

(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)



(10) 国際公開番号

WO 2020/032044 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/JP2019/030945
- (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 2018-151416 2018年8月10日(10.08.2018) JP
特願 2019-129957 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).

(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,

(54) Title: VEHICLE MASTER DEVICE, INSTALLATION INSTRUCTION DETERMINATION METHOD, AND INSTALLATION INSTRUCTION DETERMINATION PROGRAM

(54) 発明の名称: 車両用マスタ装置、インストールの指示判定方法及びインストールの指示判定プログラム

Fig. 61

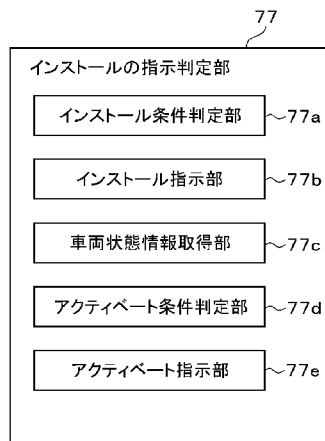


FIG. 61:

77 Installation instruction determination unit
77a Installation condition determination unit
77b Installation instruction unit
77c Vehicle state information acquisition unit
77d Activation condition determination unit
77e Activation instruction unit

(57) Abstract: A vehicle master device (11) is provided with: an installation condition determination unit (77a) for determining whether all of a first condition that a user consent relating to an installation is acquired, a second condition that data communication can be performed with a center device (3), a third condition that a vehicle is in an installation possible state, a fourth condition that a rewrite subject ECU (19) is in an installation possible state, and a fifth condition that update data is normal data are established or not; and an installation instruction unit (77b) for instructing the rewrite subject ECU to perform an installation using the update data in the case where the installation condition determination unit determines that all of the first condition, the second condition, the third condition, the fourth condition, and the fifth condition are established.

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：

- 一 国際調査報告（条約第21条(3)）

(57) 要約：車両用マスタ装置（11）は、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ECU（19）がインストール可能な状態である第4条件、更新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か否かを判定するインストール条件判定部（77a）と、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により判定された場合に、更新データを用いたインストールを書換え対象ECUに指示するインストール指示部（77b）と、を備える。

明 細 書

発明の名称：

車両用マスタ装置、インストールの指示判定方法及びインストールの指示判定プログラム

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2018-151416号及び2019年7月12日に出願された日本出願番号2019-129957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、車両用マスタ装置、インストールの指示判定方法及びインストールの指示判定プログラム

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（リプログラム）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抽出した更新データを書換え対象ECUに配信し、プログラムをインストールする。
- [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完了した後に、プログラムのインストールを書換え対象ECUに無条件に指示してしまう構成では、書換え対象ECUにおいてプログラムのインストールを正常に完了しない虞がある。書換え対象ECUにおいてプログラムのインストールを正常に完了しないと、車両動作に不具合を生じる虞がある。
- [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、書換え対象の電子制御装置に対して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車両用マスタ装置、インストールの指示判定方法及びインストールの指示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、外部から更新データを取得し、その取得した更新データを用いたインストールを書換え対象の電子制御装置に指示し、その取得した更新データを書換え対象の電子制御装置に配信する。インストール条件判定部は、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、書換え対象の電子制御装置がインストール可能な状態である第4条件、更新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か否かを判定する。インストール指示部は、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により判定されると、更新データを用いたインストールを書換え対象の電子制御装置に指示する。
- [0009] 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、書換え対象の電子制御装置がインストール可能な状態である第4条件、更新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、更新データを用いたインストールを書換え対象の電子制御装置に指示するようにした。書換え対象の電子制御装置に対して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。

図面の簡単な説明

- [0010] 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の電氣的な構成を示す図であり、
- [図3]図3は、DCMの電氣的な構成を示す図であり、
- [図4]図4は、ECUの電氣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、リプログラム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 1 5 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状態を示す図であり、

[図16]図 1 6 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状態を示す図であり、

[図17]図 1 7 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状態を示す図であり、

[図18]図 1 8 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状態を示す図であり、

[図19]図 1 9 は、組込み型の 2 面メモリにおける通常動作時の状態を示す図であり、

[図20]図 2 0 は、組込み型の 2 面メモリにおける書換え動作時の状態を示す図であり、

[図21]図 2 1 は、ダウンロード型の 2 面メモリにおける通常動作時の状態を示す図であり、

[図22]図 2 2 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状態を示す図であり、

[図23]図 2 3 は、アプリプログラムを書換える状態を示す図であり、

[図24]図 2 4 は、アプリプログラムを書換える状態を示す図であり、

[図25]図 2 5 は、アプリプログラムを書換える状態を示す図であり、

[図26]図 2 6 は、電源制御によりアプリプログラムを書換える状態を示すタイミングチャートであり、

[図27]図 2 7 は、電源制御によりアプリプログラムを書換える状態を示すタイミングチャートであり、

[図28]図 2 8 は、電源自己保持によりアプリプログラムを書換える状態を示すタイミングチャートであり、

[図29]図 2 9 は、電源自己保持によりアプリプログラムを書換える状態を示すタイミングチャートであり、

[図30]図 3 0 は、フェーズを示す図であり、

- [図31]図3 1は、通常時の画面を示す図であり、
- [図32]図3 2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3 3は、キャンペーン通知時の画面を示す図であり、
- [図34]図3 4は、ダウンロード承諾時の画面を示す図であり、
- [図35]図3 5は、ダウンロード承諾時の画面を示す図であり、
- [図36]図3 6は、ダウンロード実行中の画面を示す図であり、
- [図37]図3 7は、ダウンロード実行中の画面を示す図であり、
- [図38]図3 8は、ダウンロード完了時の画面を示す図であり、
- [図39]図3 9は、インストール承諾時の画面を示す図であり、
- [図40]図4 0は、インストール承諾時の画面を示す図であり、
- [図41]図4 1は、インストール実行中の画面を示す図であり、
- [図42]図4 2は、インストール実行中の画面を示す図であり、
- [図43]図4 3は、アクティベート承諾時の画面を示す図であり、
- [図44]図4 4は、I Gオン時の画面を示す図であり、
- [図45]図4 5は、確認操作時の画面を示す図であり、
- [図46]図4 6は、確認操作時の画面を示す図であり、
- [図47]図4 7は、センター装置の機能ブロック図であり、
- [図48]図4 8は、DCMの機能ブロック図であり、
- [図49]図4 9は、CGWの機能ブロック図であり、
- [図50]図5 0は、CGWの機能ブロック図であり、
- [図51]図5 1は、ECUの機能ブロック図であり、
- [図52]図5 2は、車載ディスプレイの機能ブロック図であり、
- [図53]図5 3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5 4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5 5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5 6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關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關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關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關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關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、バッテリー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、C GWが転送要求をD CMに送信する態様を示す図であり

、

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

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

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

[図98]図98は、E C U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E C U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 1 3 3 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 1 3 4 は、書換え進捗状況の画面を示す図であり、

[図135]図 1 3 5 は、書換え進捗状況の画面を示す図であり、

[図136]図 1 3 6 は、書換え進捗状況の画面を示す図であり、

[図137]図 1 3 7 は、書換え進捗状況の画面を示す図であり、

[図138]図 1 3 8 は、書換え進捗状況の画面を示す図であり、

[図139]図 1 3 9 は、進捗グラフ表示の遷移を示す図であり、

[図140]図 1 4 0 は、進捗グラフ表示の遷移を示す図であり、

[図141]図 1 4 1 は、進捗グラフ表示の遷移を示す図であり、

[図142]図 1 4 2 は、進捗グラフ表示の遷移を示す図であり、

[図143]図 1 4 3 は、書換え進捗状況の画面を示す図であり、

[図144]図 1 4 4 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 1 4 5 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 1 4 6 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 1 4 7 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 1 4 8 は、書換えの実行制御部の機能ブロック図であり、

[図149]図 1 4 9 は、通常動作処理を示すフローチャートであり、

[図150]図 1 5 0 は、書換え動作処理を示すフローチャートであり、

[図151]図 1 5 1 は、情報通知処理を示すフローチャートであり、

[図152]図 1 5 2 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 1 5 3 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 1 5 4 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 1 5 5 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 1 5 6 は、セッションの確立部の機能ブロック図であり、
- [図157]図 1 5 7 は、プログラムの構成を示す図であり、
- [図158]図 1 5 8 は、状態遷移を示す図であり、
- [図159]図 1 5 9 は、状態遷移を示す図であり、
- [図160]図 1 6 0 は、状態遷移を示す図であり、
- [図161]図 1 6 1 は、セッションの調停を示す図であり、
- [図162]図 1 6 2 は、セッションの調停を示す図であり、
- [図163]図 1 6 3 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 1 6 4 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 1 6 5 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 1 6 6 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 1 6 7 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 1 6 8 は、プログラムの構成を示す図であり、
- [図169]図 1 6 9 は、状態遷移を示す図であり、
- [図170]図 1 7 0 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 1 7 1 は、フラッシュメモリの構成を示す図であり、
- [図172]図 1 7 2 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 1 7 3 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 1 7 4 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 1 7 5 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 1 7 6 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 1 7 7 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 1 7 8 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 1 7 9 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 1 8 0 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 1 8 1 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 1 8 2 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 1 8 3 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 1 8 4 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 1 8 5 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 1 8 6 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 1 8 7 は、書換え諸元データを示す図であり、
- [図188]図 1 8 8 は、メニュー選択時の画面を示す図であり、
- [図189]図 1 8 9 は、ユーザ選択時の画面を示す図であり、
- [図190]図 1 9 0 は、ユーザ登録時の画面を示す図であり、
- [図191]図 1 9 1 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 1 9 2 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 1 9 3 は、メッセージフレームを示す図であり、
- [図194]図 1 9 4 は、アクティベート承諾時の画面を示す図であり、
- [図195]図 1 9 5 は、項目の表示有無の設定を示す図であり、
- [図196]図 1 9 6 は、項目の表示有無の設定を示す図であり、
- [図197]図 1 9 7 は、アクティベート承諾時の画面を示す図であり、
- [図198]図 1 9 8 は、データ通信の態様を示す図であり、
- [図199]図 1 9 9 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 2 0 0 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の電氣的な構成を示す図であり、

[図236]図236は、ECUの電氣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部を示す図であり、

[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部を示す図であり、

[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部を示す図であり、

[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部を示す図であり、

[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部を生成する処理を示すフローチャートであり、

[図250]図 2 5 0 は、諸元データの一例を示す図であり、

[図251]図 2 5 1 は、バス負荷テーブルの一例を示す図であり、

[図252]図 2 5 2 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 2 5 3 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 2 5 4 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 2 5 5 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 2 5 6 は、図 2 4 8 に示すフローチャートのステップD 6, D 7で行う処理内容をイメージ的に示す図であり、

[図257]図 2 5 7 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 2 5 8 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 2 5 9 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 2 6 0 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 2 6 1 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 2 6 2 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 2 6 3 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 2 6 4 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 2 6 5 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

[0011] 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。

[0012] 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。

[0013] 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。

[0014] 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であっても良いし、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。

[0015] 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。

[0016] 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。

- [0017] 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。
- [0018] 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。
- [0019] 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。
- [0020] 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。

[0021] 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。

[0022] 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。

[0023] 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。

[0024] 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。

[0025] 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。

[0026] 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とがイーサネットにより接続されても良い。

[0027] 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ラ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ラブとして機能する。

[0028] 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。

[0029] 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。

[0030] 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。

[0031] 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。

[0032] 図2に示すように、CGW13は、電氣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。

[0033] 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、バッテリー電源（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。

[0034] 図3に示すように、DCM12は、電氣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、CPU 28a と、ROM 28b と、RAM 28c 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。

[0035] 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 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。

[0036] 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。

[0037] 図 4 に示すように、ECU19 は、電氣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。

[0038] 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。

[0039] 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。

[0040] 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、車両バッテリー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ー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、車両バッテリー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。

[0041] I G電源ライン39は、I Gスイッチ42を介して車両バッテリー40の正極に接続されている。ユーザがI G操作を行うと、I Gスイッチ42がオフからオンに切替わり、車両バッテリー40の出力電圧がI G電源ライン39に印加される。I G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」位置に回転する操作であり、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。車両バッテリー40の負極は接地されている。

[0042] ACCスイッチ41とI G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、I G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I G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I G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I G電源とが車両側システム4に供給されている状態をI G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。

[0043] 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、I G電源状態で起動するI G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、I G系ECUに区分される。

[0044] +B電源系ECUは、+B電源ライン37、ACC電源ライン38及びI G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。

[0045] 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。

[0046] 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。

[0047] 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と車両バッテリー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と車両バッテリー40の正極を電源制御回路43の内部で途絶させる。

[0048] DCM12、CGW13、ECU19、電源管理ECU20は、それぞれ電源自己保持回路を有し、車両バッテリー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、車両バッテリー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。

[0049] 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ラムデータが生成されている場合を例示している。

[0050] 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ラムデータに含まれていても良い。

[0051] 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、CGW13、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。

[0052] 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。

[0053] 図8に示すように、C GW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、バッテリー負荷と、書換え時の車両状態と、ECU情報とを含む。C GW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も良い。グループ情報は、書換え対象ECU 19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。バッテリー負荷は、車両において許容可能な車両バッテリー40のバッテリー残量の下限值を示す情報である。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。

[0054] ECU情報は、書換え対象ECU 19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。

[0055] 接続バスは、ECU 19が接続されるバスを示す。接続電源は、ECU 19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、C GW 13が書換え対象ECU 19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

メモリ種別は、書換え対象E C U 1 9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。

[0056] 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。

[0057] D C M 1 2 は、D C M用の書換え諸元データを取得すると、その取得したD C M用の書換え諸元データを解析する。D C M 1 2 は、D C M用の書換え諸元データを解析すると、書換え対象E C U 1 9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C G W 1 3に転送する等の書換えに関与する動作を制御する。

[0058] C G W 1 3 は、C G W用の書換え諸元データを取得すると、その取得したC G W用の書換え諸元データを解析する。C G W 1 3 は、C G W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E C U 1 9の更新プログラムの所定サイズ分の転送をD C M 1 2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E C U 1 9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。

[0059] 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、O

ＥＭ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。

[0060] 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。

[0061] 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。

[0062] 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、アンパッキングとも称する）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。

[0063] 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。

[0064] 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、I G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。

[0065] 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。

[0066] 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。

[0067] 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。

[0068] 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には、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 3 3 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み出し、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、その読み出した旧データと、RAM 3 3 c 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 3 3 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き込んでアプリプログラムを書換える。

[0069] (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 1 3 及び図 1 4 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 に示したリログデータの中に、各 ECU 1 9 で実行する無線リプログファームウェアを含めておく。ECU 1 9 は、CGW 1 3 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。

[0070] 図 1 3 に示すように、マイコン 3 3 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。

[0071] 図 1 4 に示すように、マイコン 3 3 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 3 3 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み出し、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、その読み出した旧データと、RAM 3 3 c 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 3 3 は、旧データと差分データから新データを生成すると、その新データを書き込んでアプリプログラムを書換える。

[0072] (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。

[0073] 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。

[0074] 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み出し、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、その読み出した旧データと、

RAM 33c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。

[0075] (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、リプログラムウェアとリプログラム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、そのリプログラムウェアとリプログラム時ベクタテーブルを削除する点で異なる。

[0076] 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。

[0077] 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りプログラ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、RAM 33c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

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。

[0078] (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。

[0079] 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。

[0080] 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み出し、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、その読み出した旧データと、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、新データの書き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。

[0081] (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。

[0082] 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。

[0083] 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み出し、その読み出した旧データと、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。

[0084] 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ログ対象として示したが、書換えプログラムもリ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。

[0085] 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。

[0086] 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。

[0087] 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。

[0088] 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。

[0089] 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。

[0090] 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。

[0091] 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 (B 1)。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 (B 2)。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。

[0092] 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 (A 3)。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。

[0093] 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 (A 4)、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 (A 5)、書換え指示信号をマスタ装置 11 に送信する。

[0094] 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 ECU 20 に送信し、書換え対象 ECU (ID 1)、書換え対象 ECU (ID 2)、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 (X 1)。

[0095] マスタ装置 11 は、書換え対象 ECU (ID 1) 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 (ID 1) に指示する。書換え対象 ECU (ID 1) 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（C 1）。書換え対象E C U（I D 1）は、マスタ装置1 1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1 1に送信する。

[0096] マスタ装置1 1は、書換え対象E C U（I D 1）から書換え完了通知信号を受信すると、書換え対象E C U（I D 2）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E C U（I D 2）に指示する。書換え対象E C U（I D 2）は、マスタ装置1 1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（D 1）。書換え対象E C U（I D 2）は、マスタ装置1 1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1 1に送信する。マスタ装置1 1は、書換え対象E C U（I D 2）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。

[0097] センター装置3は、マスタ装置1 1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（A 6）。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。

[0098] ユーザが同期の実施を携帯端末6において設定すると（A 7）、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1 1に送信する。マスタ装置1 1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E C U（I D 1）及び書換え対象E C U（I D 2）に配信する。

- [0099] 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。
- [0100] 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。
- [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）。
- [0102] 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（A 8）。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。

[0103] 次に、アプリプログラムを書換える場合における DCM 1 2、CGW 1 3、書換え対象 ECU 1 9 の動作のタイミングチャートについて図 2 6 から図 2 9 を参照して説明する。尚、ここでは、ユーザ操作により I G スイッチ 4 2 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 I G スイッチ 4 2 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。

[0104] （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 2 6 及び図 2 7 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 I G 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 I G 電源に切替わると、DCM 1 2、CGW 1 3、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（t 1）。

[0105] DCM 1 2 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（t 2）。DCM 1 2 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。DCM 1 2 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 3）。

[0106] DCM 1 2 は、センター装置 3 又は CGW 1 3 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（t 4）。即ち、DCM 1 2は、配信パッケージから書込みデータを抽出し、CGW 1 3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CGW 1 3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。

[0107] CGW 1 3は、DCM 1 2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ラマスタ動作に移行し、リプログラ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、CGW 1 3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。

[0108] 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、DCM 1 2は、データ転送／センター通信動作を中断し、CGW 1 3は、リプログラ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（t 5）。

[0109] 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、DCM 1 2は、データ転送／センター通信動作を再開し、CGW 1 3は、リプログラ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（t 6）。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（t 7, t 8）。

[0110] 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（t 9）。

[0111] 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（t 10）、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、リプログラムスタ動作を再開し、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（t 11）。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。

[0112] 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

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。

[0113] 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）。

[0114] 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。

[0115] 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、リプログラ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）。

[0116] 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（t 1 6）。

[0117] （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 2 8 及び図 2 9 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 I G 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 I G 電源に切替わると、DCM 1 2、CGW 1 3、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（t 2 1）。

[0118] DCM 1 2 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（t 2 2）。DCM 1 2 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 2 3）。

[0119] DCM 1 2 は、センター装置 3 又は CGW 1 3 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（t 2 4）。即ち、DCM 1 2 は、配信パッケージから書込みデータを抽出し、CGW 1 3 への書込みデータの転送を開始すると共に、書換の進捗状況を CGW 1 3 から取得し、センター装置 3 への書換の進捗状況の通知を開始する。

[0120] CGW 1 3 は、DCM 1 2 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ラマスタ動作に移行し、リプログラ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、CGW 1 3 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。

[0121] 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、リプログラ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、リプログラ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ー40からの電力供給によりインストールを継続する。

[0122] 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、リプログラ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、リプログラ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。

[0123] 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（t 3 1）。

[0124] 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（t 3 2）。

[0125] 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（t 3 3）。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する（t 3 4）。

[0126] 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（t 3 5）。

[0127] 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 (t 3 6, t 3 7)。

[0128] アクティベートが完了し、CGW 1 3からのアクティベート完了指示により電源管理 ECU 2 0が車両電源を I G 電源から + B 電源に切替えると、DCM 1 2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。CGW 1 3は、リプログラ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 (t 3 8)。

[0129] これ以降、ユーザが I G 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 I G 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 (t 3 9)。

[0130] CGW 1 3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 ECU 1 9に配信する前には、以下のチェックを行う。CGW 1 3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、車両バッテリー 4 0のバッテリー残量、DCM 1 2のメモリ容量のチェックを行う。CGW 1 3は、書込みデータの書換え対象 ECU 1 9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、I G オフの検知を行い、書換え対象 ECU 1 9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、CGW 1 3は、書換え対象 ECU 1 9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。

[0131] 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。

[0132] 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。

[0133] 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。

[0134] 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。

[0135] 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。

[0136] 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。

[0137] 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。

[0138] 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 506 a、「予約して更新」ボタン 506 b、「戻る」ボタン 506 c 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 506 a 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 506 b 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 506 c 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 506 c 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 501 b 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。

[0139] この状態からユーザが「すぐ更新」ボタン 506 a 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け、インストールを開始する旨をユーザに知らせる。

[0140] 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 501 c を表示させる。ユーザは、インストール実行中アイコン 501 c 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。

[0141] この状態からユーザがインストール実行中アイコン 501 c 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。

[0142] 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。

[0143] 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。

[0144] 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51

0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。

[0145] 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。

[0146] 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。

[0147] 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

[0148] 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。

[0149] 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 5 4 と、書込みデータ選定部 5 5（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 5 5（更新データ選定部に相当する）は、マスタ装置 1 1 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 5 1 は、書込みデータ選定部 5 5 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 DCM 1 2 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。

[0150] 図 4 8 に示すように、DCM 1 2 は、ダウンロード要求送信部 6 1 と、配信パッケージダウンロード部 6 2 と、書込みデータ抽出部 6 3 と、書込みデータ転送部 6 4 と、書換え諸元データ抽出部 6 5 と、書換え諸元データ転送部 6 6 とを有する。ダウンロード要求送信部 6 1 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 6 2 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 6 3 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 6 2 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。

[0151] 書込みデータ転送部 6 4 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 6 3 により抽出されると、その抽出された書込みデータを CGW 1 3 に転送する。書換え諸元データ抽出部 6 5 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 6 2 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 6 6 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 5 6 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 CGW 1 3 に転送する。DCM 1 2 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 6 7 と、書込みデータの転送判定部 6 8 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。

[0152] 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。

[0153] 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。

[0154] 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。

[0155] 図 5 2 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。

[0156] (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 5 3 及び図 5 4 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 5 5 及び図 5 6 を参照して説明する。

[0157] 図 5 3 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 とを有する。ソフトウェア情報取得部 52a は、車両側から各 ECU 19 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。

[0158] 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。

[0159] 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。

[0160] 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。

[0161] 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。

[0162] 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。

[0163] 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。

[0164] 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。

[0165] 以上に説明したように、センター装置 3 は、マスタ装置 1 1 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 1 1 に送信すべく、キャンペーン情報をマスタ装置 1 1 に送信することができる。

[0166] 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、ECU 1 9 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 1 1 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、ECU 1 9 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 1 1 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 1 1 に送信しないようすることができる。

[0167] 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 ECU 19 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。

[0168] 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、DCM 12 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、CGW 13 が DCM 12 の機能を有することで、CGW 13 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。

[0169] 図 55 に示すように、DCM 12 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、車両バッテリー 40 のバッテリー残量が所定容量以上であるか否か、DCM 12 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。

[0170] ダウンロード可能判定部67bは、電波環境が良好であり、車両バッテリー40のバッテリー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、車両バッテリー40のバッテリー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。

[0171] 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。

[0172] 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。

[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。

[0174] 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。

[0175] 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。

[0176] 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り配信パッケージをダウンロードすることができる。

[0177] 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、車両バッテリー 40 のバッテリー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、車両バッテリー４０のバッテリー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。

[0178] 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ー４０のバッテリー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。

[0179] 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。

[0180] 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。

[0181] 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。

[0182] (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キングされ、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。

[0183] 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DCM

12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。

[0184] 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。

[0185] 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。

[0186] 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。

[0187] 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、転送可否判定フラグが第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C G W 1 3に転送することができ、書換え対象E C U 1 9においてインストールを実行することができる。

[0188] 例えば書換え対象E C U 1 9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、D C M 1 2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、D C M 1 2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。

[0189] 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、C G W 1 3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D C M 1 2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C G W 1 3が行う判定処理である。

[0190] 図59に示すように、C G W 1 3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D C M 1 2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。

[0191] 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。

[0192] 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。

[0193] 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。

[0194] 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、取得可否判定フラグが第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。

[0195] 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。

[0196] 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)がアンパッキングされた状態とする。

[0197] 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。

[0198] 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。

[0199] 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

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。

[0200] 車両状態情報取得部 77c は、センタ装置 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 ECU 19 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 ECU 19 がアクティベート可能な状態である、という条件である。

[0201] 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 ECU 19 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 ECU 19 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 ECU 19 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 ECU 19 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 ECU 19 に指示せず、待機又はアクティベート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。

[0202] 次に、CGW 13 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。CGW 13 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。

[0203] 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。

[0204] 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ー40のバッテリー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ー40のバッテリー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。

[0205] 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。

[0206] 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。

[0207] 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。

[0208] 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）。

[0209] 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ECU19に指示する。

[0210] 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 (ID 2) に指示する。

[0211] 書換え対象 ECU 19 が ECU (ID 1)、ECU (ID 2) の場合、インストールを纏めて指示する態様では、CGW 13 は、図 64 に示すように、ECU (ID 1) 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、CGW 13 は、第 1 条件から第 3 条件と、ECU (ID 1) についての第 4 条件及び第 5 条件を判定する。CGW 13 は、ECU (ID 1) についてインストール条件が成立すると判定すると、ECU (ID 2) 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、CGW 13 は、ECU (ID 2) についての第 4 条件及び第 5 条件を判定する。CGW 13 は、ECU (ID 2) 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 (ID 1) 及び ECU (ID 2) に指示する。CGW 13 は、例えば ECU (ID 1) への書換えデータの転送と、ECU (ID 2) 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 CGW 13 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、CGW 13 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。

[0212] 以上に説明したように、CGW 13 は、インストールを書換え対象 ECU 19 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 ECU 19 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 ECU 19 に指示するようにした。書換え対象 ECU 19 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。

[0213] (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、CGW 13 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。

[0214] 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。

[0215] 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。

[0216] 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、ECU 19毎にユニークな鍵である。

[0217] 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、ECU 19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。

[0218] 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。

[0219] 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 78 a は、E C U 19 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 78 b は、C G W 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 E C U 19 の E C U（I D）に対応付けられて暗号化された値である。

[0220] 鍵パターン抽出部 78 c は、C G W 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 78 d は、C G W 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。

[0221] 鍵生成部 78 e は、乱数値が乱数値抽出部 78 b により抽出されると、セキュア領域 78 a を検索し、その抽出された乱数値を、セキュア領域 78 a 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 E C U（I D）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 78 e は、鍵導出値を、鍵パターン抽出部 78 c 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 78 d 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、C G W 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 78 e 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。

[0222] セキュリティアクセス実行部 78 f は、セキュリティアクセス鍵が鍵生成部 78 e 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 E C U 19 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 78 f は、例えばセキュリティアクセス鍵を用いて E C U（I D）を暗号化した暗号化データを送信し、書換え対象 E C U 19 にアクセスを要求する。書換え対象 E C U 19 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。

[0223] 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。

[0224] 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。

[0225] (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)。

[0226] 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（S 6 0 3、鍵生成手順に相当する）

[0227] C G W 1 3 は、図 6 8 示すように、C G W 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。C G W 1 3 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（S 6 0 4）、セキュリティアクセス鍵を用い、書換え対象 E C U 1 9 に対するセキュリティアクセスを実行する（S 6 0 5）、C G W 1 3 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 E C U 1 9 に配信し（S 6 0 6）、セッション維持要求を行う（S 6 0 7）。C G W 1 3 は、インストールを完了したと判定すると（S 6 0 8 : Y E S）、セキュリティアクセス鍵の生成処理を終了する。

[0228] （6 - 2）セキュリティアクセス鍵の消去処理

C G W 1 3 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 E C U 1 9 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（S 6 1 1）。C G W 1 3 は、書換え対象 E C U 1 9 のアプリプログラムの書換えを完了したと判定すると（S 6 1 1 : Y E S）、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（S 6 1 2）、セキュリティアクセス鍵の消去処理を終了する。

[0229] 以上に説明したように、C G W 1 3 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 E C U 1 9 に対応する乱数値を抽出し、その乱数値をセキュア領域 7 8 a に記憶されている書換え対象 E C U 1 9 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 C G W 1 3 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 E C U 1 9 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。

[0230] 尚、C G W 1 3 は、書換え対象 E C U 1 9 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。

[0231] 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。

[0232] 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。

[0233] (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。

[0234] 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。

[0235] 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。

[0236] 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 ECU 19 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 ECU 19 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。

[0237] 図 71 に示すように、CGW 13 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 ECU 19 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 ECU 19 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 DCM 12 に通知し、DCM 12 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 DCM 12 に通知する。処理結果取得部 68c は、DCM 12 から処理結果が通知されることで、DCM 12 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、CGW 13 は第 1 装置及び第 1 機能部に相当し、DCM 12 は第 2 装置及び第 2 機能部に相当する。

[0238] 次に、CGW 13 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。CGW 13 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。

[0239] 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）。

[0240] 以下、CGW13が処理実行要求をDCM12に通知する幾つの場合を例示する。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。

[0241] 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。

[0242] 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。

[0243] 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。

[0244] 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。

[0245] 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換え対象ECU(ID1)に配信し、ECU(ID2)の書込みデータの書換え対象ECU(ID2)に配信し、ECU(ID3)の書込みデータの書換え対象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。

[0246] 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換え対象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換え対象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換え対象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。

[0247] 以上に説明したように、C G W 1 3 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 D C M 1 2 に実行させるようにした。C G W 1 3 や書換え対象 E C U 1 9 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 E C U 1 9 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。

[0248] 図 7 4 に例示した C G W 1 3 が第 1 検証値算出処理を行う構成では、C G W 1 3 が鍵（キー値）を保持し、その鍵を D C M 1 2 に送信することなく検証処理を行うので、D C M 1 2 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 E C U 1 9 が複数の場合には、複数の書換え対象 E C U 1 9 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 E C U 1 9 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。

[0249] 尚、以上は、C G W 1 3 が処理実行要求を D C M 1 2 に通知する構成を例示したが、例えば D C M 1 2 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、D C M 1 2 に代えてナビゲーション装置や書換え対象 E C U 1 9 以外の E C U 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 E C U 1 9 以外の E C U に通知しても良い。又、D C M 1 2 と C G W 1 3 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 E C U 内で異なるソフトコンポーネント間で行っても良い。又、D C M 1 2 及び C G W 1 3 の機能を有する 1 つの統合 E C U として構成されるマスタ装置 1 1 に対し、上述の構成を適用しても良い。例えば図 7 3 から図 7 6 において、C G W 1 3 における処理機能を第 1 機能部、D C M 1 2 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 E C U 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 ECU 19 以外の ECU に処理実行要求を通知しても良い。

[0250] 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。

[0251] 尚、セキュリティアクセスが CGW 13 と書換え対象 ECU 19 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。

[0252] 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、CGW 13 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 ECU 19 に配信する直前に検証すると良い。

[0253] （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、CGW 13 においてデータ格納面情報の送信制御処理を行う。

[0254] 図 79 に示すように、CGW 13 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。

[0255] 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。

[0256] 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。

[0257] 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。

- [0258] 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。
- [0259] 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。
- [0260] 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)。

[0261] 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。

[0262] 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。

[0263] 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)。

[0264] 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。

[0265] 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(

S 8 0 7 : Y E S)、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(S 8 0 9)、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。

[0266] 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。

[0267] 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。

[0268] 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。

[0269] 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。

[0270] 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。

[0271] 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。

[0272] 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る、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。

[0273] 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。

[0274] 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。

[0275] 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。

[0276] 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。

[0277] （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。

[0278] 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。

[0279] 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。

[0280] 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。

[0281] 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）。

[0282] 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）。

[0283] 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。

[0284] 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。

[0285] 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。

[0286] 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。

[0287] 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。

[0288] 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。

[0289] 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。

[0290] 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ー40がバッテリー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ー40がバッテリー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ー40のバッテリー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。

[0291] 以上は、駐車中に書換え対象 ECU 19 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 ECU 19 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 ECU 19 がアプリプログラムを書換える場合には、書換え対象 ECU 19 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ー 40 がバッテリー上がりとなる事態が懸念されることはないが、車両バッテリー 40 のバッテリー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 ECU 19 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 ECU 44 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、CGW 13 は、その車両走行中に動作不要な ECU 44 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。ECU 44 は、例えば盗難防止等の機能を有する ECU である。即ち、CGW 13 は、車両走行中では全ての ECU 19 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 ECU 44 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。

[0292] 又、CGW 13 は、車両バッテリー 40 のバッテリー残量を監視し、上記した非書換え対象の電源管理処理を行う。ここで、バッテリー残量の監視処理について図 87 を用いて説明する。CGW 13 は、バッテリー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 ECU 19 に配信中においてバッテリー残量を監視し (S911)、バッテリー残量が第 1 所定容量以上であるか、バッテリー残量が第 1 所定容量未満であり且つ第 2 所定容量以上であるか、バッテリー残量が第 2 所定容量未満であるかを判定する (S912~S914)。

[0293] CGW 13 は、バッテリー残量が第 1 所定容量以上であると判定すると (S912: YES)、非書換え対象 ECU 19 を起動状態のまま保持し、書込みデータの書換え対象 ECU 19 への配信を継続する (S915)。CGW

13は、バッテリー残量が第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、バッテリー残量が第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）。

[0294] 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）。

[0295] 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）、バッテリー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。

[0296] 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。

[0297] 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。

[0298] 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。

[0299] 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ー40のバッテリー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。

[0300] （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。

[0301] 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 ECU 19 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 ECU 19 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。

[0302] 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 ECU 19 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 ECU 19 へのデータ転送サイズである。

[0303] 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0×10000000から1kバイト毎に転送するように要求する。

[0304] 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。

[0305] CGW13は、DCM12からアンパッキ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。アンパッキングとは、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)。

[0306] 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)。

[0307] 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、D

CM12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。

[0308] 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。

[0309] 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。

[0310] 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。

[0311] この場合、CGW13は、図91に示すように、DCM12からアンパッキ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。

[0312] 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。

[0313] 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。

[0314] 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。

[0315] 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。

[0316] 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、どのようなであっても良い。

[0317] 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。

[0318] 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、CGW13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。

[0319] 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C G W 1 3のメモリ容量を2 k バイト確保しておき、C G W 1 3は、D C M 1 2から取得し終わった1 k バイトを、1 2 8 バイト単位で書換え対象E C U 1 9に配信すると共に、D C M 1 2から次の1 k バイトの取得を行う。そして、C G W 1 3は、書換え対象E C U 1 9への1 2 8 バイト×8回の配信が完了した後、D C M 1 2から更に次の1 k バイトの取得を行う。

[0320] このようにD C M 1 2からC G W 1 3に転送される分割ファイルのデータ量を固定値（例えば1 k バイト）とし、C G W 1 3から書換え対象E C U 1 9に配信される書込みファイルのデータ量を書換え対象E C U 1 9の仕様に応じて可変値とすれば良い。C G W 1 3は、例えば書換え諸元データに指定される各E C Uのデータ転送サイズを用いて、書換え対象E C U 1 9に配信するデータ量を決定しても良い。

[0321] C G W 1 3は、転送要求をD C M 1 2に送信し、分割ファイルの転送をD C M 1 2に要求するが、分割ファイルの転送をD C M 1 2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E C U 1 9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C G W 1 3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C G W 1 3に送信する。

[0322] 第1 配信態様について図9 3を用いて説明する。C G W 1 3は、D C M 1 2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E C U 1 9に配信する。書換え対象E C U 1 9は、書込みデータの受信を完了すると、受信完了通知をC G W 1 3に送信し、書込みデータの書込み処理を開始する。C G W 1 3は、書換え対象E C U 1 9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D C M 1 2に送信し、次の分割ファイルの転送をD C M 1 2に要求する。C G W 1 3は、D C M 1 2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E C U 1 9に配信する。

[0323] このようにC G W 1 3は、第1 配信態様では、書換え対象E C U 1 9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DCM 12から取得し、書換え対象ECU 19に配信する。そのため、第1配信態様では、CGW 13において、書換え対象ECU 19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DCM 12から取得して次の書込みデータを書換え対象ECU 19に配信しても、次の書込みデータを書換え対象ECU 19が受信不能となる虞がある。しかしながら、書換え対象ECU 19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DCM 12から速やかに取得して次の書込みデータを書換え対象ECU 19に速やかに配信することができる。

[0324] 第2配信態様について図94を用いて説明する。CGW 13は、DCM 12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ECU 19に配信する。書換え対象ECU 19は、書込みデータの受信を完了すると、受信完了通知をCGW 13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ECU 19は、書込みを完了すると、書込み完了通知をCGW 13に送信する。CGW 13は、書換え対象ECU 19から書込み完了通知を受信すると、転送要求をDCM 12に送信し、次の分割ファイルの転送をDCM 12に要求する。CGW 13は、DCM 12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ECU 19に配信する。

[0325] このようにCGW 13は、第2配信態様では、書換え対象ECU 19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DCM 12から取得し、書換え対象ECU 19に配信する。そのため、第2配信態様では、CGW 13において、次の分割ファイルをDCM 12から取得するまでに時間を要するが、書換え対象ECU 19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DCM 12に要求することができる。よって、次の分割ファイルをDCM 12から取得して次の書込みデータを書換え対象ECU 19に配信すると、次の書込みデータを書換え対象ECU 19に確実に配信することができる。

[0326] 又、C G W 1 3 は、書込みデータを S I D 3 4、3 6、3 7 により書換え対象 E C U 1 9 に配信するが、書込みデータを書換え対象 E C U 1 9 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、C G W 1 3 は、図 9 5 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 1 k バイト）で分割して配信する。第 2 配信態様では、C G W 1 3 は、図 9 6 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。C G W 1 3 は、書換え対象 E C U 1 9 に最初に配信する S I D 3 4 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。C G W 1 3 は、図 9 7 に示すように、書換え対象 E C U 1 9 に最後に配信する S I D 3 7 に対する A C K（S I D 7 4）を受信することにより、書換え対象 E C U 1 9 における書込みデータの受信を特定する。この S I D 3 7 に対する A C K が、図 9 3 及び図 9 4 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、C G W 1 3 は、書換え対象 E C U 1 9 に最後に配信する S I D 3 7 に対する A C K 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 E C U 1 9 に配信すると同時に、更に次の書込みデータを D C M 1 2 から取得する。

[0327] 又、D C M 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 1 0 に示すアンパッキングにおいて、フォルダ 1 に D C M 用の書換え諸元データ及び C G W 用の書換え諸元データを格納し、フォルダ 2 に E C U（I D 1）の認証子及び差分データを格納し、フォルダ 3 に E C U（I D 2）の認証子及び差分データを格納して管理する。

[0328] 又、C G W 1 3 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 E C U 1 9 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 E C U 1 9 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。

[0329] 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象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。

[0330] (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いように書込みデータの配信制御処理を行う。

[0331] 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。

[0332] 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。

[0333] 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。

[0334] 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。

[0335] 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。

[0336] 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。

[0337] 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。

[0338] 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。

[0339] 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。

[0340] 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。

[0341] 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。

[0342] ＣＧＷ１３は、ＤＣＭ１２からアンパッキ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。

[0343] 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。

[0344] 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、書込みデータを書換え対象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、書込みデータを書換え対象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。

[0345] 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、書込みデータを書換え対象ECU19への配信を開始する(S1109、配信制御手順に相当する)。

[0346] 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 T_1 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 T_1 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 T_1 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 T_2 ($> T_1$) 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。

[0347] CGW13 は、書込みデータを書換え対象 ECU19 への配信を開始すると、書込みデータを書換え対象 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、書込みデータを書換え対象 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、書込みデータを書換え対象 ECU19 への配信間隔を変更する (S1114)。

[0348] CGW13 は、書込みデータを書換え対象 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E C U 1 9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。

[0349] 以上に説明したように、C G W 1 3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E C U 1 9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。

[0350] 尚、以上は、C G W 1 3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、C G W 1 3において、書換え諸元データの解析結果から書換え対象E C U所属テーブルを特定する構成を例示したが、書換え対象E C U所属テーブルを予め保持する構成でも良い。

[0351] 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、C G W 1 3は、図105に示すように、車両が走行中のI G電源がオンでは、I G系E C U、A C C系E C U、+ B電源系E C UがC A N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、C G W 1 3は、図106に示すように、駐車中のI G電源がオフでは、+ B電源系E C UのみがC A N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、C G W 1 3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。

[0352] 又、図107に示すように、C G W 1 3において、書換え対象E C U 1 9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。

[0353] 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。

[0354] 書換え諸元データに組込まれるバス負荷テーブルは、例えば車両メーカー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。

[0355] 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。

[0356] (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。

[0357] 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。

[0358] 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。

[0359] 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。

[0360] 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。

[0361] 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。

[0362] 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。

[0363] 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。

[0364] 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（S1206）。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。

[0365] 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）。

[0366] 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ECU19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。

[0367] 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。

[0368] 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、アプリプロ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。

[0369] 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。

[0370] （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 1 1 2 から図 1 1 4 を参照して説明する。アクティベートの実行制御処理は、C G W 1 3 が前述した (1 2) アクティベート要求の指示処理を行うことに伴い、C G W 1 3 からアクティベート要求が指示された書換え対象 E C U 1 9 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 E C U 1 9 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 E C U 1 9 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 E C U 1 9 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。

[0371] 図 1 1 2 に示すように、E C U 1 9 は、アクティベートの実行制御部 1 0 7 において、運用面情報更新部 1 0 7 a と、実行条件判定部 1 0 7 b と、実行制御部 1 0 7 c と、通知部 1 0 7 d とを有する。運用面情報更新部 1 0 7 a は、C G W 1 3 からアクティベート要求が指示されると、次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 1 0 7 a 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。

[0372] 実行条件判定部 1 0 7 b は、アクティベートの実行条件として、C G W 1 3 からソフトウェアのリセット要求が指示されたか否か、C G W 1 3 から電源管理 E C U 2 0 へ電源のリセット要求が指示されたか否か、C G W 1 3 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 1 0 7 b 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、C G W 1 3 からの指示でなく、電源検出回路 3 6 にて検出しても良い。実行制御部 1 0 7 c 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 1 0 7 b 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 1 0 7 d は、運用面情報やバージョン情報等の通知情報

をC G W 1 3に通知する。

[0373] 次に、書換え対象E C U 1 9におけるアクティベートの実行制御部1 0 7の作用について図1 1 3及び図1 1 4を参照して説明する。書換え対象E C U 1 9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。

[0374] (1 3 - 1) 書換え処理

書換え対象E C U 1 9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(S 1 3 0 1)。書換え対象E C U 1 9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(S 1 3 0 2)。書換え対象E C U 1 9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C G W 1 3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E C U 1 9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(S 1 3 0 2 : Y E S)、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(S 1 3 0 3)。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。

[0375] 書換え対象E C U 1 9は、両者が一致していると判定すると(S 1 3 0 3 : Y E S)、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(S 1 3 0 4)、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E C U 1 9は、両者が一致していないと判定すると(S 1 3 0 3 : N O)、否定応答をC G W 1 3に送信し(S 1 3 0 5)、書換え処理を終了する。

[0376] (1 3 - 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）。

[0377] 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。

[0378] 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、これか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。

[0379] 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。

[0380] 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。

[0381] 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、C G W 1 3 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。C G W 1 3 が複数の書換え対象 E C U 1 9 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 E C U 1 9 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。

[0382] 尚、前述した(12) C G W 1 3 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 E C U 1 9 に対して C G W 1 3 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 E C U 1 9 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 E C U 1 9 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。

[0383] (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、C G W 1 3 において書換え対象のグループ管理処理を行う。C G W 1 3 は、同一グループに属する1以上の書換え対象 E C U 1 9 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、C G W 1 3 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、E C U (I D 1) 及び E C U (I D 2) が第1グループの書換え対象 E C U 1 9 であり、E C U (I D 1 1) 、 E C U (I D 1 2) 及び E C U (I D 1 3) が第2グループの書換え対象 E C U 1 9 であるとして説明する。

[0384] 図115に示すように、C G W 1 3 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、C G W 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 E C U 1 9 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。

[0385] 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）。

[0386] 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

S 1 4 0 3 ~ S 1 4 0 5 に戻り、S 1 4 0 3 ~ S 1 4 0 5 を繰返す。

[0387] C G W 1 3 は、前回の書換え対象 E C U 1 9 と異なるグループに属する書換え対象 E C U 1 9 の書換えであると判定すると (S 1 4 0 5 : Y E S)、アクティベート要求の指示処理に移行する (S 1 4 0 8、指示実行手順に相当する)。

[0388] C G W 1 3 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 E C U 1 9 が存在するか否かを判定する (S 1 4 1 1)。即ち、C G W 1 3 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。C G W 1 3 は、次の書換え対象 E C U 1 9 が存在すると判定すると (S 1 4 1 1 : Y E S)、書換えを完了したグループに属する書換え対象 E C U 1 9 にアクティベート要求を指示する (S 1 4 1 2)。即ち、C G W 1 3 は、未だ第 2 グループに属する書換え対象 E C U 1 9 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 E C U (I D 1) 及び E C U (I D 2) に対してアクティベートを指示する。

[0389] C G W 1 3 は、ソフトウェアのリセット要求を書換え対象 E C U 1 9 に指示し、電源管理 E C U 2 0 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 E C U 1 9 に指示することで、書換え対象 E C U (I D 1) 及び E C U (I D 2) のアプリプログラムを同時に起動させる。

[0390] C G W 1 3 は、次の書換え対象 E C U 1 9 の書換えタイミングを判定する (S 1 4 1 3, S 1 3 1 4)。即ち、C G W 1 3 は、第 2 グループに属する書換え対象 E C U 1 9 の書換えタイミングを判定する。C G W 1 3 は、次の書換え対象 E C U 1 9 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 (S 1 4 1 3 : Y E S)、I G 電源をオンからオフに切替え (S 1 4 1 5)、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。C G W 1 3 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 E C U 1 9 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。

[0391] 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）、車両バッテリー40のバッテリー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、車両バッテリー40のバッテリー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、車両バッテリー40のバッテリー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。

[0392] 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。

[0393] 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。

[0394] 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に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。

[0395] 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E C U 1 9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E C U 1 9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E C U 1 9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E C U 1 9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E C U 1 9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E C U 1 9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E C U 1 9に対するアクティベートを同時に行っても良い。

[0396] 又、書換え対象E C U 1 9に1面単独メモリE C Uが含まれている場合に、その1面単独メモリE C U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E C U 1 9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E C U 1 9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E C Uに対してインストールを指示しても良い。

[0397] C G W 1 3は、書換え諸元データのメモリ種別を参照し、書換え対象E C U 1 9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、C G W 1 3は、連携動作する関係にあるE C U 1 9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E C U 1 9のインストール順序を決定する。

[0398] 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人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

[0399] 又、C G W 1 3 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 E C U 1 9 及び第 2 書換え対象 E C U 1 9 に指示する場合に、第 1 書換え対象 E C U 1 9 においてインストールを成功し、第 2 書換え対象 E C U 1 9 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 E C U 1 9 に指示し、ロールバックを第 1 書換え対象 E C U 1 9 に指示する。

[0400] 又、C G W 1 3 は、インストールを第 1 グループに属する書換え対象 E C U 1 9 及び第 2 グループに属する書換え対象 E C U 1 9 に指示する場合に、第 1 グループに属する書換え対象 E C U 1 9 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 E C U 1 9 に指示する。C G W 1 3 は、例えば図 1 1 6 において、第 1 グループに属する書換え対象 E C U 1 9 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 (S 1 4 0 5 ; Y E S) 、第 1 グループに対するアクティベート要求の指示処理 (S 1 4 0 8) をスキップし、ステップ S 1 4 0 7 に進む。そして、C G W 1 3 は、ステップ S 1 4 0 3 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 (S 1 4 0 8) 。即ち、C G W 1 3 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。

[0401] 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。

[0402] 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。

[0403] (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手書き込みが開始される前の状態に戻すことである。

[0404] 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。

[0405] 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。

[0406] 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。

[0407] 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。

[0408] 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。

[0409] (15-1) ロールバック方法の特定処理

C GW 13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C GW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。C GW 13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。

[0410] 即ち、C GW 13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、C GW 13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。

[0411] C GW 13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。

[0412] 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C GW 13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。

[0413] 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。

[0414] （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。

[0415] 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(

I D 1) が1面単独メモリ、E C U (I D 2) 及びE C U (I D 3) が2面メモリであり、E C U (I D 1) へのインストールが完了し、E C U (I D 2) 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、C G W 1 3は、S 1 4 1 3において、第1グループに属する書換え対象E C U 1 9全てについてロールバックの要否を判定する。

[0416] C G W 1 3は、アプリプログラムの書換えが全部行われたE C U (I D 1) 及び一部行われたE C U (I D 2) がロールバック対象であると特定する。C G W 1 3は、その特定したロールバック対象の書換え対象E C U 1 9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 (S 1 5 1 4, S 1 5 1 5)。C G W 1 3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 (S 1 5 1 4 : Y E S)、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 (S 1 5 1 6, S 1 5 1 7)。

[0417] C G W 1 3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 (S 1 5 1 6 : Y E S)、第1ロールバック処理に移行する (S 1 5 1 8、ロールバック実行手順に相当する)。C G W 1 3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 (S 1 5 3 1)。そして、C G W 1 3は、D C M 1 2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E C U 1 9に配信する。書換え対象E C U 1 9は、C G W 1 3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 (S 1 5 3 2)、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。

[0418] C G W 1 3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 (S 1 5 1 7 : Y E S)、第2ロールバック処理に移行する (S 1 5 1 9、ロールバック実行手順に相当する)。C G W 1 3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 (S 1

541)、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。

[0419] 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。

[0420] 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。

[0421] 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。

[0422] 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）。

[0423] 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）。

[0424] 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。

[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。

[0426] 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。

[0427] (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。

[0428] 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。

[0429] 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。

[0430] 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。

[0431] 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。

[0432] 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。

[0433] 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。

[0434] 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。

[0435] 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。

[0436] 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。

[0437] 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。

[0438] 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)。C G W 1 3 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 (S 1 6 1 3)。C G W 1 3 は、第 1 ～ 第 3 ロールバック処理のそれぞれにより、書込むデータ量が異なってくる。そのため、C G W 1 3 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。C G W 1 3 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 (S 1 6 1 4)。

[0439] C G W 1 3 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 E C U 1 9 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り返す。C G W 1 3 は、S 1 6 1 3 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。C G W 1 3 は、S 1 6 1 4 において、例えば書換え途中であった E C U (I D 3) のロールバックが正常に完了したか否かを判定する。

[0440] C G W 1 3 は、ロールバック対象の書換え対象 E C U 1 9 に対するロールバックが完了したと判定すると (S 1 6 1 4 : Y E S)、ロールバック時の書換え進捗状況の表示を終了する (S 1 6 1 5)。C G W 1 3 は、例えば E C U (I D 3) についてはロールバックが 1 0 0 % 完了した旨の表示を継続する。

[0441] C G W 1 3 は、全てのロールバック対象 E C U 1 9 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 (S 1 6 1 6)。C G W 1 3 は、全てのロールバック対象 E C U 1 9 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 (S 1 6 1 6 : N O)、ステップ S 1 6 1 1 に戻り、ステップ S 1 6 1 1 以降を繰り返す。

[0442] C G W 1 3 は、例えばインストールが完了した E C U (I D 1) 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 (S 1 6 1 3)。一方、例えばインストールが完了した E C U (I D 2) 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 E C U (I

D 2) を除外する。C G W 1 3 は、E C U (I D 3) 及び E C U (I D 1) 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 E C U 1 9 について書換え完了となり (S 1 6 1 6 : Y E S) 、ロールバック時の表示制御処理を終了する。

[0443] 尚、上述した説明では、C G W 1 3 がロールバック時の表示制御処理を行うこととしたが、C G W 1 3 から必要な情報を取得しつつ、車載ディスプレイ E C U 7 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 C G W 1 3 で行い、ロールバック時の表示制御を車載ディスプレイ E C U 7 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 C G W 1 3 だけが有する構成に限らず、表示制御装置の機能を C G W 1 3 と車載ディスプレイ E C U 7 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 C G W 1 3 とセンター装置 3 とで分散して有する構成でも良い。

[0444] 以下、書換え進捗状況の表示について図 1 3 4 から図 1 4 2 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 1 3 4 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。

[0445] 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 E C U 1 9 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 E C U 1 9 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 1 3 4 は、E C U (I D 0 0 0 1) 及び E C U (I D 0 0 0 2) 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、E C U (I D 0 0 0 3) が通常書換え中の状態である場合を例示している。

[0446] 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。

[0447] 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。

[0448] 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。

[0449] 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）。

[0450] 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。

[0451] 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）。

[0452] 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、C G W 1 3 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「5 0 %」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 1 4 0（c）、図 1 4 1（c））。表示端末 5 は、C G W 1 3 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 E C U 1 9 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 1 4 0（d）、（e）、図 1 4 1（d）、（e））。表示端末 5 は、書換え対象 E C U 1 9 が新アプリプログラムの書換えを完了した後引続いて、C G W 1 3 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 E C U 1 9 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 1 4 0（f）、（g）、図 1 4 1（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。

[0453] この場合、表示端末 5 は、図 1 4 0 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「1 0 0 %」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「1 0 0 %」と表示することで、進捗グラフの幅全体を「2 0 0 %」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。

[0454] 又、表示端末 5 は、図 1 4 1 に示すように、新アプリプログラムの書換え分を「5 0 %」とし、旧アプリプログラムの書換え分を「5 0 %」とすることで、進捗グラフの幅全体を「1 0 0 %」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。

[0455] 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）。

[0456] 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。

[0457] 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。C G W 1 3 は、ロールバック処理として3個の書換え対象E C U 1 9 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。

[0458] (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E C U 1 9 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。

[0459] 図144に示すように、E C U 1 9 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。

[0460] 差分データ取得部103aは、書換え対象E C U 1 9 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。

[0461] 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。

[0462] 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ことを示す情報であり、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。

[0463] 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)。

[0464] 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。

[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）。

[0466] 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以降を繰り返す。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。

[0467] 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（S 1 7 0 5 : N O）、1 ブロック目に対する書込みであるか否かを判定する（S 1 7 0 9）。

[0468] 書換え対象 E C U 1 9 は、1 ブロック目に対する書込みであると判定すると（S 1 7 0 9 : Y E S）、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（S 1 7 0 8）。書換え対象 E C U 1 9 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（S 1 7 0 9 : N O）、書込みをリトライし（S 1 7 1 0）、全ての書込みを完了したか否かを判定する（S 1 7 0 8）。

[0469] 書換え対象 E C U 1 9 が 1 面単独メモリ E C U の場合について図 1 4 6 を参照して説明する。C G W 1 3 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 C R C 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（旧アプリケーション）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 E C U 1 9 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 E C U 1 9 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。

[0470] 書換え対象 E C U 1 9 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 C R C 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 C R C 値（C R C（B 1 ~ B n））及び新データに対する C R C 値（C R C（B 1' ~ B n'））と、その計算した C R C 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。

[0471] 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。

[0472] 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。

[0473] フラッシュメモリのA面が運用面かつバージョン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。

[0474] 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。

[0475] 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、C G W 1 3 が差分データを書換え対象E C U 1 9 に配信する前に、ヘッダ情報を書換え対象E C U 1 9 に配信しても良い。書換え対象E C U 1 9 は、ヘッダ情報をC G W 1 3 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。

[0476] 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E C U 1 9 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。

[0477] 以上に説明したように、書換え対象E C U 1 9 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り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E C U 1 9 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E C U 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。

[0478] 尚、書換え対象E C U 1 9 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E C U 1 9 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。

[0479] 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最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。

[0480] (18) 書換の実行制御処理

書換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において書換の実行制御処理を行う。

[0481] 図148に示すように、ECU19は、書換の実行制御部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。

[0482] 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。

[0483] (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)。

[0484] 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。

[0485] 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）。

[0486] 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。

[0487] 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。

[0488] （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）。

[0489] 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

(S 1 8 1 5 : Y E S)、ベリファイが正であるか否かを判定する(S 1 8 1 6)。書換え対象E C U 1 9は、ベリファイが正であると判定すると(S 1 8 1 6 : Y E S)、書換え完了フラグを「OK」に設定する(S 1 8 1 7)。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。

[0490] 書換え対象E C U 1 9は、C G W 1 3からアクティベート要求を受信したか否かを判定する(S 1 8 1 8)。書換え対象E C U 1 9は、C G W 1 3からアクティベート要求を受信したと判定すると(S 1 8 1 8 : Y E S)、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(S 1 8 1 9)。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E C U 1 9は、C G W 1 3からバージョン読出信号を受信したか否かを判定し(S 1 8 2 0)、バージョン読出信号を受信したと判定すると(S 1 8 2 0 : Y E S)、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ことを特定可能な識別情報をC G W 1 3に送信し(S 1 8 2 1)、書換え動作処理を終了する。ここで、書換え対象E C U 1 9は、S 1 8 1 1からS 1 8 2 1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E C U 1 9は、S 1 8 1 1からS 1 8 1 9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、S 1 8 1 9を行った後に再起動することで、S 1 8 2 0からS 1 8 2 1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。

[0491] (1 8 - 3) 情報通知処理

書換え対象E C U 1 9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I G電源がオンになったりC G W 1 3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E C U 1 9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C G W 1 3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。

[0492] 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。

[0493] （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。

[0494] 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E C U 1 9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、S 1 8 4 3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R A M上にて実行する。書換え対象E C U 1 9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、S 1 8 4 3において、書換えプログラムをR A Mにダウンロードして実行する。

[0495] 書換え対象E C U 1 9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（S 1 8 4 4 : Y E S）、その識別情報と書換え対象E C U 1 9の起動面情報とが一致しているか否かを判定する（S 1 8 4 5）。具体的には、書換え対象E C U 1 9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E C U 1 9は、識別情報とE C U 1 9の起動面情報とが一致していると判定すると（S 1 8 4 5 : Y E S）、アプリプログラムの書換えを行い（S 1 8 4 6）、書換えプログラムの検証処理を終了する。

[0496] 書換え対象E C U 1 9は、識別情報とE C U 1 9の起動面情報が一致していないと判定すると（S 1 8 4 2 : N O）、又は識別情報と書換え対象E C U 1 9の起動面情報とが一致していないと判定すると（S 1 8 4 5 : N O）、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C G W 1 3に送信し（S 1 8 4 7）、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E C U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。

[0497] 尚、書換え対象E C U 1 9は、図1 5 0に示すように、C G W 1 3から書込みデータを取得する前に、C G W 1 3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。

[0498] 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。

[0499] 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)。

[0500] 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)。

[0501] 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)。

- [0502] 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）。
- [0503] 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。
- [0504] 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）。CGW13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）。
- [0505] 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）。

[0506] 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。

[0507] (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。

[0508] 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。

[0509] 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。

[0510] 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。

[0511] 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。

[0512] 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。

[0513] 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。

[0514] 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み込まれていない。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。

[0515] 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。

[0516] 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

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。

[0517] 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。

[0518] 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は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は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は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は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。

[0519] 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。

[0520] 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。

[0521] 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）。

[0522] 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。

[0523] 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。

[0524] 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。

[0525] 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。

[0526] 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。

[0527] 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

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] 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。

[0529] 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。

[0530] 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。

[0531] 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

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。

[0532] 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とは一部相異なる。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。

[0533] 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。

[0534] 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。

[0535] (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。

[0536] 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)。

[0537] 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: N

Ｏ）、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。

[0538] 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。

[0539] 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。

[0540] 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（S 1 9 2 8）。マイコン 3 3 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 3 3 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（S 1 9 2 5 : Y E S）、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（S 1 9 2 7）。即ち、マイコン 3 3 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（S 1 9 2 8）。マイコン 3 3 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 3 3 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。

[0542] マイコン 3 3 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（S 1 9 1 2）。マイコン 3 3 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（S 1 9 1 2 : Y E S）、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（S 1 9 1 3）、車両制御処理を中断して有線書換え処理を開始する（S 1 9 1 4）。マイコン 3 3 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。

[0543] マイコン 3 3 は、有線書換え処理の完了条件の成立を判定し（S 1 9 1 5）、有線書換え処理の完了条件が成立したと判定すると（S 1 9 1 5 : Y E S）、有線書換え処理を完了し（S 1 9 1 6）、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（S 1 9 1 7）。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。

[0544] 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。

[0545] 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。

[0546] 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。

[0547] （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。

[0548] 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。

[0549] 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）。

[0550] 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

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（S 1 9 6 6）、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（S 1 9 6 2）。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。

[0551] 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（S 1 9 6 4 : Y E S）、無線書換え要求を廃棄して有線書換えを継続させる（S 1 9 6 7）。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（S 1 9 6 8）。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、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（S 1 9 6 5 : Y E S）、この場合も、無線書換え要求を廃棄して有線書換えを継続させる（S 1 9 6 7）。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（S 1 9 6 8）。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。

[0553] 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（S 1 9 4 5）。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（S 1 9 4 5 : Y E S）、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（S 1 9 4 6）、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（S 1 8 4 7）。マイコン 3 3 は、無線書換え処理の完了条件の成立を判定し（S 1 9 4 8）、無線書換え処理の完了条件が成立したと判定すると（S 1 9 4 8 : Y E S）、無線書換え処理を終了し（S 1 9 4 9）、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（S 1 9 5 0）。マイコン 3 3 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、例えばアプリケーション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。

[0554] マイコン 3 3 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（S 1 9 4 5 : N O）、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 3 3 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 3 3 は、状態遷移管理の完了条件が成立したと判定すると（S 1 9 5 1 : Y E S）、第 2 状態の状態遷移管理処理を終了する。

[0555] 以上は、アプリ実行部 1 0 5 a 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 1 6 5 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 1 0 5 a 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 1 0 5 a 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 1 0 5 a 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。

[0556] 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。

[0557] 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。

[0558] 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。

[0559] 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。

[0560] 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。

[0561] 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。

[0562] 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状態に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。

[0563] 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。

[0564] 又、ECU 19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。

[0565] 又、ECU 19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。

[0566] 又、ECU 19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。

[0567] 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。

- [0568] 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。
- [0569] 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。
- [0570] 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。
- [0571] リプログラムウェアが組込まれているリプログラ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。リプログラ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。
- [0572] リプログラムウェアを外部からダウンロードするリプログラ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。
- [0573] 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。

[0574] 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。

[0575] 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。

[0576] (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。

[0577] 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。

- [0578] 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。
- [0579] 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。
- [0580] 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。
- [0581] 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を行う。以下、それぞれ

の処理について説明する。

[0582] (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)。

[0583] 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。

[0584] 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。

[0585] (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)。

[0586] 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。

[0587] 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。

[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「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。

[0589] 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。

- [0590] 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。

[0591] (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。

[0592] 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。

[0593] 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。

[0594] 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。

[0595] 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。

[0596] 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。

[0597] 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。

[0598] 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。

[0599] 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。

[0600] 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。

[0601] 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。

[0602] 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。

[0603] 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。

[0604] 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。

[0605] 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。

[0606] 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:Y

ES)、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)。

[0607] 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。

[0608] 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。

[0609] 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3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。

[0610] 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。

[0611] CGW 1 3 は、インストールフェーズであると判定すると (S 2 1 0 4 : Y E S)、インストールフェーズの処理を実施し (S 2 1 0 8)、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 DCM 1 2 に送信する (S 2 1 1 1)。インストールフェーズの処理とは、例えば書換え対象 ECU 1 9 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。

[0612] CGW 1 3 は、書換え対象 ECU 1 9 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。CGW 1 3 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。CGW 1 3 は、これらの処理を全ての書換え対象 ECU 1 9 に対するインストールが完了するまで繰返す。CGW 1 3 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。

[0613] CGW 1 3 は、アクティベートフェーズであると判定すると (S 2 1 0 4 : Y E S)、アクティベートフェーズの処理を実施し (S 2 1 0 8)、そのアクティベート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 DCM 1 2 に送信する (S 2 1 1 1、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 ECU 1 9 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。CGW 1 3 は、書換え対象 ECU 1 9 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。CGW 1 3 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。

[0614] CGW 1 3 は、アクティベートフェーズを完了したか否かを判定し (S 2 1 1 2)、アクティベートフェーズを完了したと判定すると (S 2 1 1 2 : Y E S)、進捗状態の同期制御処理を終了する。CGW 1 3 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 (S 2 1 1 2 : N O)、S 2 1

02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）。

[0615] 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）。

[0616] 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。

[0617] 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。

[0618] 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。

[0619] 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。

[0620] 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ことを判定する(S2143~S2146)。

[0621] 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。

[0622] 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（S 2 1 4 5 : Y E S）、インストールフェーズの画面を表示する（S 2 1 4 9）。車載ディスプレイ 7 は、C G W 1 3 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（S 2 1 4 6 : Y E S）、アクティベートフェーズの画面を表示する（S 2 1 5 0）。車載ディスプレイ 7 は、C G W 1 3 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。

[0623] 以上に説明したように、マスタ装置 1 1 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 1 1 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。

[0624] （2 2）表示制御情報の送信制御処理、（2 3）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 1 8 1 及び図 1 8 2 を参照して説明し、マスタ装置 1 1 における表示制御情報の受信制御処理について図 1 8 3 から図 1 8 5 を参照して説明する。

[0625] 図 1 8 1 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 5 4 において、書込みデータ記憶部 5 4 a（更新データ記憶部に相当する）と、表示制御情報記憶部 5 4 b と、情報送信部 5 4 c とを有する。書込みデータ記憶部 5 4 a は、複数の書換え対象 E C U 1 9 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 E C U 1 9 に対する書込みデータを記憶する。表示制御情報記憶部 5 4 b 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 E C U 1 9 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。

- [0626] 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こと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ことを示すフェーズ識別情報である。
- [0627] 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。
- [0628] 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。

[0629] 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。

[0630] 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。

[0631] 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、C G W 1 3 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。

[0632] C G W 1 3 は、表示制御情報を用いないと判定すると（S 2 3 0 4 : N O）、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（S 2 3 0 6）。即ち、C G W 1 3 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、C G W 1 3 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。

[0633] 図 1 8 5 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 D C M 1 2 及び C G W 1 3 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。

[0634] 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 D C M 1 2 及び C G W 1 3 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。

[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。

[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。

[0637] 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。

[0638] (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。

[0639] 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。

[0640] 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 90 a 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。

[0641] 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。

[0642] 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。

[0643] 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。

[0644] 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 90 a 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。

[0645] 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。C G W 1 3 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、C G W 1 3 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。

[0646] 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 G W 1 3 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。C G W 1 3 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、C G W 1 3 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。

[0647] 画面表示指示部 9 0 b 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。

[0648] 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。

[0649] 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。

[0650] 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。

[0651] 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。

[0652] 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。

[0653] 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。

[0654] 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。

[0655] 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。

[0656] 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(S2401: 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。

[0657] 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（S 2 4 0 4）、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。C G W 1 3 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。C G W 1 3 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。

[0658] C G W 1 3 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（S 2 4 0 3 : N O）、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（S 2 4 0 5、カスタマイズモード判定手順に相当する）。C G W 1 3 は、カスタマイズモードが設定されていると判定すると（S 2 4 0 5 : Y E S）、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（S 2 4 0 6、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。

[0659] C G W 1 3 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（S 2 4 0 5 : N O）、初期設定の設定内容にしたがう表示指示処理に移行し（S 2 4 0 7、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、C G W 1 3 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。

[0660] 続いて、図 1 9 2 を用いて、S 2 4 0 4、S 2 4 0 6 及び S 2 4 0 7 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。C G W 1 3 は、表示指示処理に移行すると、画面の表示有無を設定し（S 2 4 1 1）、画面の項目の表示有無を設定し（S 2 4 1 2）、画面の項目の表示内容の変更を指示する（S 2 4 1 3）。C G W 1 3 は、画面表示要求通知を D C M 1 2 に送信し、画面表示要求を D C M 1 2 から車載ディスプレイ 7 に送信させ（S 2 4 1 4）、D C M 1 2 からの操作結果情報の受信を待機する（S 2 4 1 5）。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、C G W 1 3 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。

[0661] C G W 1 3 は、車載ディスプレイ 7 から D C M 1 2 に操作結果が送信されたことで、D C M 1 2 からの操作結果情報の受信を判定すると（S 2 4 1 5 : Y E S）、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（S 2 4 1 6）。

[0662] C G W 1 3 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（S 2 4 1 6 : Y E S）、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（S 2 4 1 7）。C G W 1 3 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（S 2 4 1 7 : Y E S）、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（S 2 4 1 8）。尚、インストールフェーズ以外では、S 2 4 1 7 及び S 2 4 1 8 を省略しても良い。C G W 1 3 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（S 2 4 1 8 : Y E S）、アプリプログラムの書換えを継続する（S 2 4 1 9）。

[0663] 一方、C G W 1 3 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。C G W 1 3 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（S 2 4 1 8 : Y E S）、アプリプログラムの書換えを継続し（S 2 4 1 9）、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。

[0664] 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。

[0665] 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。

[0666] 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…」が

タン5 1 4 a、「更新名称A…」ボタン5 1 4 b、「更新名称B…」ボタン5 1 4 c、「詳細確認」ボタン5 1 4 d、「戻る」ボタン5 1 4 e、「OK」ボタン5 1 4 fの6項目がある。この場合、図1 9 5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1 9 4に示したように、アクティベート承諾画面5 1 4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5 1 4 a、「更新名称A…」ボタン5 1 4 b、「更新名称B…」ボタン5 1 4 c、「詳細確認」ボタン5 1 4 d、「戻る」ボタン5 1 4 e、「OK」ボタン5 1 4 fの何れかを操作可能である。

[0667] 一方、図1 9 6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5 1 4 a、「更新名称A…」ボタン5 1 4 b、「更新名称B…」ボタン5 1 4 c、「詳細情報」ボタン5 1 4 d、「OK」ボタン5 1 4 fが「表示」に設定され、「戻る」ボタン5 1 4 eが非表示に設定されていれば、図1 9 7に示すように、アクティベート承諾画面5 1 4に「キャンペーンID…」ボタン5 1 4 a、「更新名称A…」ボタン5 1 4 b、「更新名称B…」ボタン5 1 4 c、「詳細情報」ボタン5 1 4 d、「OK」ボタン5 1 4 fが表示される一方で、「戻る」ボタン5 1 4 eが表示されない。即ち、ユーザは、「キャンペーンID…」ボタン5 1 4 a、「更新名称A…」ボタン5 1 4 b、「更新名称B…」ボタン5 1 4 c、「詳細確認」ボタン5 1 4 d、「OK」ボタン5 1 4 fの何れかを操作可能であるが、「戻る」ボタン5 1 4 eが表示されていないので、「戻る」ボタン5 1 4 e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5 1 4 e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5 1 4 f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。

[0668] 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。

[0669] 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。

[0670] 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。

[0671] 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。

[0672] 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。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、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。

[0673] 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。

[0674] 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。

[0675] 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。CGW

13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。

[0676] 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。

[0677] 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。

[0678] 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（S 2 4 0 4）。この場合、C G W 1 3は、図2 0 4に示すように、キャンペーン通知画面5 0 2では、「後で」ボタン5 0 2 aを非表示とする。又、C G W 1 3は、図2 0 5及び図2 0 6に示すように、ダウンロード承諾画面5 0 3では、「戻る」ボタン5 0 3 cを非表示とする。又、C G W 1 3は、図2 0 7に示すように、ダウンロード実行中画面5 0 4では、「戻る」ボタン5 0 4 bを非表示とする。又、C G W 1 3は、図2 0 8及び図2 0 9に示すように、インストール承諾画面5 0 5では、「戻る」ボタン5 0 5 bを非表示とする。又、C G W 1 3は、図2 1 0に示すように、アクティベート承諾画面5 1 8では、「戻る」ボタンを非表示とする。

[0679] 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5 0 2を表示し、ダウンロード承諾画面5 0 3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5 0 5、アクティベート承諾画面5 1 8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。

[0680] 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。

[0681] 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。

[0682] 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。

[0683] 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。

[0684] 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。

[0685] (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。

[0686] 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。

[0687] 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91cは、表示指示部91b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。

[0688] 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 9 1 e は、フェーズ特定部 9 1 a 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。

[0689] 無効化指示部 9 1 f は、駐車中にプログラム更新が行われることで電源管理 ECU 20 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 ECU 20 やユーザ操作に関わる各 ECU 19 に指示する。例えばエンジン ECU 47（図 2 1 7 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 ECU 19 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 ECU 20 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 ECU 19 のメモリ構造が 1 面メモリであり、駐車中に 1 G 電源オンしてインストールを行う場合、ユーザが 1 G 電源をオフする操作を行ったとしても、受付を無効化し、1 G 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 9 1 f 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。

[0690] 次に、上記した構成の作用について図 2 1 2 から図 2 1 7 を参照して説明する。CGW 13 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。

[0691] CGW 13 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（S 2 5 0 1）。CGW 13 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（S 2 5 0 1 : Y E S）、プログラム更新のフェーズ及びメモリ構成を特定する（S 2 5 0 2、フェーズ特定手順に相当する）。CGW 13 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 4 6 を表示するようにメータ装置 4 5 に指示し（S 2 5 0 3、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 (S 2 5 0 4)。

[0692] C G W 1 3 は、詳細表示要求の有無を判定し (S 2 5 0 5)、詳細表示要求の有りを判定すると (S 2 5 0 5 : Y E S)、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 (S 2 5 0 6)。C G W 1 3 は、例えば図 3 2 に示すキャンペーン通知アイコン 5 0 1 a、図 3 3 に示す「確認する」ボタン 5 0 2 a、図 3 4 に示す「詳細確認」ボタン 5 0 3 b 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。C G W 1 3 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 (S 2 5 0 6 : Y E S)、詳細情報を取得し (S 2 5 0 7)、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 (S 2 5 0 8)、詳細情報を表示するようにセンター装置 3 に指示する (S 2 5 0 9)。

[0693] C G W 1 3 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、C G W 1 3 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。

[0694] C G W 1 3 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 (S 2 5 1 0)。

C G W 1 3 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。C G W 1 3 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 (S 2 5 1 0 : N O)、ステップ S 2 5 0 2 に戻り、ステップ S 2 5 0 2 以降を繰り返す。C G W 1 3 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 S 2 5 0 2 以降を繰り返す。

C G W 1 3 は、プログラム更新のイベントが終了したと判定すると (S 2 5 1 0 : Y E S)、プログラム更新の報知制御処理を終了する。

- [0695] 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、C GW13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。
- [0696] 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、C GW13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。
- [0697] 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

インジケータ 4 6 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 4 6 の表示は、メモリ構成によって異なる表示態様となる。ここで、図 2 1 3 に示す I G 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 I G 電源をオフした際の表示態様であり、I G 電源オフに伴いインジケータ 4 6 を消灯させる。その後、ユーザ操作により I G 電源オンされた際は、インジケータ 4 6 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 4 5 に示す確認操作画面 5 1 0 において、ユーザが「OK」ボタン 5 1 0 b 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 4 6 を消灯させる。

[0698] 以下、メータ装置 4 5 がインジケータ 4 6 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 9 1 c がインジケータ 4 6 の報知態様を制御しても良い。図 2 1 4 には、書換え対象 E C U 1 9 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。C G W 1 3 からの指示に基づき、メータ装置 4 5 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 4 6 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 4 6 を点滅させる。メータ装置 4 5 は、その後、I G オフではインジケータ 4 6 を消灯させ、I G オンではインジケータ 4 6 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 4 6 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 4 5 は、アクティベート実行中のフェーズではインジケータ 4 6 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。

[0699] 図 2 1 5 には、書換え対象 E C U 1 9 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。C G W 1 3 からの指示に基づき、メータ装置 4 5 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。

[0700] 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。

[0701] 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。

[0702] 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。

[0703] 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46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。

- [0704] 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。

[0705] 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。

[0706] 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。

[0707] 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、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。

[0708] 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。

[0709] 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。

[0710] (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。

[0711] 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 9 2 e と、第 2 電源自己保持有効化部 9 2 f と、第 2 停止条件成立判定部 9 2 g と、第 2 電源自己保持停止部 9 2 h とを有する。

[0712] 車両電源判定部 9 2 a は、車両電源のオンオフを判定する。書換え中判定部 9 2 b 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 9 5 b は、どの書換え対象 ECU 1 9 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 9 2 c は、車両電源がオフであると車両電源判定部 9 2 a 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 9 2 b 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 9 2 c は、図 8 に示す書換え諸元データを参照し、書換え対象 ECU 1 9 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あると判定し、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。

[0713] 電源自己保持指示部 9 2 d 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あると第 1 電源自己保持判定部 9 2 c 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 9 2 d 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し続ける態様がある。電源自己保持指示部 9 2 d は、図 8 に示す書換え諸元データを参照し、書換え対象 ECU 1 9 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いが、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。

[0714] 即ち、電源自己保持指示部 9 2 d 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 9 2 d 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 9 2 d は、自己保

持要求を車両用スレーブ装置に定期的に出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し続ける。

[0715] 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。

[0716] 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。

[0717] 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、車両バッテリー40のバッテリー残量、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、車両バッテリー40のバッテリー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。

[0718] 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。

[0719] 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。

[0720] 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。

[0721] 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。

[0722] 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。

[0723] 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）。

[0724] 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（S 2 6 0 6）、電源自己保持の停止条件が成立したと判定すると（S 2 6 0 6 : Y E S）、第2電源自己保持回路を停止させ（S 2 6 0 7）、電源自己保持の実行制御処理を終了する。

[0725] 以上は、C G W 1 3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。

[0726] 書換え対象E C U 1 9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（S 2 6 1 1）。書換え対象E C U 1 9は、車両電源がオフであると判定すると（S 2 6 1 1 : Y E S）、自己保持回路を起動し（S 2 6 1 2）、電源自己保持の停止条件が成立したか否かを判定し（S 2 6 1 3）、C G W 1 3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（S 2 6 1 4）。書換え対象E C U 1 9は、C G W 1 3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（S 2 6 1 4 : Y E S）、その起動中の電源自己保持回路の動作期間を延長する（S 2 6 1 5）。書換え対象E C U 1 9は、電源自己保持の停止条件が成立したと判定すると（S 2 6 1 3 : Y E S）、電源自己保持回路を停止させ（S 2 6 1 6）、電源自己保持の実行制御処理を終了する。

[0727] 以上は、書換え対象E C U 1 9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C G W 1 3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。

[0728] 以上は、車両用スレーブ装置が書換え対象E C U 1 9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E C U 2 0の場合も同様である。図222に示すように、書換え対象E C U 1 9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。

[0729] 以上に説明したように、C G W 1 3 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 E C U 1 9 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 E C U 1 9 に指示するようにした。書換え対象 E C U 1 9 において、C G W 1 3 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。

[0730] 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 2 2 3 から図 2 3 3 を参照して説明する。ここでは、第 1 バスに接続される E C U （ I D 1 ）、E C U （ I D 2 ）及び E C U （ I D 3 ）のアプリプログラムを書換え、第 2 バスに接続される E C U （ I D 4 ）、E C U （ I D 5 ）及び E C U （ I D 6 ）のアプリプログラムを書換えない例について説明する。E C U （ I D 1 ）と E C U （ I D 4 ）が 1 面単独メモリであり、E C U （ I D 5 ）が 1 面サスペンドメモリであり、E C U （ I D 2 ）、E C U （ I D 3 ）及び E C U （ I D 6 ）が 2 面メモリである。又、E C U （ I D 1 ）、E C U （ I D 4 ）、E C U （ I D 5 ）及び E C U （ I D 6 ）は I G 電源系 E C U であり、E C U （ I D 2 ）は A C C 電源系 E C U であり、E C U （ I D 3 ）は + B 電源系 E C U である。

[0731] 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（S 5 0 0 1）。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）。

[0732] 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）。

[0733] 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）。

[0734] 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。

[0735] 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）。

[0736] 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）。

[0737] 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。

[0738] 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キングし、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。

[0739] 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。

[0740] 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、その受信した配信諸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）。

[0741] 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）。

- [0742] 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キングし（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）。
- [0743] 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ECU19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、検証しておくが良い。
- [0744] 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。
- [0745] 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。

[0746] CGW13は、各書換え対象ECU19へのインストールと並行して、バッテリー残量の監視（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ー負荷の値、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、バッテリー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。

[0747] 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ー残量があることを確認する必要がある。

[0748] 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。

[0749] 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

(I D 1) は、受信した全データの情報を用いて、書込みデータが自 E C U に整合するか否かを判定する (S 5 1 0 4) 。 E C U (I D 1) は、整合すると判定した場合、書込み処理を行う。

[0750] C G W 1 3 は、 D C M 1 2 から E C U (I D 1) への書込みデータのうち所定サイズ (例えば 1 k バイト) の分割ファイルを取得し、 E C U (I D 1) へ配信する (S 5 1 0 5) 。 E C U (I D 1) は、 C G W 1 3 から受信した分割ファイルをフラッシュメモリ 3 3 d に書込む (S 5 1 0 6) 。 E C U (I D 1) 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 (S 5 1 0 7) 。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。 E C U (I D 1) は、リトライポイントを記憶すると、 C G W 1 3 に書込み完了を通知する (S 5 1 0 8) 。

[0751] C G W 1 3 は、 E C U (I D 1) から書込み完了の通知を受けると、 D C M 1 2 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 (S 5 1 0 9) 。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 E C U (I D 1) 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、 D C M 1 2 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 (S 5 1 1 0) 。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 (S 5 1 1 1) 。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。 C G W 1 3 は、 E C U (I D 1) 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 (S 5 1 1 2) 。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 (S 5 1 1 3) 。 E C U (I D 2) 、 E C U (I D 3) 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。

[0752] 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。

[0753] 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、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。

[0754] 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。

[0755] CGW13は、ECU（ID3）に対するインストールが全て完了すると、バッテリー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）。

[0756] 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。

- [0757] 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)。
- [0758] 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)。
- [0759] 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)。
- [0760] 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（S 5 4 1 6）。尚、車両が駐車状態等、進捗表示が不要な場合、C G W 1 3 は、車載ディスプレイ 7 へ進捗を通知しない。

[0761] 最後に、C G W 1 3 は、電源管理 E C U 2 0 に対し、I G 電源オフを要求する（S 5 4 1 8）。電源管理 E C U 2 0 は、インストール開始前の I G 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 4 3 に要求する。電源制御回路 4 3 により、I G 電源ライン 3 9 及び A C C 電源ライン 3 8 への電力供給が遮断されると、E C U（I D 1）、E C U（I D 2）、E C U（I D 4）、E C U（I D 5）及び E C U（I D 6）は、停止状態となる。

[0762] 上述の例では、1 面単独メモリである E C U（I D 1）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 E C U 1 9 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 E C U 1 9 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。

[0763] 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 2 3 0 から図 2 3 3 を参照して説明する。具体的には、E C U（I D 1）に対してインストールが完了し、E C U（I D 2）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。

[0764] 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（S 6 0 0 1）。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（S 6 0 0 2）。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（S 6 0 0 3）。

[0765] C G W 1 3 は、D C M 1 2 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 E C U（I D 1）、E C U（I D 2

）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。

[0766] 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。

[0767] CGW13は、ECU（ID2）に対するロールバック処理として、書き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。

[0768] 具体的には、CGW13は、DCM12からECU（ID2）に対する書き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）。書き込みが完了すると、ECU（ID2）は、途中から書き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に書き込み完了を通知する（S6010）。

[0769] CGW13は、ECU（ID2）から書き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。

[0770] 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。

[0771] 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。

[0772] 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1 k 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に、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）。

[0773] 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の処理を繰り返す。

[0774] 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、バッテリー残量の監視及びバスの通信負荷の監視を終了する（S6116、S6117）。

[0775] 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（S 6 2 0 1）。CGW 1 3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（ID 1）、ECU（ID 2）及びECU（ID 3）に対し、ロールバック用のアクティベートを要求する（S 6 2 0 2）。1面単独メモリであるECU（ID 1）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（ID 2）及びECU（ID 3）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。

[0776] ECU（ID 1）は、CGW 1 3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（S 6 2 0 3）。ECU（ID 1）は、再起動が完了すると、CGW 1 3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（S 6 2 0 4）。

[0777] ECU（ID 2）は、CGW 1 3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（S 6 2 0 5）。ECU（ID 2）は、引き続き運用面であるA面で正常に起動すると、CGW 1 3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（S 6 2 0 6）。

[0778] ECU（ID 3）は、CGW 1 3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（S 6 2 0 7）。ECU（ID 3）は、引き続き運用面であるA面で正常に起動すると、CGW 1 3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（S 6 2 0 8）。

