオフであると判定した場合に電源自己保持回路を起動する構成であるが、車両電源がオフであると判定した場合に電源自己保持回路を起動せず、車両電源がオフであると判定し、且つＣＧＷ１３から電源自己保持回路の有効化が指示されたと判定すると、停止中の電源自己保持回路を起動させる構成でも良い。

[0729] 以上は、車両用スレーブ装置が書換え対象ＥＣＵ１９の場合を説明したが、車両用スレーブ装置が車載ディスプレイ７や電源管理ＥＣＵ２０の場合も同様である。図２２２に示すように、書換え対象ＥＣＵ１９では、インストール準備から書換え後処理までの期間で電源自己保持回路の動作が必要であり、車載ディスプレイ７では、更新承諾待ち、ダウンロード承諾待ち、インストール承諾待ち、アクティベート承諾待ちの期間で電源自己保持回路の動作が必要である。

[0730] 以上に説明したように、ＣＧＷ１３は、電源自己保持の実行制御処理を行うことで、車両電源がオフであり、アプリプログラムの書換え中であると判定すると、書換え対象ＥＣＵ１９において電源を自己保持する必要性を判定し、電源を自己保持する必要が有ると判定すると、電源自己保持回路の有効化を書換え対象ＥＣＵ１９に指示するようにした。書換え対象ＥＣＵ１９において、ＣＧＷ１３から電源自己保持回路の有効化が指示されたと判定すると、電源自己保持回路を有効化するようにした。電源自己保持回路を有効化することで、アプリプログラムの書換えを行うための動作電源を確保することができ、アプリプログラムの書換えを適切に完了することができる。

[0731] 上述した特徴的な処理（１）～（２６）を含め、プログラム更新の全体シーケンスについて図２２３から図２３３を参照して説明する。ここでは、第１バスに接続されるＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）のアプリプログラムを書換え、第２バスに接続されるＥＣＵ（ＩＤ４）

、ＥＣＵ（ＩＤ５）及びＥＣＵ（ＩＤ６）のアプリプログラムを書換えない例について説明する。ＥＣＵ（ＩＤ１）とＥＣＵ（ＩＤ４）が１面単独メモリであり、ＥＣＵ（ＩＤ５）が１面サスペンドメモリであり、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）及びＥＣＵ（ＩＤ６）が２面メモリである。又、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ４）、ＥＣＵ（ＩＤ５）及びＥＣＵ（ＩＤ６）はＩＧ電源系ＥＣＵであり、ＥＣＵ（ＩＤ２）はＡＣＣ電源系ＥＣＵであり、ＥＣＵ（ＩＤ３）は＋Ｂ電源系ＥＣＵである。

[0732] まず、事前準備として、ユーザは携帯端末６等を操作し、車両番号（車両の識別番号）や携帯電話番号等の個人情報を入力し、センター装置３に対してアカウントを登録する（Ｓ５００１）。又、ユーザは携帯端末６等を操作し、実行条件を入力し、プログラム更新の実行を許可する条件として、車両位置や時間帯等を指定する。センター装置３は、携帯端末６を介して受信した個人情報等をデータベースに記憶する（Ｓ５００２）。

[0733] 又、車両側システム４は、車両に関する情報をＣＧＷ１３が収集し（Ｓ５０１１）、ＤＣＭ１２を介してセンター装置３へアップロードする（Ｓ５０１２）。具体的には、プログラムバージョン、各ＥＣＵ１９のメモリ構成、運用面情報、車両に搭載される電装部品、車両位置、車両の電源状態等の情報である。センター装置３は、車両側システム４から受信した情報をデータベースに記憶する（Ｓ５０１３）。

[0734] プログラム更新の必要性が生じると、センター装置３は、アプリプログラムの提供事業者であるサプライヤから提供される書込みデータと、データベースに記憶した情報とから、図７及び図８に示す書換え諸元データを生成する。そして、センター装置３は、これら書込みデータ及びその認証子と、書換え諸元データとから、リプログデータを生成する。センター装置３は、生成したリプログデータと、別途生成される配信諸元データ（図９）と、パッケージ認証子とを１つのファイルにパッケージングし、配信パッケージを生成し、登録する（Ｓ５０２１）。

[0735] センター装置３は、配信パッケージの準備が整った後、ユーザに対してプ

ログラム更新の告知を行う。センター装置３は、データベースに記憶した個人情報を参照し、携帯端末６に対し、ショートメッセージサービス（ＳＭＳ）を送信する（Ｓ５０３１）。ユーザ操作により、携帯端末６は、ＳＭＳに記載されたＵＲＬ（Uniform Resource Locator）に接続し、告知内容を表示する（Ｓ５０３２）。携帯端末６は、ユーザ操作によるプログラム更新に承諾する旨、又は不承諾の旨をセンター装置３に通知する（Ｓ５０３３）。センター装置３は、ユーザの意思情報（承諾又は不承諾）をデータベースに登録する（Ｓ５０３４）。ここで、携帯端末６に代えて、車載ディスプレイ７を用いて、ユーザへの告知を行うことも可能である。

[0736] ＣＧＷ１３は、センター装置３から送信された配信諸元データを、ＤＣＭ１２を介して受信し、車載ディスプレイ７に転送する（Ｓ５０３５）。車載ディスプレイ７は、配信諸元データを解析し、告知内容である表示文言等を表示する（Ｓ５０３６）。又、車載ディスプレイ７は、アイコン等の画像データを表示し、ユーザがプログラム更新に承諾するか否かの入力を受け付ける。ＣＧＷ１３は、ユーザの意思情報を車載ディスプレイ７から受信し、ＤＣＭ１２を介してセンター装置３に通知する（Ｓ５０３７）。

[0737] ユーザからプログラム更新の承諾を得た場合、車両側システム４は、センター装置３から配信パッケージをダウンロードする。まず、センター装置３は、予めユーザに指定された実行条件を充足しているかチェックする（Ｓ５０４１）。センター装置３は、実行条件のうち１つでも充足していない場合、配信パッケージをＤＣＭ１２に送信しない。センター装置３は、全ての実行条件を充足している場合、配信パッケージをＤＣＭ１２に送信する（Ｓ５０４２）。ＤＣＭ１２は、センター装置３から配信パッケージをダウンロードすると、そのダウンロードした配信パッケージをフラッシュメモリに保存する。そして、ＤＣＭ１２は、配信パッケージから配信パッケージ認証子を抽出し、リプログデータ及び配信諸元データの完全性を検証する（Ｓ５０４３）。

[0738] ＤＣＭ１２は、例えばＣＧＷ１３が記憶する鍵情報を用いて、リプログデー

タ及び配信諸元データの認証子を演算する。ＤＣＭ１２は、演算した認証子と、配信パッケージから抽出した配信パッケージ認証子とを比較し、一致する場合は検証成功と判定し、一致しない場合は検証失敗と判定する。ＤＣＭ１２は、検証失敗と判定すると、配信パッケージを削除すると共に、ＣＧＷ１３及びセンター装置３に検証失敗の旨を通知する。

[0739] ＤＣＭ１２は、配信パッケージに対する検証成功と判定した場合、配信パッケージに含まれるリプログデータを、図１０に示すようにアンパッケージングし、各書換え対象ＥＣＵ１９に対する書込みデータ及び書換え諸元データとに分割する（Ｓ５０４４）。書換え諸元データは、ＤＣＭ用の書換え諸元データと、ＣＧＷ用の書換え諸元データとに分割しておく。

[0740] ＤＣＭ１２は、ＣＧＷ用の書換え諸元データをＣＧＷ１３に送信する（Ｓ５０４５）。ＣＧＷ１３は、ＤＣＭ１２から受信したＣＧＷ用の書換え諸元データを解析し、必要な情報を抽出した後、ＤＣＭ１２との間で各ＥＣＵ１９に対する書込みデータの認証を行う（Ｓ５０４６）。ＣＧＷ１３は、例えば自己が記憶するＥＣＵ（ＩＤ１）の鍵情報を用いて、ＥＣＵ（ＩＤ１）の書込みデータ（差分データ）の認証子を演算する。ＣＧＷ１３は、演算した認証子と、リプログデータから抽出した認証子とを比較し、一致する場合は検証成功と判定し、一致しない場合は検証失敗と判定する。ＣＧＷ１３は、検証失敗と判定すると、配信パッケージを削除すると共に、ＤＣＭ１２及びセンター装置３に検証失敗の旨を通知する。ここで、ＣＧＷ１３は、何れか１つの書込みデータに対して検証失敗と判定された場合、全てのＥＣＵ１９に対してプログラム更新を行わないとする。

[0741] ＣＧＷ１３は、全ての書込みデータに対して検証成功と判定すると、ＤＣＭ１２から配信諸元データを受信し、その受信した配信緒元データを車載ディスプレイ７に転送する（Ｓ５０４７）。車載ディスプレイ７は、ＣＧＷ１３から転送された配信諸元データを記憶する。以上のダウンロード処理が完了すると、ＣＧＷ１３は、ＤＣＭ１２を介してセンター装置３にダウンロード完了の旨を通知する（Ｓ５０４８）。

[0742] センター装置３は、車両側システム４からダウンロード完了が通知されると、携帯端末６に対し、ＳＭＳを送信する（Ｓ５０４９）。携帯端末６は、ユーザ操作により、ＳＭＳに記載されたＵＲＬに接続し、インストール予約画面を表示する（Ｓ５０５０）。携帯端末６は、ユーザ操作により入力されたインストール日時をセンター装置３に通知する（Ｓ５０５１）。センター装置３は、個人情報と紐付けて、インストール日時をデータベースに記憶する（Ｓ５０５２）。ここで、携帯端末６に代えて、車載ディスプレイ７を用いて、ユーザにインストール日時を予約させることも可能である。車載ディスプレイ７は、ＣＧＷ１３からダウンロード完了を通知されると（Ｓ５０５３）、インストール予約画面を表示する（Ｓ５０５４）。ＣＧＷ１３は、車載ディスプレイ７から受信したインストール日時を、ＤＣＭ１２を介してセンター装置３に通知する（Ｓ５０５５）。

[0743] センター装置３は、現在日時がデータベースに登録したインストール日時になった場合、インストール開始を車両側システム４に指示する（Ｓ５０７１）。ＤＣＭ１２は、センター装置３からインストールが指示されると、インストール実行条件をチェックする（Ｓ５０７２）。ＤＣＭ１２は、例えば車両位置やセンター装置３との通信状況等をチェックする。ＤＣＭ１２は、全ての実行条件を充足している場合、パッケージ認証子を用いて配信パッケージを認証する（Ｓ５０７３）。ＤＣＭ１２は、認証に成功すると、配信パッケージをアンパッケージングし（Ｓ５０７４）、ＤＣＭ用の書換え諸元データ及びＣＧＷ用の書換え諸元データを抽出し、ＥＣＵ１９毎の書込みデータに分割した上で、インストール開始をＣＧＷ１３に通知する（Ｓ５０７５）。

[0744] ＣＧＷ１３は、ＤＣＭ１２からインストール開始が通知されると、ＤＣＭ１２から取得したＣＧＷ用の書換え諸元データを解析し、どのＥＣＵ１９をどの順序で書換えるか判定する（Ｓ５０７６）。ここでは、１番目にＥＣＵ（ＩＤ１）を、２番目にＥＣＵ（ＩＤ２）を、３番目にＥＣＵ（ＩＤ３）を書換える順序とする。ＣＧＷ１３は、ＤＣＭ１２が保持する書換え対象ＥＣ

Ｕ１９毎の書込みデータを、各認証子を用いて全て検証する（Ｓ５０７７）。ここで、バージョンアップのための書込みデータだけでなく、ロールバックのための書込みデータについても、検証しておくと良い。

[0745] ＣＧＷ１３は、書込みデータの検証に成功すると、電源管理ＥＣＵ２０に対し、ＩＧ電源オンを要求する（Ｓ５０７８）。駐車中（ＩＧスイッチ４２がオフ且つＡＣＣスイッチ４１がオフ）にインストールする際、書換え対象ＥＣＵ１９がＩＧ系ＥＣＵ又はＡＣＣ系ＥＣＵである場合、電力を供給して書換え対象ＥＣＵ１９を起動させる必要がある。電源管理ＥＣＵ２０は、ＩＧ電源オンと同じ電力供給を行うように電源制御回路４３に要求する（Ｓ５０７９）。電源制御回路４３によりＩＧ電源ライン３９へ電力供給がなされると、ＩＧ系ＥＣＵ及びＡＣＣ系ＥＣＵが起動（ウェイクアップ）する。

[0746] その後、ＣＧＷ１３は、非書換え対象ＥＣＵ１９であるＥＣＵ（ＩＤ５）、ＥＣＵ（ＩＤ５）及びＥＣＵ（ＩＤ６）と、２番目以降に書換えるＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に対し、スリープするように要求する（Ｓ５０８０）。尚、ここでは、１番目の書換え対象ＥＣＵ１９を書換えた後に２番目の書換え対象ＥＣＵ１９を書換えることとしたが、複数の書換え対象ＥＣＵ１９を同時並行して書換えても良い。この場合、非書換え対象ＥＣＵ１９に対してのみ、スリープするように要求する。

[0747] ＣＧＷ１３は、各書換え対象ＥＣＵ１９へのインストールと並行して、バッテリ残量の監視（Ｓ５０８１）及びバスの通信負荷の監視（Ｓ５０８２）を行う。ＣＧＷ１３は、ＣＧＷ用の書換え諸元データから抽出したバッテリ負荷の値、バス負荷の値（バス負荷テーブル）を参照し、許容値を超えない範囲でインストールを制御する。ＣＧＷ１３は、例えば駐車状態において、バッテリ負荷が許容値に達したら、その時点でインストールを中断する。

[0748] 又、ＣＧＷ１４は、例えば書換え対象ＥＣＵ（ＩＤ１）が接続される第１バスのバス負荷が許容値に達したら書込みデータをＥＣＵ（ＩＤ１）へ送信する頻度を遅くする。これらの監視は、全ての書換え対象ＥＣＵ１９へのインストールが完了したら終了する。尚、１面単独メモリの場合、インストー

ルの途中で終了することはできないため、インストール開始前に十分なバッテリ残量があることを確認する必要がある。

[0749] ＣＧＷ１３は、１番目に書換えるＥＣＵ（ＩＤ１）へインストール開始を通知する（Ｓ５１０１）。ＥＣＵ（ＩＤ１）は、ＣＧＷ１３からインストール開始を通知されると、無線によるプログラム更新モードへ状態を遷移する（Ｓ５１０２）。ＥＣＵ（ＩＤ１）は１面単独メモリメモリＥＣＵであるため、並行してアプリプログラムの実行やツールを用いた診断処理を行うことはできず、無線によるプログラム更新専用モードとなる。

[0750] ＣＧＷ１３は、１番目に書換えるＥＣＵ（ＩＤ１）へのインストールを行うにあたり、セキュリティアクセス鍵を用いてアクセス認証を行う（Ｓ５１０３）。ＥＣＵ（ＩＤ１）へのアクセス認証に成功すると、ＣＧＷ１３は、書込みデータである全データの情報をＥＣＵ（ＩＤ１）へ送信する。ＥＣＵ（ＩＤ１）は、受信した全データの情報を用いて、書込みデータが自ＥＣＵに整合するか否かを判定する（Ｓ５１０４）。ＥＣＵ（ＩＤ１）は、整合すると判定した場合、書込み処理を行う。

[0751] ＣＧＷ１３は、ＤＣＭ１２からＥＣＵ（ＩＤ１）への書込みデータのうち所定サイズ（例えば１ｋバイト）の分割ファイルを取得し、ＥＣＵ（ＩＤ１）へ配信する（Ｓ５１０５）。ＥＣＵ（ＩＤ１）は、ＣＧＷ１３から受信した分割ファイルをフラッシュメモリ３３ｄに書込む（Ｓ５１０６）。ＥＣＵ（ＩＤ１）は、書込みが完了すると、途中から書込みを再開できるよう、どこまで書込んだかのフラッシュメモリアドレスを示すリトライポイントを記憶する（Ｓ５１０７）。リトライポイントとして、フラッシュメモリの消去、書込み、及びそれ以降の処理のうちどこまで実行されたかを示すフラグを記憶しても良い。ＥＣＵ（ＩＤ１）は、リトライポイントを記憶すると、ＣＧＷ１３に書込み完了を通知する（Ｓ５１０８）。

[0752] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から書込み完了の通知を受けると、ＤＣＭ１２を介してセンター装置３へ書換え状況の進捗情報を通知する（Ｓ５１０９）。進捗情報とは、例えばインストールフェーズであること及びＥＣＵ

（ＩＤ１）の書込みデータが累積で何バイト書込みを完了したか等のデータである。センター装置３は、ＤＣＭ１２から送信された進捗情報に基づいて、携帯端末６から接続可能なウェブ画面を更新する（Ｓ５１１０）。携帯端末６は、センター装置３に接続し、更新された進捗状況として、例えば現在何％までインストールが進んだか等を表示する（Ｓ５１１１）。これにより、車両が駐車状態であり、ユーザが車外に居る場合であっても、携帯端末６によりインストールの進捗状況を把握することができる。ここで、携帯端末６に代えて、車載ディスプレイ７で進捗を表示することも可能である。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から書換え完了の通知を受けると、車載ディスプレイ７へ書換え状況の進捗情報を通知する（Ｓ５１１２）。車載ディスプレイ７は、進捗状況の画面を更新して表示する（Ｓ５１１３）。ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ３）のように２面メモリ構成の場合は、車両が走行状態であってもインストールが可能である。そのため、例えば車両がＩＧスイッチオンである場合には、車載ディスプレイ７が進捗状況を表示すると良い。

[0753] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から書込み完了の通知を受けると、次の書込みデータとして２番目の分割ファイルを取得し、ＥＣＵ（ＩＤ１）に配信する。以降、最後の書込みデータとしてＮ番目の分割ファイルまで、Ｓ５１０５～Ｓ５１１３の処理を繰返す。ＥＣＵ（ＩＤ１）は、Ｎ番目の分割ファイルまで書込みを完了すると、フラッシュメモリの更新プログラムに対して完全性検証を行い、正しく書込まれたか否かを確認する（Ｓ５１１４）。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から全ての分割ファイルの書込みを完了し、完全性検証に成功した旨の通知を受けると、ＥＣＵ（ＩＤ１）に対してスリープするように要求する（Ｓ５１１５）。ＥＣＵ（ＩＤ１）は、インストールされた更新プログラムで起動することなく、一旦スリープする。

[0754] ＣＧＷ１３は、２番目に書換えるＥＣＵ（ＩＤ２）に対し、ウェイクアップするように要求する（Ｓ５２０１）。ＣＧＷ１３は、無線によるプログラム更新であって、インストールを開始する旨をＥＣＵ（ＩＤ２）に通知する

（Ｓ５２０２）。ＥＣＵ（ＩＤ２）は、内部状態として、無線によるプログラム更新モードへ状態を遷移する（Ｓ５２０３）。２面メモリであるＥＣＵ（ＩＤ２）は、無線によるプログラム更新モードの間、アプリプログラムの実行やツールによる診断の実行が可能である。ＣＧＷ１３は、ＥＣＵ（ＩＤ２）にアクセス認証を行う（Ｓ５２０４）。ＥＣＵ（ＩＤ２）は、書込みデータである差分データが自ＥＣＵに整合するか否かを判定する（Ｓ５２０５）。ＥＣＵ（ＩＤ２）は２面メモリであるため、フラッシュメモリの非運用面に整合する書込みデータか否かを含め、判定する。例えばＥＣＵ（ＩＤ２）のＡ面が運用面であり、Ｂ面が非運用面であるとすると、書込みデータがＢ面に合致しないアドレスだった場合、以降の処理に進むことなく、ＣＧＷ１３は、書込みデータが誤っている旨をＤＣＭ１２を介してセンター装置３に通知する。そして、ＣＧＷ１３は、後述するロールバックの処理を行う。書込みデータが自ＥＣＵに整合すると判定された場合、ＥＣＵ（ＩＤ２）への書込み処理を行う。以降、ＥＣＵ（ＩＤ２）に関するＳ５２０６～Ｓ５２１６までの処理は、Ｓ５１０５～Ｓ５１１５と同様である。Ｓ５２０７において、２面メモリであるＥＣＵ（ＩＤ２）へ差分データを書込む際は、図１８に示すように、旧データと差分データとから差分を復元して新データを生成し、フラッシュメモリ３３ｄに書込む。

[0755] ＣＧＷ１３は、ＥＣＵ（ＩＤ２）に対するインストールが全て完了し、ＥＣＵ（ＩＤ２）をスリープさせると、３番目に書換えるＥＣＵ（ＩＤ３）に対し、ウェイクアップするように要求する（Ｓ５３０１）。ＣＧＷ１３は、無線によるプログラム更新であって、インストールを開始する旨をＥＣＵ（ＩＤ３）に通知する（Ｓ５３０２）。ＥＣＵ（ＩＤ３）は、内部状態として、無線によるプログラム更新モードへ状態を遷移する（Ｓ５３０３）。ＣＧＷ１３は、ＥＣＵ（ＩＤ３）にアクセス認証を行う（Ｓ５３０４）。ＥＣＵ（ＩＤ３）は、書込みデータである差分データが自ＥＣＵに整合するか否かを判定する（Ｓ５３０５）。書込みデータが自ＥＣＵに整合すると判定された場合、ＥＣＵ（ＩＤ３）への書込み処理を行う。以降、ＥＣＵ（ＩＤ３）

に関するＳ５３０６～Ｓ５３１５までの処理は、Ｓ５１０５～Ｓ５１１４と同様である。

[0756] ＣＧＷ１３は、ＥＣＵ（ＩＤ３）に対するインストールが全て完了すると、バッテリ残量の監視及びバスの通信負荷の監視を終了する（Ｓ５３１６、Ｓ５３１７）。そして、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）及びＥＣＵ（ＩＤ２）に対してウェイクアップするように要求する（Ｓ５４０１）。

[0757] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）を、更新したプログラムで同時に起動させるべく、それぞれのＥＣＵに対し、更新したプログラムをアクティベートするように要求する（Ｓ５４０２）。尚、アクティベートの要求に対応しないＥＣＵである場合は、アクティベート要求に代えて、電源オフ及び電源オンを通知し、再起動を行わせると良い。

[0758] ＥＣＵ（ＩＤ１）は、ＣＧＷ１３からのアクティベート要求を受けると、自己を再起動させる（Ｓ５４０３）。ＥＣＵ（ＩＤ１）は１面単独メモリであるため、再起動により、更新したプログラムで起動されることとなる。ＥＣＵ（ＩＤ１）は、インストール後の再起動が完了すると、ＣＧＷ１３へアクティベート完了と共に更新後のプログラムバージョンを通知する（Ｓ５４０４）。

[0759] ＥＣＵ（ＩＤ２）は、ＣＧＷ１３からのアクティベート要求を受けると、記憶している運用面情報をＡ面からＢ面に更新し（Ｓ５４０５）、自己を再起動させる（Ｓ５４０６）。そして、ＥＣＵ（ＩＤ２）は、Ｂ面で正常に起動すると、ＣＧＷ１３へ更新後のプログラムバージョン及び運用面情報と共にアクティベート完了を通知する（Ｓ５４０７）。

[0760] ＥＣＵ（ＩＤ３）は、ＣＧＷ１３からのアクティベート要求を受けると、記憶している運用面情報をＡ面からＢ面に更新し（Ｓ５４０８）、自己を再起動させる（Ｓ５４０９）。そして、ＥＣＵ（ＩＤ３）は、Ｂ面で正常に起動すると、ＣＧＷ１３へ更新後のプログラムバージョン及び運用面情報と共にアクティベート完了を通知する（Ｓ５４１０）。

[0761] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）からのアクティベート完了通知を受けると、ＤＣＭ１２を介してセンター装置３へ書換え対象ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に関する更新後のプログラムバージョン及び運用面情報と共にプログラムの更新完了を通知する（Ｓ５４１１）。センター装置３は、ＤＣＭ１２から通知された情報をデータベースへ登録すると共に（Ｓ５４１２）、進捗状況として完了を示す表示にウェブ画面を更新する（Ｓ５４１３）。携帯端末６は、センター装置３へ接続し、プログラム更新が完了した旨のウェブ画面を表示する（Ｓ５４１４）。又、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）からのアクティベート完了通知を受けると、車載ディスプレイ７へ進捗状況としてプログラム更新が完了した旨を通知する（Ｓ５４１５）。車載ディスプレイ７は、プログラム更新が完了した旨を表示する（Ｓ５４１６）。尚、車両が駐車状態等、進捗表示が不要な場合、ＣＧＷ１３は、車載ディスプレイ７へ進捗を通知しない。

[0762] 最後に、ＣＧＷ１３は、電源管理ＥＣＵ２０に対し、ＩＧ電源オフを要求する（Ｓ５４１８）。電源管理ＥＣＵ２０は、インストール開始前のＩＧスイッチオフの電源状態に戻すべく電力供給を遮断するように電源制御回路４３に要求する。電源制御回路４３により、ＩＧ電源ライン３９及びＡＣＣ電源ライン３８への電力供給が遮断されると、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ４）、ＥＣＵ（ＩＤ５）及びＥＣＵ（ＩＤ６）は、停止状態となる。

[0763] 上述の例では、１面単独メモリであるＥＣＵ（ＩＤ１）のプログラム更新を含むため、車両が駐車状態のときに、インストールからアクティベートまでを連続して行うものとして説明した。しかしながら、例えば書換え対象ＥＣＵ１９が全て２面メモリである場合には、走行中にバックグラウンドでインストールを行うことも可能である。又、書換え対象ＥＣＵ１９のインストールが完了した時点で、携帯端末６によりユーザからアクティベートの承諾を得るように構成しても良い。

[0764] 次に、アプリプログラムのインストール中において、ユーザによりプログラム更新のキャンセルが選択された場合のロールバックシーケンスについて図２３０から図２３３を参照して説明する。具体的には、ＥＣＵ（ＩＤ１）に対してインストールが完了し、ＥＣＵ（ＩＤ２）に対してインストール途中の時点でユーザによりキャンセルが選択された場合について説明する。

[0765] センター装置３は、携帯端末６よりプログラム更新のキャンセルを通知された場合、車両側システム４へプログラム更新をキャンセルするように指示する（Ｓ６００１）。そして、センター装置３は、進捗状況としてロールバック中の表示態様にウェブ画面を変更する（Ｓ６００２）。携帯端末６は、ロールバック中の進捗状況を示すウェブ画面を表示する（Ｓ６００３）。

[0766] ＣＧＷ１３は、ＤＣＭ１２を介してセンター装置３からプログラム更新のキャンセルが指示されると、書換え対象ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）のメモリ構成及びインストール状況に基づき、どのＥＣＵに対してどのようなロールバック処理が必要か判定する（Ｓ６００４）。この例においては、ＥＣＵ（ＩＤ２）へのインストールを完了させると共に、ＥＣＵ（ＩＤ１）を元のバージョンに戻すというロールバック処理が必要となる旨を判定する。

[0767] そして、ＣＧＷ１３は、車載ディスプレイ７へロールバック用の進捗を通知する（Ｓ６００５）。車載ディスプレイ７は、ＣＧＷ１３からロールバック用の進捗が通知されると、ロールバック用の表示態様に変更して進捗を表示する（Ｓ６００６）。車載ディスプレイ７は、例えば「ロールバック中」と表示させると共に、ロールバックが必要なＥＣＵ（ＩＤ１）の進捗を０％、ＥＣＵ（ＩＤ２）の進捗を０％と表示する。

[0768] ＣＧＷ１３は、ＥＣＵ（ＩＤ２）に対するロールバック処理として、書込みデータのインストールを継続する。ＥＣＵ（ＩＤ２）は２面メモリであるため、非運用面であるＢ面へのインストールを途中までで中断し、引き続きＡ面を運用面として動作することも可能である。しかしながら、Ｂ面が途中までインストールされた不完全な状態である場合、次回の差分データを用い

たインストール時に、差分を正しく復元できなくなる。よって、ＥＣＵ（ＩＤ２）に対しては最後までインストールを継続する。

[0769] 具体的には、ＣＧＷ１３は、ＤＣＭ１２からＥＣＵ（ＩＤ２）に対する書込みデータの分割ファイル（例えば１ｋバイト分）を取得し、ＥＣＵ（ＩＤ２）に配信する（Ｓ６００７）。ＥＣＵ（ＩＤ２）は、ＣＧＷ１３から受信した分割ファイルをフラッシュメモリ３３ｄに書込む（Ｓ６００８）。書込みが完了すると、ＥＣＵ（ＩＤ２）は、途中から書込みを再開できるようにリトライポイントを記憶し（Ｓ６００９）、ＣＧＷ１３に書込み完了を通知する（Ｓ６０１０）。

[0770] ＣＧＷ１３は、ＥＣＵ（ＩＤ２）から書込み完了の通知を受けると、ＤＣＭ１２を介してセンター装置３へロールバック状況の進捗情報を通知する（Ｓ６０１１）。ロールバック状況の進捗情報とは、例えばＥＣＵ（ＩＤ２）のロールバックとして何バイトの書込みが必要で、そのうち累積で何バイト書込みを完了したか等のデータである。センター装置３は、ＤＣＭ１２から送信された進捗情報に基づいて、携帯端末６から接続可能なウェブ画面を更新する（Ｓ６０１２）。携帯端末６は、更新された進捗状況として例えば現在何％までロールバックが進んだか等のウェブ画面を表示する（Ｓ６０１３）。ここで、携帯端末６に代えて、車載ディスプレイ７で進捗を表示することも可能である。ＣＧＷ１３は、ＥＣＵ（ＩＤ２）から書換え完了の通知を受けると、車載ディスプレイ７へロールバック状況の進捗情報を通知する（Ｓ６０１４）。車載ディスプレイ７は、進捗状況の画面を更新し、表示する（Ｓ６０１５）。以降、最後の書込みデータとしてＮ番目の分割ファイルまで、Ｓ６００７～Ｓ６０１５の処理を繰返す。

[0771] ＥＣＵ（ＩＤ２）は、Ｎ番目の分割ファイルまで書込むと、フラッシュメモリ３３ｄの更新プログラムの完全性を検証する（Ｓ６０１６）。ＣＧＷ１３は、ＥＣＵ（ＩＤ２）からインストール完了の通知を受けると、ＥＣＵ（ＩＤ２）に対してスリープするように要求する（Ｓ６０１７）。ＥＣＵ（ＩＤ２）は、非運用面であるＢ面にインストールされた更新プログラムで起動

することなく、スリープする。

[0772] 続いて、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）に対するロールバック処理を行うべくＥＣＵ（ＩＤ１）に対してウェイクアップを要求する（Ｓ６１０１）。ＣＧＷ１３は、ロールバックのためのインストールを開始する旨をＥＣＵ（ＩＤ１）に通知する（Ｓ６１０２）。ＥＣＵ（ＩＤ１）は、ＣＧＷ１３からインストール開始が通知されると、無線によるプログラム更新モードへ状態を遷移する（Ｓ６１０３）。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）とアクセス認証を行う（Ｓ６１０４）。ＥＣＵ（ＩＤ１）は、アクセス認証に成功すると、ロールバック用の書込みデータが自ＥＣＵに整合するか否かを判定する（Ｓ６１０５）。ロールバック用の書込みデータが自ＥＣＵに整合すると判定された場合、ＥＣＵ（ＩＤ１）への書込み処理を行う。

[0773] ＣＧＷ１３は、ＤＣＭ１２からＥＣＵ（ＩＤ１）へのロールバック用の書込みデータのうち所定サイズ（例えば１ｋバイト）の分割ファイルを取得し、ＥＣＵ（ＩＤ１）へ配信する（Ｓ６０１６）。ＥＣＵ（ＩＤ１）は、ＣＧＷ１３から受信した分割ファイルをフラッシュメモリ３３ｄに書込む（Ｓ６１０７）。ＥＣＵ（ＩＤ１）は、書込みが完了すると、途中から書込みを再開できるよう、どこまで書込んだかのフラッシュメモリアドレスを示すリトライポイントを記憶する（Ｓ６１０８）。ＥＣＵ（ＩＤ１）は、リトライポイントを記憶すると、ＣＧＷ１３に書込み完了を通知する（Ｓ６１０９）。

[0774] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から書込み完了の通知を受けると、ＤＣＭ１２を介してセンター装置３へ書換え状況の進捗情報を通知する（Ｓ６１１０）。センター装置３は、ＤＣＭ１２から送信された進捗情報に基づいて、携帯端末６から接続可能なウェブ画面を更新する（Ｓ６１１１）。携帯端末６は、センター装置３に接続し、更新された進捗状況として、例えば現在何％までロールバックが進んだか等を表示する（Ｓ６１１２）。ここで、携帯端末６に代えて、車載ディスプレイ７で進捗を表示することも可能である。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から書込み完了の通知を受けると、車載ディスプレイ７へ書換え状況の進捗情報を通知する（Ｓ６１１３）。車載デ

ィスプレイ７は、ロールバックの進捗状況の画面を更新し、表示する（Ｓ６１１４）。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から書込み完了の通知を受けると、次の書込みデータとして２番目の分割ファイルを取得し、ＥＣＵ（ＩＤ１）に配信する。以降、最後の書込みデータとしてＮ番目の分割ファイルまで、Ｓ６１０６～Ｓ６１１４の処理を繰返す。

[0775] ＥＣＵ（ＩＤ１）は、Ｎ番目の分割ファイルまで書込みを完了すると、フラッシュメモリのロールバック用プログラムに対して完全性検証を行い、正しく書込まれたか否かを確認する（Ｓ６１１５）。ＣＧＷ１３は、ＥＣＵ（ＩＤ１）から全ての分割ファイルの書込みを完了し、完全性検証に成功した旨の通知を受けると、バッテリ残量の監視及びバスの通信負荷の監視を終了する（Ｓ６１１６、Ｓ６１１７）。

[0776] 続いて、ＣＧＷ１３は、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に対してウェイクアップするように要求する（Ｓ６２０１）。ＣＧＷ１３は、インストールを行う前の旧バージョンで起動すべく、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に対し、ロールバック用のアクティベートを要求する（Ｓ６２０２）。１面単独メモリであるＥＣＵ（ＩＤ１）は、通常時の書換えと同様、再起動により旧バージョンのプログラムを起動する。２面メモリであるＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）は、通常時の書換えと異なり、運用面を切り替えることなく、現運用面であるＡ面のプログラムを起動する。

[0777] ＥＣＵ（ＩＤ１）は、ＣＧＷ１３からロールバック用のアクティベート要求を受けると、自己を再起動させる（Ｓ６２０３）。ＥＣＵ（ＩＤ１）は、再起動が完了すると、ＣＧＷ１３へロールバック用のアクティベート完了と共にプログラムバージョンを通知する（Ｓ６２０４）。

[0778] ＥＣＵ（ＩＤ２）は、ＣＧＷ１３からロールバック用のアクティベート要求を受けると、記憶している運用面情報を更新することなく、自己を再起動させる（Ｓ６２０５）。ＥＣＵ（ＩＤ２）は、引き続き運用面であるＡ面で正常に起動すると、ＣＧＷ１３へロールバック用のアクティベート完了と共

にプログラムバージョン及び運用面情報を通知する（Ｓ６２０６）。

[0779] ＥＣＵ（ＩＤ３）は、ＣＧＷ１３からロールバック用のアクティベート要求を受けると、記憶している運用面情報を更新することなく、自己を再起動させる（Ｓ６２０７）。ＥＣＵ（ＩＤ３）は、引き続き運用面であるＡ面で正常に起動すると、ＣＧＷ１３へロールバック用のアクティベート完了と共にプログラムバージョン及び運用面情報を通知する（Ｓ６２０８）。

[0780] ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）からロールバック用のアクティベート完了通知を受けると、ＤＣＭ１２を介してセンター装置３へロールバック完了を通知する（Ｓ６２０９）。ここで、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）に関するプログラムバージョン及び運用面情報も合わせて通知する。センター装置３は、ＤＣＭ１２から通知された情報をデータベースへ登録すると共に（Ｓ６２１０）、進捗状況としてキャンセル完了を示す表示にウェブ画面を更新する（Ｓ６２１１）。携帯端末６は、センター装置３へ接続し、キャンセルが完了した旨のウェブ画面を表示する（Ｓ６２１２）。

[0781] 又、ＣＧＷ１３は、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）からアロールバック用のアクティベート完了通知を受けると、車載ディスプレイ７へ進捗状況としてロールバックが完了した旨を通知する（Ｓ６２１３）。車載ディスプレイ７は、ロールバックが完了した旨を表示する（Ｓ６２１４）。

[0782] 最後に、ＣＧＷ１３は、電源管理ＥＣＵ２０に対し、ＩＧ電源オフを要求する（Ｓ６２１５）。電源管理ＥＣＵ２０は、インストール開始前のＩＧスイッチオフの状態に戻すべく、電力供給を遮断するよう、電源制御回路４３に要求する。電源制御回路４３により、ＩＧ電源ライン３９及びＡＣＣ電源ライン３８への電力供給が遮断されると、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）、ＥＣＵ（ＩＤ４）、ＥＣＵ（ＩＤ５）及びＥＣＵ（ＩＤ６）は、停止状態となる。

[0783] 以上のように、ＣＧＷ１３をリプログマスタとして複数の書換え対象ＥＣ

Ｕ１９に対するプログラムの更新を行うことができる。本実施形態では、ＥＣＵ（ＩＤ１）、ＥＣＵ（ＩＤ２）及びＥＣＵ（ＩＤ３）を１つのグループとしてアプリプログラムを書換える旨を説明したが、２つ目のグループとしてＥＣＵ（ＩＤ４）、ＥＣＵ（ＩＤ５）及びＥＣＵ（ＩＤ６）についてアプリプログラムを書換える際も同様である。この場合、第１グループのＥＣＵ１９に対してインストール及びアクティベートした後、第２グループのＥＣＵ１９に対してインストール及びアクティベートを行う。

[0784] 又、ＤＣＭ１２、ＣＧＷ１３、車載ディスプレイ装置７及び電源管理ＥＣＵ２０等のアプリプログラムについても、同様に書換え可能である。ただし、これらのＥＣＵは、プログラム更新中にアプリプログラムが動作できる必要があるため、２面メモリで構成されることが望ましい。

[0785] 次に、センター装置３の構成について図２３４から図２７０を参照して説明する。尚、第１実施形態から第５実施形態を説明する。

[0786] （第１実施形態）

以下、第１実施形態について図２３４から図２５３を参照して説明する。車両用プログラム書換えシステムは、車両に搭載されているＥＣＵの車両制御や診断等のアプリプログラムをＯＴＡにより書換え可能なシステムである。図２３４に示すように、車両用プログラム書換えシステム１は、通信ネットワーク２側のセンター装置３と、車両側の車両側システム４と、表示端末５とを有する。通信ネットワーク２は、例えば４Ｇ回線等による移動体通信ネットワークやインターネットやＷｉＦｉ（Wireless Fidelity）（登録商標）等を含んで構成される。

[0787] 表示端末５は、ユーザからの操作入力を受付ける機能や各種画面を表示する機能を有する端末であり、例えばユーザが携帯可能なスマートフォンやタブレット等の携帯端末６、車室内に配置されているナビゲーション機能を兼用するディスプレイやメータディスプレイ等の車載ディスプレイ７である。携帯端末６は、移動体通信ネットワークの通信圏内であれば、通信ネットワーク２に接続可能である。車載ディスプレイ７は、車両側システム４に接続

されている。

[0788] ユーザは、車室外であって移動体通信ネットワークの通信圏内であれば、アプリプログラムの書換えに関与する各種画面を携帯端末６で確認しながら操作入力を行い、アプリプログラムの書換えに関与する手続きを可能である。ユーザは、車室内では、アプリプログラムの書換えに関与する各種画面を車載ディスプレイ７で確認しながら操作入力を行い、アプリプログラムの書換えに関与する手続きを可能である。即ち、ユーザは、車室外と車室内で携帯端末６と車載ディスプレイ７を使い分け、アプリプログラムの書換えに関与する手続きを可能である。

[0789] センター装置３は、車両用プログラム書換えシステム１において通信ネットワーク２側のＯＴＡの機能を統括し、ＯＴＡセンターとして機能する。センター装置３は、ファイルサーバ８と、ウェブサーバ９と、管理サーバ１０とを有し、各サーバ８～１０が相互にデータ通信可能に構成されている。

[0790] ファイルサーバ８は、センター装置３から車両側システム４に送信されるアプリプログラムの管理機能を備え、アプリプログラムの提供事業者であるサプライヤ等から提供されるＥＣＵプログラム及びそれに付随する情報、ＯＥＭ（Original Equipment Manufacturer）から提供される配信諸元データ、車両側システム４から取得する車両状態等を管理するサーバである。ファイルサーバ８は、通信ネットワーク２を介して車両側システム４との間でデータ通信可能であり、配信パッケージのダウンロード要求が発生すると、リプログデータと配信諸元データをパッケージ化した配信パッケージを車両側システム４に送信する。ウェブサーバ９は、ウェブ情報を管理するサーバであり、携帯端末６に対し、アプリプログラムの書換えに関与する各種画面を提供する。管理サーバ１０は、アプリプログラムの書換えのサービスに登録しているユーザの個人情報等を管理し、車両毎のアプリプログラムの書換え履歴等を管理する。

[0791] 車両側システム４は、マスタ装置１１を有する。マスタ装置１１は、ＤＣＭ１２とＣＧＷ１３を有し、ＤＣＭ１２とＣＧＷ１３が第１バス１４を介し

てデータ通信可能に接続されている。ＤＣＭ１２は、センター装置３との間で通信ネットワーク２を介してデータ通信を行う車載通信機であり、ファイルサーバ８から配信パッケージをダウンロードすると、その配信パッケージから書込みデータを抽出してＣＧＷ１３に転送する。

[0792] ＣＧＷ１３は、データ中継機能を有する車両用ゲートウェイ装置であり、ＤＣＭ１２から書込みデータを取得すると、その書込みデータを、アプリプログラムを書換える書換え対象ＥＣＵに配信する。マスタ装置１１は、車両用プログラム書換えシステム１において車両側のＯＴＡの機能を統括し、ＯＴＡマスタとして機能する。尚、図２３４では、ＤＣＭ１２と車載ディスプレイ７が同一の第１バス１４に接続されている構成を例示しているが、ＤＣＭ１２と車載ディスプレイ７が別々のバスに接続されている構成でも良い。

[0793] ＣＧＷ１３には、第１バス１４に加え、第２バス１５、第３バス１６、第４バス１７、第５バス１８が車内側のバスとして接続されており、バス１５～１７を介して各種ＥＣＵ１９が接続されていると共に、バス１８を介して電源管理ＥＣＵ２０が接続されている。

[0794] 第２バス１５は、例えばボディ系ネットワークのバスである。第２バス１５に接続されているＥＣＵ１９は、例えばドアのロック／アンロックを制御するドアＥＣＵ、メータ表示を制御するメータＥＣＵ、エアコンの駆動を制御するエアコンＥＣＵ、ウィンドウの開閉を制御するウィンドウＥＣＵ等のボディ系の制御を行うＥＣＵである。第３バス１６は、例えば走行系ネットワークのバスである。第３バス１６に接続されているＥＣＵ１９は、例えばエンジンの駆動を制御するエンジンＥＣＵ、ブレーキの駆動を制御するブレーキＥＣＵ、自動変速機の駆動を制御するＥＣＴ（ＥＴＣ（Electronic Toll Collection System、登録商標））ＥＣＵ、パワーステアリングの駆動を制御するパワーステアリングＥＣＵ等の走行系の制御を行うＥＣＵである。

[0795] 第４バス１７は、例えばマルチメディア系ネットワークのバスである。第４バス１７に接続されているＥＣＵ１９は、例えばナビゲーションシステムを制御するためのナビゲーションＥＣＵ、電子式料金収受システム，すなわ

ちＥＣＴシステムを制御するＥＴＣＥＣＵ等のマルチメディア系の制御を行うＥＣＵである。バス１５～１７は、ボディ系ネットワークのバス、走行系ネットワークのバス、マルチメディア系ネットワークのバス以外の系統のバスであっても良い。又、バスの本数やＥＣＵ１９の個数は例示した構成に限らない。

[0796] 電源管理ＥＣＵ２０は、ＤＣＭ１２、ＣＧＷ１３、各種ＥＣＵ１９等の電源管理を行う機能を有するＥＣＵである。

[0797] ＣＧＷ１３には、第６バス２１が車外側のバスとして接続されている。第６バス２１には、ツール２３が着脱可能に接続されるＤＬＣ（Data Link Coupler）コネクタ２２が接続されている。車内側のバス１４～１８及び車外側のバス２１は、例えばＣＡＮ（Controller Area Network、登録商標）バスにより構成されており、ＣＧＷ１３は、ＣＡＮのデータ通信規格や診断通信規格（ＵＤＳ：ＩＳＯ１４２２９）にしたがってＤＣＭ１２、各種ＥＣＵ１９、ツール２３との間でデータ通信を行う。尚、ＤＣＭ１２とＣＧＷ１３がイーサーネットにより接続されていても良いし、ＤＬＣコネクタ２２とＣＧＷ１３がイーサーネットにより接続されても良い。

[0798] 書換え対象ＥＣＵ１９は、ＣＧＷ１３から書込みデータを受信すると、その書込みデータをフラッシュメモリに書込んでアプリプログラムを書換える。上記した構成では、ＣＧＷ１３は、書換え対象ＥＣＵ１９から書込みデータの取得要求を受信すると、書込みデータを書換え対象ＥＣＵ１９に配信するリプログマスタとして機能する。書換え対象ＥＣＵ１９は、ＣＧＷ１３から書込みデータを受信すると、その書込みデータをフラッシュメモリに書込んでアプリプログラムを書換えるリプログスレーブとして機能する。

[0799] アプリプログラムを書換える態様としては、有線で書換える態様と、無線で書換える態様とがある。アプリプログラムを有線で書換える態様では、ツール２３がＤＬＣコネクタ２２に接続されると、ツール２３は、書込みデータをＣＧＷ１３に転送する。ＣＧＷ１３は、ツール２３から転送された書込みデータを書換え対象ＥＣＵ１９に中継又は配信する。アプリプログラムを

無線で書換える態様では、上記したように、ＤＣＭ１２は、ファイルサーバ８から配信パッケージをダウンロードすると、その配信パッケージから書込みデータを抽出し、その書込みデータをＣＧＷ１３に転送する。

[0800] 図２３５に示すように、ＣＧＷ１３は、電気的な機能ブロックとして、マイクロコンピュータ（以下、マイコンと称する）２４と、データ転送回路２５と、電源回路２６と、電源検出回路２７とを有する。マイコン２４は、ＣＰＵ（Central Processing Unit）２４ａと、ＲＯＭ（Read Only Memory）２４ｂと、ＲＡＭ（Random Access Memory）２４ｃと、フラッシュメモリ２４ｄとを有する。マイコン２４は、非遷移的実体的記憶媒体に格納されている各種制御プログラムを実行して各種処理を行い、ＣＧＷ１３の動作を制御する。

[0801] データ転送回路２５は、バス１４～１８，２１との間のＣＡＮのデータ通信規格や診断通信規格に準拠したデータ通信を制御する。電源回路２６は、バッテリ電源（以下、＋Ｂ電源と称する）、アクセサリ電源（以下、ＡＣＣ電源と称する）、イグニッション電源（以下、ＩＧ電源と称する）を入力する。電源検出回路２７は、電源回路２６が入力する＋Ｂ電源の電圧値、ＡＣＣ電源の電圧値、ＩＧ電源の電圧値を検出し、これらの検出した電圧値を所定の電圧閾値と比較し、その比較結果をマイコン２４に出力する。マイコン２４は、電源検出回路２７から入力する比較結果により、外部からＣＧＷ１３に供給されている＋Ｂ電源、ＡＣＣ電源、ＩＧ電源が正常であるか異常であるかを判定する。

[0802] 図２３６に示すように、ＥＣＵ１９は、電気的な機能ブロックとして、マイコン２８と、データ転送回路２９と、電源回路３０と、電源検出回路３１とを有する。マイコン２８は、ＣＰＵ２８ａと、ＲＯＭ２８ｂと、ＲＡＭ２８ｃと、フラッシュメモリ２８ｄとを有する。マイコン２８は、非遷移的実体的記憶媒体に格納されている各種制御プログラムを実行して各種処理を行い、ＥＣＵ１９の動作を制御する。

[0803] データ転送回路２９は、バス１５～１７との間のＣＡＮのデータ通信規格

に準拠したデータ通信を制御する。電源回路３０は、＋Ｂ電源、ＡＣＣ電源、ＩＧ電源を入力する。電源検出回路３１は、電源回路３０が入力する＋Ｂ電源の電圧値、ＡＣＣ電源の電圧値、ＩＧ電源の電圧値を検出し、これらの検出した電圧値を所定の電圧閾値と比較し、その比較結果をマイコン２８に出力する。マイコン２８は、電源検出回路２７から入力する比較結果により、外部からＥＣＵ１９に供給されている＋Ｂ電源、ＡＣＣ電源、ＩＧ電源が正常であるか異常であるかを判定する。尚、ＥＣＵ１９は、接続する例えばセンサやアクチュエータ等の負荷が異なり、基本的には同等の構成である。又、ＤＣＭ１２、車載ディスプレイ７、及び電源管理ＥＣＵも、基本構成は図２３６に示すＥＣＵ１９と同様である。

[0804] 図２３７に示すように、電源管理ＥＣＵ２０、ＣＧＷ１３、ＥＣＵ１９は、＋Ｂ電源ライン３２、ＡＣＣ電源ライン３３、ＩＧ電源ライン３４に接続されている。＋Ｂ電源ライン３２は、車両バッテリ３５の正極に接続されている。ＡＣＣ電源ライン３３は、ＡＣＣスイッチ３６を介して車両バッテリ３５の正極に接続されている。ユーザがＡＣＣ操作を行うと、ＡＣＣスイッチ３６がオフからオンに切替わり、車両バッテリ３５の出力電圧がＡＣＣ電源ライン３３に印加される。ＡＣＣ操作とは、例えばキーを差込口に挿入する型の車両であれば、キーを差込口に挿入して「ＯＦＦ」位置から「ＡＣＣ」位置に回動する操作であり、スタートボタンを押下する型の車両であれば、スタートボタンを１回押下する操作である。

[0805] ＩＧ電源ライン３４は、ＩＧスイッチ３７を介して車両バッテリ３５の正極に接続されている。ユーザがＩＧ操作を行うと、ＩＧスイッチ３７がオフからオンに切替わり、車両バッテリ３５の出力電圧がＩＧ電源ライン３４に印加される。ＩＧ操作とは、例えばキーを差込口に挿入する型の車両であれば、キーを差込口に挿入して「ＯＦＦ」位置から「ＯＮ」位置に回動する操作であり、スタートボタンを押下する型の車両であれば、スタートボタンを２回押下する操作である。車両バッテリ３５の負極は接地されている。

[0806] ＡＣＣスイッチ３６とＩＧスイッチ３７の両方がオフであるときには、＋

Ｂ電源だけが車両側システム４に供給される。＋Ｂ電源だけが車両側システム４に供給されている状態を＋Ｂ電源状態と称する。ＡＣＣスイッチ３６がオンであり、ＩＧスイッチ３７がオフであるときには、ＡＣＣ電源と＋Ｂ電源が車両側システム４に供給される。ＡＣＣ電源と＋Ｂ電源が車両側システム４に供給されている状態をＡＣＣ電源状態と称する。ＡＣＣスイッチ３６とＩＧスイッチ３７の両方がオンであるときには、＋Ｂ電源とＡＣＣ電源とＩＧ電源が車両側システム４に供給される。＋Ｂ電源とＡＣＣ電源とＩＧ電源が車両側システム４に供給されている状態をＩＧ電源状態と称する。

[0807] ＥＣＵ１９は、電源状態に応じて起動条件が異なり、＋Ｂ電源状態で起動する＋Ｂ系ＥＣＵ、ＡＣＣ電源状態で起動するＡＣＣ系ＥＣＵ、ＩＧ電源状態で起動するＩＧ系ＥＣＵに区分される。例えば車両盗難等の用途で駆動するＥＣＵ１９は＋Ｂ系ＥＣＵである。例えばオーディオ等の非走行系の用途で駆動するＥＣＵ１９はＡＣＣ系ＥＣＵである。例えばエンジン制御等の走行系の用途で駆動するＥＣＵ１９はＩＧ系ＥＣＵである。

[0808] ＣＧＷ１３は、スリープ状態にあるＥＣＵ１９に対して起動要求を送信することで、その起動要求の送信先のＥＣＵ１９をスリープ状態から起動状態に移行させる。又、ＣＧＷ１３は、起動状態にあるＥＣＵ１９に対してスリープ要求を送信することで、そのスリープ要求の送信先のＥＣＵ１９を起動状態からスリープ状態に移行させる。ＣＧＷ１３は、例えばバス１５～１７に送信する送信信号の波形を異ならせることで、起動要求やスリープ要求の送信先のＥＣＵ１９を複数のＥＣＵの中から選択する。

[0809] ＡＣＣスイッチ３６及びＩＧスイッチ３７に対して電源制御回路３８が並列接続されている。ＣＧＷ１３は、電源制御要求を電源管理ＥＣＵ２０に送信し、電源管理ＥＣＵ２０に電源制御回路３８を制御させる。即ち、ＣＧＷ１３は、電源制御要求として電源起動要求を電源管理ＥＣＵ２０に送信し、ＡＣＣ電源ライン３３やＩＧ電源ライン３４と車両バッテリ３５の正極を電源制御回路３８の内部で接続させる。この状態では、ＡＣＣスイッチ３６やＩＧスイッチ３７がオフであってもＡＣＣ電源やＩＧ電源が車両側システム

４に供給される。ＣＧＷ１３は、電源制御要求として電源停止要求を電源管理ＥＣＵ２０に送信し、ＡＣＣ電源ライン３３やＩＧ電源ライン３４と車両バッテリ３５の正極を電源制御回路３８の内部で途絶させる。

[0810] ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９は、電源自己保持機能を有する。即ち、ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９は、起動状態にあるときに車両電源がＡＣＣ電源又はＩＧ電源から＋Ｂ電源に切替わると、その切替わった直後に起動状態からスリープ状態又は停止状態に移行するのではなく、その切替わった直後でも起動状態を所定時間に亘って継続して駆動電源を自己保持する。ＤＣＭ１２、ＣＧＷ１３、ＥＣＵ１９は、車両電源がＡＣＣ電源又はＩＧ電源から＋Ｂ電源に切替わった直後から所定時間（例えば数秒）が経過した後に起動状態からスリープ状態又は停止状態に移行する。

[0811] 次に、センター装置３からマスタ装置１１に配信される配信パッケージについて図２３８から図２３９を参照して説明する。車両用プログラム書換えシステム１においては、アプリプログラムの提供事業者であるサプライヤから提供される書込みデータと、主にＯＥＭから提供される書換え諸元データとからリプログデータが生成される。サプライヤから提供される書込みデータとしては、旧アプリプログラムと新アプリプログラムとの差分に相当する差分データと、新アプリプログラムの全体に相当する全データとがある。差分データや全データは周知のデータ圧縮技術により圧縮されていても良い。図２３８では、サプライヤＡ～Ｃから書込みデータとして差分データが提供され、サプライヤＡから提供されるＥＣＵ（ＩＤ１）の暗号済みの差分データと認証子、サプライヤＢから提供されるＥＣＵ（ＩＤ２）の暗号済みの差分データと認証子、サプライヤＣから提供されるＥＣＵ（ＩＤ３）の暗号済みの差分データと認証子、ＯＥＭから提供される書換え諸元データからリプログデータが生成されている場合を例示している。認証子は書込みデータ毎に付与されている。

[0812] 尚、図２３８では、旧アプリプログラムから新アプリプログラムに更新する際の差分データを示しているが、新アプリプログラムから旧アプリプログ

ラムに書き戻すためのロールバック用差分データを、合わせてリプログデータに含める構成としても良い。例えば、書換え対象ＥＣＵ１９が１面メモリの場合、リプログデータにロールバック用差分データを含める。

[0813] ＯＥＭから提供される書換え諸元データは、アプリプログラムの書換えに関与する情報として、書換え対象ＥＣＵ１９を特定可能な情報、書換え対象ＥＣＵ１９が複数であるときの書換え順序を特定可能な情報、後述するロールバック方法を特定可能な情報等を含み、ＤＣＭ１２やＣＧＷ１３や書換え対象ＥＣＵ１９における書換えに関与する動作を定義するデータである。書換え諸元データは、ＤＣＭ１２が使用するＤＣＭ用の書換え諸元データと、ＣＧＷ１３が使用するＣＧＷ用の書換え諸元データとに区分される。ＤＣＭ用の書換え諸元データには、書換え対象ＥＣＵ１９に対応するファイルの読出しに必要な情報が記載されている。ＣＧＷ用書換え諸元データには、上述のように、書換え対象ＥＣＵ１９における書換えを制御するために必要な情報が記載されている。

[0814] ＤＣＭ１２は、ＤＣＭ用の書換え諸元データを取得すると、そのＤＣＭ用の書換え諸元データを解析し、その解析結果にしたがってＣＧＷ１３への書込みデータの転送等の書換えに関与する動作を制御する。ＣＧＷ１３は、ＣＧＷ用の書換え諸元データを取得すると、そのＣＧＷ用の書換え諸元データを解析し、その解析結果にしたがってＤＣＭ１２からの書込みデータの取得や書換え対象ＥＣＵ１９への書込みデータの配信等の書換えに関与する動作を制御する。

[0815] ファイルサーバ８には、上記したリプログデータが登録されると共に、ＯＥＭから提供される配信諸元データが登録される。ＯＥＭから提供される配信諸元データは、表示端末５における各種画面の表示に関与する動作を定義するデータである。

[0816] ファイルサーバ８は、リプログデータと配信諸元データが登録されると、リプログデータを暗号化し、パッケージを認証するためのパッケージ認証子と、暗号済みのリプログデータと、配信諸元データとを１つのファイルにパ

ッケージングした配信パッケージを生成する。ファイルサーバ８は、外部から配信パッケージのダウンロード要求を受信すると、その配信パッケージをＤＣＭ１２に送信する。尚、ファイルサーバ８は、図２３８では、リプログデータと配信諸元データを格納した配信パッケージを生成し、リプログデータと配信諸元データを同時にＤＣＭ１２に送信する場合を例示しているが、リプログデータと配信諸元データを別々にＤＣＭ１２に送信しても良い。即ち、ファイルサーバ８は、先に配信諸元データをＤＣＭ１２に送信し、後からリプログデータをＤＣＭ１２に送信しても良い。又、ファイルサーバ８は、リプログデータと配信諸元データとを１つのファイルである配信パッケージとし、配信パッケージとパッケージ認証子とをＤＣＭ１２へ送信しても良い。

[0817] ＤＣＭ１２は、ファイルサーバ８から配信パッケージをダウンロードすると、その配信パッケージに格納されているパッケージ認証子と、暗号済みのリプログデータとを検証し、検証結果が正であると、暗号済みのリプログデータを復号化する。ＤＣＭ１２は、暗号済みのリプログデータを復号化すると、その復号化したリプログデータをアンパッケージングし、ＥＣＵ毎の暗号済みの差分データと認証子、ＤＣＭ用の書換え諸元データ、ＣＧＷ用の書換え諸元データを生成する。図２３９では、ＥＣＵ（ＩＤ１）の暗号済みの差分データと認証子、ＥＣＵ（ＩＤ２）の暗号済みの差分データと認証子、ＥＣＵ（ＩＤ３）の暗号済みの差分データと認証子、書換え諸元データを生成する場合を例示している。

[0818] 図２４０は、センター装置３における主としてサーバ８～１０の各機能に係る部分をブロック図化して示す。又、図２４１は、センター装置３がＥＣＵのプログラム更新に関して行う処理の概要を示す。尚、以下では「データベース」を「ＤＢ」と表記することがある。図２４０に示すように、センター装置３は、パッケージ管理部３Ａ，構成情報管理部３Ｂ，個車情報管理部３Ｃ及びキャンペーン管理部３Ｄを備えている。パッケージ管理部３Ａは、諸元データ生成部２０１，パッケージ生成部２０２及びパッケージ配信部２

０３と、ＥＣＵリプロデータＤＢ２０４，ＥＣＵメタデータＤＢ２０５及びパッケージＤＢ２０６とを有している。構成情報管理部３Ｂは、構成情報登録部２０７及び構成情報ＤＢ２０８を有している。

[0819] サプライヤは、管理サーバ１０のユーザインターフェイス（ＵＩ）機能である入力部２１８及び表示部２１９を用いて、ＥＣＵ個別のデータを登録する。ＥＣＵ個別のデータとして、新プログラムや差分データ等のプログラムファイル、プログラムファイルの検証データやサイズ、暗号化方式等のプログラムファイル関連情報、及びＥＣＵ１９のメモリ構造などＥＣＵ属性情報に関するものなどがある。プログラムファイルは、ＥＣＵリプロデータＤＢ２０４に記憶される。ＥＣＵ属性情報は、ＥＣＵメタデータＤＢ２０５に記憶される。プログラムファイル関連情報は、ＥＣＵリプロデータＤＢ２０４に記憶されてもよいし、ＥＣＵメタデータＤＢ２０５に記憶されても良い。ＥＣＵリプログデータＤＢ２０４は、更新データ記憶部の一例である。又、ＥＣＵメタデータＤＢ２０５は、装置関連情報記憶部の一例である。

[0820] ＯＥＭは、構成情報登録部２０７を介して、車両型式ごとに、正規の構成情報を構成情報ＤＢ２０８に登録する。正規の構成情報とは、公的な機関により認可された車両の構成情報である。構成情報は、車両に搭載されるＥＣＵ１９のハードウェア及びソフトウェアに関する識別情報であり、車両関連情報の一例である。構成情報には、複数のＥＣＵ１９から成るシステム構成の識別情報や、複数のシステムから成る車両構成の識別情報も含まれる。又、構成情報として、プログラムの更新に関する車両の制約情報を登録しても良い。例えば、書換え諸元データに記載されるＥＣＵのグループ情報，バス負荷テーブル，バッテリ負荷に関する情報等を登録しても良い。ＥＣＵメタデータＤＢ２０５は、装置関連情報記憶部の一例である。又、構成情報ＤＢ２０８は、車両情報記憶部の一例である。

[0821] 諸元データ生成部２０１は、各ＤＢを参照し、書換え諸元データを生成する。パッケージ生成部２０２は、書換え諸元データとリプログデータとを含む配信パッケージを生成し、パッケージＤＢ２０６に登録する。パッケージ

生成部２０２は、配信諸元データを含めて配信パッケージを生成しても良い。パッケージ配信部２０３は、登録された配信パッケージを車両側システム４に配信する。配信パッケージはファイルに相当する。

[0822] 個車情報管理部３Ｃは、個車情報登録部２０９，構成情報確認部２１０，更新有無確認部２１１及びＳＭＳ送信制御部２１２と、個車情報ＤＢ２１３とを有している。個車情報登録部２０９は、個々の車両よりアップロードされる個車情報を個車情報ＤＢ２１３に登録する。個車情報登録部２０９は、初期値として、車両生産又は販売時点での個車情報を、個車情報ＤＢ２１３に登録しても良い。構成情報確認部２１０は、アップロードされる個車情報の登録を行う際に、個車情報を、構成情報ＤＢ２０８に登録されている同一型式車両の構成情報と照合。更新有無確認部２１１は、個車情報について新たなプログラムによる更新の有無、すなわちキャンペーンの有無を確認する。ＳＭＳ送信制御部２１２は、個車情報が更新されている場合は、更新に関するメッセージを対応する車両にＳＭＳ（Short Message Service）により送信する。

[0823] キャンペーン管理部３Ｄは、キャンペーン生成部２１４，キャンペーン配信部２１５及び指示通知部２１６とキャンペーンＤＢ２１７とを備えている。ＯＥＭは、キャンペーン生成部２１４によりプログラム更新に関する情報であるキャンペーン情報を生成して、キャンペーンＤＢ２１７に登録する。尚、ここでのキャンペーン情報は、前述した「配信諸元データ」に相当し、主に車両側システム４で表示する更新内容に関する情報である。キャンペーン配信部２１５は、キャンペーン情報を車両に配信する。指示通知部２１６は、プログラム更新に関連して必要な指示を車両に通知する。車両側システム４では、センター装置３より送信されたキャンペーン情報に基づいて、更新プログラムのダウンロードを行うか否かを例えばユーザが判断し、必要であればダウンロードを行う。尚、各管理部３Ａ～３Ｄの各データベースを除く部分は、コンピュータのハードウェア及びソフトウェアにより実現されている機能である。車両通信部２２２は、センター装置３と車両側システム４

との間で無線により相互にデータ通信を行うための機能ブロックである。

[0824] 以下、上記の処理についてより詳細に説明するが、先ず各データベースに登録されるデータの内容を説明する。図２４２に示すように、構成情報ＤＢ２０８には、一例として以下のデータが登録される。「車両型式」は車種を示す。「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」は、車両全体に対するソフトウェアＩＤであり、車両ソフトウェアＩＤに相当する。「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」は各車両に1つだけ付与され、何れか1つ以上のＥＣＵのアプリプログラムのバージョンが更新されるのに伴い更新される。「Ｓｙｓ　ＩＤ」は、各車両に搭載されている複数のＥＣＵ１９のグループを「システム」とすると、そのシステムのＩＤである。

[0825] 例えば、図２３４において、ボディ系ＥＣＵ１９のグループがボディ系システム、走行系ＥＣＵ１９のグループが走行系システムである。「Ｓｙｓ　ＩＤ」は、システムを構成する何れか1つ以上のＥＣＵのアプリプログラムのバージョンが更新されるのに伴い更新される。「ＥＣＵ　ＩＤ」は、各ＥＣＵの種別を示す装置識別用のＩＤである。「ＥＣＵ　ＳＷ　ＩＤ」は、各ＥＣＵに対するソフトウェアＩＤであり、ＥＣＵソフトウェアＩＤに相当する。ここでは便宜上、「ＥＣＵ　ＩＤ」にソフトウェアのバージョンを付したもので示している。「ＥＣＵ　ＳＷ　ＩＤ」は、当該ＥＣＵのアプリプログラムのバージョンが更新されるのに伴い更新される。又、同一の「ＥＣＵ　ＩＤ」で同一のプログラムバージョンであったとしても、ハードウェア構成が異なる場合は、異なる「ＥＣＵ　ＳＷ　ＩＤ」を用いる。即ち、「ＥＣＵ　ＳＷ　ＩＤ」はＥＣＵの品番を示す情報でもある。

[0826] 図２４２では、「車両型式」＝「ａａａ」の車両に関する構成情報を示している。車両に搭載されるＥＣＵ１９のうち、自動運転ＥＣＵ（ＡＤＳ）、エンジンＥＣＵ（ＥＮＧ）、ブレーキＥＣＵ（ＢＲＫ）、及び電動パワーステアリングＥＣＵ（ＥＰＳ）を例示している。例えば、「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」＝「０００１」の「ＥＣＵ　ＳＷ　ＩＤ」が、「ａｄｓ＿００１」，「ｅｎｇ＿０１０」，「ｂｒｋ＿００１」，「ｅｐｓ＿０１０」であ

るのに対し、「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」＝「０００２」の「ＥＣＵ　ＳＷ　ＩＤ」は、「ａｄｓ＿００２」，「ｅｎｇ＿０１０」，「ｂｒｋ＿００５」，「ｅｐｓ＿０１１」であり、３つのソフトウェアバージョンが更新されている。これに伴い、「Ｓｙｓ　ＩＤ」＝「ＳＡ０１」は「ＳＡ０２」に更新され、「Ｓｙｓ　ＩＤ」＝「ＳＡ０２」は「ＳＡ０３」に更新される。このように、構成情報ＤＢ２０８には、車両の生産又は販売時点で初期値が登録され、その後、何れか1つ以上のＥＣＵのアプリプログラムのバージョンが更新されるのに伴い更新される。すなわち、構成情報ＤＢ２０８は、各車両型式について、市場で正規に存在する構成情報を示す。

[0827] 図２４３に示すように、ＥＣＵリプロデータＤＢ２０４には、一例として以下のプログラムやデータが登録される。図２４３では、ある車両型式に搭載されるＥＣＵ１９のうち、アプリプログラムが更新されるＥＣＵ１９として、自動運転ＥＣＵ（ＡＤＳ）、ブレーキＥＣＵ（ＢＲＫ）、及び電動パワーステアリングＥＣＵ（ＥＰＳ）を例示している。これら更新対象ＥＣＵ１９の最新の「ＥＣＵ　ＳＷ　ＩＤ」について、ＥＣＵの旧プログラム及び新プログラムファイル，新プログラムの完全性検証データ，新プログラムと旧プログラムとの差分データである更新データファイル，更新データの完全性検証データ，同じく差分データであるロールバックデータファイル，ロールバックデータの完全性検証データ等が登録される。完全性検証データは、データ値にハッシュ関数を適用して得られるハッシュ値である。尚、更新データを、差分データに替えて新プログラムの全データとする際には、更新データの完全性検証データは、新プログラムの同データに等しくなる。

[0828] 尚、図２４３では、最新の「ＥＣＵ　ＳＷ　ＩＤ」についてのデータ構造を示したが、古い「ＥＣＵ　ＳＷ　ＩＤ」についてのデータが保存されている場合、旧プログラムファイルについては、１つ古い「ＥＣＵ　ＳＷ　ＩＤ」の新プログラムファイルを参照するよう構成しても良い。又、各完全性検証データは、サプライヤにて演算した値を登録する形式としても良いし、センター装置３が演算して登録する形式としても良い。

[0829] 図２４４に示すように、ＥＣＵメタデータＤＢ２０５には、一例として以下に示すＥＣＵ個別の諸元データが登録される。最新の「ＥＣＵ　ＳＷ　ＩＤ」について、更新データファイルのサイズ，ロールバックデータファイルのサイズ，ＥＣＵ１９が備えるフラッシュメモリ２８ｄが２面以上の構成である場合に、Ａ面，Ｂ面，Ｃ面等何れの面用のプログラムであるかを示す面情報，転送サイズ，プログラムファイルの読出し用アドレス等である。これらは更新データ関連情報の一例である。

[0830] 又、ＥＣＵメタデータＤＢ２０５には、ＥＣＵ１９の属性を示す属性情報も登録される。属性情報とは、ＥＣＵに関するハードウェア属性、及びソフトウェア属性を示す情報である。「転送サイズ」は、ＣＧＷ１３からＥＣＵ１９へ書換えデータを分割して転送する際の転送サイズ、「鍵」は、ＣＧＷ１３がＥＣＵ１９へセキュアにアクセスする際に用いる鍵である。これらは、ソフトウェア属性情報の一例である。又、「車両型式」及び「ＥＣＵ　ＩＤ」について、ＥＣＵ１９が備えるフラッシュメモリ２８ｄのメモリ構成，ＥＣＵ１９が接続されているバス種別，ＥＣＵ１９に接続されている電源の種類なども含まれる。これらは、ハードウェア属性情報の一例である。

[0831] ここで、メモリ構成「１面」はフラッシュ面を１面で持つ１面単独方式メモリであり、「２面」はフラッシュ面を２面で持つ２面メモリであり、「サスペンド」はフラッシュ面を疑似的な２面で持つ１面サスペンド方式メモリである。ハードウェア属性情報及びソフトウェア属性情報は、車両側システム４において、個々のＥＣＵ１９の書換え制御に用いられる情報である。ハードウェア属性情報は、予めＣＧＷ１３が記憶しておくことも可能であるが、本実施例では、車両側システム４での管理負荷を軽減するため、センター装置３にて管理することとした。又、ソフトウェア属性情報は、個々のＥＣＵ１９の書換え動作を直接指定するデータである。車両側システム４における柔軟な制御が実現できるよう、センター装置３にて管理することとした。

[0832] 図２４５に示すように、個車情報ＤＢ２１３には、一例として以下に示す個車毎のデータが登録される。主に、個車毎の構成情報や、プログラム更新

に対する個車のステータス情報が登録される。具体的には、各車両のＩＤである「ＶＩＮ」について、構成情報である「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」，「Ｓｙｓ　ＩＤ」，「ＥＣＵ　ＩＤ」，「ＥＣＵ　ＳＷ　ＩＤ」等である。これら構成情報についてのハッシュ値である「Ｄｉｇｅｓｔ」値も、センター装置３にて演算され、記憶される。「運用面」は、メモリ構成が２面である場合に、ＥＣＵ１９が現在運用しているプログラムが書き込まれている面であり、構成情報とともにアップロードされた値が登録される。

[0833] 「アクセスログ」は、車両が個車情報をセンター装置３にアップロードした年月日及び時刻である。「リプロステータス」は、車両におけるリプログのステータスを示し、例えば「キャンペーン発行済み」，「アクティベート完了」，「ダウンロード完了」等がある。つまり、この進捗ステータスにより、車両におけるリプログが、どのフェーズまで進み、どのフェーズで停滞しているかが分かる。尚、車両側システム４よりセンター装置３に対して構成情報等がアップロードされる際には、その情報等に各車両の「ＶＩＮ」が付与される。

[0834] 図２４６に示すように、パッケージＤＢ２０６には、配信パッケージのＩＤ，配信パッケージファイル及び配信パッケージの完全性検証用のデータが登録される。図２４７に示すように、キャンペーンＤＢ２１７には、以下のデータが登録される。キャンペーン情報のＩＤ，配信パッケージＩＤ，キャンペーン内容として具体的な更新内容を示すテキスト文等のメッセージ情報，キャンペーンの対象となる車両のＩＤである「ＶＩＮ」のリスト，更新前後の「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」，更新前後の「ＥＣＵ　ＳＷ　ＩＤ」のリスト等である。「対象ＶＩＮ」リストは、個車情報ＤＢ２１３とキャンペーンＤＢ２１７とを照合して登録することができる。尚、これらのキャンペーン情報は、パッケージＤＢ２０６に併せて登録しても良い。

[0835] 次に、本実施形態の作用について説明する。図２４８では、パッケージ管理部３ＡにおけるＥＣＵリプロデータＤＢ２０４への登録処理について説明する。図２４８に示すように、表示部２１９及び入力部２１８は、管理サー

バ１０のリプロデータ登録用の画面を起動し、サプライヤの作業者からＥＣＵ１９の新旧プログラムファイルの入力を受け付ける（Ａ１）。例えば、構成情報をＣＳＶ形式等で記入したファイルを、ファイルとして登録させるＵＩ等を用いても良い。続いて、パッケージ管理部３Ａは、新プログラムの完全性検証データを生成し（Ａ２）、更新用の差分データとして旧プログラムをベースとして新プログラムへ更新する際の差分データファイル及び更新用差分データの完全性検証データを生成する（Ａ３，Ａ４）。

[0836] 次に、ロールバック用の差分データとして新プログラムをベースとして旧プログラムへ更新する際の差分データファイル及び当該データの完全性検証データを生成する（Ａ５，Ａ６）。これらのプログラムファイル及び検証データをＥＣＵリプロデータＤＢ２０４に登録すると共に、１つ古い「ＥＣＵ　ＳＷ　ＩＤ」に基づいて新たな「ＥＣＵ　ＳＷ　ＩＤ」を生成し、登録する（Ａ７）。ここで、差分でなく全データを配信する場合は、差分データに関するステップは省略可能である。

[0837] 完全性検証データは、例えばハッシュ関数を適用して生成されるハッシュ値である。例えばハッシュ関数としてＳＨＡ－２５６（Secure Hash Algorithm 256-bit）を用いる場合は、データ値を６４バイト毎にメッセージブロックに区切る。そして、初期ハッシュ値に対して最初のメッセージブロックのデータ値を適用し、３２バイト長のハッシュ値を得ると、そのハッシュ値に次のメッセージブロックのデータ値を適用し、同様に３２バイト長のハッシュ値を得ることを順次繰り返す。

[0838] 図２４９では、諸元データ生成部２０１における書換え諸元データの生成処理について説明する。ここでは、「車両型式」＝「ａａａ」の車両に対する書換え諸元データの生成処理について説明するが、他の車両についても同様である。

[0839] センター装置３は、諸元データ生成部２０１の諸元データ生成プログラムを起動し、表示部２１９及び入力部２１８を介してＯＥＭの作業者からの入力を受付ける。先ず、諸元データ生成部２０１は、更新対象とするＥＣＵ１

９を決定する。図２４９に示すように、諸元データ生成部２０１は、ＥＣＵリプロデータＤＢ２０４にアクセスして、登録されている「ＥＣＵ　ＳＷ　ＩＤ」のうち、更新対象とするものを選択できる表示画面を表示部２１９に出力する。諸元データ生成部２０１は、入力部２１８を介してＯＥＭの作業者により選択された１以上の「ＥＣＵ　ＳＷ　ＩＤ」を、特定のＥＣＵ順序で保持する（Ｂ１）。ここでＥＣＵ順序とは、車両側システム４におけるＥＣＵ１９の書換え順序を示すものである。諸元データ生成部２０１は、ＯＥＭの作業者により指定された順番を特定のＥＣＵ順序とする。

[0840] 又、諸元データ生成部２０１は、構成情報ＤＢ２０８にアクセスして、ＯＥＭの作業者からの入力を受けることなく、更新対象とするＥＣＵ１９を決定しても良い。諸元データ生成部２０１は、最新の「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」に対する「ＥＣＵ　ＳＷ　ＩＤ」と、１つ古い「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」に対する「ＥＣＵ　ＳＷ　ＩＤ」とを参照し、更新のあったＥＣＵ１９を抽出する。例えば、図２４２において、「ＡＤＳ」「ＢＲＫ」「ＥＰＳ」が更新対象ＥＣＵ１９である。諸元データ生成部２０１は、構成情報ＤＢ２０８に登録されている順番を、特定のＥＣＵ順序とする。

[0841] そして、諸元データ生成部２０１は、更新対象とする複数の「ＥＣＵ　ＳＷ　ＩＤ」を有するＥＣＵについてグループ情報を生成する（Ｂ２）。ここでは、構成情報ＤＢ２０８を参照し、「Ｓｙｓ　ＩＤ」を用い、例えばグループ１を「Ｓｙｓ　ＩＤ」が「ＳＡ０１＿０２」である「ＥＣＵ　ＩＤ」でまとめ、グループ２を「Ｓｙｓ　ＩＤ」が「ＳＡ０２＿０２」である「ＥＣＵ　ＩＤ」でまとめる。例えば、図２４２において、グループ１を「ＡＤＳ」とし、グループ２を１番目が「ＢＲＫ」、２番目が「ＥＰＳ」とする。このように、諸元データ生成部２０１は、更新対象とするＥＣＵと、ＥＣＵの属するグループと、グループ内のＥＣＵ順序とを決定する。

[0842] 次に、諸元データ生成部２０１は、ＥＣＵメタデータＤＢ２０５にアクセスして、更新対象としたＥＣＵ１９に関する諸元データとして、更新データ関連情報、ハードウェア属性情報、及びソフトウェア属性情報を取得する（

Ｂ３）。例えば図２５０に示すように、更新データ関連情報は、「更新プログラムバージョン」「更新プログラム取得アドレス」「更新プログラムサイズ」「ロールバックプログラムバージョン」「ロールバックプログラム取得アドレス」「ロールバックプログラムサイズ」「書込みデータ種別」「書込み面」である。ハードウェア属性情報は、「接続バス」「接続電源」「メモリ種別」である。ソフトウェア属性情報は、「書換え面情報」「セキュリティアクセス鍵情報」「書換え方法」「転送サイズ」である。「書換え方法」とは、ＩＧオンからオフに切り替わった際、電源自己保持回路を有効として書換えを行うか（電源自己保持）、それとも、ＩＧオン及びＩＧオフに従って書換えを行うか（電源制御）、を示すデータである。「セキュリティアクセス鍵情報」として、鍵以外の情報を含めても良い。

[0843] 以下、各情報について説明する。

・「書込みデータ種別」は、プログラムが差分データか全データかを示す種別である。更新プログラムに対する書込みデータ種別と、ロールバックプログラムに対する書込みデータ種別とを別々に記載しても良い。

・「書込み面」は、２面メモリのＥＣＵ１９に対し、いずれの面に書込むためのプログラムかを示す情報である。

・「接続バス」は、ＥＣＵ１９が接続されるバスを識別する情報である。

・「接続電源」は、ＥＣＵ１９が接続される電源状態を示す情報であり、バッテリ電源（＋Ｂ電源）、アクセサリ電源（ＡＣＣ電源）、及びイグニッション電源（ＩＧ電源）のいずれかを示す値が記載される。

・「メモリ種別」は、ＥＣＵ１９のメモリ構成を識別する情報であり、２面メモリ、１面サスペンド方式メモリ（疑似２面メモリ）、及び１面メモリ等を示す値が記載される。

・「書換え面情報」は、ＥＣＵ１９のいずれの面が起動面（運用面）で、いずれの面が書換え面（非運用面）であるかを示す情報である。

・「セキュリティアクセス鍵情報」は、鍵を用いてＥＣＵ１９へのアクセス認証を行うための情報であり、鍵導出鍵、鍵パターン、及び復号演算パター

ンの情報を含む。

・「転送サイズ」は、ＥＣＵ１９へプログラムを分割して転送する際のデータサイズである。

[0844] これらの情報は、例えば図２５０に示すように、「ＥＣＵ　ＩＤ」をキーとして、上述した特定のＥＣＵ順序として保持する。諸元データ生成部２０１は、全てのＥＣＵについて情報を取得すると（Ｂ４；ＹＥＳ）、更新対象となる車両について「書換え環境情報」を指定する（Ｂ５）。「書換え環境情報」とは、ＥＣＵのグループ又は車両全体を対象とした、車両側システム４における書換え制御に用いられる情報であって、書換え動作を直接指定するデータである。例えば、車両全体を対象とした書換え環境情報としては、車両側システム４におけるプログラム更新を車両の走行中（ＩＧスイッチのオン中）に行うか駐車中（ＩＧスイッチのオフ中）に行うかを示す「車両状態」、車両側システム４においてプログラム更新を実行可能なバッテリ残量の制約を示す「バッテリ負荷（バッテリの残量）」，車両側システム４において書込みデータを転送可能なバス負荷の制約を示すバス負荷テーブル情報等である。

[0845] 又、グループを対象とした書換え環境情報としては、そのグループに属するＥＣＵ１９及びグループ内のＥＣＵ順序等である。車両側システム４では、プログラム更新がグループ単位で同期するよう制御し、指定されたＥＣＵ順序でＥＣＵ１９への書込みを実行する。諸元データ生成部２０１は、書換え環境情報登録用の画面を起動し，ＯＥＭの作業者から入力を受付ける。又は、書換え環境情報が入力されたエクセル（登録商標）をインポートする形式としても良い。又は、構成情報ＤＢ２０８に登録された制約情報を抽出する形式としても良い。尚、諸元データ生成部２０１は、グループを対象とした書換え環境情報としては、上述したステップＢ２の生成結果を用いる。

[0846] バス負荷テーブルは、電源状態とバスの伝送許容量との対応関係を示すテーブルである。図２５１に示すように、伝送許容量は、最大伝送許容量に対して伝送可能な車両制御データと書込みデータとの伝送量の合計である。こ

の例示では、第１バスについて、伝送許容量が最大伝送許容量に対して「８０％」であるので、ＣＧＷ１３は、ＩＧ電源状態では、車両制御データの伝送許容量として最大伝送許容量に対して「５０％」を許容し、書込みデータの伝送許容量として最大伝送許容量に対して「３０％」を許容する。又、ＣＧＷ１３は、ＡＣＣ電源状態では、車両制御データの伝送許容量として最大伝送許容量に対して「３０％」を許容し、書込みデータの伝送許容量として最大伝送許容量に対して「５０％」を許容する。又、ＣＧＷ１３は、＋Ｂ電源状態では、車両制御データの伝送許容量として最大伝送許容量に対して「２０％」を許容し、書込みデータの伝送許容量として最大伝送許容量に対して「６０％」を許容する。第２バス及び第３バスについても同様である。

[0847] 最後に、諸元データ生成部２０１は、生成又は取得した各データを、予め定められた所定のデータ構造に合せて配置し、図２５０に示すような書換え諸元データを生成する（Ｂ６）。すなわち、諸元データ生成部２０１は、車両側システム４で解釈可能なデータ構造にて書換え諸元データを生成する。尚、各ＥＣＵ情報については、グループの若い順かつグループ内ＥＣＵ順序に従って書換え諸元データに記載すると良い。例えば、図２４２において、グループ１を「ＡＤＳ」とし、グループ２を１番目が「ＢＲＫ」、２番目が「ＥＰＳ」とする場合、諸元データのＥＣＵ情報欄は、最初に「ＡＤＳ」のＥＣＵ情報、次に「ＢＲＫ」のＥＣＵ情報、最後に「ＥＰＳ」のＥＣＵ情報が並ぶこととなる。

[0848] 図２５０に示す諸元データにおいて、ＥＣＵ情報の「ＥＣＵ　ＩＤ」～「転送サイズ」は、対象ＥＣＵ１９の種別を含む対象装置関連情報の一例であり、上述したハードウェア属性情報及びソフトウェア属性情報に対応する。又、「更新プログラムバージョン」～「書込み面」は更新データ関連情報の一例である。又、ＥＣＵのグループ又は車両全体を対象とした「書換え環境」は、車両における更新処理を指定する更新処理情報の一例である。

[0849] 図２５２では、パッケージ生成部２０２におけるパッケージ生成処理について説明する。前述と同様、ここでは、「車両型式」＝「ａａａ」の車両に

対するパッケージ生成処理について説明する。図２５２に示すように、作業者の指示を契機として、センター装置３はパッケージ管理部３Ａのパッケージ生成部２０２を起動する。パッケージ生成部２０２は、ステップＢ１と同様に更新対象とする「ＥＣＵ　ＳＷ　ＩＤ」を決定する（Ｃ１）。パッケージ生成部２０２は、更新対象とする「ＥＣＵ　ＳＷ　ＩＤ」に対応する各データをＥＣＵリプロデータＤＢ２０４より取得して１つのリプログデータを生成する（Ｃ２）。例えば、図２４３において、パッケージ生成部２０１は、新プログラムの完全性検証データ、差分データである更新データ、更新データの完全性検証データ、旧プログラムの完全性検証データ、差分データであるロールバックデータ、及びロールバックデータの完全性検証データを取得し、リプログデータを生成する。そして、生成したリプログデータとステップＢ１～Ｂ６にて説明した、対応する書換え諸元データとを統合して一つの配信パッケージファイルを生成する（Ｃ３）。次に、生成したパッケージファイルについての完全性検証データを生成し（Ｃ４）、パッケージファイルと共にパッケージＤＢ２０６に登録する（Ｃ５）。

[0850] 図２５３は、上記のように生成されたパッケージファイルの内容をイメージ的に示したものである。更新対象とする「ＡＤＳ」、「ＢＲＫ」及び「ＥＰＳ」に対応する更新データや完全性検証データを、ＥＣＵ順序に従って１つのリプログデータに統合し、さらに書換え諸元データと統合して一つの配信パッケージファイルを生成するイメージを示している。ここで、ロールバックデータは、更新対象とするＥＣＵ１９のメモリ構成が１面の場合にのみ、リプログデータへ含めるとしても良い。メモリ構成が２面又はサスペンドの場合、運用面に対する書換えは行わないため、旧プログラムであるロールバックデータは省略可能である。

[0851] 以上のように本実施形態によれば、センター装置３のＥＣＵリプロデータＤＢ２０４には、車両に搭載される複数のＥＣＵ１９のうち、アプリプログラムを更新する対象となるＥＣＵ１９の更新プログラムのデータが記憶される。構成情報ＤＢ２０８には、車両に搭載される複数のＥＣＵ１９それぞれ

に対する「ＥＣＵ　ＩＤ」及びＥＣＵ１９に記憶されるアプリプログラムの「ＥＣＵ　ＳＷ　ＩＤ」等の車両関連情報が、車両の種別と共に記憶される。ＥＣＵメタデータＤＢ２０５には、書換え対象ＥＣＵ１９の属性及び更新データに関連する更新データ関連情報が記憶される。

[0852] そして、諸元データ生成部２０１は、対象ＥＣＵ１９に書込む更新データと共に車両へ送信する諸元データを、構成情報ＤＢ２０８及びＥＣＵメタデータＤＢ２０５に記憶された情報に基づいて、対象ＥＣＵ１９についての種別、属性、更新データ関連情報、及びデータ更新に関する書換え環境を示す情報を含むように生成する。更に、パッケージ生成部２０２は、諸元データとリプログデータとを含む配信パッケージを生成し、パッケージＤＢ２０６に登録する。そして、パッケージ配信部２０３は、登録された配信パッケージを車両側システム４に配信する。これにより、車両側システム４は、更新データと共に送信される諸元データを受信することで、その諸元データに基づいて、対象ＥＣＵ１９を適切に選択し、更新データを用いた書き込み処理を適切に制御することが可能になる。

[0853] そして、諸元データ生成部２０１は、複数のＥＣＵ１９に対する諸元データを１つのファイルとして生成し、さらにパッケージ生成部２０２が複数のＥＣＵ１９に対するリプログデータとともに１つのファイルとしてパッケージ化するので、車両側システム４は、１つの配信パッケージを受信すれば複数のＥＣＵ１９に更新データを書き込むことができる。

[0854] 又、諸元データとしての車両関連情報には、複数のＥＣＵ１９の一部をグルーピングしたグループ情報を含むので、車両側システム４は、グループ情報で規定される順序に従って対象となるＥＣＵ１９を選択し、更新データを書き込むことができる。例えば、ある機能改善の対象となるＥＣＵ１９が多数ある場合、グループ１をボディ系ＥＣＵ１９、グループ２を走行系ＥＣＵ１９、グループ３をＭＭ系ＥＣＵ１９とすることで、車両側システム４におけるプログラム更新を、３回に分けて実行させることが可能となる。そのため、プログラム更新を全ＥＣＵまとめて実行する場合に比べ、回ごとのユー

ザの待ち時間を短縮することができる。

[0855] 又、書換え環境情報には、車両に関する「車両状態（ＩＧオン状態）」及び「バッテリ負荷」と、ＥＣＵ１９に関する「バス負荷テーブル」とを含むので、車両側システム４は、これらの情報に基づいて更新データを書き込むタイミング等を決定できる。つまり、ＯＥＭ又はセンター装置３を用いたサービス事業者は、書換え環境情報として、車両に対する実行制約条件を指定することにより、柔軟なプログラム更新を運用可能となる。

[0856] 加えて、諸元データ生成部２０１は、予め設定された書換え順番の早いＥＣＵ１９に関する情報から順に、予め定められたデータ構造に従って諸元データを生成するので、車両側システム４は、諸元データにおけるＥＣＵ　ＩＤの配置順に従って更新データを書き込むことができる。つまり、互いに連携し合う処理を有するＥＣＵ１９を１つのグループにグルーピングし、その連携し合う処理の内容を考慮し、ＥＣＵ順序を規定することで、車両側システム４において、新プログラムへの更新タイミングが完全に同期しなかった場合でも、不都合なくプログラム更新を完了させることができる。例えば、ＥＣＵ（ＩＤ１）の新プログラムが、ＥＣＵ（ＩＤ２）へ所定メッセージを送信する処理を有しており、ＥＣＵ（ＩＤ２）の新プログラムが、ＥＣＵ（ＩＤ１）から送信される所定メッセージが受信できない場合にタイムアウトエラーとなる処理を有している場合、ＥＣＵ（ＩＤ１）を先に更新し、ＥＣＵ（ＩＤ２）を後から更新するようＥＣＵ順序を規定すると良い。

[0857] （第２実施形態）

図２５４に示すように、第２実施形態は、図２４１において車両側システム４が最初にセンター装置３に送信を行う「車両構成情報同期」に関するものである。車両側でＩＧスイッチ３７がオンされると、それを契機としてＣＧＷ１３は、ＤＣＭ１２に対して「同期開始要求」を送信する。ＤＣＭ１２はそれを受けて「構成情報収集要求」をＣＧＷ１３に返信する。すると、ＣＧＷ１３は、各ＥＣＵ１９に対してプログラムバージョンの問い合わせを行う。各ＥＣＵ１９は、「ＥＣＵ　ＳＷ　ＩＤ」をＣＧＷ１３に返信する。又

、メモリ構成が２面又はサスペンドのＥＣＵ１９は、複数ある面のうち何れが運用面であって、何れが非運用面であるかを示す面情報も、合わせてＣＧＷ１３へ返信する。更に、各ＥＣＵ１９は、制御対象となるアクチュエータ等のキャリブレーション情報や、プログラム更新サービスを受けるためのライセンス情報や、ＥＣＵ１９に発生している故障コードを、合わせてＣＧＷ１３へ送信しても良い。

[0858] ＣＧＷ１３は、各ＥＣＵ１９からの「ＥＣＵ　ＳＷ　ＩＤ」の受信を完了すると、それらの全てを「ＶＩＮ」と共にＤＣＭ１２に送信する。このとき、ＣＧＷ１３で管理している「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」及び「Ｓｙｓ　ＩＤ」も合わせてＤＣＭ１２へ送信しても良い。ＤＣＭ１２はそれを受けて、全ての「ＥＣＵ　ＳＷ　ＩＤ」を対象とし、例えばハッシュ関数を用いてダイジェスト値であるハッシュ値を１つ生成する。前述のように、ハッシュ関数としてＳＨＡ－２５６を用いる場合は、全ての「ＥＣＵ　ＳＷ　ＩＤ」の値をシリアルに連結したデータ値を６４バイト毎にメッセージブロックに区切り、初期ハッシュ値に対して最初のメッセージブロックのデータ値を適用し３２バイト長のハッシュ値を得て、そのハッシュ値に順次後続のメッセージブロックのデータ値を適用し、最終的に３２バイト長のハッシュ値を得る。ここで、ＤＣＭ１２は、全ての「ＥＣＵ　ＳＷ　ＩＤ」だけでなく「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」、「Ｓｙｓ　ＩＤ」、面情報及びキャリブレーション情報を含む値を対象とし、１つのハッシュ値を生成しても良い。

[0859] ＤＣＭ１２は、上記のようにして得た「ＥＣＵ　ＳＷ　ＩＤ」のダイジェスト値を、「ＶＩＮ」と共にセンター装置３に送信する。又、ＤＣＭ１２は、故障コードやライセンス情報を、ダイジェスト値と合わせて送信しても良い。以下では、前記ダイジェスト値を「構成情報ダイジェスト」と称し、その元である「ＥＣＵ　ＳＷ　ＩＤ」の全てのデータ値を「構成情報オール」と称する場合がある。「構成情報オール」には、「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」、「Ｓｙｓ　ＩＤ」、面情報、及びキャリブレーション情報を含めるとしても良い。

[0860] センター装置３は、後述するように、ダイジェスト値の比較や個車情報ＤＢ２１３の更新を行う。構成情報を同期させたセンター装置３は、プログラム更新の有無を確認し、更新がある場合はキャンペーン情報を車両側システム４へ通知する。その後、車両側システム４が、配信パッケージをダウンロードし、対象となるＥＣＵ１９へのインストールを行い、新プログラムのアクティベートを行う。これら更新処理が完了したことを契機として、ＣＧＷ１３は、ＤＣＭ１２に対して「同期開始要求」を送信し、以降、同期完了通知まで前述と同様の処理を行う。又、ＩＧスイッチ３７がオンされたことを契機として行われる上述の処理を、プログラムの更新後にも行っても良い。

[0861] 図２５５に示すように、センター装置３の個車情報管理部３Ｃは、車両側システム４より「構成情報ダイジェスト」を受信すると（Ｄ１）、その時点で個車情報ＤＢ２１３に登録されている対応する車両の「構成情報ダイジェスト」と照合し、両者が一致するか否かを判断する（Ｄ２）。「個車情報ダイジェスト」は、個車情報ＤＢ２１３に予め演算した値を登録しておいても良いし、車両側システム４から受信した時点で、個車情報ＤＢ２１３に登録されている構成情報を用いてダイジェスト値を演算しても良い。両者が一致すれば（ＹＥＳ）、車両の個車情報が構成情報ＤＢ２０８に登録されている正規の組み合わせに適合するか否かを判断する（Ｄ６）。尚、構成情報ＤＢ２０８が所定のタイミングで更新される可能性もあるため、ステップＤ２において両者が一致した場合も（ＹＥＳ）、両者が不一致の場合も（ＮＯ）、ステップＤ６の判断は行うこととする。

[0862] ここで、上記の適合するか否かの判断は、例えば図２５６に示すように、車両側システム４からアップロードされた構成情報の「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」と「ＥＣＵ　ＳＷ　ＩＤ」との組み合わせが正規か否かをチェックする。同図に示すリストにおいて、構成情報ＤＢ２０８に登録されている「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ＝０００１」に対応する「ＥＣＵ　ＩＤ＝ＡＤＳ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ａｄｓ＿００１」，「ＥＣＵ　ＩＤ＝ＢＲＫ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ｂｒｋ＿００１」、「ＥＣＵ　ＩＤ

＝ＥＰＳ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ｅｐｓ＿０１０」である。

[0863] これに対して、ＶＩＮ＝３００の車両Ｃは同じく「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ＝０００１」であるが、「ＥＣＵ　ＩＤ＝ＡＤＳ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ａｄｓ＿００２」，「ＥＣＵ　ＩＤ＝ＢＲＫ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ｂｒｋ＿００３」であり、これら２つのＥＣＵ１９は、構成情報ＤＢ２０８に登録されている構成情報とは異なっている。したがって、ステップＤ６では「ＮＯ」，つまり非正規であり「ＮＧ」と判断し、構成情報確認部２１０が車両側システム４及びＯＥＭ等の生産した車両の情報を管理する装置である、図２４１に示す管理装置２２０に異常を通知する（Ｄ１２）。異常の通知は、例えばＳＭＳ送信制御部２１２によりＳＭＳを用いて行う。ＳＭＳ送信制御部２１２は通信部の一例である。仮に、これら２つのＥＣＵ１９が、新プログラムによる更新対象ＥＣＵでなかったとしても、センター装置３は、当該車両を非正規と判断し、ステップＤ７以降の処理を行わないものとする。

[0864] 一方、ＶＩＮ＝１００の車両Ａは「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ＝０００１」であり、「ＥＣＵ　ＩＤ＝ＡＤＳ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ａｄｓ＿００１」，「ＥＣＵ　ＩＤ＝ＢＲＫ」の「ＥＣＵ　ＳＷ　ＩＤ」は「ｂｒｋ＿００１」であり、構成情報ＤＢ２０８に登録されている構成情報と全て一致している。したがって、ステップＤ６では「ＹＥＳ」、つまり正規であり「ＯＫ」と判断し、ステップＤ７へ進む。ここで、構成情報確認部２１０は、車両Ｃの「ＥＣＵ　ＳＷ　ＩＤ」の組合せが構成情報ＤＢ２０８に存在するか否かで、正規か非正規かを判断しても良い。又、「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」に加え、「Ｓｙｓ　ＩＤ」を判断の材料に加えても良い。

[0865] 次に、更新有無確認部２１１がキャンペーン管理部３Ｄを介してキャンペーンＤＢ２１７にアクセスし、新プログラムによる更新の有無を確認する（Ｄ７）。更新の有無は、車両側システム４からアップロードされた「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」と、キャンペーンＤＢ２１７の「更新前Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」とを比較して判断する。例えば図２３に示すように、Ｖ

ＩＮ＝１００の車両Ａは更新前の「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ＝０００１」であるから、更新有りと判断される（ＹＥＳ）。この場合、更新有無確認部２１１は、対応するキャンペーンＩＤ「Ｃｐｎ＿００１」を上記車両Ａの車両側システム４に通知する（Ｄ８）。キャンペーン情報は更新通知情報に相当し、キャンペーンＤＢ２１７は、更新通知情報記憶部の一例である。

[0866] 尚、キャンペーンＤＢ２１７に更新前後の「Ｓｙｓ　ＩＤ」を持たせるようにすれば、「Ｓｙｓ　ＩＤ」により更新の有無を確認することも可能である。又、「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」に代えて、アップロードされた「ＥＣＵ　ＳＷ　ＩＤ」リストと、キャンペーンＤＢ２１７の「更新前ＥＣＵ　ＳＷ　ＩＤリスト」とを比較して、更新有無を判断しても良い。

[0867] 車両側システム４は、通知されたキャンペーンＩＤをキーとしてセンター装置３から前記ＩＤに対応するキャンペーンファイルを取得する（Ｄ９）。キャンペーンファイルには、キャンペーン内容を説明するテキスト文や、プログラム更新を実行する際の制約事項等が含まれている。制約事項とは、ダウンロードやインストールを実行する際の条件であり、例えば、バッテリ残量、配信パッケージのダウンロードに必要なＲＡＭの空き容量、車両の現在位置等である。車両側システム４は、キャンペーンファイルを解析し、車載ディスプレイ７を用いてキャンペーン内容等を表示する。ユーザは、キャンペーン内容に応じて車載ディスプレイ７に表示されるメッセージを参照し、ＥＣＵ１９のアプリプログラムを更新するか否かを決定する。車載ディスプレイ７を介してユーザの承諾操作を受付けると、ＣＧＷ１３は、ＤＣＭ１２を介して、センター装置３に更新を承諾する旨を通知する。すると、センター装置３は、前記キャンペーンＩＤに対応するパッケージＩＤの配信パッケージファイル及び完全性検証データを車両側システム４に送信する（Ｄ１０）。

[0868] 又、ステップＤ７において更新が無ければ（ＮＯ）、車両側システム４に「更新なし」を通知する（Ｄ１１）。例えば図２５６に示すように、ＶＩＮ＝２００の車両Ａは更新後の「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ＝０００２」で

あり、キャンペーンＤＢ２１７の「更新前Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」いずれにも合致しないから、更新無しと判断される。

[0869] 一方、ステップＤ２において「構成情報ダイジェスト」の照合結果が不一致であれば（ＮＯ）、センター装置３は、車両側システム４に「構成情報オール」の送信を要求する（Ｄ３）。この送信が「全データ送信要求の通知」に対応する。それに応じて、車両側システム４が「構成情報オール」を送信すると、センター装置３はそれを受信する（Ｄ４）。そして、センター装置３の個車情報管理部３Ｃは、個車情報ＤＢ２１３に登録されている当該車両の情報を更新する（Ｄ４）。それから、ステップＤ６に移行する。個車情報ＤＢ２１３は、車両側構成情報記憶部の一例である。尚、ＣＧＷ１３による「同期開始要求」の送信は、ＩＧスイッチ３７がオフされたタイミング等に行っても良い。

[0870] 以上のように第２実施形態によれば、車両側システム４は、複数のＥＣＵ１９より、各ＥＣＵ１９の構成に関する構成情報を受信すると、複数の構成情報のデータ値に基づいたハッシュ値を生成し、そのハッシュ値をセンター装置３に送信する。センター装置３は、個車情報ＤＢ２１３を有し、車両側システム４より送信されたハッシュ値と個車情報ＤＢ２１３に記憶されている車両の構成情報のハッシュ値とを比較する。そして、両者が不一致であれば、車両側システム４に「構成情報オール」の送信を要求する。すると、車両側システム４は、その送信を受けて、「構成情報オール」をセンター装置３に送信し、センター装置３は、「構成情報オール」を受信すると、そのデータ値に基づいて個車情報ＤＢ２１３に記憶されている構成情報を更新する。

[0871] このように構成すれば、車両側システム４は、当初はセンター装置３に構成情報のハッシュ値を送信し、センター装置３におけるハッシュ値の比較結果が不一致であった際にだけ、構成情報の全てのデータ値をセンター装置３に送信する。これにより、車両側システム４が送信するデータのサイズを縮減できるので、車両側システム４が多数の車両に搭載されたとしても、通信

量を総じて削減できる。特に、車両側システム４において、ＩＧオン時など予め定められたタイミングで構成情報をアップロードする場合、その通信が集中する時間帯が発生し得る。そのため、ハッシュ値を用いて送信データ量を削減することで、通信負荷を低減することができる。

[0872] 又、ＣＧＷ１３は、更新データの書換え対象となる全てのＥＣＵ１９より構成情報を受信し、それら全てのデータ値に基づいたハッシュ値を生成し、ＤＣＭ１２は、車両のイグニッションスイッチ３７がオン又はオフされたタイミングでハッシュ値を送信するので、車両の走行が開始される又は終了するタイミングで、センター装置３にハッシュ値を送信できる。そのため、センター装置３は、個車情報ＤＢ２１３の構成情報を、適切に車両と同期させることができる。

[0873] 又、車両側システム４は、複数のＥＣＵ１９より各ＥＣＵ１９の「ＥＣＵ　ＳＷ　ＩＤ」を受信すると、それらに「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」を組み合わせた構成情報リストをセンター装置３に送信する。センター装置３は、車両側システム４より送信された「ＥＣＵ　ＳＷ　ＩＤ」リストと、構成情報ＤＢ２０８に記憶されている対応する車両の正規のＥＣＵ　ＳＷ　ＩＤ」リストとを比較して、送信されたリストの組合せが非正規であると判断すると異常検知を車両側システム４及び管理装置２２０に送信する。

[0874] このように構成すれば、センター装置３は、車両の構成情報の組み合わせが、複数のＥＣＵ１９が協働できず車両の走行に支障を来すような状態にあることを異常として検知し、車両側システム４に通知できる。これにより、車両側システム４は、車両の走行を禁止する等の対応を行うことが可能になる。

[0875] センター装置３は、車両の構成情報の組合せが非正規の車両に対しては、更新有無の確認処理（Ｄ７）を実施しない。そのため、正規でない車両においてプログラム更新が実行されることを防ぐことができる。仮に、正規でないＥＣＵ１９が、新プログラムによる更新対象ＥＣＵではなかったとしても、センター装置３は、更新有無の確認処理（Ｄ７）を実施しない。車両側シ

ステム４において、プログラム更新を実行する際、更新対象でないＥＣＵ１９に対する制御も発生する。そのため、正規でないＥＣＵ１９を有する車両では、プログラム更新が正常に完了しない可能性があるため、センター装置３は、当該車両に対してプログラム更新が実行されないようにする。

[0876] 又、センター装置３は、新プログラムによる更新が発生したことを車両側に通知するために使用するキャンペーン情報が記憶されているキャンペーンＤＢ２１７を備え、正規と判断された車両に対しては、対応する車両のキャンペーン情報の有無を確認する。更新が有れば、そのキャンペーン情報を車両側システム４に送信する。これにより、ユーザに対してキャンペーン情報を提示し、アプリプログラムの更新を促すことができる。これら構成情報の同期、正規の構成情報か否かの判断、及び更新有無の確認を、車両からの構成情報アップロードを契機とし、センター装置３が一連の処理として実行することで、適切な車両に対してプログラムの更新を速やかに通知することができる。

[0877] 尚、第２実施形態を以下のように変形して実施しても良い。

・「同期開始要求」の送信は、センター装置３が車両側システム４に対して行うようにし、「同期開始要求」を受信するとＤＣＭ１２がＣＧＷ１３に対して「構成情報収集要求」を送信しても良い。例えば、「車両型式＝ａａａ」の構成情報ＤＢ２０８が更新された際に、センター装置３は、当該車両型式の車両に対し、「同期開始要求」を送信する。

・又、更新データの書換え対象となったＥＣＵ１９において、書換えが完了したタイミングでハッシュ値をセンター装置３に送信しても良い。すなわち、書換え対象となったＥＣＵ１９全てのプログラム更新が完了したタイミングにおいても、図２５５に示すステップＤ１～Ｄ１２のフローチャートを実行する。

・センター装置３は、双方のハッシュ値の比較結果が一致であった際に、車両側システム４に対して各ＥＣＵ１６の構成情報の組合せリストの送信を要求する。そして、前記組合せリストを受信すると、ステップＤ６～Ｄ１２の

処理を行っても良い。

・センター装置３は、双方のハッシュ値の比較結果が一致であった際にもキャンペーンＤＢ２１７を参照し、対応する車両のキャンペーン情報の有無を確認しても良い。

[0878] 車両側システム４からセンター装置３へのハッシュ値の送信を、図２５６に示すように行っても良い。図２５６は、ＣＧＷ１３の処理を示すフローチャートである。例えば、ＩＧスイッチ３７がオンされた際に、ＣＧＷ１３が各ＥＣＵ１９より構成情報を収集し（Ｄ２１）、収集した構成情報のデータ値についてハッシュ値を生成する（Ｄ２２）。そして、生成したハッシュ値をフラッシュメモリ２４ｄに記憶しているハッシュ値（前回生成値）と比較し、差異があるか否かを判断する（Ｄ２３）。差異があれば（ＹＥＳ）、今回生成したハッシュ値をフラッシュメモリ２４ｄに記憶し（Ｄ２４）、前記ハッシュ値をセンター装置３に送信する。ステップＤ２３において、双方のハッシュ値に差異が無ければ（ＮＯ）処理を終了する。尚、フラッシュメモリ２４ｄには、構成情報の初期値に対するハッシュ値は予め記憶されているものとする。これにより、車両側システム４が、センター装置３へ、構成情報をアップロードする回数を削減することができる。

[0879] （第３実施形態）

第３実施形態は、車両側システム４におけるアプリプログラムの更新率を向上させるため、センター装置３のキャンペーン管理部３Ｄが実行する機能に関する。図２５８に示すように、例えば車両側システム４において、ユーザがＣｏｎｆｉｇファイルによりＨＴＴＰポーリングのインターバルを３日程度に設定しておくことで、車両側システム４がセンター装置３に対して周期的にアプリプログラムの更新有無を確認する。これにより、キャンペーンＤＢ２１７に対応する車両；ＶＩＮのキャンペーン情報が設定された後に更新確認が行われた時点で、センター装置３より車両側システム４に「更新あり」が通知される。すなわち、第２実施形態にて説明したように、車両側システム４からＨＴＴＰを用いて構成情報がアップロードされることを契機と

して、センター装置３が更新確認を行うという処理が、３日経過後のＩＧオンのタイミングで実行されることとなる。

[0880] このように車両からの通知を契機として更新有無を行うよう構成すれば、センター装置３は、キャンペーン情報が設定された時点でそのキャンペーンの対象となる全ての車両にセンター装置３からキャンペーン情報を送信する必要がなくなる。しかしながら、ユーザが長期に渡り車両を使用しない場合、その間ずっとＨＴＴＰを用いた更新有無の確認が行われない。そのため、ユーザは新たなキャンペーンが発行されたことを知らず、アプリプログラムの更新が行われない車両が発生することも想定される。

[0881] そこで、図２５９に示すように、センター装置３のＳＭＳ送信制御部２１２は、定期的又は所定のタイミングで、個車情報ＤＢ２１３を参照して各車両のアクセスログをチェックする（Ｅ１）。そして、センター装置３へのアクセス，つまりアプリプログラムの更新確認のための構成情報の送信を所定期間行っていない車両があるか否かを判断する（Ｅ２）。所定期間は、キャンペーンＤＢ２１７に新たなキャンペーンが設定された日を起算日として、例えば７日間程度とする。つまり、ＳＭＳ送信制御部２１２は、個車情報ＤＢ２１３の「Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」がキャンペーンＤＢ２１７の「更新前Ｖｅｈｉｃｌｅ　ＳＷ　ＩＤ」に該当する車両を対象として、更新確認が７日間行われていない車両を特定する。尚、ＳＭＳ送信制御部２１２は、全ての車両を対象として、更新確認が所定期間行われていない車両を特定してもよい。

[0882] 尚、個車情報ＤＢ２１３には、車両が工場で生産された際にＯＥＭによって初期データが登録されるが、その後、例えば車両が販売されたことに伴うＯＥＭからの通知によって最初のアクセスログを入力する。このアクセスログは、実質的には以降のプログラムの更新を有効化するための通知に相当する。アクセスログが入力されていない車両は、ステップＥ２の判断対象外とする。

[0883] 更新確認を所定期間行っていない車両があれば（ＹＥＳ）、ＳＭＳ送信制

御部２１２は、その車両の特性を個車情報ＤＢ２１３の型式や装備情報等より判断する（Ｅ３）。ここでの特性として、ＳＭＳ送信制御部２１２は、電気自動車；ＳＭＳ（Short Message Service）受信可能なＥＶであるか、ＳＭＳ受信可能な従来のガソリンエンジン車，つまりコンベンショナルエンジン車；コンベ車か、ＳＭＳを受信困難な車両か否かを判断する。例えば、車両に搭載されるＤＣＭ１２が、ＳＭＳを受信する機能を有していない場合やＳＭＳを受信する契約をしていない場合には、ＳＭＳを受信困難な車両と判断する。

[0884] ＥＶであれば、その車両のＥＣＵ１９を起動させて構成情報送信シーケンスを開始させるＳＭＳを送信する（Ｅ５，図２６０参照）。ＤＣＭ１２がＳＭＳを受信し、ＳＭＳに記載されたコマンドを実行すると、ＩＧオン電源状態となり、起動したＣＧＷ１３は、ＤＣＭ１２を介してセンター装置３へ構成情報を送信する。その後、図２５５に示したステップＤ１～Ｄ１２のように、更新確認が行われ、配信パッケージのダウンロード等が実行される。ＥＶの場合、バッテリの容量が大きいため、駐車状態のままＩＧオン電源状態としてプログラムのダウンロードを行うことが十分可能であると考えられる。したがって、ＳＭＳを用いてＥＣＵ１９を起動させて自動的に更新確認及びダウンロード以降のシーケンスを開始させる。

[0885] 仮に、ＥＶ車のバッテリの残量が少ない場合は、車両側システム４において、図２５０に示す書換え諸元データを参照し、指定されたバッテリ残量を下回る状態の場合は、インストールを開始しないよう制御される。又は、センター装置３がステップＤ９にて送信するキャンペーンファイルに制約事項として記載されるバッテリ残量を参照し、指定されたバッテリ残量を下回る状態の場合は、車両側システム４において配信パッケージのダウンロードを開始しないよう制御される。

[0886] コンベ車において、ＤＣＭ１２が間欠的に起動している期間に当たりＳＭＳを受信可能な状態にある車両には、ＳＭＳ送信制御部２１２が車載ディスプレイ７に表示可能なＳＭＳを送信する（Ｅ４，図２６０参照）。例えば、

ＣＧＷ１３は、受信したＳＭＳに記載されたテキスト文を、次回ＩＧオンのタイミングで車載ディスプレイ７へ表示指示する。又、個車情報ＤＢ２１３にユーザの携帯端末６の情報が登録されている場合は、その携帯端末６にＳＭＳを送信しても良い。例えば、「キャンペーン情報があります。ＩＧ－ＯＮしてください。」といった文字メッセージを表示させる。個車情報ＤＢ２１３は、ユーザ情報記憶部の一例である。一方、ＳＭＳを受信困難な状態にある車両には何もせず、別途ユーザに郵送を行うなどして対応する（Ｅ６）。

[0887] 以上のように第３実施形態によれば、車両側システム４は、複数のＥＣＵ１９の構成情報をセンター装置３に送信し、個車情報ＤＢ２１３には、各車両より送信された構成情報が送信日と共に記憶される。又、キャンペーンＤＢ２１７には、キャンペーン情報として、キャンペーンＩＤ及びデータ更新の対象車両を識別可能な対象ＶＩＮリストが記憶される。そして、センター装置３は、個車構成ＤＢ２１３を参照し、対象車両に紐づく送信日から所定期間内に構成情報の送信がなければ、対象車両の車両側システム４にデータ更新を促すためのメッセージをＳＭＳにより送信する。

[0888] このように構成すれば、ユーザが車両に乗車する機会が無いため、構成情報がセンター装置３に送信されない状況が継続された場合でも、センター装置３が、個車情報ＤＢ２１３に記憶されている送信日から所定期間を経過すると、対象車両の車両側システム４にデータ更新を促すためのメッセージを送信する。したがって、ユーザは、そのメッセージを参照することでデータ更新が必要であることを認識できる。

[0889] そして、センター装置３は、個車情報ＤＢ２１３とキャンペーンＤＢ２１７とを参照することでプログラム更新の対象車両を決定する。すなわち、個車情報ＤＢ２１３には、各車両より構成情報が送信された日付が記憶されており、キャンペーンＤＢ２１７には、対象ＶＩＮリストが記憶されている。したがって、センター装置３は、各車両からの構成情報の送信日と対象ＶＩＮリストとによりプログラム更新の対象車両を決定できる。

[0890] 又、車両側システム４は、車両のイグニッションスイッチ３７がオンされたことを契機として、各ＥＣＵ１９よりそれぞれの構成情報を受信すると、構成情報をセンター装置３に送信する。したがって、ユーザが車両に乗車した際には、構成情報を確実にセンター装置３に送信できる。

[0891] そして、センター装置３は、対象車両が電気自動車であれば、その対象車両のＥＣＵを起動させる指令をメッセージに含ませて送信し、そのメッセージを受信した車両側システム４は、ＥＣＵ１９を起動させ、データ更新に関する処理を実行させる。すなわち、電気自動車はバッテリの容量に比較的余裕があるため、ユーザの操作を待つことなくＥＣＵ１９にデータ更新に関する処理を実行させることが可能である。したがって、データ更新を効率的に実行させることができる。

[0892] 又、センター装置３は、対象車両がコンベ車であれば、メッセージとして、少なくとも対象車両の車載ディスプレイ７に表示可能な文字情報を送信する。したがって、コンベ車のユーザは、車載ディスプレイ７に表示された文字情報を参照することで、データ更新が必要であることを認識できる。

[0893] 又、センター装置３は、個車情報ＤＢ２１３にユーザの携帯端末６の送信先が記憶されている際には、メッセージとして携帯端末６に表示可能な文字情報を送信する。これにより、ユーザは、車両に乗車する機会が無くても、携帯端末６に表示された文字情報を参照することで、データ更新が必要であることを認識できる。

[0894] 更に、ユーザが携帯端末６を介して、予めキャンペーンの送信日と送信先とをセンター装置３に送信すると、センター装置３は、その送信日及び送信先を個車情報ＤＢ２１３に記憶する。例えば、ユーザは、送信日としてキャンペーン発行の翌日を指定し、送信先として車載ディスプレイ７でなく携帯端末６を指定する。又、ユーザは、送信日として乗車しない所定時刻を指定し、送信先として車両を指定し、自動的にプログラム更新されることへの承諾操作を行う。これにより、センター装置３は、構成情報の送信の有無にかかわらず、キャンペーン情報を、前記送信日に前記送信先に対して送信する

。したがって、ユーザが車両に乗車する機会が暫くないことを予め把握している際には、ユーザが設定した送信日にキャンペーン情報を受信するように設定できる。

[0895] 尚、第３実施形態を以下のように変形して実施しても良い。

・ユーザ情報記憶部を、個車情報ＤＢ２１３と別個に設けても良い。

・キャンペーン情報の送信には、ＳＭＳ以外を用いても良い。

・センター装置３が、送信日を個車情報ＤＢ２１３に記憶する替わりに、例えば車両側からの送信が無かった日を記憶し、その日が７日間連続した際にデータ更新を促すメッセージを送信しても良い。

[0896] （第４実施形態）

第４実施形態は、ユーザがキャンペーン情報，メッセージの通知方法を指定する場合を示す。例えば、ユーザが１か月間程度乗車せず、ＩＧスイッチ３７をＯＮにする機会が無いことが予め確定している場合を想定する。図２６１に示すように、ユーザは、携帯端末６によりセンター装置３にキャンペーン発生時の通知先及び通知する日時の設定を送信する。例えば、１か月後にキャンペーン情報を携帯端末６に通知する、といった設定を行う。これにより、個車情報管理部３Ｃは、前記通知先及び通知日時の情報を個車情報ＤＢ２１３に記憶させ、設定に従いユーザに通知を行う。例えば、その１か月の間にキャンペーン（１，２）の２つが設定されたとすれば、ＳＭＳ送信制御部２１２が、１か月後にキャンペーン（１，２）の情報をユーザの携帯端末６に通知して、プログラム更新を促す。

[0897] 以上のように第４実施形態によれば、ユーザが携帯端末６を介して、キャンペーン情報の送信日と送信先とをセンター装置３に送信すると、センター装置３は、前記送信日及び送信先を個車情報ＤＢ２１３に記憶する。そして、センター装置３は、記憶した送信日に送信先に対してキャンペーン情報を送信する。これにより、ユーザが一定期間車両に乗車しないことが確定している場合に、センター装置３からの不要なキャンペーン情報の送信を停止できる。

[0898] （第５実施形態）

第５実施形態は、センター装置３が車両側システム４に更新プログラムのデータを送信する際に、車両側システム４がデータの完全性を検証するために用いる検証データを付与する機能について示す。図２６２及び図２６３に示すように、サプライヤは、パッケージ管理部３Ａを用い、ＥＣＵリプロデータＤＢ２０４に登録するデータを作成する。具体的には、パッケージ管理部３Ａは、更新データとして旧プログラムを新プログラムに書き換えるための新差分データを作成し（Ｙ１）、ＥＣＵ１９の新プログラムに対する完全性検証データであるハッシュ値、及び新差分データに対するハッシュ値を作成する（Ｙ２）。ここで、ＥＣＵが１面メモリの場合、ロールバックデータとして新プログラムを旧プログラムに書き換えるための旧差分データを作成し、ＥＣＵ１９の旧プログラムに対するハッシュ値、及び旧差分データに対するハッシュ値を作成しても良い。

[0899] パッケージ管理部３Ａは、各ハッシュ値に対して所定の鍵であるキー値を用いた暗号化を適用して認証子を生成する（Ｙ３）。そして、パッケージ管理部３Ａは、更新データ及び各認証子付き完全性検証データを送信し、ＥＣＵリプロデータＤＢ２０４に記憶する（Ｙ４）。パッケージ管理部３Ａは前述したように、パッケージを生成し、パッケージに対する完全性検証データを生成し、車両側システム４へ送信する（Ｙ５）。

[0900] マスタ装置（ＯＴＡマスタ）１１は、パッケージに対する完全性検証データを演算し、その演算値と受信したパッケージの完全性検証データとを比較し、パッケージの完全性検証を行う（Ｙ６）。パッケージの完全性検証に成功すると、マスタ装置１１は、ＥＣＵの更新データ及び完全性検証データを書換え対象ＥＣＵ（ターゲットＥＣＵ）１９へ送信する（Ｙ７）。

[0901] 書換え対象ＥＣＵ１９は、更新データに対する完全性検証データを演算し、その演算値と受信した更新データの完全性検証データとを比較し、更新データの完全性検証を行う（Ｙ８）。更新データの完全性検証に成功すると、書換え対象ＥＣＵ１９は、更新データである差分データを復元し、フラッシ

ュメモリ２８ｄへの書込みを行う（Ｙ９）。書込みが完了すると、書換え対象ＥＣＵ１９は、フラッシュメモリ２８ｄへ書込まれたデータに対する完全性検証データを演算し、その演算値と受信した新プログラムの完全性検証データとを比較し、フラッシュメモリ２８ｄの完全性検証を行う（Ｙ１０）。書換え対象ＥＣＵ１９は、その検証結果をマスタ装置１１へ送信し（Ｙ１１）、マスタ装置１１は、受信したその検証結果をインストール結果通知としてセンター装置３へ送信する（Ｙ１２）。

[0902] 例えば図２４３に示したように、パッケージ管理部３Ａは、最新の「ＥＣＵ　ＳＷ　ＩＤ」について、以下の完全性検証データを生成する。ＥＣＵのメモリ構成が２面メモリ又はサスペンドの場合、以下（３）（４）は省略可能である。

（１）ＥＣＵの新プログラムに対する完全性検証データであるハッシュ値を生成する。この処理を行う機能部分が、第１検証値生成部（ステップＡ１）の一例である。

（２）ＥＣＵの旧プログラムをベースに新プログラムへ更新するための差分データである更新データ，その更新データの完全性検証データであるハッシュ値を生成する。この処理を行う機能部分が、第２検証値生成部（ステップＡ４）の一例である。

（３）ＥＣＵの旧プログラムに対する完全性検証データであるハッシュ値を生成する。この処理を行う機能部分が、第４検証値生成部（ステップＡ５）の一例である。

（４）ＥＣＵの新プログラムをベースに旧プログラムへ更新するための差分データである更新データ，その更新データの完全性検証データであるハッシュ値を生成する。この処理を行う機能部分が、第５検証値生成部（ステップＡ７）の一例である。

[0903] 尚、「プログラム」にはプログラム中で使用する定数データ等も含む。「ＥＣＵ　ＳＷ　ＩＤ＝ａｄｓ＿００２」であれば、更新データ「Ａｄｓｆｉｌｅ００１－００２」に対して、そのハッシュ値ｘ１を生成する。ハッシュ

関数には、前述したように例えばＳＨＡ－２５６を用いる。ハッシュ値は検証値に相当する。ここで、パッケージ管理部３Ａは、ハッシュ値に対して所定の鍵であるキー値を用いた暗号化を適用して認証子を生成することで認証子付き完全性検証データを生成するよう構成しても良い。

[0904] 次に、サプライヤは、完全性検証データに対して所定の鍵であるキー値を用いた暗号化を適用して認証子を生成することで認証子付き完全性検証データを生成し、更新データと認証子付き完全性検証データとを対応付けてＯＥＭに提供する。つまり、パッケージ管理部３Ａにより、各プログラムとそれに対する認証子付き完全性検証データがＥＣＵリプロデータＤＢ２０４へ登録されることをもって、ＯＥＭに提供となる。ＯＥＭの指示により、パッケージ管理部３Ａは、ＥＣＵリプロデータＤＢ２０４等を用いて、前述のように書換え諸元データを生成し、配信パッケージを生成し、パッケージＤＢ２０６に登録する。センター装置３は、車両側システム４から更新データのダウンロード要求が発生すると、そのダウンロード要求に従って更新データと認証子付き完全性検証データとを含む配信パッケージを車両側システム４に配信する。尚、特許請求の範囲における「完全性検証データ」は、ハッシュ値のみのものと、鍵による暗号化を含む認証子付き完全性検証データの何れをも含む。

[0905] 車両側システム４のマスタ装置１１は、配信パッケージを受信すると、配信パッケージに付与された完全性検証データ（第３検証値）を用いて、配信パッケージの妥当性を検証する。具体的には、配信パッケージを用いて演算した完全性検証データと、受信した完全性検証データとを比較し、合致すれば正常と判断する。検証の結果、正常と確認された場合、マスタ装置１１は、配信パッケージをＥＣＵ毎のデータにアンパッケージングする（図２３９参照）。そして、マスタ装置１１は、更新データ及び認証子付き完全性検証データを書込み先のＥＣＵ１９に転送する。

[0906] ＥＣＵ１９は、認証子付き完全性検証データ（第２検証値）を用いて、更新データの妥当性を検証する。具体的には、受信した更新データを用いて演

算した完全性検証データと、受信した完全性検証データとを比較し、合致すれば正常と判断する。検証の結果、正常と確認された場合、ＥＣＵ１９のＣＰＵ２８ａはフラッシュメモリ２８ｄへの書込み処理を行う。書込み処理が完了すると、ＥＣＵ１９は、認証子付き完全性検証データ（第１検証値）を用いて、フラッシュメモリ２８ｄに書込んだデータを読み出して、その妥当性を検証する。具体的には、読み出したデータを用いて演算した完全性検証データと、受信した完全性検証データとを比較し、合致すれば正常と判断する。尚、ここでの完全性検証データは、ＥＣＵ１９の起動時にも使用するため、フラッシュメモリ２８ｄの所定領域へ記憶しておく。ＥＣＵ１９は、これらの処理が完了すると、検証結果を含め、書込み応答をマスタ装置１１に送信する。マスタ装置１１は、センター装置３にインストール結果を通知する。尚、図中の「ターゲットＥＣＵ」は「対象ＥＣＵ」と同義であり、「ＯＴＡマスタ」は「ＤＣＭ」と同義である。ＣＰＵ２８ａは書き込み処理部の一例である。

[0907] ここで、インストールの途中に、プログラム更新のキャンセルが発生した場合、ＥＣＵ１９はロールバック処理を行うこととなる。ＥＣＵ１９は、更新データを書込むとともに、認証子付き完全性検証データ（第５検証値）を用いて、ロールバック用差分データの妥当性を検証する。具体的には、ロールバック用差分データを用いて演算した完全性検証データと、受信した完全性検証データとを比較し、合致すれば正常と判断する。検証の結果、正常と確認された場合、ＥＣＵ１９は、更新データの書込みを完了した後、ロールバック用差分データを用いた書込みを開始する。そして、書込みを完了した後、ＥＣＵ１９は、認証子付き完全性検証データ（第４検証値）を用いて、フラッシュメモリ２８ｄに書込んだデータを読み出して、その妥当性を検証する。尚、受信した差分データ（更新データ、ロールバック用差分データ）の完全性検証は、ＥＣＵ１９でなく、マスタ装置１１が行う構成としても良い。

[0908] 図２６４に示すように、その後、上記車両のＩＧスイッチ３７がＯＮされ

ると、それを契機としてＥＣＵ１９は、起動時のデータ検証を行う。ＥＣＵ１９は、認証子付き完全性検証データ（第１検証値又は第４検証値）を用いて起動するプログラム等の完全性を検証する。先ず、フラッシュメモリ２８ｄにおいて、更新されたプログラムや定数データが書き込まれている評価対象領域のデータ値に対してハッシュ関数を適用し、ハッシュ値を取得する。次に、認証子付き完全性検証データを復号し、復号結果に含まれているハッシュ値（期待値）と取得したハッシュ値（演算値）とを照合し、フラッシュメモリ２８ｄに書き込まれたプログラム等が改竄されているか否かを判断する。双方のハッシュ値が一致して「ＯＫ」であれば、ＥＣＵ１９は通常通り起動処理を行う。各ＥＣＵ１９について同様の処理が行われ、全ての評価対象ＥＣＵ１９の結果が「ＯＫ」であれば、処理を終了する。

[0909] 一方、何れかのＥＣＵ１９について検証の結果が異常；「ＮＧ」であれば、ＥＣＵ１９は、処理のログを保存してマスタ装置１１にエラーを通知する。マスタ装置１１は、同様にログを保存してセンター装置３にエラーを通知する。センター装置３は、同様にログを保存してＯＥＭ等の管理装置２２０にエラーを通知する。管理装置２２０への通知は、例えばＳＭＳ送信制御部２１２によりＳＭＳを用いて行ったり、インターネット回線を介した電子メールの送信等により行う。

[0910] 上述した実施例では、車両側システム４において、完全性の検証を行う構成とした。図２６５では、完全性の検証（期待値との比較）をセンター装置３にて行う場合について説明する。図２６５は、例えばＩＧオン等のタイミングにおいて、ＥＣＵ１９は、マスタ装置１１に更新したアプリプログラムのバージョン情報を送信する際に、バージョン情報と共に上記と同様に認証子付き完全性検証データを生成して送信する（Ｘ１）。ＥＣＵ１９は、フラッシュメモリ２８ｄのデータに対する完全性検証データを演算し、その演算値をマスタ装置１１へ送信する。マスタ装置１１は、構成情報として認証子付き完全性検証データを含めてセンター装置３に送信する（Ｘ２）。

[0911] センター装置３は、ＥＣＵリプロデータＤＢ２０４にアクセスし、ターゲ

ットＥＣＵ１９の「ＥＣＵ　ＳＷ　ＩＤ」に合致する認証子付き完全性検証データを取得し（Ｘ３，Ｘ４）、車両側よりアップロードされた完全性検証データと照合する（Ｘ５）。具体的には、ＥＣＵリプロデータＤＢより、「ＥＣＵ　ＳＷ　ＩＤ」に対応する新プログラムの完全性検証データを取得し、照合する。照合の結果が不一致；ＮＧであれば（Ｘ６；ＮＧ）、ＯＥＭの管理装置２２０に対して異常を通知する（Ｘ７）。この処理部分の機能が異常報知部に相当する。

[0912] センター装置３は、照合結果を、マスタ装置１１へ送信し（Ｘ８）、マスタ装置１１は受信した照合結果を書換え対象ＥＣＵ１９へ送信する（Ｘ９）。書換え対象ＥＣＵ１９は、照合結果がＯＫの場合、通常通りアプリプログラムを動作させ、照合結果がＮＧの場合、アプリプログラムを動作させない。尚、本実施例において、パッケージ管理部３Ａは、新プログラムの完全性検証データ生成（ステップＡ１）や旧ＥＣＵプログラムの完全性検証データ生成（ステップＡ５）を省略可能となる。

[0913] 尚、上記では、ＥＣＵ１９は、更新データの書き込みを行った後、車両のＩＧスイッチ３７がＯＮされたタイミングで更新データの完全性を検証するが、それに替えて、更新データの書き込みを行った直後に完全性を検証しても良い。

[0914] 又、上記の実施形態では、更新データのみについて認証子付き完全性検証データを付与しているが、これを以下のように実施しても良い。

・ＥＣＵリプロデータＤＢ２０４より、新プログラム及び対応する更新データを取得する（データ取得手順；ステップＡ１）。

・第１検証値生成部は、新プログラムについて第１ハッシュ値を生成する（第１検証値生成手順；ステップＡ２）。

・第２検証値生成部は、更新データについて第２ハッシュ値を生成する（第２検証値生成手順；ステップＡ４）。パッケージ生成部２０２は、配信パッケージに、更新データ、諸元データ並びに第１及び第２ハッシュ値を含ませる（配信パッケージ生成手順）。更新データは新差分データに対応する。

・第３検証値生成部は、配信パッケージについて第３ハッシュ値を生成する（第３検証値生成手順；ステップＣ４）。

・パッケージ配信部２０３は、配信パッケージ及び第３ハッシュ値を車両側システム４に送信する（送信手順）。

尚、認証子については、配信パッケージ及び第３ハッシュ値についてのみ付与しても良いし、各ハッシュ値を生成する段階毎に付与しても良い。パッケージ配信部２０３は送信部に相当する。

[0915] この場合、車両側システム４では、

・受信処理部であるＤＣＭ１２が、配信パッケージ及び第３ハッシュ値を受信する。

・第３検証処理部は、配信パッケージデータより生成したハッシュ値と受信した第３ハッシュ値とを比較して、配信パッケージデータの完全性を検証する。

・第２検証処理部は、更新データより生成したハッシュ値と受信した第２ハッシュ値とを比較して、更新データの完全性を検証する。

・書込み処理部の一例であるＣＰＵ２８ａは、更新データをフラッシュメモリ２８ｄに書き込む。

・第１検証処理部は、更新データを書込むことで新プログラムとなったフラッシュメモリ２８ｄ内のデータ値についてハッシュ値を生成し、受信した第１ハッシュ値と比較して、新プログラムの完全性を検証する。

更新データの検証結果がＮＧであれば、フラッシュメモリ２８ｄへの書き込みは中止する。又、フラッシュメモリ２８ｄに書き込んだ新プログラムの検証結果がＮＧであれば、新プログラムを無効とし、必要に応じてロールバック処理を行う。尚、第１～第３検証処理部は、ＣＰＵ２８ａにより実現されても良い。又、第１～第３検証処理部の何れかの検証結果がＮＧであれば、送信処理部としてのＤＣＭ１２は、センター装置３に異常を通知する。

[0916] 更に、上記に加えて、図２４３に示したように、更新データを書き加える前の旧プログラムの状態に戻すためのロールバックデータが存在する際には

、以下のように実施しても良い。

・第４検証値生成部は、旧プログラムについて第４ハッシュ値を生成する（第４検証値生成手順；ステップＡ５）。

・第５検証値生成部は、新プログラムを旧プログラムに戻すためのロールバックデータについて第５ハッシュ値を生成する（第５検証値生成手順；ステップＡ７）。ロールバックデータは、ロールバック用差分データを示しており、旧差分データに対応する。

・パッケージ生成部２０２は、配信パッケージに、更新データ、ロールバック用差分データ、書換え諸元データ並びに第１及、第２、第３及び第４ハッシュ値を含ませる（配信パッケージ生成手順）。

[0917] この場合、車両側システム４において、フラッシュメモリ２８ｄに更新データを書換えている間に、例えばユーザにより書換え中止が指示されると書き換えキャンセルとなり、旧プログラムへの復旧，つまりロールバックが行われる。これは、ＥＣＵ１９のメモリ構成が１面メモリの場合のみである。

・第２検証処理部が、配信パッケージに含まれるロールバックデータに対するハッシュ値を算出し、算出したハッシュ値と第５ハッシュ値とを比較してロールバックデータの完全性を検証する。

・ＣＰＵ２８ａは、ロールバックデータを用いてフラッシュメモリ２８ｄへの書込みを行う。

・第１検証処理部が、フラッシュメモリ２８ｄへの書込みにより復旧された旧プログラムについてハッシュ値を算出し、算出したハッシュ値と第４ハッシュ値とを比較して旧プログラムの完全性を検証する。

[0918] 以上のように第５実施形態によれば、ＥＣＵリプロデータＤＢ２０４には、書換え対象であるターゲットＥＣＵ１９の新プログラム、旧プログラム、及び旧プログラムから新プログラムに更新するための新差分データである更新データが記憶される。第１検証値生成部は、新プログラムを用いて第１ハッシュ値を生成し、第２検証値生成部は、更新データを用いて第２ハッシュ値を生成する。パッケージ生成部２０２は、複数のターゲットＥＣＵ１９に

対する更新データと第１及び第２検証値並びに諸元データを含むパッケージを生成する。第３検証値生成部は、配信パッケージを用いて第３ハッシュ値を生成し、パッケージ配信部２０３は、配信パッケージを第３ハッシュ値と共に車両側システム４に送信する。

[0919] 車両側システム４は、配信パッケージ及び第３ハッシュ値を受信すると、第３検証処理部が、配信パッケージに対するハッシュ値を算出し、第３ハッシュ値と比較して配信パッケージの完全性を検証する。第２検証処理部は、配信パッケージに含まれるターゲットＥＣＵ１９に対応する更新データについてハッシュ値を算出し、配信パッケージに含まれる第２ハッシュ値とを比較して更新データの完全性を検証する。

[0920] ＣＰＵ２８ａは、更新データをフラッシュメモリ２８ｄに書込み、第１検証処理部は、フラッシュメモリ２８ｄの更新された新プログラムのデータに対するハッシュ値を算出し、第１ハッシュ値とを比較して、新プログラムのデータの完全性を検証する。このように、各ハッシュ値を用いて複数段階で各データ値の完全性を検証できる。そして、新プログラムについては完全性を３重に検証できることになり、車両側システム４が不完全な新プログラムを書込むこと、不正な新プログラムで動作することを回避させることができる。

[0921] 又、ＥＣＵリプロデータＤＢ２０４にロールバックデータが存在する際に、第４検証値生成部が旧プログラムについて第４ハッシュ値を生成し、第５検証値生成部がロールバックデータについて第５ハッシュ値を生成する。パッケージ生成部２０２は、配信パッケージに、更新データ、第１及び第２ハッシュ値、ロールバックデータ、第４及び第５ハッシュ値を含ませる。

[0922] そして、車両側システム４においてロールバックが行われる際には、第２検証処理部が、配信パッケージに含まれるロールバックデータに対するハッシュ値を算出し、第５ハッシュ値と比較してロールバックデータの完全性を検証する。ＣＰＵ２８ａは、ロールバックデータを用いてフラッシュメモリ２８ｄへの書込みを行う。第１検証処理部は、フラッシュメモリ２８ｄへの

書込みにより復旧された旧プログラムについてハッシュ値を算出し、第４ハッシュ値と比較して旧プログラムの完全性を検証する。これにより、書き戻された旧プログラムについても完全性を検証できる。上記において、第１～第５検証値生成部は、センター装置３のパッケージ管理部３Ａ内の機能ブロックである。第１、第２、第４及び第５検証処理部は、車両側システム４のターゲットＥＣＵ１９内の機能ブロックである。又、第３検証処理部は、車両側システム４のマスタ装置１１（ＯＴＡマスタ１１）内の機能ブロックである。

[0923] （第１実施形態の変形その１）

図２６６及び図２６７に示すように、１つのキャンペーン「ｃｐｎ＿００１」について複数のパッケージ「ｐｋｇ＿００１＿１」及び「ｐｋｇ＿００１＿２」を対応させても良い。又複数のパッケージを複数のグループとしても良い。前述の実施例では、１つのパッケージの中に、複数のグループを含む構成とした。本変形例では、１つのグループで１つのパッケージを生成し、１つのキャンペーンに対して複数のパッケージを配信する。例えば、パッケージ「ｐｋｇ＿００１＿１」には、グループ１に所属するＥＣＵである「ＡＤＳ」及び「ＢＲＫ」が含まれ、パッケージ「ｐｋｇ＿００１＿２」には、グループ２に所属するＥＣＵである「ＥＰＳ」が含まれる。

[0924] この場合、図２６８及び図２６９に示すように、諸元データ及び配信パッケージを、グループ毎に個別に生成する。図２６８において、諸元データ生成部２０１は、グループ１の諸元データとして、例えば「ＡＤＳ」及び「ＢＲＫ」のＥＣＵ情報を記載した第１諸元データを生成する。諸元データ生成部２０１は、グループ２の諸元データとして、例えば「ＥＰＳ」のＥＣＵ情報を記載した第２諸元データを生成する。そして、図２６９において、パッケージ生成部２０２は、例えばグループ１に所属する「ＡＤＳ」及び「ＢＲＫ」の更新データ等をＥＣＵ順序に従って統合したリプログデータを生成し、第１諸元データと統合してパッケージファイル「ｐｋｇ００１＿１．ｄａｔ」を生成する。パッケージ生成部２０２は、グループ２に所属する「ＥＰ

Ｓ」の更新データ等を用いてリプログデータを生成し、第２諸元データと統合してパッケージファイル「ｐｋｇ００１＿２．ｄａｔ」を生成する。

[0925] （第１実施形態の変形その２）

図２７０は、諸元データ生成部２０１及びパッケージ生成部２０２の機能を統合して１つのパッケージ生成ツール２２１を構成した場合の処理内容を示す。以下、各処理について改めて説明する。

[0926] 諸元データ生成処理では、諸元データ情報として作業者により入力された値を、ビット数や並び順が予め定められたデータ構造で出力し、諸元データ生成する。諸元データ情報としては、例えば図２５０に例示した値であり、ＥＣＵ（ＩＤ１），ＥＣＵ（ＩＤ２），ＥＣＵ（ＩＤ３）といったＥＣＵ単位の情報に加え、車両単位又はシステム（グループ）単位の情報を入力する。車両単位の情報とは、例えば図２５０に示す書換え環境情報であり、システム単位の情報とは、例えば図２５０に示すグループ情報やＥＣＵ順序の情報である。車両単位、システム単位の入力情報は、それぞれを別ファイルとしても良い。諸元データ生成処理に、更新データのファイルサイズ等、一部の値を自動的に計算して諸元データに反映させる機能を持たせても良い。

パッケージ生成処理では、生成された諸元データや各ＥＣＵの更新データ，各ＥＣＵの完全性検証データとして入力された値やファイルを、ビット数や並び順が予め定められたデータ構造で出力し配信パッケージのファイルを生成する。各ＥＣＵの更新データ及び完全性検証データは、グループの若い順、ＥＣＵ順序の若い順に並べる。ここで、更新データ（新差分データ）に加え、ロールバック用データ（旧差分データ）も入力に加えて良い。完全性検証データとしては、「ＥＣＵプログラム（新）の完全性検証データ」「更新データの完全性検証データ」が入力される。ロールバックデータも加える場合は、「ECU旧プログラムの完全性検証データ」「旧差分データの完全性検証データ」も入力に加える。

完全性検証データ生成処理では、図２５２のステップＣ４について述べたように、生成されたパッケージファイルについて完全性検証データを生成す

る。

生成されたパッケージファイルやパッケージファイルについて生成された完全性検証データは、作業者がパッケージＤＢ２０６に登録する。

[0927] センター装置３が実行する機能は、ハードウェアで実現しても良いし、ソフトウェアで実現しても良い。又、ハードウェアとソフトウェアとの協働により実現しても良い。

書換えるデータは、アプリプログラムだけでなく、地図等のデータや、制御パラメータ等のデータであっても良い。

構成情報の内容は例示したものに限ることなく、個別の設計に応じて適宜選択すれば良い。

諸元データの内容についても、例示したものに限ることはない。

キャンペーン情報，配信諸元データについては、配信パッケージに含めて車両側に送信しても良く、配信パッケージとは別個に車両側に送信しても良い。

第５実施形態において、予め配信パッケージ及び第３検証値をパッケージ記憶部に記憶しておき、パッケージ送信部２１３は、車載側システム４からの要求に応じて、当該要求に紐づく配信パッケージ及び第３検証値を車載側システム４に送信しても良い。

[0928] 本実施形態によれば、前述した（１）配信パッケージの送信判定処理、（２）配信パッケージのダウンロード判定処理を行うことで以下に示す作用効果を得ることができる。センター装置３において、車両に対する更新データが有ると判定し、車両状態が配信パッケージを用いたプログラム等の更新に適する状態であると判定すると、キャンペーン情報をマスタ装置１１に送信し、マスタ装置１１において、車両状態が配信パッケージをダウンロード可能な状態であると判定すると、センター装置３から配信パッケージをダウンロードするようにした。センター装置３において、車両に対する更新データの有無を判定し、車両状態が更新に適する状態であるか否かを判定し、マスタ装置１１において、車両状態が配信パッケージをダウンロード可能な状態

であるか否かを判定し、センター装置３による判定とマスタ装置１１による判定とを組み合わせて行うことで、マスタ装置１１がセンター装置３からの配信パッケージのダウンロードを適切に開始することができる。

[0929] センター装置３において、ライセンス契約、車両位置、車両のアラーム機能、ＥＣＵ１９の故障情報に基づいて車両状態が配信パッケージを用いたプログラム等の更新に適する状態であるか否かを判定するようにした。ライセンス契約が成立しており、車両位置がユーザにより予め登録された所定範囲内であり、車両のアラーム機能の設定が有効化されており、ＥＣＵ１９の故障情報が発生していない場合に、キャンペーン情報をマスタ装置１１に送信することができる。即ち、ライセンス契約が未成立であったり、車両位置が自宅から遠く離れた位置等の所定範囲外であったり、車両のアラーム機能の設定が無効化されていたり、ＥＣＵ１９の故障情報が発生していたりする場合に、キャンペーン情報をマスタ装置１１に送信する事態を回避することができる。

[0930] マスタ装置１１において、電波環境、車両バッテリ４０のバッテリ残量、ＤＣＭ１２のメモリの空き容量に基づいて車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定するようにした。電波環境が良好であり、車両バッテリ４０のバッテリ残量が所定容量以上であり、ＤＣＭ１２のメモリ空き容量が所定容量以上である場合に、センター装置３から配信パッケージをダウンロードすることができる。即ち、電波環境が良好でなかったり、車両バッテリ４０のバッテリ残量が所定容量未満であったり、ＤＣＭ１２のメモリ空き容量が所定容量未満であったりする場合に、センター装置３から配信パッケージをダウンロードする事態を回避することができる。

[0931] 本開示は、実施例に準拠して記述されたが、当該実施例や構造に限定されるものではないと理解される。本開示は、様々な変形例や均等範囲内の変形をも包含する。加えて、様々な組み合わせや形態、更には、それらに一要素のみ、それ以上、或いはそれ以下を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。

[0932] 本開示に記載の制御部及びその手法は、コンピュータプログラムにより具体化された一つ乃至は複数の機能を実行するようにプログラムされたプロセッサ及びメモリを構成することにより提供された専用コンピュータにより実現されても良い。或いは、本開示に記載の制御部及びその手法は、一つ以上の専用ハードウェア論理回路によりプロセッサを構成することにより提供された専用コンピュータにより実現されても良い。若しくは、本開示に記載の制御部及びその手法は、一つ乃至は複数の機能を実行するようにプログラムされたプロセッサ及びメモリと一つ以上のハードウェア論理回路により構成されたプロセッサとの組み合わせにより構成された一つ以上の専用コンピュータにより実現されても良い。又、コンピュータプログラムは、コンピュータにより実行されるインストラクションとして、コンピュータ読み取り可能な非遷移有形記録媒体に記憶されていても良い。

請求の範囲

[請求項1] 更新データを含む配信パッケージを車両用マスタ装置に配信するセンター装置（３）と、センター装置から配信パッケージをダウンロードする車両用マスタ装置（１１）と、を備える車両用電子制御システム（１）において、

前記センター装置は、

車両側から電子制御装置のソフトウェア情報を取得するソフトウェア情報取得部（５２ａ）と、

前記ソフトウェア情報取得部により取得されたソフトウェア情報に基づいて、車両に対する更新データの有無を判定する更新有無判定部（５２ｂ）と、

車両に対する更新データが有ると前記更新有無判定部により判定された場合に、車両状態が更新に適する状態であるか否かを判定する更新適否判定部（５２ｃ）と、

車両状態が更新に適する状態であると前記更新適否判定部により判定された場合に、更新に関するキャンペーン情報を車両用マスタ装置に送信するキャンペーン情報送信部（５２ｄ）と、を備え、

前記車両用マスタ装置は、

センター装置からキャンペーン情報を受信するキャンペーン情報受信部（６７ａ）と、

キャンペーン情報が前記キャンペーン情報受信部により受信された場合に、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定するダウンロード可能判定部（６７ｂ）と、

車両状態が配信パッケージをダウンロード可能な状態であると前記ダウンロード可能判定部により判定された場合に、センター装置から配信パッケージをダウンロードするダウンロード実行部（６７ｃ）と、を備える車両用電子制御システム。

[請求項2] 前記更新適否判定部は、ライセンス契約、車両位置、車両のアラー

ム機能、電子制御装置の故障情報のうち少なくとも何れか基づいて、車両状態が更新に適する状態であるか否かを判定する請求項１に記載した車両用電子制御システム。

[請求項3] 前記更新適否判定部は、ユーザの意に反する更新となり得る車両状態である場合、又は、更新データの書込みに失敗する可能性のある車両状態である場合に、車両状態が更新に適する状態でないと判定する請求項１又は２に記載した車両用電子制御システム。

[請求項4] 前記センター装置は、前記更新適否判定部により更新に適さないと判断された場合に、更新に適さない旨及びその理由をマスタ装置に送信する請求項１から３の何れか一項に記載した車両用電子制御システム。

[請求項5] 前記ダウンロード可能判定部は、電波環境、車両バッテリのバッテリ残量、前記車両用マスタ装置のメモリの空き容量のうち少なくとも何れか基づいて、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定する請求項１から４の何れか一項に記載した車両用電子制御システム。

[請求項6] 前記ダウンロード可能判定部は、ダウンロードを正常に完了することができない可能性のある車両状態である場合に、車両状態が配信パッケージをダウンロード可能な状態でないと判定する請求項１から５の何れか一項に記載した車両用電子制御システム。

[請求項7] 更新データを含む配信パッケージを車両用マスタ装置に配信するセンター装置（３）と、センター装置から更新データを含む配信パッケージをダウンロードする車両用マスタ装置（１１）と、を備える車両用電子制御システム（１）において、

車両側から電子制御装置のソフトウェア情報を取得するソフトウェア情報取得手順と、

前記ソフトウェア情報取得手順により取得したソフトウェア情報に基づいて、車両に対する更新データの有無を判定する更新有無判定手

順と、

車両に対する更新データが有ると前記更新有無判定手順により判定した場合に、車両状態が更新に適する状態であるか否かを判定する更新適否判定手順と、

車両状態が更新に適する状態であると前記更新適否判定手順により判定した場合に、更新に関するキャンペーン情報を車両用マスタ装置に送信するキャンペーン情報送信手順と、

センター装置からキャンペーン情報を受信するキャンペーン情報受信手順と、

キャンペーン情報を前記キャンペーン情報受信手順により受信した場合に、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定するダウンロード可能判定手順と、

車両状態が配信パッケージをダウンロード可能な状態であると前記ダウンロード可能判定手順により判定した場合に、センター装置から配信パッケージをダウンロードするダウンロード実行手順と、を行う配信パッケージのダウンロード判定方法。

[請求項8] 更新データを含む配信パッケージを車両用マスタ装置に配信するセンター装置（３）と、センター装置から更新データを含む配信パッケージをダウンロードする車両用マスタ装置（１１）と、を備える車両用電子制御システム（１）に、

車両側から電子制御装置のソフトウェア情報を取得するソフトウェア情報取得手順と、

前記ソフトウェア情報取得手順により取得したソフトウェア情報に基づいて、車両に対する更新データの有無を判定する更新有無判定手順と、

車両に対する更新データが有ると前記更新有無判定手順により判定した場合に、車両状態が更新に適する状態であるか否かを判定する更新適否判定手順と、

車両状態が更新に適する状態であると前記更新適否判定手順により判定した場合に、更新に関するキャンペーン情報を車両用マスタ装置に送信するキャンペーン情報送信手順と、

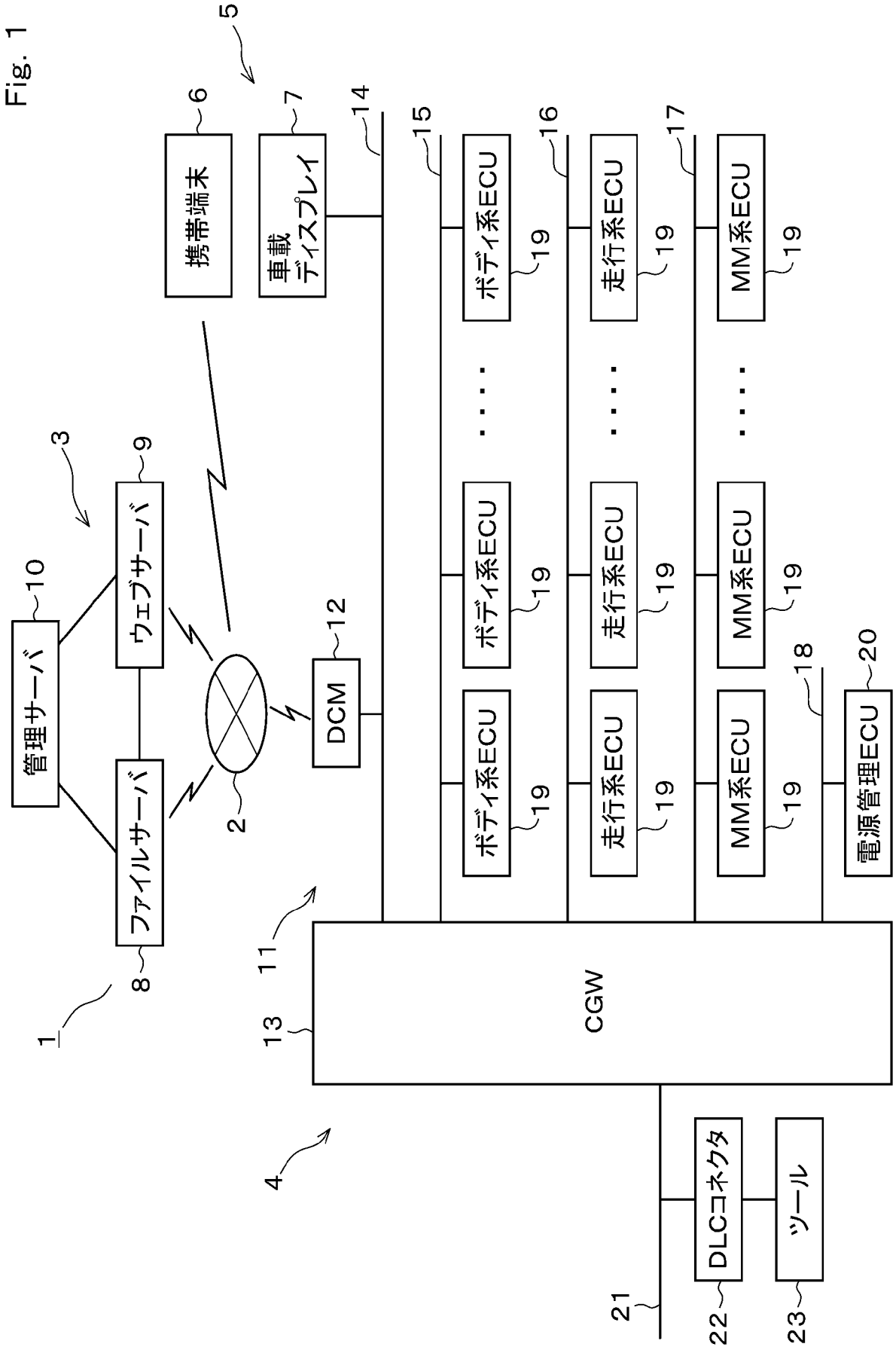
センター装置からキャンペーン情報を受信するキャンペーン情報受信手順と、

キャンペーン情報を前記キャンペーン情報受信手順により受信した場合に、車両状態が配信パッケージをダウンロード可能な状態であるか否かを判定するダウンロード可能判定手順と、

車両状態が配信パッケージをダウンロード可能な状態であると前記ダウンロード可能判定手順により判定した場合に、センター装置から配信パッケージをダウンロードするダウンロード実行手順と、を実行させる配信パッケージのダウンロード判定プログラム。

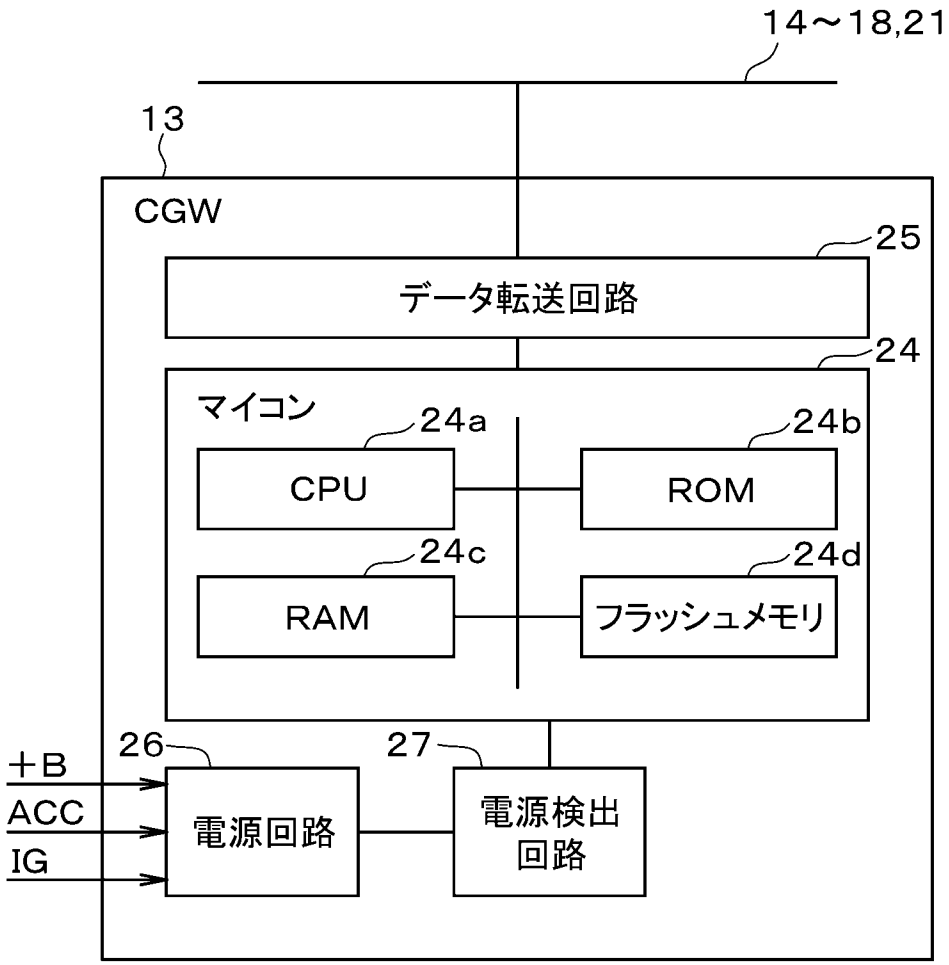
[図1]

Fig. 1


1
2
3
4
5
6
携帯端末
7
車載ディスプレイ
8
ファイルサーバ
9
ウェブサーバ
10
管理サーバ
11
12
DCM
13
CGW
14
15
16
17
18
19
ボディ系ECU
走行系ECU
MM系ECU
20
電源管理ECU
21
22
DLCコネクタ
23
ツール

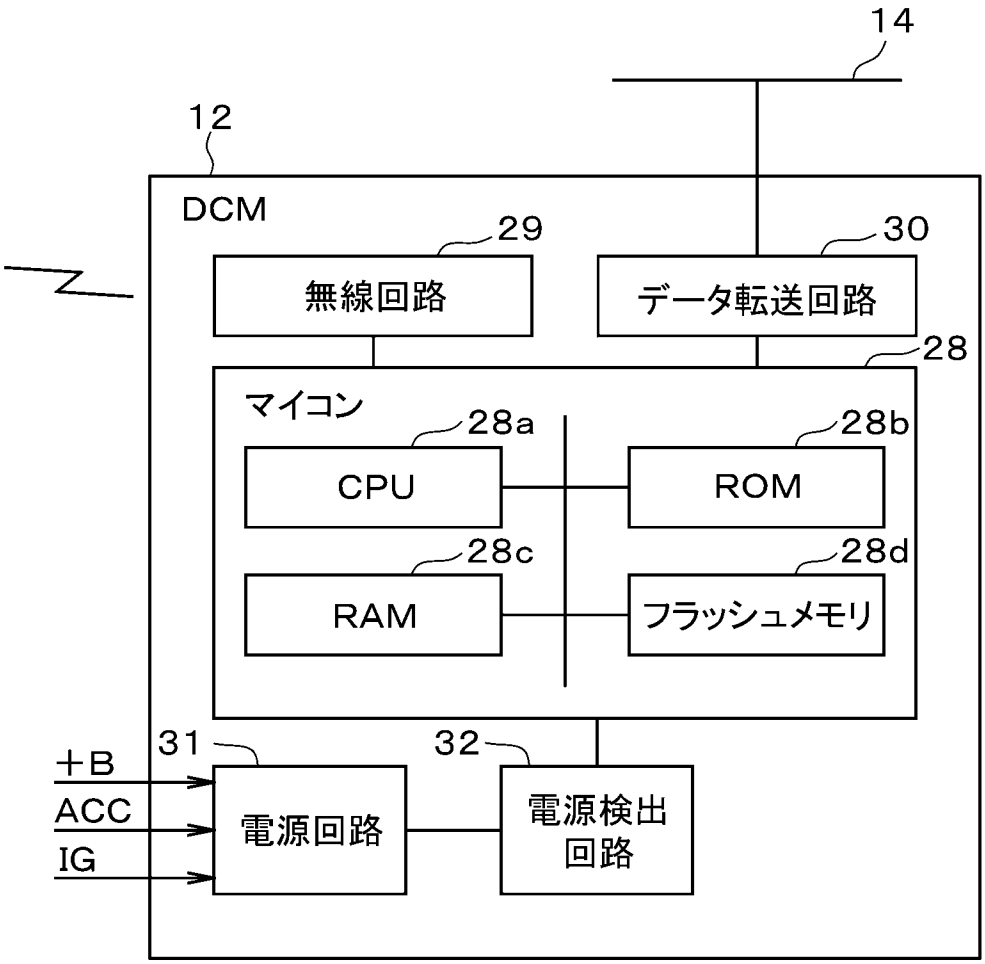
[図2]

Fig. 2


14～18,21
13
CGW
25
データ転送回路
24
マイコン
24a
CPU
24b
ROM
24c
RAM
24d
フラッシュメモリ
26
27
＋B
ACC
IG
電源回路
電源検出
回路

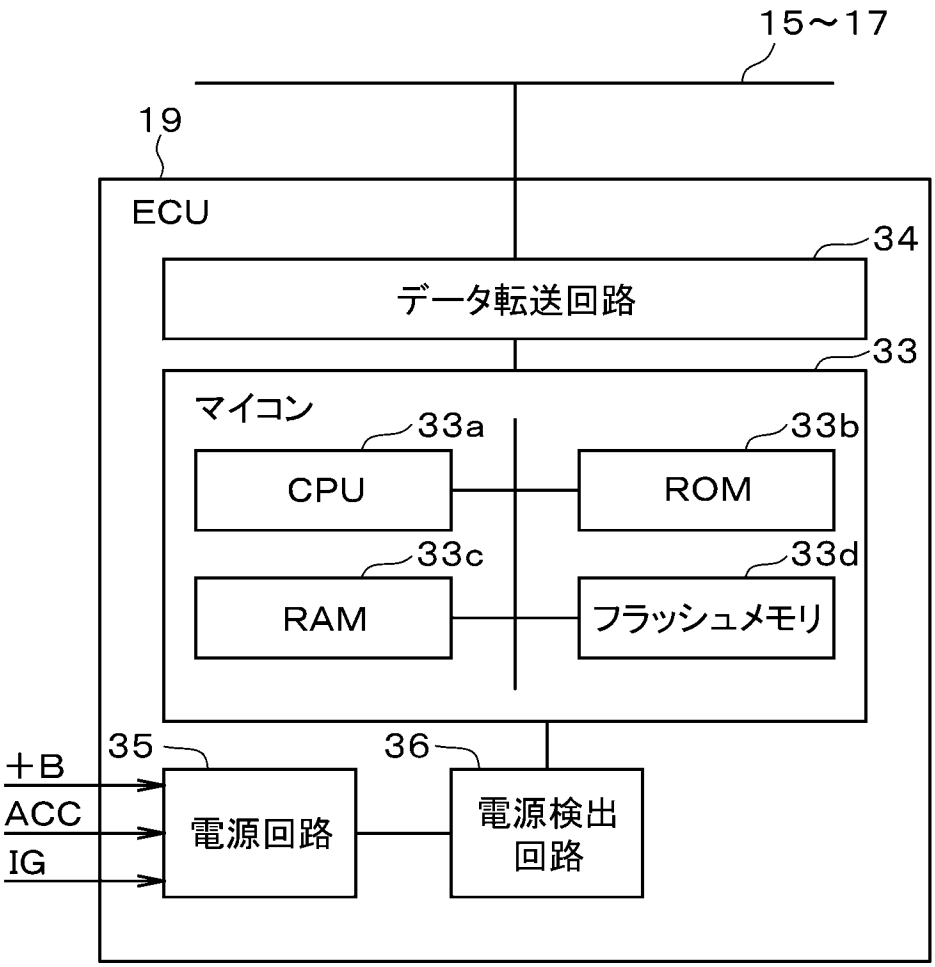
[図3]

Fig. 3


14
12
DCM
29
30
無線回路
データ転送回路
28
マイコン
28a
28b
CPU
ROM
28c
28d
RAM
フラッシュメモリ
31
32
＋B
ACC
IG
電源回路
電源検出
回路

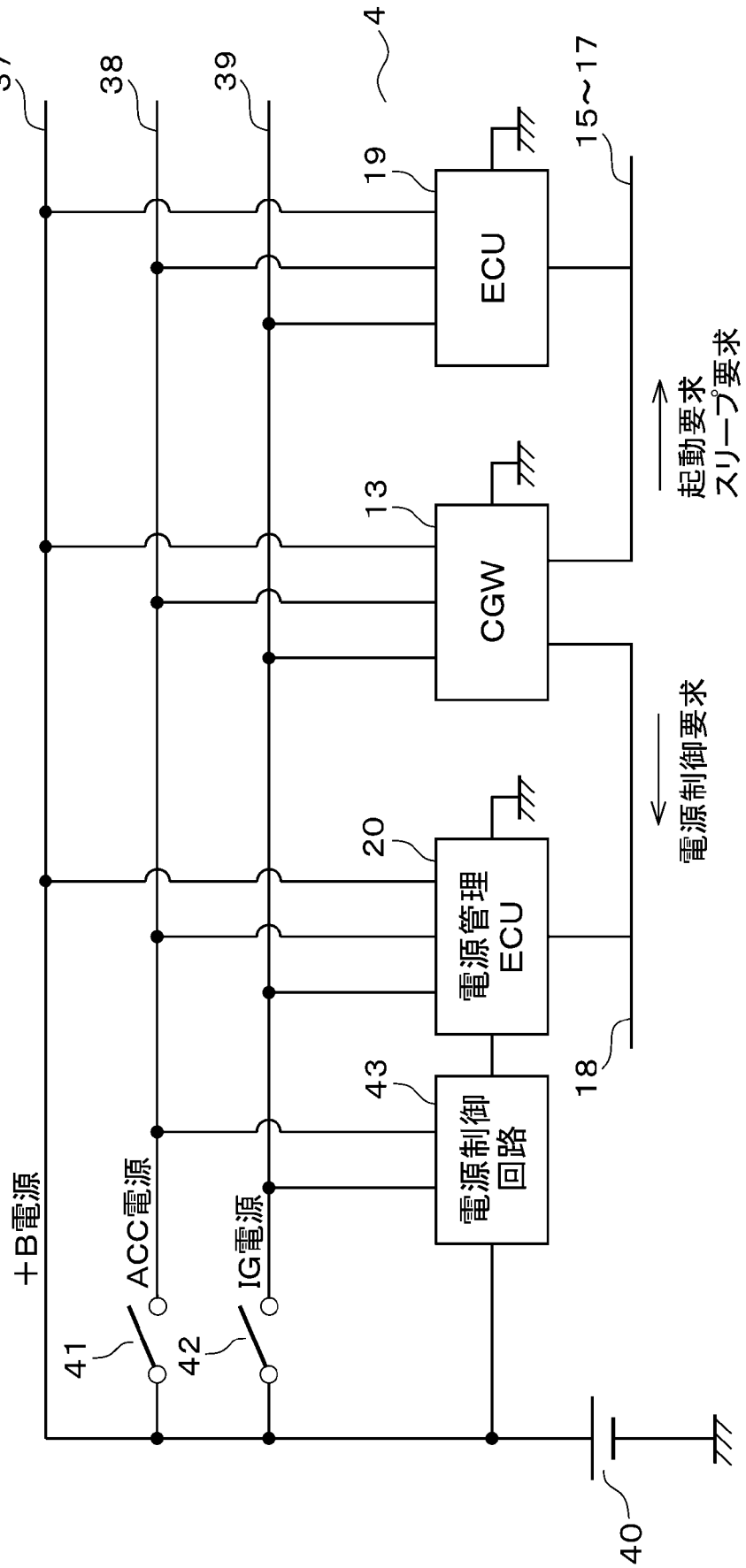
[図4]

Fig. 4


15～17
19
ECU
34
データ転送回路
33
マイコン
33a
CPU
33b
ROM
33c
RAM
33d
フラッシュメモリ
35
36
＋B
ACC
IG
電源回路
電源検出
回路

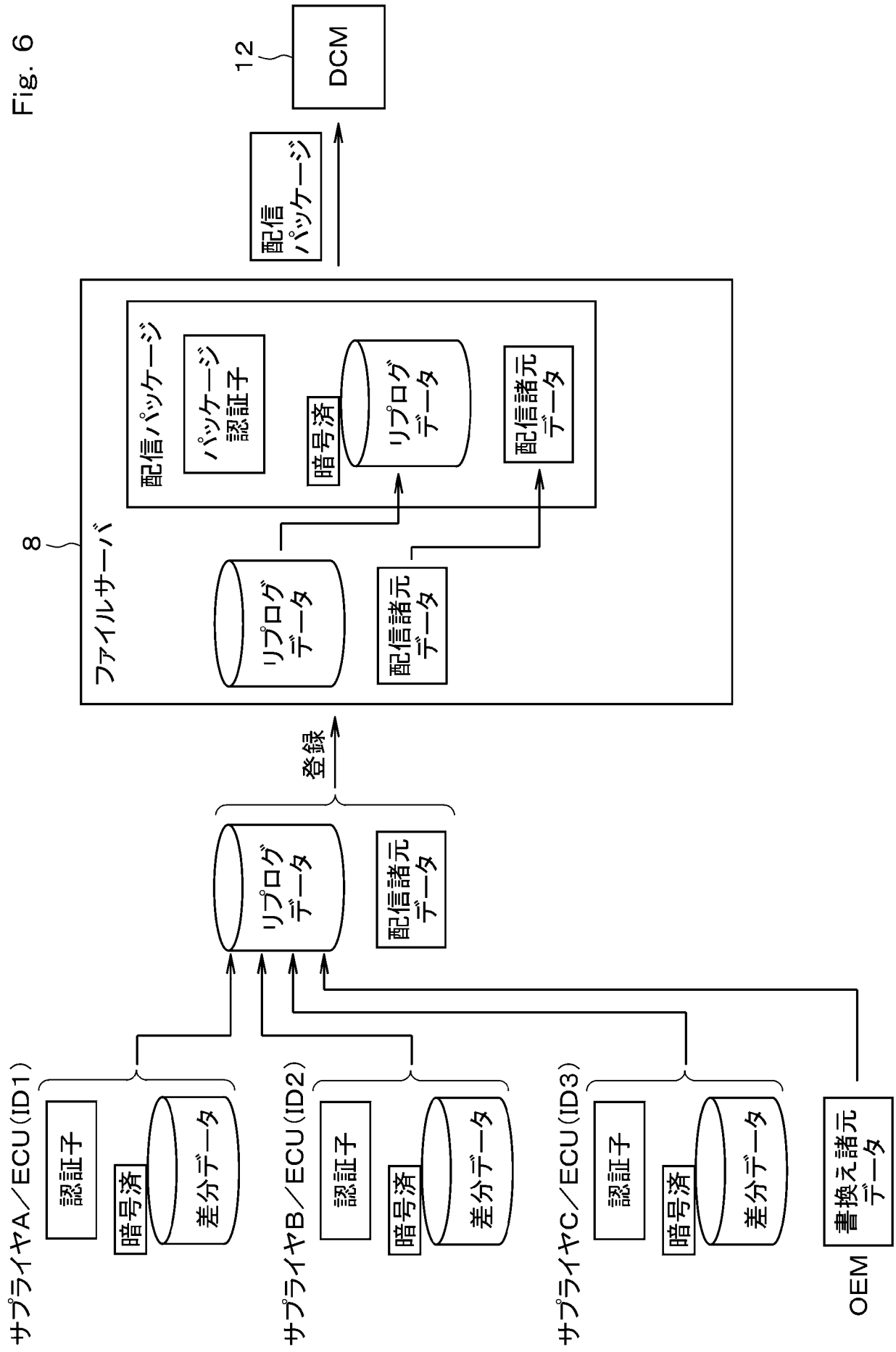
[図5]

Fig. 5


37
38
39
4
15～17
19
ECU
13
CGW
20
電源管理
ECU
43
電源制御
回路
18
起動要求
スリープ要求
電源制御要求
＋B電源
ACC電源
IG電源
41
42
40

[図6]

Fig. 6


12
DCM
配信
パッケージ
8
ファイルサーバ
配信パッケージ
パッケージ
認証子
暗号済
リプログ
データ
配信諸元
データ
リプログ
データ
配信諸元
データ
登録
リプログ
データ
配信諸元
データ
サプライヤA／ECU(ID1)
認証子
暗号済
差分データ
サプライヤB／ECU(ID2)
認証子
暗号済
差分データ
サプライヤC／ECU(ID3)
認証子
暗号済
差分データ
OEM
書換え諸元
データ

[図7]

Fig.7

DCM用の書換え諸元データ

項目		値(例示)
諸元データ情報	アドレス情報	0x10000000
	ファイル名	諸元. bin
ECU(ID1)情報	ECU_ID	1
	更新プログラム取得アドレス	0x10000000
	更新プログラムサイズ	1Mbyte
	ロールバックプログラム取得アドレス	0x20000000
	ロールバックプログラムサイズ	1Mbyte
ECU(ID2)情報	ECU_ID	2
	更新プログラム取得アドレス	0x30000000
	更新プログラムサイズ	1Mbyte
	ロールバックプログラム取得アドレス	0x40000000
	ロールバックプログラムサイズ	1Mbyte
ECU(ID3)情報	ECU_ID	3
	更新プログラム取得アドレス	0x50000000
	更新プログラムサイズ	1Mbyte
	ロールバックプログラム取得アドレス	0x60000000
	ロールバックプログラムサイズ	1Mbyte
ECU(ID4)情報	ECU_ID	4
	更新プログラム取得アドレス	0x70000000
	更新プログラムサイズ	1Mbyte
	ロールバックプログラム取得アドレス	0x80000000
	ロールバックプログラムサイズ	1Mbyte
ECU(ID5)情報	ECU_ID	5
	更新プログラム取得アドレス	0x90000000
	更新プログラムサイズ	1Mbyte
	ロールバックプログラム取得アドレス	0xA0000000
	ロールバックプログラムサイズ	1Mbyte
ECU(ID6)情報	ECU_ID	6
	更新プログラム取得アドレス	0xB0000000
	更新プログラムサイズ	1Mbyte
	ロールバックプログラム取得アドレス	0xC0000000
	ロールバックプログラムサイズ	1Mbyte

[図8]

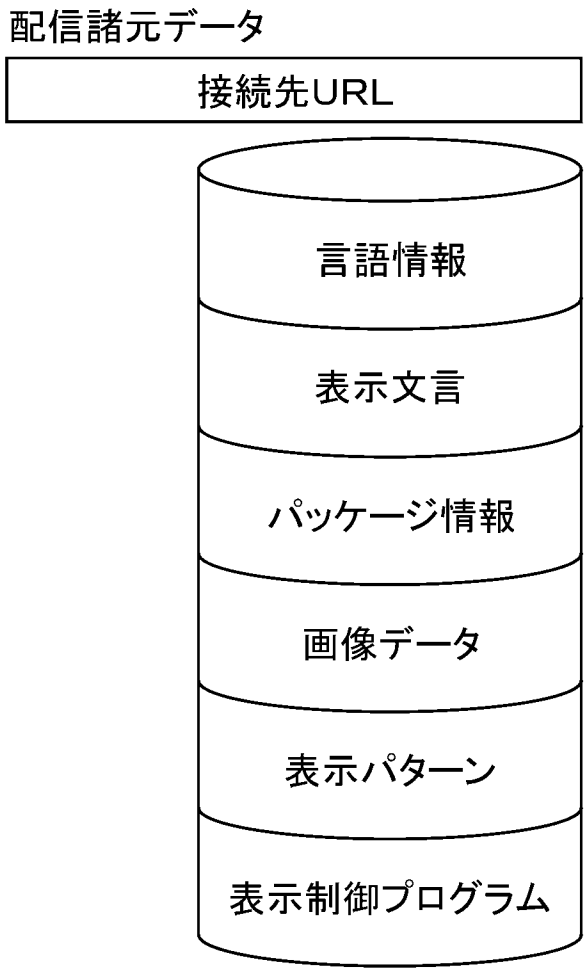
Fig.8

CGW用の書換え諸元データ

項目		値(例示)
グループ情報	第1グループ情報	ECU(ID1)→ECU(ID2)→ECU(ID3)
	第2グループ情報	ECU(ID4)→ECU(ID5)→ECU(ID6)
バス負荷テーブル		図100参照
バッテリ負荷		40%
書換え時の車両状態		全て駐車中／全て走行中／最適
シーン情報		リコール／ディーラー／工場用／ 機能更新通知／強制実行
ECU(IDn)情報 n＝1～6	ECU_ID	ECU_ID
	接続バス	第1バス
	接続電源	+B電源、ACC電源、IG電源
	セキュリティアクセス鍵情報	乱数値
		鍵パターン
		復号演算パターン
	メモリ種別	1面単独メモリ／疑似2面メモリ／2面メモリ
	書換え方法	電源自己保持／電源制御
	電源自己保持時間	5分
	書換え面情報	A面が起動面、B面が書換え面
	更新プログラムバージョン	2．0
	更新プログラム取得アドレス	1
	更新プログラムサイズ	10Mbyte
	ロールバックプログラムバージョン	1．0
	ロールバックプログラム取得アドレス	0x8000
	ロールバックプログラムサイズ	10Mbyte
	更新プログラムデータ種別	差分データ／全データ
	ロールバックプログラムデータ種別	差分データ／全データ

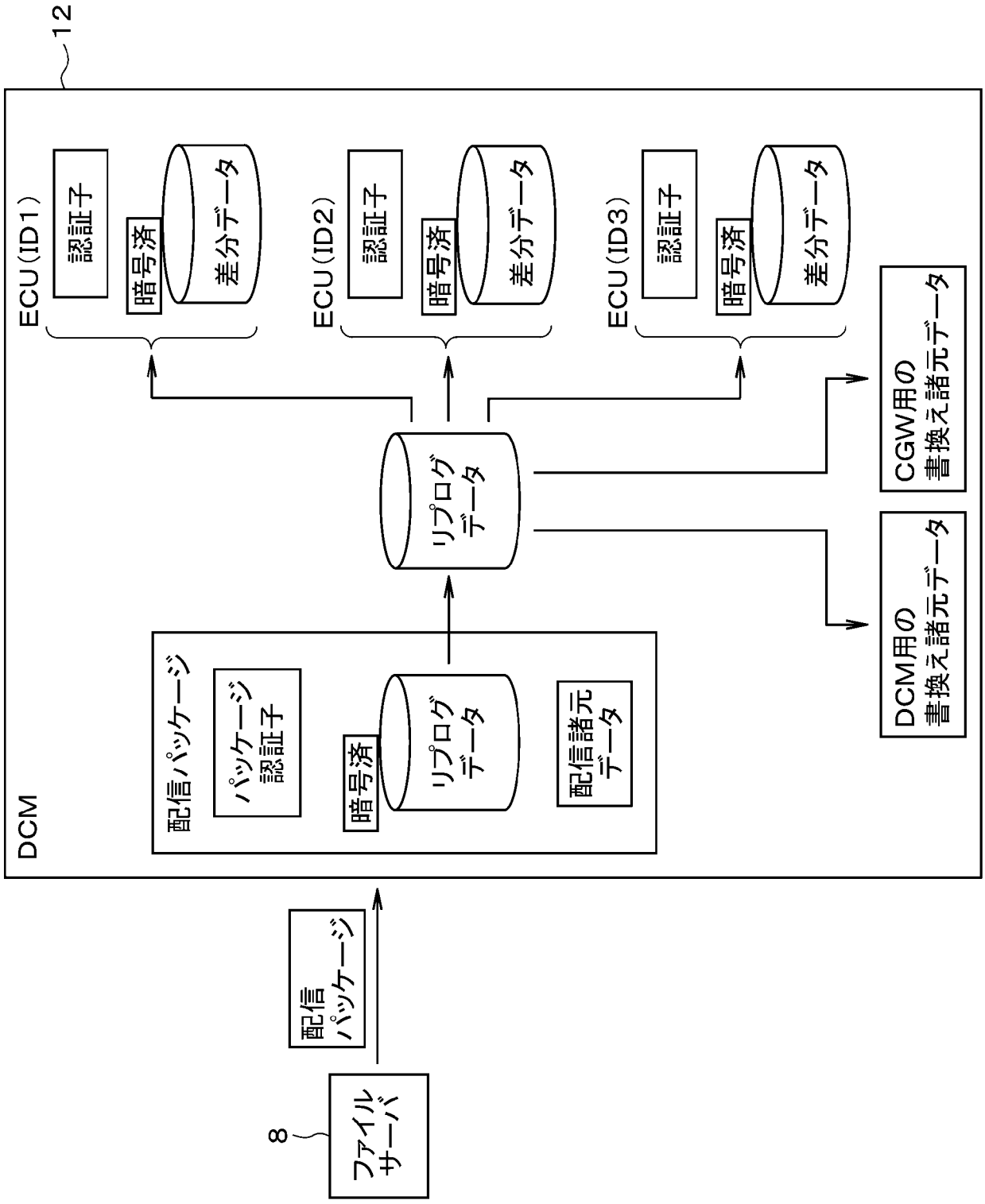
[図9]

Fig. 9



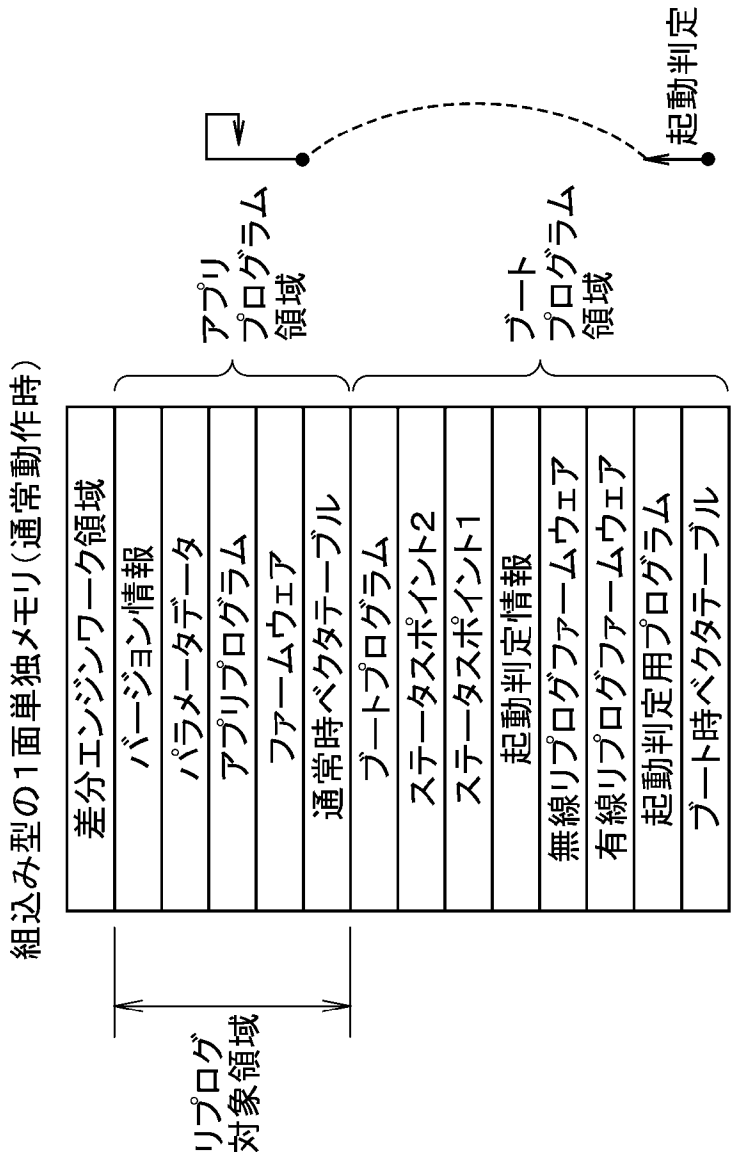
[図10]

Fig. 10


12
ECU(ID1)
認証子
暗号済
差分データ
ECU(ID2)
認証子
暗号済
差分データ
ECU(ID3)
認証子
暗号済
差分データ
リプログデータ
CGW用の書換え諸元データ
DCM用の書換え諸元データ
DCM
配信パッケージ
パッケージ認証子
暗号済
リプログデータ
配信諸元データ
配信パッケージ
8
ファイルサーバ

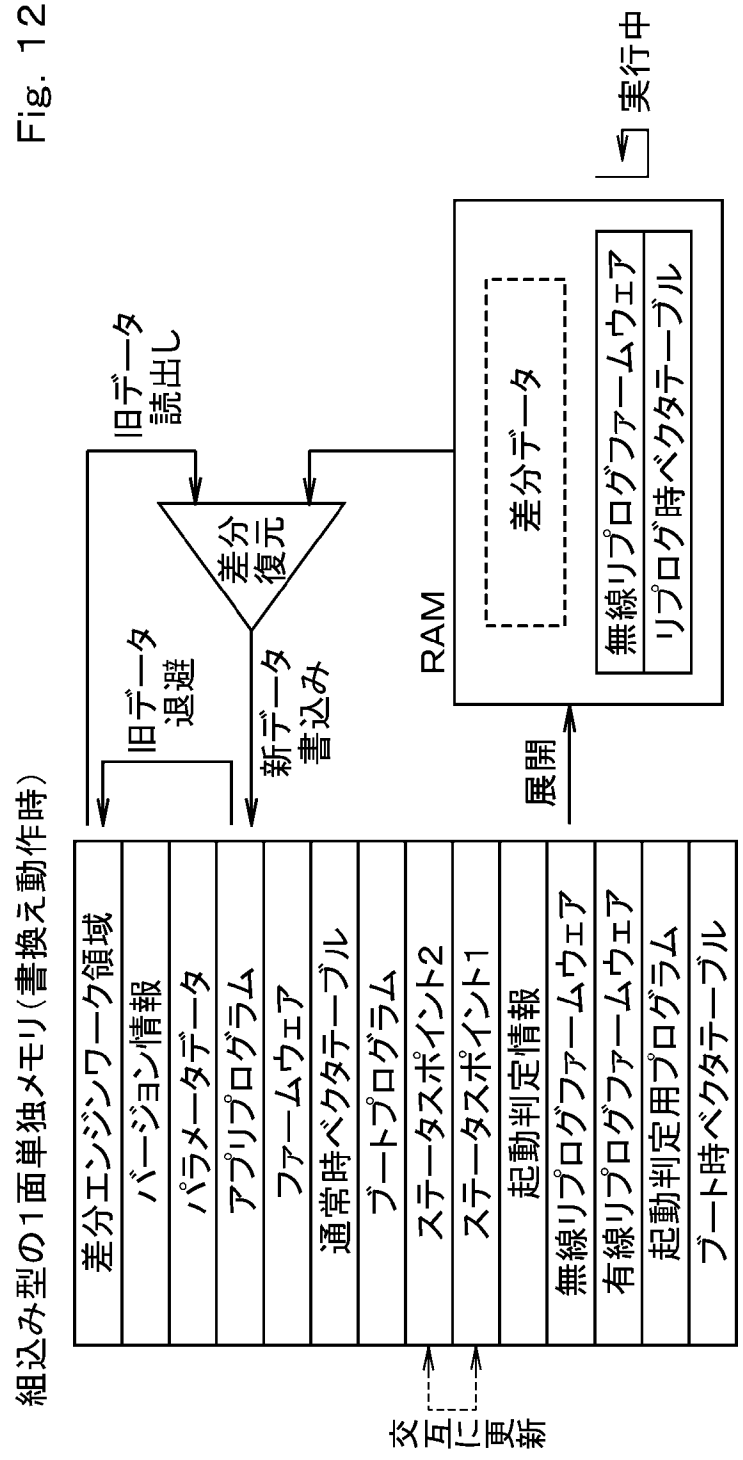
[図11]

Fig. 11


組込み型の1面単独メモリ（通常動作時）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル
ブートプログラム
ステータスポイント2
ステータスポイント1
起動判定情報
無線リプログファームウェア
有線リプログファームウェア
起動判定用プログラム
ブート時ベクタテーブル
リプログ対象領域
アプリプログラム領域
ブートプログラム領域
起動判定

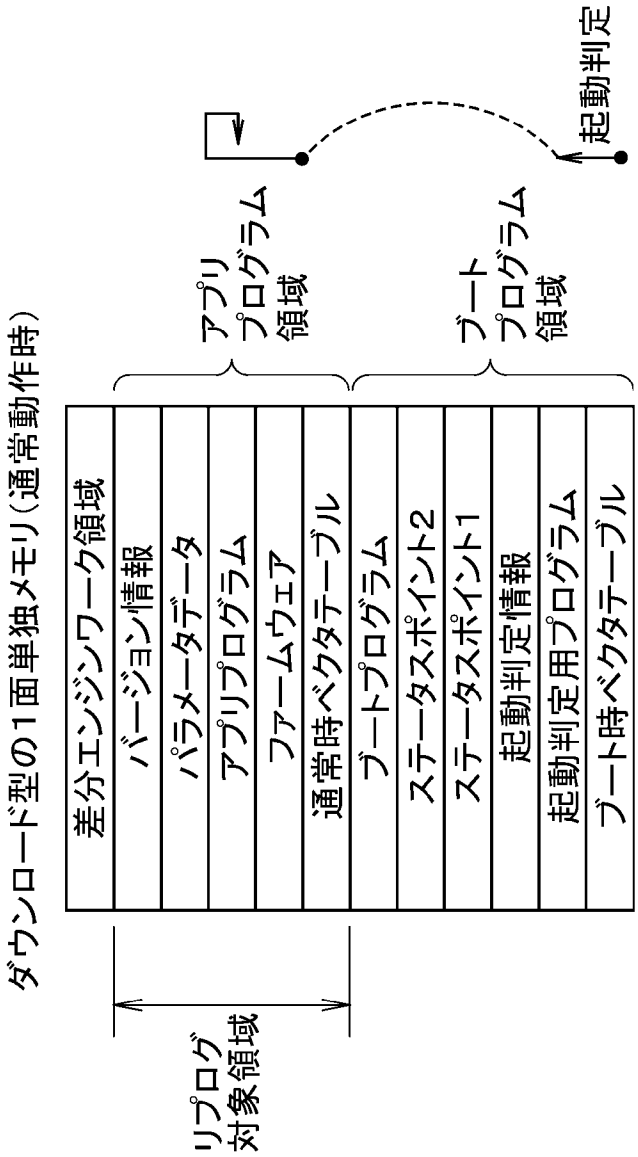
[図12]

Fig. 12


組込み型の1面単独メモリ（書換え動作時）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル
ブートプログラム
ステータスポイント2
ステータスポイント1
起動判定情報
無線リプログファームウェア
有線リプログファームウェア
起動判定用プログラム
ブート時ベクタテーブル
交互に更新
旧データ読出し
旧データ退避
差分復元
新データ書込み
展開
RAM
差分データ
無線リプログファームウェア
リプログ時ベクタテーブル
実行中

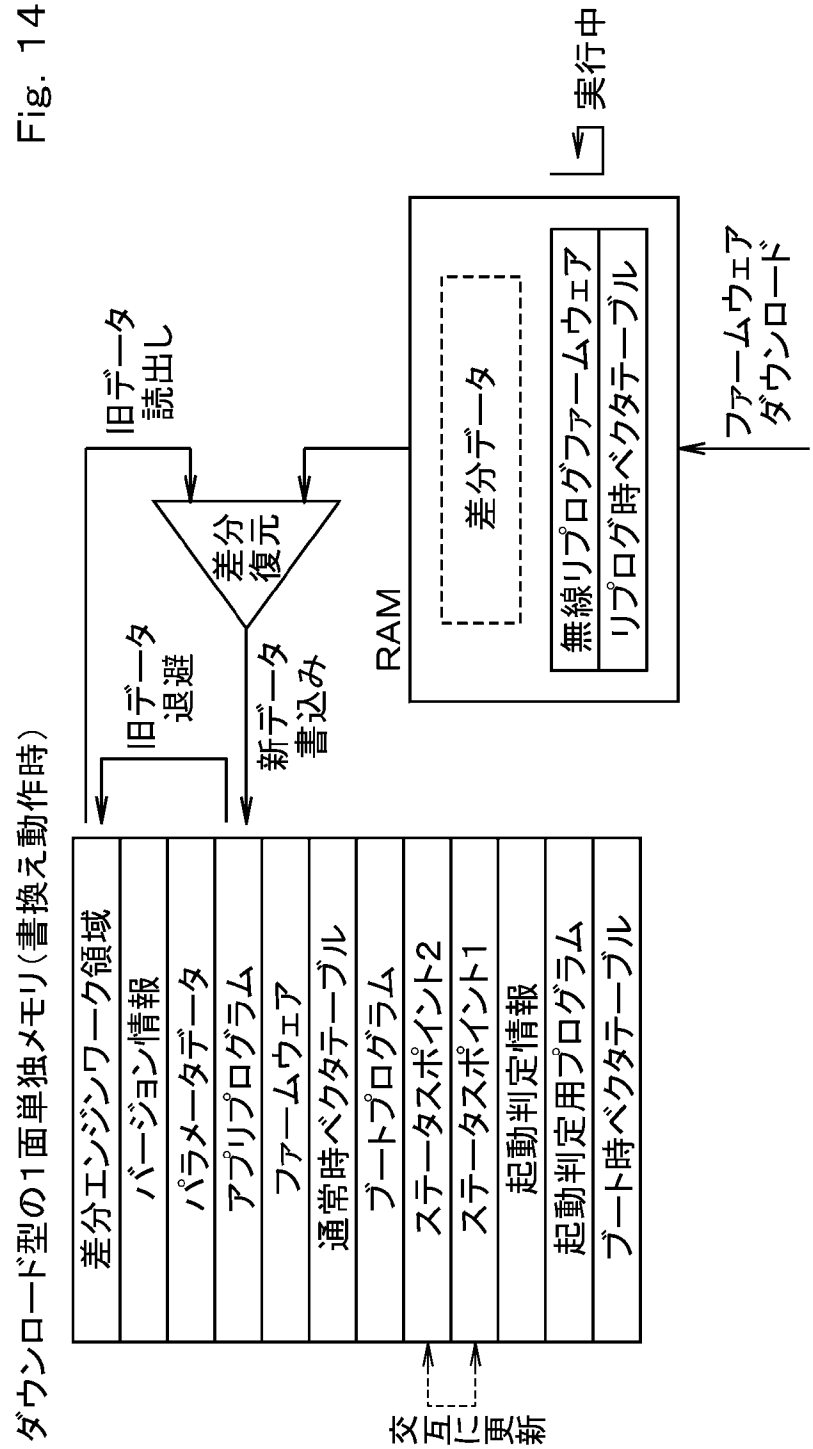
[図13]

Fig. 13


ダウンロード型の1面単独メモリ（通常動作時）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル
ブートプログラム
ステータスポイント2
ステータスポイント1
起動判定情報
起動判定用プログラム
ブート時ベクタテーブル
リプログ対象領域
アプリプログラム領域
ブートプログラム領域
起動判定

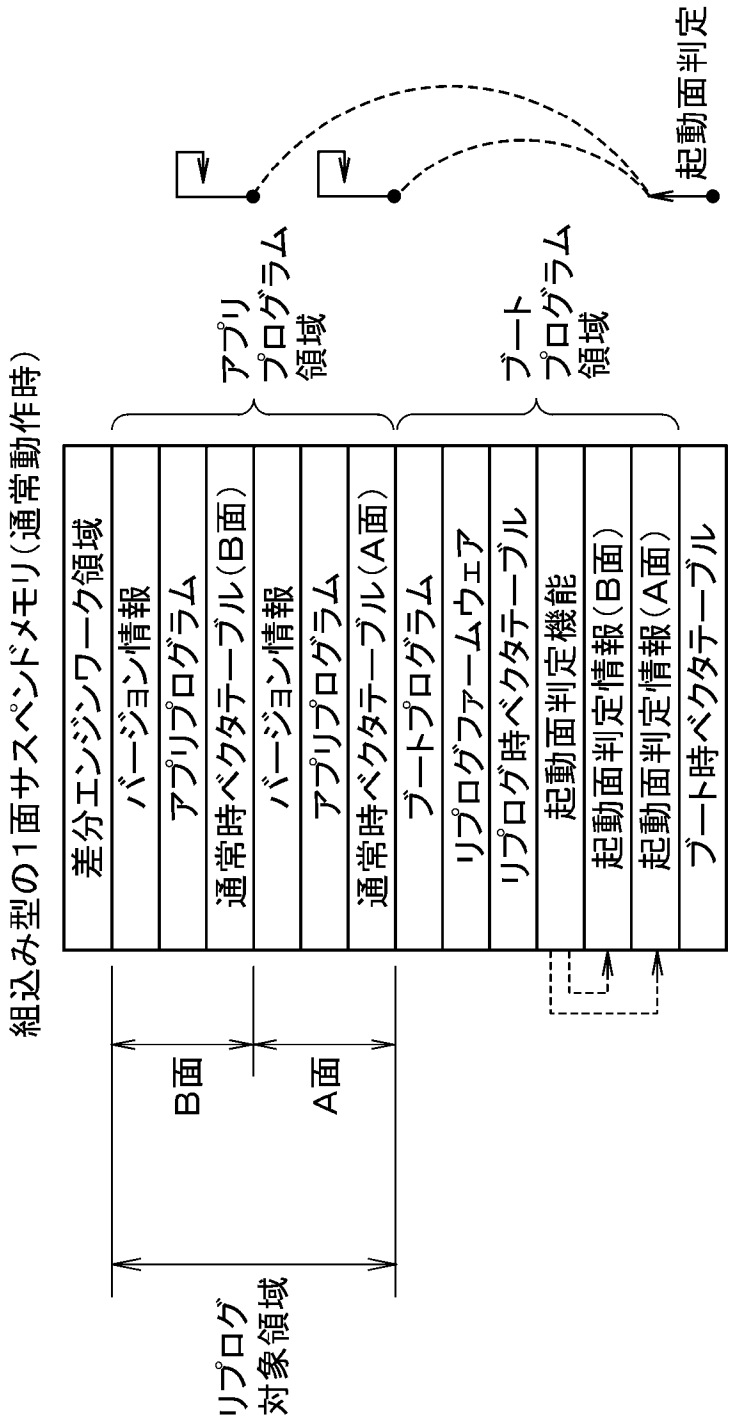
[図14]

Fig. 14


ダウンロード型の1面単独メモリ(書換え動作時)
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル
ブートプログラム
ステータスポイント2
ステータスポイント1
起動判定情報
起動判定用プログラム
ブート時ベクタテーブル
交互に更新
旧データ読出し
旧データ退避
差分復元
新データ書込み
RAM
差分データ
無線リプログファームウェア
リプログ時ベクタテーブル
実行中
ファームウェアダウンロード

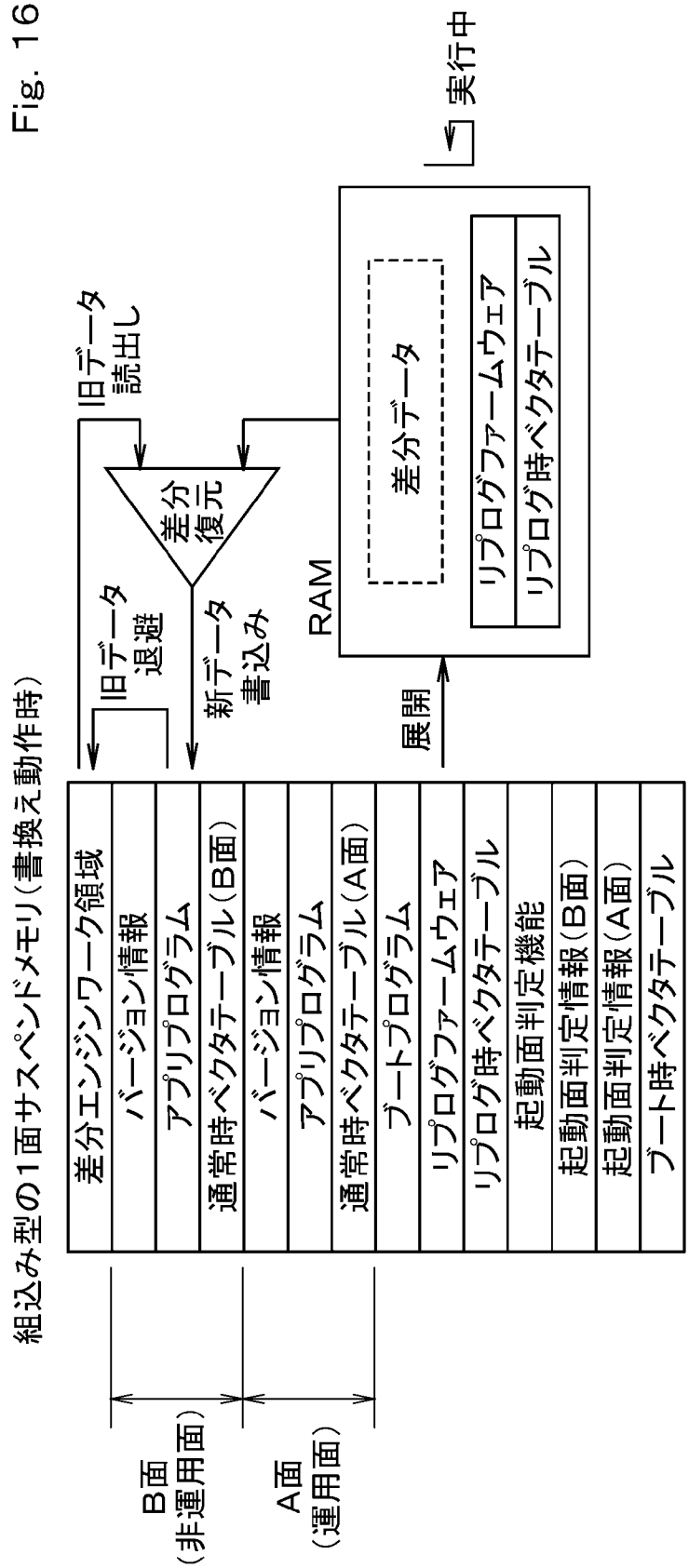
[図15]

Fig. 15


組込み型の1面サスペンドメモリ（通常動作時）
差分エンジンワーク領域
バージョン情報
アプリプログラム
通常時ベクタテーブル（B面）
バージョン情報
アプリプログラム
通常時ベクタテーブル（A面）
ブートプログラム
リプログファームウェア
リプログ時ベクタテーブル
起動面判定機能
起動面判定情報（B面）
起動面判定情報（A面）
ブート時ベクタテーブル
アプリ
プログラム
領域
ブート
プログラム
領域
起動面判定
B面
A面
リプログ
対象領域

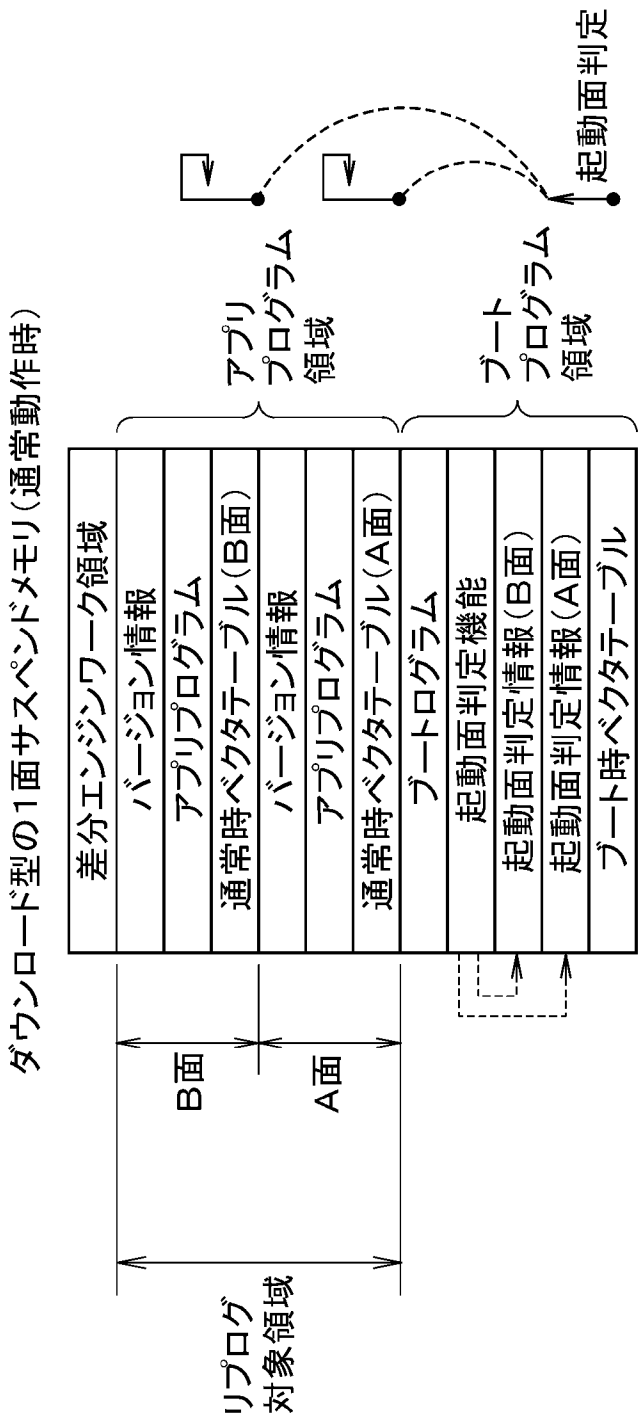
[図16]

Fig. 16


組込み型の1面サスペンドメモリ（書換え動作時）
差分エンジンワーク領域
バージョン情報
アプリプログラム
通常時ベクタテーブル（B面）
バージョン情報
アプリプログラム
通常時ベクタテーブル（A面）
ブートプログラム
リプログファームウェア
リプログ時ベクタテーブル
起動面判定機能
起動面判定情報（B面）
起動面判定情報（A面）
ブート時ベクタテーブル
B面
（非運用面）
A面
（運用面）
旧データ
読出し
旧データ
退避
差分
復元
新データ
書込み
RAM
差分データ
リプログファームウェア
リプログ時ベクタテーブル
展開
実行中

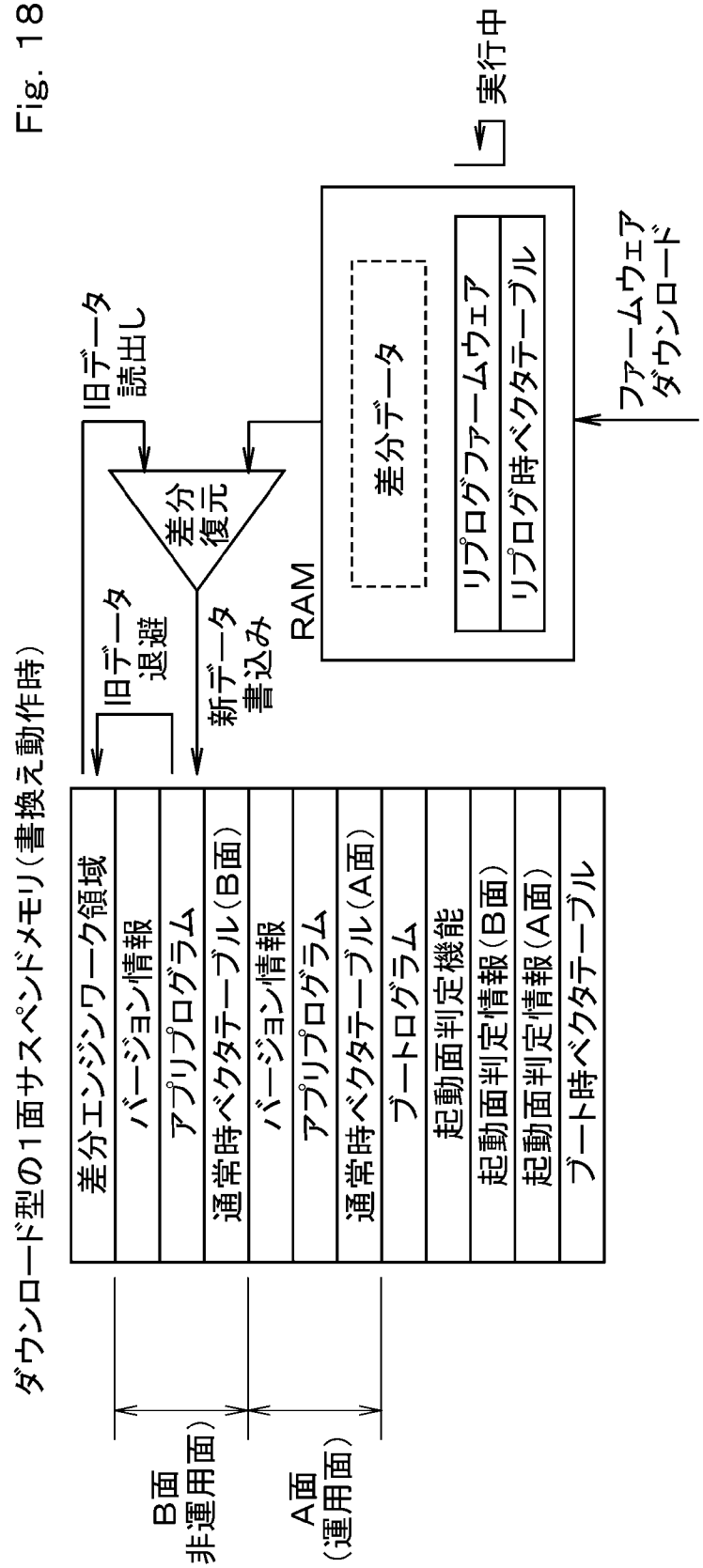
[図17]

Fig. 17


ダウンロード型の1面サスペンドメモリ（通常動作時）
差分エンジンワーク領域
バージョン情報
アプリプログラム
通常時ベクタテーブル（B面）
バージョン情報
アプリプログラム
通常時ベクタテーブル（A面）
ブートプログラム
起動面判定機能
起動面判定情報（B面）
起動面判定情報（A面）
ブート時ベクタテーブル
B面
A面
リプログ
対象領域
アプリ
プログラム
領域
ブート
プログラム
領域
起動面判定

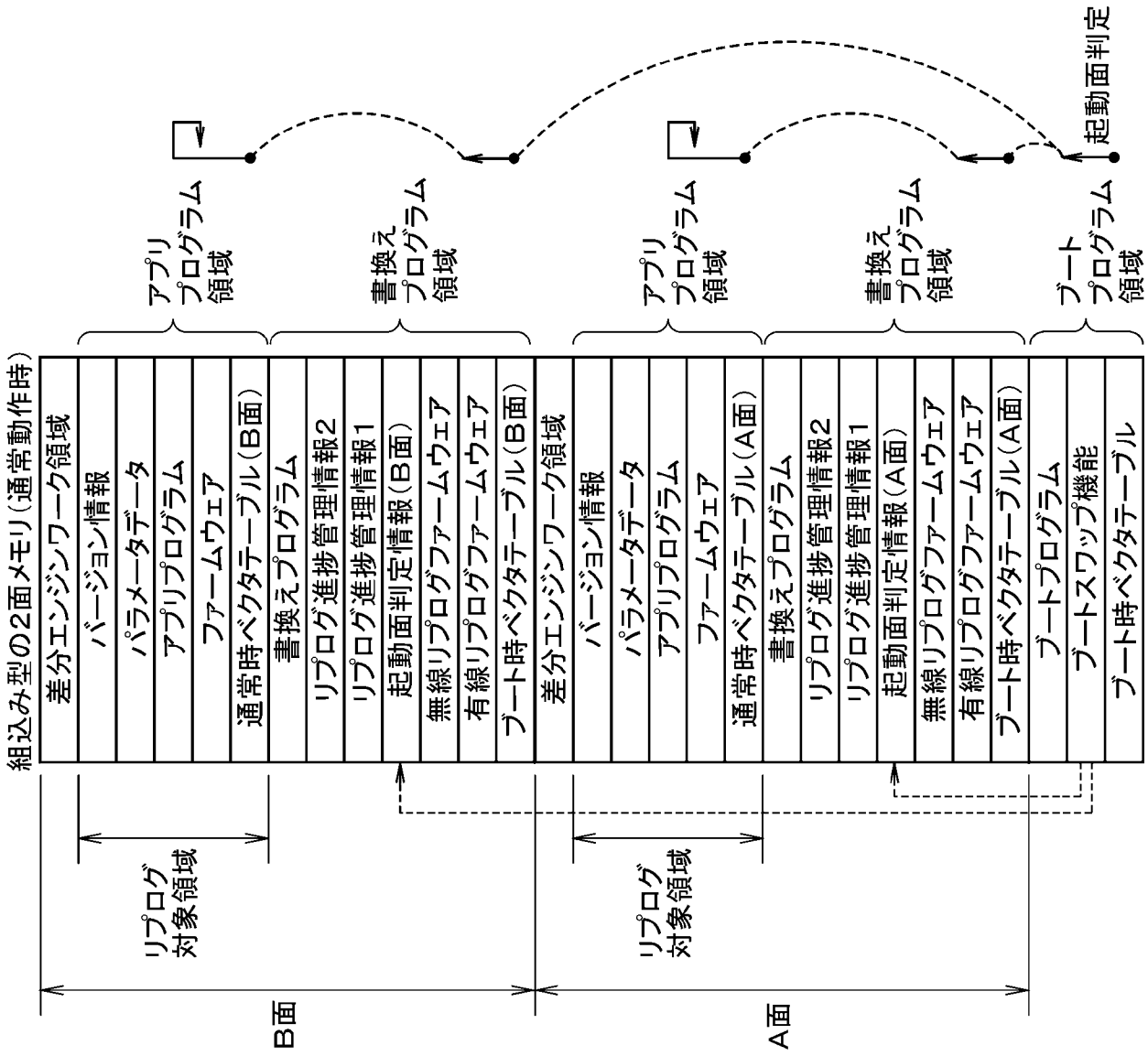
[図18]

Fig. 18


ダウンロード型の1面サスペンドメモリ（書換え動作時）
差分エンジンワーク領域
バージョン情報
アプリプログラム
通常時ベクタテーブル（B面）
バージョン情報
アプリプログラム
通常時ベクタテーブル（A面）
ブートログラム
起動面判定機能
起動面判定情報（B面）
起動面判定情報（A面）
ブート時ベクタテーブル
B面
（非運用面）
A面
（運用面）
旧データ
退避
旧データ
読出し
差分
復元
新データ
書込み
RAM
差分データ
リプログファームウェア
リプログ時ベクタテーブル
ファームウェア
ダウンロード
実行中

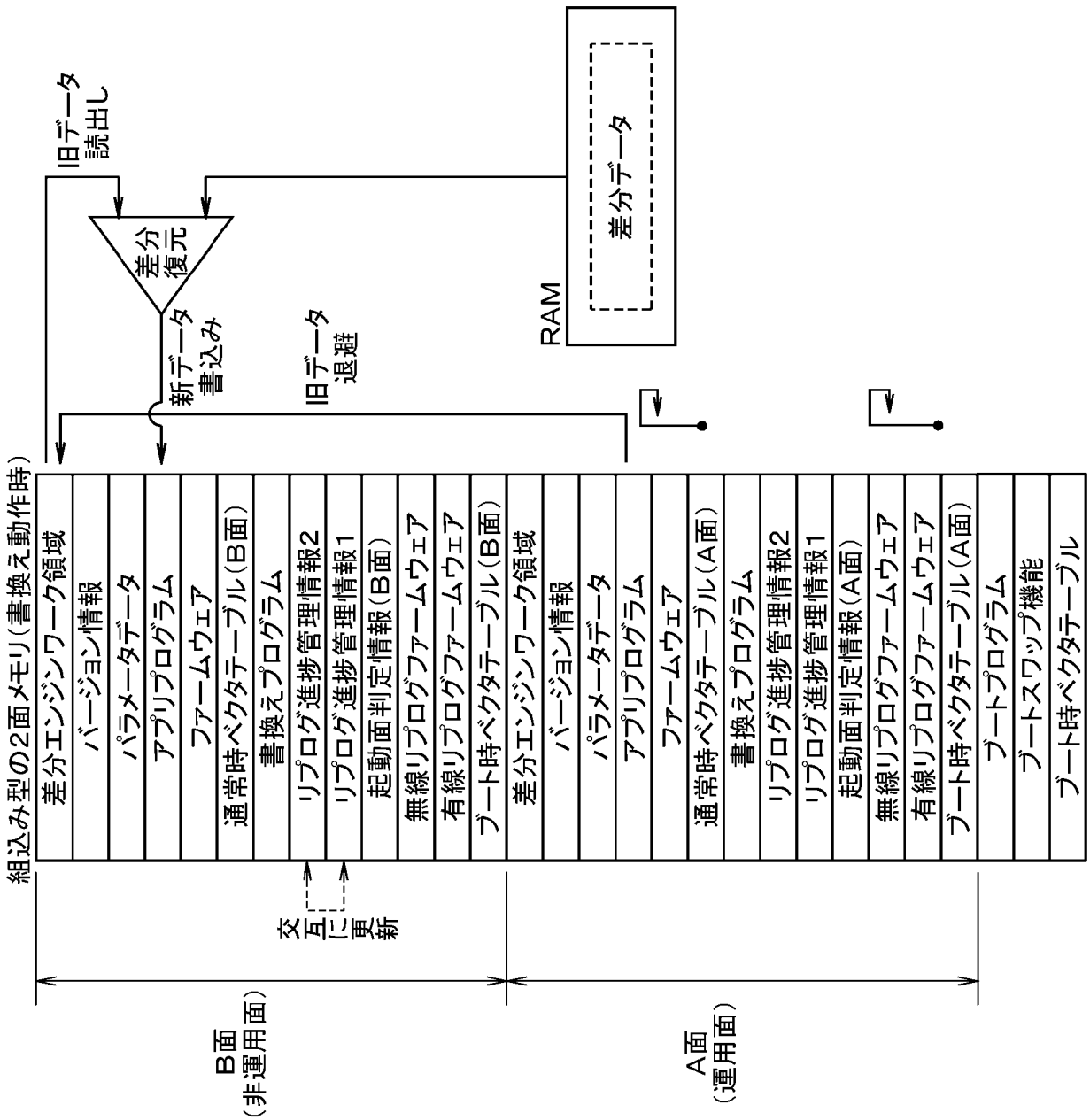
[図19]

Fig. 19


組込み型の2面メモリ(通常動作時)
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル(B面)
書換えプログラム
リプログ進捗管理情報2
リプログ進捗管理情報1
起動面判定情報(B面)
無線リプログファームウェア
有線リプログファームウェア
ブート時ベクタテーブル(B面)
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル(A面)
書換えプログラム
リプログ進捗管理情報2
リプログ進捗管理情報1
起動面判定情報(A面)
無線リプログファームウェア
有線リプログファームウェア
ブート時ベクタテーブル(A面)
ブートプログラム
ブートスワップ機能
ブート時ベクタテーブル
アプリ プログラム 領域
書換え プログラム 領域
アプリ プログラム 領域
書換え プログラム 領域
ブート プログラム 領域
起動面判定
リプログ 対象領域
リプログ 対象領域
B面
A面

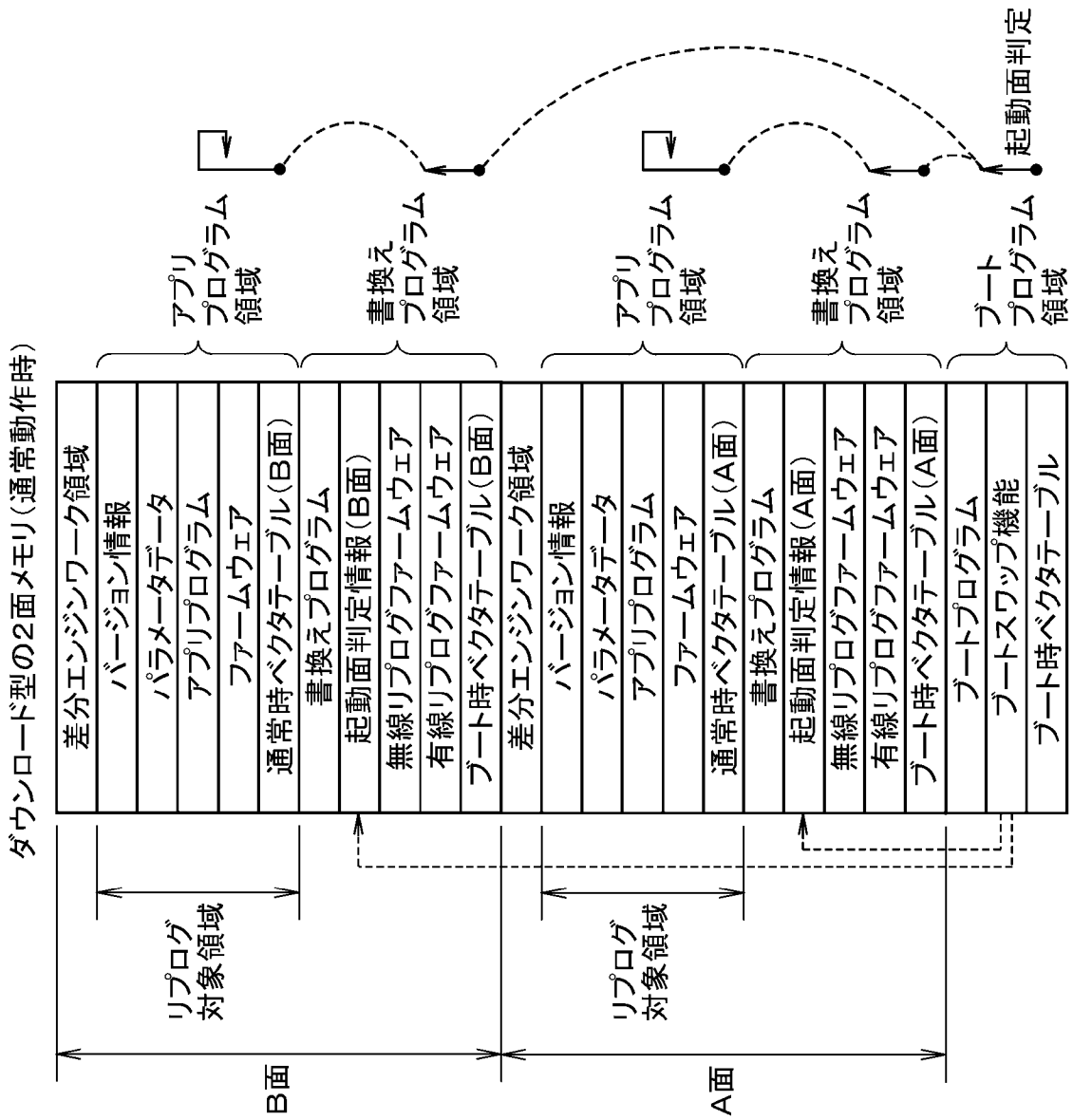
[図20]

Fig. 20


組込み型の2面メモリ(書換え動作時)
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル(B面)
書換えプログラム
リプログ進捗管理情報2
リプログ進捗管理情報1
起動面判定情報(B面)
無線リプログファームウェア
有線リプログファームウェア
ブート時ベクタテーブル(B面)
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル(A面)
書換えプログラム
リプログ進捗管理情報2
リプログ進捗管理情報1
起動面判定情報(A面)
無線リプログファームウェア
有線リプログファームウェア
ブート時ベクタテーブル(A面)
ブートプログラム
ブートスワップ機能
ブート時ベクタテーブル
交互に更新
B面
(非運用面)
A面
(運用面)
旧データ
読出し
差分
復元
新データ
書込み
旧データ
退避
RAM
差分データ

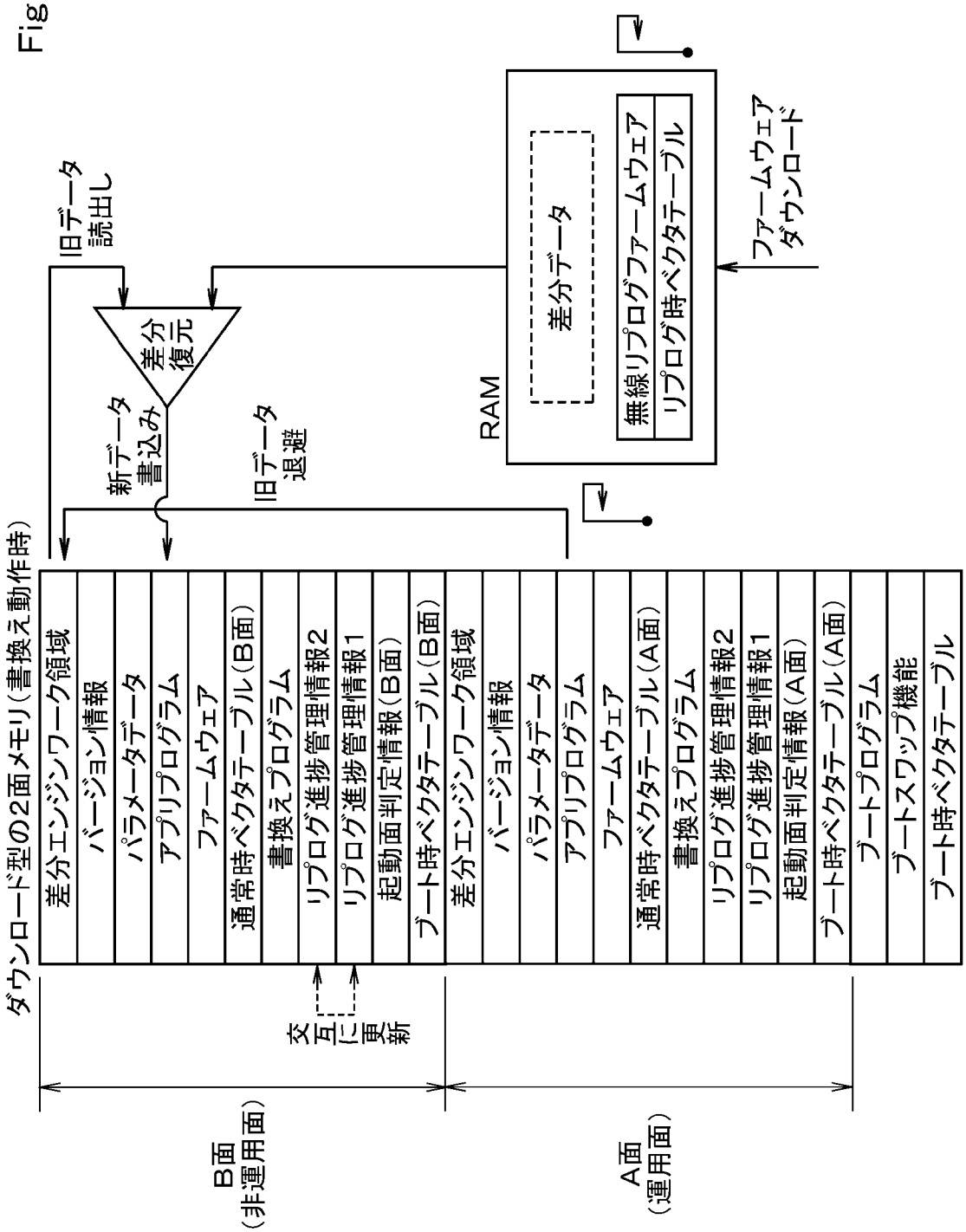
[図21]

Fig. 21


ダウンロード型の2面メモリ（通常動作時）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル（B面）
書換えプログラム
起動面判定情報（B面）
無線リプログファームウェア
有線リプログファームウェア
ブート時ベクタテーブル（B面）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル（A面）
書換えプログラム
起動面判定情報（A面）
無線リプログファームウェア
有線リプログファームウェア
ブート時ベクタテーブル（A面）
ブートプログラム
ブートスワップ機能
ブート時ベクタテーブル
アプリ
プログラム
領域
書換え
プログラム
領域
アプリ
プログラム
領域
書換え
プログラム
領域
ブート
プログラム
領域
起動面判定
リプログ
対象領域
リプログ
対象領域
B面
A面

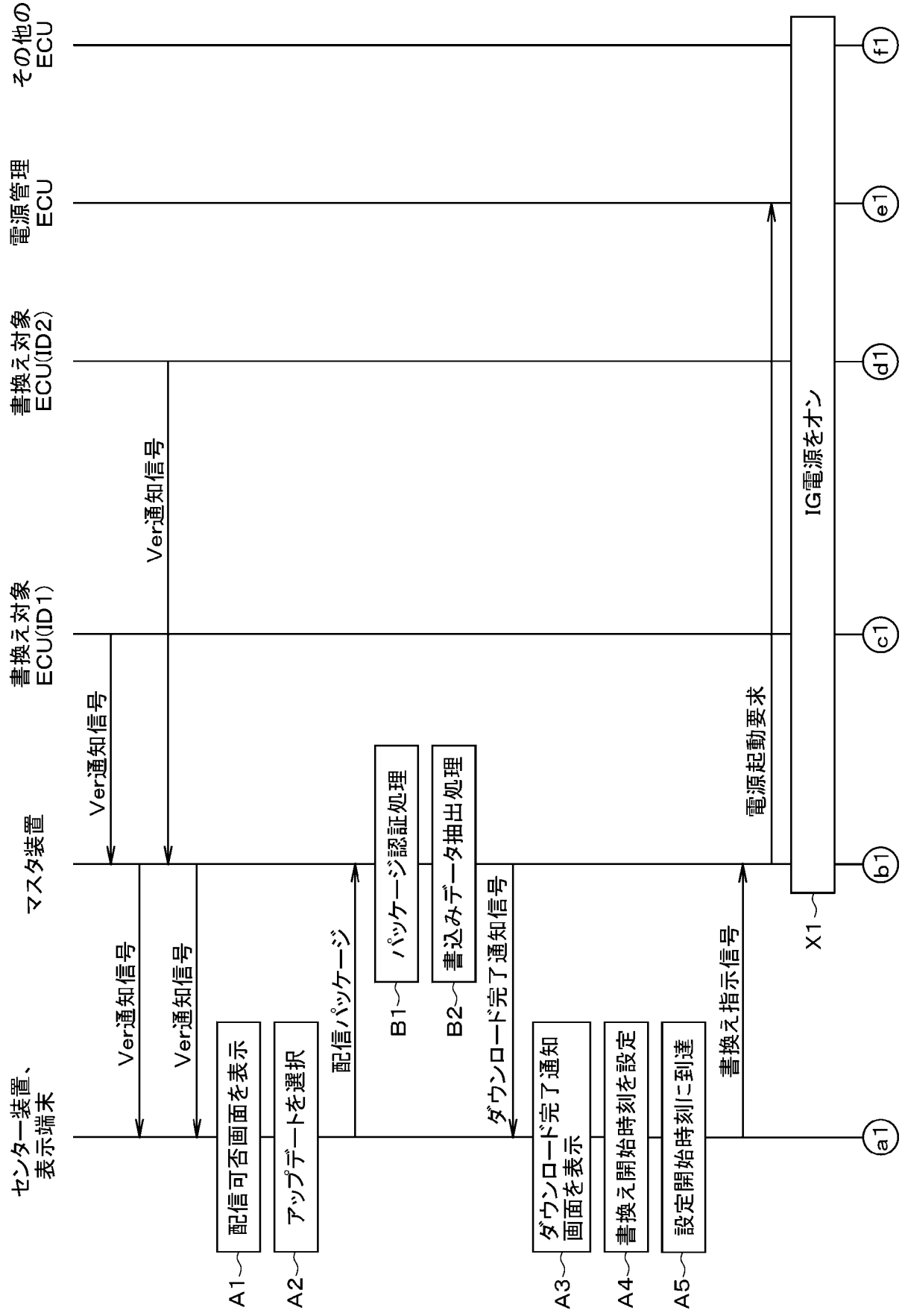
[図22]

Fig. 22


ダウンロード型の2面メモリ（書換え動作時）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル（B面）
書換えプログラム
リプログ進捗管理情報2
リプログ進捗管理情報1
起動面判定情報（B面）
ブート時ベクタテーブル（B面）
差分エンジンワーク領域
バージョン情報
パラメータデータ
アプリプログラム
ファームウェア
通常時ベクタテーブル（A面）
書換えプログラム
リプログ進捗管理情報2
リプログ進捗管理情報1
起動面判定情報（A面）
ブート時ベクタテーブル（A面）
ブートプログラム
ブートスワップ機能
ブート時ベクタテーブル
交互に更新
B面（非運用面）
A面（運用面）
旧データ読出し
差分復元
新データ書込み
旧データ退避
RAM
差分データ
無線リプログファームウェア
リプログ時ベクタテーブル
ファームウェアダウンロード

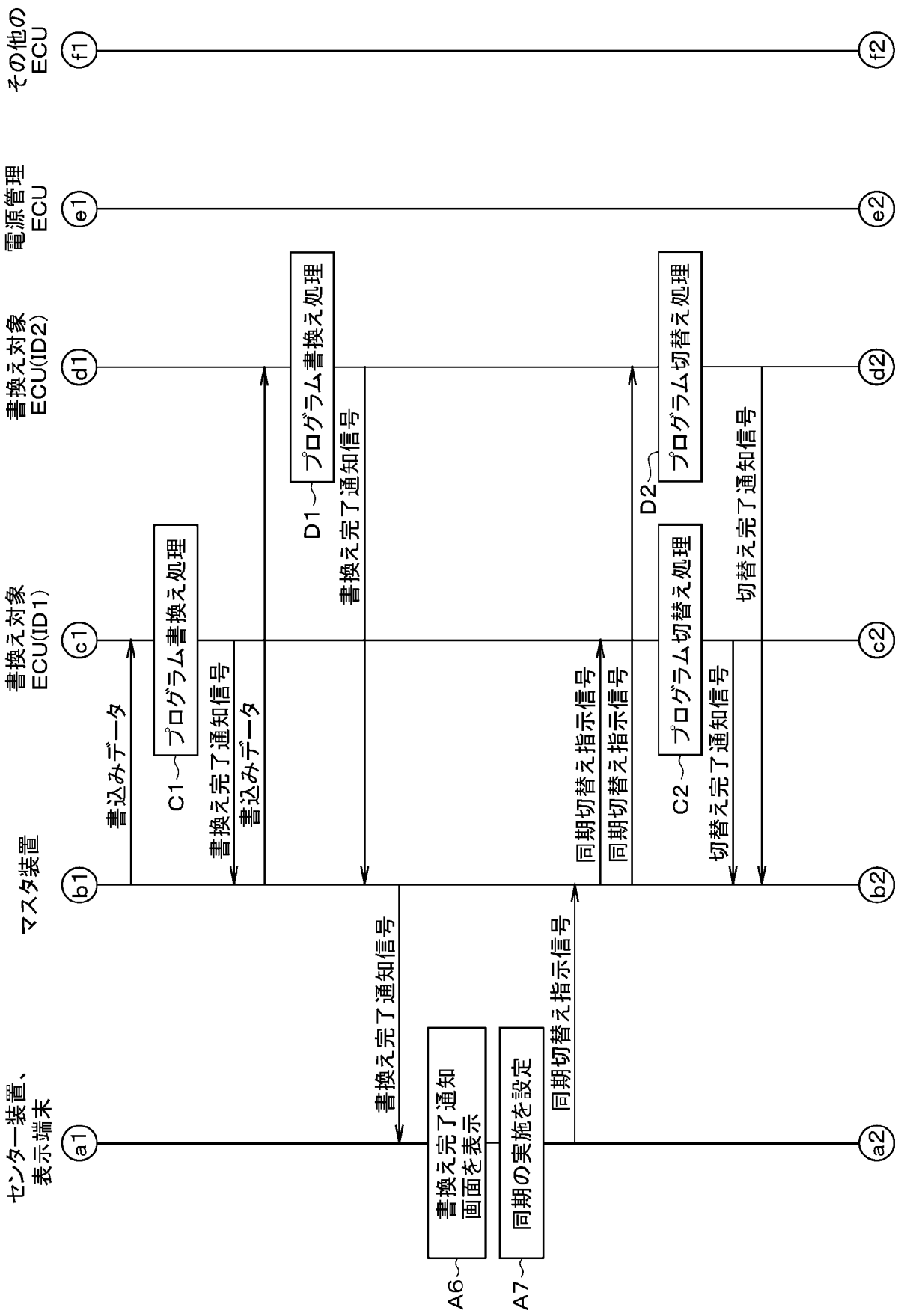
[図23]

Fig. 23


センター装置、表示端末
マスタ装置
書換え対象ECU(ID1)
書換え対象ECU(ID2)
電源管理ECU
その他のECU
Ver通知信号
Ver通知信号
Ver通知信号
Ver通知信号
配信可否画面を表示
アップデートを選択
配信パッケージ
パッケージ認証処理
書込みデータ抽出処理
ダウンロード完了通知信号
ダウンロード完了通知画面を表示
書換え開始時刻を設定
設定開始時刻に到達
書換え指示信号
電源起動要求
IG電源をオン
A1
A2
B1
B2
A3
A4
A5
X1
a1
b1
c1
d1
e1
f1

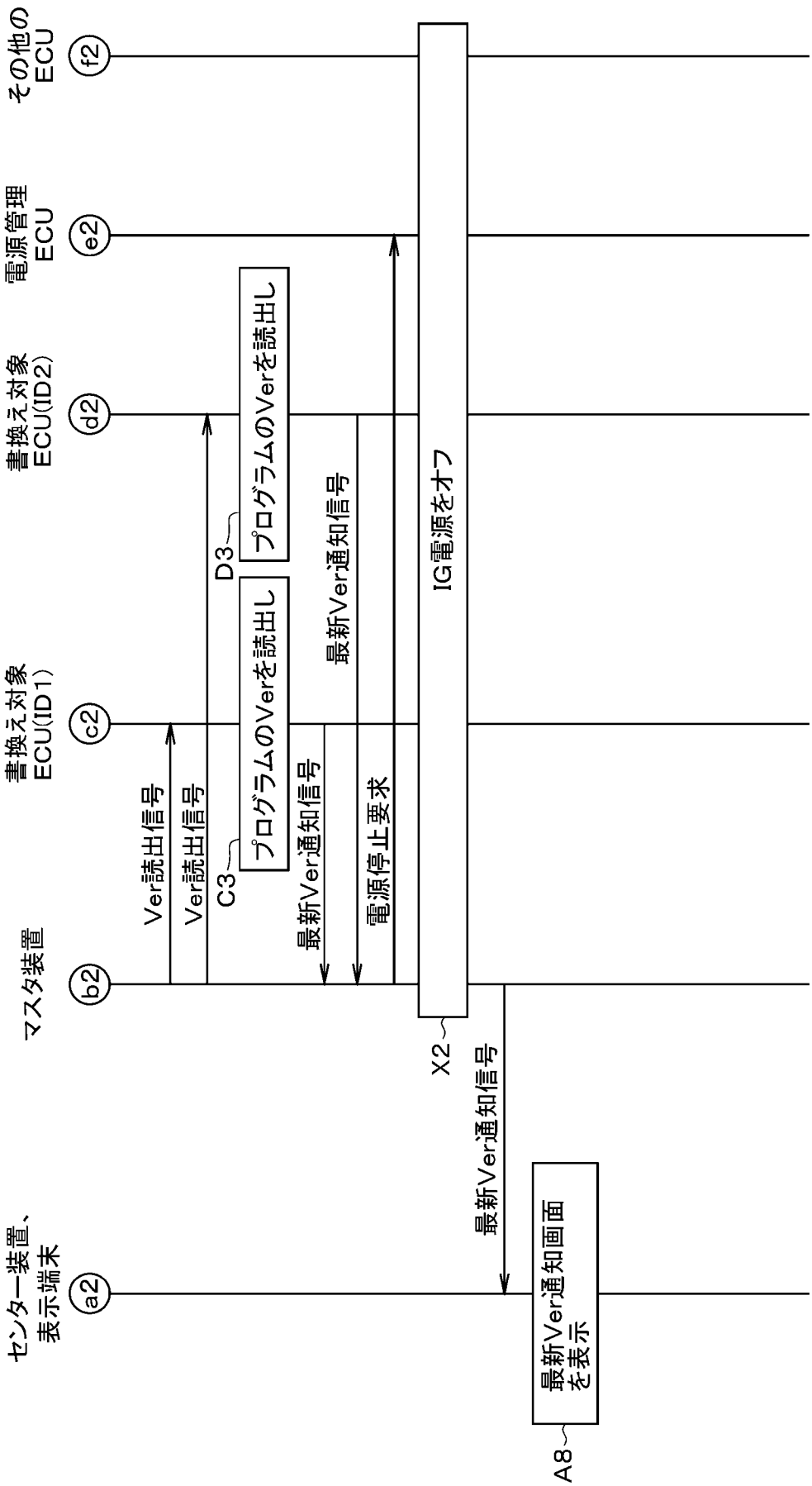
[図24]

Fig. 24


センター装置、表示端末
マスタ装置
書換え対象ECU(ID1)
書換え対象ECU(ID2)
電源管理ECU
その他のECU
a1
b1
c1
d1
e1
f1
a2
b2
c2
d2
e2
f2
書込みデータ
C1
プログラム書換え処理
書換え完了通知信号
書込みデータ
D1
プログラム書換え処理
書換え完了通知信号
書換え完了通知信号
書換え完了通知
画面を表示
A6
同期の実施を設定
A7
同期切替え指示信号
同期切替え指示信号
C2
プログラム切替え処理
切替え完了通知信号
D2
プログラム切替え処理
切替え完了通知信号
同期切替え指示信号

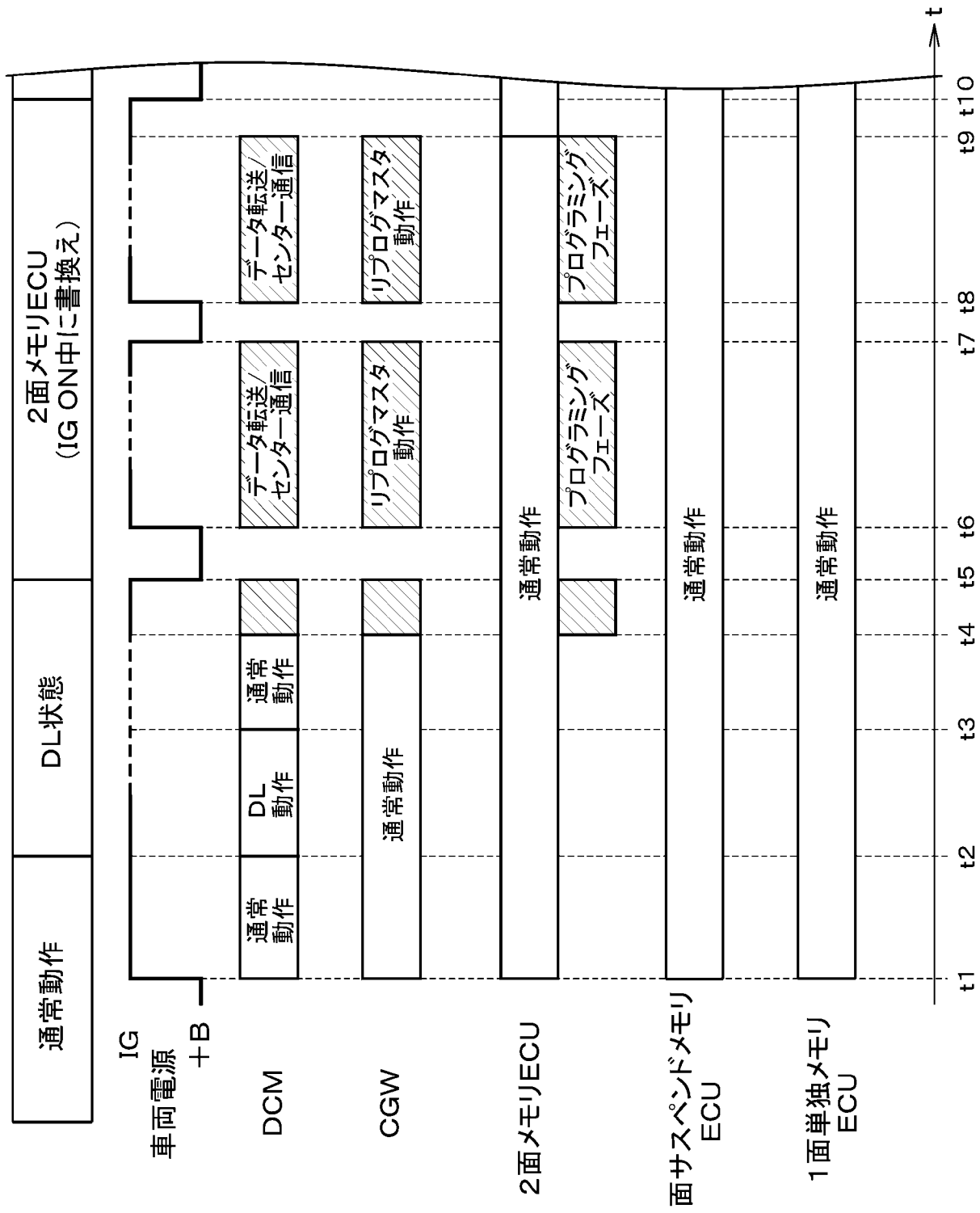
[図25]

Fig. 25


センター装置、表示端末
マスタ装置
書換え対象ECU(ID1)
書換え対象ECU(ID2)
電源管理ECU
その他のECU
a2
b2
c2
d2
e2
f2
Ver読出信号
Ver読出信号
C3
プログラムのVerを読出し
D3
プログラムのVerを読出し
最新Ver通知信号
最新Ver通知信号
電源停止要求
IG電源をオフ
X2
最新Ver通知信号
最新Ver通知画面を表示
A8

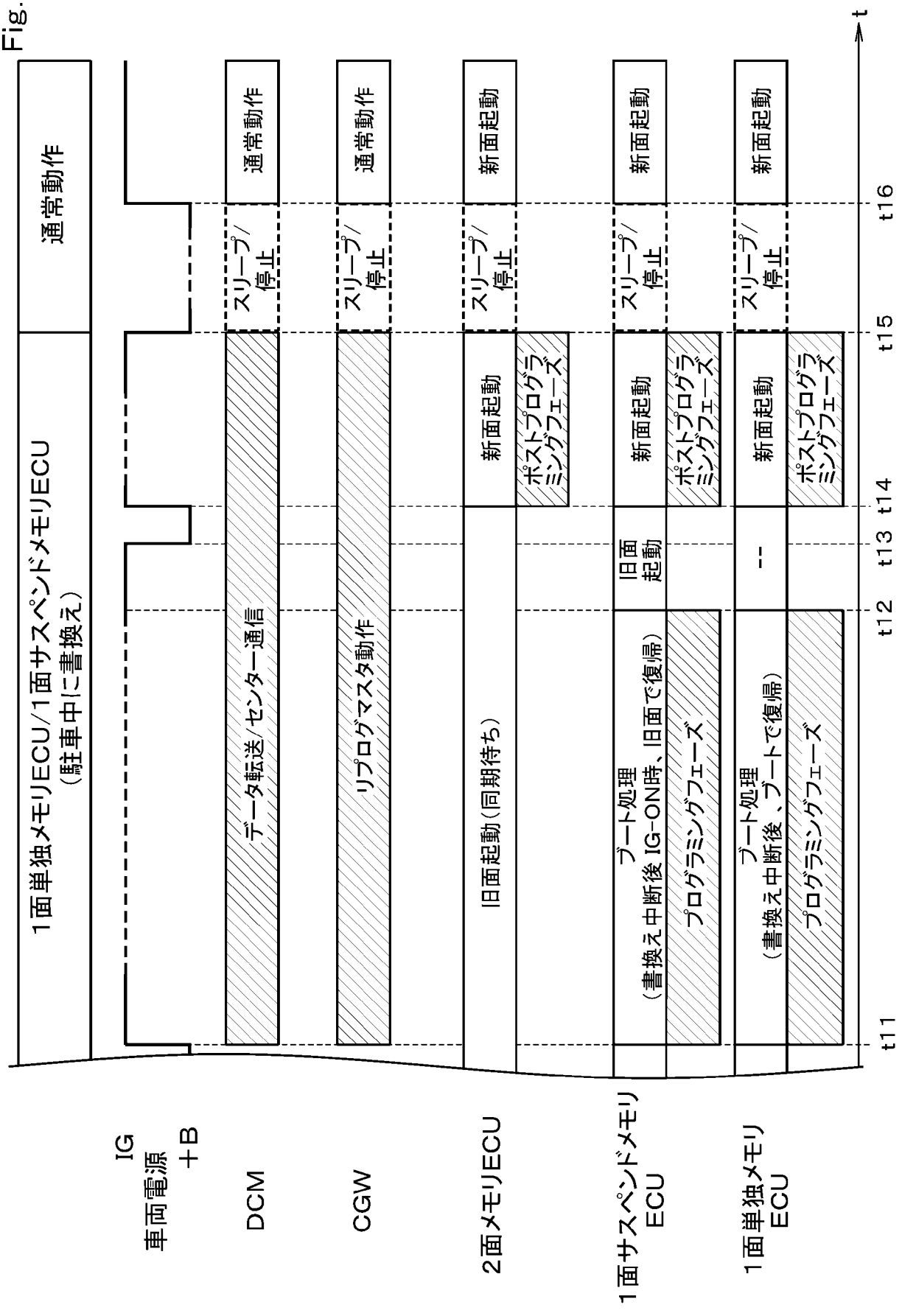
[図26]

Fig. 26


通常動作
DL状態
2面メモリECU
(IG ON中に書換え)
IG
車両電源
+B
DCM
CGW
2面メモリECU
1面サスペンドメモリ
ECU
1面単独メモリ
ECU
通常
動作
DL
動作
通常
動作
通常動作
データ転送/
センター通信
リプログマスタ
動作
データ転送/
センター通信
リプログマスタ
動作
通常動作
プログラミング
フェーズ
プログラミング
フェーズ
通常動作
通常動作
t
t1
t2
t3
t4
t5
t6
t7
t8
t9
t10

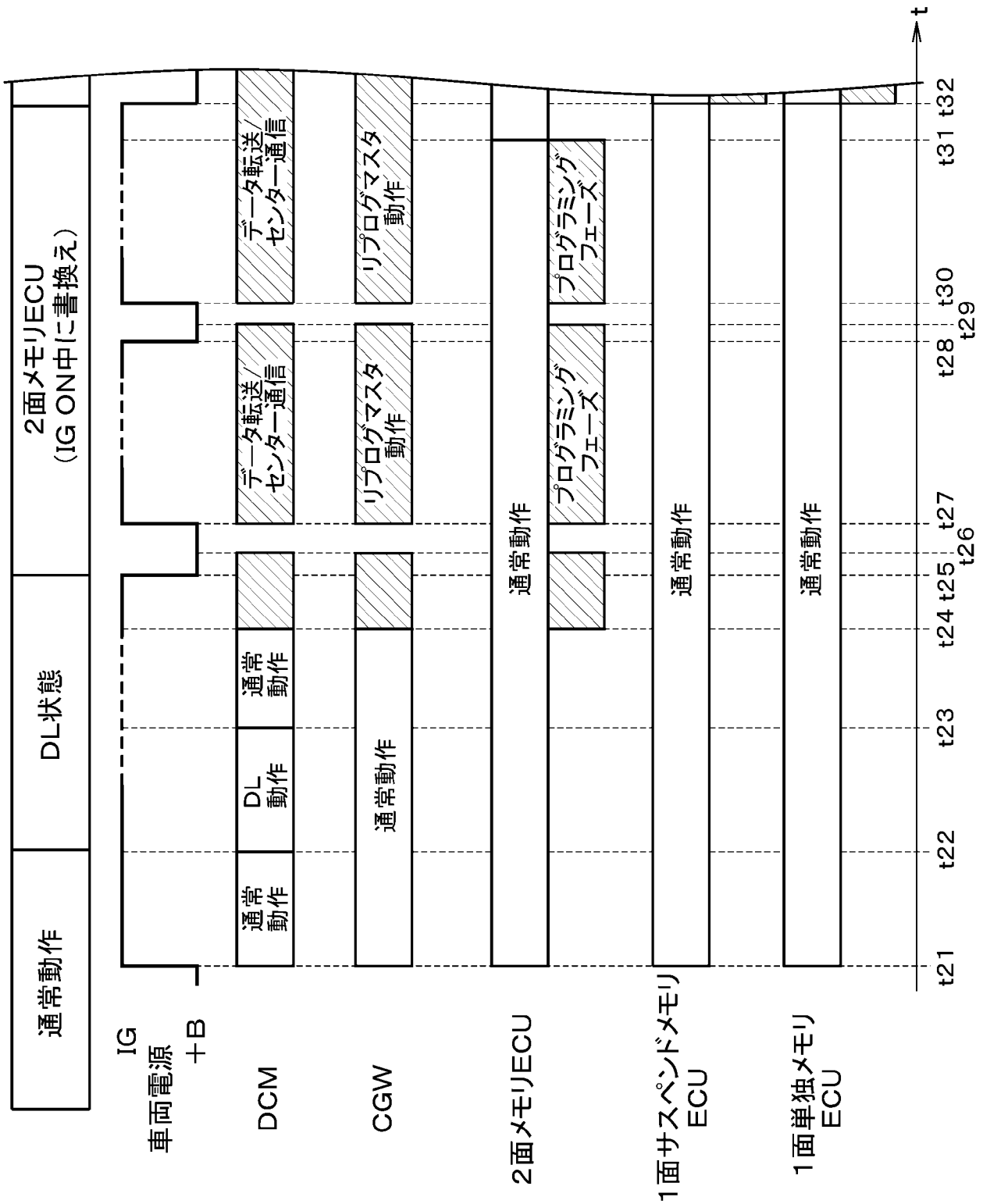
[図27]

Fig. 27


IG
車両電源
＋B
DCM
CGW
2面メモリECU
1面サスペンドメモリ
ECU
1面単独メモリ
ECU
1面単独メモリECU/1面サスペンドメモリECU
（駐車中に書換え）
通常動作
データ転送/センター通信
スリープ/
停止
通常動作
リプログマスタ動作
スリープ/
停止
新面起動
旧面起動（同期待ち）
スリープ/
停止
新面起動
ポストプログラミングフェーズ
新面起動
ブート処理
（書換え中断後 IG-ON時、旧面で復帰）
旧面
起動
プログラミングフェーズ
スリープ/
停止
新面起動
ポストプログラミングフェーズ
新面起動
ブート処理
（書換え中断後、ブートで復帰）
--
プログラミングフェーズ
スリープ/
停止
新面起動
ポストプログラミングフェーズ
t
t11
t12
t13
t14
t15
t16

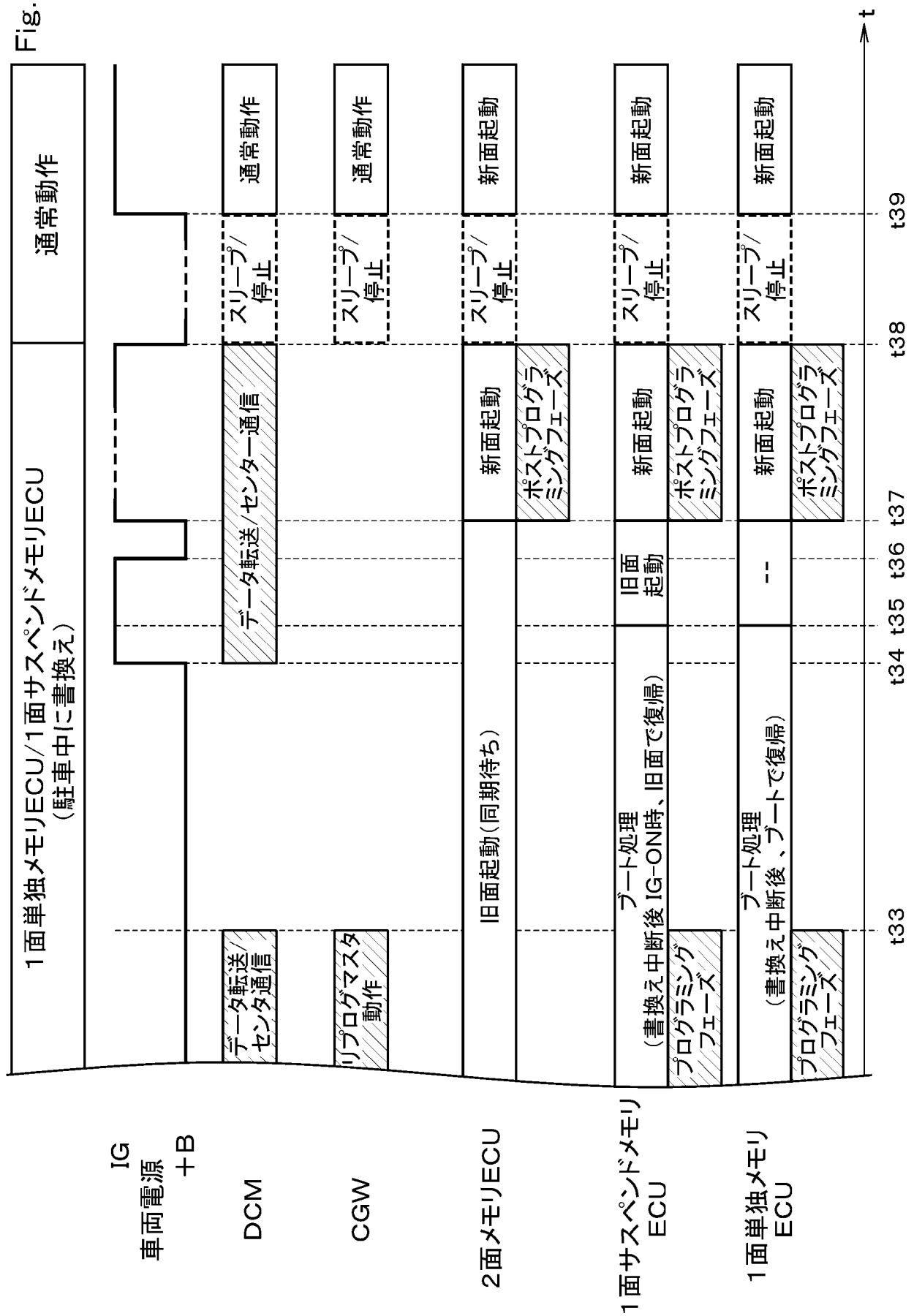
[図28]