[0779] CGW 1 3は、ECU（ID 1）、ECU（ID 2）及びECU（ID 3）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、DCM 1 2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（S 6 2 0 9）。ここで、CGW 1 3は、ECU（ID 1）、ECU（ID 2）及びECU（ID 3）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、DCM 1 2から通知された情報をデータベースへ登録する

と共に（S 6 2 1 0）、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（S 6 2 1 1）。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（S 6 2 1 2）。

[0780] 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（S 6 2 1 3）。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（S 6 2 1 4）。

[0781] 最後に、CGW13は、電源管理ECU20に対し、IG電源オフを要求する（S 6 2 1 5）。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。

[0782] 以上のように、CGW13をリプログラマスタとして複数の書換え対象ECU19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。

[0783] 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。

[0784] 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。

[0785] (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Wi-Fi (Wireless Fidelity) (登録商標) 等を含んで構成される。

[0786] 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。

[0787] 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。

[0788] 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。

[0789] 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、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。

[0790] 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。

[0791] 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。

[0792] 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。

[0793] 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。

[0794] 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。

[0795] 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。

[0796] 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がイーサネットにより接続されても良い。

[0797] 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ラ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ラブとして機能する。

[0798] 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。

[0799] 図235に示すように、CGW13は、電氣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。

[0800] 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、バッテリー電源（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。

[0801] 図236に示すように、ECU19は、電氣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。

[0802] 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。

[0803] 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、車両バッテリー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ー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、車両バッテリー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。

[0804] I G電源ライン34は、I Gスイッチ37を介して車両バッテリー35の正極に接続されている。ユーザがI G操作を行うと、I Gスイッチ37がオフからオンに切替わり、車両バッテリー35の出力電圧がI G電源ライン34に印加される。I G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。車両バッテリー35の負極は接地されている。

[0805] ACCスイッチ36とI G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、I G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I G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I G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I G電源が車両側システム4に供給されている状態をI G電源状態と称する。

[0806] 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、I G電源状態で起動するI G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。

[0807] 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。

[0808] 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と車両バッテリー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と車両バッテリー35の正極を電源制御回路38の内部で途絶させる。

[0809] 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。

[0810] 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。

[0811] 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。

[0812] 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E C U 1 9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。

[0813] D C M 1 2 は、D C M 用の書換え諸元データを取得すると、そのD C M 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C G W 1 3 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。C G W 1 3 は、C G W 用の書換え諸元データを取得すると、そのC G W 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D C M 1 2 からの書込みデータの取得や書換え対象E C U 1 9 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。

[0814] ファイルサーバ8には、上記したリログデータが登録されると共に、O E M から提供される配信諸元データが登録される。O E M 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。

[0815] ファイルサーバ8は、リログデータと配信諸元データが登録されると、リ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D C M 1 2 に送信する。尚、ファイルサーバ8は、図238では、リ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、リログデータと配信諸元データを同時にD C M 1 2 に送信する場合を例示しているが、リログデータと配信諸元データを別々にD C M 1 2 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D C M 1 2 に送信し、後からリログデータをD C M 1 2 に送信しても良い。又、ファイルサーバ8は、リ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D C M 1 2 へ送信しても良い。

[0816] D C M 1 2 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ラムデータとを検証し、検証結果が正であると、暗号済みのリプログラムデータを復号化する。DCM12は、暗号済みのリプログラムデータを復号化すると、その復号化したリプログラム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。

[0817] 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203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。

[0818] 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。

[0819] 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、バッテリー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。

[0820] 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。

[0821] 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。

[0822] 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。

[0823] 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。

[0824] 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。

[0825] 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。

[0826] 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ECU 19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。

[0827] 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、センタ装置3が演算して登録する形式としても良い。

[0828] 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、ECU 19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。

[0829] 又、ECUメタデータDB205には、ECU 19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ECU 19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ECU 19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、ECU 19が備えるフラッシュメモリ28dのメモリ構成、ECU 19が接続されているバス種別、ECU 19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。

[0830] 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ECU 19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CGW 13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ECU 19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。

[0831] 図245に示すように、個車情報DB 213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、ECU 19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。

[0832] 「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。

[0833] 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。

[0834] 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、サプライヤの作業員から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)。

[0835] 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。

[0836] 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。

[0837] 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。

[0838] 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の作業からの入力を受け付ける。まず、諸元データ生成部201は、更新対象とするECU19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の作業により指定された順番を特定のECU順序とする。

[0839] 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ECU 19を抽出する。例えば、図242において、「ADS」「BRK」「EPS」が更新対象ECU 19である。諸元データ生成部201は、構成情報DB 208に登録されている順番を、特定のECU順序とする。

[0840] 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DB 208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。

[0841] 次に、諸元データ生成部201は、ECUメタデータDB 205にアクセスして、更新対象としたECU 19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。

[0842] 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、バッテリー電源（+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。

[0843] 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ー残量の制約を示す「バッテリー負荷（バッテリーの残量）」、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。

[0844] 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に制御し、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。

[0845] 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。

[0846] 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（B 6）。すなわち、諸元データ生成部 2 0 1 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 E C U 情報については、グループの若い順かつグループ内 E C U 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 2 4 2 において、グループ 1 を「A D S」とし、グループ 2 を 1 番目が「B R K」、2 番目が「E P S」とする場合、諸元データの E C U 情報欄は、最初に「A D S」の E C U 情報、次に「B R K」の E C U 情報、最後に「E P S」の E C U 情報が並ぶこととなる。

[0847] 図 2 5 0 に示す諸元データにおいて、E C U 情報の「E C U I D」～「転送サイズ」は、対象 E C U 1 9 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、E C U 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。

[0848] 図 2 5 2 では、パッケージ生成部 2 0 2 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」＝「a a a」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 2 5 2 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 3 A のパッケージ生成部 2 0 2 を起動する。パッケージ生成部 2 0 2 は、ステップ B 1 と同様に更新対象とする「E C U S W I D」を決定する（C 1）。パッケージ生成部 2 0 2 は、更新対象とする「E C U S W I D」に対応する各データを E C U リプロデータ D B 2 0 4 より取得して 1 つのリプロデータを生成する（C 2）。例えば、図 2 4 3 において、パッケージ生成部 2 0 1 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、リプロデータを生成する。そして、生成したリプロデータとステップ B 1 ～ B 6 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）。

[0849] 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。

[0850] 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「ECUID」及びECU19に記憶されるアプリプログラムの「ECUSWID」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。

[0851] 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。

[0852] 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。

[0853] 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。

[0854] 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「バッテリー負荷」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。

[0855] 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ECUID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。

[0856] (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。

[0857] 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

ユ関数として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。

[0858] 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。

[0859] 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。

[0860] 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。

[0861] 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。

[0862] 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。

[0863] 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。

[0864] 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、VIN=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。

[0865] 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。

[0866] 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、バッテリー残量、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)。

[0867] 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。

[0868] 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。

[0869] 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。

[0870] 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。

[0871] 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。

[0872] 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。

[0873] 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。

[0874] 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。

[0875] 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。

[0876] 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。

[0877] 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 D 2 3 において、双方のハッシュ値に差異が無ければ（N O）処理を終了する。尚、フラッシュメモリ 2 4 d 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。

[0878] （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 3 D が実行する機能に関する。図 2 5 8 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 C o n f i g ファイルにより H T T P 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 に対して定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 D B 2 1 7 に対応する車両；V I N 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 H T T P 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 I G オンのタイミングで実行されることとなる。

[0879] 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 H T T P 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。

[0880] そこで、図 2 5 9 に示すように、センター装置 3 の S M S 送信制御部 2 1 2 は、定期的又は所定のタイミングで、個車情報 D B 2 1 3 を参照して各車両のアクセスログをチェックする（E 1）。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。

[0881] 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。

[0882] 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。

[0883] 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、バッテリー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。

[0884] 仮に、EV車のバッテリー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ー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ー残量を参照し、指定されたバッテリー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。

[0885] 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）。

[0886] 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。

[0887] 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場合、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。

[0888] 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。

[0889] 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。

[0890] 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ー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。

[0891] 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。

[0892] 又、センター装置 3 は、個車情報 DB 213 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。

[0893] 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 DB 213 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。

[0894] 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 DB 213 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 DB 213 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。

[0895] (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。

[0896] 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。

[0897] (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。

[0898] 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)。

[0899] 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)。

[0900] 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)。

[0901] 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。

[0902] 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×1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。

[0903] 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DB2

06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。

[0904] 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キングする（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。

[0905] 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、「O

「T A マスタ」は「D C M」と同義である。C P U 2 8 a は書き込み処理部の一例である。

[0906] 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、E C U 1 9 はロールバック処理を行うこととなる。E C U 1 9 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、E C U 1 9 は、更新データの書き込みを完了した後、ロールバック用差分データを用いた書き込みを開始する。そして、書き込みを完了した後、E C U 1 9 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 2 8 d 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、E C U 1 9 でなく、マスタ装置 1 1 が行う構成としても良い。

[0907] 図 2 6 4 に示すように、その後、上記車両の I G スイッチ 3 7 が O N されると、それを契機として E C U 1 9 は、起動時のデータ検証を行う。E C U 1 9 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。まず、フラッシュメモリ 2 8 d 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 2 8 d 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「O K」であれば、E C U 1 9 は通常通り起動処理を行う。各 E C U 1 9 について同様の処理が行われ、全ての評価対象 E C U 1 9 の結果が「O K」であれば、処理を終了する。

[0908] 一方、何れかの E C U 1 9 について検証の結果が異常；「N G」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。

[0909] 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）。

[0910] 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。

[0911] 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。

[0912] 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。

[0913] 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。

[0914] 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。

[0915] 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）。

[0916] 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、E C U 1 9 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。

- ・C P U 2 8 a は、ロールバックデータを用いてフラッシュメモリ 2 8 d への書込みを行う。

- ・第 1 検証処理部が、フラッシュメモリ 2 8 d 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。

[0917] 以上のように第 5 実施形態によれば、E C U リプロデータ D B 2 0 4 には、書換え対象であるターゲット E C U 1 9 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 2 0 2 は、複数のターゲット E C U 1 9 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 2 0 3 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。

[0918] 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 E C U 1 9 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。

[0919] C P U 2 8 a は、更新データをフラッシュメモリ 2 8 d に書込み、第 1 検証処理部は、フラッシュメモリ 2 8 d 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。

[0920] 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。

[0921] 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。

[0922] （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「c p n__001」について複数のパッケージ「p k g__001__1」及び「p k g__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「p k g __ 0 0 1 __ 1」には、グループ1に所属するECUである「A D S」及び「B R K」が含まれ、パッケージ「p k g __ 0 0 1 __ 2」には、グループ2に所属するECUである「E P S」が含まれる。

[0923] 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「A D S」及び「B R K」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「E P S」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「A D S」及び「B R K」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「p k g 0 0 1 __ 1 . d a t」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「E P 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「p k g 0 0 1 __ 2 . d a t」を生成する。

[0924] （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。

[0925] 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（I D 1）、ECU（I D 2）、ECU（I D 3）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。

[0926] 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。

[0927] 本実施形態によれば、前述した(5)書込みデータの配信判定処理を行うことで示す作用効果を得ることができる。CGW13において、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。

[0928] CGW13において、第1条件が成立しているか否かを判定し、第1条件が成立していると判定した後に、第1条件以外の条件が成立しているか否かを判定するようにした。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他の条件よりも先に判定することで、インストールに関するユーザ承諾を、最初に得るように構成することができる。第2条件から第5条件による判定結果は、車両動作に伴って変動し得るので、第1条件が成立したことを契機として第2条件から第5条件を判定する方が効率的である。第1条件が成立していると判定した後に、第1条件以外の条件が成立しているか否かを判定することで、第1条件から第5条件を効率的に判定することができる。又、第5条件は、改ざん等を考慮してインストールの直前、即ち、最後に判定することで、改ざん等によるリスクを適切に回避することができる。

[0929] CGW13において、第1条件以外の条件が成立しているか否かを判定し

、第1条件以外の条件が成立していると判定した後に、第1条件が成立しているか否かを判定するようにした。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他の条件よりも後に判定することで、インストールに関するユーザ承諾を、第1条件以外の条件が成立した状態で得るように構成することができる。例えば書換え対象ECU19が故障コードを発生していたり書込みデータが改ざんされていたりすると、インストール承諾画面506において更新ボタン506aが操作されても、インストールが開始されないこととなるが、第1条件以外の条件が成立しているか否かを先に判定することで、インストール承諾画面506において更新ボタン506aが操作されたにも拘らずインストールが開始されない状況を未然に回避することができる。

[0930] CGW13において、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すると、アクティベートに関するユーザ承諾が得られている第6条件、車両状態がアクティベート可能な状態である第7条件、書換え対象の電子制御装置がアクティベート可能な状態である第8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アクティベートを書換え対象ECU19に指示するようにした。書換え対象ECU19に対してアクティベートを適切に指示することができる。

[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〕 外部から更新データを取得し、その取得した更新データを用いたインストールを書換え対象の電子制御装置に指示し、その取得した更新データを書換え対象の電子制御装置に配信する車両用マスタ装置（11）において、

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、書換え対象の電子制御装置がインストール可能な状態である第4条件、更新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か否かを判定するインストール条件判定部（77a）と、

前記第1条件、前記第2条件、前記第3条件、前記第4条件及び前記第5条件の全てが成立していると前記インストール条件判定部により判定された場合に、前記更新データを用いたインストールを書換え対象の電子制御装置に指示するインストール指示部（77b）と、を備える車両用マスタ装置。

〔請求項2〕 前記インストール条件判定部は、前記第1条件が成立しているか否かを判定し、前記第1条件が成立していると判定した後に、前記第2条件、前記第3条件、前記第4条件及び前記第5条件が成立しているか否かを判定する請求項1に記載した車両用マスタ装置。

〔請求項3〕 前記インストール条件判定部は、前記第2条件、前記第3条件、前記第4条件及び前記第5条件が成立しているか否かを判定し、前記第2条件、前記第3条件、前記第4条件、及び前記第5条件の全てが成立していると判定した後に、前記第1条件が成立しているか否かを判定する請求項1に記載した車両用マスタ装置。

〔請求項4〕 センター装置から更新に関する車両状態情報を取得する車両状態情報取得部（77c）を備え、

前記インストール条件判定部は、センター装置から前記車両状態情

報取得部により取得された車両状態情報に基づいて前記第3条件が成立しているか否かを判定する請求項1から3の何れか一項に記載した車両用マスタ装置。

[請求項5] 前記インストール条件判定部は、第1書換え対象の電子制御装置に対して前記第4条件及び前記第5条件が成立しているか否かを判定し、

前記インストール指示部は、前記第1条件、前記第2条件、前記第3条件、前記第1書換え対象の電子制御装置に対する前記第4条件及び前記第5条件の全てが成立していると前記インストール条件判定部により判定された場合に、更新データを用いたインストールを第1書換え対象の電子制御装置に指示し、

前記インストール条件判定部は、前記インストール指示部がプログラムのインストールを第1書換え対象の電子制御装置に指示した後に、第2書換え対象の電子制御装置に対して前記第4条件及び前記第5条件が成立しているか否かを判定し、

前記インストール指示部は、前記第1条件、前記第2条件、前記第3条件、第2書換え対象の電子制御装置に対する前記第4条件及び前記第5条件の全てが成立していると前記インストール条件判定部により判定された場合に、更新データを用いたインストールを第2書換え対象の電子制御装置に指示する請求項1から4の何れか一項に記載した車両用マスタ装置。

[請求項6] 前記インストール条件判定部は、第1書換え対象の電子制御装置に対して前記第4条件及び前記第5条件が成立しているか否かを判定し、第2書換え対象の電子制御装置に対して前記第4条件及び前記第5条件が成立しているか否かを判定し、

前記インストール指示部は、前記第1条件、前記第2条件、前記第3条件、第1書換え対象の電子制御装置に対する前記第4条件及び前記第5条件、第2書換え対象の電子制御装置に対する前記第4条件及

び前記第5条件の全てが成立していると前記インストール条件判定部により判定された場合に、更新データを用いたインストールを第1書換え対象の電子制御装置又は第2書換え対象の電子制御装置に指示する請求項1から4の何れか一項に記載した車両用マスタ装置。

[請求項7] 書換え対象の全ての電子制御装置においてインストールが完了した場合に、インストールした前記更新データを有効化するアクティベートに関するユーザ承諾が得られている第6条件、車両状態がアクティベート可能な状態である第7条件、書換え対象の電子制御装置がアクティベート可能な状態である第8条件、の全てが成立しているか否かを判定するアクティベート条件判定部（77d）と、

前記第6条件、前記第7条件及び前記第8条件の全てが成立していると前記アクティベート条件判定部により判定された場合に、アクティベートを書換え対象の電子制御装置に指示するアクティベート指示部（77e）と、を備える請求項1から6の何れか一項に記載した車両用マスタ装置。

[請求項8] 前記アクティベート条件判定部は、車両状態が駐車状態であるか否かに基づいて前記第7条件が成立しているか否かを判定する請求項7に記載した車両用マスタ装置。

[請求項9] 外部から更新データを取得し、その取得した更新データを用いたインストールを書換え対象の電子制御装置に指示し、その取得した更新データを書換え対象の電子制御装置に配信する車両用マスタ装置（11）において、

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、書換え対象の電子制御装置がインストール可能な状態である第4条件、更新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か否かを判定するインストール条件判定手順と、

前記第1条件、前記第2条件、前記第3条件、前記第4条件及び前記第5条件の全てが成立していると前記インストール条件判定手順により判定した場合に、前記更新データを用いたインストールを書換え対象の電子制御装置に指示するインストール指示手順と、を行うインストールの指示判定方法。

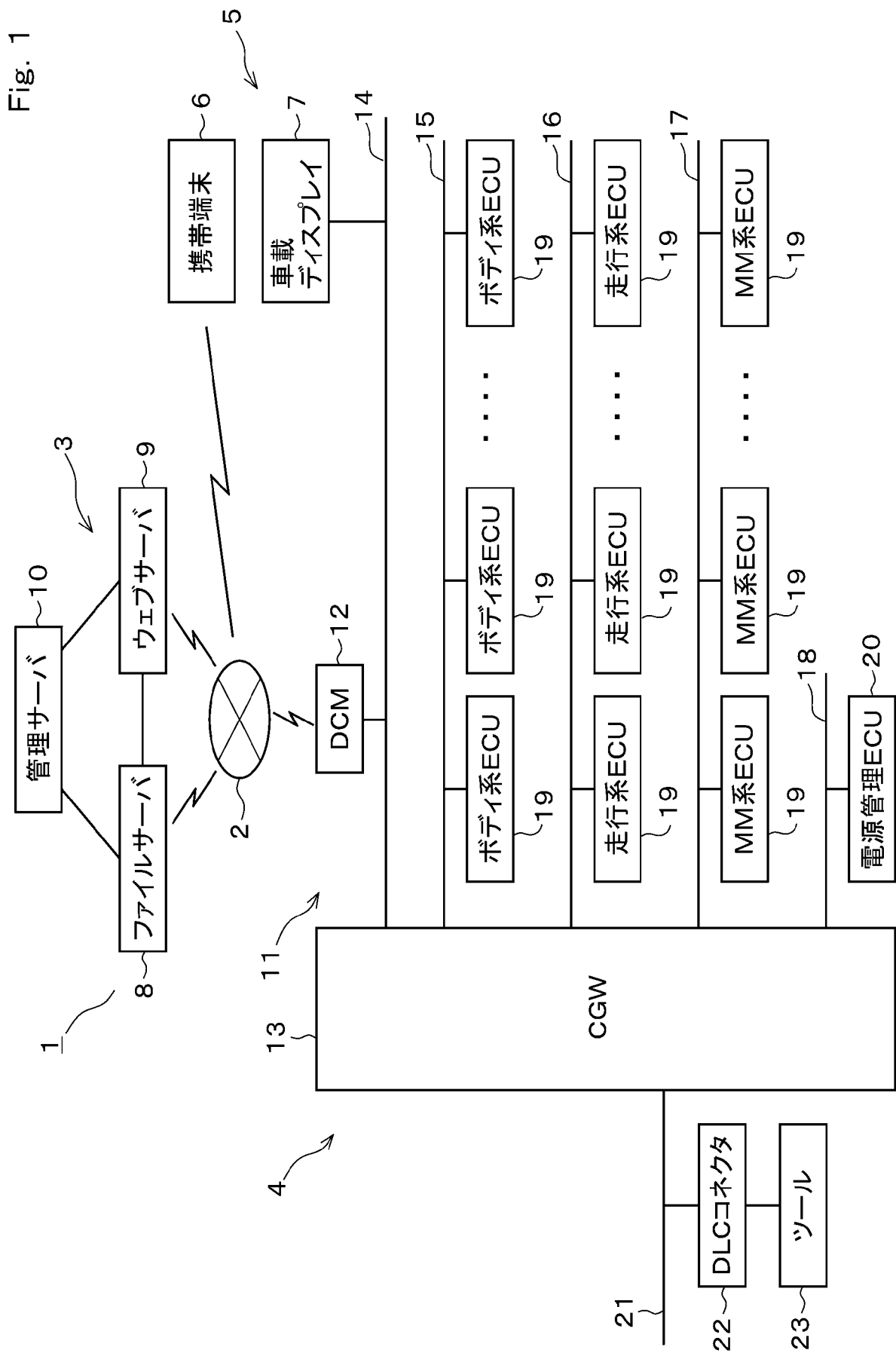
[請求項10]

外部から更新データを取得し、その取得した更新データを用いたインストールを書換え対象の電子制御装置に指示し、その取得した更新データを書換え対象の電子制御装置に配信する車両用マスタ装置（11）に、

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、センタ装置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、書換え対象の電子制御装置がインストール可能な状態である第4条件、更新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か否かを判定するインストール条件判定手順と、

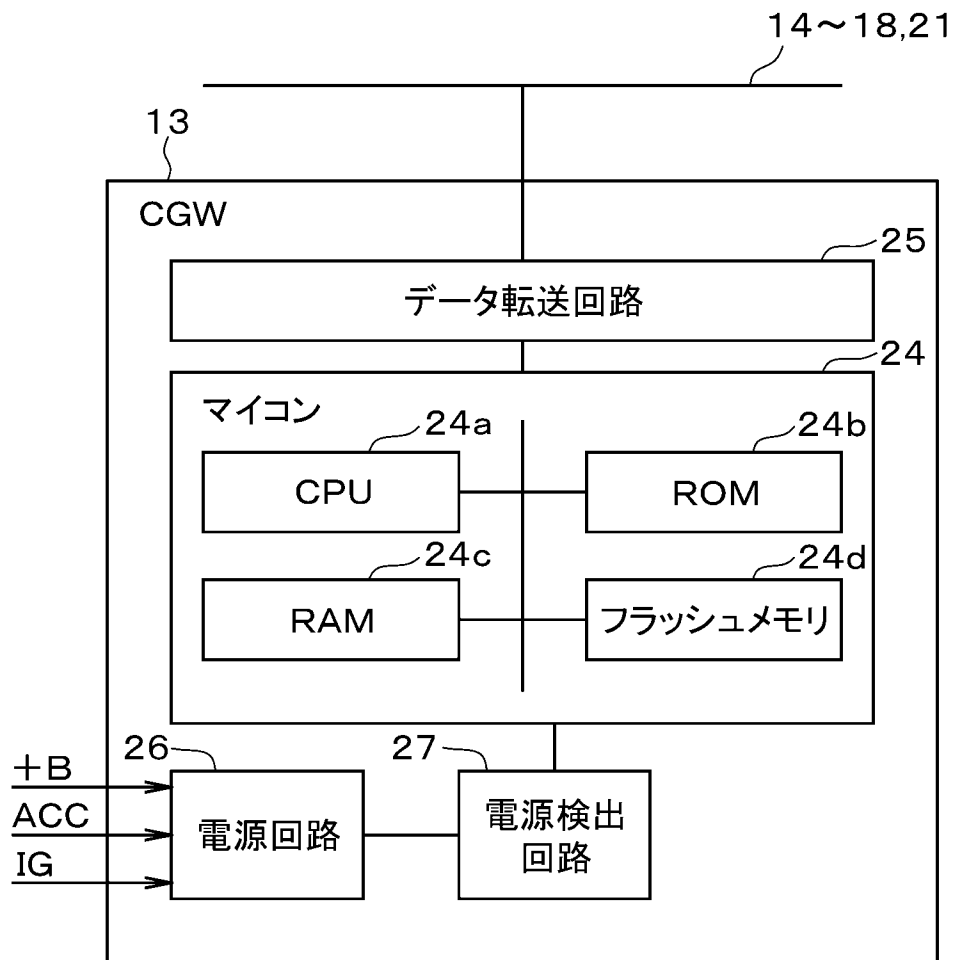
前記第1条件、前記第2条件、前記第3条件、前記第4条件及び前記第5条件の全てが成立していると前記インストール条件判定手順により判定した場合に、前記更新データを用いたインストールを書換え対象の電子制御装置に指示するインストール指示手順と、を実行させるインストールの指示判定プログラム。

[図1]



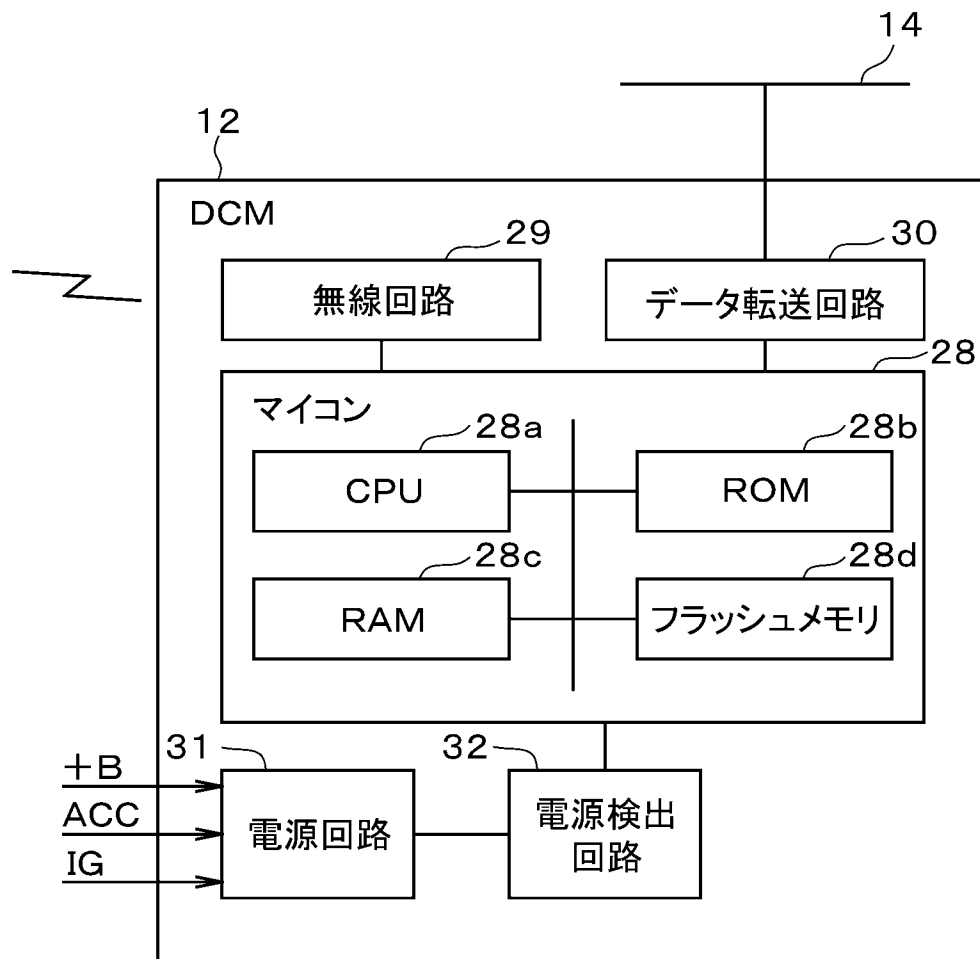
[図2]

Fig. 2



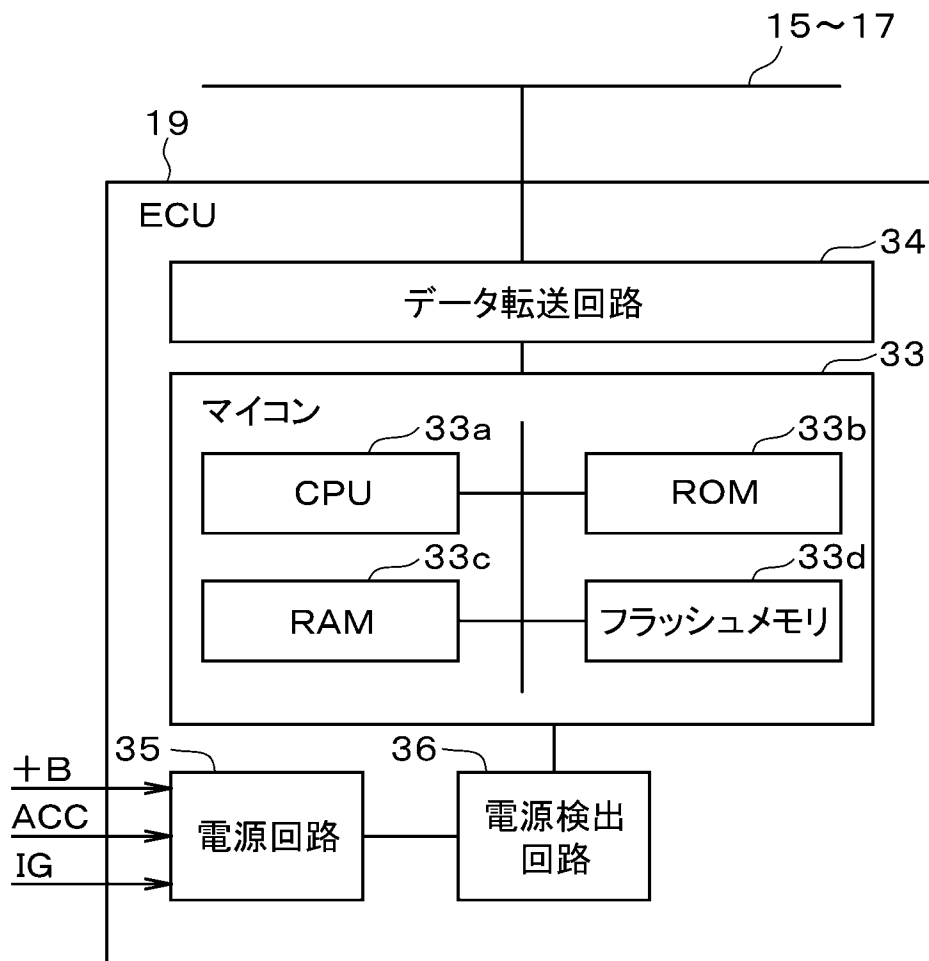
[図3]

Fig. 3

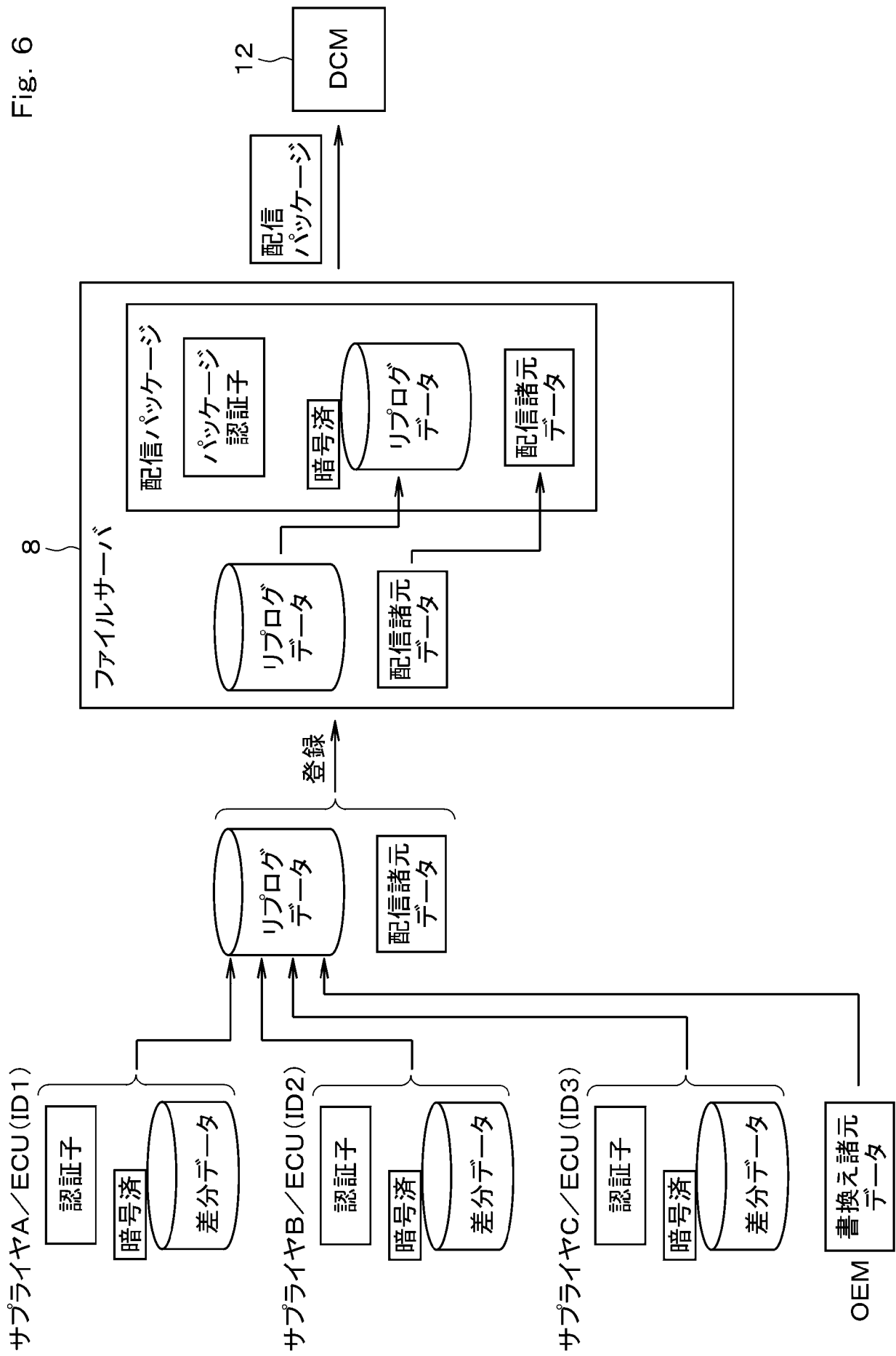


[図4]

Fig. 4



[図6]



[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
ECU (ID2) 情報	ロールバックプログラムサイズ	1Mbyte
	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
ECU (ID3) 情報	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_ID	3
	更新プログラム取得アドレス	0x50000000
ECU (ID4) 情報	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_ID	4
ECU (ID5) 情報	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 (ID6) 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
ECU (ID6) 情報	ロールバックプログラムサイズ	1Mbyte
	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
ECU (ID6) 情報	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]

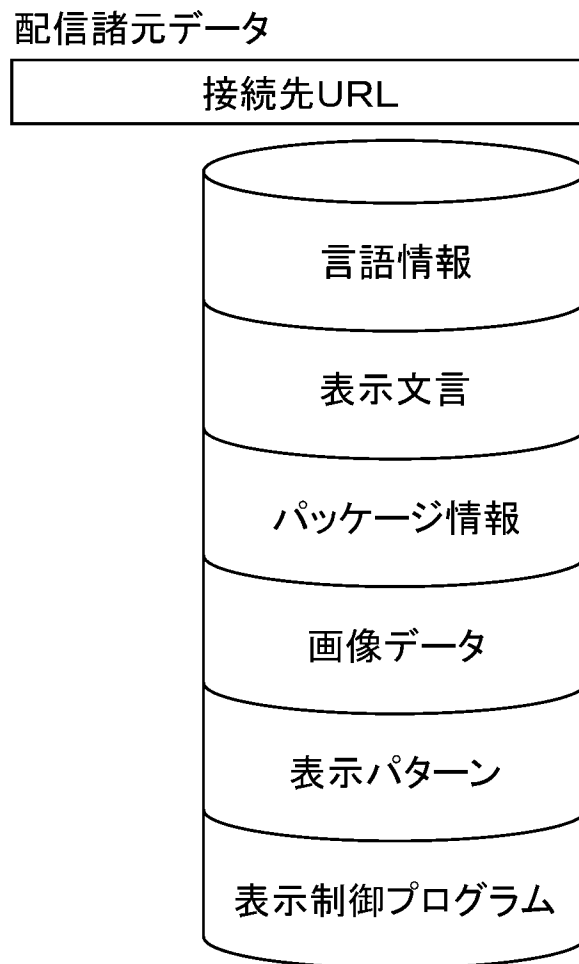
Fig.8

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
	バッテリー負荷	40%
書換え時の車両状態 シーン情報		全て駐車中／全て走行中／最適 リコール／ディーラー／工場用／ 機能更新通知／強制実行
	ECU ID	ECU ID
	接続バス	第1バス
ECU(IDn)情報 n=1~6	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

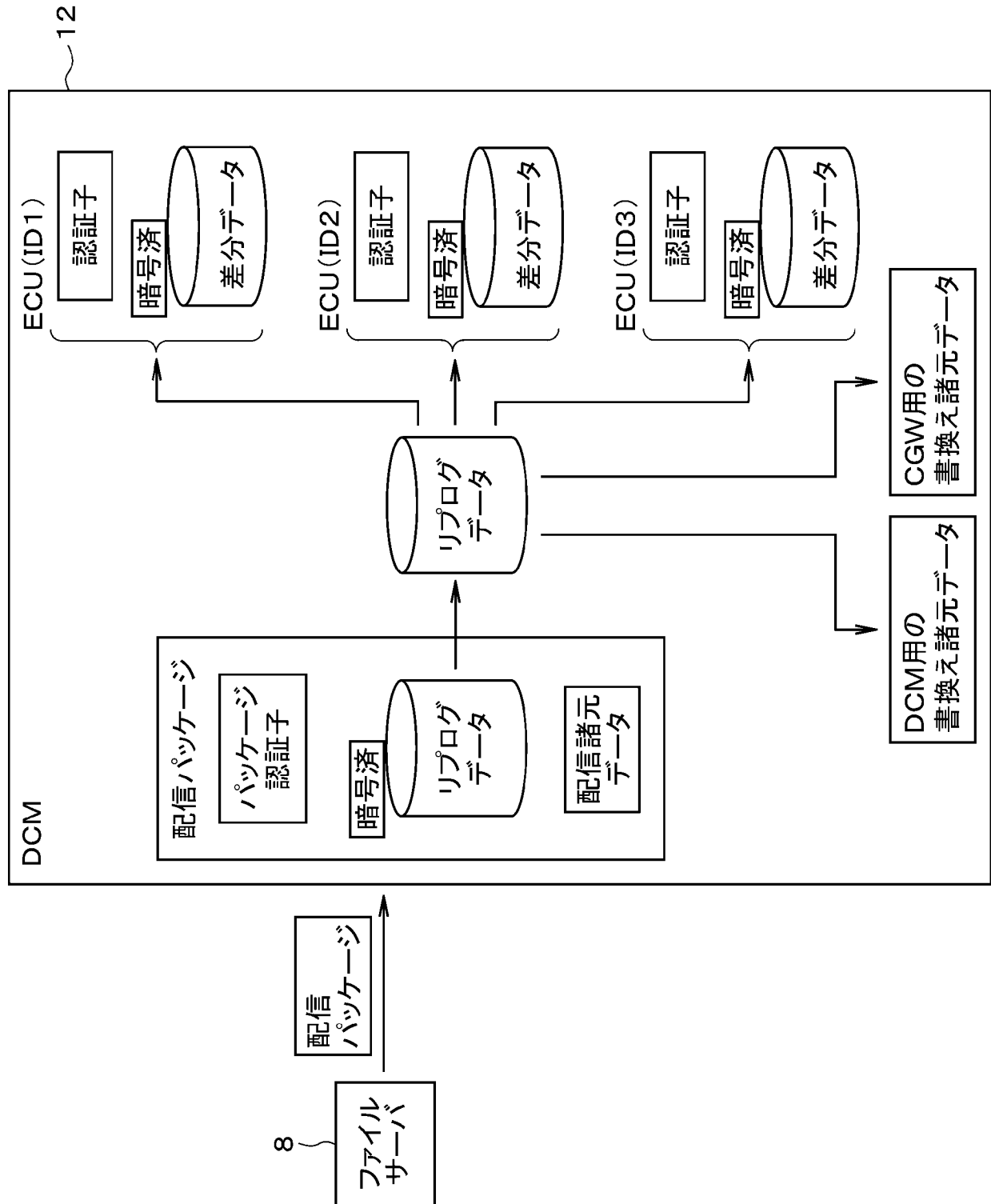
[図9]

Fig. 9



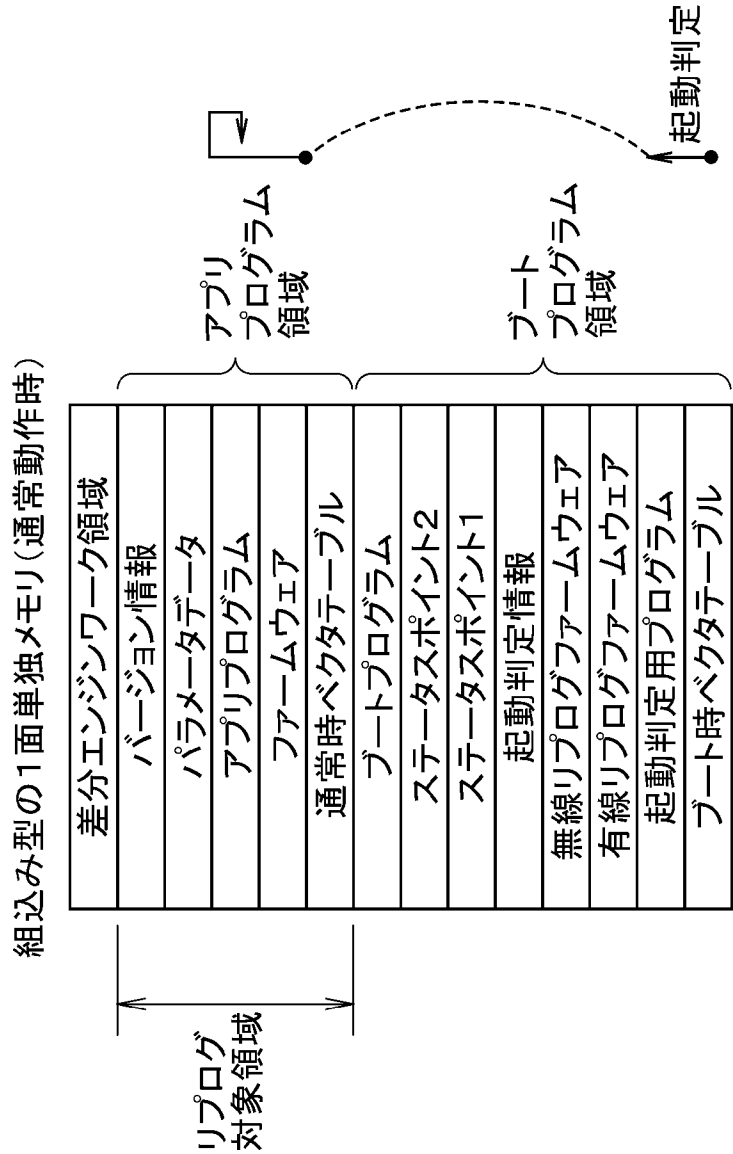
[図10]

Fig. 10



[図11]

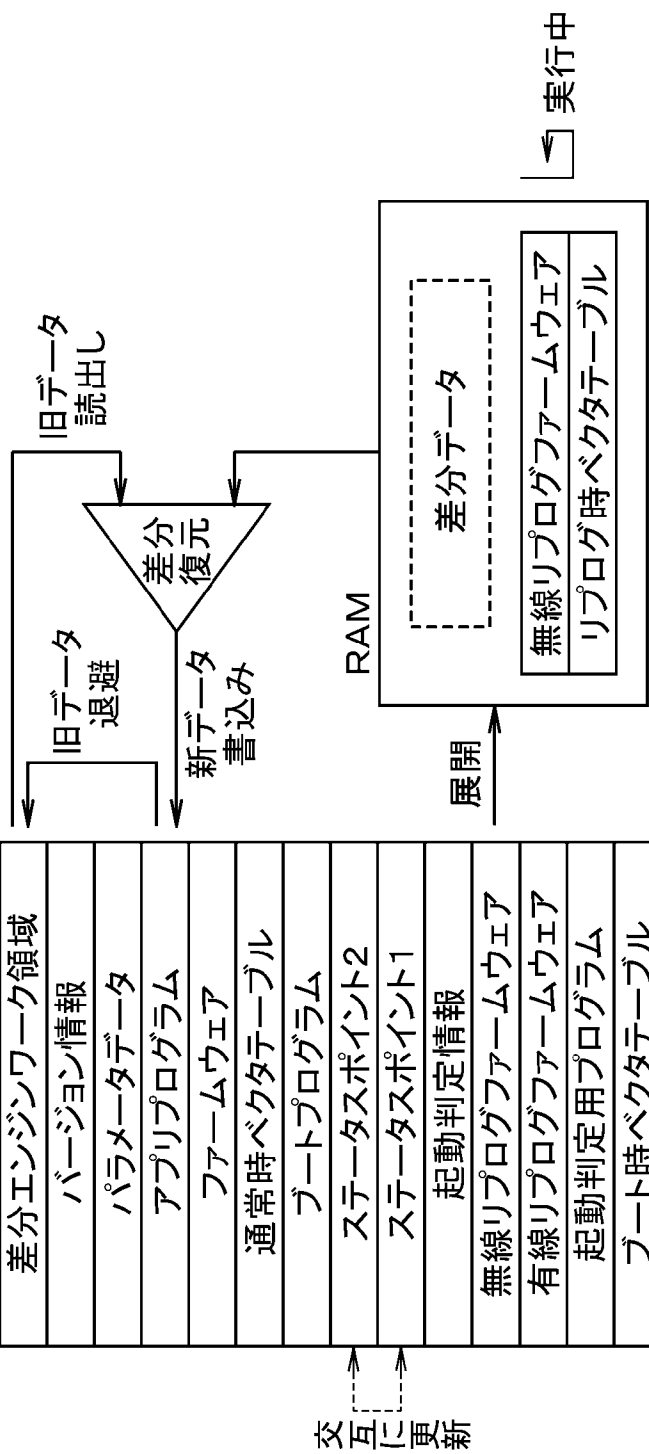
Fig. 11



[図12]

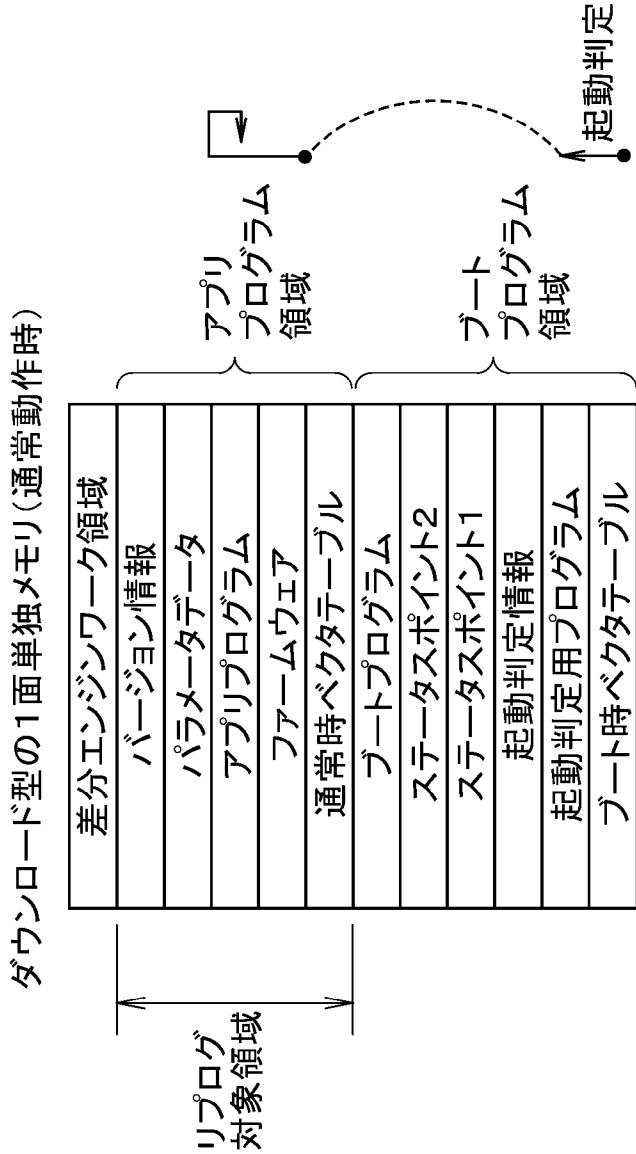
Fig. 12

組込み型の1面単独メモリ(書換え動作時)



[図13]

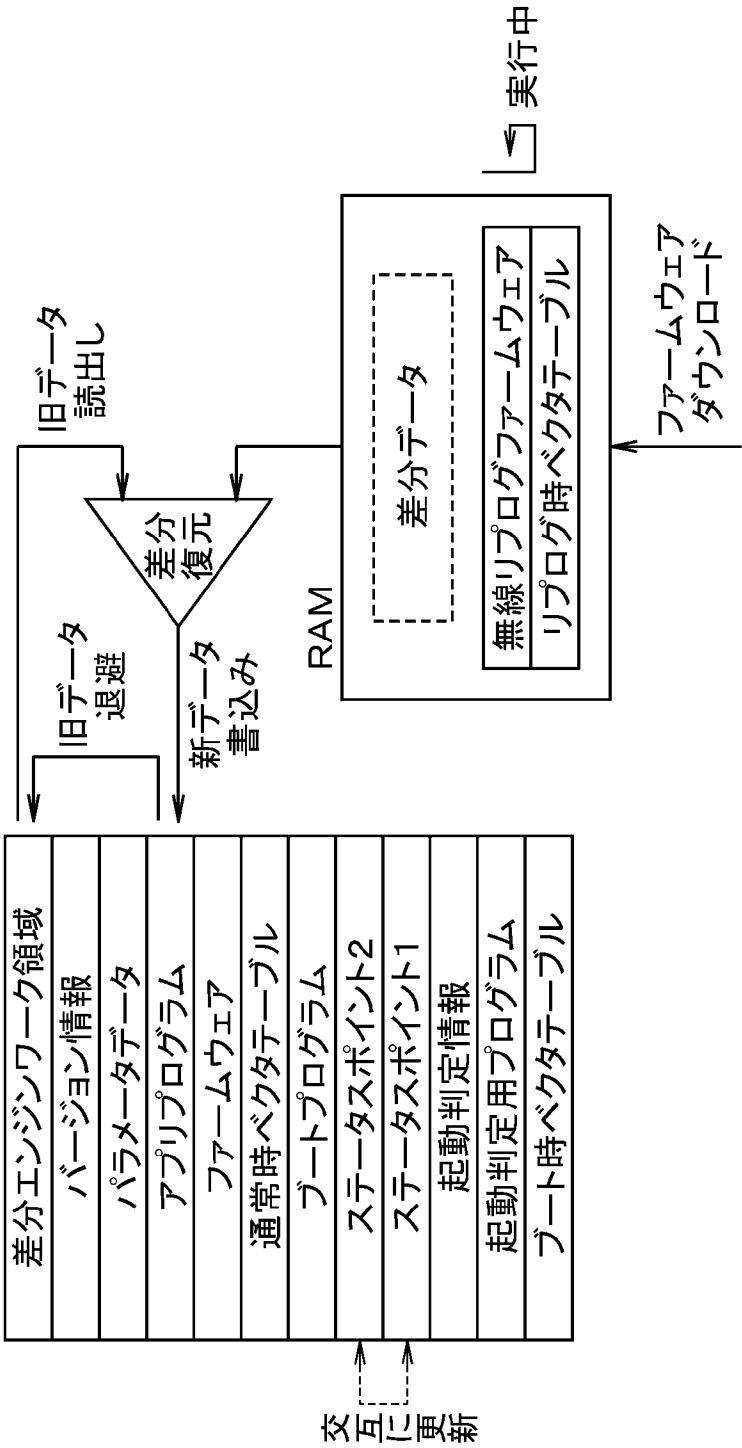
Fig. 13



[図14]

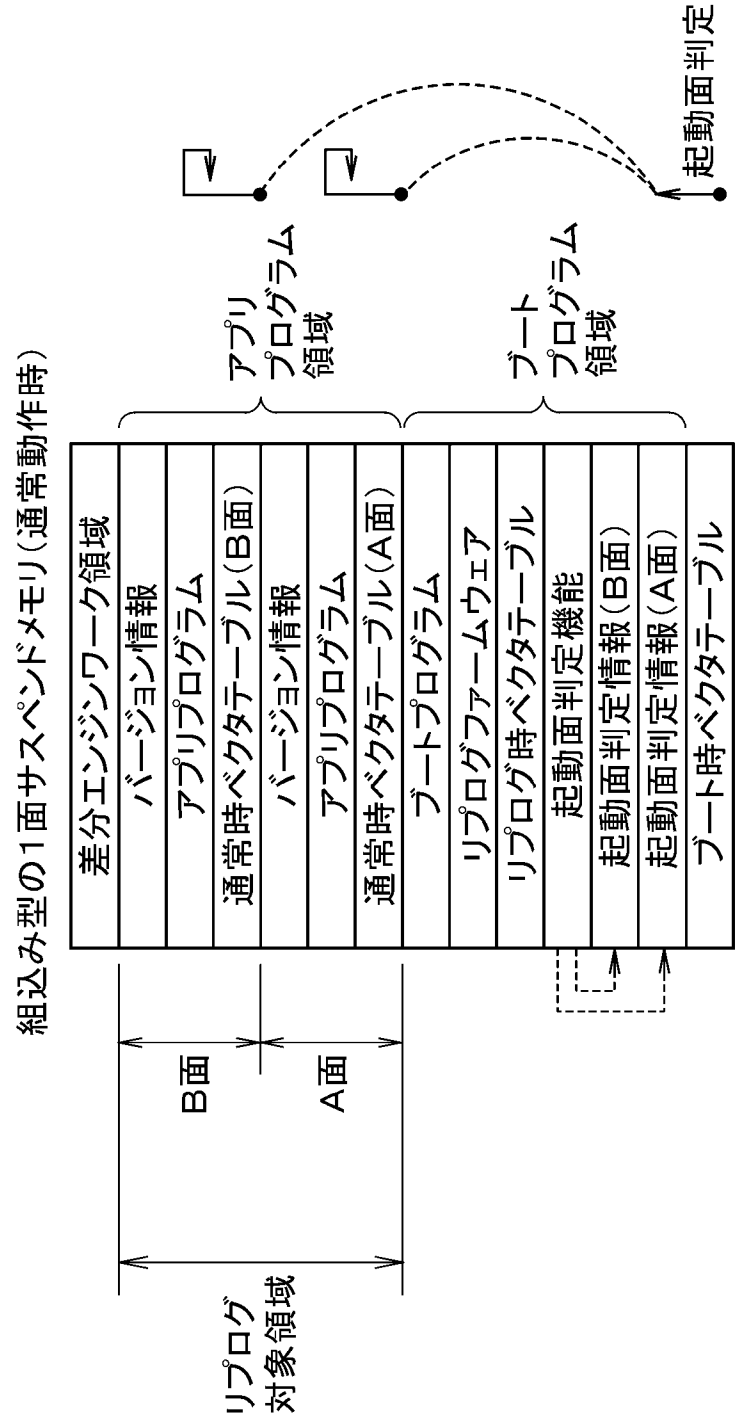
Fig. 14

ダウンロード型の1面単独メモリ(書換え動作時)



[図15]

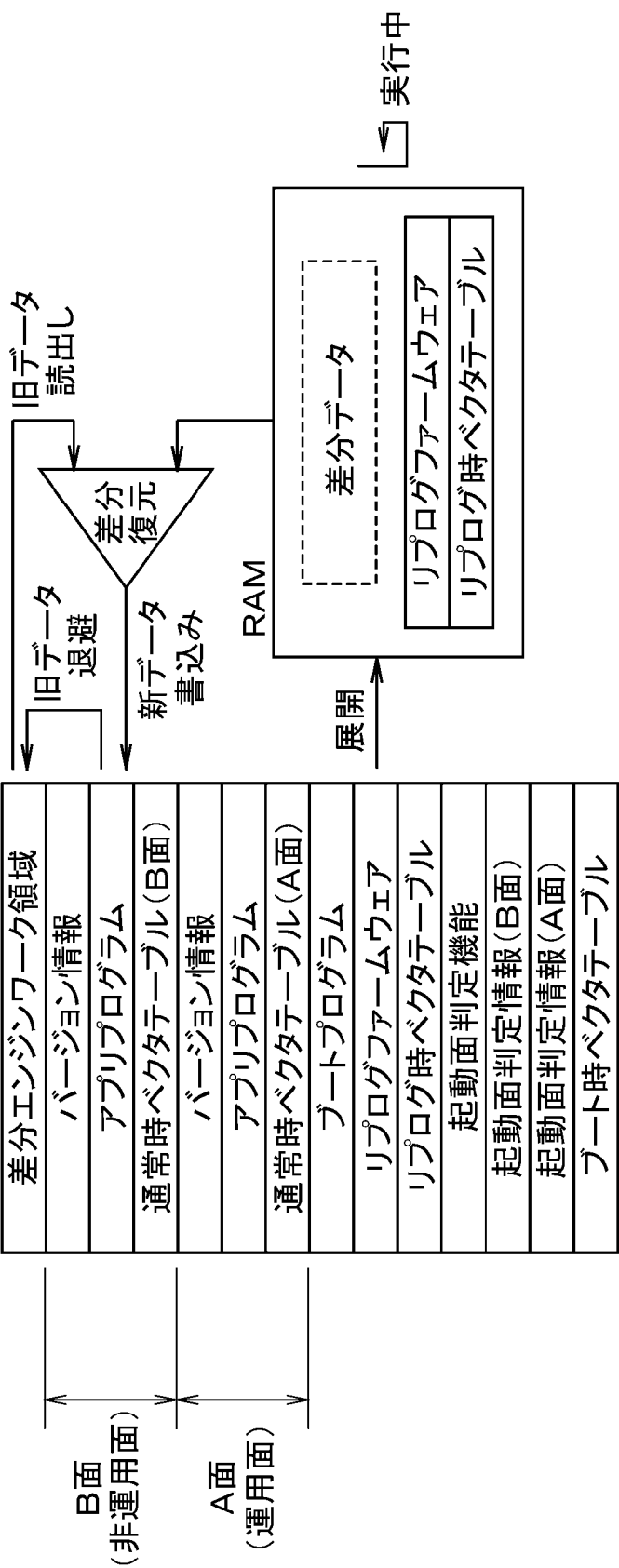
Fig. 15



[図16]

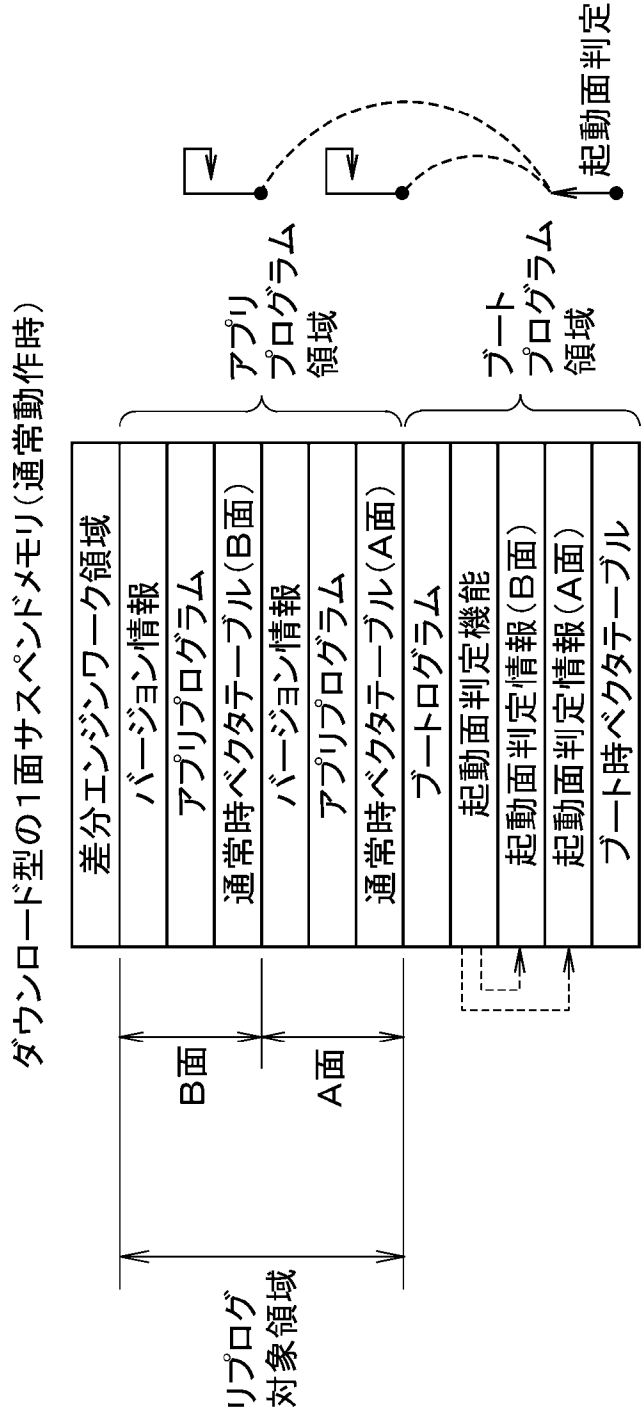
Fig. 16

組込み型の1面サスペンドメモリ(書換え動作時)



[図17]

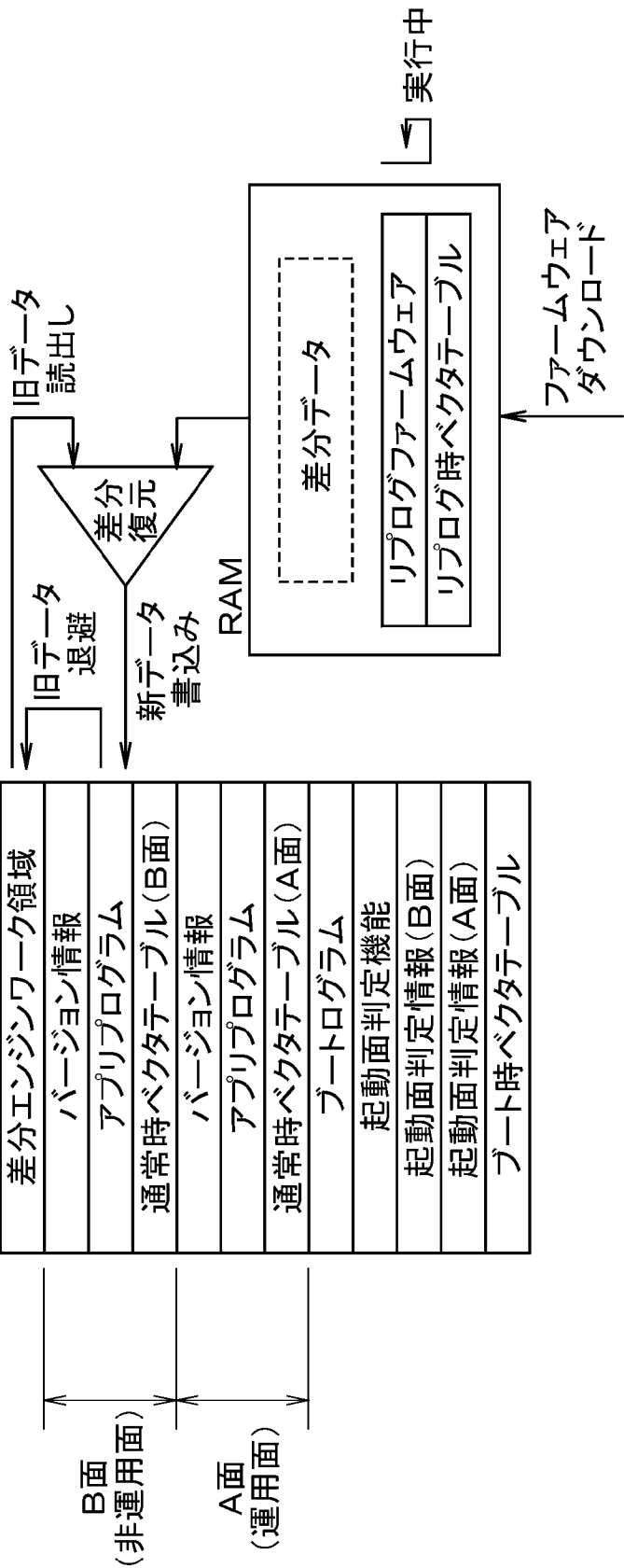
Fig. 17



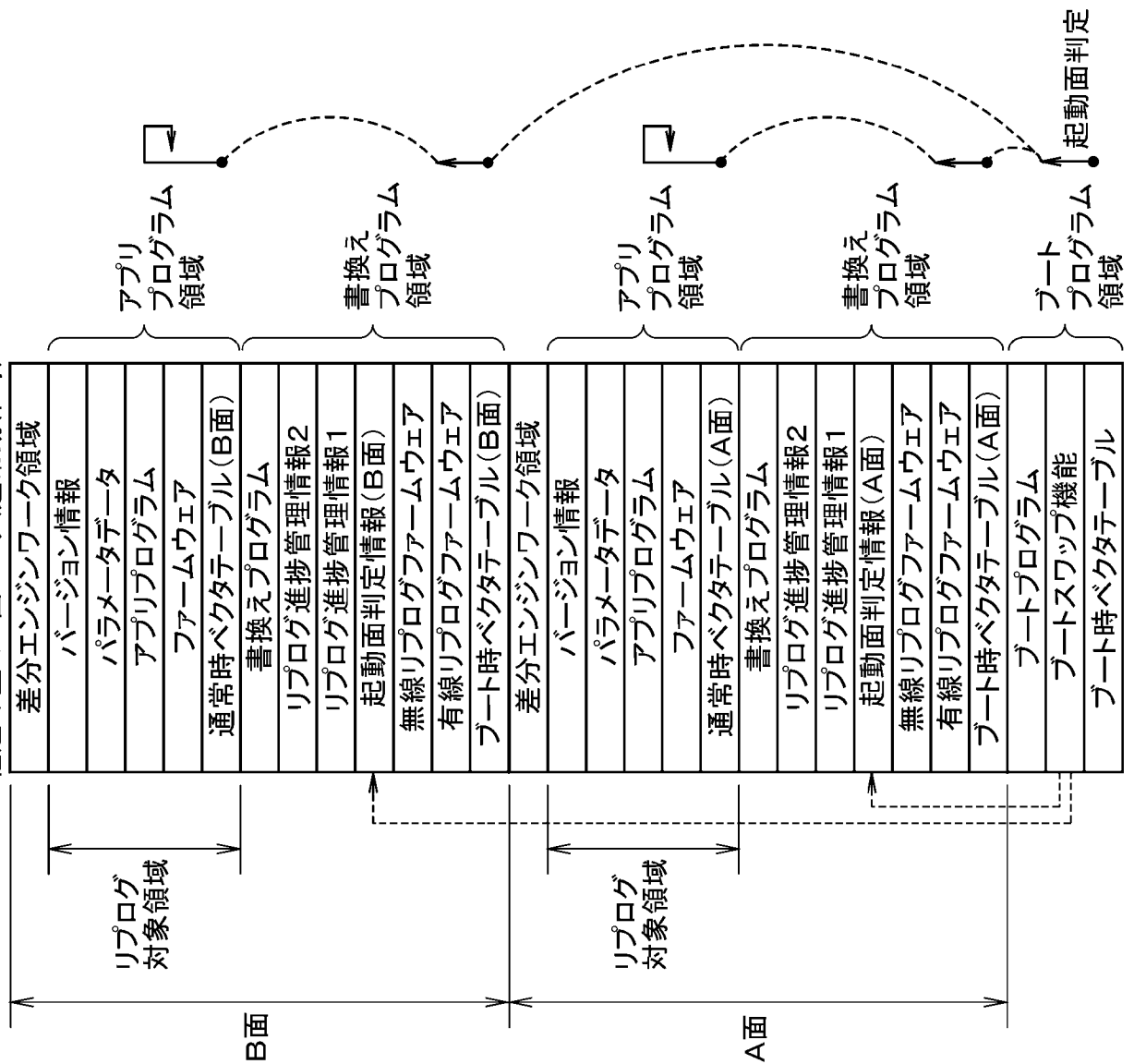
[図18]

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)



組込み型の2面メモリ(通常動作時)



[図20]

Fig. 20

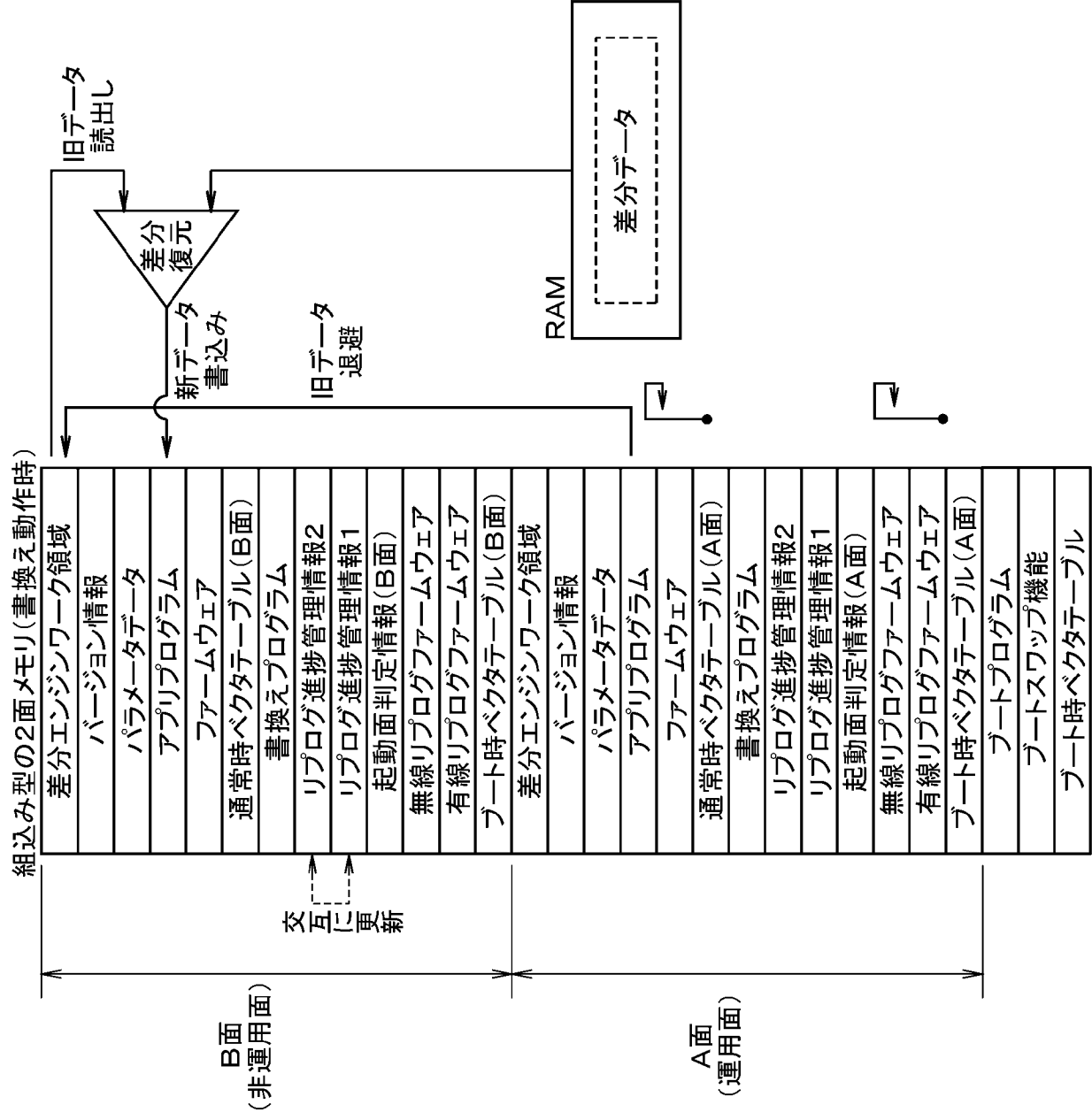
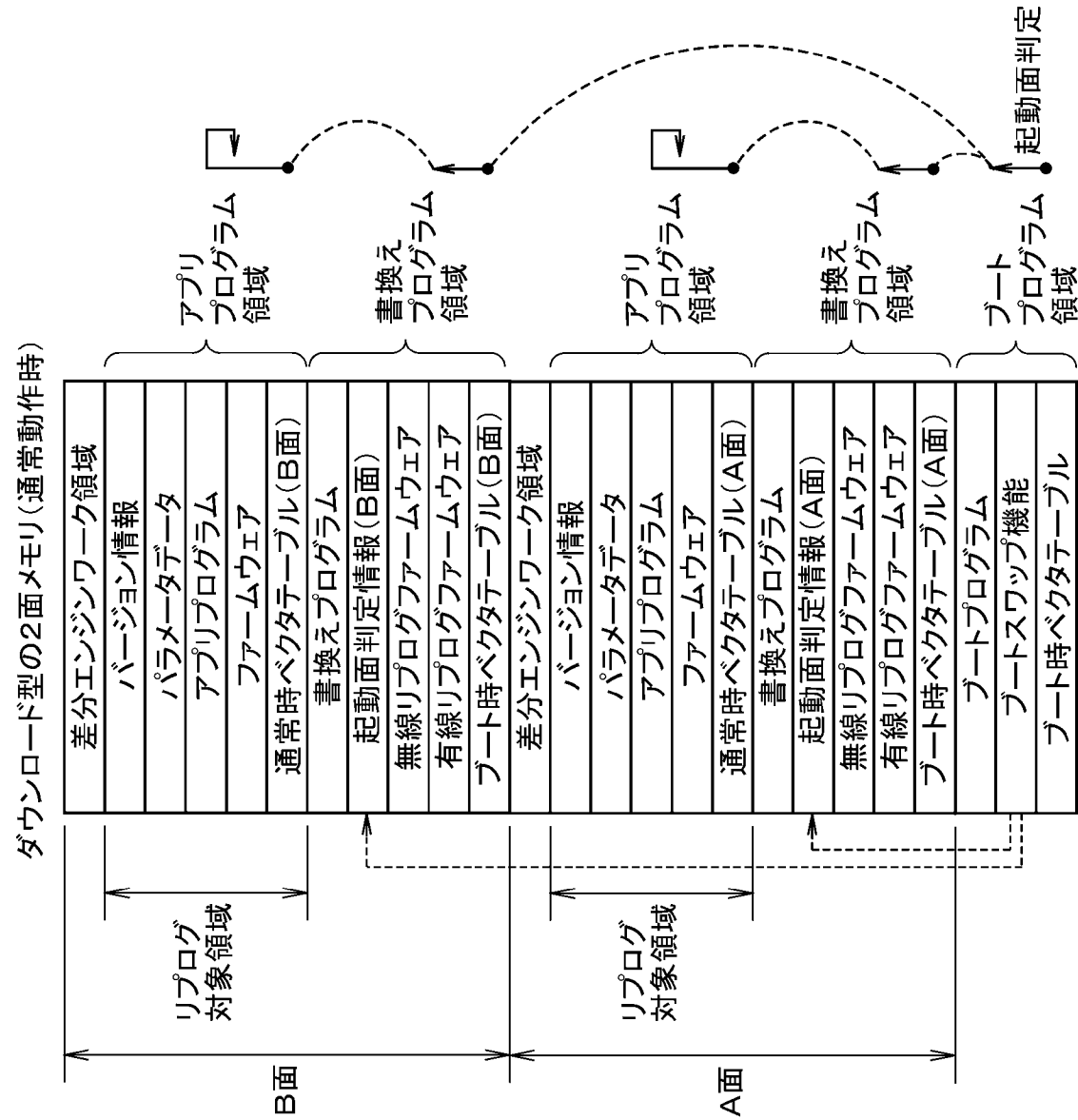
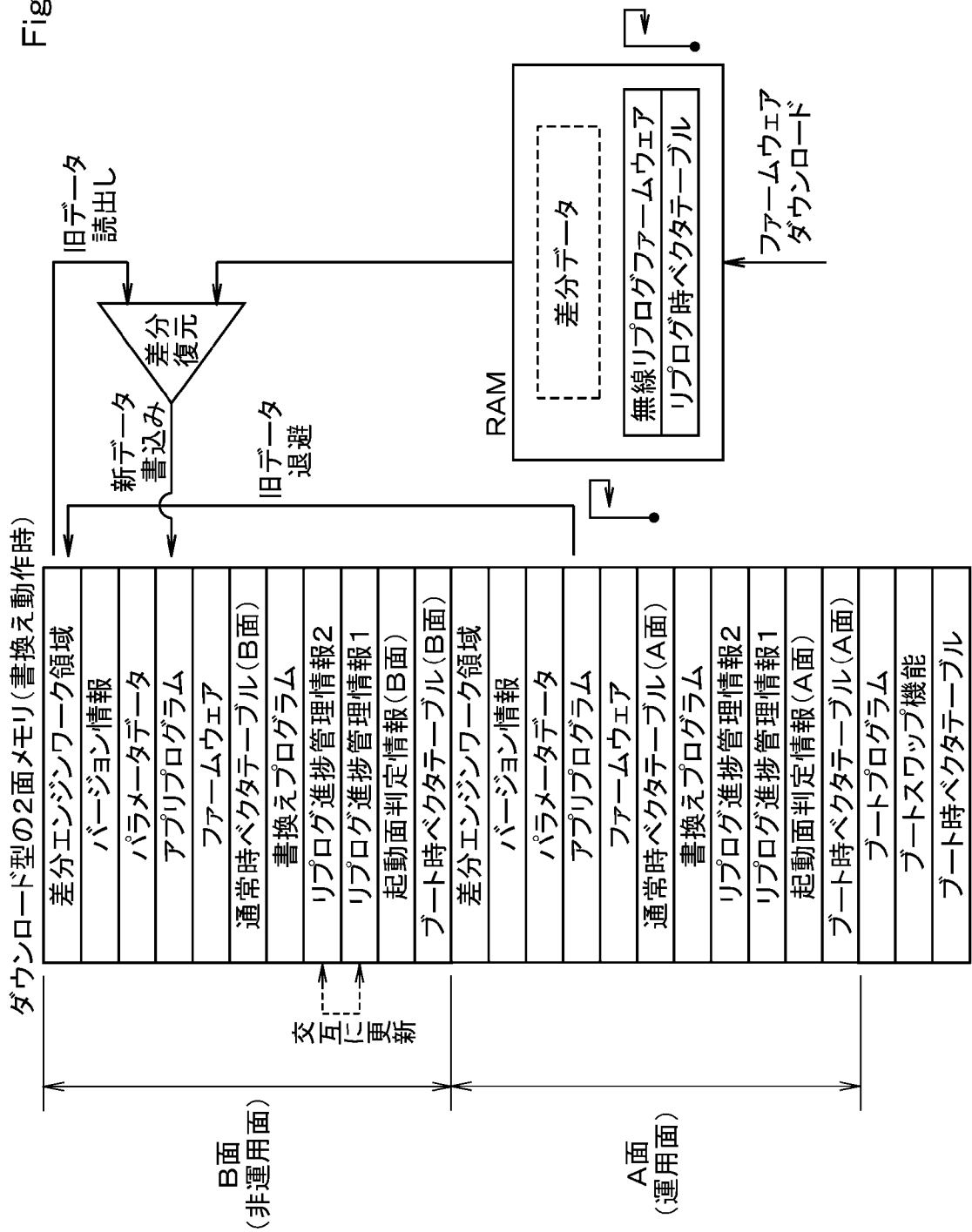


Fig. 21



[図22]

Fig. 22



Fi. 23

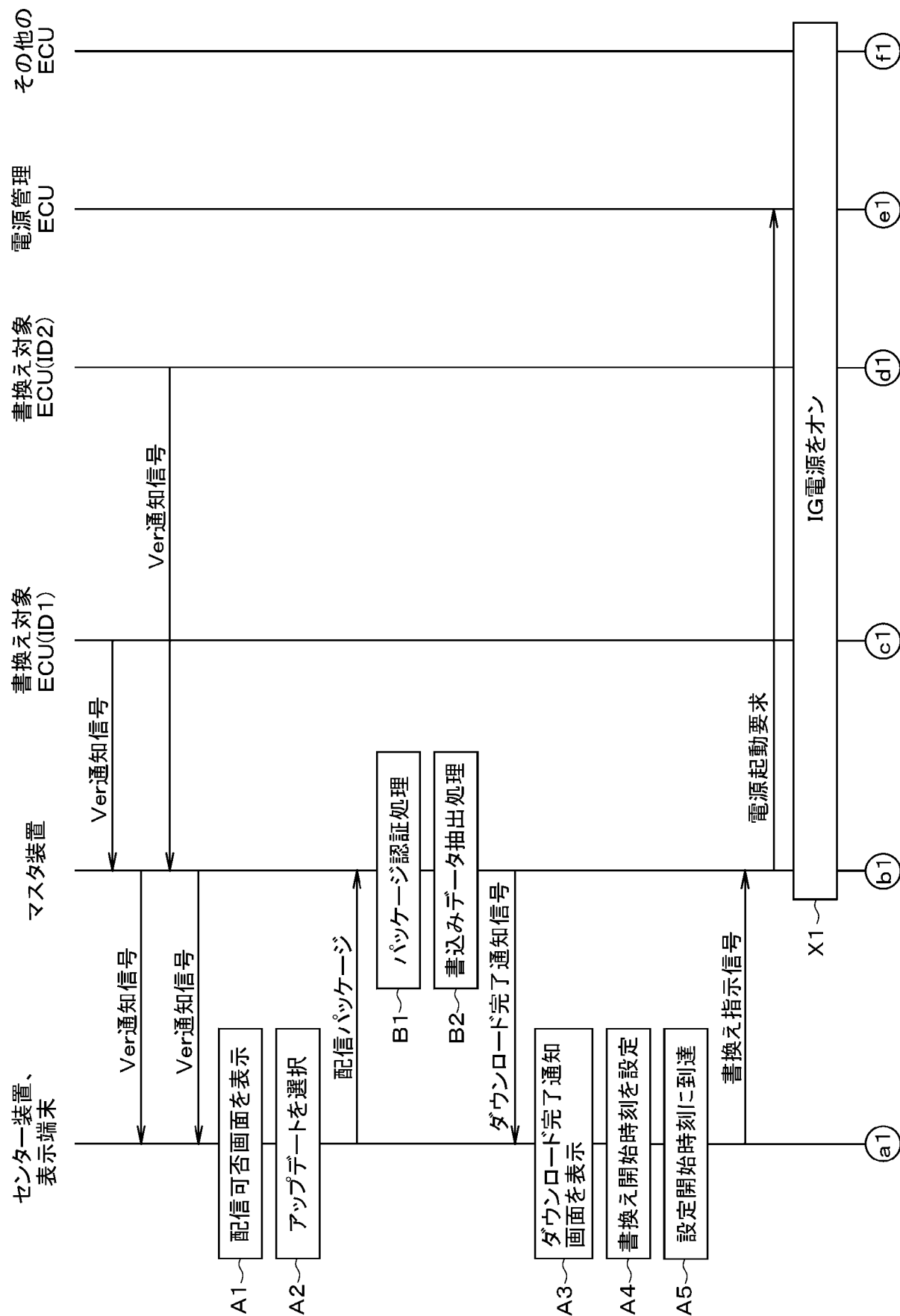
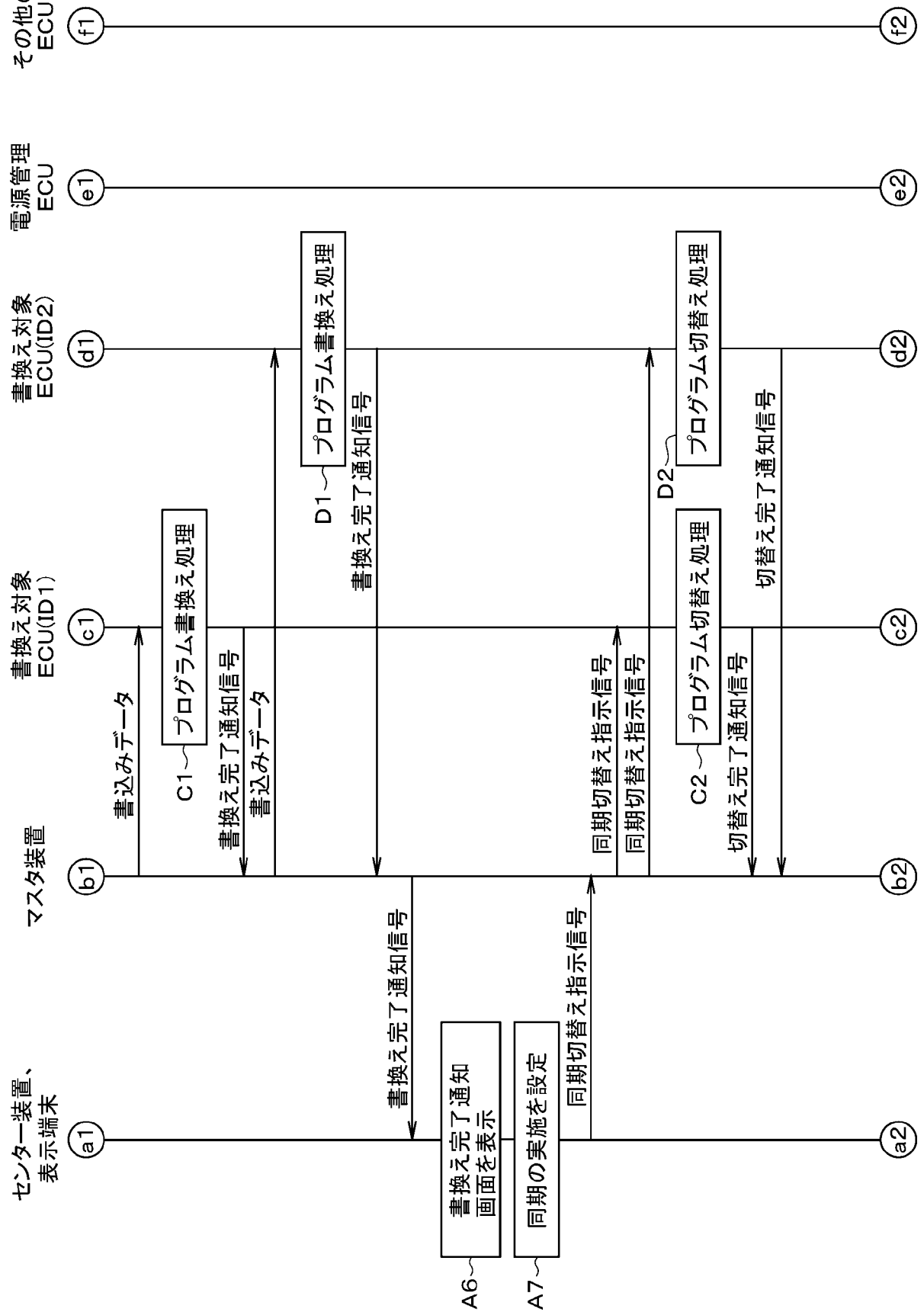