Fig. 28


通常動作
DL状態
2面メモリECU
(IG ON中に書換え)
IG
車両電源
+B
DCM
CGW
2面メモリECU
1面サスペンドメモリ
ECU
1面単独メモリ
ECU
通常
動作
DL
動作
通常
動作
データ転送/
センター通信
リプログマスタ
動作
通常動作
プログラミング
フェーズ
通常動作
通常動作
データ転送/
センター通信
リプログマスタ
動作
プログラミング
フェーズ
t
t21
t22
t23
t24
t25
t26
t27
t28
t29
t30
t31
t32

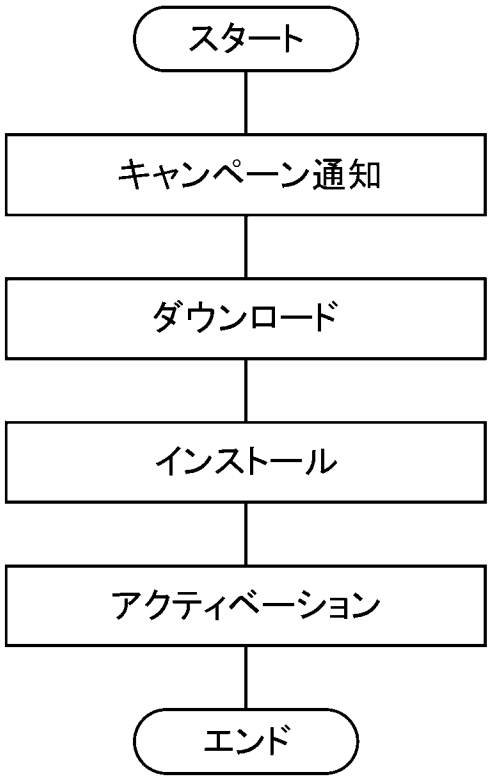
[図29]

Fig. 29


IG
車両電源
+B
DCM
CGW
2面メモリECU
1面サスペンドメモリ
ECU
1面単独メモリ
ECU
1面単独メモリECU/1面サスペンドメモリECU
(駐車中に書換え)
通常動作
データ転送/
センタ通信
リプログマスタ
動作
旧面起動(同期待ち)
ブート処理
(書換え中断後IG-ON時、旧面で復帰)
プログラミング
フェーズ
ブート処理
(書換え中断後、ブートで復帰)
プログラミング
フェーズ
データ転送/センター通信
スリープ/
停止
通常動作
スリープ/
停止
新面起動
ポストプログラ
ミングフェーズ
スリープ/
停止
旧面
起動
新面起動
ポストプログラ
ミングフェーズ
スリープ/
停止
--
新面起動
ポストプログラ
ミングフェーズ
スリープ/
停止
新面起動
t
t33
t34
t35
t36
t37
t38
t39

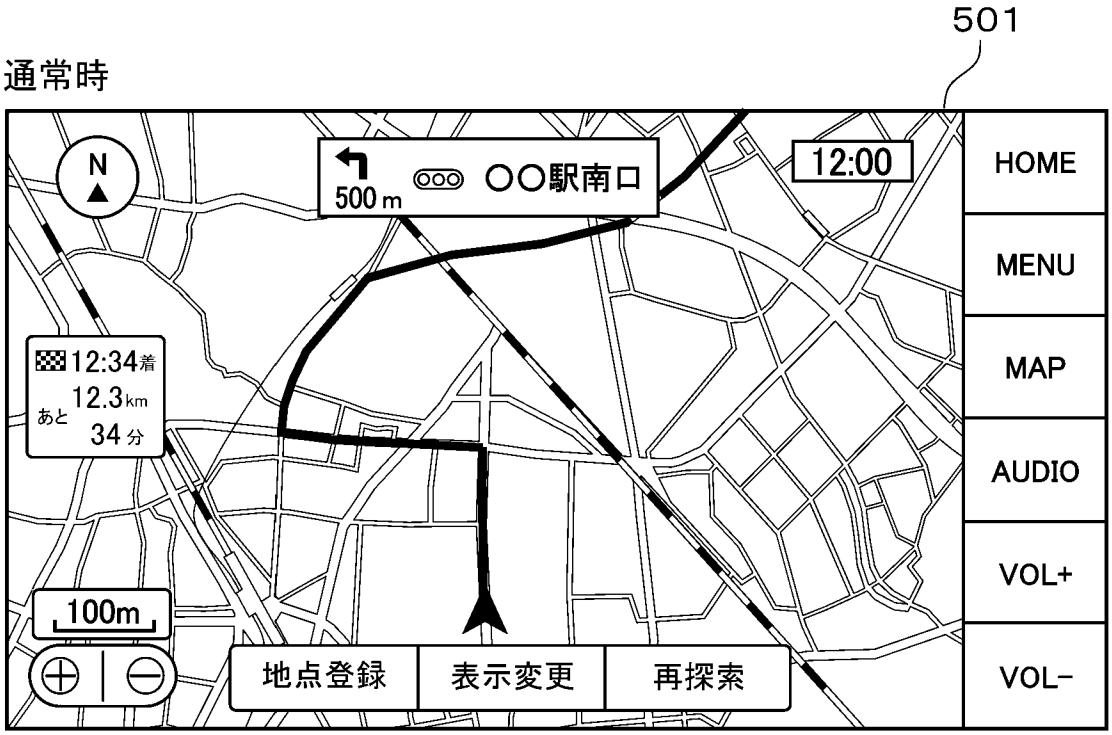
[図30]

Fig. 30



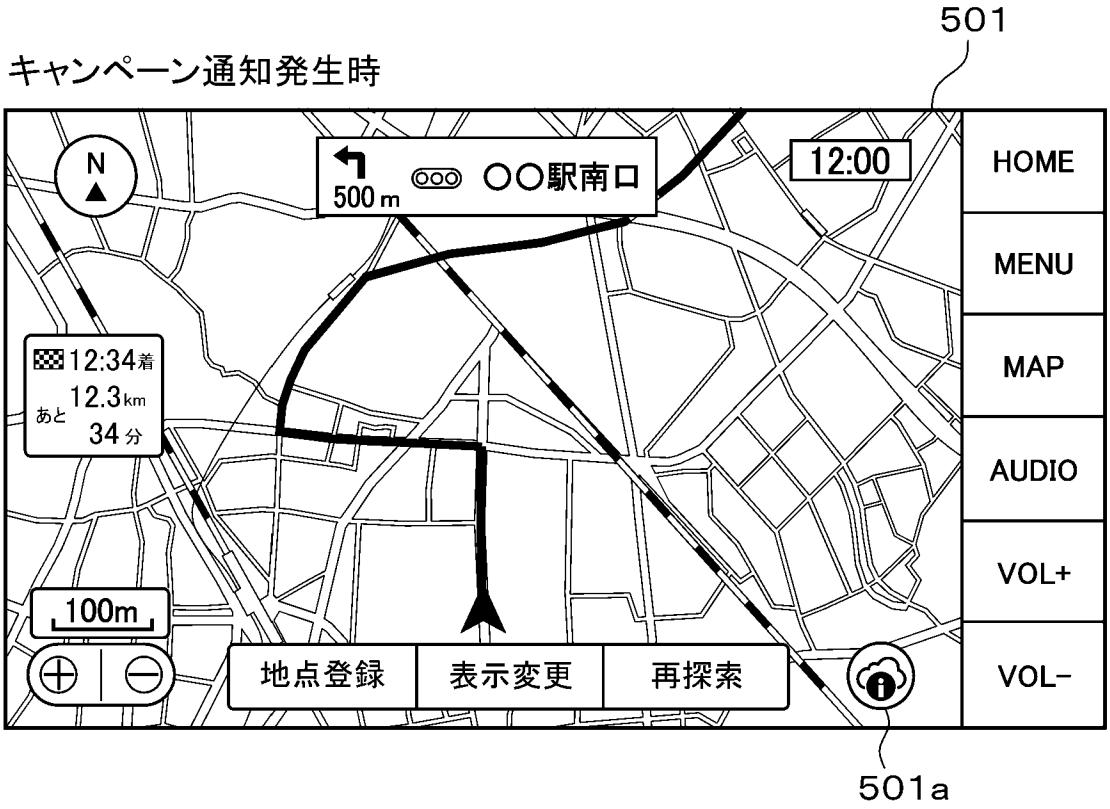
[図31]

Fig. 31


501
通常時
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34着
あと
12.3km
34分
100m
地点登録
表示変更
再探索

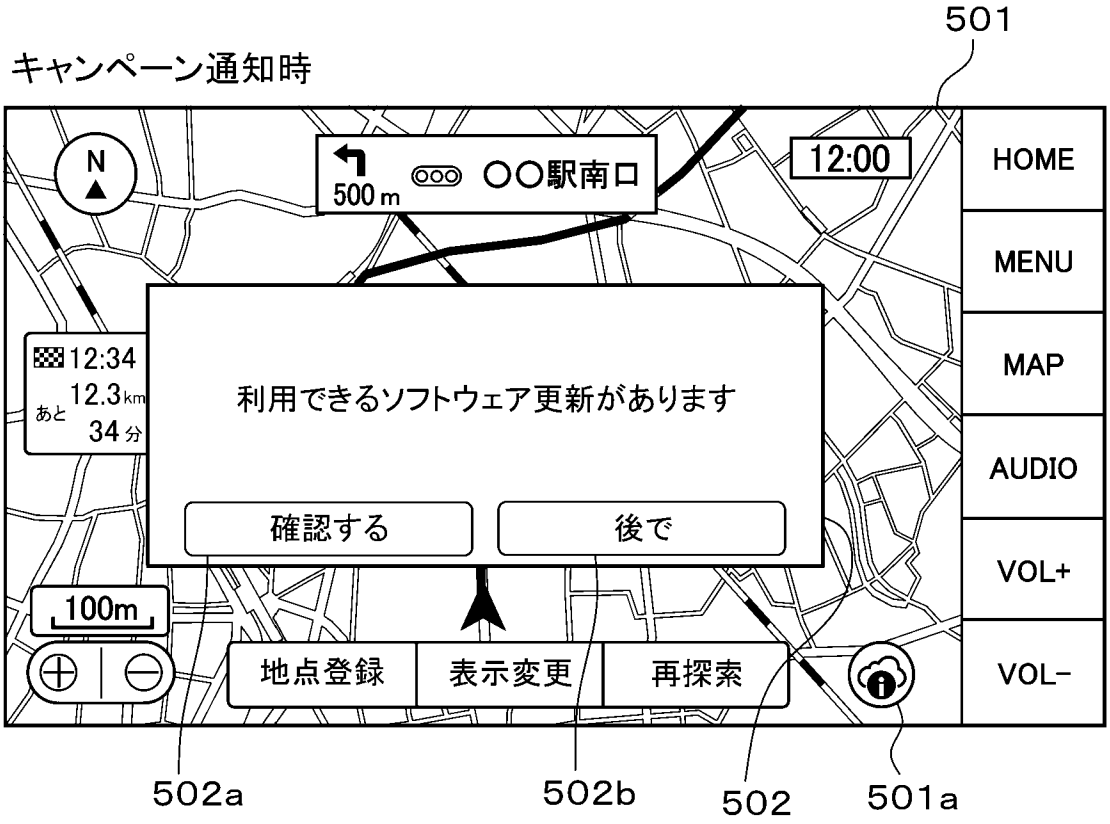
[図32]

Fig. 32


501
キャンペーン通知発生時
N
500m
○○駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34着
あと 12.3km
34分
100m
地点登録
表示変更
再探索
501a

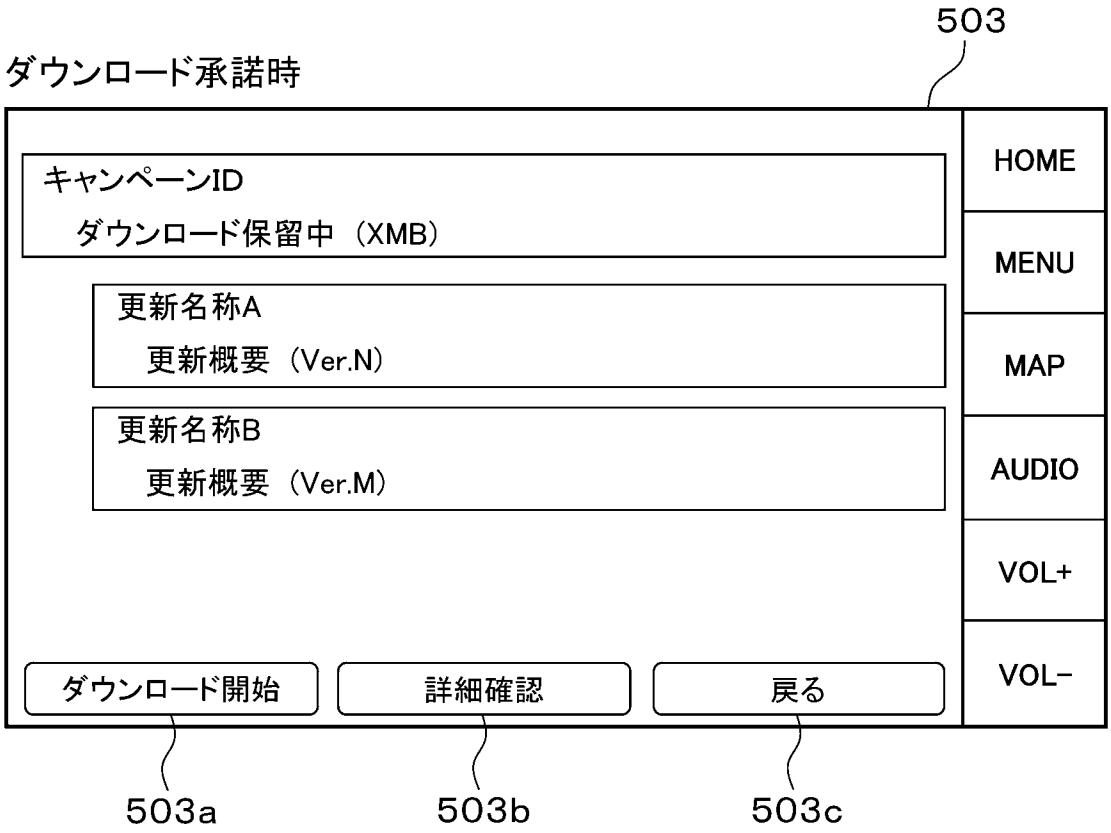
[図33]

Fig. 33


501
キャンペーン通知時
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34
あと 12.3km
34 分
利用できるソフトウェア更新があります
確認する
後で
100m
地点登録
表示変更
再探索
502a
502b
502
501a

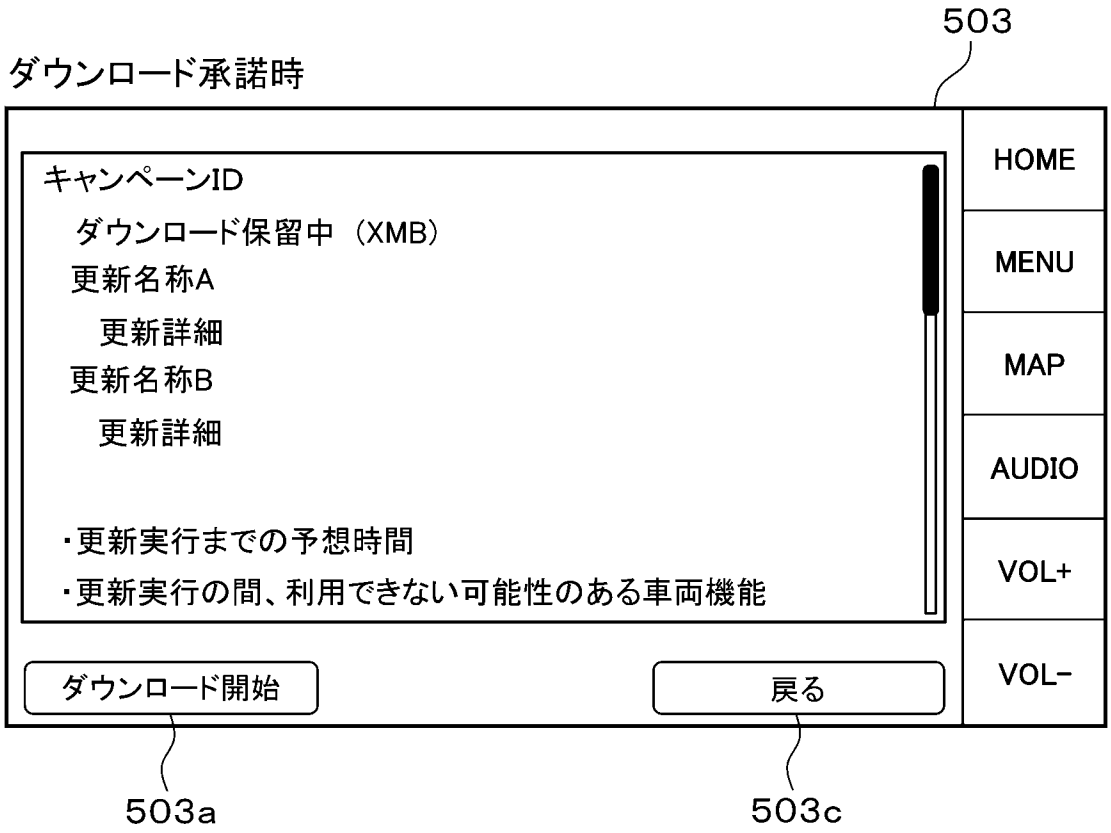
[図34]

Fig. 34


503
ダウンロード承諾時
キャンペーンID
ダウンロード保留中（XMB）
更新名称A
更新概要（Ver.N）
更新名称B
更新概要（Ver.M）
HOME
MENU
MAP
AUDIO
VOL+
VOL−
ダウンロード開始
詳細確認
戻る
503a
503b
503c

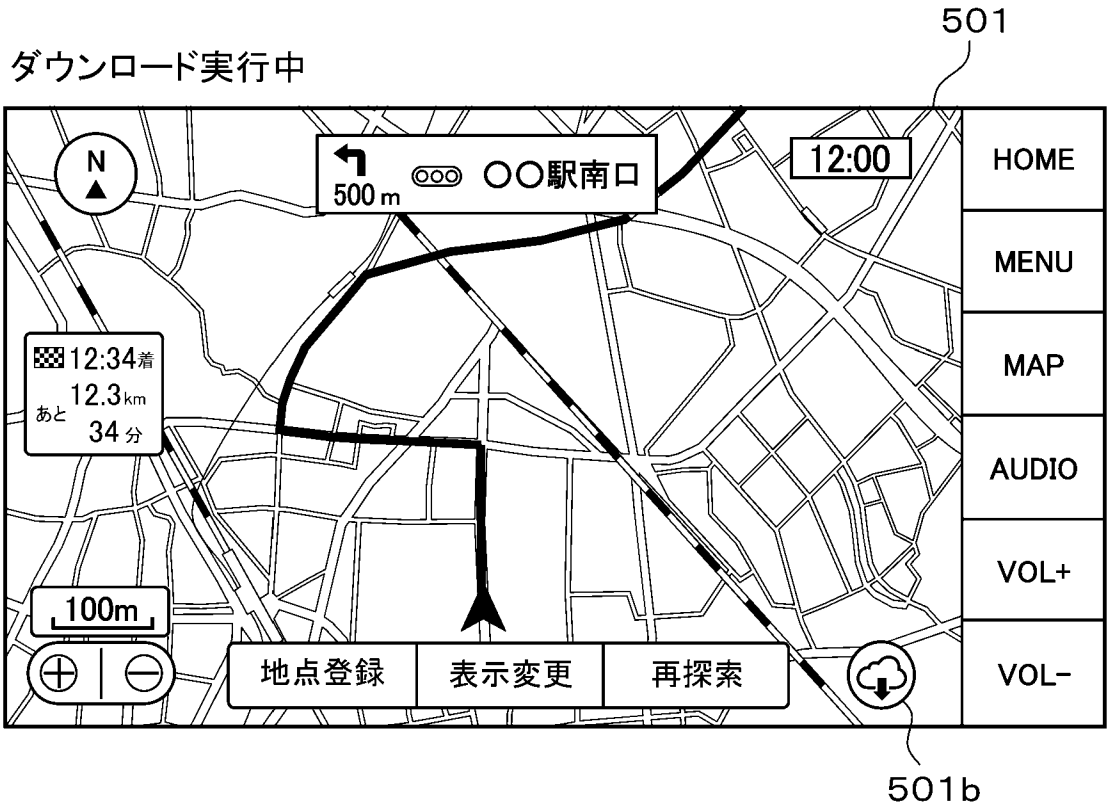
[図35]

Fig. 35


503
ダウンロード承諾時
キャンペーンID
ダウンロード保留中（XMB）
更新名称A
更新詳細
更新名称B
更新詳細
・更新実行までの予想時間
・更新実行の間、利用できない可能性のある車両機能
HOME
MENU
MAP
AUDIO
VOL+
VOL−
ダウンロード開始
戻る
503a
503c

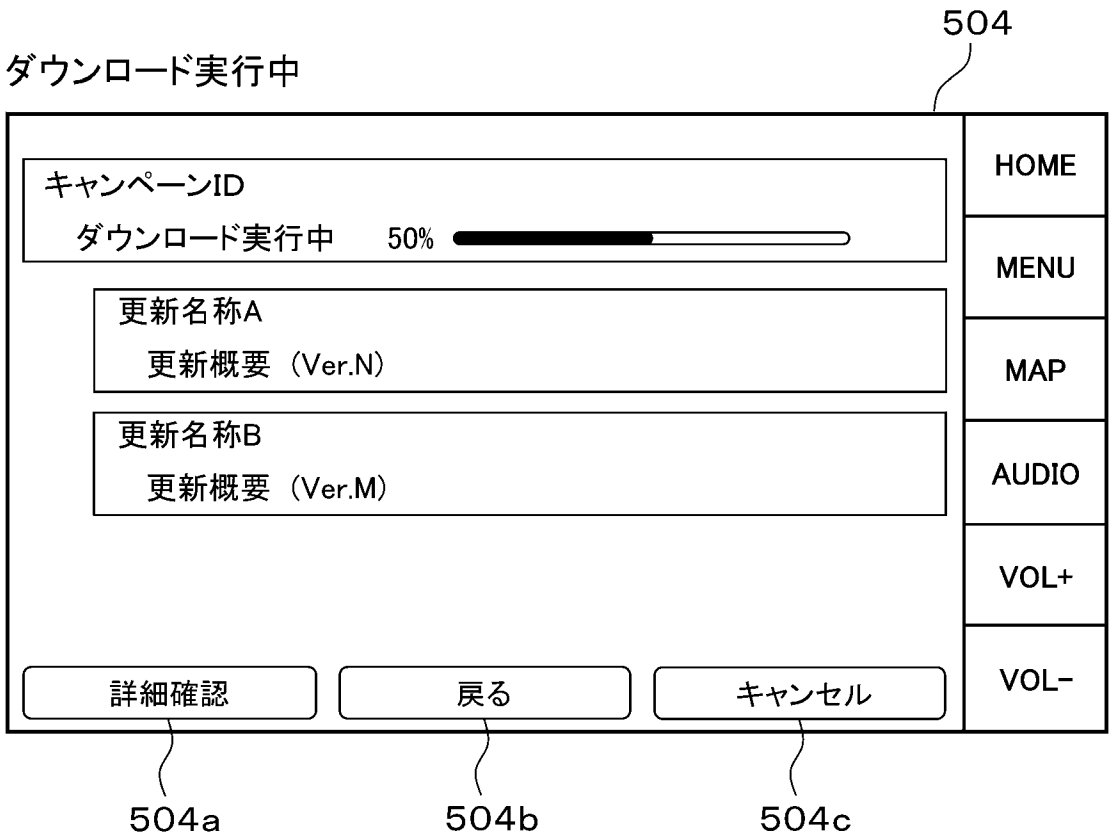
[図36]

Fig. 36


501
ダウンロード実行中
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34着
あと 12.3km
34 分
100m
地点登録
表示変更
再探索
501b

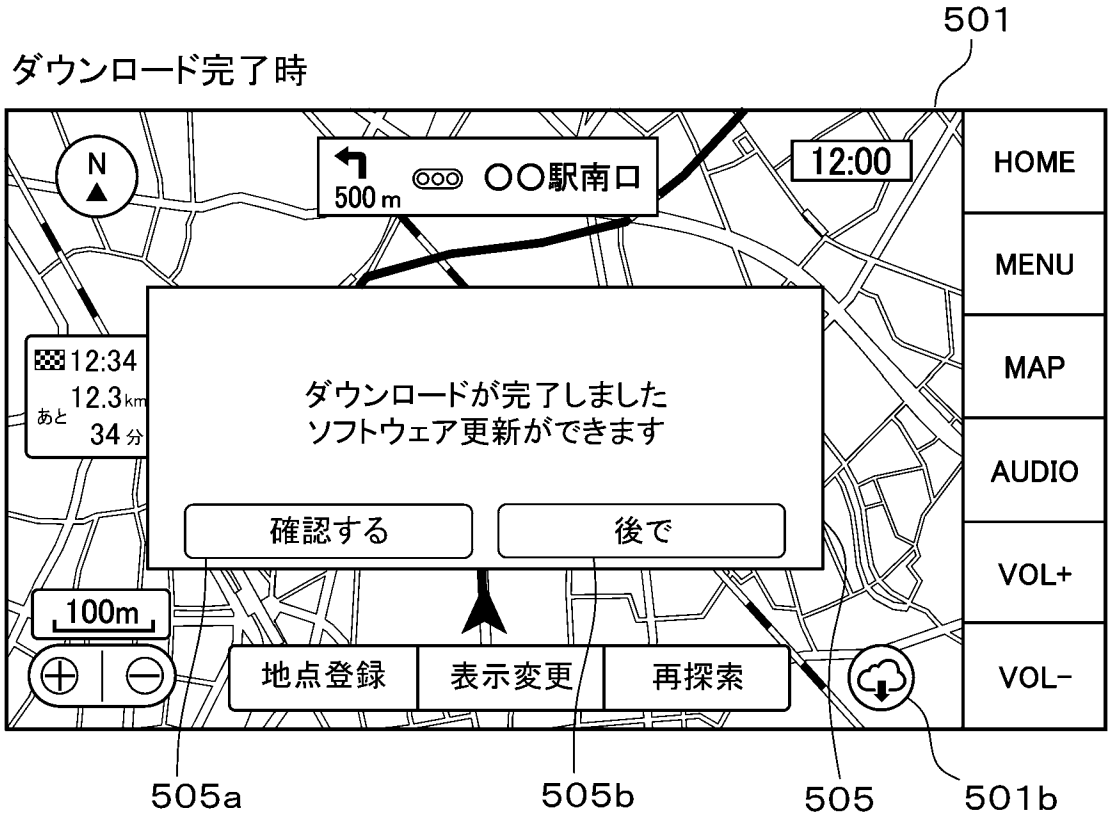
[図37]

Fig. 37


504
ダウンロード実行中
キャンペーンID
ダウンロード実行中 50%
更新名称A
更新概要 (Ver.N)
更新名称B
更新概要 (Ver.M)
HOME
MENU
MAP
AUDIO
VOL+
VOL−
詳細確認
戻る
キャンセル
504a
504b
504c

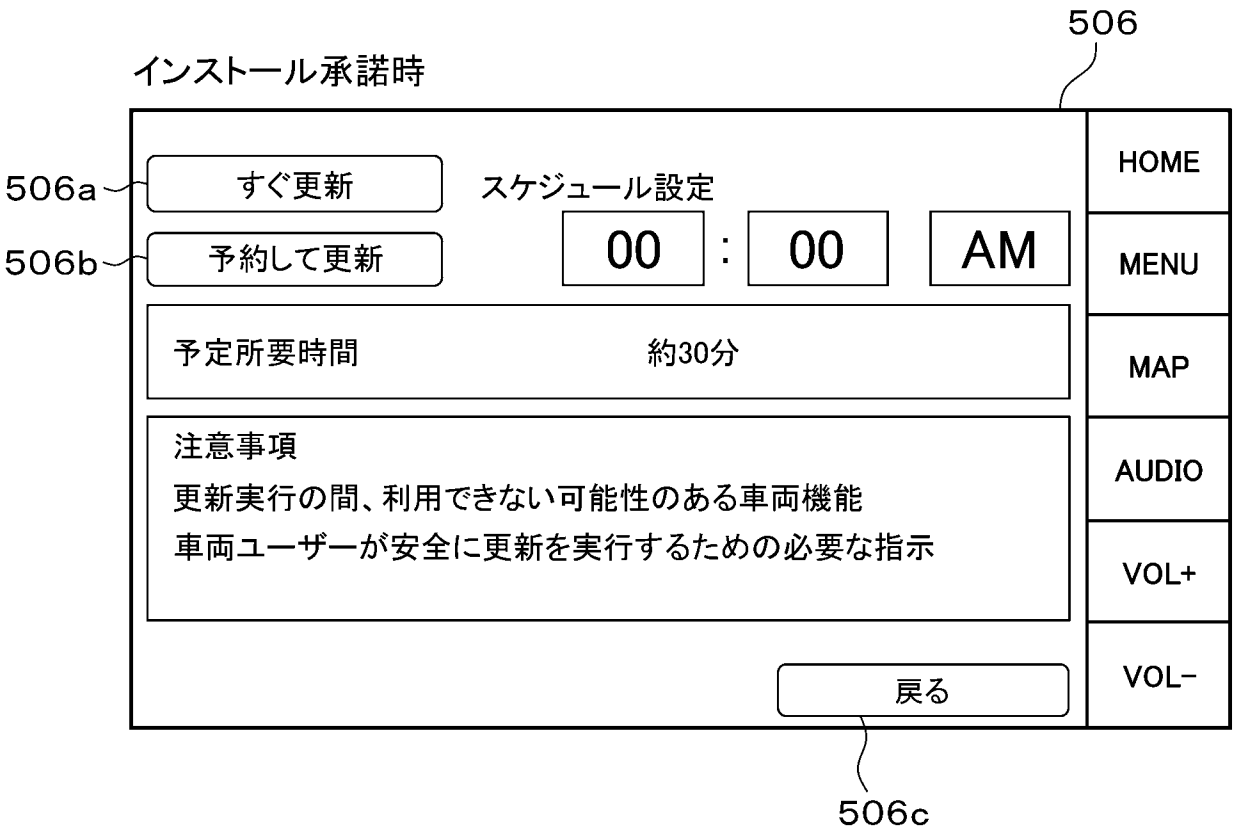
[図38]

Fig. 38


501
ダウンロード完了時
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34
12.3km
あと
34 分
ダウンロードが完了しました
ソフトウェア更新ができます
確認する
後で
100m
地点登録
表示変更
再探索
505a
505b
505
501b

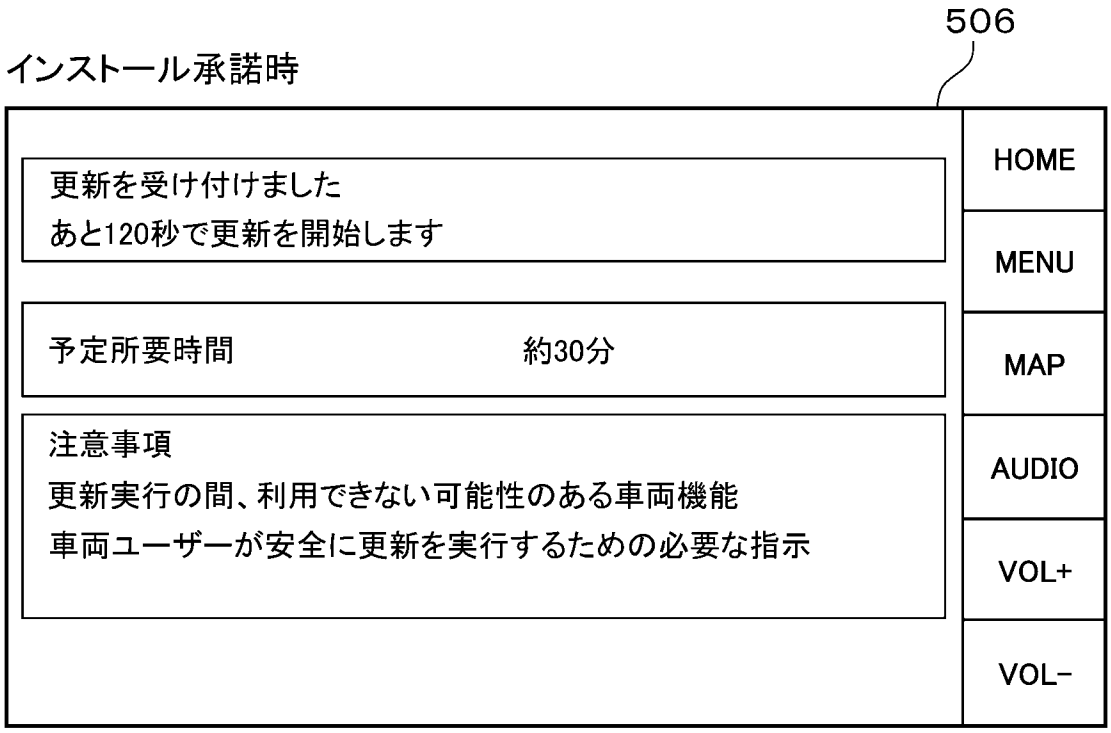
[図39]

Fig. 39


506
インストール承諾時
506a
すぐ更新
スケジュール設定
506b
予約して更新
00
:
00
AM
予定所要時間
約30分
注意事項
更新実行の間、利用できない可能性のある車両機能
車両ユーザーが安全に更新を実行するための必要な指示
戻る
506c
HOME
MENU
MAP
AUDIO
VOL+
VOL−

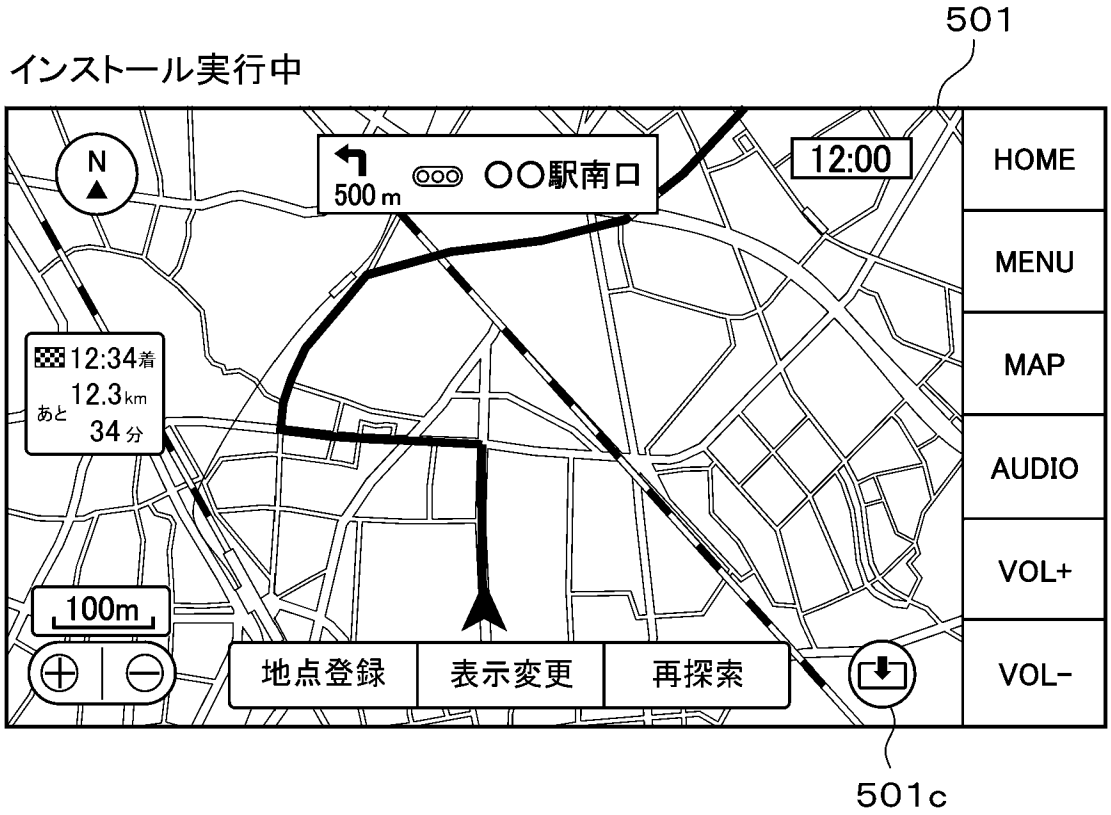
[図40]

Fig. 40


506
インストール承諾時
更新を受け付けました
あと120秒で更新を開始します
予定所要時間 約30分
注意事項
更新実行の間、利用できない可能性のある車両機能
車両ユーザーが安全に更新を実行するための必要な指示
HOME
MENU
MAP
AUDIO
VOL+
VOL-

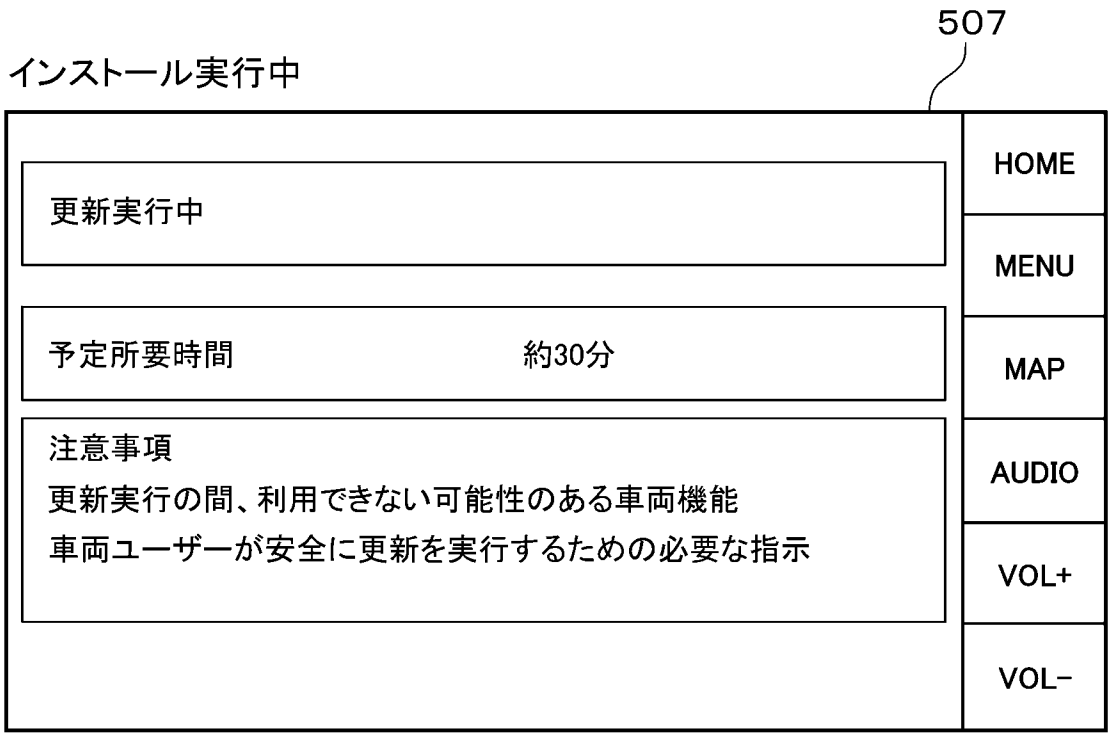
[図41]

Fig. 41


501
インストール実行中
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34着
あと 12.3km
34分
100m
地点登録
表示変更
再探索
501c

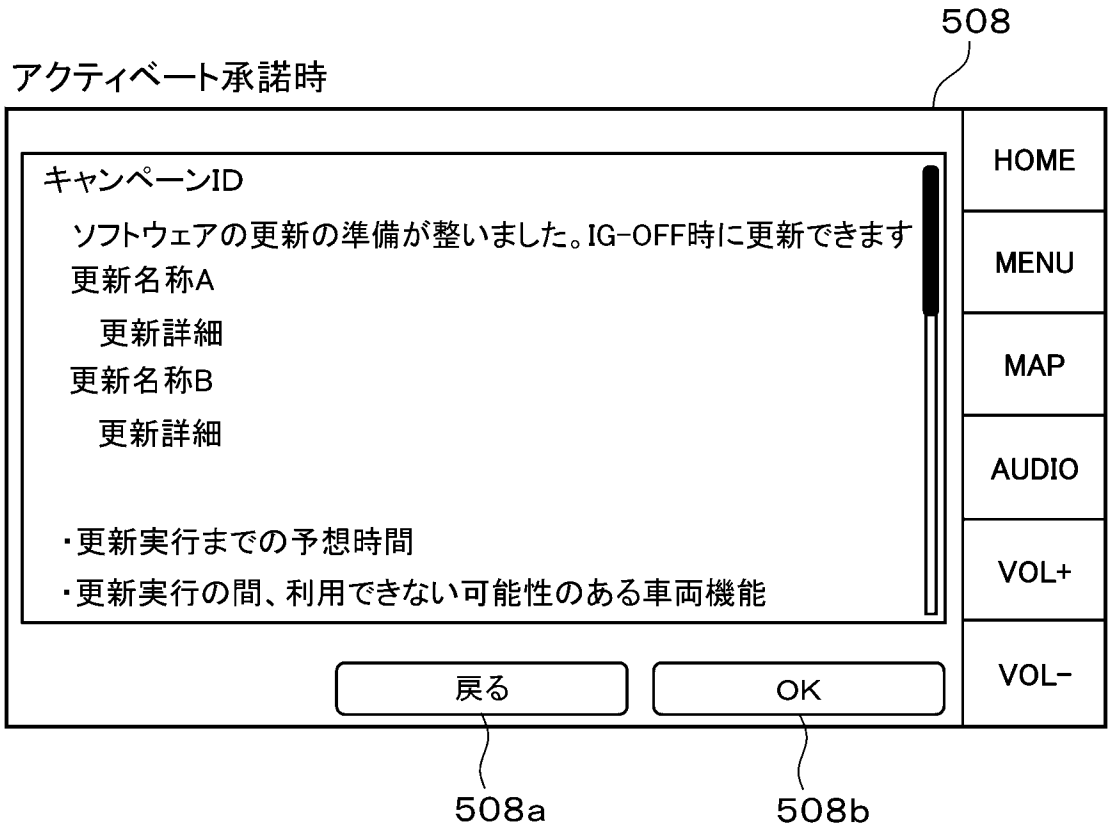
[図42]

Fig. 42


507
インストール実行中
更新実行中
予定所要時間
約30分
注意事項
更新実行の間、利用できない可能性のある車両機能
車両ユーザーが安全に更新を実行するための必要な指示
HOME
MENU
MAP
AUDIO
VOL+
VOL−

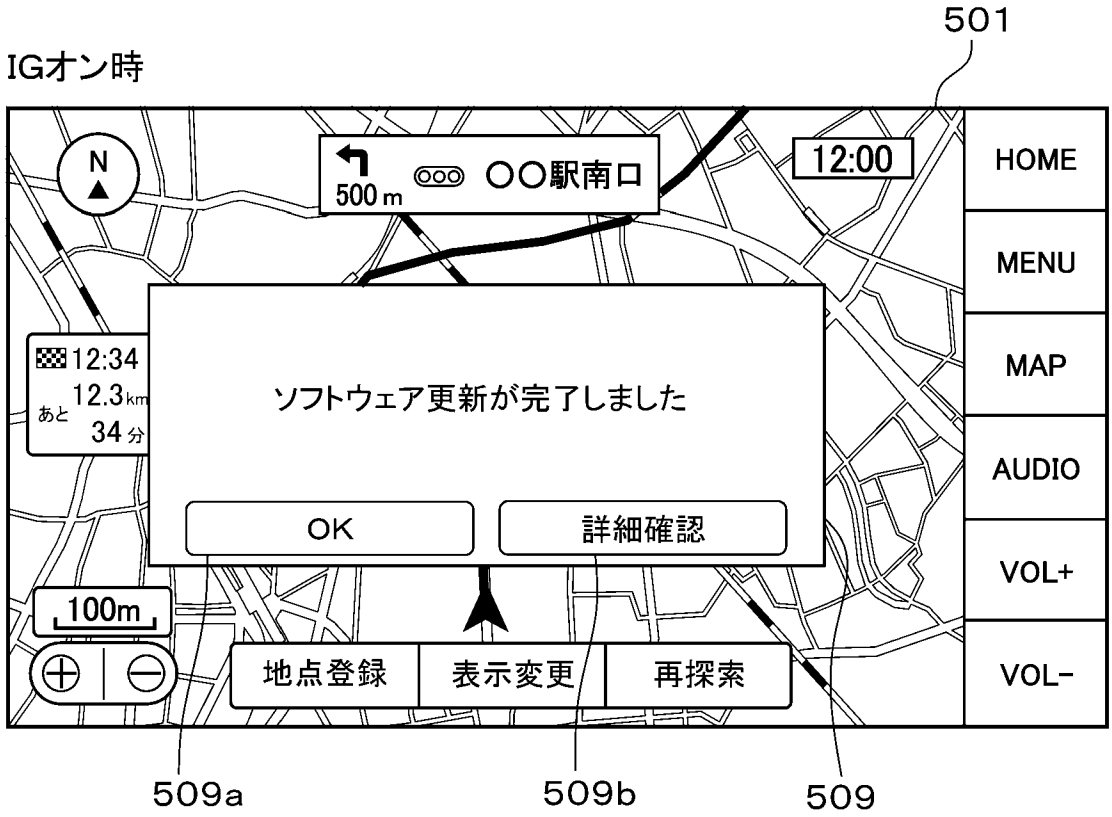
[図43]

Fig. 43


508
アクティベート承諾時
キャンペーンID
ソフトウェアの更新の準備が整いました。IG-OFF時に更新できます
更新名称A
更新詳細
更新名称B
更新詳細
・更新実行までの予想時間
・更新実行の間、利用できない可能性のある車両機能
戻る
OK
HOME
MENU
MAP
AUDIO
VOL+
VOL-
508a
508b

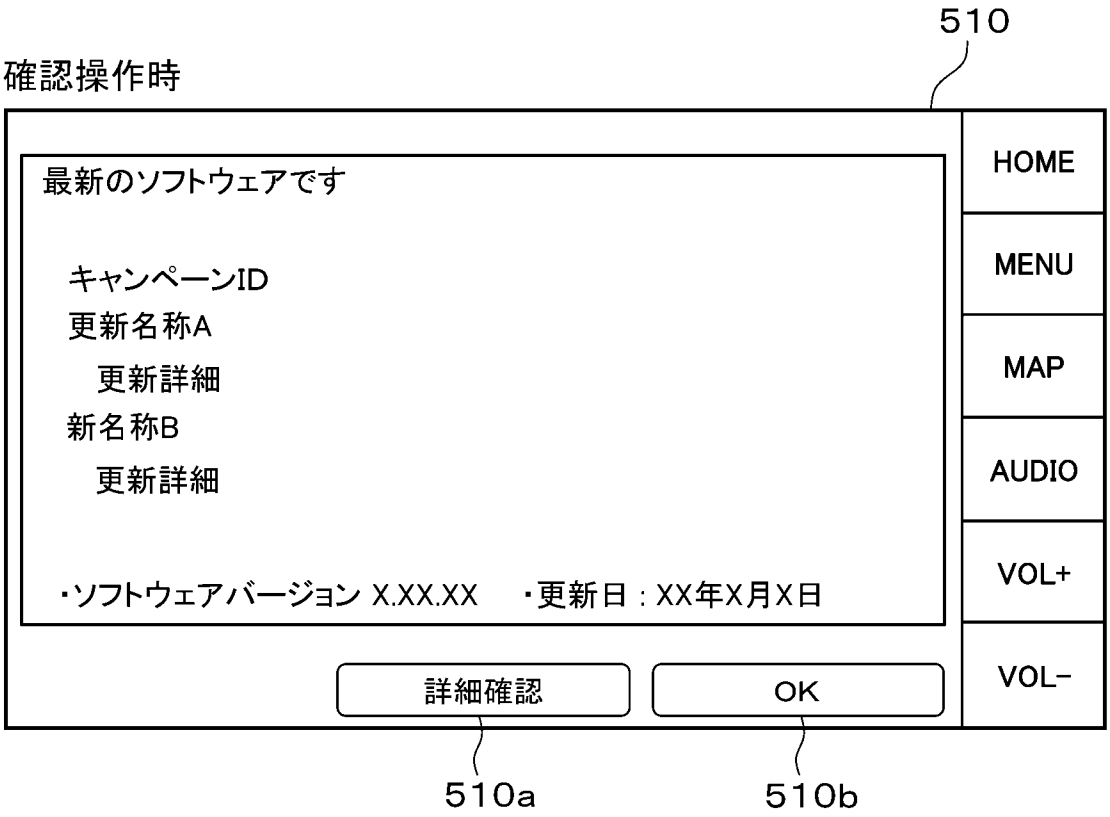
[図44]

Fig. 44


501
IGオン時
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34
あと 12.3km
34 分
ソフトウェア更新が完了しました
OK
詳細確認
100m
地点登録
表示変更
再探索
509a
509b
509

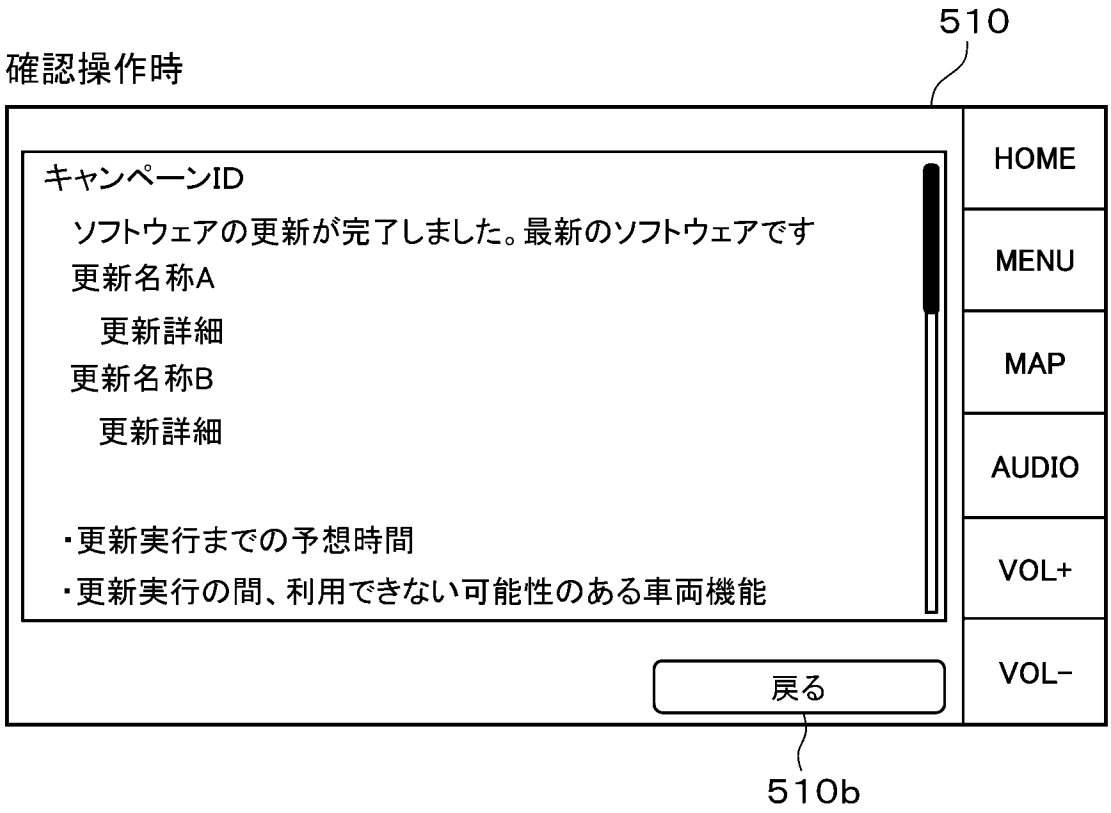
[図45]

Fig. 45


510
確認操作時
最新のソフトウェアです
キャンペーンID
更新名称A
更新詳細
新名称B
更新詳細
・ソフトウェアバージョン X.XX.XX
・更新日：XX年X月X日
詳細確認
OK
HOME
MENU
MAP
AUDIO
VOL+
VOL−
510a
510b

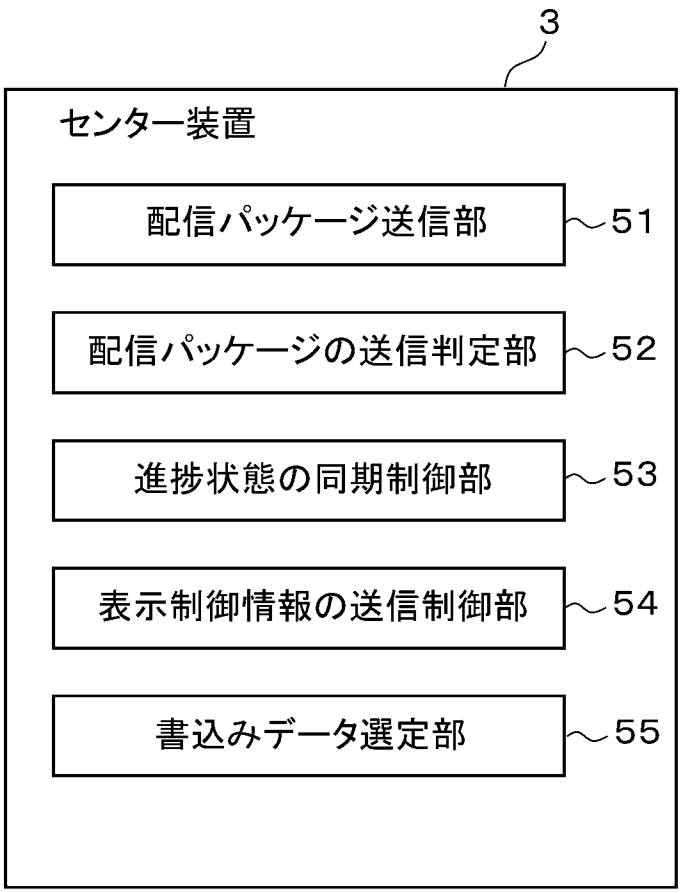
[図46]

Fig. 46


510
確認操作時
キャンペーンID
ソフトウェアの更新が完了しました。最新のソフトウェアです
更新名称A
更新詳細
更新名称B
更新詳細
・更新実行までの予想時間
・更新実行の間、利用できない可能性のある車両機能
戻る
HOME
MENU
MAP
AUDIO
VOL+
VOL−
510b

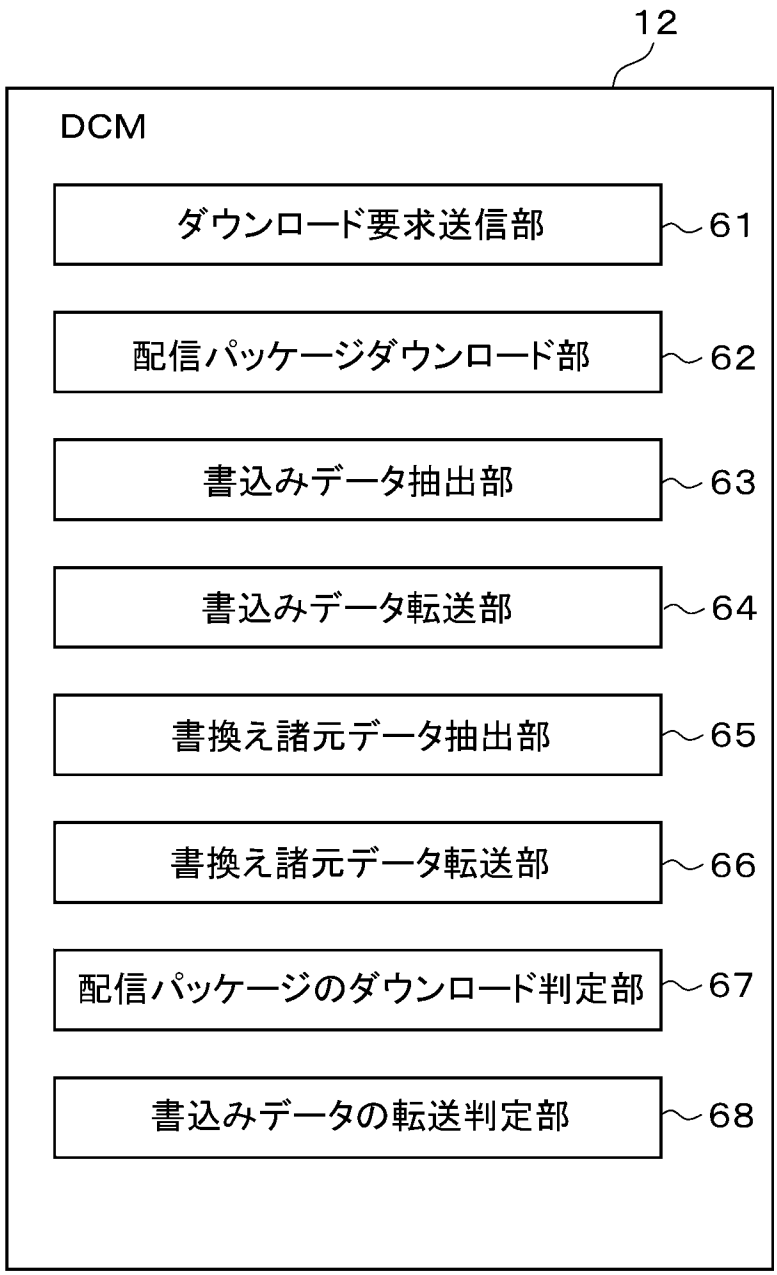
[図47]

Fig. 47


3
センター装置
配信パッケージ送信部
51
配信パッケージの送信判定部
52
進捗状態の同期制御部
53
表示制御情報の送信制御部
54
書込みデータ選定部
55

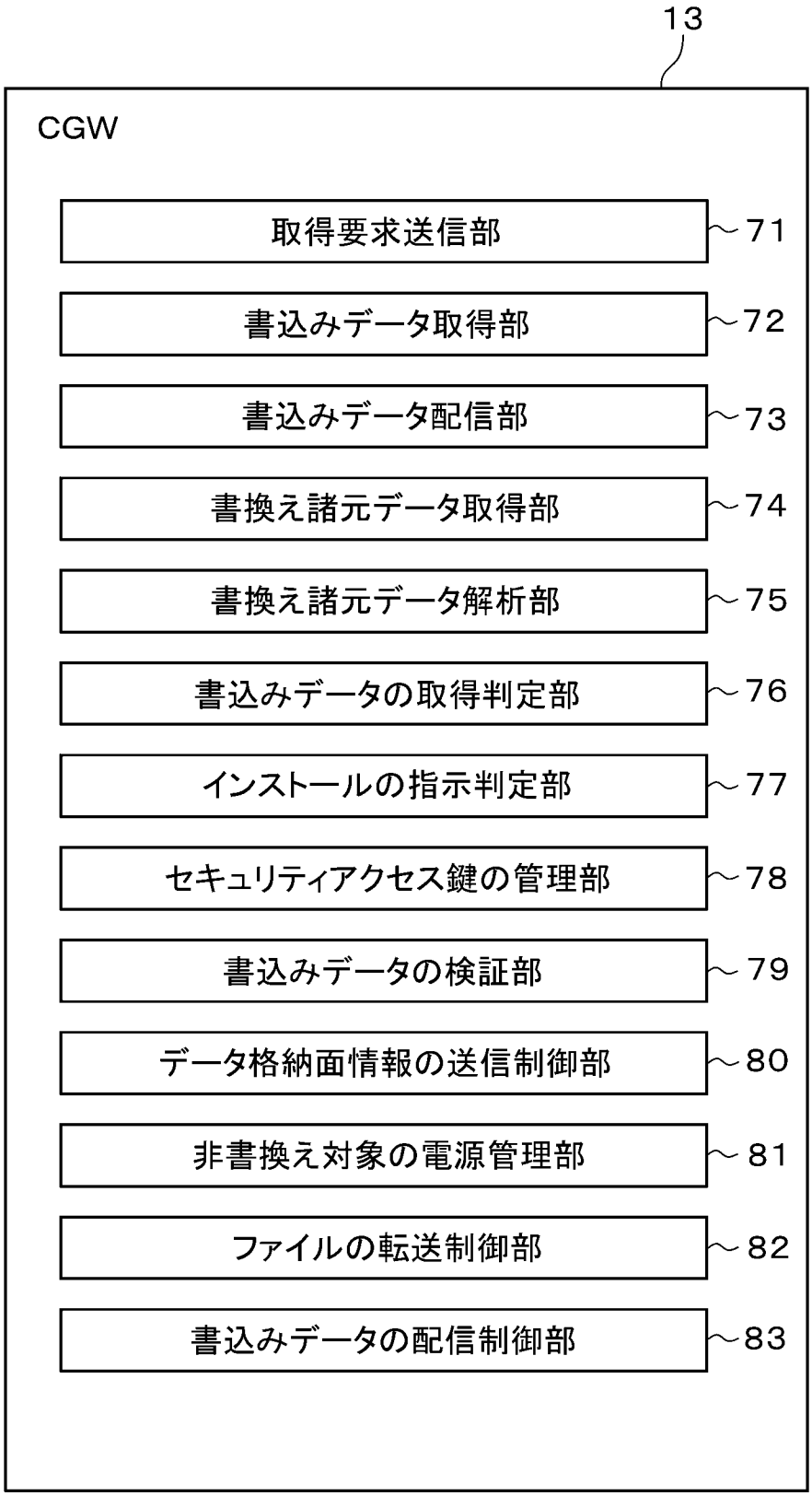
[図48]

Fig. 48


12
DCM
ダウンロード要求送信部
61
配信パッケージダウンロード部
62
書込みデータ抽出部
63
書込みデータ転送部
64
書換え諸元データ抽出部
65
書換え諸元データ転送部
66
配信パッケージのダウンロード判定部
67
書込みデータの転送判定部
68

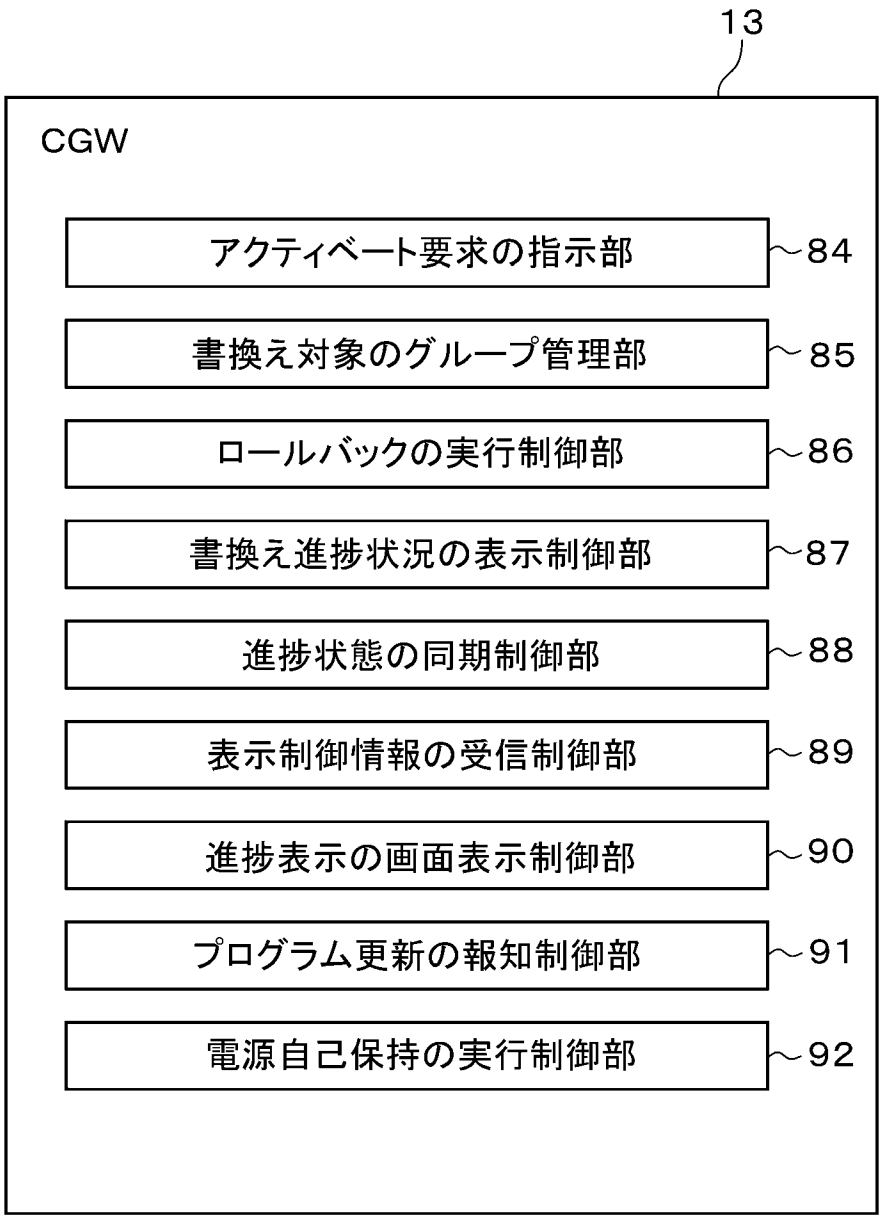
[図49]

Fig. 49


13
CGW
取得要求送信部
71
書込みデータ取得部
72
書込みデータ配信部
73
書換え諸元データ取得部
74
書換え諸元データ解析部
75
書込みデータの取得判定部
76
インストールの指示判定部
77
セキュリティアクセス鍵の管理部
78
書込みデータの検証部
79
データ格納面情報の送信制御部
80
非書換え対象の電源管理部
81
ファイルの転送制御部
82
書込みデータの配信制御部
83

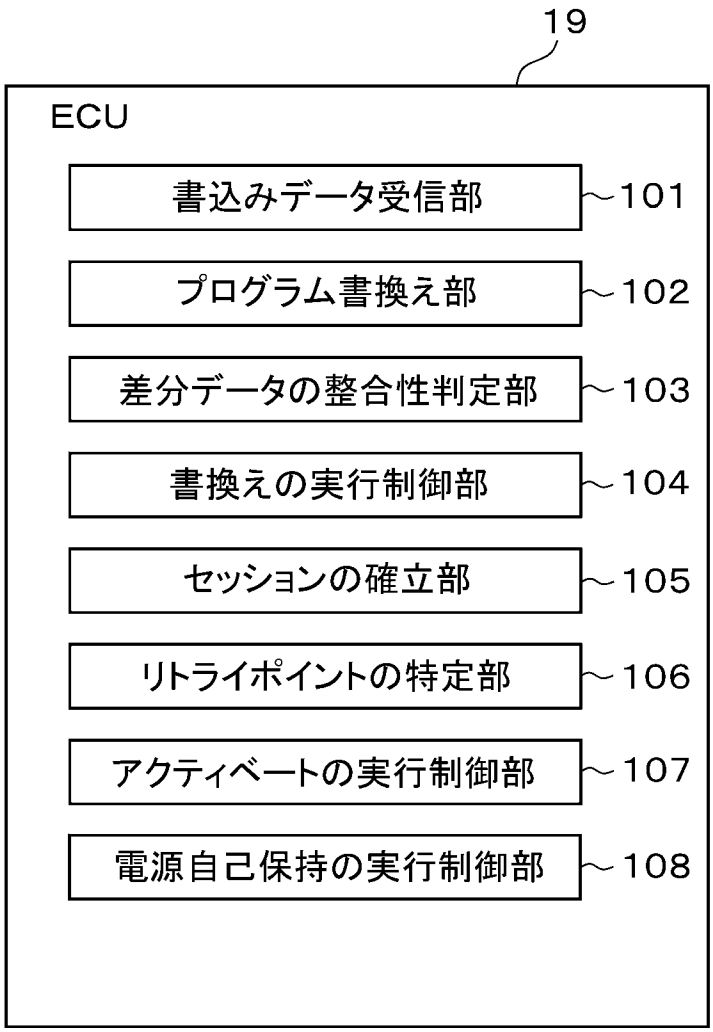
[図50]

Fig. 50


13
CGW
アクティベート要求の指示部
84
書換え対象のグループ管理部
85
ロールバックの実行制御部
86
書換え進捗状況の表示制御部
87
進捗状態の同期制御部
88
表示制御情報の受信制御部
89
進捗表示の画面表示制御部
90
プログラム更新の報知制御部
91
電源自己保持の実行制御部
92

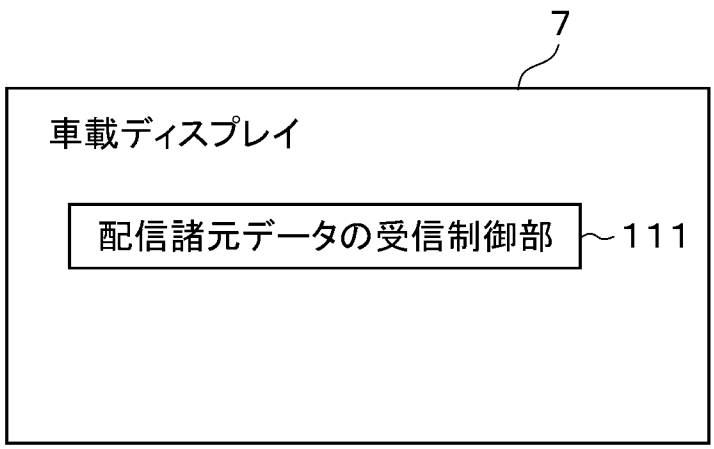
[図51]

Fig. 51



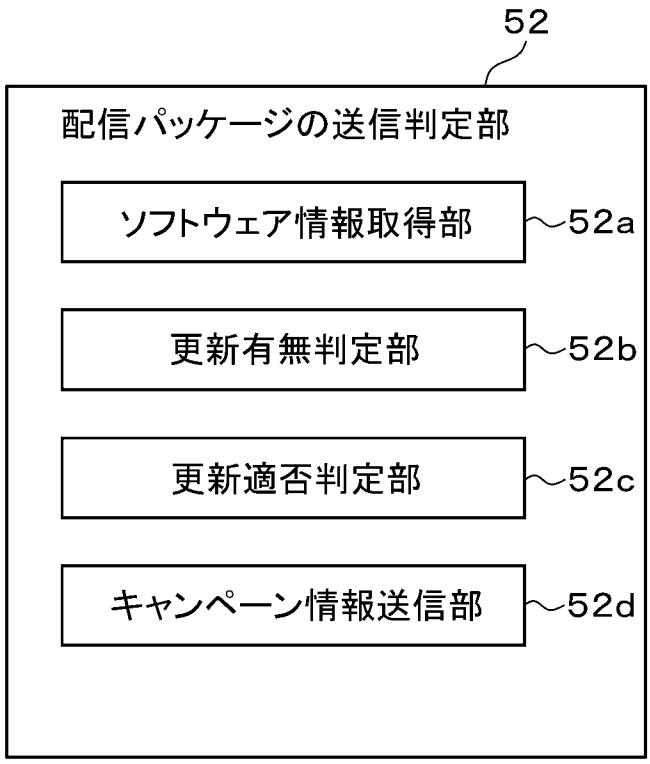
[図52]

Fig. 52



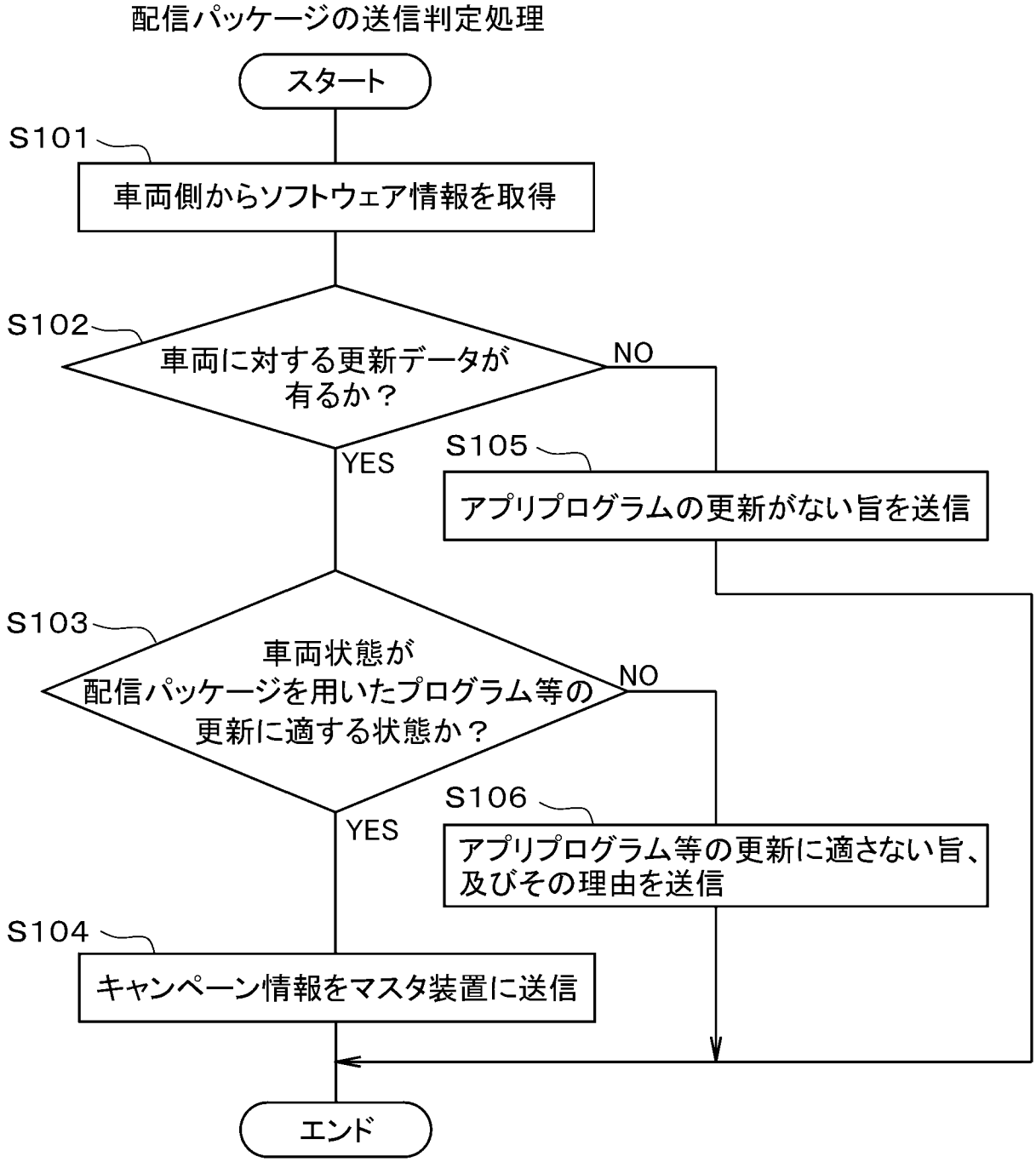
[図53]

Fig. 53


52
配信パッケージの送信判定部
ソフトウェア情報取得部
52a
更新有無判定部
52b
更新適否判定部
52c
キャンペーン情報送信部
52d

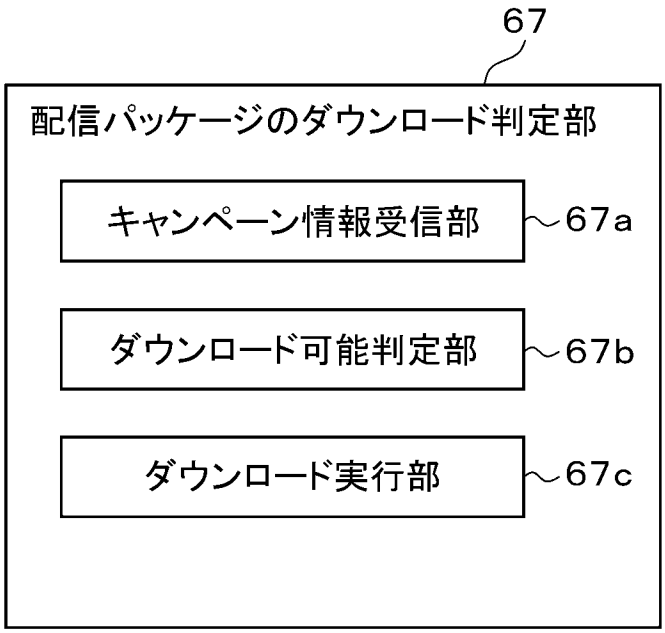
[図54]

Fig. 54


配信パッケージの送信判定処理
スタート
S101
車両側からソフトウェア情報を取得
S102
車両に対する更新データが有るか？
NO
YES
S105
アプリプログラムの更新がない旨を送信
S103
車両状態が配信パッケージを用いたプログラム等の更新に適する状態か？
NO
YES
S106
アプリプログラム等の更新に適さない旨、及びその理由を送信
S104
キャンペーン情報をマスタ装置に送信
エンド

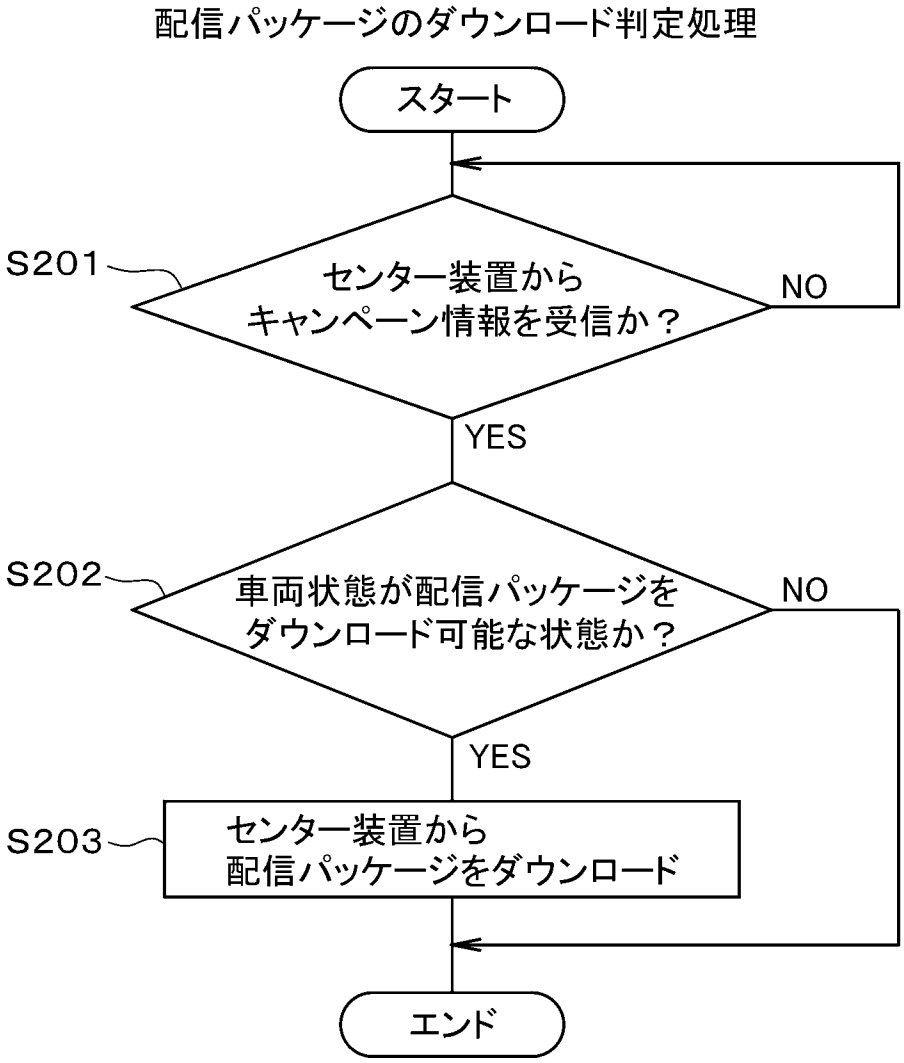
[図55]

Fig. 55


67
配信パッケージのダウンロード判定部
キャンペーン情報受信部
67a
ダウンロード可能判定部
67b
ダウンロード実行部
67c

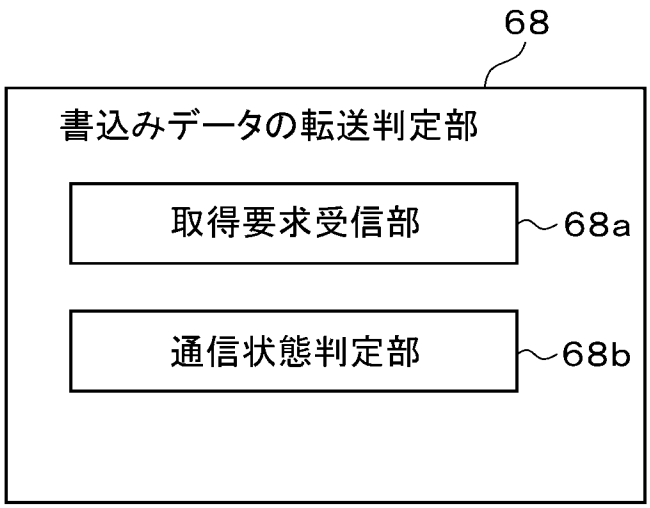
[図56]

Fig. 56



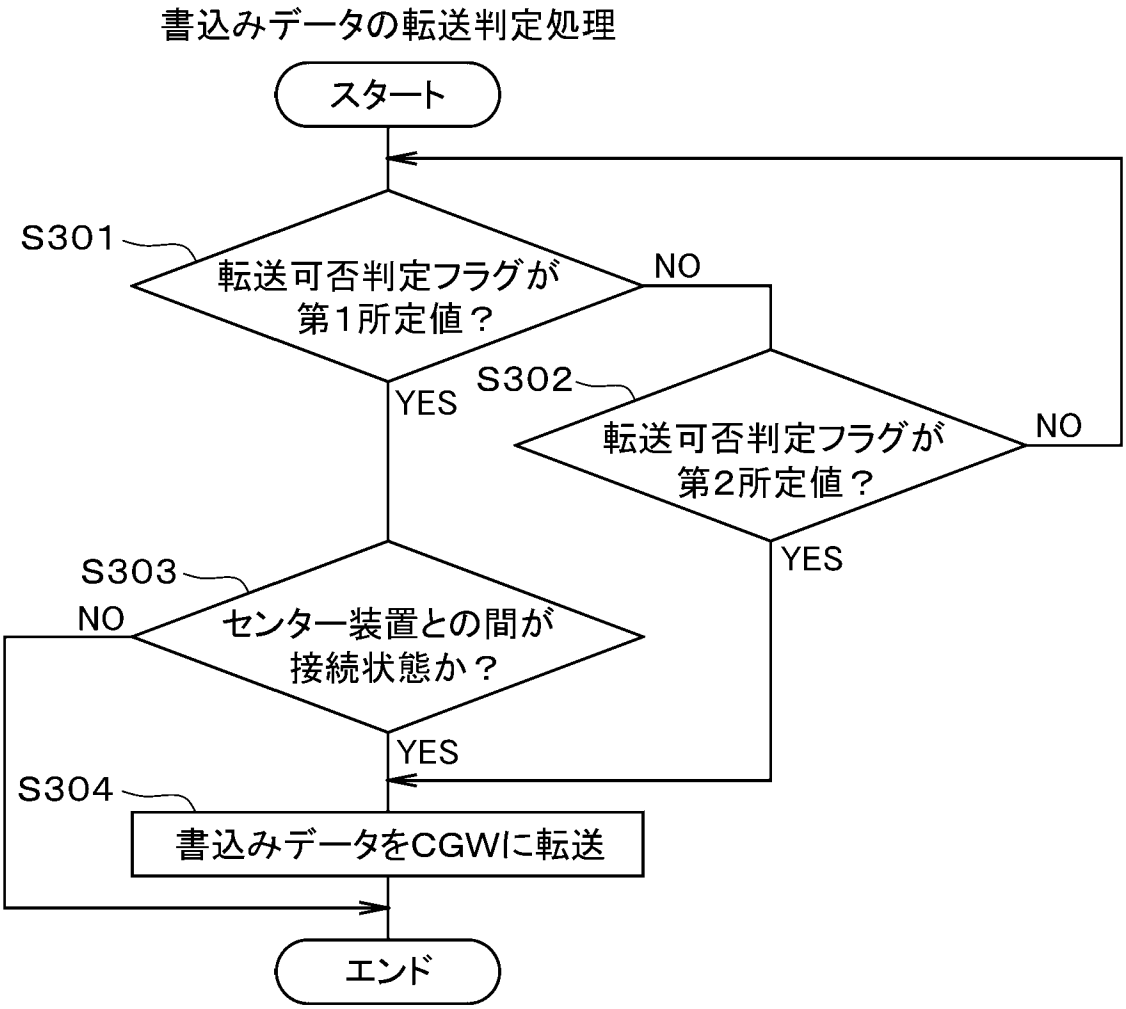
[図57]

Fig. 57



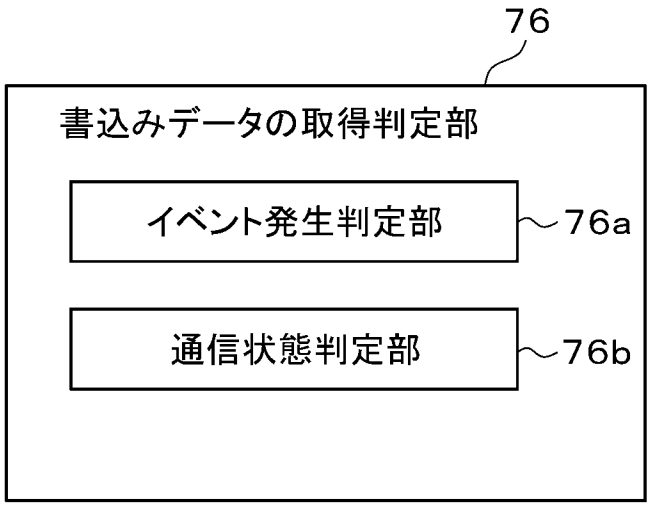
[図58]

Fig. 58



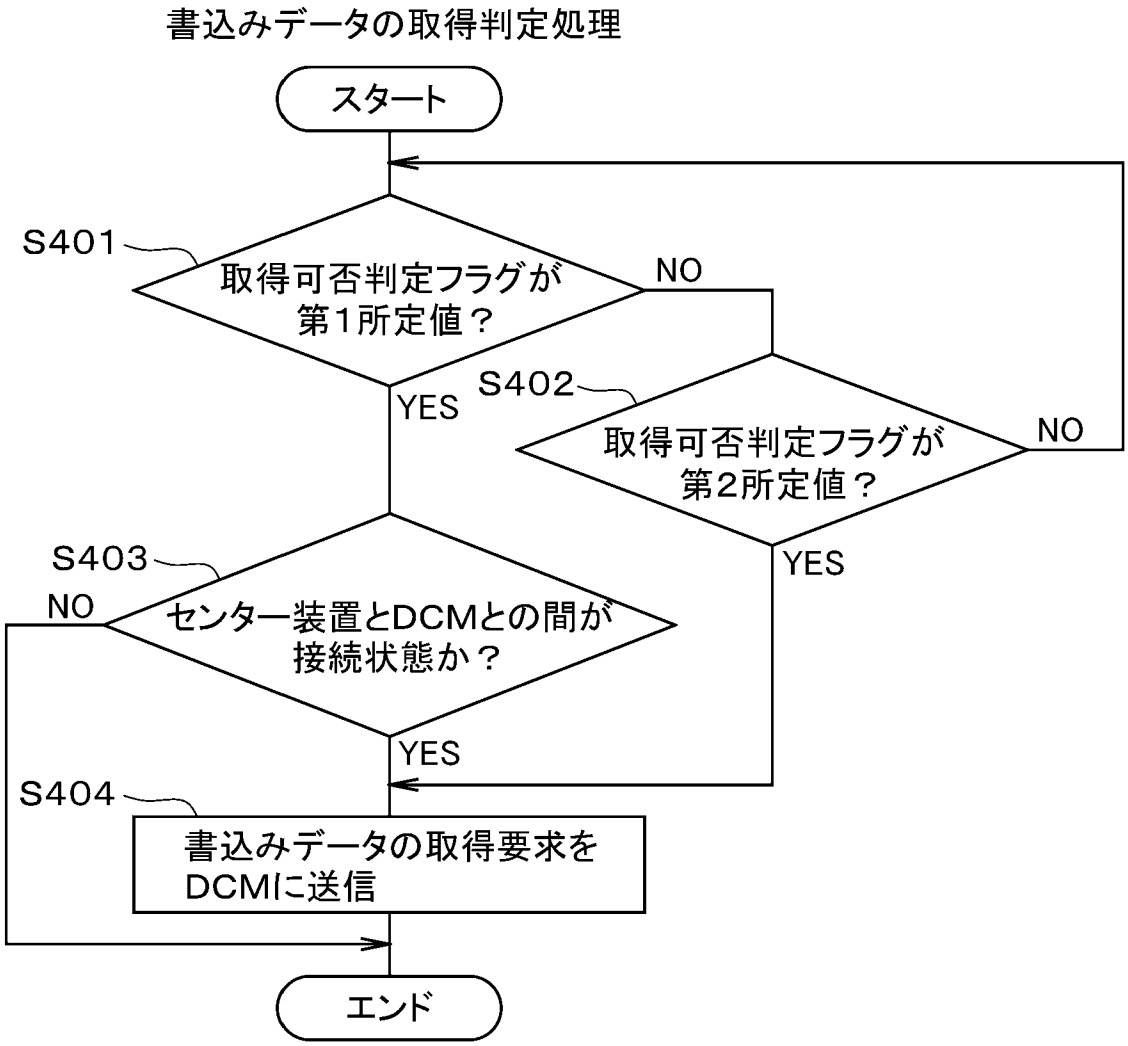
[図59]

Fig. 59



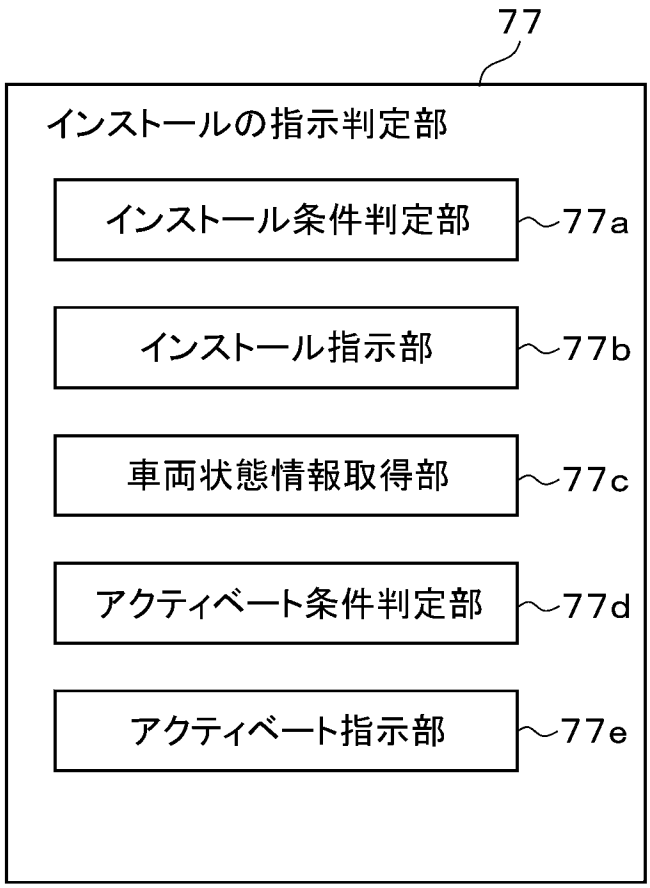
[図60]

Fig. 60


書込みデータの取得判定処理
スタート
S401
取得可否判定フラグが
第1所定値？
NO
YES
S402
取得可否判定フラグが
第2所定値？
NO
YES
S403
センター装置とDCMとの間が
接続状態か？
NO
YES
S404
書込みデータの取得要求を
DCMに送信
エンド

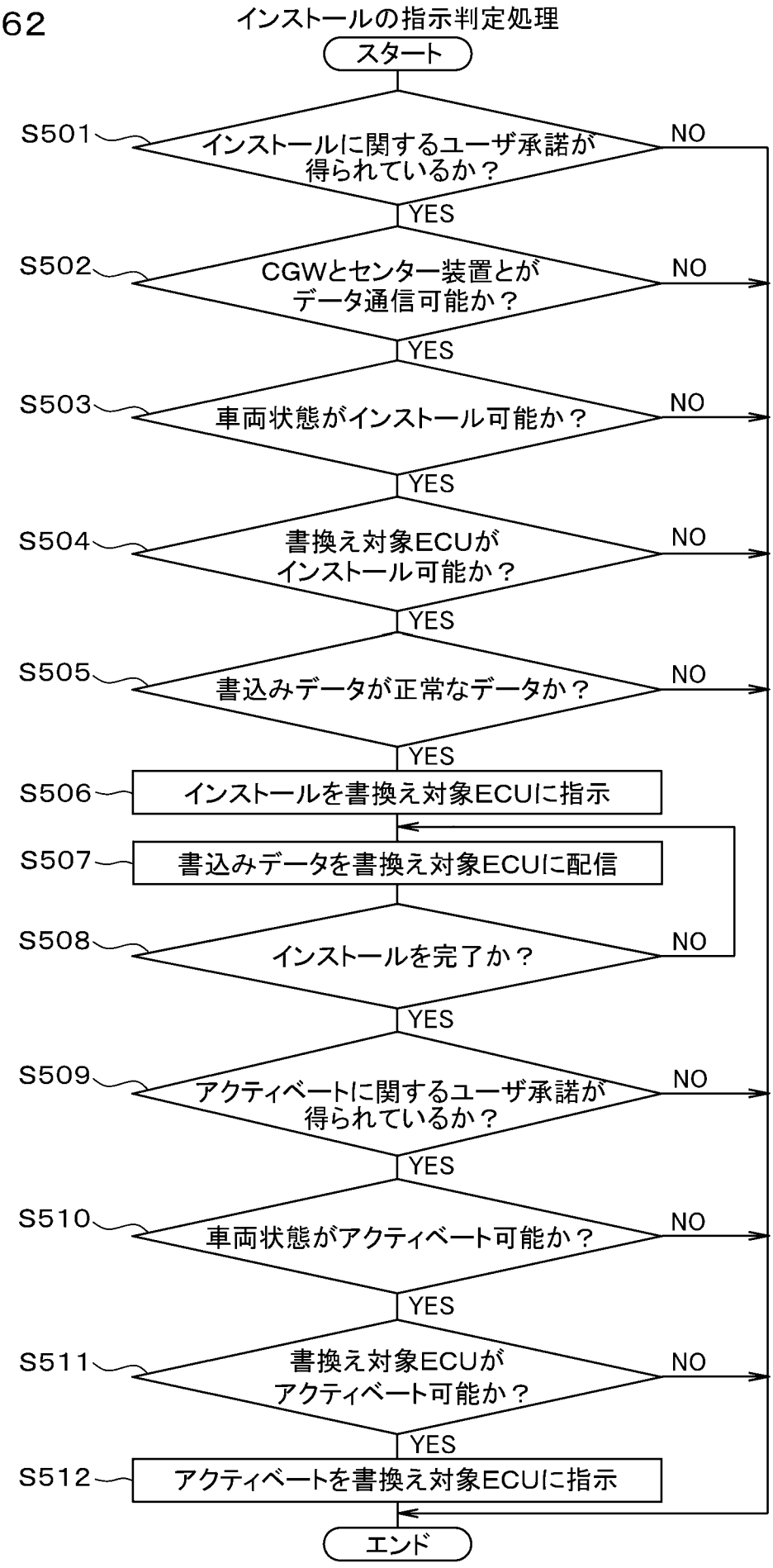
[図61]

Fig. 61


77
インストールの指示判定部
インストール条件判定部
77a
インストール指示部
77b
車両状態情報取得部
77c
アクティベート条件判定部
77d
アクティベート指示部
77e

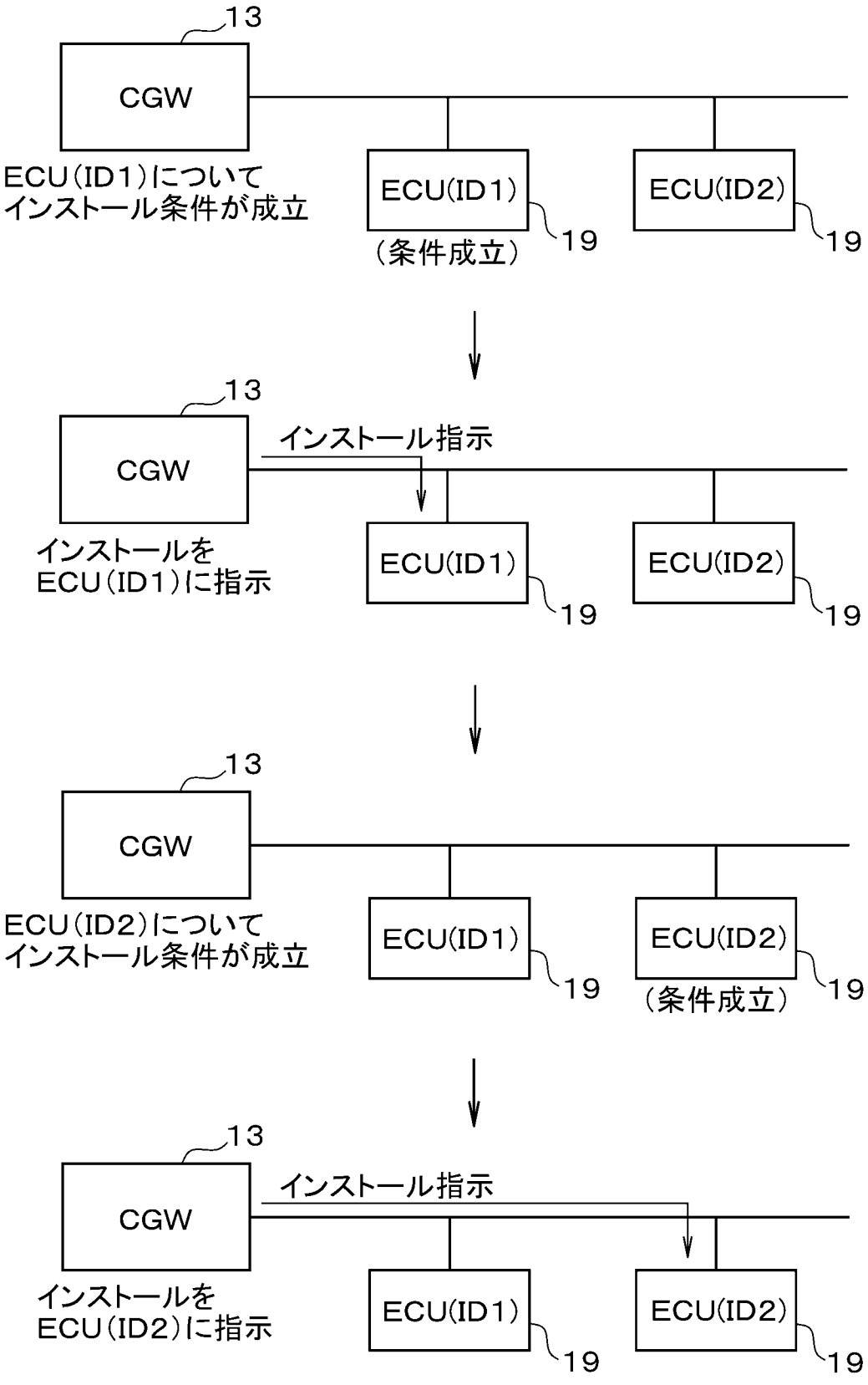
[図62]

Fig. 62


インストールの指示判定処理
スタート
S501
インストールに関するユーザ承諾が得られているか？
NO
YES
S502
CGWとセンター装置とがデータ通信可能か？
NO
YES
S503
車両状態がインストール可能か？
NO
YES
S504
書換え対象ECUがインストール可能か？
NO
YES
S505
書込みデータが正常なデータか？
NO
YES
S506
インストールを書換え対象ECUに指示
S507
書込みデータを書換え対象ECUに配信
S508
インストールを完了か？
NO
YES
S509
アクティベートに関するユーザ承諾が得られているか？
NO
YES
S510
車両状態がアクティベート可能か？
NO
YES
S511
書換え対象ECUがアクティベート可能か？
NO
YES
S512
アクティベートを書換え対象ECUに指示
エンド

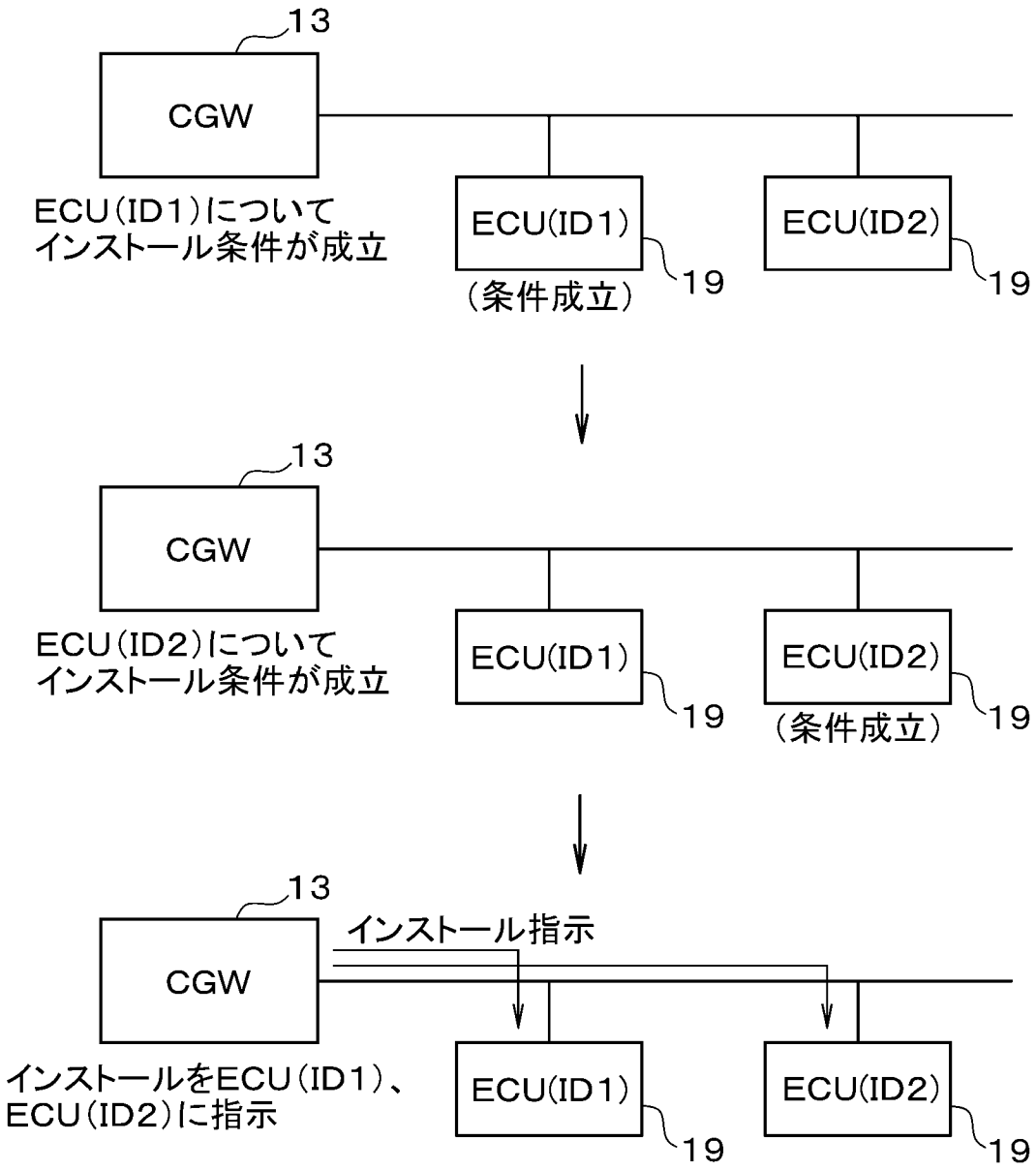
[図63]

Fig. 63


13
CGW
ECU(ID1)について
インストール条件が成立
ECU(ID1)
19
(条件成立)
ECU(ID2)
19
13
CGW
インストール指示
インストールを
ECU(ID1)に指示
ECU(ID1)
19
ECU(ID2)
19
13
CGW
ECU(ID2)について
インストール条件が成立
ECU(ID1)
19
ECU(ID2)
19
(条件成立)
13
CGW
インストール指示
インストールを
ECU(ID2)に指示
ECU(ID1)
19
ECU(ID2)
19

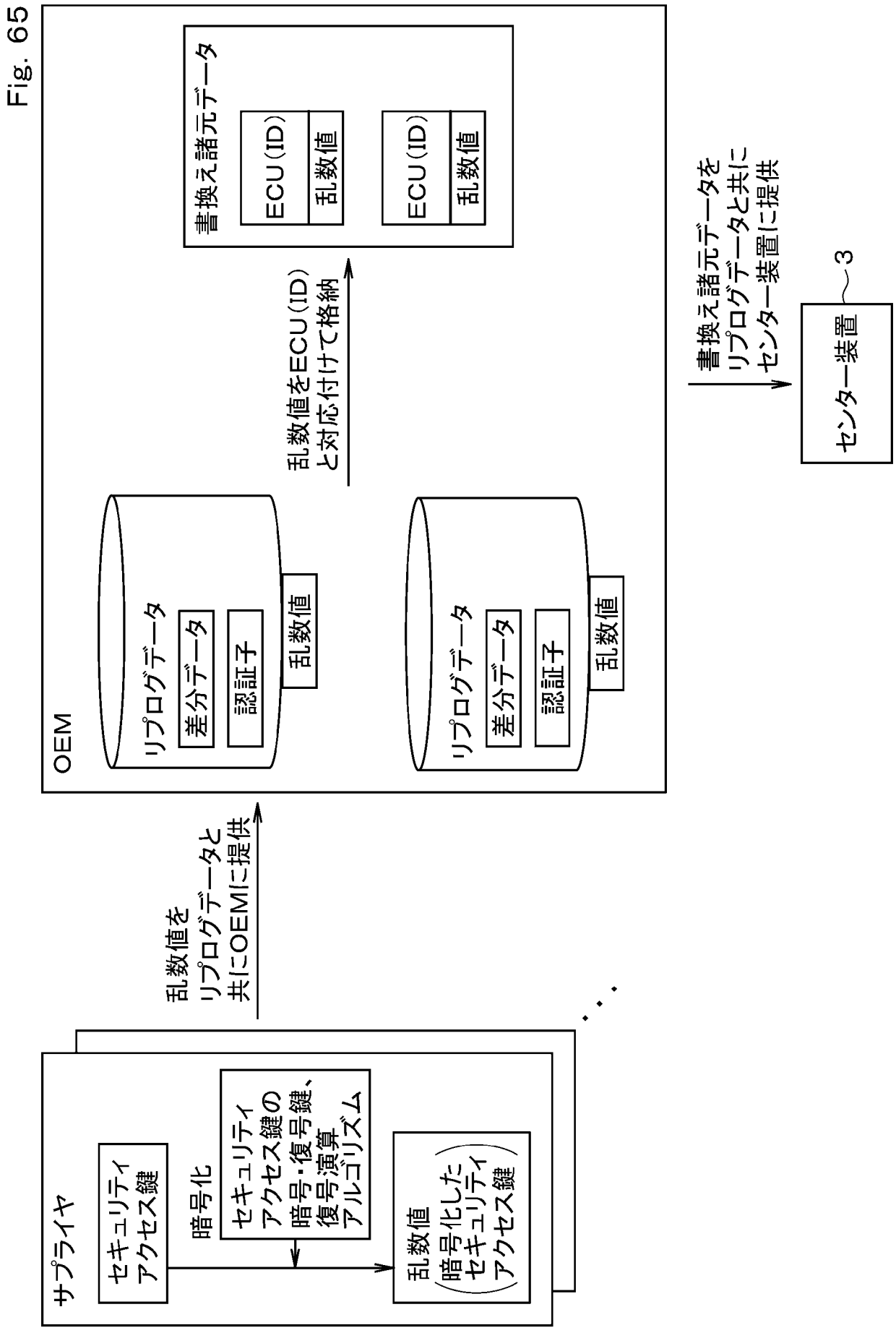
[図64]

Fig. 64


13
CGW
ECU(ID1)について
インストール条件が成立
ECU(ID1)
(条件成立)
19
ECU(ID2)
19
13
CGW
ECU(ID2)について
インストール条件が成立
ECU(ID1)
19
ECU(ID2)
(条件成立)
19
13
CGW
インストール指示
インストールをECU(ID1)、
ECU(ID2)に指示
ECU(ID1)
19
ECU(ID2)
19

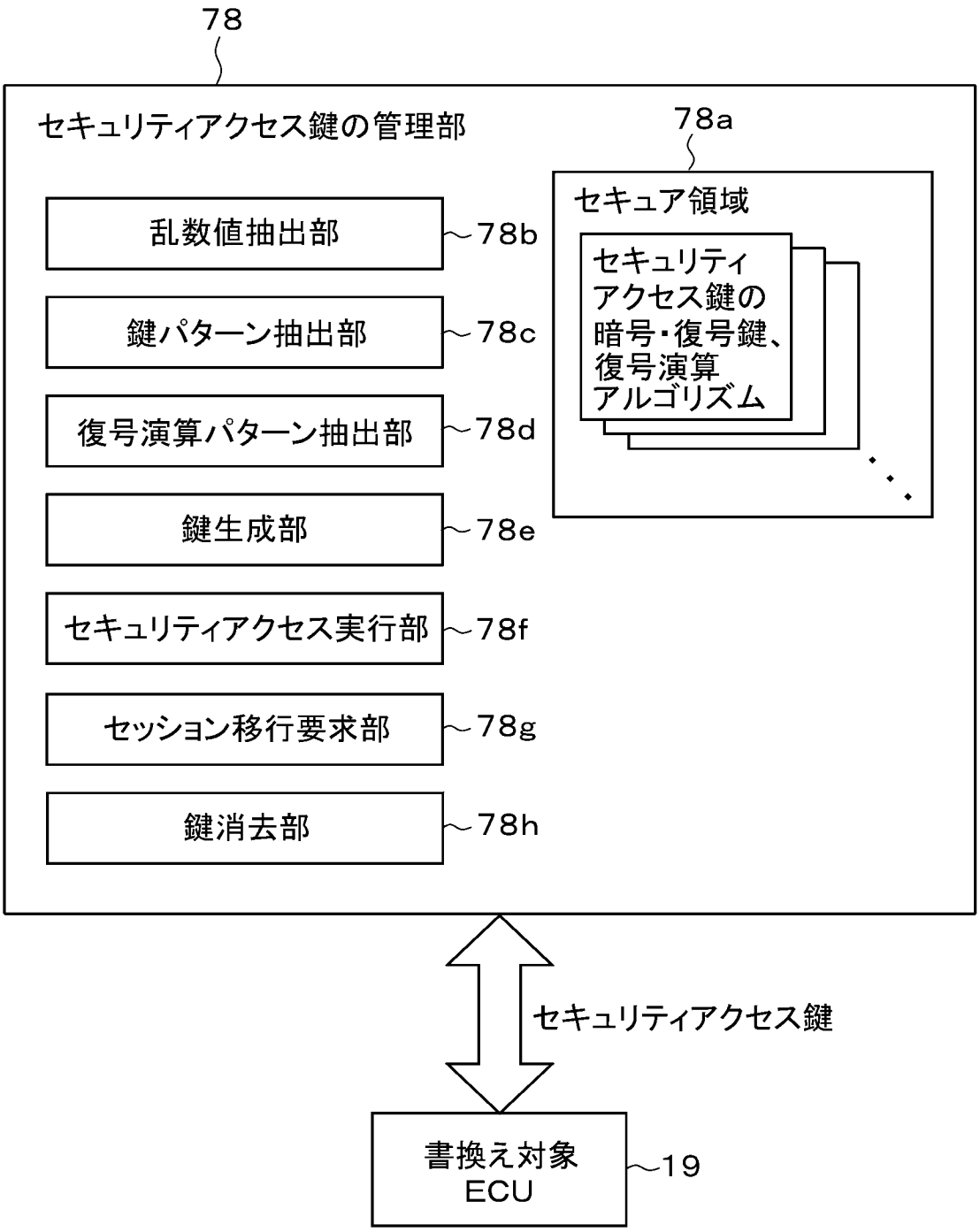
[図65]

Fig. 65


サプライヤ
セキュリティアクセス鍵
暗号化
セキュリティアクセス鍵の暗号・復号鍵、復号演算アルゴリズム
乱数値（暗号化したセキュリティアクセス鍵）
乱数値をリプログデータと共にOEMに提供
OEM
リプログデータ
差分データ
認証子
乱数値
乱数値をECU（ID）と対応付けて格納
書換え諸元データ
ECU（ID）
乱数値
ECU（ID）
乱数値
書換え諸元データをリプログデータと共にセンター装置に提供
センター装置
3

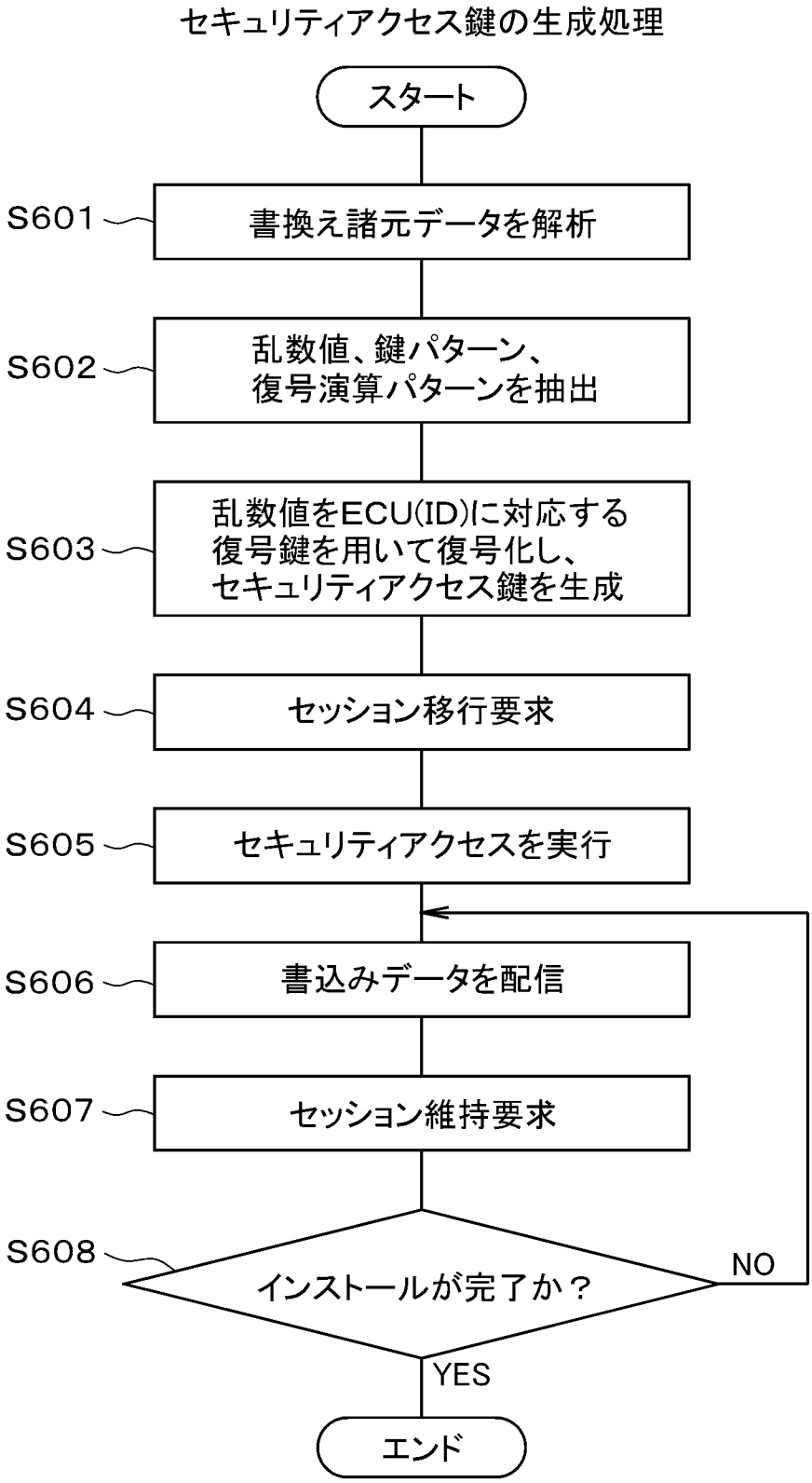
[図66]

Fig. 66


78
セキュリティアクセス鍵の管理部
78a
セキュア領域
セキュリティアクセス鍵の暗号・復号鍵、復号演算アルゴリズム
乱数値抽出部
78b
鍵パターン抽出部
78c
復号演算パターン抽出部
78d
鍵生成部
78e
セキュリティアクセス実行部
78f
セッション移行要求部
78g
鍵消去部
78h
セキュリティアクセス鍵
書換え対象ECU
19

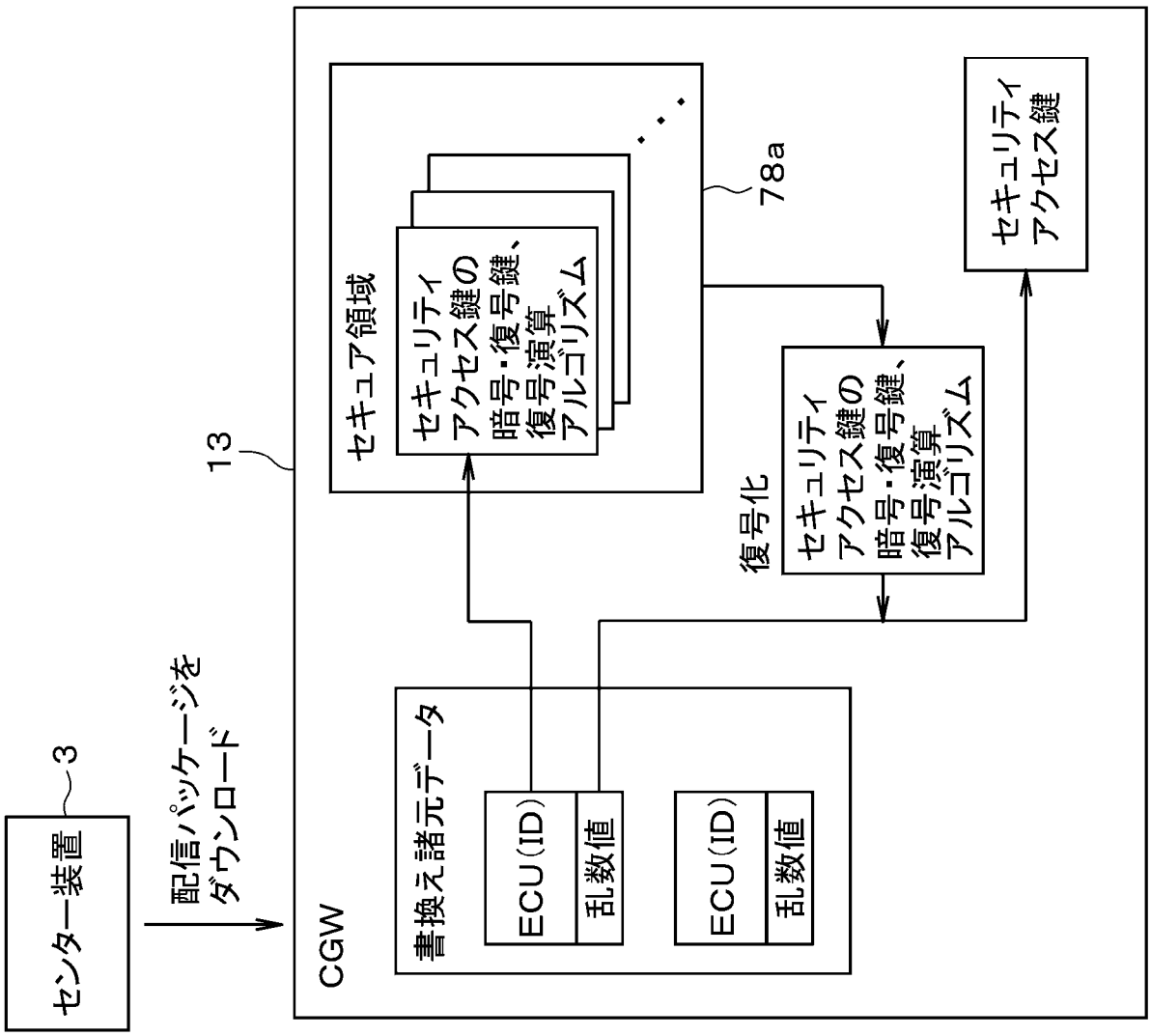
[図67]

Fig. 67


セキュリティアクセス鍵の生成処理
スタート
S601
書換え諸元データを解析
S602
乱数値、鍵パターン、
復号演算パターンを抽出
S603
乱数値をECU(ID)に対応する
復号鍵を用いて復号化し、
セキュリティアクセス鍵を生成
S604
セッション移行要求
S605
セキュリティアクセスを実行
S606
書込みデータを配信
S607
セッション維持要求
S608
インストールが完了か？
NO
YES
エンド

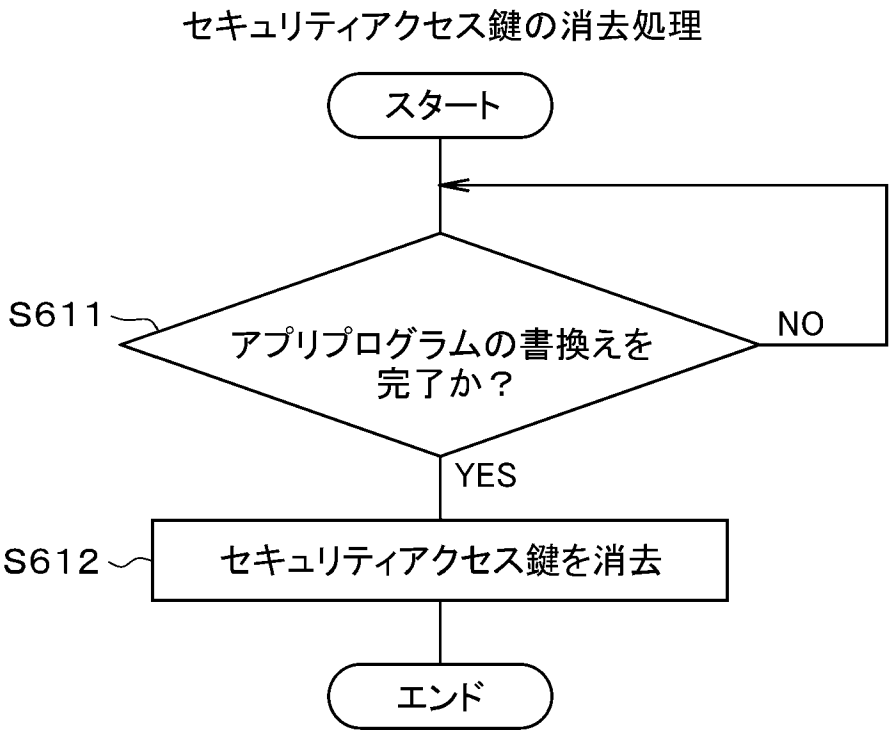
[図68]

Fig. 68


センター装置
3
配信パッケージを
ダウンロード
13
CGW
書換え諸元データ
ECU(ID)
乱数値
ECU(ID)
乱数値
セキュア領域
セキュリティ
アクセス鍵の
暗号・復号鍵、
復号演算
アルゴリズム
78a
復号化
セキュリティ
アクセス鍵の
暗号・復号鍵、
復号演算
アルゴリズム
セキュリティ
アクセス鍵

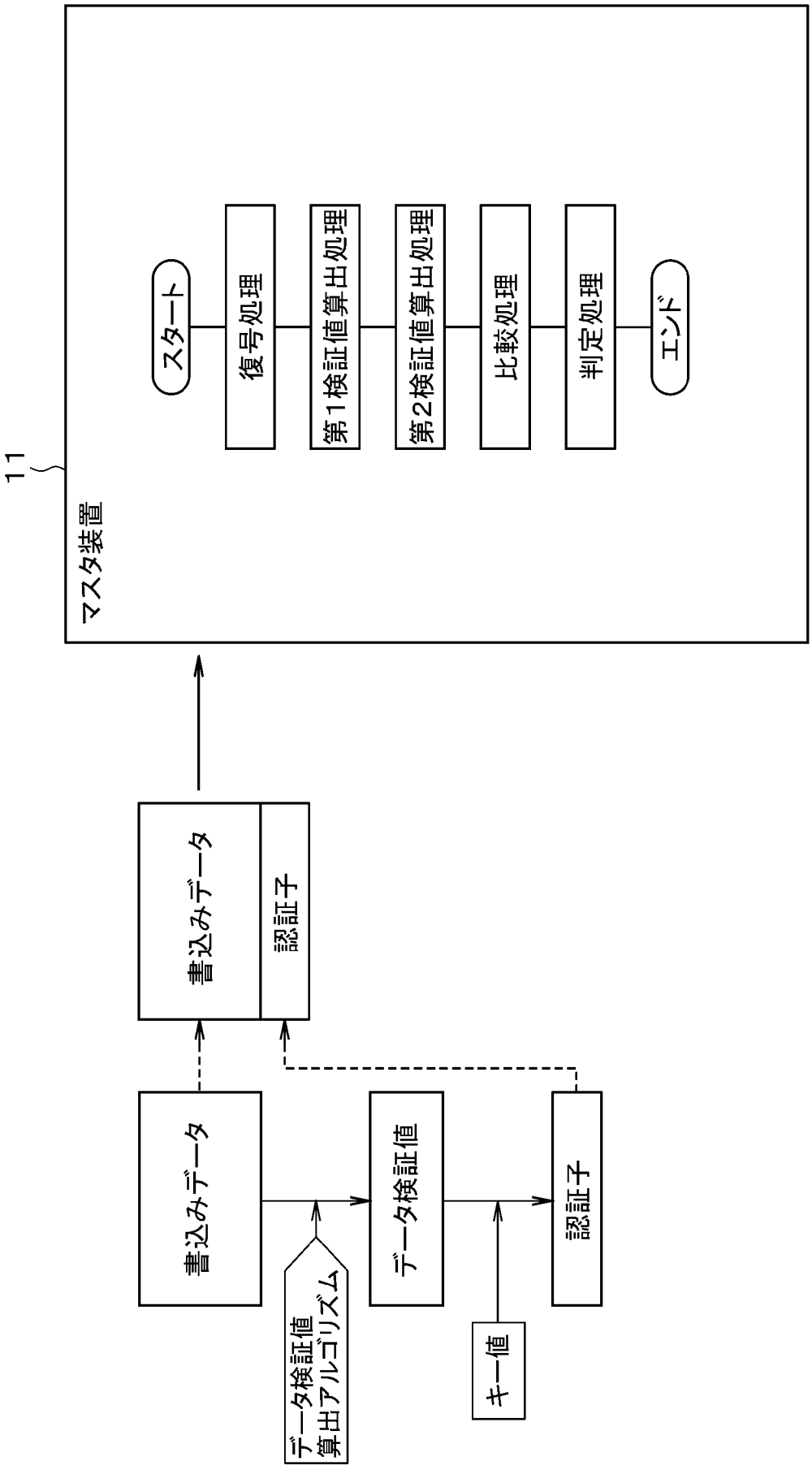
[図69]