Fig. 24



[図25]

Fig. 25

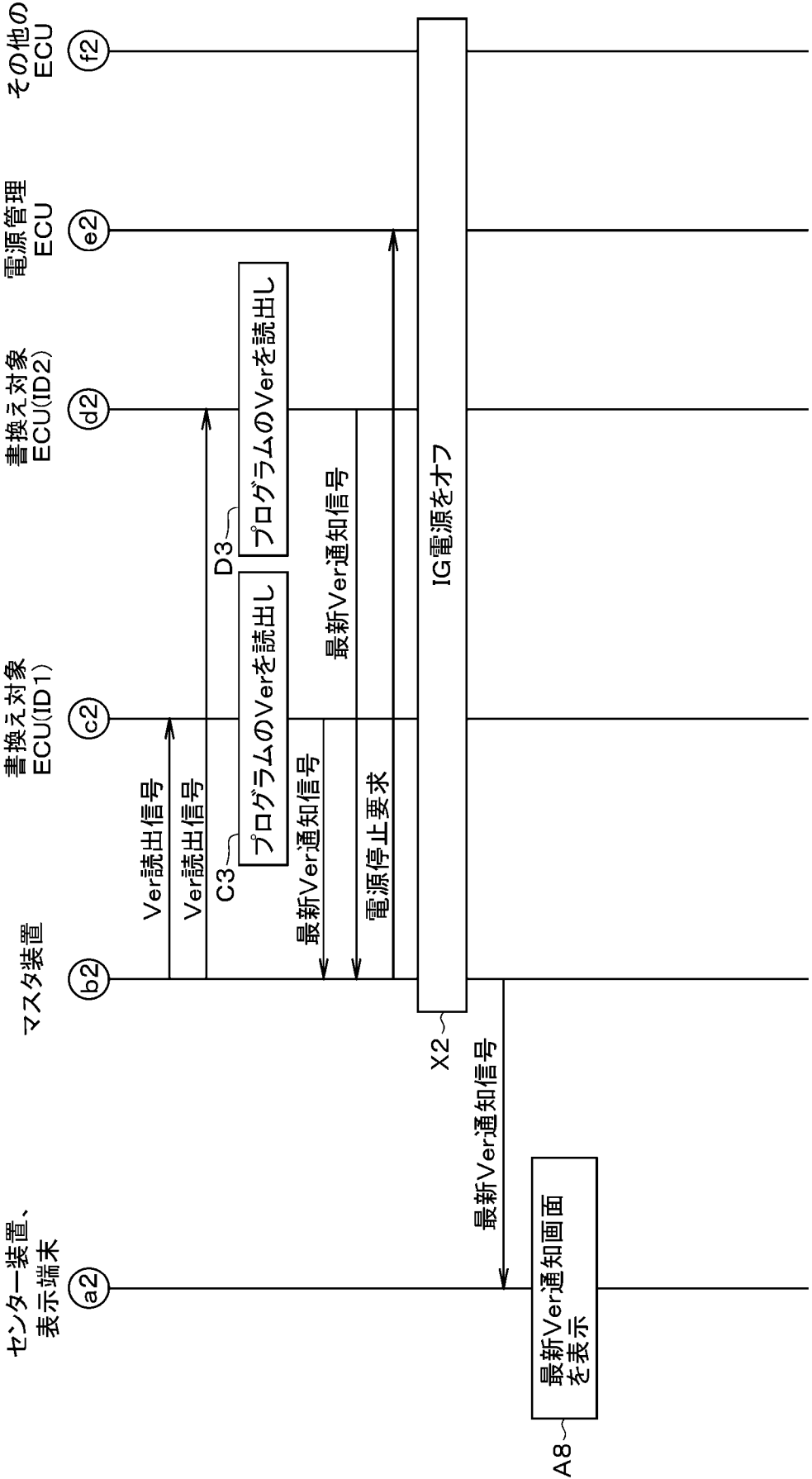


Fig. 26

[図26]

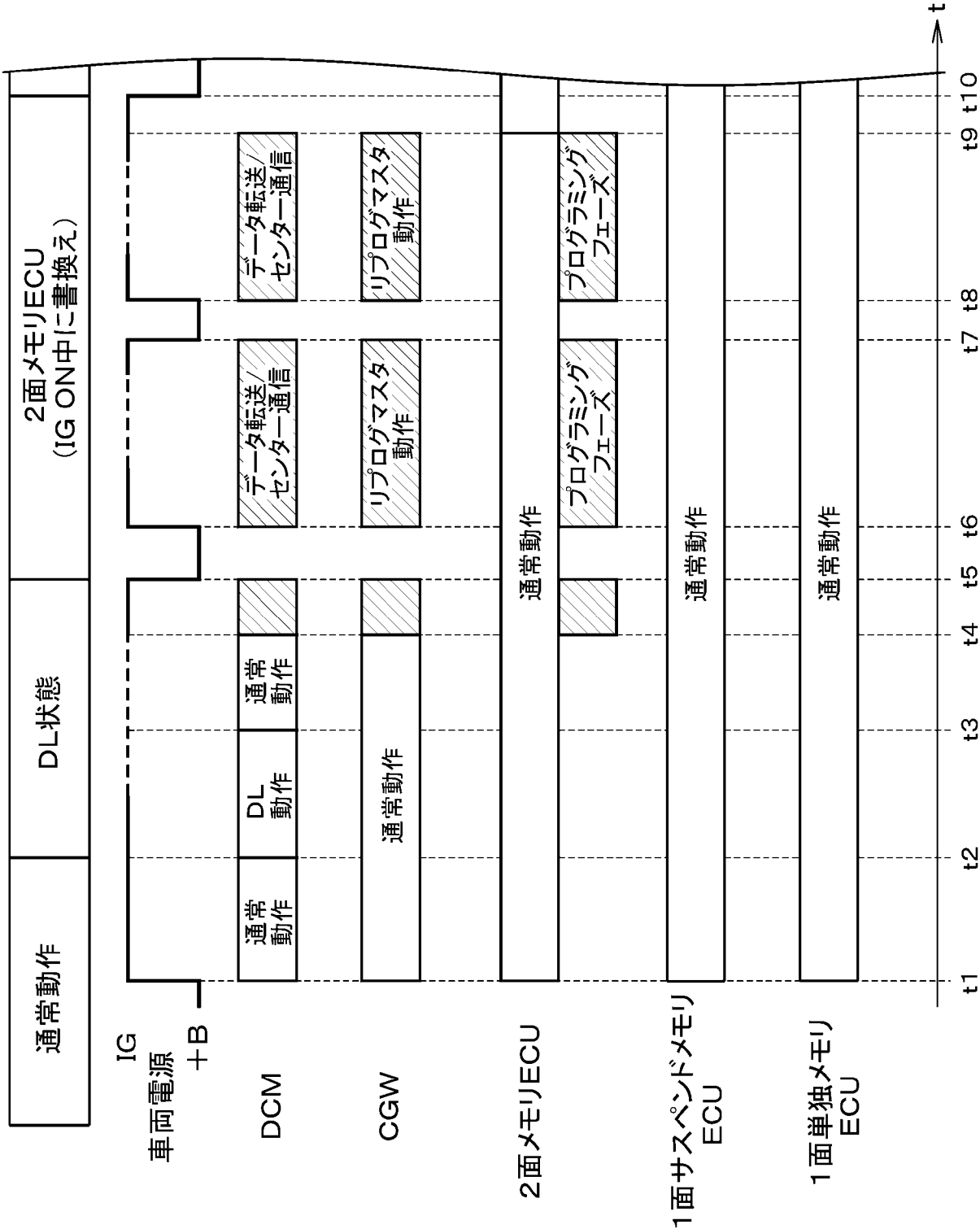
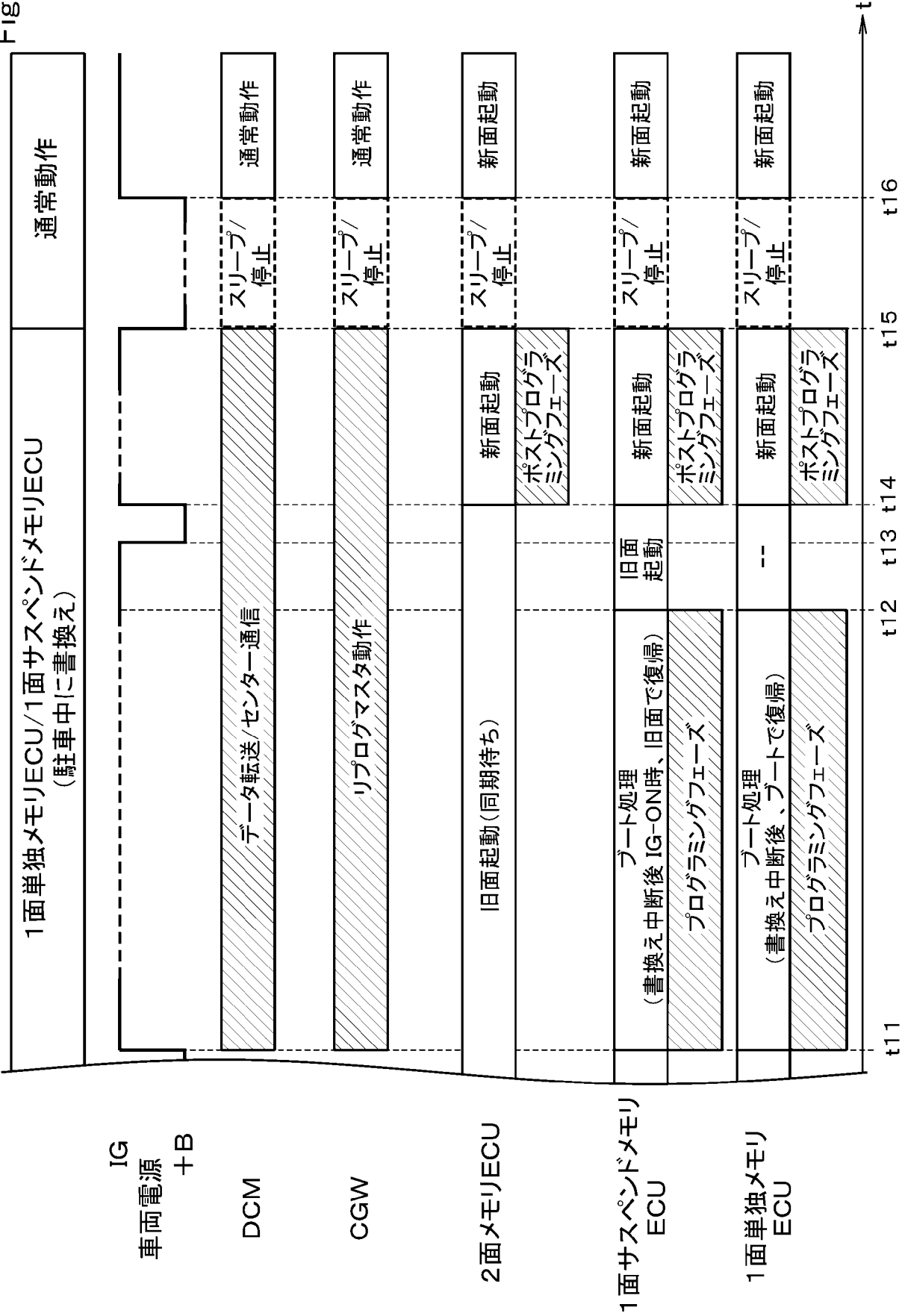
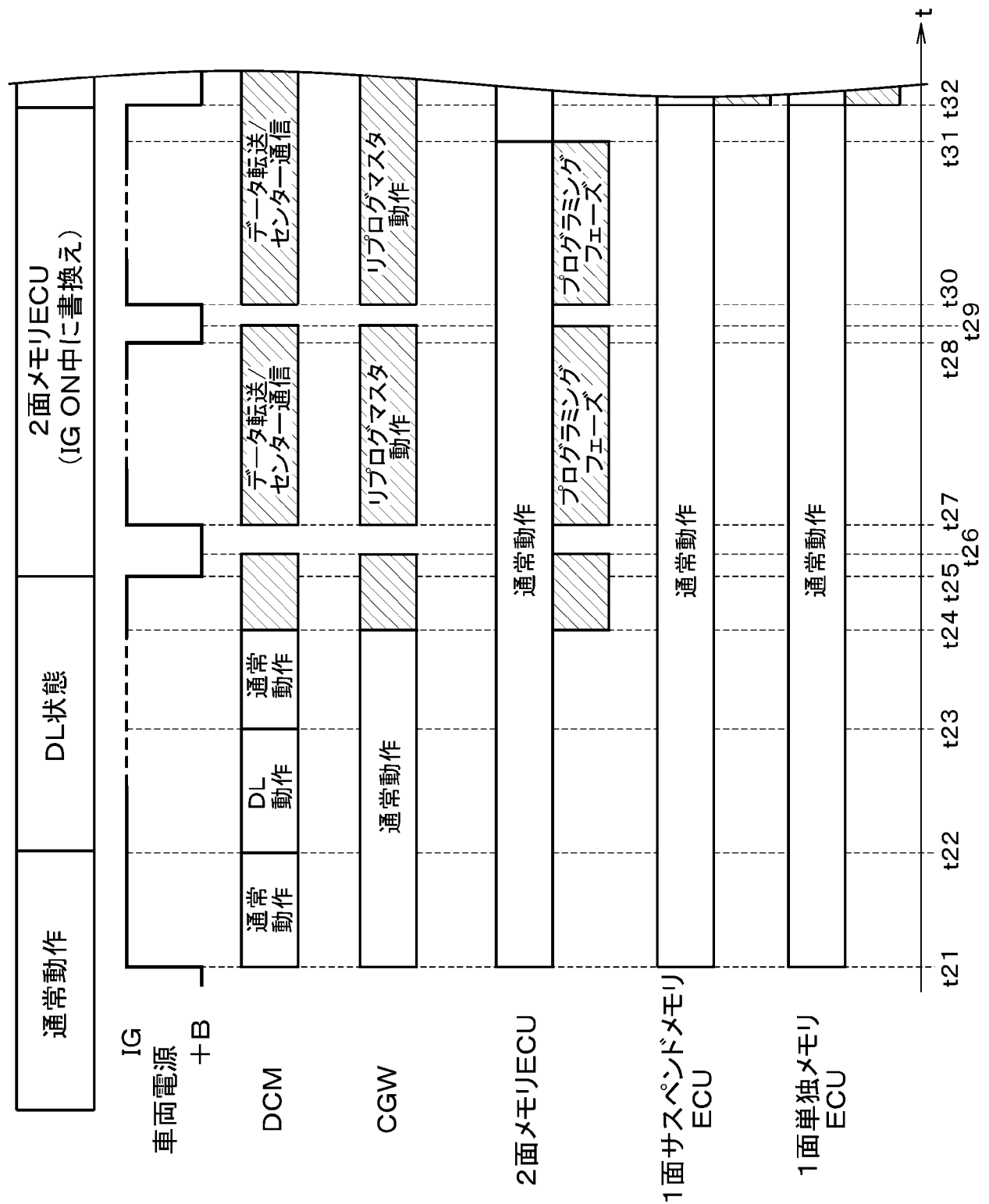


Fig. 27

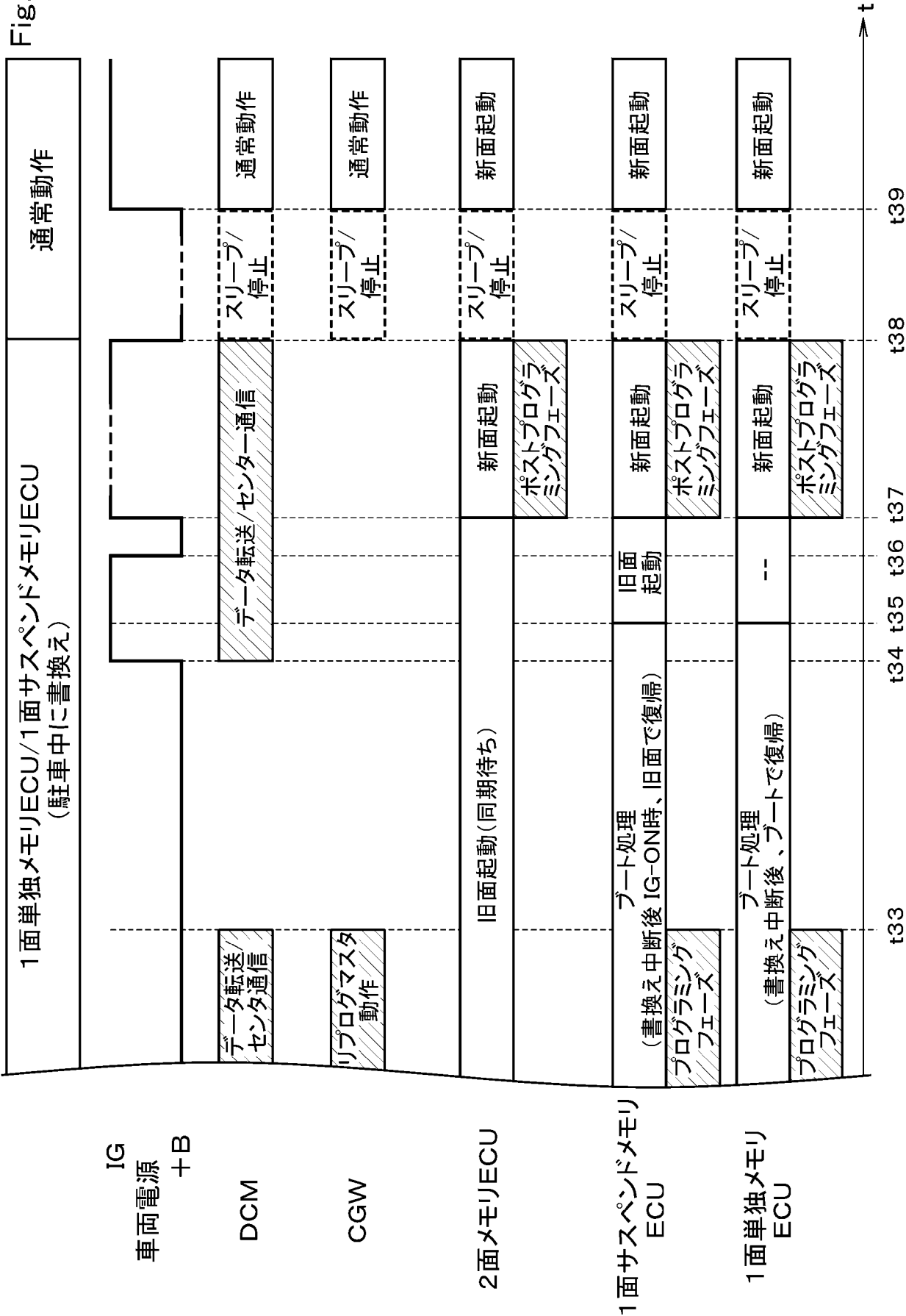


Fi. 28



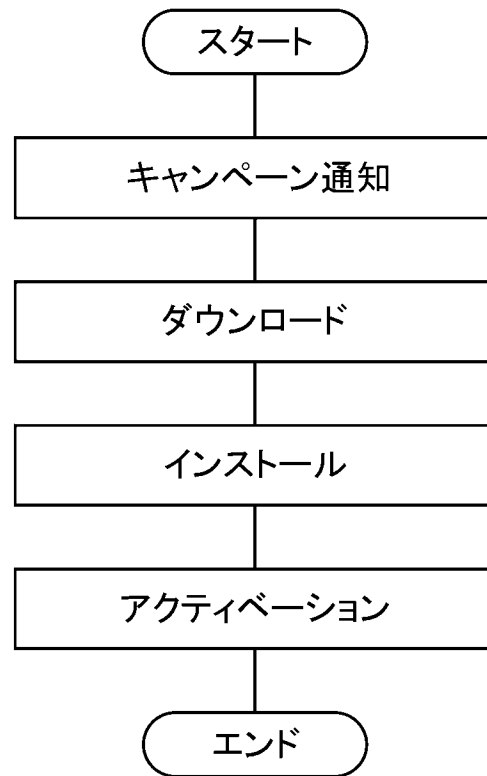
[図29]

Fig. 29



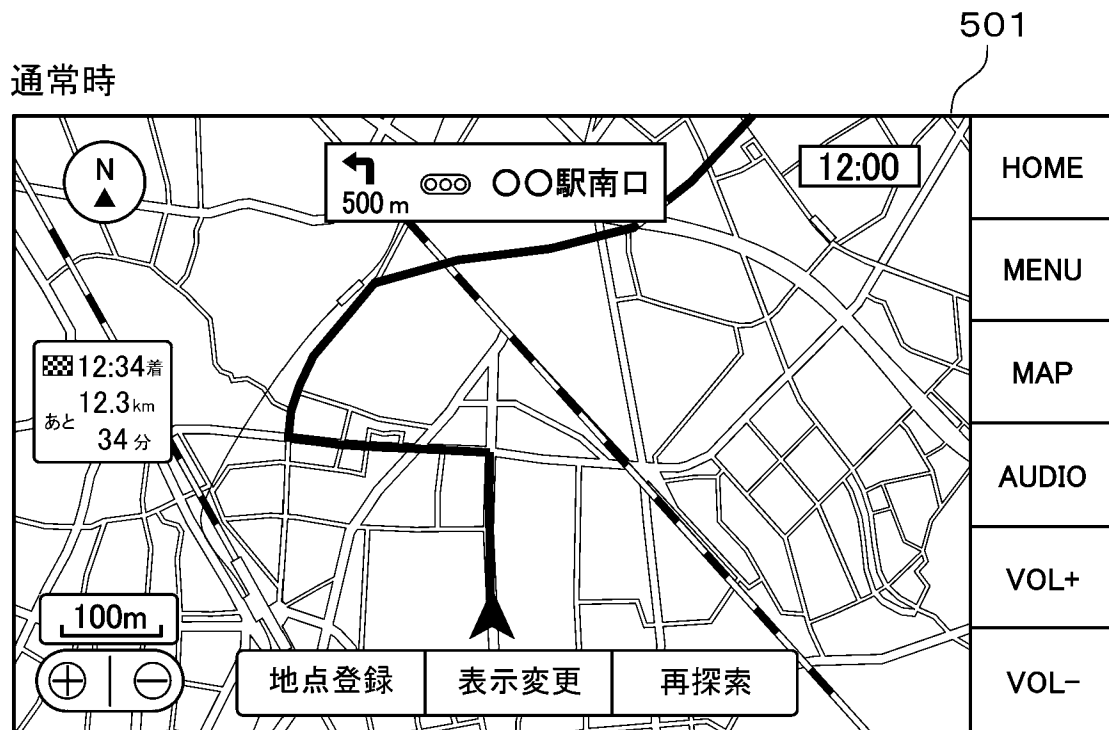
[図30]

Fig. 30



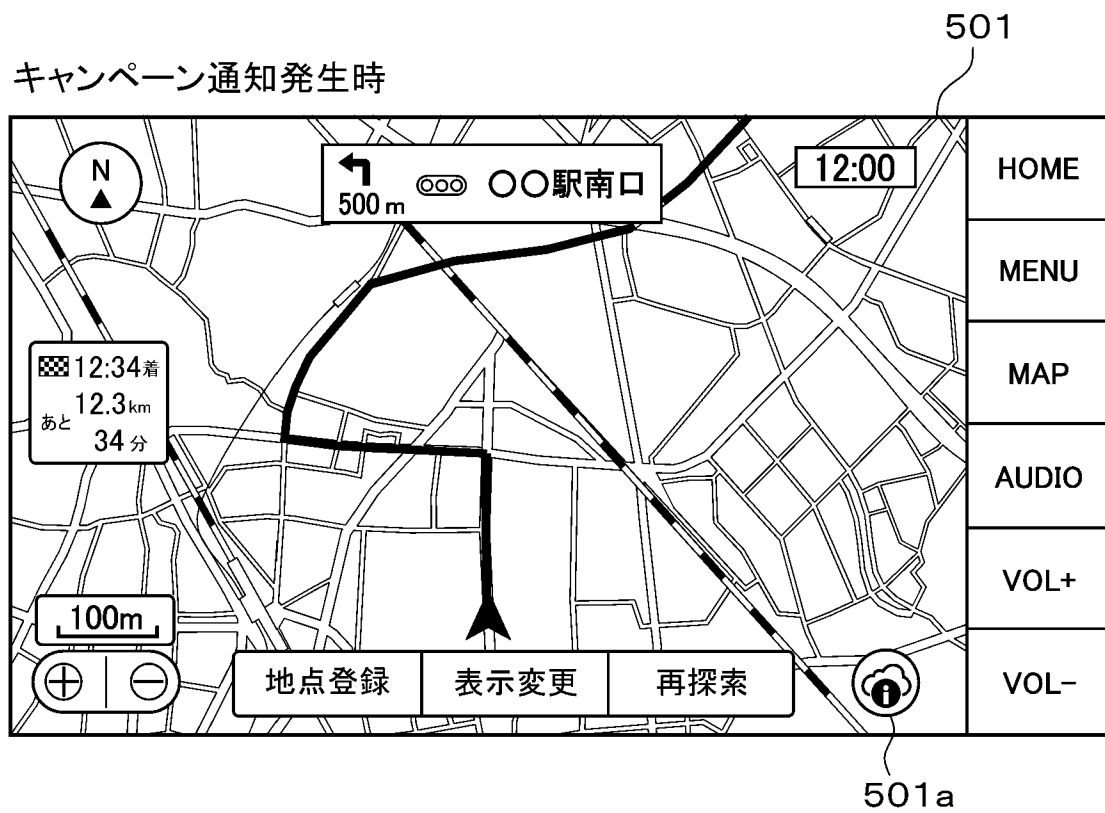
[図31]

Fig. 31



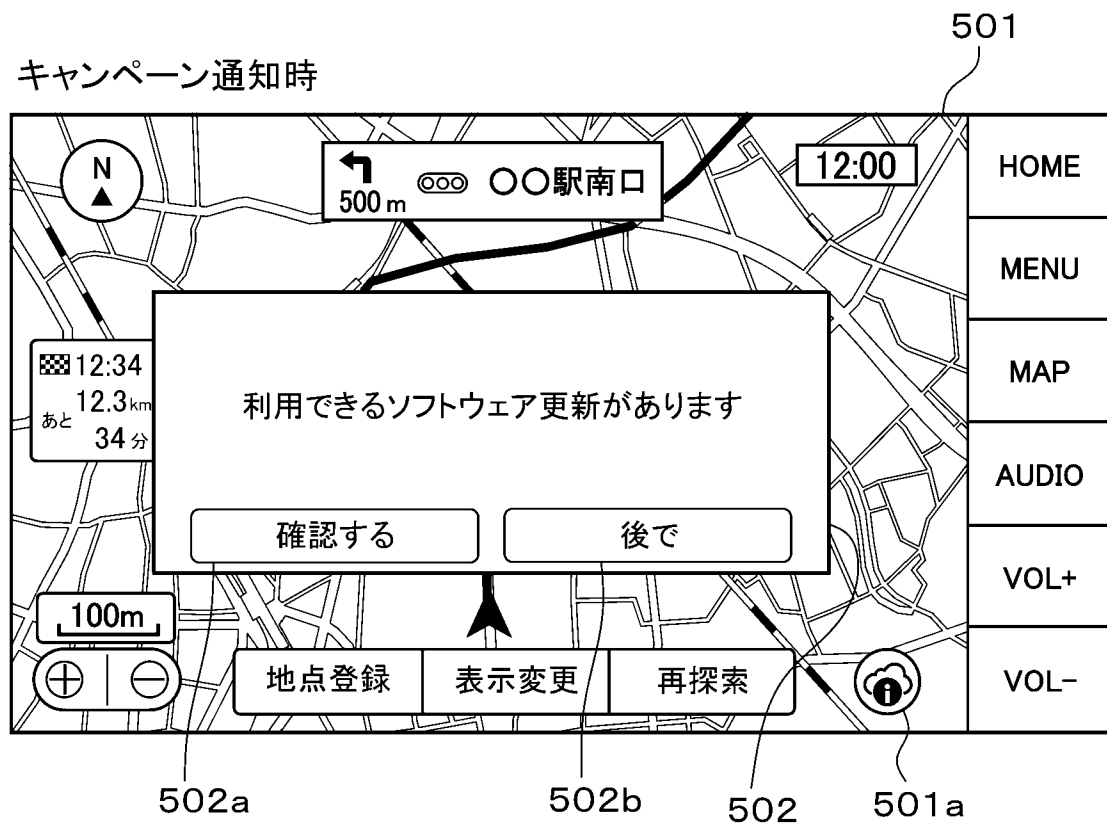
[図32]

Fig. 32



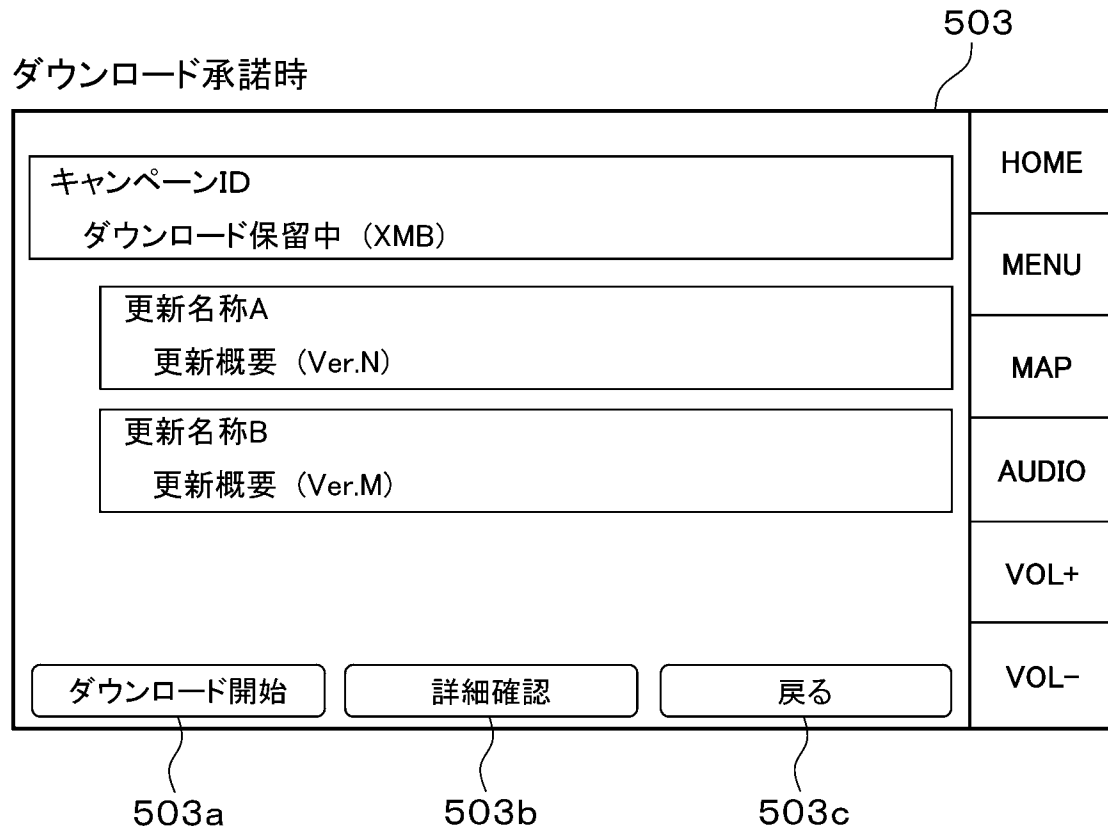
[図33]

Fig. 33



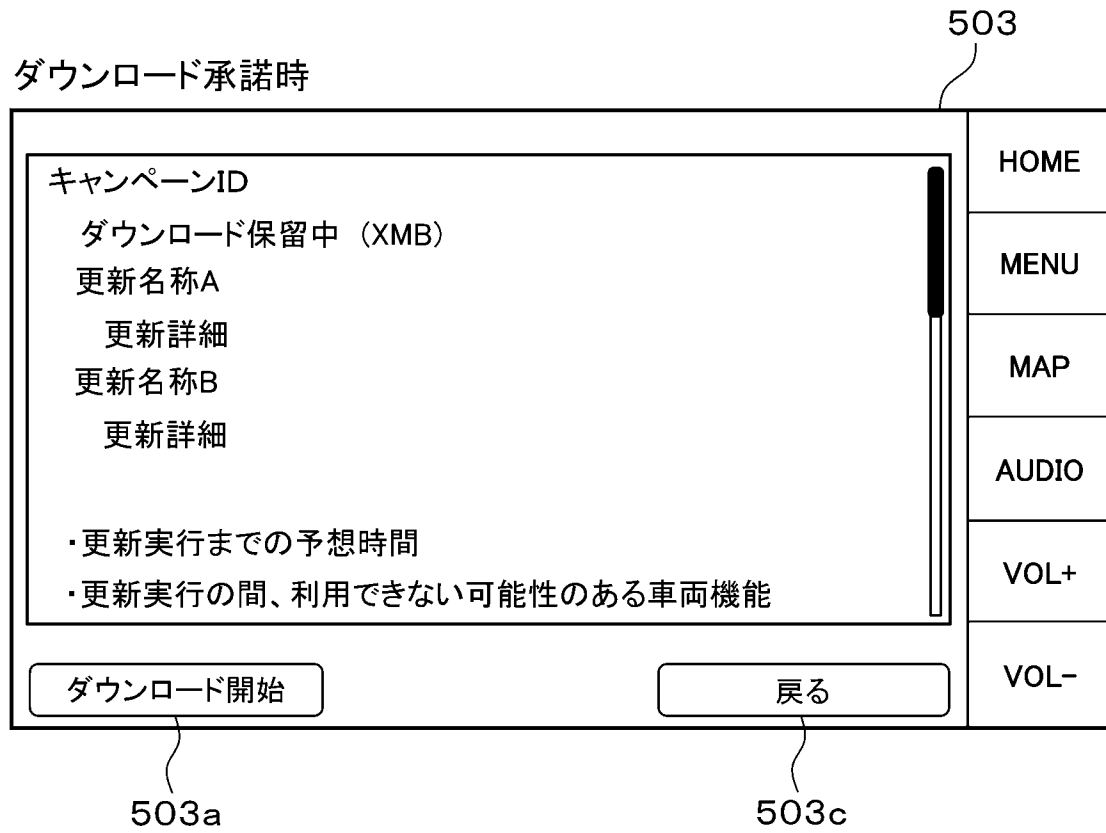
[図34]

Fig. 34



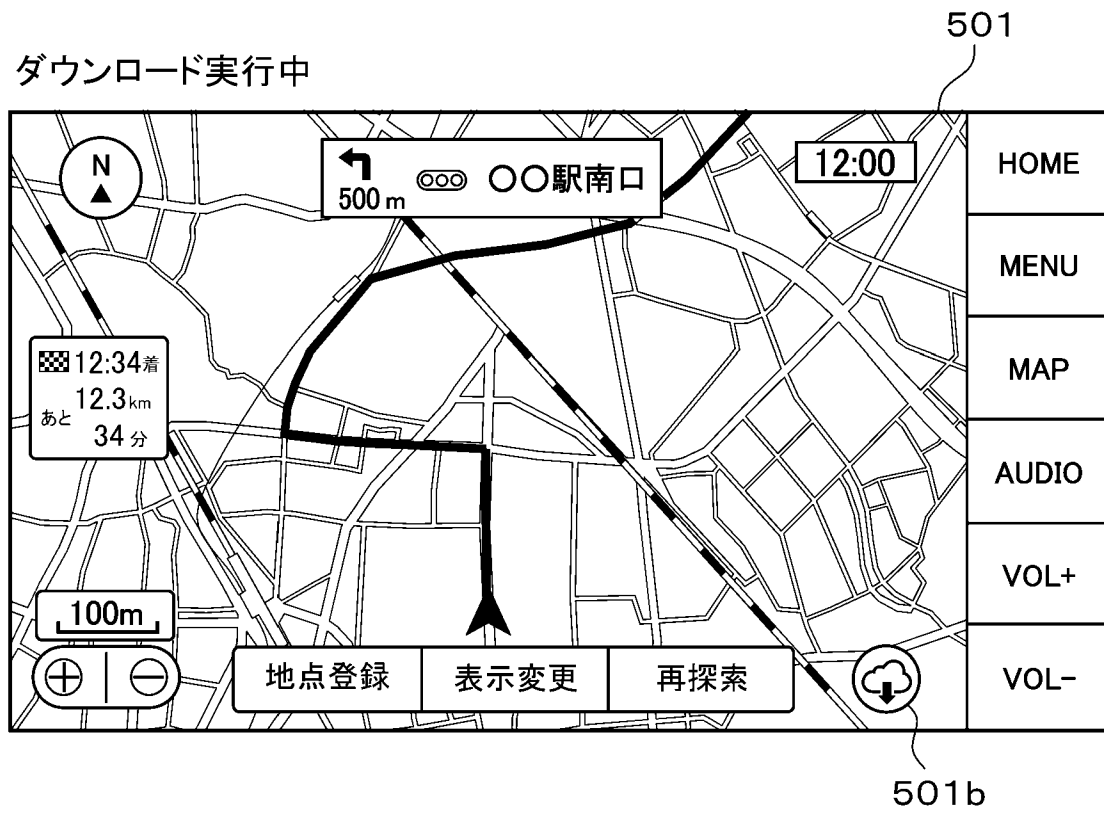
[図35]

Fig. 35



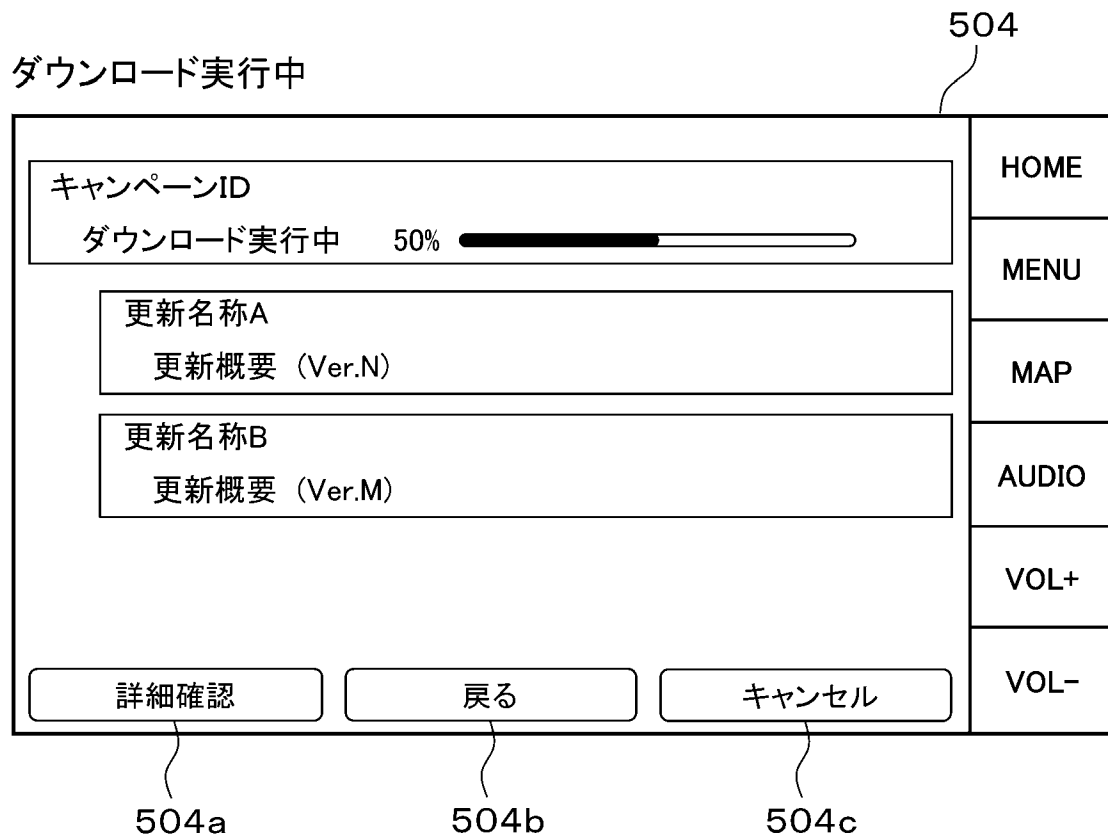
[図36]

Fig. 36



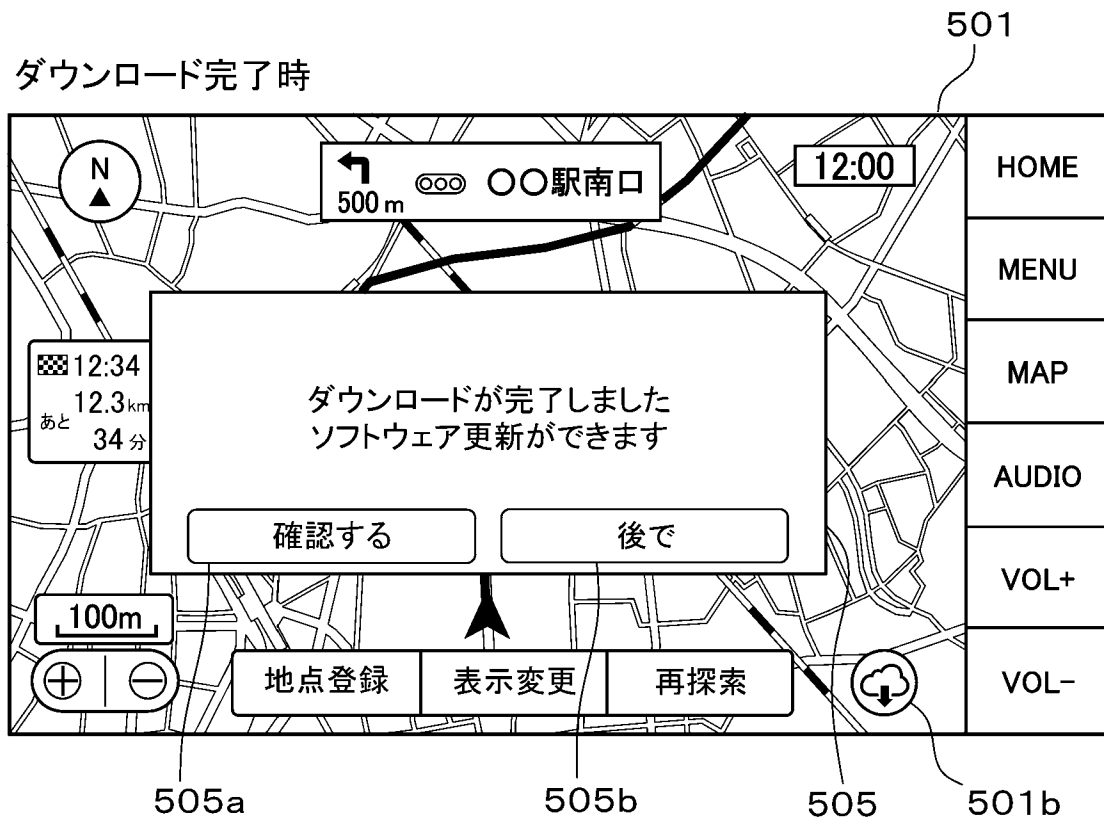
[図37]

Fig. 37



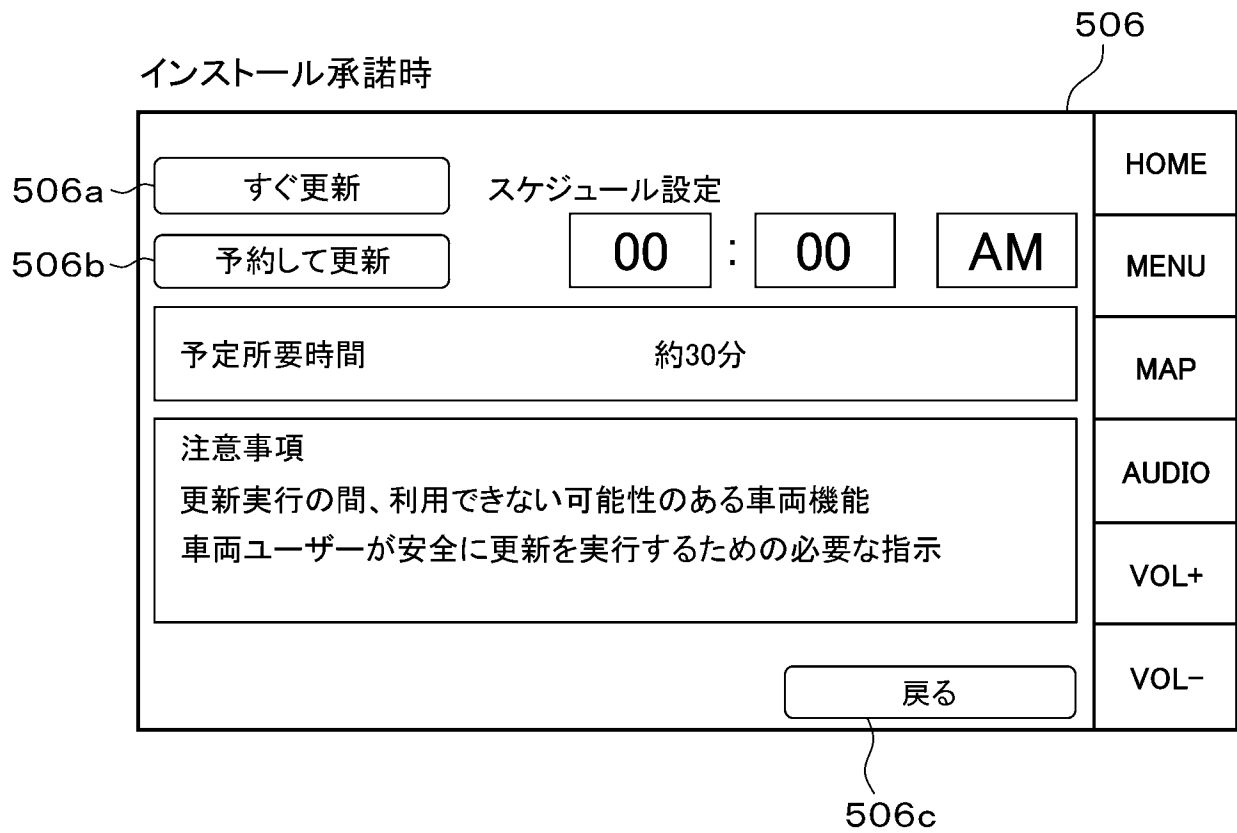
[図38]

Fig. 38



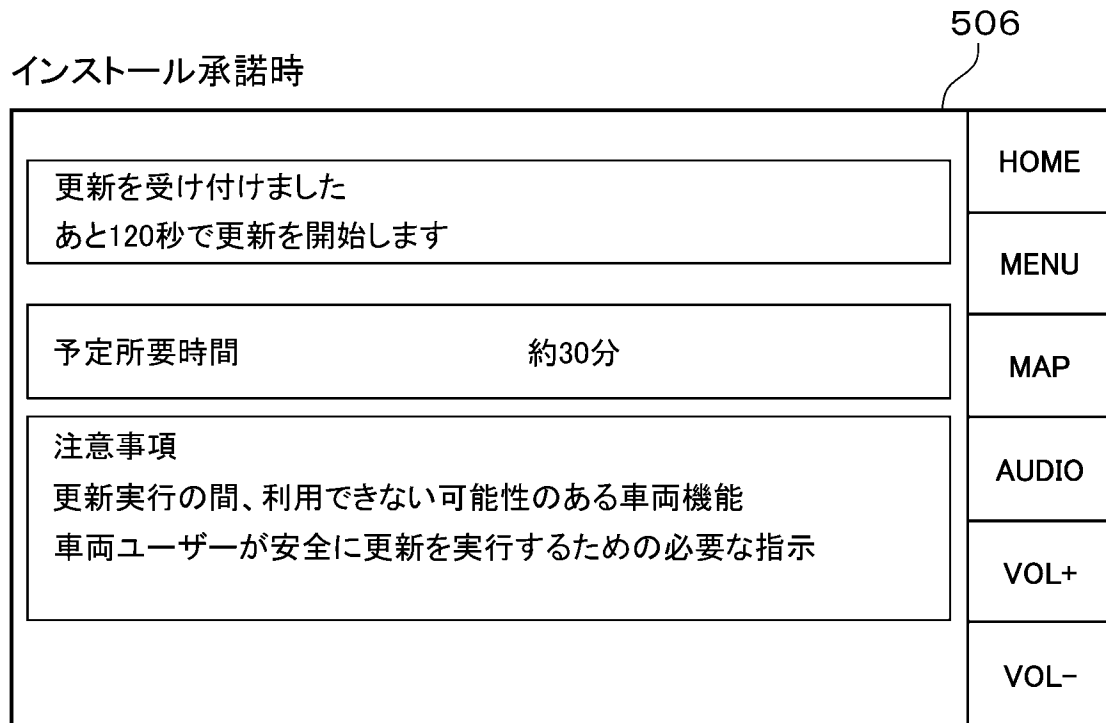
[図39]

Fig. 39



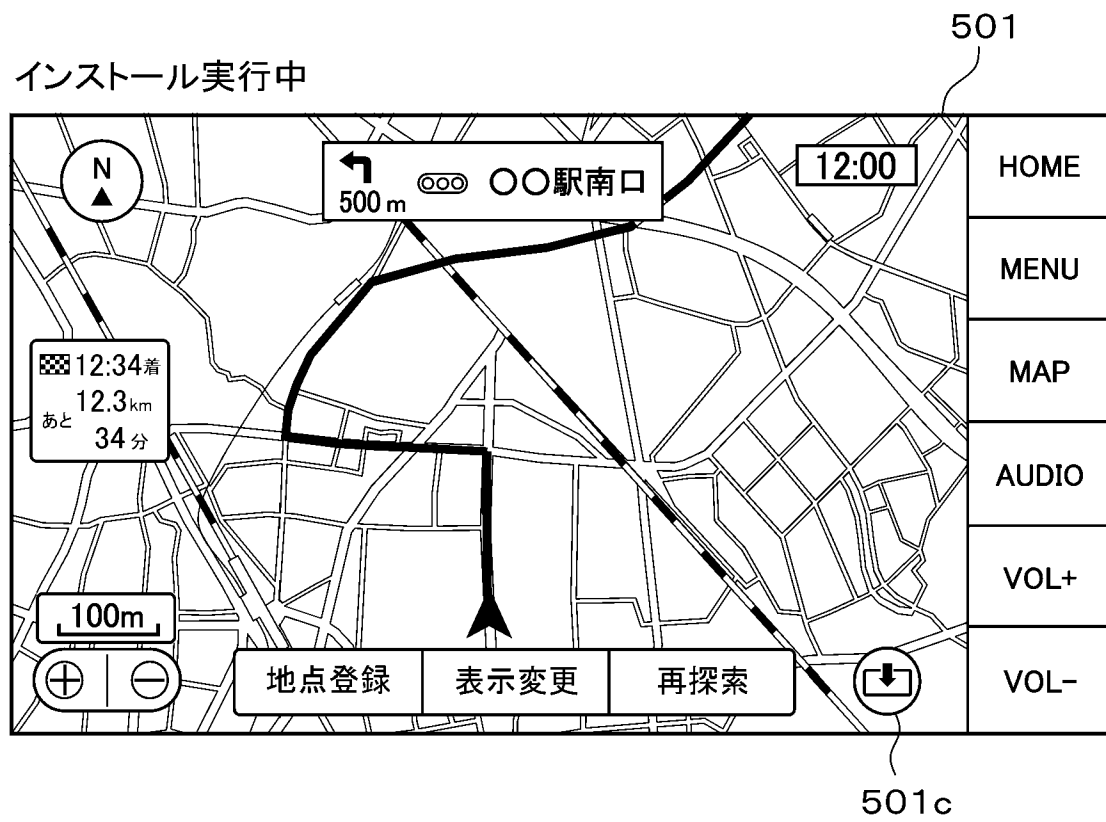
[図40]

Fig. 40

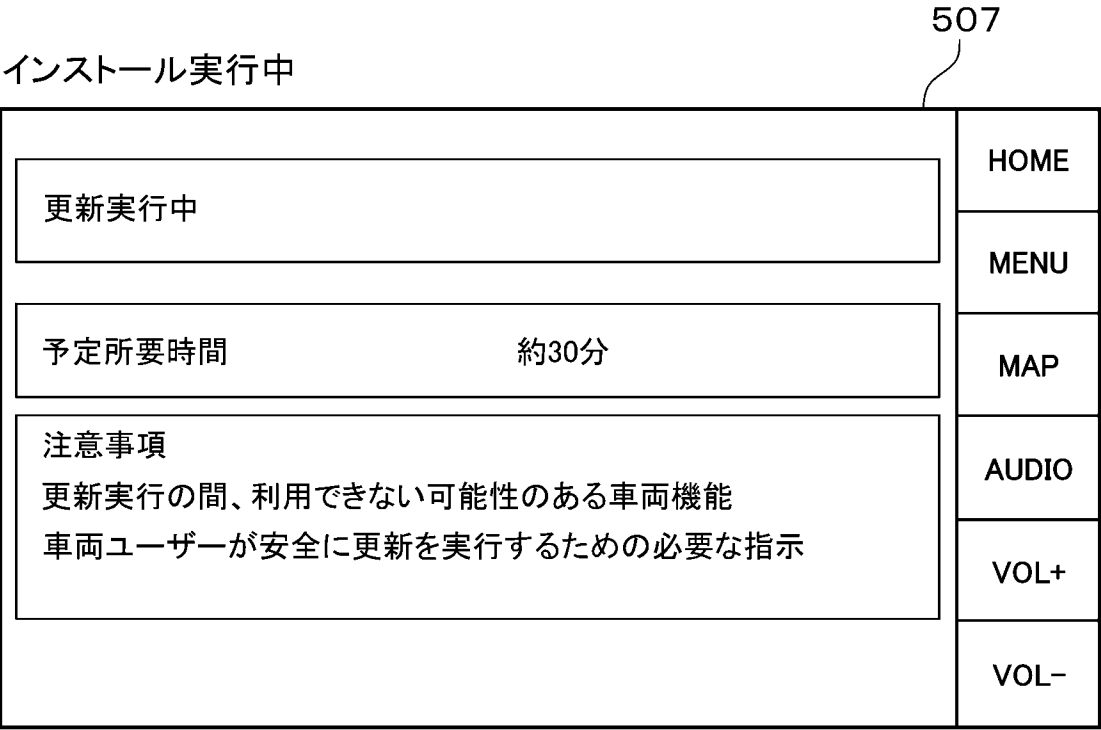


[図41]

Fig. 41

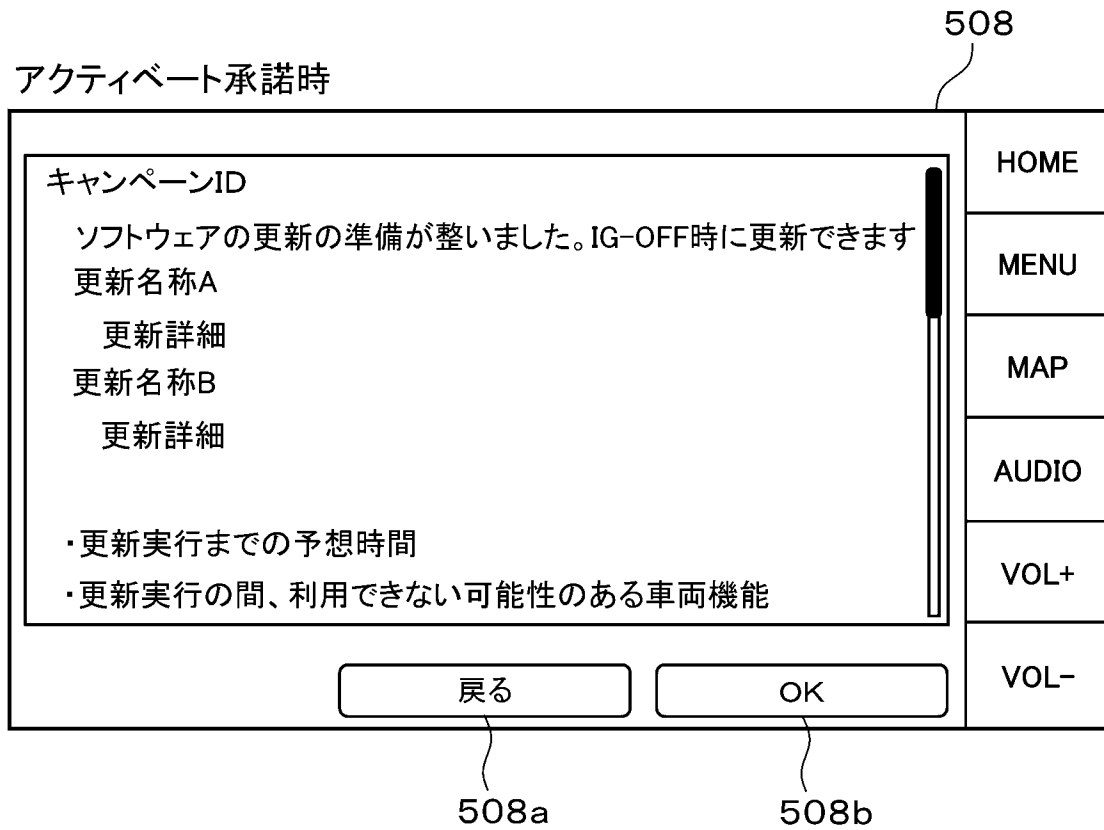


[図42]
Fig. 42



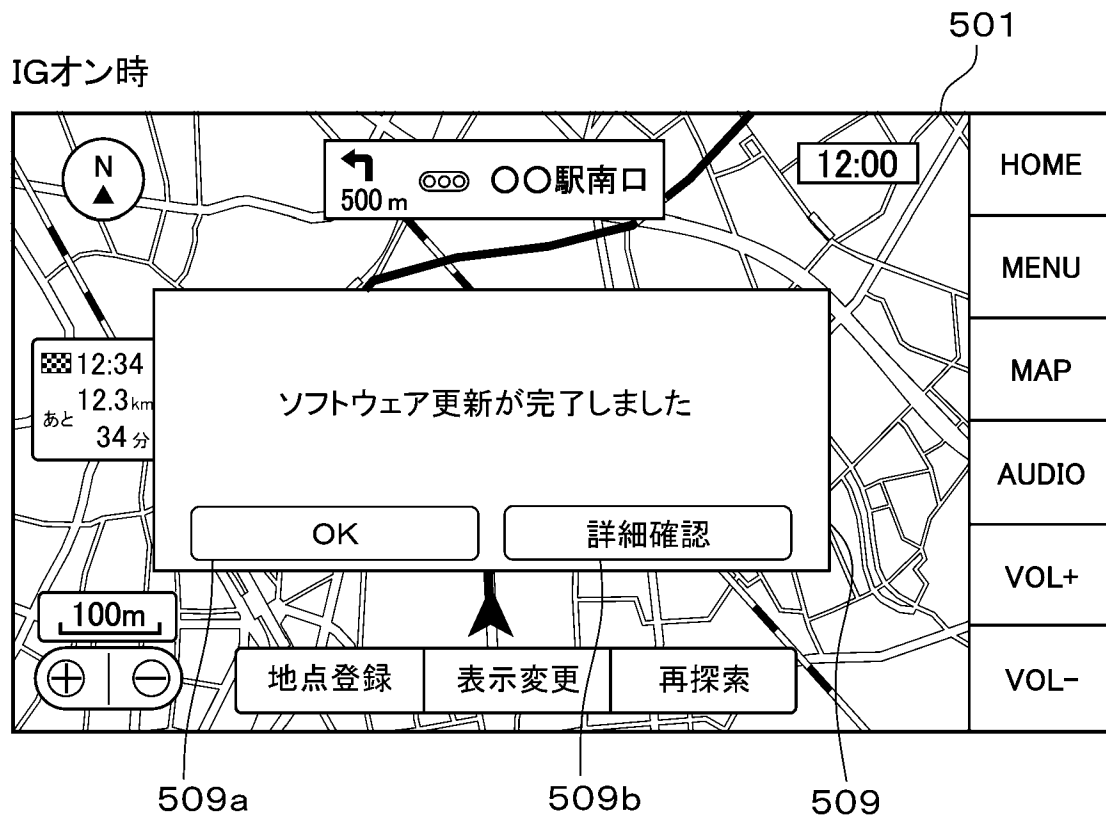
[図43]

Fig. 43



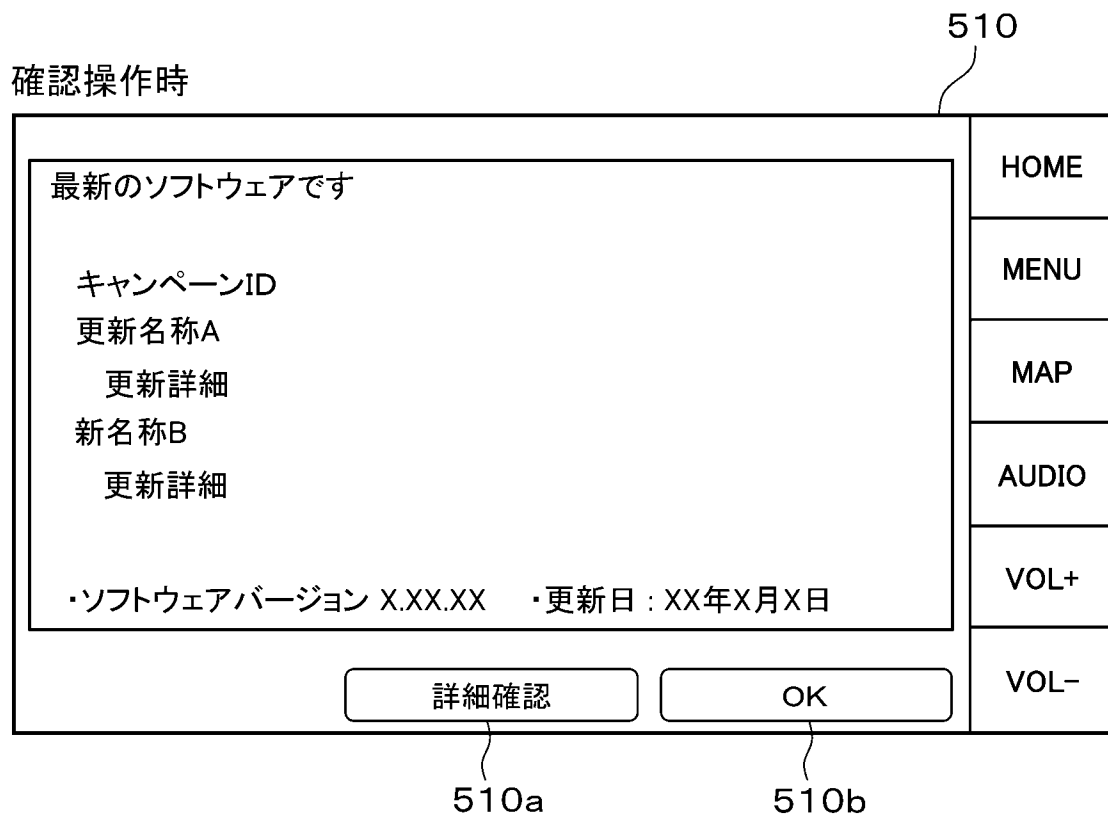
[図44]

Fig. 44



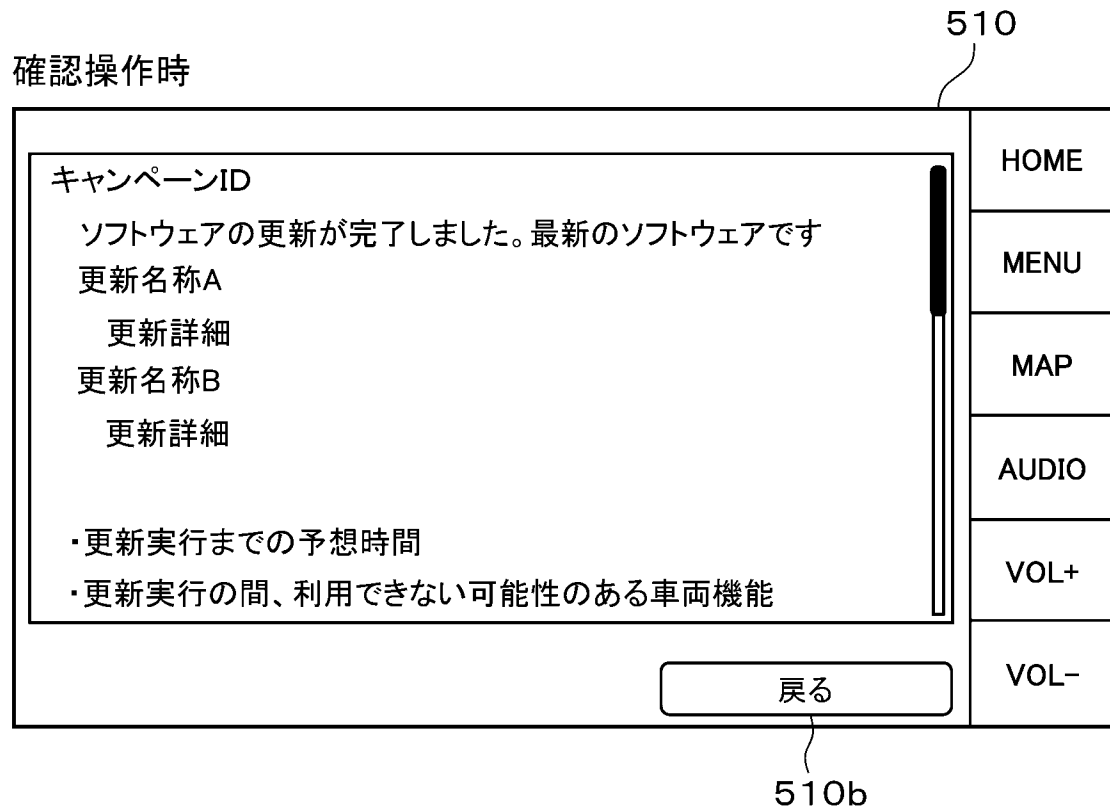
[図45]

Fig. 45



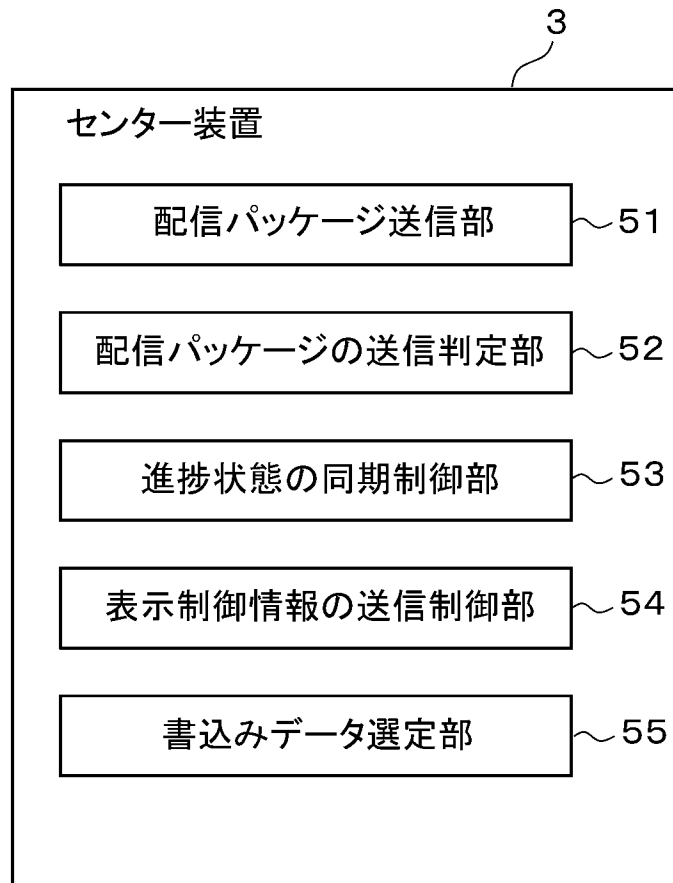
[図46]

Fig. 46



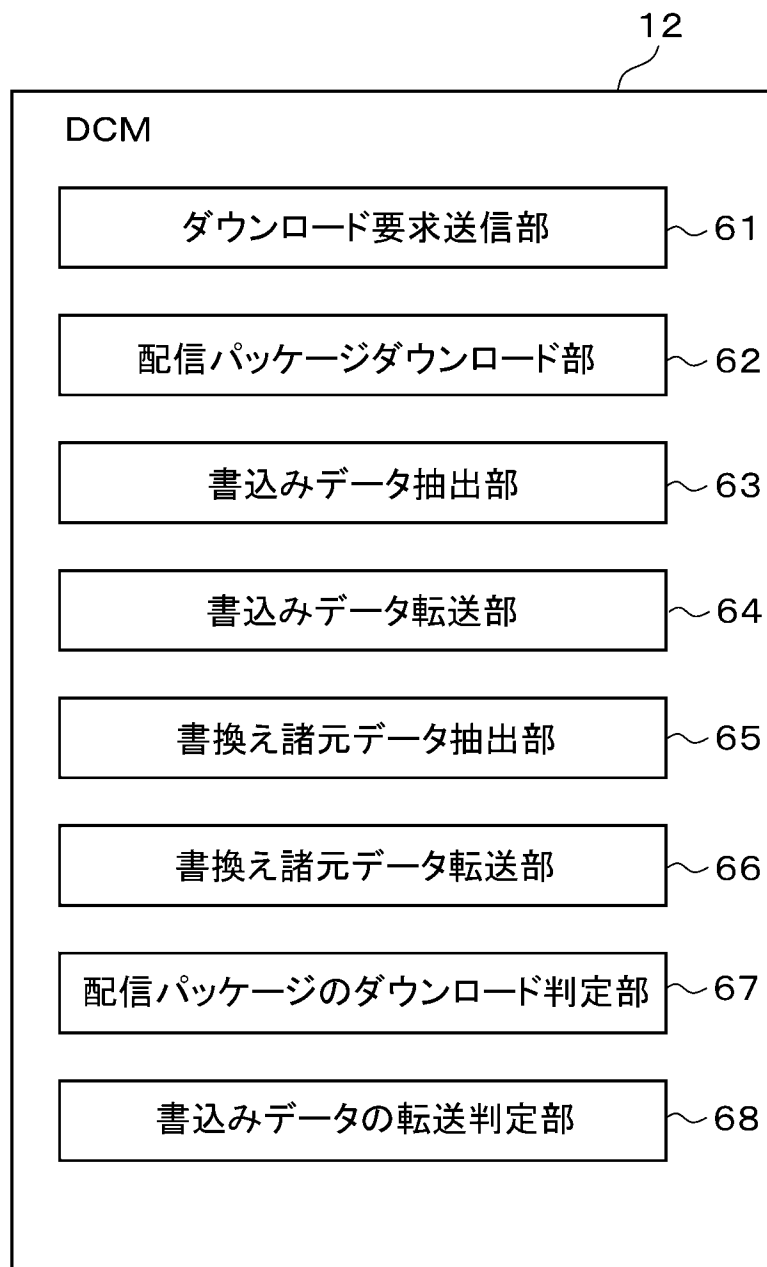
[図47]

Fig. 47



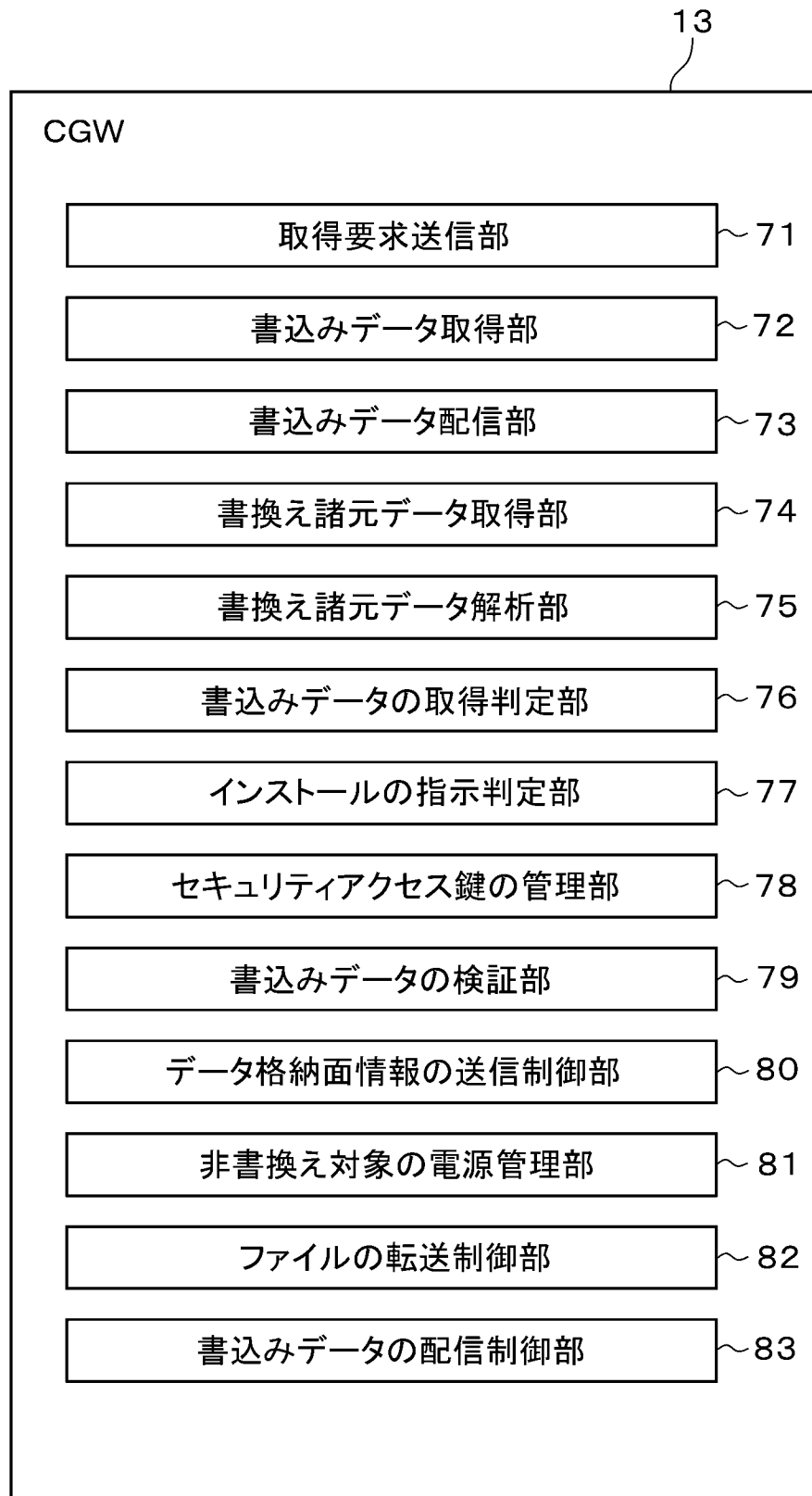
[図48]

Fig. 48



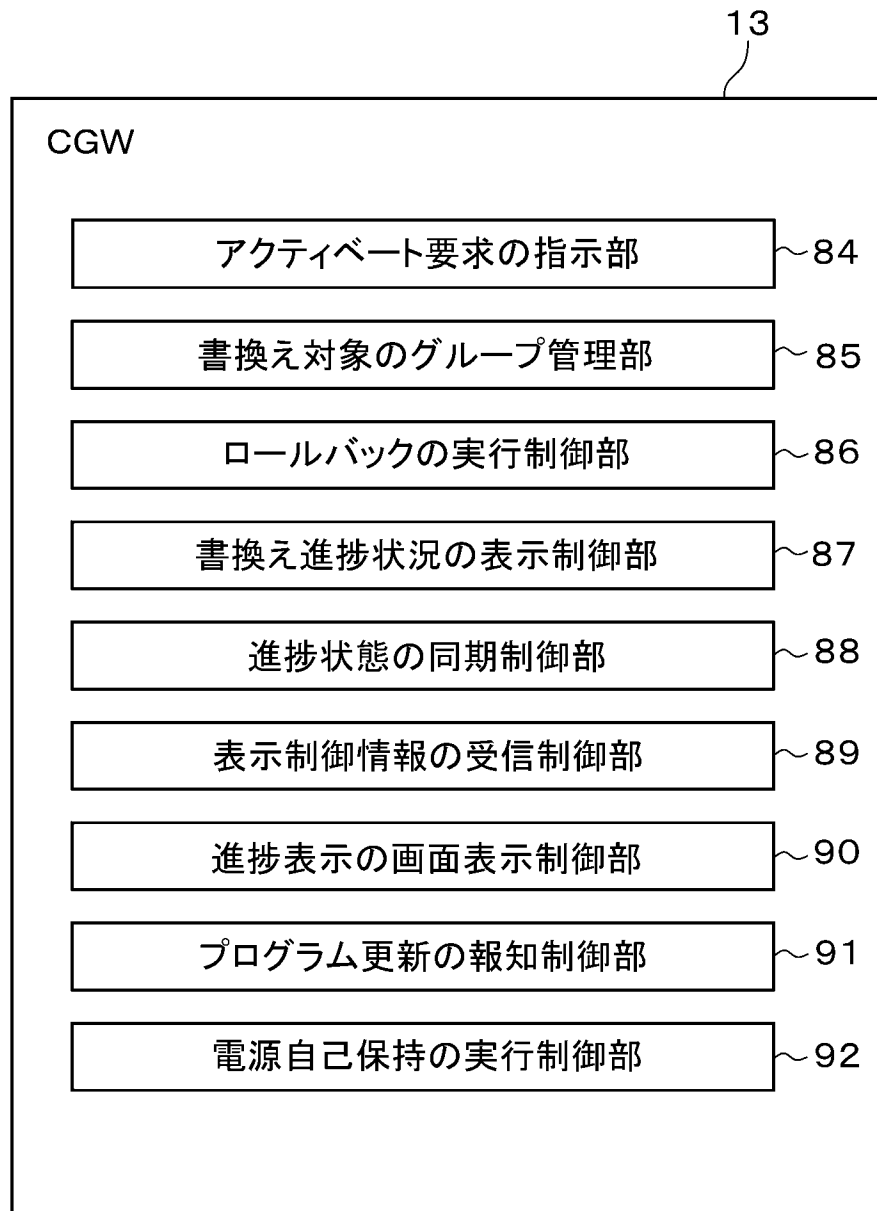
[図49]

Fig. 49



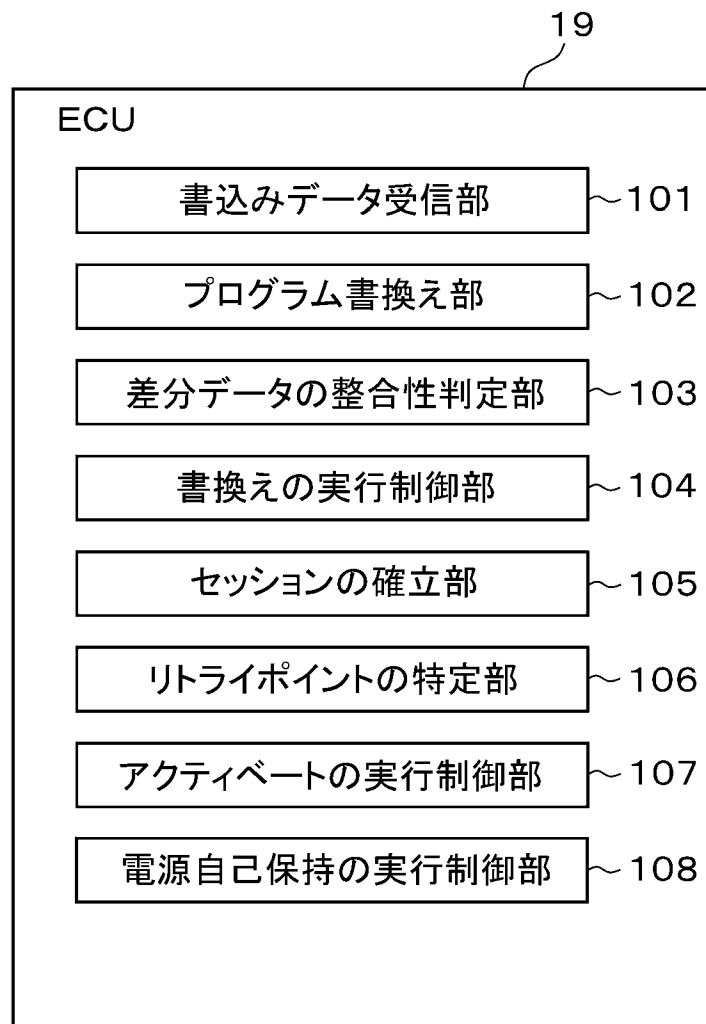
[図50]

Fig. 50



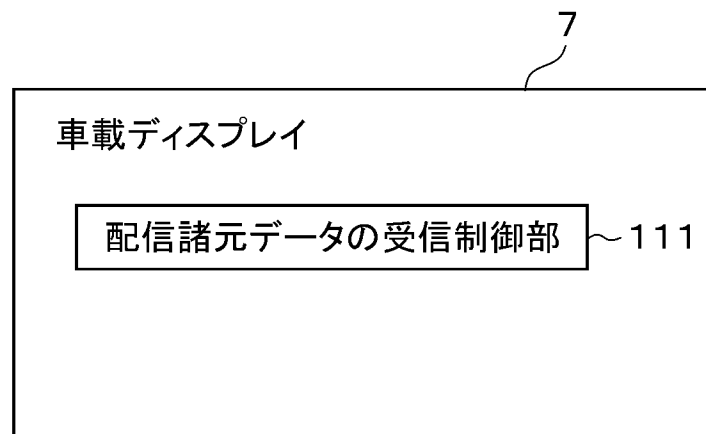
[図51]