Fig. 69


セキュリティアクセス鍵の消去処理
スタート
S611
アプリプログラムの書換えを
完了か？
NO
YES
S612
セキュリティアクセス鍵を消去
エンド

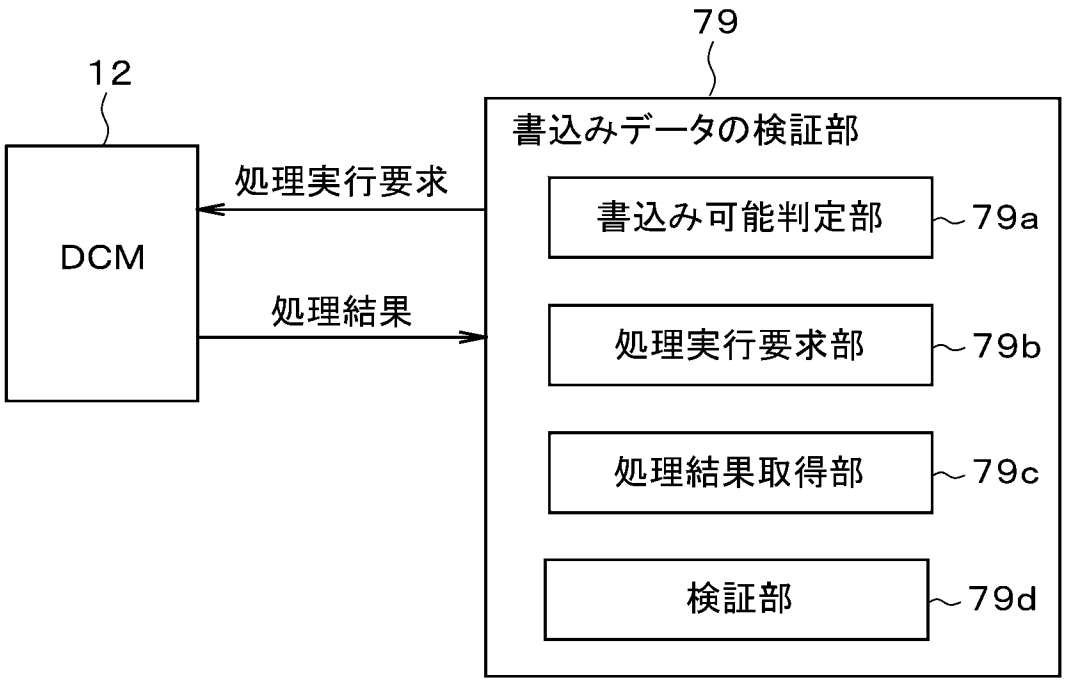
[図70]

Fig. 70


11
マスタ装置
スタート
復号処理
第1検証値算出処理
第2検証値算出処理
比較処理
判定処理
エンド
書込みデータ
認証子
書込みデータ
データ検証値
算出アルゴリズム
データ検証値
キー値
認証子

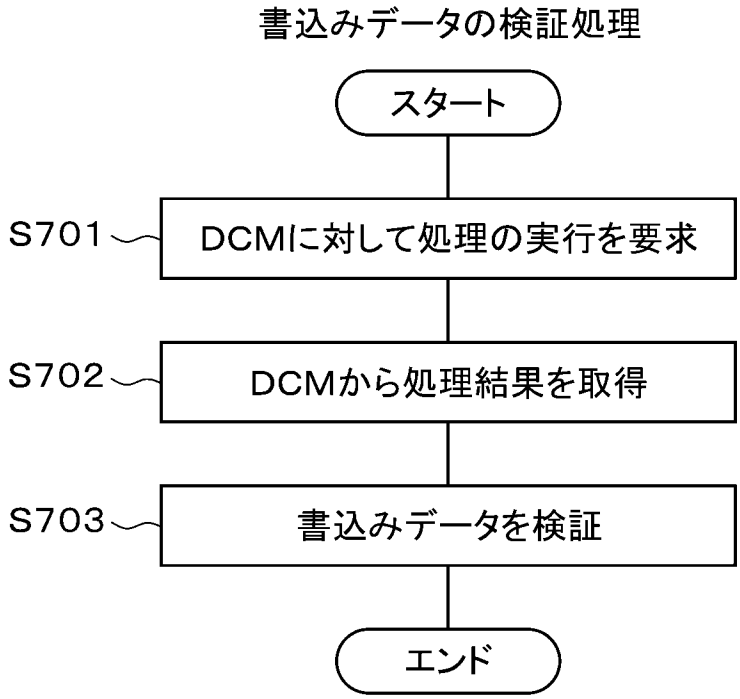
[図71]

Fig. 71



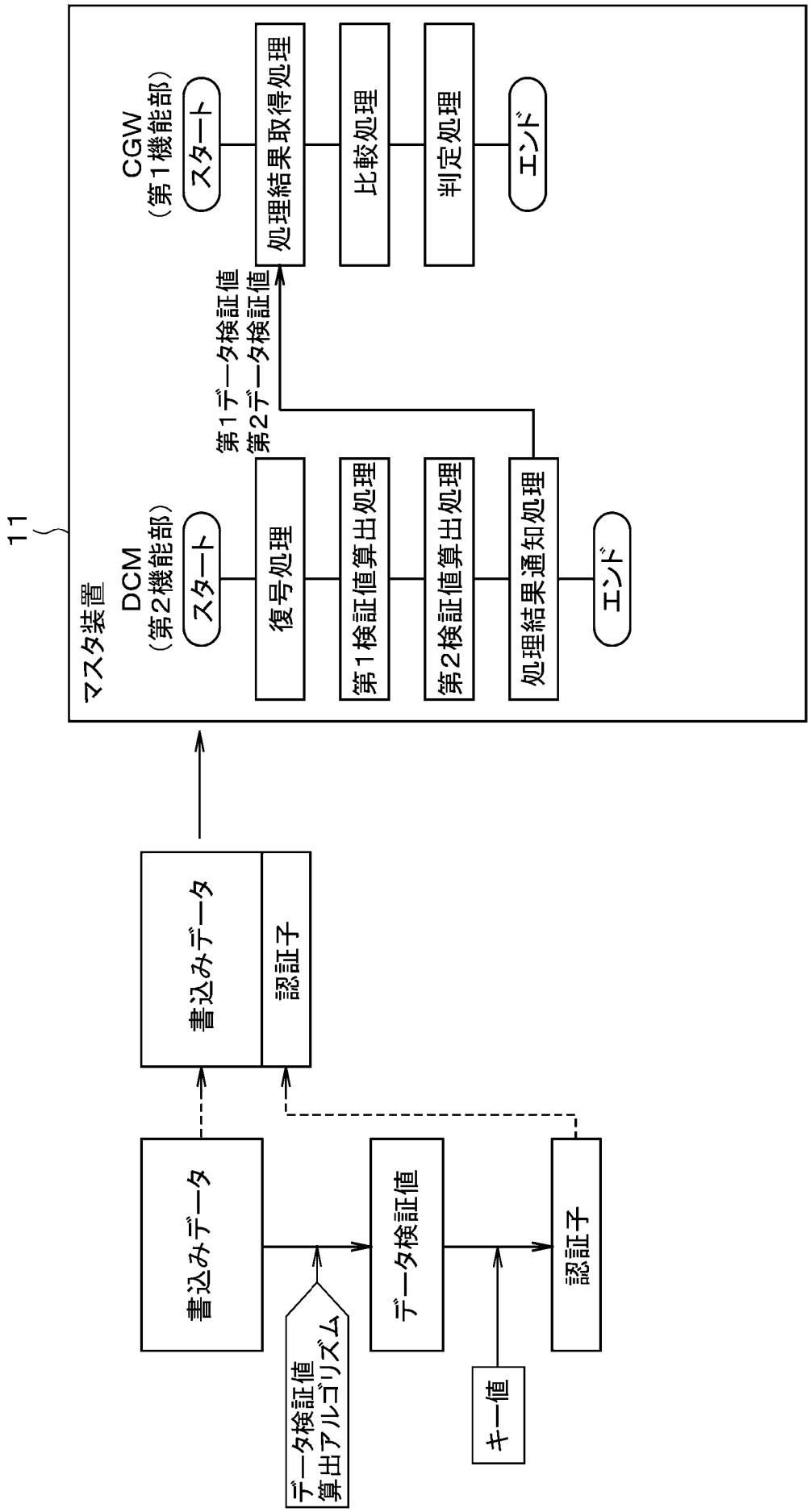
[図72]

Fig. 72



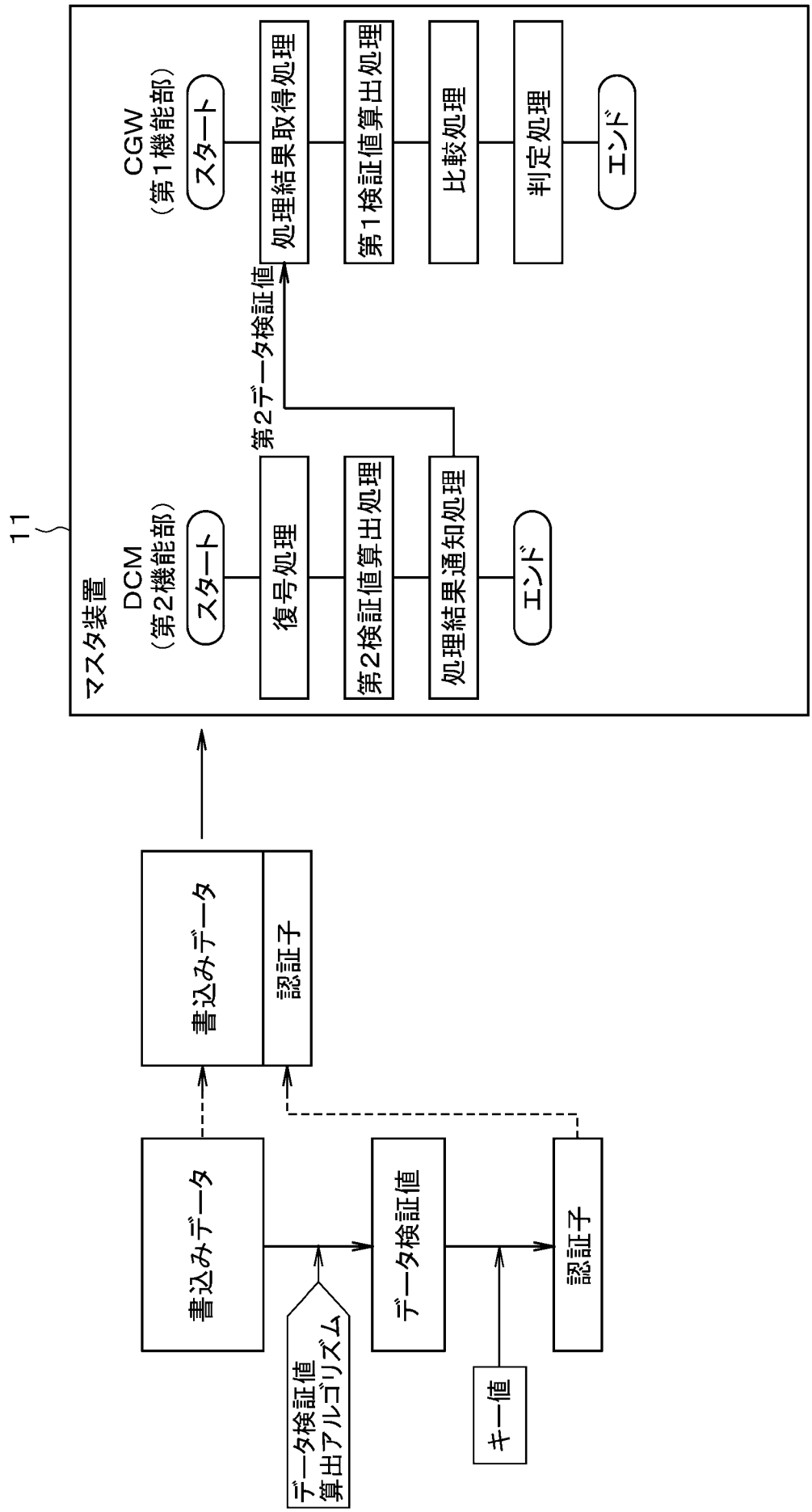
[図73]

Fig. 73


11
マスタ装置
DCM
（第2機能部）
スタート
復号処理
第1検証値算出処理
第2検証値算出処理
処理結果通知処理
エンド
第1データ検証値
第2データ検証値
CGW
（第1機能部）
スタート
処理結果取得処理
比較処理
判定処理
エンド
書込みデータ
認証子
書込みデータ
データ検証値
算出アルゴリズム
データ検証値
キー値
認証子

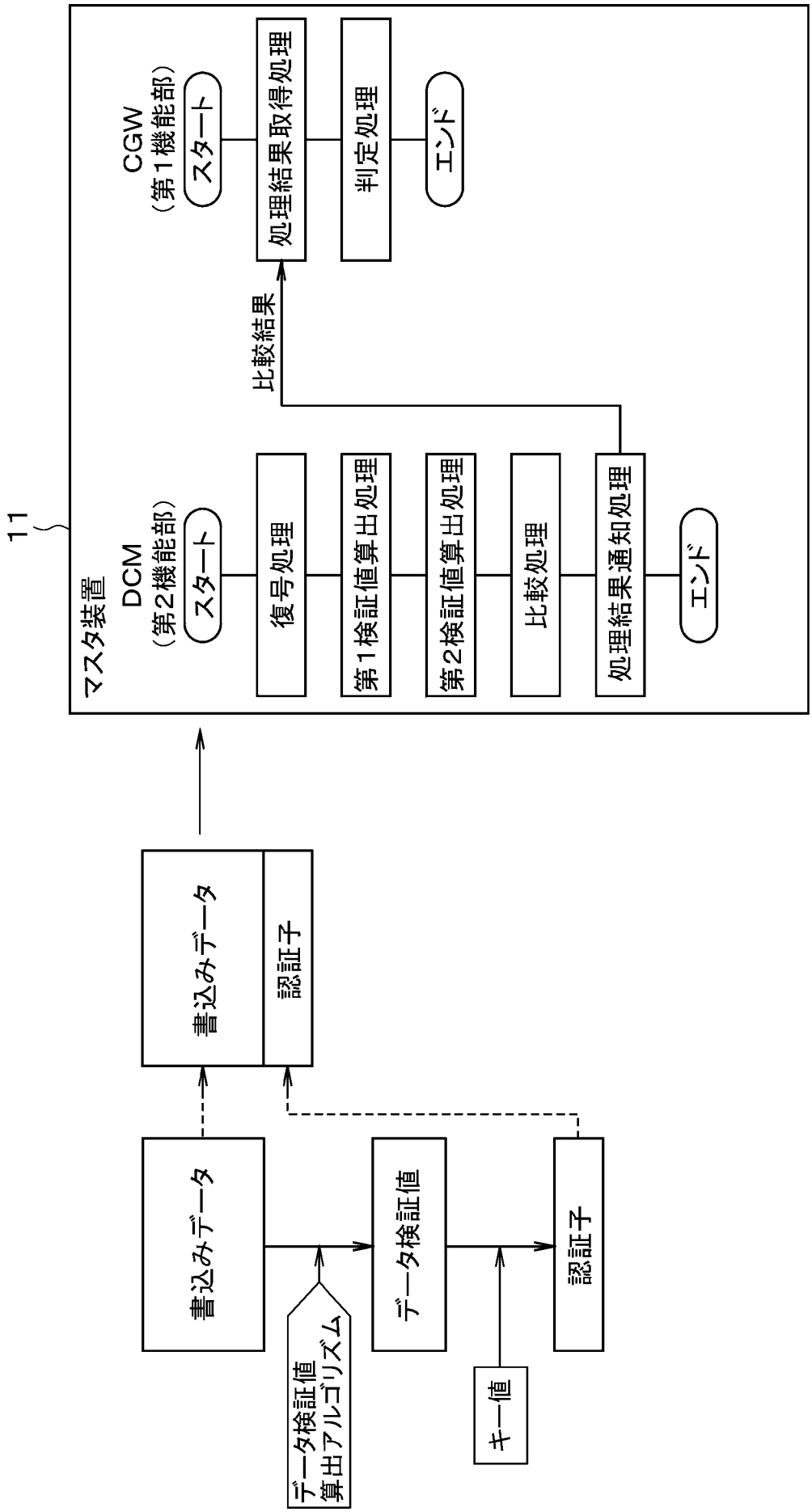
[図74]

Fig. 74


11
マスタ装置
DCM
（第2機能部）
スタート
復号処理
第2検証値算出処理
処理結果通知処理
エンド
CGW
（第1機能部）
スタート
処理結果取得処理
第1検証値算出処理
比較処理
判定処理
エンド
第2データ検証値
書込みデータ
認証子
書込みデータ
データ検証値
算出アルゴリズム
データ検証値
認証子
キー値

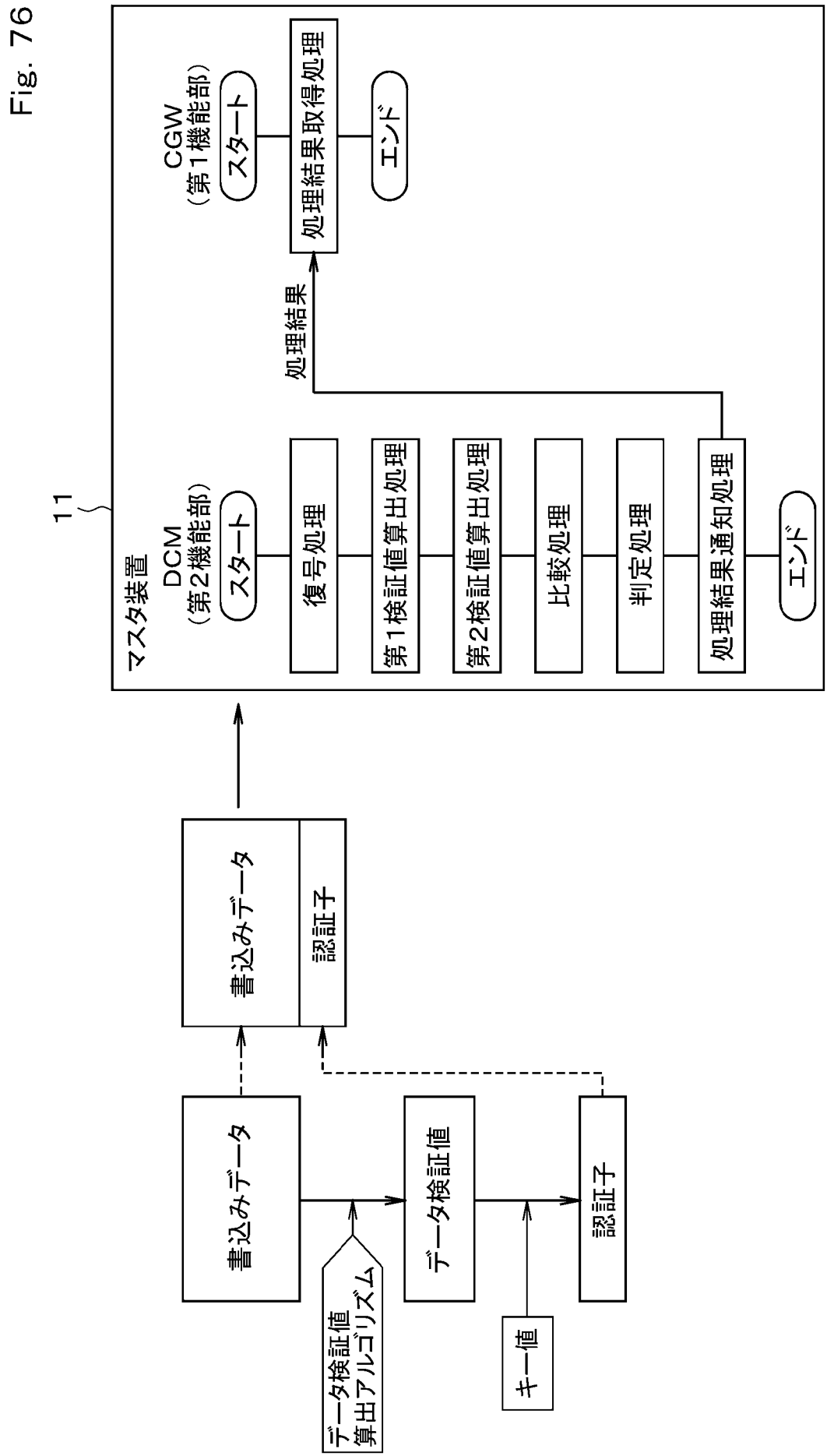
[図75]

Fig. 75


11
マスタ装置
DCM
（第2機能部）
スタート
復号処理
第1検証値算出処理
第2検証値算出処理
比較処理
処理結果通知処理
エンド
CGW
（第1機能部）
スタート
処理結果取得処理
判定処理
エンド
比較結果
書込みデータ
認証子
書込みデータ
データ検証値
算出アルゴリズム
データ検証値
キー値
認証子

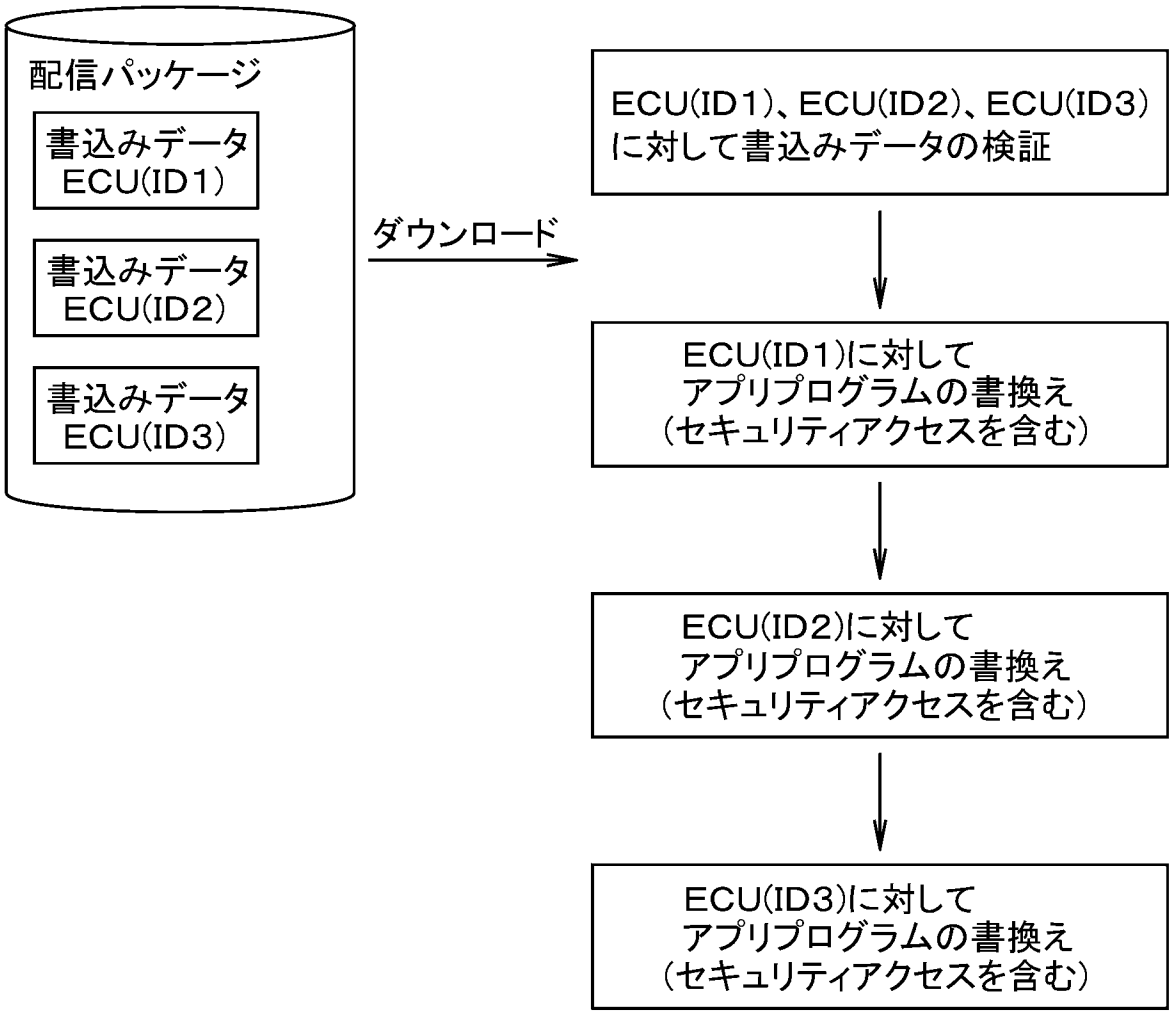
[図76]

Fig. 76


11
マスタ装置
DCM
（第2機能部）
スタート
復号処理
第1検証値算出処理
第2検証値算出処理
比較処理
判定処理
処理結果通知処理
エンド
処理結果
CGW
（第1機能部）
スタート
処理結果取得処理
エンド
書込みデータ
認証子
書込みデータ
データ検証値
算出アルゴリズム
データ検証値
キー値
認証子

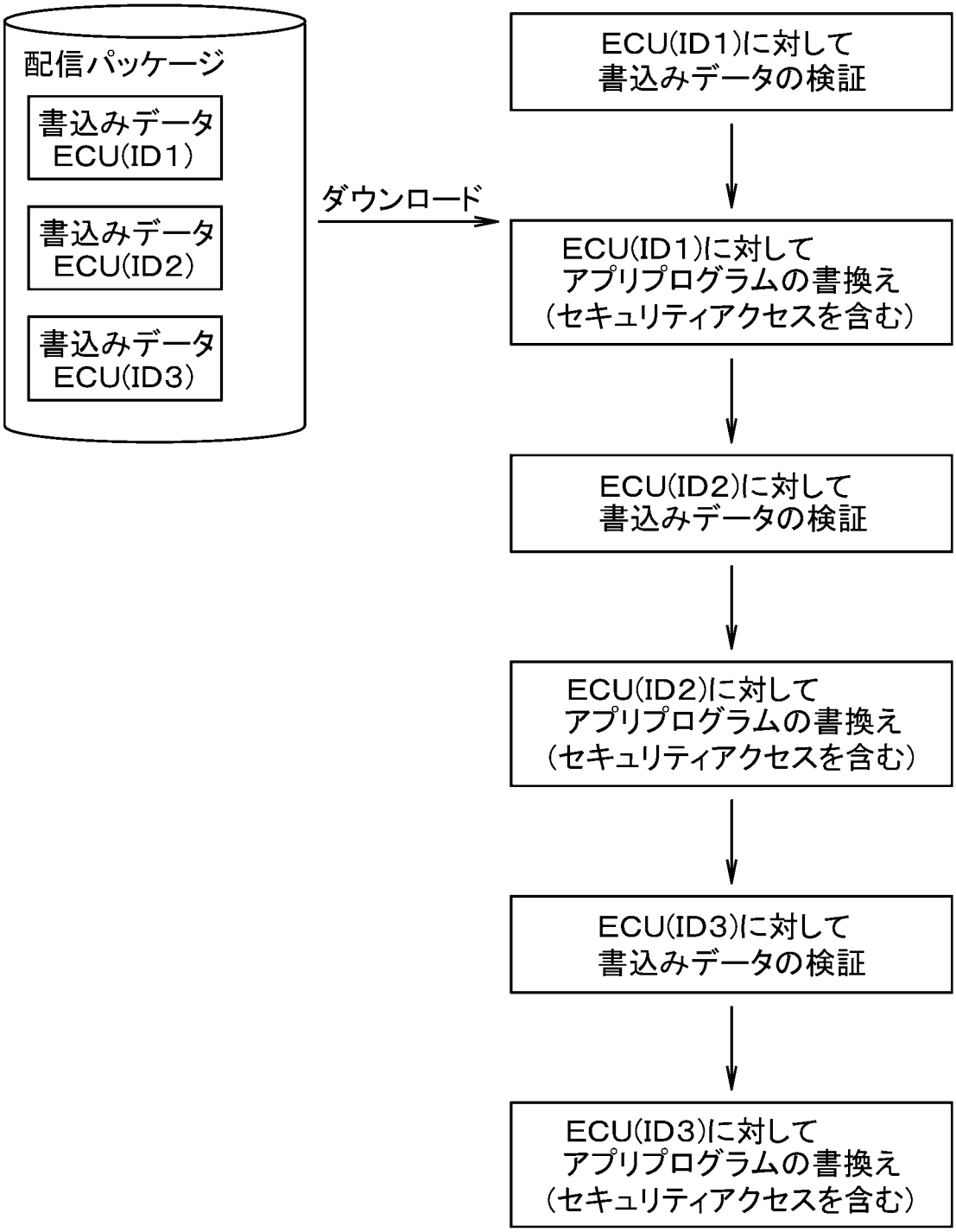
[図77]

Fig. 77


配信パッケージ
書込みデータ
ECU(ID1)
書込みデータ
ECU(ID2)
書込みデータ
ECU(ID3)
ダウンロード
ECU(ID1)、ECU(ID2)、ECU(ID3)
に対して書込みデータの検証
ECU(ID1)に対して
アプリプログラムの書換え
(セキュリティアクセスを含む)
ECU(ID2)に対して
アプリプログラムの書換え
(セキュリティアクセスを含む)
ECU(ID3)に対して
アプリプログラムの書換え
(セキュリティアクセスを含む)

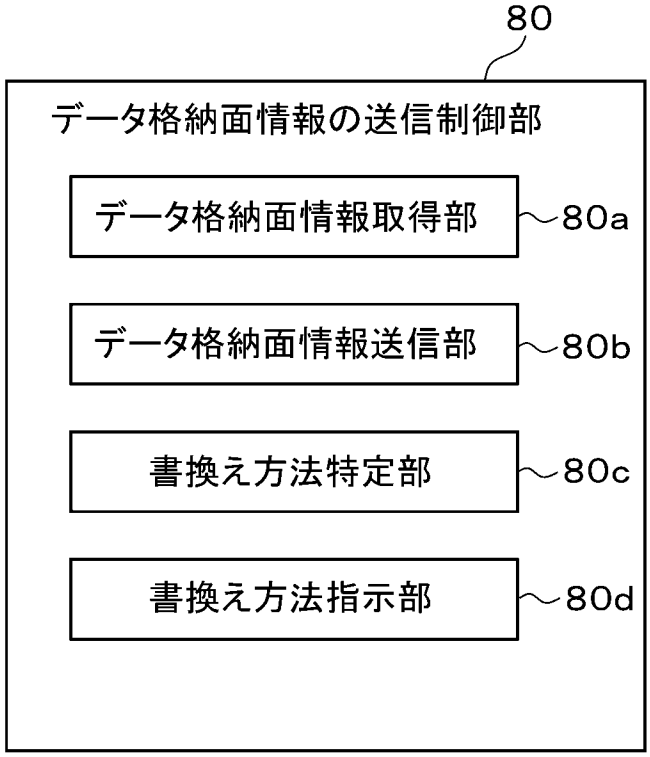
[図78]

Fig. 78


配信パッケージ
書込みデータ ECU(ID1)
書込みデータ ECU(ID2)
書込みデータ ECU(ID3)
ダウンロード
ECU(ID1)に対して 書込みデータの検証
ECU(ID1)に対して アプリプログラムの書換え (セキュリティアクセスを含む)
ECU(ID2)に対して 書込みデータの検証
ECU(ID2)に対して アプリプログラムの書換え (セキュリティアクセスを含む)
ECU(ID3)に対して 書込みデータの検証
ECU(ID3)に対して アプリプログラムの書換え (セキュリティアクセスを含む)

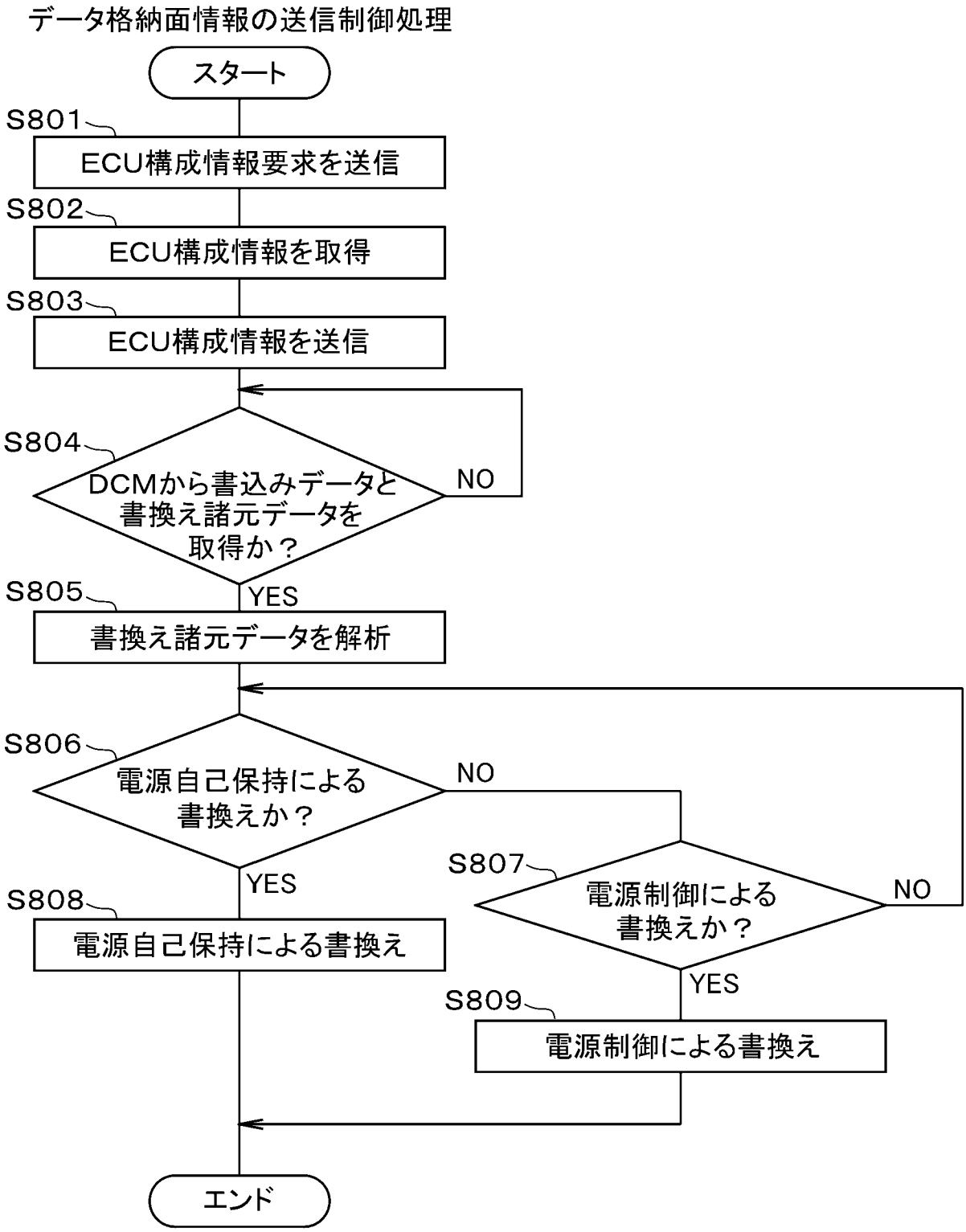
[図79]

Fig. 79


80
データ格納面情報の送信制御部
データ格納面情報取得部
80a
データ格納面情報送信部
80b
書換え方法特定部
80c
書換え方法指示部
80d

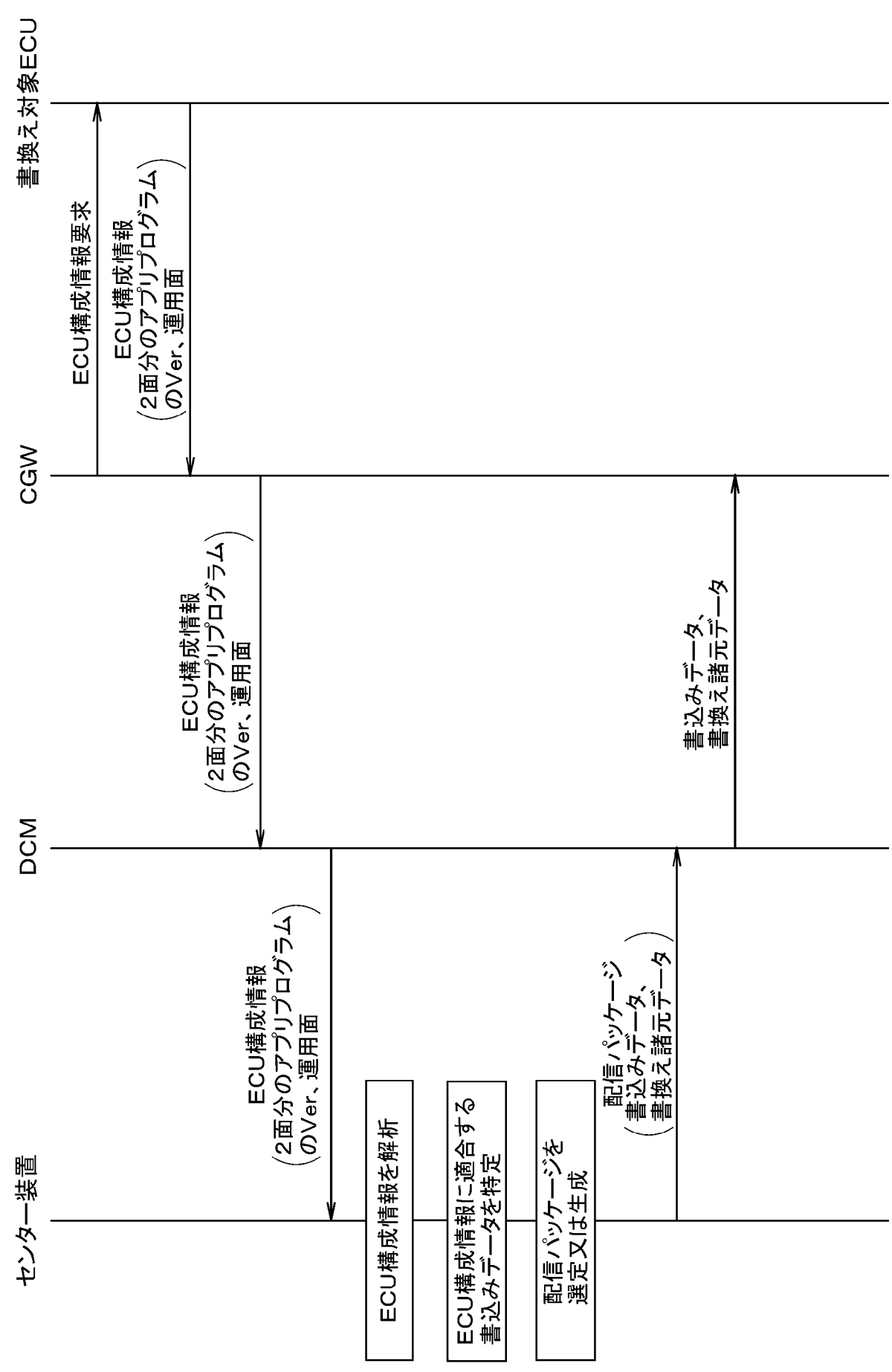
[図80]

Fig. 80


データ格納面情報の送信制御処理
スタート
S801
ECU構成情報要求を送信
S802
ECU構成情報を取得
S803
ECU構成情報を送信
S804
DCMから書込みデータと書換え諸元データを取得か？
NO
YES
S805
書換え諸元データを解析
S806
電源自己保持による書換えか？
NO
YES
S807
電源制御による書換えか？
NO
YES
S808
電源自己保持による書換え
S809
電源制御による書換え
エンド

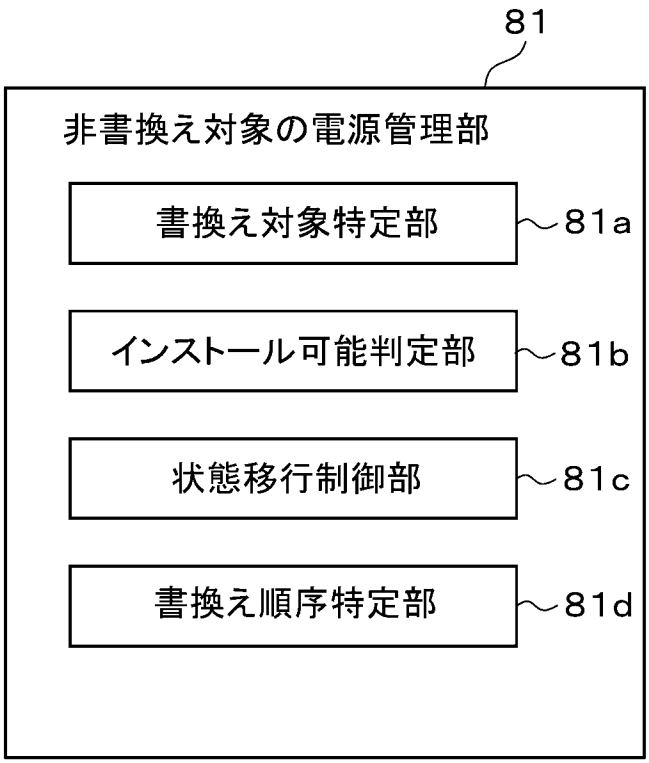
[図81]

Fig. 81


書換え対象ECU
CGW
DCM
センター装置
ECU構成情報要求
ECU構成情報
(2面分のアプリプログラム
のVer、運用面)
ECU構成情報
(2面分のアプリプログラム
のVer、運用面)
書込みデータ、
書換え諸元データ
ECU構成情報
(2面分のアプリプログラム
のVer、運用面)
ECU構成情報を解析
ECU構成情報に適合する
書込みデータを特定
配信パッケージを
選定又は生成
配信パッケージ
(書込みデータ、
書換え諸元データ)

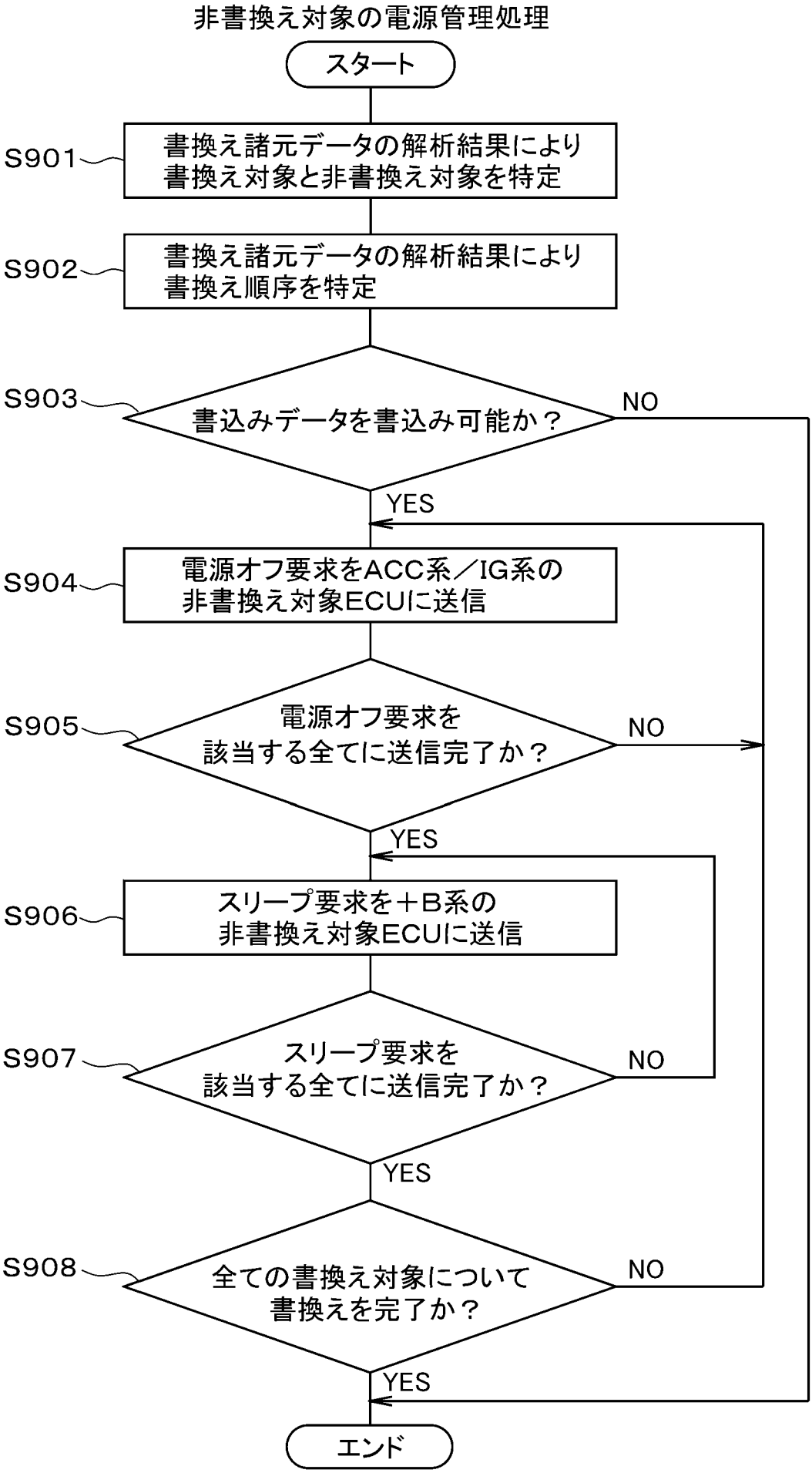
[図82]

Fig. 82


81
非書換え対象の電源管理部
書換え対象特定部
81a
インストール可能判定部
81b
状態移行制御部
81c
書換え順序特定部
81d

[図83]

Fig. 83


非書換え対象の電源管理処理
スタート
S901
書換え諸元データの解析結果により
書換え対象と非書換え対象を特定
S902
書換え諸元データの解析結果により
書換え順序を特定
S903
書込みデータを書込み可能か？
NO
YES
S904
電源オフ要求をACC系／IG系の
非書換え対象ECUに送信
S905
電源オフ要求を
該当する全てに送信完了か？
NO
YES
S906
スリープ要求を＋B系の
非書換え対象ECUに送信
S907
スリープ要求を
該当する全てに送信完了か？
NO
YES
S908
全ての書換え対象について
書換えを完了か？
NO
YES
エンド

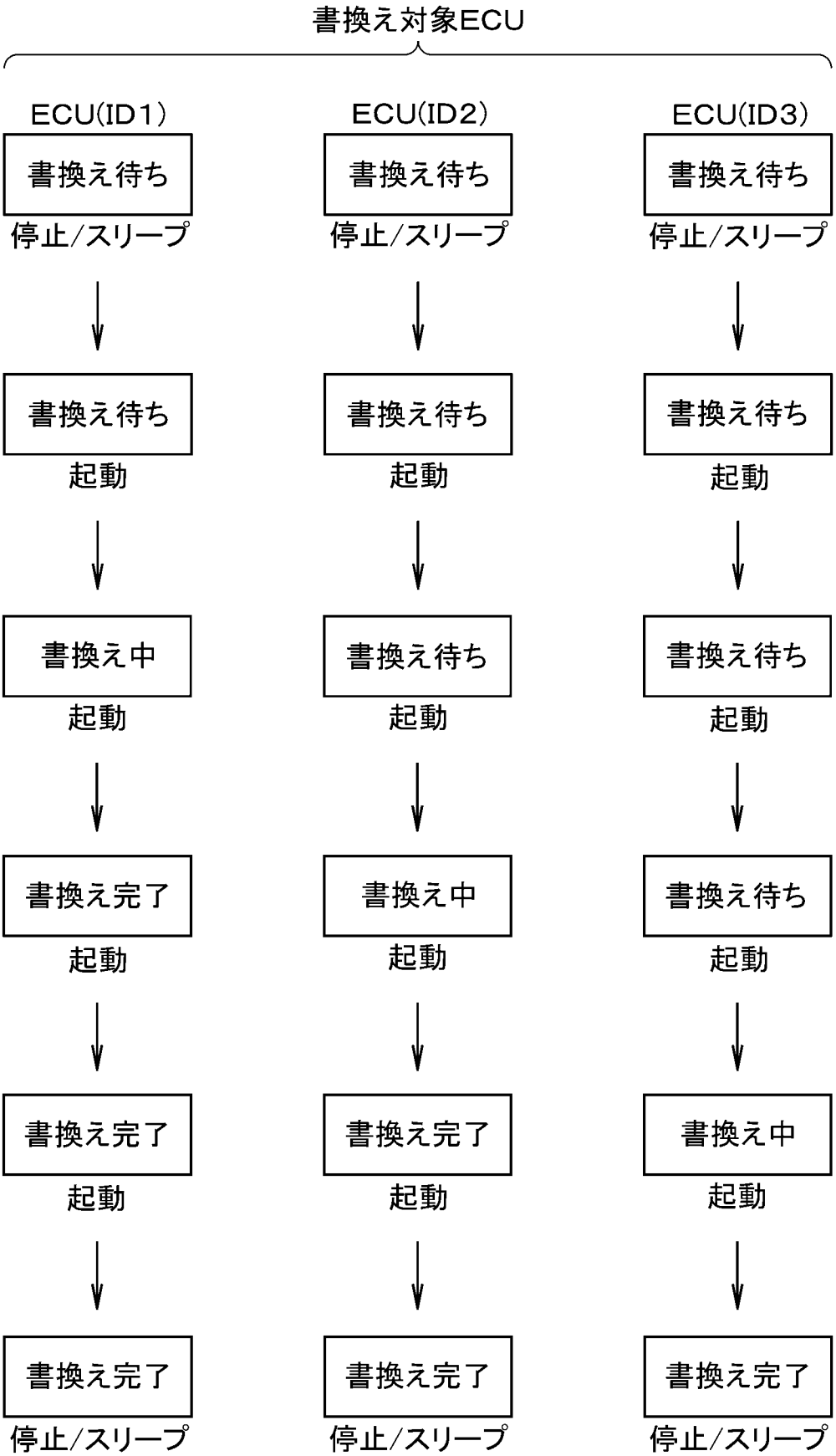
[図84]

Fig. 84

書換え対象ECU
ECU(ID1)
ECU(ID2)
ECU(ID3)
書換え待ち
停止/スリープ
書換え待ち
起動
書換え中
起動
書換え完了
停止/スリープ
書換え完了
停止/スリープ

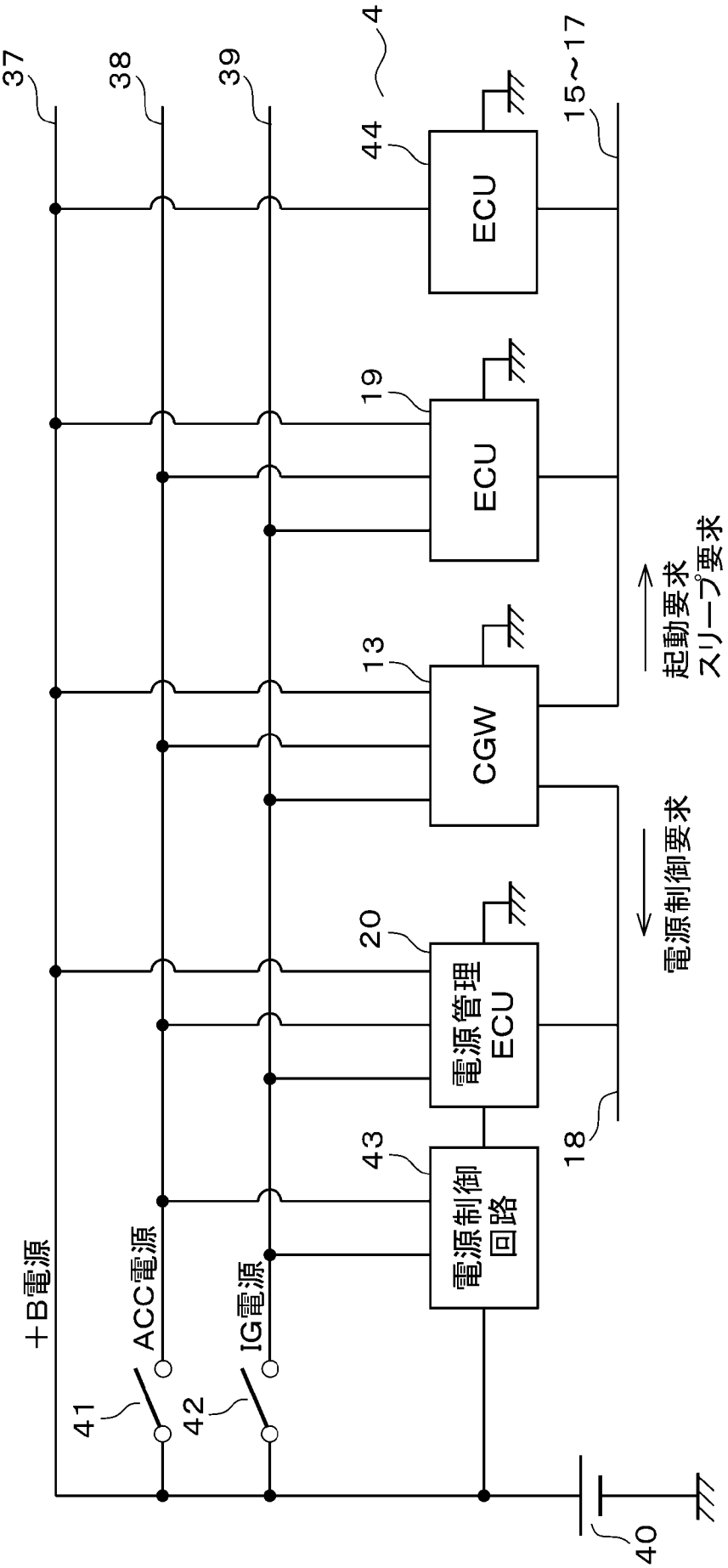
[図85]

Fig. 85


書換え対象ECU
ECU(ID1)
ECU(ID2)
ECU(ID3)
書換え待ち
停止/スリープ
書換え待ち
起動
書換え中
起動
書換え完了
起動
書換え完了
停止/スリープ

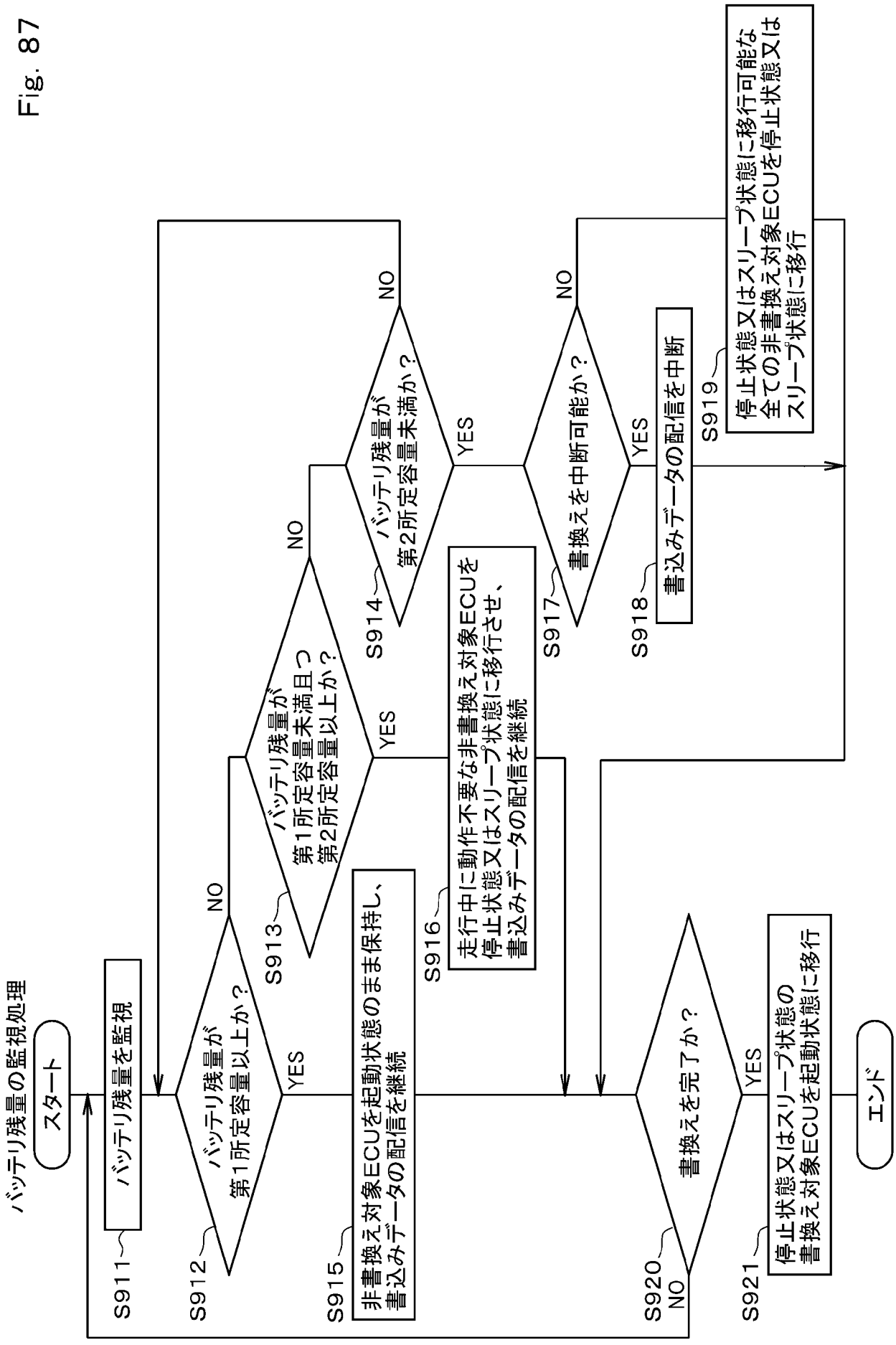
[図86]

Fig. 86


37
38
39
4
44
ECU
15～17
19
ECU
13
CGW
起動要求
スリープ要求
20
電源管理
ECU
電源制御要求
43
電源制御
回路
18
＋B電源
ACC電源
IG電源
41
42
40

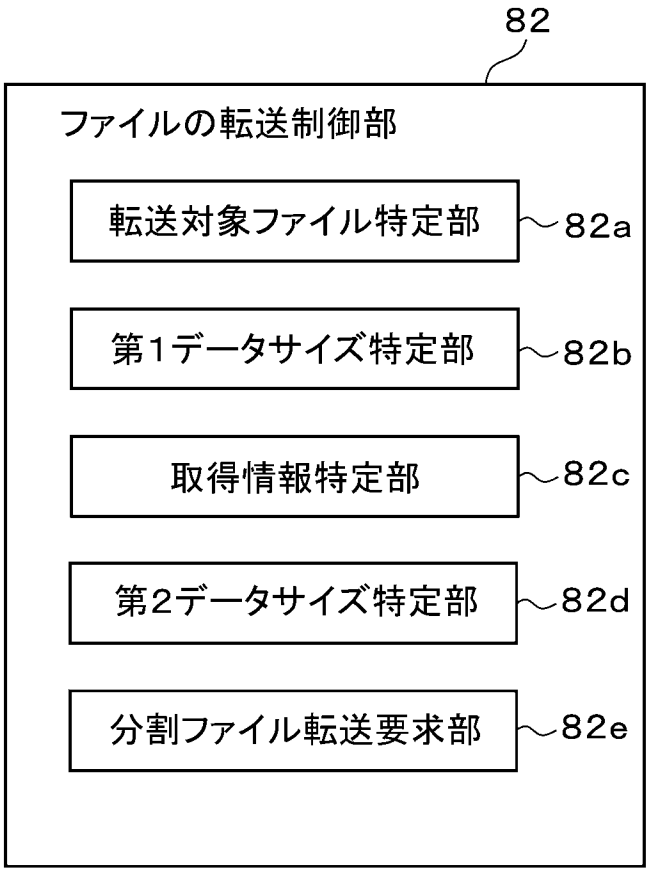
[図87]

Fig. 87


バッテリ残量の監視処理
スタート
S911
バッテリ残量を監視
S912
バッテリ残量が第1所定容量以上か？
NO
YES
S913
バッテリ残量が第1所定容量未満且つ第2所定容量以上か？
NO
YES
S914
バッテリ残量が第2所定容量未満か？
NO
YES
S915
非書換え対象ECUを起動状態のまま保持し、書込みデータの配信を継続
S916
走行中に動作不要な非書換え対象ECUを停止状態又はスリープ状態に移行させ、書込みデータの配信を継続
S917
書換えを中断可能か？
NO
YES
S918
書込みデータの配信を中断
S919
停止状態又はスリープ状態に移行可能な全ての非書換え対象ECUを停止状態又はスリープ状態に移行
S920
書換えを完了か？
NO
YES
S921
停止状態又はスリープ状態の書換え対象ECUを起動状態に移行
エンド

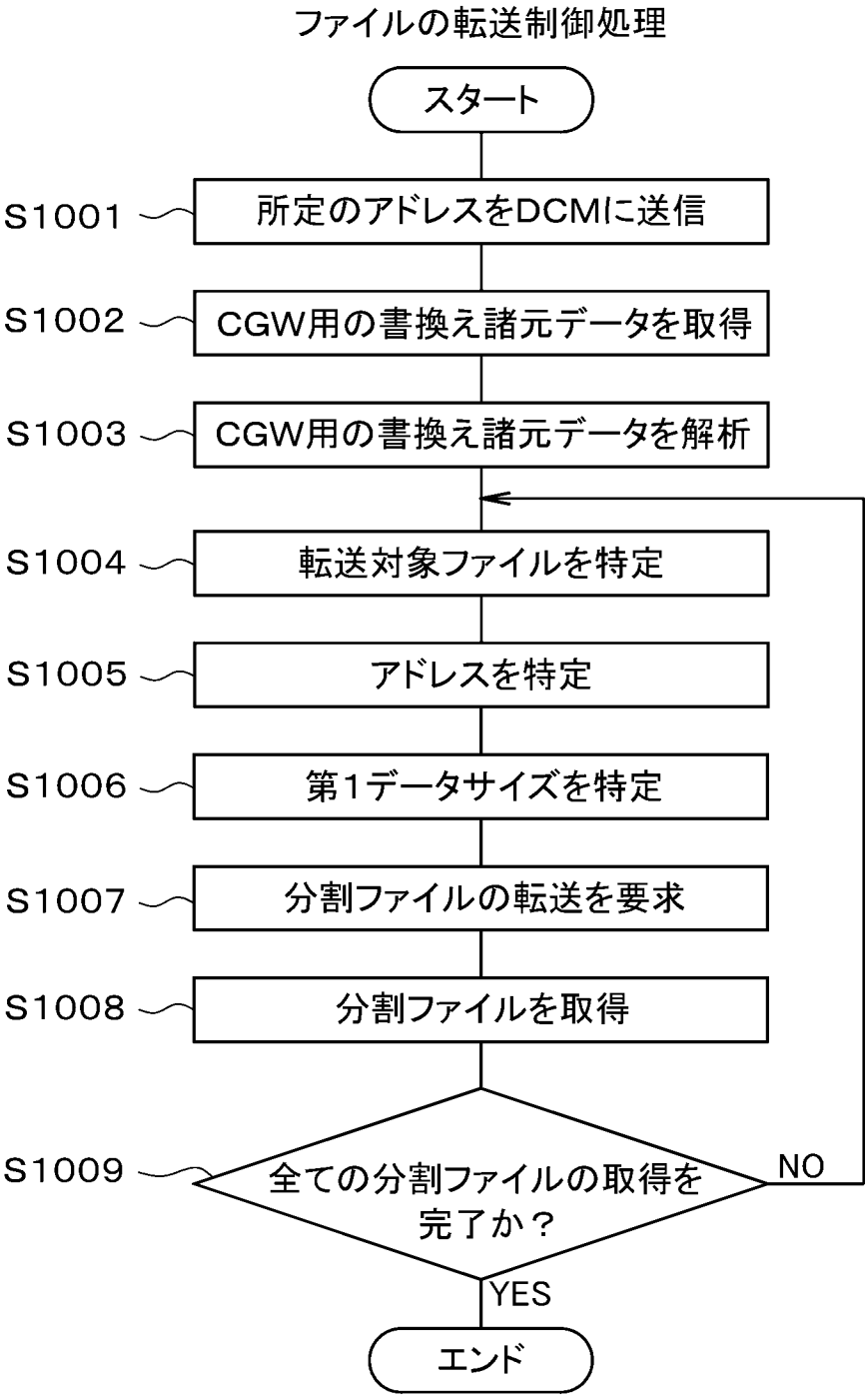
[図88]

Fig. 88


82
ファイルの転送制御部
転送対象ファイル特定部
82a
第1データサイズ特定部
82b
取得情報特定部
82c
第2データサイズ特定部
82d
分割ファイル転送要求部
82e

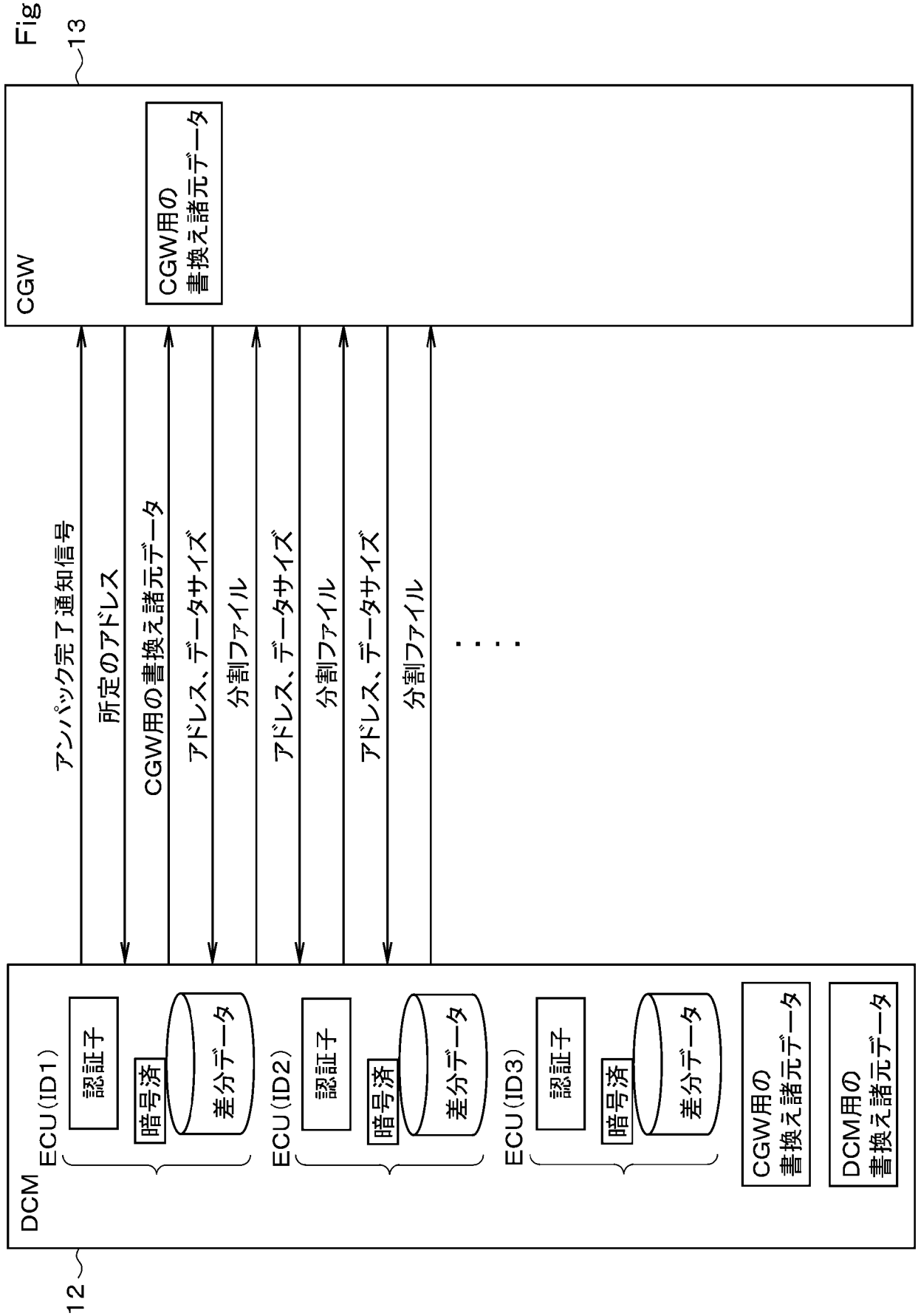
[図89]

Fig. 89


ファイルの転送制御処理
スタート
S1001
所定のアドレスをDCMに送信
S1002
CGW用の書換え諸元データを取得
S1003
CGW用の書換え諸元データを解析
S1004
転送対象ファイルを特定
S1005
アドレスを特定
S1006
第1データサイズを特定
S1007
分割ファイルの転送を要求
S1008
分割ファイルを取得
S1009
全ての分割ファイルの取得を完了か？
NO
YES
エンド

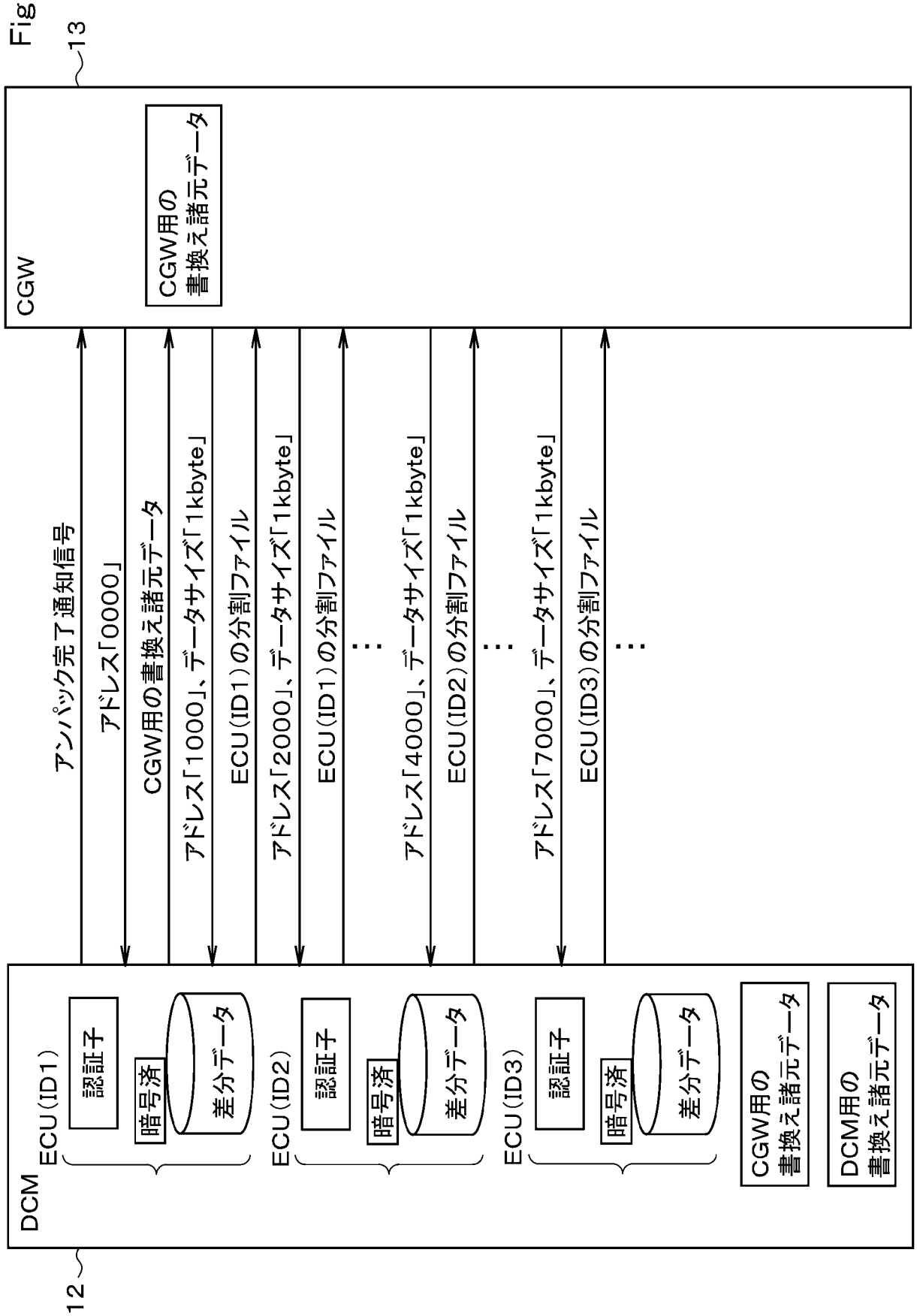
[図90]

Fig. 90


13
CGW
CGW用の
書換え諸元データ
アンパック完了通知信号
所定のアドレス
CGW用の書換え諸元データ
アドレス、データサイズ
分割ファイル
アドレス、データサイズ
分割ファイル
アドレス、データサイズ
分割ファイル
DCM
ECU(ID1)
認証子
暗号済
差分データ
ECU(ID2)
認証子
暗号済
差分データ
ECU(ID3)
認証子
暗号済
差分データ
CGW用の
書換え諸元データ
DCM用の
書換え諸元データ
12

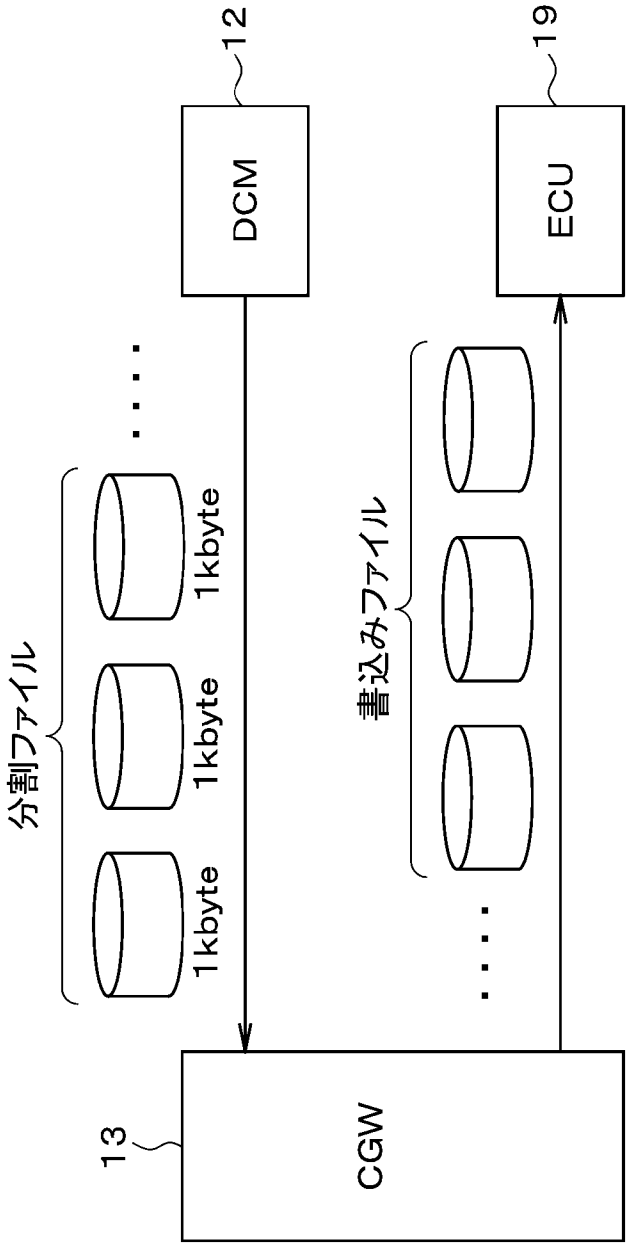
[図91]

Fig. 91


CGW
13
CGW用の
書換え諸元データ
アンパック完了通知信号
アドレス「0000」
CGW用の書換え諸元データ
アドレス「1000」、データサイズ「1kbyte」
ECU(ID1)の分割ファイル
アドレス「2000」、データサイズ「1kbyte」
ECU(ID1)の分割ファイル
アドレス「4000」、データサイズ「1kbyte」
ECU(ID2)の分割ファイル
アドレス「7000」、データサイズ「1kbyte」
ECU(ID3)の分割ファイル
DCM
12
ECU(ID1)
認証子
暗号済
差分データ
ECU(ID2)
認証子
暗号済
差分データ
ECU(ID3)
認証子
暗号済
差分データ
CGW用の
書換え諸元データ
DCM用の
書換え諸元データ

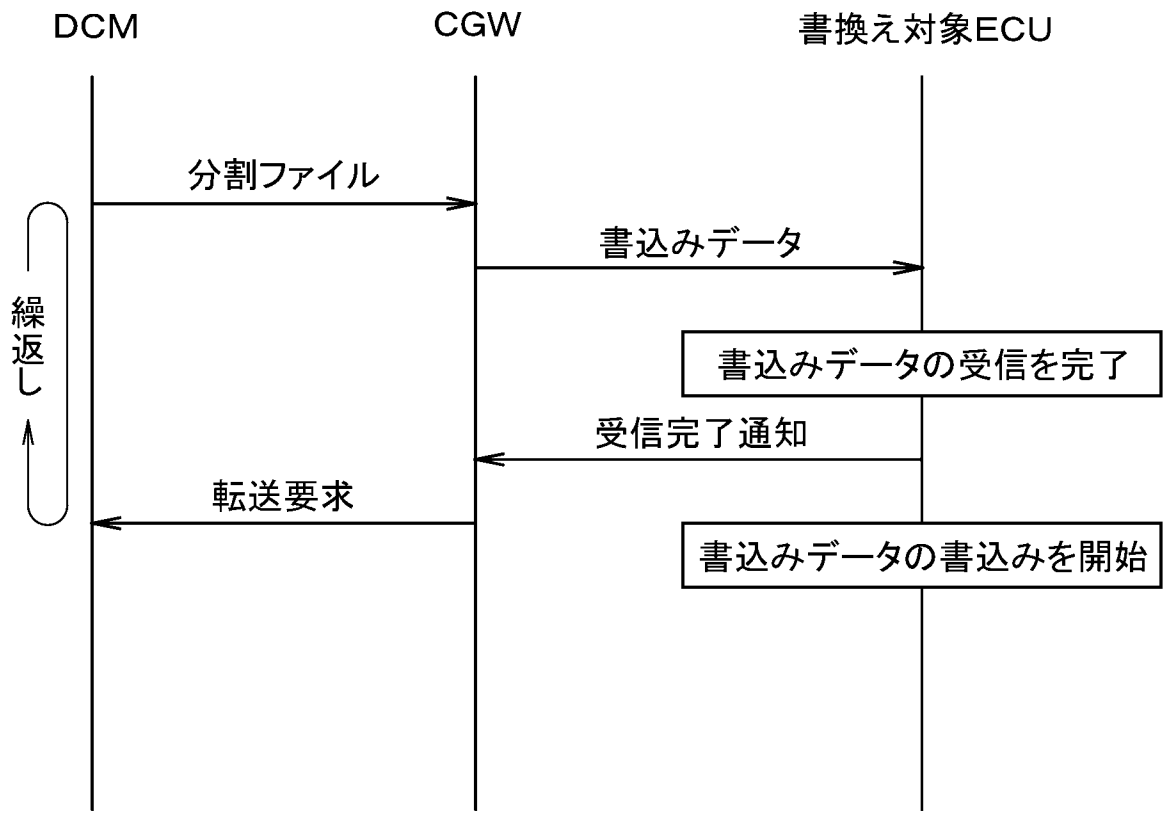
[図92]

Fig. 92



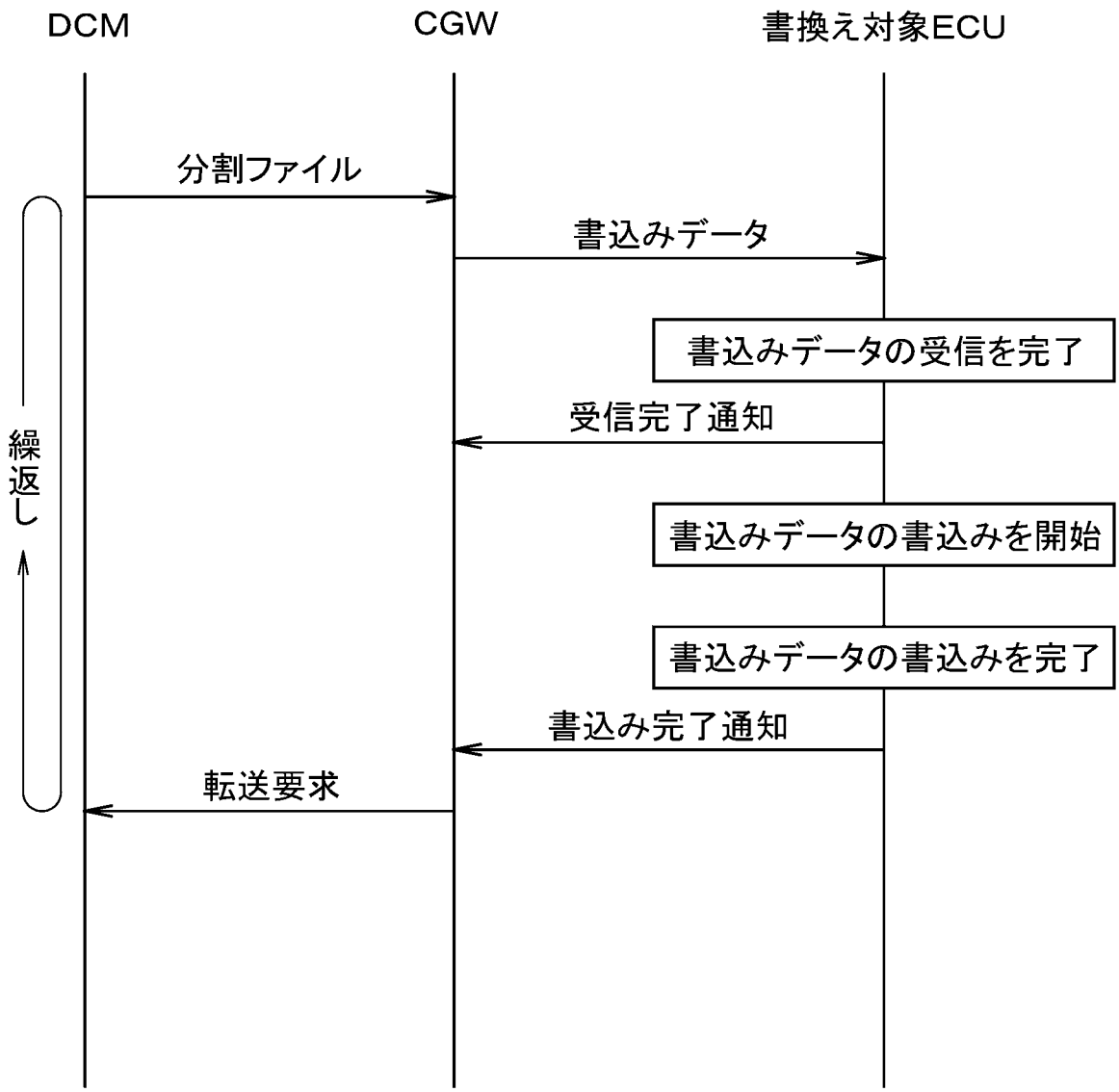
[図93]

Fig. 93


DCM
CGW
書換え対象ECU
分割ファイル
書込みデータ
繰返し
書込みデータの受信を完了
受信完了通知
転送要求
書込みデータの書込みを開始

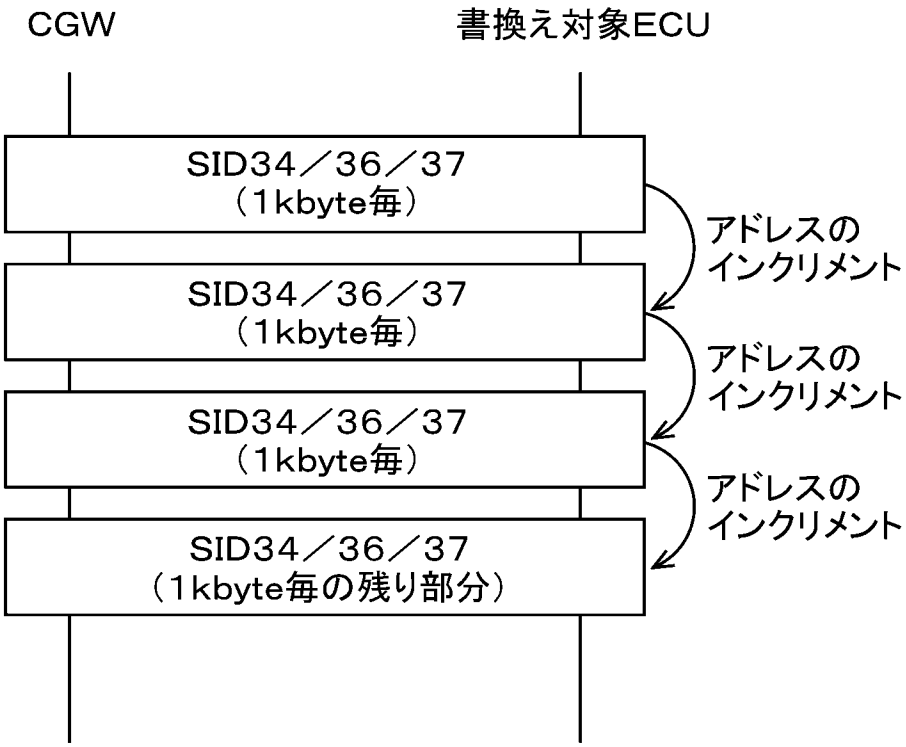
[図94]

Fig. 94


DCM
CGW
書換え対象ECU
分割ファイル
書込みデータ
書込みデータの受信を完了
受信完了通知
繰返し
書込みデータの書込みを開始
書込みデータの書込みを完了
書込み完了通知
転送要求

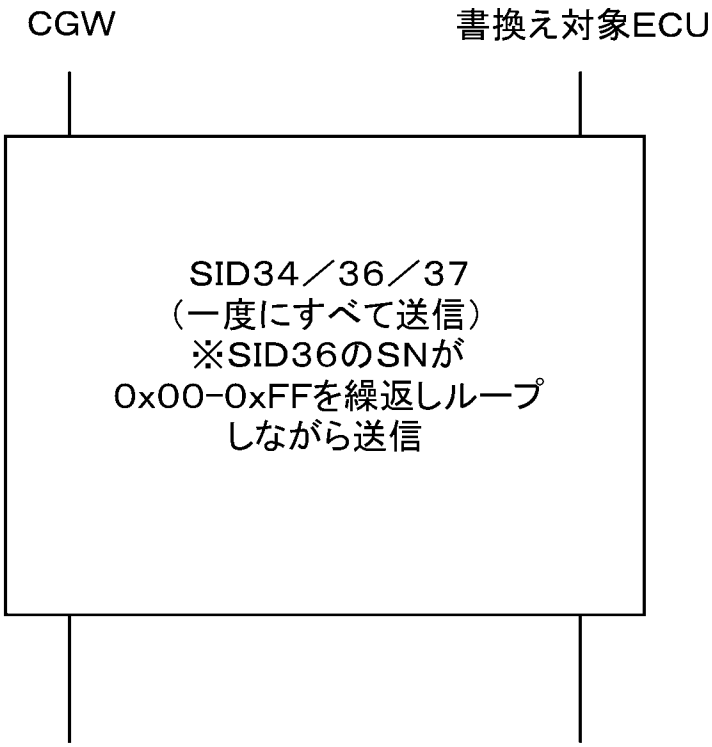
[図95]

Fig. 95



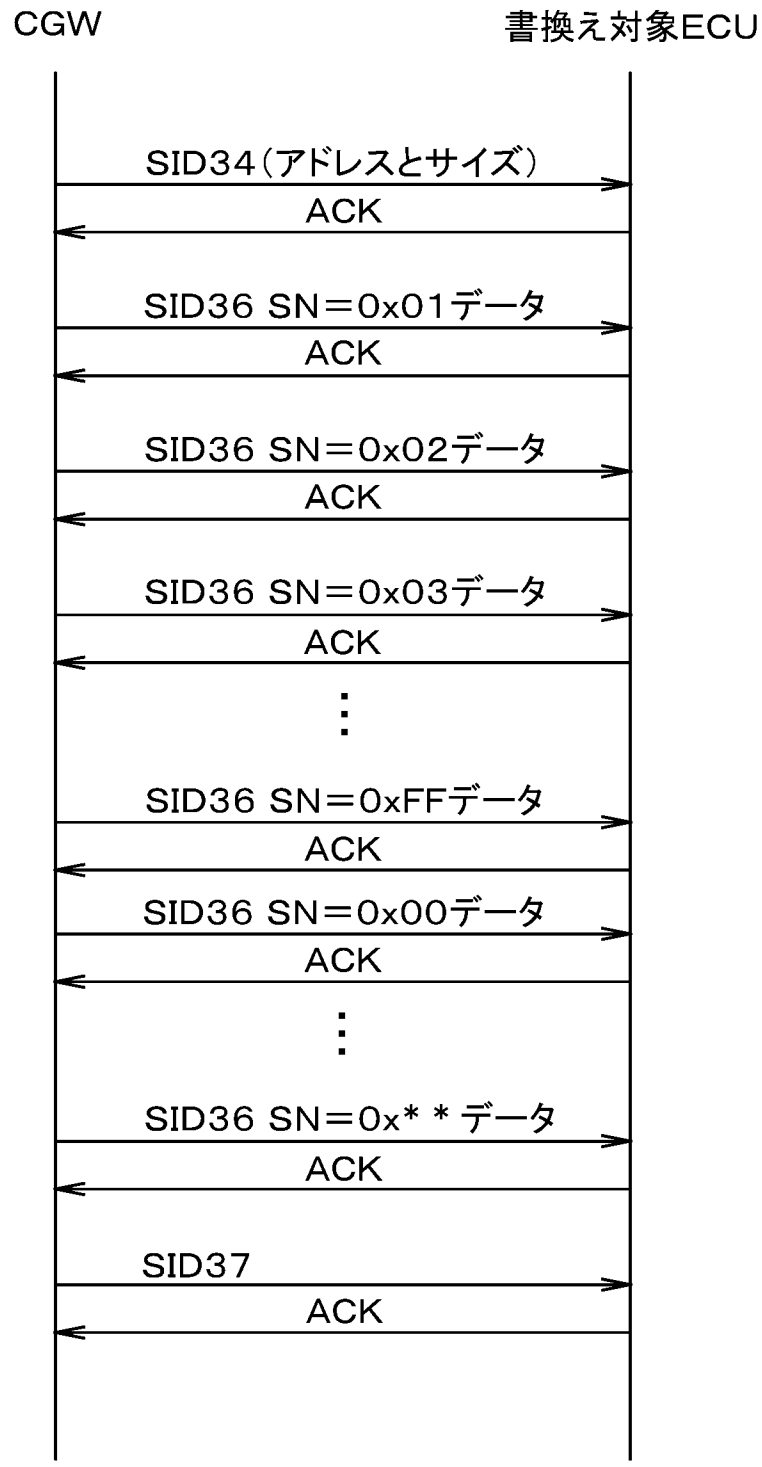
[図96]

Fig. 96



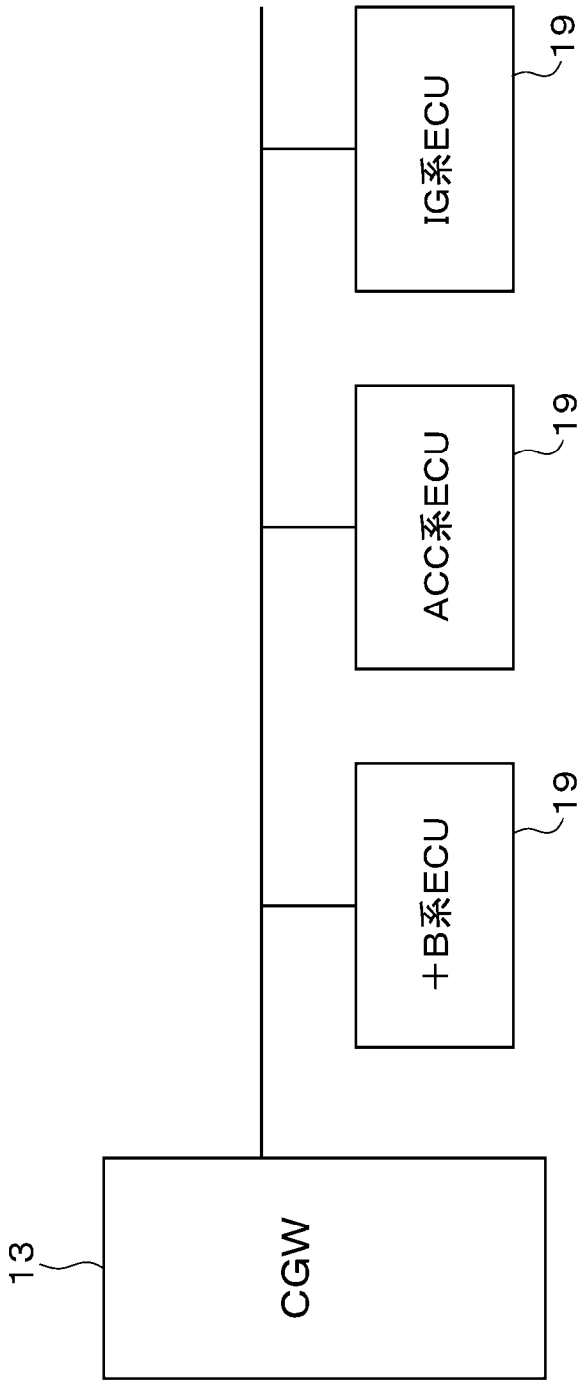
[図97]

Fig. 97


CGW
書換え対象ECU
SID34（アドレスとサイズ）
ACK
SID36 SN＝0x01データ
ACK
SID36 SN＝0x02データ
ACK
SID36 SN＝0x03データ
ACK
SID36 SN＝0xFFデータ
ACK
SID36 SN＝0x00データ
ACK
SID36 SN＝0x＊＊データ
ACK
SID37
ACK

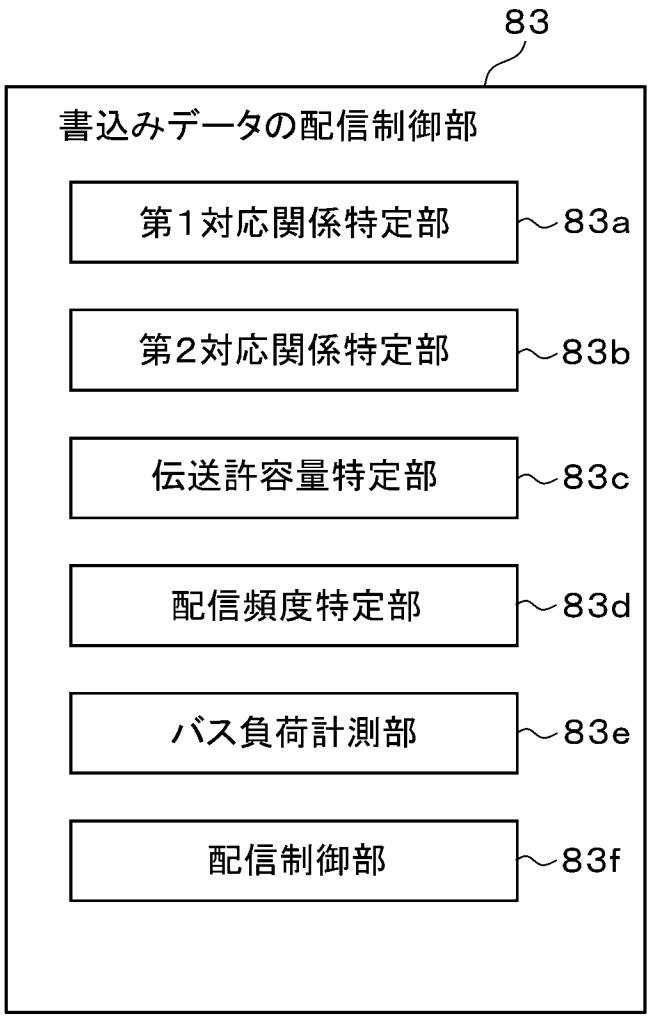
[図98]

Fig. 98



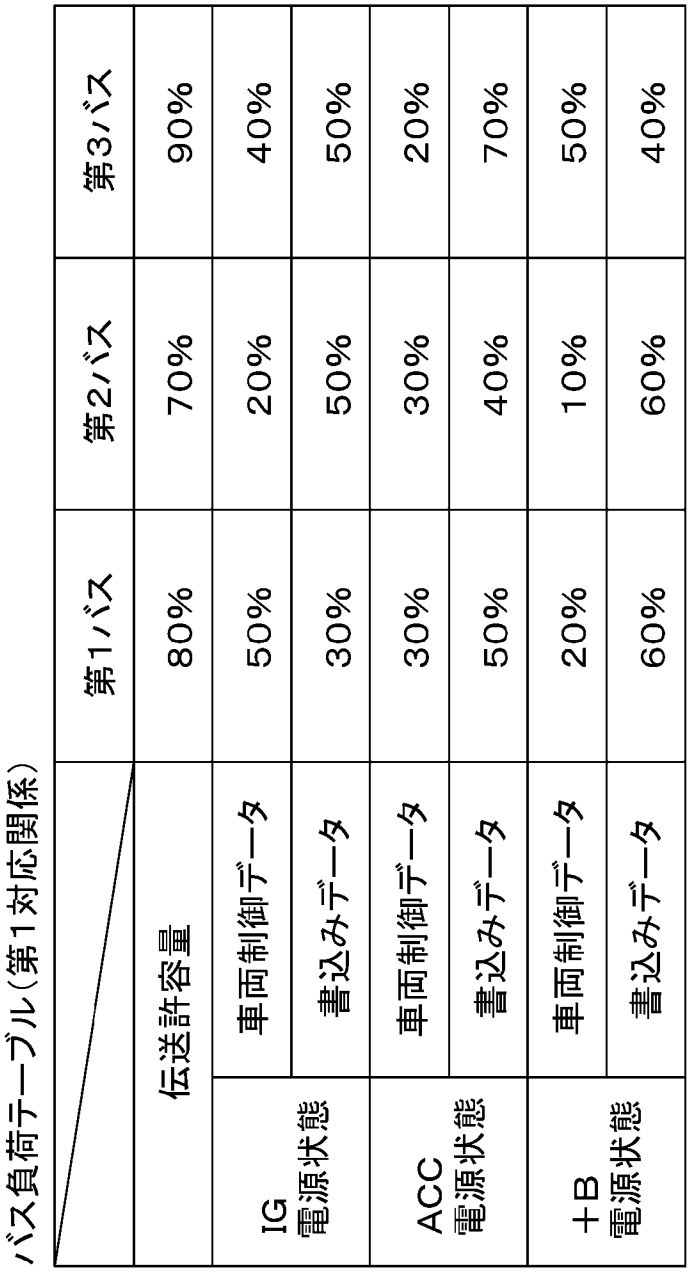
[図99]

Fig. 99


83
書込みデータの配信制御部
第1対応関係特定部
83a
第2対応関係特定部
83b
伝送許容量特定部
83c
配信頻度特定部
83d
バス負荷計測部
83e
配信制御部
83f

[図100]

Fig. 100



バス負荷テーブル（第1対応関係）

		第1バス	第2バス	第3バス
伝送許容量		80%	70%	90%
IG電源状態	車両制御データ	50%	20%	40%
	書込みデータ	30%	50%	50%
ACC電源状態	車両制御データ	30%	30%	20%
	書込みデータ	50%	40%	70%
+B電源状態	車両制御データ	20%	10%	50%
	書込みデータ	60%	60%	40%

[図101]

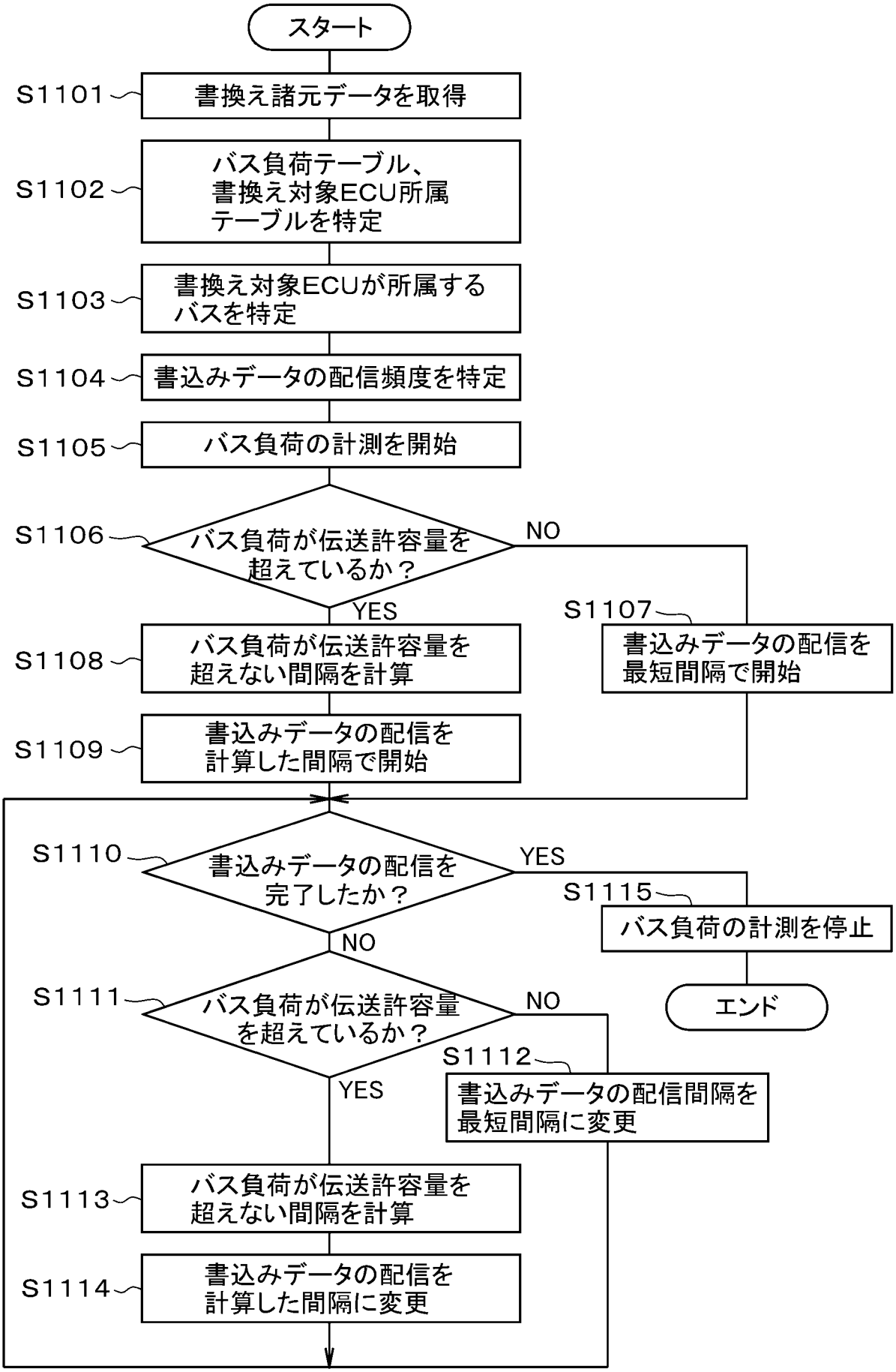
Fig. 101

書換え対象ECU所属テーブル(第2対応関係)

	所属バス	+B 電源状態	ACC 電源状態	IG 電源状態
第1書換え対象 ECU	第1バス	起動	起動	起動
第2書換え対象 ECU	第2バス	スリープ	起動	起動
第3書換え対象 ECU	第3バス	スリープ	スリープ	起動

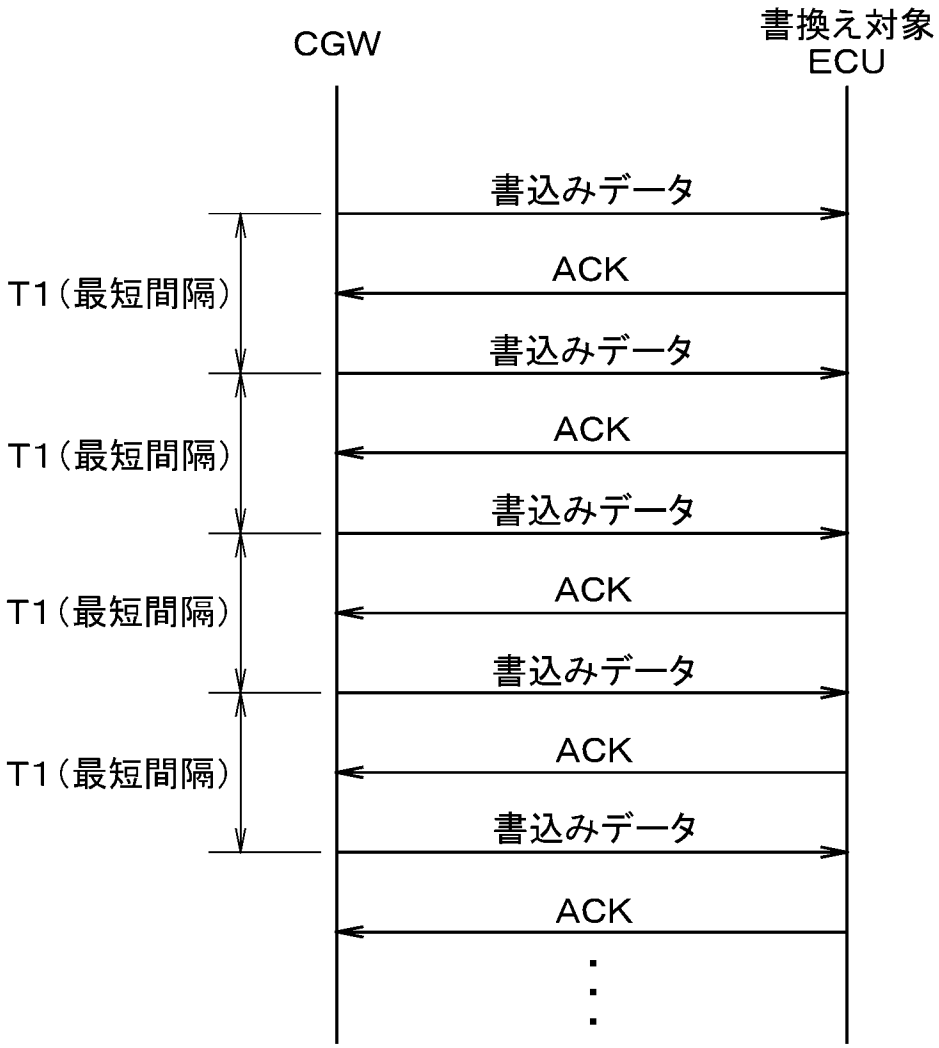
[図102]

Fig. 102 書込みデータの配信制御処理



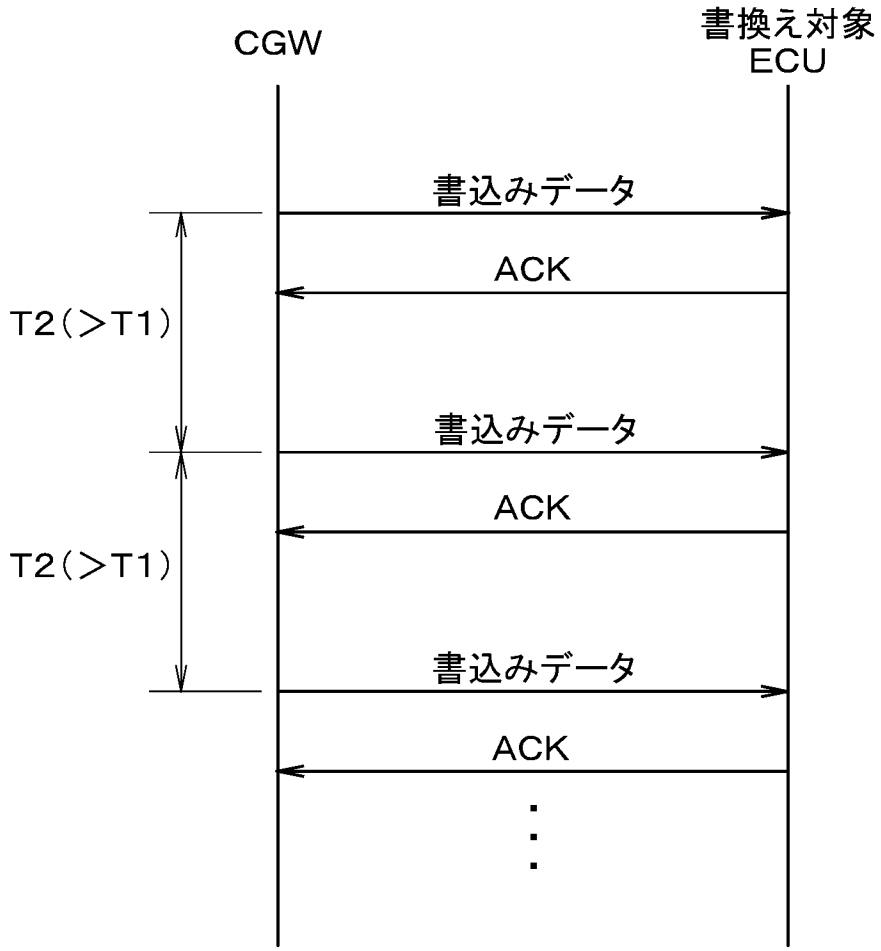
[図103]

Fig. 103


CGW
書換え対象
ECU
書込みデータ
ACK
書込みデータ
ACK
書込みデータ
ACK
書込みデータ
ACK
書込みデータ
ACK
T1（最短間隔）
T1（最短間隔）
T1（最短間隔）
T1（最短間隔）

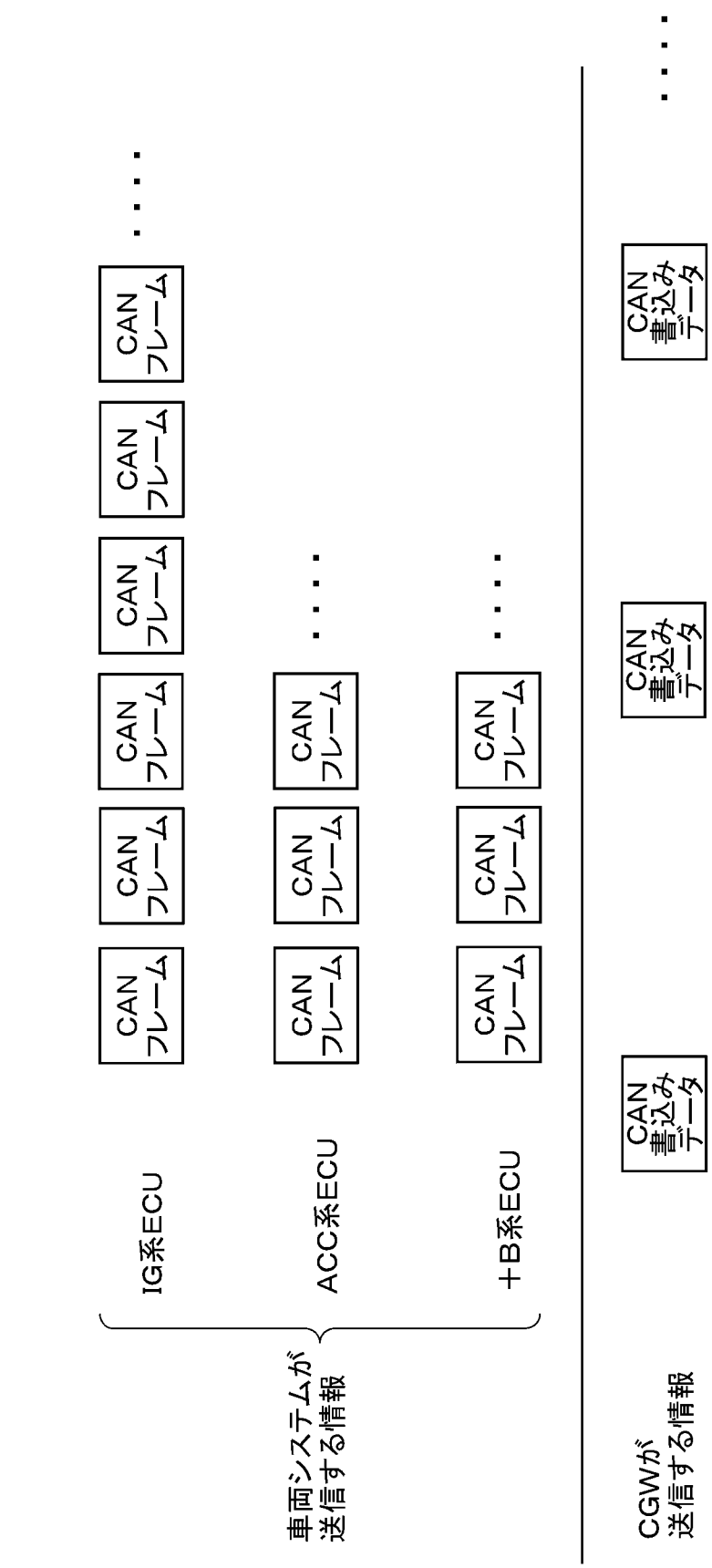
[図104]

Fig. 104



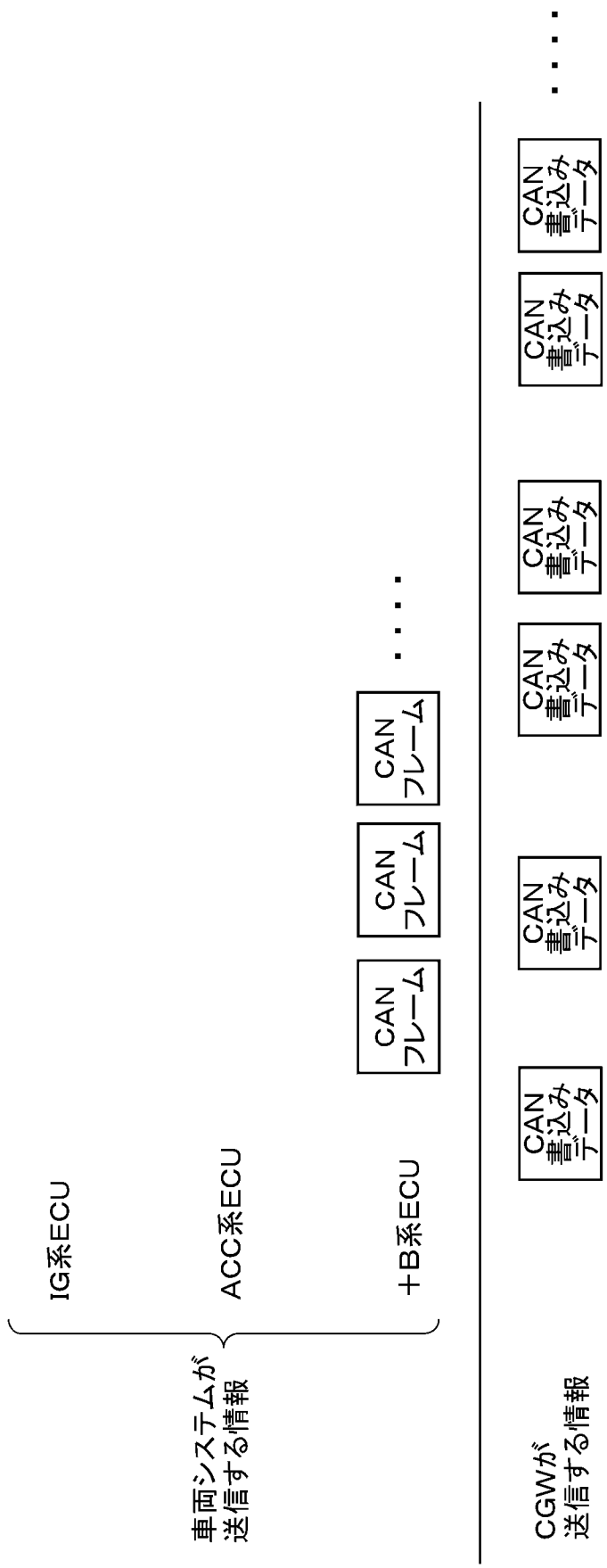
[図105]

Fig. 105


車両システムが
送信する情報
IG系ECU
ACC系ECU
＋B系ECU
CAN
フレーム
CGWが
送信する情報
CAN
書込み
データ

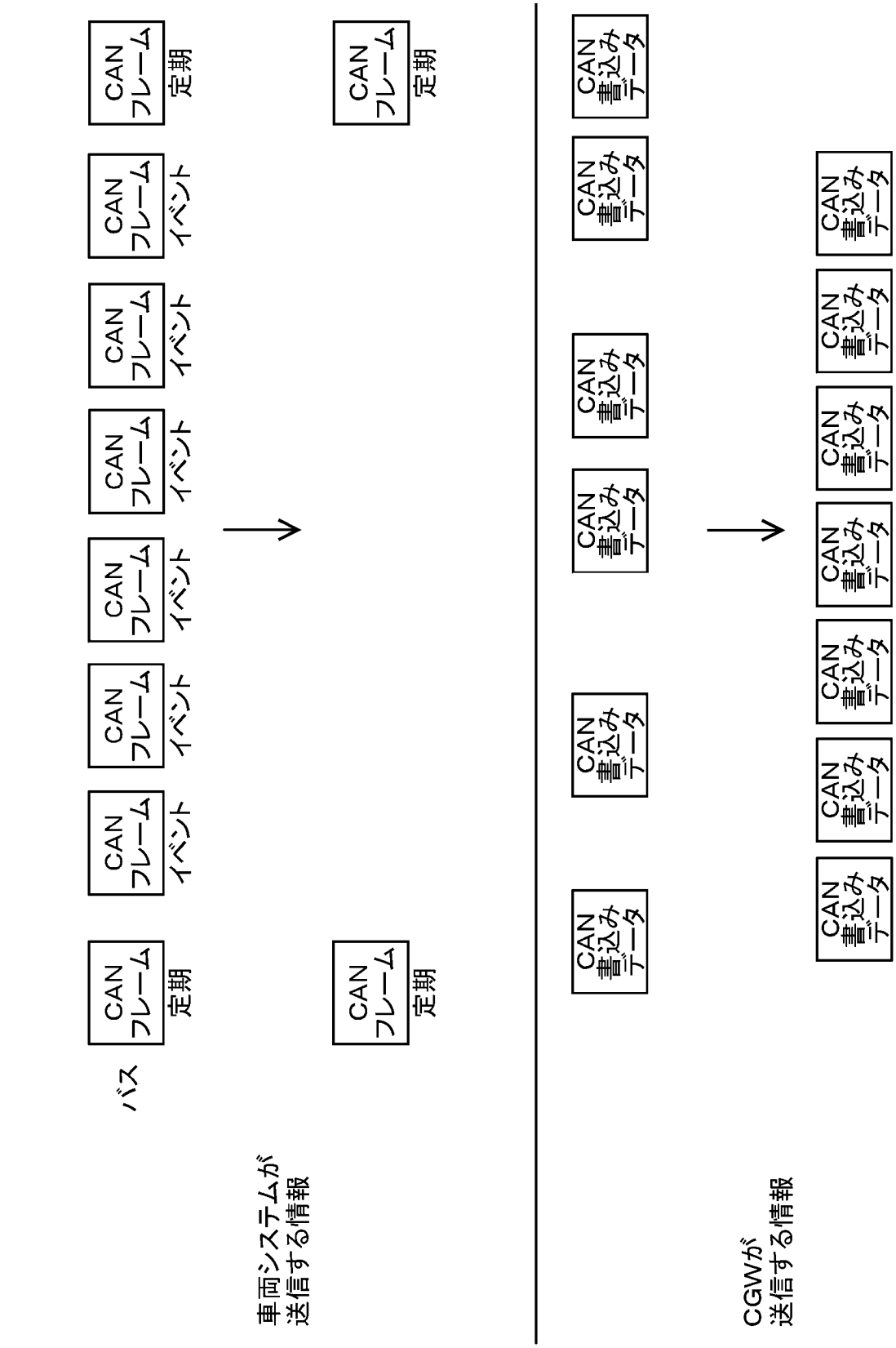
[図106]

Fig. 106


車両システムが送信する情報
IG系ECU
ACC系ECU
+B系ECU
CANフレーム
CANフレーム
CANフレーム
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CGWが送信する情報

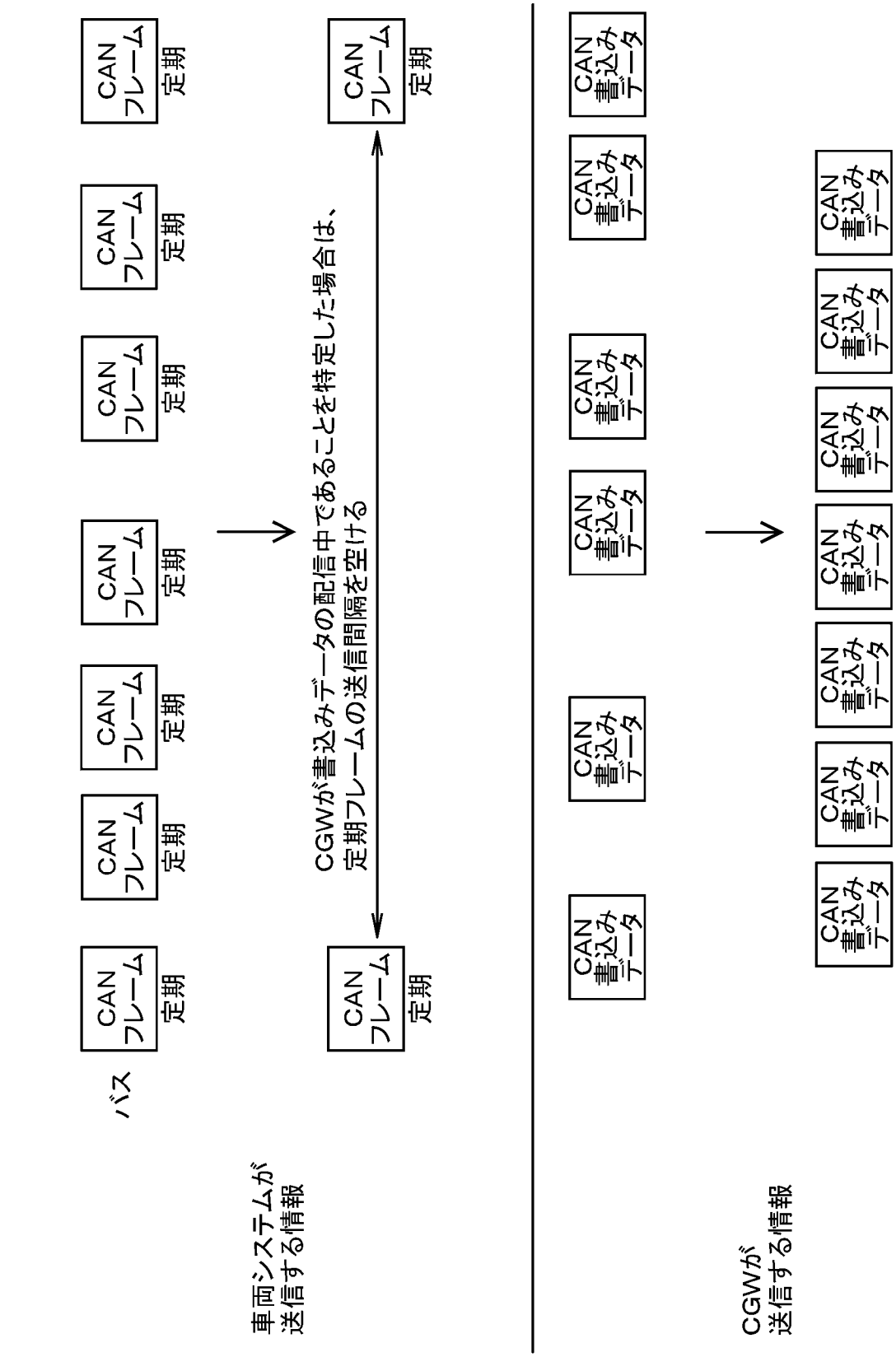
[図107]

Fig. 107


バス
CANフレーム 定期
CANフレーム イベント
CANフレーム イベント
CANフレーム イベント
CANフレーム イベント
CANフレーム イベント
CANフレーム 定期
CANフレーム 定期
車両システムが送信する情報
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CAN書込みデータ
CGWが送信する情報

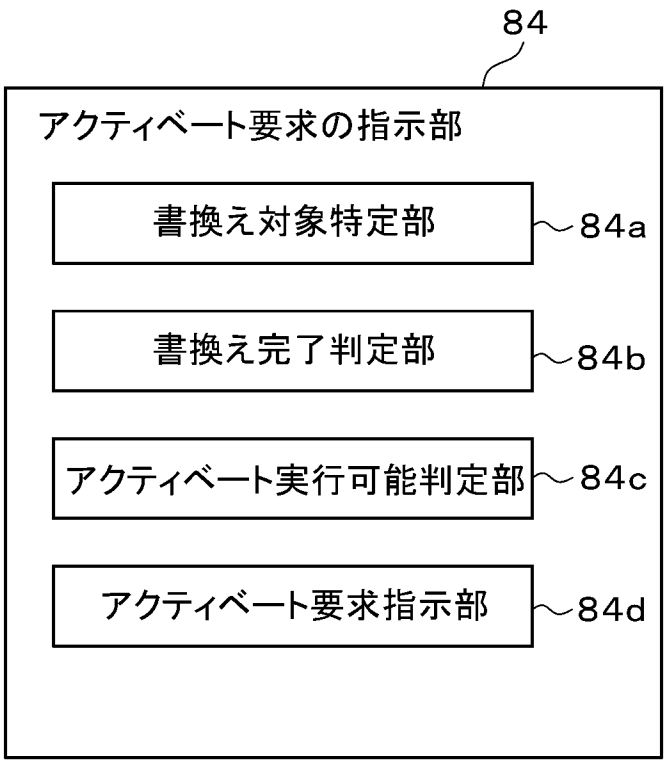
[図108]

Fig. 108


バス
CANフレーム 定期
CANフレーム 定期
CANフレーム 定期
CANフレーム 定期
CANフレーム 定期
CANフレーム 定期
CANフレーム 定期
CANフレーム 定期
CGWが書込みデータの配信中であることを特定した場合は、
定期フレームの送信間隔を空ける
車両システムが
送信する情報
CAN
書込み
データ
CGWが
送信する情報

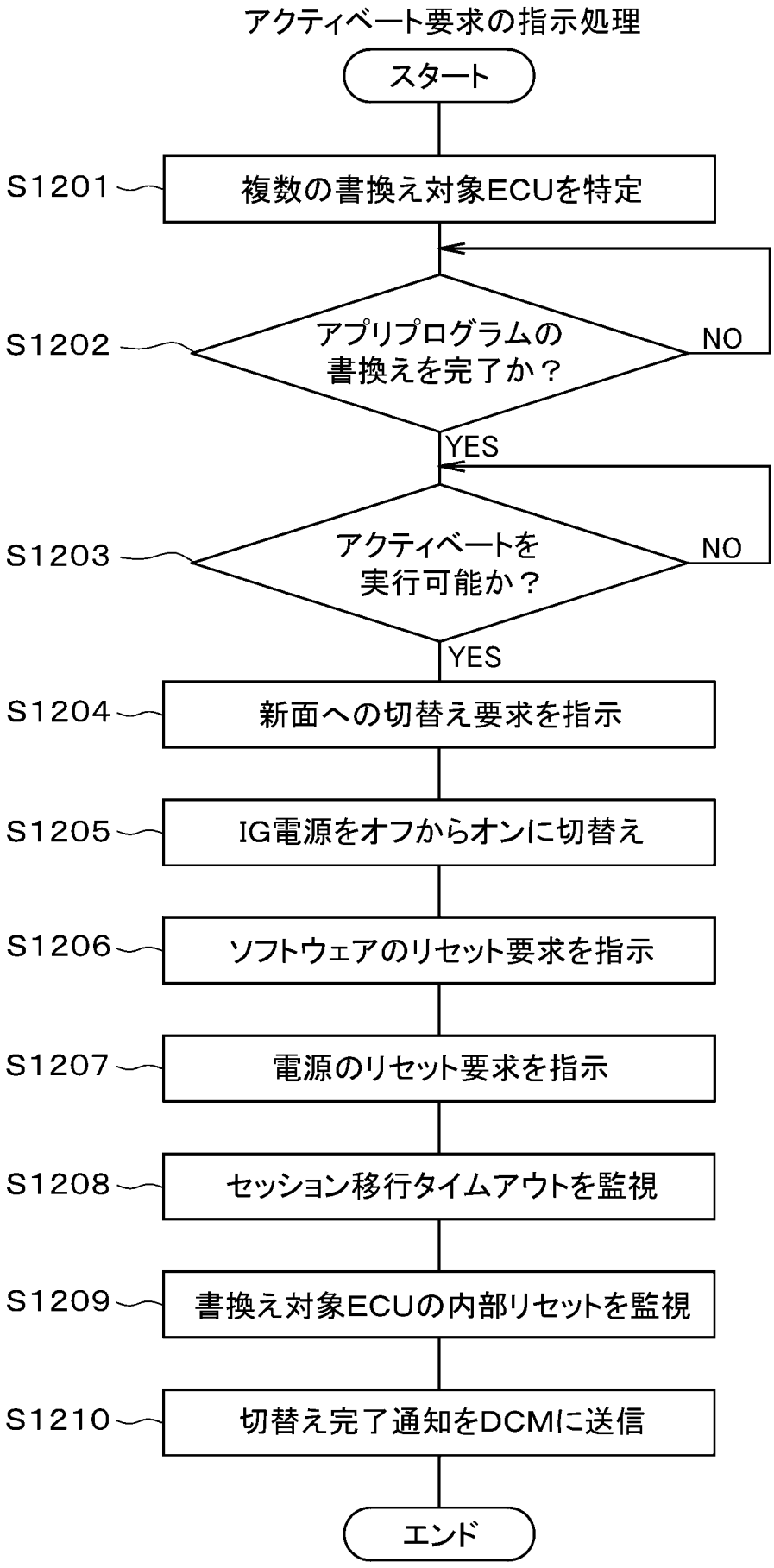
[図109]

Fig. 109


84
アクティベート要求の指示部
書換え対象特定部
84a
書換え完了判定部
84b
アクティベート実行可能判定部
84c
アクティベート要求指示部
84d

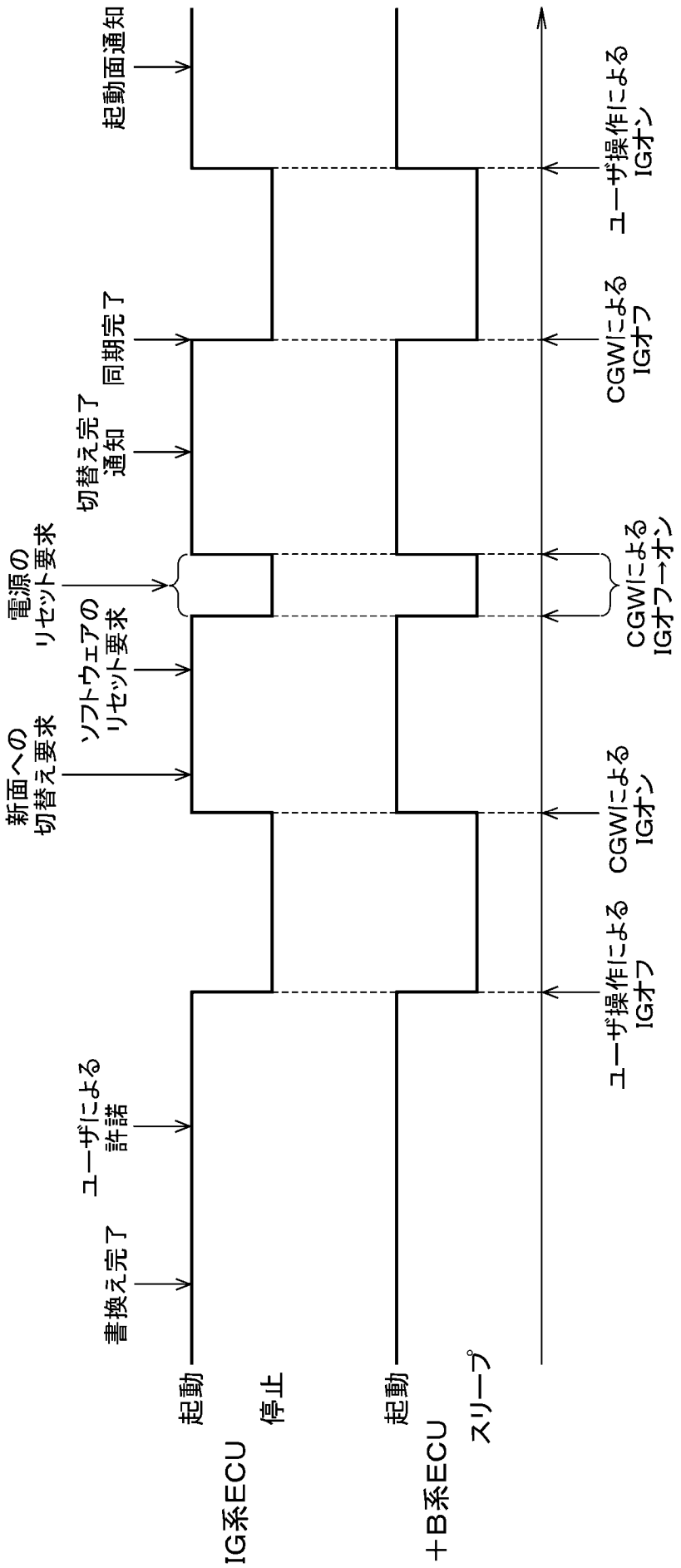
[図110]

Fig. 110


アクティベート要求の指示処理
スタート
S1201
複数の書換え対象ECUを特定
S1202
アプリプログラムの
書換えを完了か？
NO
YES
S1203
アクティベートを
実行可能か？
NO
YES
S1204
新面への切替え要求を指示
S1205
IG電源をオフからオンに切替え
S1206
ソフトウェアのリセット要求を指示
S1207
電源のリセット要求を指示
S1208
セッション移行タイムアウトを監視
S1209
書換え対象ECUの内部リセットを監視
S1210
切替え完了通知をDCMに送信
エンド

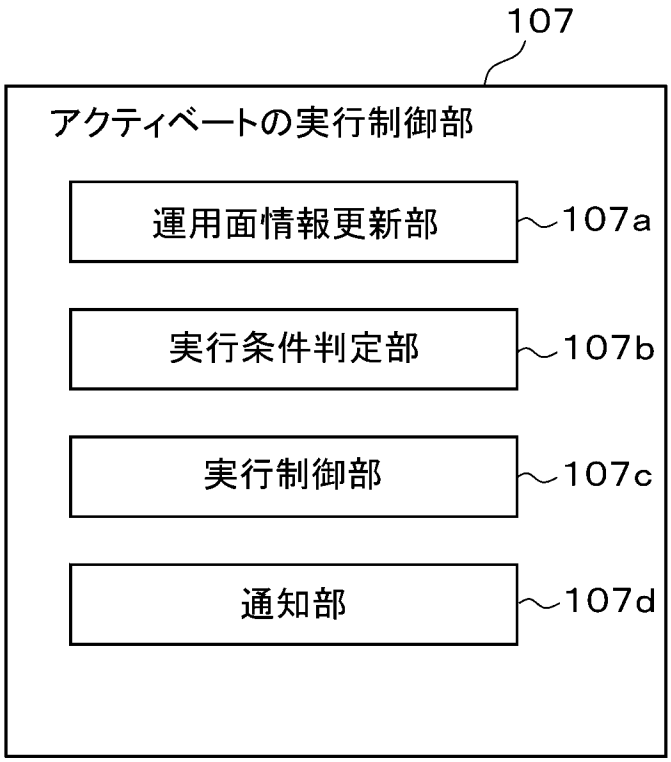
[図111]

Fig. 111


IG系ECU
起動
停止
＋B系ECU
起動
スリープ
書換え完了
ユーザによる許諾
新面への切替え要求
電源のリセット要求
ソフトウェアのリセット要求
切替え完了通知
同期完了
起動面通知
ユーザ操作によるIGオフ
CGWによるIGオン
CGWによるIGオフ
CGWによるIGオフ→オン
ユーザ操作によるIGオン

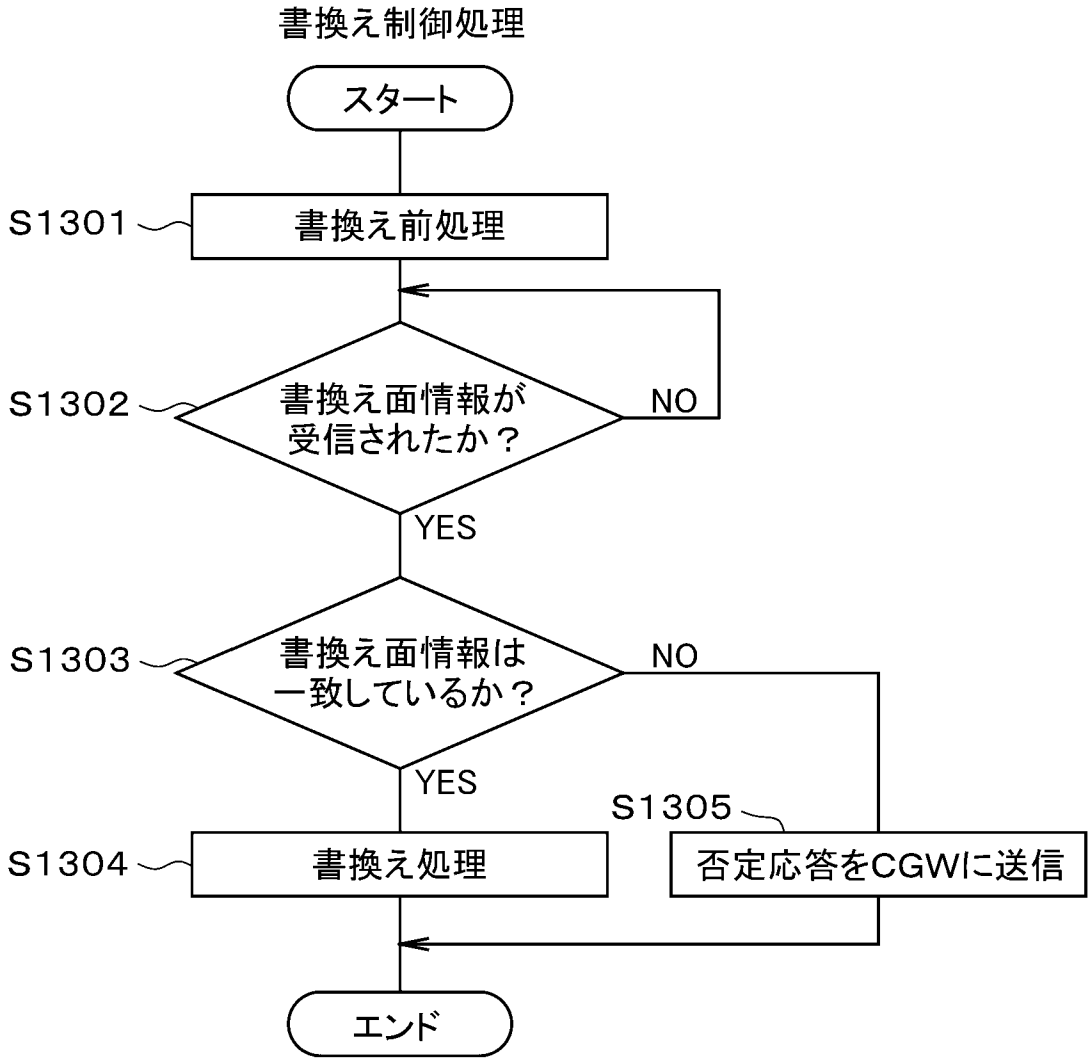
[図112]

Fig. 112


107
アクティベートの実行制御部
運用面情報更新部
107a
実行条件判定部
107b
実行制御部
107c
通知部
107d

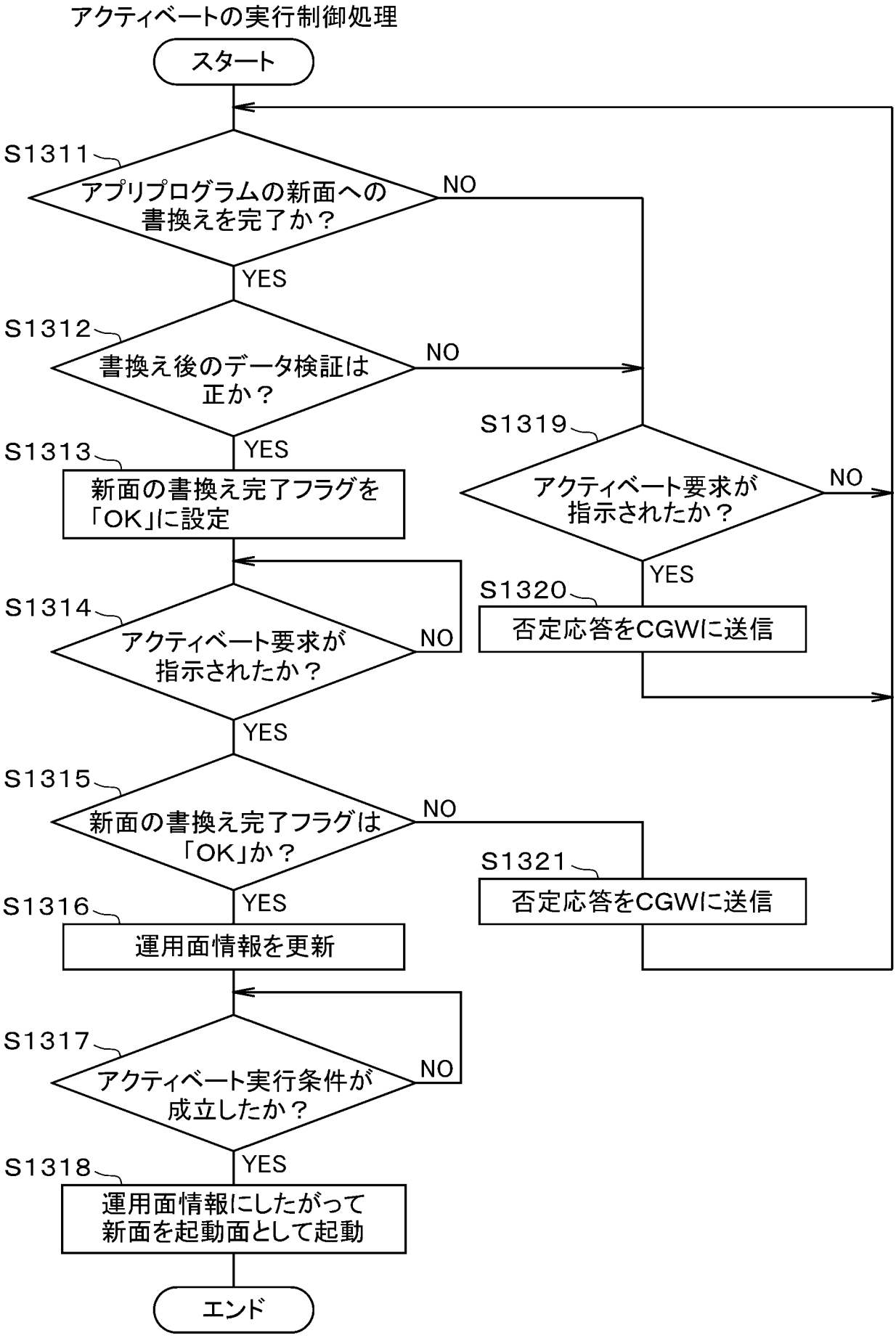
[図113]

Fig. 113


書換え制御処理
スタート
S1301
書換え前処理
S1302
書換え面情報が
受信されたか？
NO
YES
S1303
書換え面情報は
一致しているか？
NO
YES
S1305
S1304
書換え処理
否定応答をCGWに送信
エンド

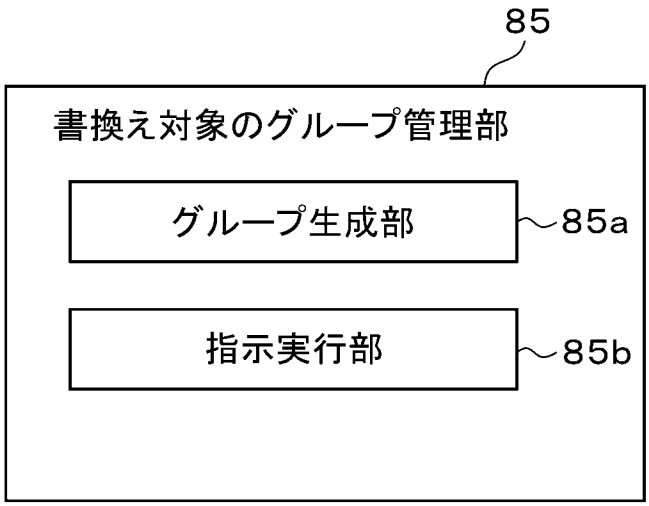
[図114]

Fig. 114


アクティベートの実行制御処理
スタート
S1311
アプリプログラムの新面への書換えを完了か？
NO
YES
S1312
書換え後のデータ検証は正か？
NO
YES
S1313
新面の書換え完了フラグを「OK」に設定
S1314
アクティベート要求が指示されたか？
NO
YES
S1315
新面の書換え完了フラグは「OK」か？
NO
YES
S1316
運用面情報を更新
S1317
アクティベート実行条件が成立したか？
NO
YES
S1318
運用面情報にしたがって新面を起動面として起動
エンド
S1319
アクティベート要求が指示されたか？
NO
YES
S1320
否定応答をCGWに送信
S1321
否定応答をCGWに送信

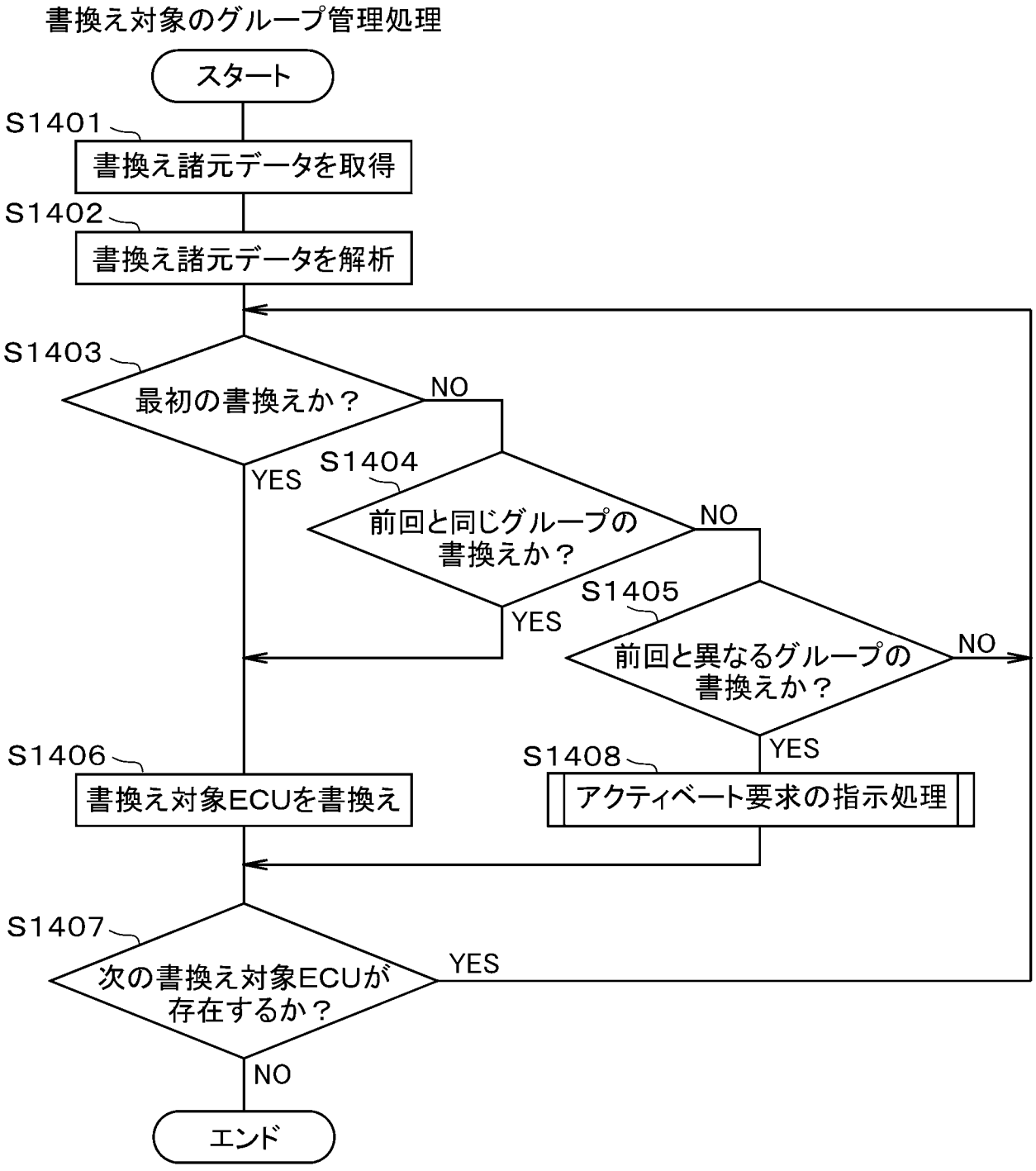
[図115]

Fig. 115



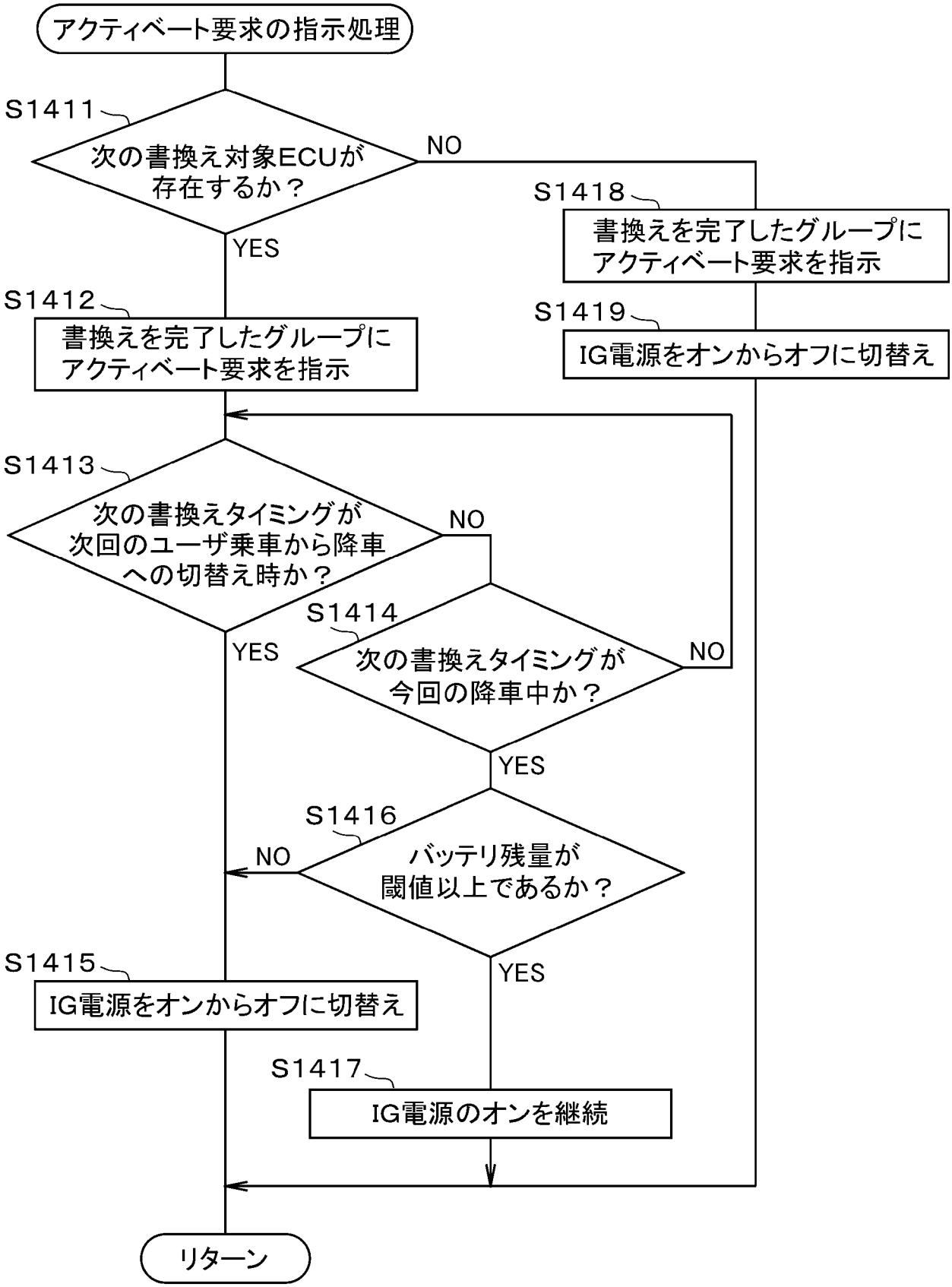
[図116]

Fig. 116


書換え対象のグループ管理処理
スタート
S1401
書換え諸元データを取得
S1402
書換え諸元データを解析
S1403
最初の書換えか？
NO
YES
S1404
前回と同じグループの書換えか？
NO
YES
S1405
前回と異なるグループの書換えか？
NO
YES
S1406
書換え対象ECUを書換え
S1408
アクティベート要求の指示処理
S1407
次の書換え対象ECUが存在するか？
YES
NO
エンド

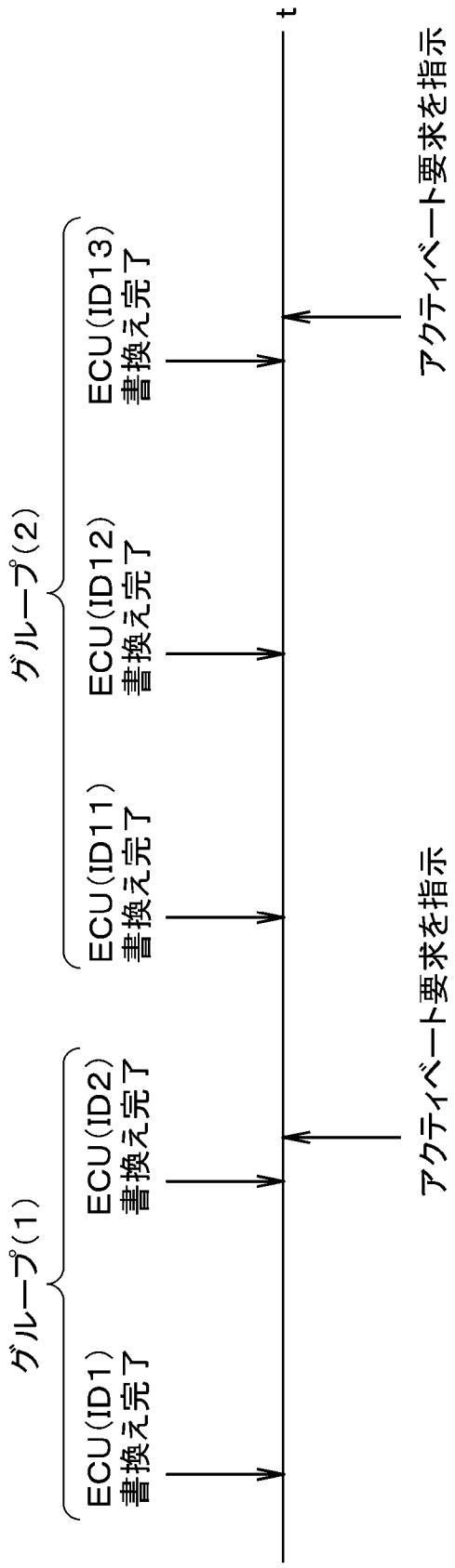
[図117]

Fig. 117


アクティベート要求の指示処理
S1411
次の書換え対象ECUが存在するか？
NO
YES
S1418
書換えを完了したグループにアクティベート要求を指示
S1419
IG電源をオンからオフに切替え
S1412
書換えを完了したグループにアクティベート要求を指示
S1413
次の書換えタイミングが次回のユーザ乗車から降車への切替え時か？
NO
YES
S1414
次の書換えタイミングが今回の降車中か？
NO
YES
S1416
バッテリ残量が閾値以上であるか？
NO
YES
S1415
IG電源をオンからオフに切替え
S1417
IG電源のオンを継続
リターン

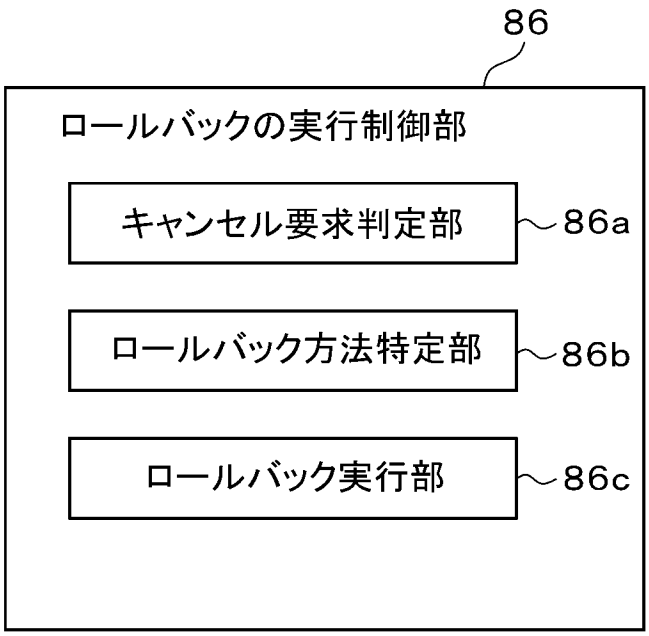
[図118]

Fig. 118


t
グループ(1)
ECU(ID1)
書換え完了
ECU(ID2)
書換え完了
アクティベート要求を指示
グループ(2)
ECU(ID11)
書換え完了
ECU(ID12)
書換え完了
ECU(ID13)
書換え完了
アクティベート要求を指示

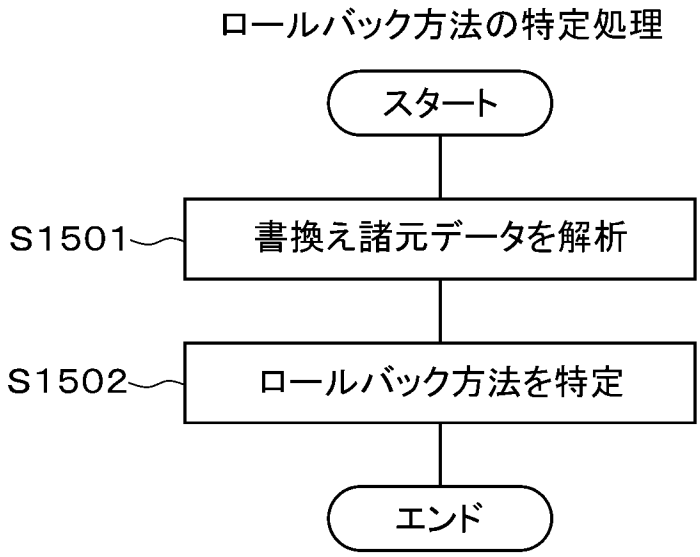
[図119]

Fig. 119



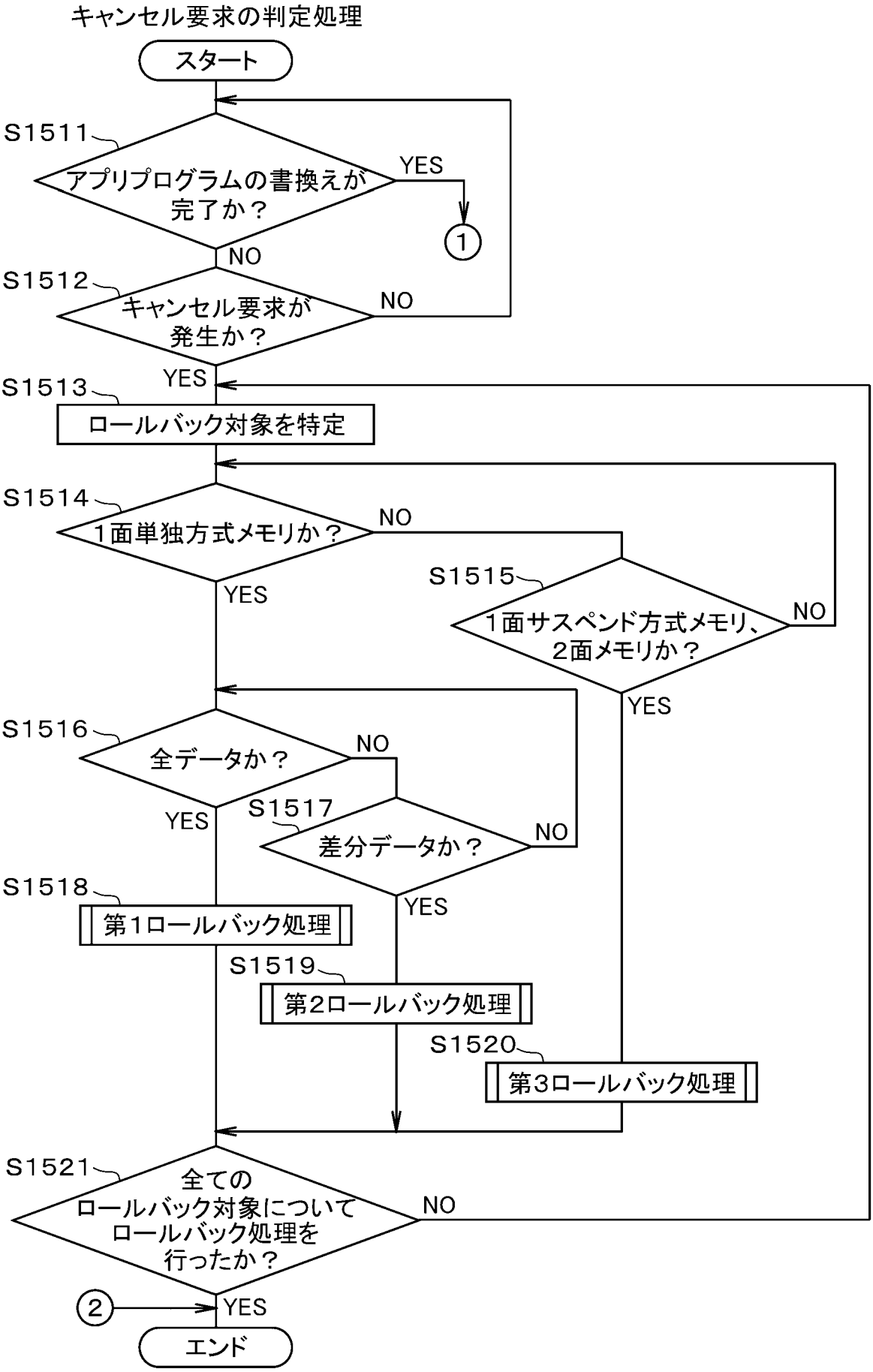
[図120]

Fig. 120



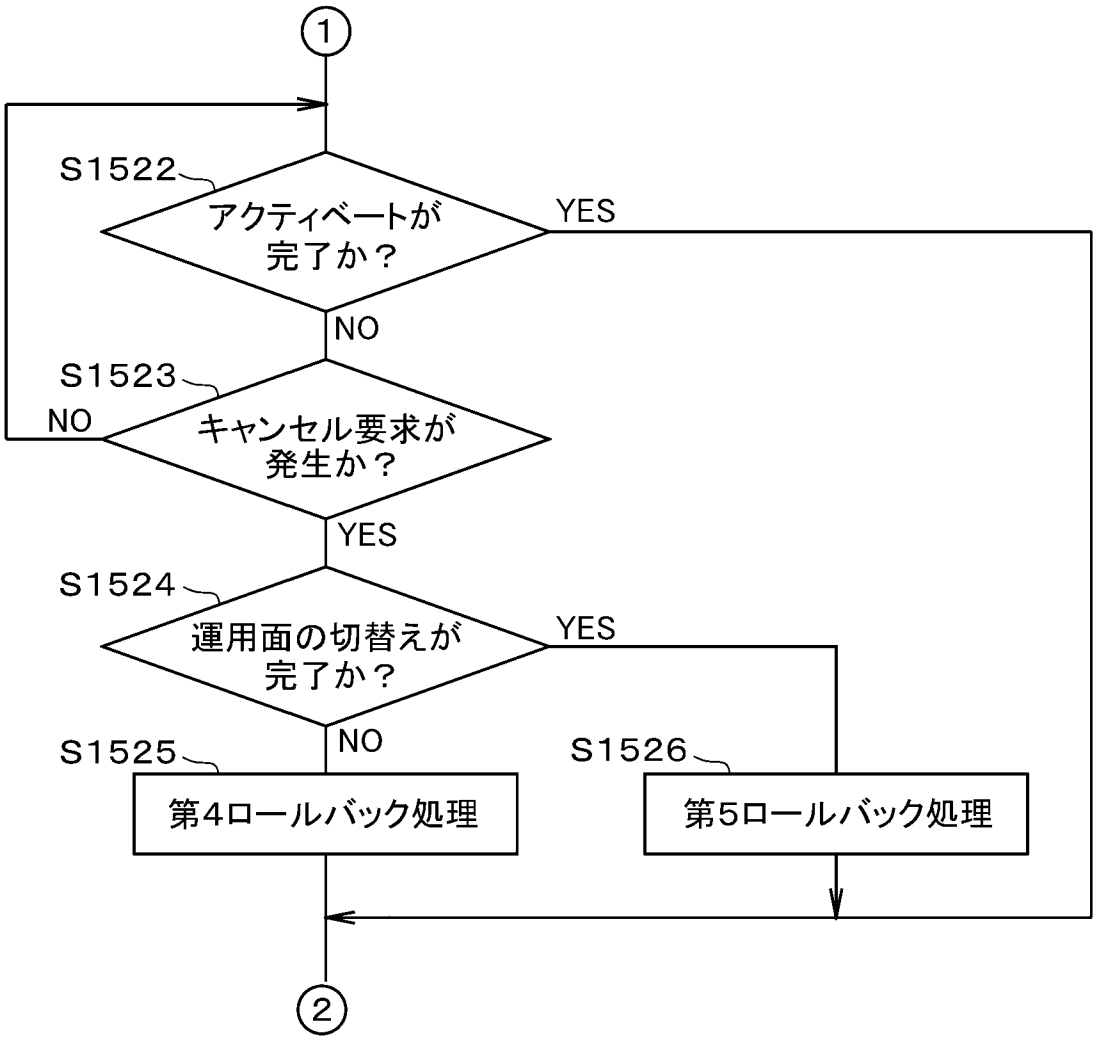
[図121]

Fig. 121


キャンセル要求の判定処理
スタート
S1511
アプリプログラムの書換えが完了か？
YES
1
NO
S1512
キャンセル要求が発生か？
NO
YES
S1513
ロールバック対象を特定
S1514
1面単独方式メモリか？
NO
YES
S1515
1面サスペンド方式メモリ、2面メモリか？
NO
YES
S1516
全データか？
NO
YES
S1517
差分データか？
NO
YES
S1518
第1ロールバック処理
S1519
第2ロールバック処理
S1520
第3ロールバック処理
S1521
全てのロールバック対象についてロールバック処理を行ったか？
NO
2
YES
エンド

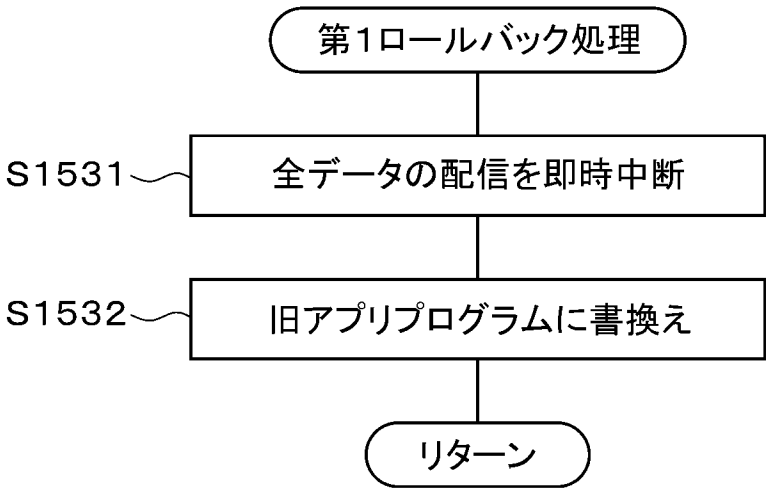
[図122]

Fig. 122



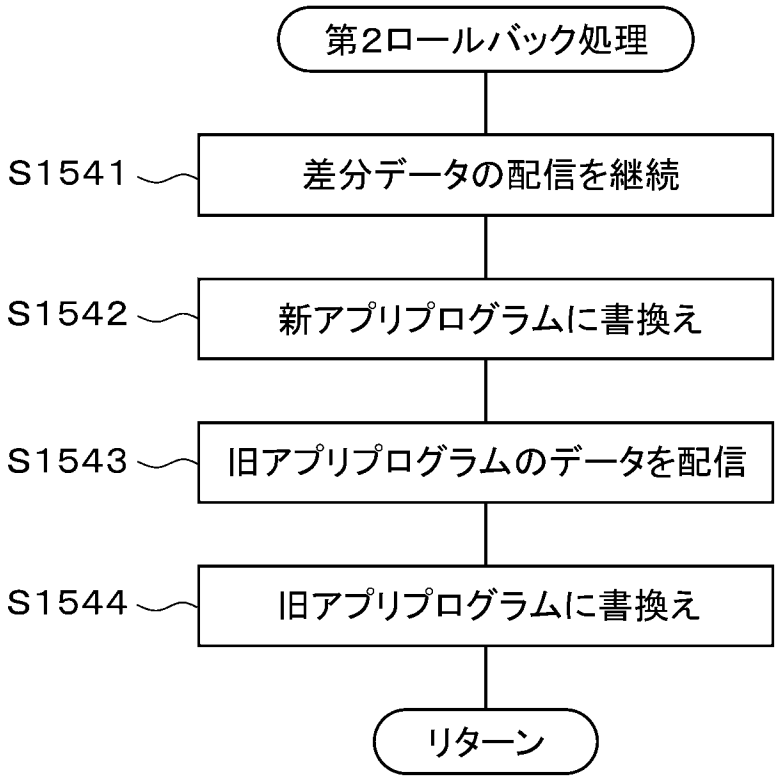
[図123]

Fig. 123



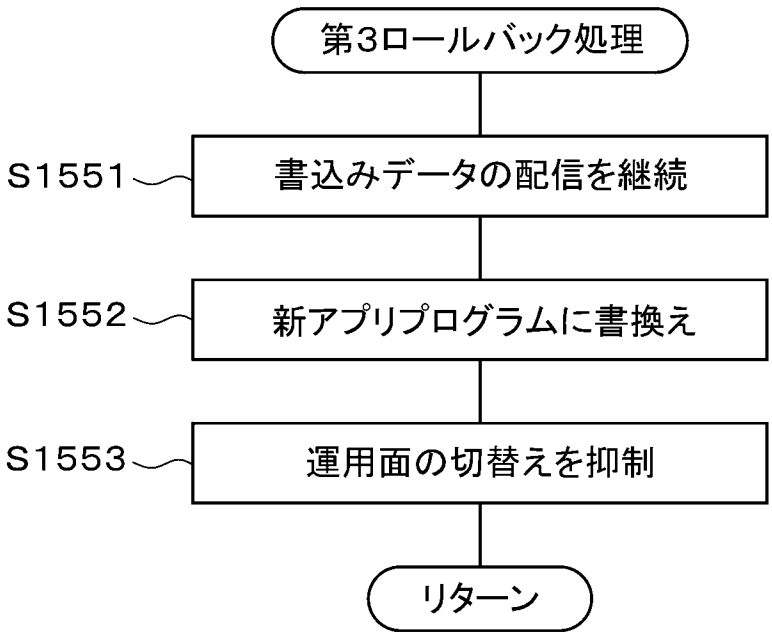
[図124]

Fig. 124



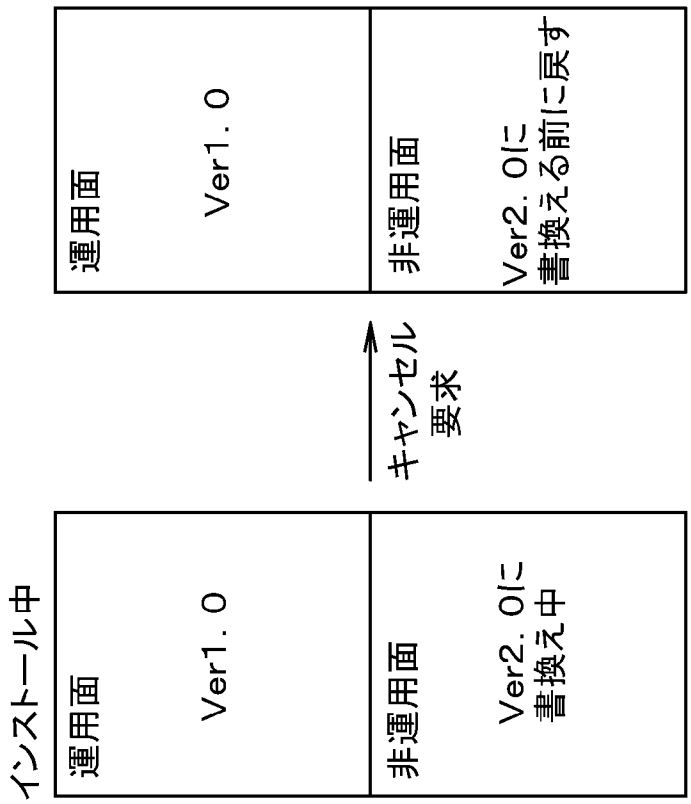
[図125]

Fig. 125



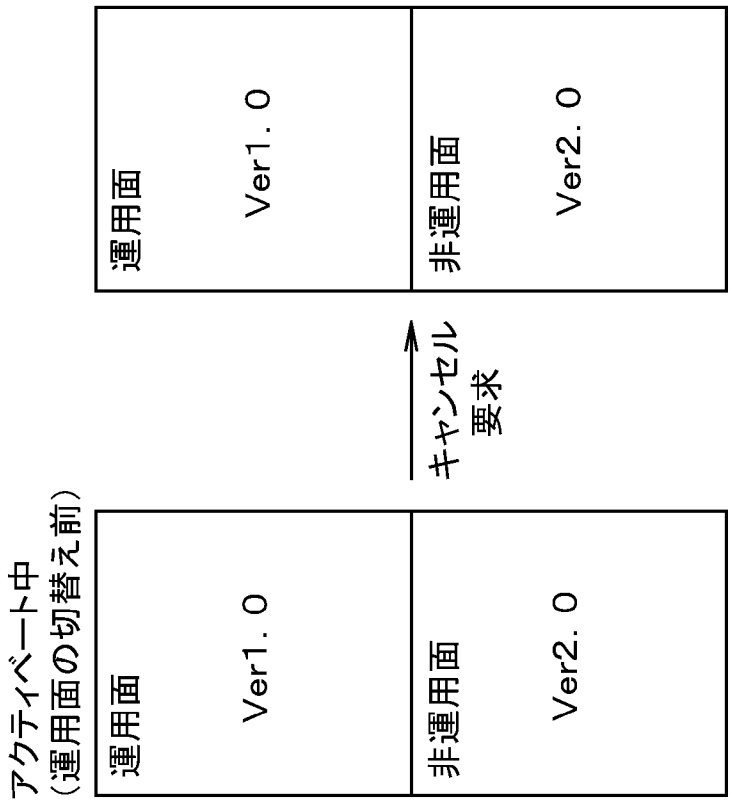
[図126]

Fig. 126


インストール中
運用面
Ver1．0
非運用面
Ver2．0に
書換え中
キャンセル
要求
運用面
Ver1．0
非運用面
Ver2．0に
書換える前に戻す

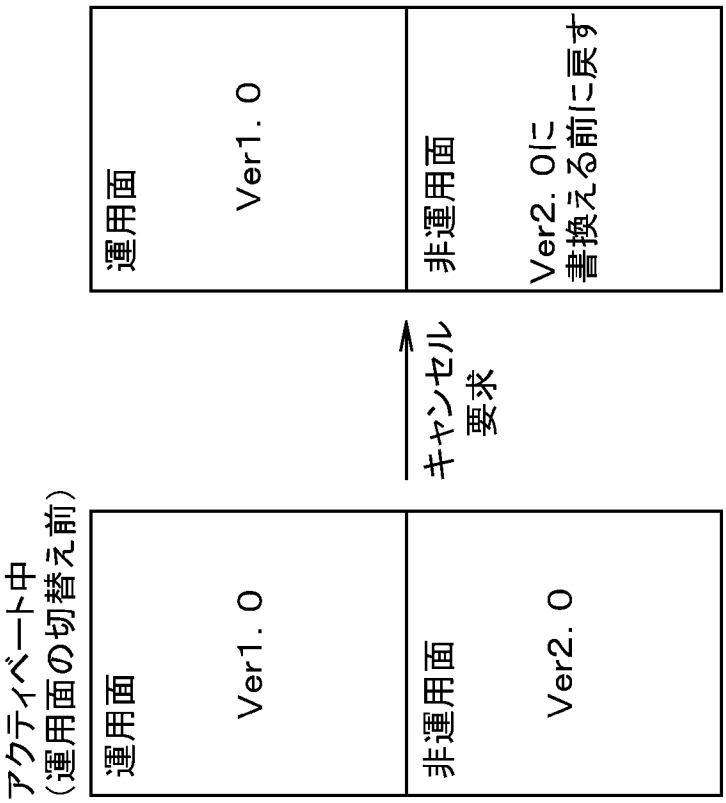
[図127]

Fig. 127


アクティベート中
（運用面の切替え前）
運用面
Ver1.0
非運用面
Ver2.0
キャンセル
要求
運用面
Ver1.0
非運用面
Ver2.0

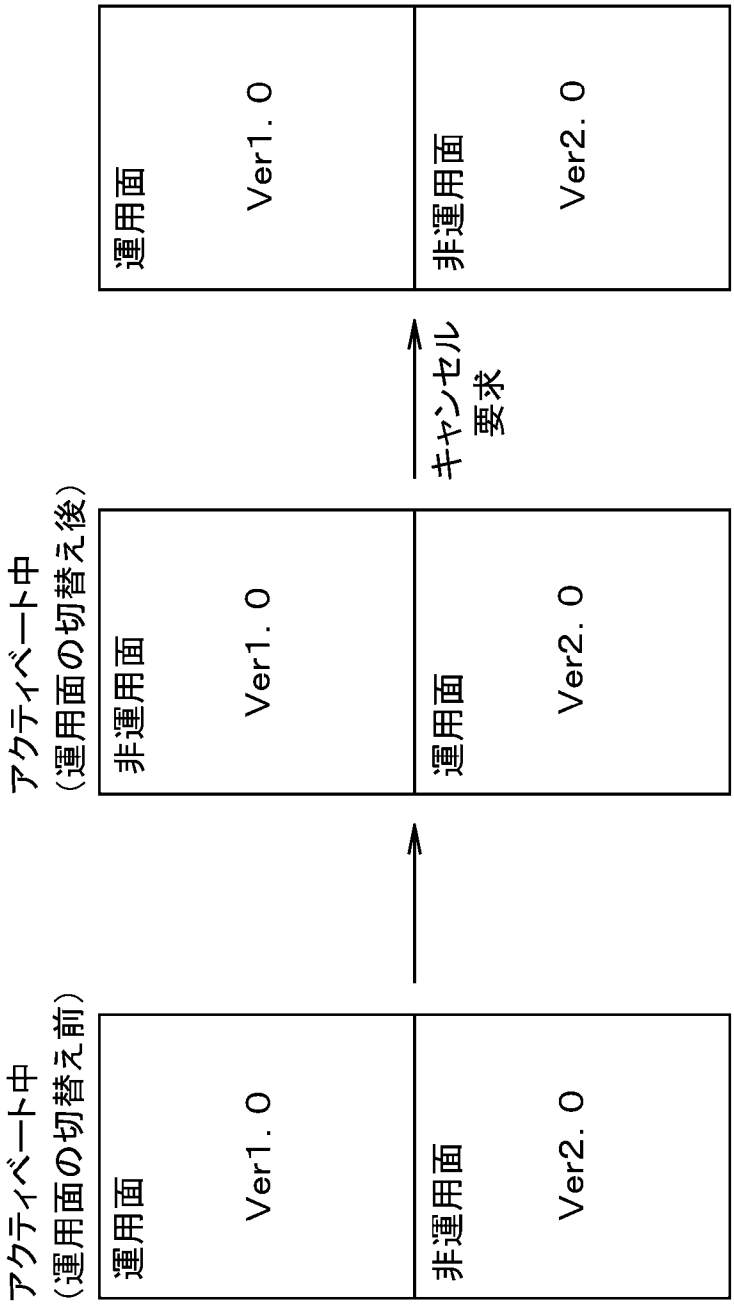
[図128]

Fig. 128


アクティベート中
(運用面の切替え前)
運用面
Ver1.0
非運用面
Ver2.0
キャンセル
要求
運用面
Ver1.0
非運用面
Ver2.0に
書換える前に戻す

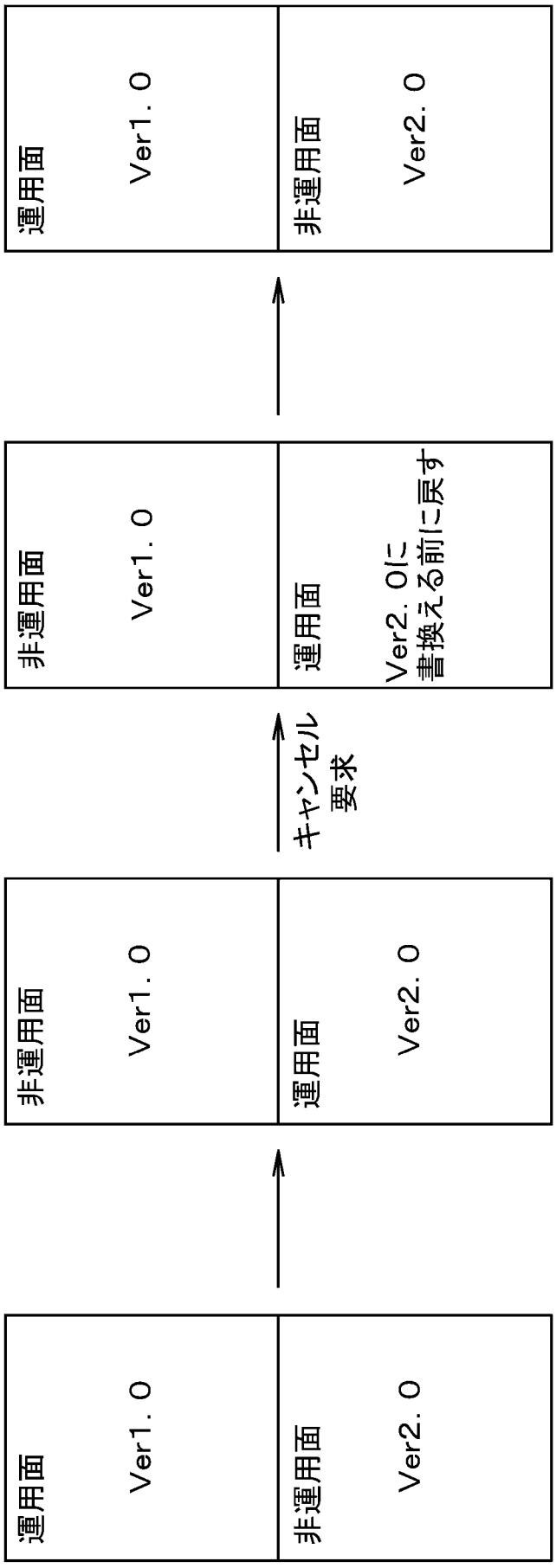
[図129]

Fig. 129


アクティベート中
（運用面の切替え前）
運用面
Ver1．0
非運用面
Ver2．0
アクティベート中
（運用面の切替え後）
非運用面
Ver1．0
運用面
Ver2．0
キャンセル
要求
運用面
Ver1．0
非運用面
Ver2．0

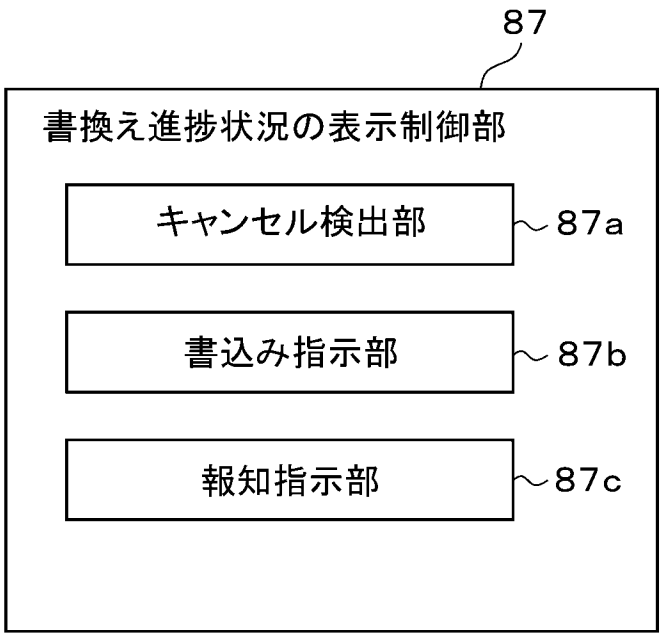
[図130]

Fig. 130


運用面
Ver1.0
非運用面
Ver2.0
非運用面
Ver1.0
運用面
Ver2.0に
書換える前に戻す
キャンセル
要求
非運用面
Ver1.0
運用面
Ver2.0
運用面
Ver1.0
非運用面
Ver2.0

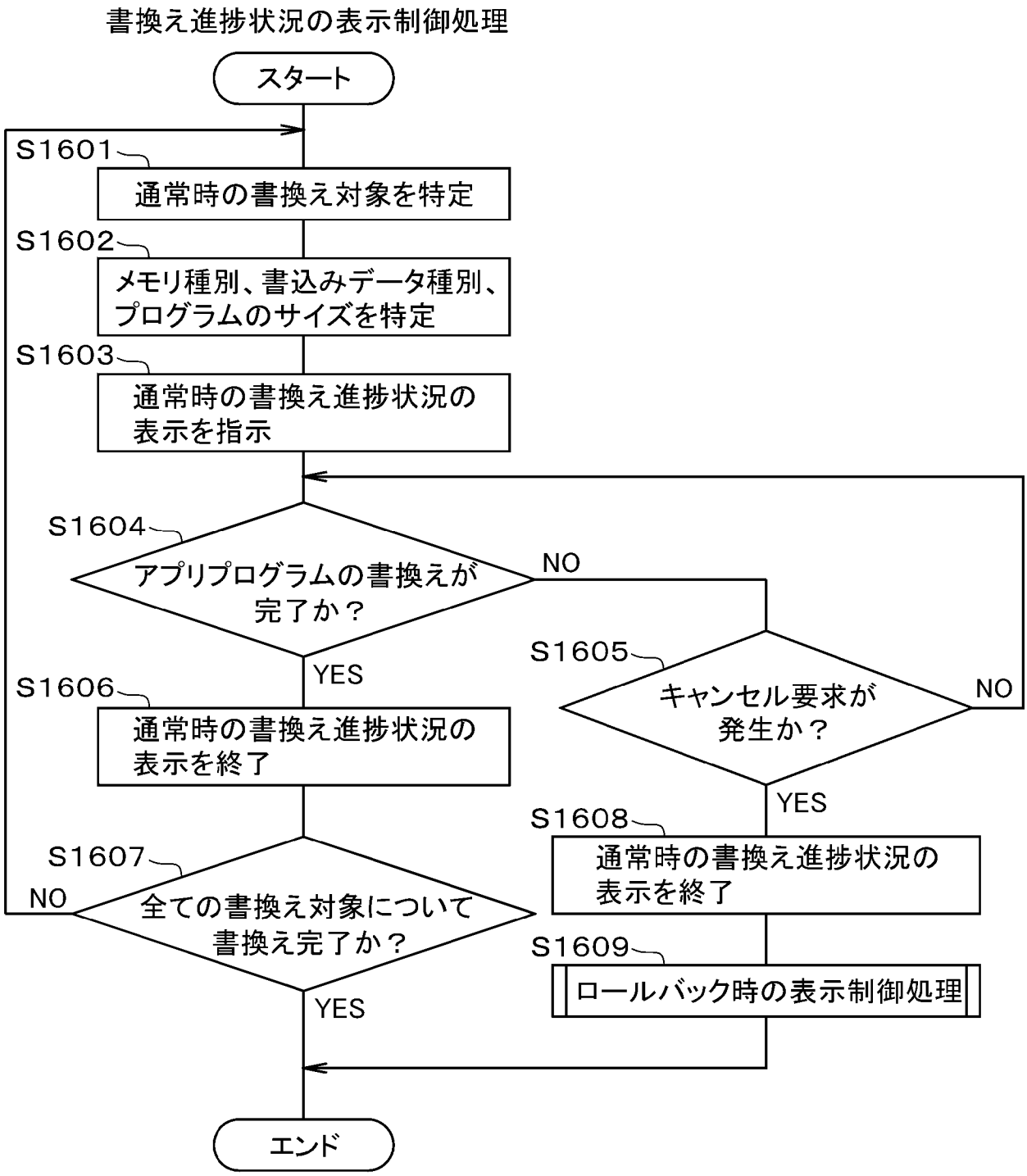
[図131]

Fig. 131



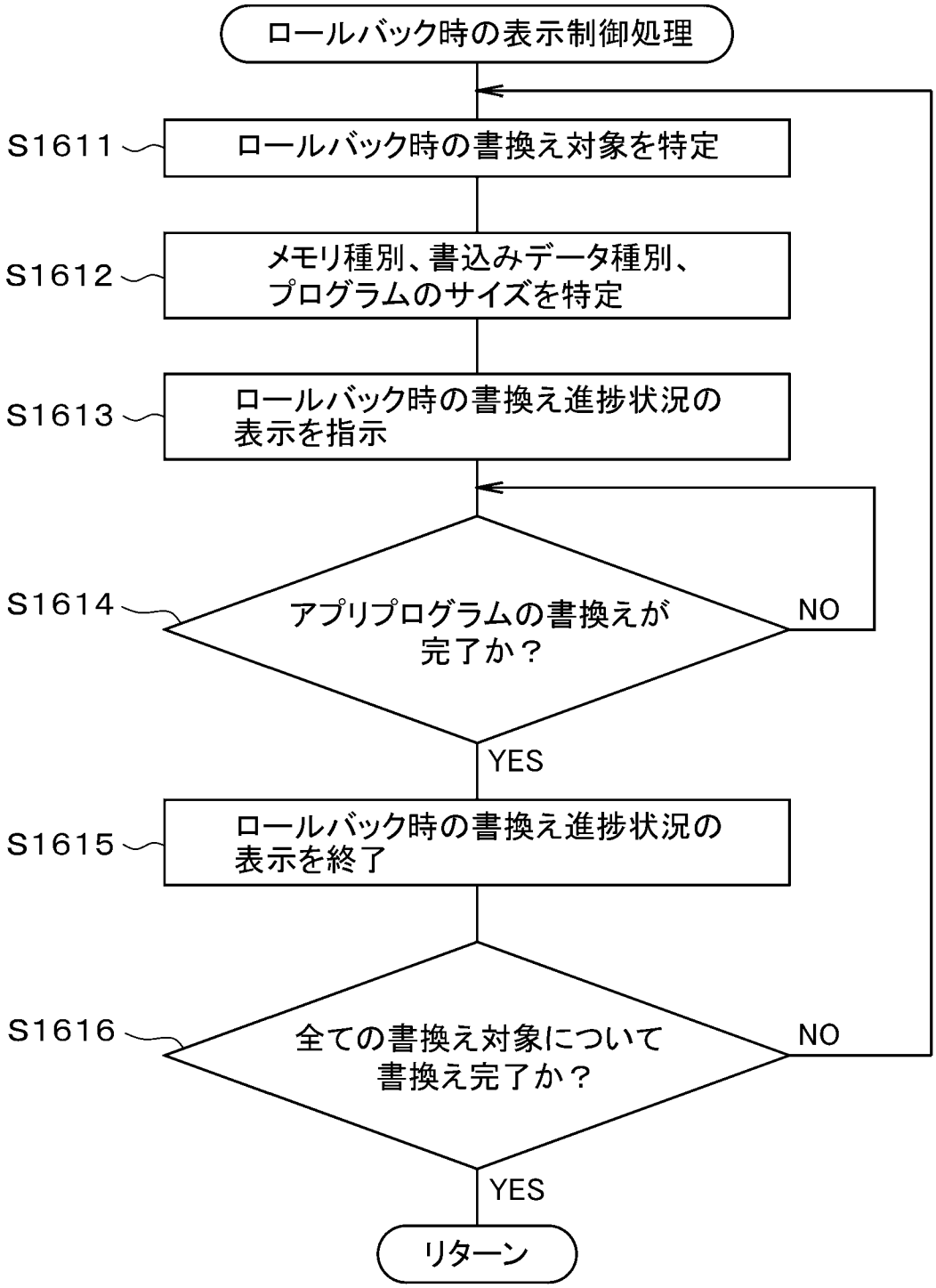
[図132]

Fig. 132


書換え進捗状況の表示制御処理
スタート
S1601
通常時の書換え対象を特定
S1602
メモリ種別、書込みデータ種別、プログラムのサイズを特定
S1603
通常時の書換え進捗状況の表示を指示
S1604
アプリプログラムの書換えが完了か？
NO
YES
S1605
キャンセル要求が発生か？
NO
YES
S1606
通常時の書換え進捗状況の表示を終了
S1607
全ての書換え対象について書換え完了か？
NO
YES
S1608
通常時の書換え進捗状況の表示を終了
S1609
ロールバック時の表示制御処理
エンド

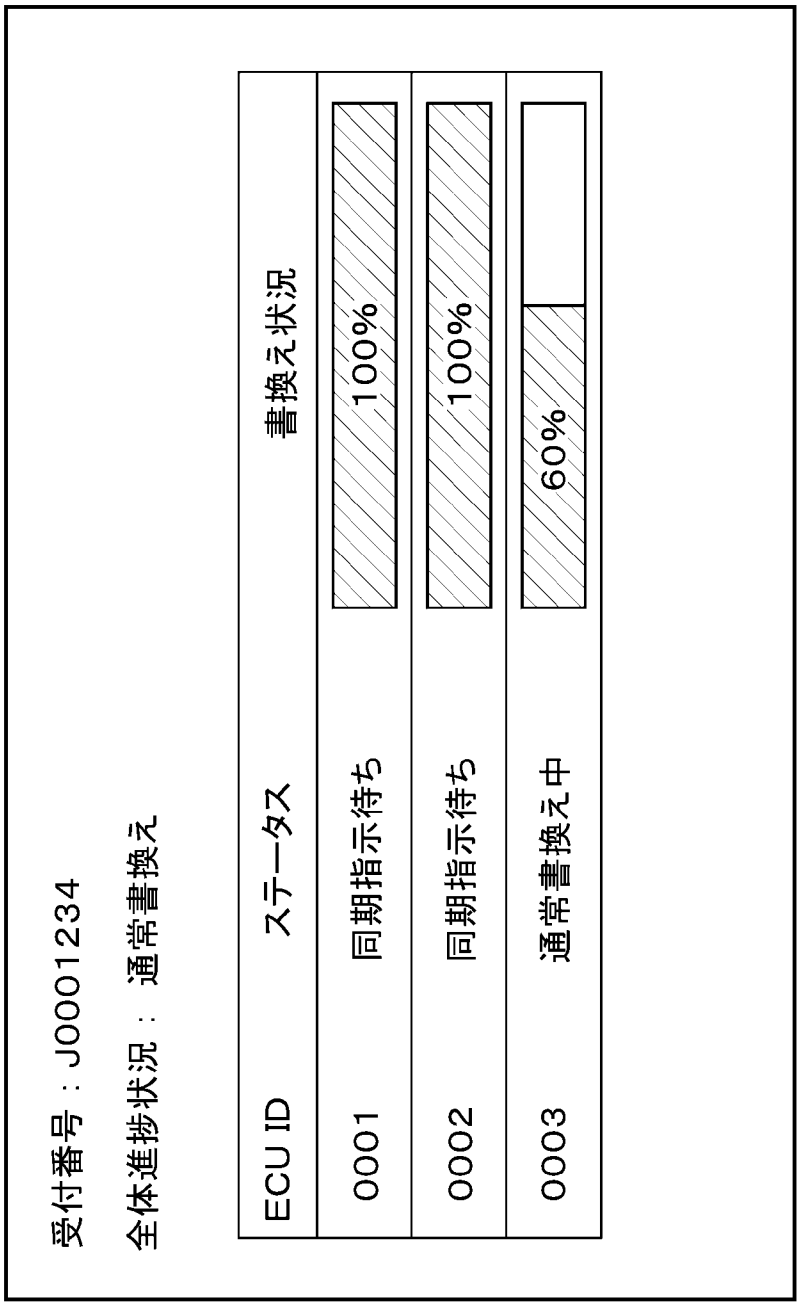
[図133]

Fig. 133


ロールバック時の表示制御処理
S1611
ロールバック時の書換え対象を特定
S1612
メモリ種別、書込みデータ種別、
プログラムのサイズを特定
S1613
ロールバック時の書換え進捗状況の
表示を指示
S1614
アプリプログラムの書換えが
完了か？
NO
YES
S1615
ロールバック時の書換え進捗状況の
表示を終了
S1616
全ての書換え対象について
書換え完了か？
NO
YES
リターン

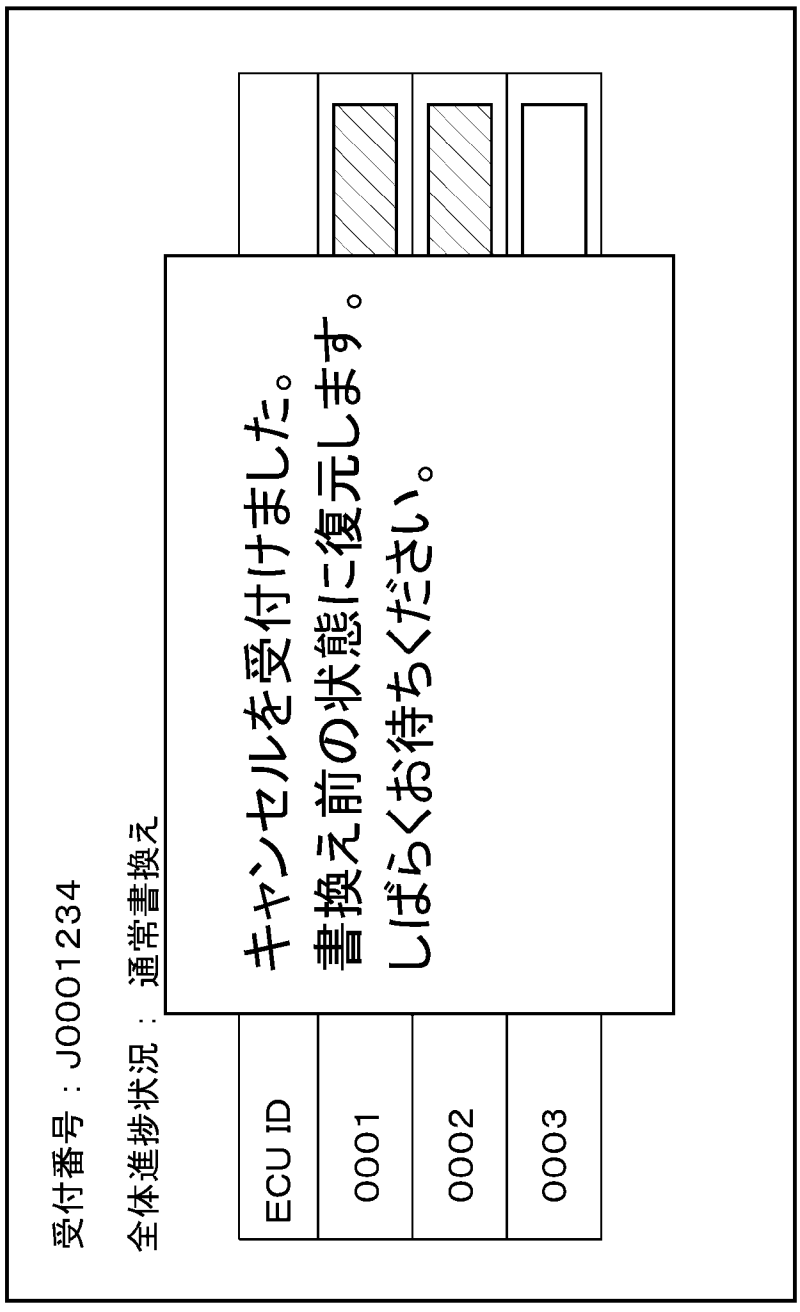
[図134]

Fig. 134


受付番号：J0001234
全体進捗状況：通常書換え
ECU ID
ステータス
書換え状況
0001
同期指示待ち
100%
0002
同期指示待ち
100%
0003
通常書換え中
60%

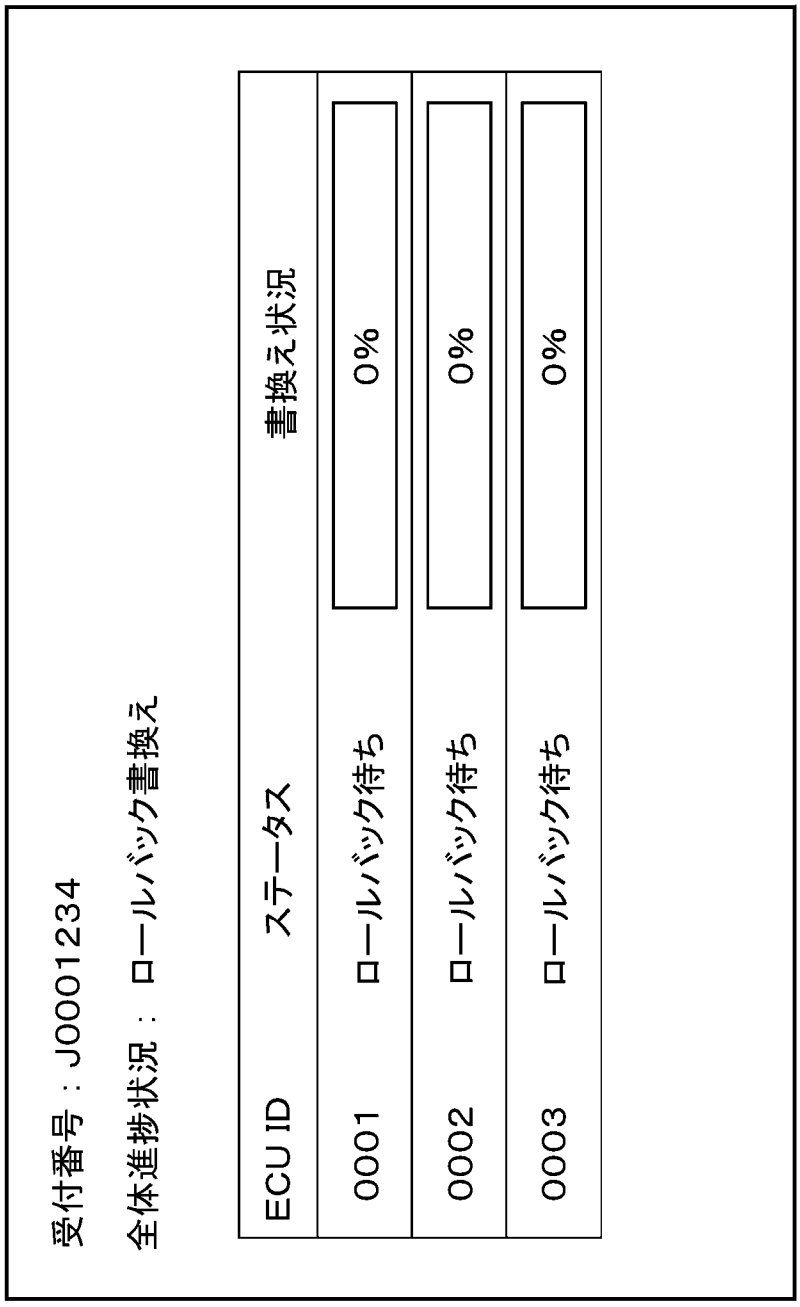
[図135]

Fig. 135


受付番号：J0001234
全体進捗状況：通常書換え
ECU ID
0001
0002
0003
キャンセルを受付けました。
書換え前の状態に復元します。
しばらくお待ちください。

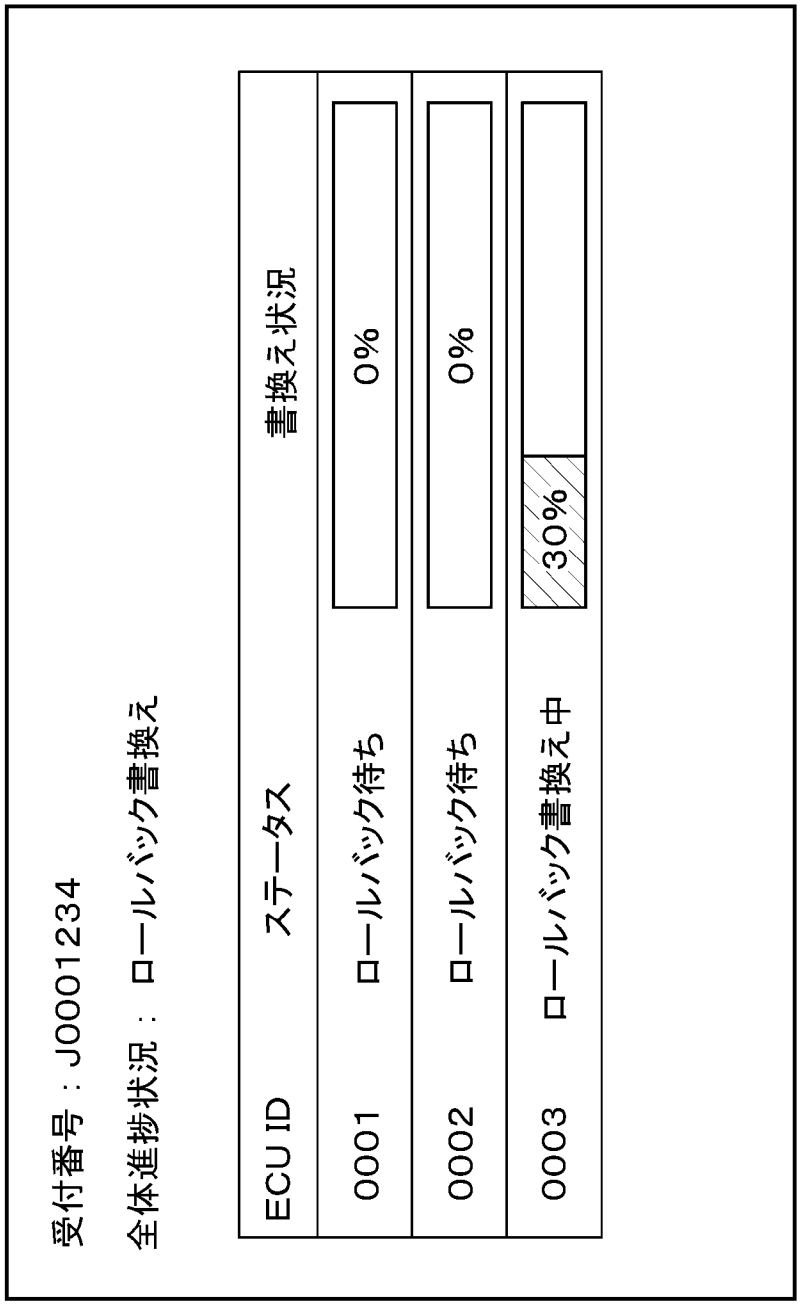
[図136]

Fig. 136


受付番号：J0001234
全体進捗状況： ロールバック書換え
ECU ID
ステータス
書換え状況
0001
ロールバック待ち
0%
0002
ロールバック待ち
0%
0003
ロールバック待ち
0%

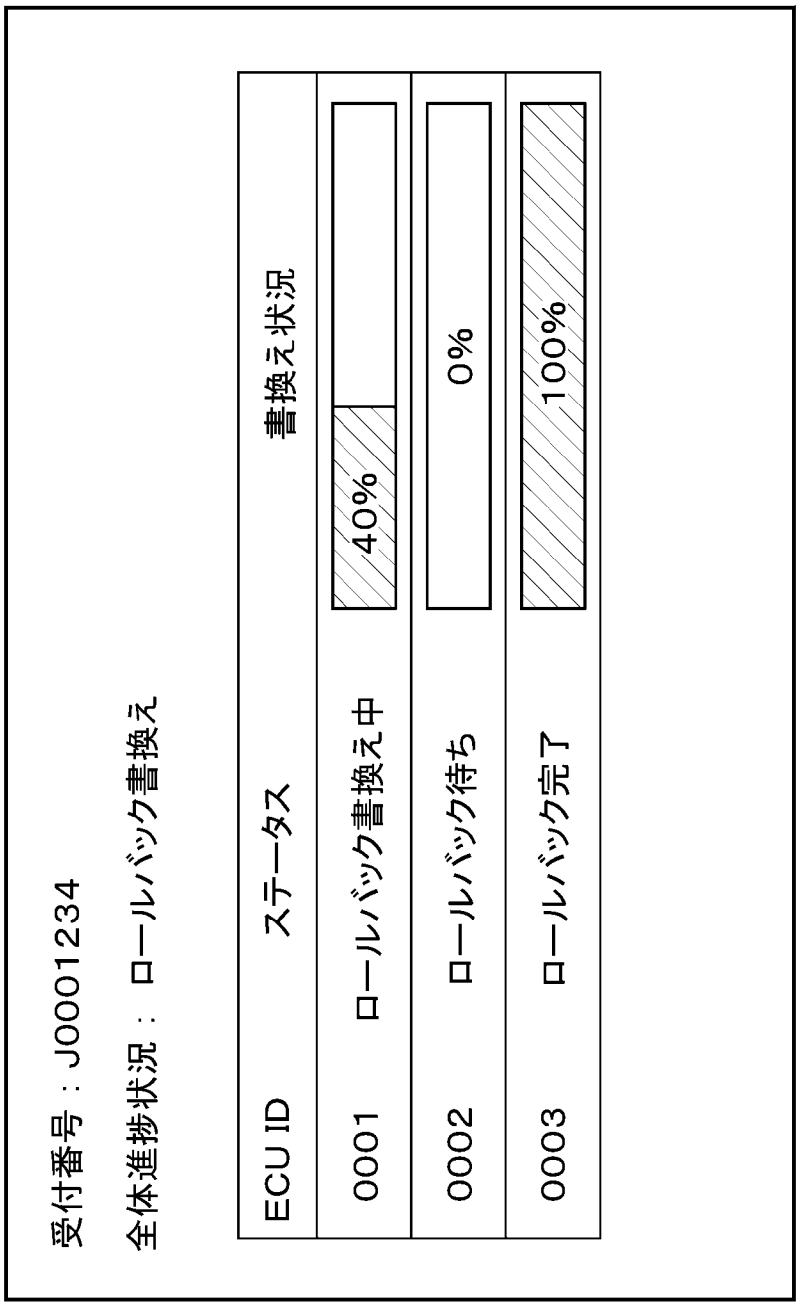
[図137]

Fig. 137


受付番号：J00001234
全体進捗状況： ロールバック書換え
ECU ID
ステータス
書換え状況
0001
ロールバック待ち
0%
0002
ロールバック待ち
0%
0003
ロールバック書換え中
30%

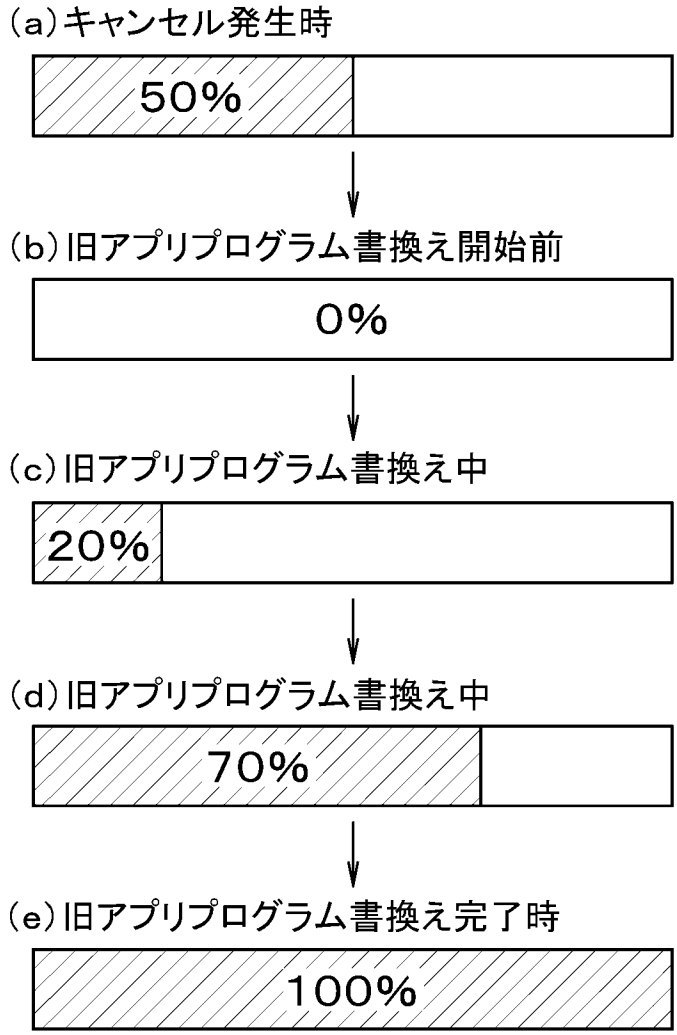
[図138]

Fig. 138


受付番号：J0001234
全体進捗状況： ロールバック書換え
ECU ID
ステータス
書換え状況
0001
ロールバック書換え中
40%
0002
ロールバック待ち
0%
0003
ロールバック完了
100%

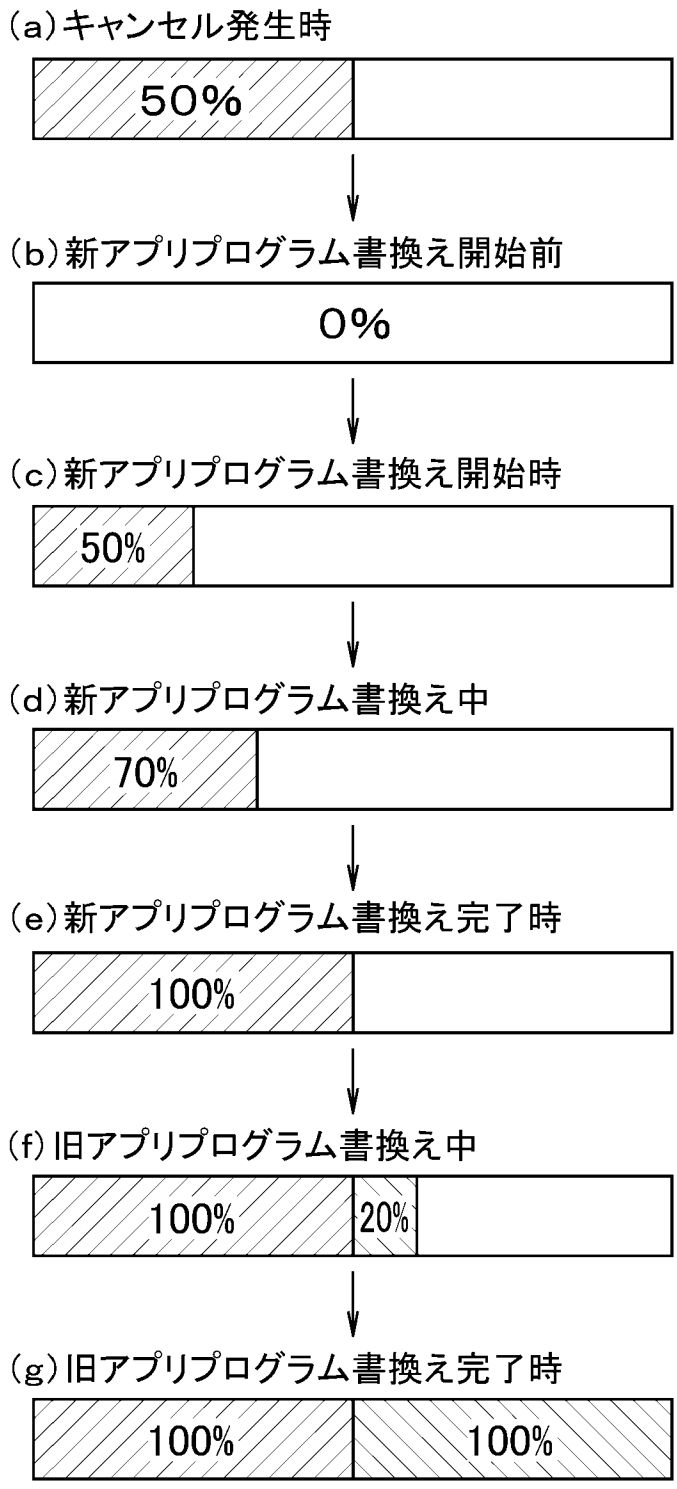
[図139]

Fig. 139


(a)キャンセル発生時
50%
(b)旧アプリプログラム書換え開始前
0%
(c)旧アプリプログラム書換え中
20%
(d)旧アプリプログラム書換え中
70%
(e)旧アプリプログラム書換え完了時
100%

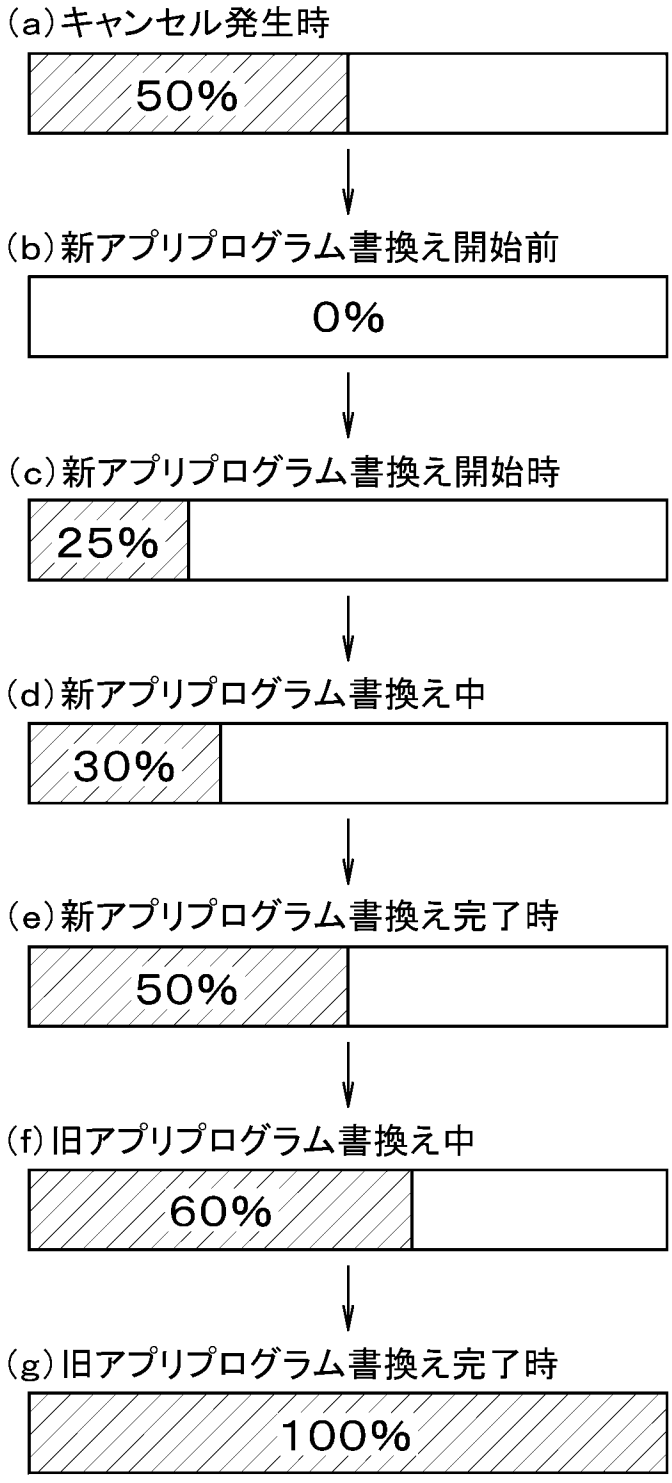
[図140]

Fig. 140


(a)キャンセル発生時
50%
(b)新アプリプログラム書換え開始前
0%
(c)新アプリプログラム書換え開始時
50%
(d)新アプリプログラム書換え中
70%
(e)新アプリプログラム書換え完了時
100%
(f)旧アプリプログラム書換え中
100%
20%
(g)旧アプリプログラム書換え完了時
100%
100%

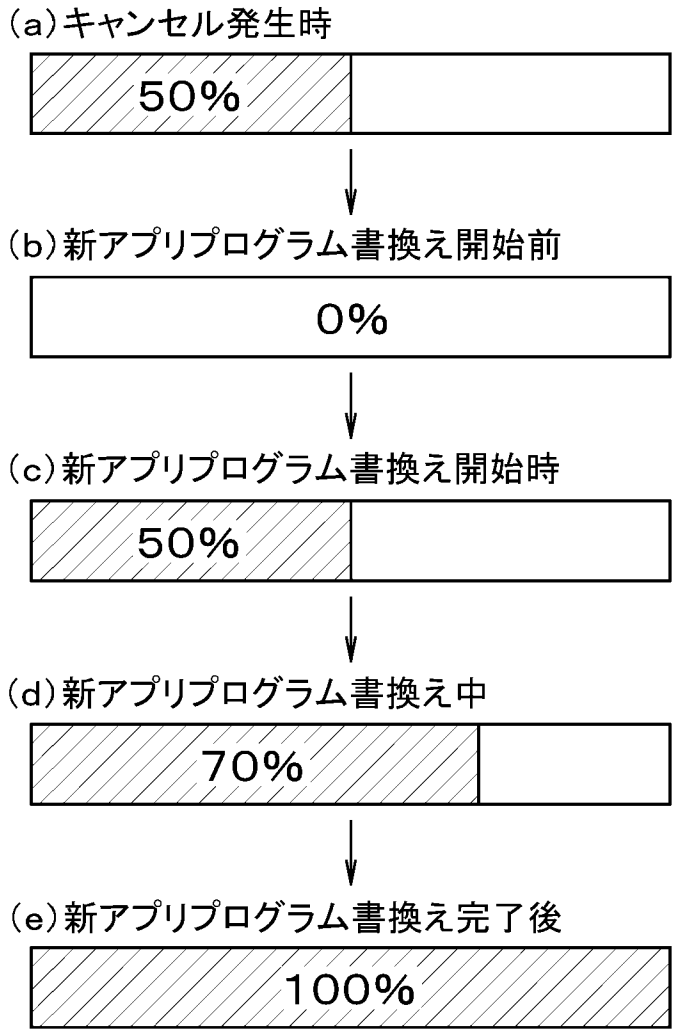
[図141]

Fig. 141


(a)キャンセル発生時
50%
(b)新アプリプログラム書換え開始前
0%
(c)新アプリプログラム書換え開始時
25%
(d)新アプリプログラム書換え中
30%
(e)新アプリプログラム書換え完了時
50%
(f)旧アプリプログラム書換え中
60%
(g)旧アプリプログラム書換え完了時
100%

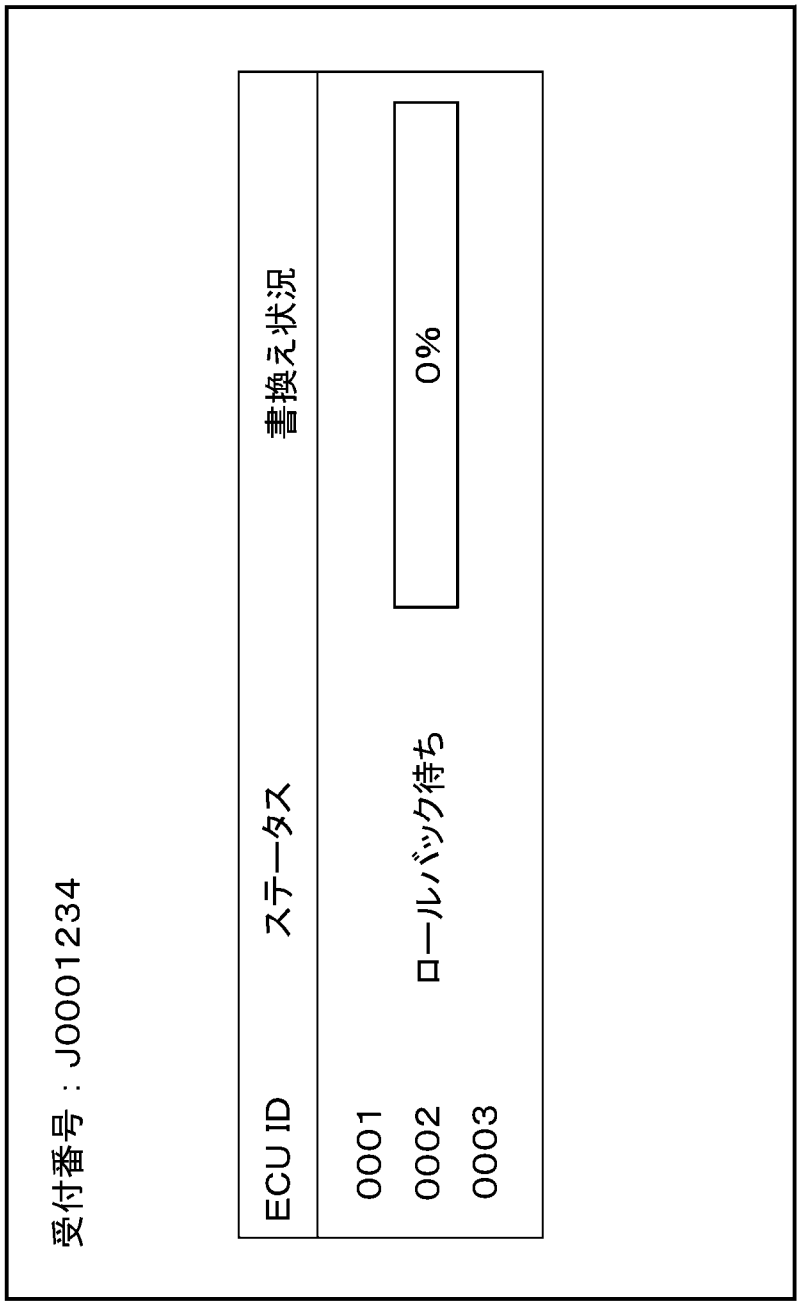
[図142]

Fig. 142


(a)キャンセル発生時
50%
(b)新アプリプログラム書換え開始前
0%
(c)新アプリプログラム書換え開始時
50%
(d)新アプリプログラム書換え中
70%
(e)新アプリプログラム書換え完了後
100%

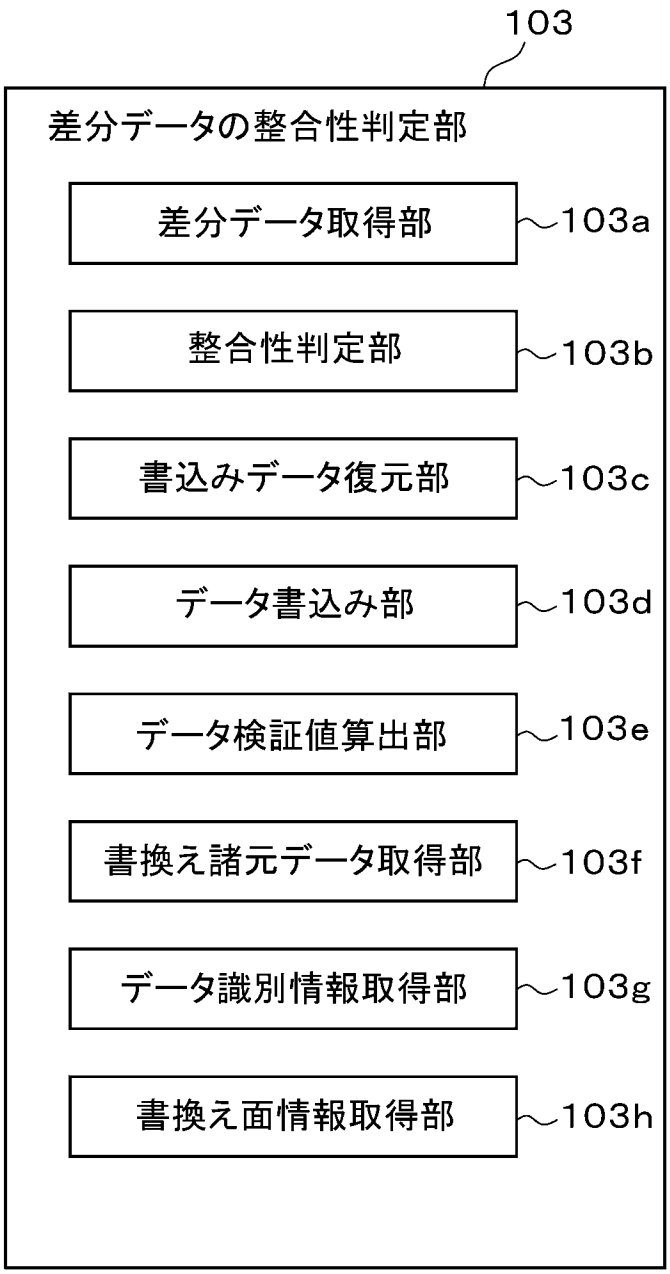
[図143]

Fig. 143



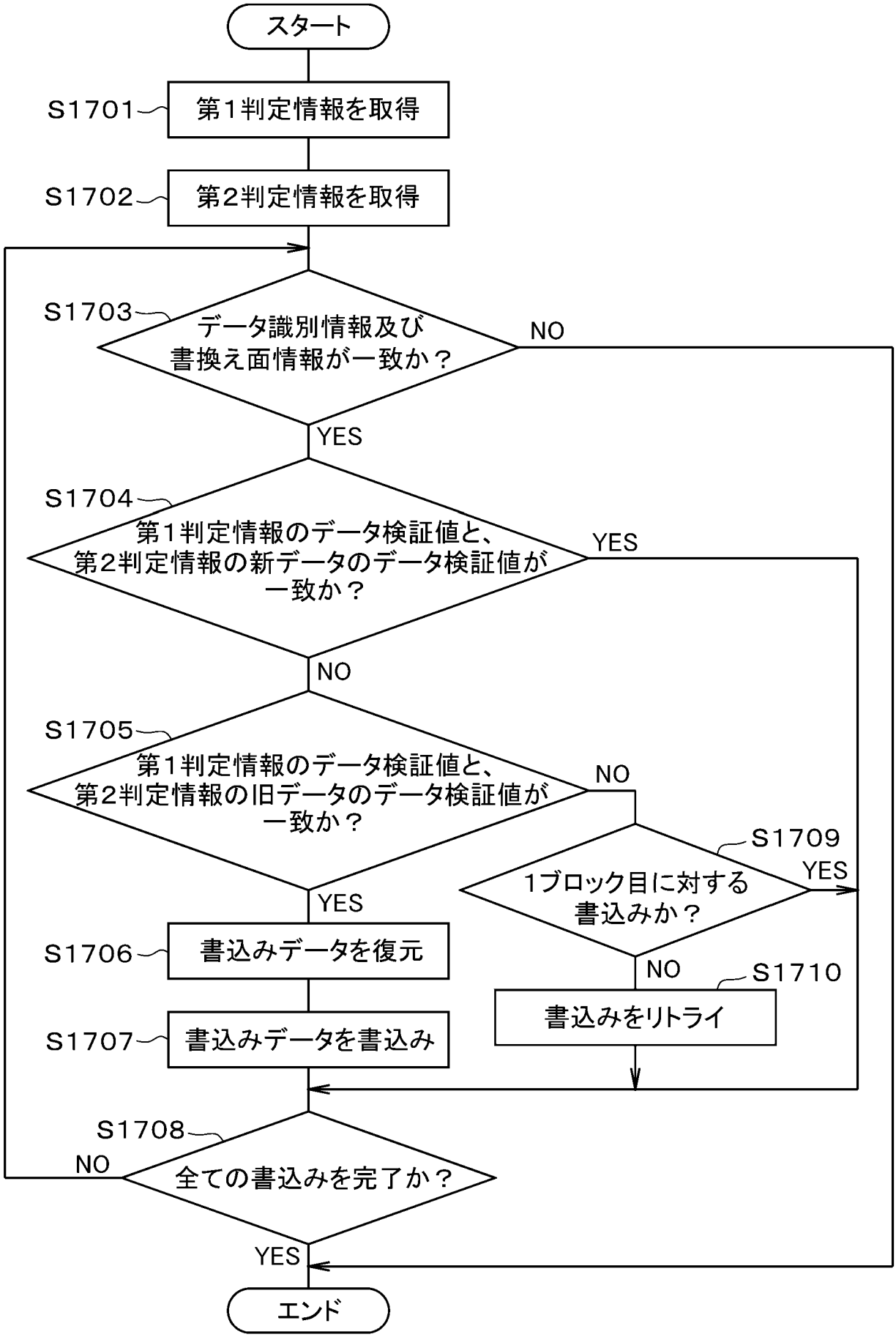
[図144]

Fig. 144


103
差分データの整合性判定部
差分データ取得部
103a
整合性判定部
103b
書込みデータ復元部
103c
データ書込み部
103d
データ検証値算出部
103e
書換え諸元データ取得部
103f
データ識別情報取得部
103g
書換え面情報取得部
103h

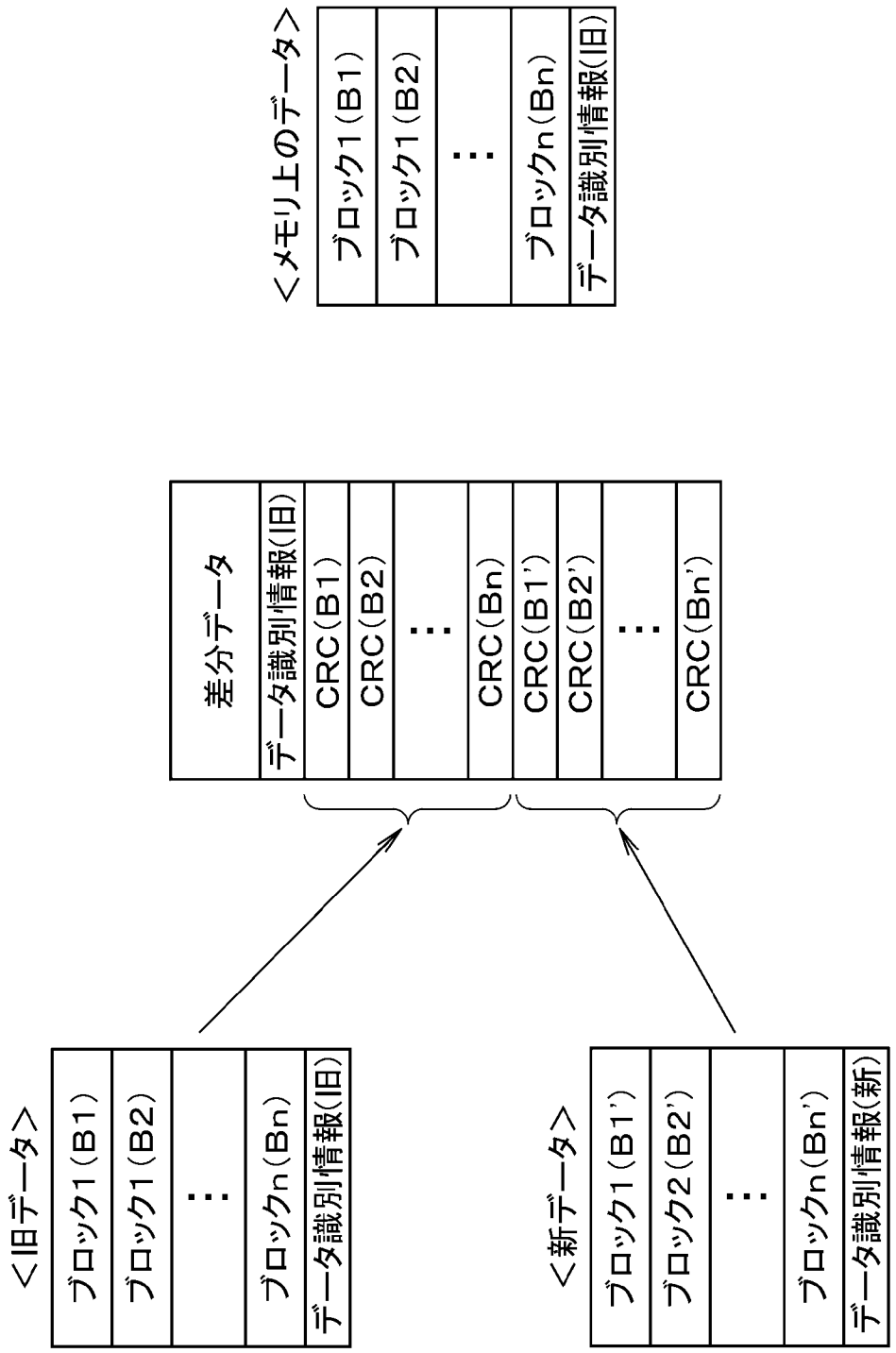
[図145]

Fig. 145 差分データの整合性判定処理



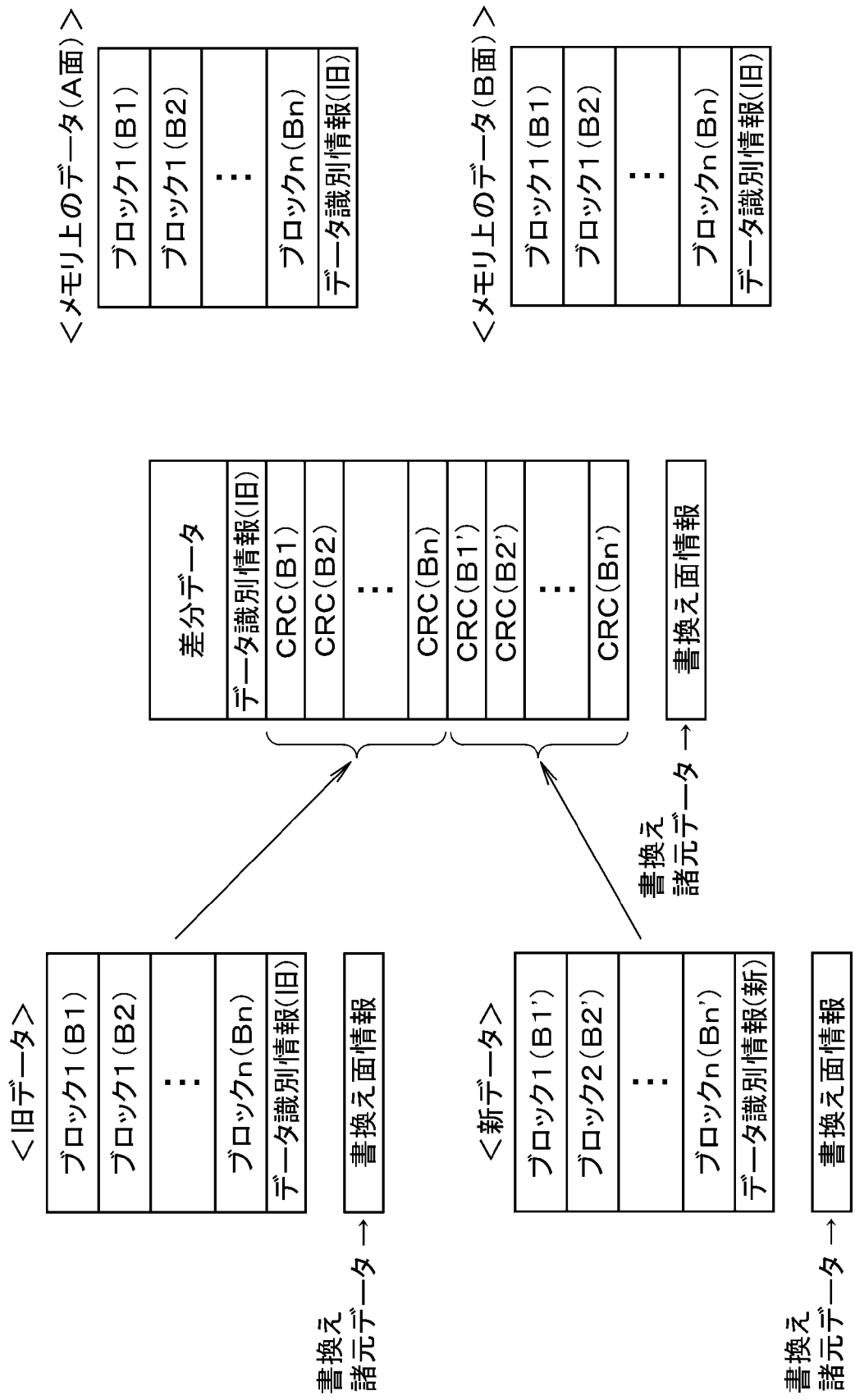
[図146]

Fig. 146


<メモリ上のデータ>
ブロック1(B1)
ブロック1(B2)
ブロックn(Bn)
データ識別情報(旧)
差分データ
データ識別情報(旧)
CRC(B1)
CRC(B2)
CRC(Bn)
CRC(B1')
CRC(B2')
CRC(Bn')
<旧データ>
ブロック1(B1)
ブロック1(B2)
ブロックn(Bn)
データ識別情報(旧)
<新データ>
ブロック1(B1')
ブロック2(B2')
ブロックn(Bn')
データ識別情報(新)

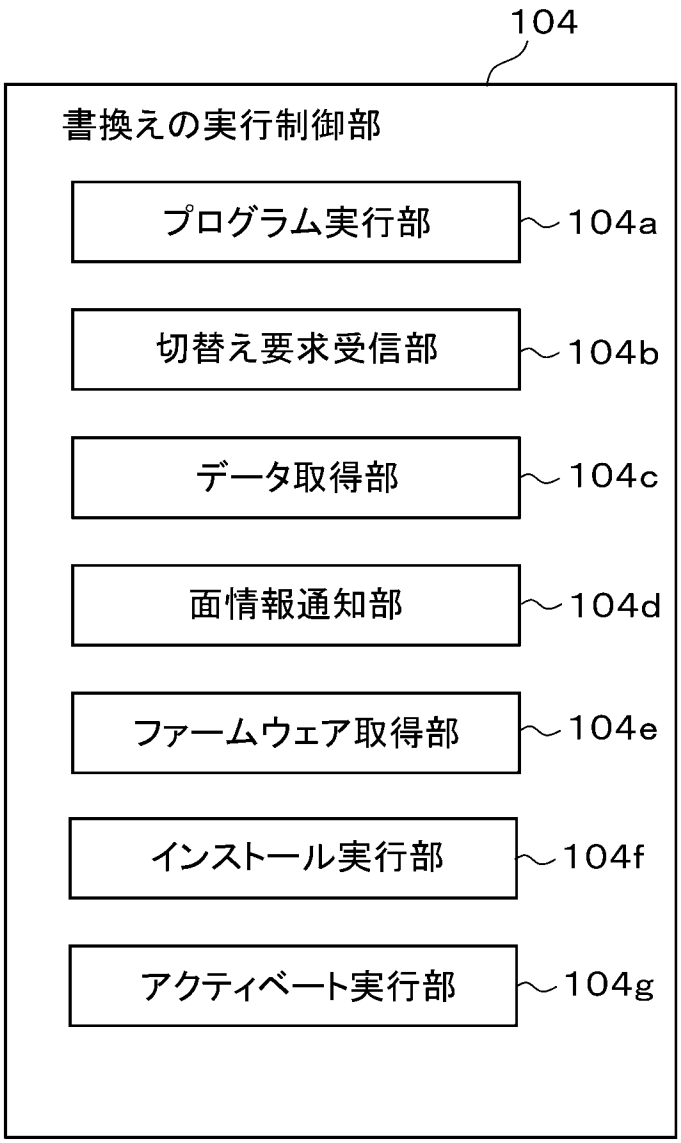
[図147]

Fig. 147


<メモリ上のデータ(A面)>
ブロック1(B1)
ブロック1(B2)
ブロックn(Bn)
データ識別情報(旧)
<メモリ上のデータ(B面)>
ブロック1(B1)
ブロック1(B2)
ブロックn(Bn)
データ識別情報(旧)
差分データ
データ識別情報(旧)
CRC(B1)
CRC(B2)
CRC(Bn)
CRC(B1')
CRC(B2')
CRC(Bn')
書換え面情報
書換え面情報
<旧データ>
ブロック1(B1)
ブロック1(B2)
ブロックn(Bn)
データ識別情報(旧)
書換え面情報
書換え
諸元データ→
<新データ>
ブロック1(B1')
ブロック2(B2')
ブロックn(Bn')
データ識別情報(新)
書換え面情報
書換え
諸元データ→

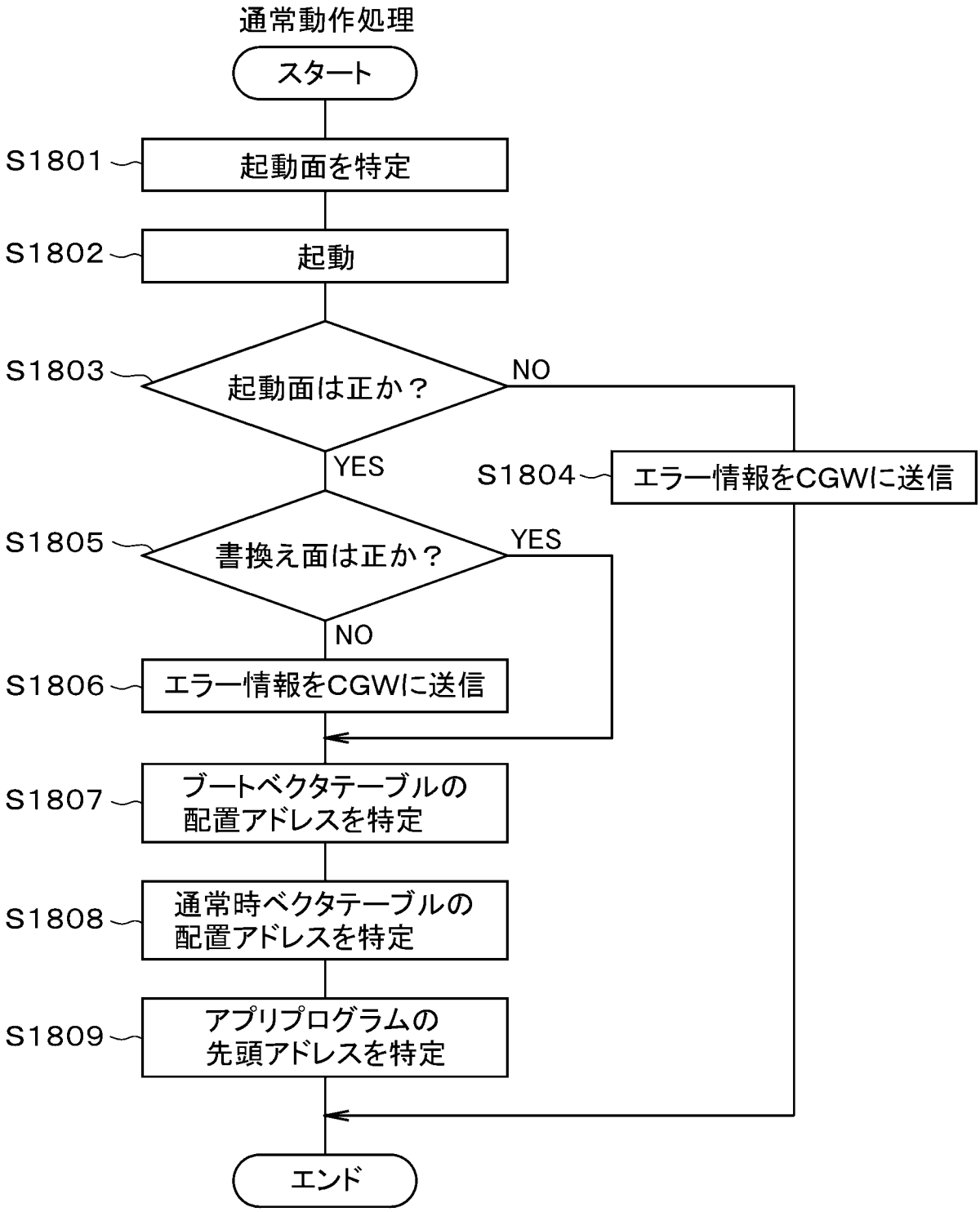
[図148]

Fig. 148


104
書換えの実行制御部
プログラム実行部
104a
切替え要求受信部
104b
データ取得部
104c
面情報通知部
104d
ファームウェア取得部
104e
インストール実行部
104f
アクティベート実行部
104g

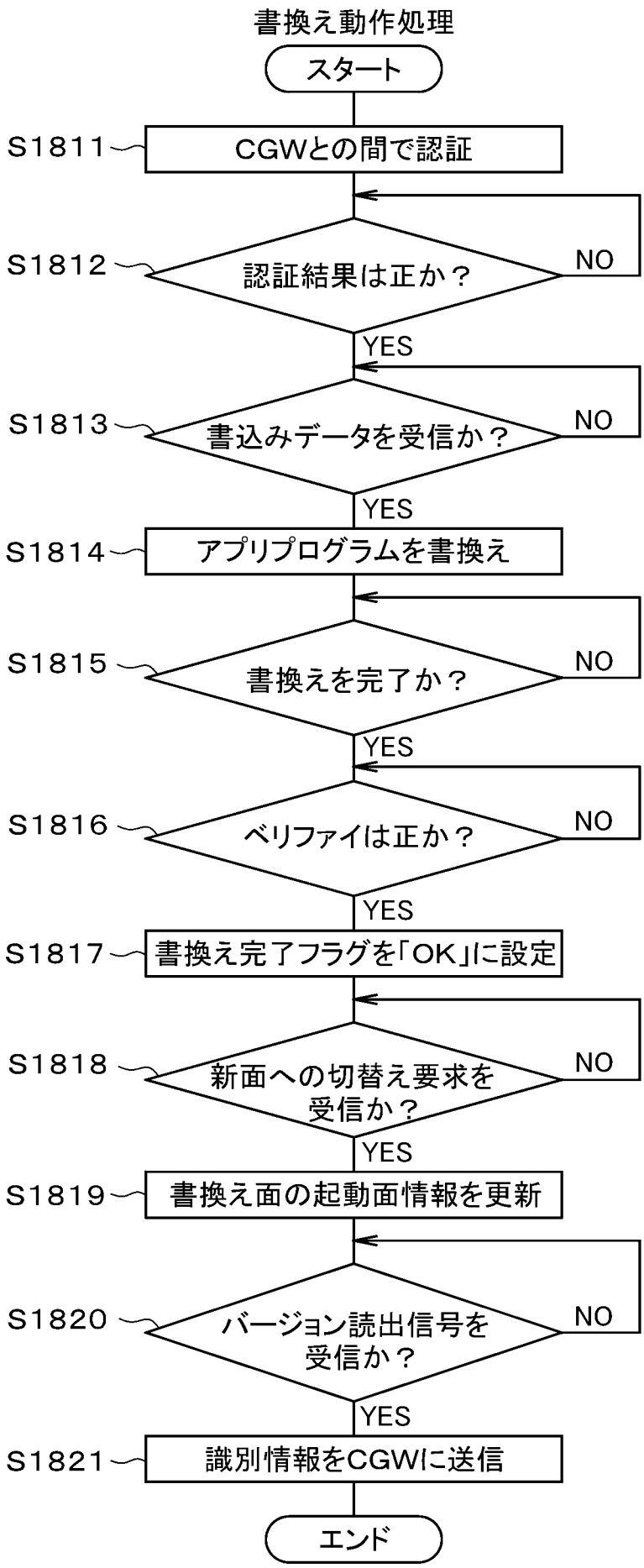
[図149]

Fig. 149


通常動作処理
スタート
S1801
起動面を特定
S1802
起動
S1803
起動面は正か？
NO
YES
S1804
エラー情報をCGWに送信
S1805
書換え面は正か？
YES
NO
S1806
エラー情報をCGWに送信
S1807
ブートベクタテーブルの
配置アドレスを特定
S1808
通常時ベクタテーブルの
配置アドレスを特定
S1809
アプリプログラムの
先頭アドレスを特定
エンド

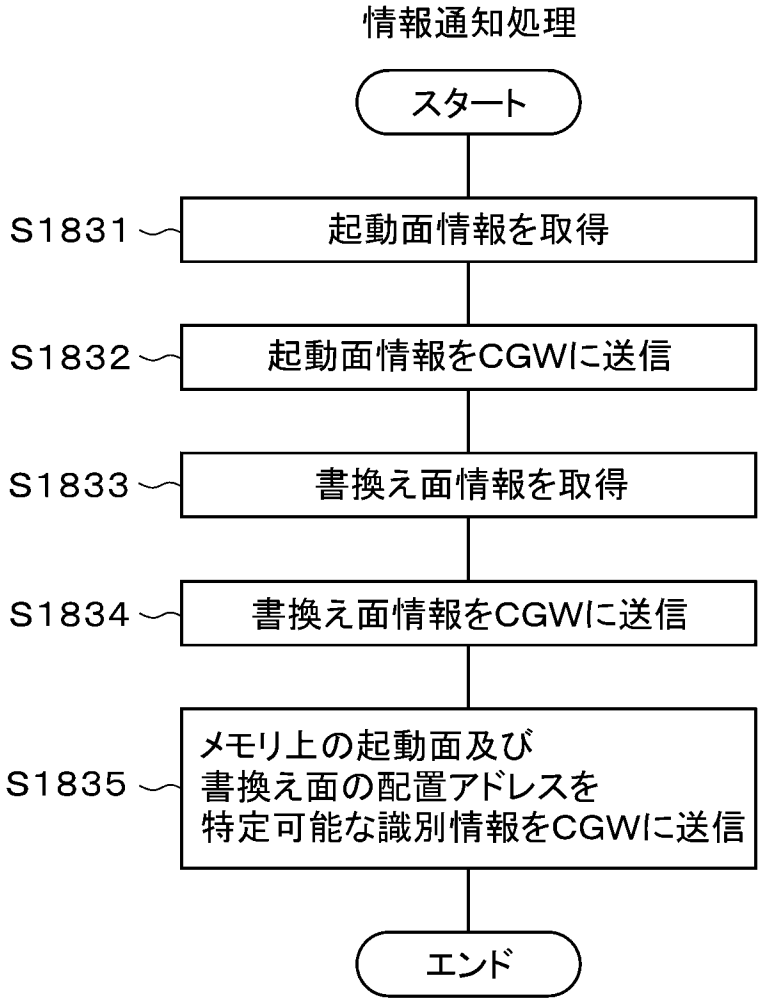
[図150]

Fig. 150


書換え動作処理
スタート
S1811
CGWとの間で認証
S1812
認証結果は正か？
NO
YES
S1813
書込みデータを受信か？
NO
YES
S1814
アプリプログラムを書換え
S1815
書換えを完了か？
NO
YES
S1816
ベリファイは正か？
NO
YES
S1817
書換え完了フラグを「OK」に設定
S1818
新面への切替え要求を受信か？
NO
YES
S1819
書換え面の起動面情報を更新
S1820
バージョン読出信号を受信か？
NO
YES
S1821
識別情報をCGWに送信
エンド

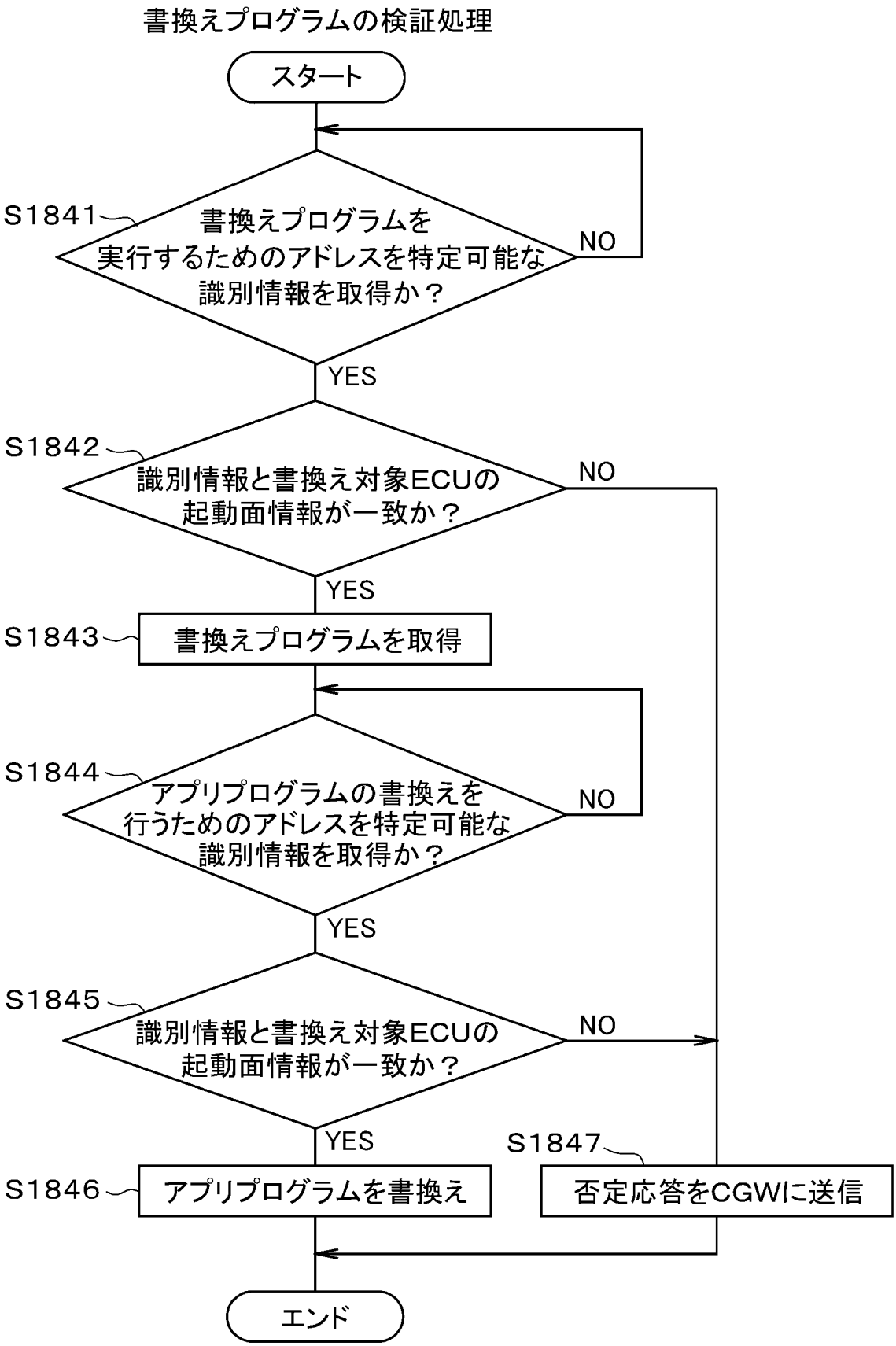
[図151]