Fig. 51



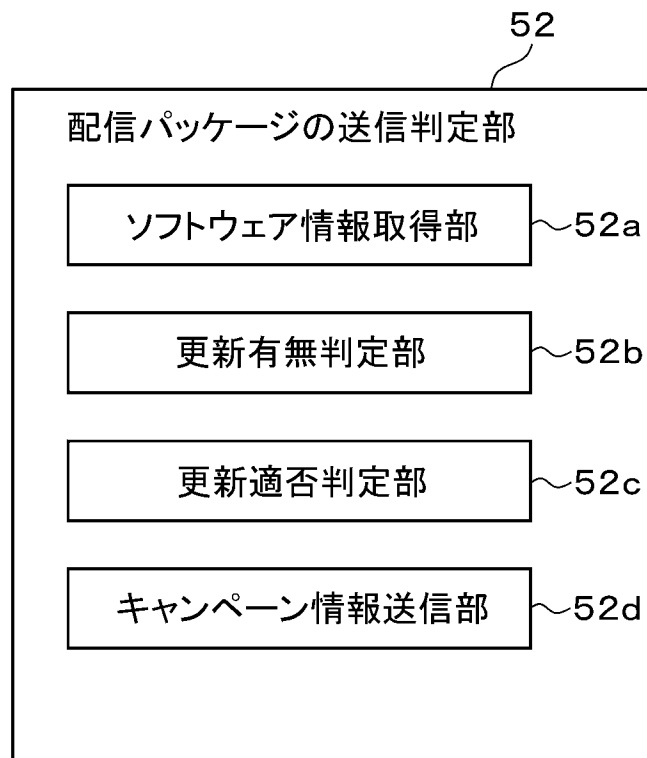
[図52]

Fig. 52



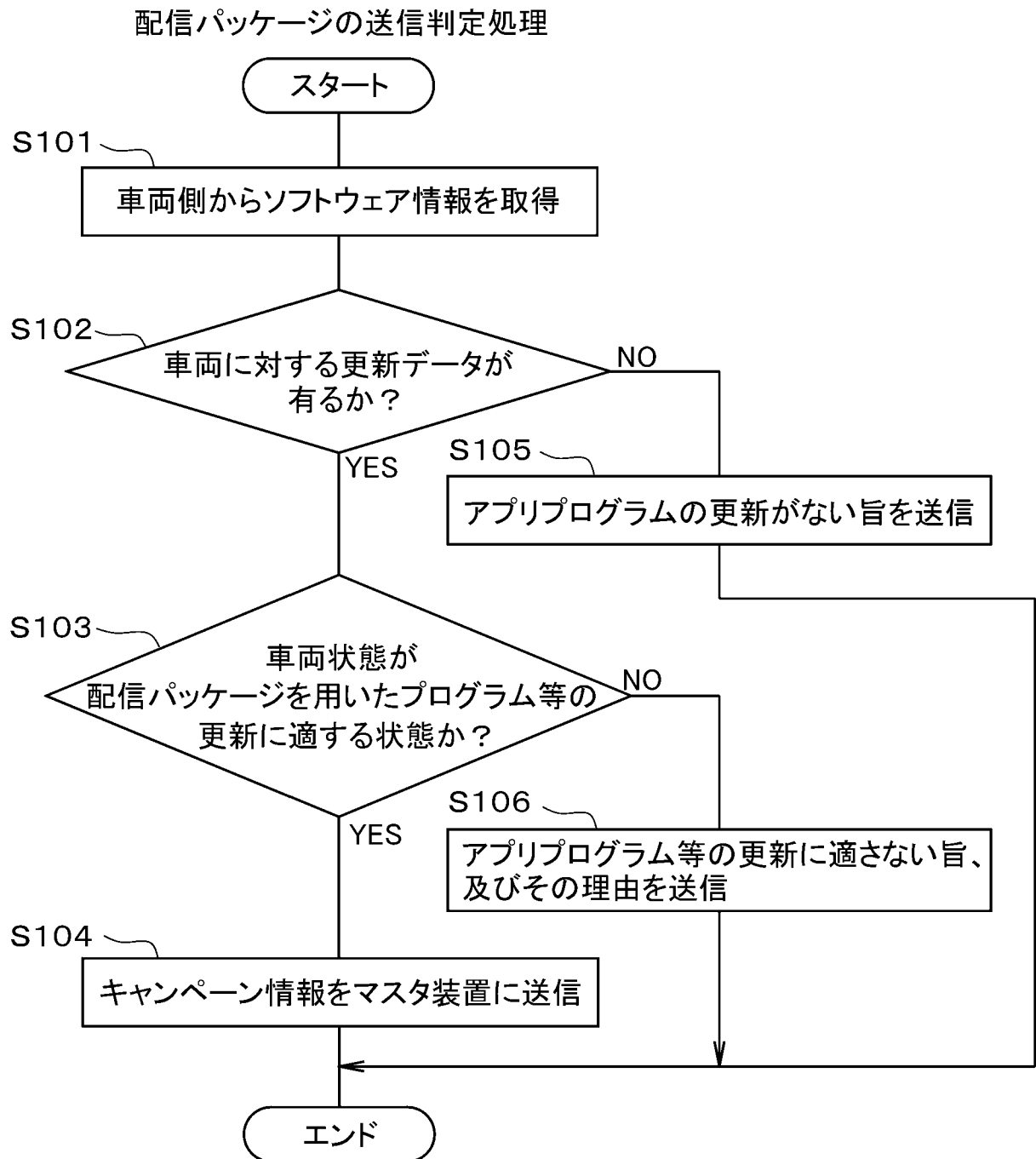
[図53]

Fig. 53



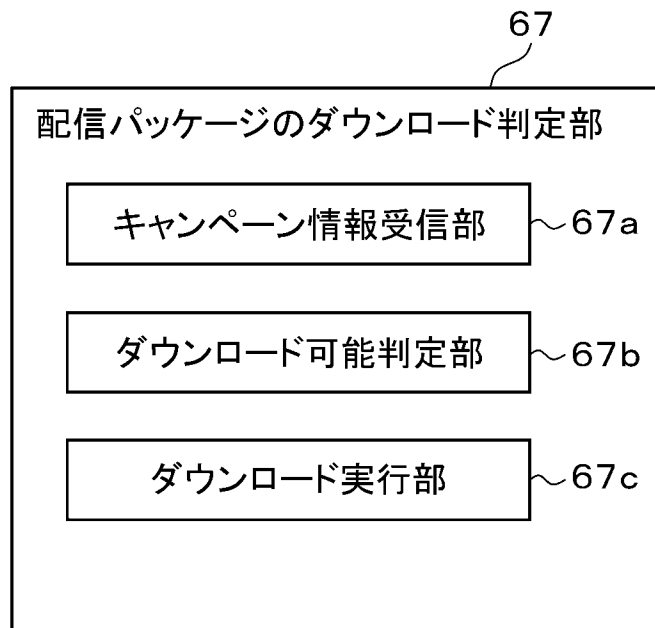
[図54]

Fig. 54



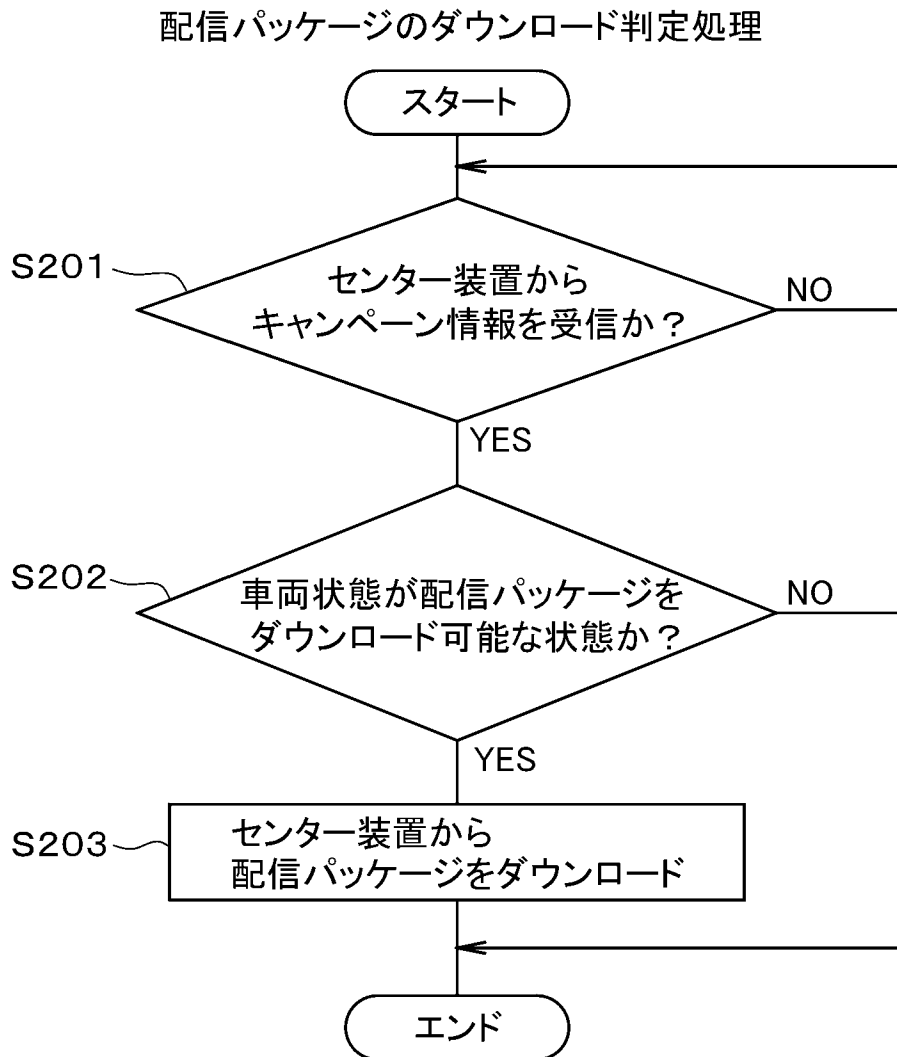
[図55]

Fig. 55



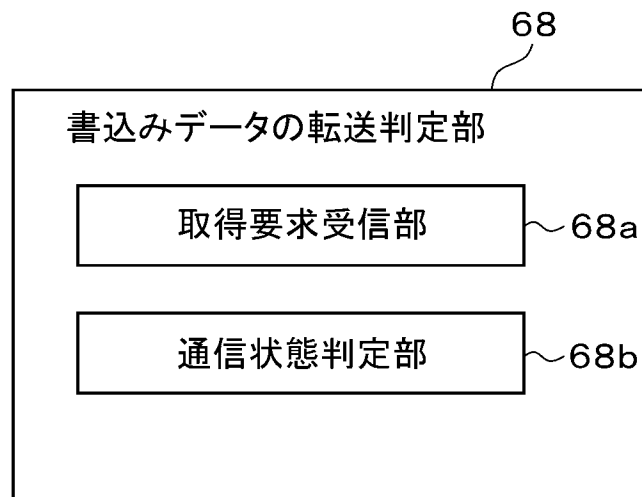
[図56]

Fig. 56



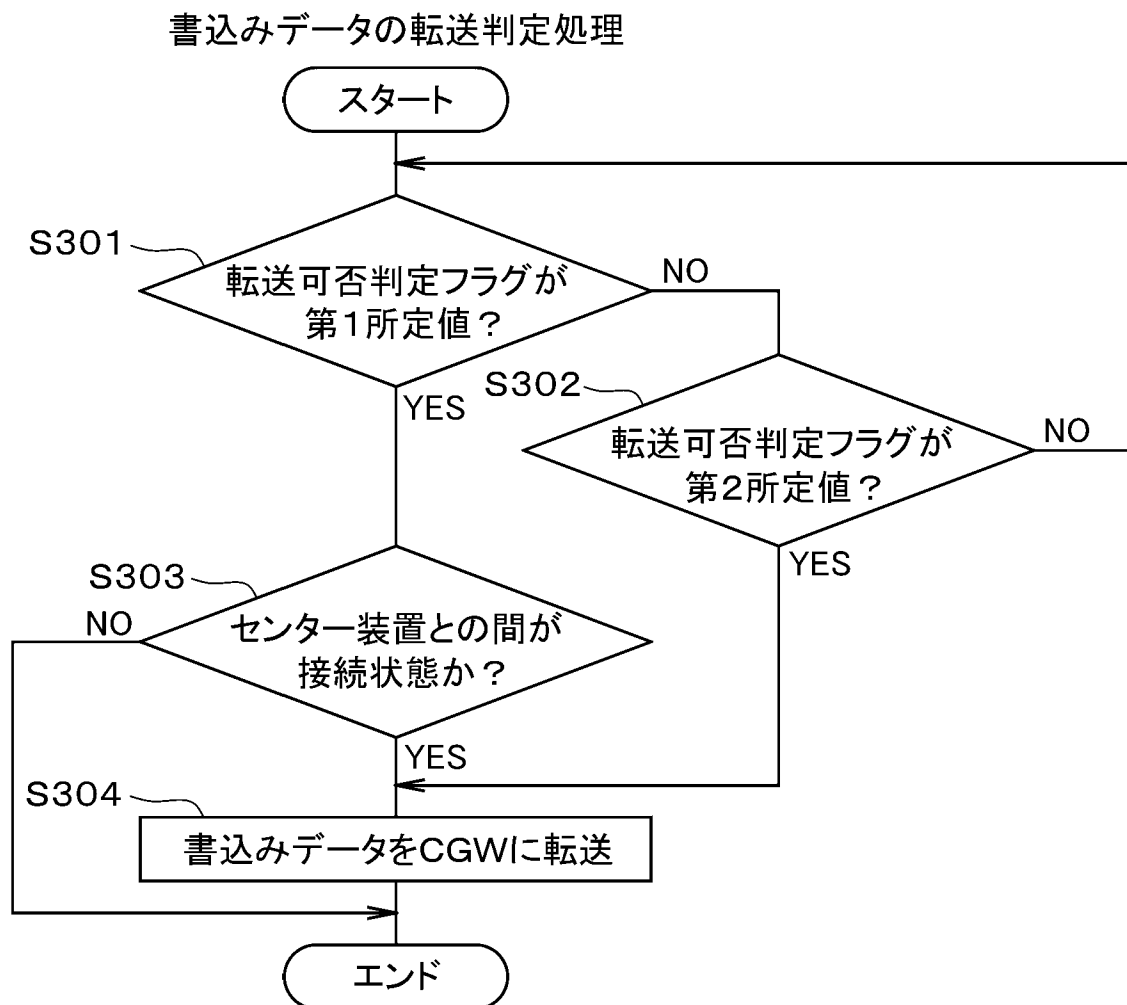
[図57]

Fig. 57



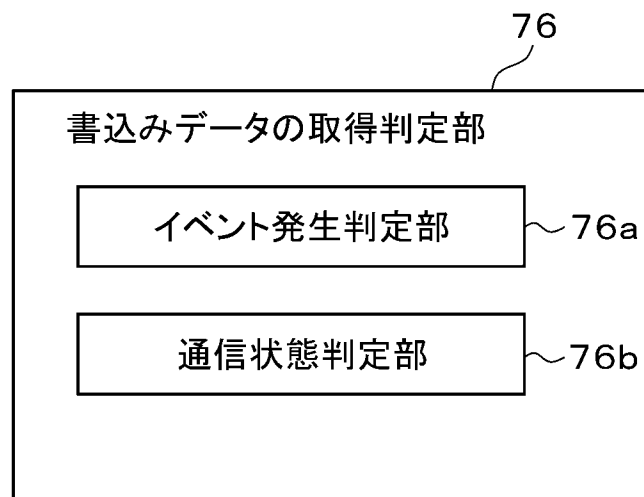
[図58]

Fig. 58



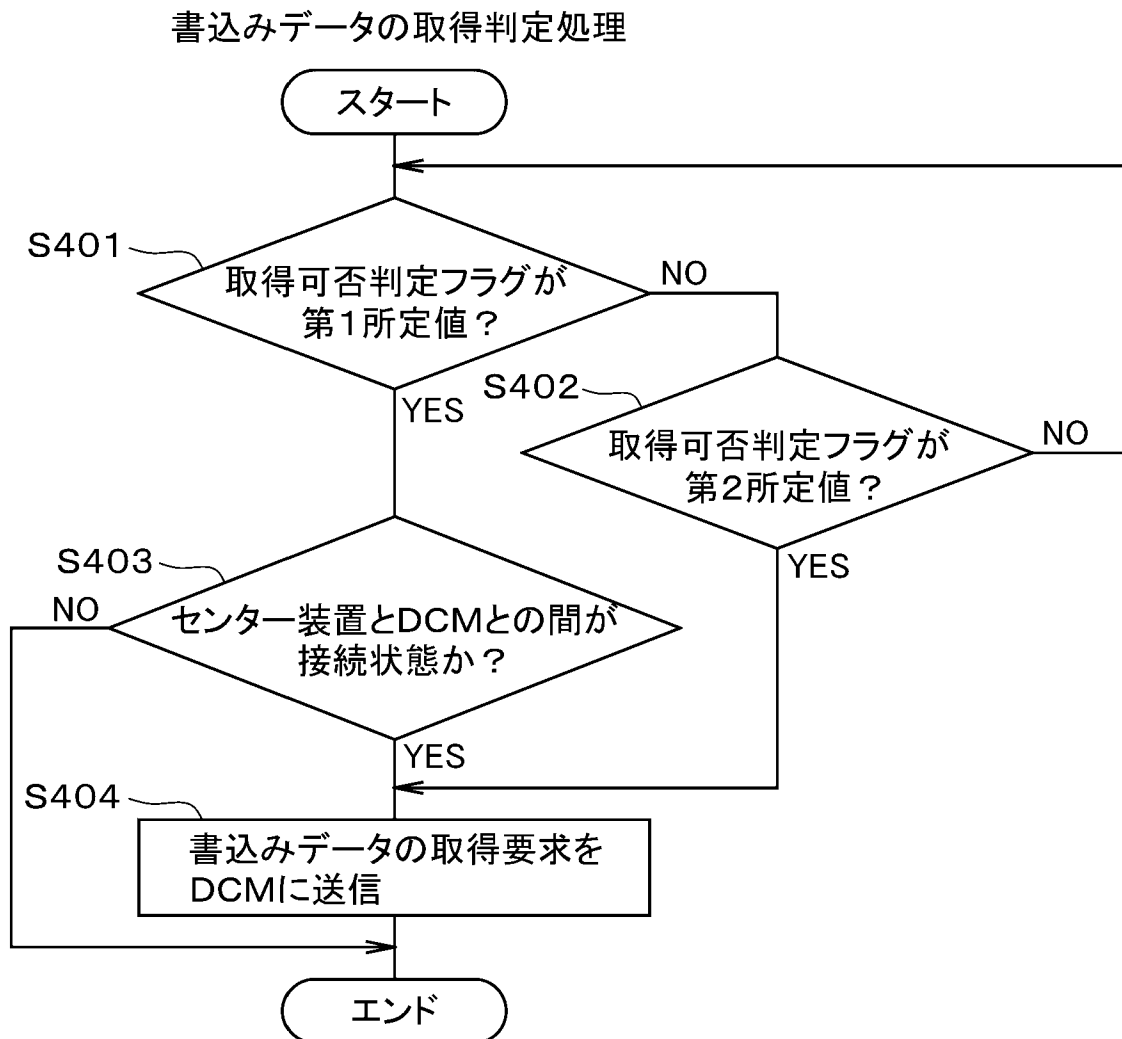
[図59]

Fig. 59



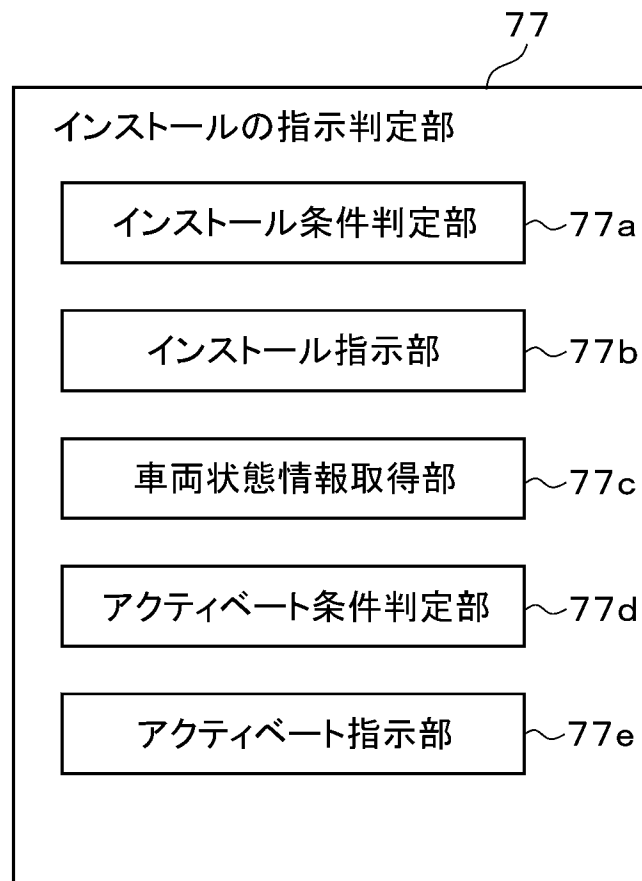
[図60]

Fig. 60



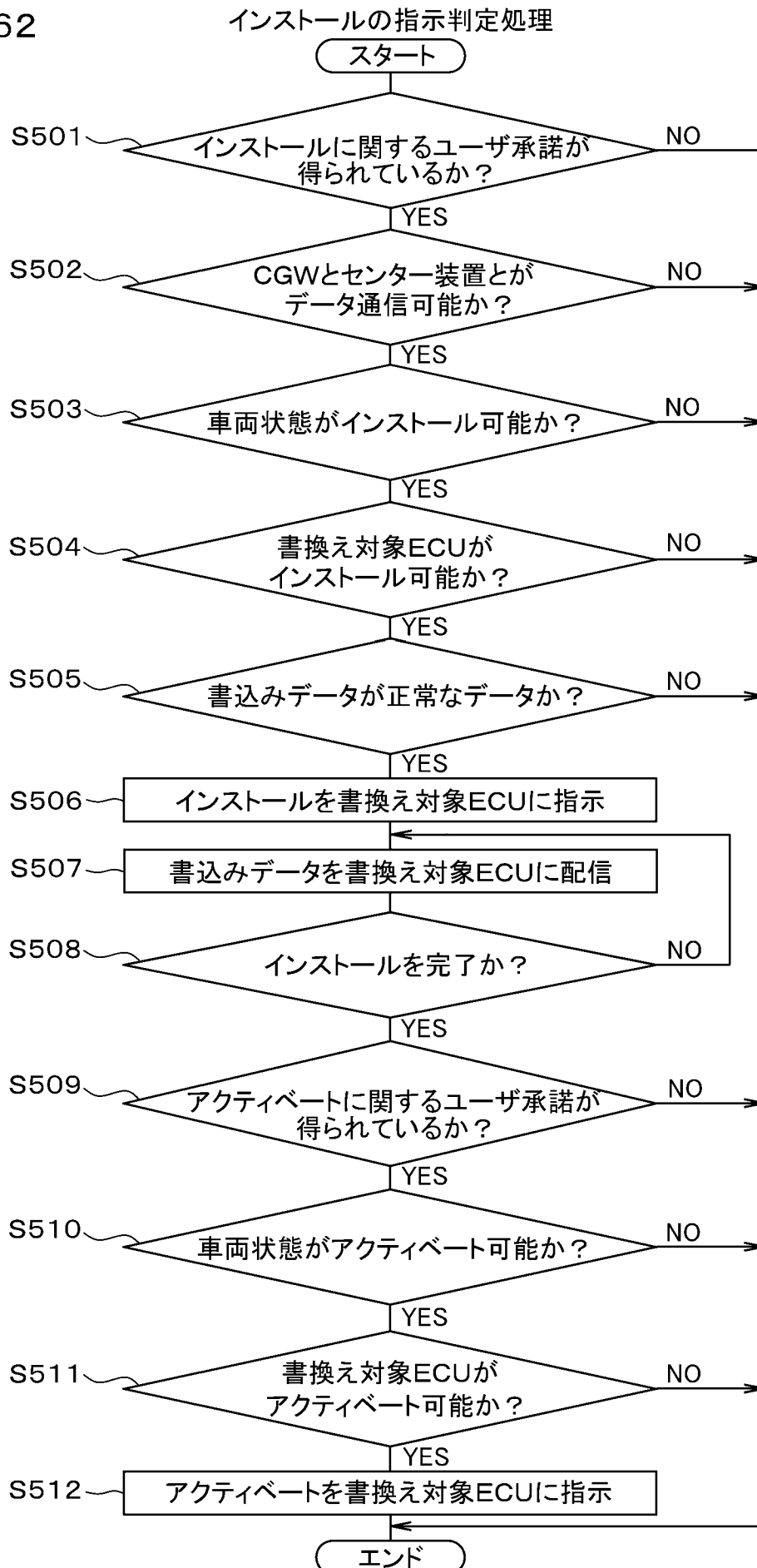
[図61]

Fig. 61



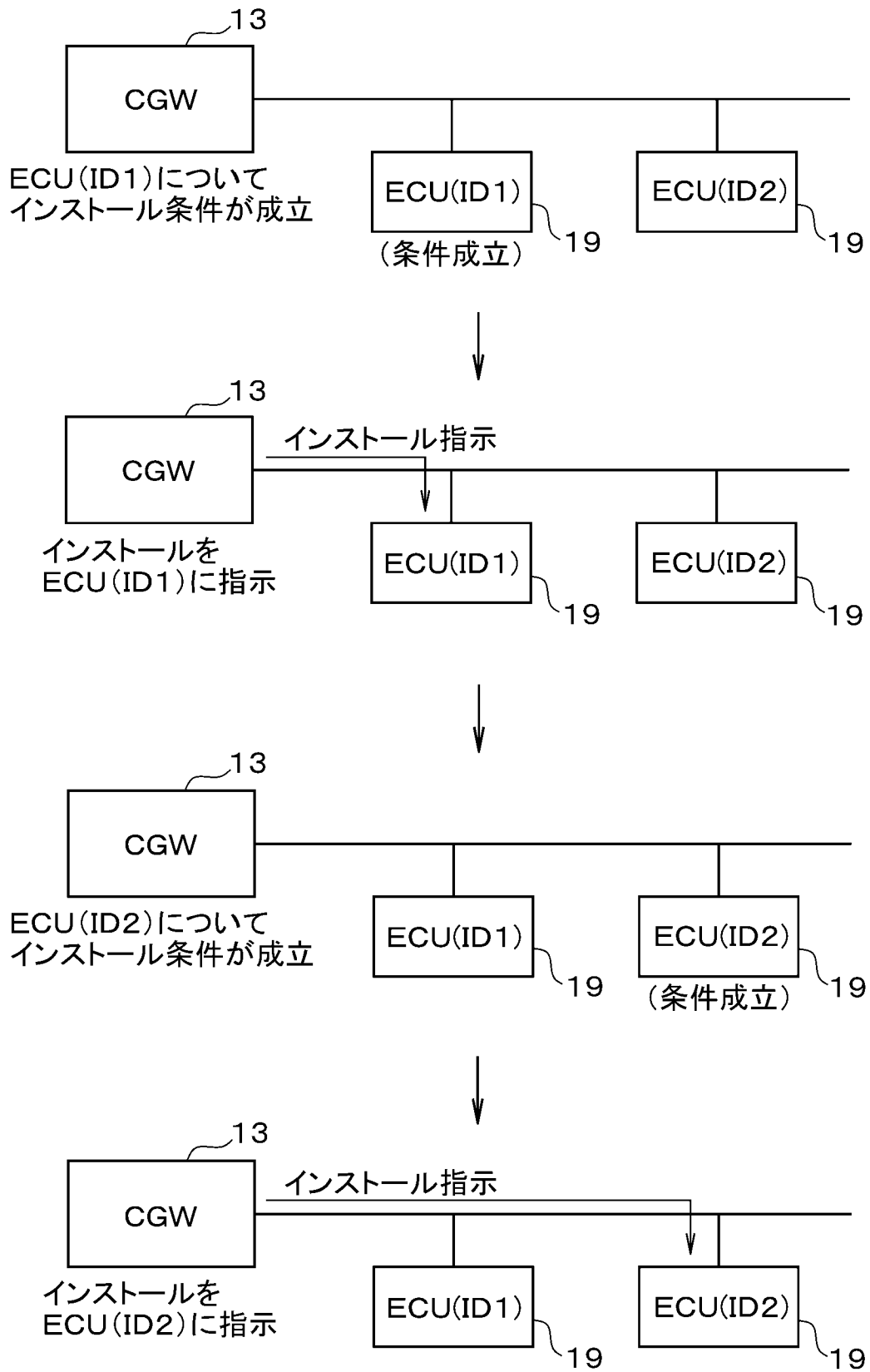
[図62]

Fig. 62



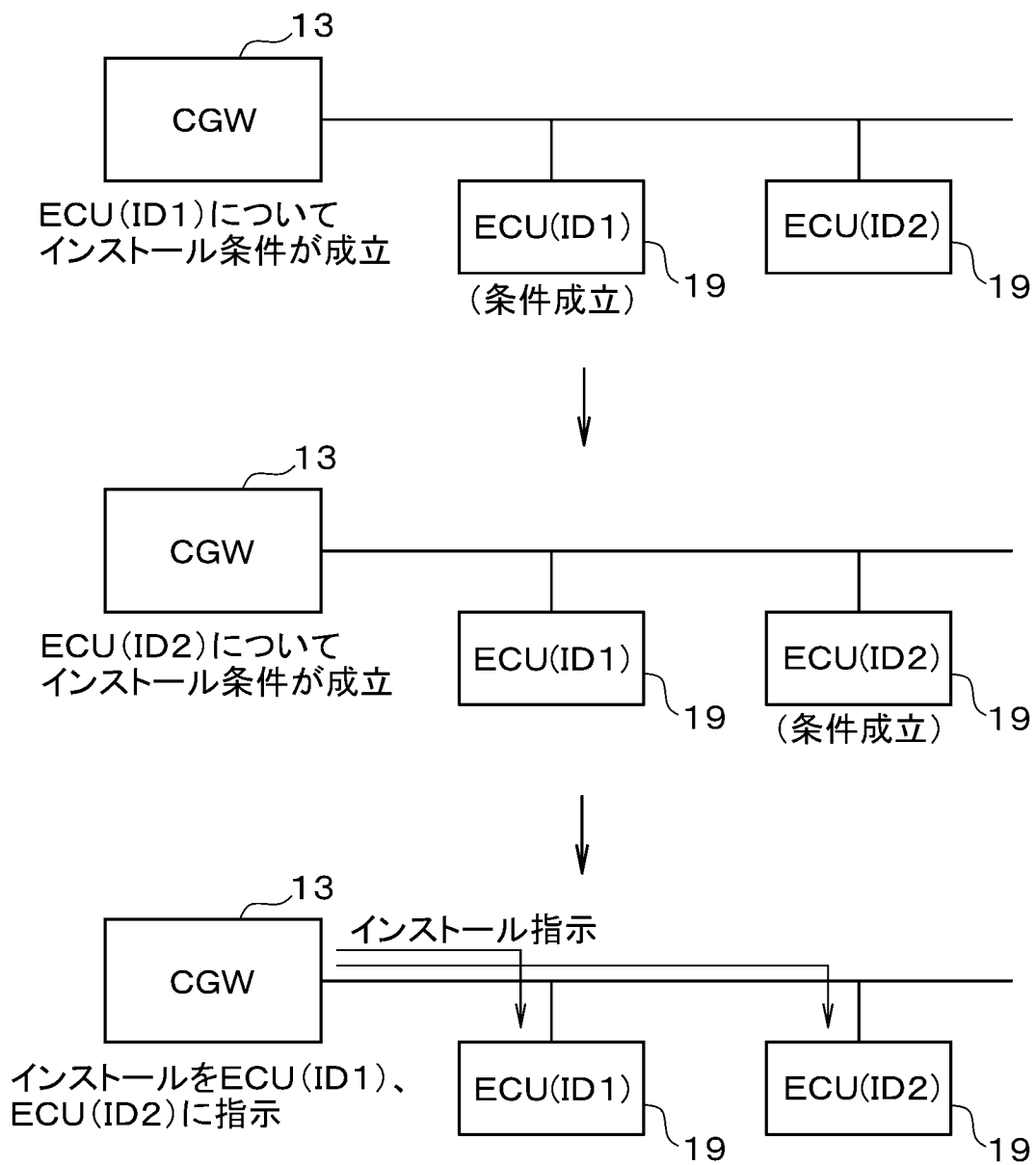
[図63]

Fig. 63



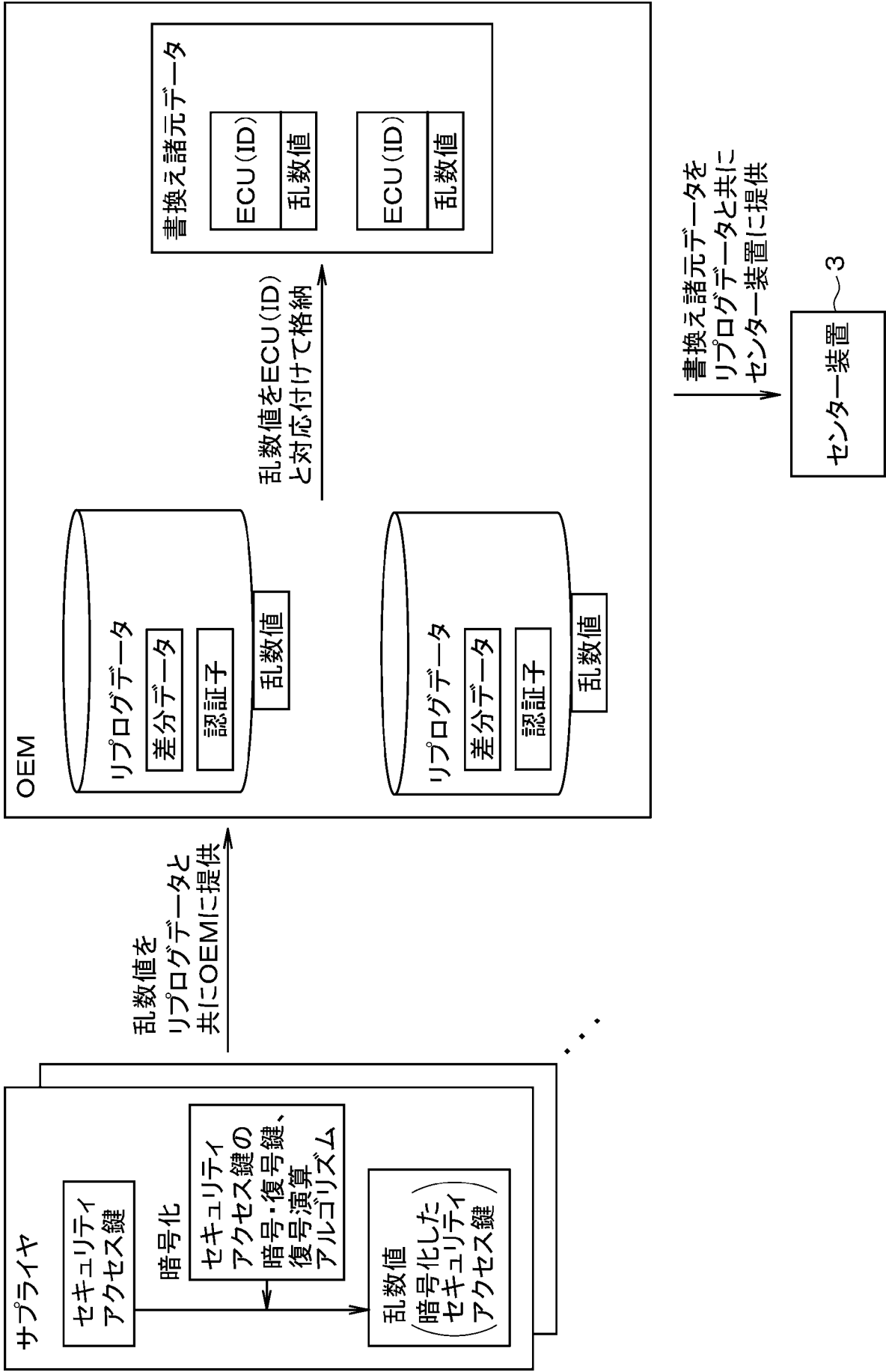
[図64]

Fig. 64



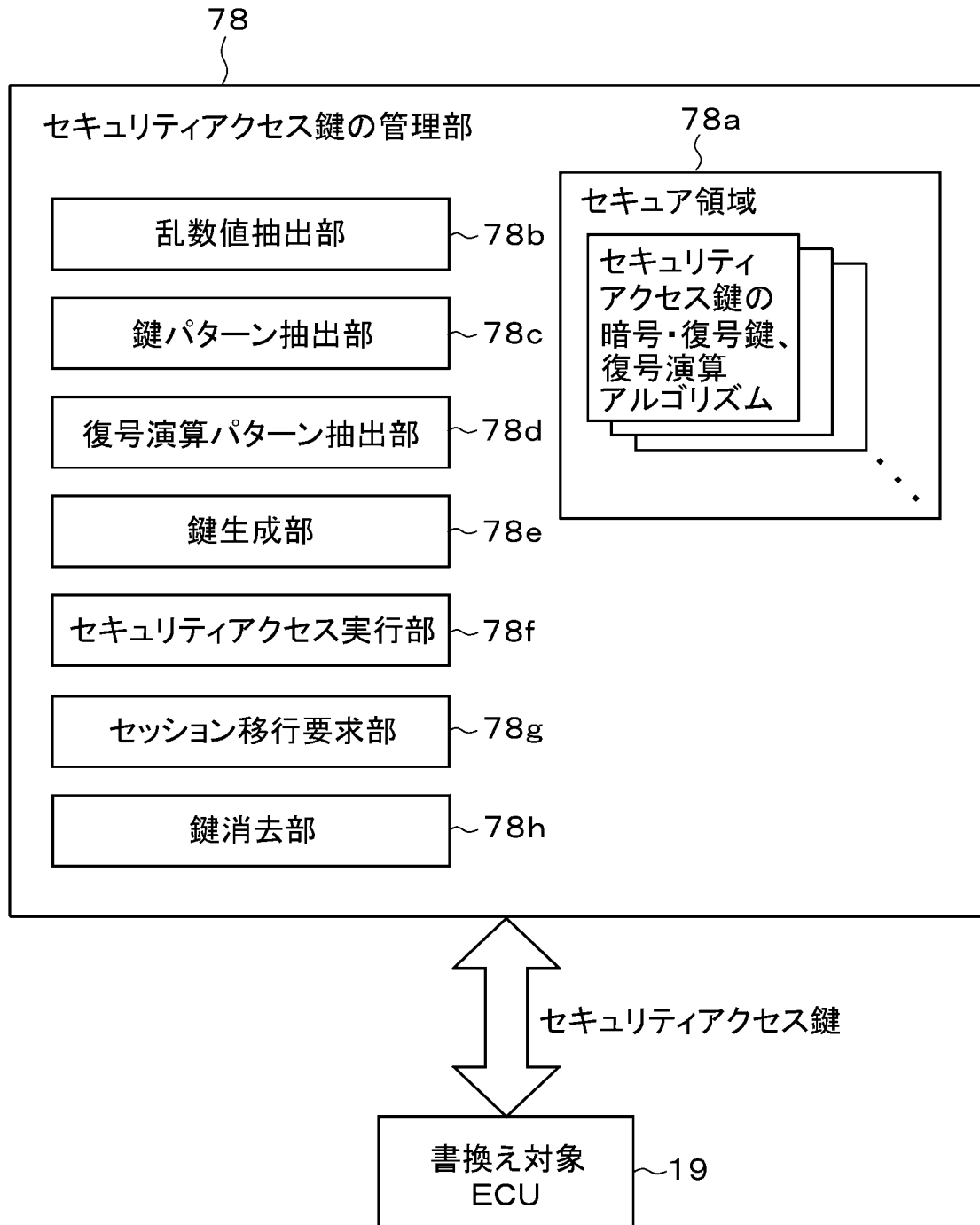
[図65]

Fig. 65



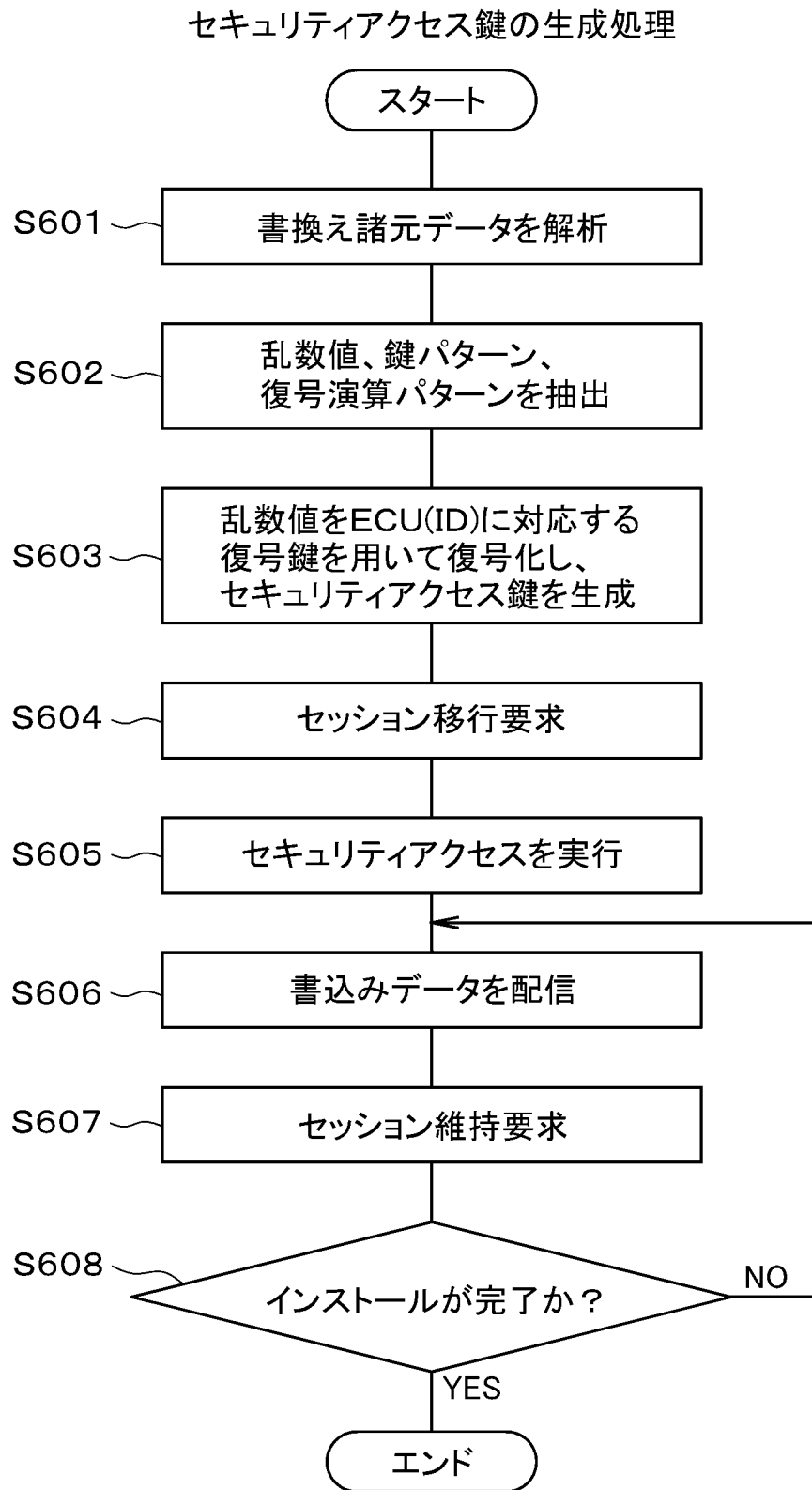
[図66]

Fig. 66



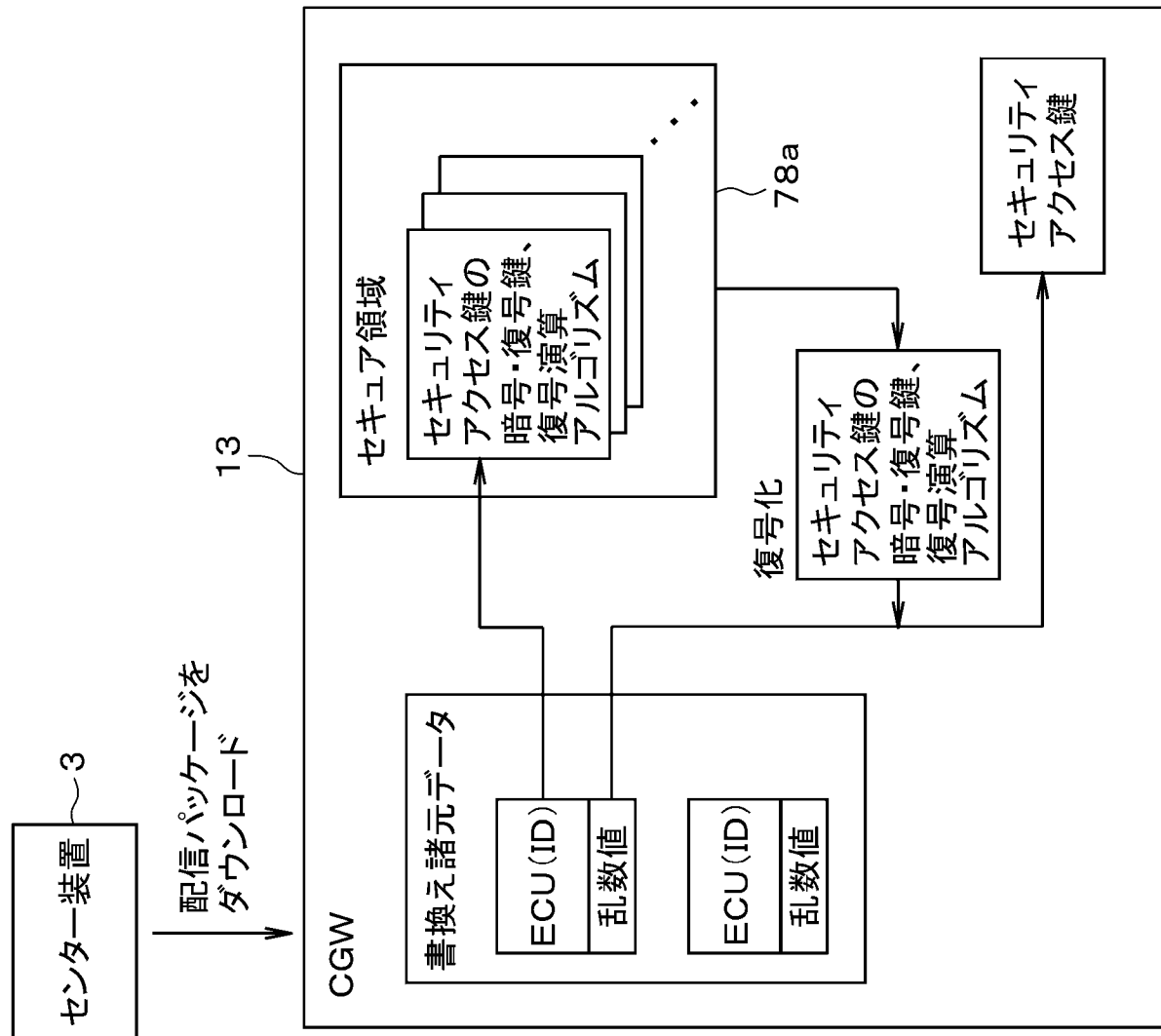
[図67]

Fig. 67



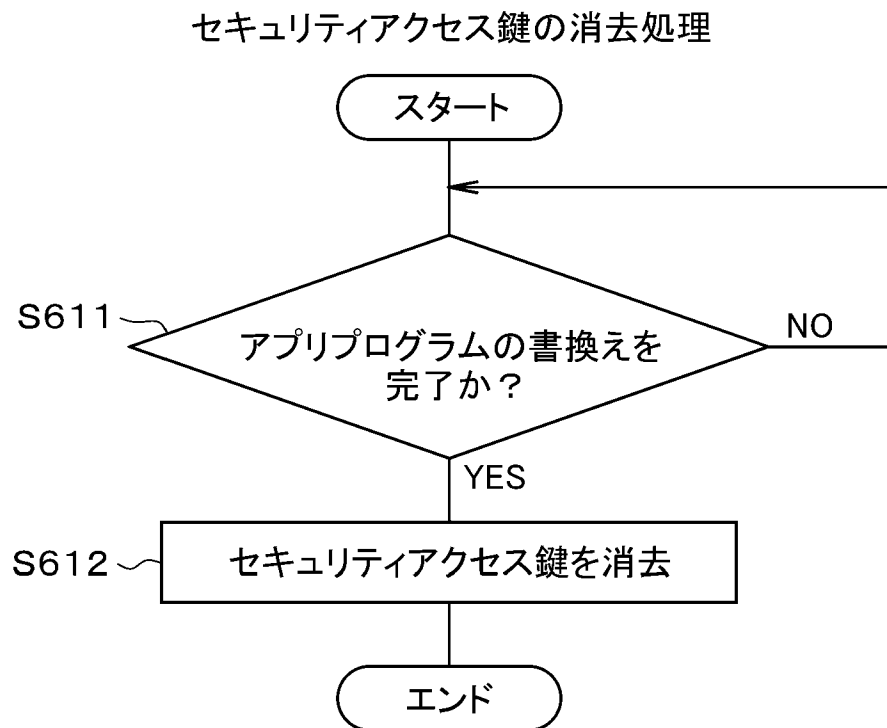
[図68]

Fig. 68



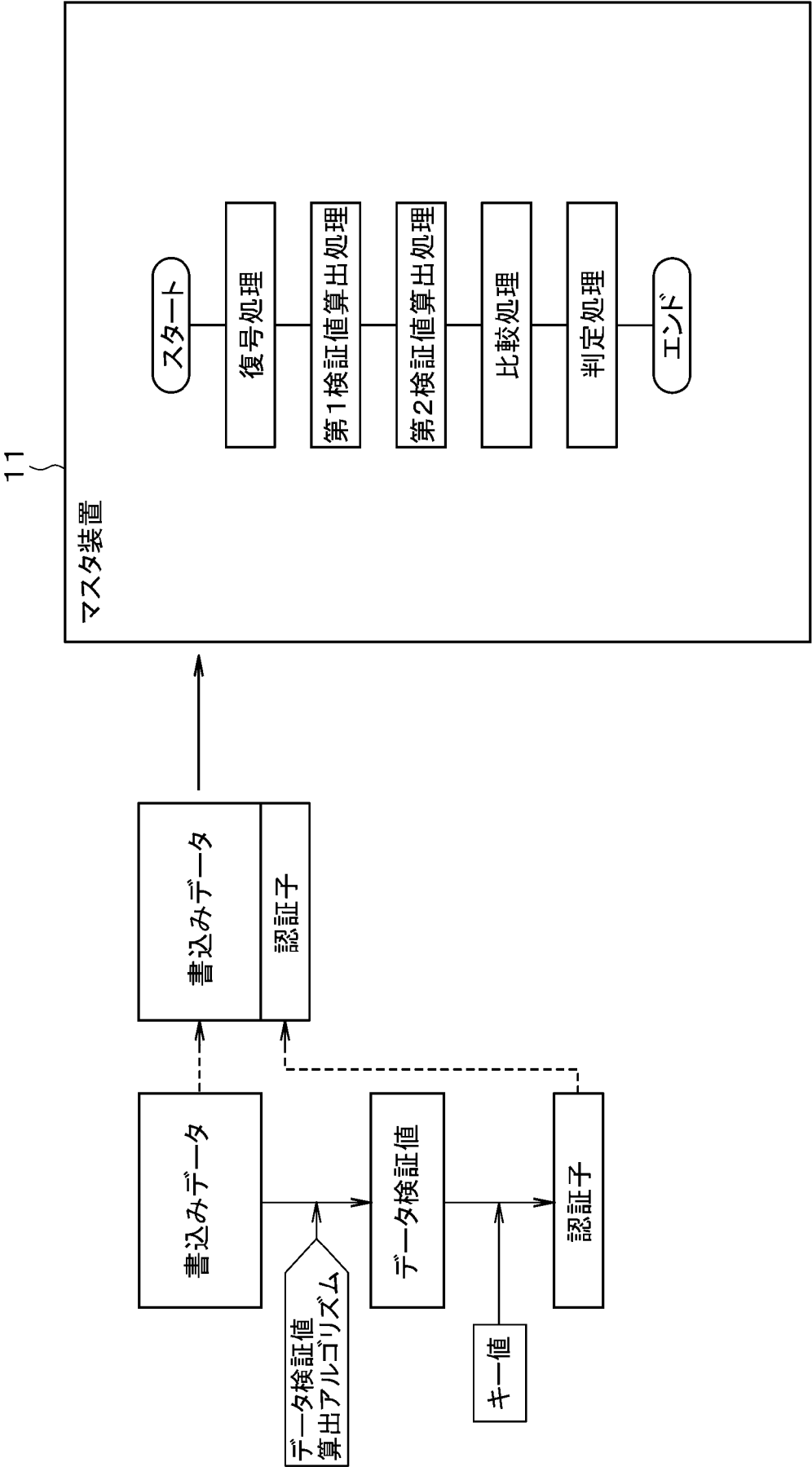
[図69]

Fig. 69



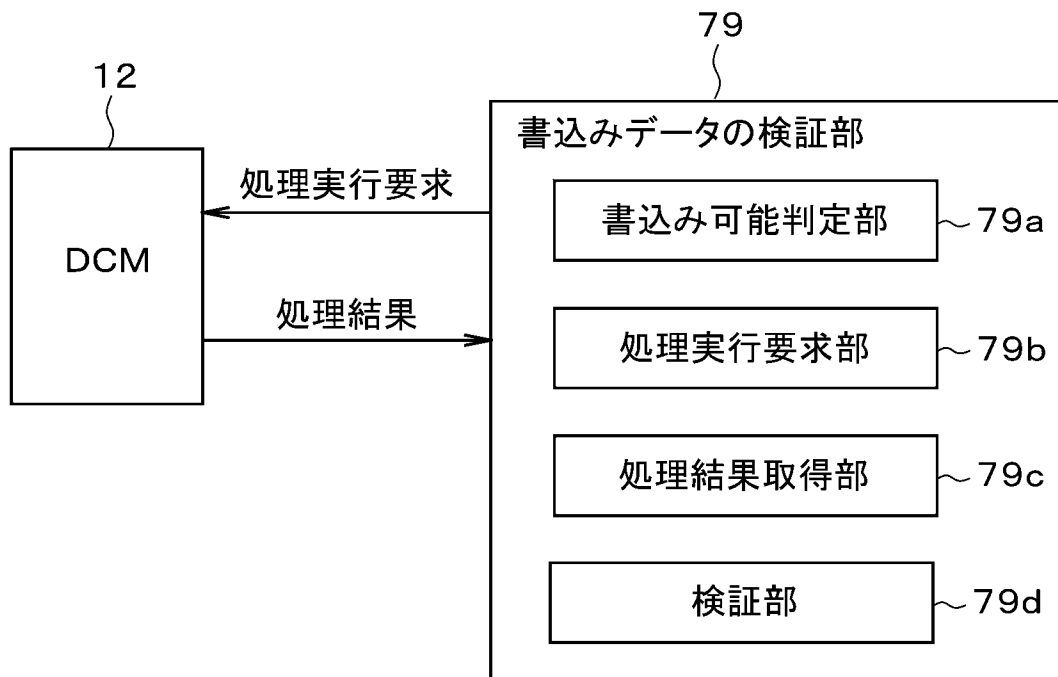
[図70]

Fig. 70



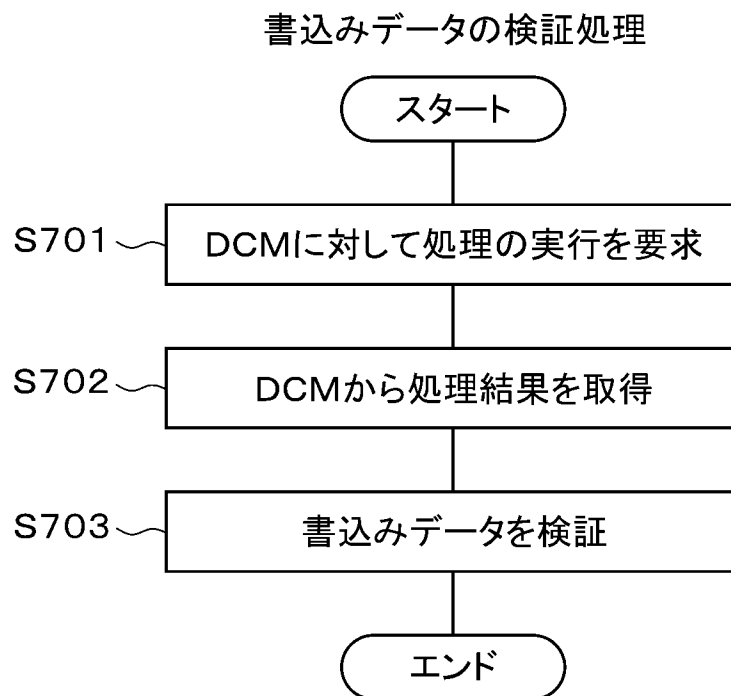
[図71]

Fig. 71



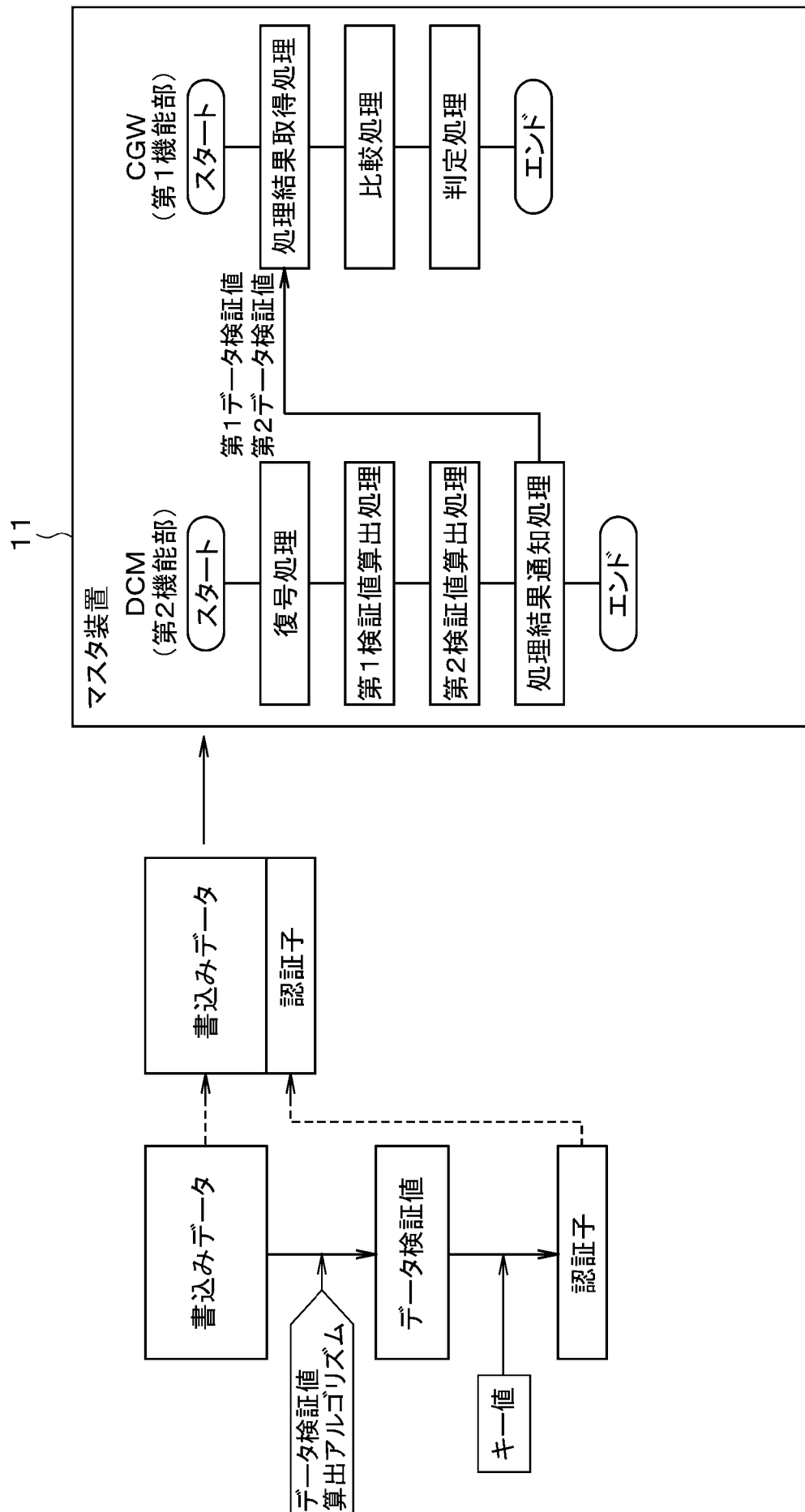
[図72]

Fig. 72



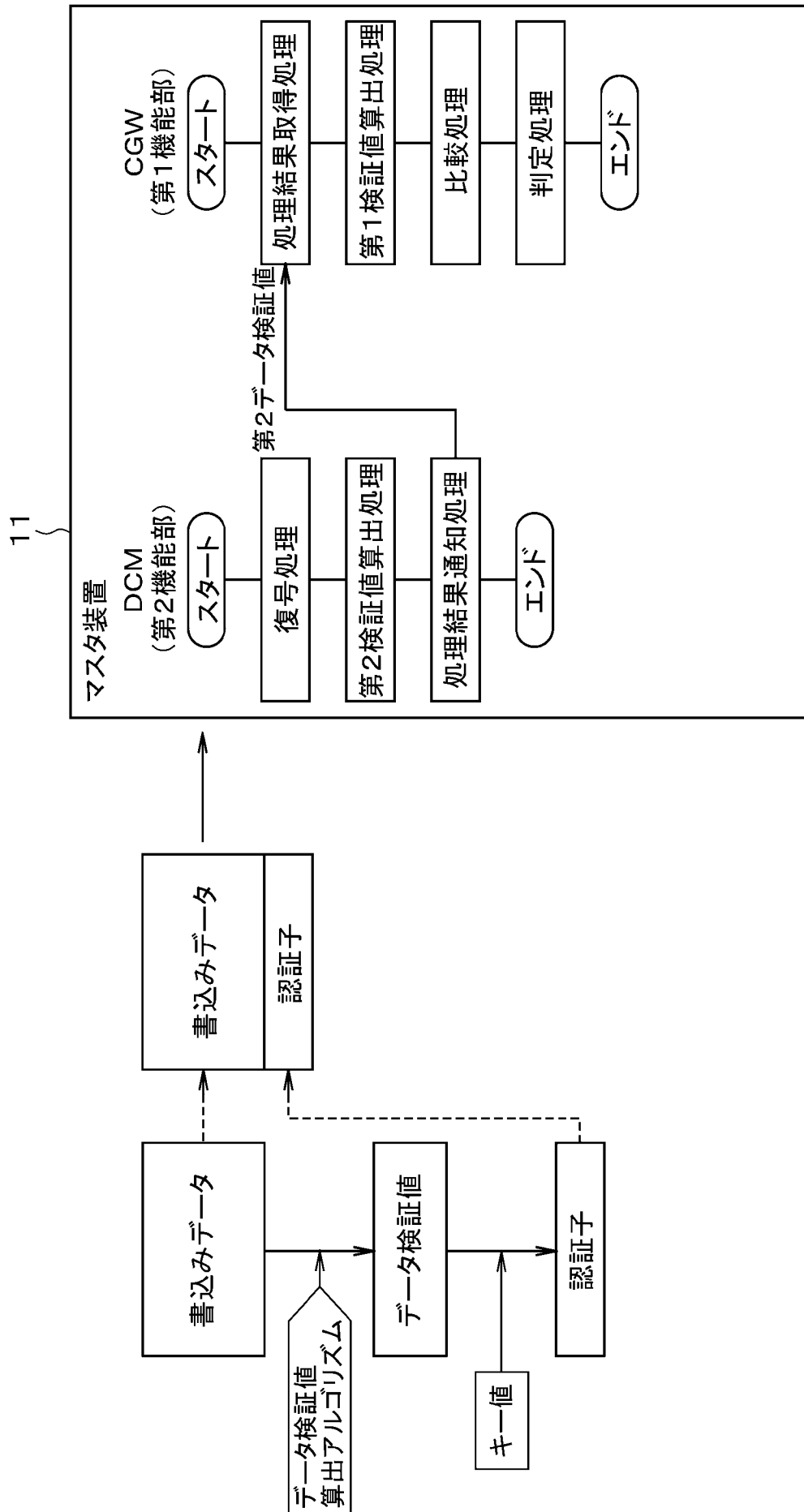
[図73]

Fig. 73

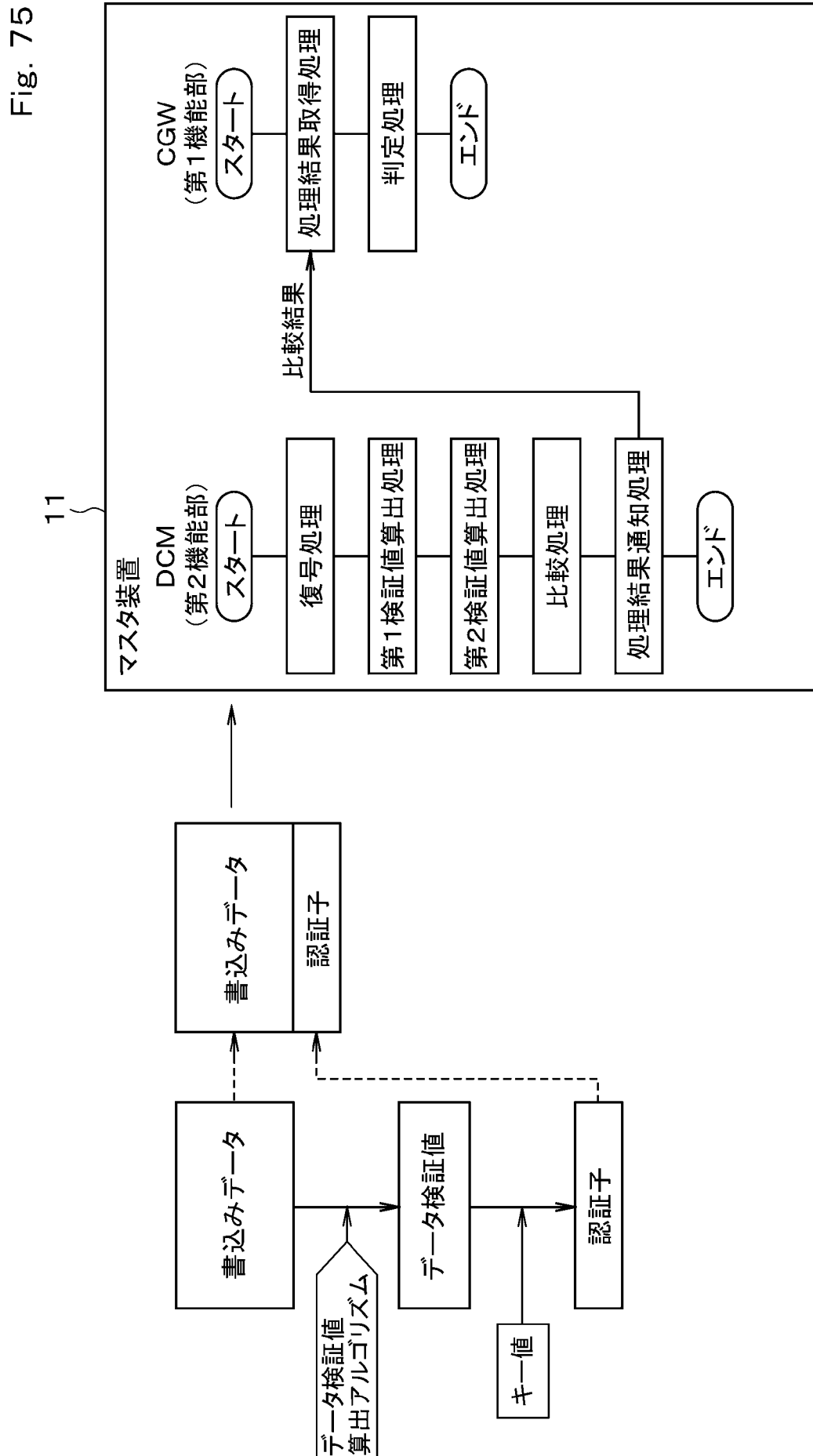


[図74]

Fig. 74

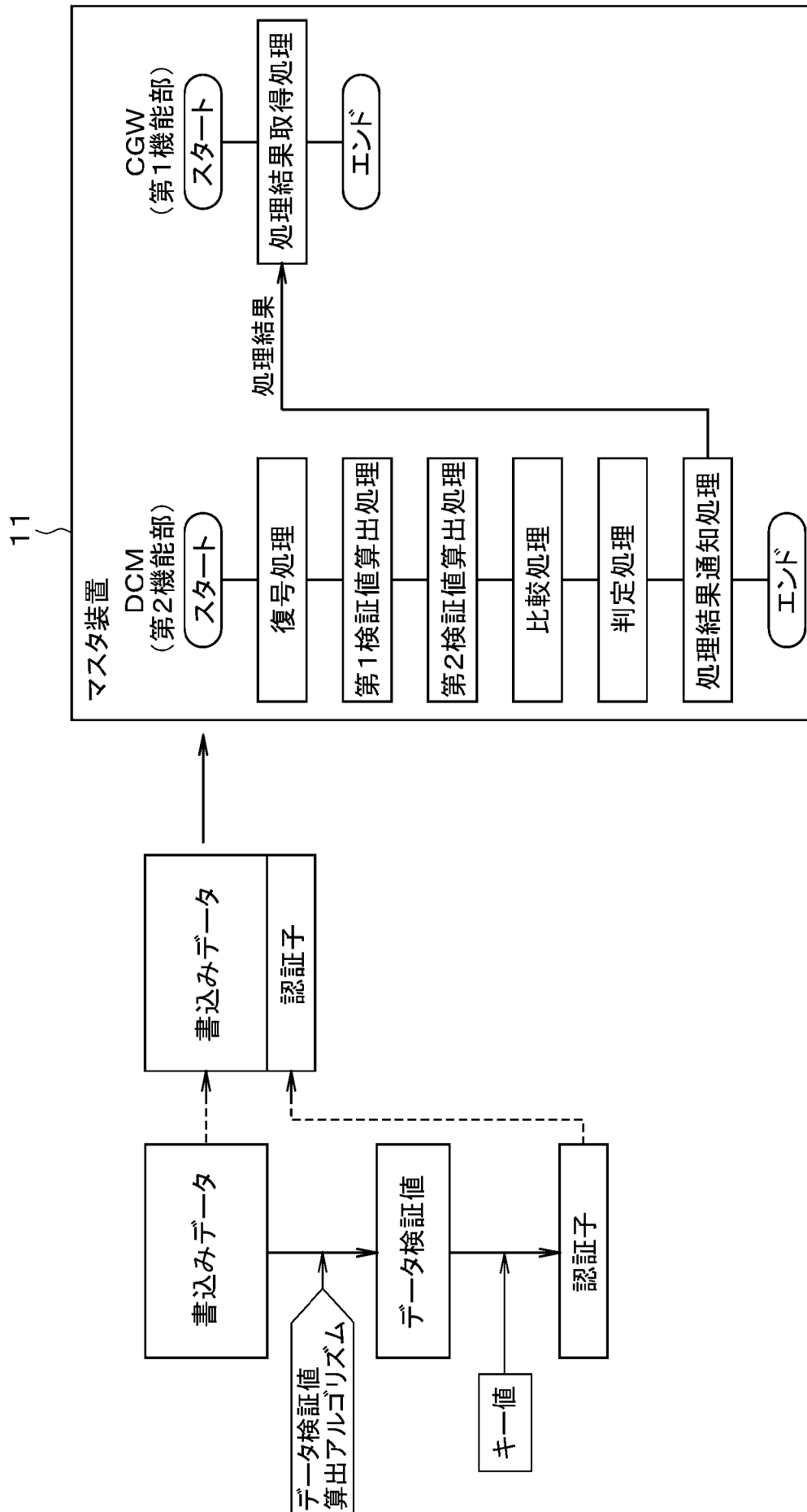


[図 75]



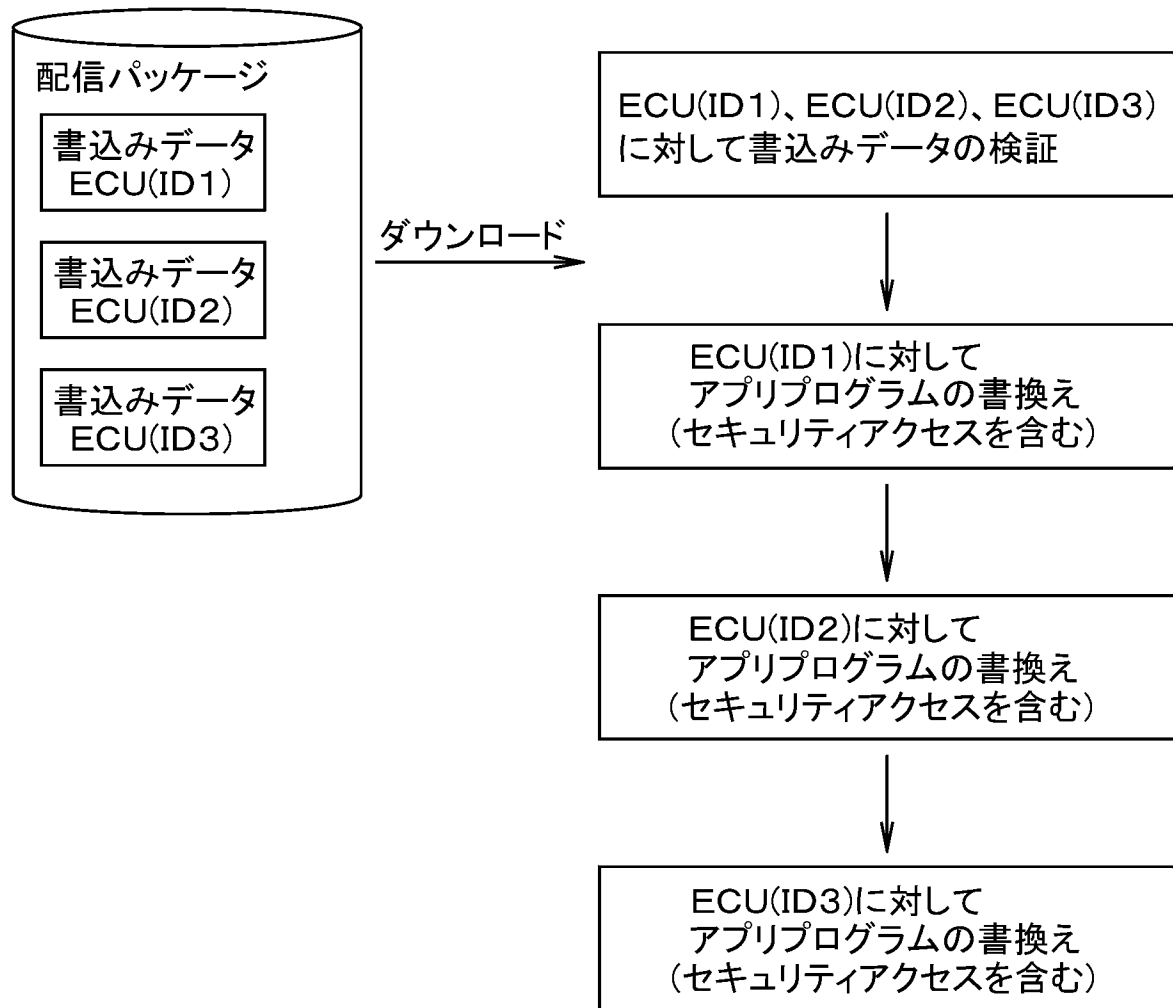
[図76]

Fig. 76



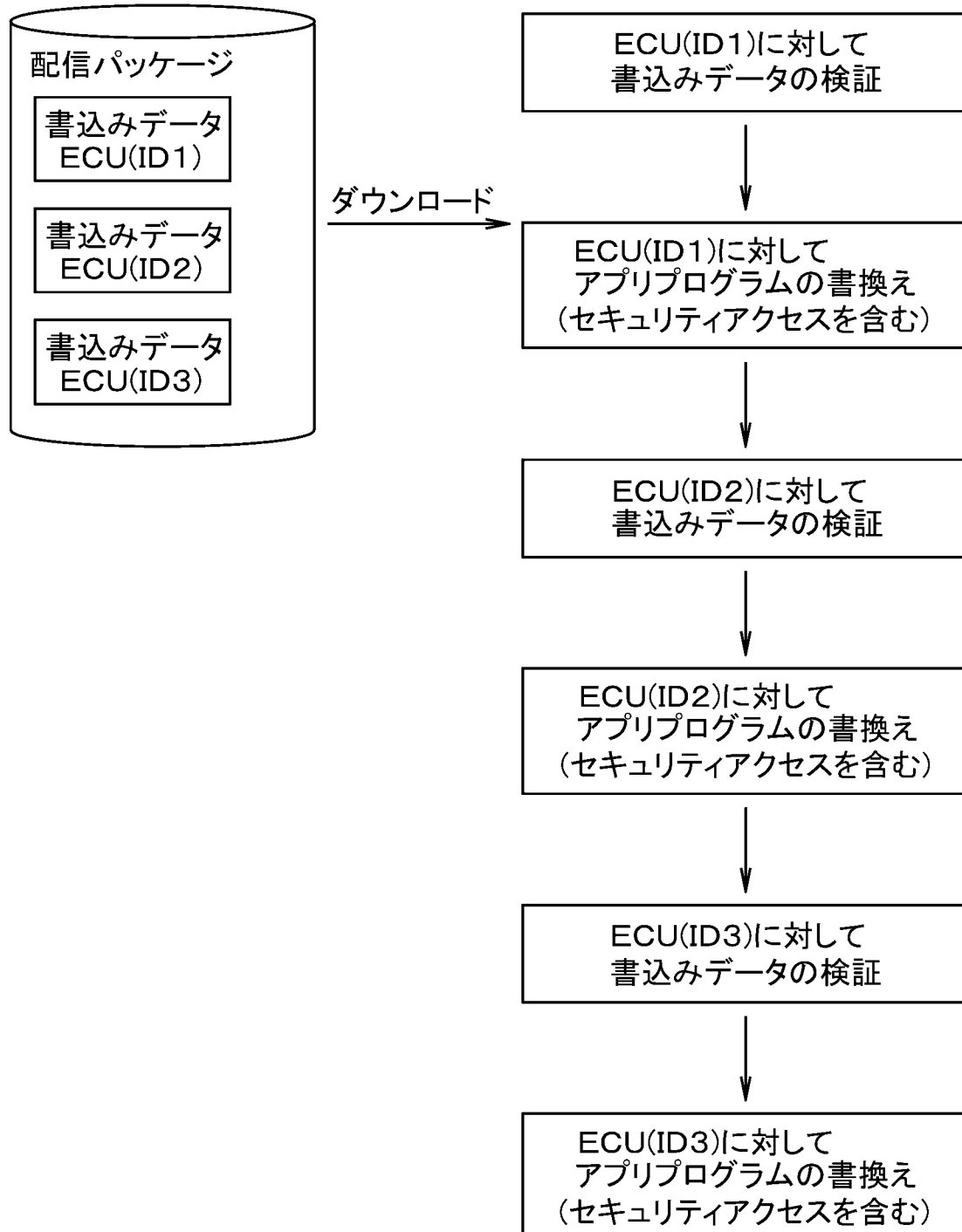
[図77]

Fig. 77



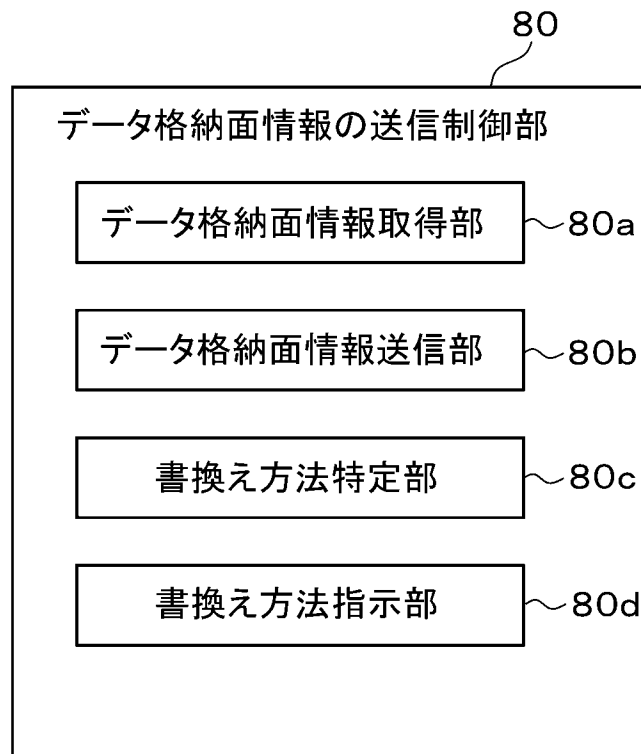
[図78]

Fig. 78



[図79]

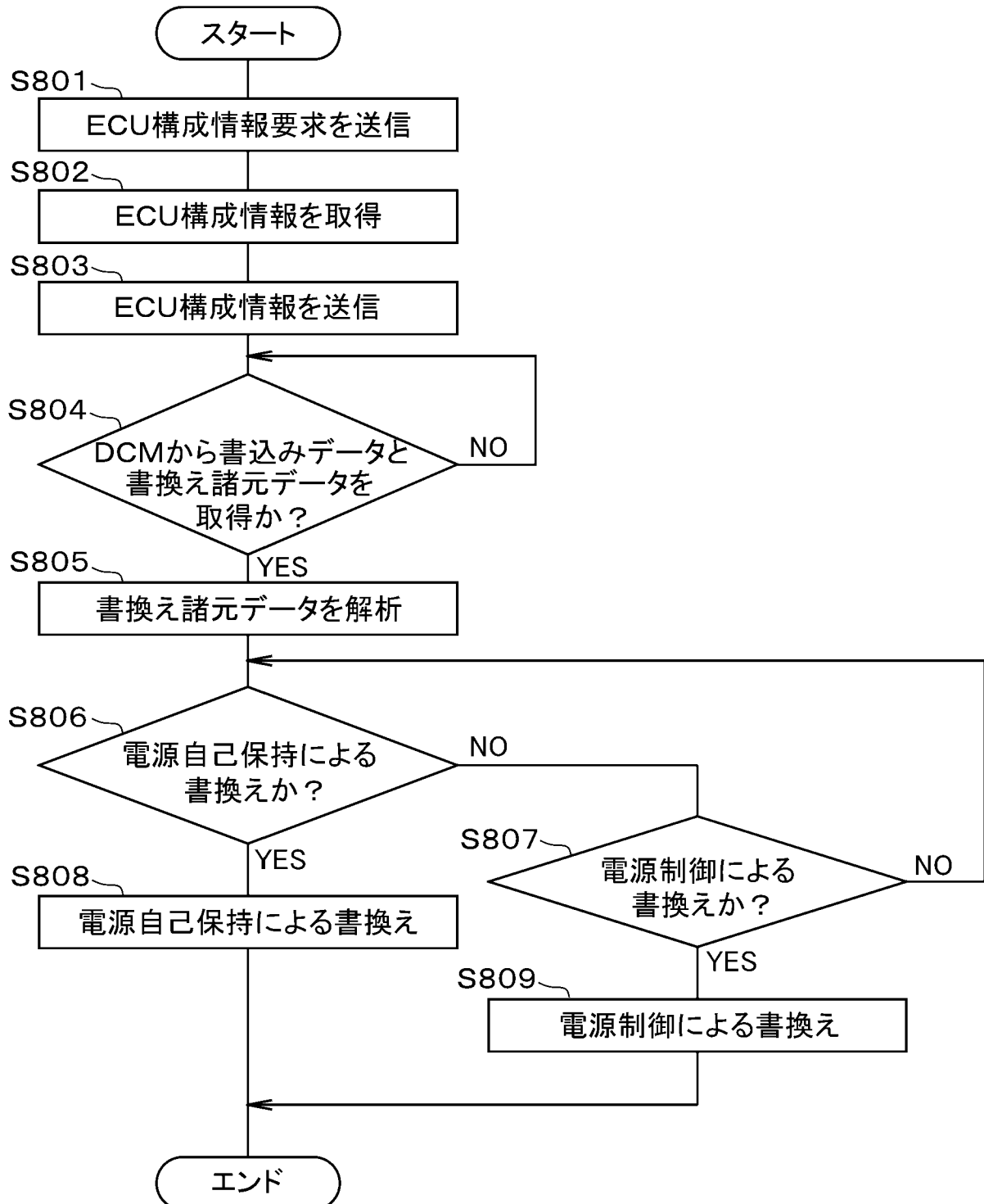
Fig. 79



[図80]

Fig. 80

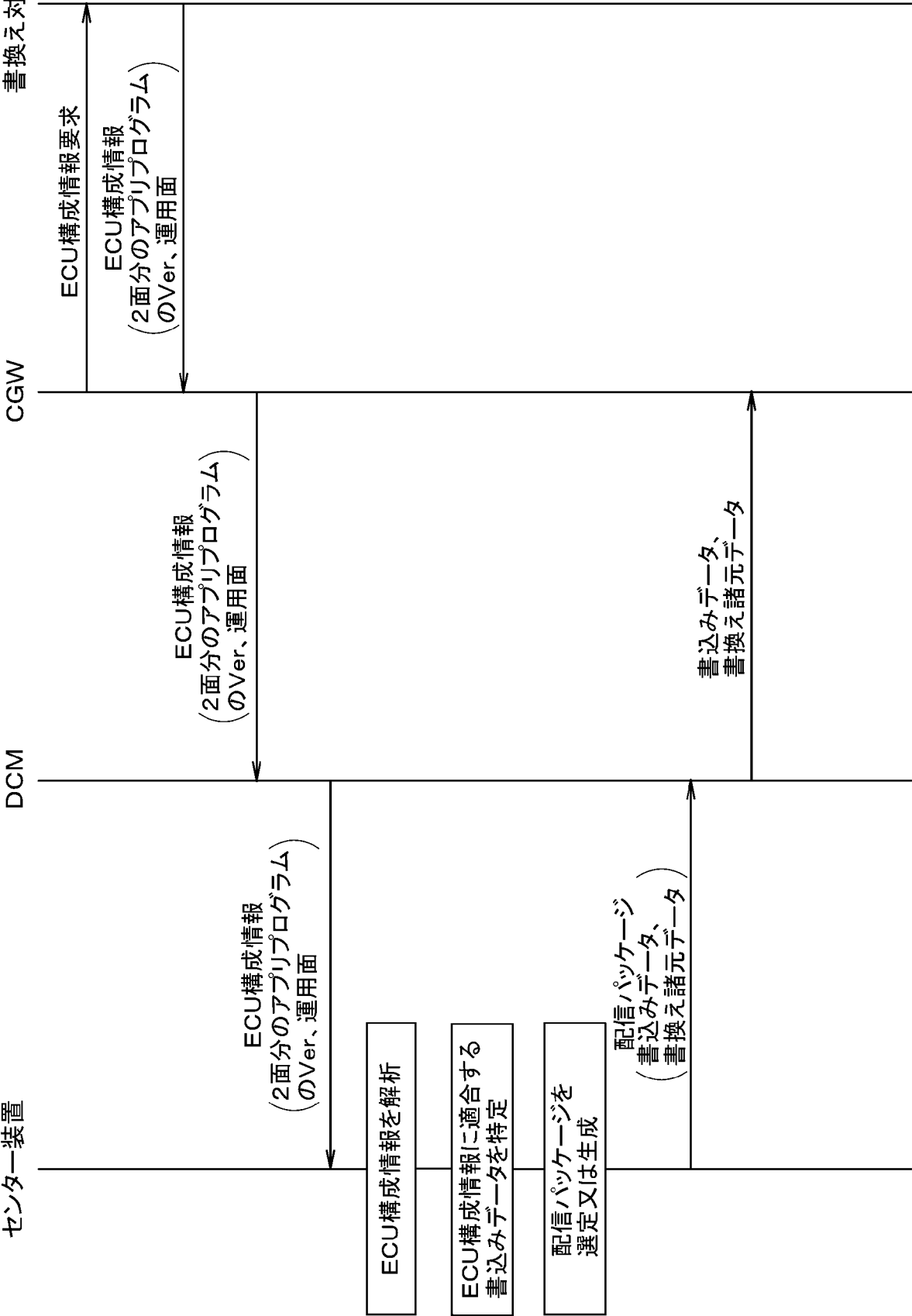
データ格納面情報の送信制御処理



[図81]

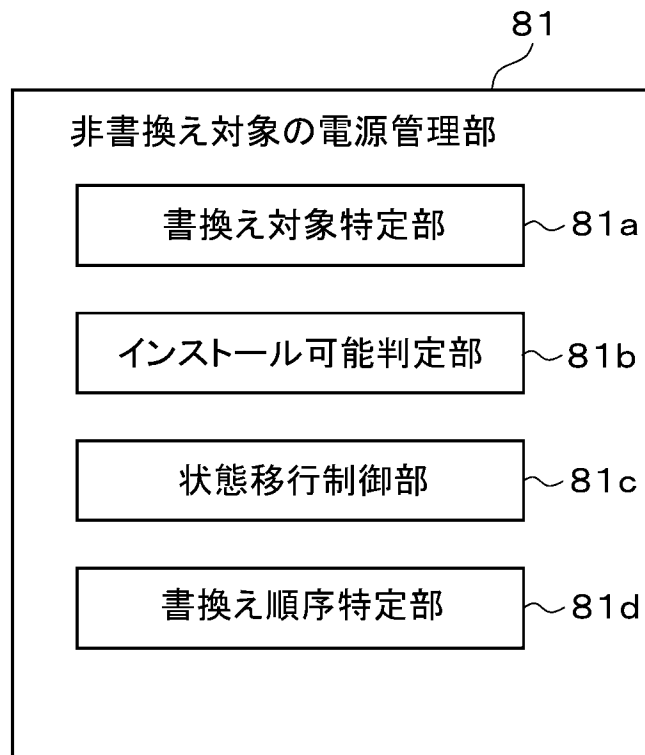
Fig. 81

書換え対象ECU



[図82]

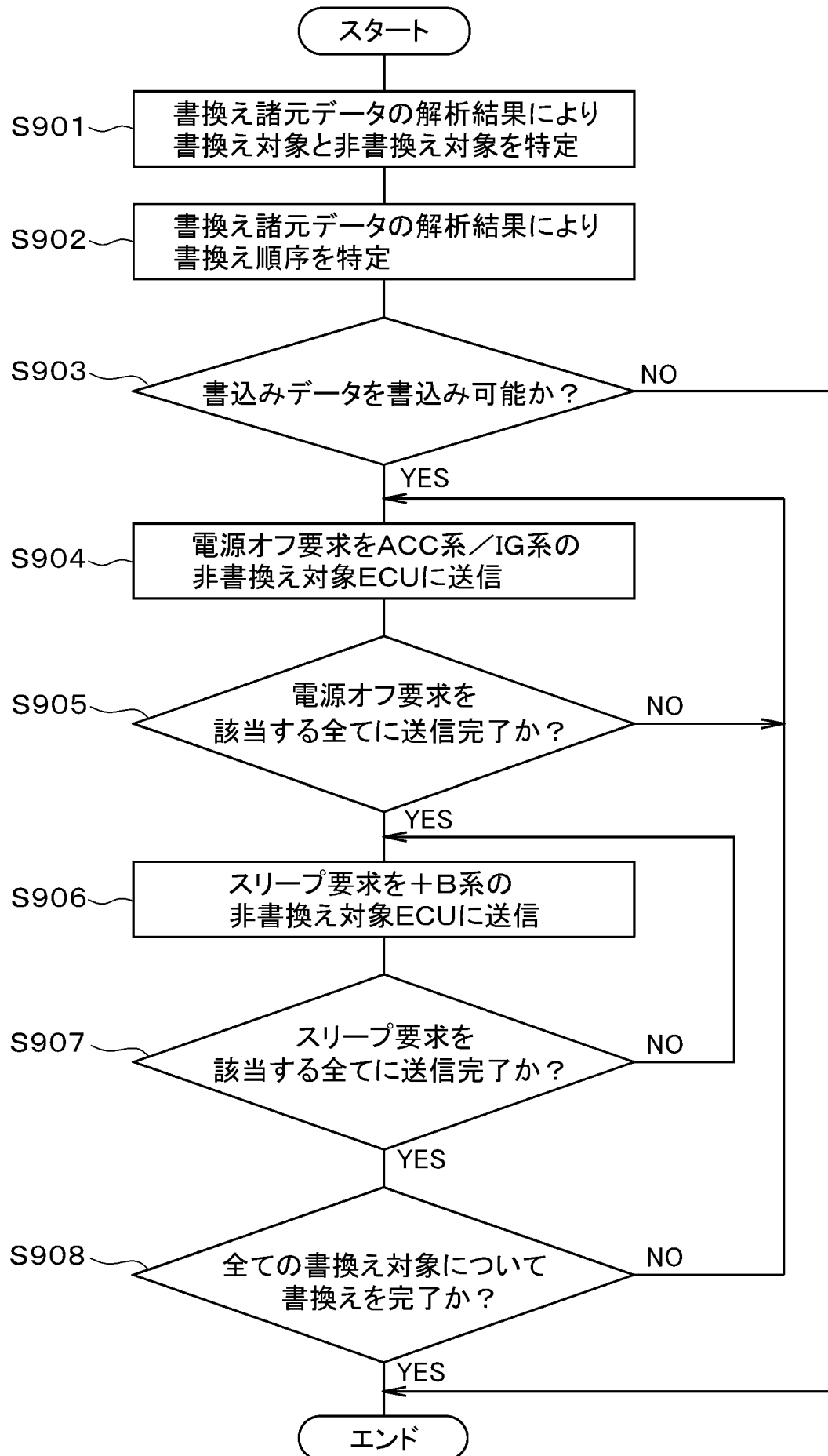
Fig. 82



[図83]

Fig. 83

非書換え対象の電源管理処理



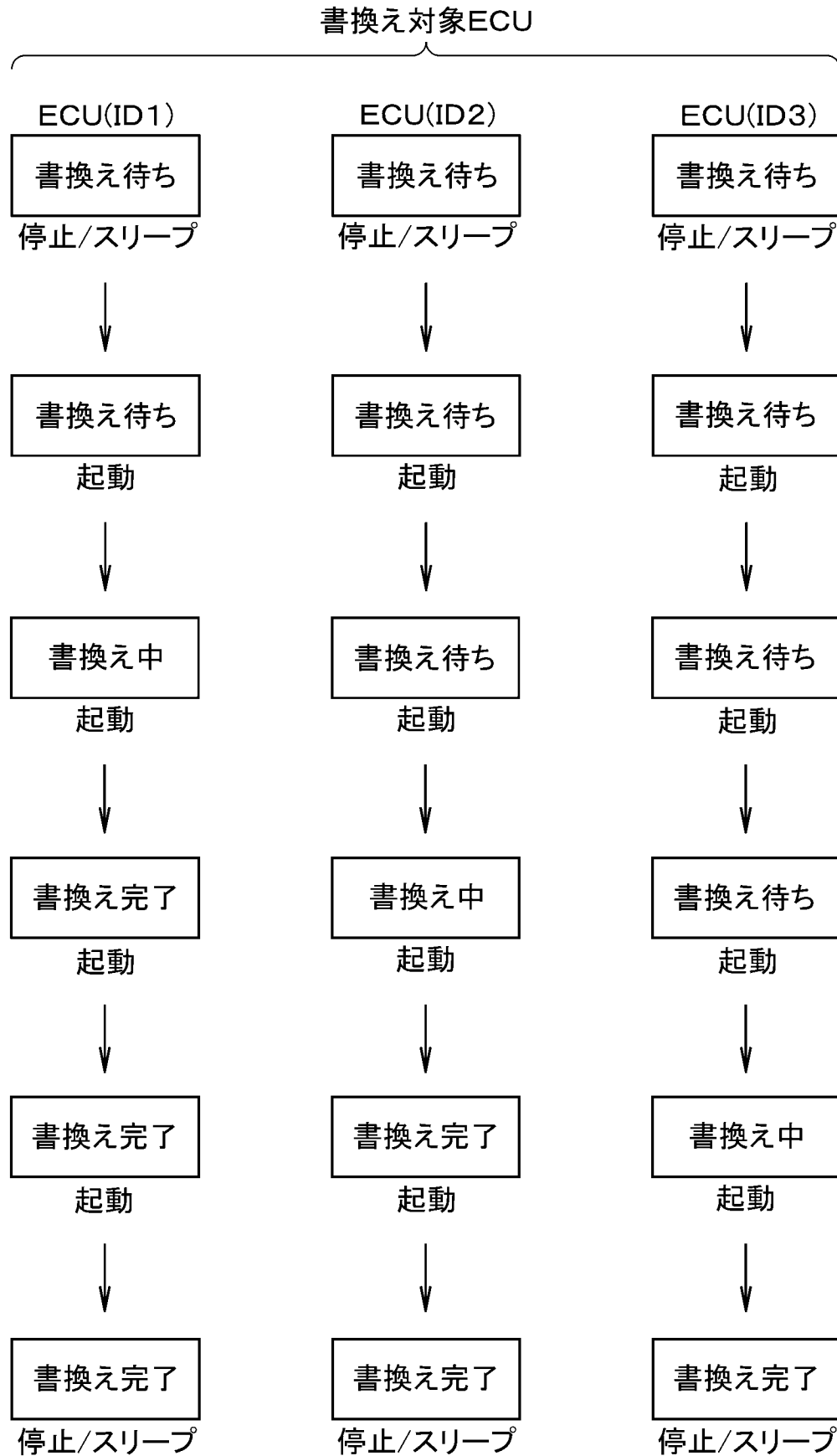
[図84]

Fig. 84



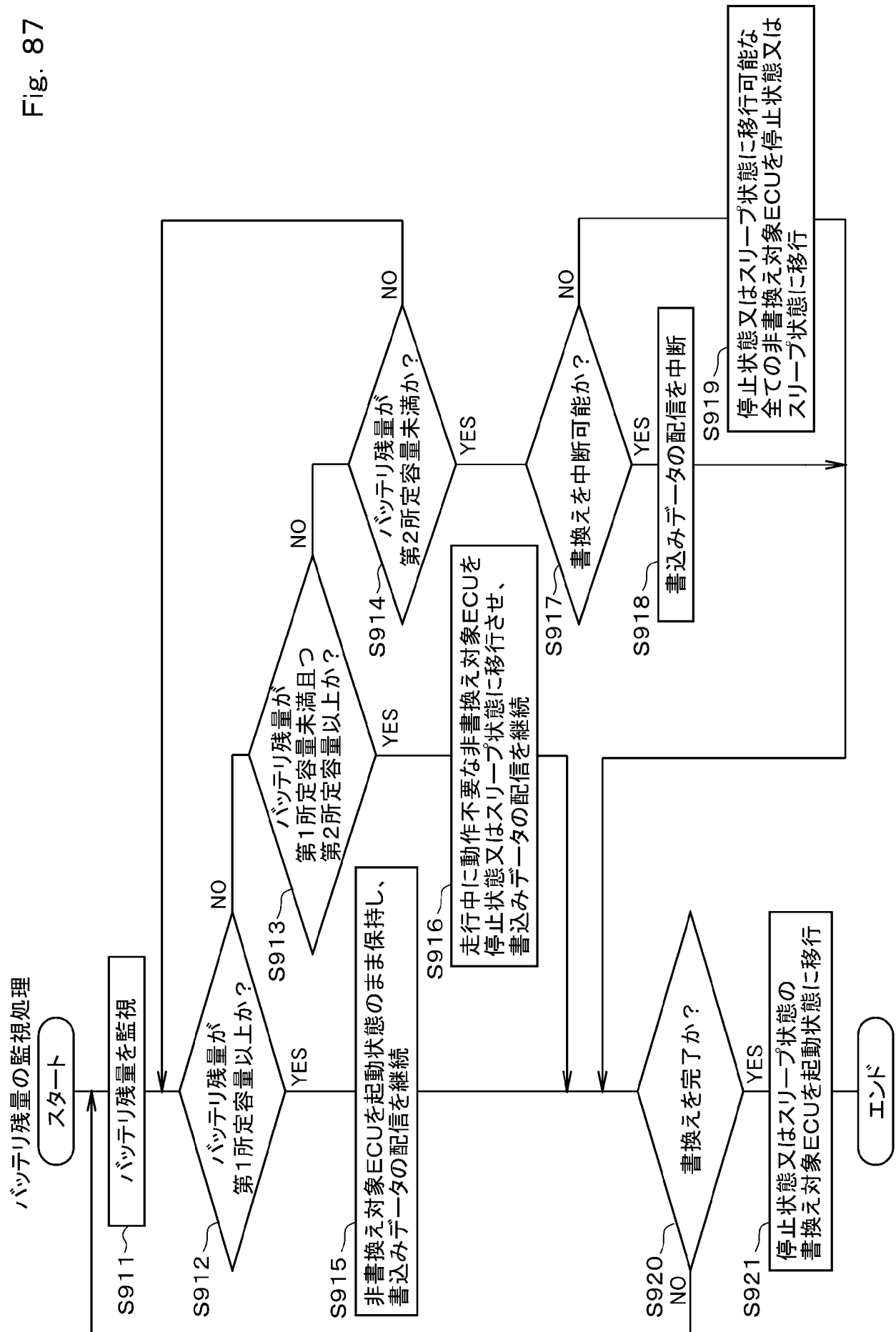
[図85]

Fig. 85



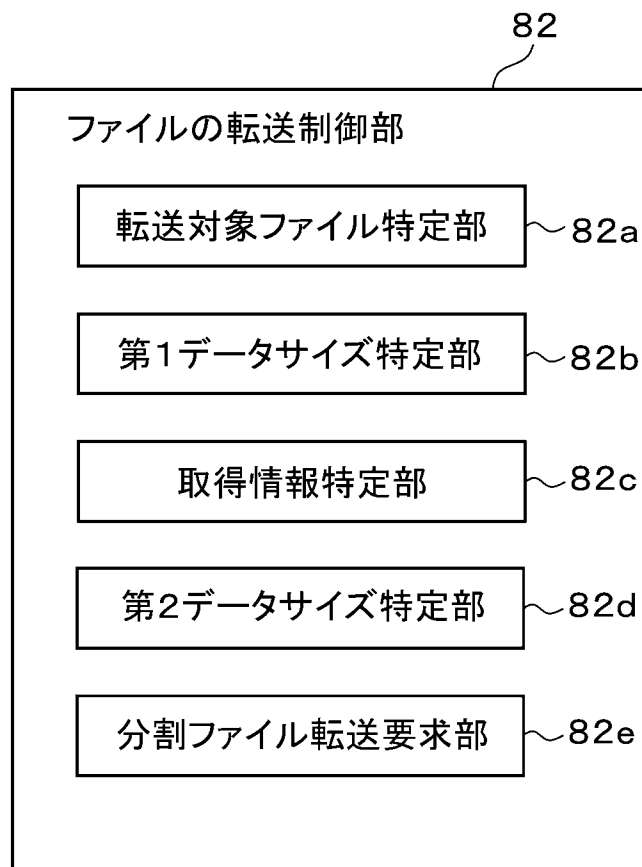
[図87]

Fig. 87



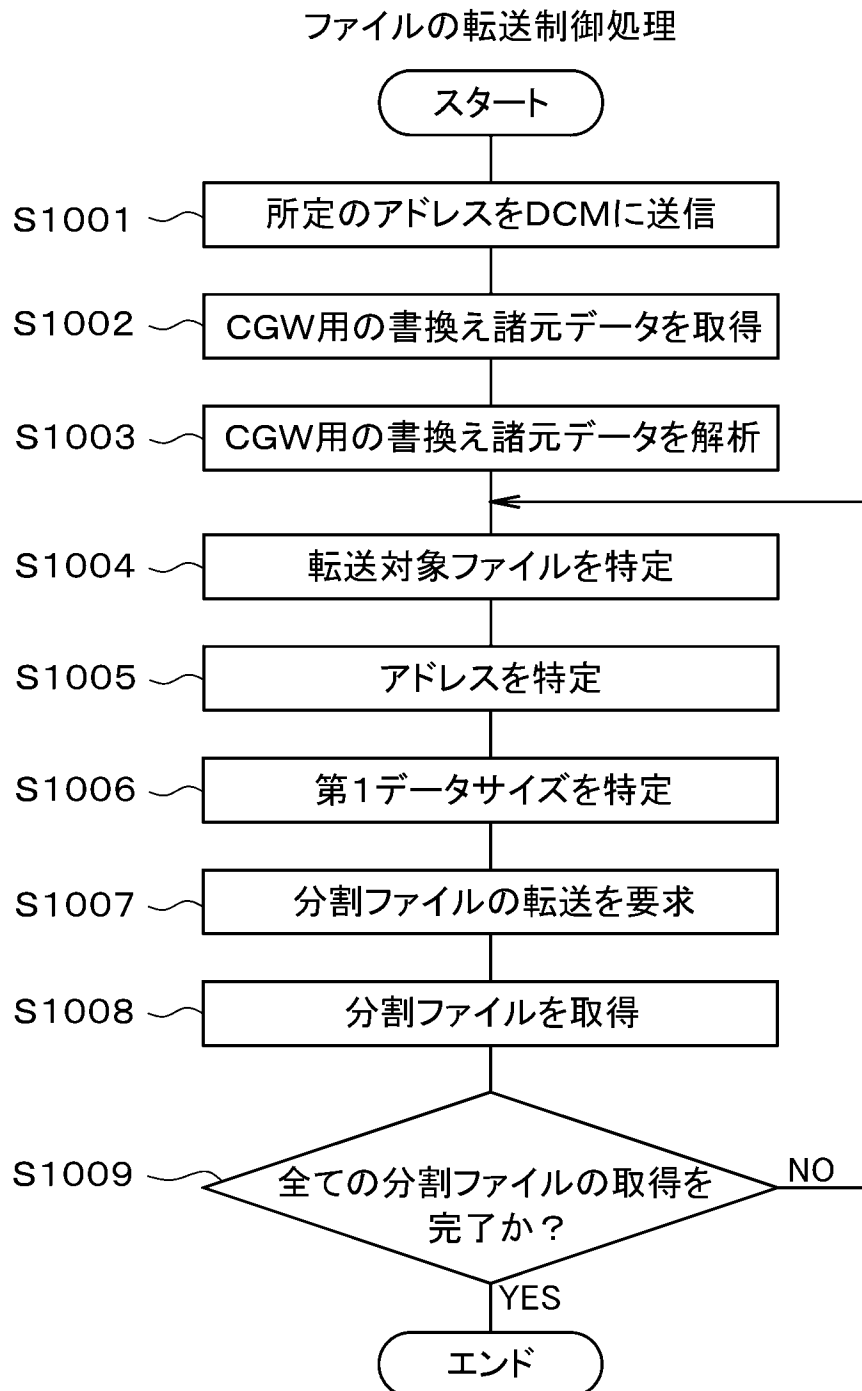
[図88]

Fig. 88



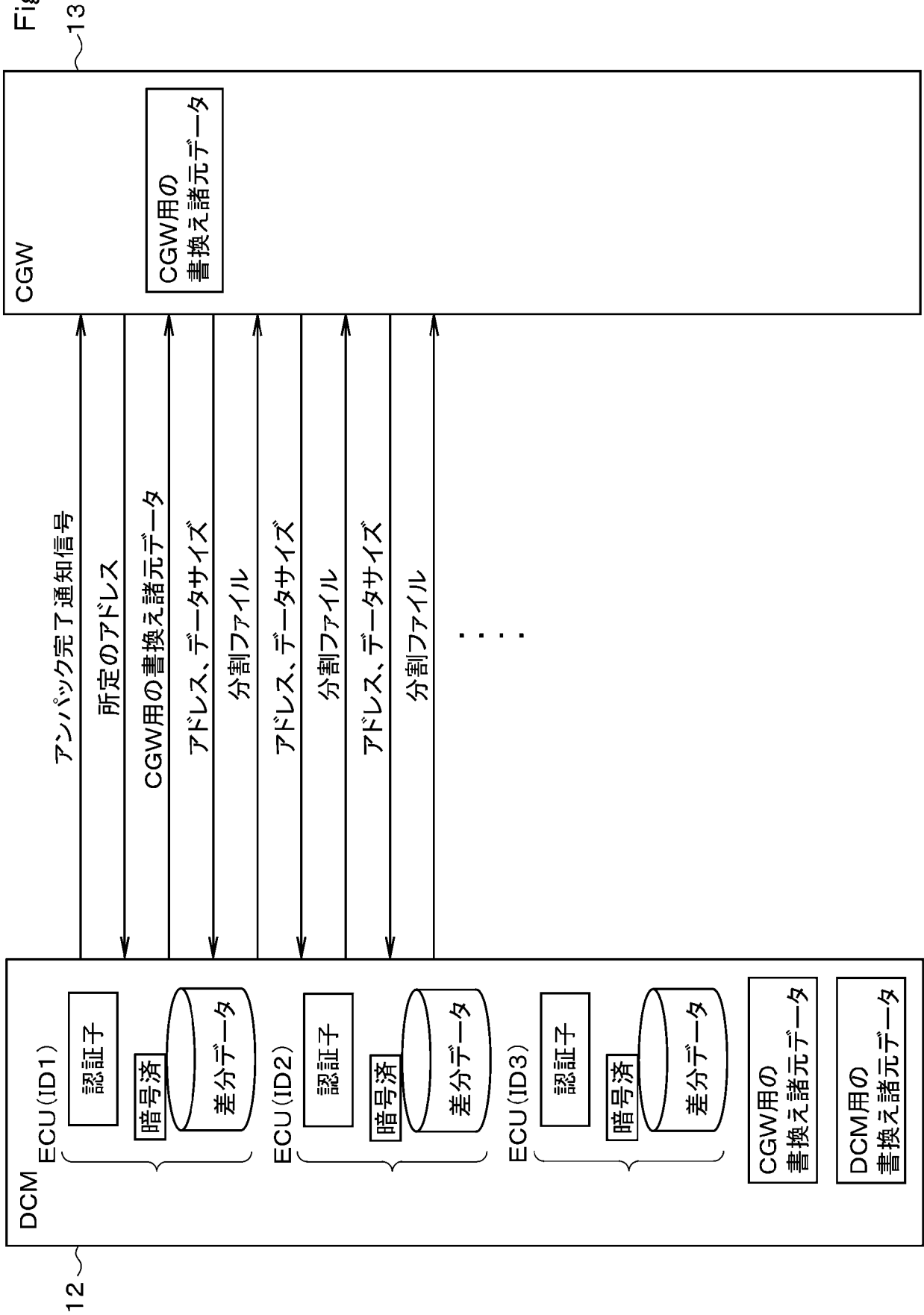
[図89]

Fig. 89



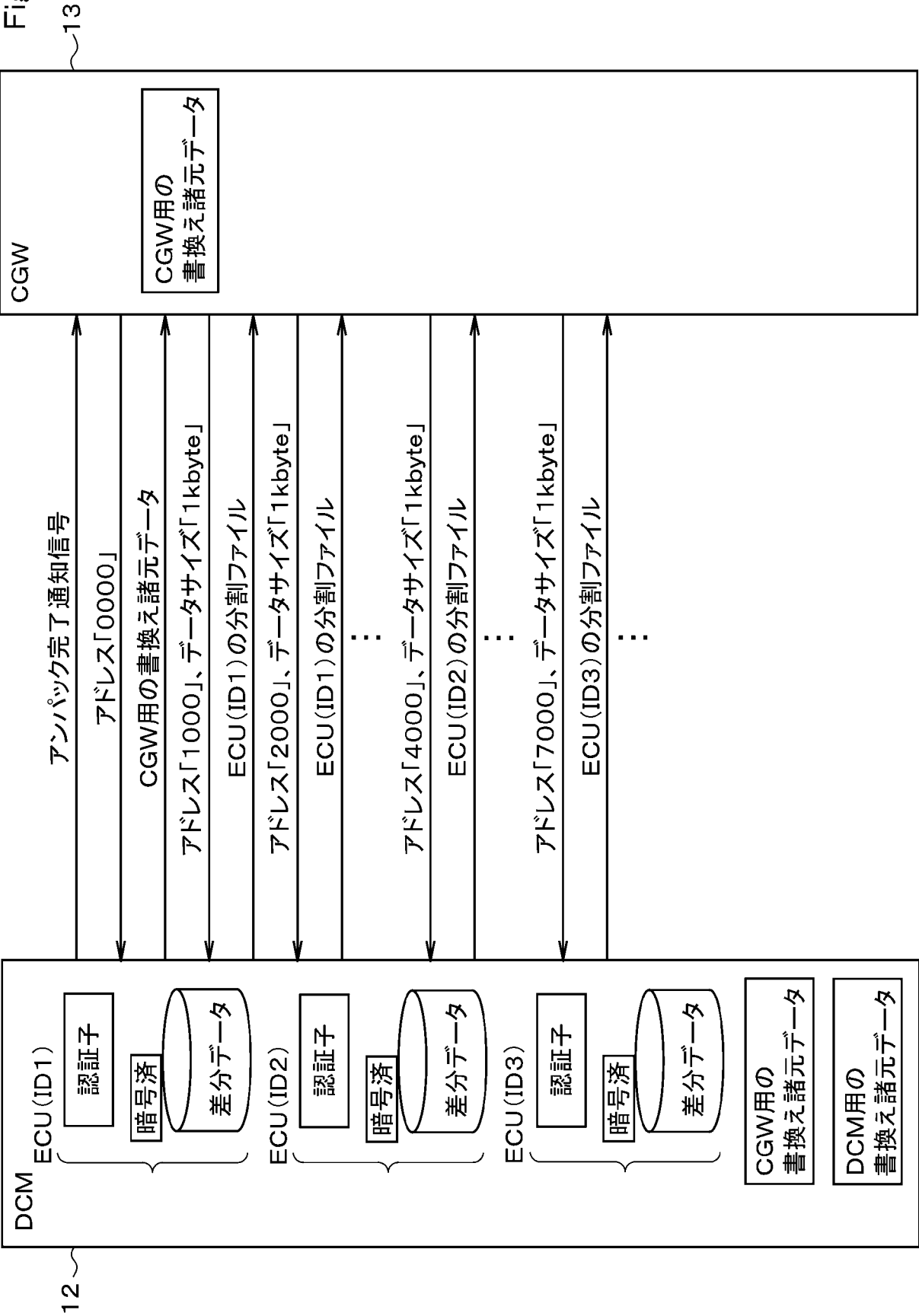
[図90]

Fig. 90



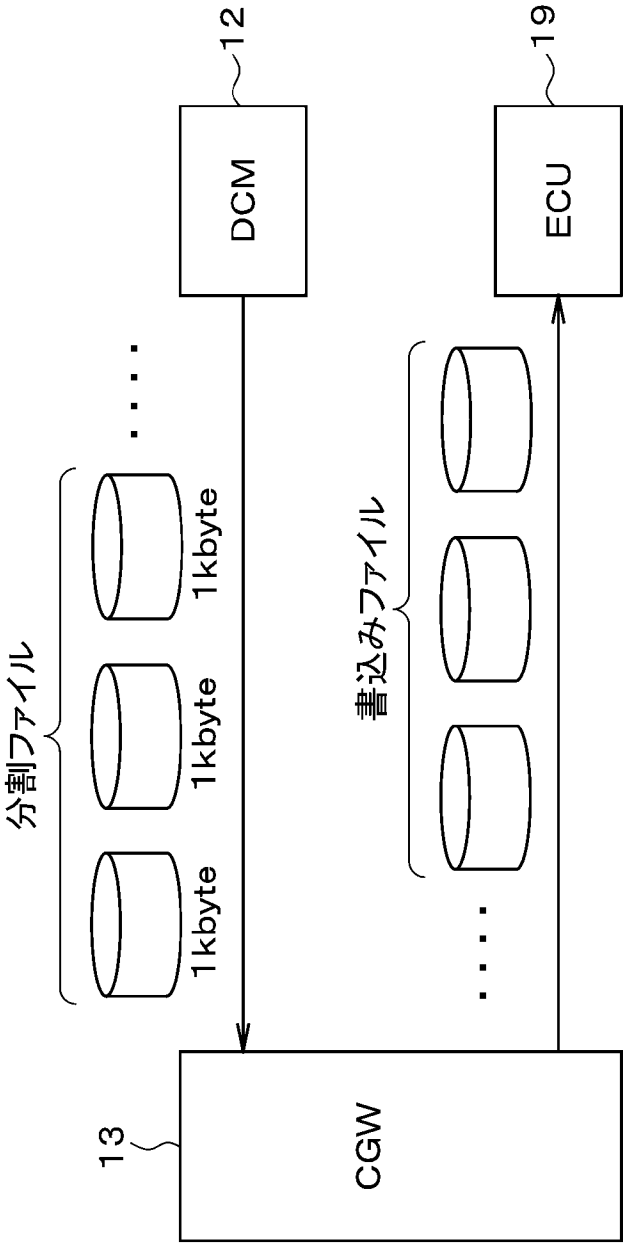
[図91]

Fig. 91



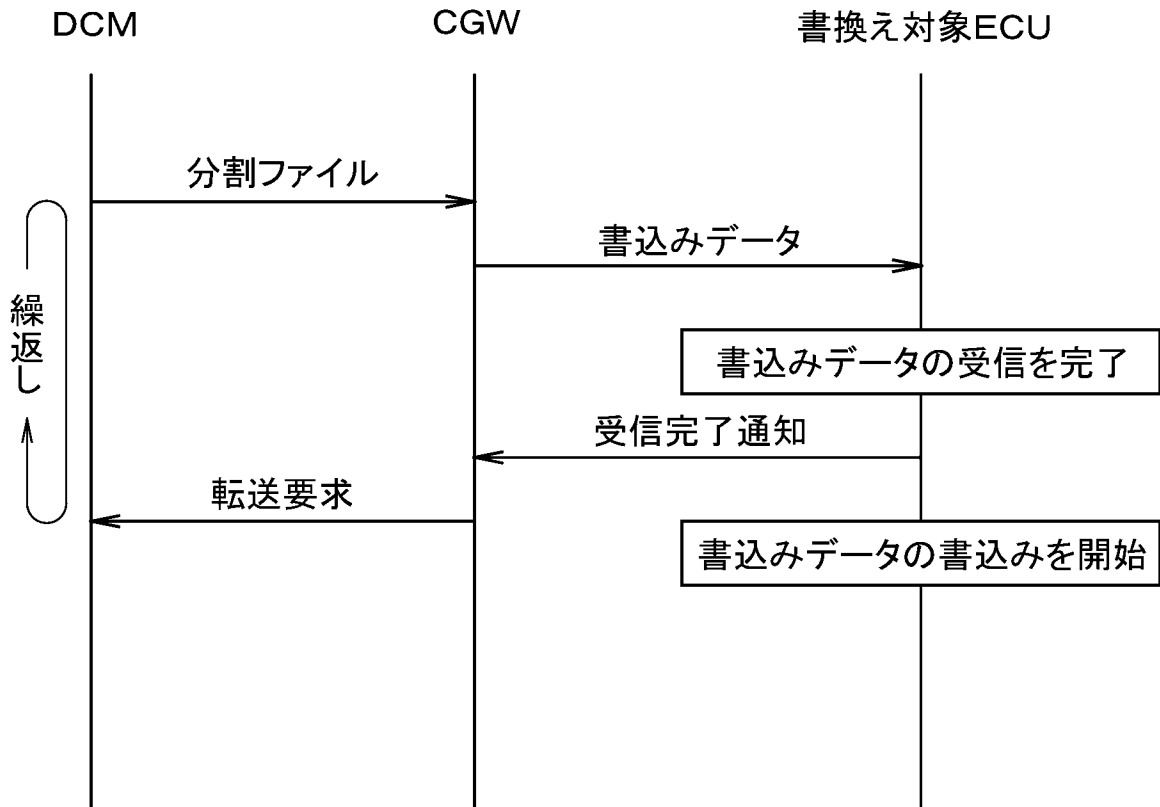
[図92]

Fig. 92



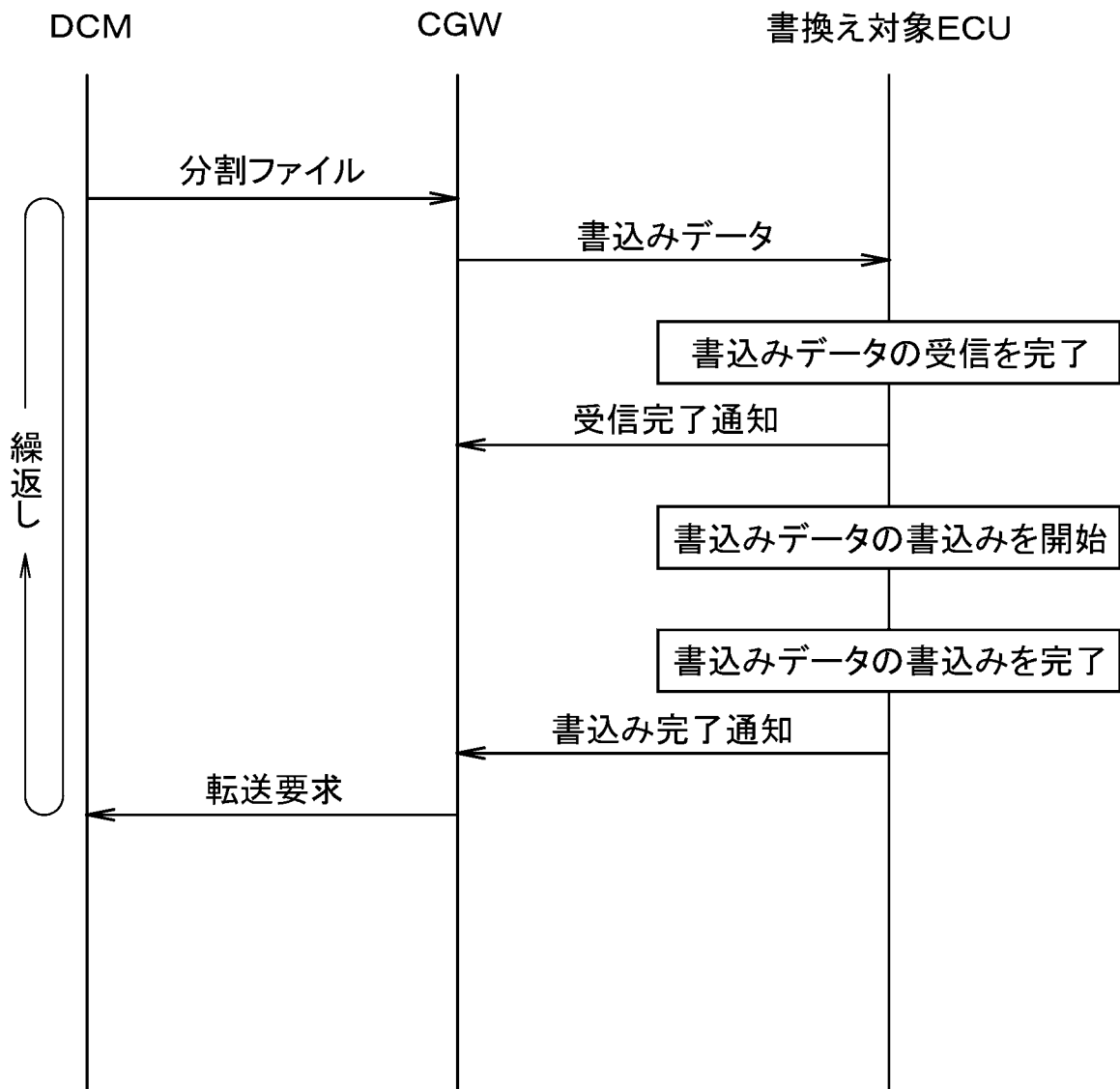
[図93]

Fig. 93



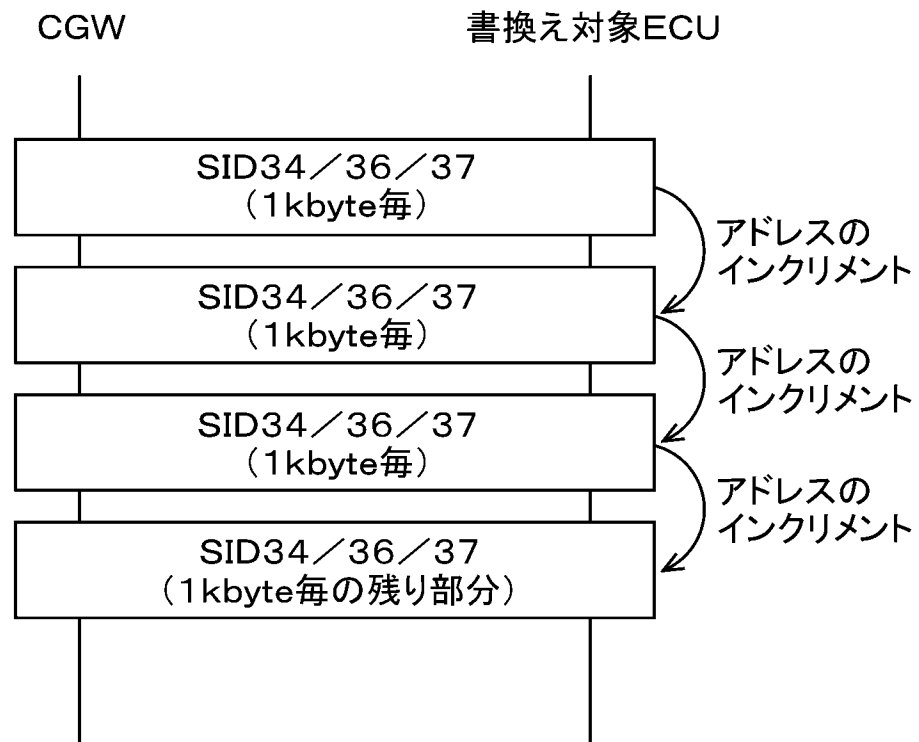
[図94]

Fig. 94



[図95]

Fig. 95



[図96]

Fig. 96

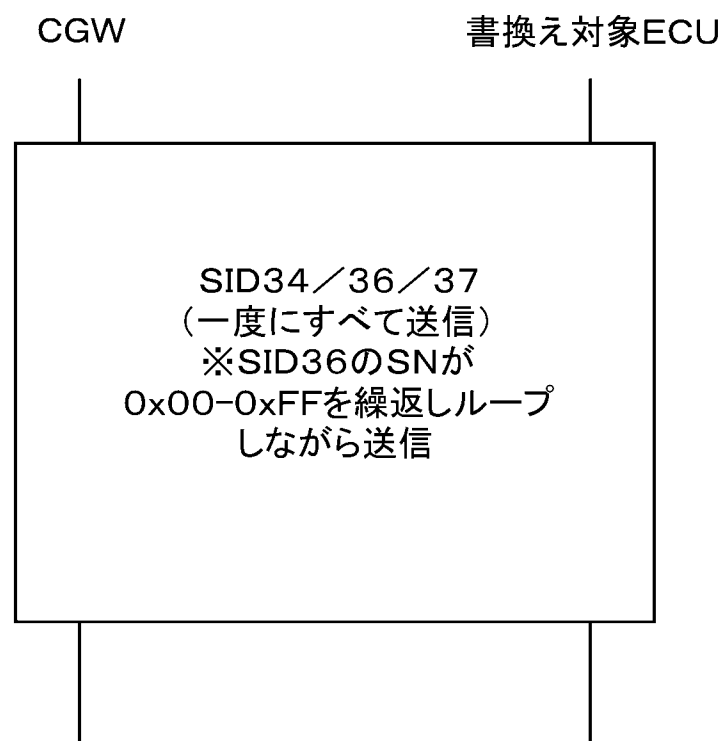
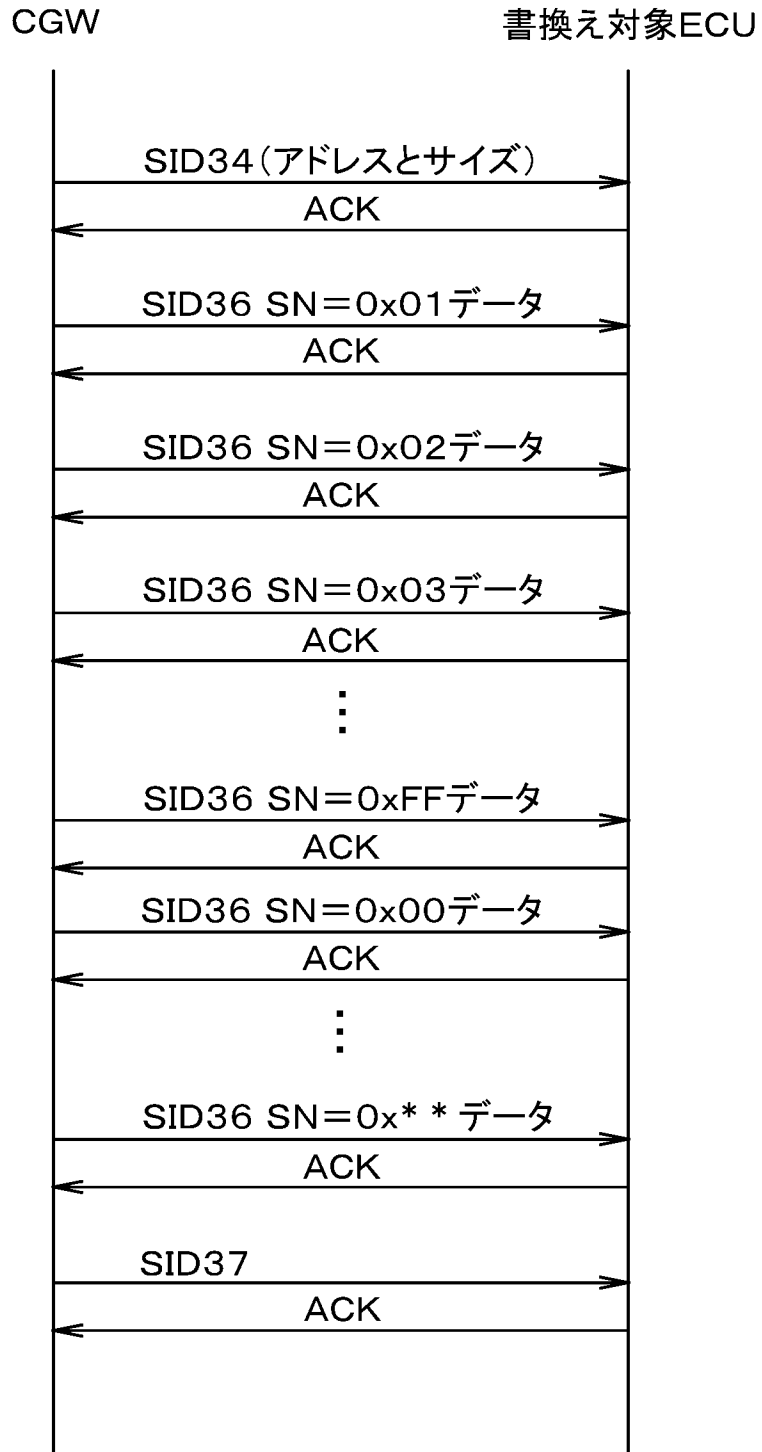
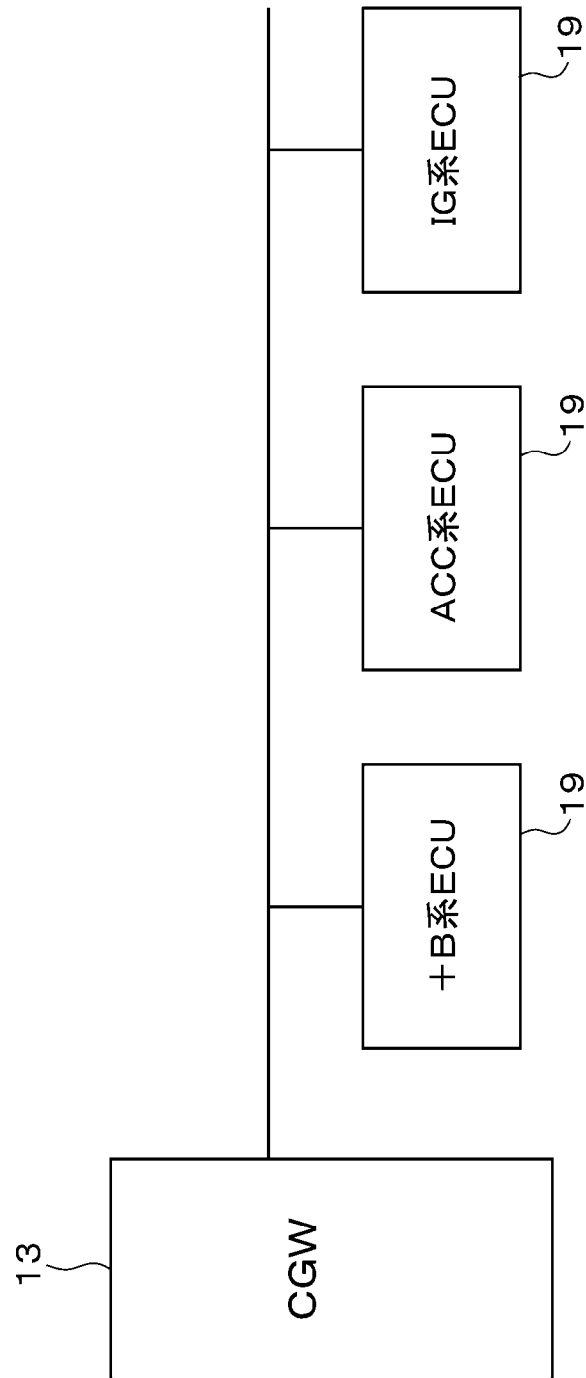


Fig. 97



[図98]

Fig. 98



[図99]

Fig. 99

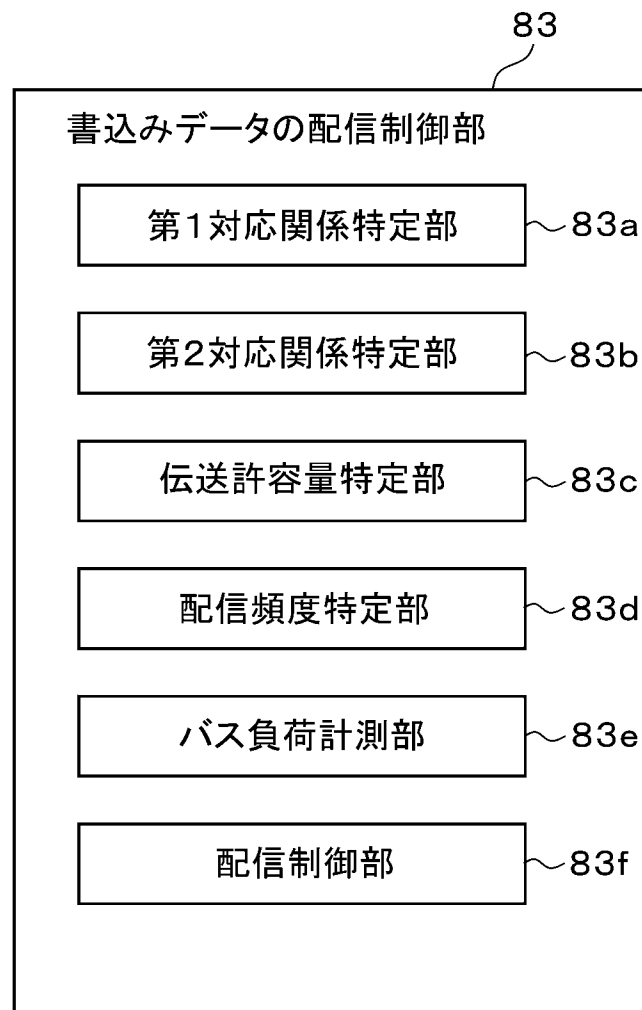


Fig. 100 [図100]

バス負荷テーブル(第1対応関係)			
		第1バス	第2バス
伝送許容量		80%	70%
IG 電源状態	車両制御データ	50%	20%
	書込みデータ	30%	50%
ACC 電源状態	車両制御データ	30%	30%
	書込みデータ	50%	40%
+B 電源状態	車両制御データ	20%	10%
	書込みデータ	60%	60%
		第3バス	90%
		40%	50%
		20%	70%
		50%	40%

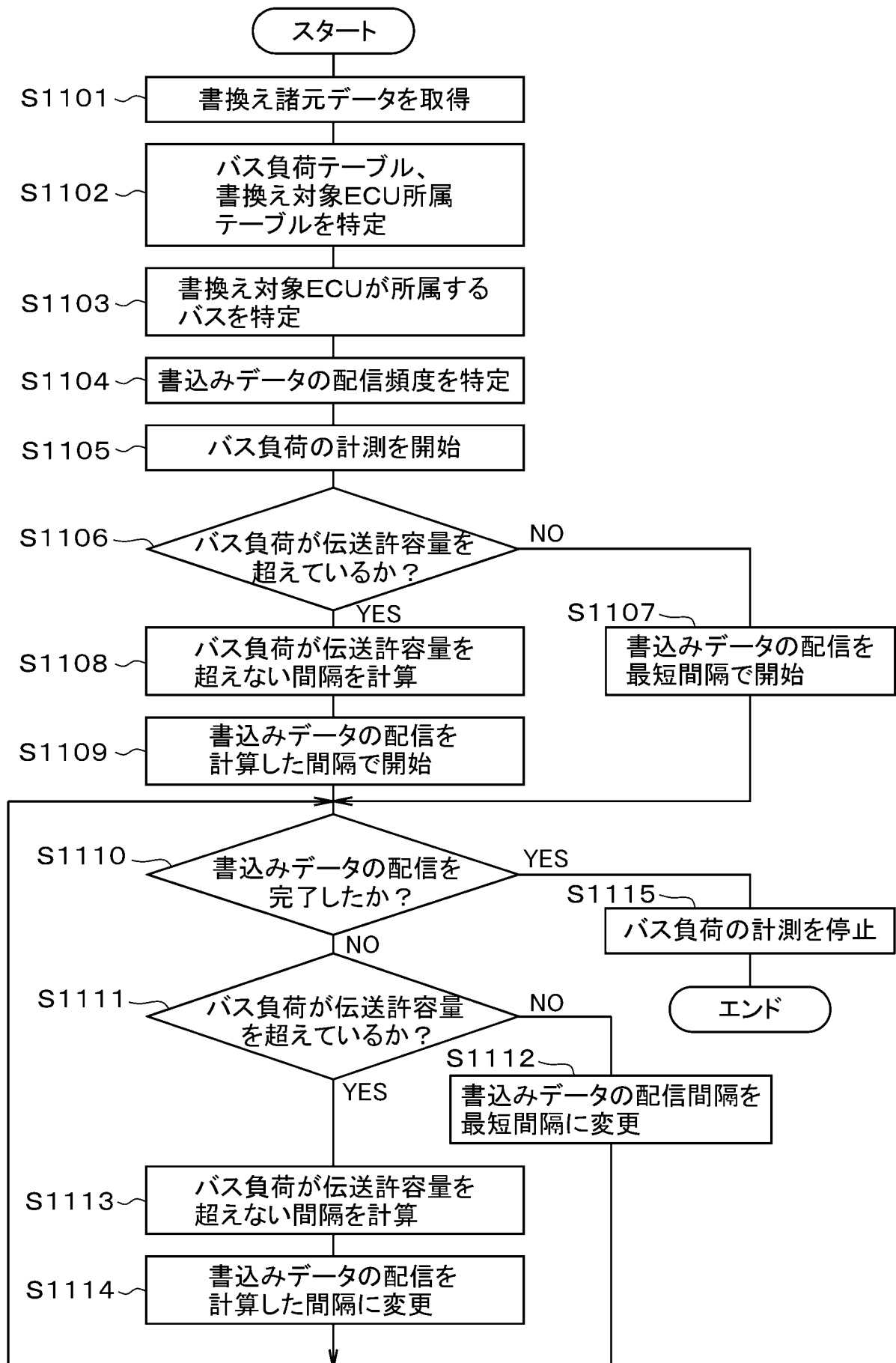
[図101]

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	

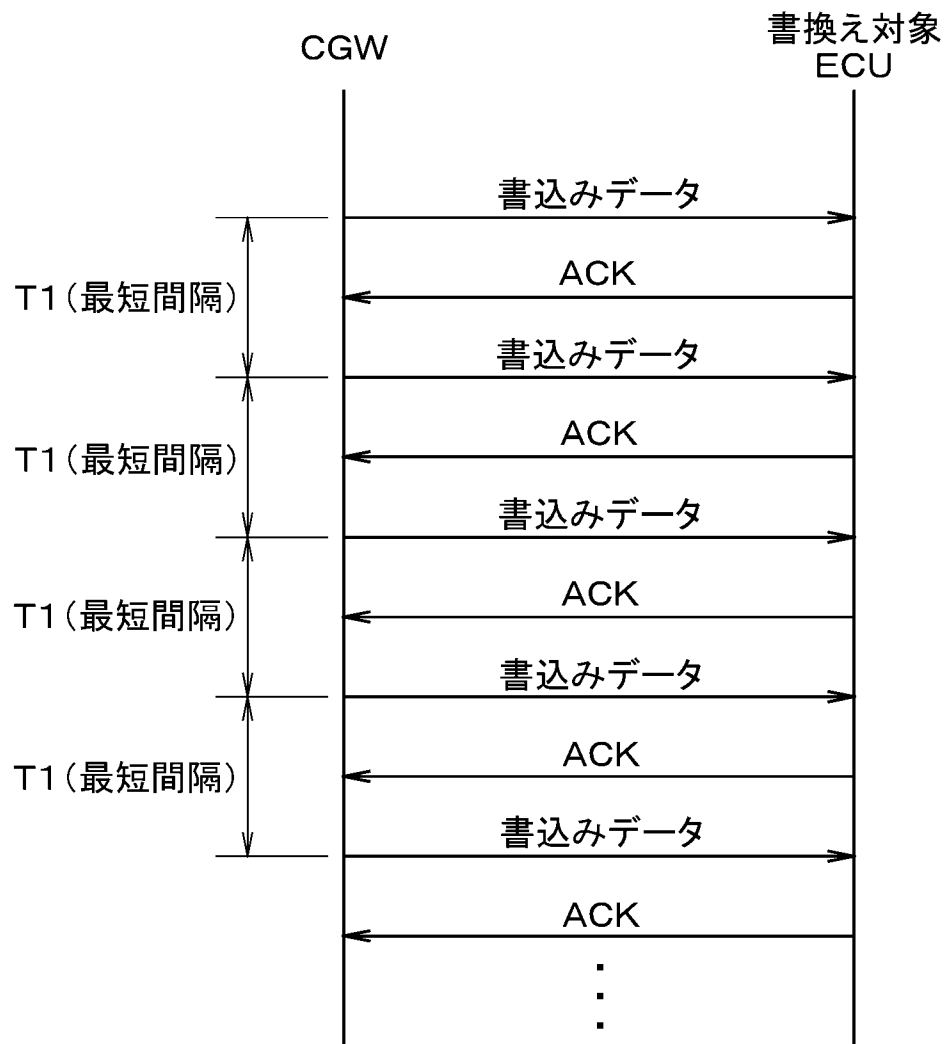
[図102]

Fig. 102 書込みデータの配信制御処理



[図103]

Fig. 103



[図104]

Fig. 104

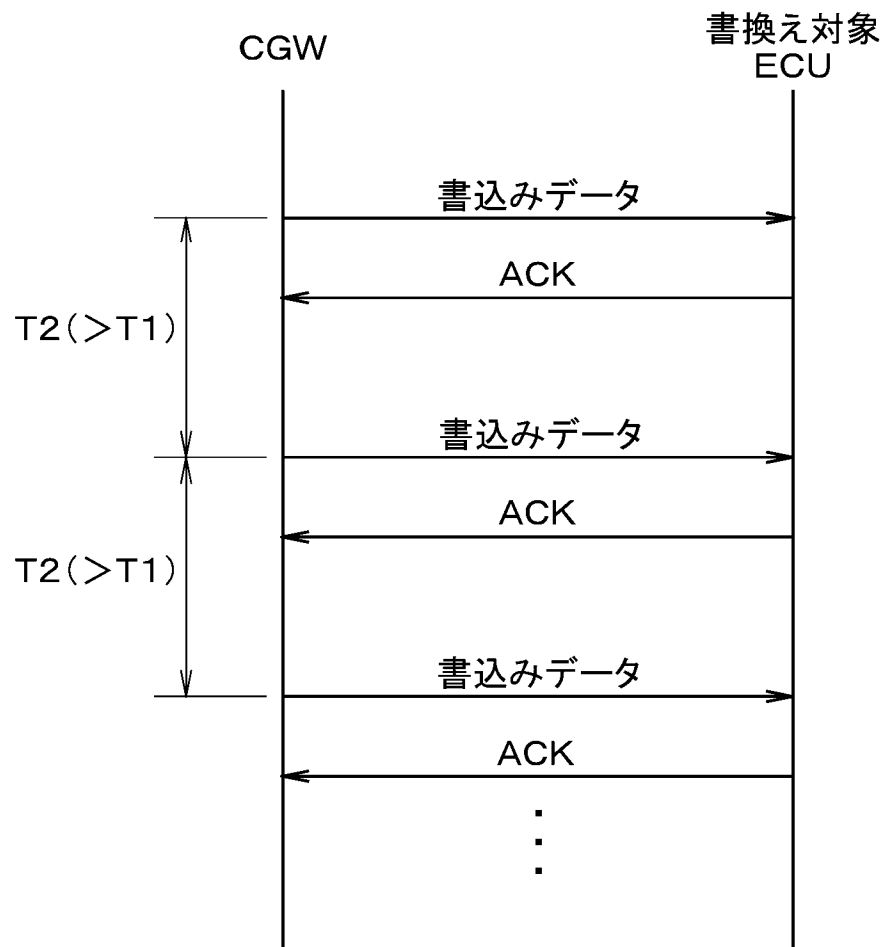
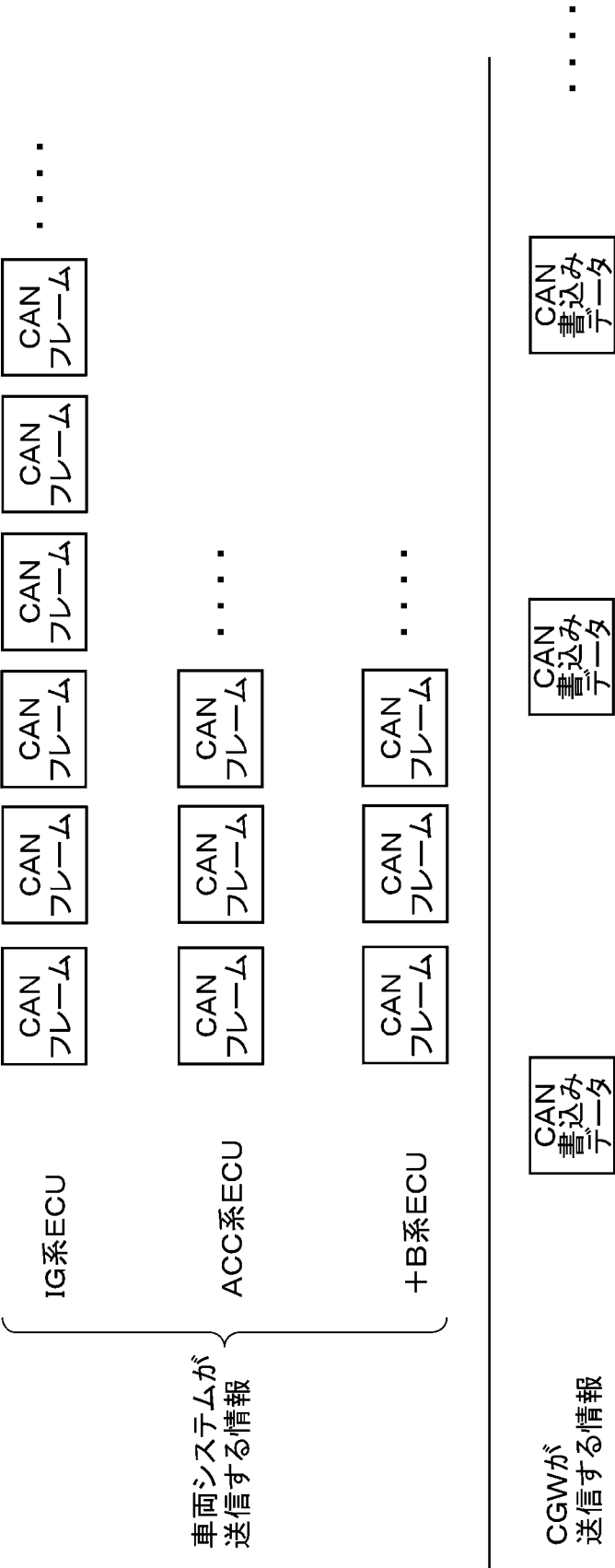
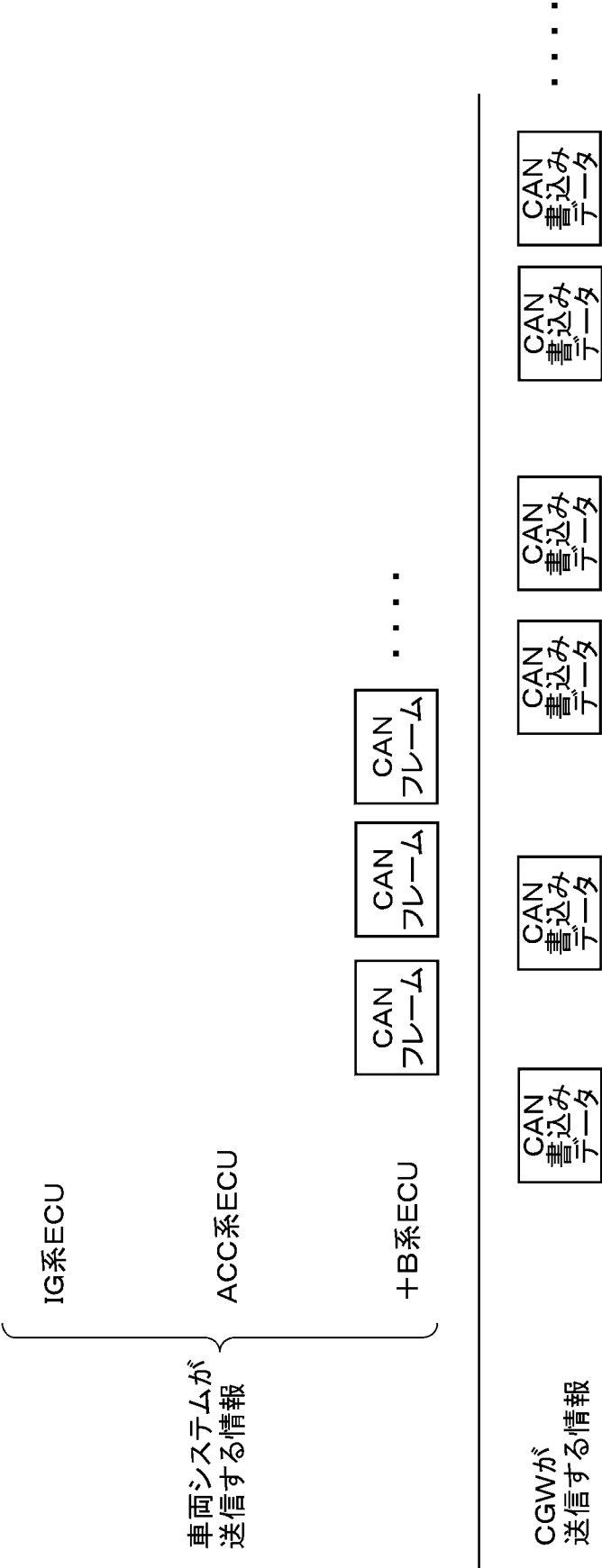


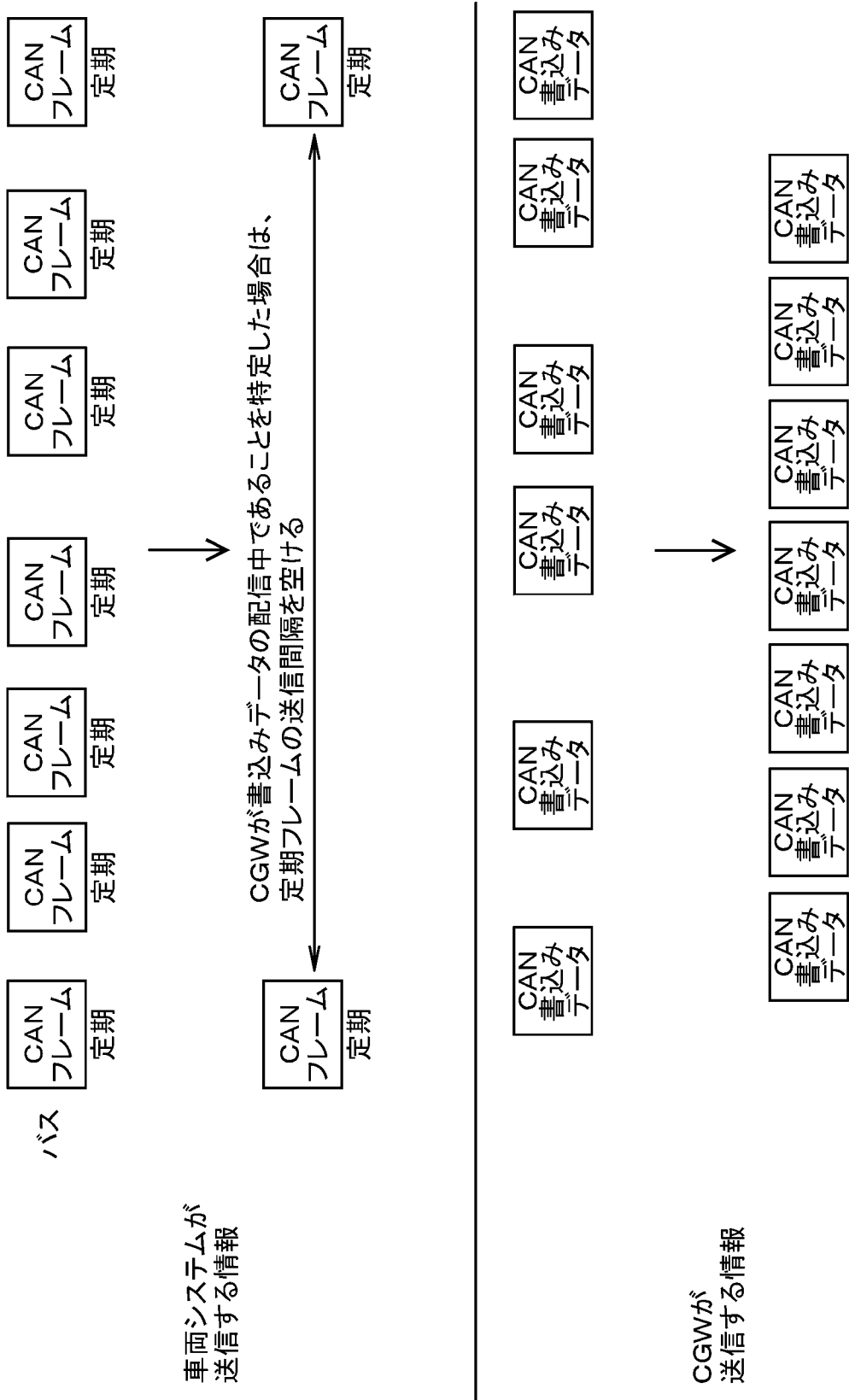
Fig. 105



[図106]
Fig. 106

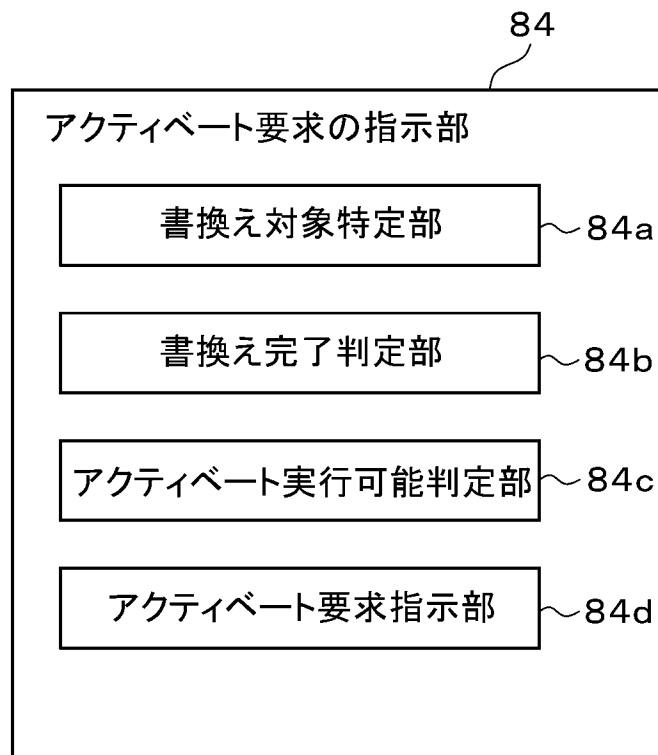


[図108]
Fig. 108



[図109]

Fig. 109



[図110]

Fig. 110

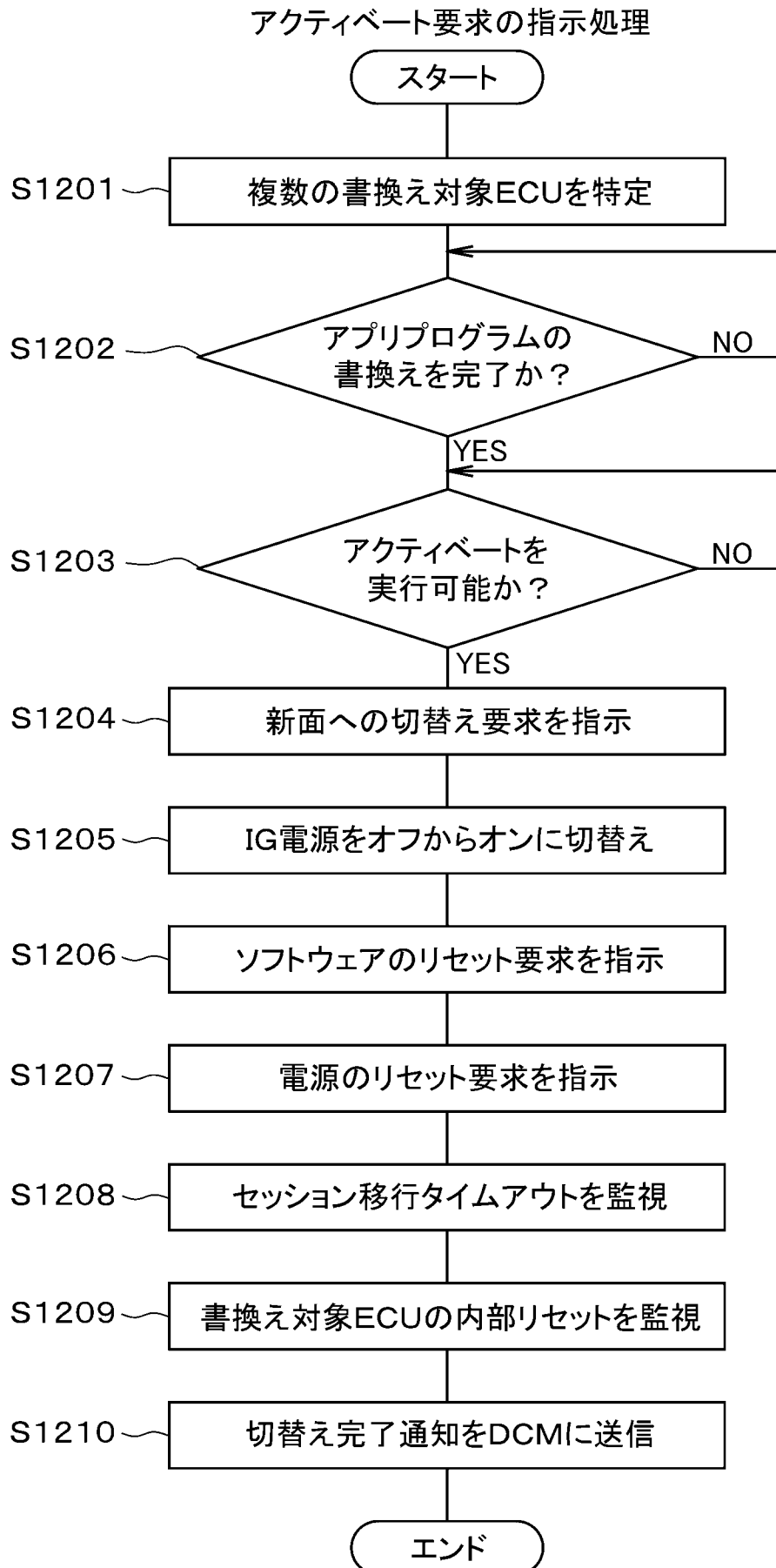
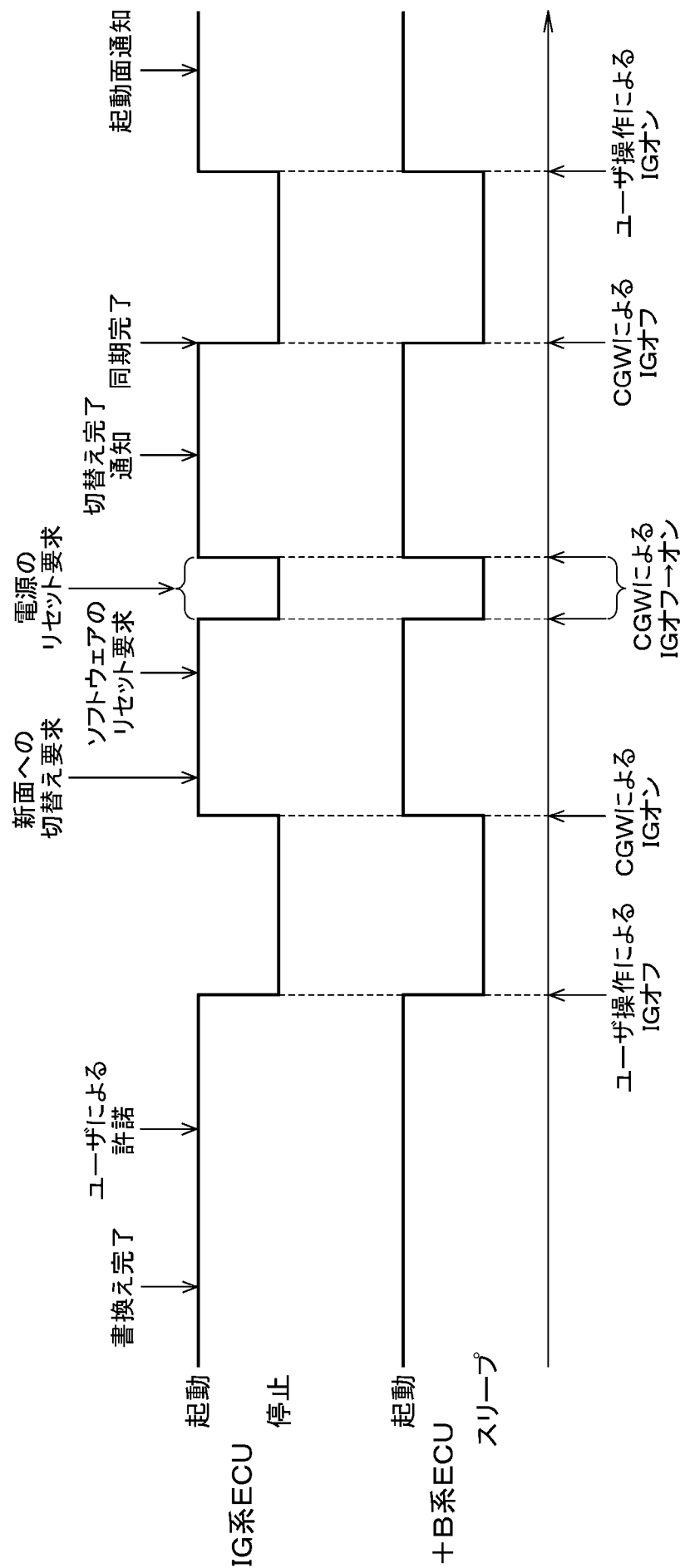
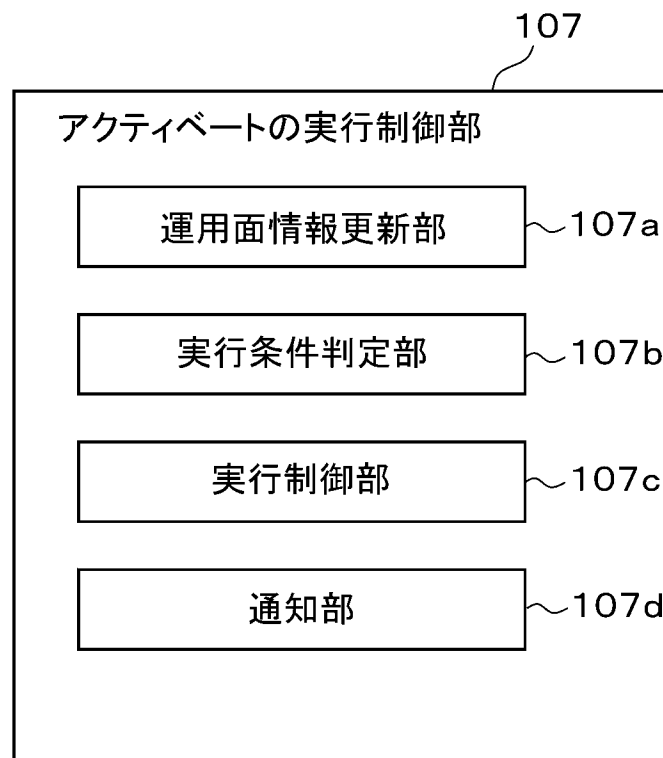


Fig. 111 [図111]