Fig. 151


情報通知処理
スタート
S1831
起動面情報を取得
S1832
起動面情報をCGWに送信
S1833
書換え面情報を取得
S1834
書換え面情報をCGWに送信
S1835
メモリ上の起動面及び
書換え面の配置アドレスを
特定可能な識別情報をCGWに送信
エンド

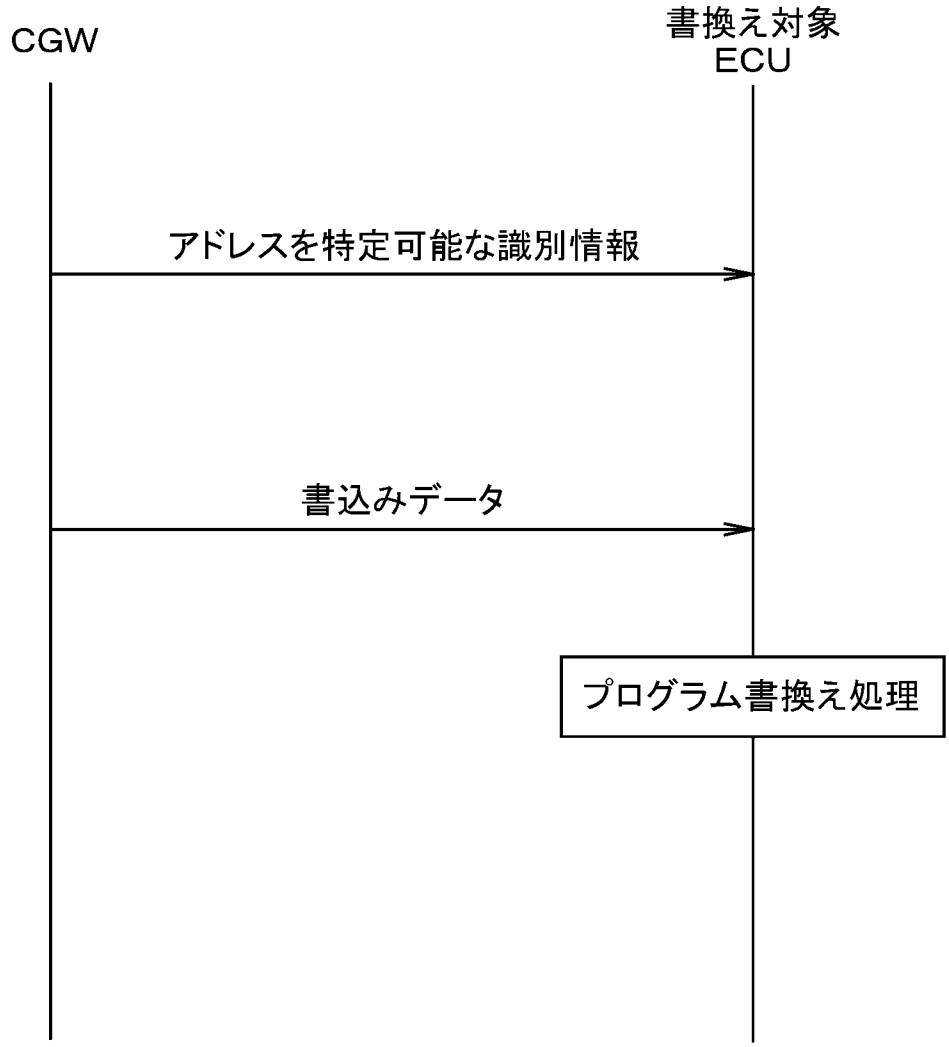
[図152]

Fig. 152


書換えプログラムの検証処理
スタート
S1841
書換えプログラムを
実行するためのアドレスを特定可能な
識別情報を取得か？
NO
YES
S1842
識別情報と書換え対象ECUの
起動面情報が一致か？
NO
YES
S1843
書換えプログラムを取得
S1844
アプリプログラムの書換えを
行うためのアドレスを特定可能な
識別情報を取得か？
NO
YES
S1845
識別情報と書換え対象ECUの
起動面情報が一致か？
NO
YES
S1847
S1846
アプリプログラムを書換え
否定応答をCGWに送信
エンド

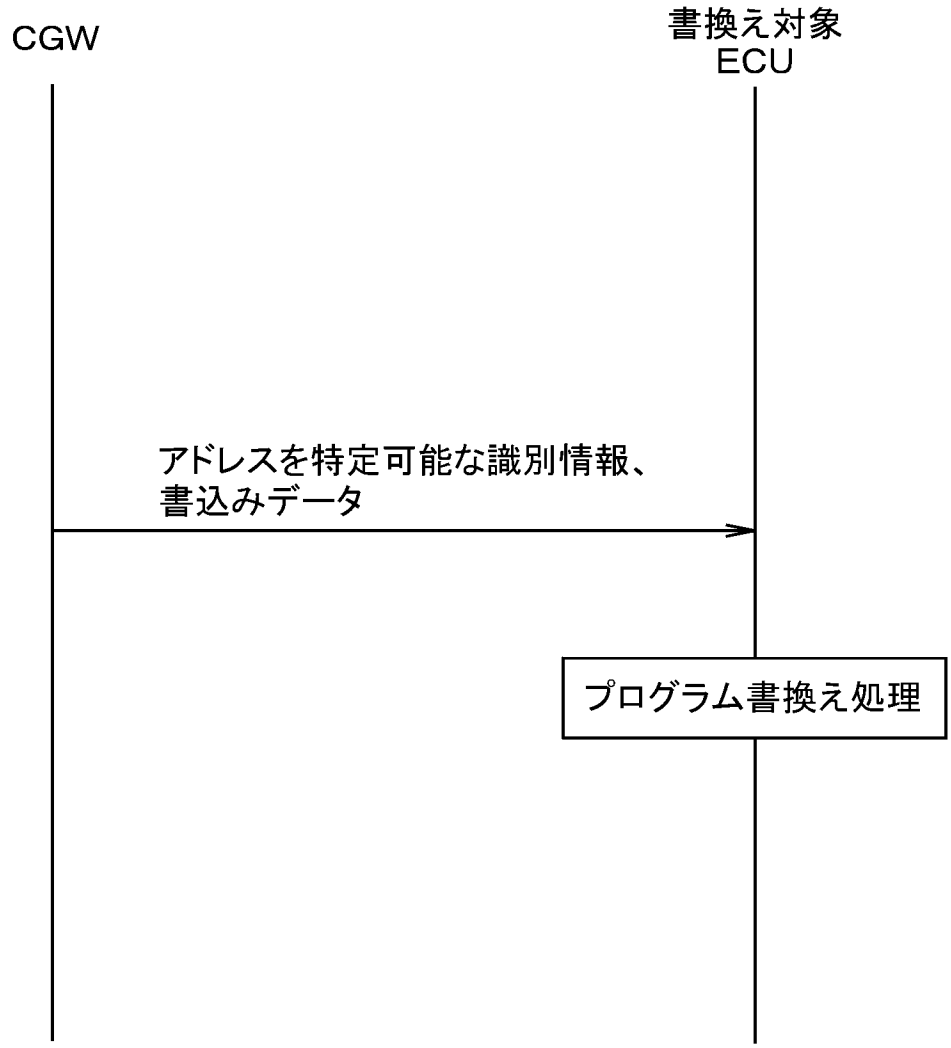
[図153]

Fig. 153



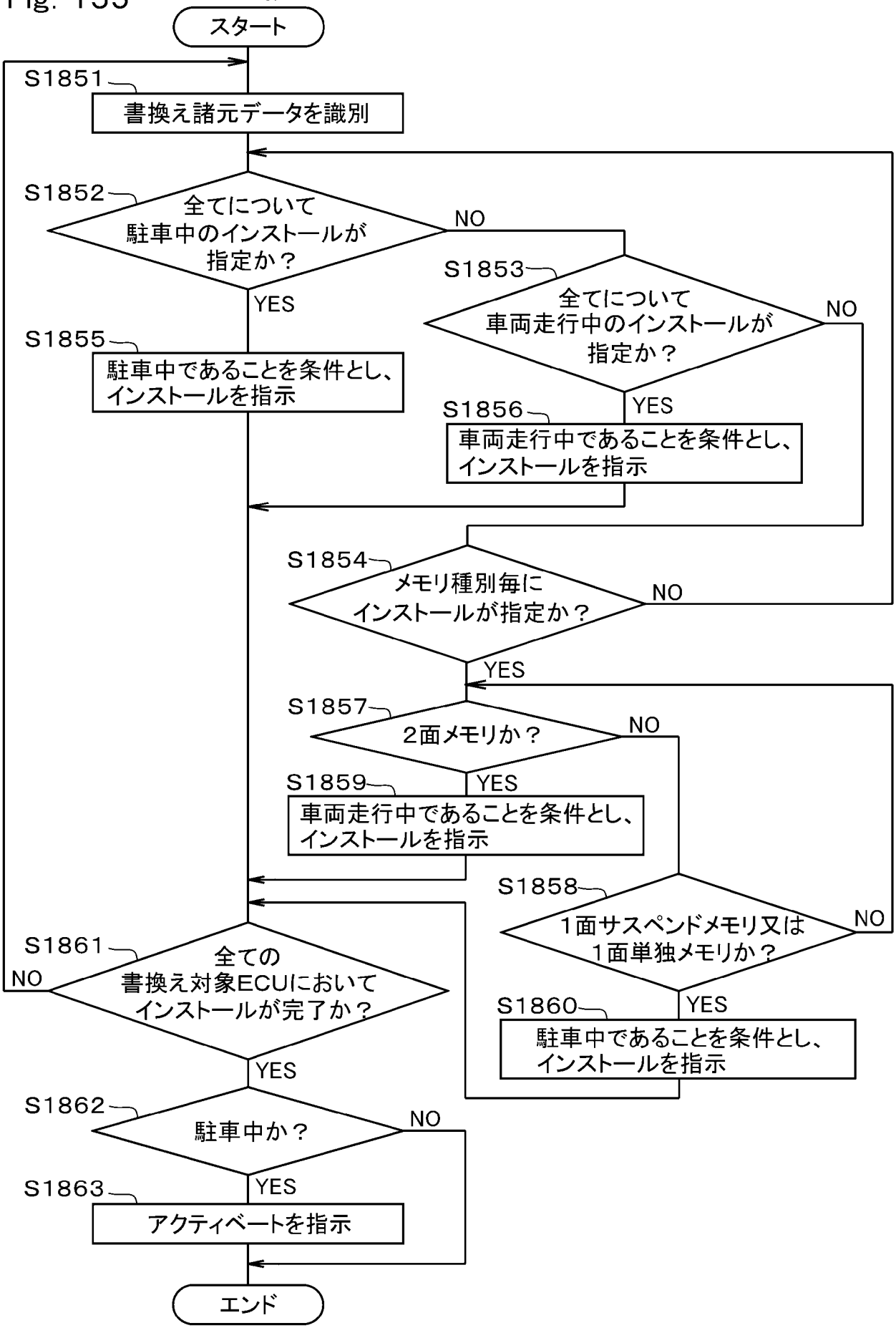
[図154]

Fig. 154



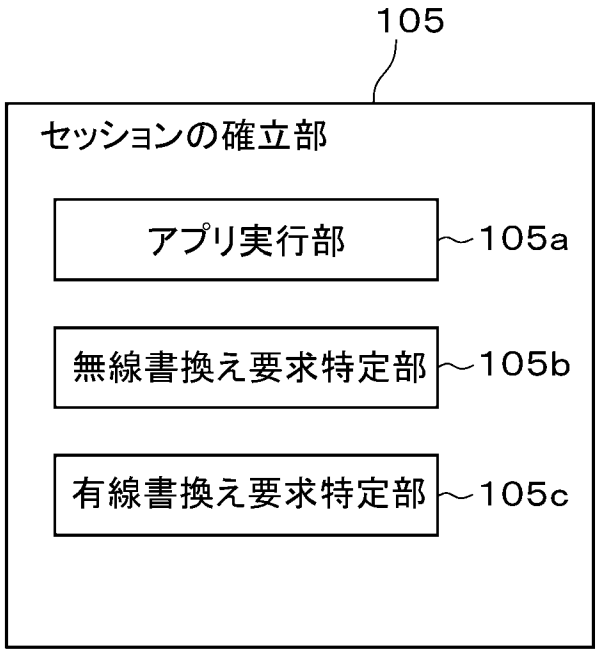
[図155]

Fig. 155 インストール指示処理



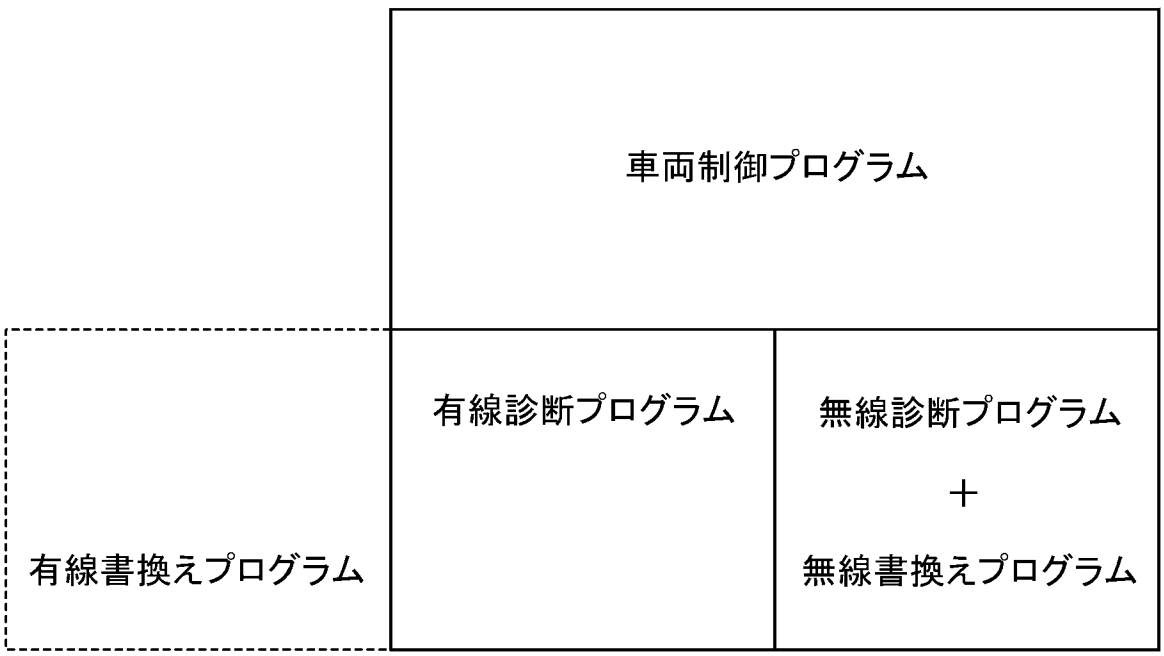
[図156]

Fig. 156



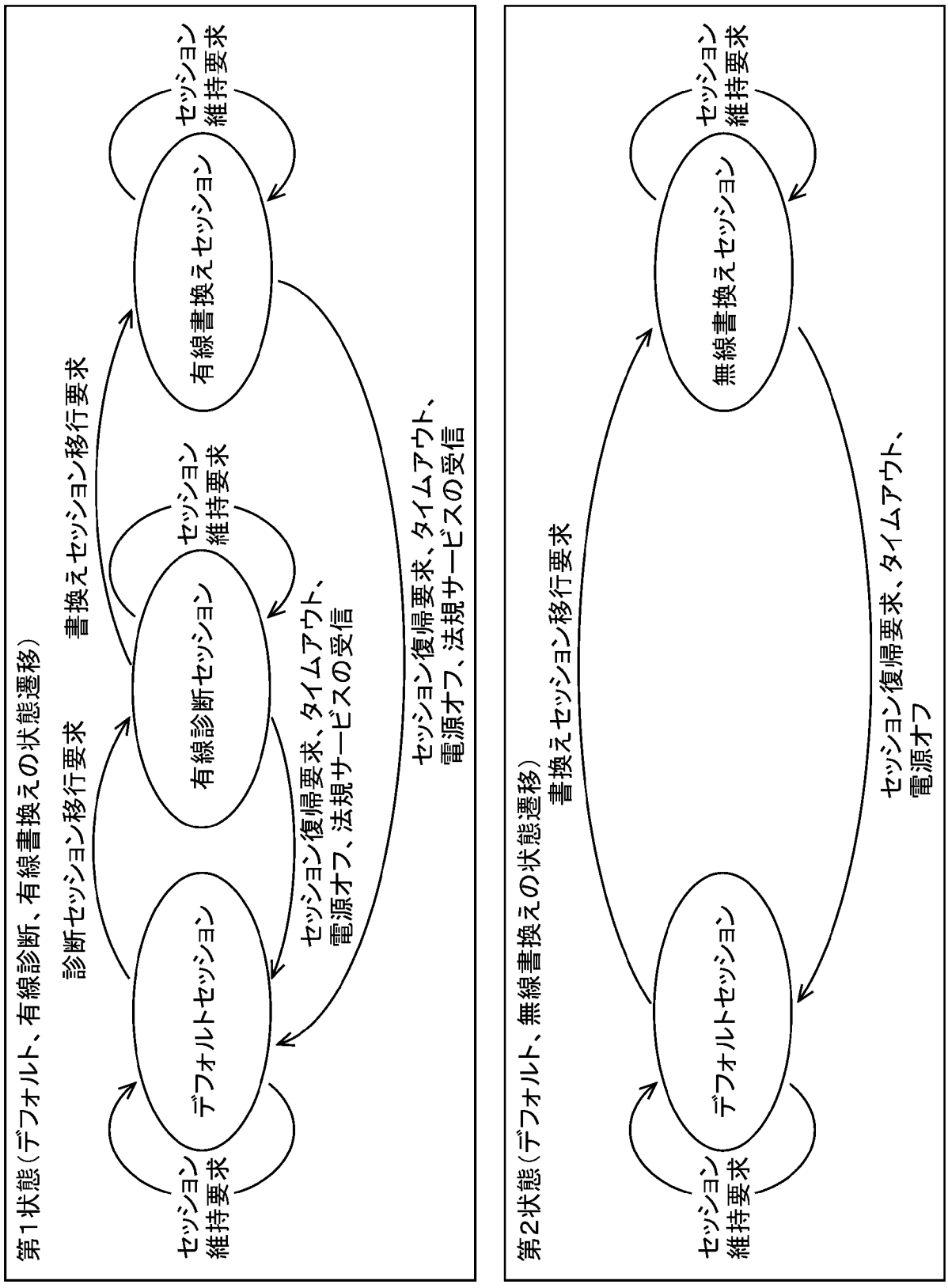
[図157]

Fig. 157



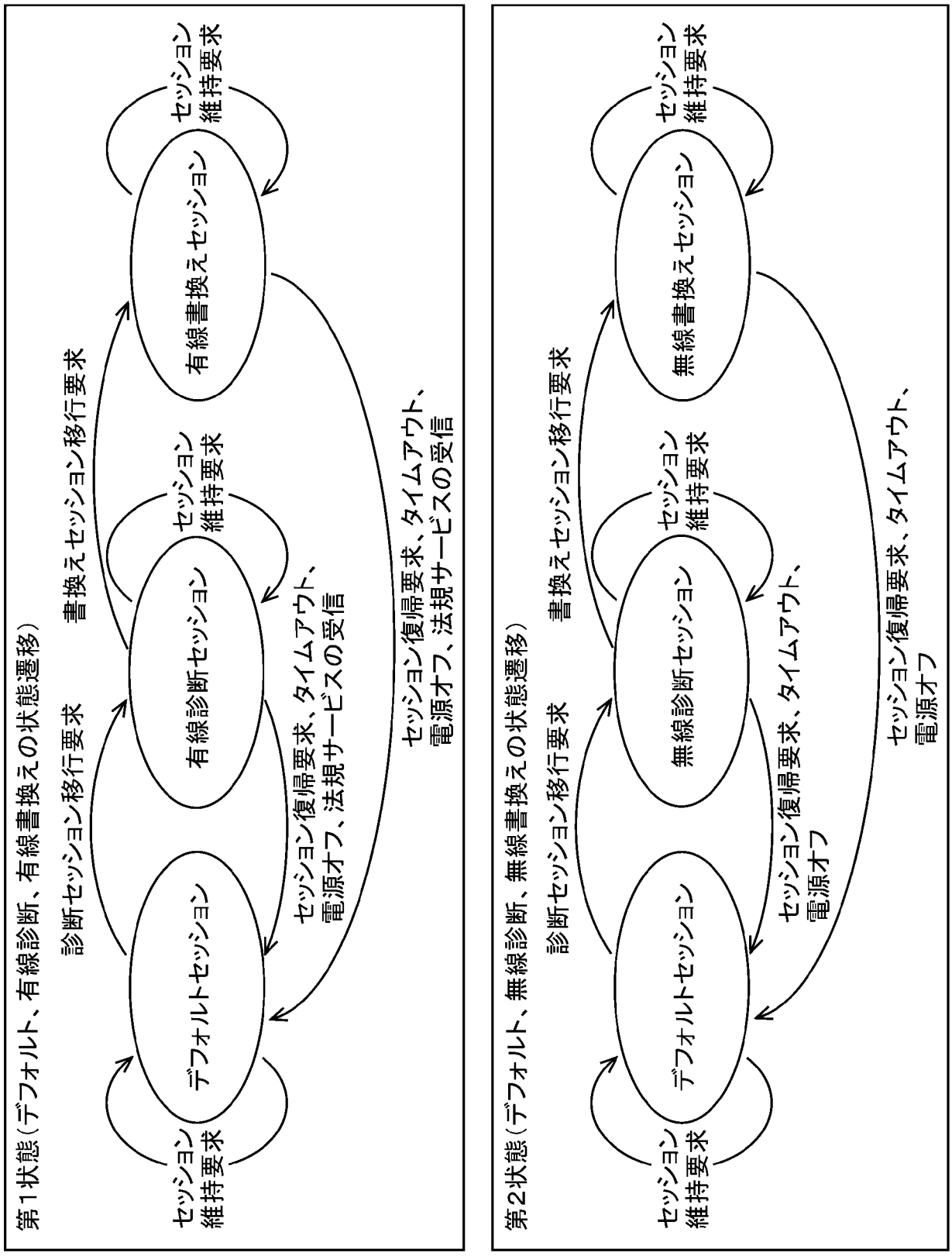
[図158]

Fig. 158


第1状態（デフォルト、有線診断、有線書換えの状態遷移）
診断セッション移行要求
書換えセッション移行要求
セッション維持要求
デフォルトセッション
有線診断セッション
有線書換えセッション
セッション維持要求
セッション維持要求
セッション復帰要求、タイムアウト、電源オフ、法規サービスの受信
セッション復帰要求、タイムアウト、電源オフ、法規サービスの受信
第2状態（デフォルト、無線書換えの状態遷移）
書換えセッション移行要求
セッション維持要求
デフォルトセッション
無線書換えセッション
セッション維持要求
セッション復帰要求、タイムアウト、電源オフ

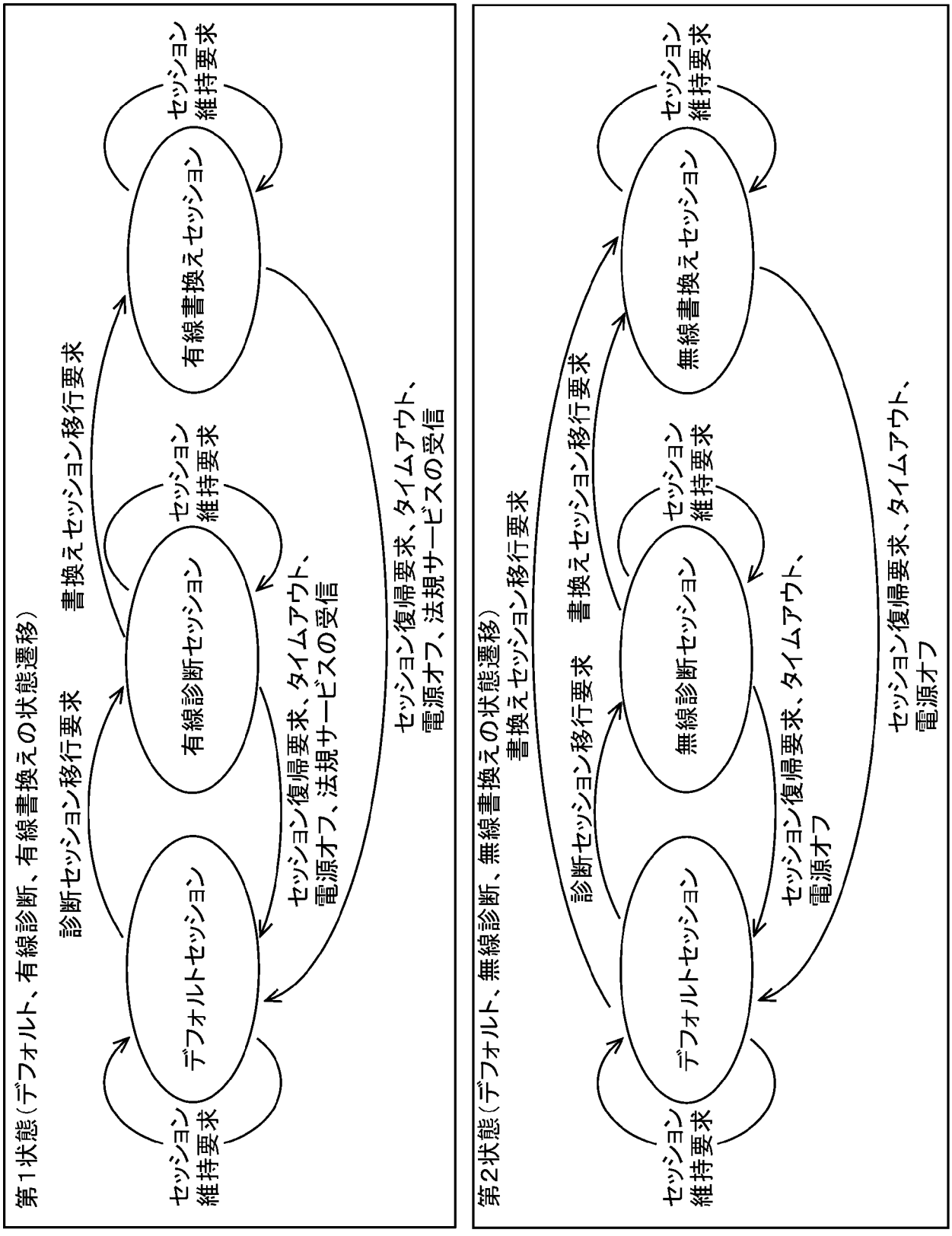
[図159]

Fig. 159


第1状態（デフォルト、有線診断、有線書換えの状態遷移）
診断セッション移行要求
書換えセッション移行要求
セッション維持要求
デフォルトセッション
有線診断セッション
有線書換えセッション
セッション維持要求
セッション維持要求
セッション復帰要求、タイムアウト、電源オフ、法規サービスの受信
セッション復帰要求、タイムアウト、電源オフ、法規サービスの受信
第2状態（デフォルト、無線診断、無線書換えの状態遷移）
診断セッション移行要求
書換えセッション移行要求
セッション維持要求
デフォルトセッション
無線診断セッション
無線書換えセッション
セッション維持要求
セッション維持要求
セッション復帰要求、タイムアウト、電源オフ
セッション復帰要求、タイムアウト、電源オフ

[図160]

Fig. 160


第1状態（デフォルト、有線診断、有線書換えの状態遷移）
診断セッション移行要求
書換えセッション移行要求
セッション維持要求
デフォルトセッション
有線診断セッション
有線書換えセッション
セッション維持要求
セッション維持要求
セッション復帰要求、タイムアウト、電源オフ、法規サービスの受信
セッション復帰要求、タイムアウト、電源オフ、法規サービスの受信
第2状態（デフォルト、無線診断、無線書換えの状態遷移）
診断セッション移行要求
書換えセッション移行要求
セッション維持要求
デフォルトセッション
無線診断セッション
無線書換えセッション
セッション維持要求
セッション復帰要求、タイムアウト、電源オフ
セッション復帰要求、タイムアウト、電源オフ

[図161]

Fig. 161

第1状態 / 第2状態	デフォルトセッション	有線診断セッション	有線書換えセッション
デフォルトセッション	○ 車両制御	○ 有線診断 ○ 車両制御	○ 有線書換え × 車両制御
無線診断セッション	○ 無線診断 ○ 車両制御	○ 有線診断 ○ 無線診断 ○ 車両制御	○ 有線書換え × 無線診断 × 車両制御
無線書換えセッション	○ 無線書換え ○ 車両制御	○ 無線書換え ○ 有線診断 ○ 車両制御	○ 有線書換え × 無線書換え （有線書換え優先の場合） × 車両制御

○：実行可能
×：実行不能

[図162]

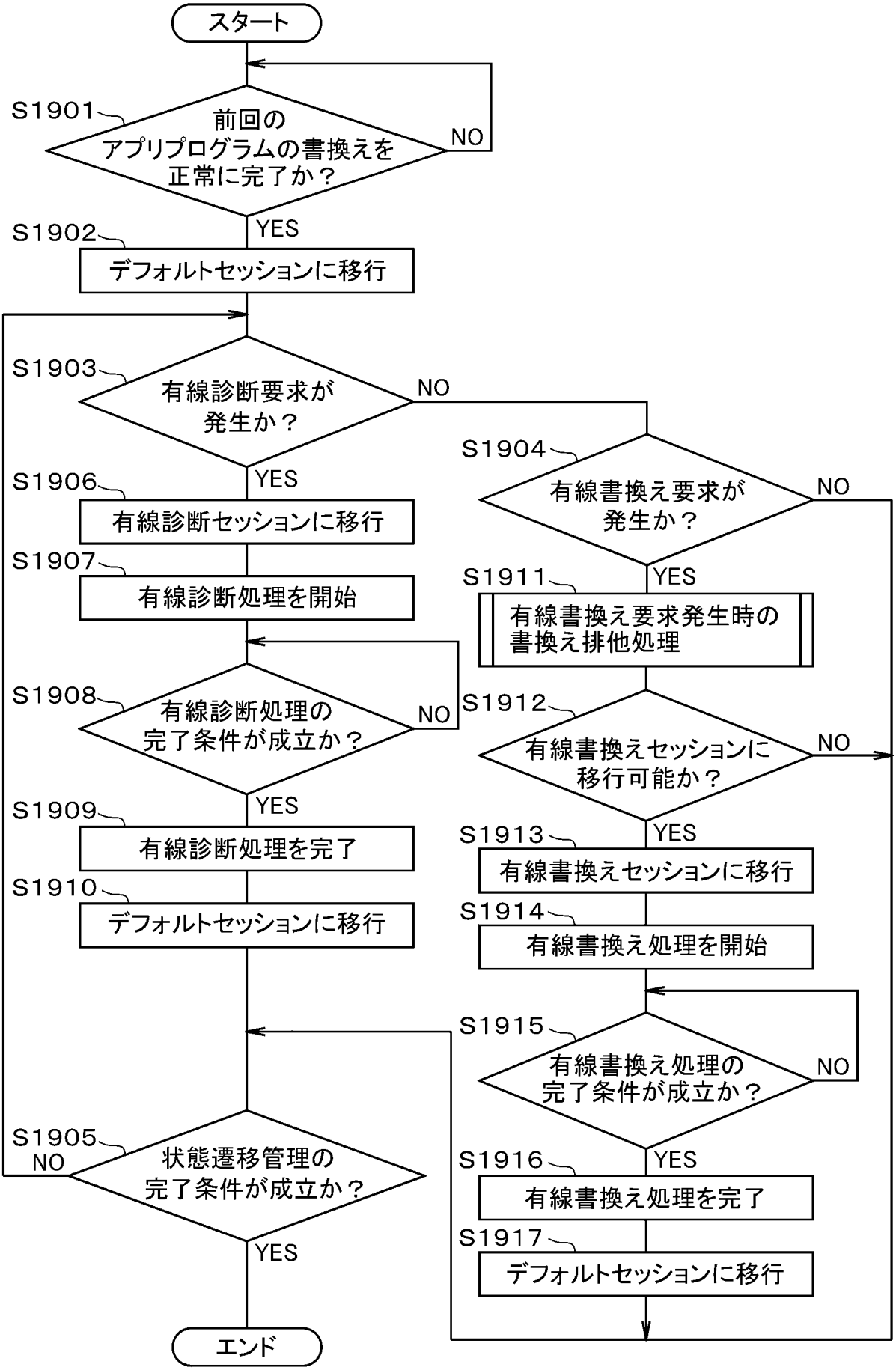
Fig. 162

第1状態 / 第2状態	デフォルトセッション	有線診断セッション	有線書換えセッション
デフォルトセッション	○ 車両制御	○ 有線診断 ○ 車両制御	○ 有線書換え ○ 車両制御
無線診断セッション	○ 無線診断 ○ 車両制御	○ 有線診断 ○ 無線診断 ○ 車両制御	○ 有線書換え ○ 無線診断 ○ 車両制御
無線書換えセッション	○ 無線書換え ○ 車両制御	○ 無線書換え ○ 有線診断 ○ 車両制御	○ 有線書換え × 無線書換え （有線書換え優先の場合） ○ 車両制御

○：実行可能
×：実行不能

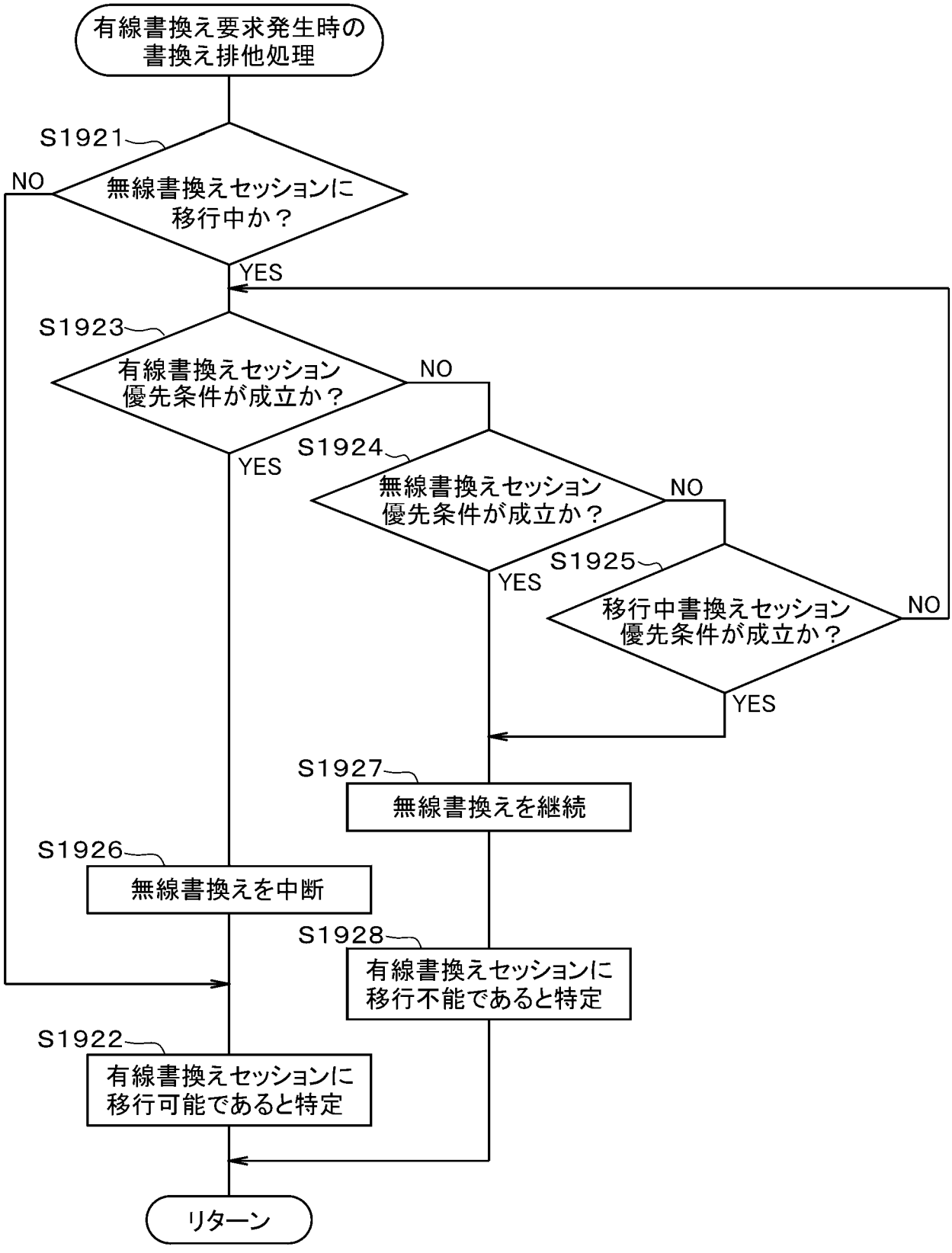
[図163]

Fig. 163 第1状態の状態遷移管理



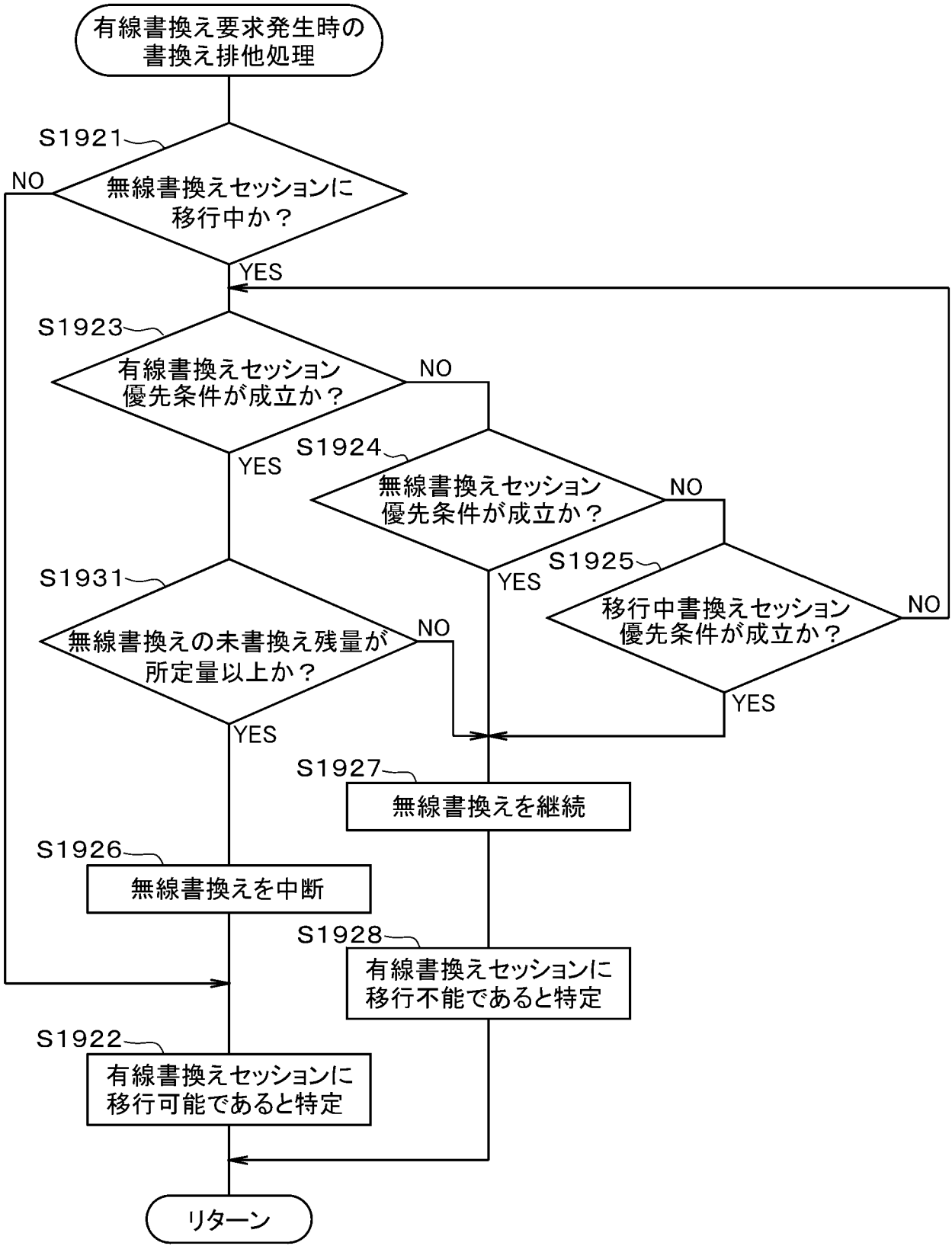
[図164]

Fig. 164


有線書換え要求発生時の
書換え排他処理
S1921
無線書換えセッションに
移行中か？
NO
YES
S1923
有線書換えセッション
優先条件が成立か？
NO
YES
S1924
無線書換えセッション
優先条件が成立か？
NO
YES
S1925
移行中書換えセッション
優先条件が成立か？
NO
YES
S1927
無線書換えを継続
S1926
無線書換えを中断
S1928
有線書換えセッションに
移行不能であると特定
S1922
有線書換えセッションに
移行可能であると特定
リターン

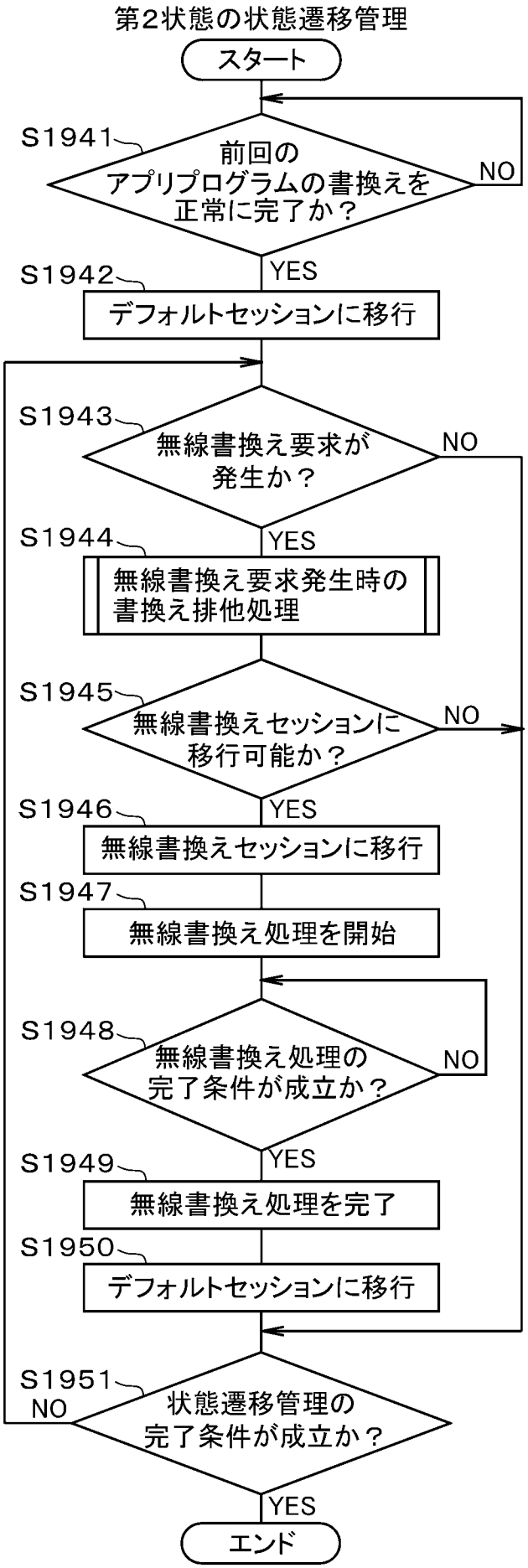
[図165]

Fig. 165


有線書換え要求発生時の
書換え排他処理
S1921
無線書換えセッションに
移行中か？
NO
YES
S1923
有線書換えセッション
優先条件が成立か？
NO
YES
S1924
無線書換えセッション
優先条件が成立か？
NO
YES
S1925
移行中書換えセッション
優先条件が成立か？
NO
YES
S1931
無線書換えの未書換え残量が
所定量以上か？
NO
YES
S1927
無線書換えを継続
S1926
無線書換えを中断
S1928
有線書換えセッションに
移行不能であると特定
S1922
有線書換えセッションに
移行可能であると特定
リターン

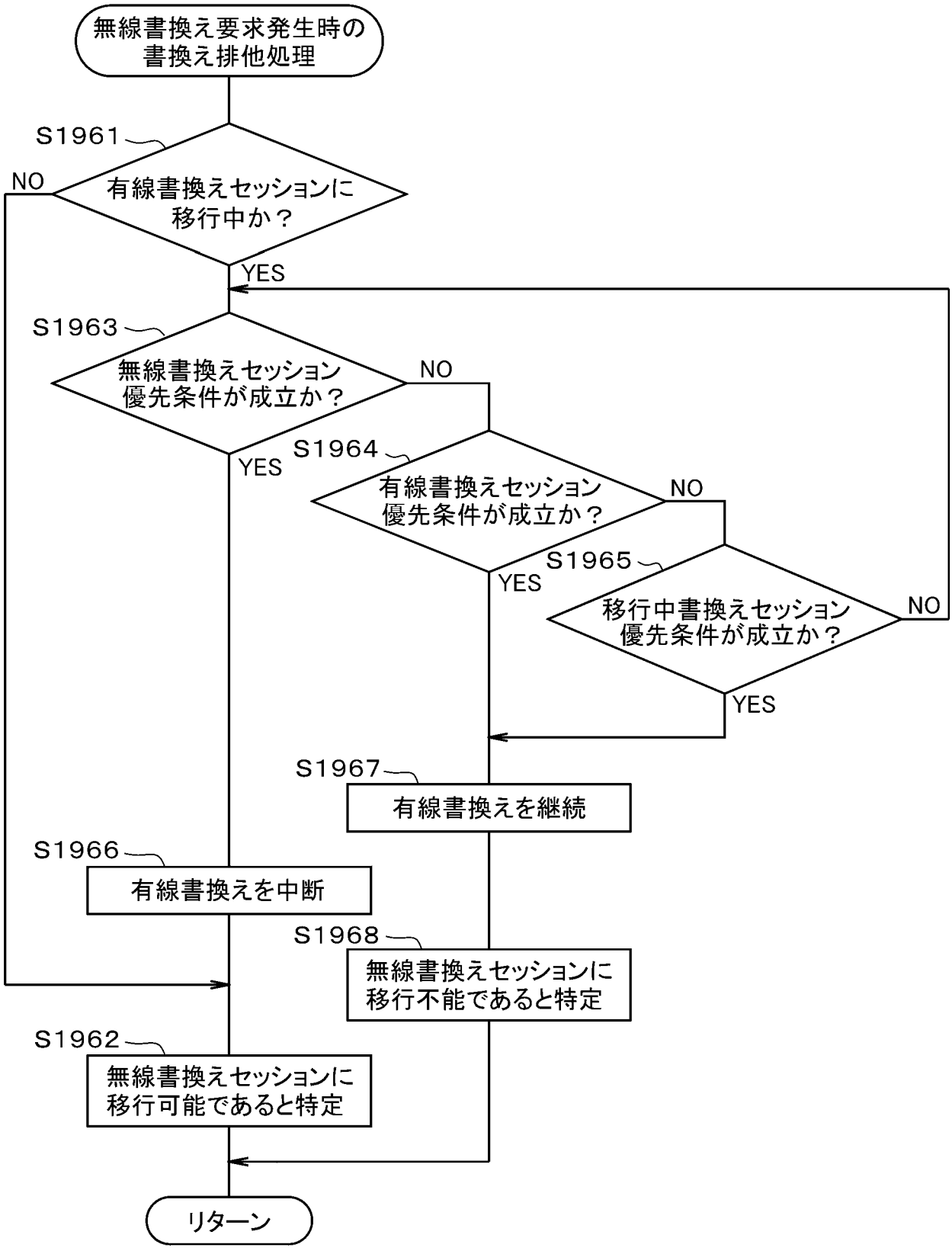
[図166]

Fig. 166


第2状態の状態遷移管理
スタート
S1941
前回の
アプリプログラムの書換えを
正常に完了か？
NO
YES
S1942
デフォルトセッションに移行
S1943
無線書換え要求が
発生か？
NO
YES
S1944
無線書換え要求発生時の
書換え排他処理
S1945
無線書換えセッションに
移行可能か？
NO
YES
S1946
無線書換えセッションに移行
S1947
無線書換え処理を開始
S1948
無線書換え処理の
完了条件が成立か？
NO
YES
S1949
無線書換え処理を完了
S1950
デフォルトセッションに移行
S1951
状態遷移管理の
完了条件が成立か？
NO
YES
エンド

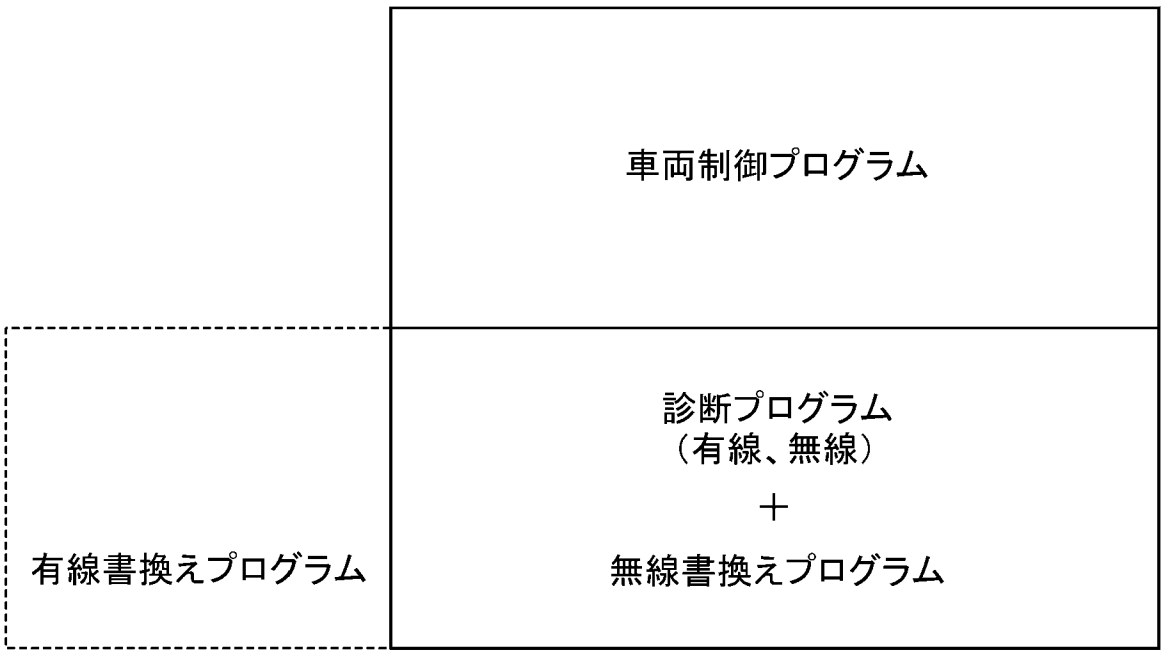
[図167]

Fig. 167


無線書換え要求発生時の
書換え排他処理
S1961
有線書換えセッションに
移行中か？
NO
YES
S1963
無線書換えセッション
優先条件が成立か？
NO
YES
S1964
有線書換えセッション
優先条件が成立か？
NO
YES
S1965
移行中書換えセッション
優先条件が成立か？
NO
YES
S1967
有線書換えを継続
S1966
有線書換えを中断
S1968
無線書換えセッションに
移行不能であると特定
S1962
無線書換えセッションに
移行可能であると特定
リターン

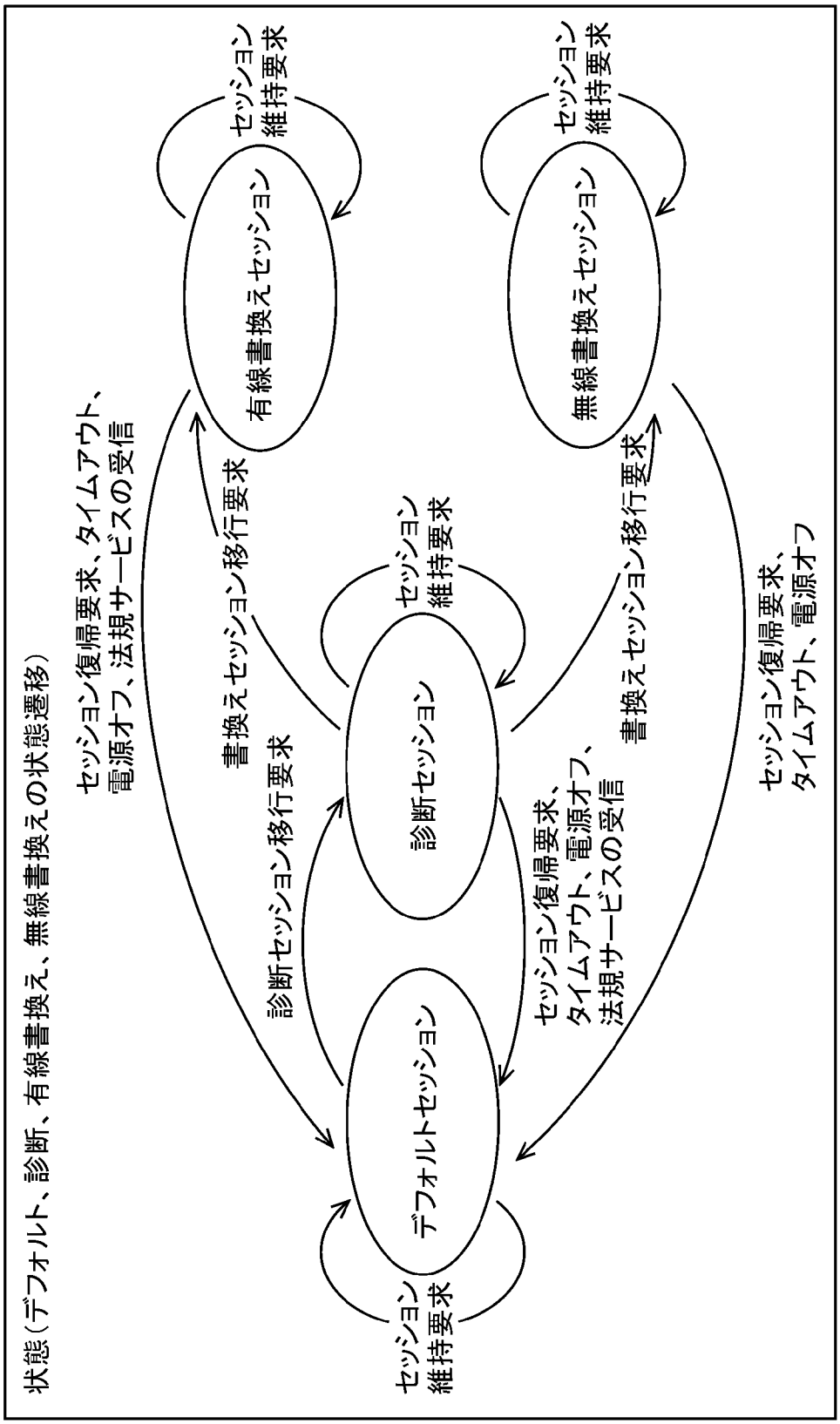
[図168]

Fig. 168



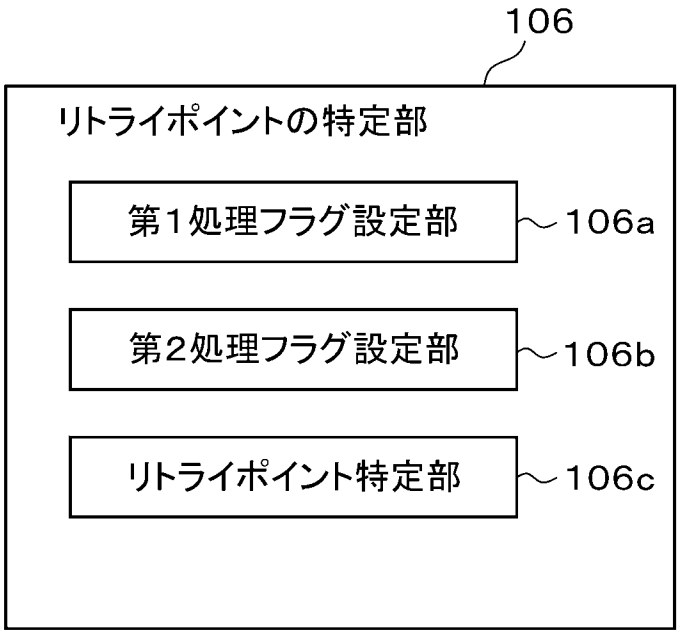
[図169]

Fig. 169


状態（デフォルト、診断、有線書換え、無線書換えの状態遷移）
セッション復帰要求、タイムアウト、
電源オフ、法規サービスの受信
セッション
維持要求
有線書換えセッション
書換えセッション移行要求
セッション
維持要求
無線書換えセッション
書換えセッション移行要求
セッション
維持要求
診断セッション
診断セッション移行要求
セッション復帰要求、
タイムアウト、電源オフ、
法規サービスの受信
セッション復帰要求、
タイムアウト、電源オフ
セッション
維持要求
デフォルトセッション

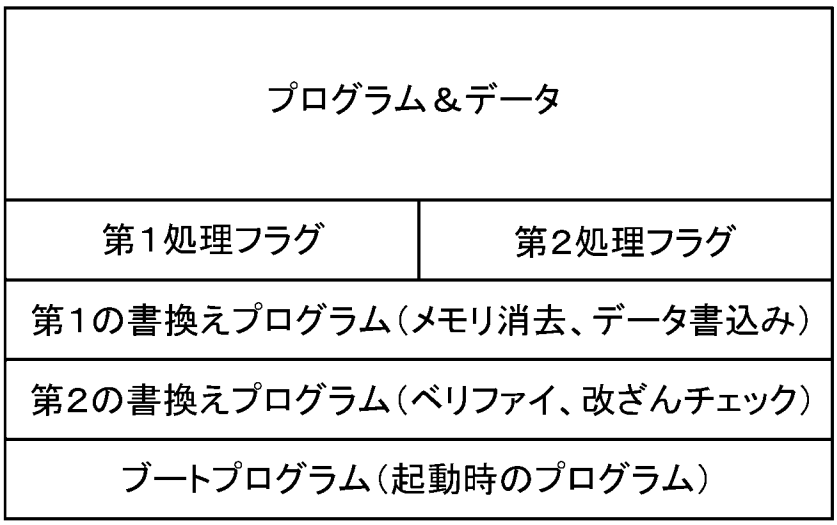
[図170]

Fig. 170



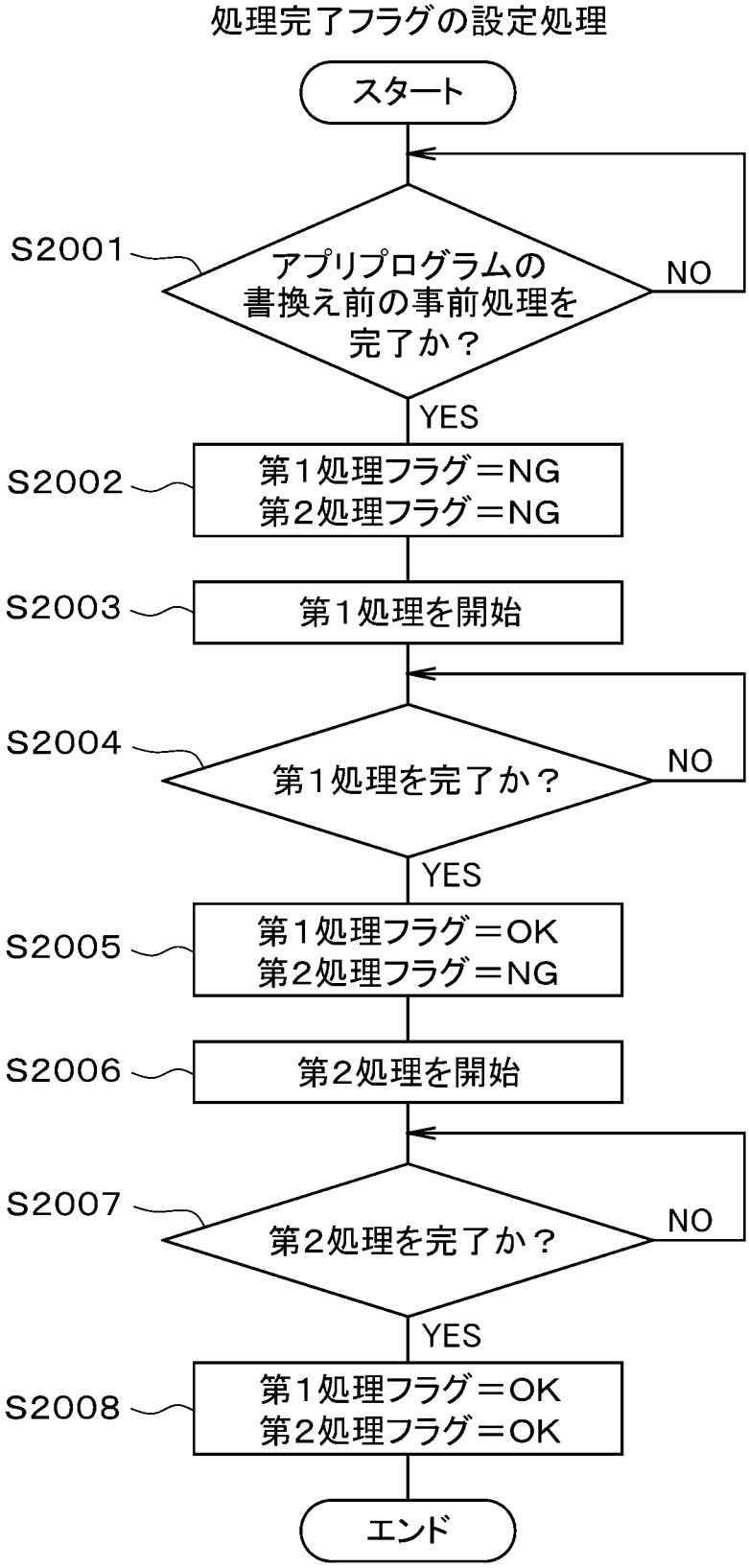
[図171]

Fig. 171



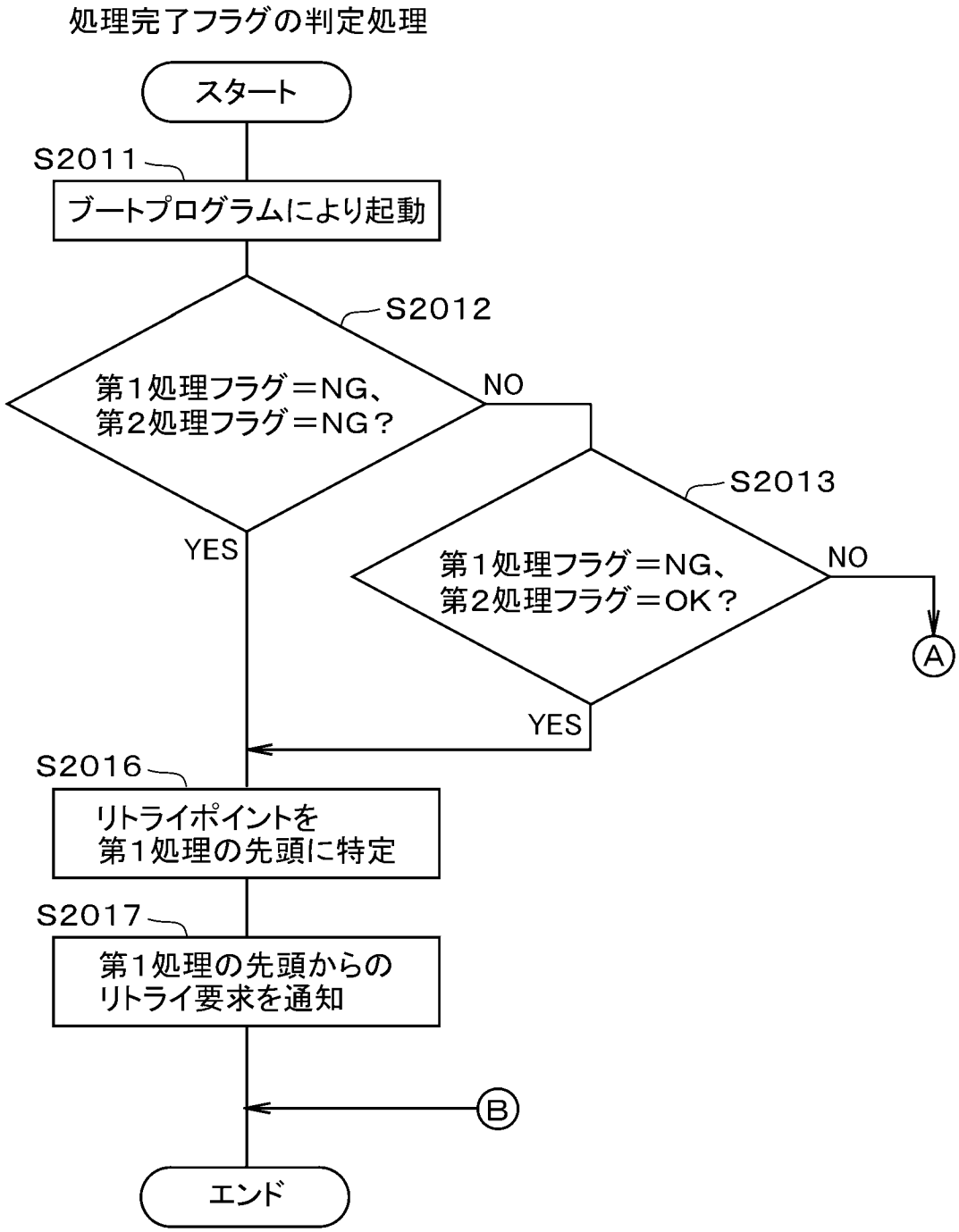
[図172]

Fig. 172


処理完了フラグの設定処理
スタート
S2001
アプリプログラムの
書換え前の事前処理を
完了か？
NO
YES
S2002
第1処理フラグ＝NG
第2処理フラグ＝NG
S2003
第1処理を開始
S2004
第1処理を完了か？
NO
YES
S2005
第1処理フラグ＝OK
第2処理フラグ＝NG
S2006
第2処理を開始
S2007
第2処理を完了か？
NO
YES
S2008
第1処理フラグ＝OK
第2処理フラグ＝OK
エンド

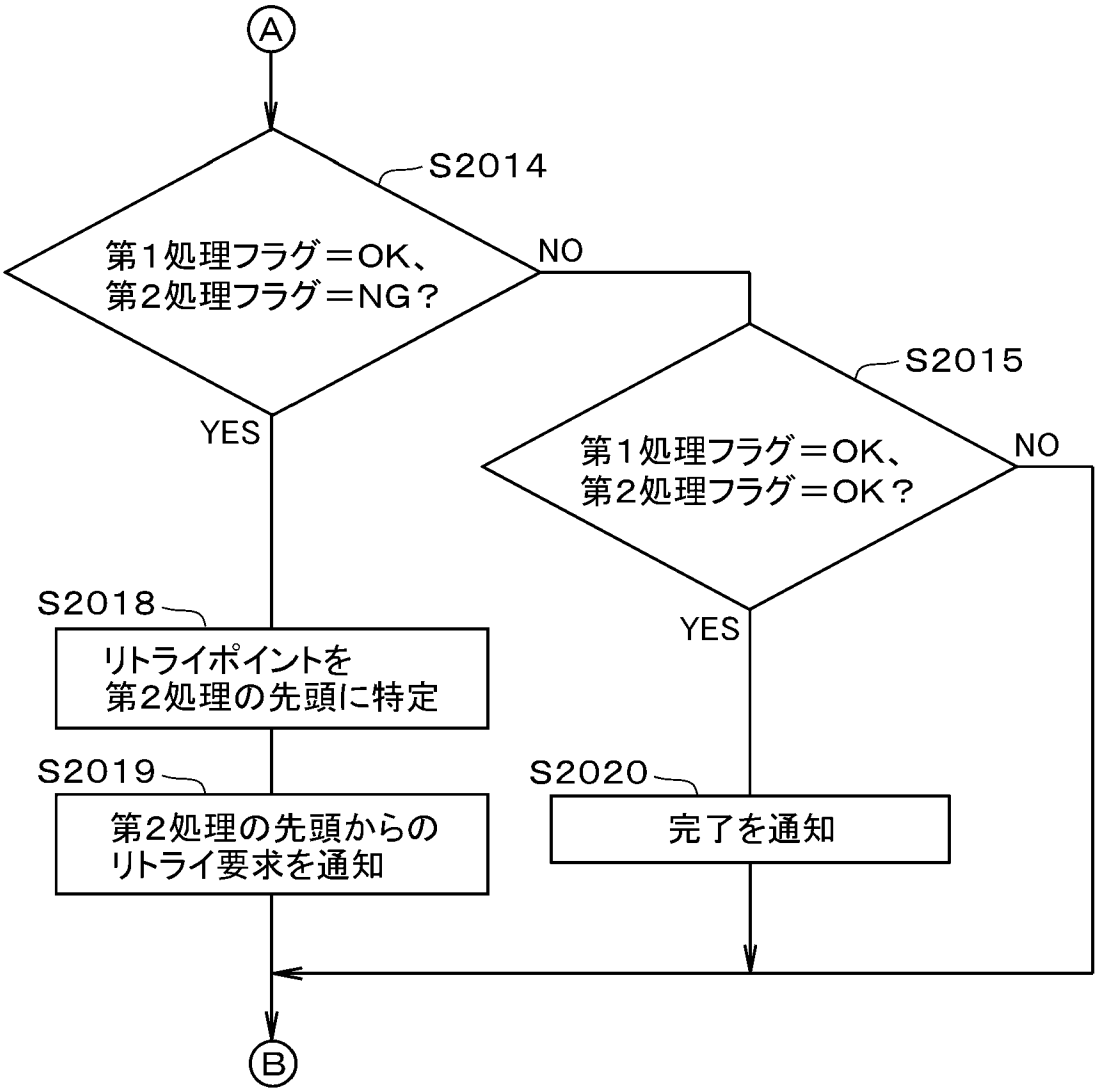
[図173]

Fig. 173


処理完了フラグの判定処理
スタート
S2011
ブートプログラムにより起動
S2012
第1処理フラグ＝NG、
第2処理フラグ＝NG？
NO
YES
S2013
第1処理フラグ＝NG、
第2処理フラグ＝OK？
NO
YES
A
S2016
リトライポイントを
第1処理の先頭に特定
S2017
第1処理の先頭からの
リトライ要求を通知
B
エンド

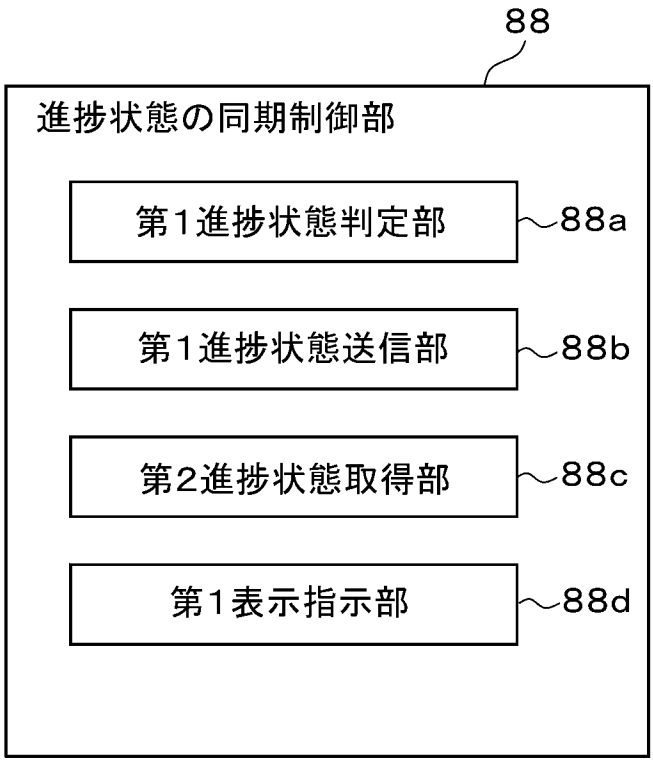
[図174]

Fig. 174


A
S2014
第1処理フラグ＝OK、
第2処理フラグ＝NG？
NO
YES
S2015
第1処理フラグ＝OK、
第2処理フラグ＝OK？
NO
YES
S2018
リトライポイントを
第2処理の先頭に特定
S2019
第2処理の先頭からの
リトライ要求を通知
S2020
完了を通知
B

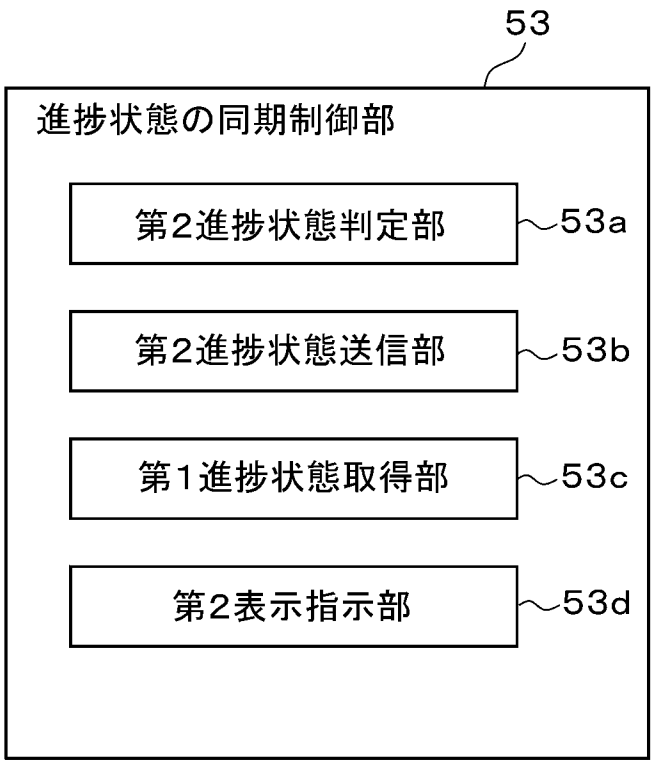
[図175]

Fig. 175



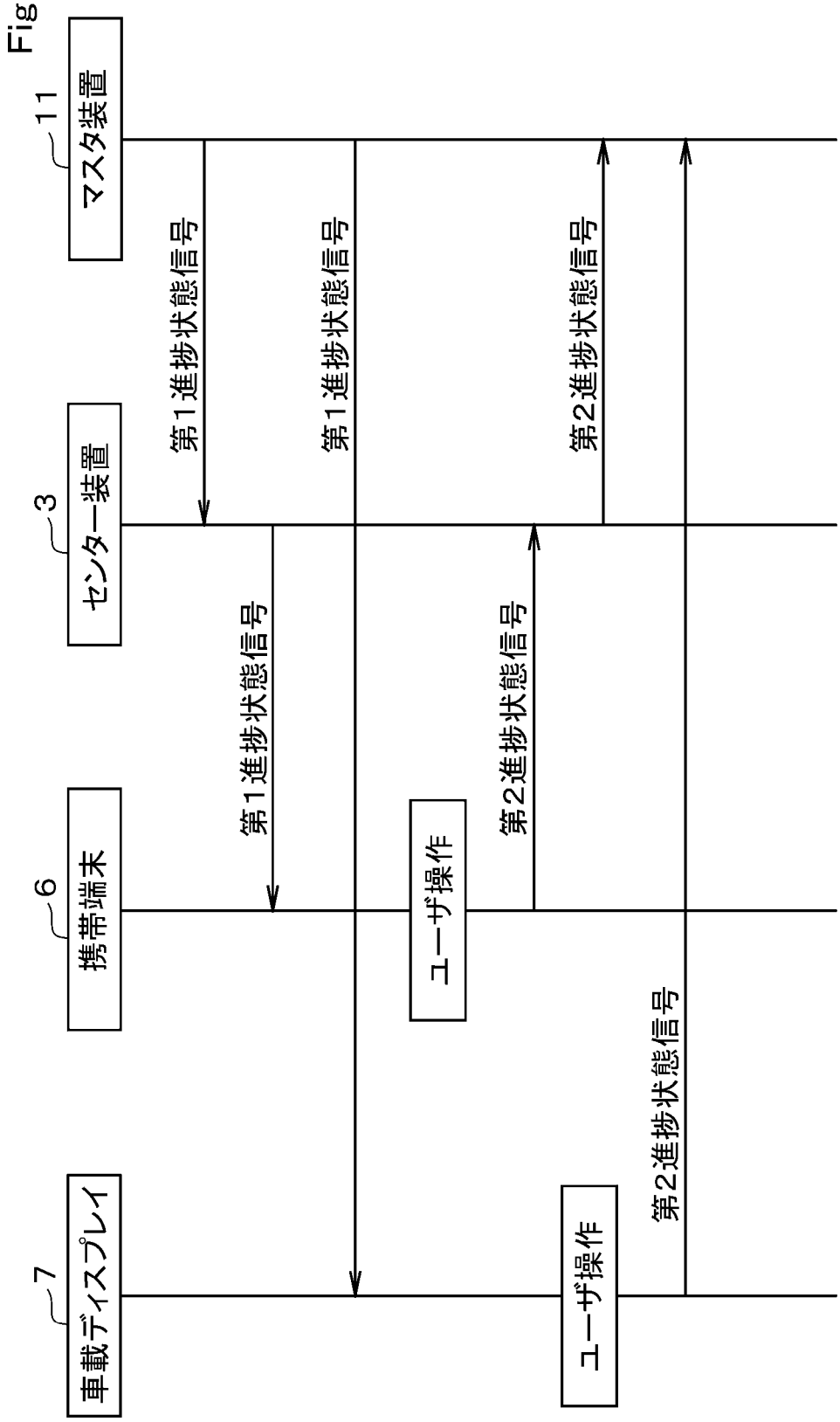
[図176]

Fig. 176



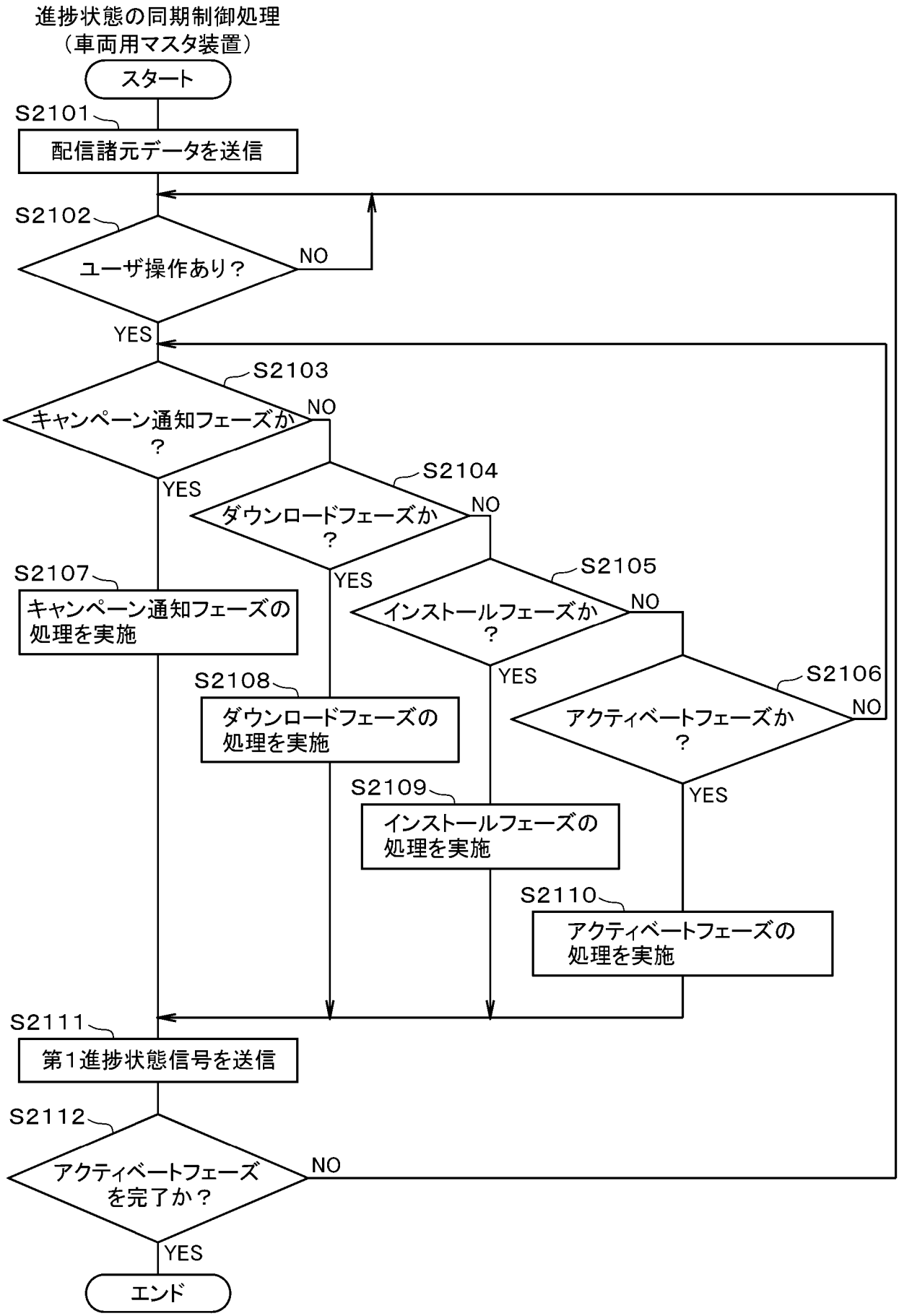
[図177]

Fig. 177


11
マスタ装置
3
センター装置
6
携帯端末
7
車載ディスプレイ
第1進捗状態信号
第1進捗状態信号
第2進捗状態信号
第1進捗状態信号
第2進捗状態信号
ユーザ操作
ユーザ操作
第2進捗状態信号

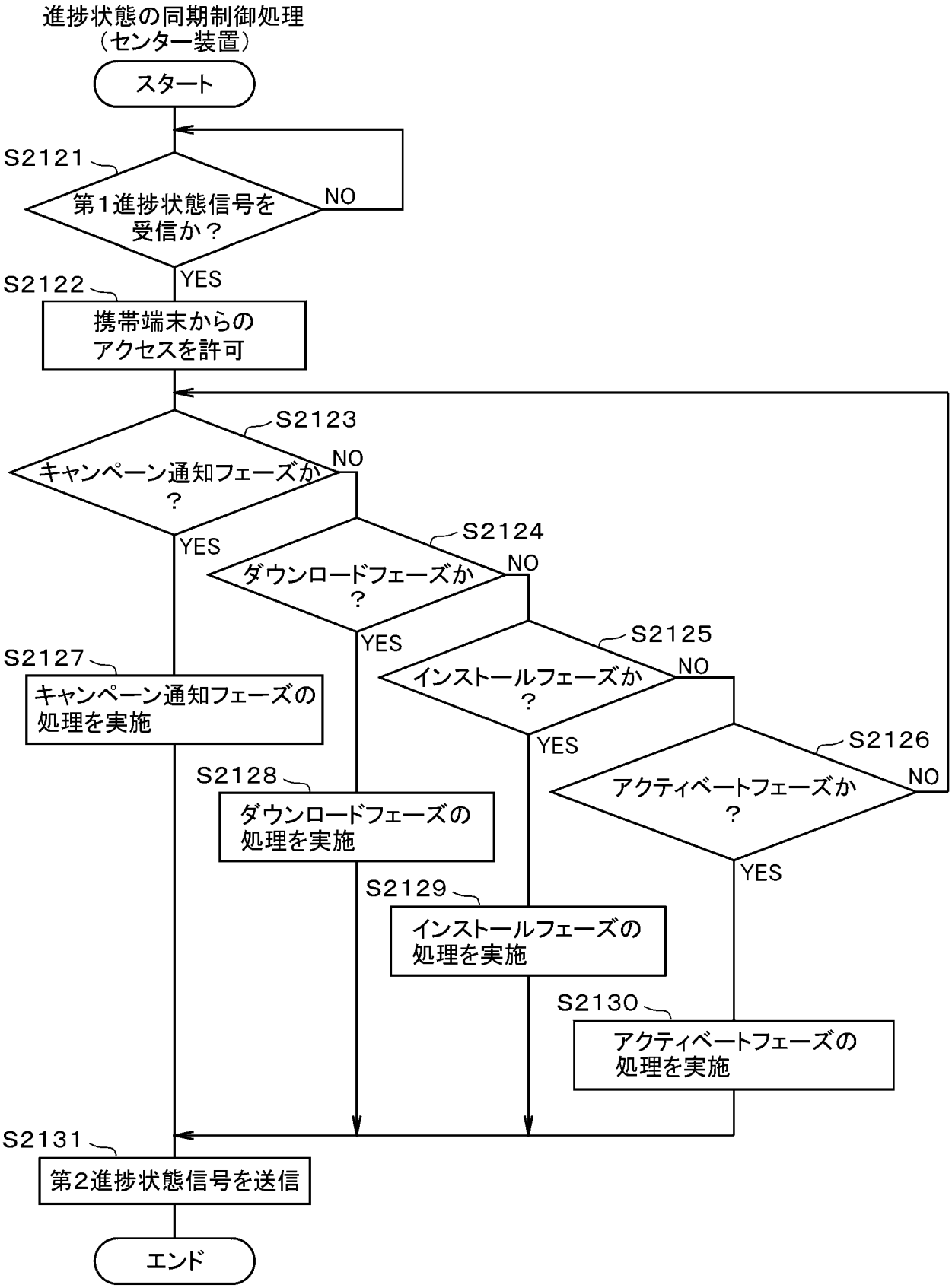
[図178]

Fig. 178


進捗状態の同期制御処理
（車両用マスタ装置）
スタート
S2101
配信諸元データを送信
S2102
ユーザ操作あり？
NO
YES
S2103
キャンペーン通知フェーズか？
NO
YES
S2104
ダウンロードフェーズか？
NO
YES
S2105
インストールフェーズか？
NO
YES
S2106
アクティベートフェーズか？
NO
YES
S2107
キャンペーン通知フェーズの処理を実施
S2108
ダウンロードフェーズの処理を実施
S2109
インストールフェーズの処理を実施
S2110
アクティベートフェーズの処理を実施
S2111
第1進捗状態信号を送信
S2112
アクティベートフェーズを完了か？
NO
YES
エンド

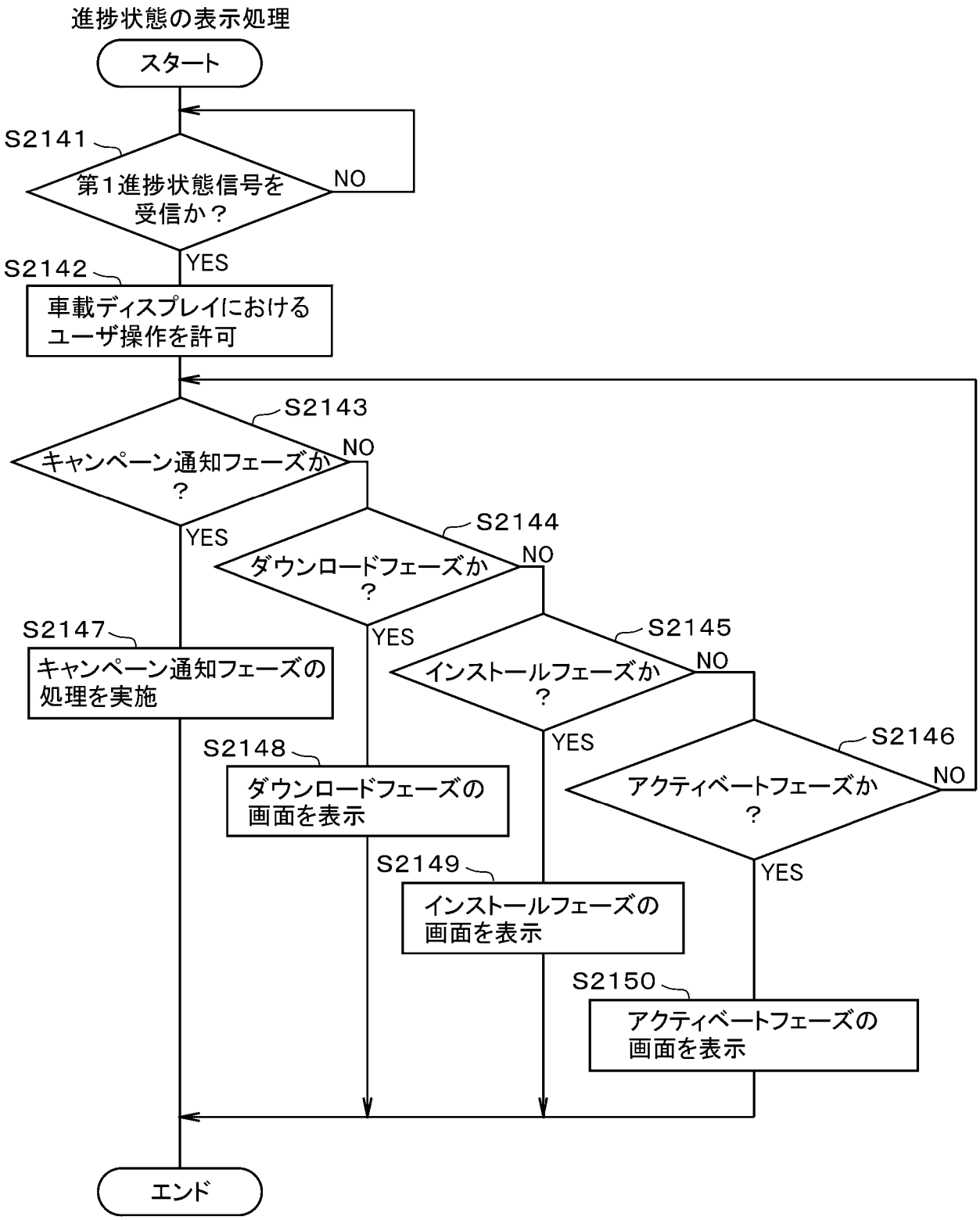
[図179]

Fig. 179


進捗状態の同期制御処理
（センター装置）
スタート
S2121
第1進捗状態信号を受信か？
NO
YES
S2122
携帯端末からのアクセスを許可
S2123
キャンペーン通知フェーズか？
NO
YES
S2124
ダウンロードフェーズか？
NO
YES
S2125
インストールフェーズか？
NO
YES
S2126
アクティベートフェーズか？
NO
YES
S2127
キャンペーン通知フェーズの処理を実施
S2128
ダウンロードフェーズの処理を実施
S2129
インストールフェーズの処理を実施
S2130
アクティベートフェーズの処理を実施
S2131
第2進捗状態信号を送信
エンド

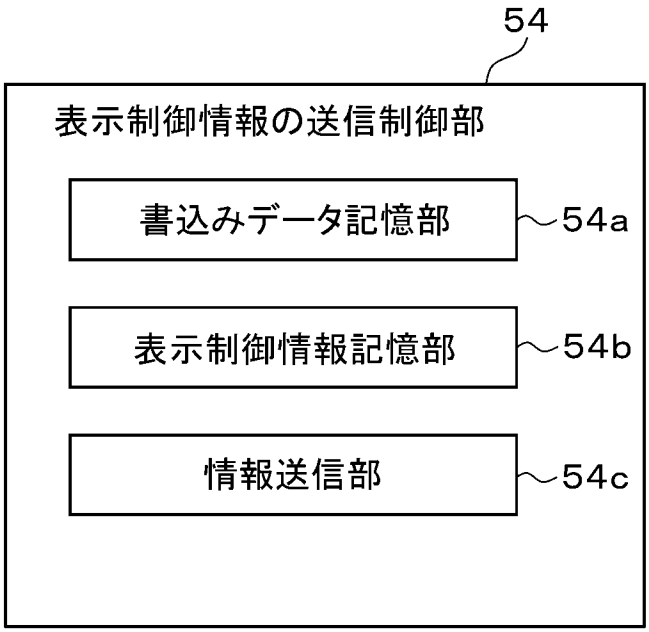
[図180]

Fig. 180


進捗状態の表示処理
スタート
S2141
第1進捗状態信号を受信か？
NO
YES
S2142
車載ディスプレイにおけるユーザ操作を許可
S2143
キャンペーン通知フェーズか？
NO
YES
S2144
ダウンロードフェーズか？
NO
YES
S2145
インストールフェーズか？
NO
YES
S2146
アクティベートフェーズか？
NO
YES
S2147
キャンペーン通知フェーズの処理を実施
S2148
ダウンロードフェーズの画面を表示
S2149
インストールフェーズの画面を表示
S2150
アクティベートフェーズの画面を表示
エンド

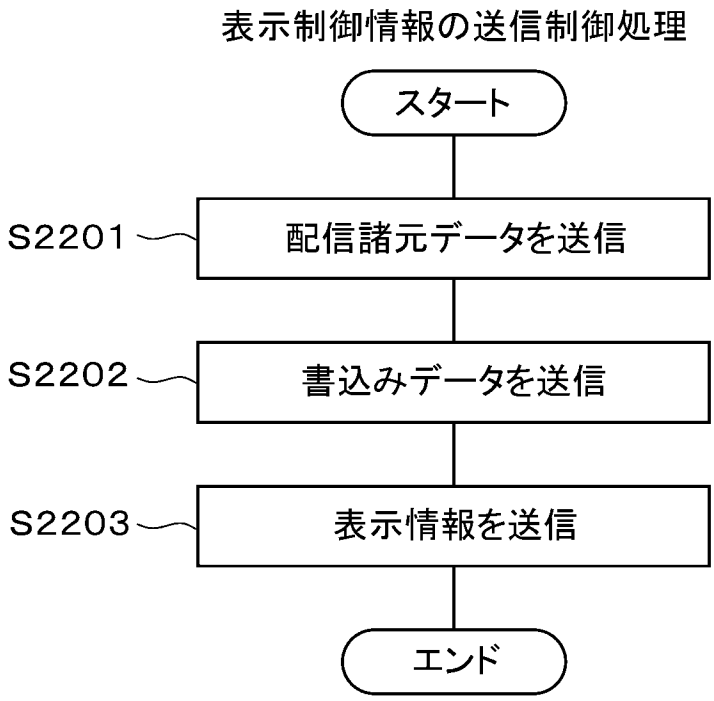
[図181]

Fig. 181



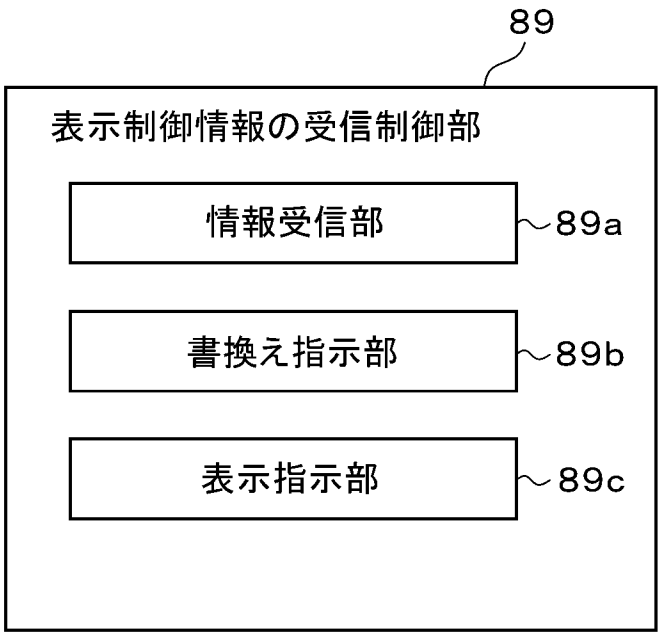
[図182]

Fig. 182



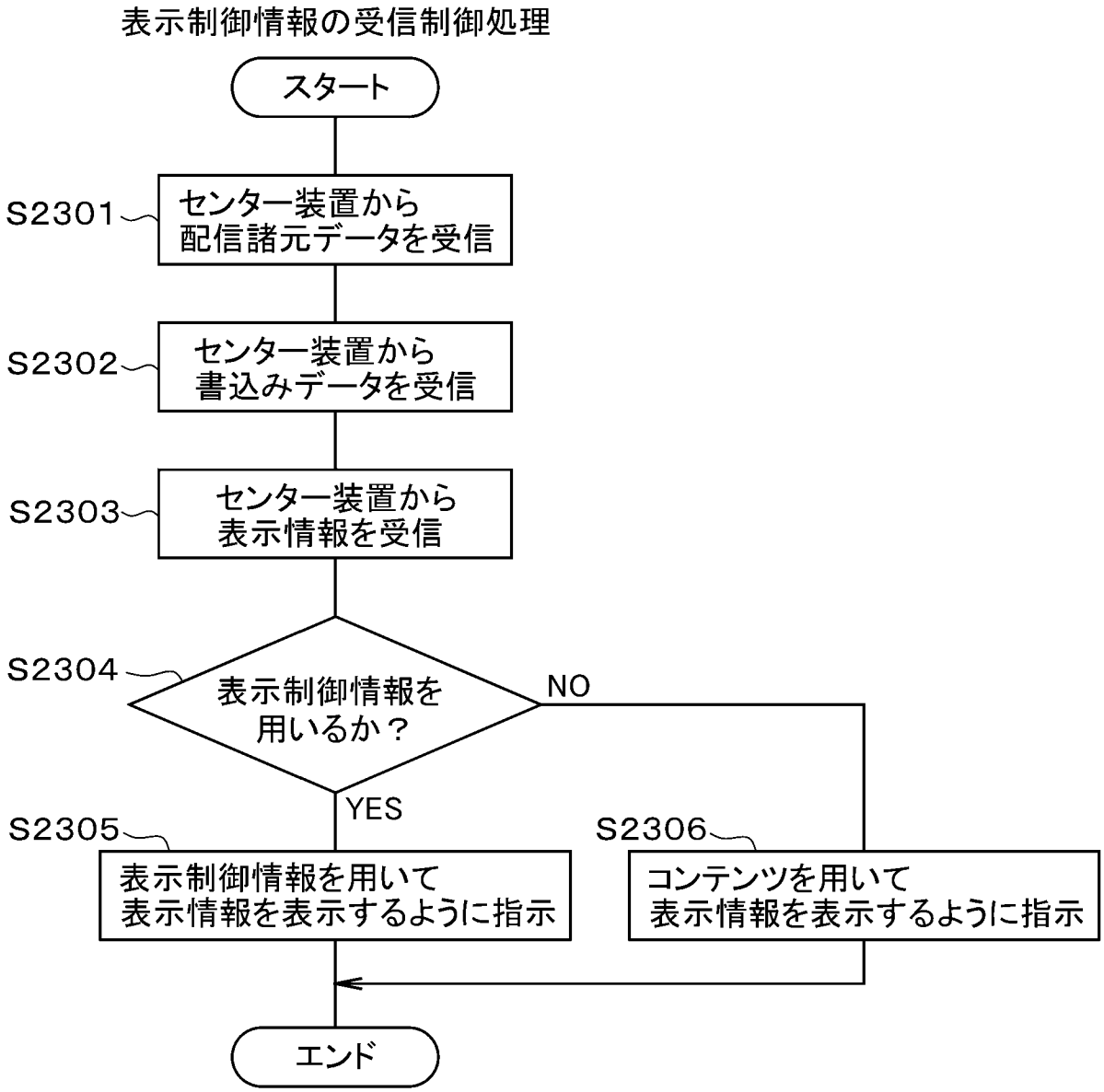
[図183]

Fig. 183



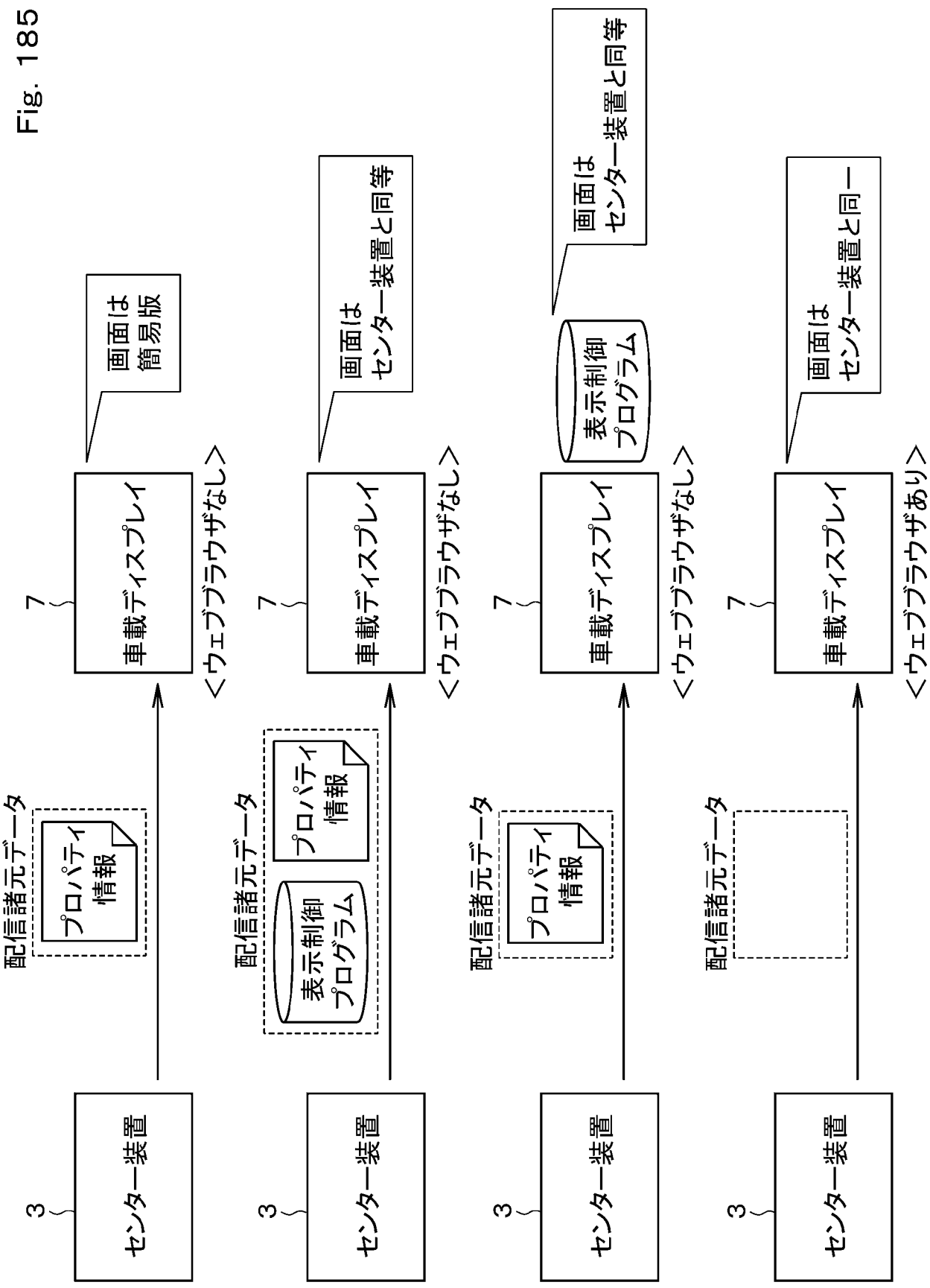
[図184]

Fig. 184


表示制御情報の受信制御処理
スタート
S2301
センター装置から
配信諸元データを受信
S2302
センター装置から
書込みデータを受信
S2303
センター装置から
表示情報を受信
S2304
表示制御情報を
用いるか？
NO
YES
S2305
表示制御情報を用いて
表示情報を表示するように指示
S2306
コンテンツを用いて
表示情報を表示するように指示
エンド

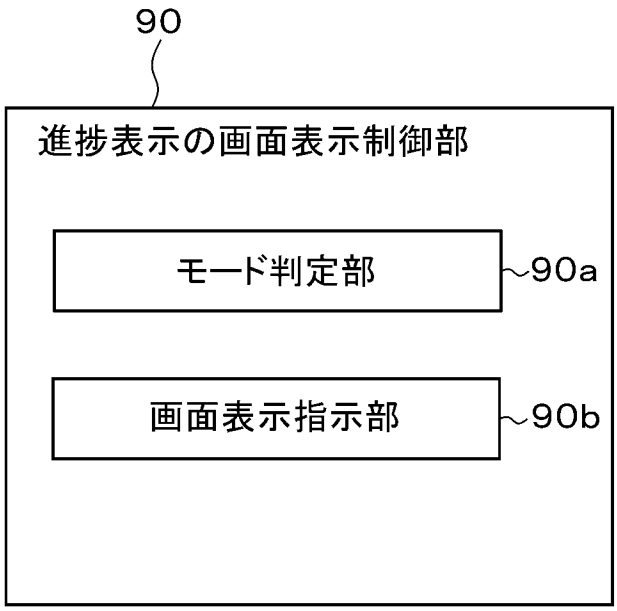
[図185]

Fig. 185


3
センター装置
配信諸元データ
プロパティ情報
7
車載ディスプレイ
画面は簡易版
<ウェブブラウザなし>
3
センター装置
配信諸元データ
プロパティ情報
表示制御プログラム
7
車載ディスプレイ
画面はセンター装置と同等
<ウェブブラウザなし>
3
センター装置
配信諸元データ
プロパティ情報
7
車載ディスプレイ
表示制御プログラム
画面はセンター装置と同等
<ウェブブラウザなし>
3
センター装置
配信諸元データ
7
車載ディスプレイ
画面はセンター装置と同一
<ウェブブラウザあり>

[図186]

Fig. 186



[図187]

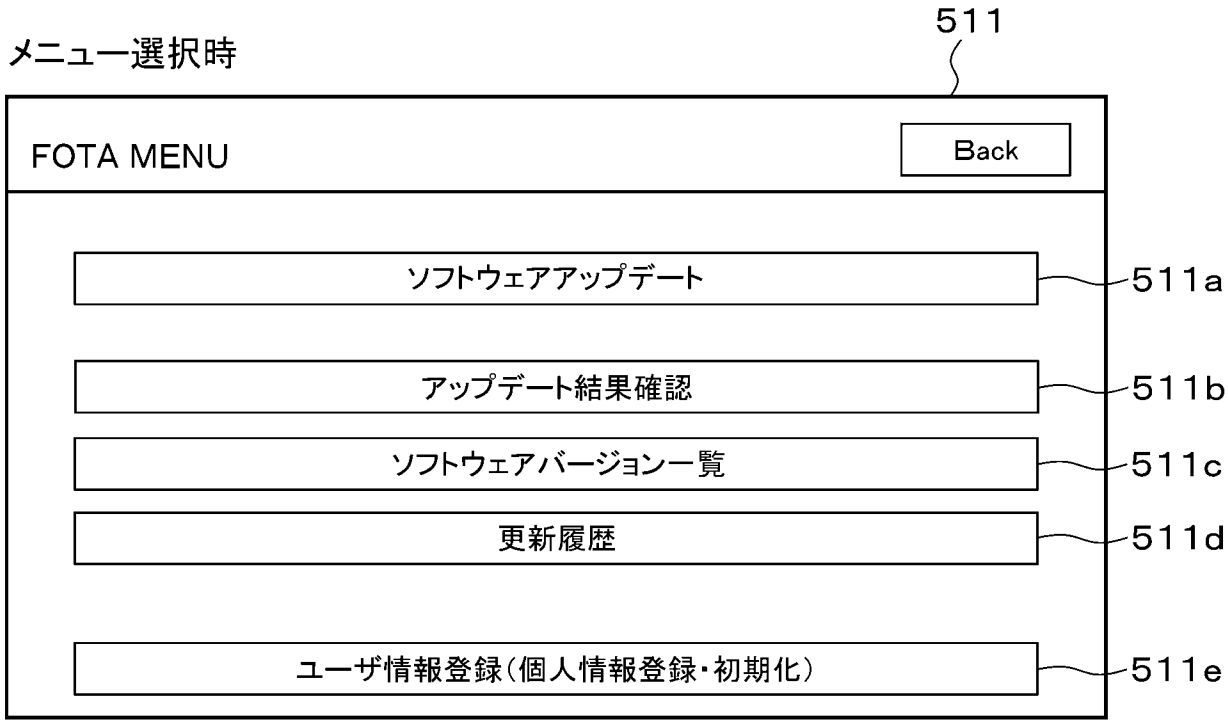
Fig. 187

書換え諸元データ

シーン情報	リコールフラグ
	ディーラーフラグ
	工場フラグ
	機能更新通知フラグ
	強制実行フラグ
有効期限情報	
位置情報	

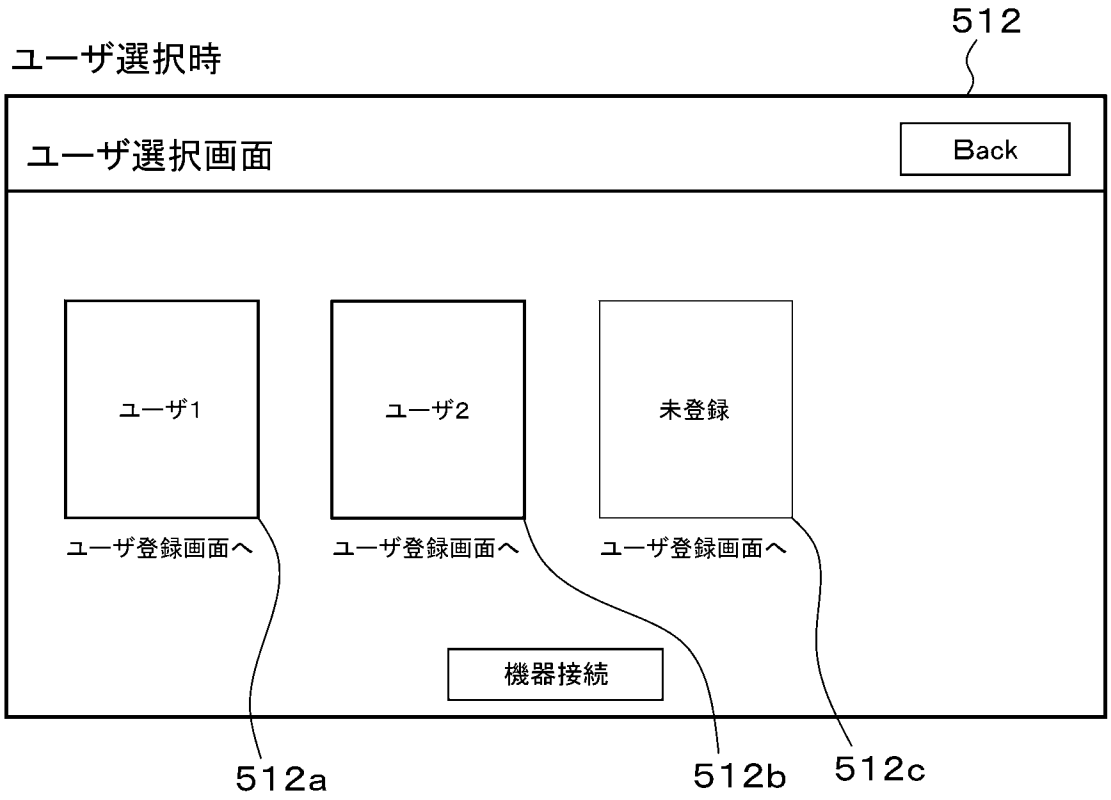
[図188]

Fig. 188


メニュー選択時
511
FOTA MENU
Back
ソフトウェアアップデート
511a
アップデート結果確認
511b
ソフトウェアバージョン一覧
511c
更新履歴
511d
ユーザ情報登録（個人情報登録・初期化）
511e

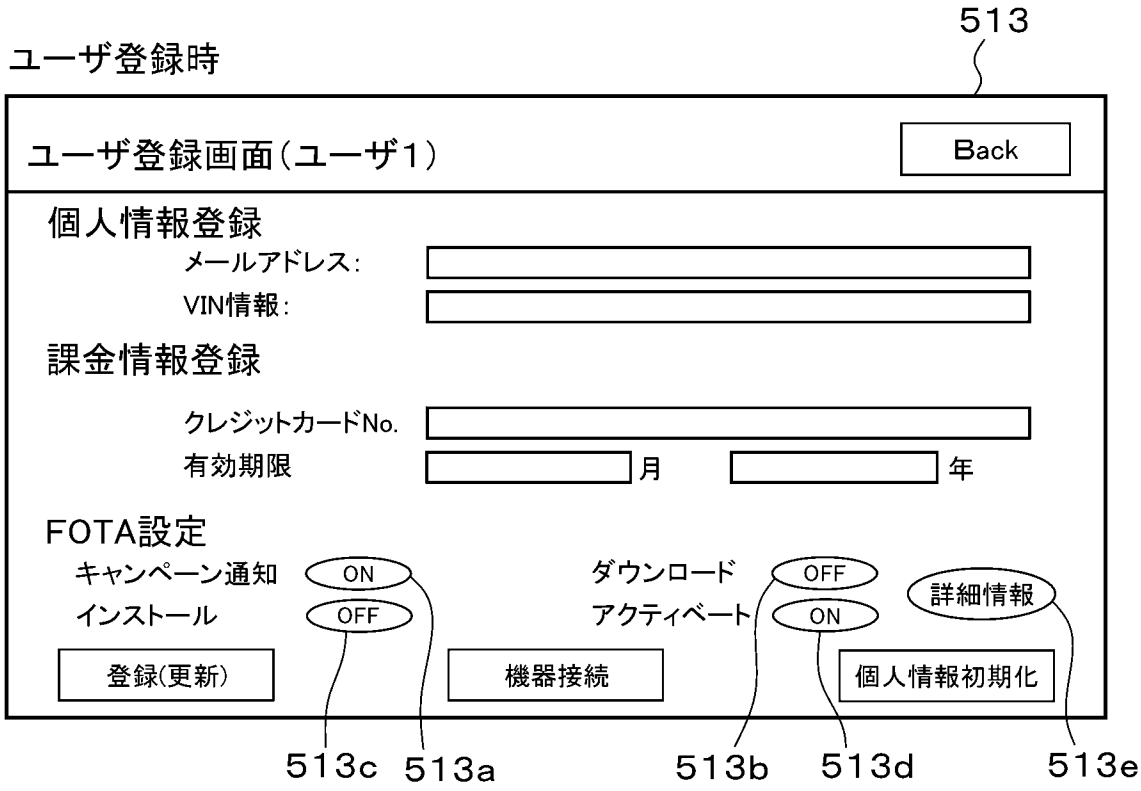
[図189]

Fig. 189


512
ユーザ選択時
ユーザ選択画面
Back
ユーザ1
ユーザ2
未登録
ユーザ登録画面へ
ユーザ登録画面へ
ユーザ登録画面へ
機器接続
512a
512b
512c

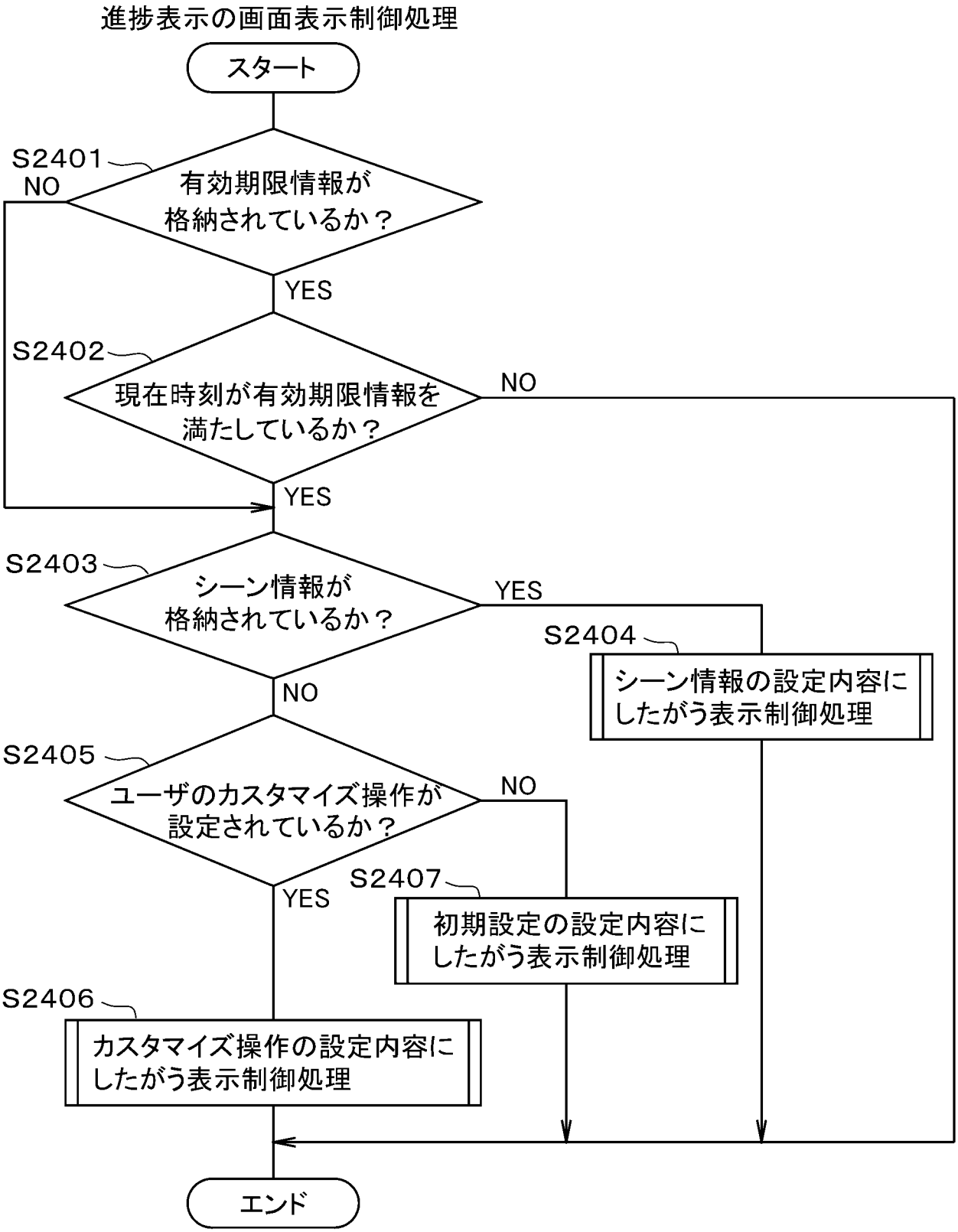
[図190]

Fig. 190


513
ユーザ登録時
ユーザ登録画面(ユーザ1)
Back
個人情報登録
メールアドレス:
VIN情報:
課金情報登録
クレジットカードNo.
有効期限
月
年
FOTA設定
キャンペーン通知
ON
インストール
OFF
ダウンロード
OFF
アクティベート
ON
詳細情報
登録(更新)
機器接続
個人情報初期化
513c
513a
513b
513d
513e

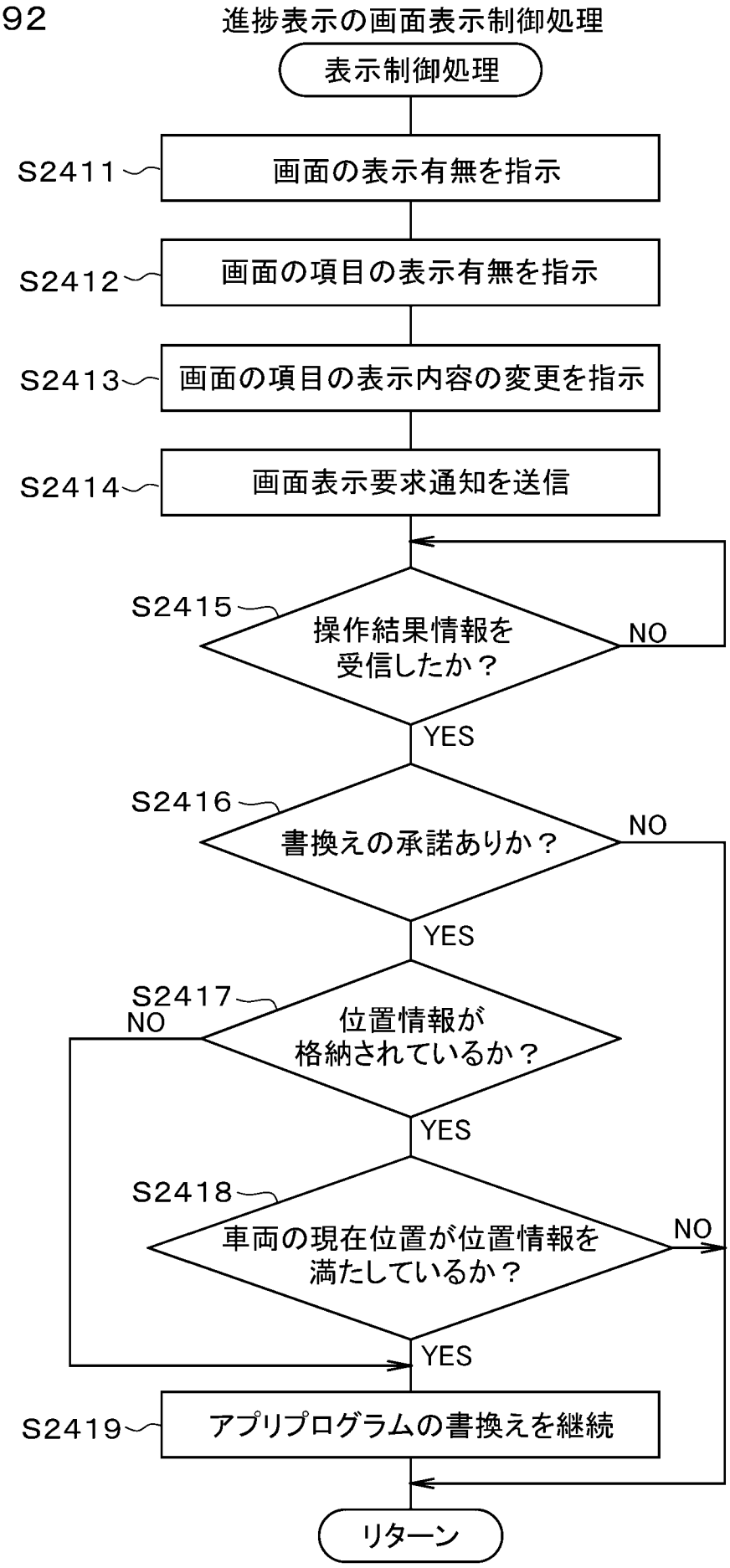
[図191]

Fig. 191


進捗表示の画面表示制御処理
スタート
S2401
有効期限情報が
格納されているか？
NO
YES
S2402
現在時刻が有効期限情報を
満たしているか？
NO
YES
S2403
シーン情報が
格納されているか？
YES
S2404
シーン情報の設定内容に
したがう表示制御処理
NO
S2405
ユーザのカスタマイズ操作が
設定されているか？
NO
S2407
初期設定の設定内容に
したがう表示制御処理
YES
S2406
カスタマイズ操作の設定内容に
したがう表示制御処理
エンド

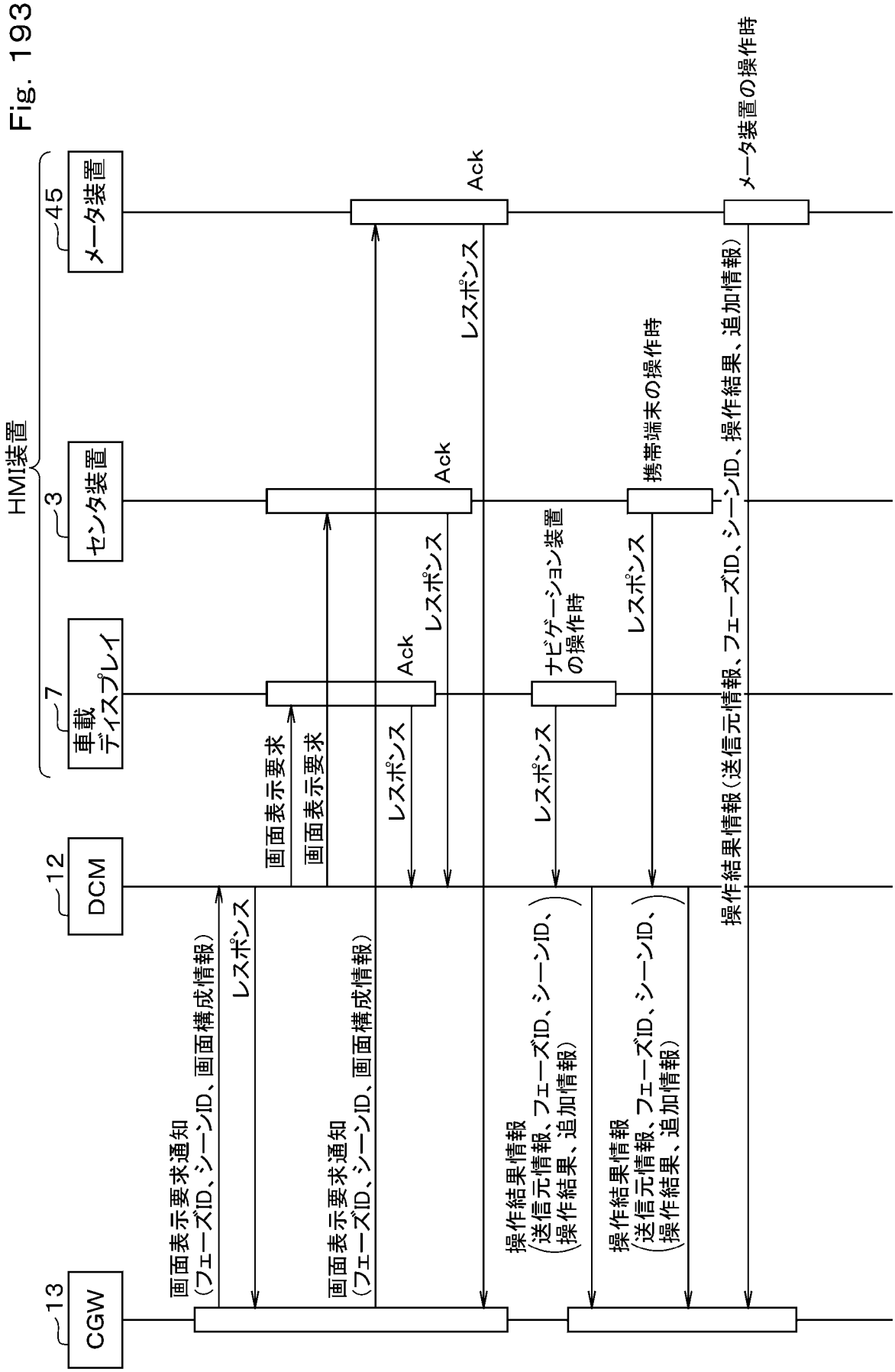
[図192]

Fig. 192


進捗表示の画面表示制御処理
表示制御処理
S2411
画面の表示有無を指示
S2412
画面の項目の表示有無を指示
S2413
画面の項目の表示内容の変更を指示
S2414
画面表示要求通知を送信
S2415
操作結果情報を
受信したか？
NO
YES
S2416
書換えの承諾ありか？
NO
YES
S2417
位置情報が
格納されているか？
NO
YES
S2418
車両の現在位置が位置情報を
満たしているか？
NO
YES
S2419
アプリプログラムの書換えを継続
リターン