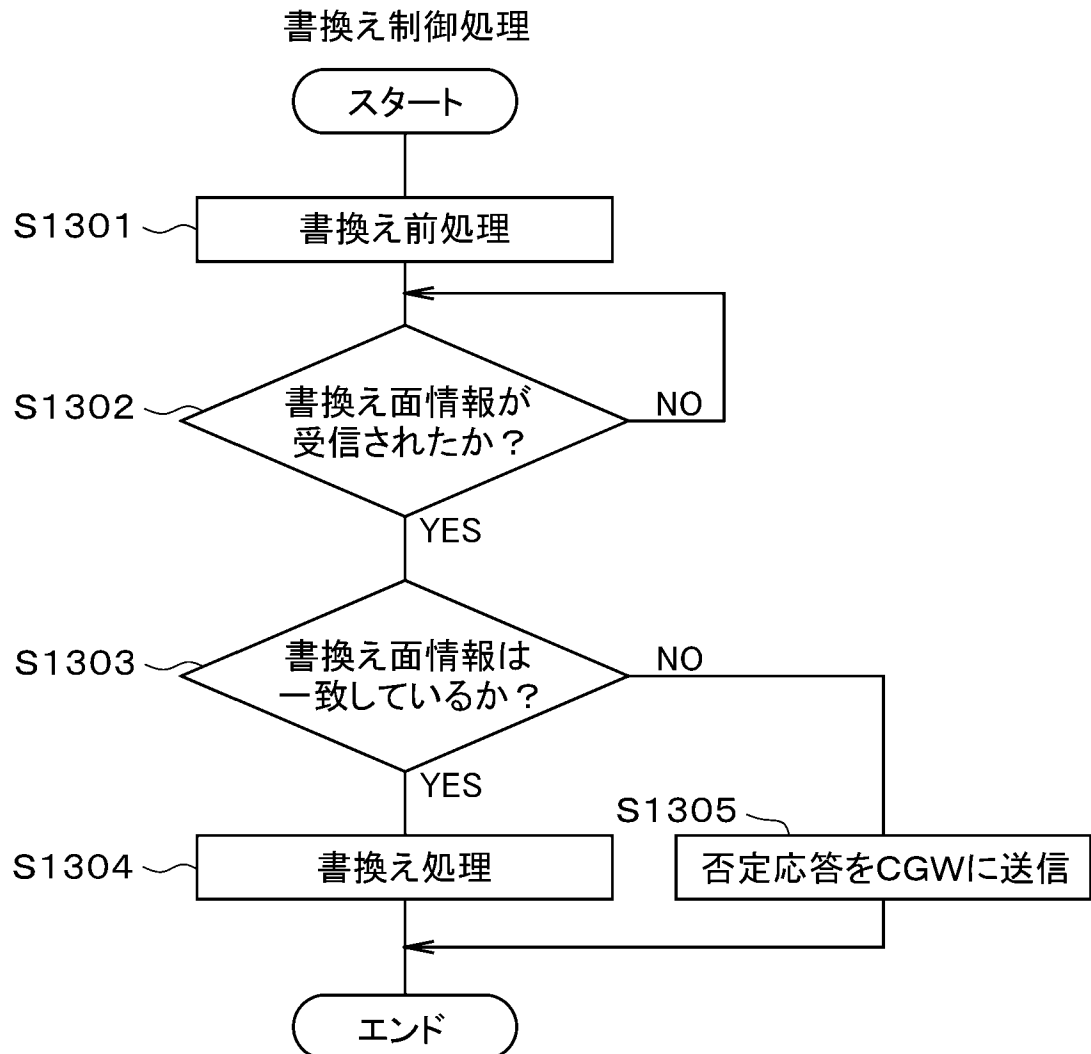
[図112]

Fig. 112



[図113]

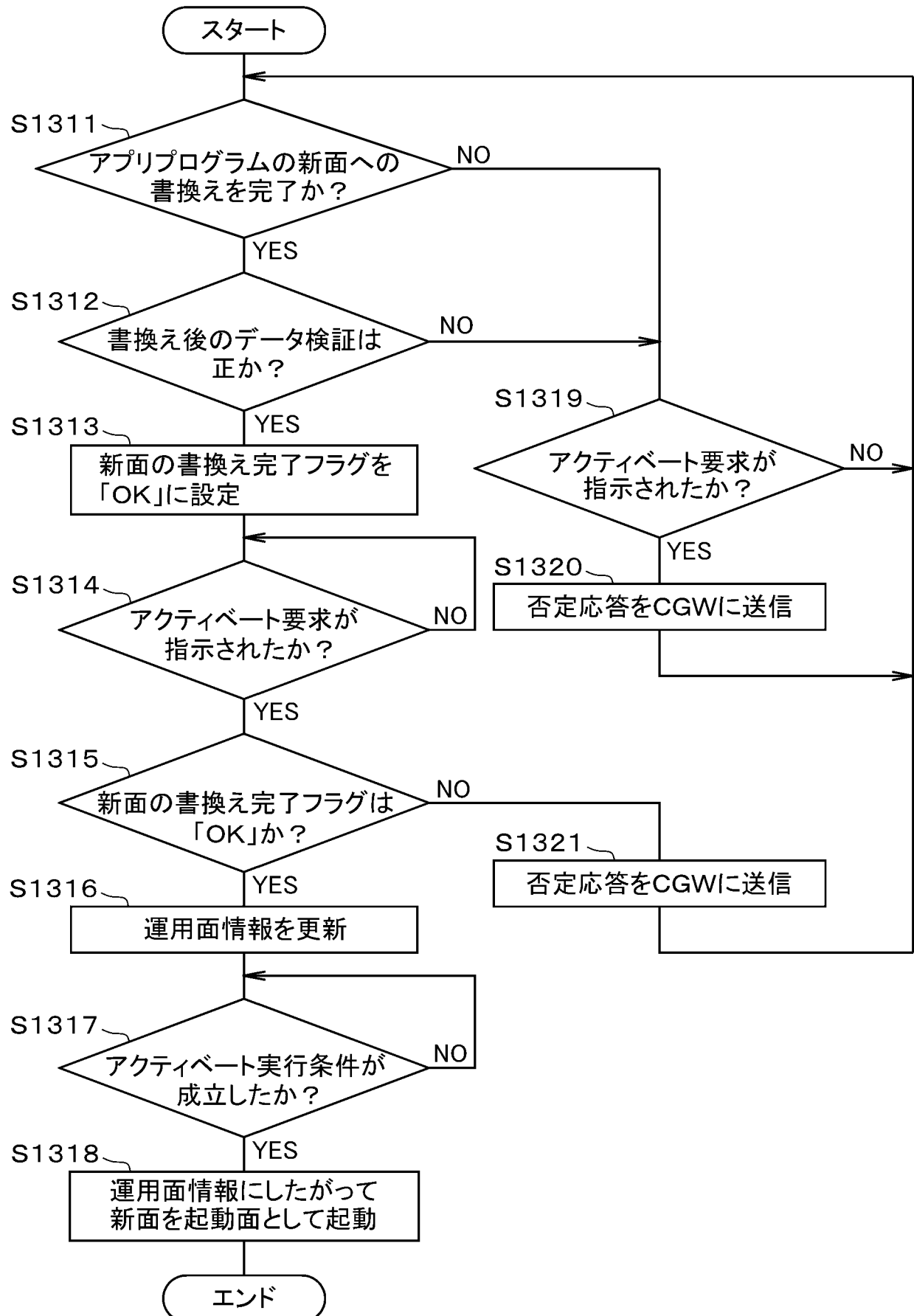
Fig. 113



[図114]

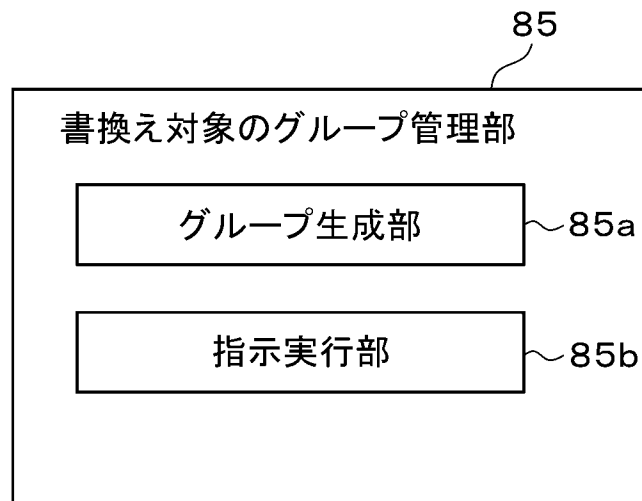
Fig. 114

アクティベートの実行制御処理



[図115]

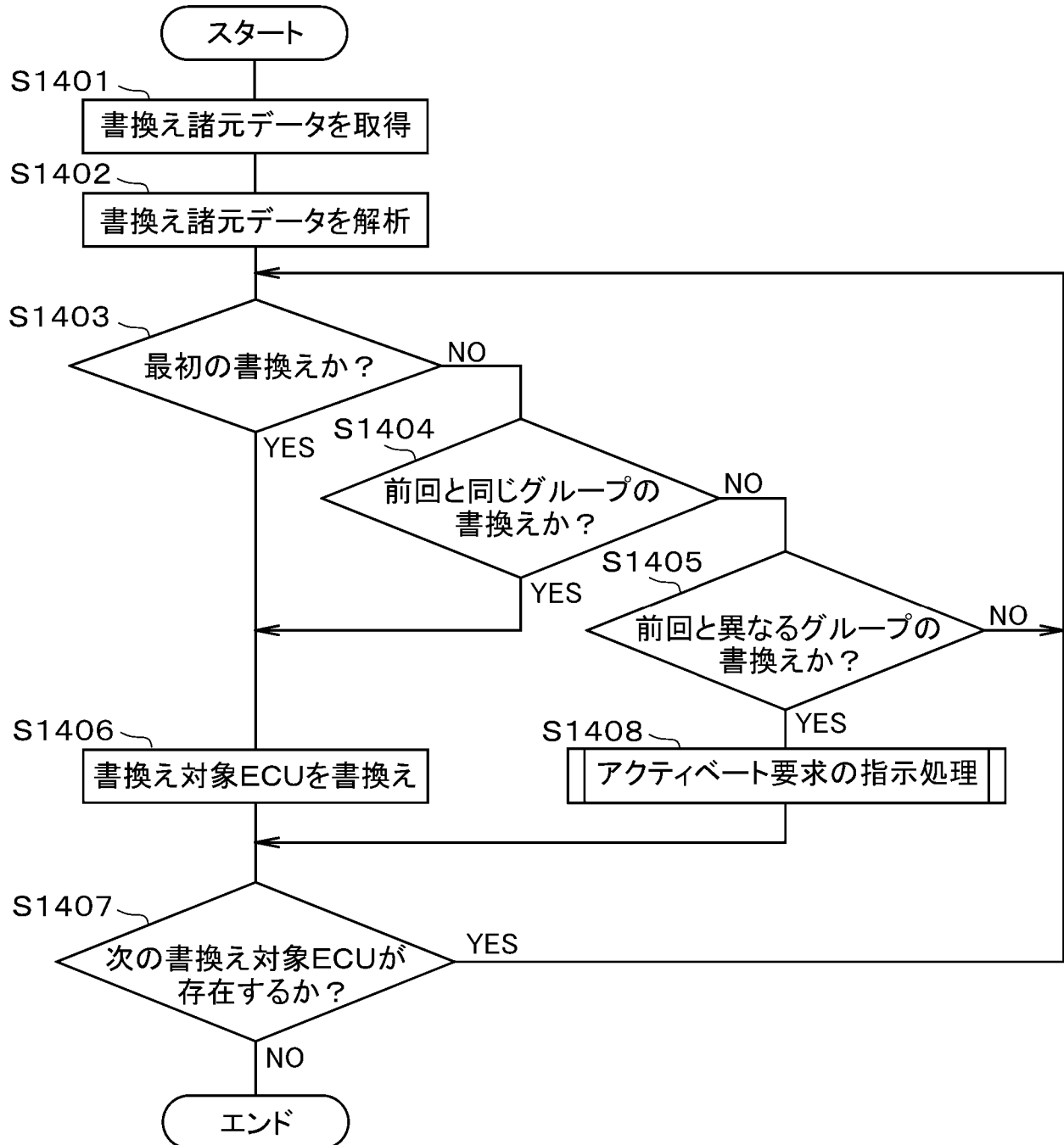
Fig. 115



[図116]

Fig. 116

書換え対象のグループ管理処理



[図117]

Fig. 117

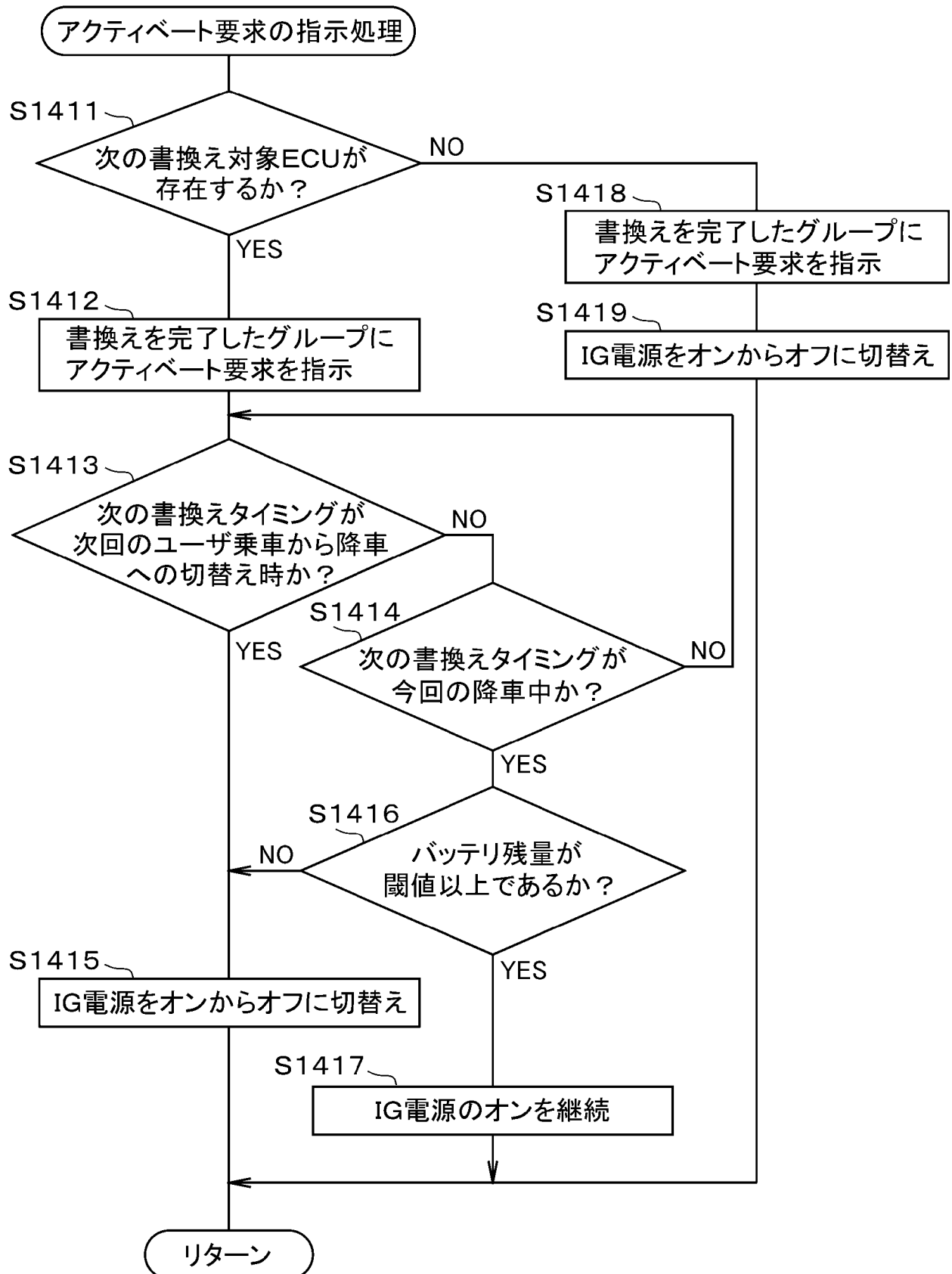
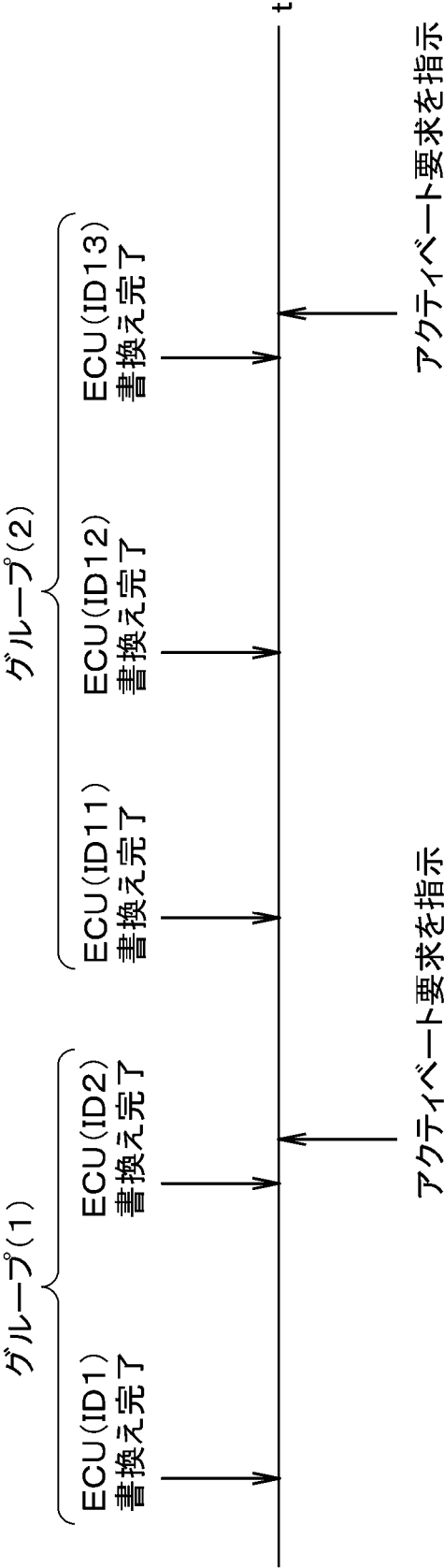
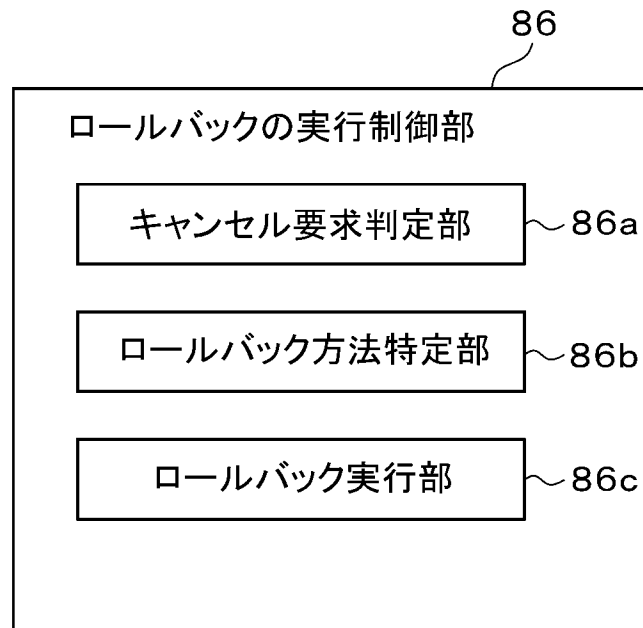


Fig. 118 [図118]



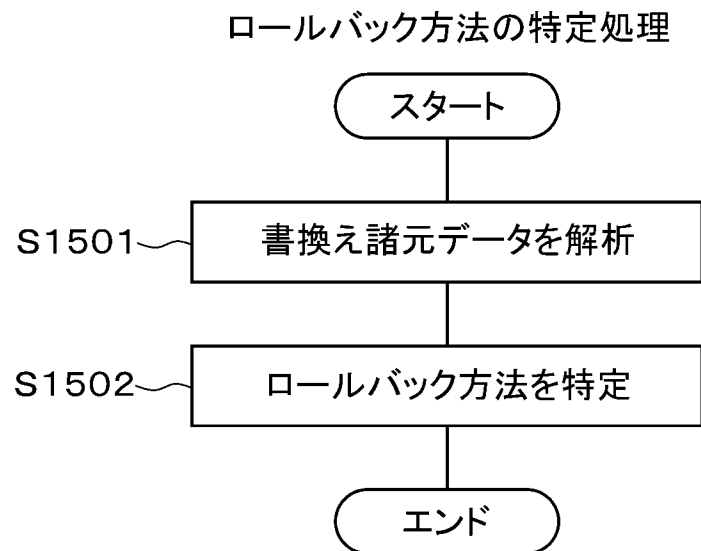
[図119]

Fig. 119



[図120]

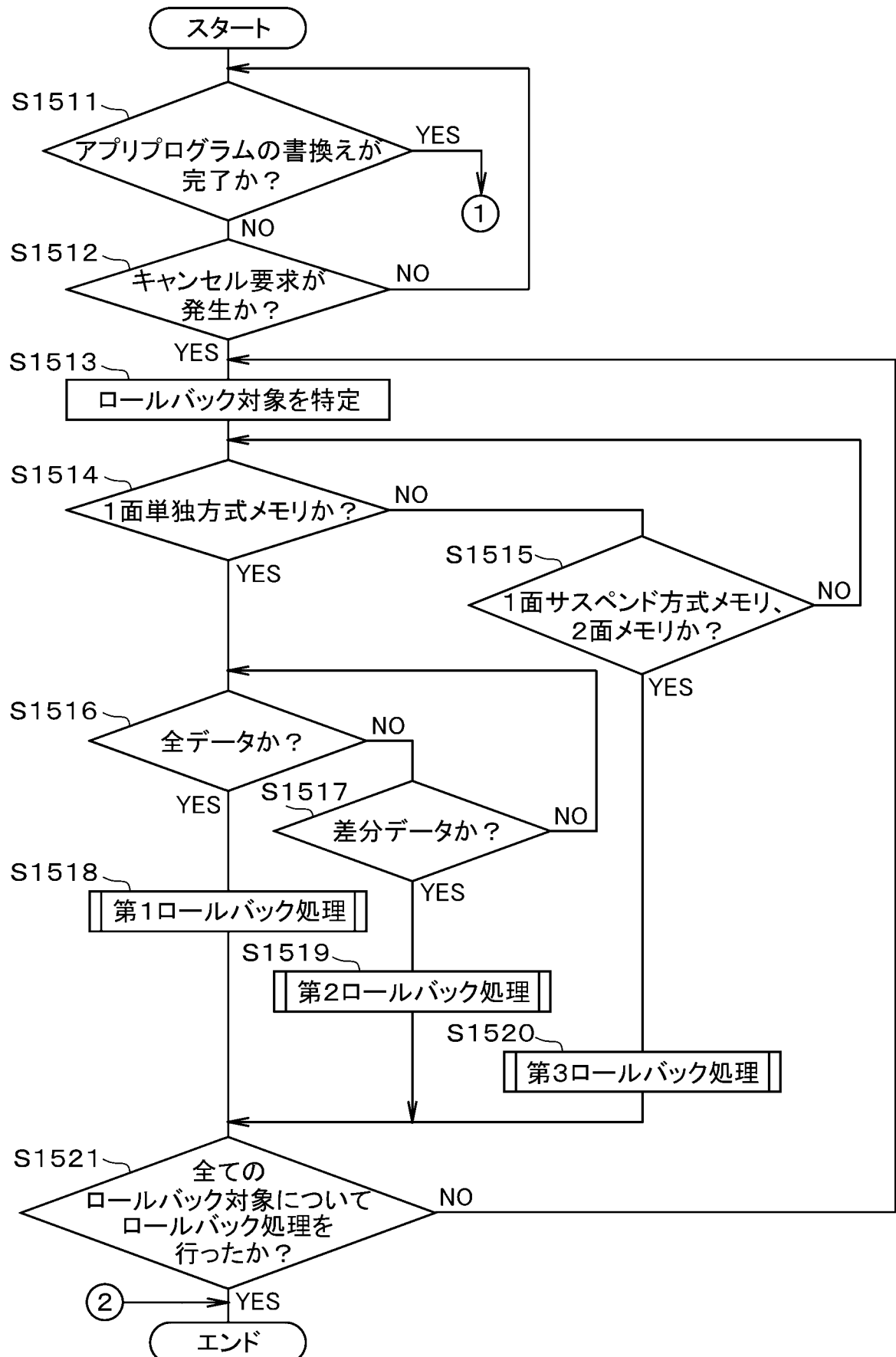
Fig. 120



[図121]

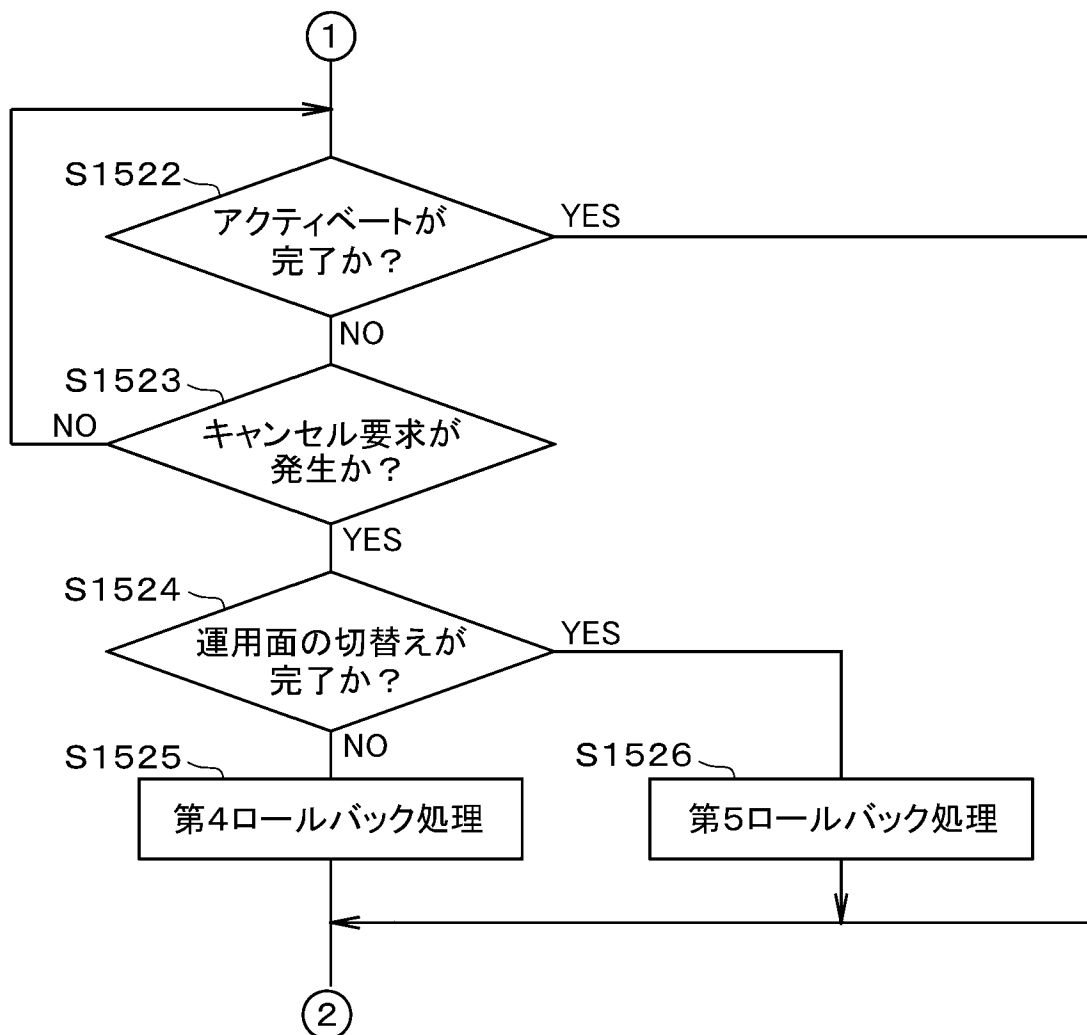
Fig. 121

キャンセル要求の判定処理



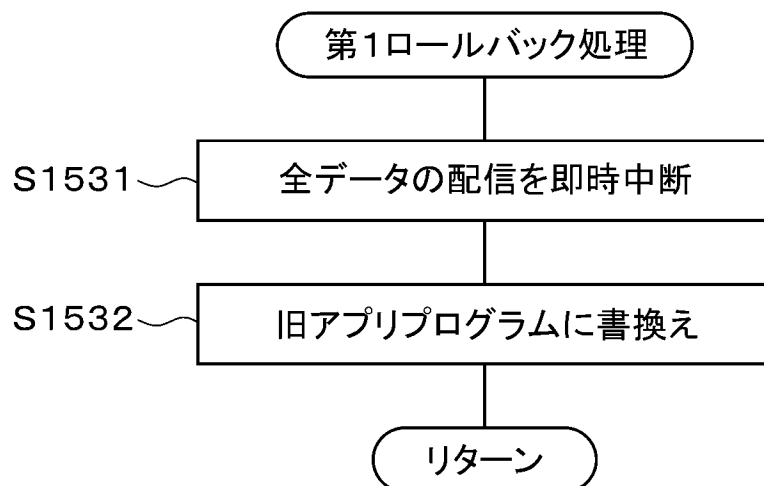
[図122]

Fig. 122



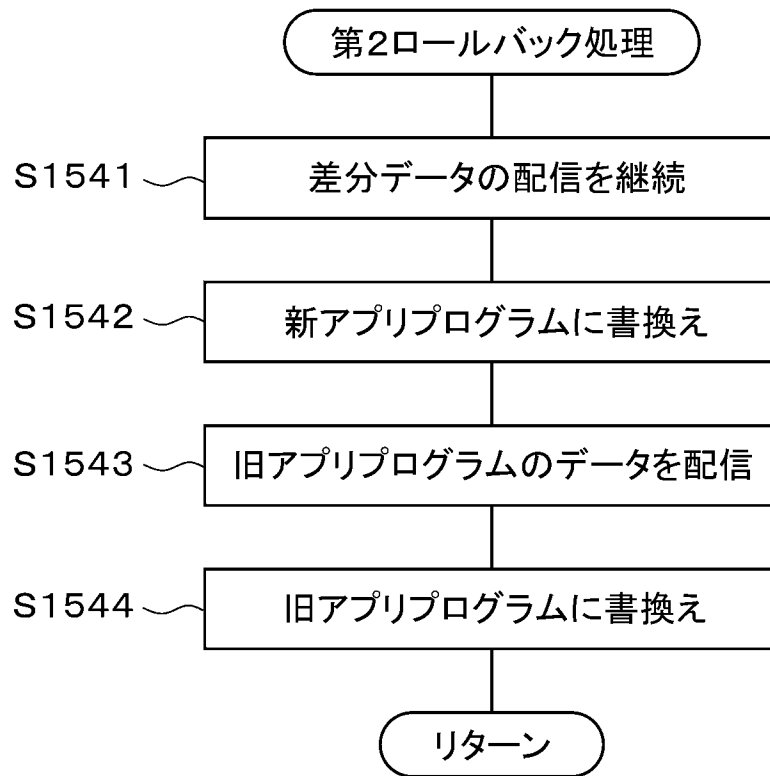
[図123]

Fig. 123



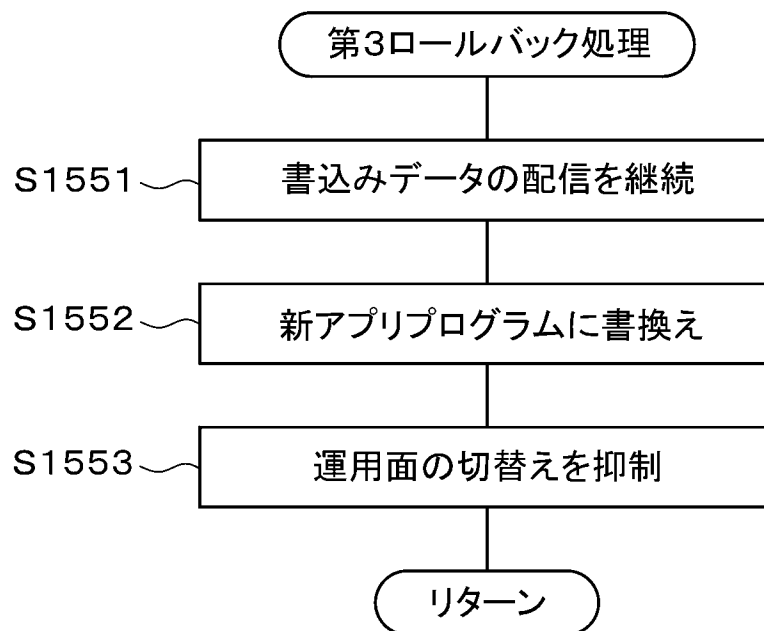
[図124]

Fig. 124



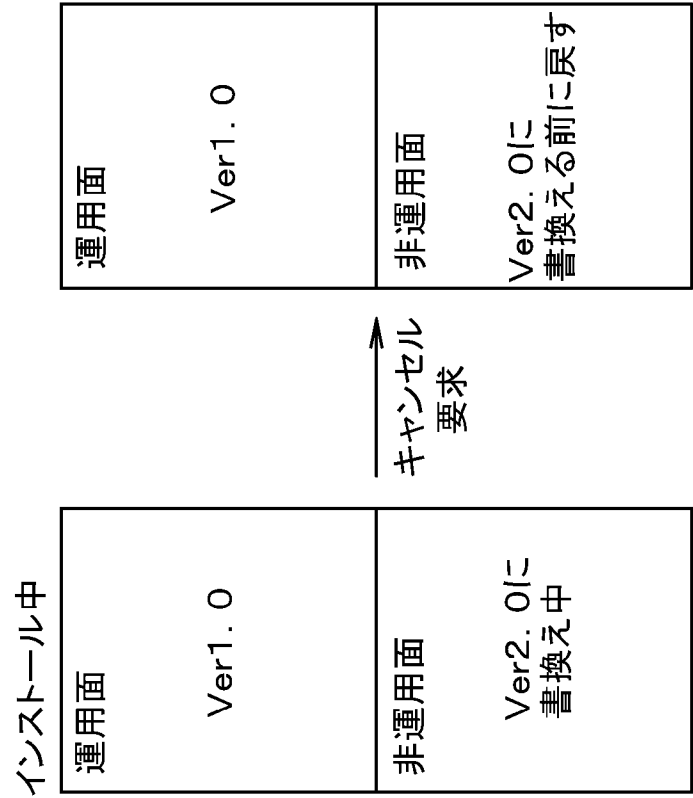
[図125]

Fig. 125



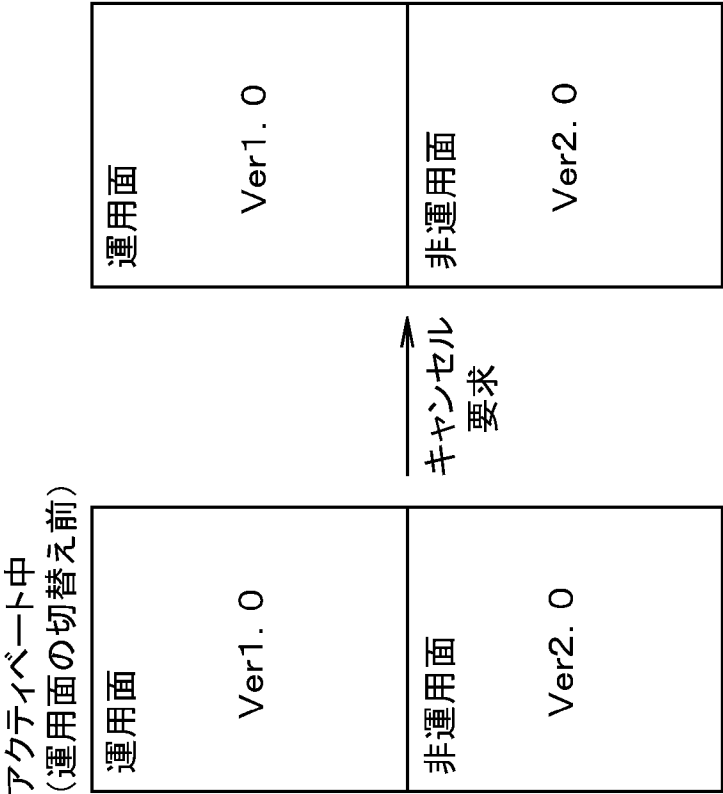
[図126]

Fig. 126



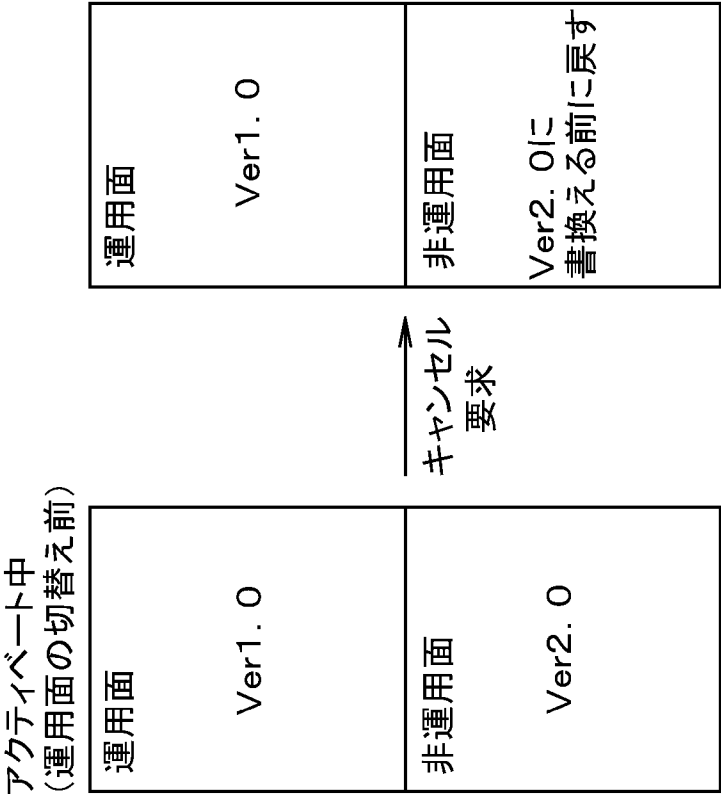
[図127]

Fig. 127



[図128]

Fig. 128



[図129]
Fig. 129

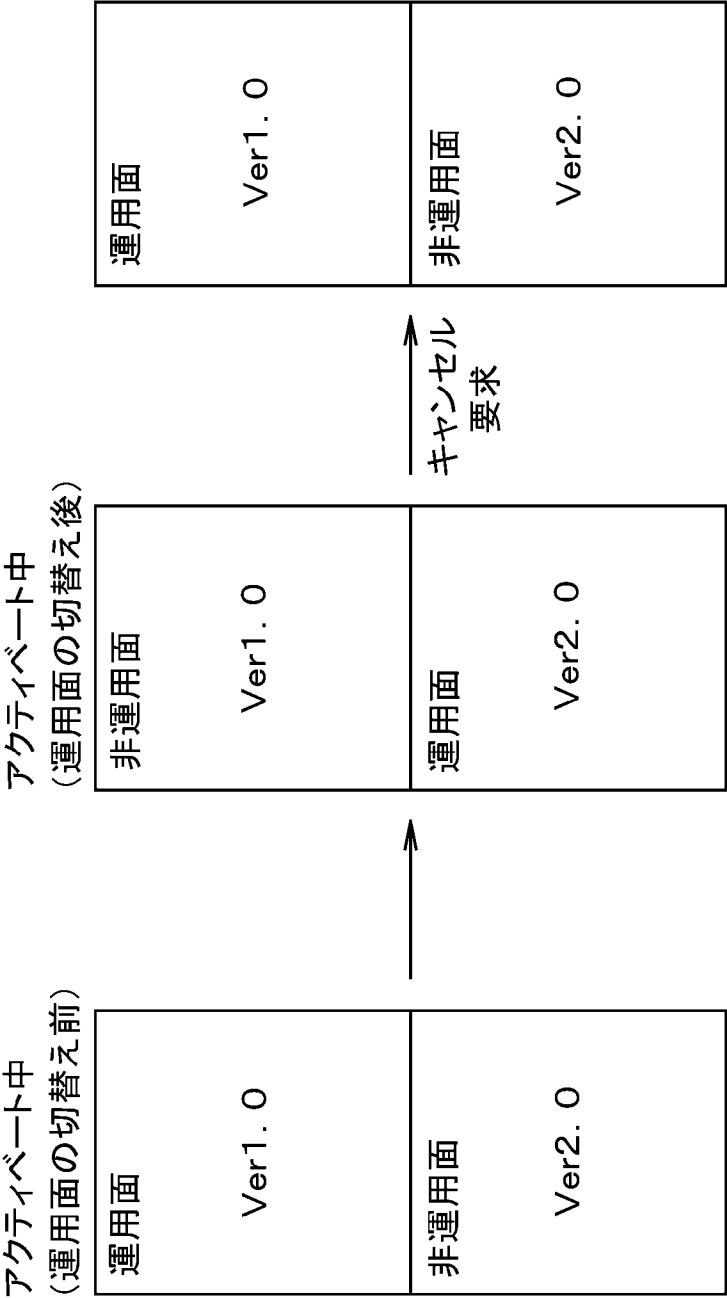
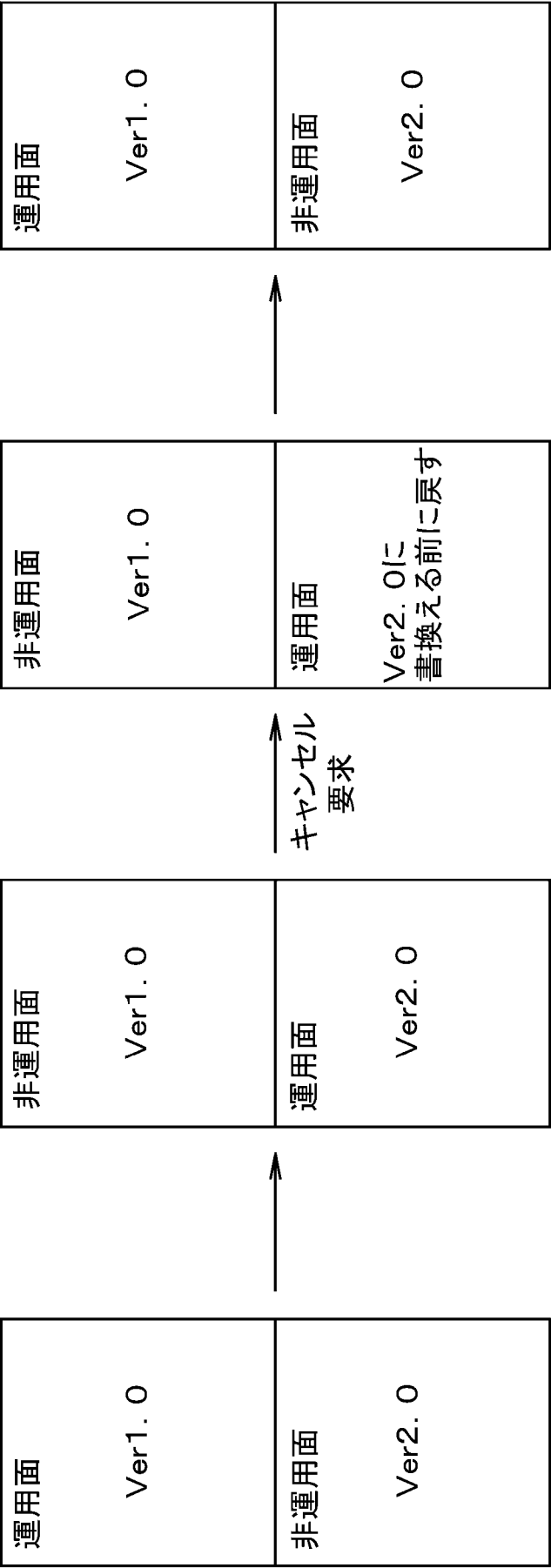


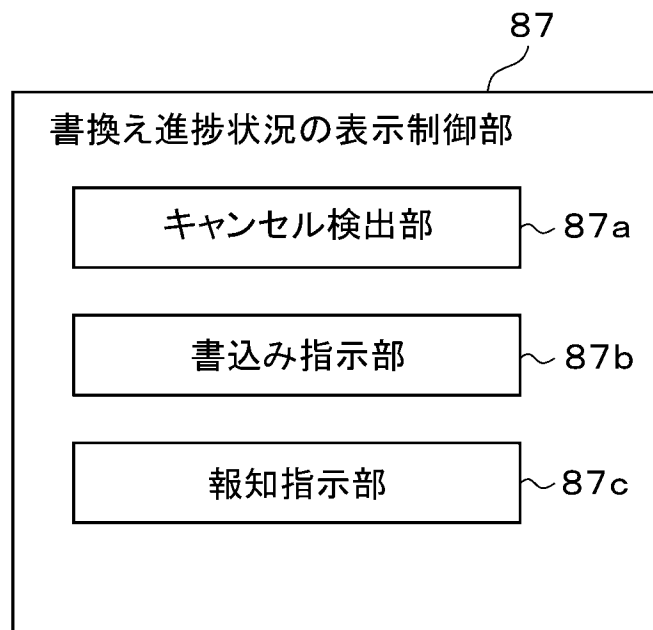
Fig. 130

[図130]



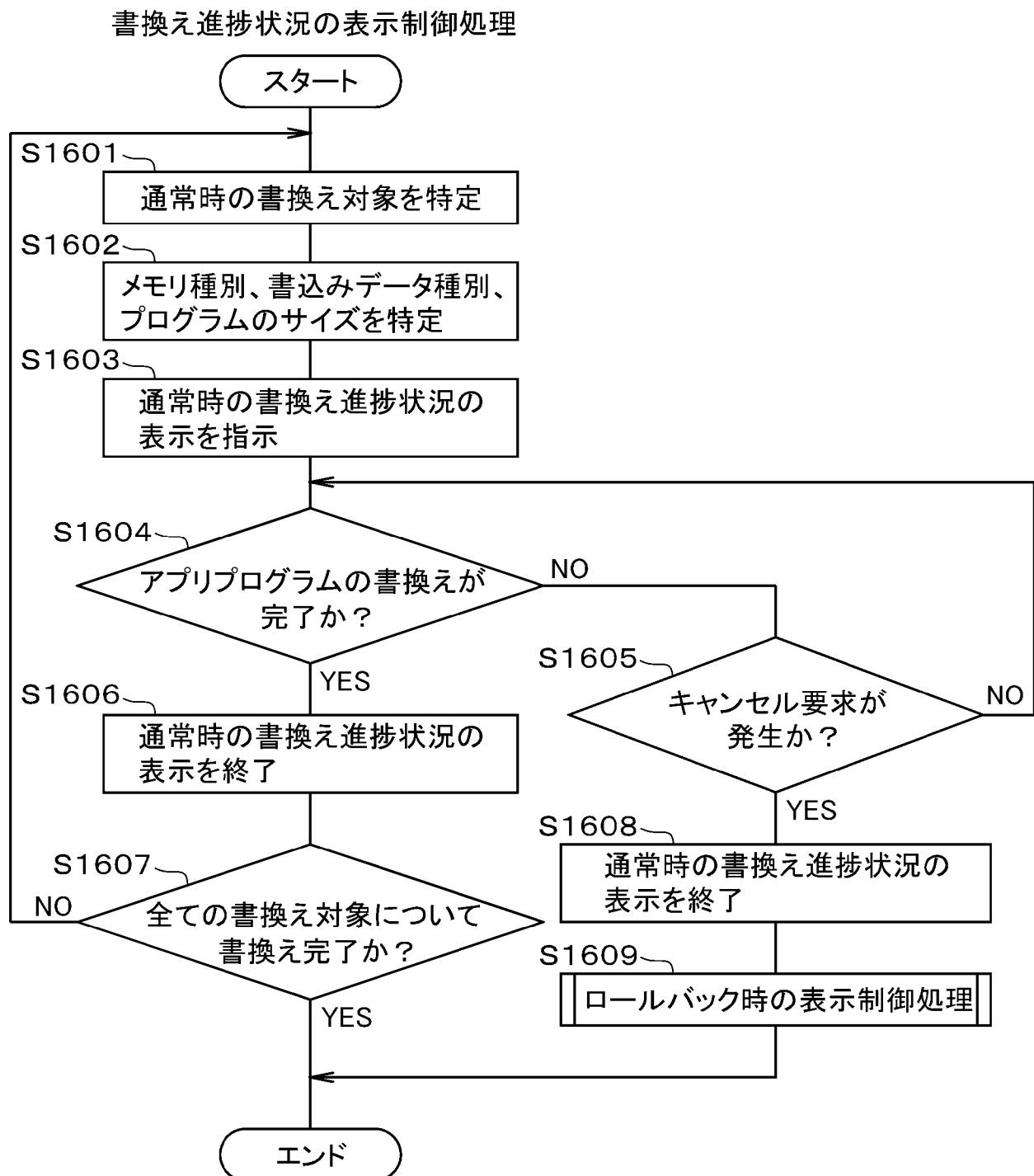
[図131]

Fig. 131



[図132]

Fig. 132



[図133]

Fig. 133

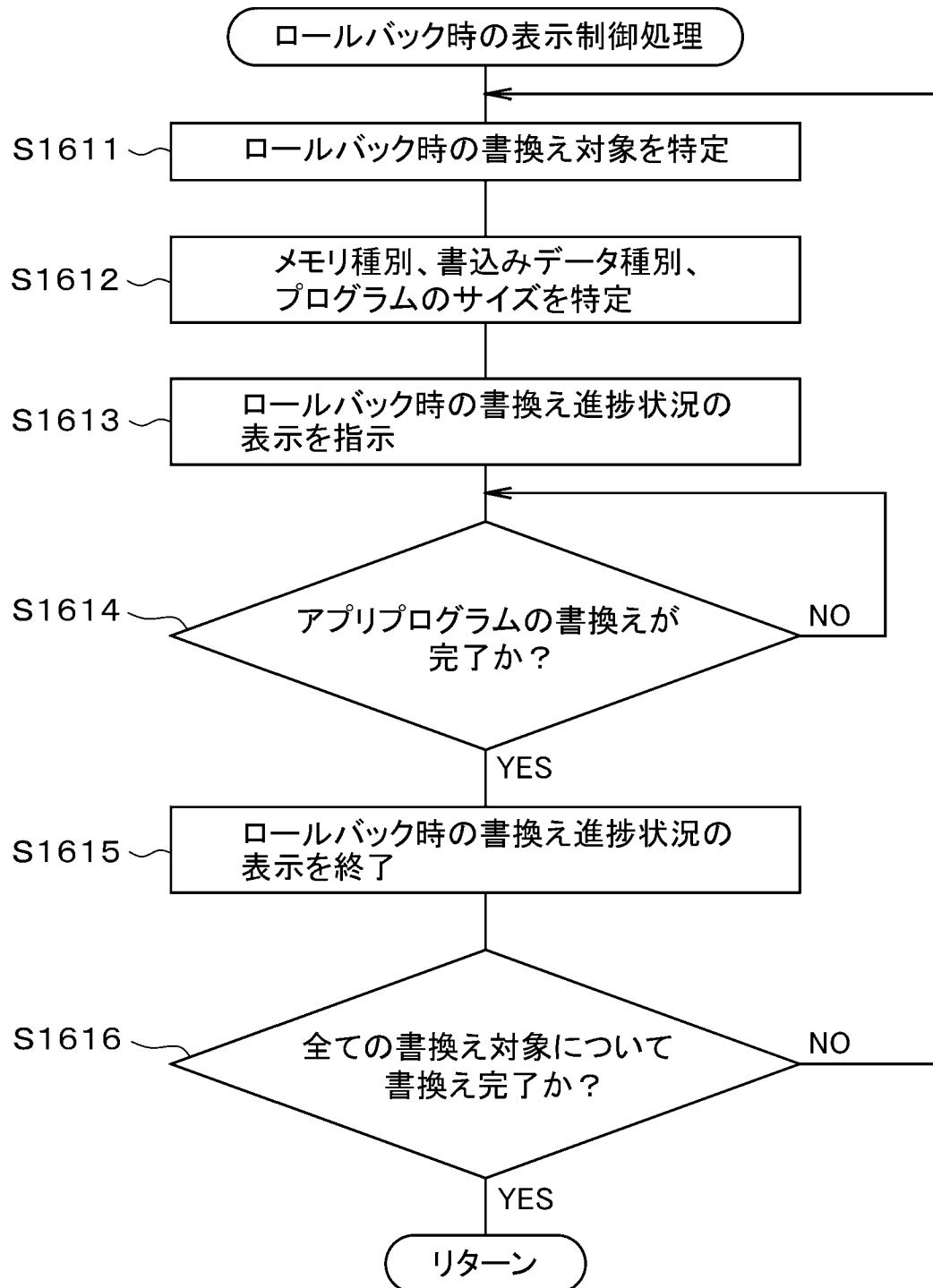


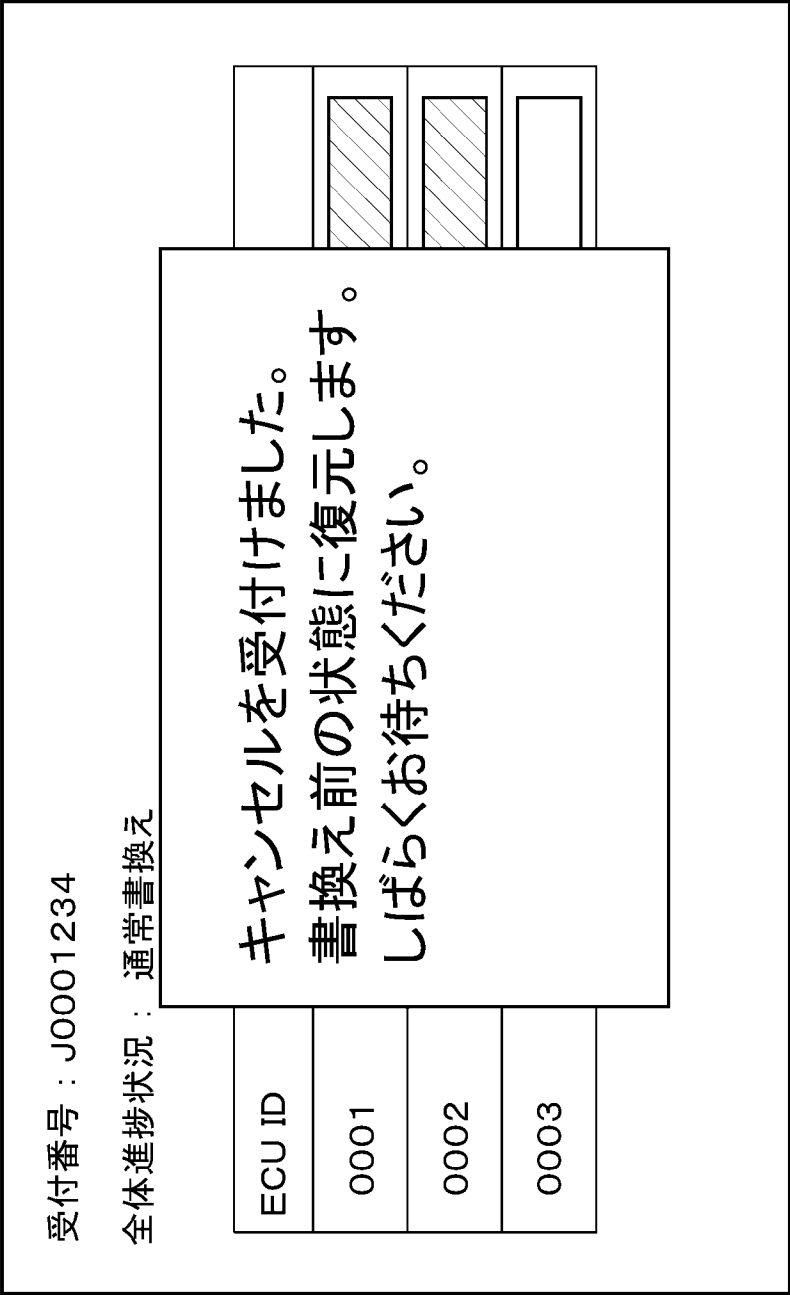
Fig. 134

[図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



[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%

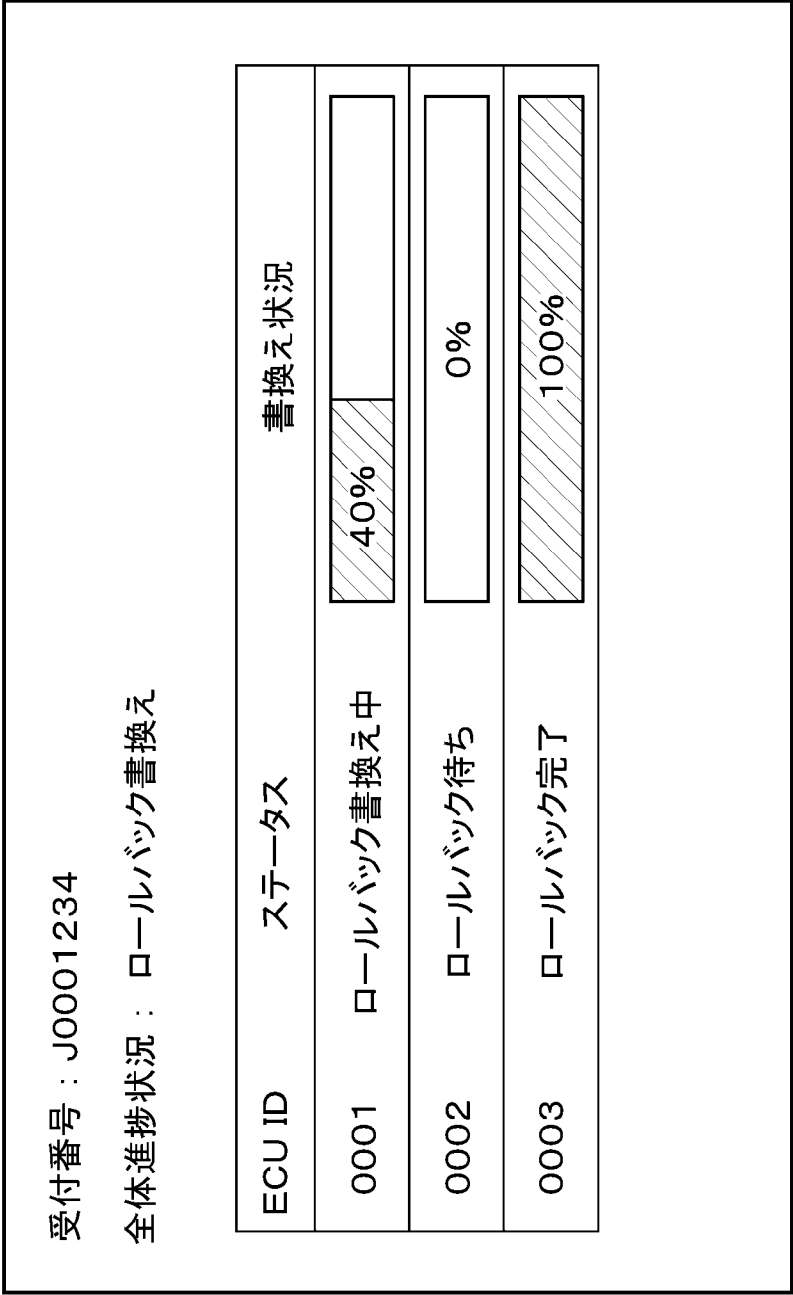
Fig. 137

受付番号：J0001234

全体進捗状況：ロールバック書換え

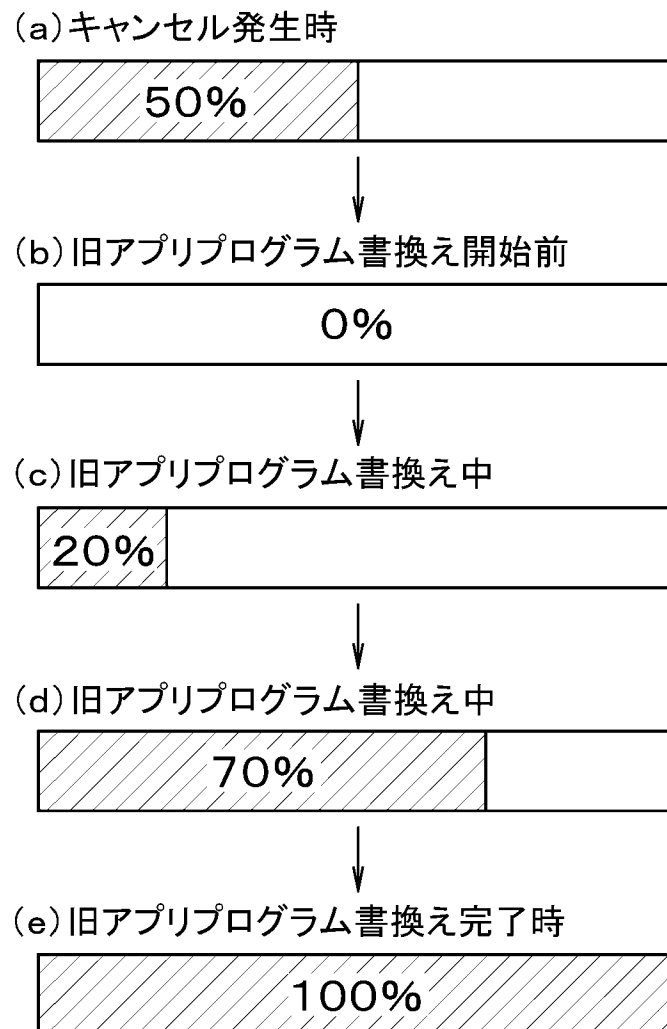
ECU ID	ステータス	書換え状況
0001	ロールバック待ち	0%
0002	ロールバック待ち	0%
0003	ロールバック書換え中	30%

Fig. 138 [図138]

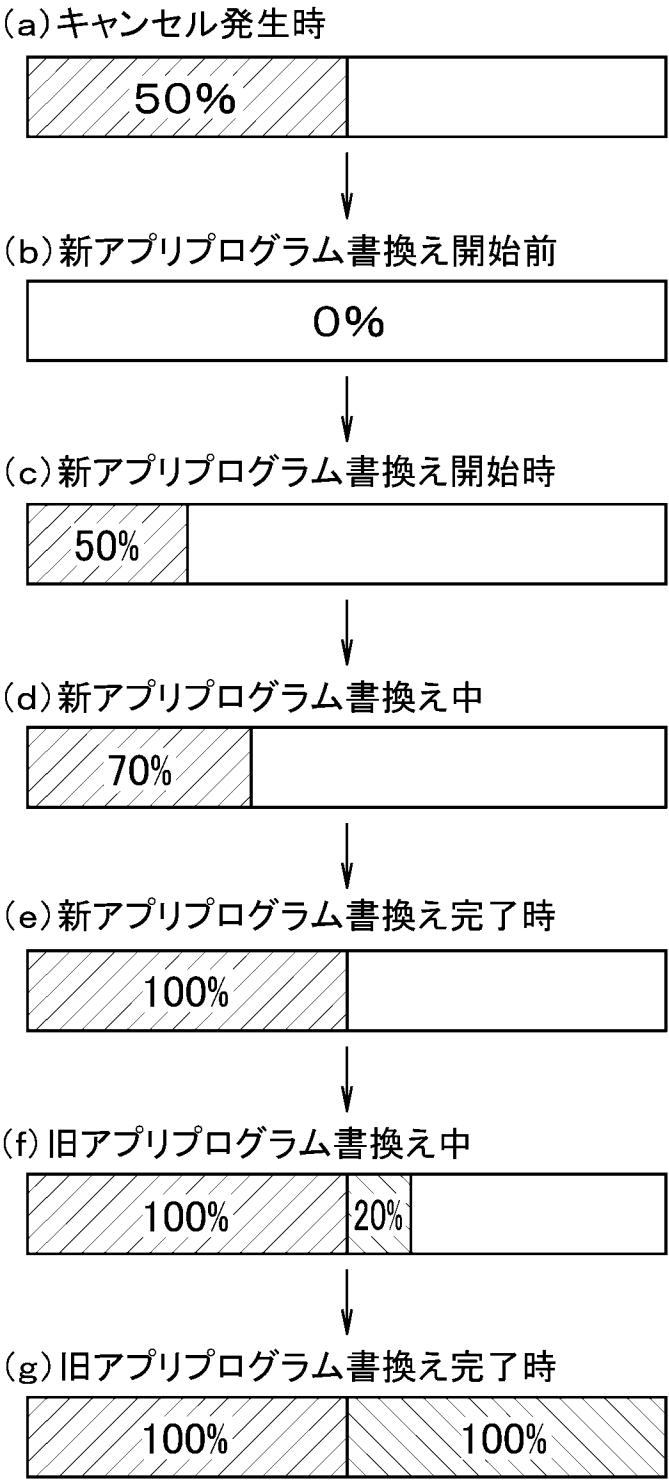


[図139]

Fig. 139

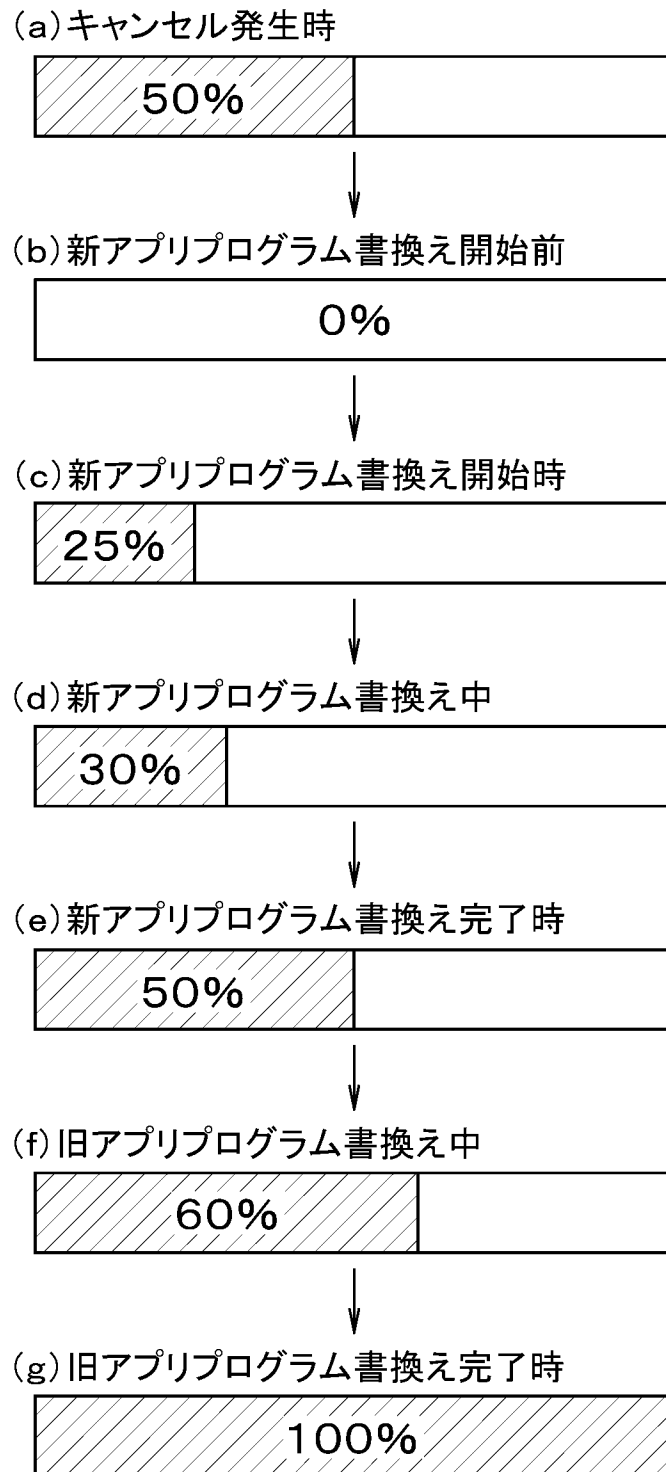


[図140]
Fig. 140



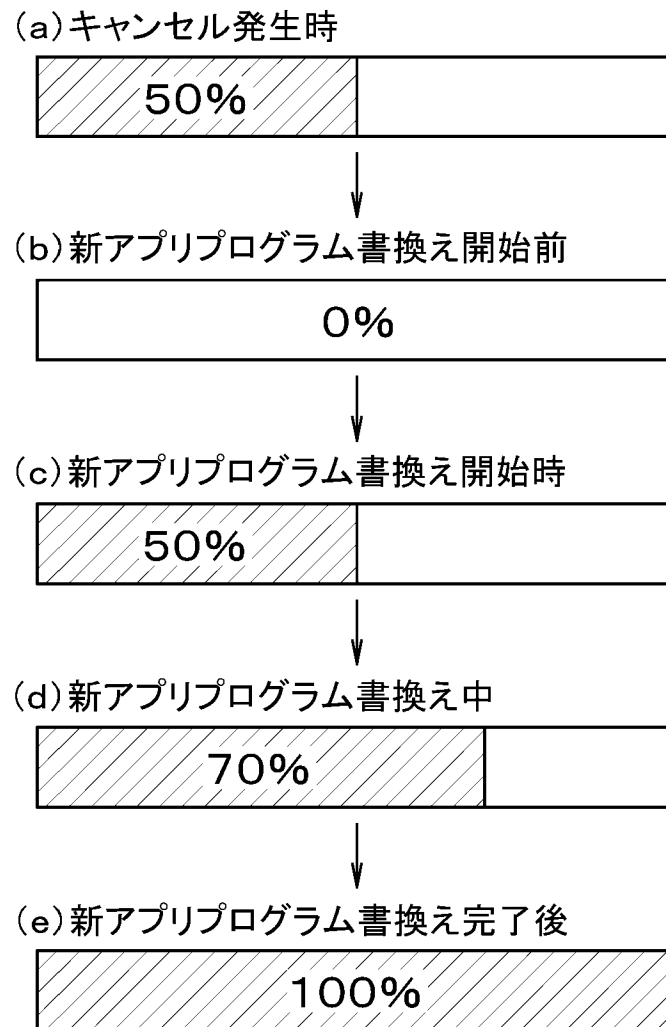
[図141]

Fig. 141



[図142]

Fig. 142



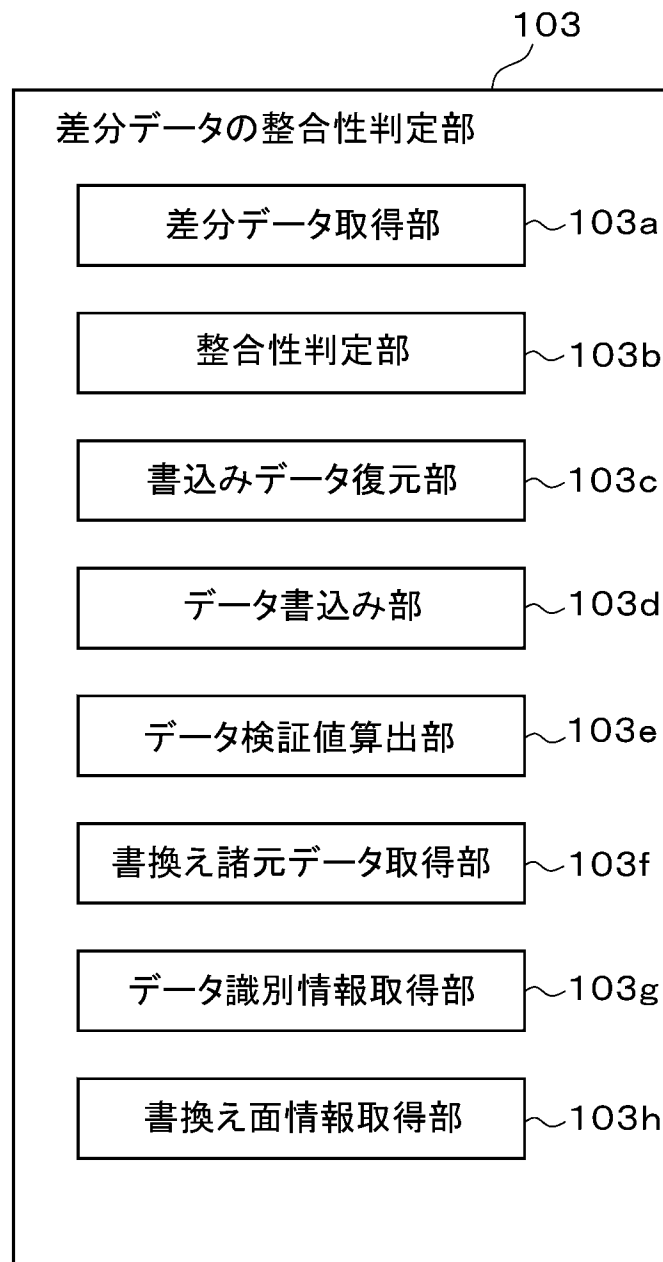
[図143]

Fig. 143

受付番号：J0001234		
ECU ID	ステータス	書換え状況
0001	ロールバック待ち	0%
0002		
0003		

[図144]

Fig. 144



[図145]

Fig. 145 差分データの整合性判定処理

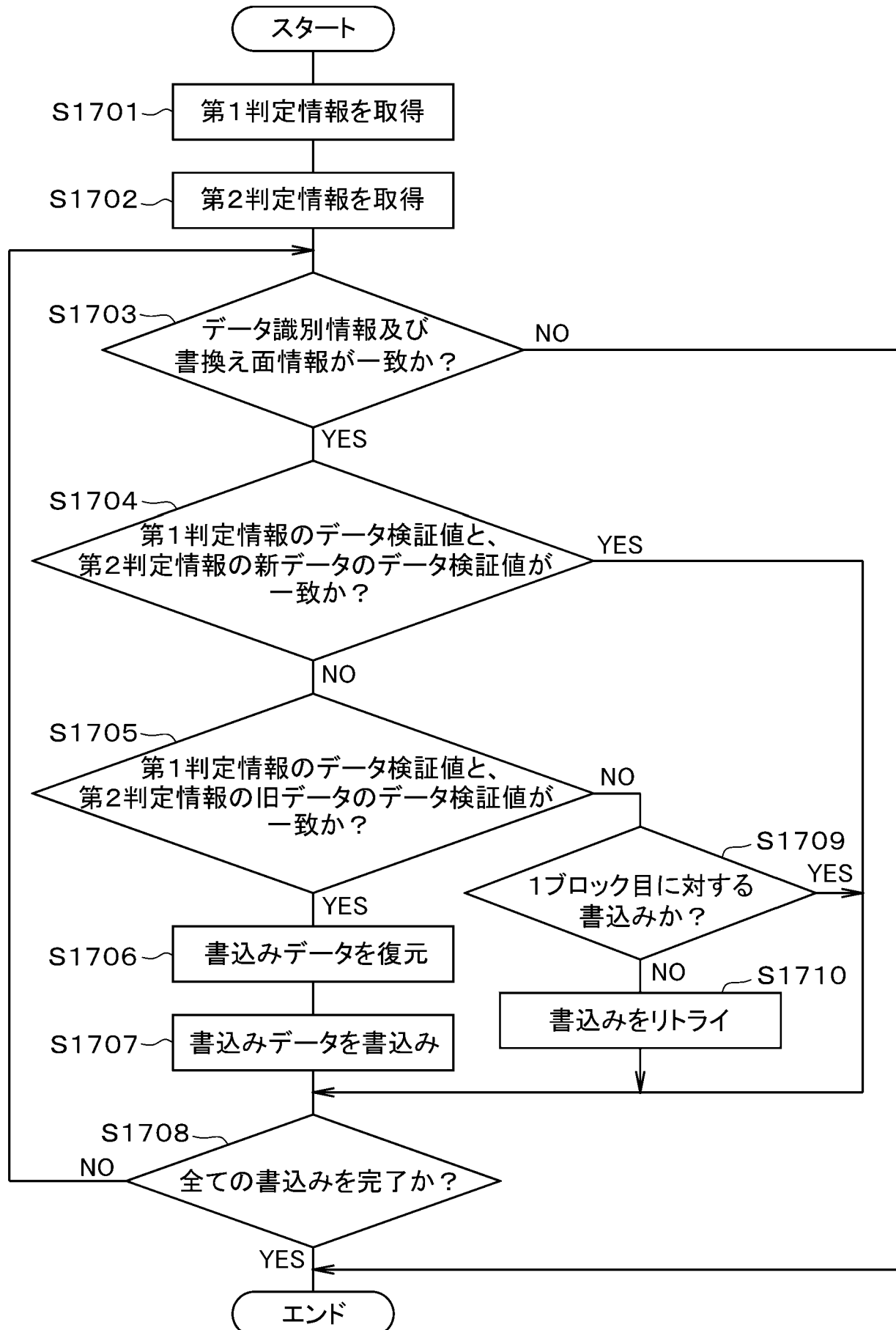
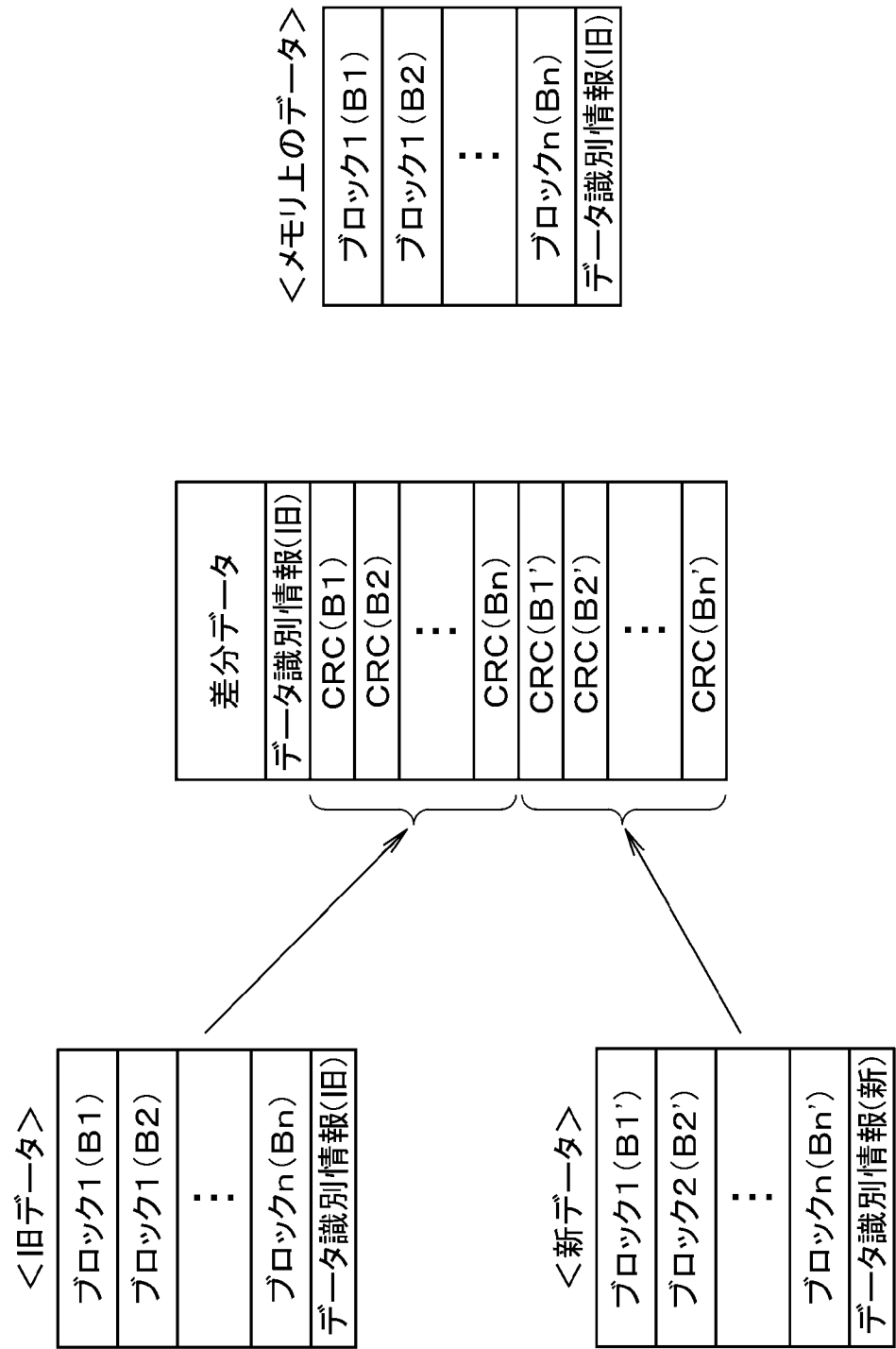


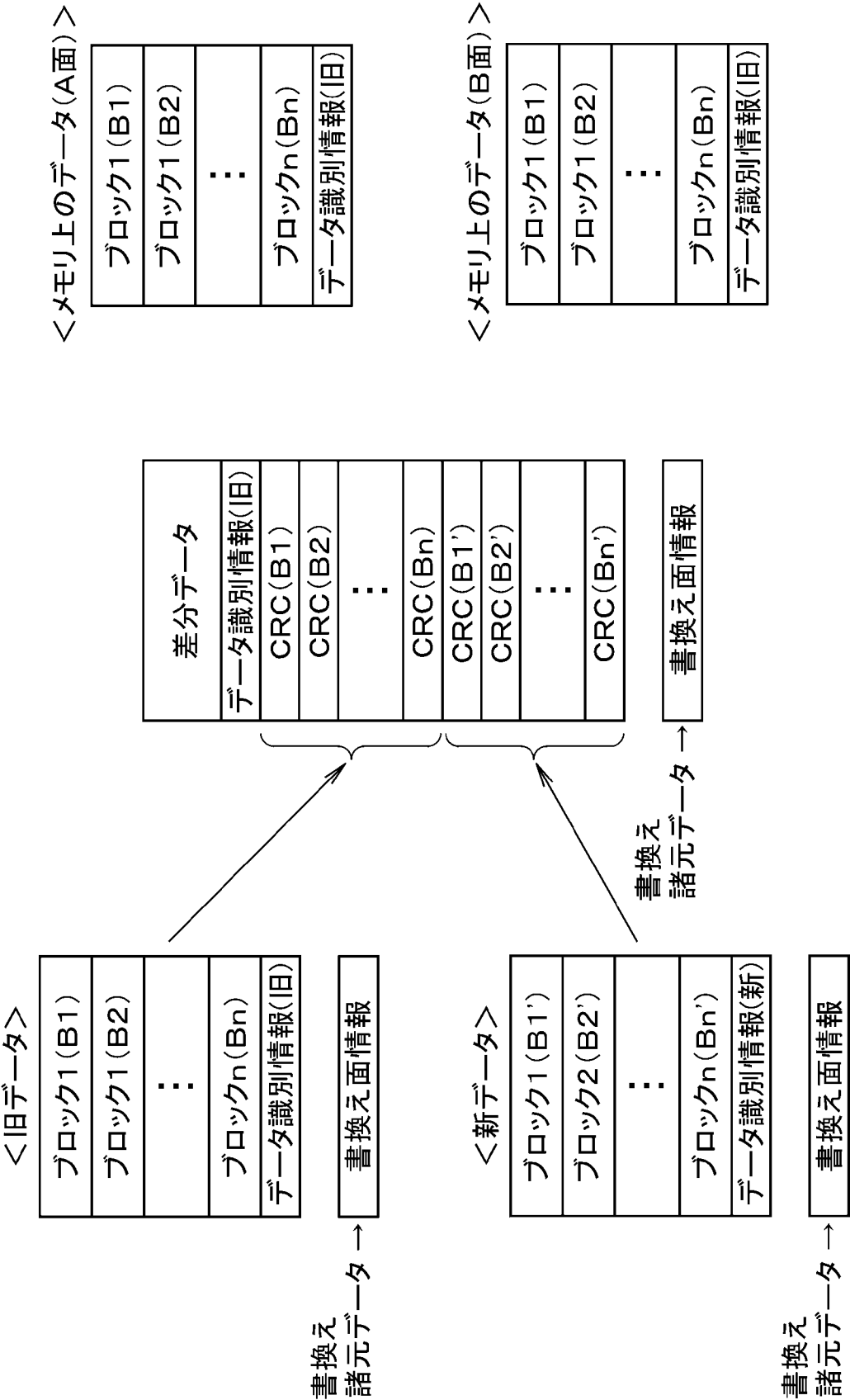
Fig. 146

[図146]



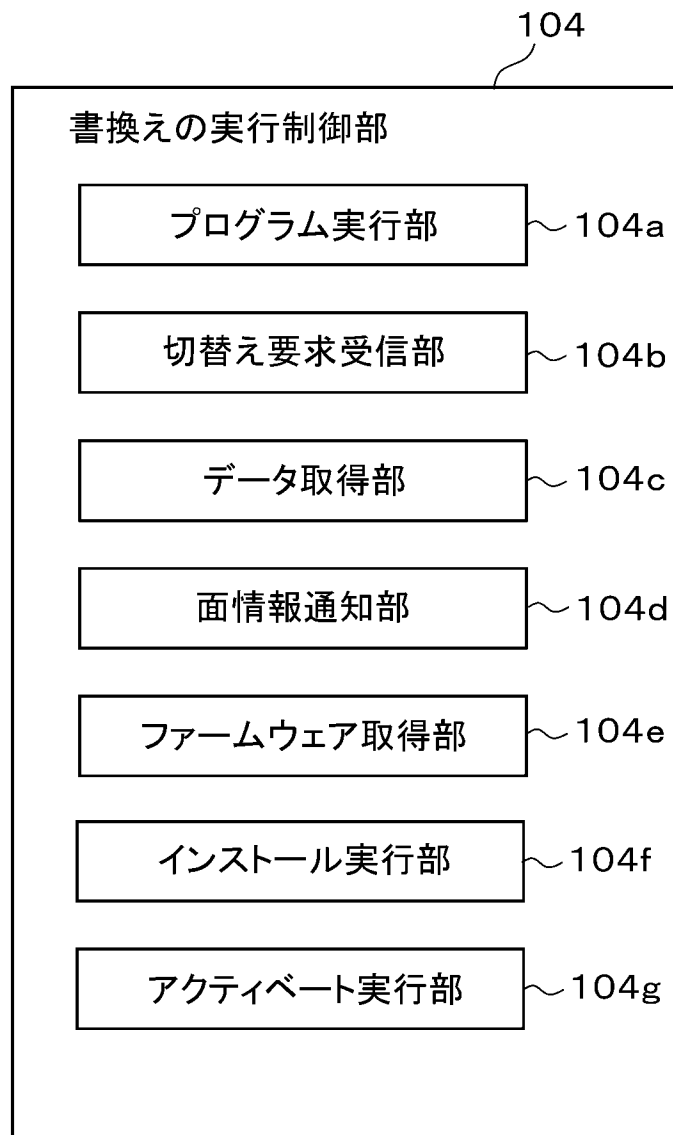
[図147]

Fig. 147



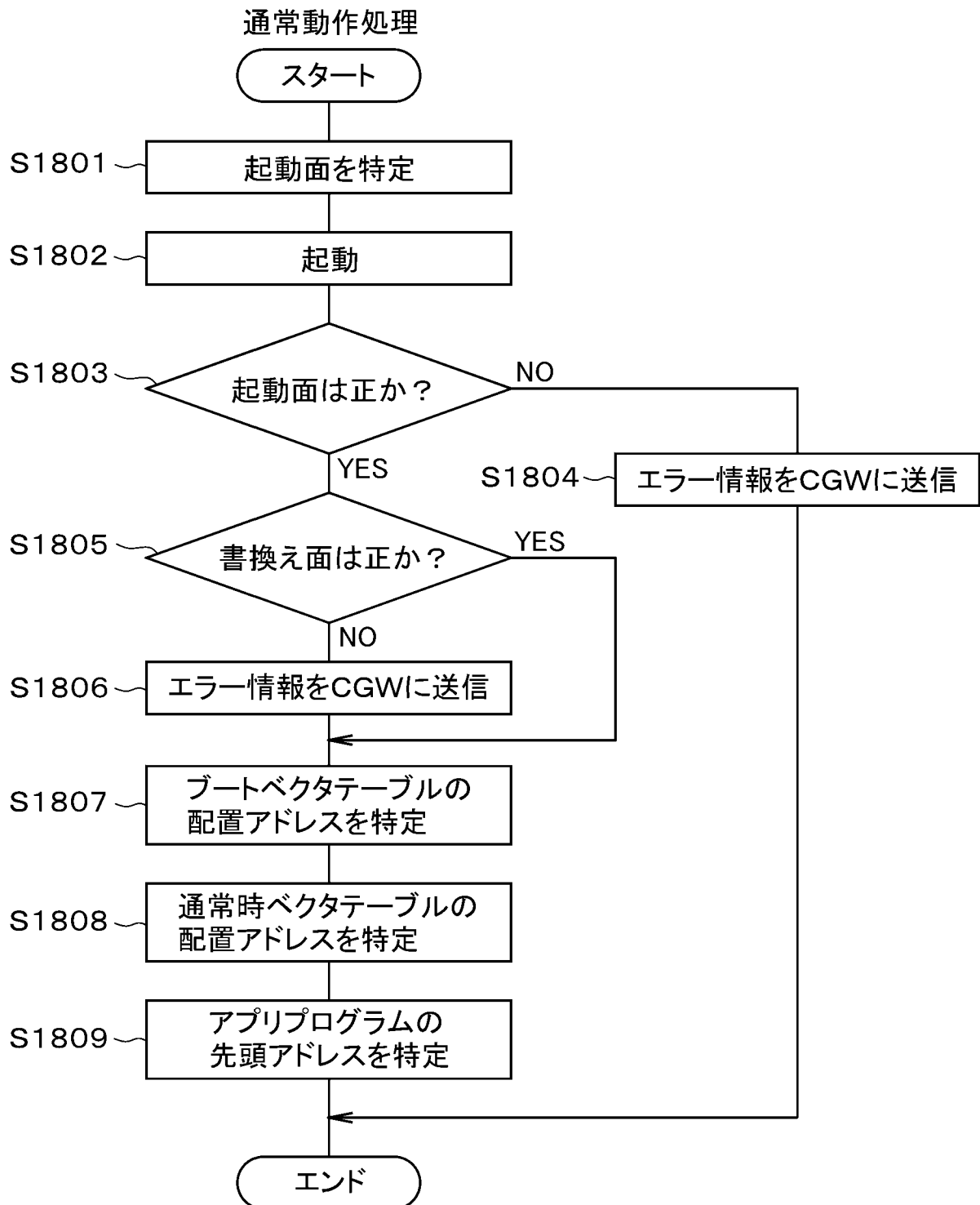
[図148]

Fig. 148



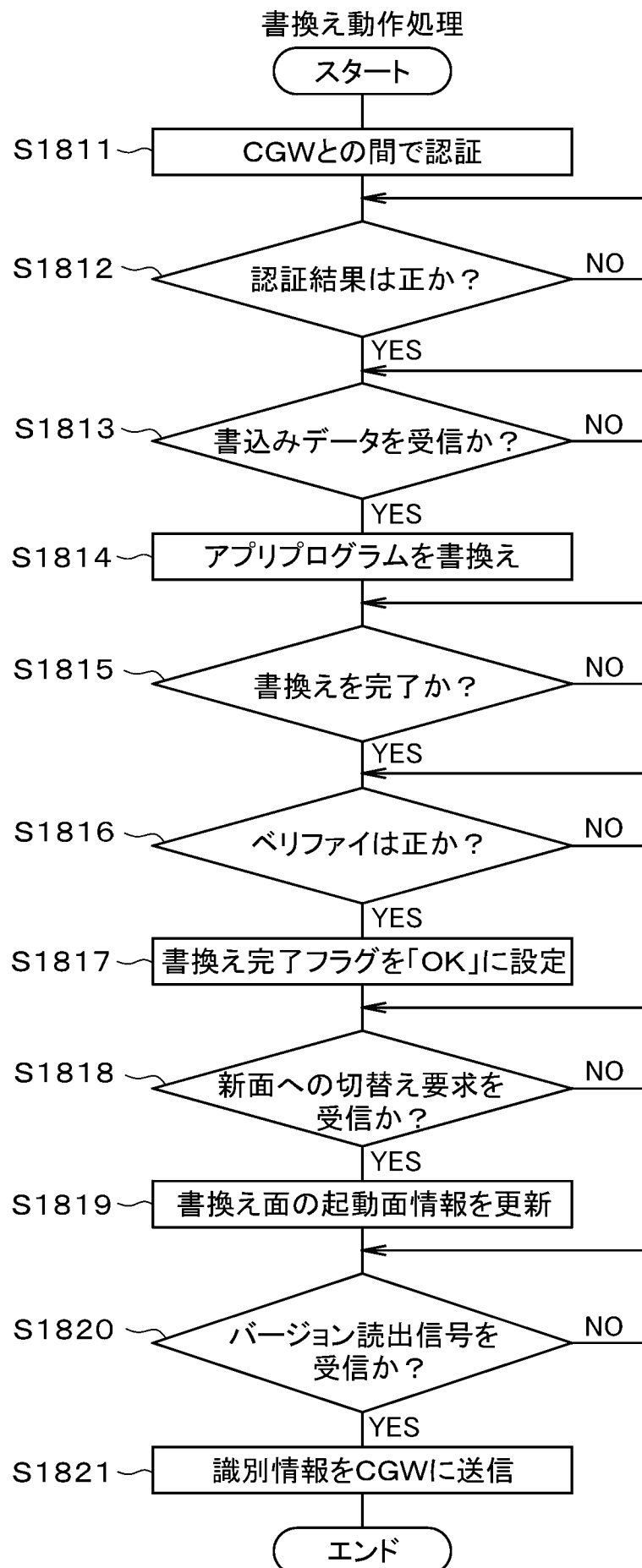
[図149]

Fig. 149



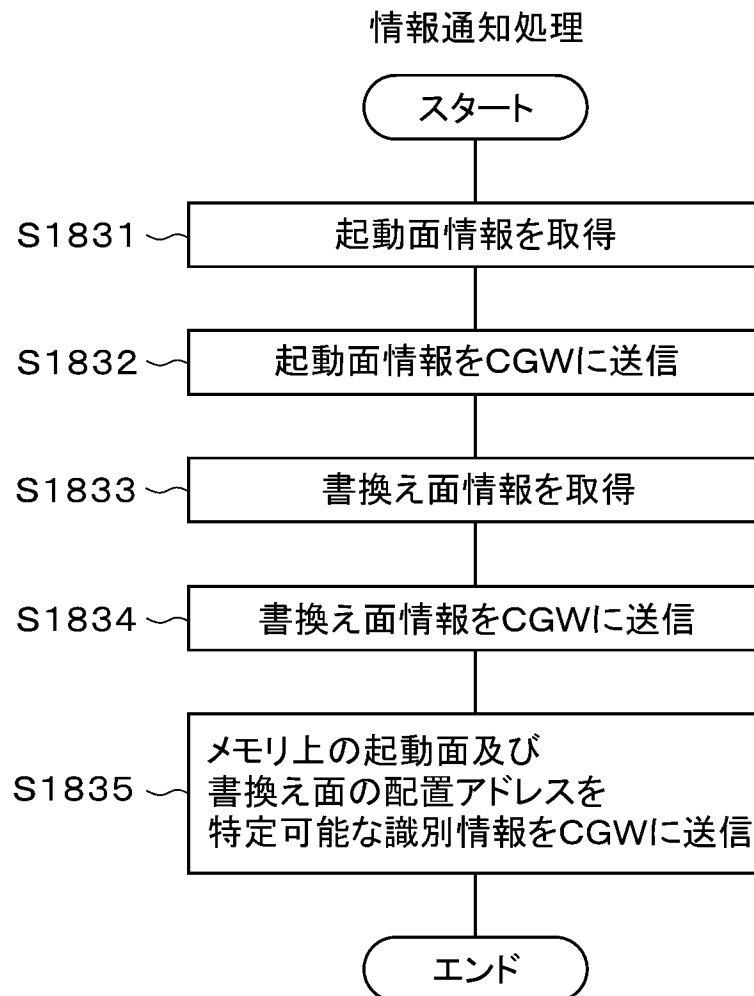
[図150]

Fig. 150



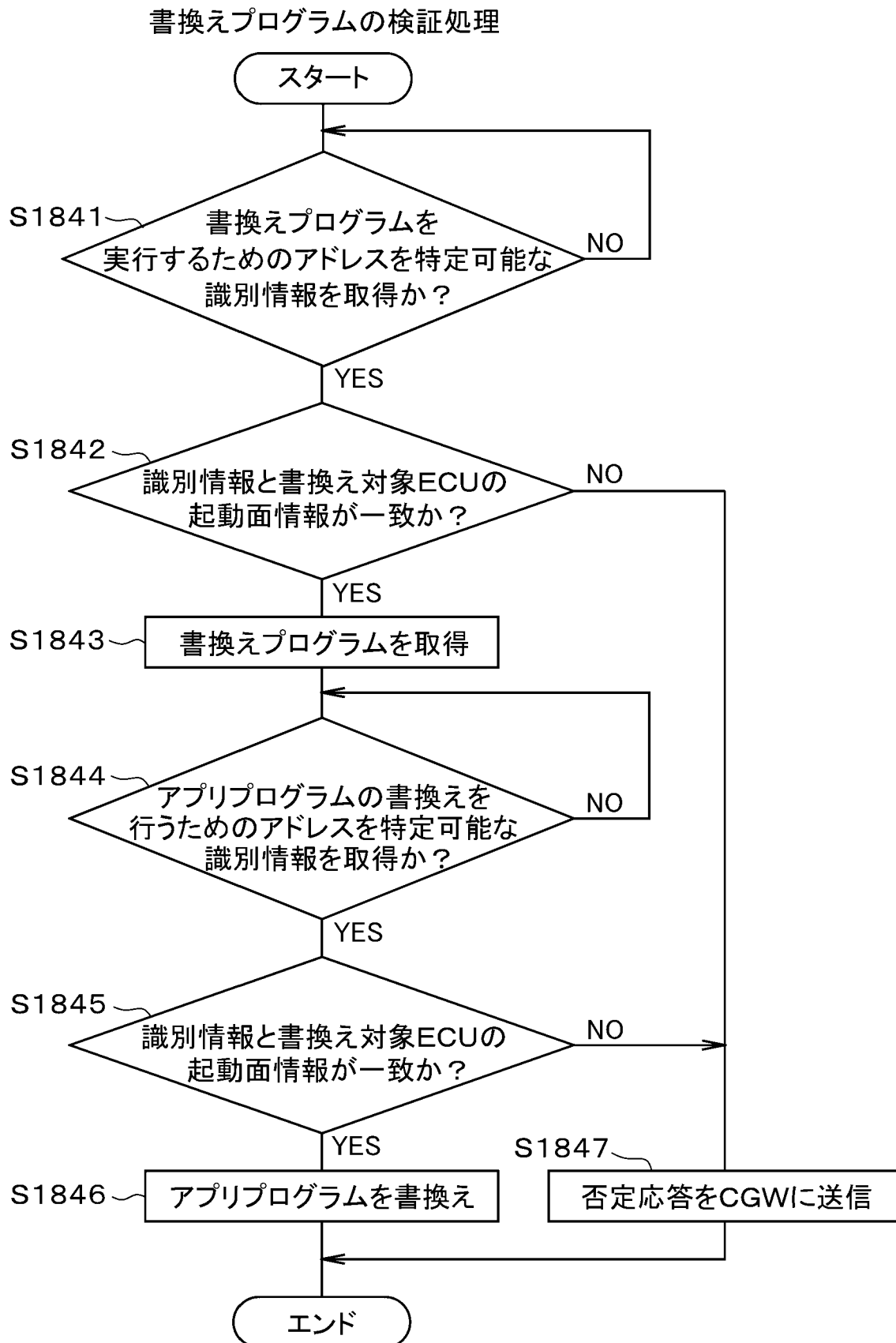
[図151]

Fig. 151

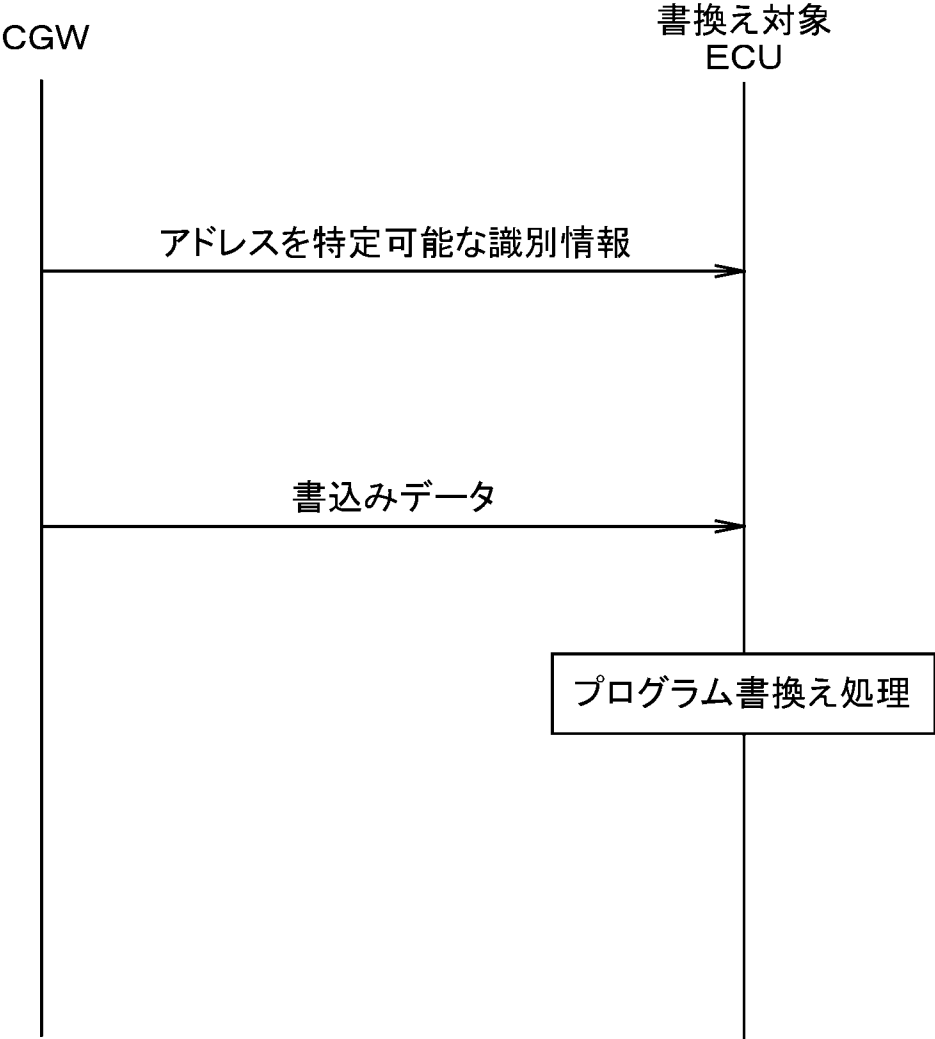


[図152]

Fig. 152

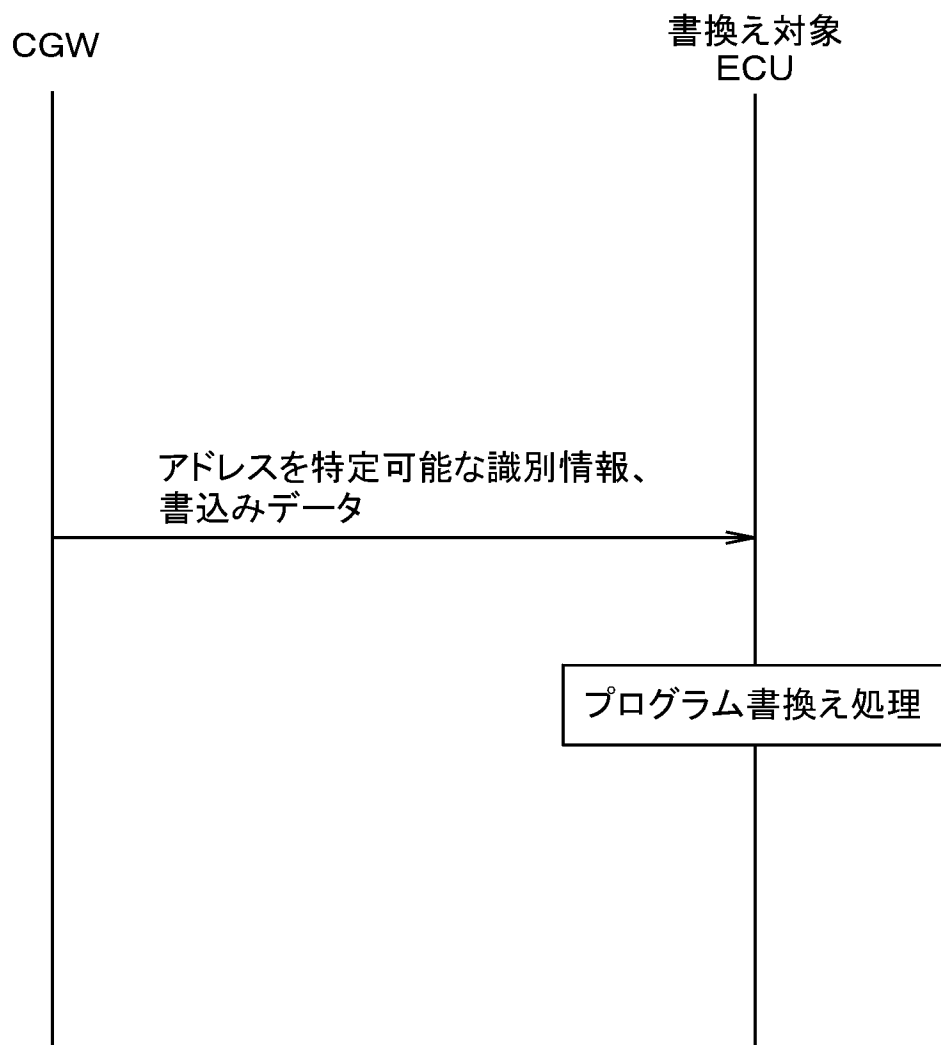


[図153]
Fig. 153



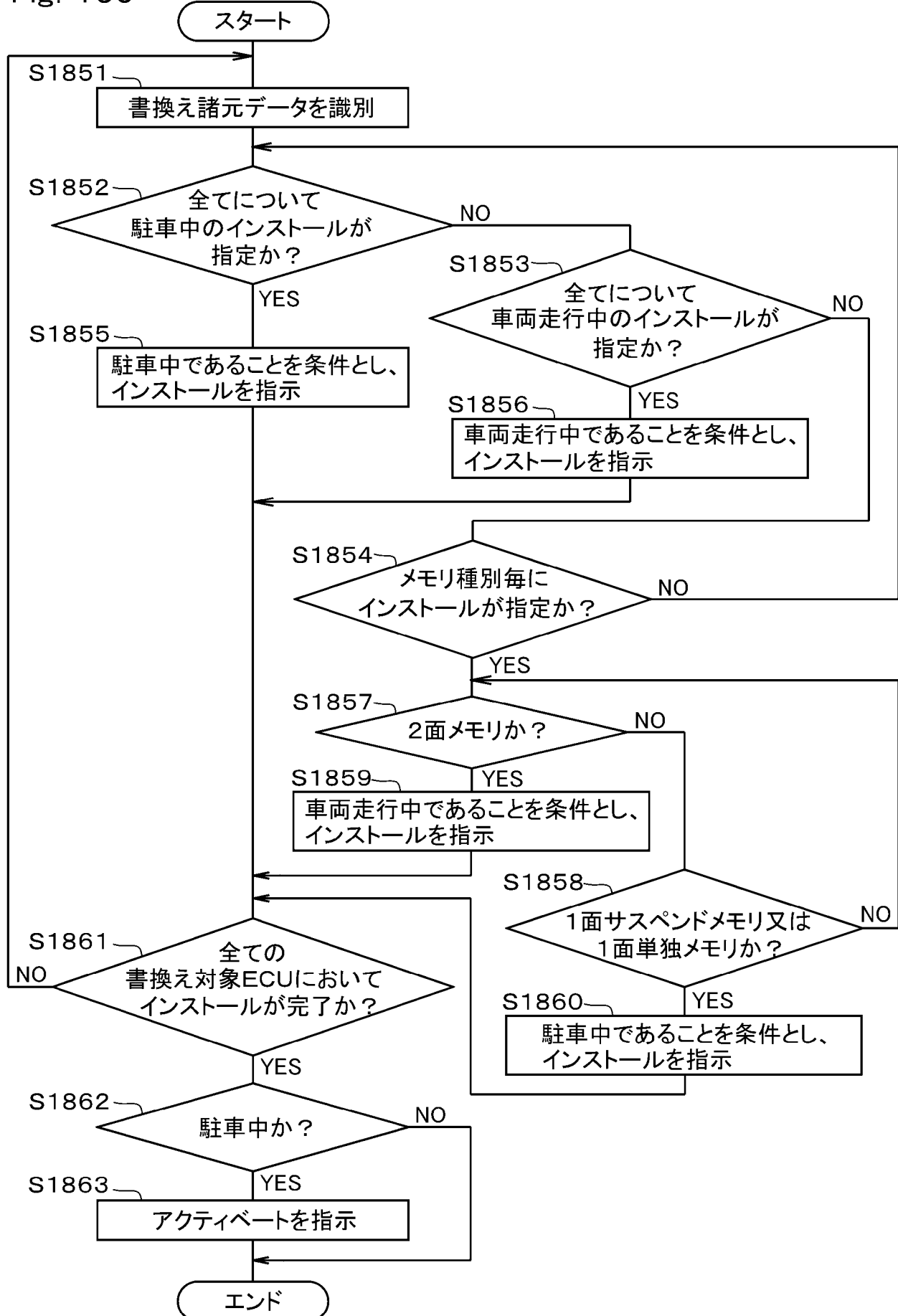
[図154]

Fig. 154

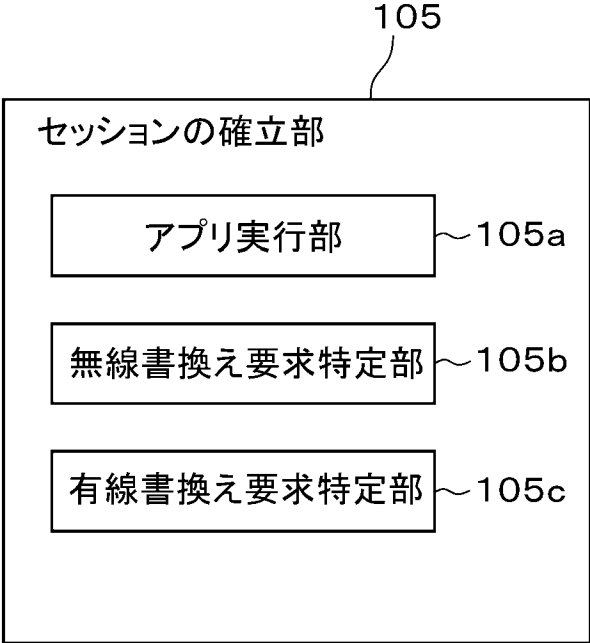


[図155]

Fig. 155 インストール指示処理



[図156]
Fig. 156

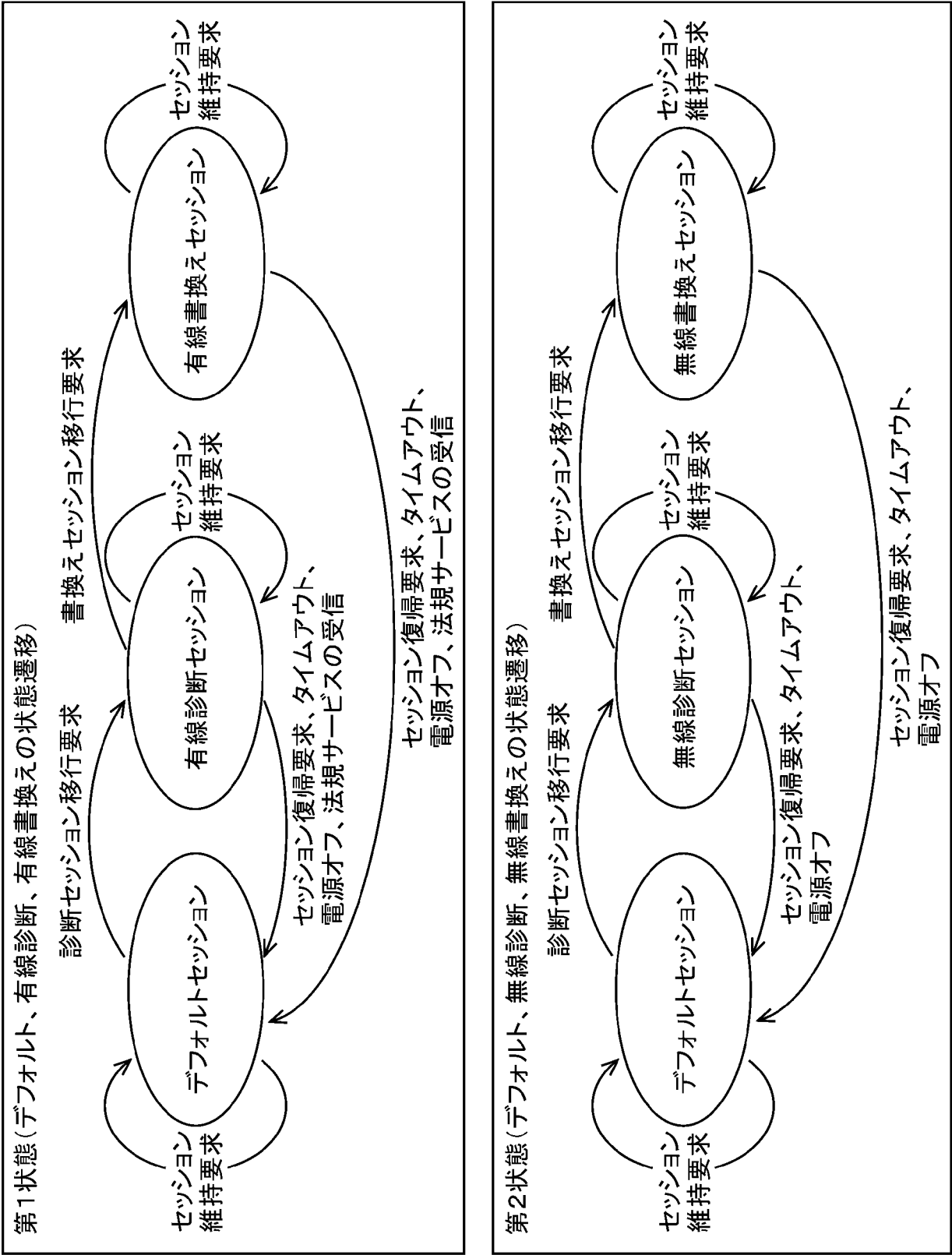


[図157]
Fig. 157



[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)



書換えセツシヨン移行要求

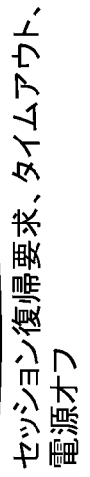


Fig. 161

[図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

Fig. 162

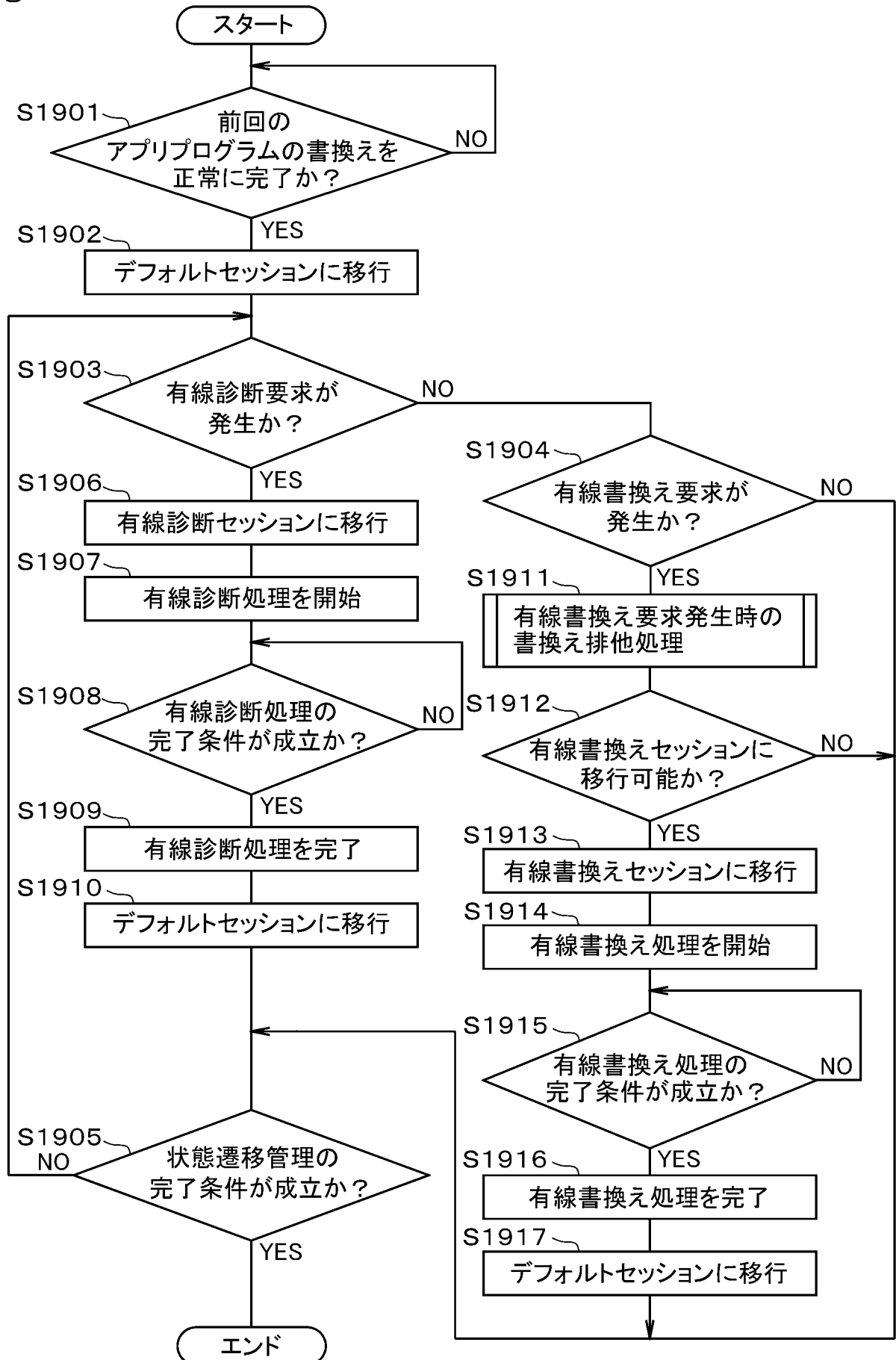
[図162]

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

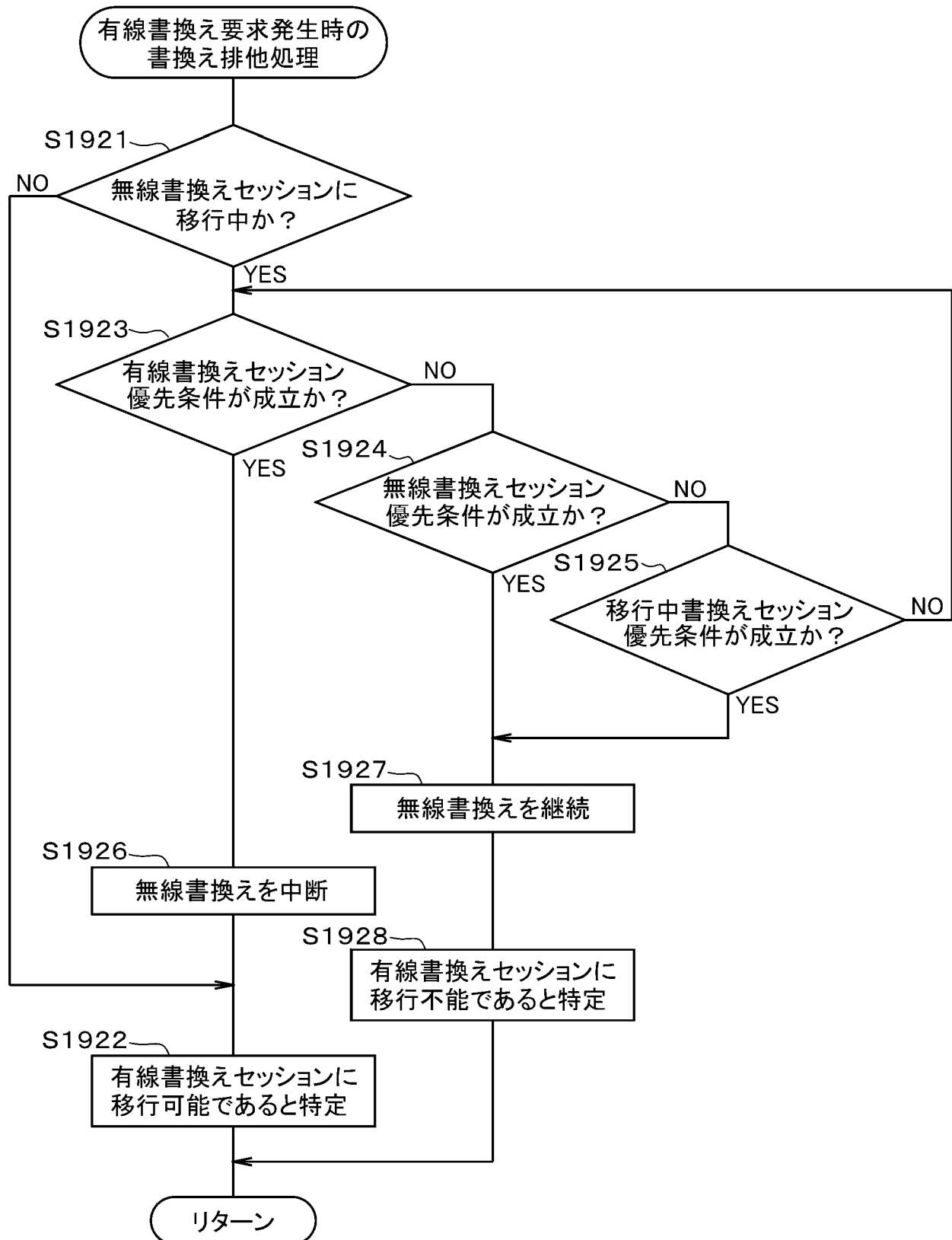
[図163]

Fig. 163 第1状態の状態遷移管理



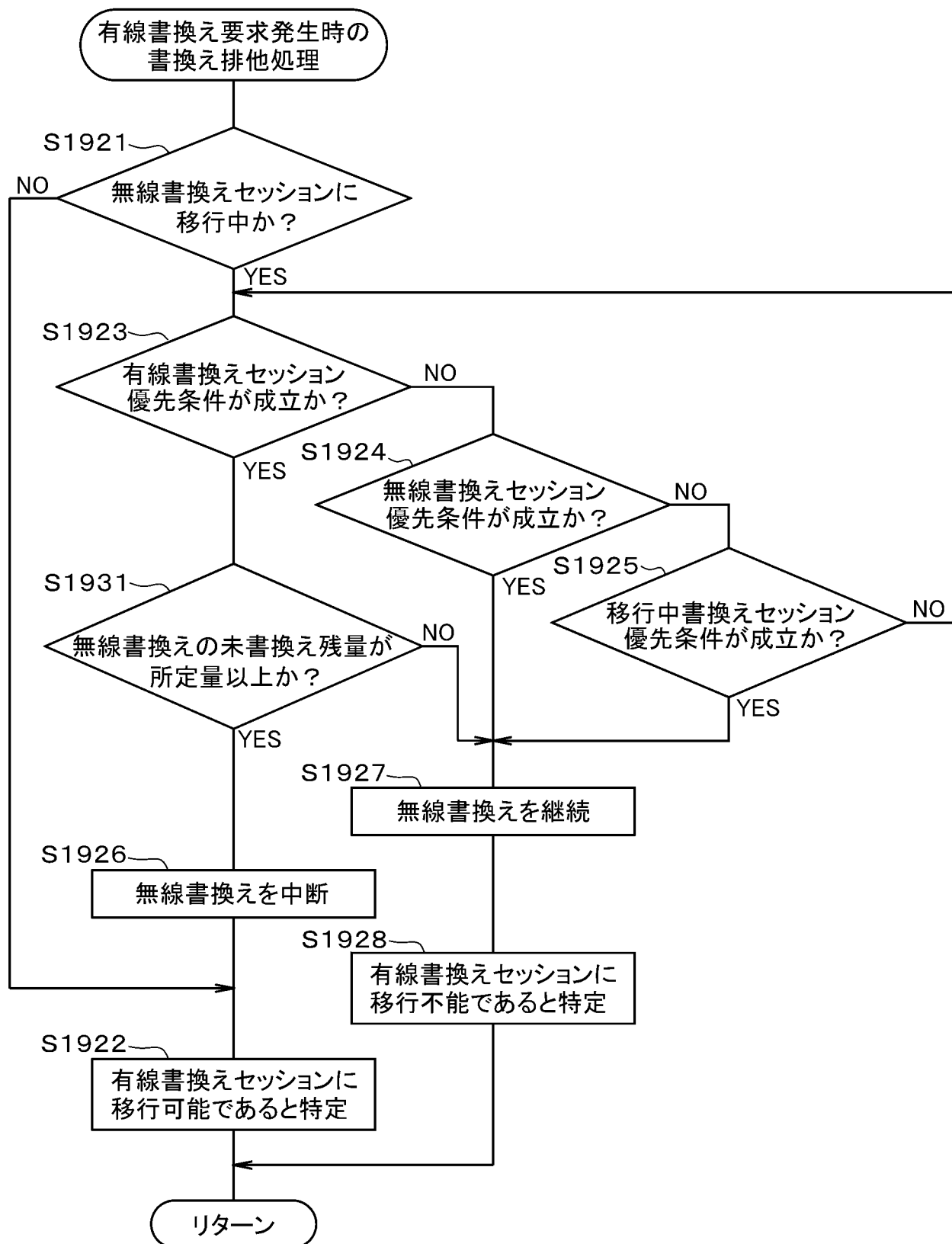
[図164]

Fig. 164



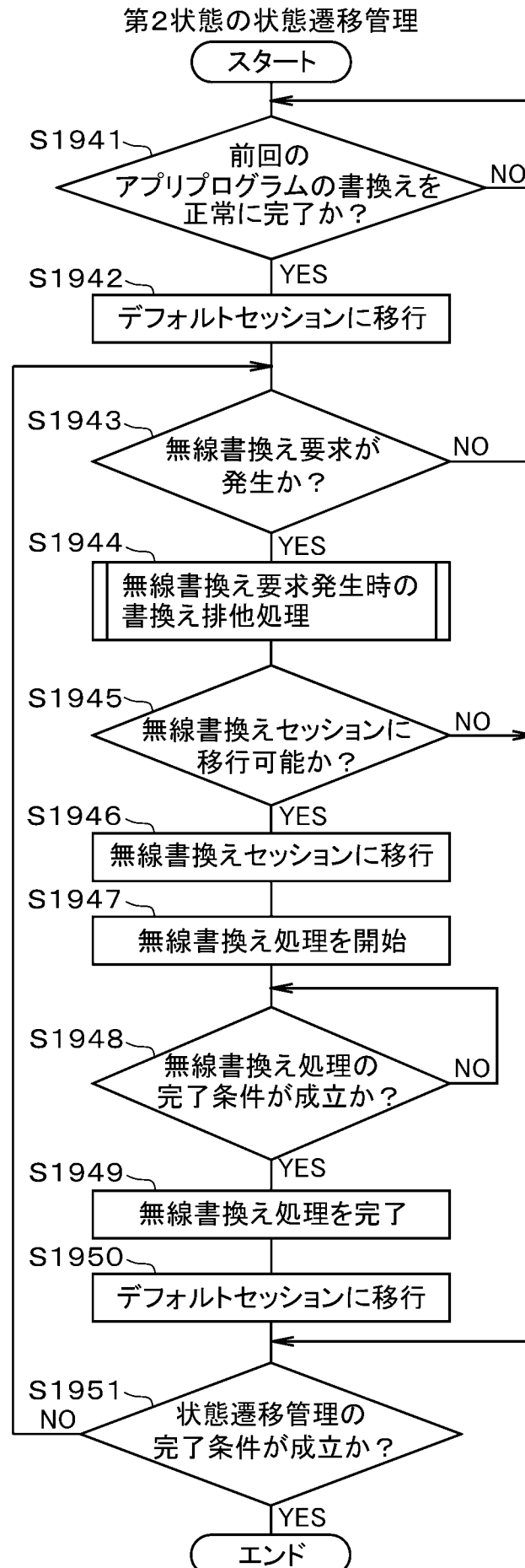
[図165]

Fig. 165



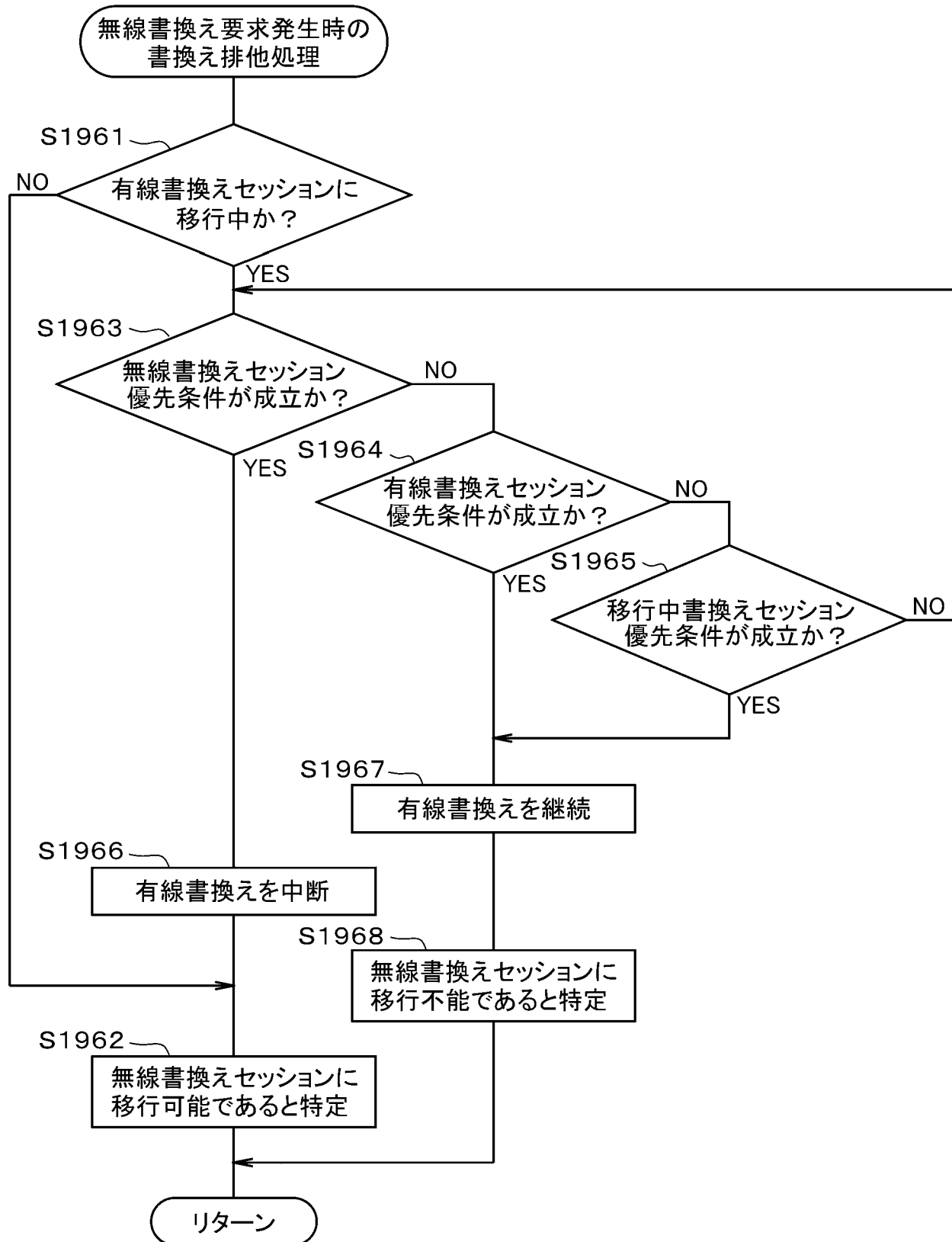
[図166]

Fig. 166

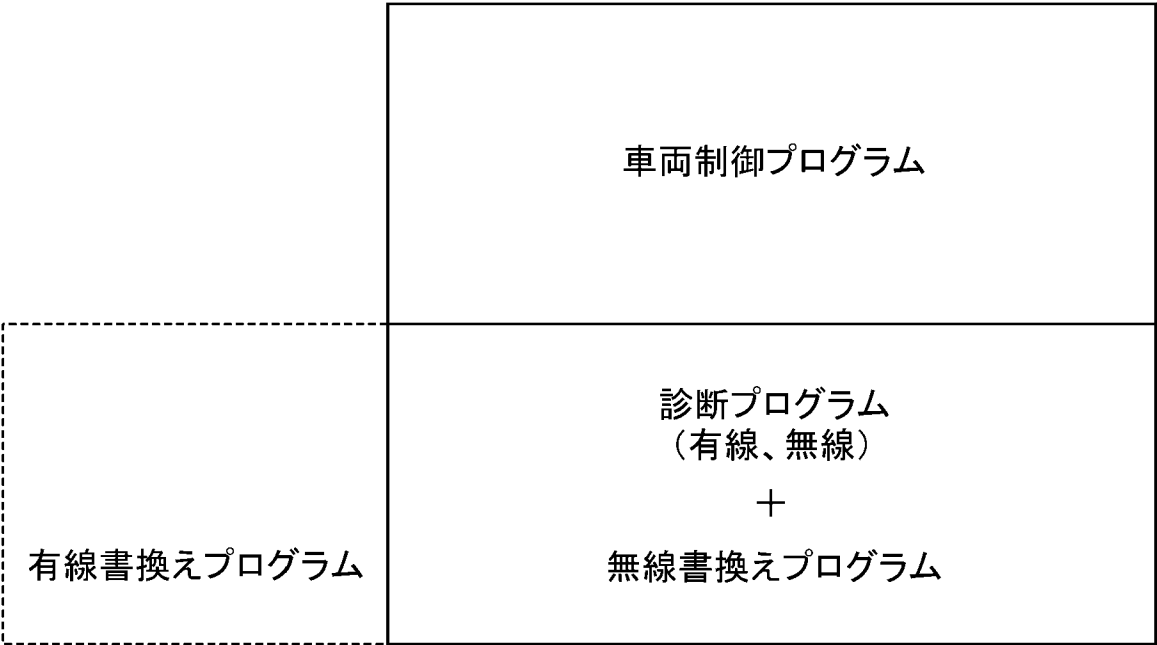


[図167]

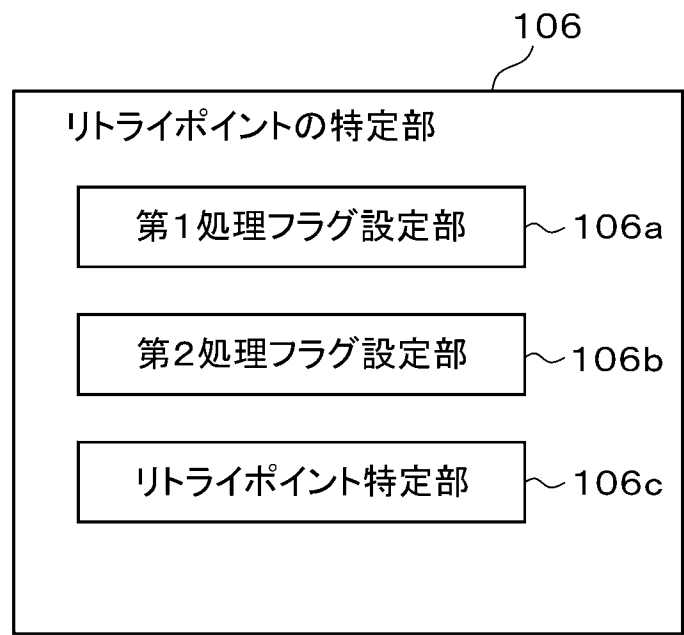
Fig. 167



[図168]
Fig. 168



[図170]
Fig. 170

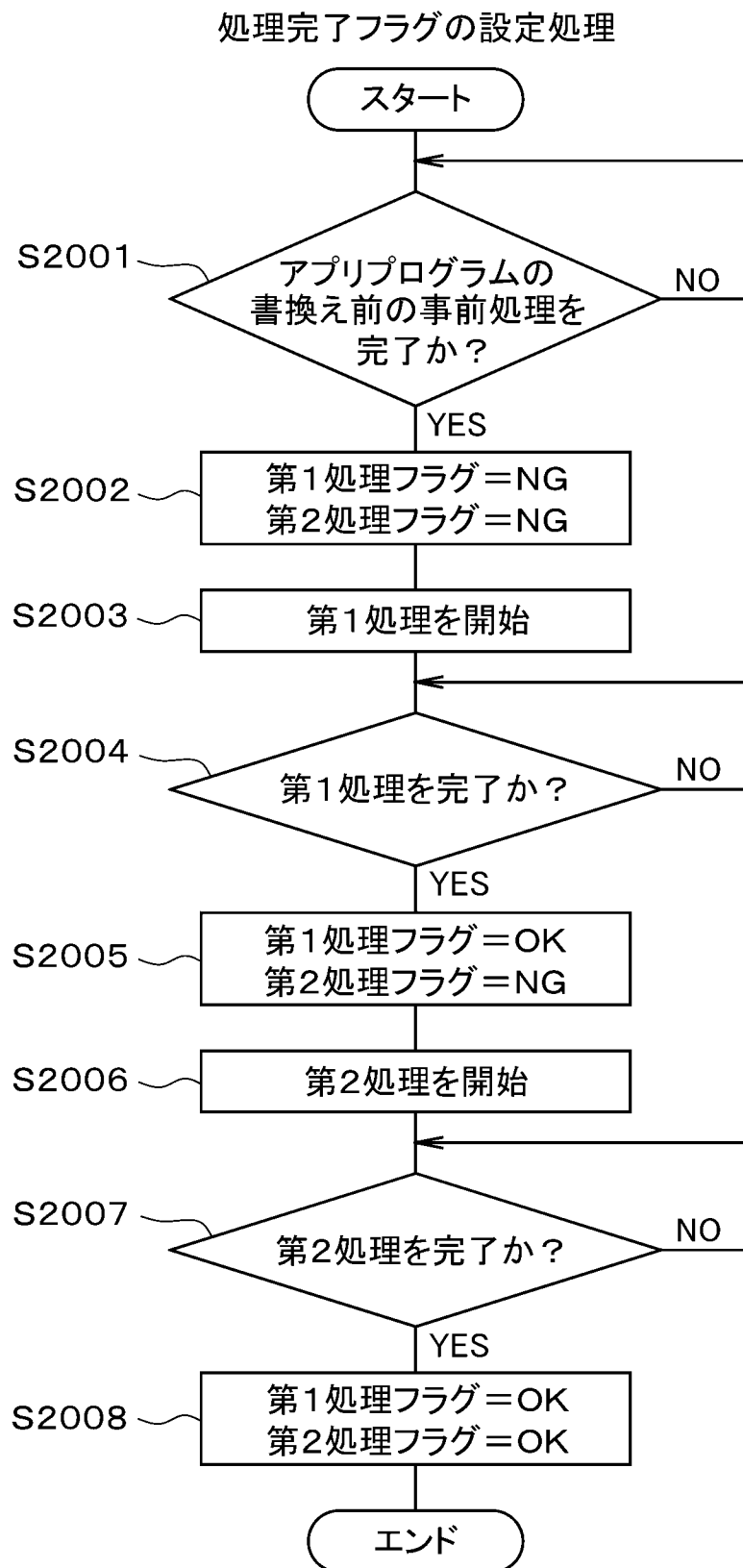


[図171]
Fig. 171

プログラム&データ	
第1処理フラグ	第2処理フラグ
第1の書換えプログラム(メモリ消去、データ書込み)	
第2の書換えプログラム(ベリファイ、改ざんチェック)	
ブートプログラム(起動時のプログラム)	

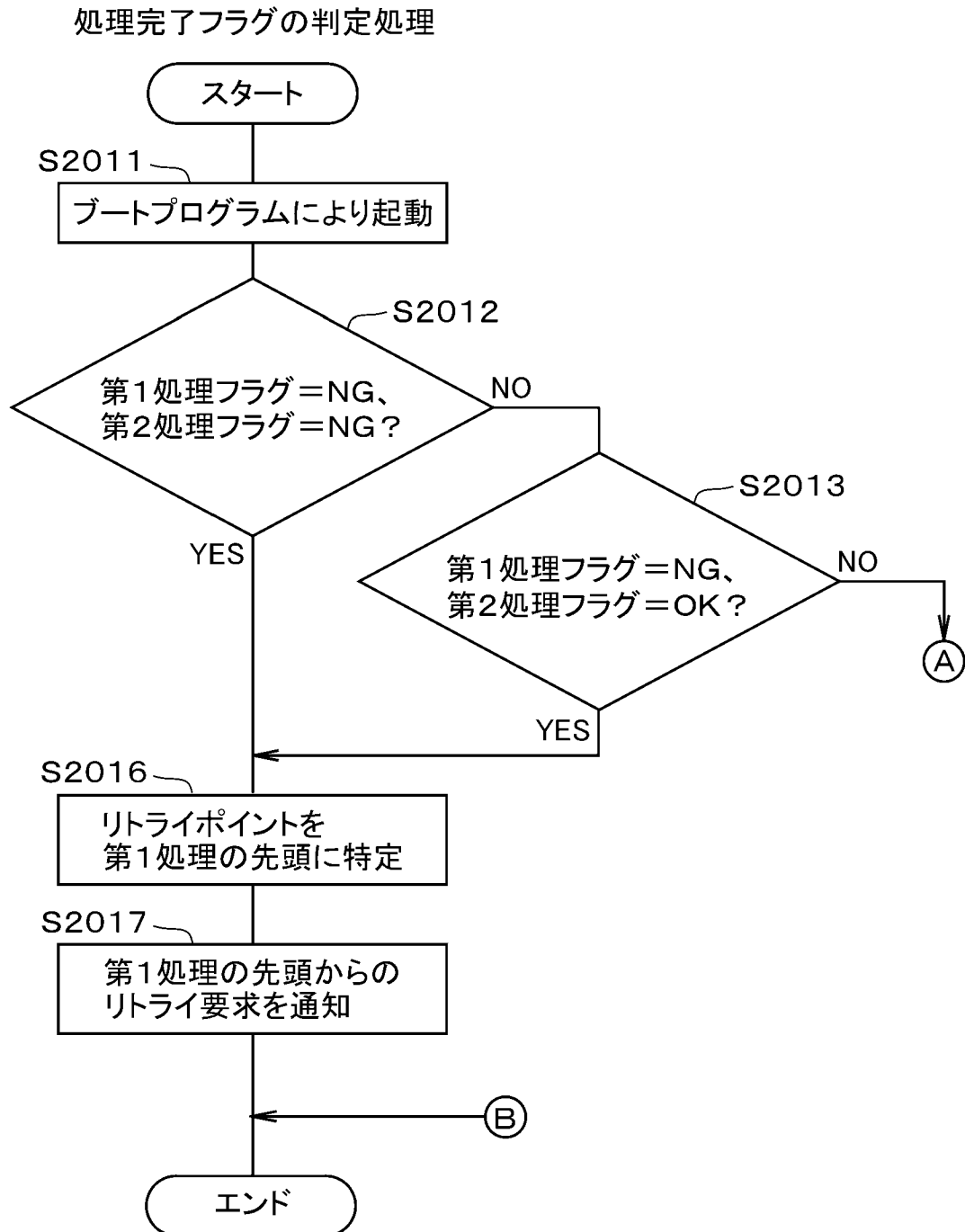
[図172]

Fig. 172



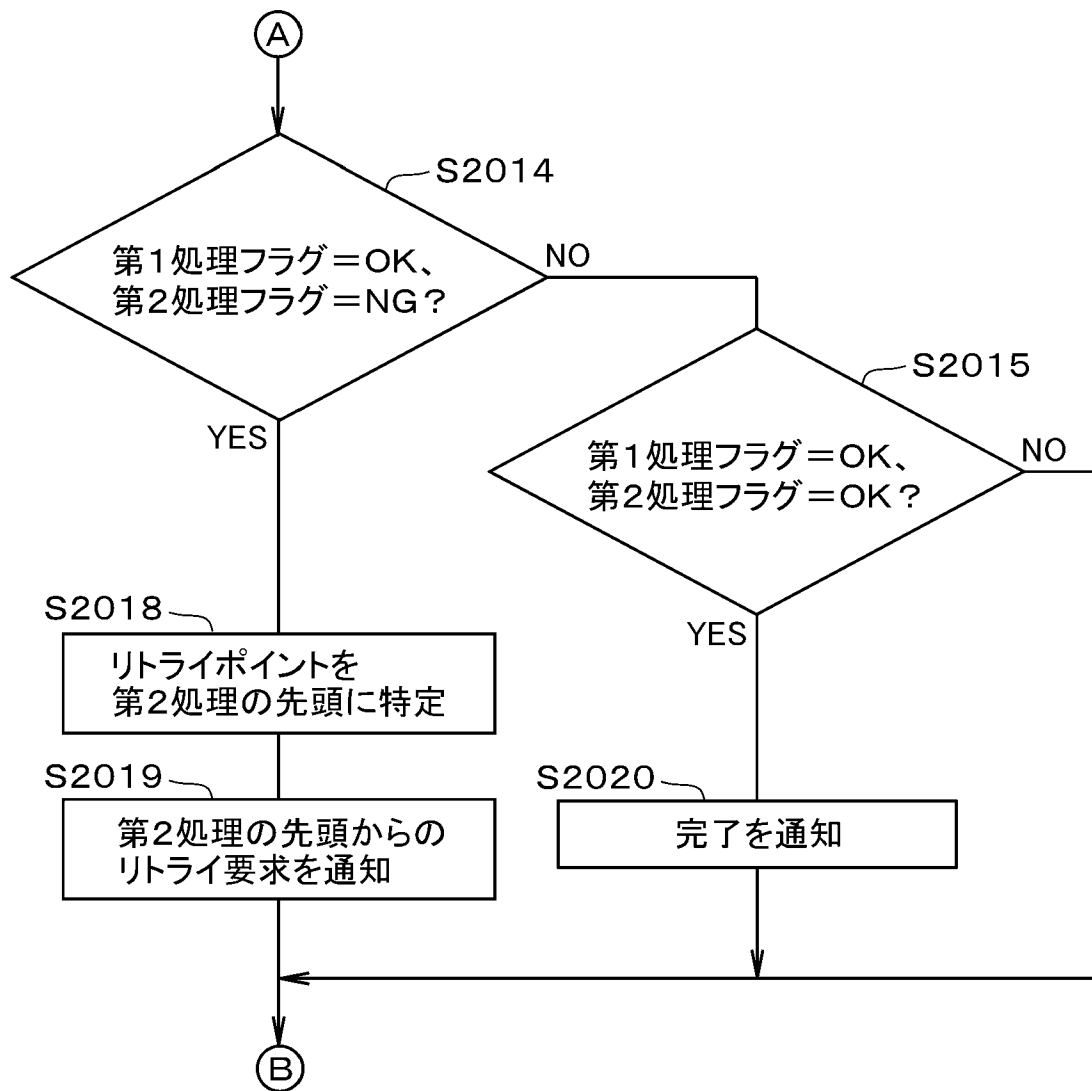
[図173]

Fig. 173

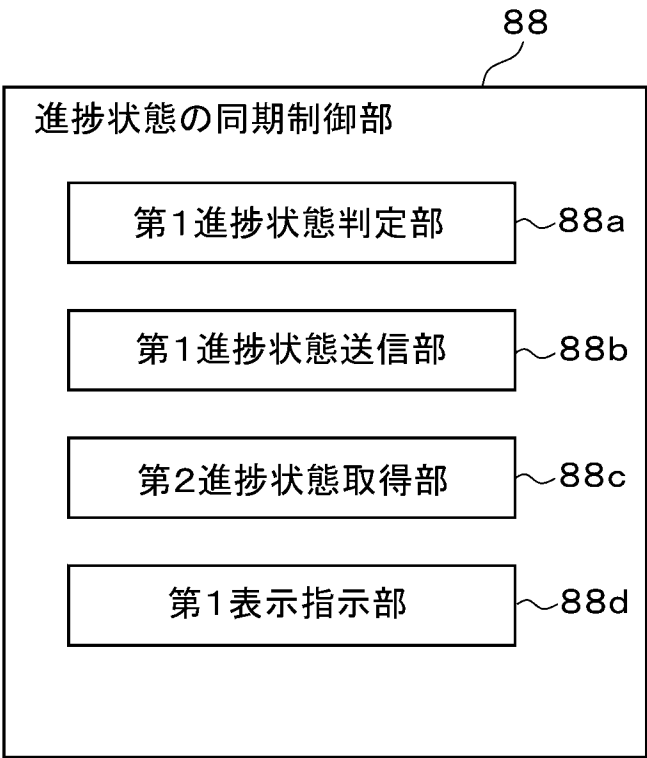


[図174]

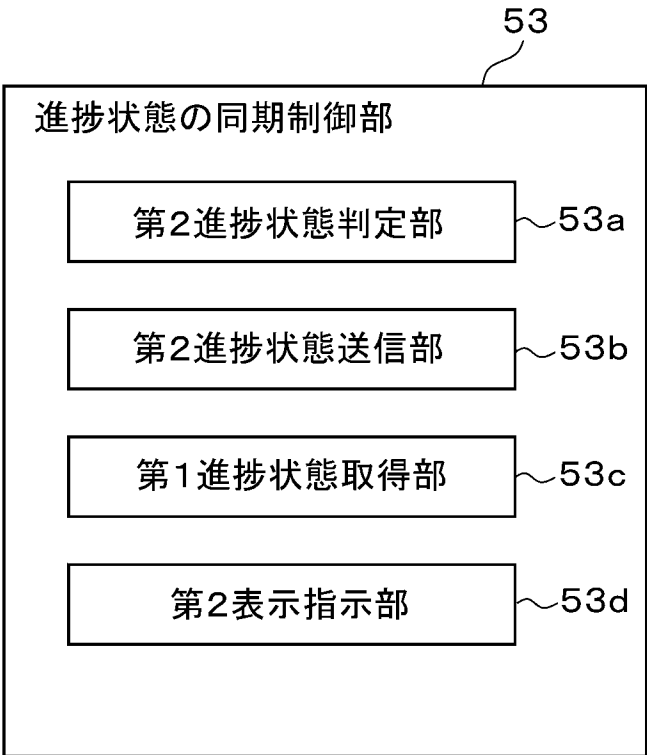
Fig. 174



[図175]
Fig. 175

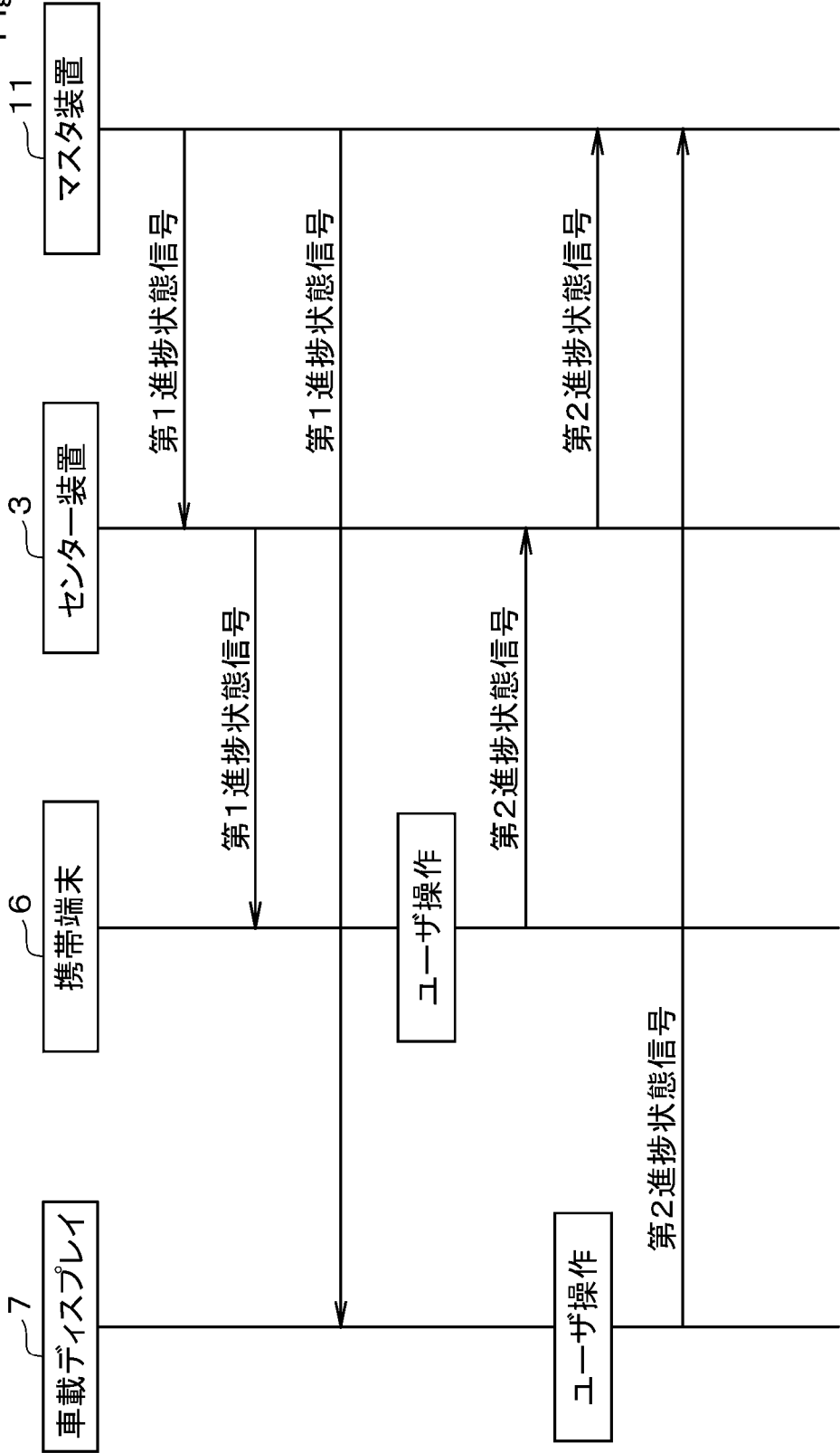


[図176]
Fig. 176



[図177]

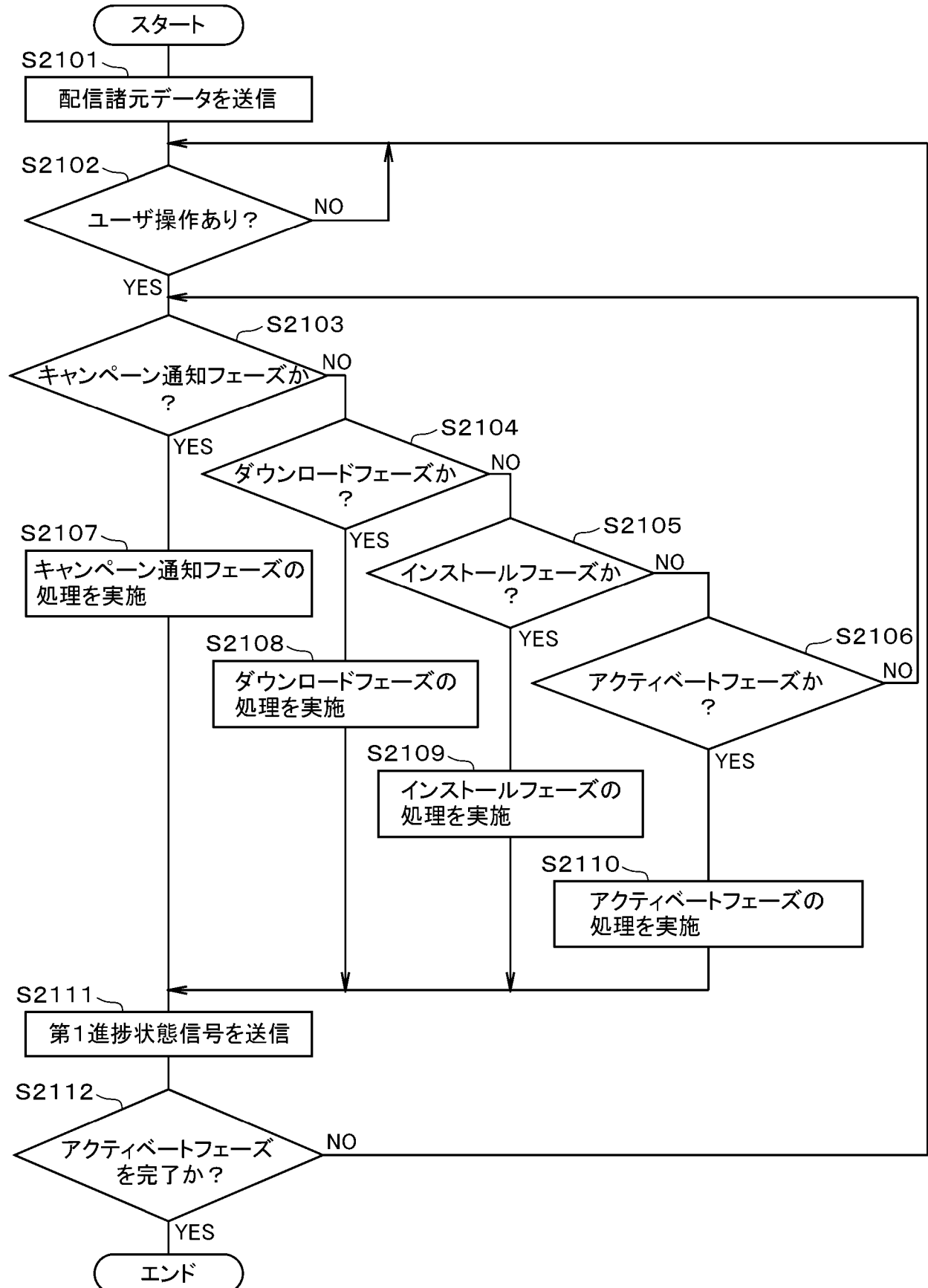
Fig. 177



[図178]

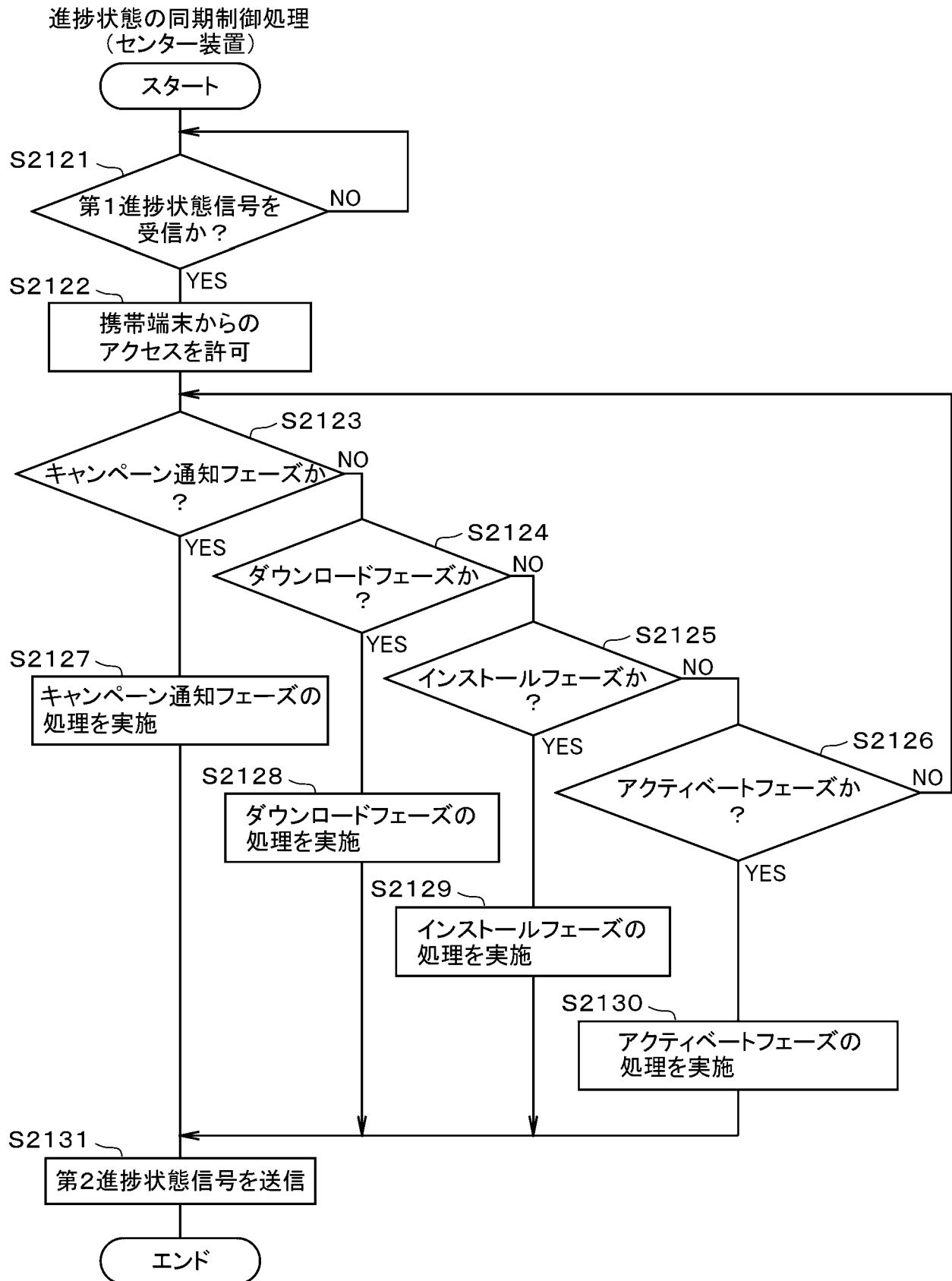
Fig. 178

進捗状態の同期制御処理
(車両用マスタ装置)



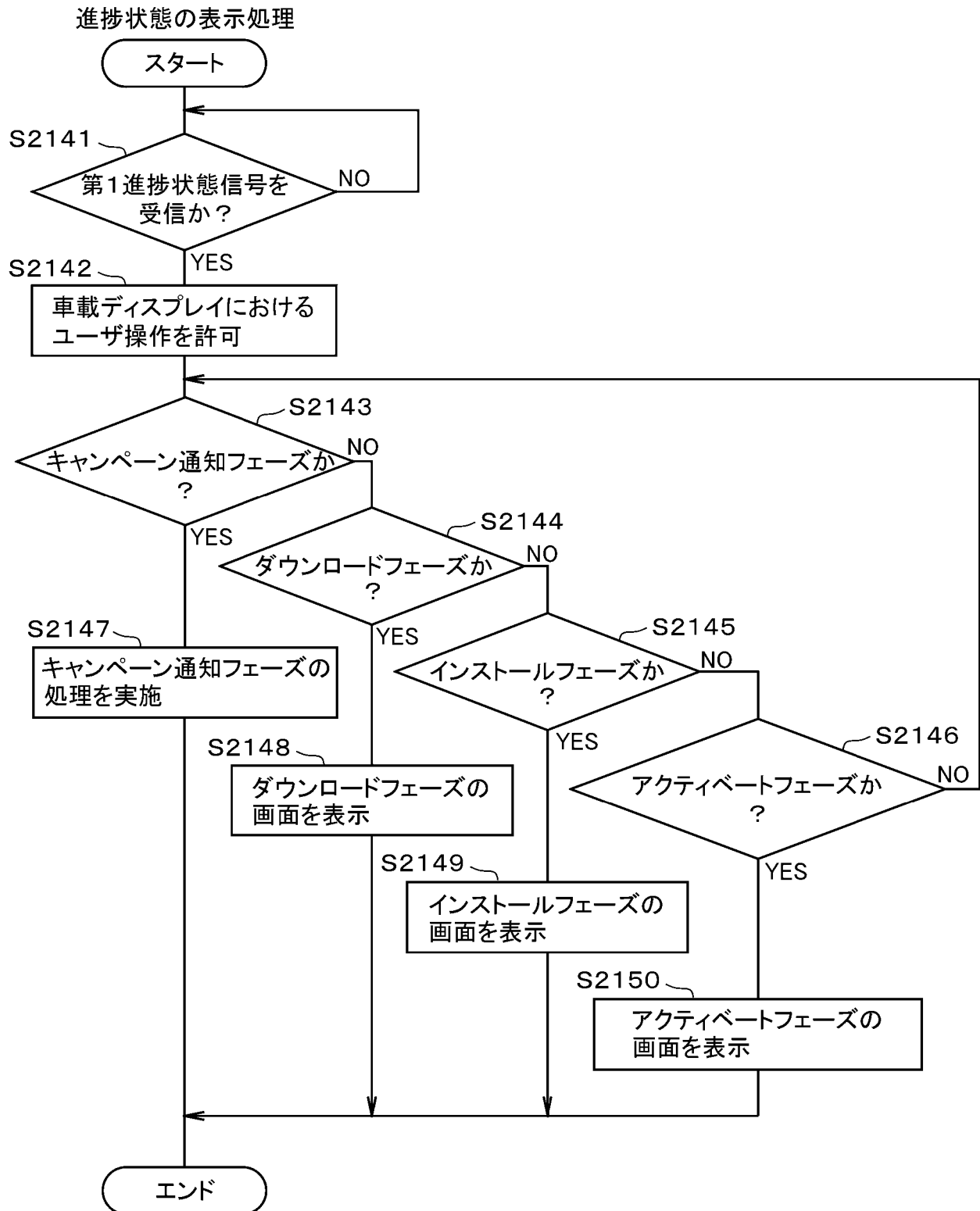
[図179]

Fig. 179



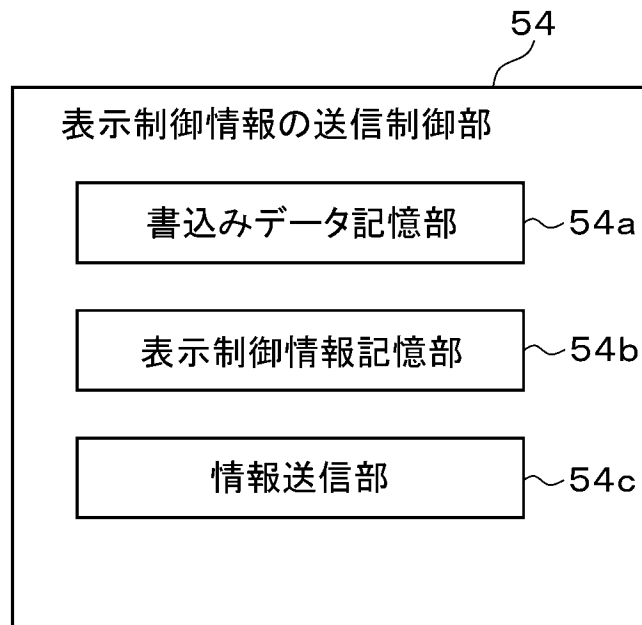
[図180]

Fig. 180



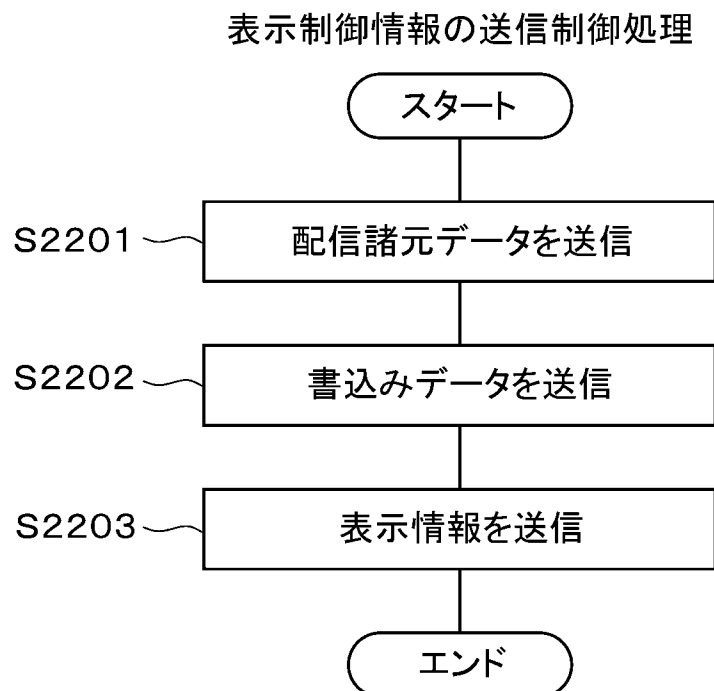
[図181]

Fig. 181



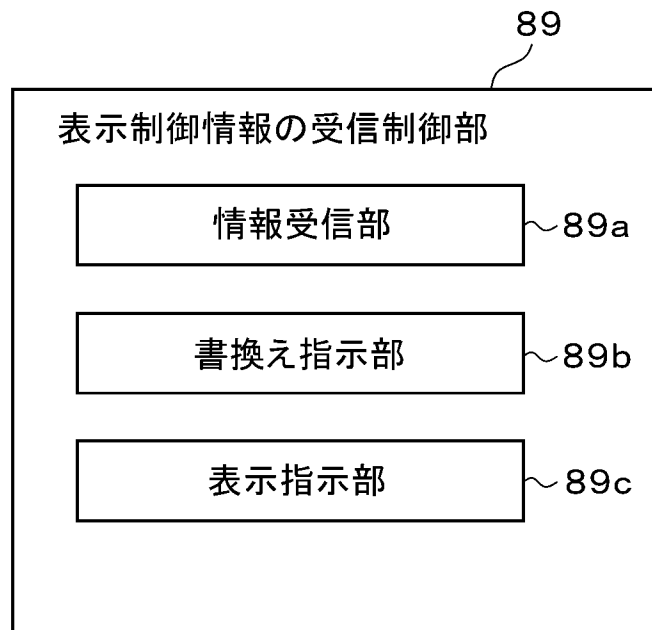
[図182]