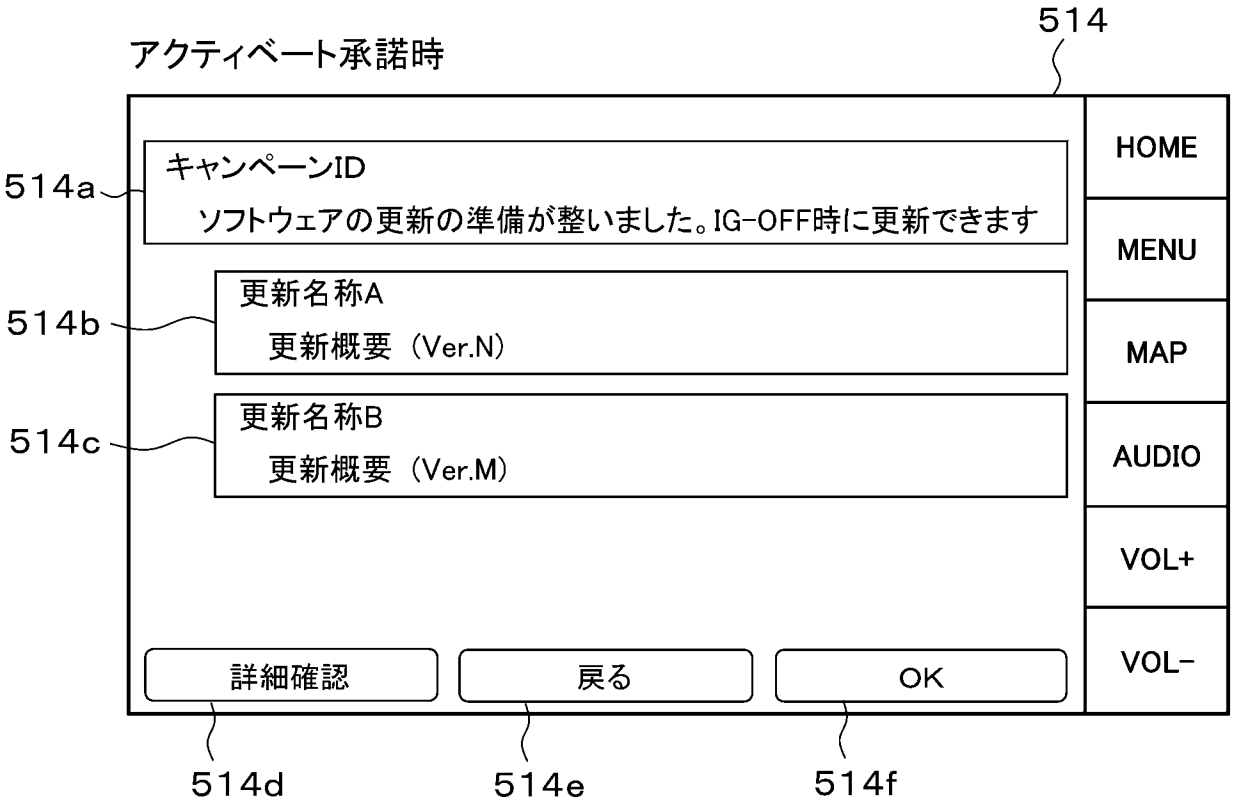
[図193]

Fig. 193


HMI装置
13 CGW
12 DCM
7 車載ディスプレイ
3 センタ装置
45 メータ装置
画面表示要求通知 (フェーズID、シーンID、画面構成情報)
レスポンス
画面表示要求
画面表示要求
Ack
レスポンス
Ack
レスポンス
Ack
レスポンス
画面表示要求通知 (フェーズID、シーンID、画面構成情報)
操作結果情報 (送信元情報、フェーズID、シーンID、操作結果、追加情報)
ナビゲーション装置の操作時
レスポンス
携帯端末の操作時
レスポンス
操作結果情報 (送信元情報、フェーズID、シーンID、操作結果、追加情報)
メータ装置の操作時
操作結果情報 (送信元情報、フェーズID、シーンID、操作結果、追加情報)

[図194]

Fig. 194



[図195]

Fig. 195

項目	表示／非表示
キャンペーン…	表示
更新名称A…	表示
更新名称B…	表示
詳細確認	表示
戻る	表示
OK	表示

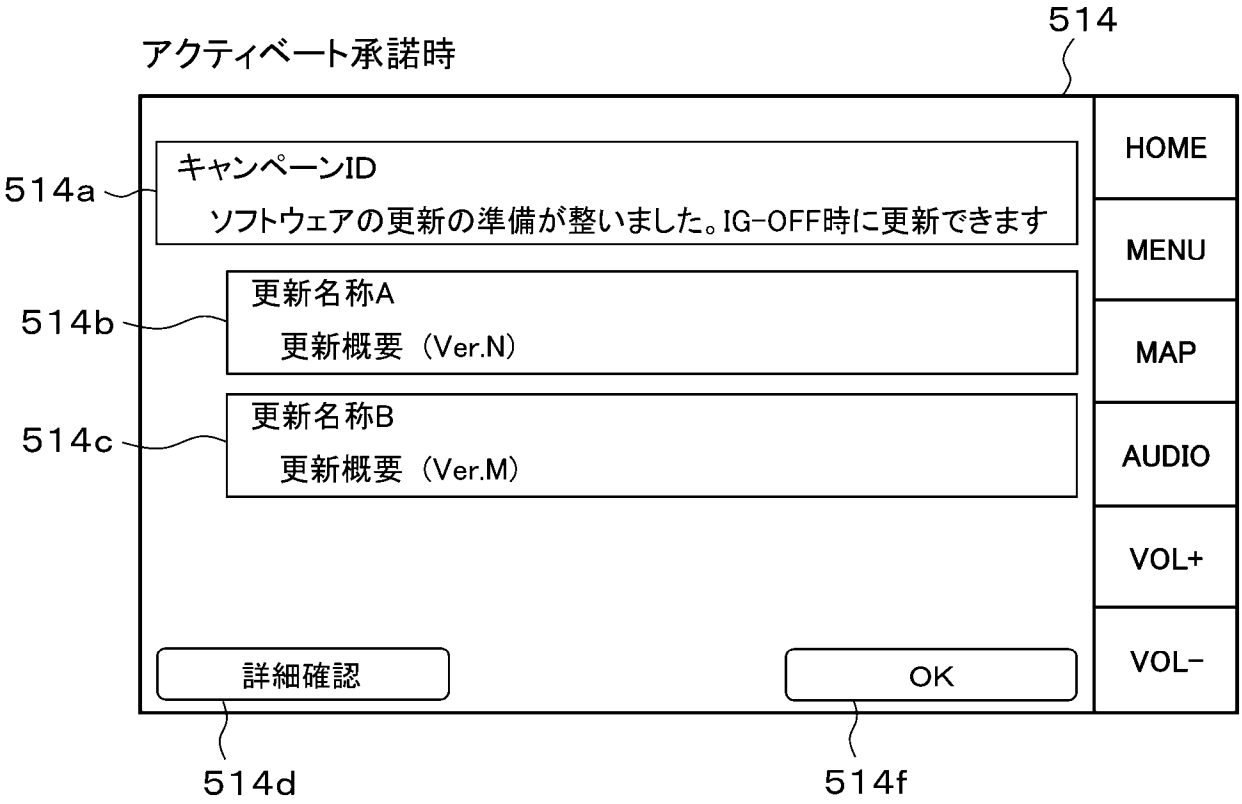
[図196]

Fig. 196

項目	表示／非表示
キャンペーン…	表示
更新名称A…	表示
更新名称B…	表示
詳細確認	表示
戻る	非表示
OK	表示

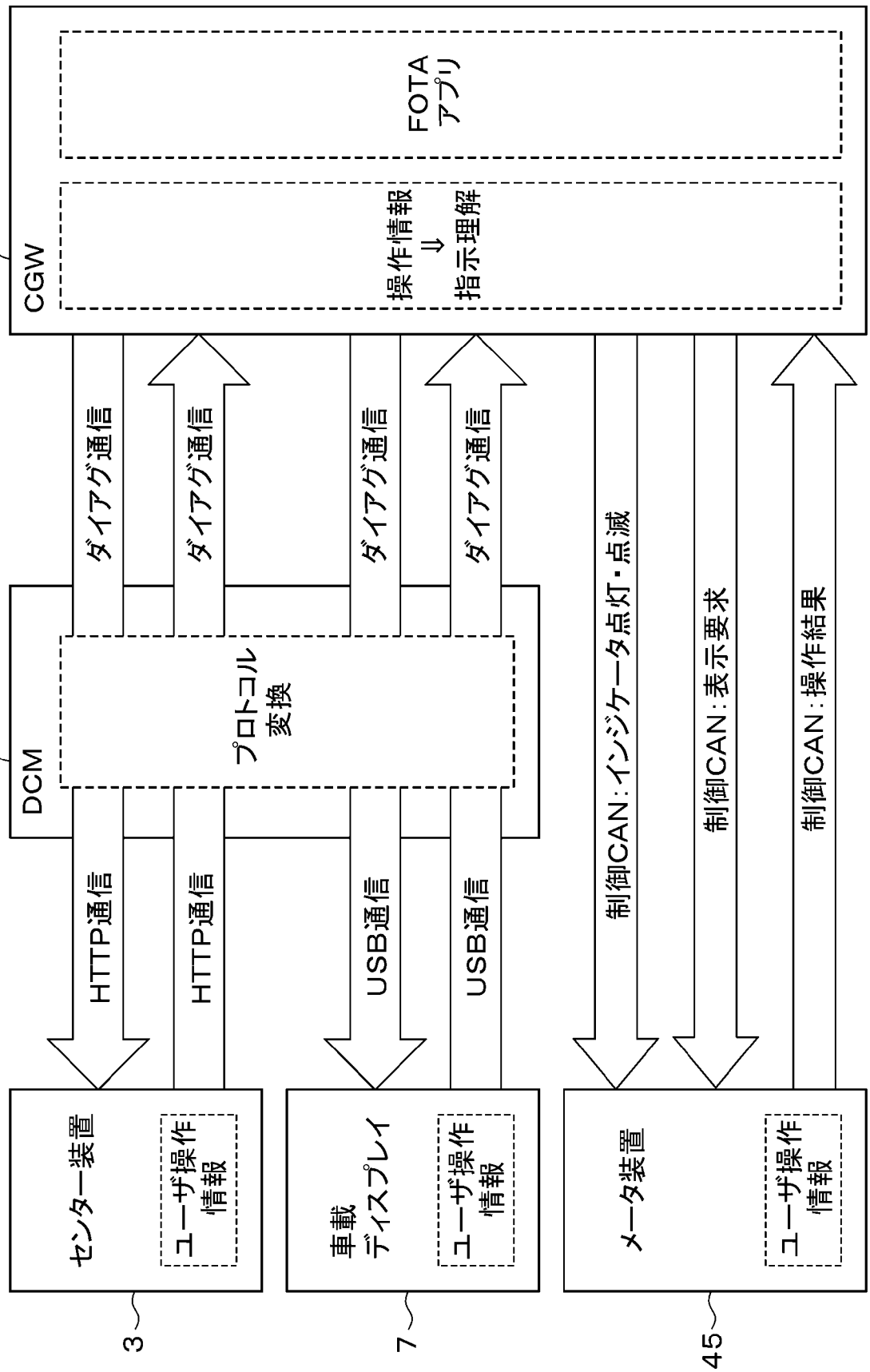
[図197]

Fig. 197



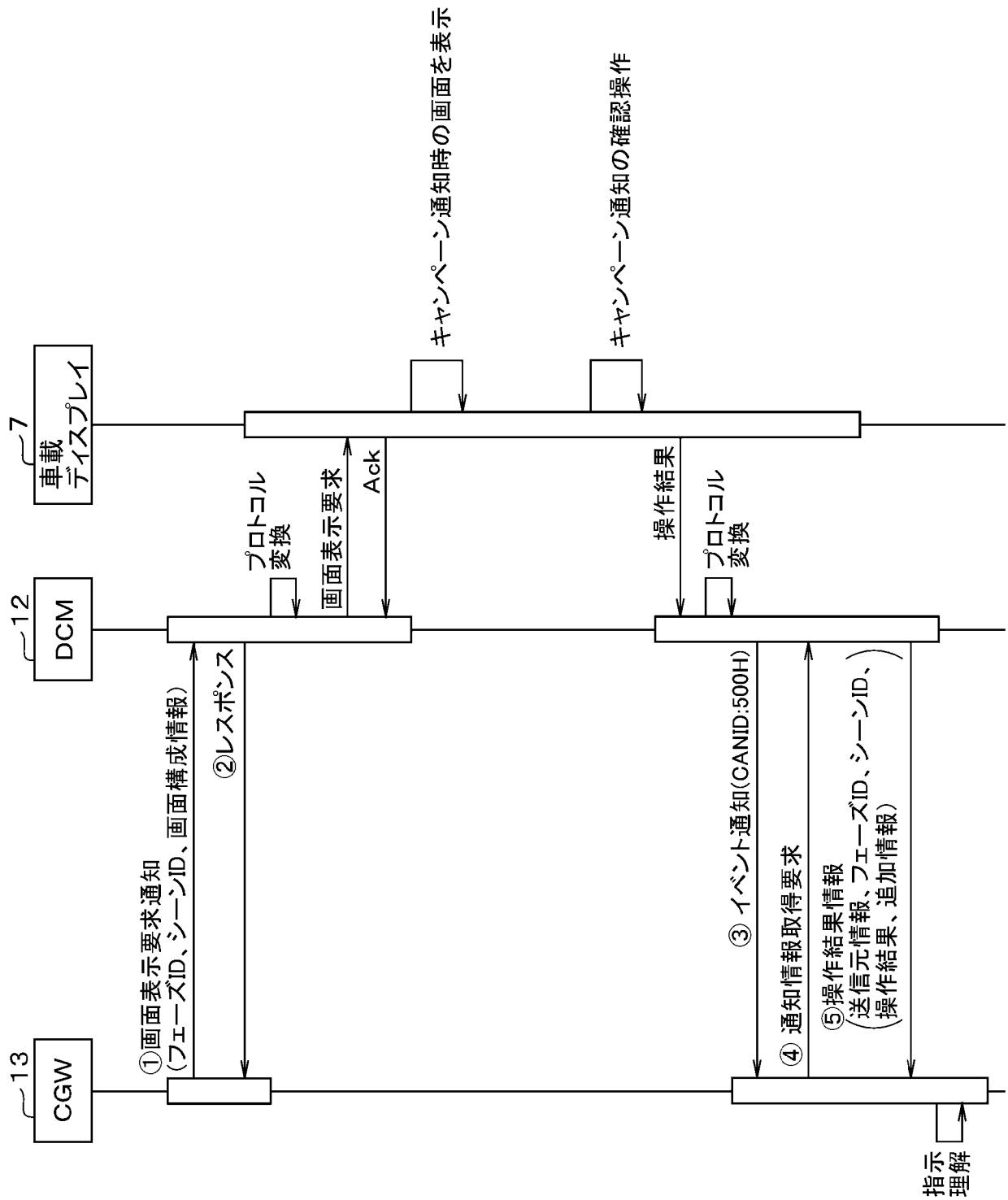
[図198]

Fig. 198


13
CGW
操作情報
⇓
指示理解
FOTA
アプリ
12
DCM
プロトコル
変換
ダイアグ通信
ダイアグ通信
ダイアグ通信
ダイアグ通信
HTTP通信
HTTP通信
USB通信
USB通信
制御CAN:インジケータ点灯・点滅
制御CAN:表示要求
制御CAN:操作結果
センター装置
ユーザ操作
情報
車載
ディスプレイ
ユーザ操作
情報
メータ装置
ユーザ操作
情報
3
7
45

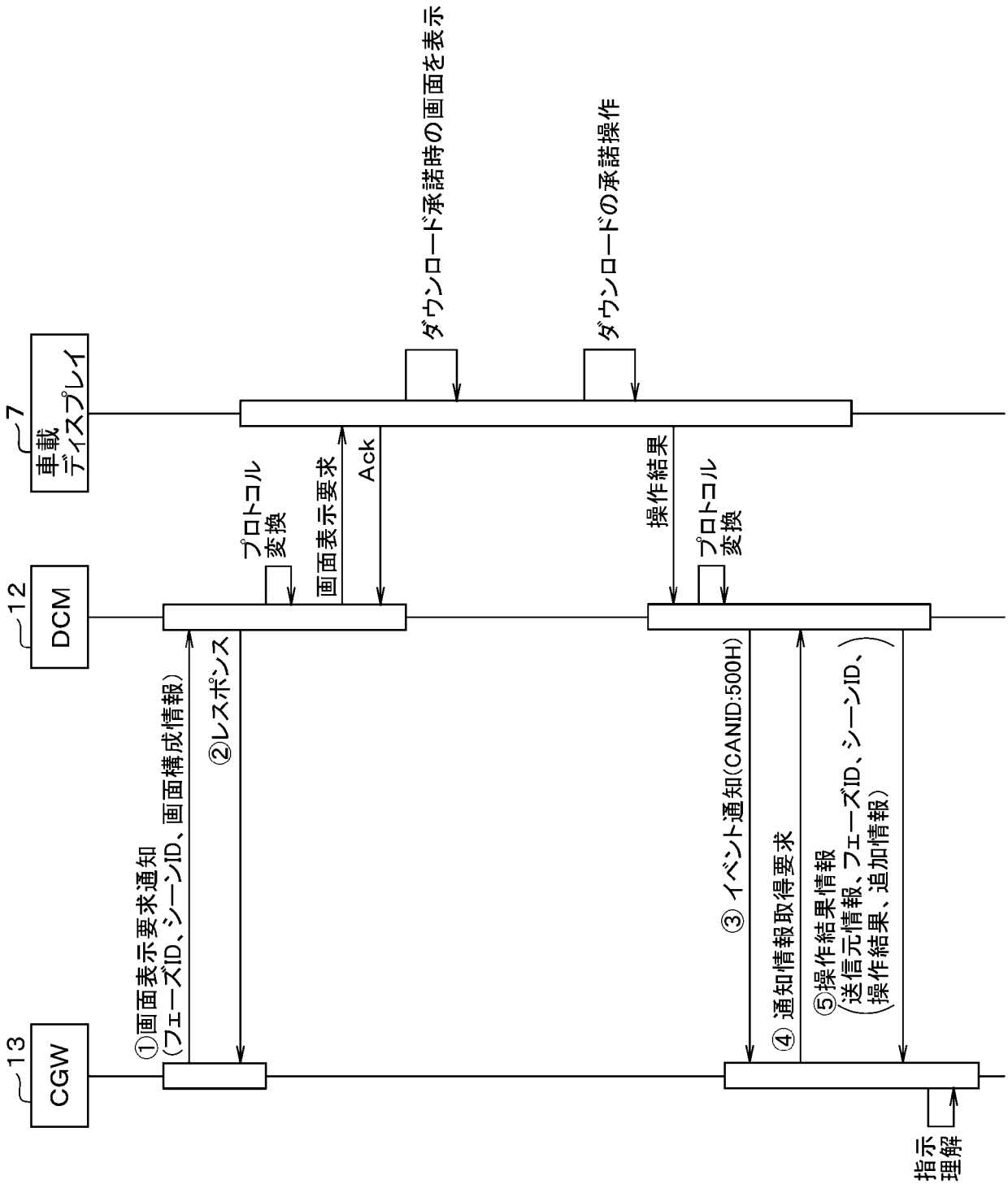
[図199]

Fig. 199


13
CGW
12
DCM
7
車載
ディスプレイ
①画面表示要求通知
(フェーズID、シーンID、画面構成情報)
②レスポンス
プロトコル
変換
画面表示要求
Ack
キャンペーン通知時の画面を表示
キャンペーン通知の確認操作
操作結果
プロトコル
変換
③ イベント通知(CANID:500H)
④ 通知情報取得要求
⑤操作結果情報
(送信元情報、フェーズID、シーンID、
操作結果、追加情報)
指示
理解

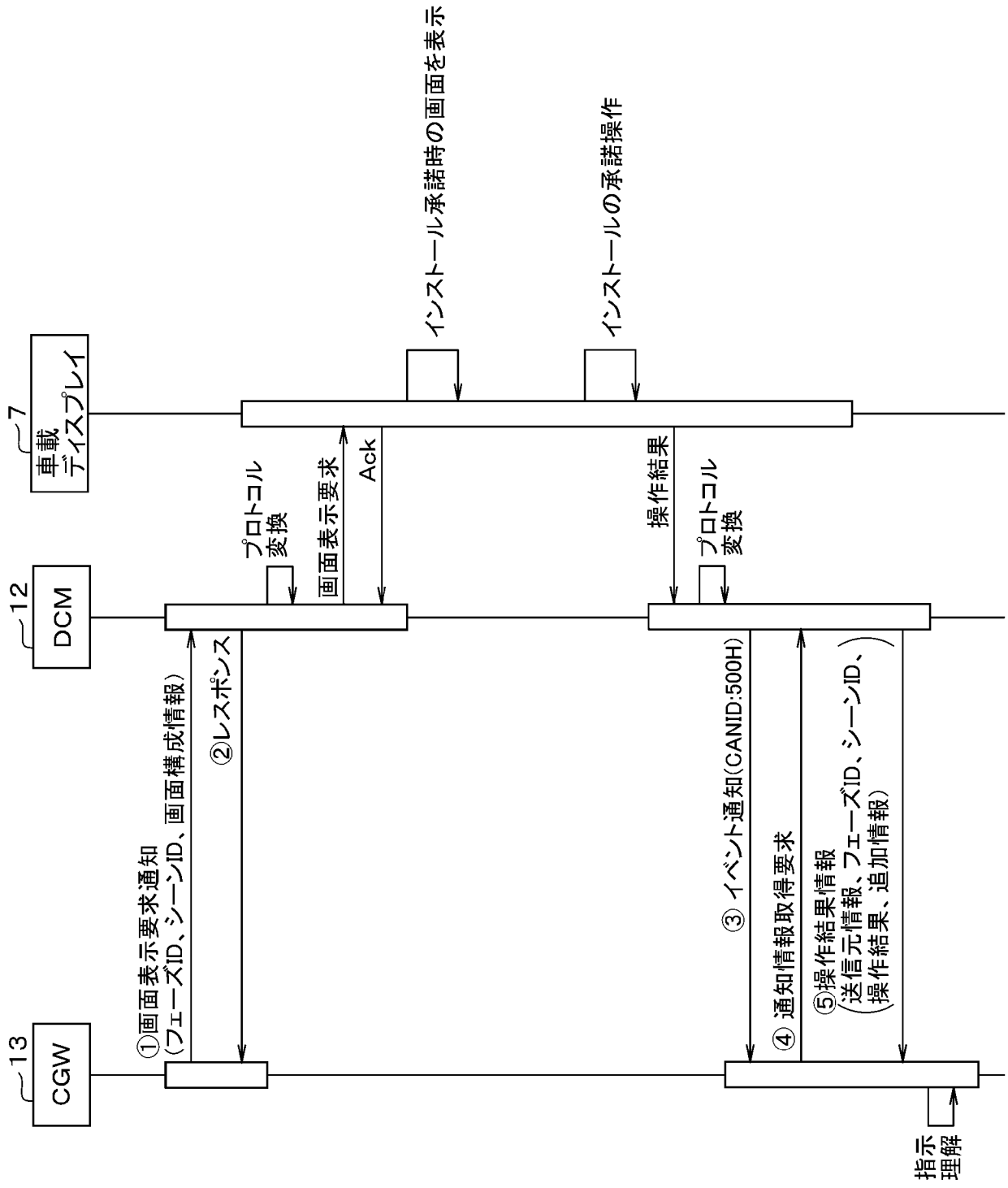
[図200]

Fig. 200


7
車載
ディスプレイ
12
DCM
13
CGW
ダウンロード承諾時の画面を表示
ダウンロードの承諾操作
プロトコル
変換
画面表示要求
Ack
操作結果
プロトコル
変換
①画面表示要求通知
(フェーズID、シーンID、画面構成情報)
②レスポンス
③ イベント通知(CANID:500H)
④ 通知情報取得要求
⑤操作結果情報
(送信元情報、フェーズID、シーンID、
操作結果、追加情報)
指示
理解

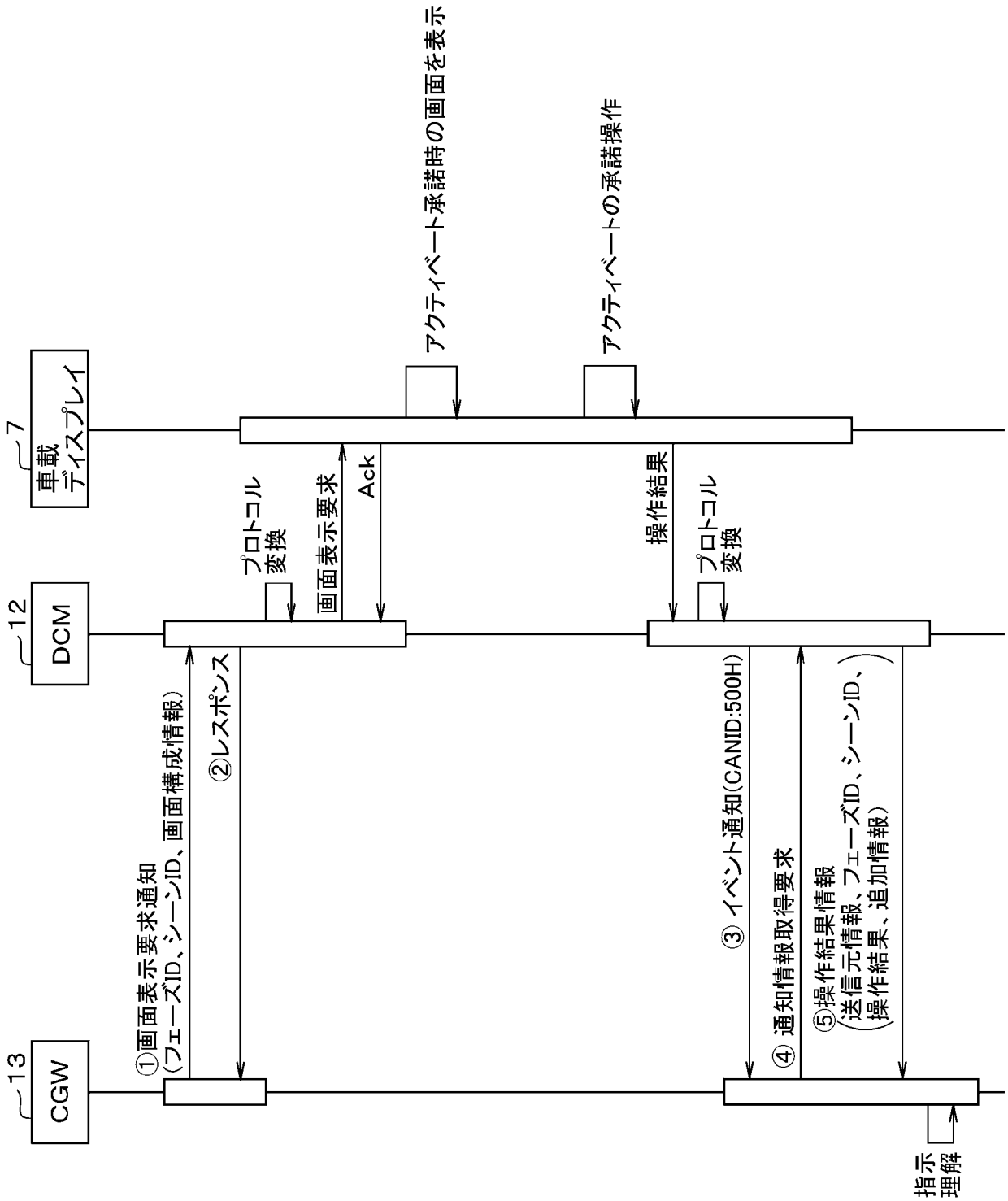
[図201]

Fig. 201


7
車載
ディスプレイ
12
DCM
13
CGW
インストール承諾時の画面を表示
インストールの承諾操作
プロトコル
変換
画面表示要求
Ack
操作結果
プロトコル
変換
①画面表示要求通知
(フェーズID、シーンID、画面構成情報)
②レスポンス
③ イベント通知(CANID:500H)
④ 通知情報取得要求
⑤操作結果情報
(送信元情報、フェーズID、シーンID、
操作結果、追加情報)
指示
理解

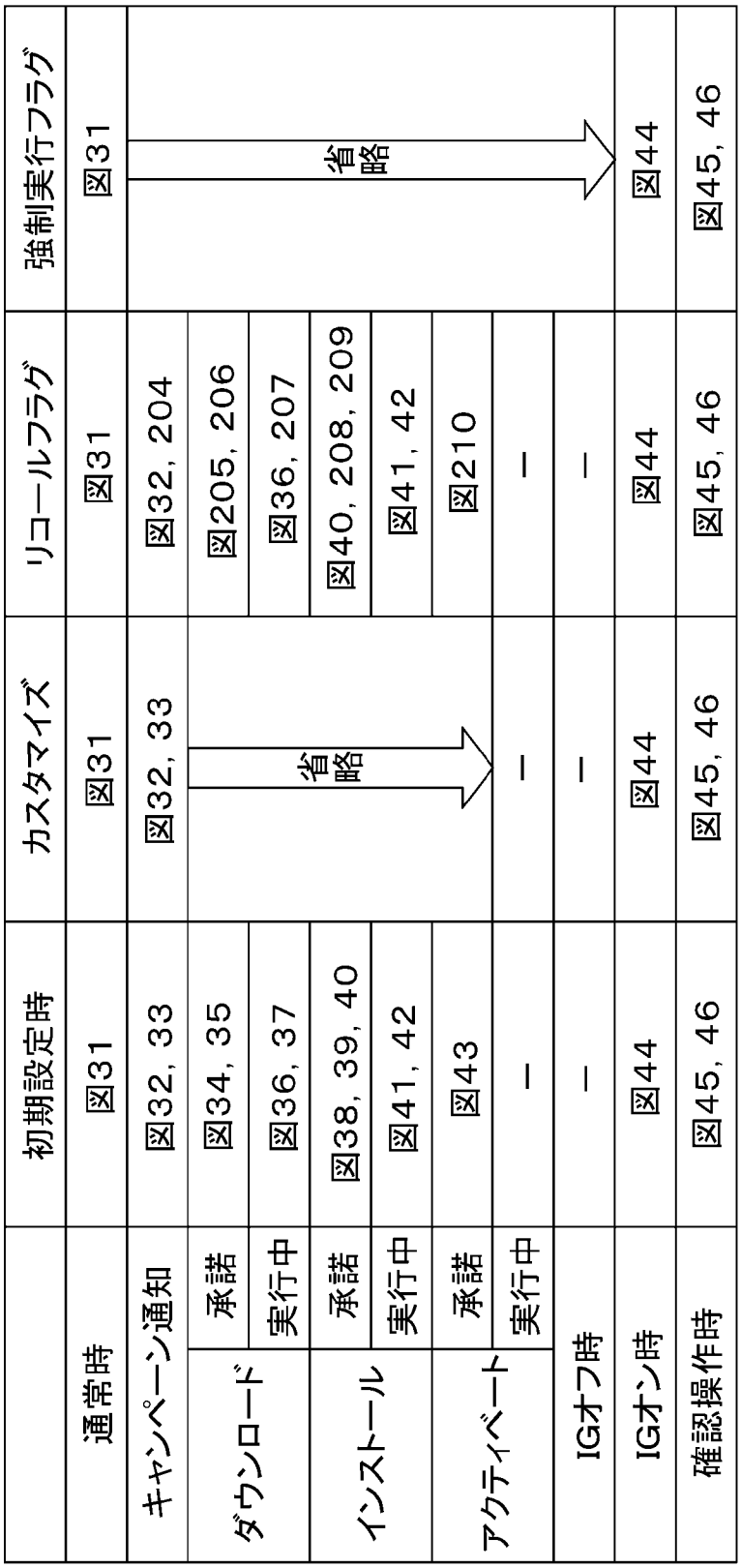
[図202]

Fig. 202


13
CGW
12
DCM
7
車載
ディスプレイ
①画面表示要求通知
(フェーズID、シーンID、画面構成情報)
②レスポンス
プロトコル
変換
画面表示要求
Ack
アクティベート承諾時の画面を表示
操作結果
プロトコル
変換
アクティベートの承諾操作
③ イベント通知(CANID:500H)
④ 通知情報取得要求
⑤操作結果情報
(送信元情報、フェーズID、シーンID、
操作結果、追加情報)
指示
理解

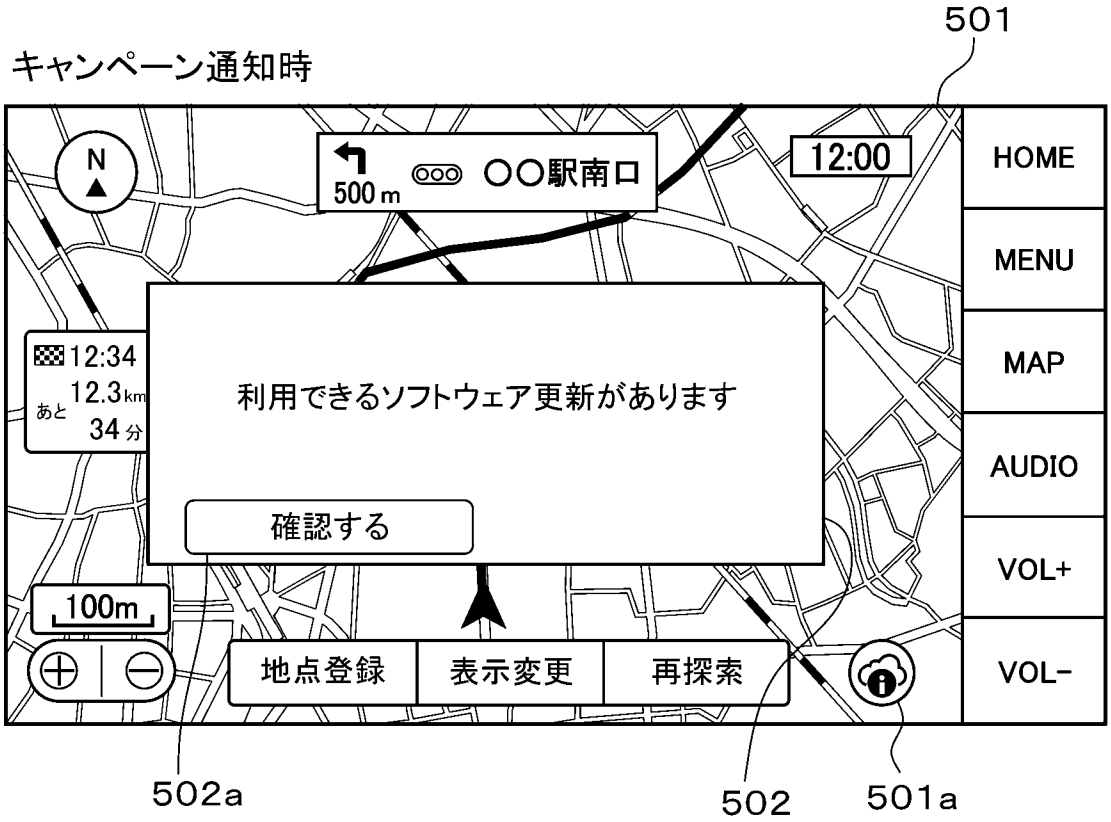
[図203]

Fig. 203


初期設定時
カスタマイズ
リコールフラグ
強制実行フラグ
通常時
図31
図31
図31
図31
キャンペーン通知
図32, 33
図32, 33
図32, 204
ダウンロード
承諾
図34, 35
省略
図205, 206
実行中
図36, 37
図36, 207
インストール
承諾
図38, 39, 40
図40, 208, 209
実行中
図41, 42
図41, 42
アクティベート
承諾
図43
図210
実行中
－
－
－
IGオフ時
－
－
－
IGオン時
図44
図44
図44
図44
確認操作時
図45, 46
図45, 46
図45, 46
図45, 46
省略

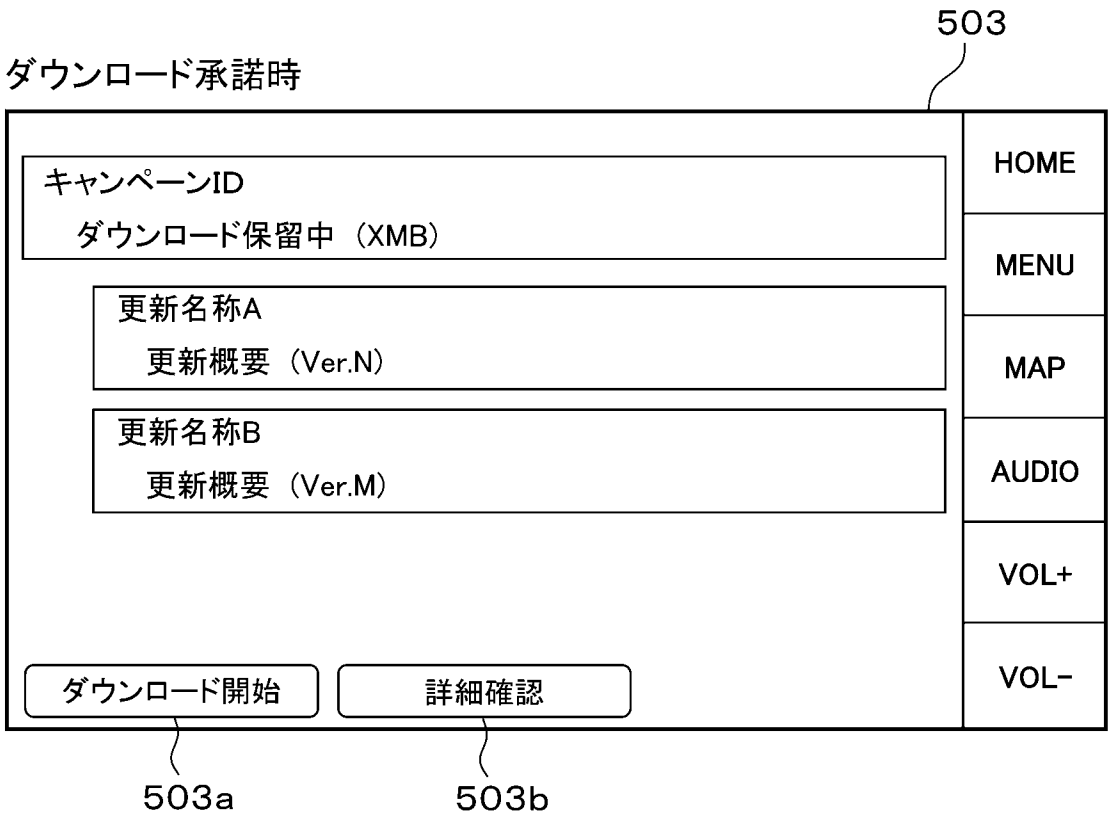
[図204]

Fig. 204


501
キャンペーン通知時
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34
あと 12.3km
34 分
利用できるソフトウェア更新があります
確認する
100m
地点登録
表示変更
再探索
502a
502
501a

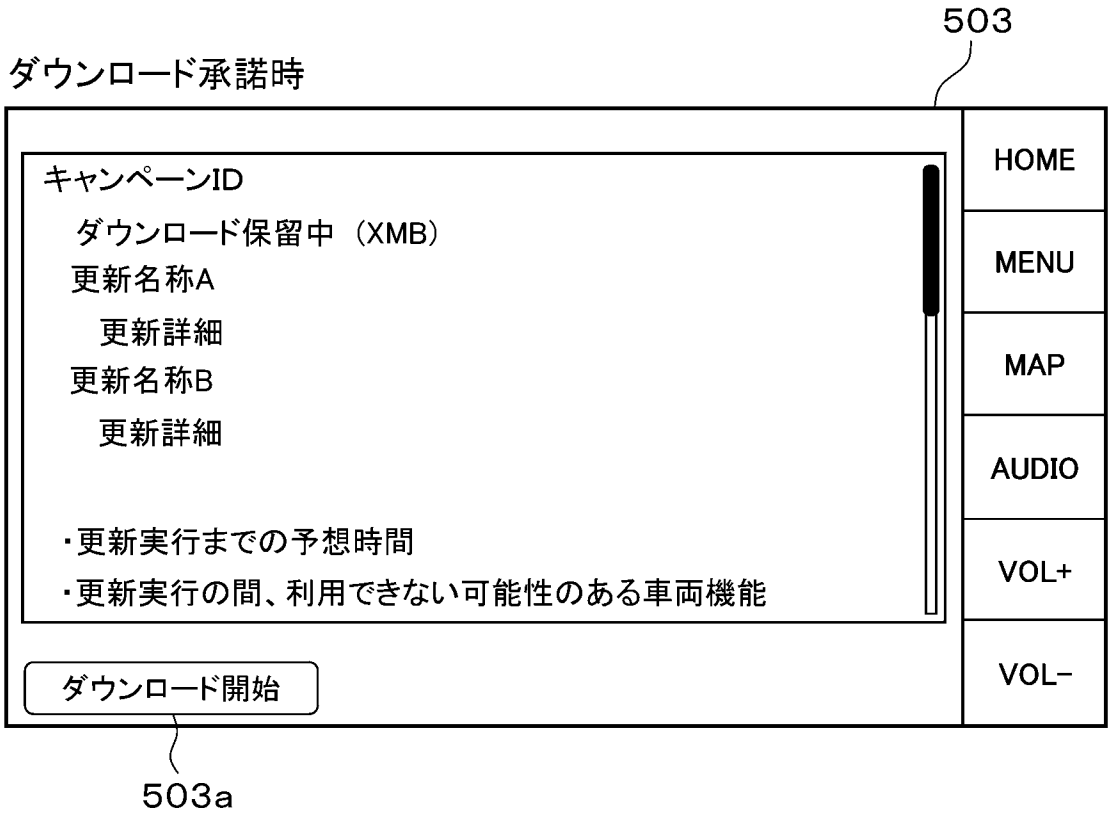
[図205]

Fig. 205


503
ダウンロード承諾時
キャンペーンID
ダウンロード保留中（XMB）
更新名称A
更新概要（Ver.N）
更新名称B
更新概要（Ver.M）
HOME
MENU
MAP
AUDIO
VOL+
VOL-
ダウンロード開始
詳細確認
503a
503b

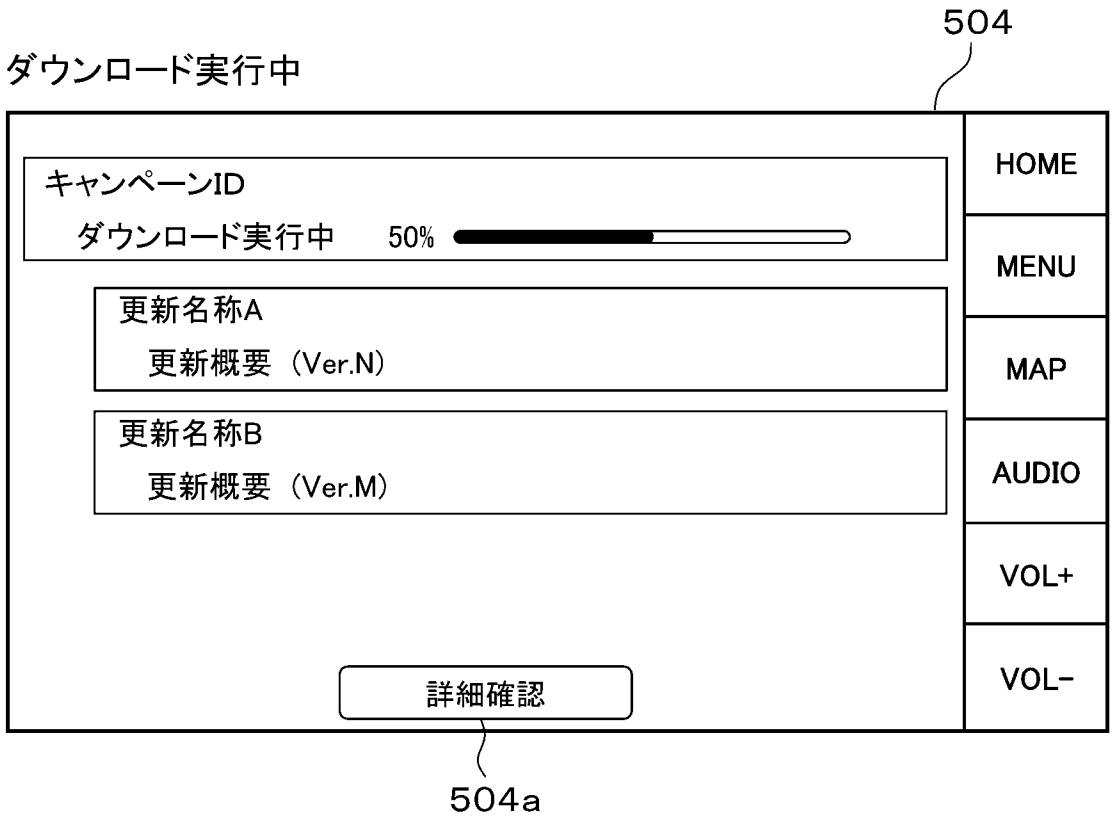
[図206]

Fig. 206


503
ダウンロード承諾時
キャンペーンID
ダウンロード保留中（XMB）
更新名称A
更新詳細
更新名称B
更新詳細
・更新実行までの予想時間
・更新実行の間、利用できない可能性のある車両機能
ダウンロード開始
503a
HOME
MENU
MAP
AUDIO
VOL+
VOL−

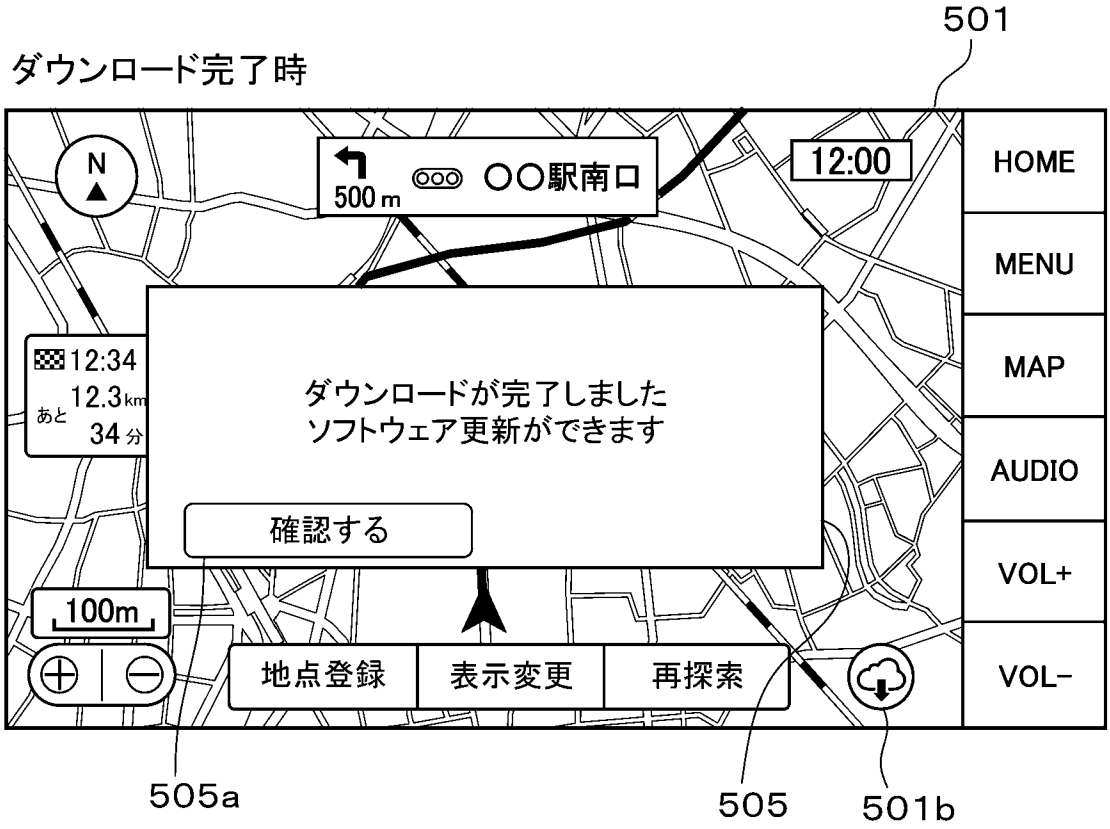
[図207]

Fig. 207


504
ダウンロード実行中
キャンペーンID
ダウンロード実行中 50%
更新名称A
更新概要 (Ver.N)
更新名称B
更新概要 (Ver.M)
詳細確認
504a
HOME
MENU
MAP
AUDIO
VOL+
VOL-

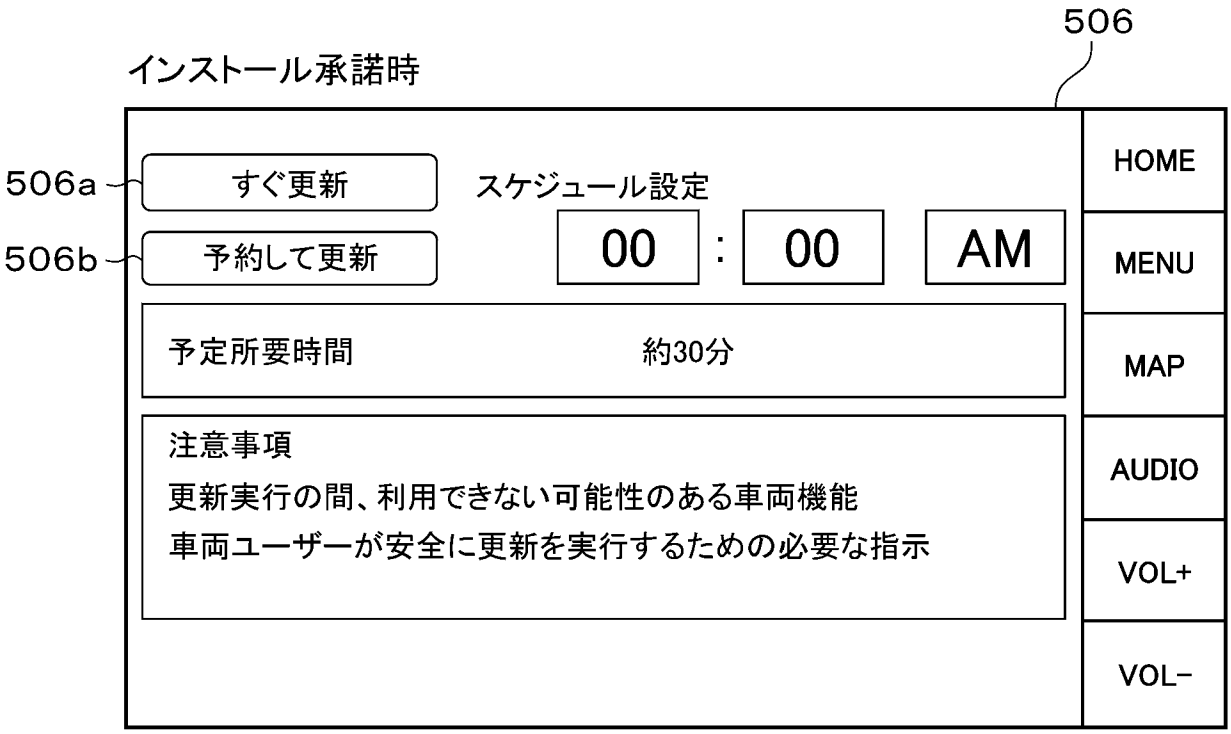
[図208]

Fig. 208


501
ダウンロード完了時
N
500 m
〇〇駅南口
12:00
HOME
MENU
MAP
AUDIO
VOL+
VOL−
12:34
あと 12.3km
34 分
ダウンロードが完了しました
ソフトウェア更新ができます
確認する
100m
地点登録
表示変更
再探索
505a
505
501b

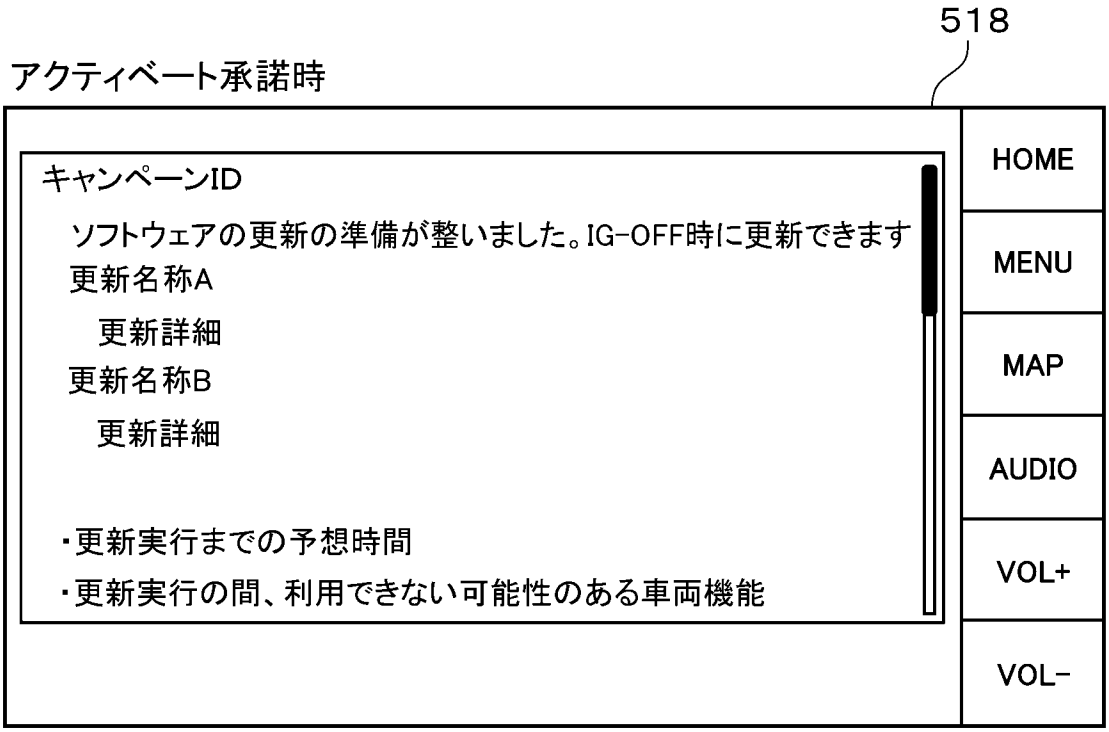
[図209]

Fig. 209


506
インストール承諾時
506a
すぐ更新
スケジュール設定
506b
予約して更新
00
:
00
AM
予定所要時間
約30分
注意事項
更新実行の間、利用できない可能性のある車両機能
車両ユーザーが安全に更新を実行するための必要な指示
HOME
MENU
MAP
AUDIO
VOL+
VOL−

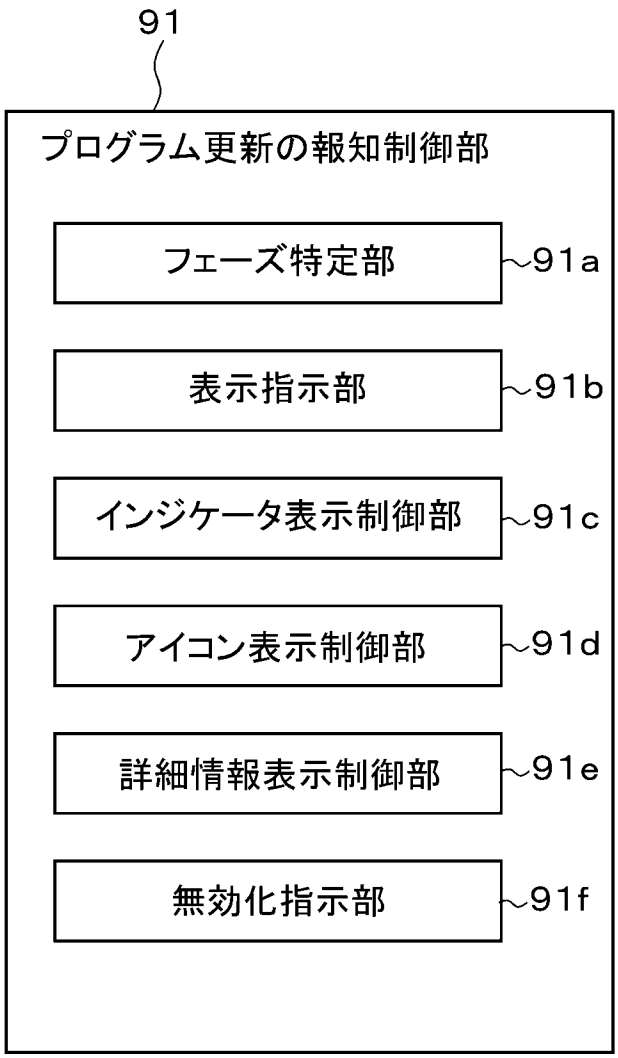
[図210]

Fig. 210


518
アクティベート承諾時
キャンペーンID
ソフトウェアの更新の準備が整いました。IG-OFF時に更新できます
更新名称A
更新詳細
更新名称B
更新詳細
・更新実行までの予想時間
・更新実行の間、利用できない可能性のある車両機能
HOME
MENU
MAP
AUDIO
VOL+
VOL-

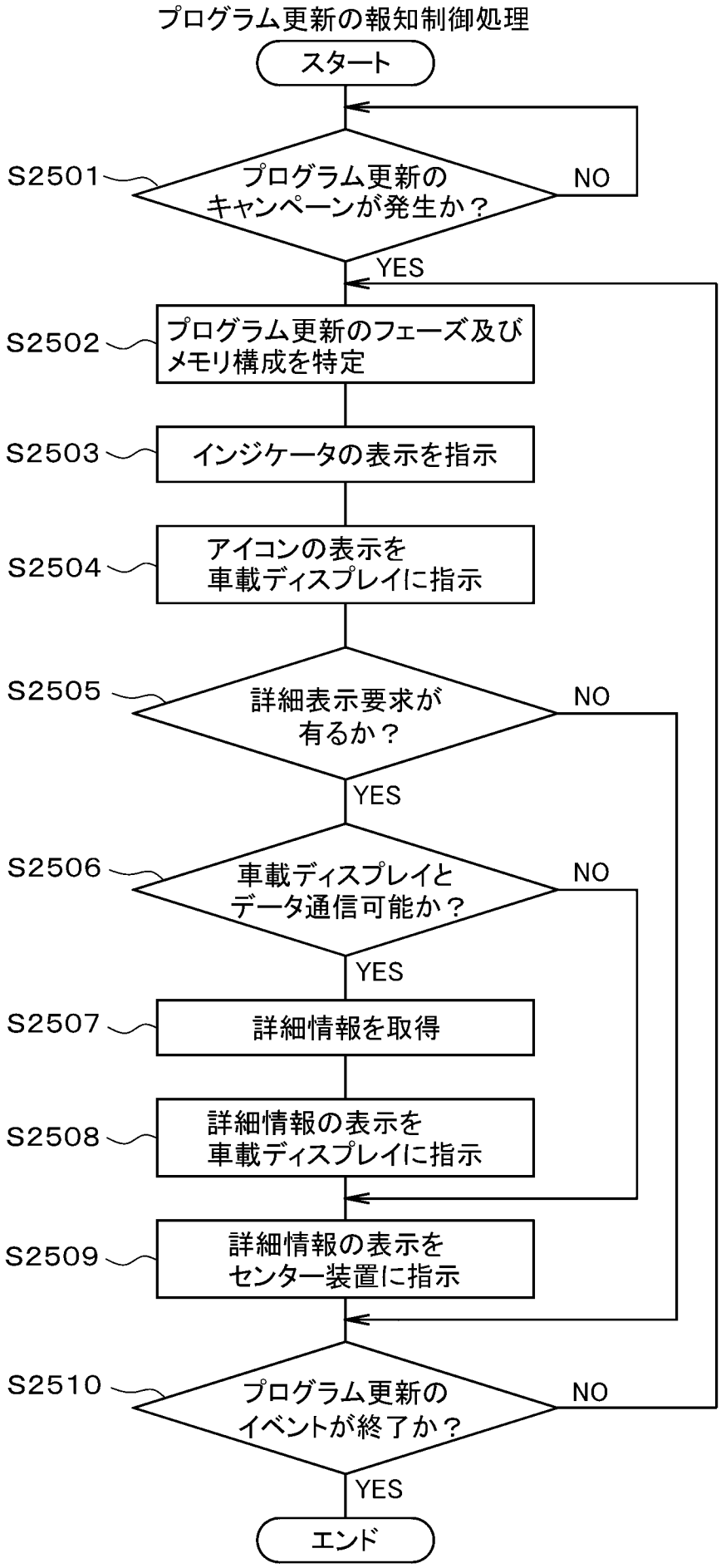
[図211]

Fig. 211


91
プログラム更新の報知制御部
フェーズ特定部
91a
表示指示部
91b
インジケータ表示制御部
91c
アイコン表示制御部
91d
詳細情報表示制御部
91e
無効化指示部
91f

[図212]

Fig. 212


プログラム更新の報知制御処理
スタート
S2501
プログラム更新の
キャンペーンが発生か？
NO
YES
S2502
プログラム更新のフェーズ及び
メモリ構成を特定
S2503
インジケータの表示を指示
S2504
アイコンの表示を
車載ディスプレイに指示
S2505
詳細表示要求が
有るか？
NO
YES
S2506
車載ディスプレイと
データ通信可能か？
NO
YES
S2507
詳細情報を取得
S2508
詳細情報の表示を
車載ディスプレイに指示
S2509
詳細情報の表示を
センター装置に指示
S2510
プログラム更新の
イベントが終了か？
NO
YES
エンド

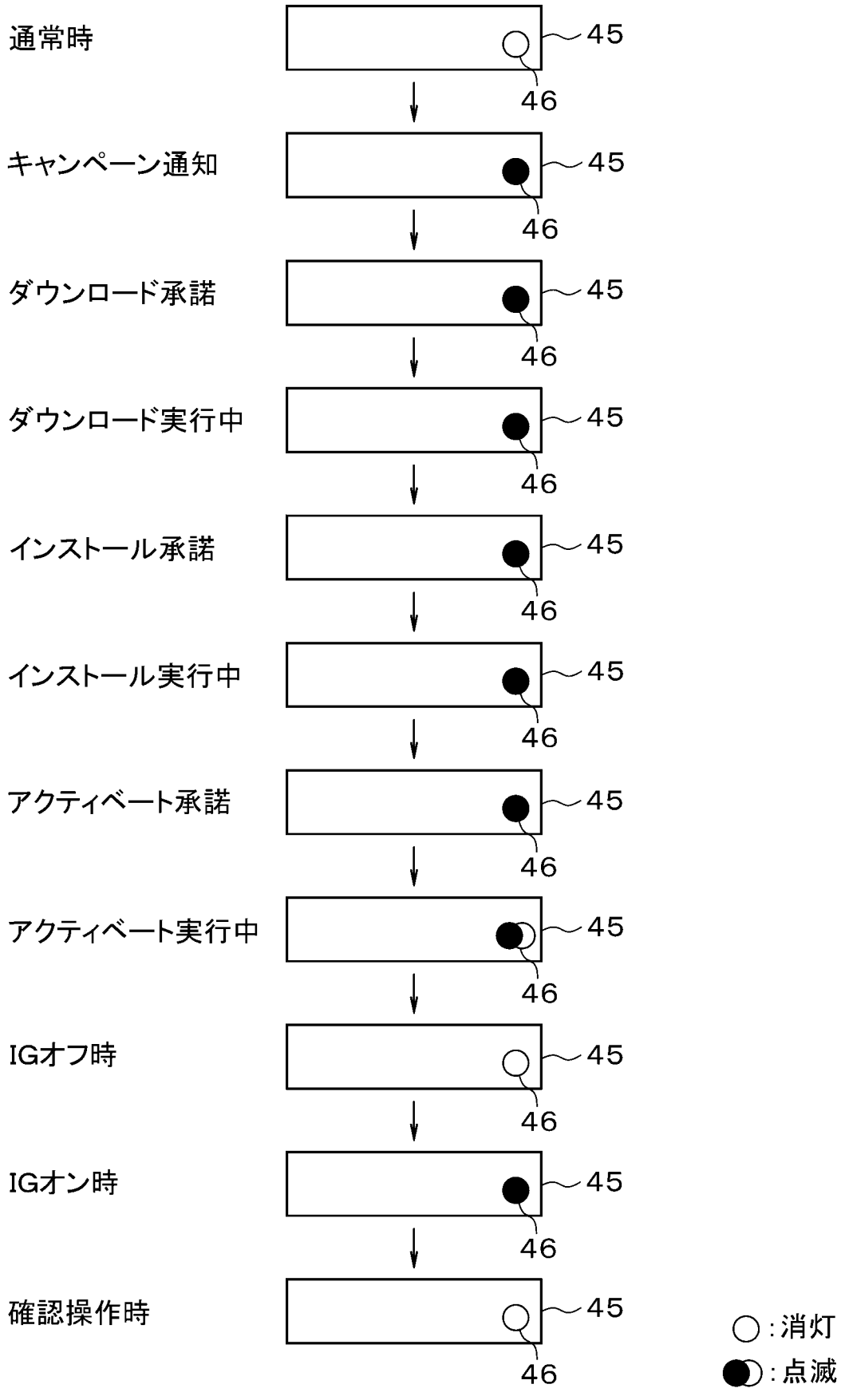
[図213]

Fig. 213

		メータ装置		車載ディスプレイ
		2面メモリ	1面サスペンドメモリ	1面単独メモリ	
通常時		消灯	消灯	消灯	図31
キャンペーン通知		点灯	点灯	点灯	図32，33
ダウンロード	承諾	点灯	点灯	点灯	図34，35
	実行中	点灯	点灯	点灯	図36，37
インストール	承諾	点灯	点灯	点灯	図38，39，40
	実行中	点灯	点灯（IGオン）・点滅（IGオフ）	点滅	図41，42
アクティベート	承諾	点灯	点滅	点滅	図43
	実行中	点滅	点滅	点滅	
IGオフ時		消灯	消灯	消灯	
IGオン時		点灯	点灯	点灯	図44
確認操作時		消灯	消灯	消灯	図45，46

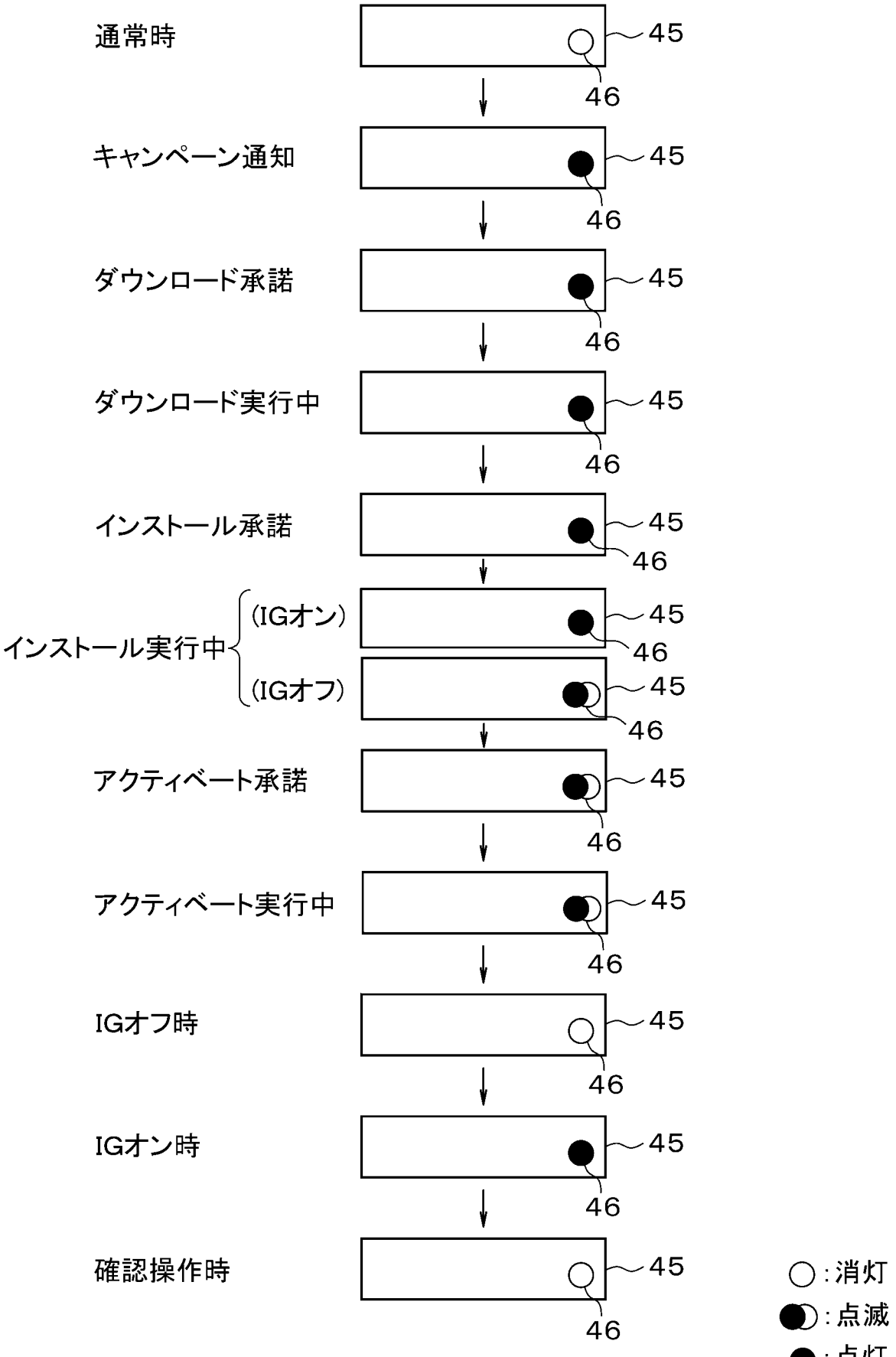
[図214]

Fig. 214


通常時
キャンペーン通知
ダウンロード承諾
ダウンロード実行中
インストール承諾
インストール実行中
アクティベート承諾
アクティベート実行中
IGオフ時
IGオン時
確認操作時
45
46
○：消灯
●○：点滅
●：点灯

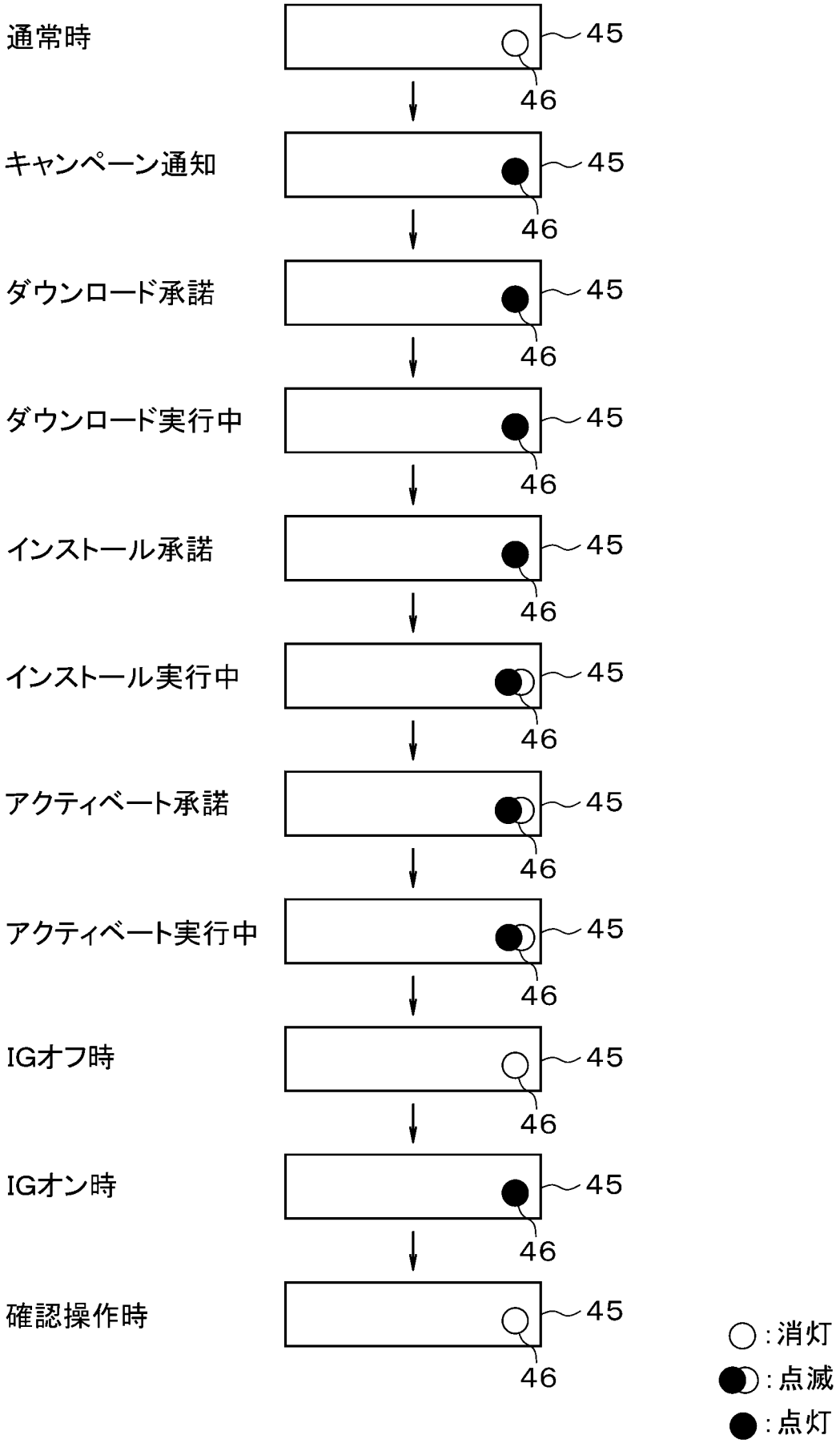
[図215]

Fig. 215


通常時
キャンペーン通知
ダウンロード承諾
ダウンロード実行中
インストール承諾
インストール実行中
(IGオン)
(IGオフ)
アクティベート承諾
アクティベート実行中
IGオフ時
IGオン時
確認操作時
45
46
○:消灯
:点滅
●:点灯

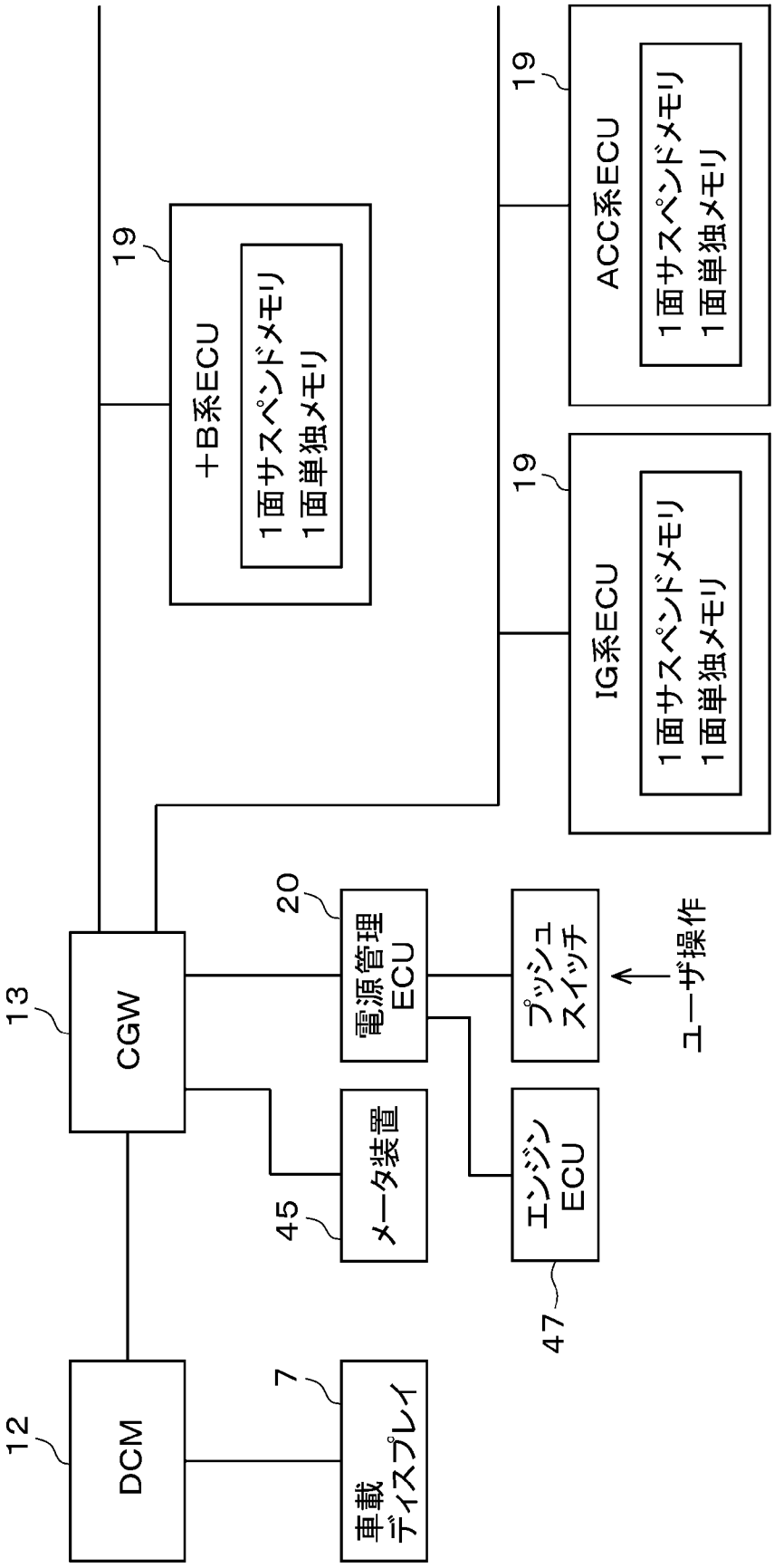
[図216]

Fig. 216


通常時
キャンペーン通知
ダウンロード承諾
ダウンロード実行中
インストール承諾
インストール実行中
アクティベート承諾
アクティベート実行中
IGオフ時
IGオン時
確認操作時
45
46
○：消灯
●○：点滅
●：点灯

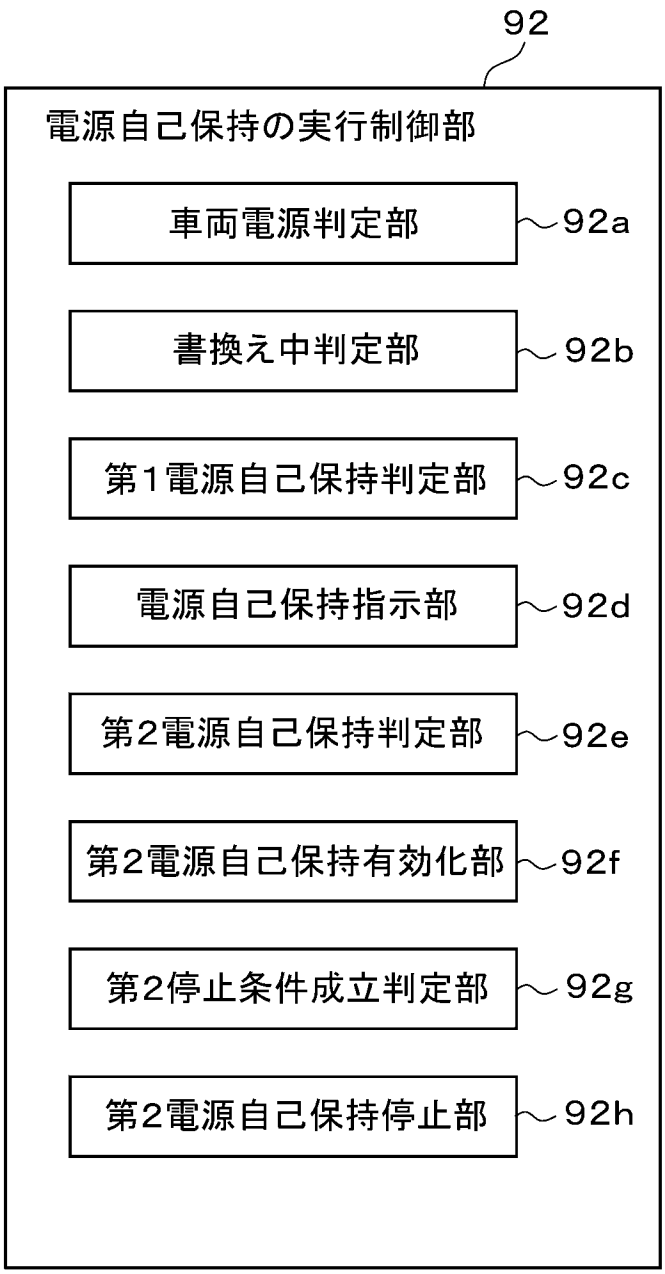
[図217]

Fig. 217


12
DCM
7
車載
ディスプレイ
13
CGW
45
メータ装置
20
電源管理
ECU
47
エンジン
ECU
プッシュ
スイッチ
ユーザ操作
19
＋B系ECU
1面サスペンドメモリ
1面単独メモリ
19
IG系ECU
1面サスペンドメモリ
1面単独メモリ
19
ACC系ECU
1面サスペンドメモリ
1面単独メモリ

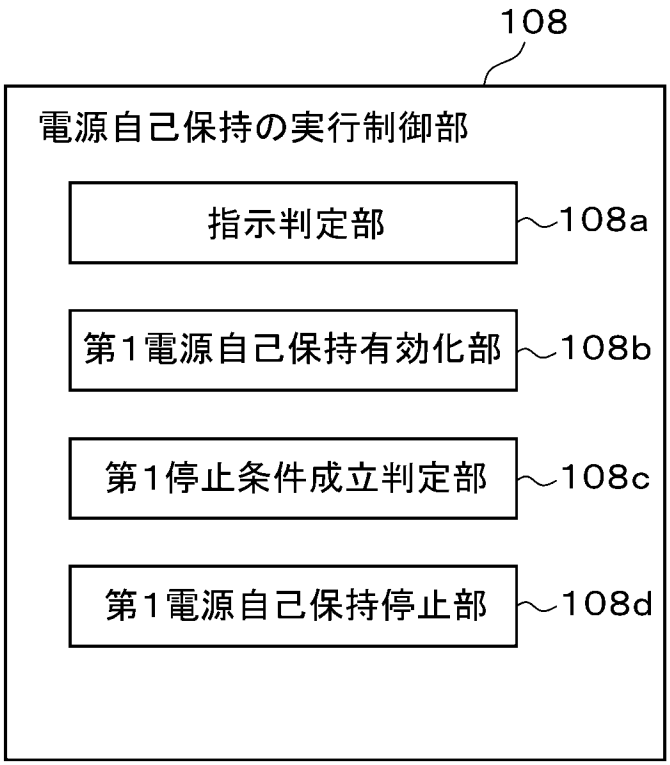
[図218]

Fig. 218


92
電源自己保持の実行制御部
車両電源判定部
92a
書換え中判定部
92b
第1電源自己保持判定部
92c
電源自己保持指示部
92d
第2電源自己保持判定部
92e
第2電源自己保持有効化部
92f
第2停止条件成立判定部
92g
第2電源自己保持停止部
92h

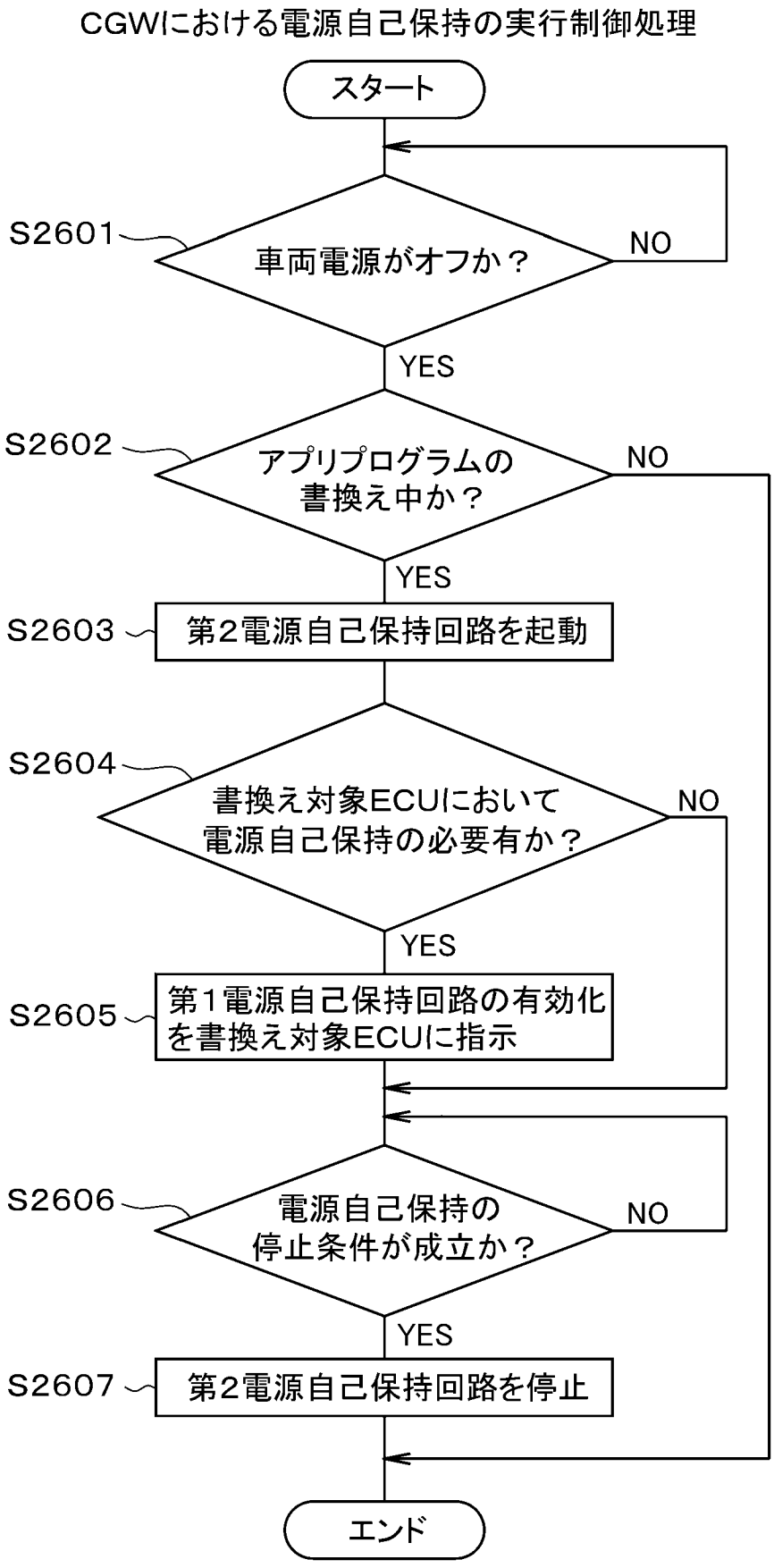
[図219]

Fig. 219


108
電源自己保持の実行制御部
指示判定部
108a
第1電源自己保持有効化部
108b
第1停止条件成立判定部
108c
第1電源自己保持停止部
108d

[図220]

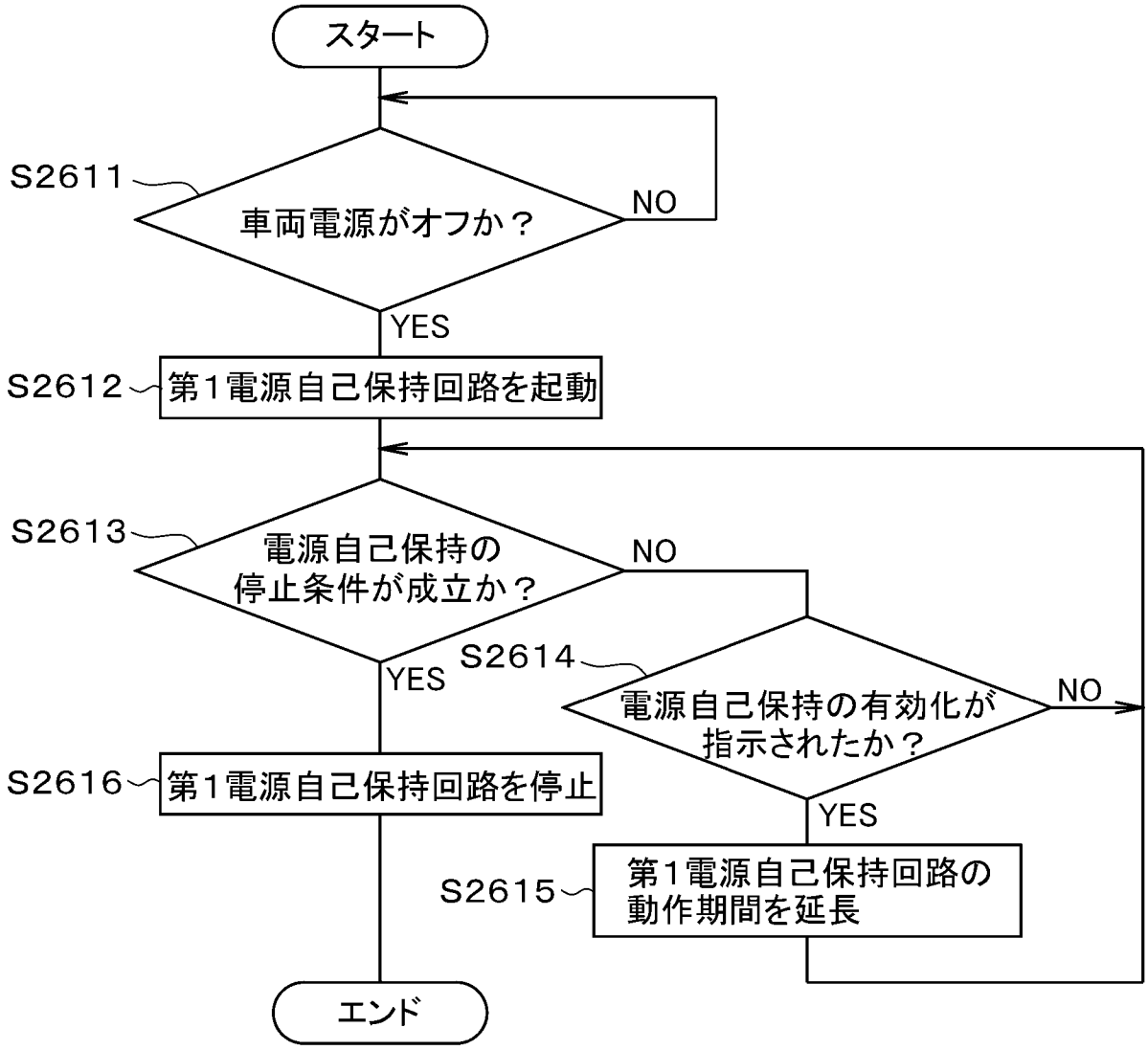
Fig. 220


CGWにおける電源自己保持の実行制御処理
スタート
S2601
車両電源がオフか？
NO
YES
S2602
アプリプログラムの
書換え中か？
NO
YES
S2603
第2電源自己保持回路を起動
S2604
書換え対象ECUにおいて
電源自己保持の必要有か？
NO
YES
S2605
第1電源自己保持回路の有効化
を書換え対象ECUに指示
S2606
電源自己保持の
停止条件が成立か？
NO
YES
S2607
第2電源自己保持回路を停止
エンド

[図221]

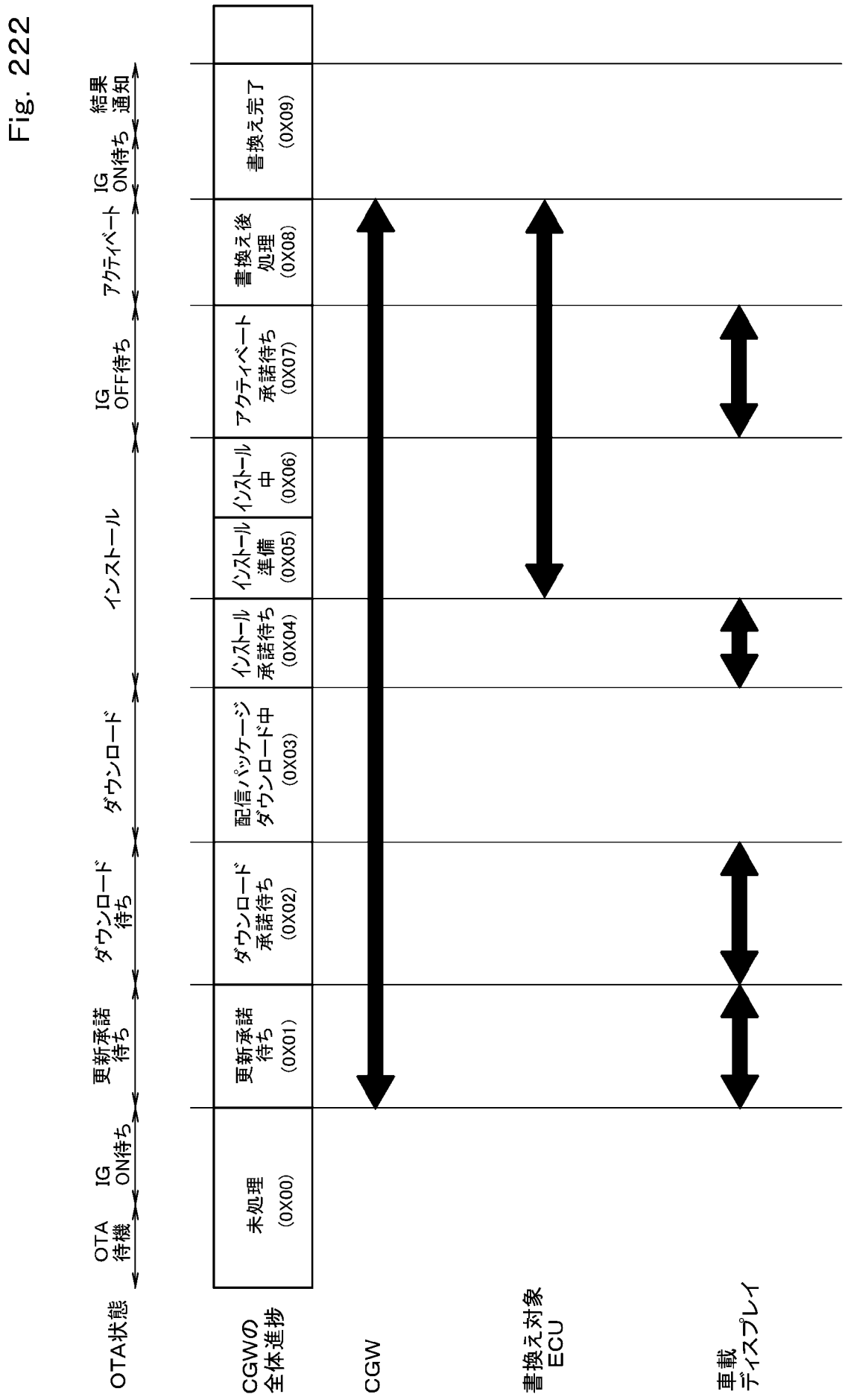
Fig. 221

書換え対象ECUにおける電源自己保持の実行制御処理



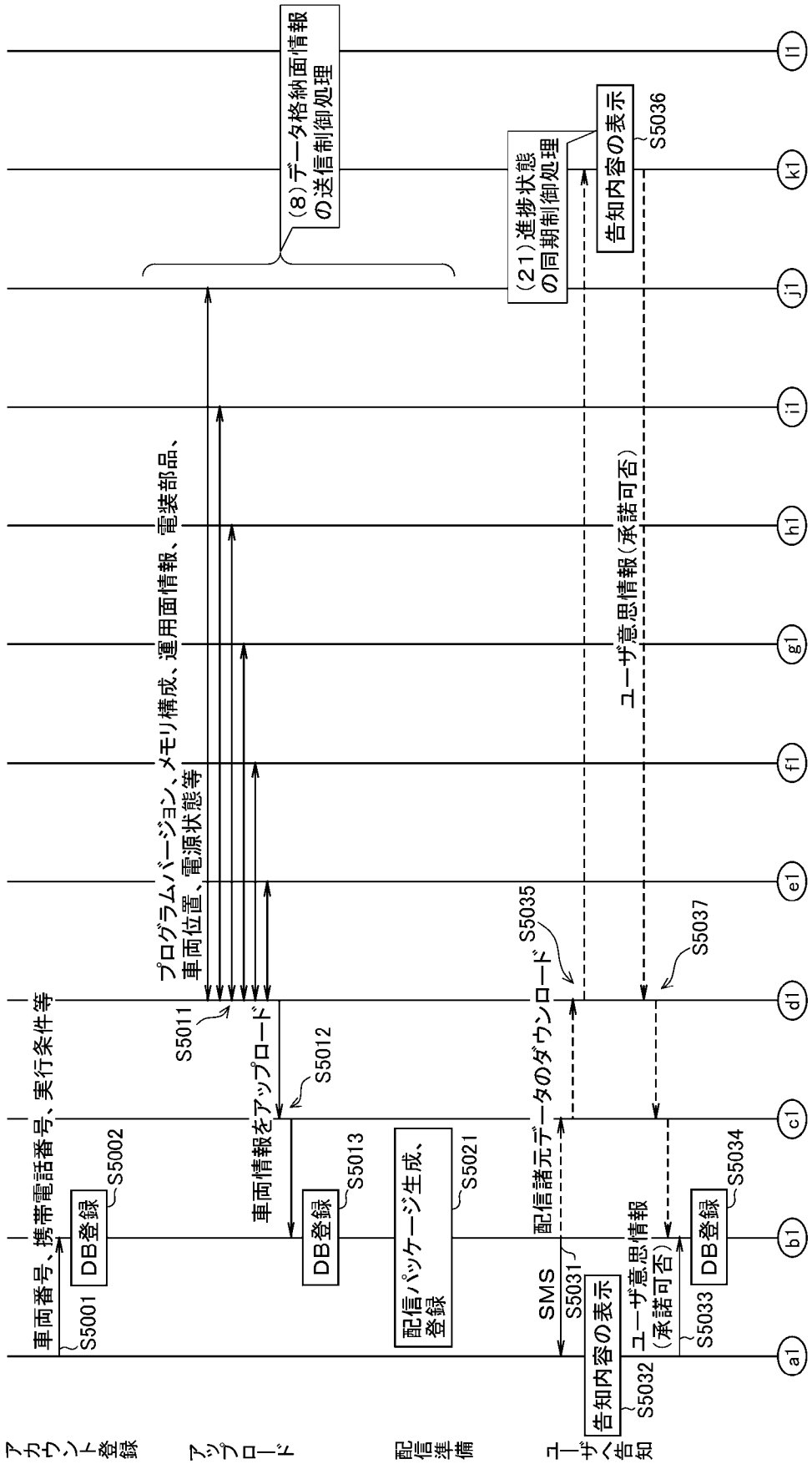
[図222]

Fig. 222


OTA状態
CGWの全体進捗
CGW
書換え対象ECU
車載ディスプレイ
OTA待機
IG ON待ち
更新承諾待ち
ダウンロード待ち
ダウンロード
インストール
IG OFF待ち
アクティベート
IG ON待ち
結果通知
未処理 (0X00)
更新承諾待ち (0X01)
ダウンロード承諾待ち (0X02)
配信パッケージダウンロード中 (0X03)
インストール承諾待ち (0X04)
インストール準備 (0X05)
インストール中 (0X06)
アクティベート承諾待ち (0X07)
書換え後処理 (0X08)
書換え完了 (0X09)

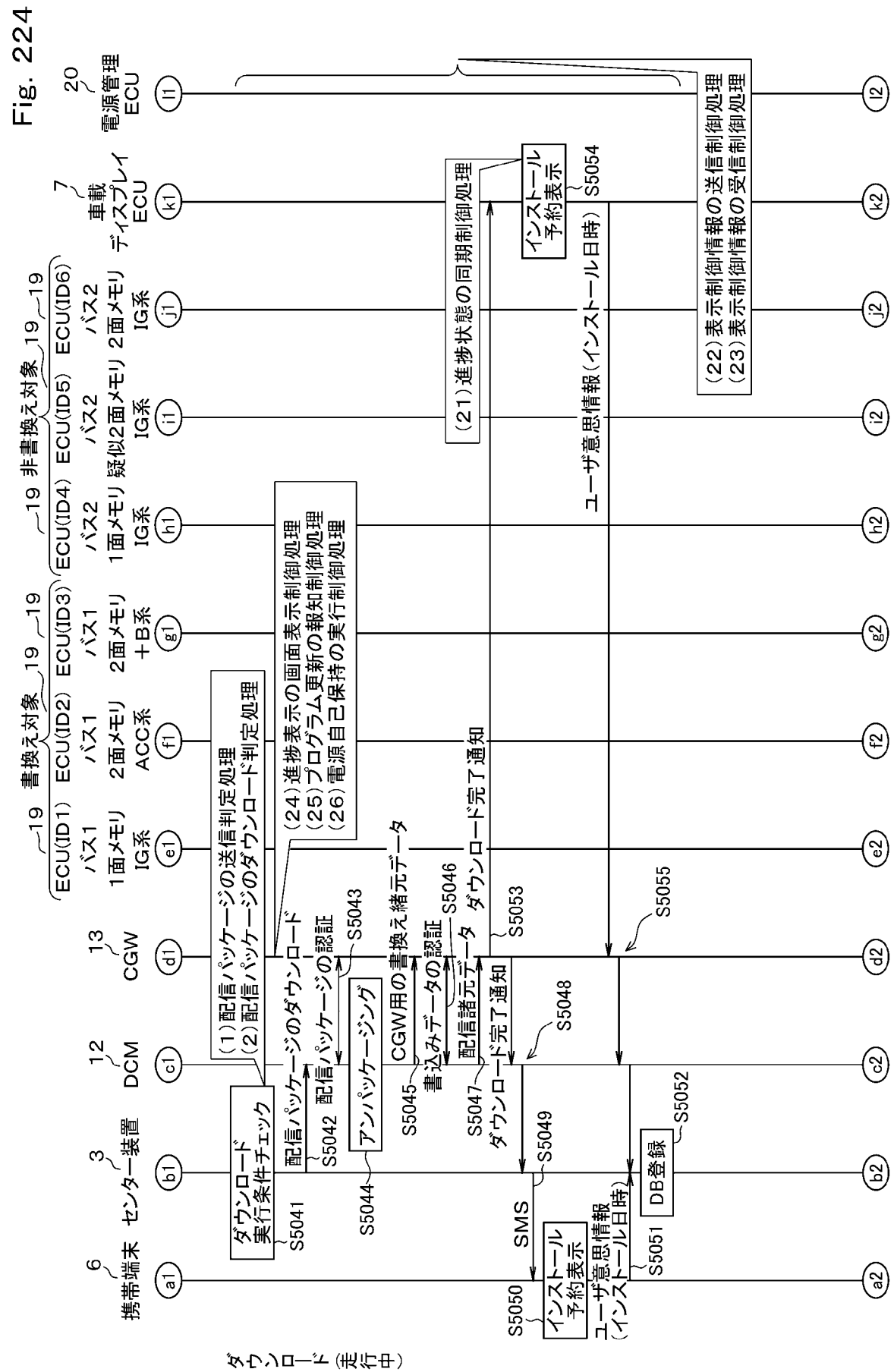
[図223]

Fig. 223


6 携帯端末
3 センター装置
12 DCM
13 CGW
19 書換え対象
19 非書換え対象
20 電源管理ECU
7 車載ディスプレイECU
ECU(ID1) バス1 1面メモリ IG系
ECU(ID2) バス1 2面メモリ ACC系
ECU(ID3) バス1 2面メモリ +B系
ECU(ID4) バス2 1面メモリ IG系
ECU(ID5) バス2 疑似2面メモリ IG系
ECU(ID6) バス2 2面メモリ IG系
車両番号、携帯電話番号、実行条件等
S5001
DB登録
S5002
プログラムバージョン、メモリ構成、運用面情報、電装部品、車両位置、電源状態等
S5011
車両情報をアップロード
S5012
DB登録
S5013
配信パッケージ生成、登録
S5021
配信諸元データのダウンロード
S5035
(8)データ格納面情報の送信制御処理
(21)進捗状態の同期制御処理
ユーザ意思情報(承諾可否)
S5037
SMS
S5031
告知内容の表示
S5032
ユーザ意思情報(承諾可否)
S5033
DB登録
S5034
告知内容の表示
S5036
アカウント登録
アップロード
配信準備
ユーザへ告知
a1
b1
c1
d1
e1
f1
g1
h1
i1
j1
k1
l1

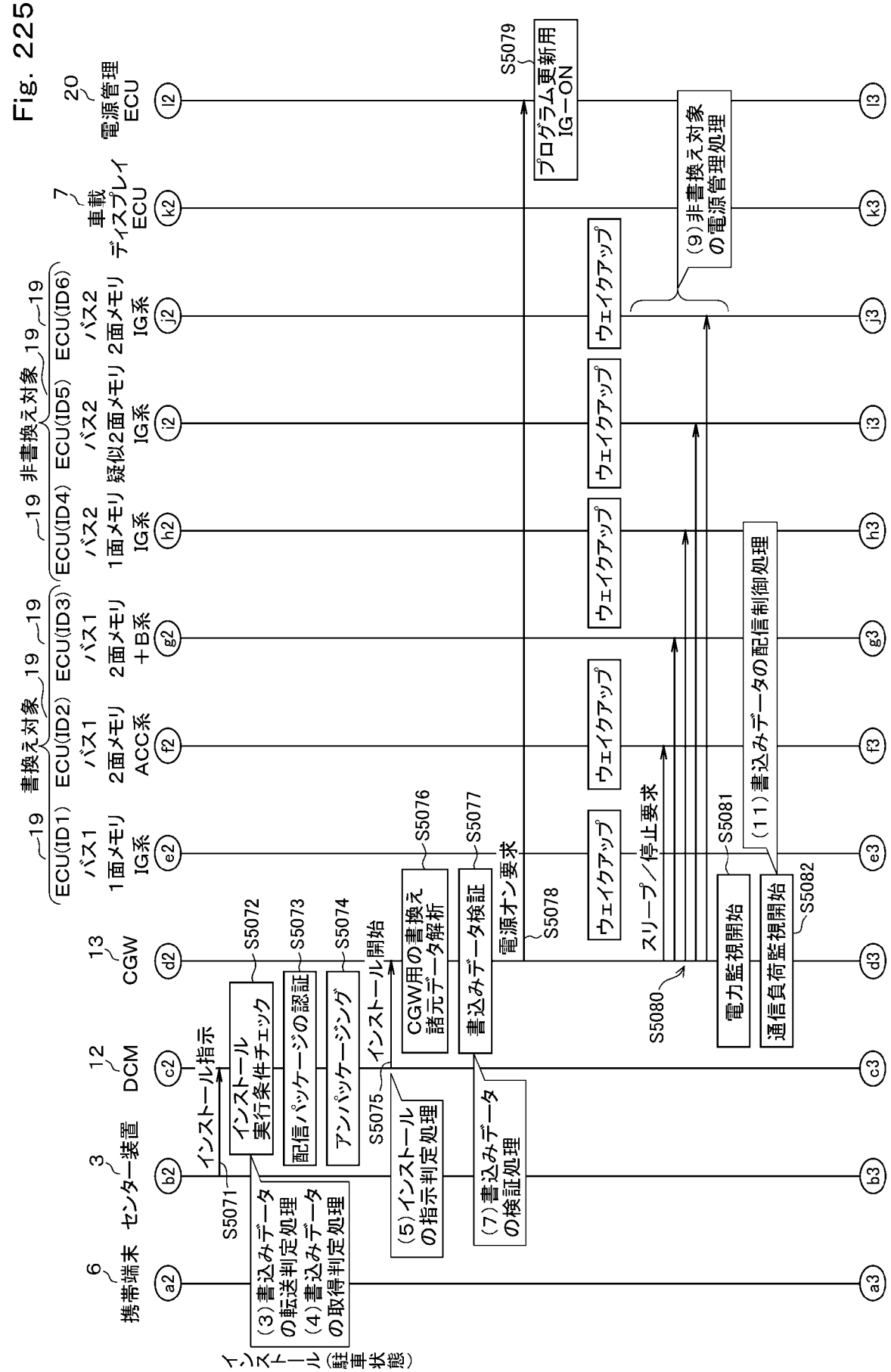
[図224]

Fig. 224


携帯端末 6
センター装置 3
DCM 12
CGW 13
書換え対象 19
非書換え対象 19
電源管理ECU 20
車載ディスプレイECU 7
ECU(ID1)
ECU(ID2)
ECU(ID3)
ECU(ID4)
ECU(ID5)
ECU(ID6)
バス1 1面メモリ IG系
バス1 2面メモリ ACC系
バス1 2面メモリ +B系
バス2 1面メモリ 疑似2面メモリ IG系
バス2 2面メモリ IG系
(1)配信パッケージの送信判定処理
(2)配信パッケージのダウンロード判定処理
(24)進捗表示の画面表示制御処理
(25)プログラム更新の報知制御処理
(26)電源自己保持の実行制御処理
(21)進捗状態の同期制御処理
(22)表示制御情報の送信制御処理
(23)表示制御情報の受信制御処理
ダウンロード実行条件チェック
S5041
配信パッケージのダウンロード
S5042
配信パッケージの認証
S5043
アンパッケージング
S5044
CGW用の書換え緒元データ
書込みデータの認証
S5045
S5046
配信諸元データ
ダウンロード完了通知
S5047
S5048
ダウンロード完了通知
S5053
S5055
SMS
S5049
S5050
インストール予約表示
ユーザ意思情報(インストール日時)
S5051
DB登録
S5052
インストール予約表示
S5054
ユーザ意思情報(インストール日時)
ダウンロード(走行中)

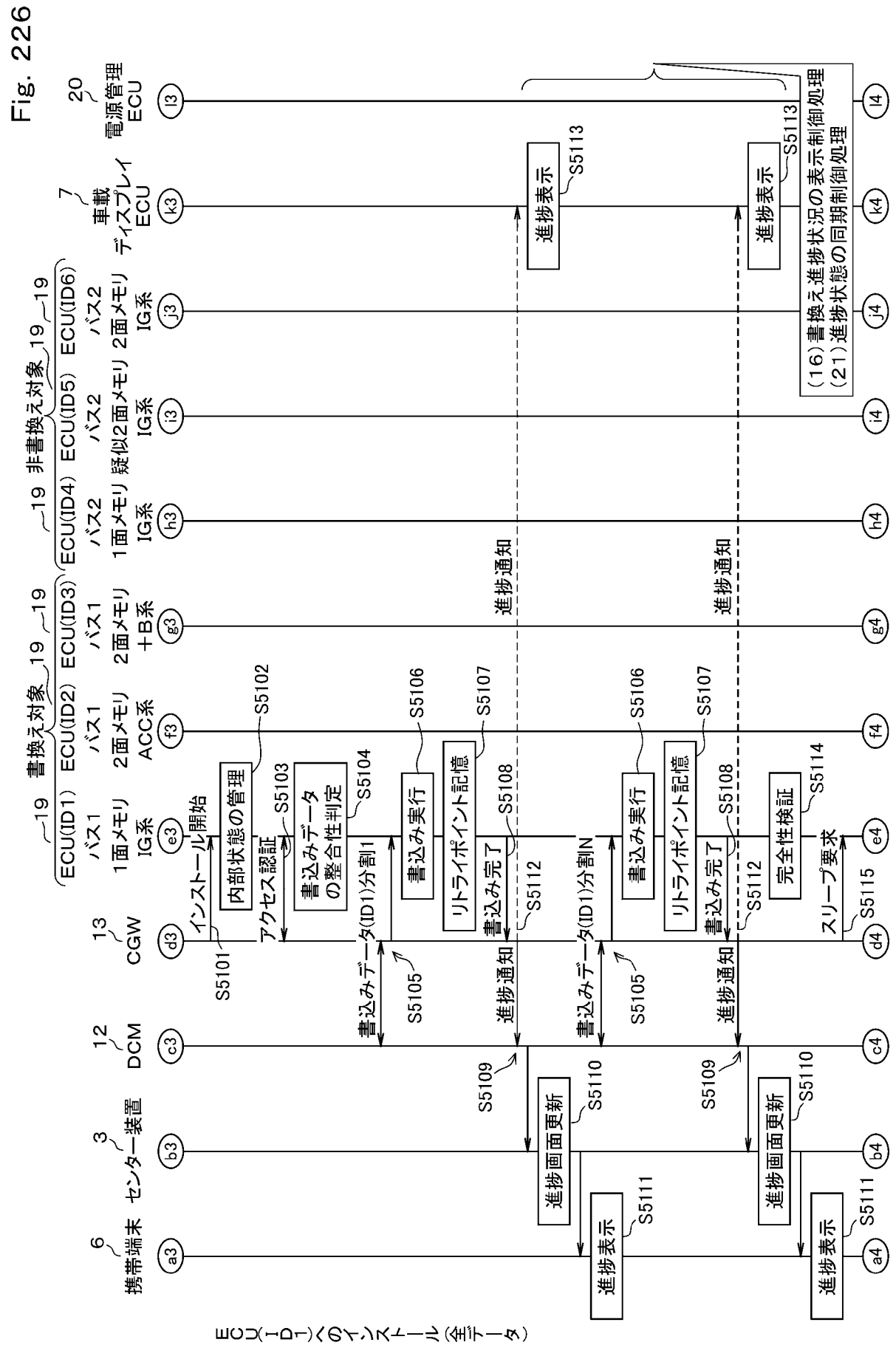
[図225]

Fig. 225


6
携帯端末
a2
3
センター装置
b2
12
DCM
c2
13
CGW
d2
19 書換え対象
ECU(ID1)
バス1
1面メモリ
IG系
e2
ECU(ID2)
バス1
2面メモリ
ACC系
f2
19
ECU(ID3)
バス1
2面メモリ
＋B系
g2
19 非書換え対象
ECU(ID4)
バス2
1面メモリ
IG系
h2
ECU(ID5)
バス2
疑似2面メモリ
IG系
i2
ECU(ID6)
バス2
2面メモリ
IG系
j2
7
車載ディスプレイ
ECU
k2
20
電源管理ECU
l2
a3
b3
c3
d3
e3
f3
g3
h3
i3
j3
k3
l3
インストール（駐車状態）
S5071
(3)書込みデータの転送判定処理
(4)書込みデータの取得判定処理
インストール指示
インストール実行条件チェック
S5072
配信パッケージの認証
S5073
アンパッケージング
S5074
インストール開始
S5075
(5)インストールの指示判定処理
CGW用の書換え諸元データ解析
S5076
書込みデータ検証
S5077
(7)書込みデータの検証処理
電源オン要求
S5078
プログラム更新用IG−ON
S5079
ウェイクアップ
スリープ／停止要求
S5080
電力監視開始
S5081
通信負荷監視開始
S5082
(11)書込みデータの配信制御処理
(9)非書換え対象の電源管理処理

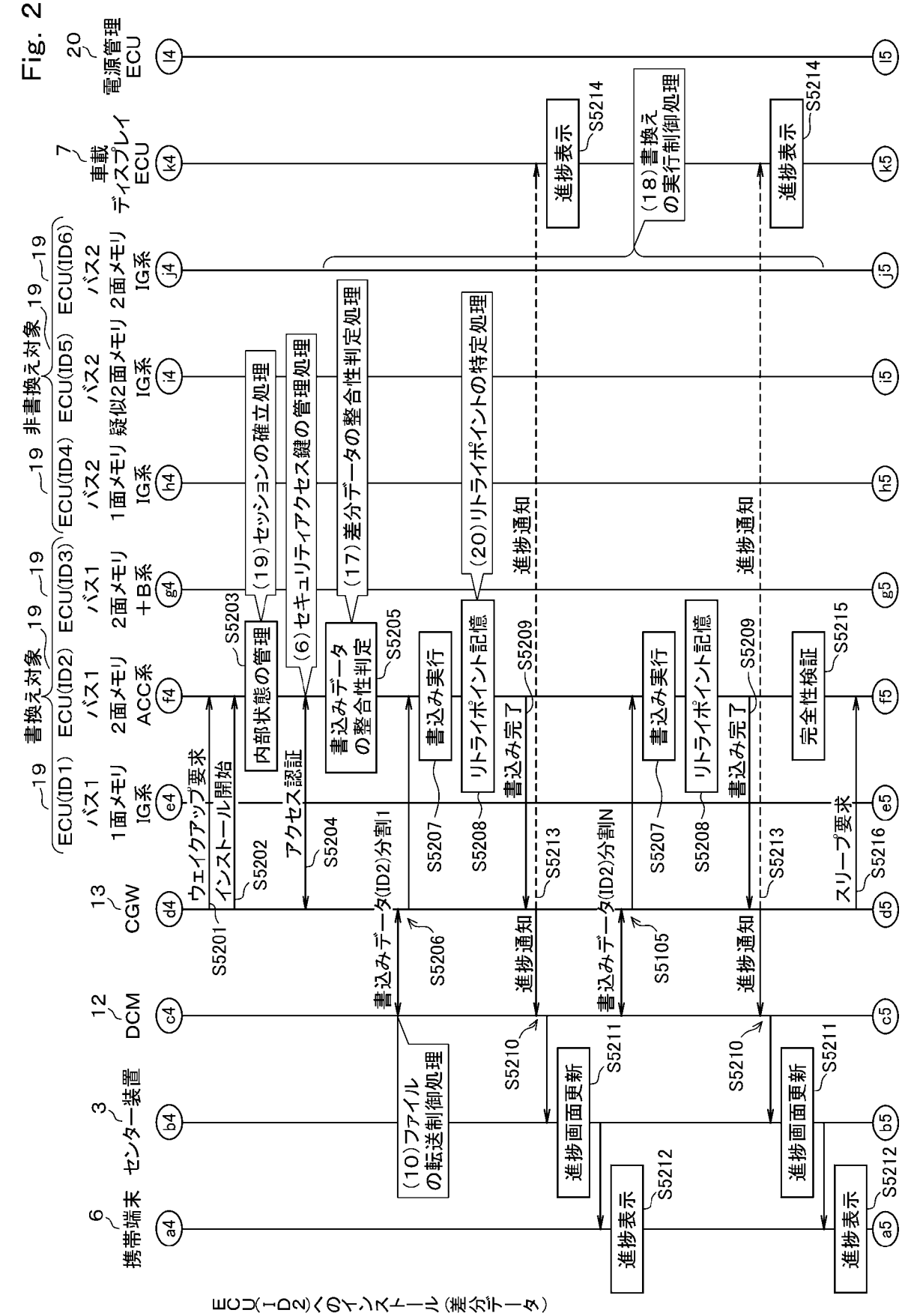
[図226]

Fig. 226


携帯端末 6
センター装置 3
DCM 12
CGW 13
ECU(ID1)
ECU(ID2)
ECU(ID3)
ECU(ID4)
ECU(ID5)
ECU(ID6)
書換え対象 19
非書換え対象 19
バス1 1面メモリ IG系
バス1 2面メモリ ACC系
バス1 2面メモリ +B系
バス2 1面メモリ IG系
バス2 疑似2面メモリ IG系
バス2 2面メモリ IG系
車載ディスプレイ ECU 7
電源管理 ECU 20
インストール開始
内部状態の管理
アクセス認証
書込みデータの整合性判定
書込みデータ(ID1)分割1
書込み実行
リトライポイント記憶
書込み完了
書込みデータ(ID1)分割N
進捗通知
進捗表示
進捗画面更新
完全性検証
スリープ要求
S5101
S5102
S5103
S5104
S5105
S5106
S5107
S5108
S5109
S5110
S5111
S5112
S5113
S5114
S5115
(16)書換え進捗状況の表示制御処理
(21)進捗状態の同期制御処理
ECU(ID1)へのインストール(全データ)

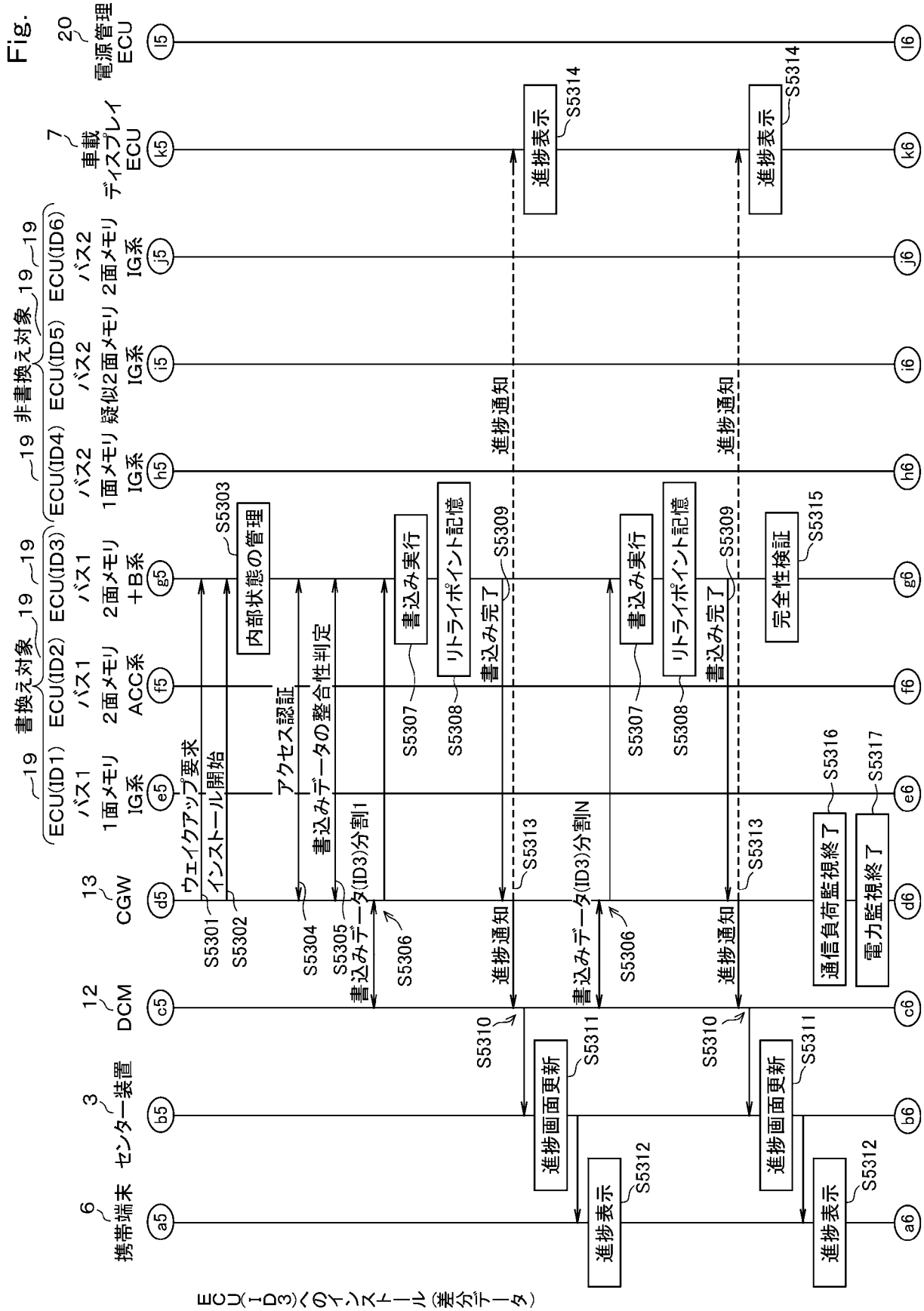
[図227]

Fig. 227


携帯端末 6
センター装置 3
DCM 12
CGW 13
電源管理ECU 20
車載ディスプレイECU 7
書換え対象 19
非書換え対象 19
ECU(ID1) バス1 1面メモリ IG系
ECU(ID2) バス1 2面メモリ ACC系
ECU(ID3) バス1 2面メモリ +B系
ECU(ID4) バス2 1面メモリ IG系
ECU(ID5) バス2 疑似2面メモリ IG系
ECU(ID6) バス2 2面メモリ IG系
ウェイクアップ要求
インストール開始
アクセス認証
内部状態の管理
(6)セキュリティアクセス鍵の管理処理
(19)セッションの確立処理
書込みデータの整合性判定
(17)差分データの整合性判定処理
書込み実行
リトライポイント記憶
(20)リトライポイントの特定処理
書込み完了
進捗通知
完全性検証
スリープ要求
(10)ファイルの転送制御処理
書込みデータ(ID2)分割1
書込みデータ(ID2)分割N
進捗画面更新
進捗表示
(18)書換えの実行制御処理
S5201
S5202
S5203
S5204
S5205
S5206
S5207
S5208
S5209
S5210
S5211
S5212
S5213
S5214
S5215
S5216
S5105
ECU(ID2)へのインストール(差分データ)

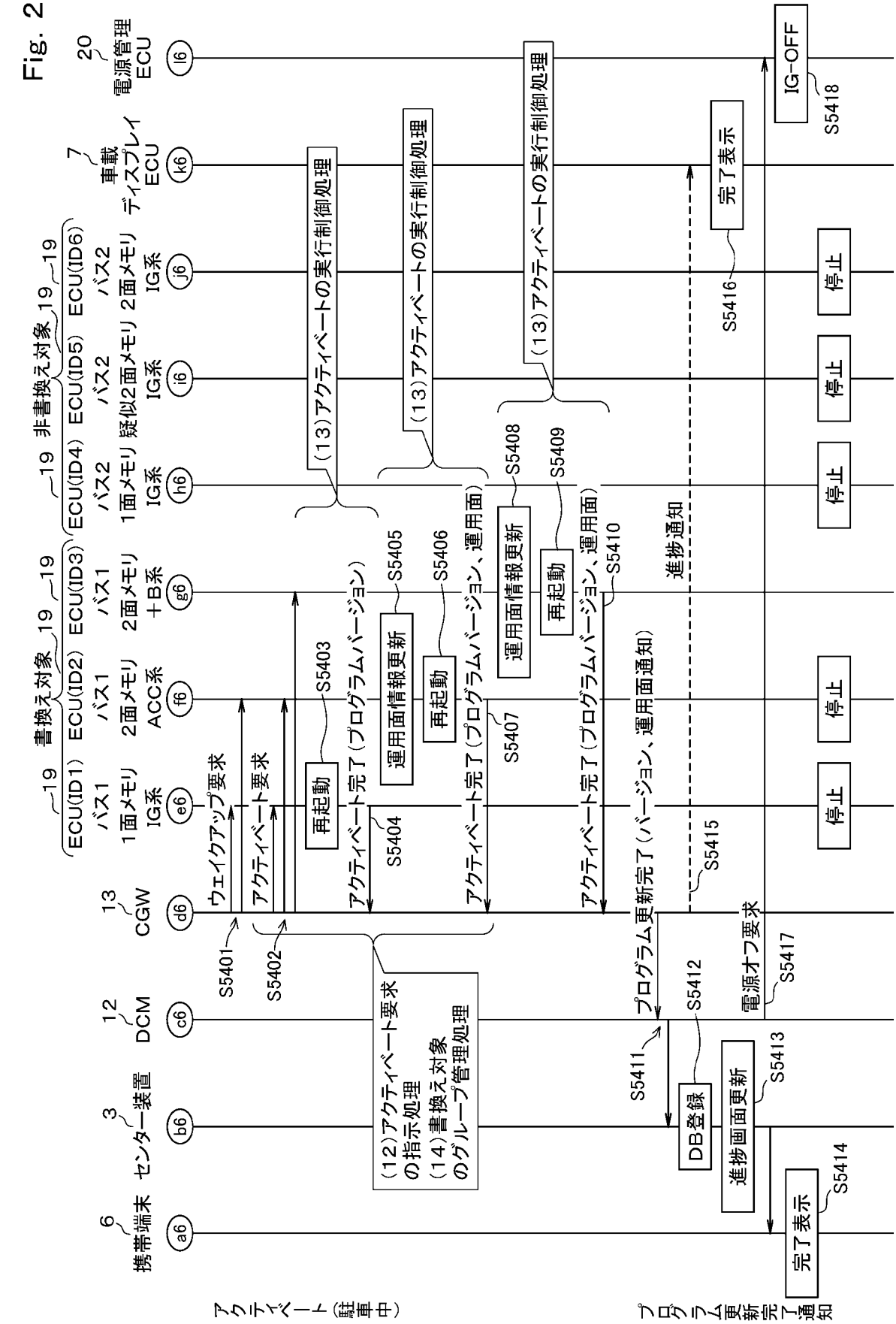
[図228]

Fig. 228


携帯端末 6
センター装置 3
DCM 12
CGW 13
車載ディスプレイ ECU 7
電源管理 ECU 20
19 書換え対象 19 19 非書換え対象 19 19
ECU(ID1) バス1 1面メモリ IG系 e5
ECU(ID2) バス1 2面メモリ ACC系 f5
ECU(ID3) バス1 2面メモリ +B系 g5
ECU(ID4) バス2 1面メモリ IG系 h5
ECU(ID5) バス2 疑似2面メモリ IG系 i5
ECU(ID6) バス2 2面メモリ IG系 j5
ウェイクアップ要求
インストール開始
アクセス認証
書込みデータの整合性判定
内部状態の管理
書込み実行
リトライポイント記憶
書込み完了
書込みデータ(ID3)分割1
書込みデータ(ID3)分割N
進捗通知
進捗画面更新
進捗表示
通信負荷監視終了
電力監視終了
完全性検証
S5301
S5302
S5303
S5304
S5305
S5306
S5307
S5308
S5309
S5310
S5311
S5312
S5313
S5314
S5315
S5316
S5317
ECU(ID3)へのインストール(差分データ)

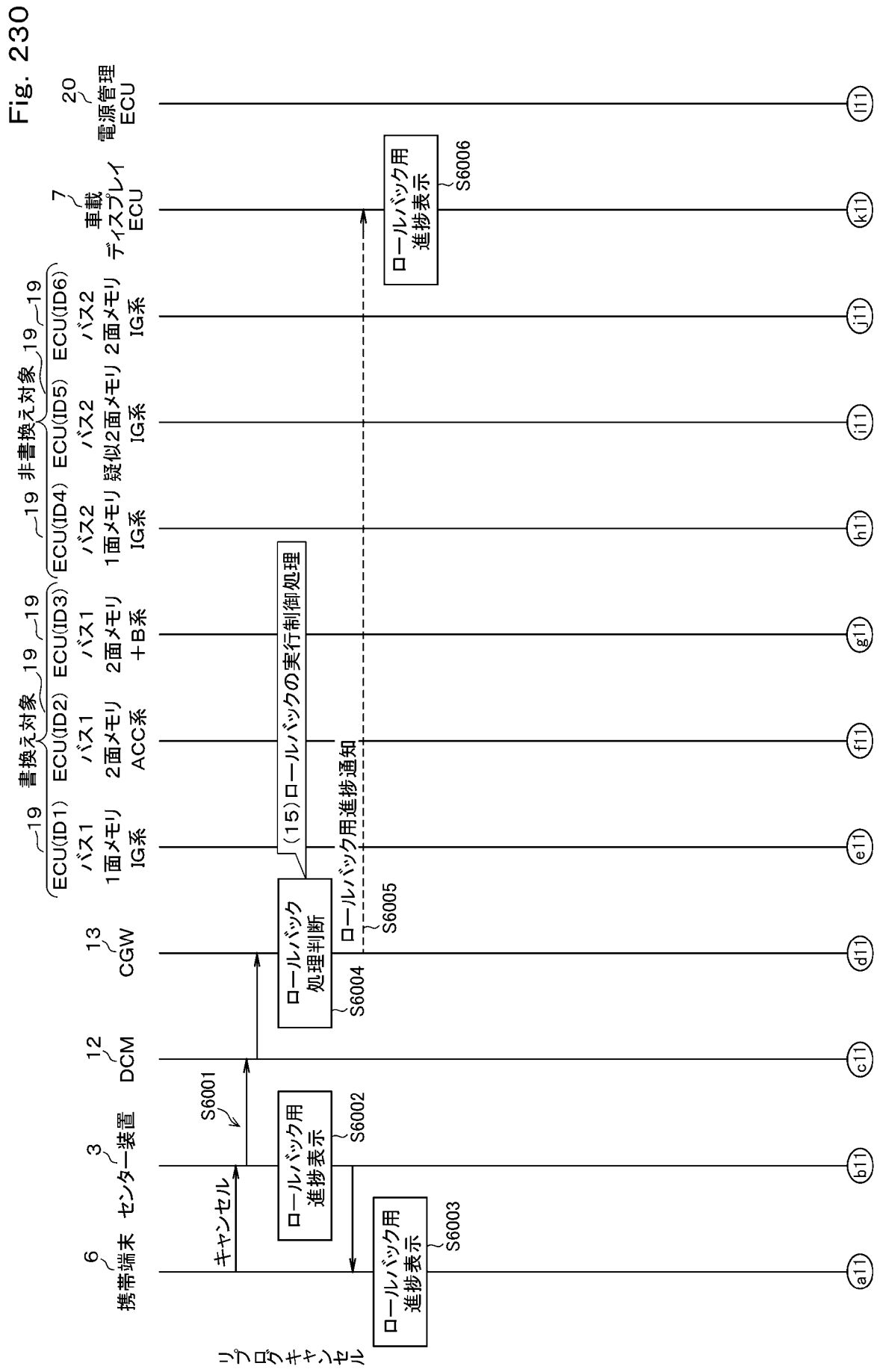
[図229]

Fig. 229


書換え対象
非書換え対象
ECU(ID1) バス1 1面メモリ IG系 e6
ECU(ID2) バス1 2面メモリ ACC系 f6
ECU(ID3) バス1 2面メモリ +B系 g6
ECU(ID4) バス2 1面メモリ IG系 h6
ECU(ID5) バス2 疑似2面メモリ IG系 i6
ECU(ID6) バス2 2面メモリ IG系 j6
19
6 携帯端末 a6
3 センター装置 b6
12 DCM c6
13 CGW d6
7 車載ディスプレイ ECU k6
20 電源管理 ECU l6
ウェイクアップ要求
アクティベート要求
再起動
S5403
アクティベート完了(プログラムバージョン)
S5404
運用面情報更新
S5405
再起動
S5406
アクティベート完了(プログラムバージョン、運用面)
S5407
運用面情報更新
S5408
再起動
S5409
アクティベート完了(プログラムバージョン、運用面)
S5410
進捗通知
S5415
(13)アクティベートの実行制御処理
(13)アクティベートの実行制御処理
(13)アクティベートの実行制御処理
S5401
S5402
(12)アクティベート要求の指示処理
(14)書換え対象のグループ管理処理
プログラム更新完了(バージョン、運用面通知)
S5411
S5412
DB登録
進捗画面更新
S5413
電源オフ要求
S5417
S5414
完了表示
S5416
完了表示
IG-OFF
S5418
停止
停止
停止
停止
停止
アクティベート(駐車中)
プログラム更新完了通知

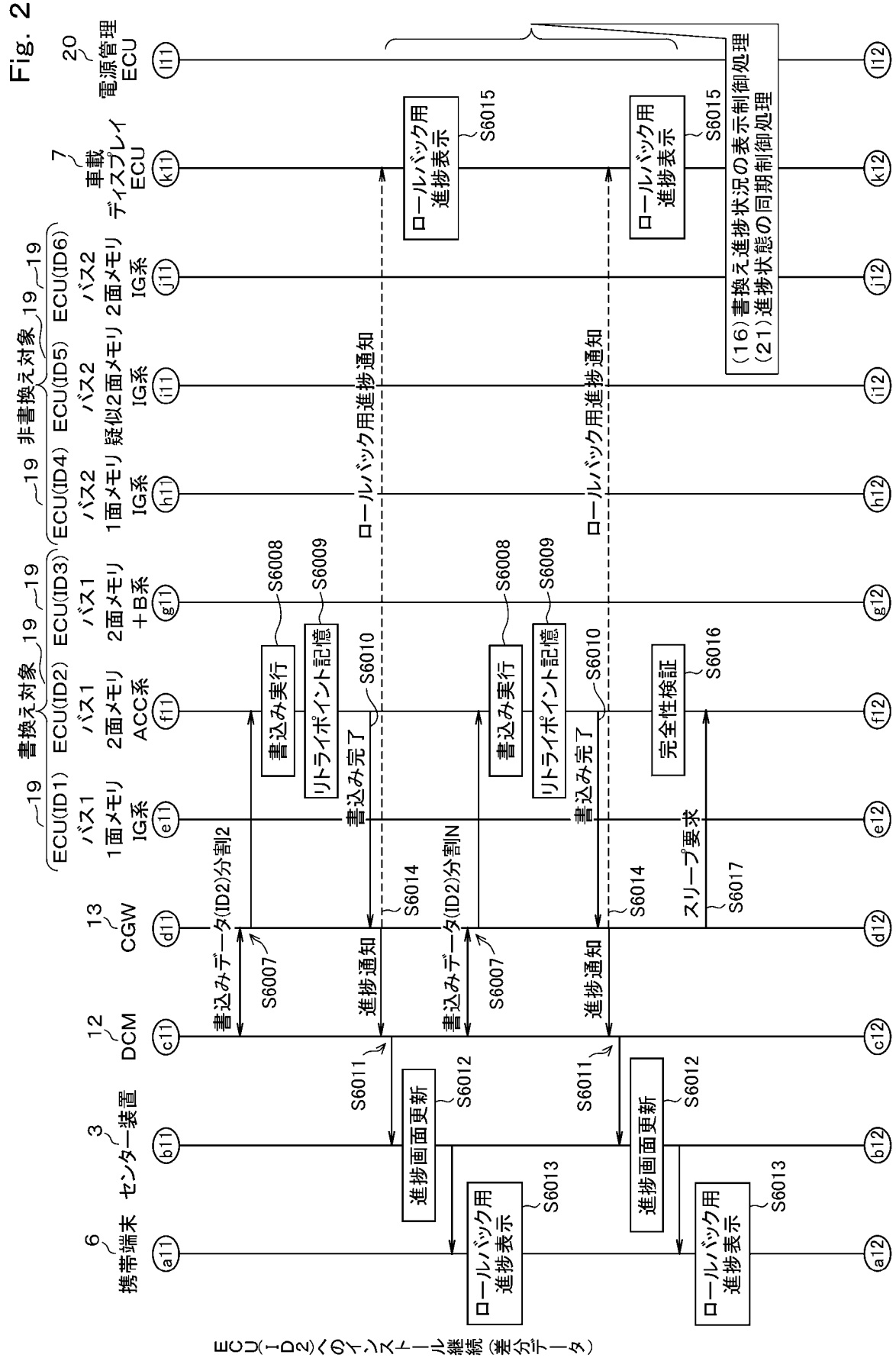
[図230]

Fig. 230


6
携帯端末
3
センター装置
12
DCM
13
CGW
20
電源管理ECU
7
車載ディスプレイECU
19
書換え対象
19
非書換え対象
ECU(ID1)
バス1
1面メモリ
IG系
ECU(ID2)
バス1
2面メモリ
ACC系
ECU(ID3)
バス1
2面メモリ
+B系
ECU(ID4)
バス2
1面メモリ
IG系
ECU(ID5)
バス2
疑似2面メモリ
IG系
ECU(ID6)
バス2
2面メモリ
IG系
リプログキャンセル
キャンセル
S6001
ロールバック用進捗表示
S6002
ロールバック用進捗表示
S6003
ロールバック処理判断
S6004
(15)ロールバックの実行制御処理
ロールバック用進捗通知
S6005
ロールバック用進捗表示
S6006
a11
b11
c11
d11
e11
f11
g11
h11
i11
j11
k11
l11

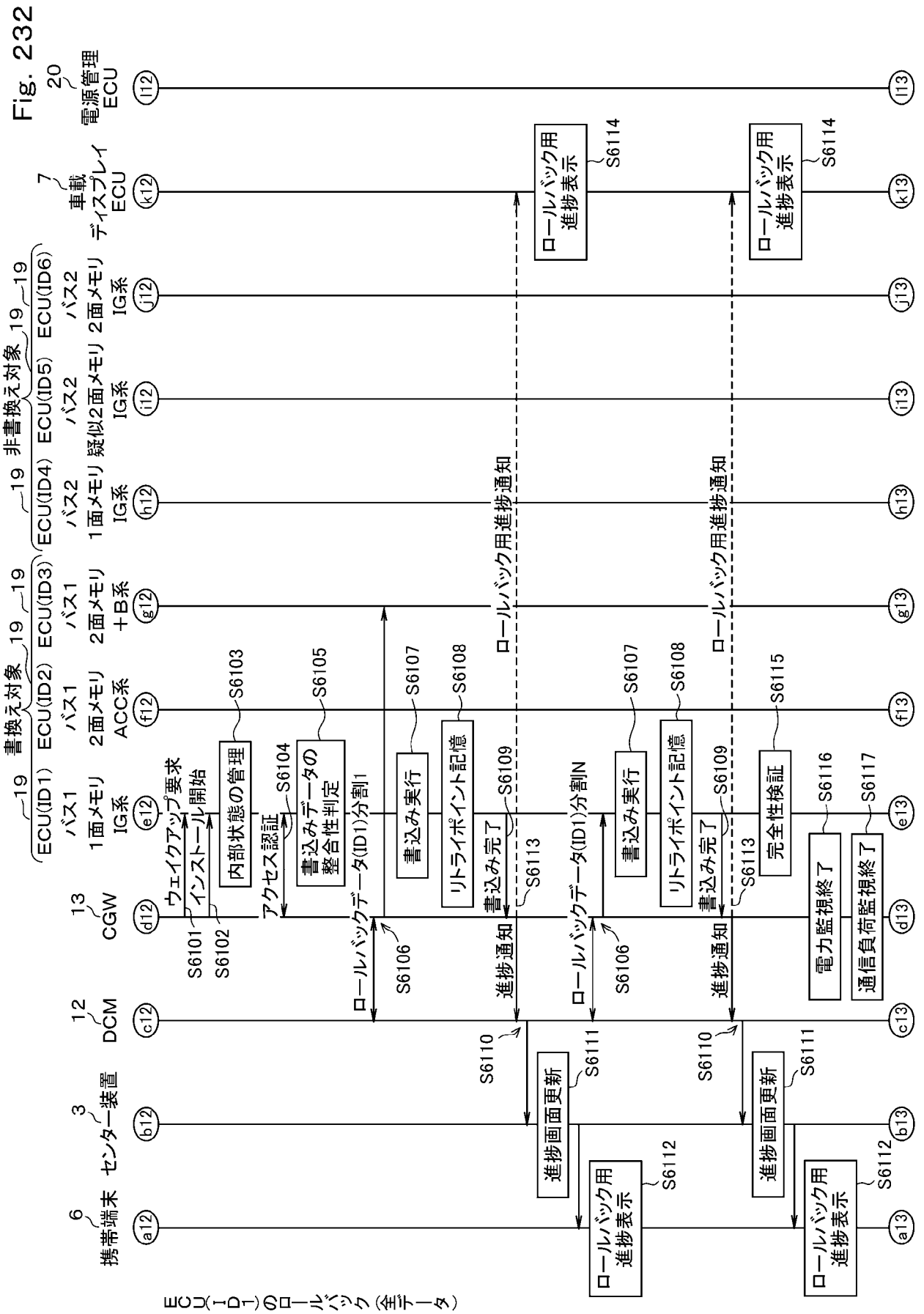
[図231]

Fig. 231


6 携帯端末
3 センター装置
12 DCM
13 CGW
19 書換え対象 ECU(ID1) バス1 1面メモリ IG系 e11
19 書換え対象 ECU(ID2) バス1 2面メモリ ACC系 f11
19 ECU(ID3) バス1 2面メモリ +B系 g11
19 非書換え対象 ECU(ID4) バス2 1面メモリ IG系 h11
19 ECU(ID5) バス2 疑似2面メモリ IG系 i11
19 ECU(ID6) バス2 2面メモリ IG系 j11
7 車載ディスプレイ ECU k11
20 電源管理 ECU l11
a11 b11 c11 d11 e11 f11 g11 h11 i11 j11 k11 l11
a12 b12 c12 d12 e12 f12 g12 h12 i12 j12 k12 l12
ECU(ID2)へのインストール継続（差分データ）
書込みデータ(ID2)分割2
書込みデータ(ID2)分割N
S6007
進捗通知
S6008 書込み実行
S6009 リトライポイント記憶
S6010 書込み完了
S6011
S6012 進捗画面更新
S6013 ロールバック用進捗表示
S6014 ロールバック用進捗通知
S6015 ロールバック用進捗表示
S6016 完全性検証
スリープ要求
S6017
（16）書換え進捗状況の表示制御処理
（21）進捗状態の同期制御処理

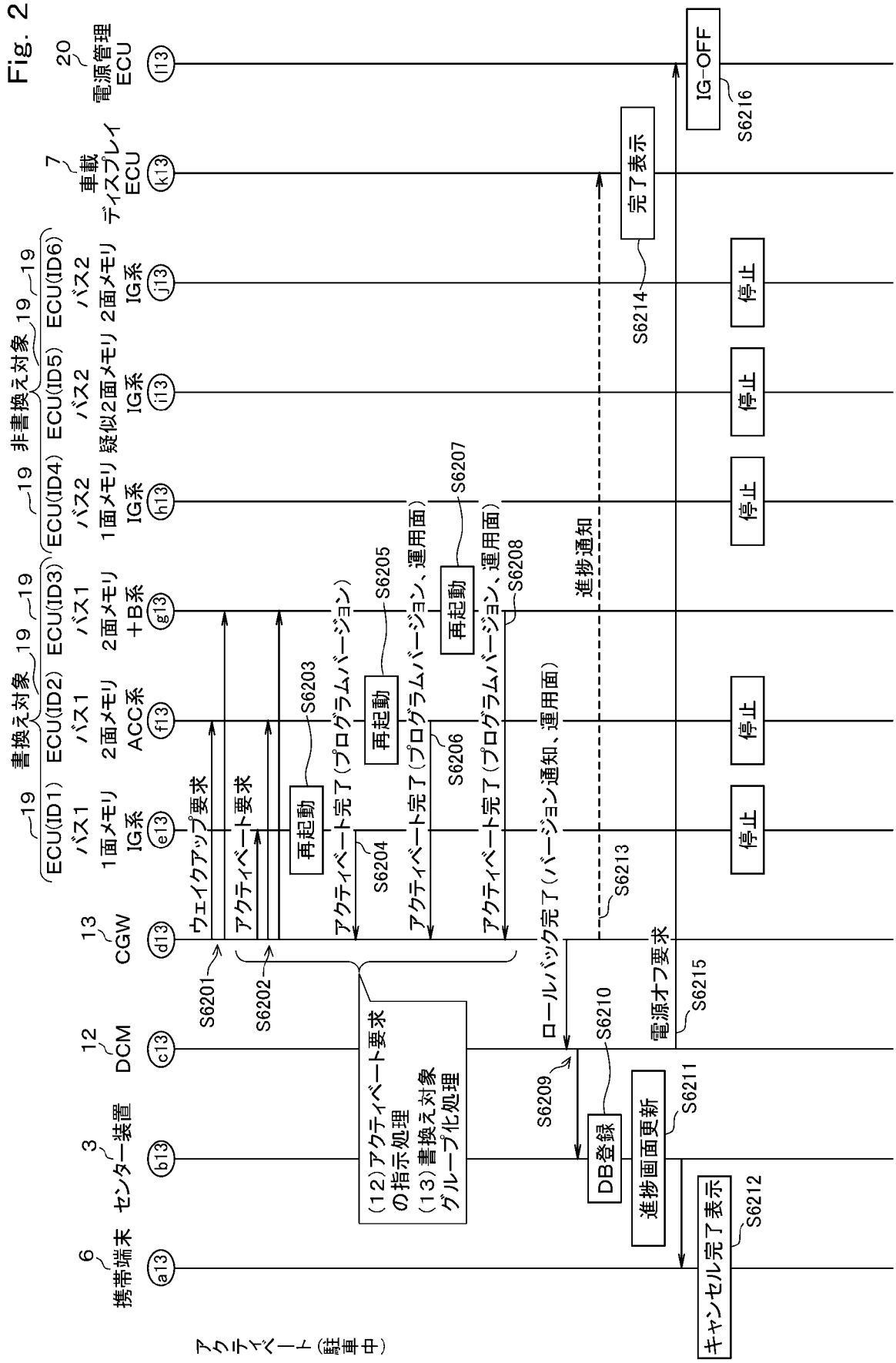
[図232]

Fig. 232


携帯端末 6
センター装置 3
DCM 12
CGW 13
書換え対象 19
ECU(ID1) バス1 1面メモリ IG系
ECU(ID2) バス1 2面メモリ ACC系
ECU(ID3) バス1 2面メモリ +B系
非書換え対象 19
ECU(ID4) バス2 1面メモリ IG系
ECU(ID5) バス2 疑似2面メモリ IG系
ECU(ID6) バス2 2面メモリ IG系
車載ディスプレイ ECU 7
電源管理 ECU 20
ウェイクアップ要求
インストール開始
S6101
S6102
内部状態の管理
S6103
アクセス認証
S6104
書込みデータの整合性判定
S6105
ロールバックデータ(ID1)分割1
S6106
書込み実行
S6107
リトライポイント記憶
S6108
書込み完了
S6109
S6113
進捗通知
S6110
進捗画面更新
S6111
ロールバック用進捗表示
S6112
ロールバック用進捗通知
ロールバック用進捗表示
S6114
ロールバックデータ(ID1)分割N
S6106
書込み実行
S6107
リトライポイント記憶
S6108
書込み完了
S6109
S6113
進捗通知
S6110
進捗画面更新
S6111
ロールバック用進捗表示
S6112
ロールバック用進捗通知
ロールバック用進捗表示
S6114
完全性検証
S6115
電力監視終了
S6116
通信負荷監視終了
S6117
ECU(1つ)のロールバック(全データ)

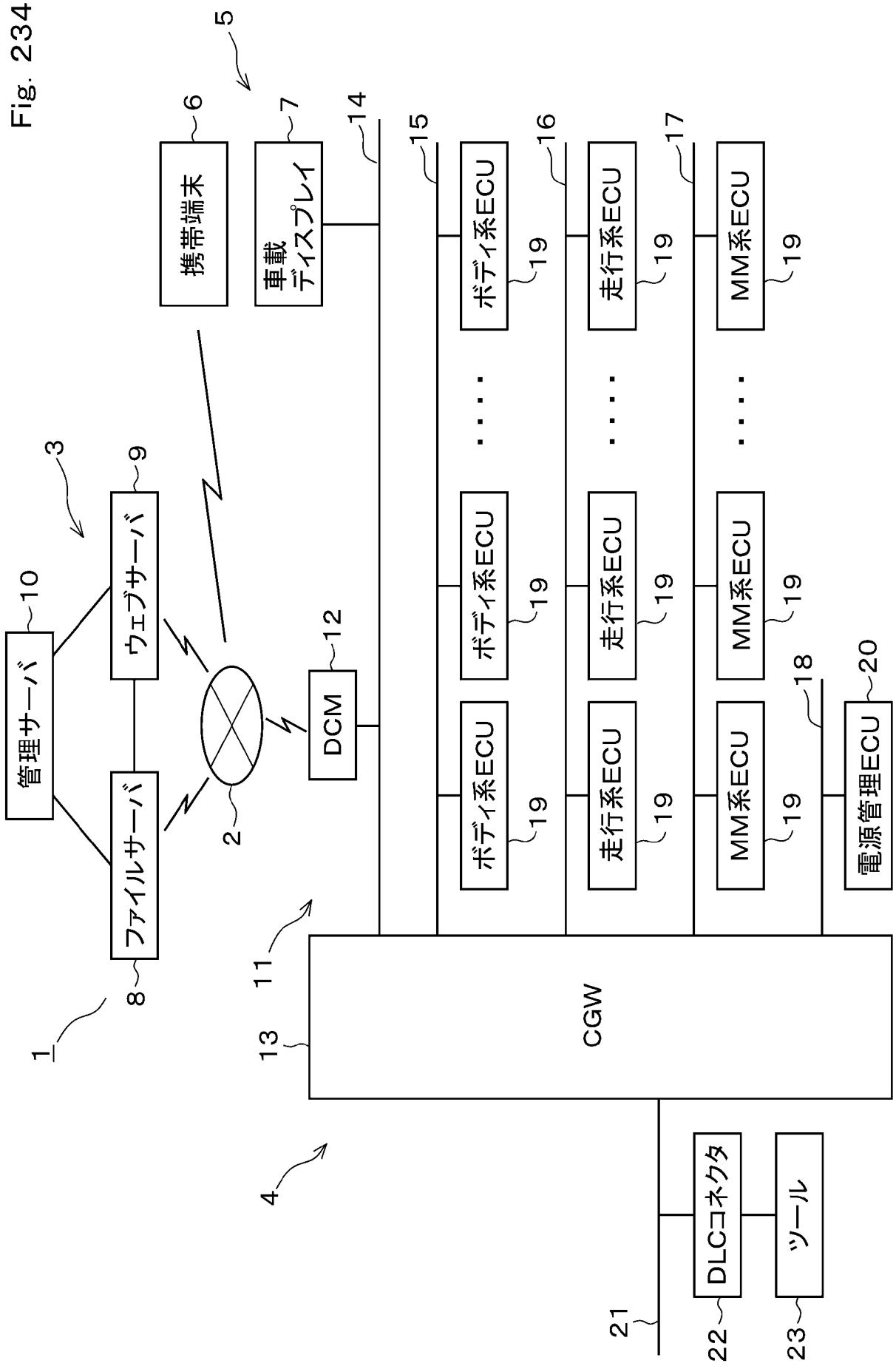
[図233]

Fig. 233


6 携帯端末 a13
3 センター装置 b13
12 DCM c13
13 CGW d13
19 書換え対象 ECU(ID1) バス1 1面メモリ IG系 e13
19 書換え対象 ECU(ID2) バス1 2面メモリ ACC系 f13
19 書換え対象 ECU(ID3) バス1 2面メモリ +B系 g13
19 非書換え対象 ECU(ID4) バス2 1面メモリ 疑似2面メモリ IG系 h13
19 非書換え対象 ECU(ID5) バス2 2面メモリ IG系 i13
19 非書換え対象 ECU(ID6) バス2 2面メモリ IG系 j13
7 車載ディスプレイ ECU k13
20 電源管理 ECU l13
アクティベート(駐車中)
S6201 ウェイクアップ要求
S6202 アクティベート要求
S6203 再起動
アクティベート完了(プログラムバージョン)
S6204
S6205 再起動
アクティベート完了(プログラムバージョン、運用面)
S6206
S6207 再起動
アクティベート完了(プログラムバージョン、運用面)
S6208
進捗通知
S6213
ロールバック完了(バージョン通知、運用面)
S6209
S6210 DB登録
電源オフ要求
S6215
S6211 進捗画面更新
S6212 キャンセル完了表示
(12)アクティベート要求の指示処理
(13)書換え対象グループ化処理
S6214 完了表示
S6216 IG-OFF
停止
停止
停止
停止
停止

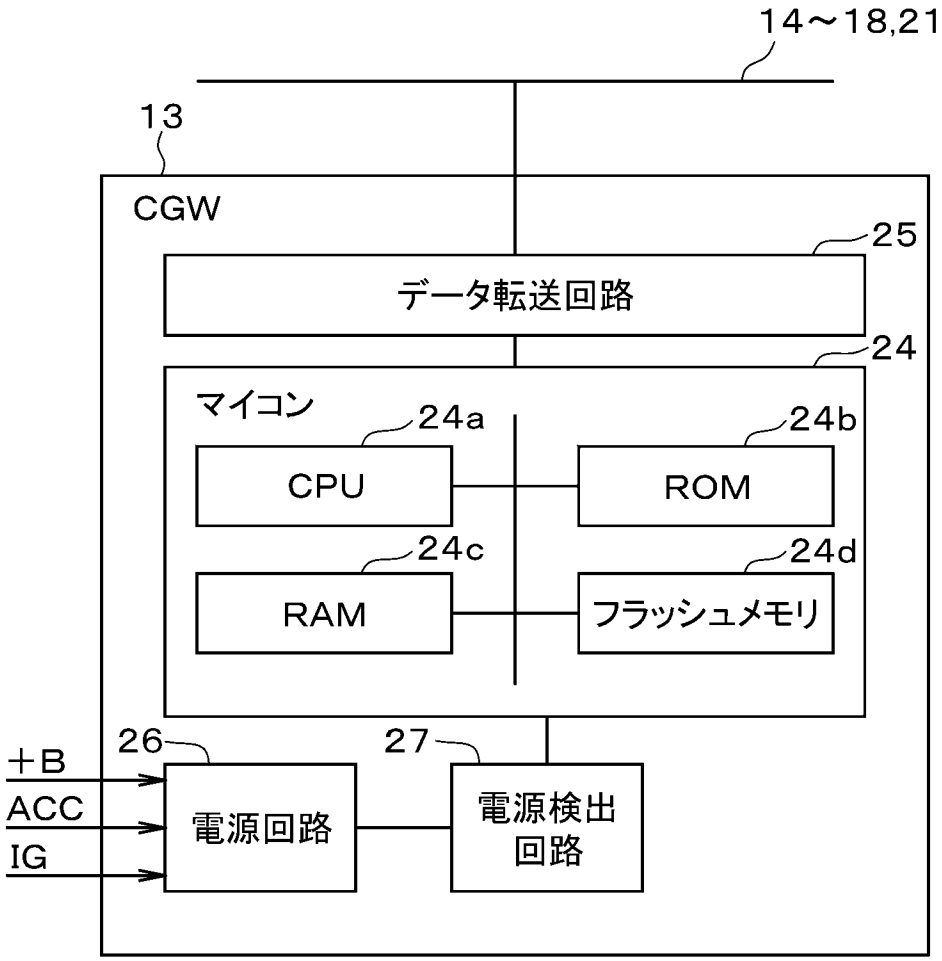
[図234]

Fig. 234


1
2
3
4
5
6
携帯端末
7
車載ディスプレイ
8
ファイルサーバ
9
ウェブサーバ
10
管理サーバ
11
13
CGW
12
DCM
14
15
16
17
18
19
ボディ系ECU
走行系ECU
MM系ECU
20
電源管理ECU
21
22
DLCコネクタ
23
ツール

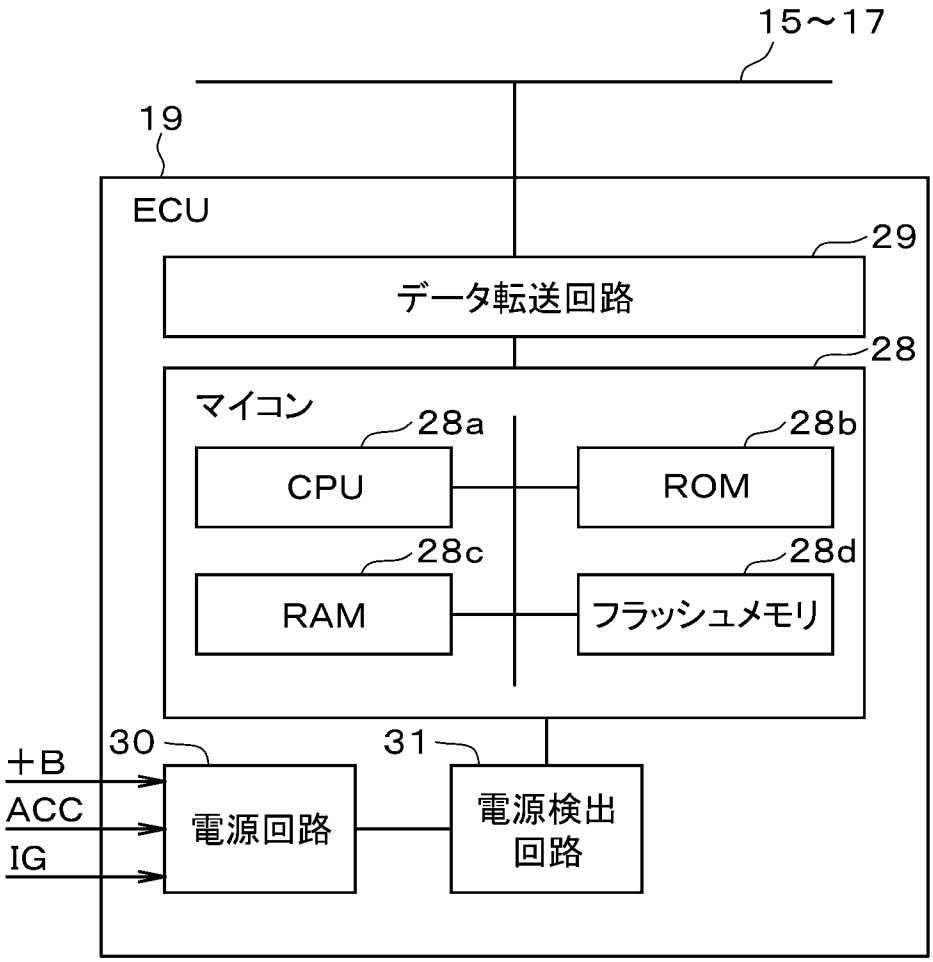
[図235]

Fig. 235


14～18,21
13
CGW
25
データ転送回路
24
マイコン
24a
CPU
24b
ROM
24c
RAM
24d
フラッシュメモリ
26
27
＋B
ACC
IG
電源回路
電源検出
回路

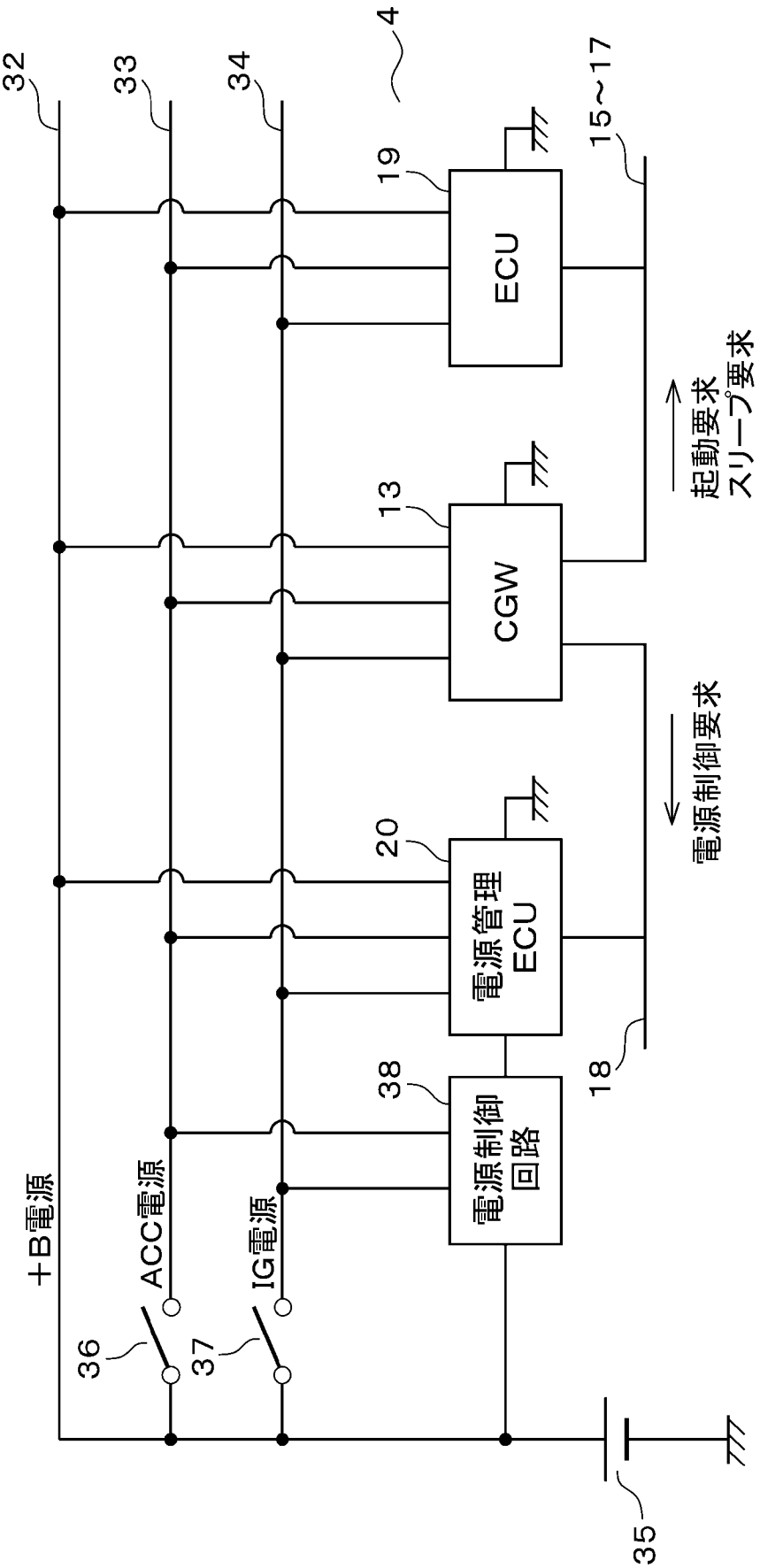
[図236]

Fig. 236


15～17
19
ECU
29
データ転送回路
28
マイコン
28a
CPU
28b
ROM
28c
RAM
28d
フラッシュメモリ
30
31
＋B
ACC
IG
電源回路
電源検出
回路

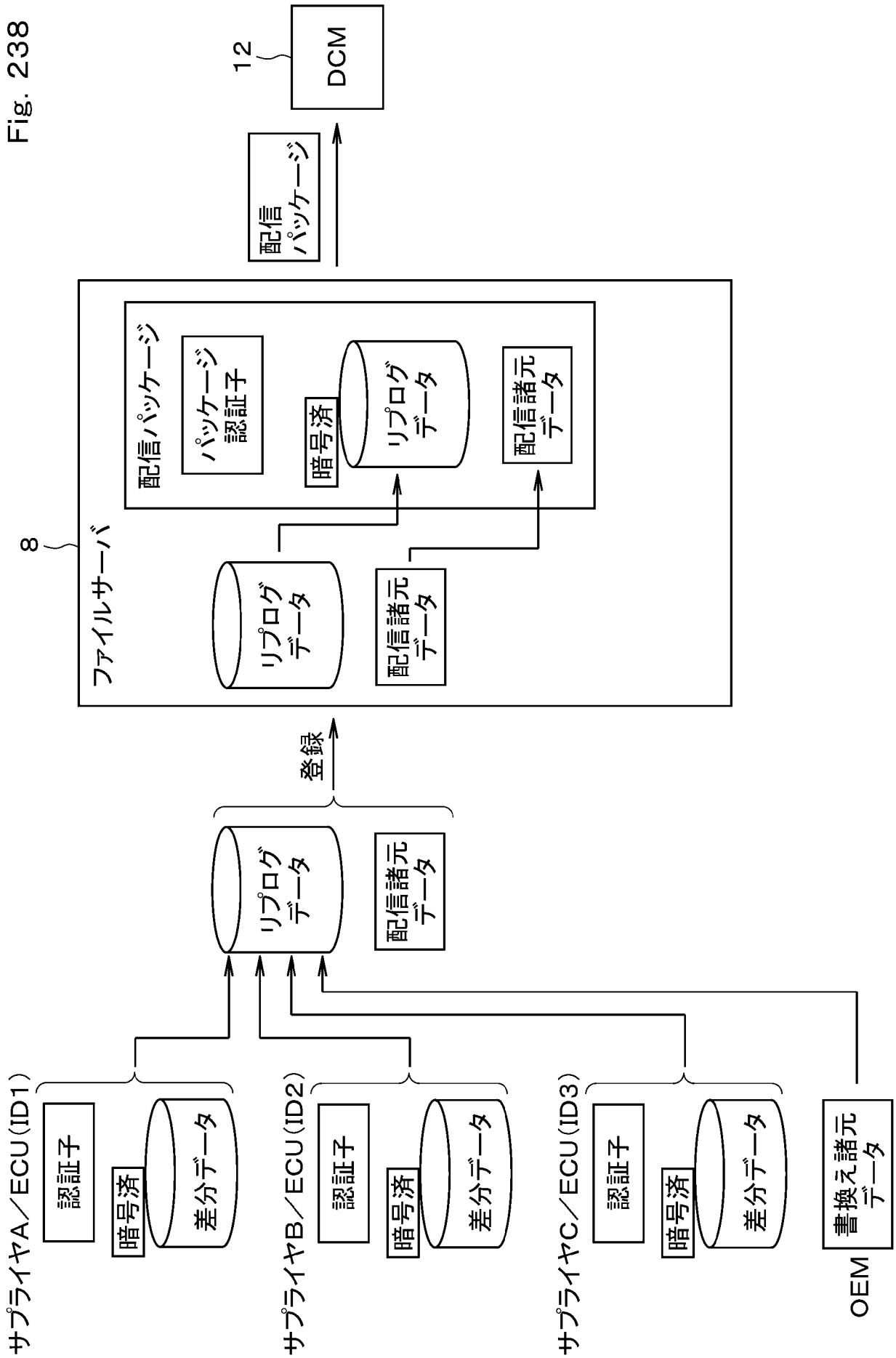
[図237]

Fig. 237


32
33
34
4
15～17
19
ECU
起動要求
スリープ要求
13
CGW
電源制御要求
20
電源管理
ECU
38
電源制御
回路
18
＋B電源
ACC電源
IG電源
36
37
35

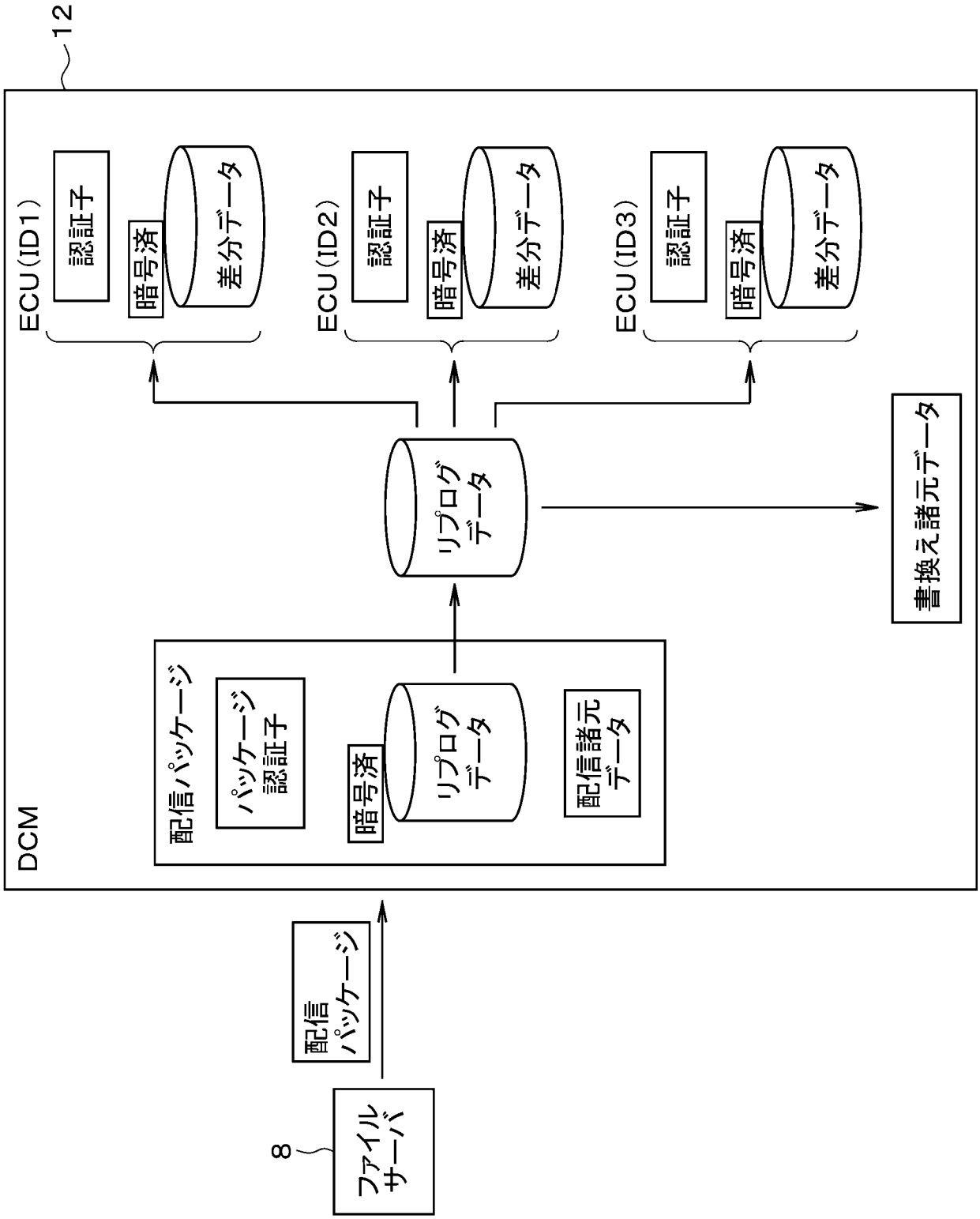
[図238]

Fig. 238


12
DCM
配信
パッケージ
8
ファイルサーバ
配信パッケージ
パッケージ
認証子
暗号済
リプログ
データ
配信諸元
データ
リプログ
データ
配信諸元
データ
登録
リプログ
データ
配信諸元
データ
サプライヤA／ECU(ID1)
認証子
暗号済
差分データ
サプライヤB／ECU(ID2)
認証子
暗号済
差分データ
サプライヤC／ECU(ID3)
認証子
暗号済
差分データ
OEM
書換え諸元
データ

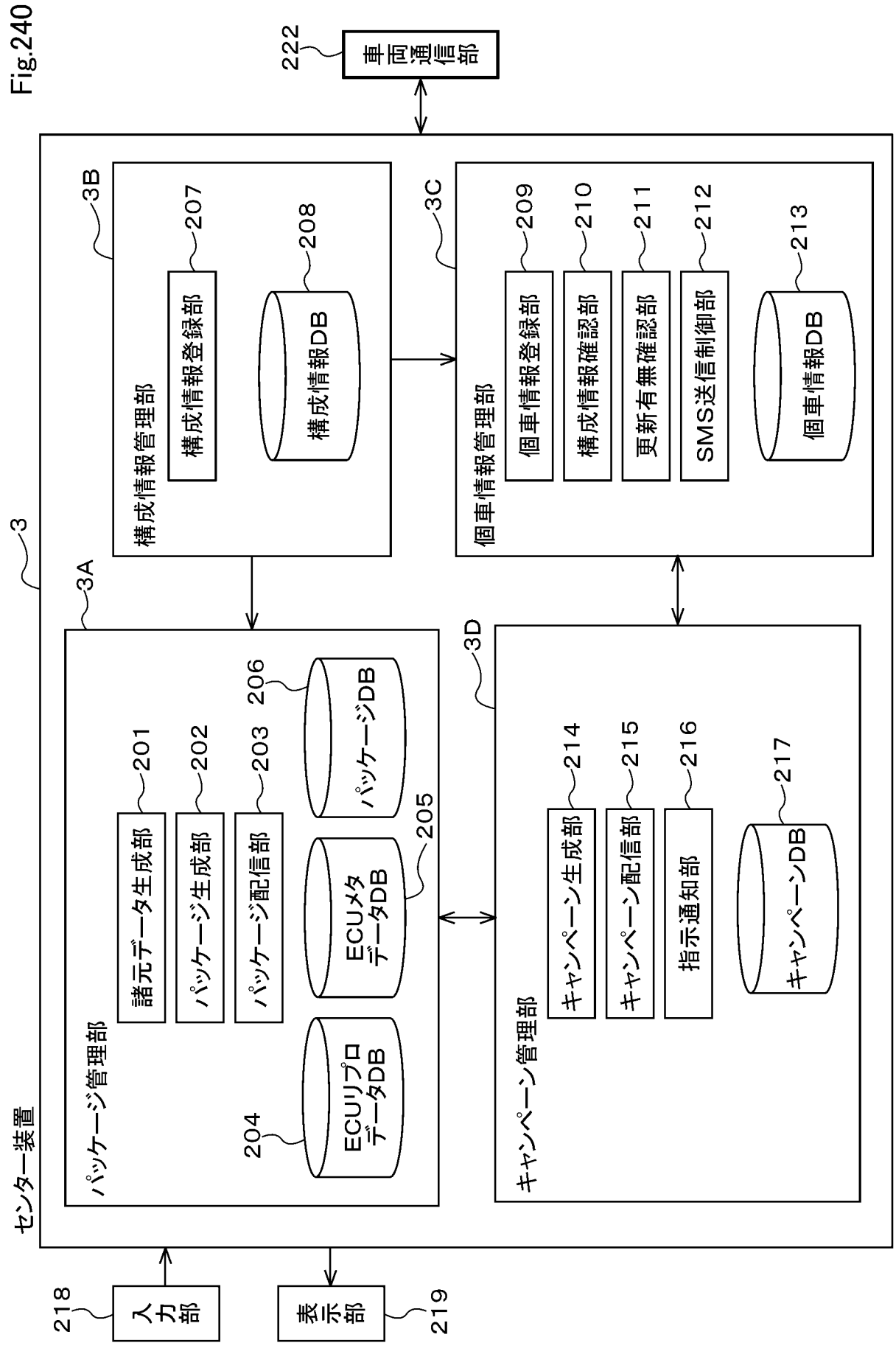
[図239]

Fig. 239


12
DCM
ECU(ID1)
認証子
暗号済
差分データ
ECU(ID2)
認証子
暗号済
差分データ
ECU(ID3)
認証子
暗号済
差分データ
リプログデータ
書換え諸元データ
配信パッケージ
パッケージ認証子
暗号済
リプログデータ
配信諸元データ
配信パッケージ
8
ファイルサーバ

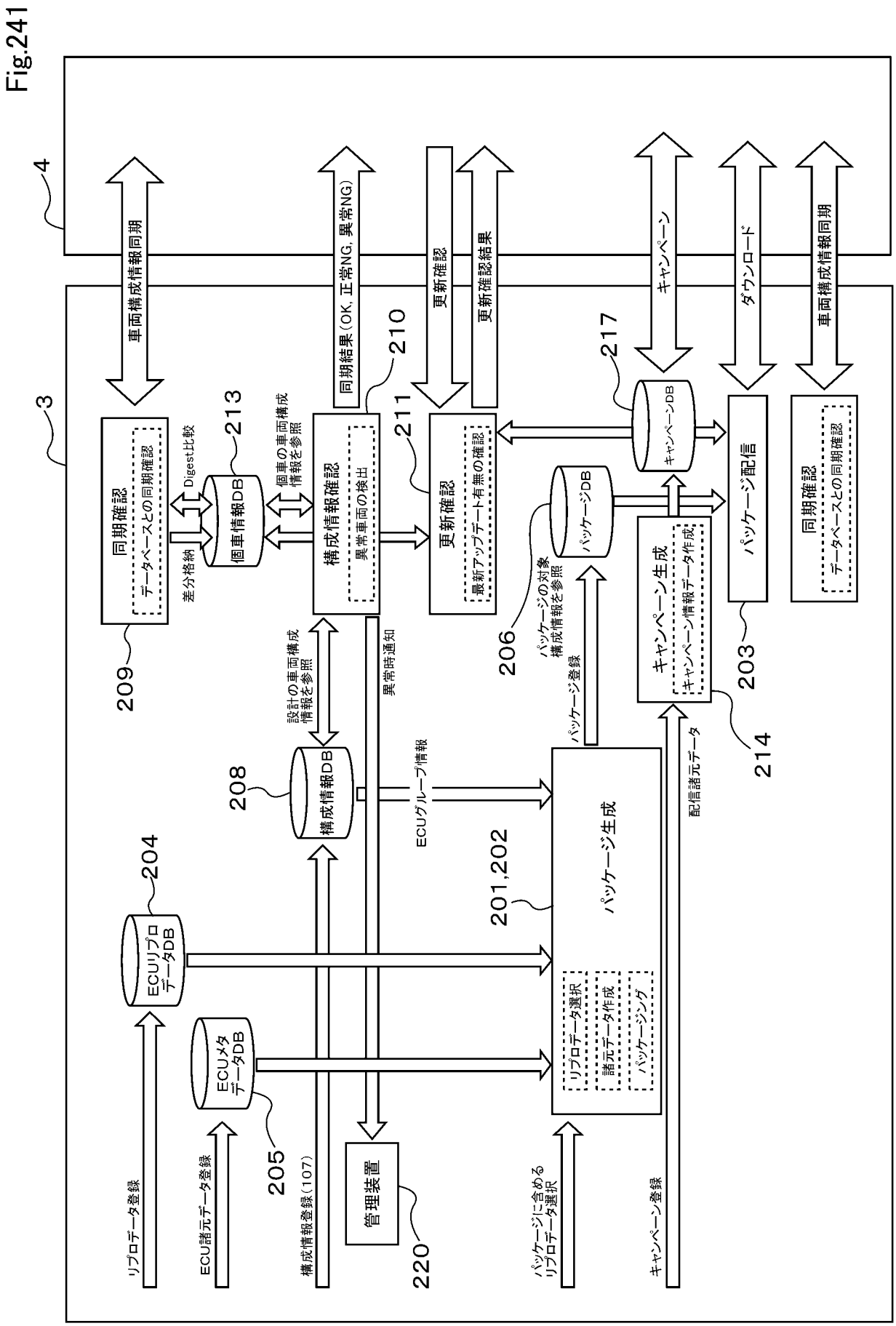
[図240]

Fig.240


センター装置
3
222
車両通信部
3B
構成情報管理部
207
構成情報登録部
208
構成情報DB
3C
個車情報管理部
209
個車情報登録部
210
構成情報確認部
211
更新有無確認部
212
SMS送信制御部
213
個車情報DB
3A
パッケージ管理部
201
諸元データ生成部
202
パッケージ生成部
203
パッケージ配信部
206
パッケージDB
205
ECUメタデータDB
204
ECUリプロデータDB
3D
キャンペーン管理部
214
キャンペーン生成部
215
キャンペーン配信部
216
指示通知部
217
キャンペーンDB
218
入力部
219
表示部

[図241]

Fig.241


4
車両構成情報同期
3
同期確認
データベースとの同期確認
209
差分格納
Digest比較
個車情報DB
213
個車の車両構成情報を参照
構成情報確認
異常車両の検出
211
同期結果（OK, 正常NG, 異常NG）
210
更新確認
最新アップデート有無の確認
更新確認結果
217
キャンペーンDB
キャンペーン
ダウンロード
パッケージDB
パッケージの対象構成情報を参照
206
パッケージ登録
パッケージ配信
203
同期確認
データベースとの同期確認
車両構成情報同期
設計の車両構成情報を参照
構成情報DB
208
異常時通知
ECUグループ情報
201,202
パッケージ生成
リプロデータ選択
諸元データ作成
パッケージング
キャンペーン生成
キャンペーン情報データ作成
214
配信諸元データ
ECUリプロデータDB
204
ECUメタデータDB
205
リプロデータ登録
ECU諸元データ登録
構成情報登録（107）
管理装置
220
パッケージに含めるリプロデータ選択
キャンペーン登録

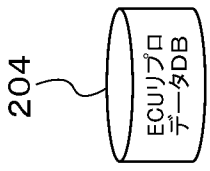
[図242]

Fig.242

車両型式	Vehicle SW ID	Sys ID	ECU ID	ECU SW ID
aaa	0001	SA01_01	ADS	ads_001
aaa	0001	SA02_01	ENG	eng_010
aaa	0001	SA02_01	BRK	brk_001
aaa	0001	SA02_01	EPS	eps_010
⋮				
aaa	0002	SA01_02	ADS	ads_002
aaa	0002	SA02_02	ENG	eng_010
aaa	0002	SA02_02	BRK	brk_005
aaa	0002	SA02_02	EPS	eps_011
⋮				

[図243]

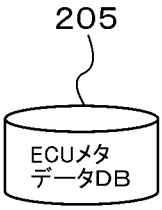
Fig.243



ECU SW ID	ECUプログラム（旧）	ECUプログラム（新）	ECUプログラム（旧）の完全性検証データ	ECUプログラム（新）の完全性検証データ	更新データ（差分データ）	更新データの完全性検証データ	ロールバックデータ（差分データ）	ロールバックデータ（差分データ）の完全性検証データ
ads_002	adsfile001	adsfile002	w1	z1	adsfile001-002	x1	adsfile002-001	y1
brk_005	brkfile001	brkfile005	w2	z2	brkfile001-005	x2	brkfile005-001	y2
eps_011	epsfile010	epsfile011	w3	z3	epsfile010-011	x3	epsfile011-010	y3

[図244]

Fig.244

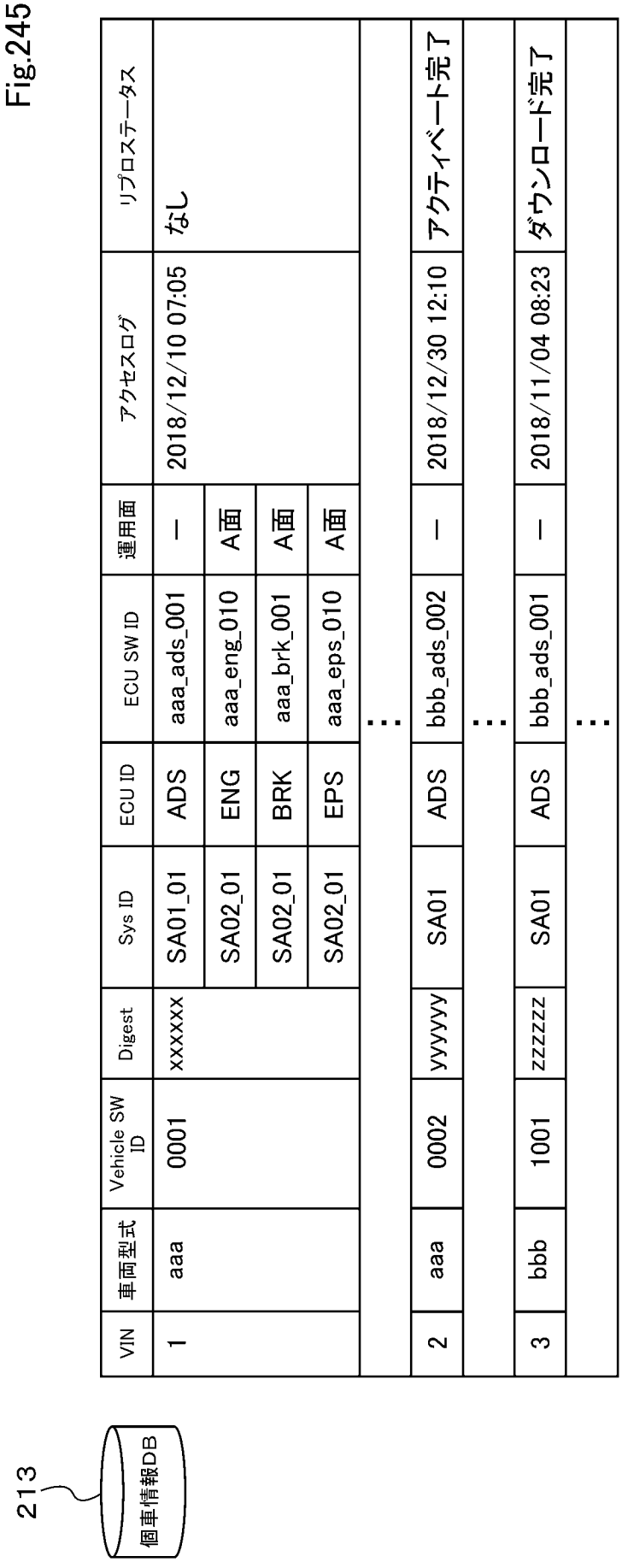


ECU SW ID	更新データサイズ	ロールバックデータサイズ	面	転送サイズ	読出し用アドレス
ads_002	N1 Mbyte	M1 Mbyte	—	1Kbyte	****
brk_005	N2 Mbyte	M2 Mbyte	B面用	4Kbyte	****
eps_011	N3 Mbyte	M3 Mbyte	B面用	1Kbyte	****

車両型式	ECU ID	メモリ	バス	電源	鍵
aaa	ADS	1面	第2	IG	ads_key
aaa	ENG	2面	第1	ACC	eng_key
aaa	BRK	サスペンド	第1	+B	brk_key
aaa	EPS	2面	第1	+B	eps_key

[図245]

Fig.245



VIN	車両型式	Vehicle SW ID	Digest	Sys ID	ECU ID	ECU SW ID	運用面	アクセスログ	リプロステータス
1	aaa	0001	xxxxxx	SA01_01	ADS	aaa_ads_001	—	2018/12/10 07:05	なし
				SA02_01	ENG	aaa_eng_010	A面		
				SA02_01	BRK	aaa_brk_001	A面		
				SA02_01	EPS	aaa_eps_010	A面		
				⋮					
2	aaa	0002	yyyyyy	SA01	ADS	bbb_ads_002	—	2018/12/30 12:10	アクティベート完了
				⋮					
3	bbb	1001	zzzzzz	SA01	ADS	bbb_ads_001	—	2018/11/04 08:23	ダウンロード完了
				⋮					

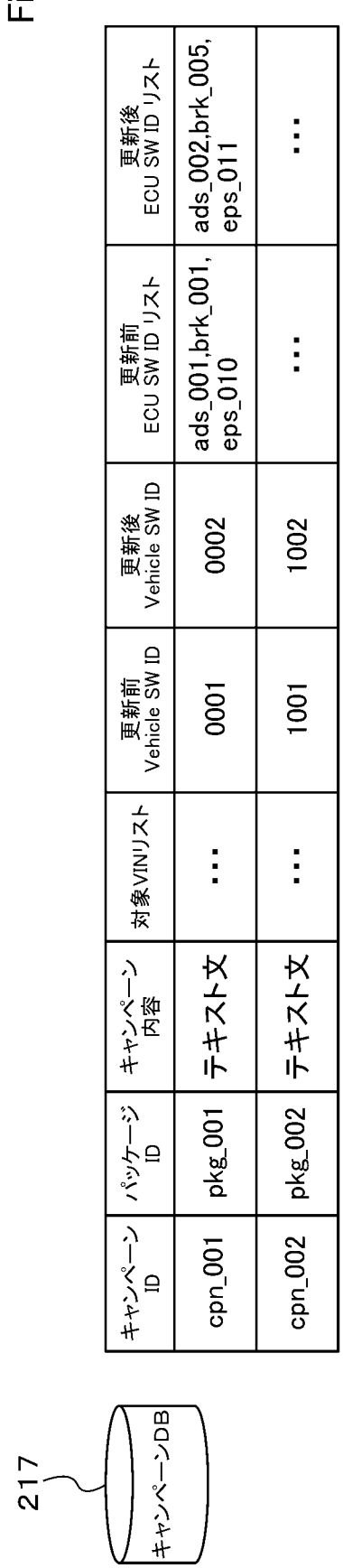
[図246]

Fig.246

パッケージID	ファイル	完全性検証データ
pkg_001	pkg001.dat	xx1.dat
pkg_002	pkg002.dat	xx2.dat

[図247]

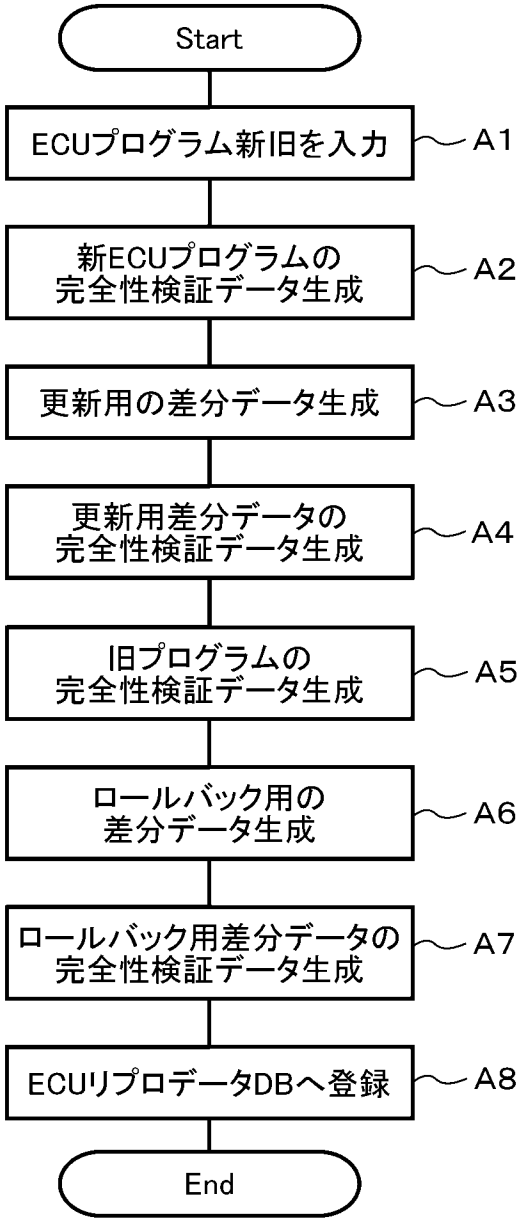
Fig.247



キャンペーンID	パッケージID	キャンペーン内容	対象VINリスト	更新前 Vehicle SW ID	更新後 Vehicle SW ID	更新前 ECU SW ID リスト	更新後 ECU SW ID リスト
cpn_001	pkg_001	テキスト文	・・・	0001	0002	ads_001,brk_001, eps_010	ads_002,brk_005, eps_011
cpn_002	pkg_002	テキスト文	・・・	1001	1002	・・・	・・・

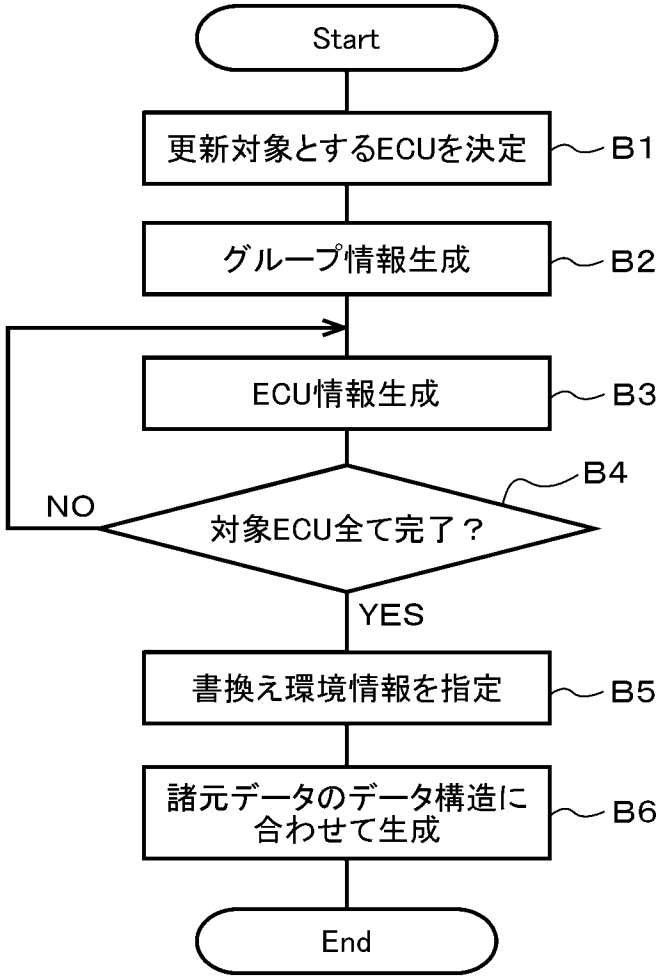
[図248]

Fig.248


Start
ECUプログラム新旧を入力
A1
新ECUプログラムの
完全性検証データ生成
A2
更新用の差分データ生成
A3
更新用差分データの
完全性検証データ生成
A4
旧プログラムの
完全性検証データ生成
A5
ロールバック用の
差分データ生成
A6
ロールバック用差分データの
完全性検証データ生成
A7
ECUリプロデータDBへ登録
A8
End

[図249]

Fig.249


Start
更新対象とするECUを決定
B1
グループ情報生成
B2
ECU情報生成
B3
B4
NO
対象ECU全て完了？
YES
書換え環境情報を指定
B5
諸元データのデータ構造に
合わせて生成
B6
End

[図250]

Fig.250

諸元データ

項目		値(例示)
書換え環境	車両状態	走行中(IGオン中)可／駐車中(IGオフ中)のみ
	バッテリ負荷(残量)	40%以上
	バス負荷テーブル	図251参照
グループ情報	第1グループ情報	ECU(ID1)→ECU(ID2)→ECU(ID3)
	第2グループ情報	ECU(ID4)→ECU(ID5)→ECU(ID6)
ECU(IDn)情報 n＝1～6	ECU ID	ECU ID
	接続バス	第1バス
	接続電源	+B電源, ACC電源, IG電源
	メモリ種別	1面メモリ／疑似2面メモリ／2面メモリ
	書換え面情報	A面が起動面, B面が書換え面
	セキュリティアクセス鍵情報	乱数値(鍵導出鍵)
		鍵パターン
		復号演算パターン
	書換え方法	電源自己保持／電源制御
	転送サイズ	1Kbyte
	更新プログラムバージョン	2.0
	更新プログラム取得アドレス	1
	更新プログラムサイズ	10Mbyte
	ロールバックプログラムバージョン	1.0
	ロールバックプログラム取得アドレス	0x80000
	ロールバックプログラムサイズ	10Mbyte
	書込みデータ種別	差分データ／全データ
	書込み面	B面用

[図251]

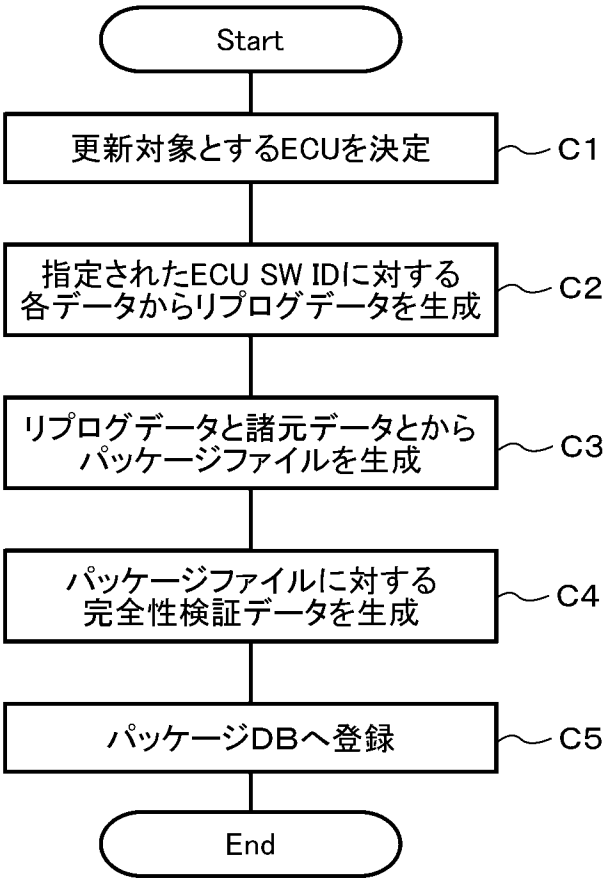
Fig.251

バス負荷テーブル

		第1バス	第2バス	第3バス
伝送許容量		80%	70%	90%
IG 電源状態	車両制御データ	50%	20%	40%
	書込みデータ	30%	50%	50%
ACC 電源状態	車両制御データ	30%	30%	20%
	書込みデータ	50%	40%	70%
+B 電源状態	車両制御データ	20%	10%	50%
	書込みデータ	60%	60%	40%

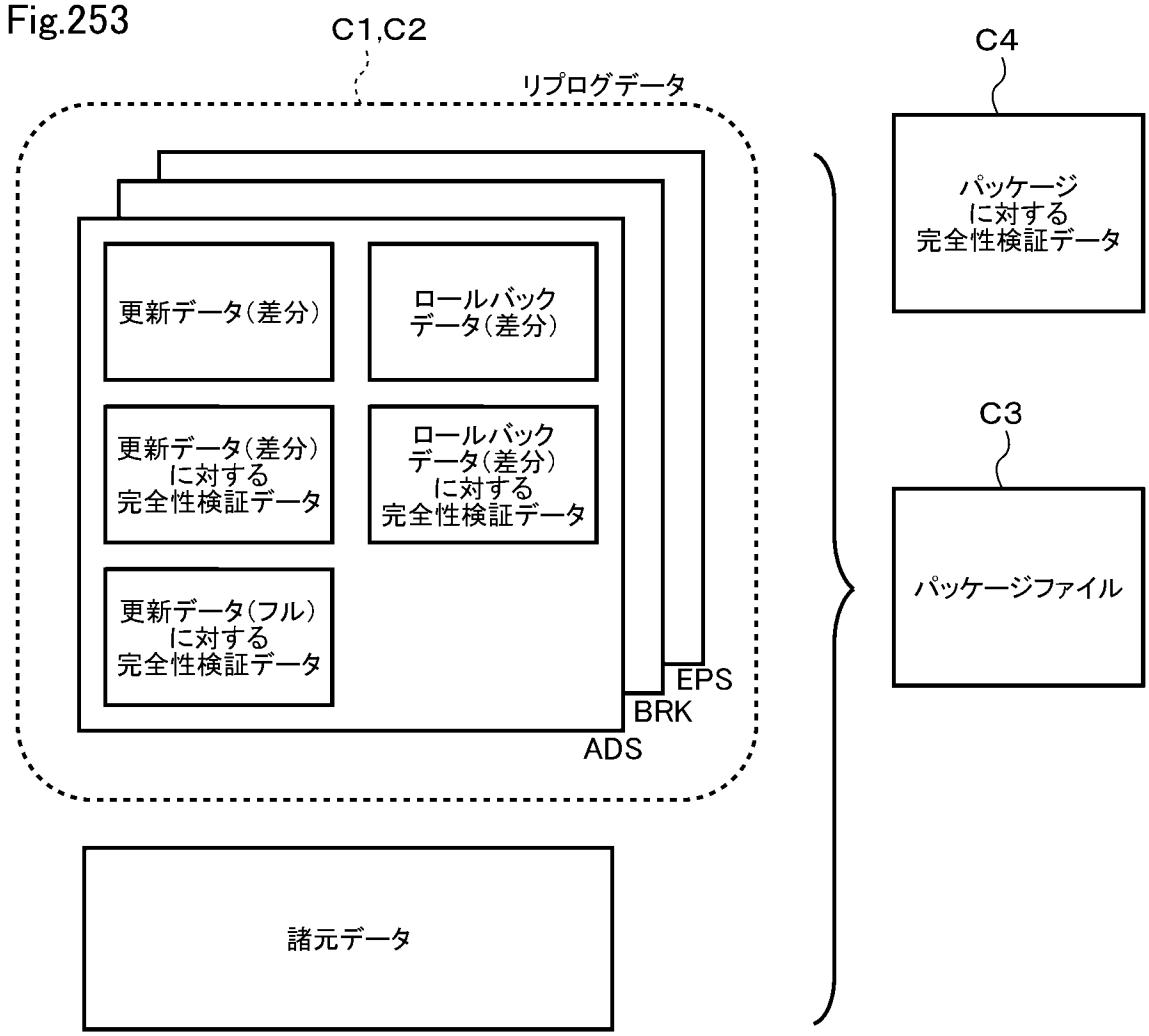
[図252]

Fig.252



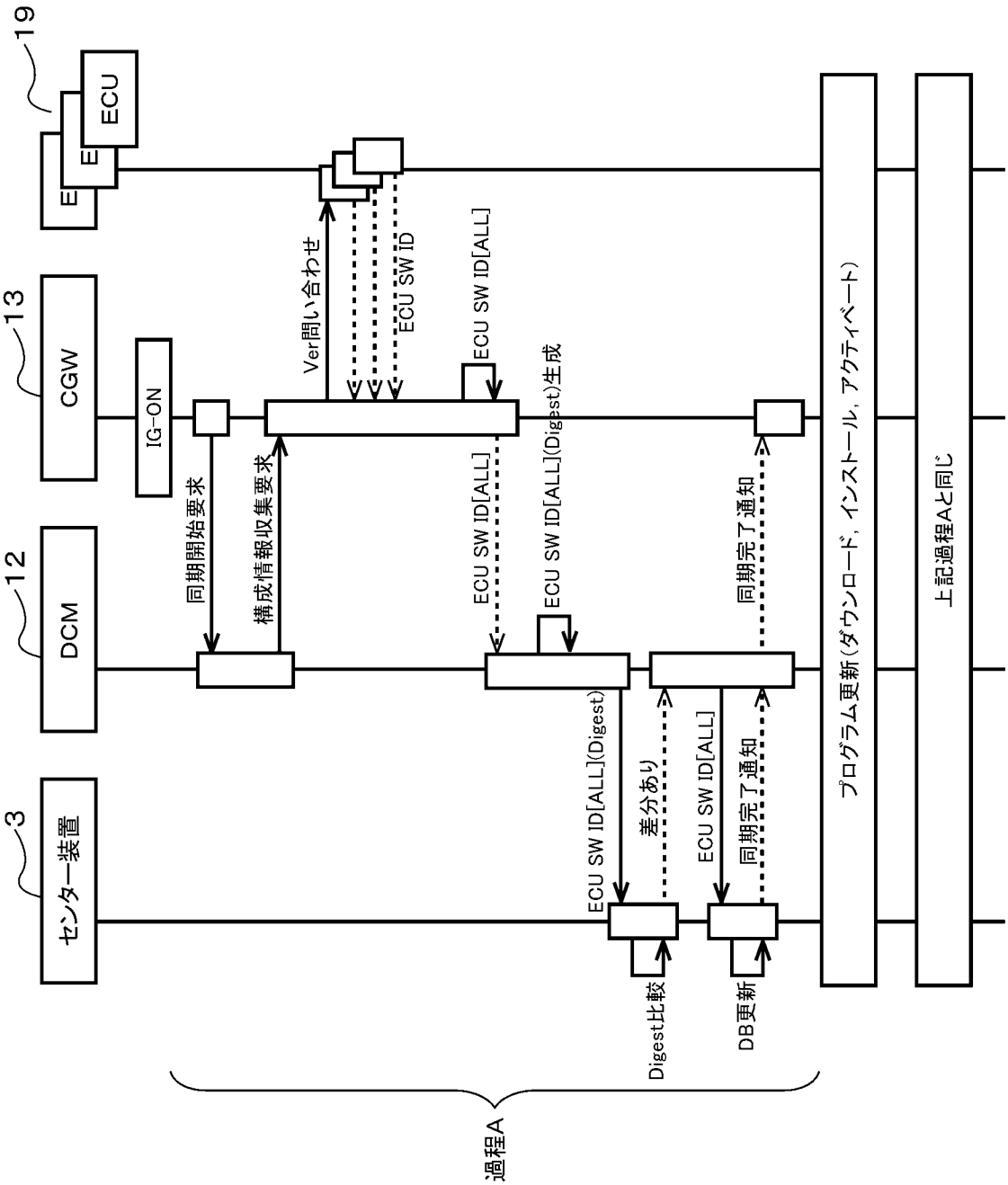
[図253]

Fig.253


C1,C2
リプログデータ
更新データ(差分)
ロールバック
データ(差分)
更新データ(差分)
に対する
完全性検証データ
ロールバック
データ(差分)
に対する
完全性検証データ
更新データ(フル)
に対する
完全性検証データ
EPS
BRK
ADS
諸元データ
C4
パッケージ
に対する
完全性検証データ
C3
パッケージファイル

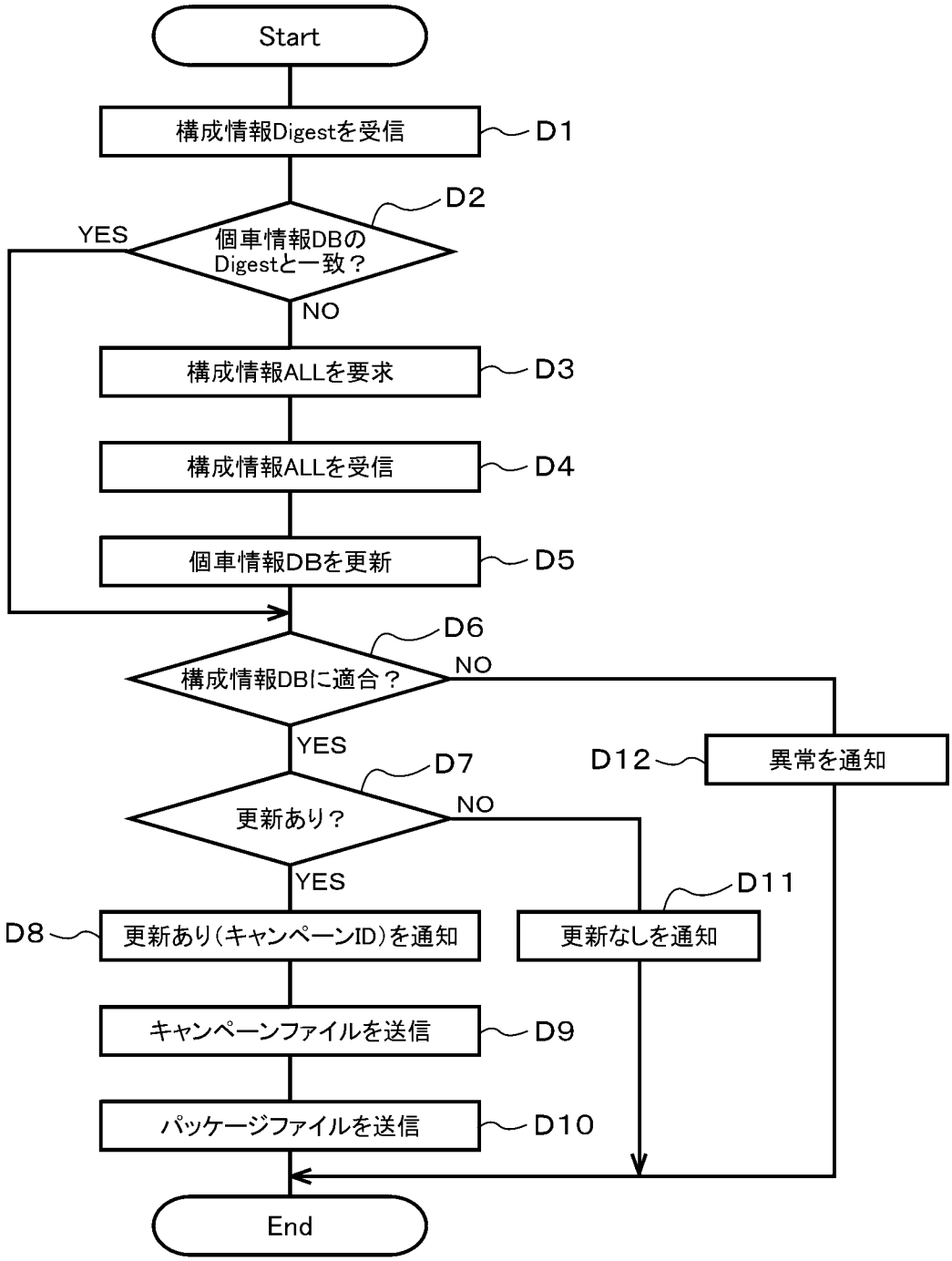
[図254]

Fig.254


19
ECU
E
E
13
CGW
IG-ON
12
DCM
3
センター装置
Ver問い合わせ
ECU SW ID
ECU SW ID[ALL]
ECU SW ID[ALL](Digest)生成
同期開始要求
構成情報収集要求
ECU SW ID[ALL]
ECU SW ID[ALL](Digest)
同期完了通知
ECU SW ID[ALL](Digest)
差分あり
ECU SW ID[ALL]
同期完了通知
Digest比較
DB更新
プログラム更新(ダウンロード, インストール, アクティベート)
上記過程Aと同じ
過程A

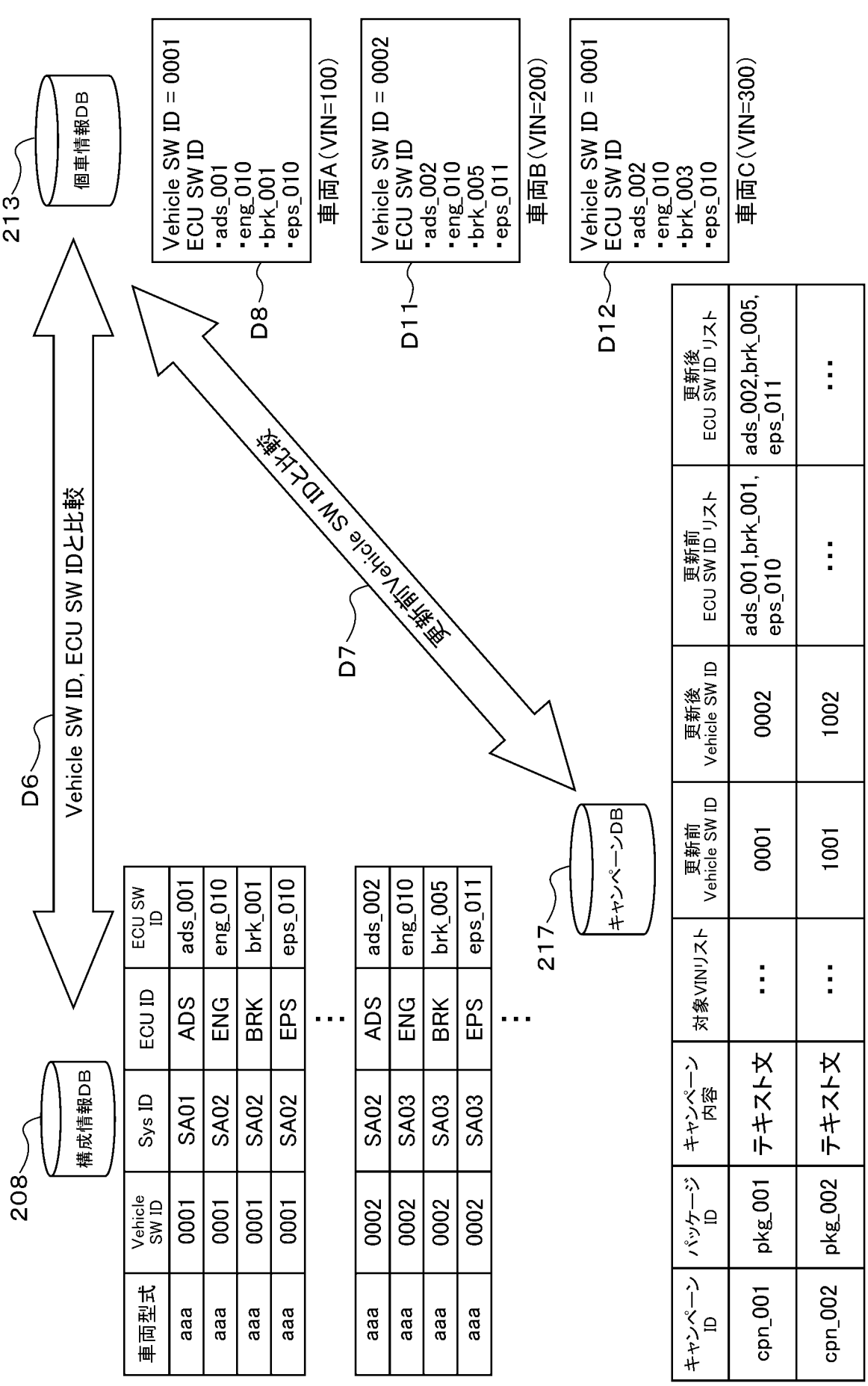
[図255]

Fig.255


Start
構成情報Digestを受信
D1
D2
個車情報DBの
Digestと一致？
YES
NO
構成情報ALLを要求
D3
構成情報ALLを受信
D4
個車情報DBを更新
D5
D6
構成情報DBに適合？
NO
YES
D12
異常を通知
D7
更新あり？
NO
YES
D11
D8
更新あり（キャンペーンID）を通知
更新なしを通知
キャンペーンファイルを送信
D9
パッケージファイルを送信
D10
End

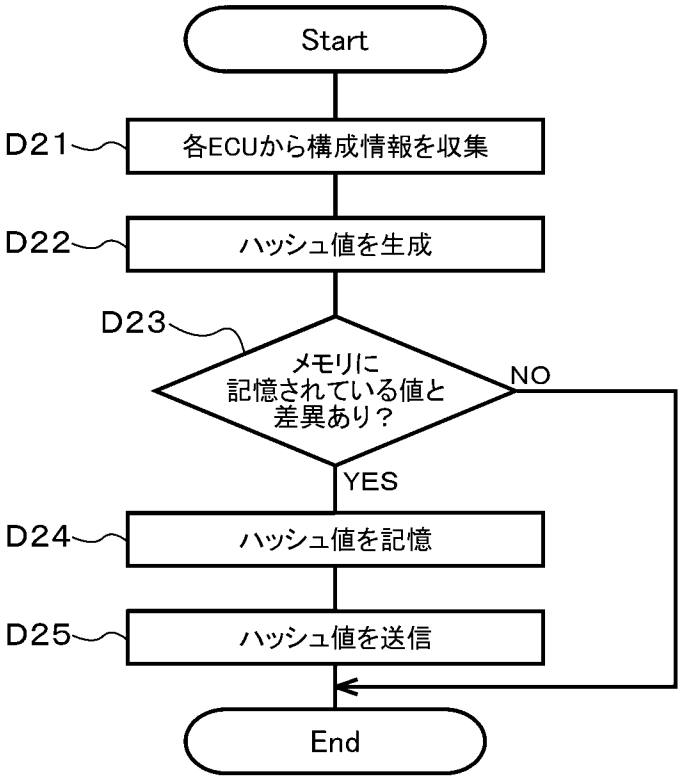
[図256]

Fig.256


213
個車情報DB
Vehicle SW ID = 0001
ECU SW ID
・ads_001
・eng_010
・brk_001
・eps_010
車両A（VIN=100）
D8
Vehicle SW ID = 0002
ECU SW ID
・ads_002
・eng_010
・brk_005
・eps_011
車両B（VIN=200）
D11
Vehicle SW ID = 0001
ECU SW ID
・ads_002
・eng_010
・brk_003
・eps_010
車両C（VIN=300）
D12
D6
Vehicle SW ID, ECU SW IDと比較
D7
更新前Vehicle SW IDと比較
208
構成情報DB
217
キャンペーンDB
車両型式
Vehicle SW ID
Sys ID
ECU ID
ECU SW ID
aaa 0001 SA01 ADS ads_001
aaa 0001 SA02 ENG eng_010
aaa 0001 SA02 BRK brk_001
aaa 0001 SA02 EPS eps_010
aaa 0002 SA02 ADS ads_002
aaa 0002 SA03 ENG eng_010
aaa 0002 SA03 BRK brk_005
aaa 0002 SA03 EPS eps_011
キャンペーンID
パッケージID
キャンペーン内容
対象VINリスト
更新前Vehicle SW ID
更新後Vehicle SW ID
更新前ECU SW IDリスト
更新後ECU SW IDリスト
cpn_001 pkg_001 テキスト文 ・・・ 0001 0002 ads_001,brk_001, eps_010 ads_002,brk_005, eps_011
cpn_002 pkg_002 テキスト文 ・・・ 1001 1002 ・・・ ・・・

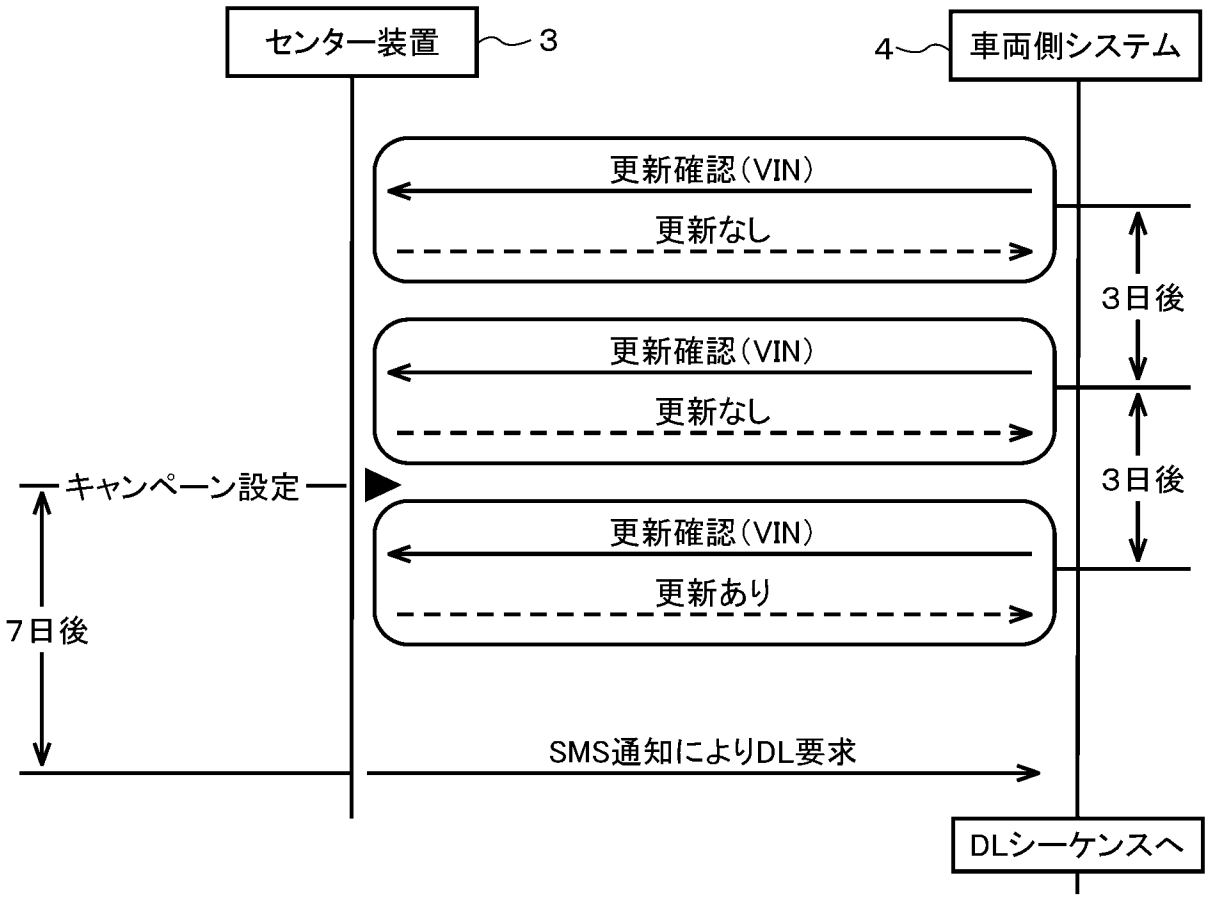
[図257]

Fig.257


Start
D21
各ECUから構成情報を収集
D22
ハッシュ値を生成
D23
メモリに
記憶されている値と
差異あり？
NO
YES
D24
ハッシュ値を記憶
D25
ハッシュ値を送信
End

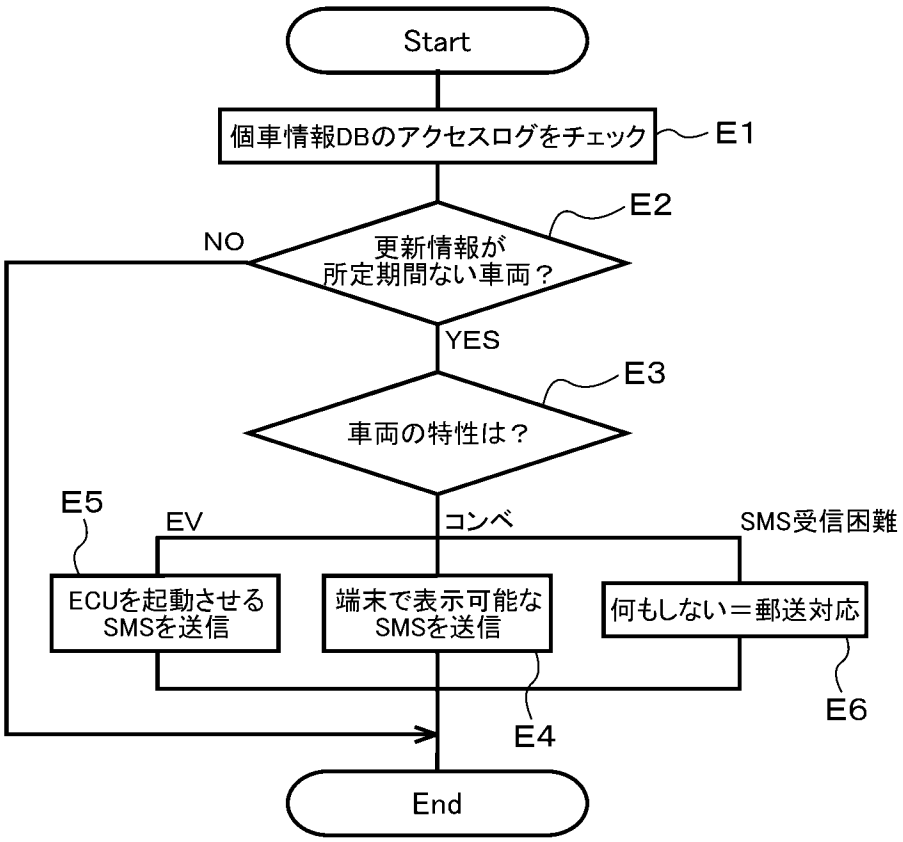
[図258]

Fig.258


センター装置
3
4
車両側システム
更新確認（VIN）
更新なし
3日後
更新確認（VIN）
更新なし
3日後
キャンペーン設定
更新確認（VIN）
更新あり
7日後
SMS通知によりDL要求
DLシーケンスへ

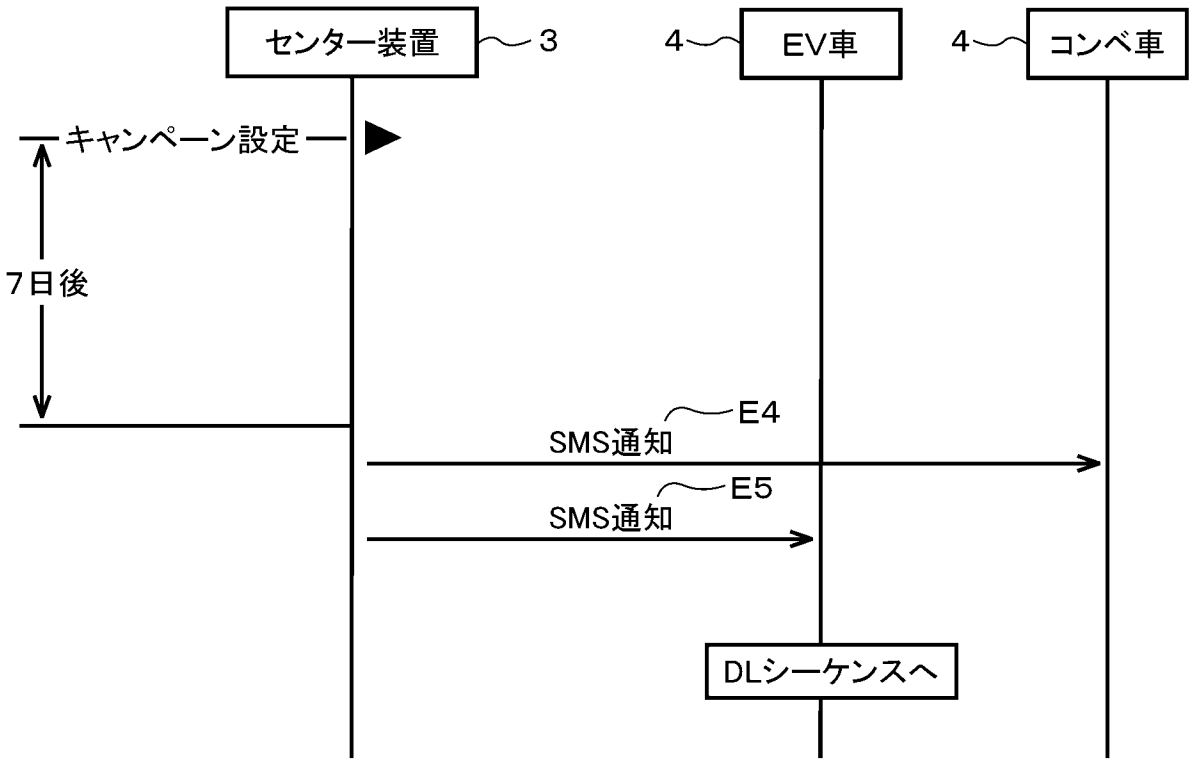
[図259]

Fig.259



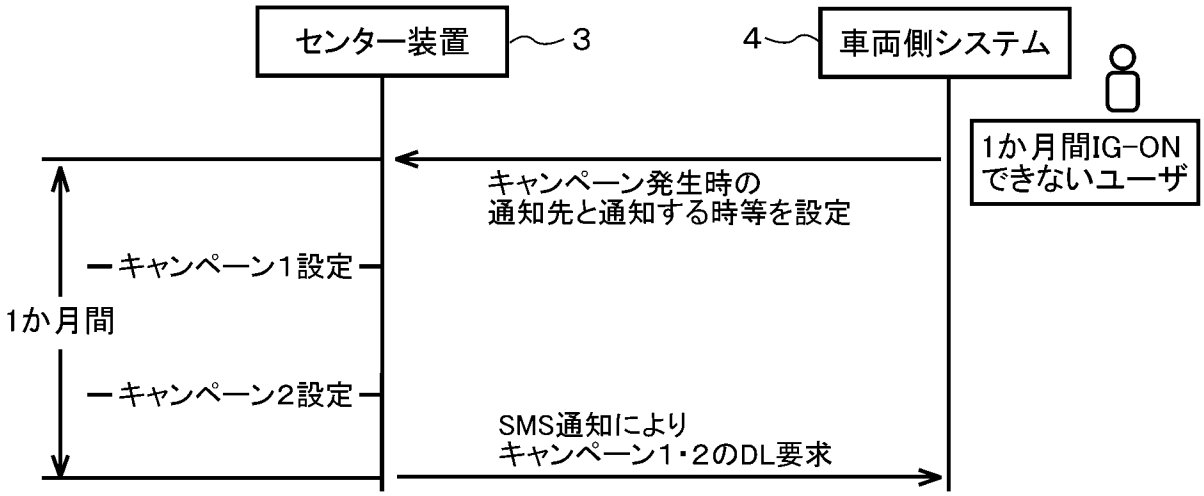
[図260]

Fig.260



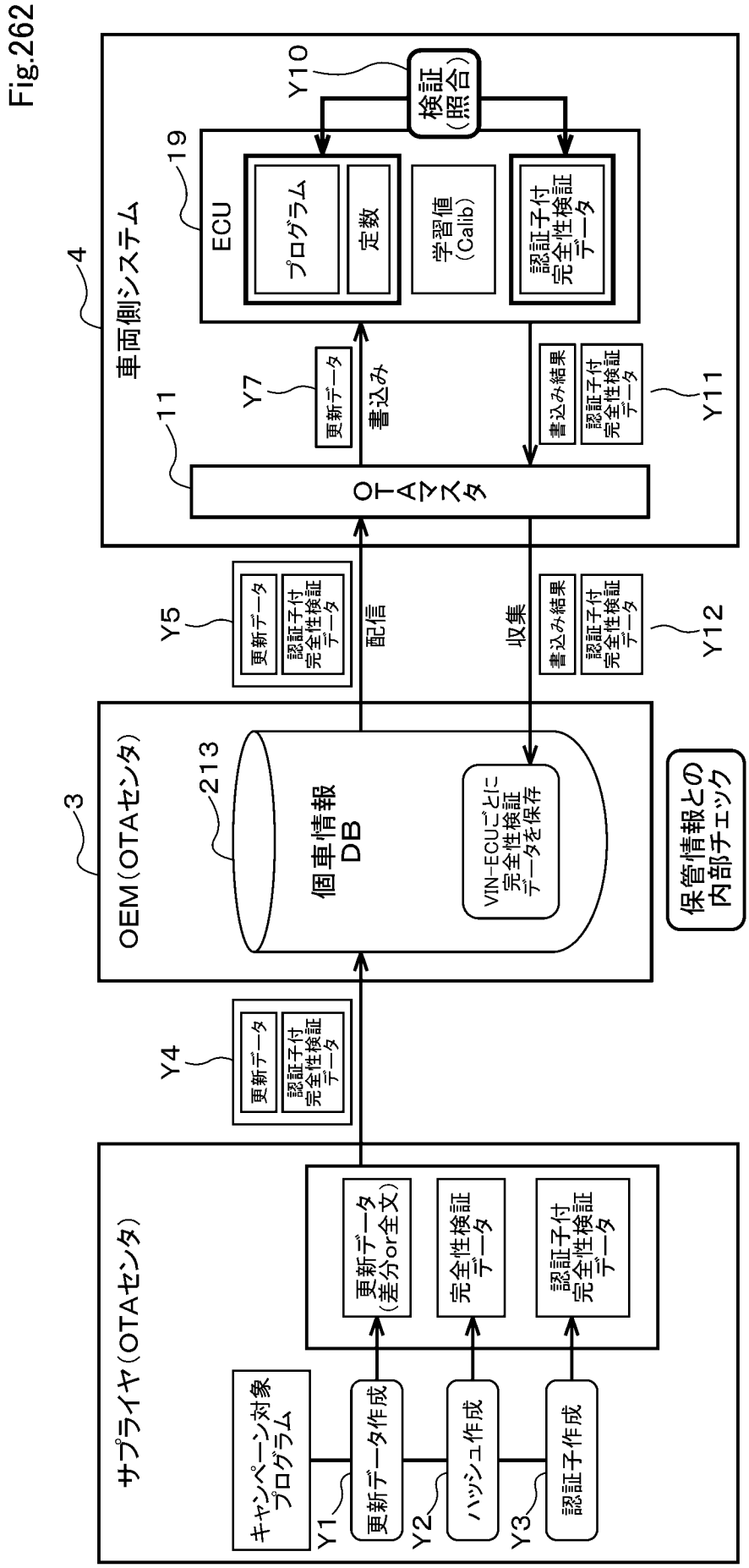
[図261]

Fig.261


センター装置
3
4
車両側システム
1か月間IG-ON
できないユーザ
キャンペーン発生時の
通知先と通知する時等を設定
キャンペーン1設定
1か月間
キャンペーン2設定
SMS通知により
キャンペーン1・2のDL要求

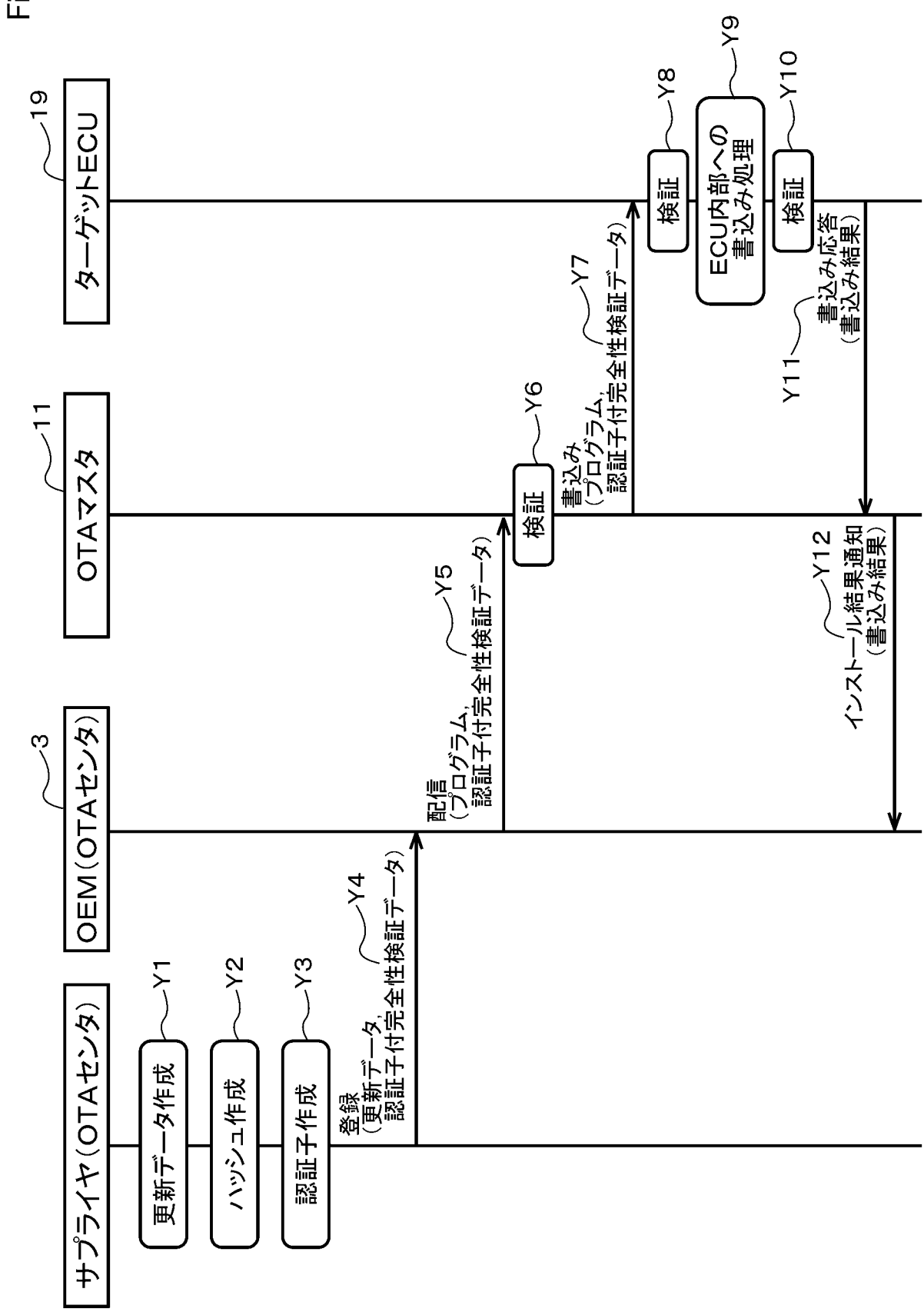
[図262]

Fig.262


サプライヤ(OTAセンタ)
キャンペーン対象プログラム
更新データ作成
ハッシュ作成
認証子作成
更新データ(差分or全文)
完全性検証データ
認証子付完全性検証データ
Y1
Y2
Y3
Y4
Y5
Y10
Y11
Y12
OEM(OTAセンタ)
3
213
個車情報DB
VIN-ECUごとに完全性検証データを保存
保管情報との内部チェック
配信
収集
更新データ
認証子付完全性検証データ
書込み結果
車両側システム
4
11
OTAマスタ
Y7
書込み
19
ECU
プログラム
定数
学習値(Calib)
検証(照合)

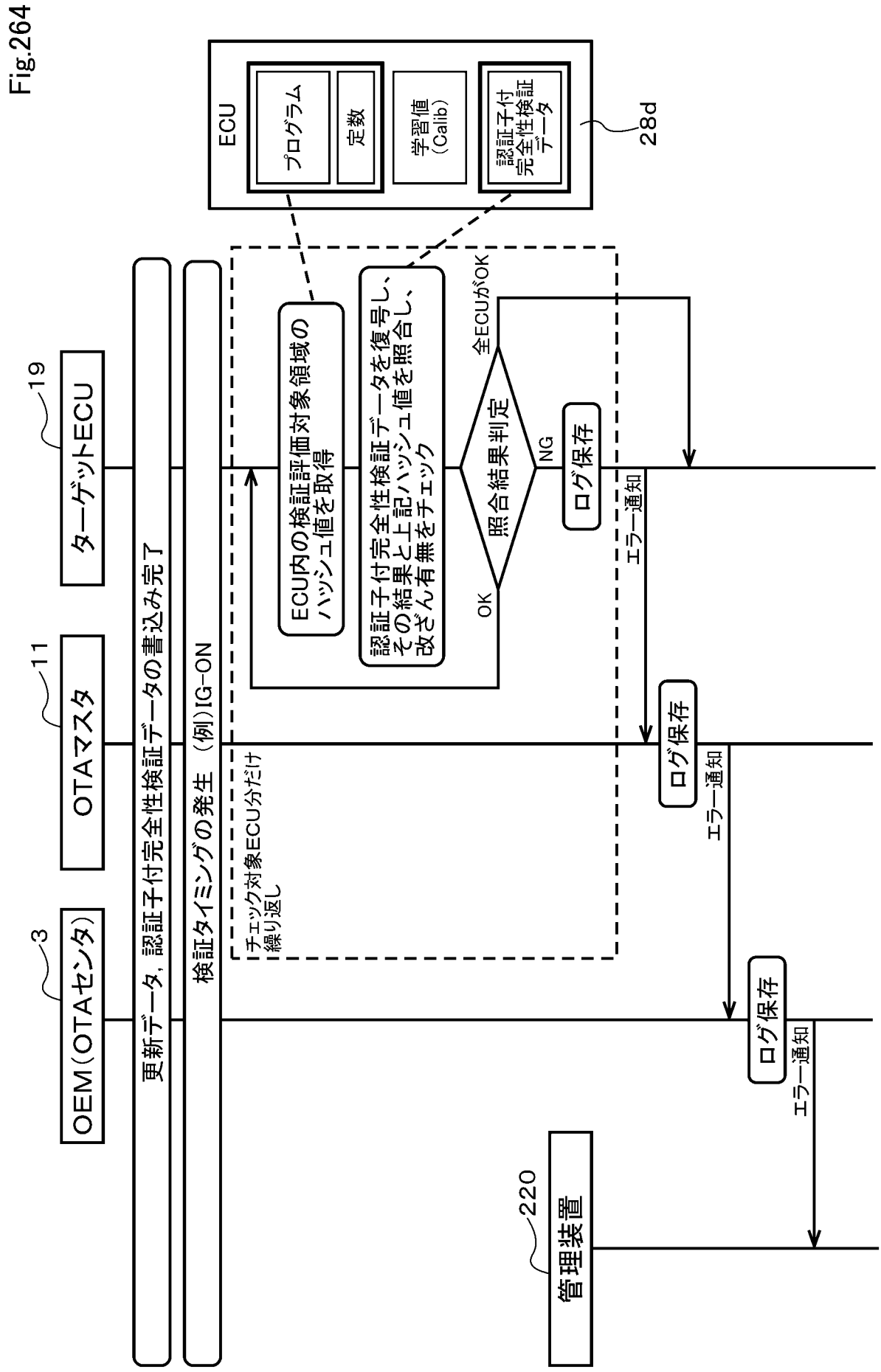
[図263]

Fig.263


サプライヤ（OTAセンタ）
OEM（OTAセンタ）
3
OTAマスタ
11
ターゲットECU
19
更新データ作成
Y1
ハッシュ作成
Y2
認証子作成
Y3
登録
（更新データ，
認証子付完全性検証データ）
Y4
配信
（プログラム，
認証子付完全性検証データ）
Y5
検証
Y6
書込み
（プログラム，
認証子付完全性検証データ）
Y7
検証
Y8
ECU内部への
書込み処理
Y9
検証
Y10
書込み応答
（書込み結果）
Y11
インストール結果通知
（書込み結果）
Y12

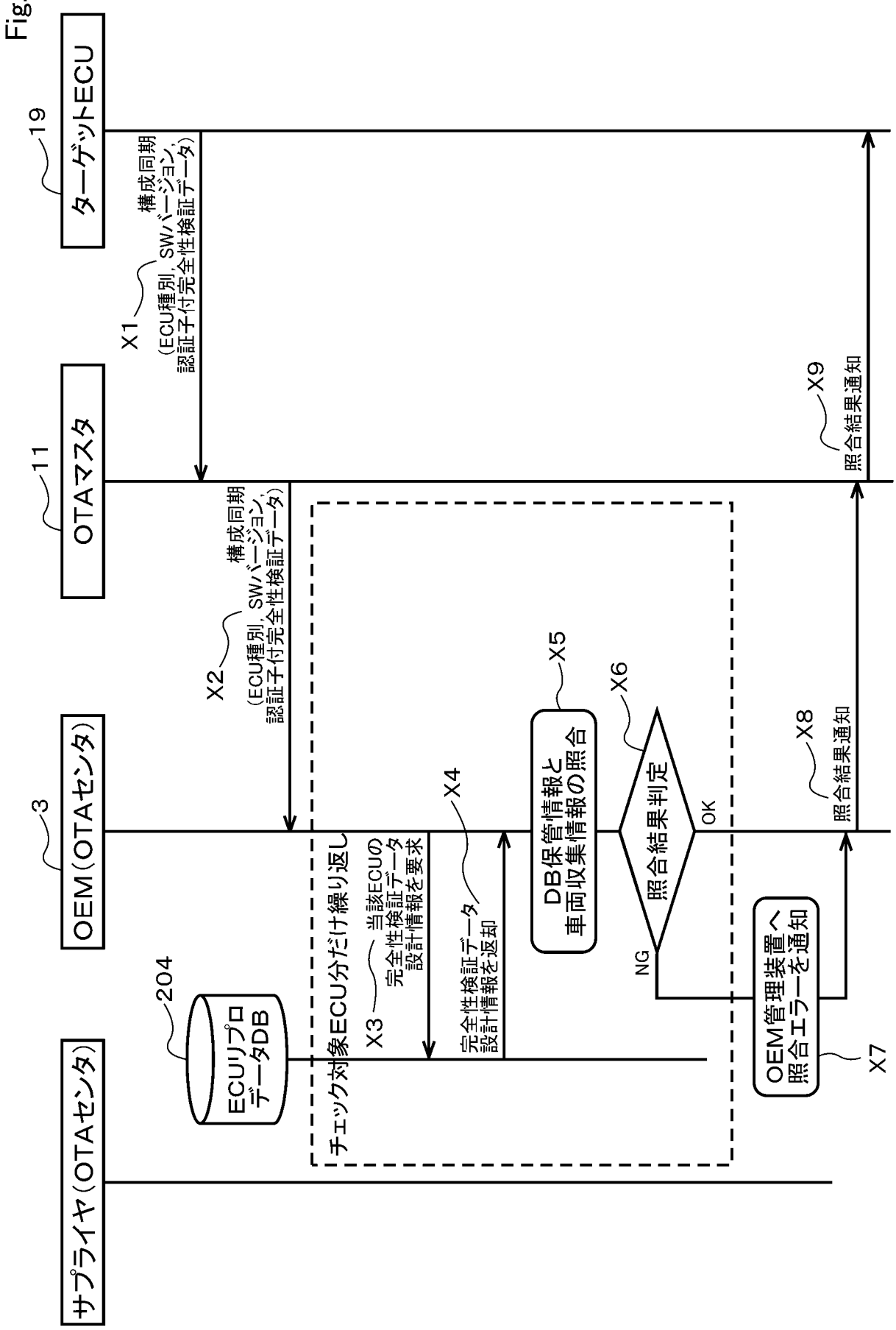
[図264]

Fig.264


ECU
プログラム
定数
学習値
(Calib)
認証子付
完全性検証
データ
28d
19
ターゲットECU
11
OTAマスタ
3
OEM(OTAセンタ)
更新データ，認証子付完全性検証データの書込み完了
検証タイミングの発生 （例）IG-ON
チェック対象ECU分だけ
繰り返し
ECU内の検証評価対象領域の
ハッシュ値を取得
認証子付完全性検証データを復号し、
その結果と上記ハッシュ値を照合し、
改ざん有無をチェック
照合結果判定
全ECUがOK
OK
NG
ログ保存
エラー通知
ログ保存
エラー通知
ログ保存
エラー通知
220
管理装置

[図265]

Fig.265


サプライヤ（OTAセンタ）
OEM（OTAセンタ）
OTAマスタ
ターゲットECU
3
11
19
204
ECUリプロデータDB
X1
（ECU種別，SWバージョン，認証子付完全性検証データ）
構成同期
X2
（ECU種別，SWバージョン，認証子付完全性検証データ）
構成同期
チェック対象ECU分だけ繰り返し
X3
当該ECUの完全性検証データ設計情報を要求
X4
完全性検証データ設計情報を返却
X5
DB保管情報と車両収集情報の照合
X6
照合結果判定
OK
NG
X7
OEM管理装置へ照合エラーを通知
X8
照合結果通知
X9
照合結果通知

[図266]

Fig.266

パッケージID	ファイル	完全性検証データ
pkg_001_1	pkg001_1.dat	xx1_1.dat
pkg_001_2	pkg001_2.dat	xx1_2.dat
pkg_002	pkg002.dat	xx2.dat

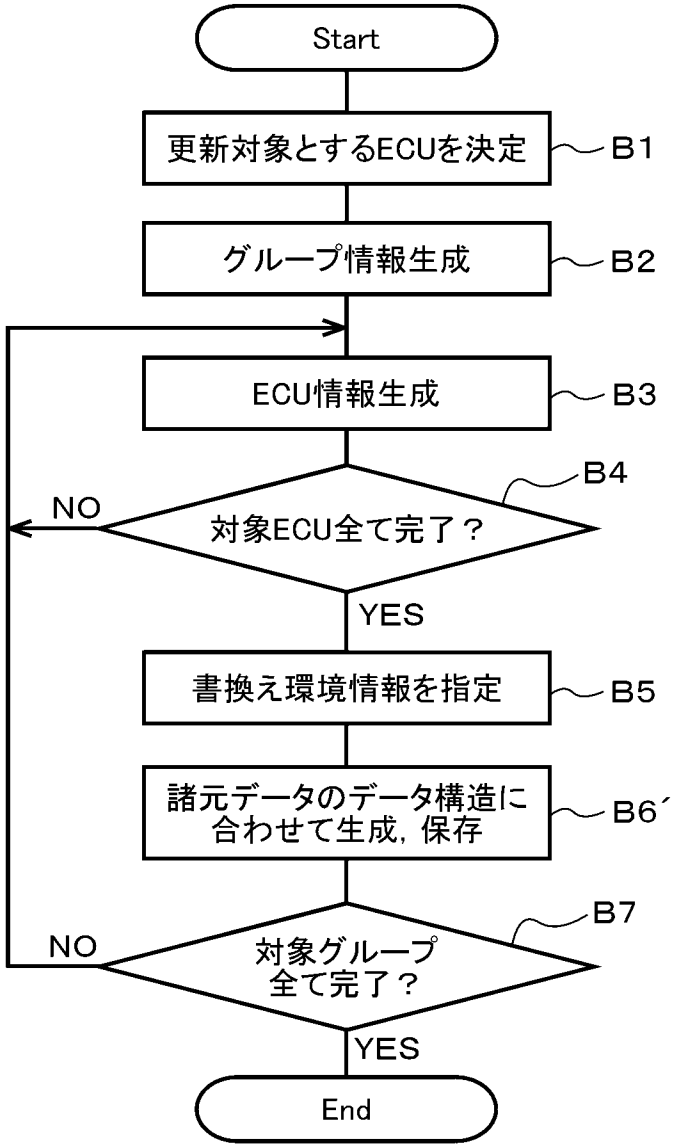
[図267]

Fig.267

キャンペーンID	パッケージID	キャンペーン内容	対象VINリスト	更新前 Vehicle SW ID	更新後 Vehicle SW ID	更新前 ECU SW ID リスト	更新後 ECU SW ID リスト
cpn_001	pkg_001_1 pkg_001_2	テキスト文	・・・	0001	0002	ads_001,brk_001, eps_010,・・・	ads_002,brk_005, eps_011,・・・
cpn_002	pkg_002	テキスト文	・・・	1001	1002	・・・	・・・

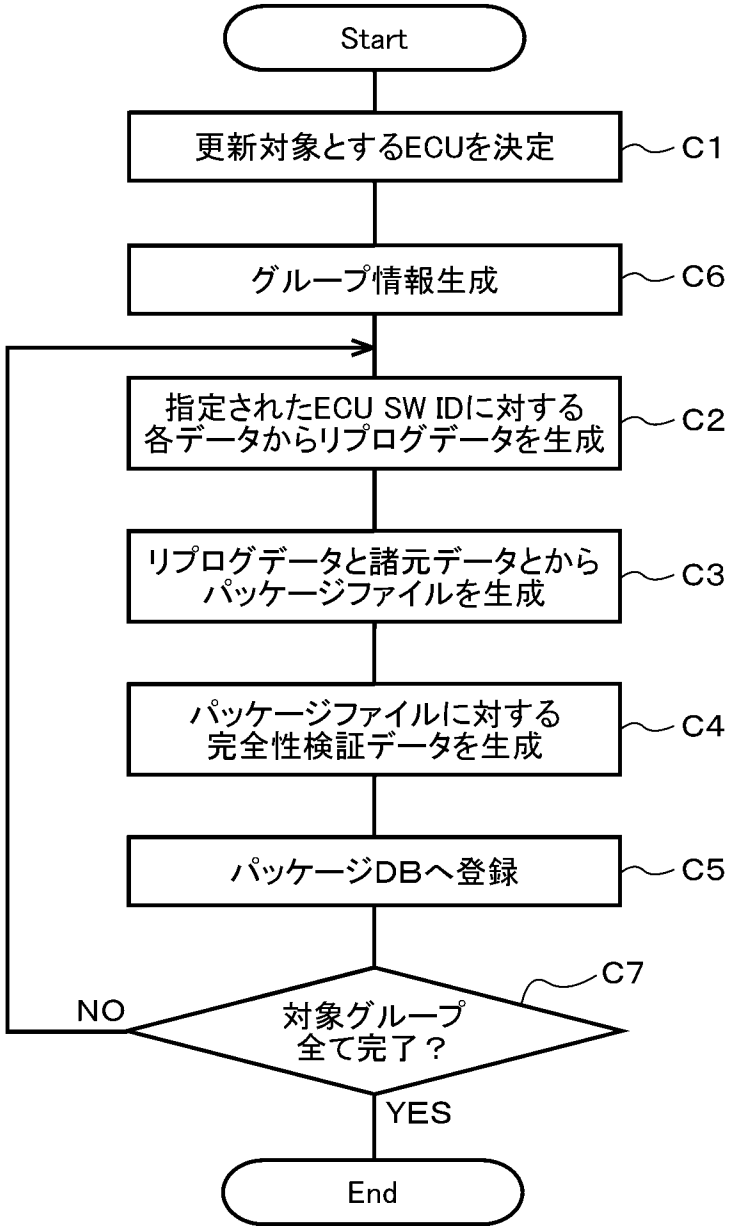
[図268]

Fig.268


Start
更新対象とするECUを決定
B1
グループ情報生成
B2
ECU情報生成
B3
B4
NO
対象ECU全て完了？
YES
書換え環境情報を指定
B5
諸元データのデータ構造に
合わせて生成，保存
B6´
B7
NO
対象グループ
全て完了？
YES
End

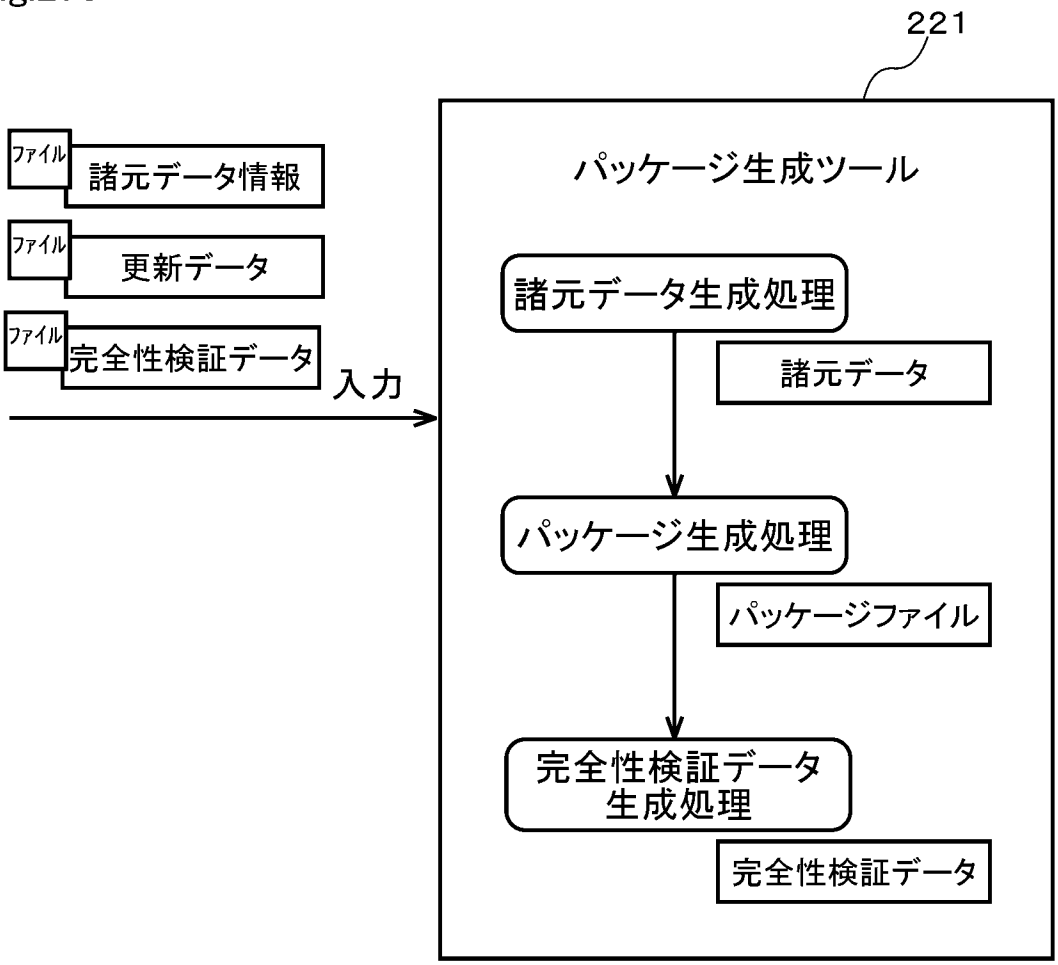
[図269]

Fig.269


Start
更新対象とするECUを決定
C1
グループ情報生成
C6
指定されたECU SW IDに対する
各データからリプログデータを生成
C2
リプログデータと諸元データとから
パッケージファイルを生成
C3
パッケージファイルに対する
完全性検証データを生成
C4
パッケージDBへ登録
C5
C7
NO
対象グループ
全て完了？
YES
End

[図270]

Fig.270


221
ファイル
諸元データ情報
ファイル
更新データ
ファイル
完全性検証データ
入力
パッケージ生成ツール
諸元データ生成処理
諸元データ
パッケージ生成処理
パッケージファイル
完全性検証データ
生成処理
完全性検証データ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/030944

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F8/65(2018.01)i, B60R16/02(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)
Int.Cl. G06F8/65, B60R16/02

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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.
X Y	JP 2005-349878 A (FUJITSU TEN LTD.) 22 December 2005, paragraphs [0072]-[0102], [0111]-[0132] (Family: none)	1, 7-8 2-6
Y	JP 2018-100002 A (AUTONETWORKS TECHNOLOGIES LTD.) 28 June 2018, paragraphs [0036]-[0046] & WO 2018/117016 A1	2-6
Y	WO 2012/017719 A1 (HONDA MOTOR CO., LTD.) 09 February 2012, paragraphs [0086]-[0089] & US 2013/0197712 A1, paragraphs [0114]-[0122] & EP 2602157 A1 & CN 103052539 A	2-6

☒ 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 30.08.2019	Date of mailing of the international search report 10.09.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/030944

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2017-220091 A (DENSO CORPORATION) 14 December 2017, paragraph [0046] & US 2019/0111907 A1, paragraph [0079] & CN 109313592 A	5-6

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０３０９４４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F8/65(2018.01)i, B60R16/02(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（ＩＰＣ））

Int.Cl.　G06F8/65, B60R16/02

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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
X Y	JP 2005-349878 A（富士通テン株式会社）2005.12.22, 段落[0072]-[0102],[0111]-[0132]（ファミリーなし）	1, 7-8 2-6
Y	JP 2018-100002 A（株式会社オートネットワーク技術研究所）2018.06.28, 段落[0036]-[0046] & WO 2018/117016 A1	2-6
Y	WO 2012/017719 A1（本田技研工業株式会社）2012.02.09, 段落[0086]-[0089] & US 2013/0197712 A1,段落[0114]-[0122] & EP 2602157 A1 & CN 103052539 A	2-6

☑　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	国際調査報告の発送日
３０．０８．２０１９	１０．０９．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｂ　３５６２
多胡　滋
電話番号　０３－３５８１－１１０１　内線　３５４５

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
Y	JP 2017-220091 A (株式会社デンソー) 2017.12.14, 段落[0046] & US 2019/0111907 A1,段落[0079] & CN 109313592 A	5-6