Fig. 182



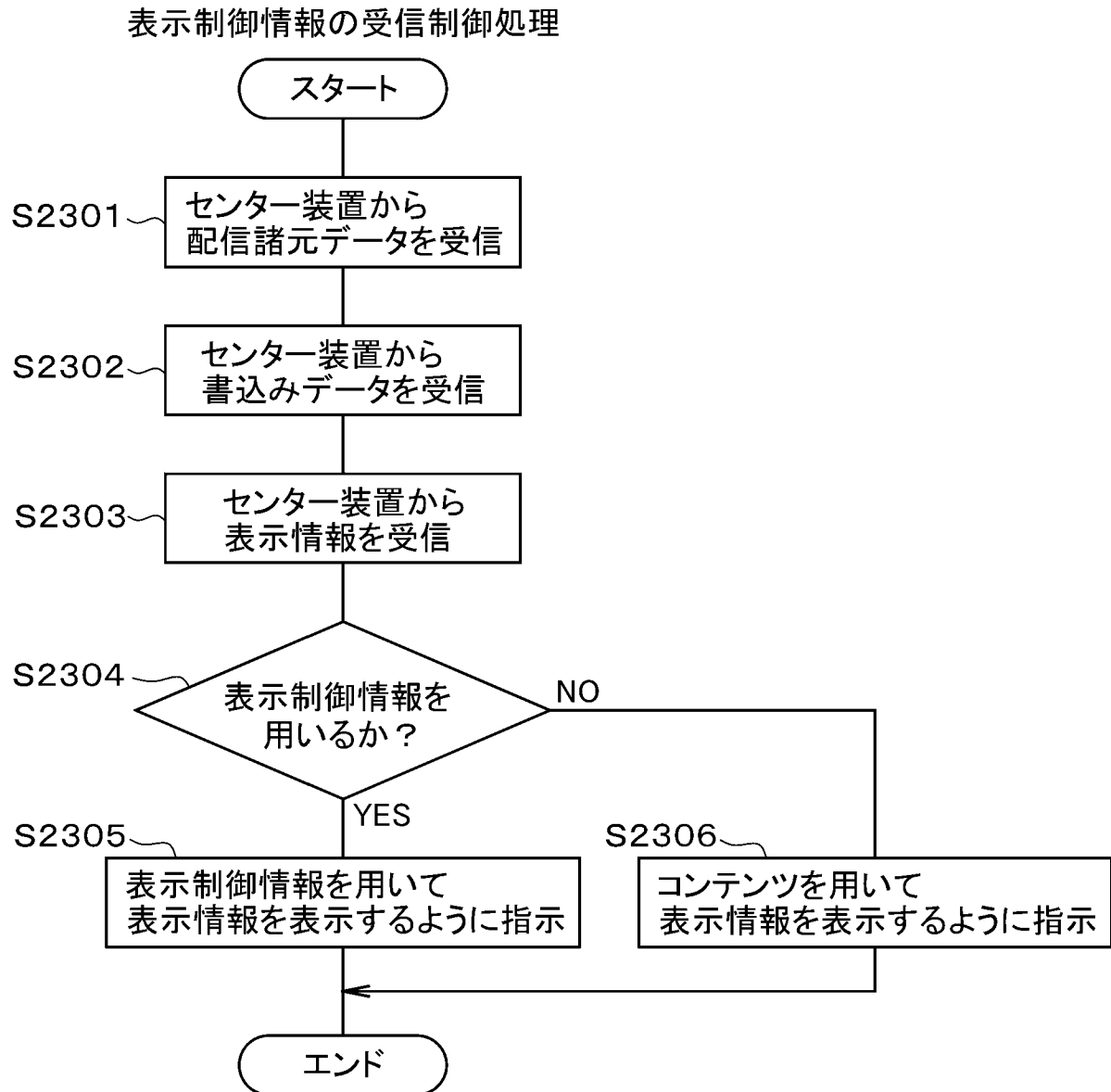
[図183]

Fig. 183

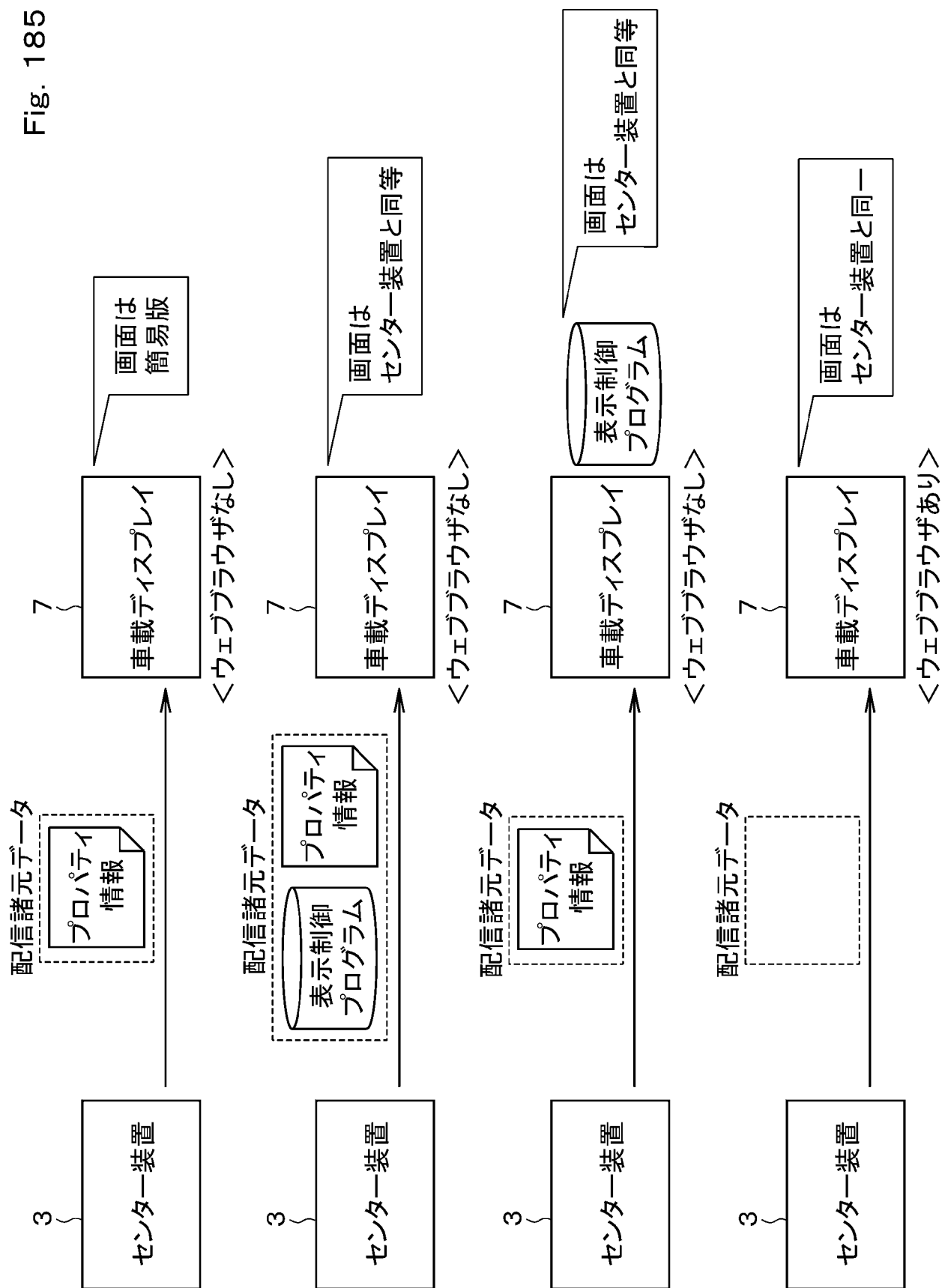


[図184]

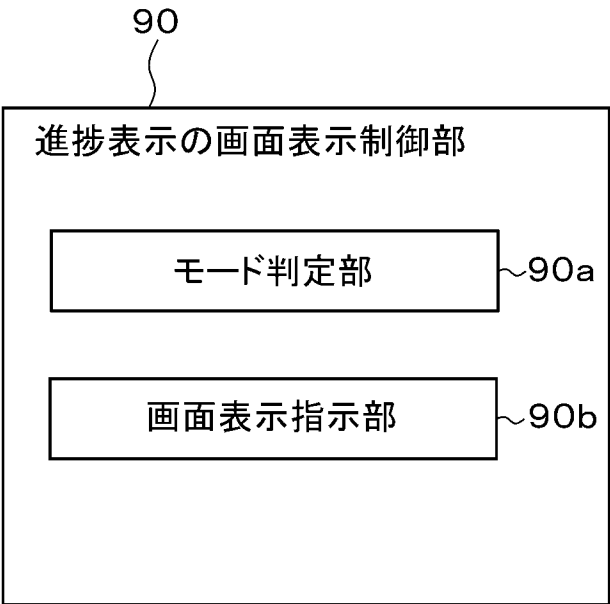
Fig. 184



[図185]



[図186]
Fig. 186



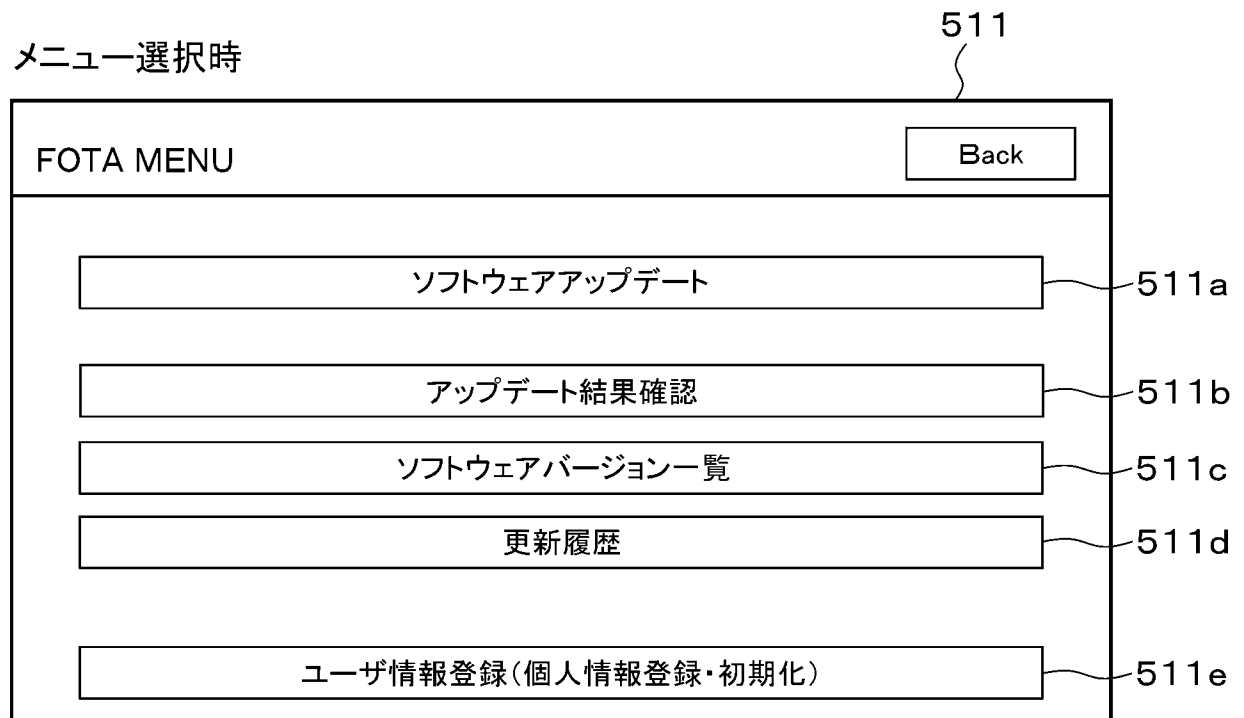
[図187]
Fig. 187

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	

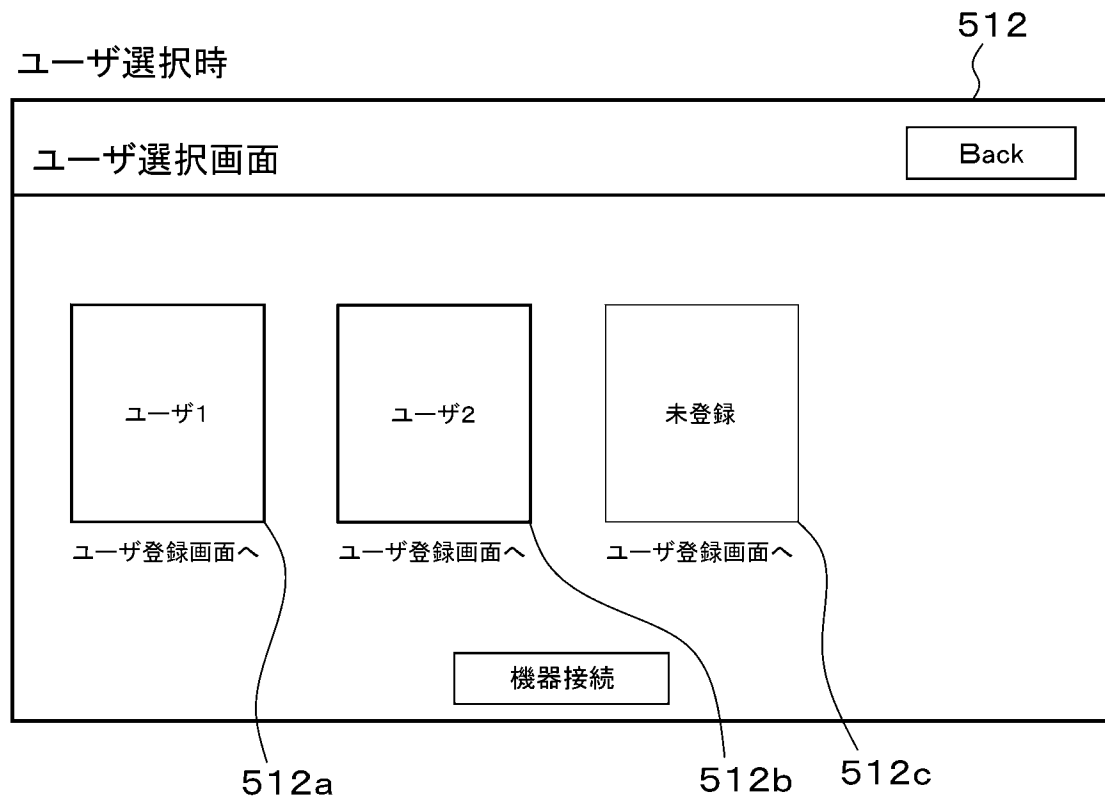
[図188]

Fig. 188

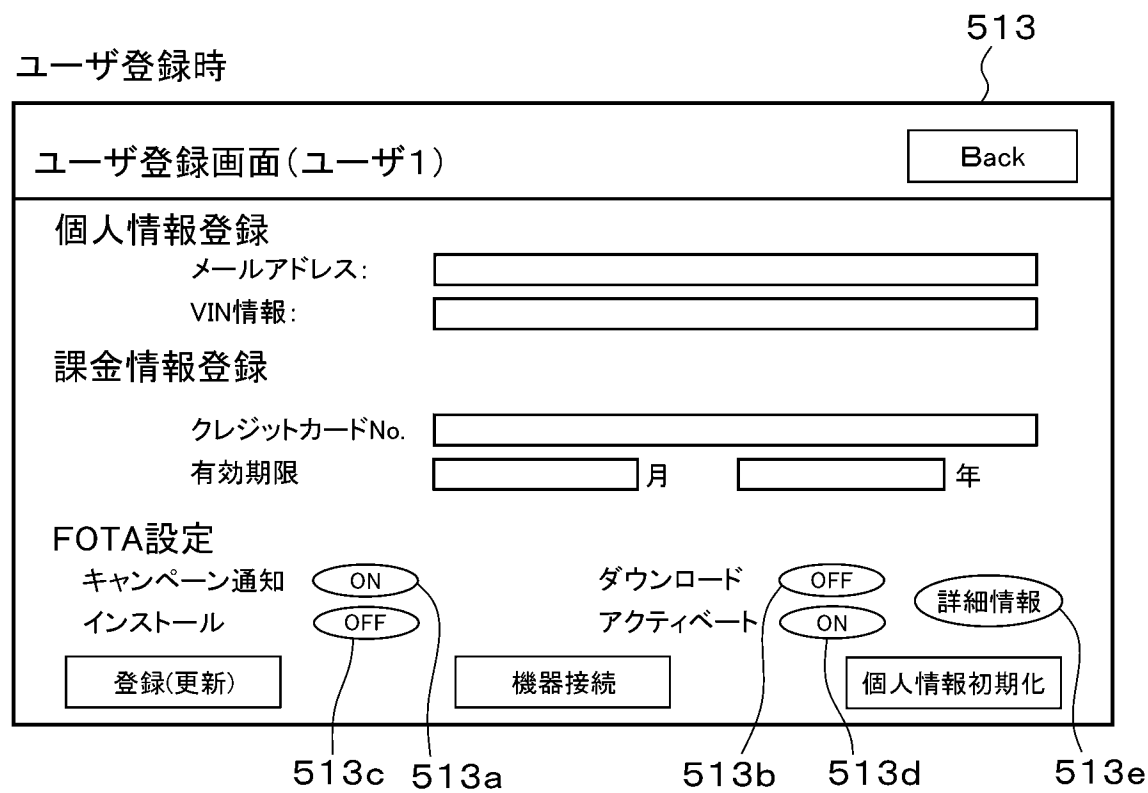


[図189]

Fig. 189

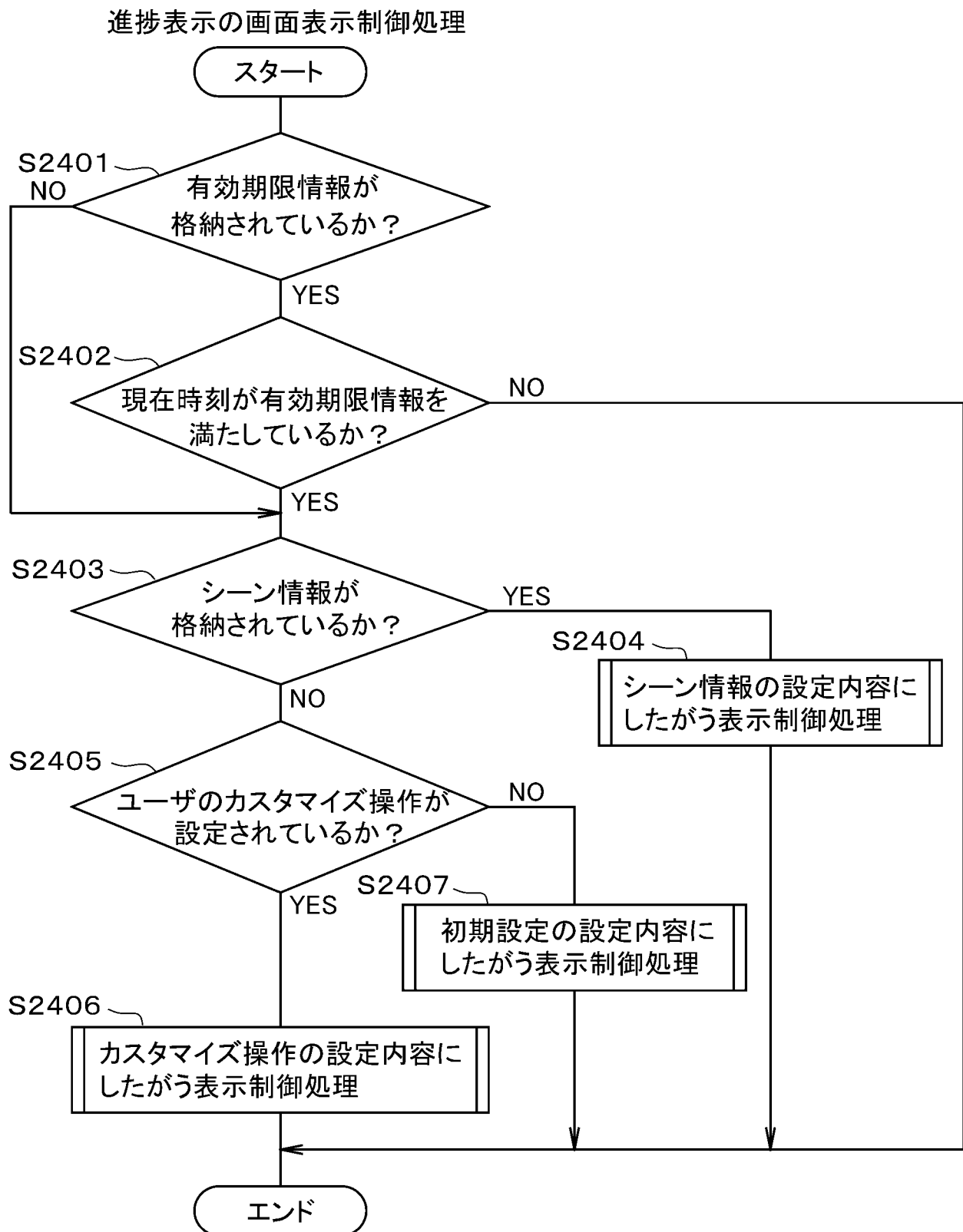


[図190]
Fig. 190



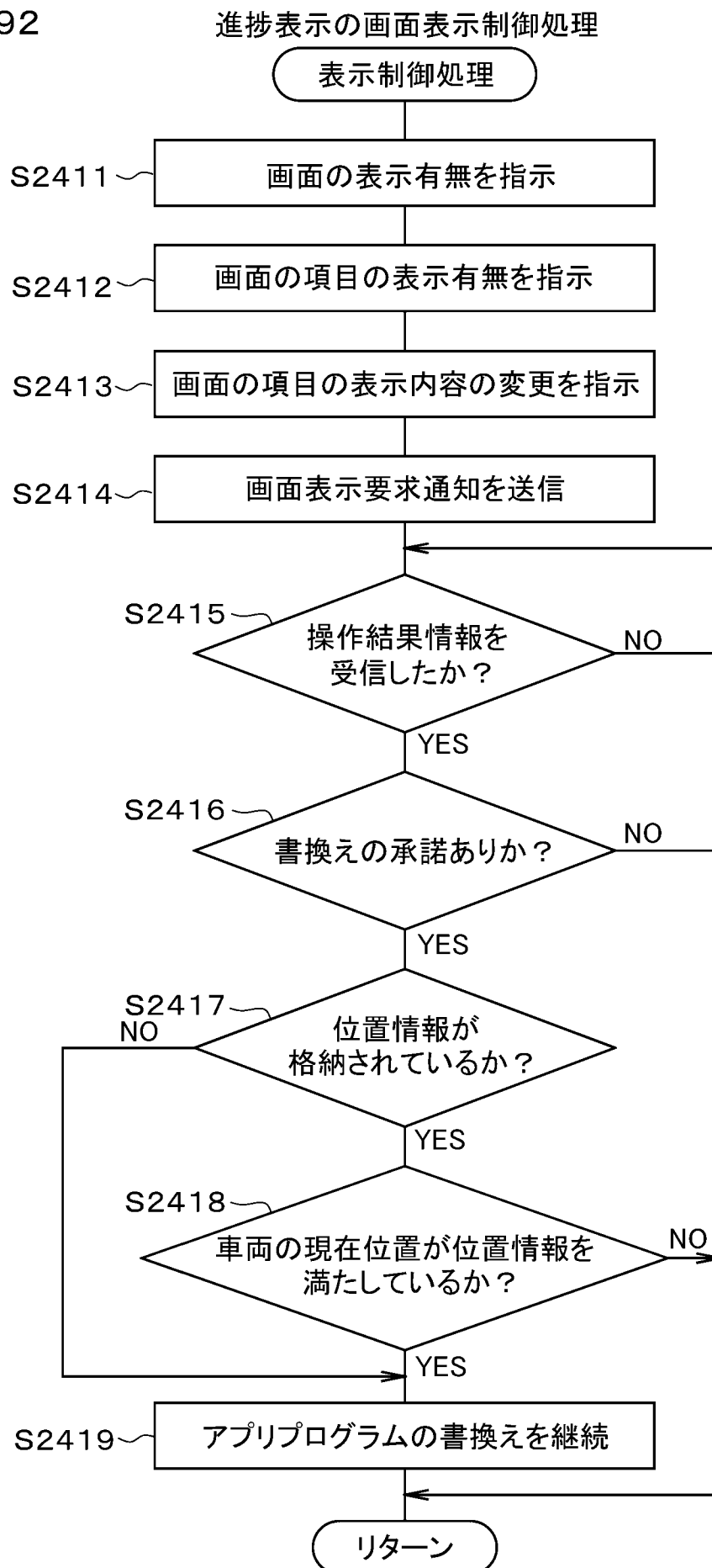
[図191]

Fig. 191

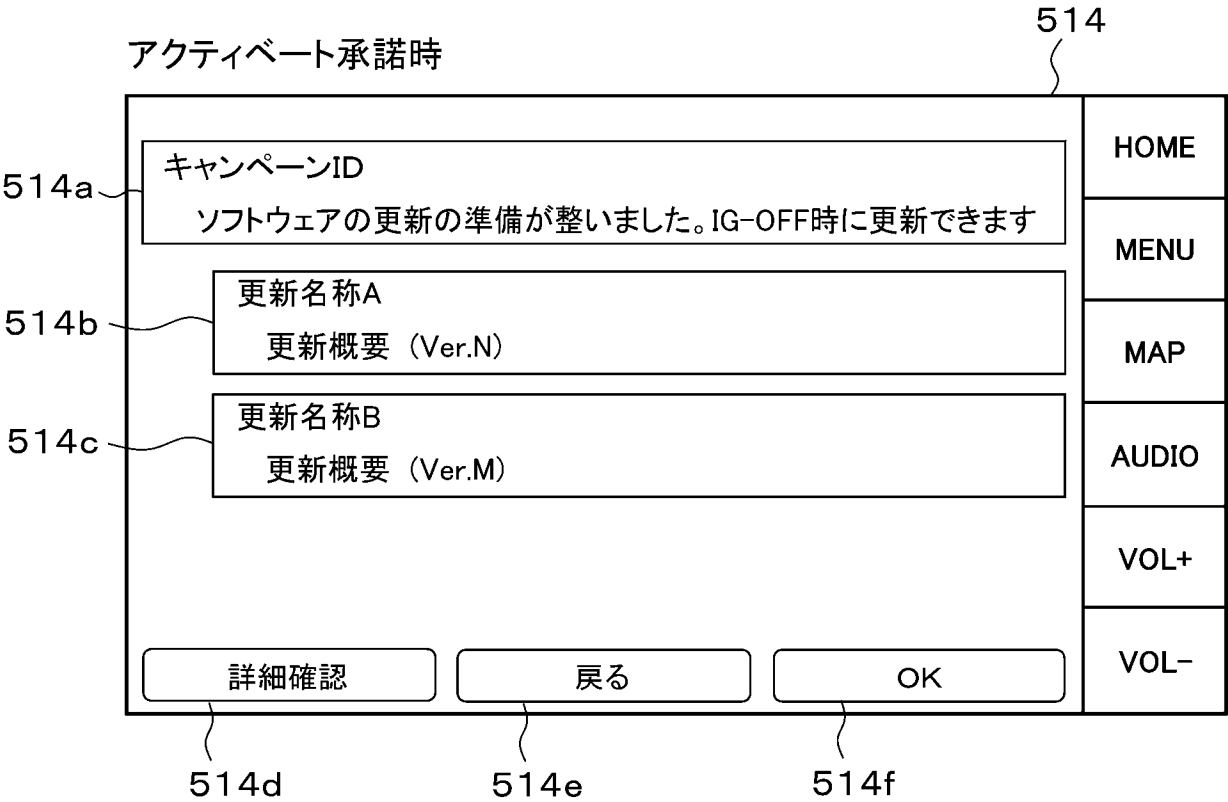


[図192]

Fig. 192



[図194]
Fig. 194



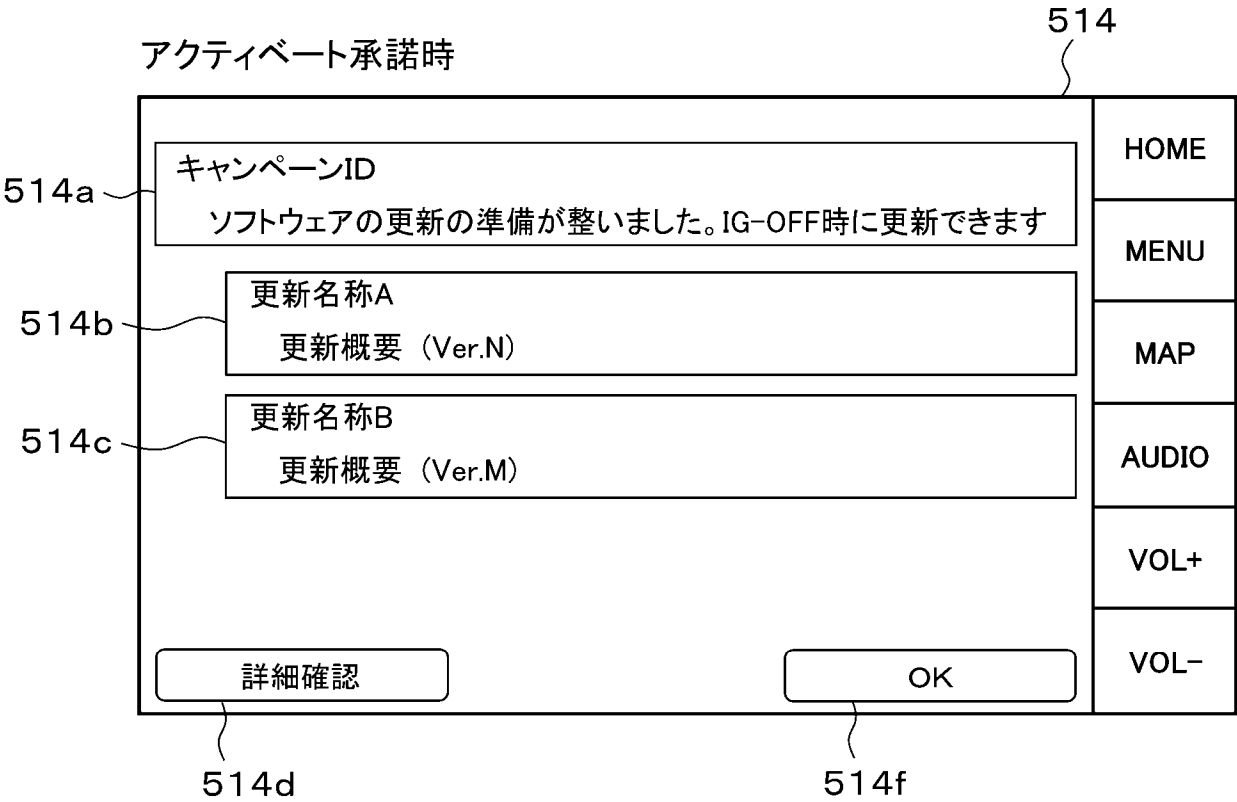
[図195]
Fig. 195

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

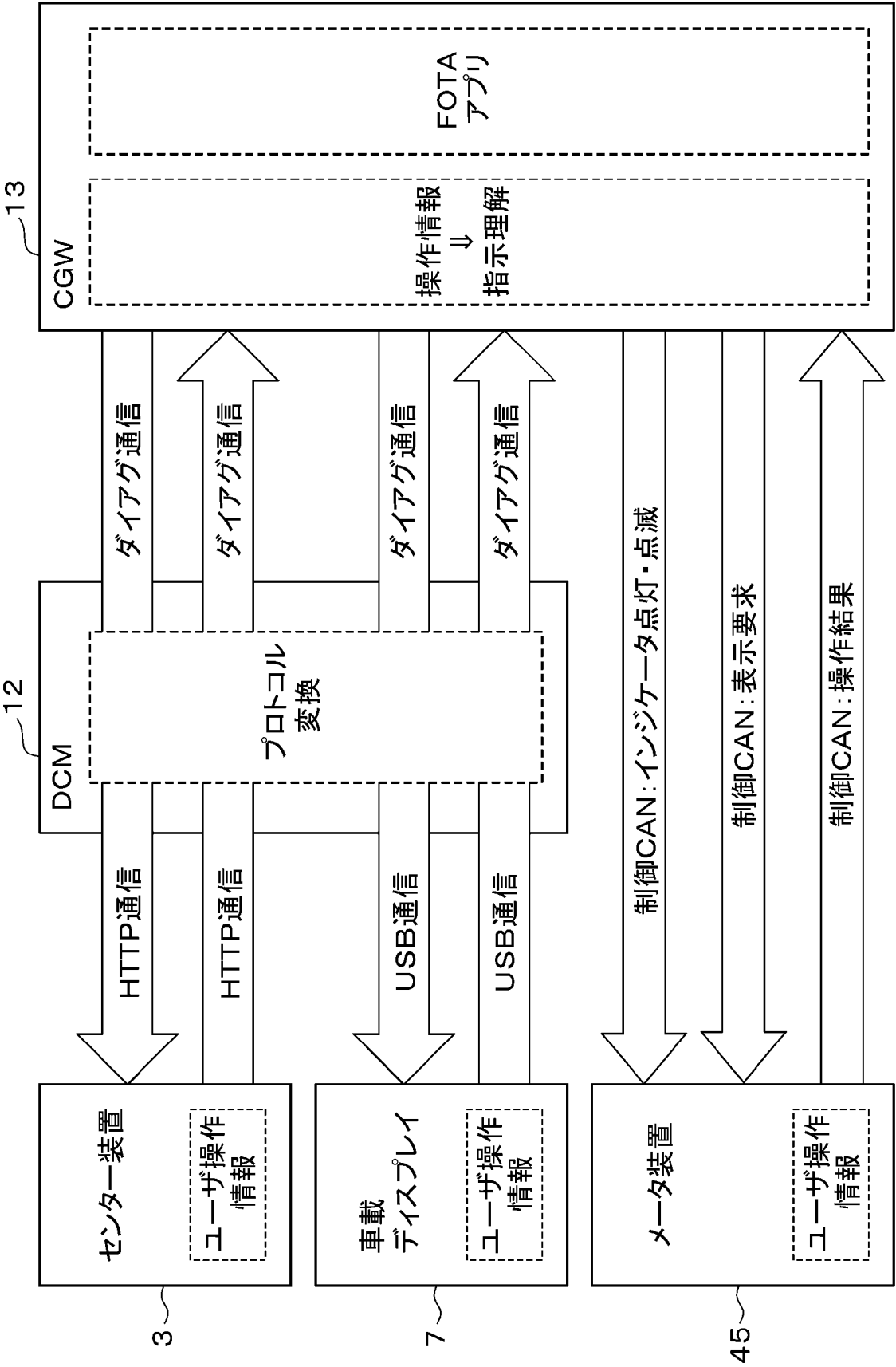
項目	表示／非表示
キャンペーン…	表示
更新名称A…	表示
更新名称B…	表示
詳細確認	表示
戻る	非表示
OK	表示

[図197]
Fig. 197



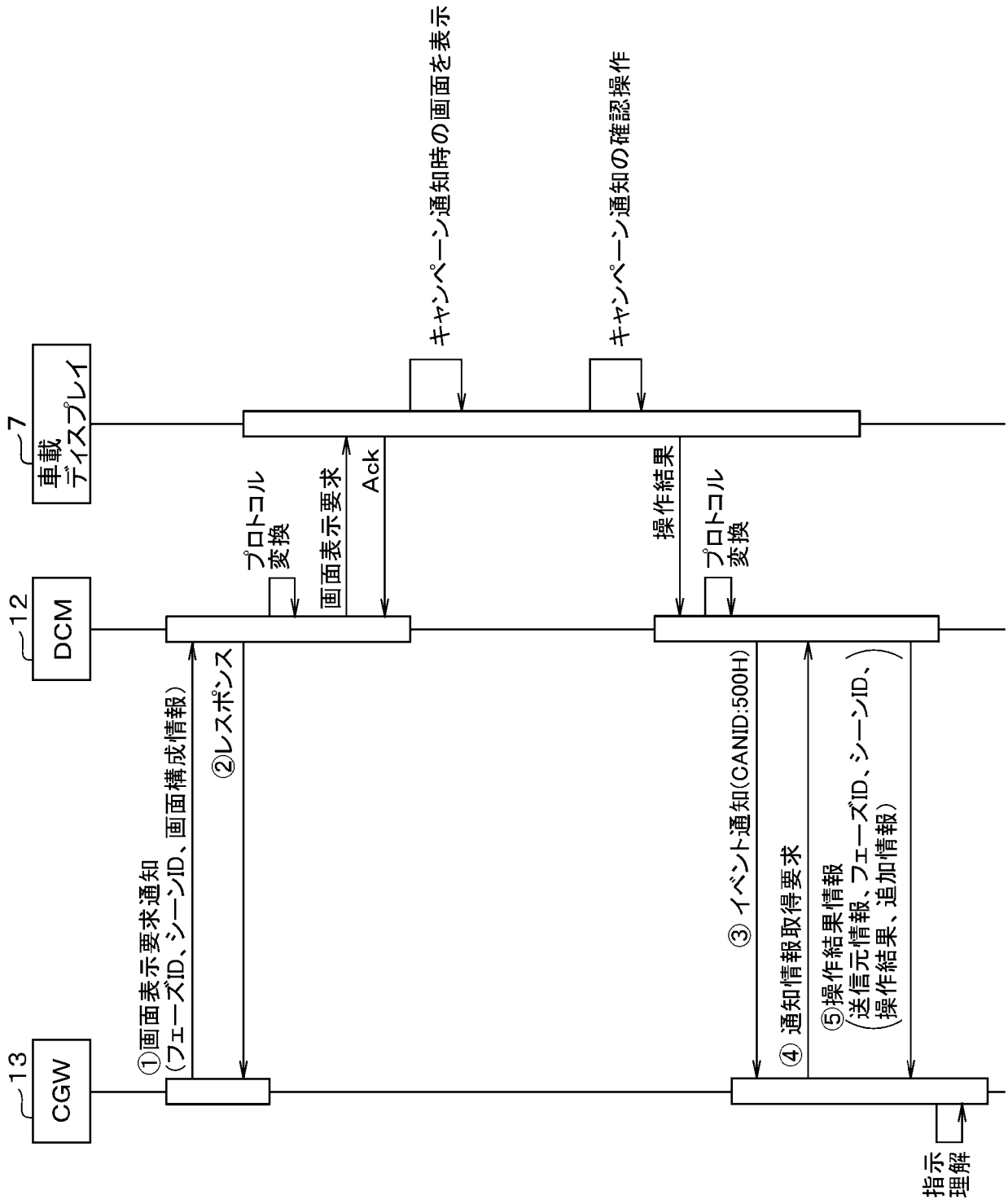
[図198]

Fig. 198



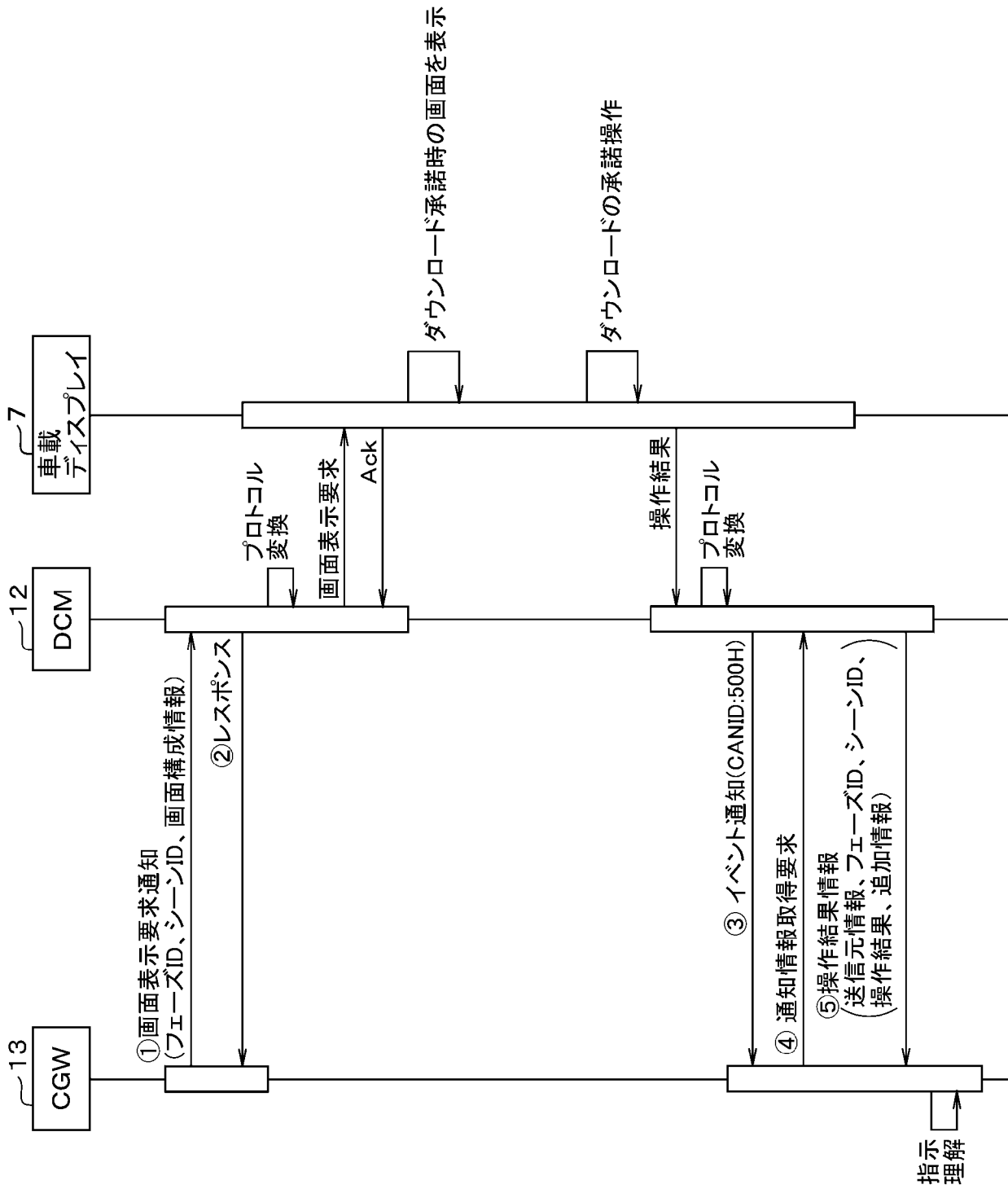
[図199]

Fig. 199



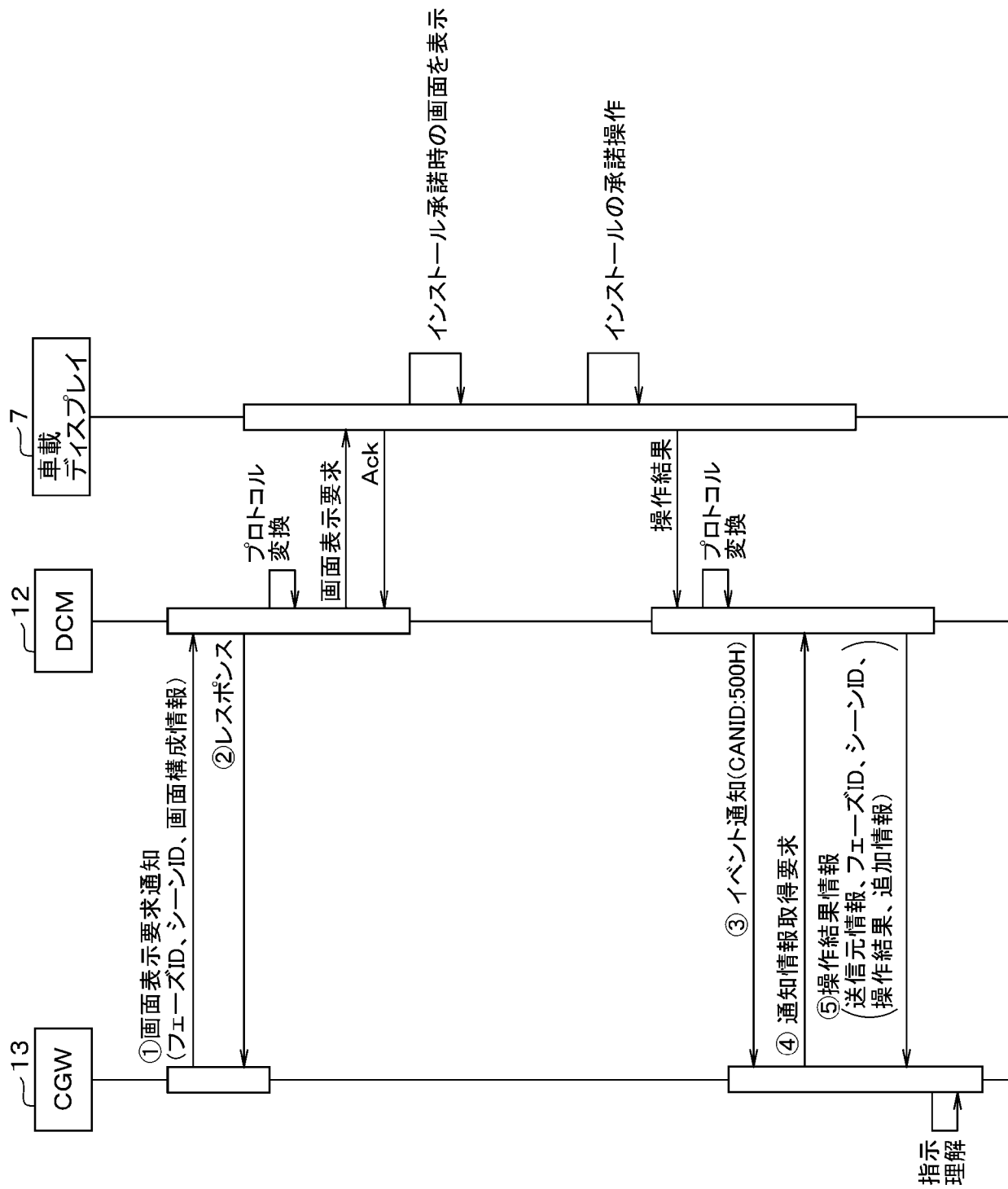
[図200]

Fig. 200



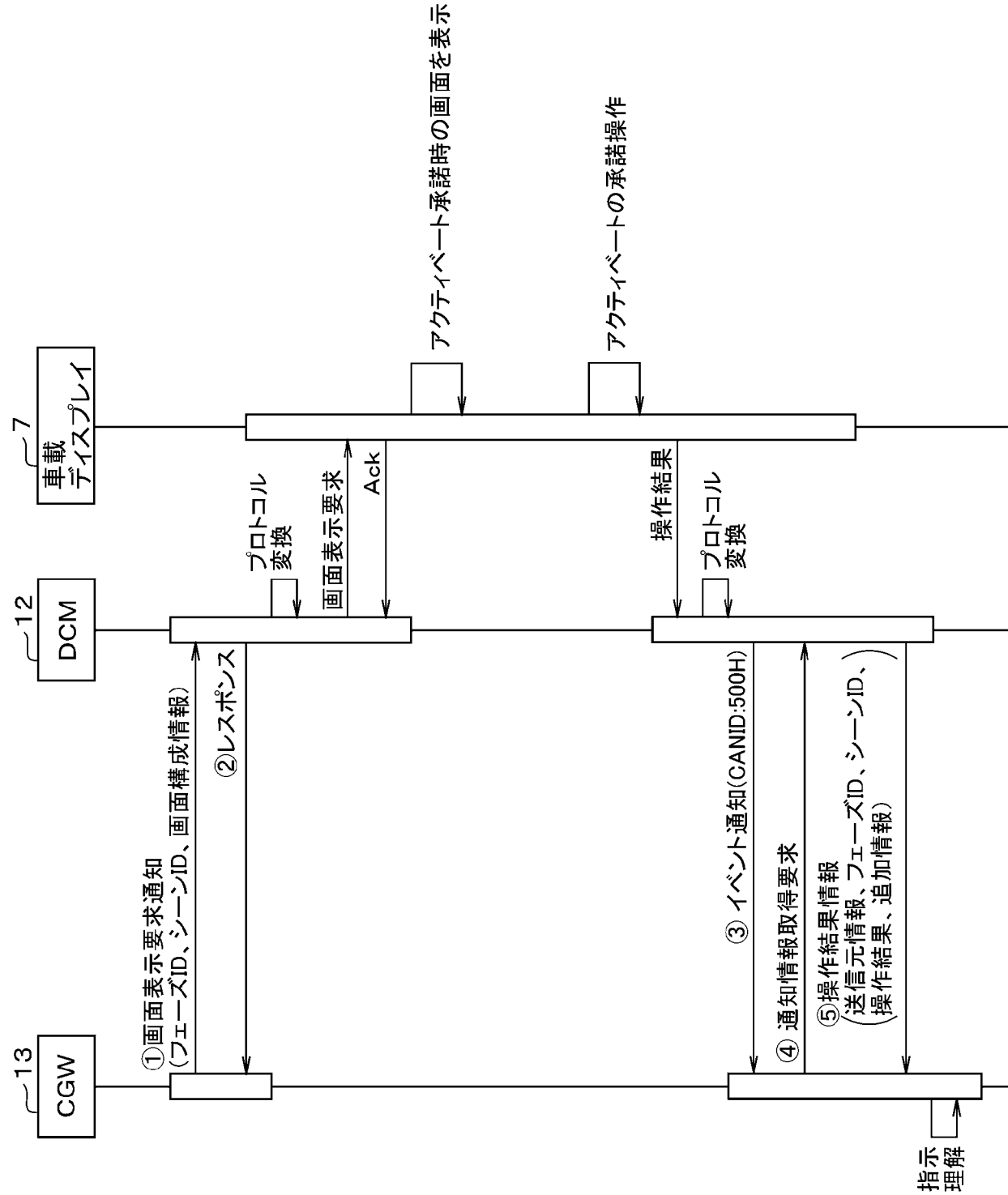
[図201]

Fig. 201



[図202]

Fig. 202

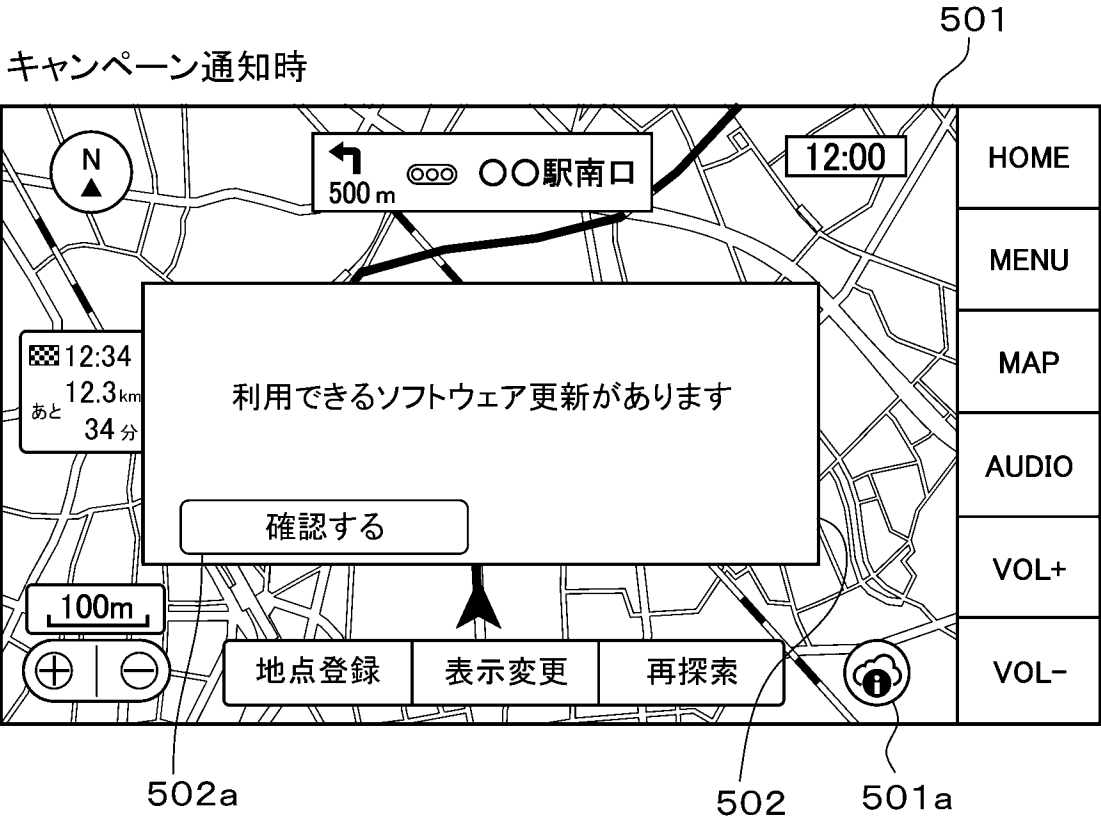


[図203]

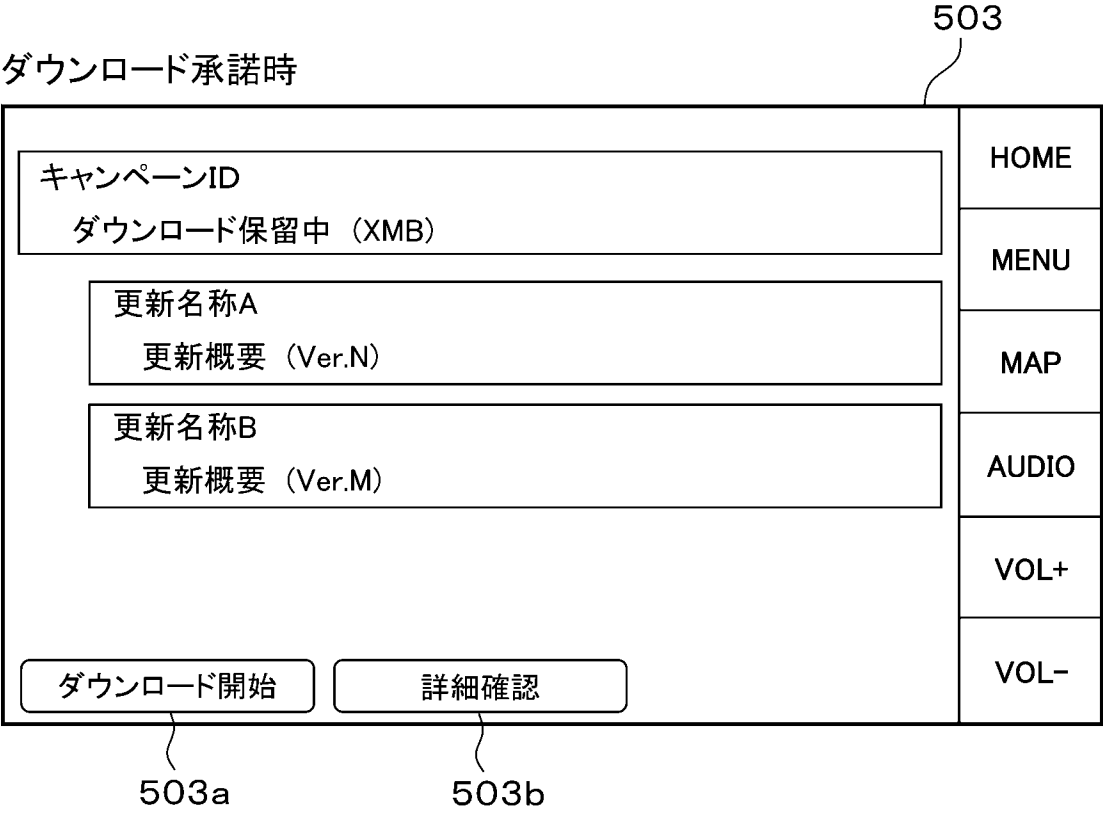
Fig. 203

	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	省略
ダウンロード	承諾	省略	図205, 206	
	実行中		図36, 207	
インストール	承諾		図40, 208, 209	
	実行中		図41, 42	
アクティベート	承諾		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

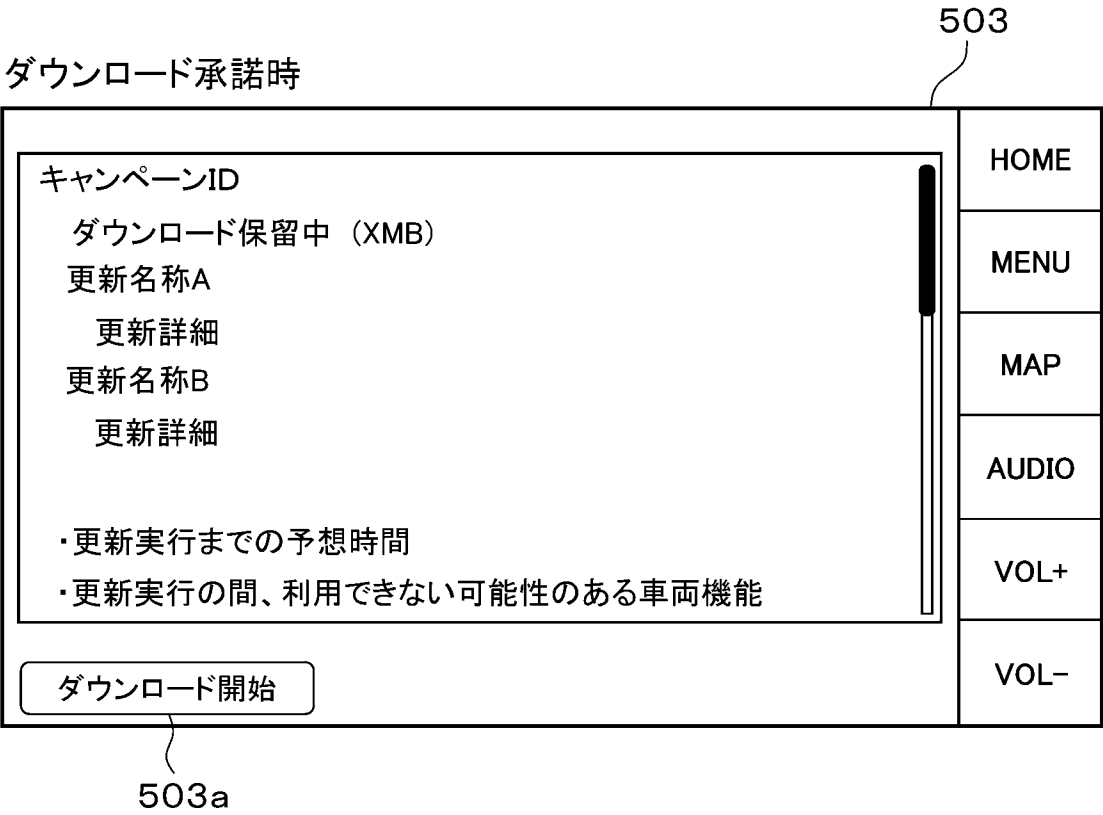
[図204]
Fig. 204



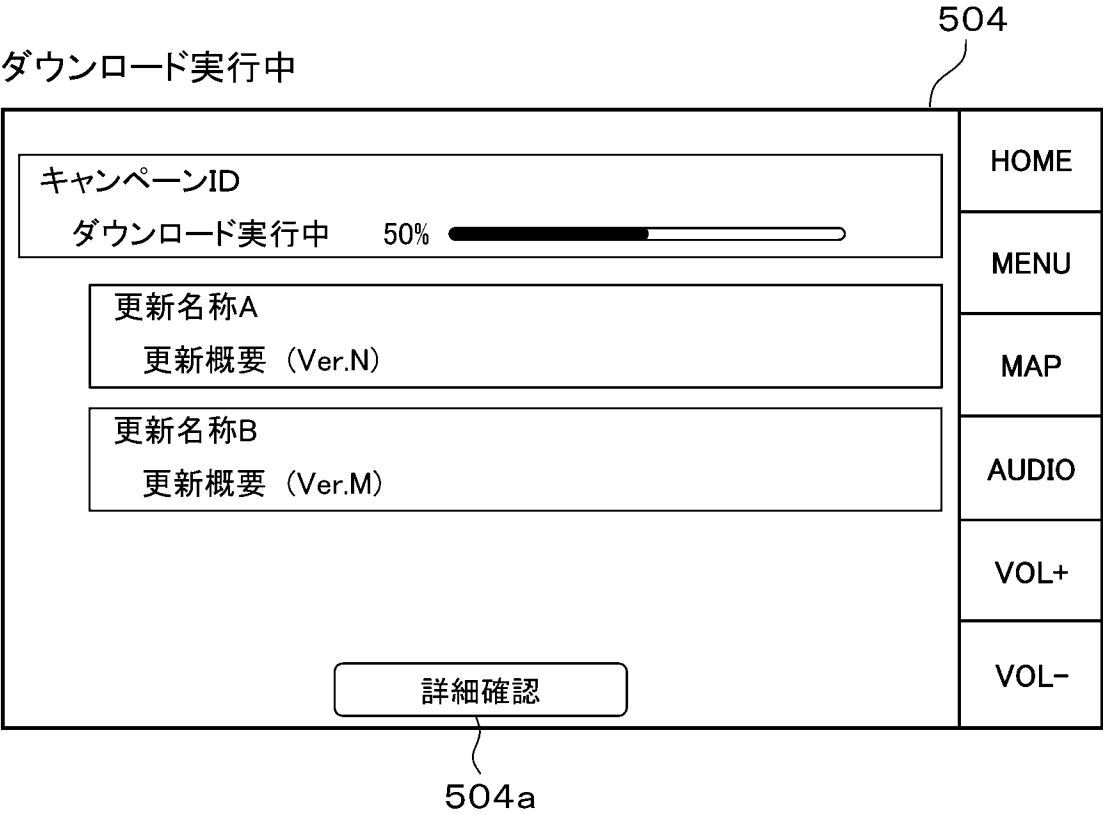
[図205]
Fig. 205



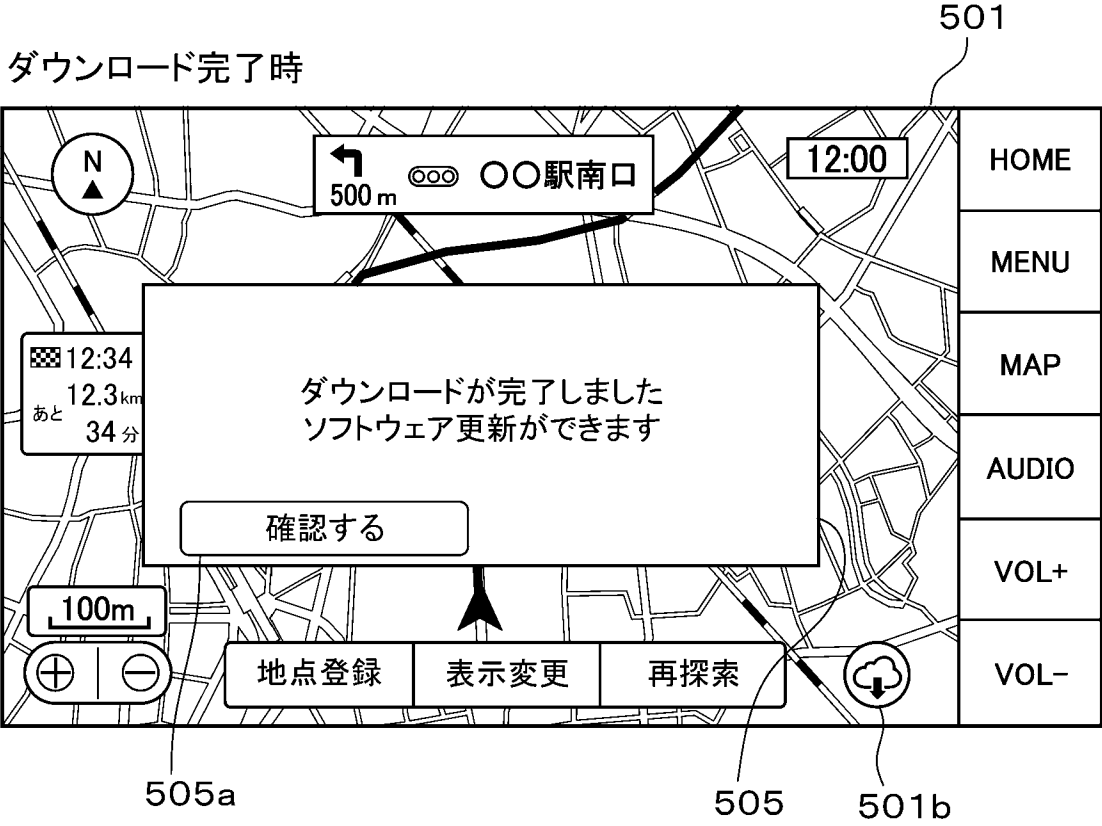
[図206]
Fig. 206



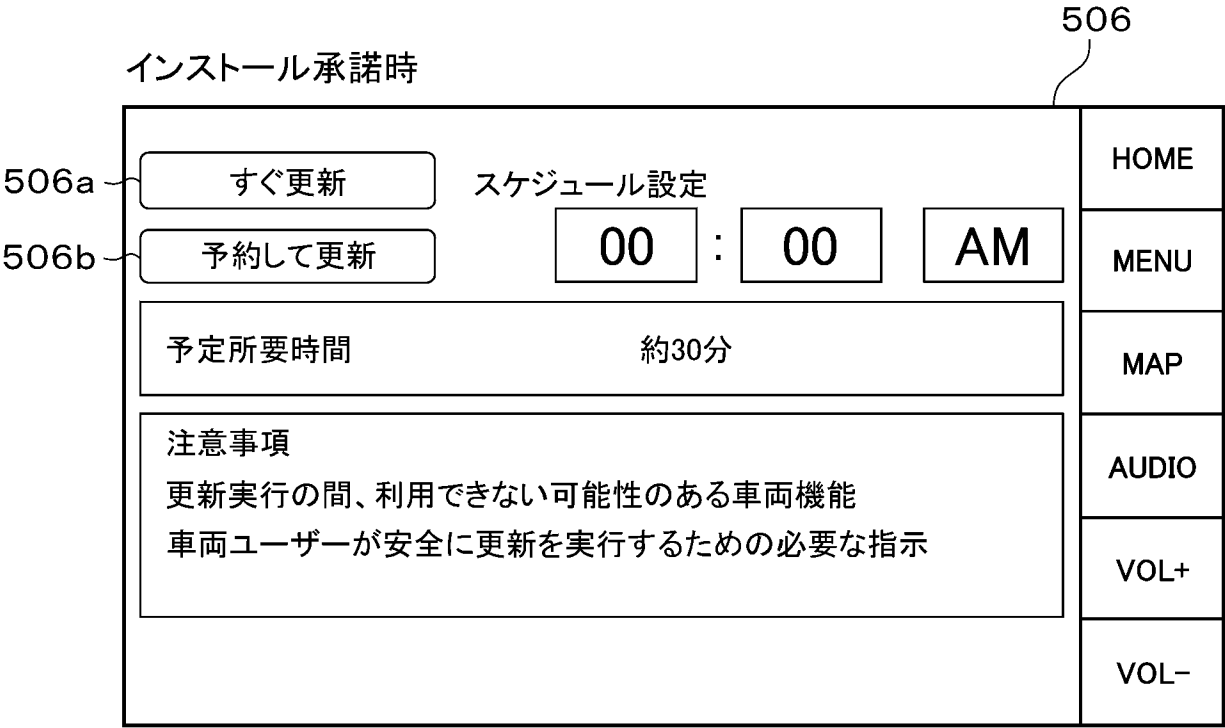
[図207]
Fig. 207



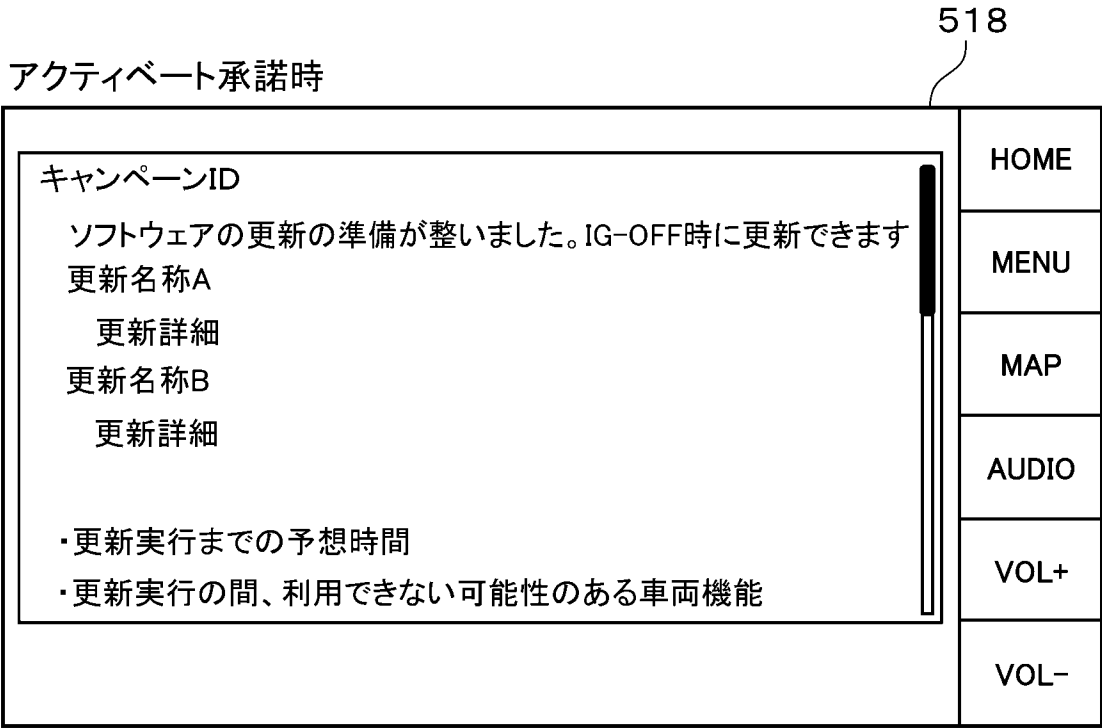
[図208]
Fig. 208



[図209]
Fig. 209

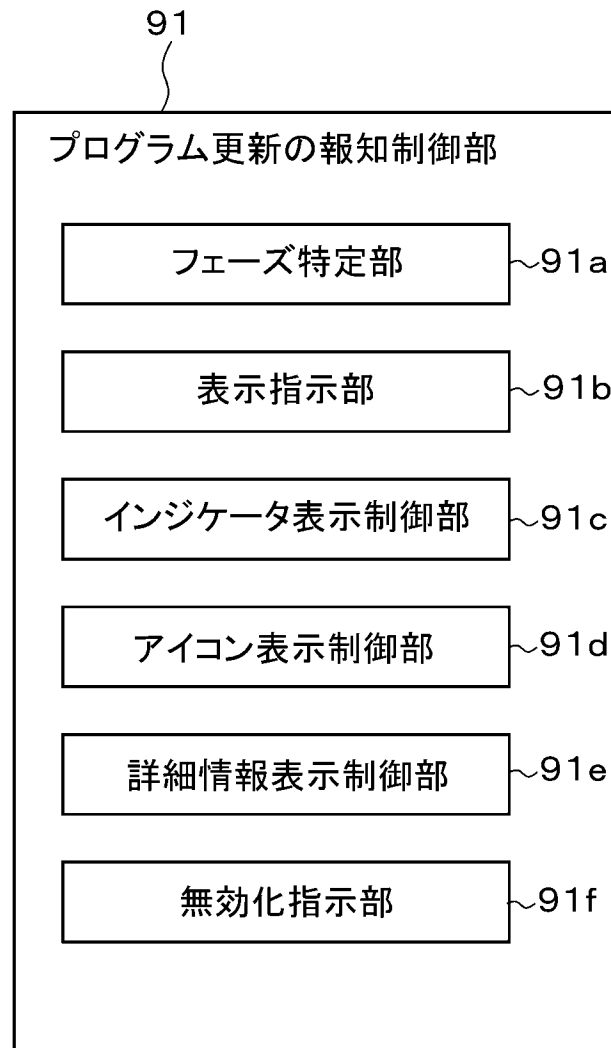


[図210]
Fig. 210



[図211]

Fig. 211



[図212]

Fig. 212

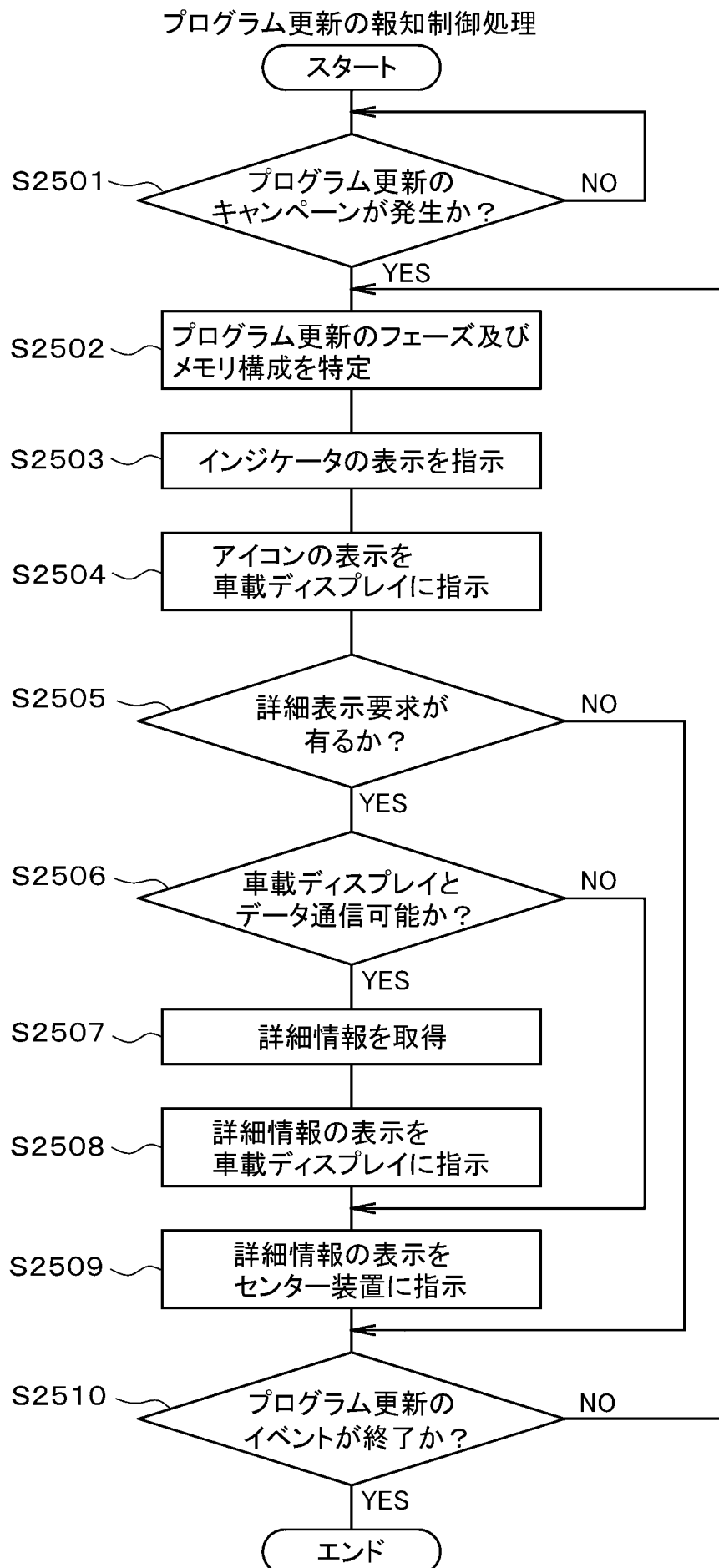
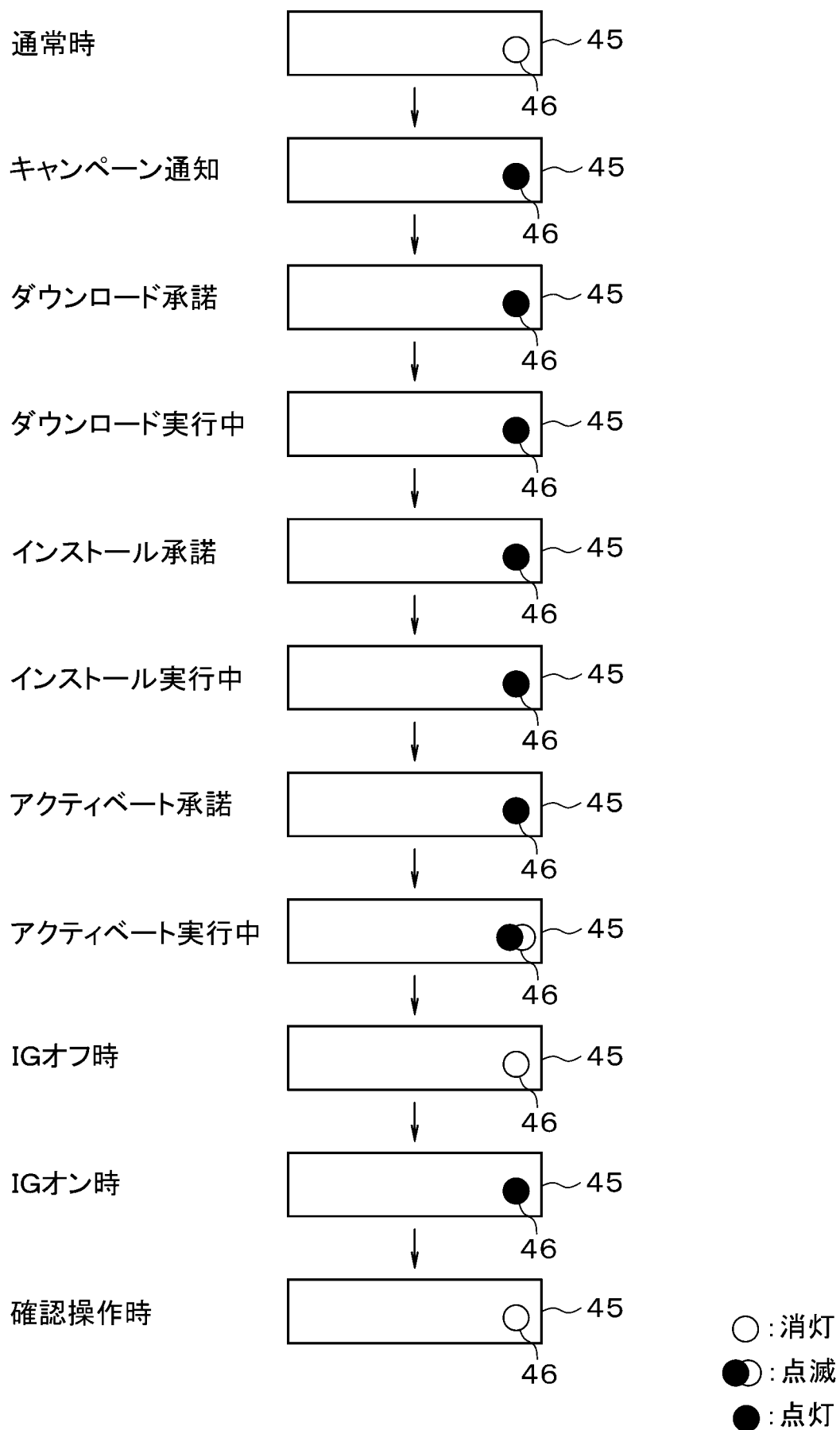


Fig. 213

[図213]

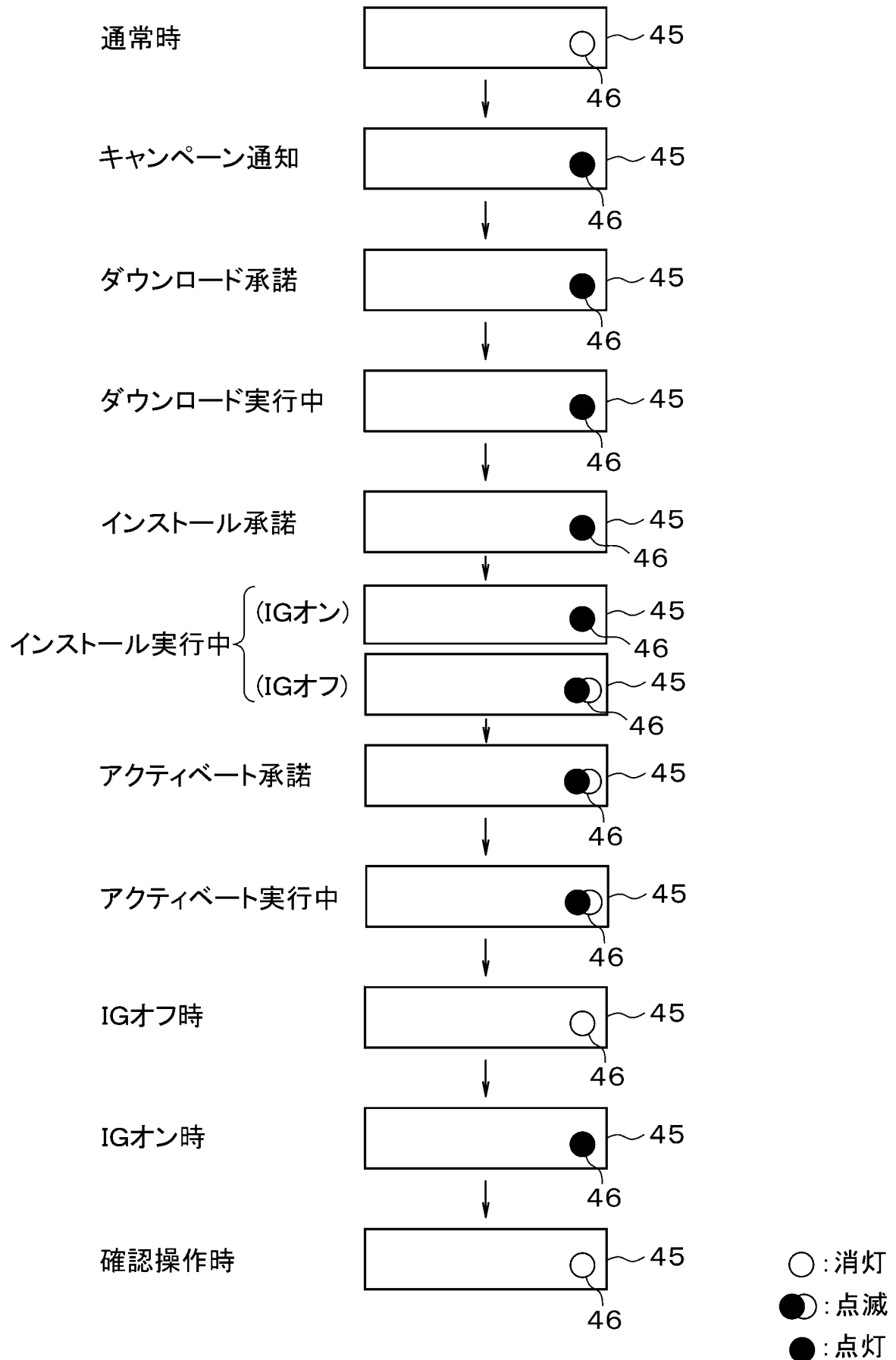
	メータ装置			車載ディスプレイ
	2面メモリ	1面サスペンドメモリ	1面単独メモリ	
通常時	消灯	消灯	消灯	図31
	点灯	点灯	点灯	図32, 33
キャンペーン通知	点灯	点灯	点灯	図34, 35
	点灯	点灯	点灯	図36, 37
ダウンロード	点灯	点灯	点灯	図38, 39, 40
	点灯	点灯・点滅 (IGオン)・点滅 (IGオフ)	点滅	図41, 42
インストール	点灯	点滅	点滅	図43
	点滅	点滅	点滅	
アクティベート	消灯	消灯	消灯	
	点灯	点灯	点灯	図44
確認操作時	消灯	消灯	消灯	図45, 46

Fig. 214



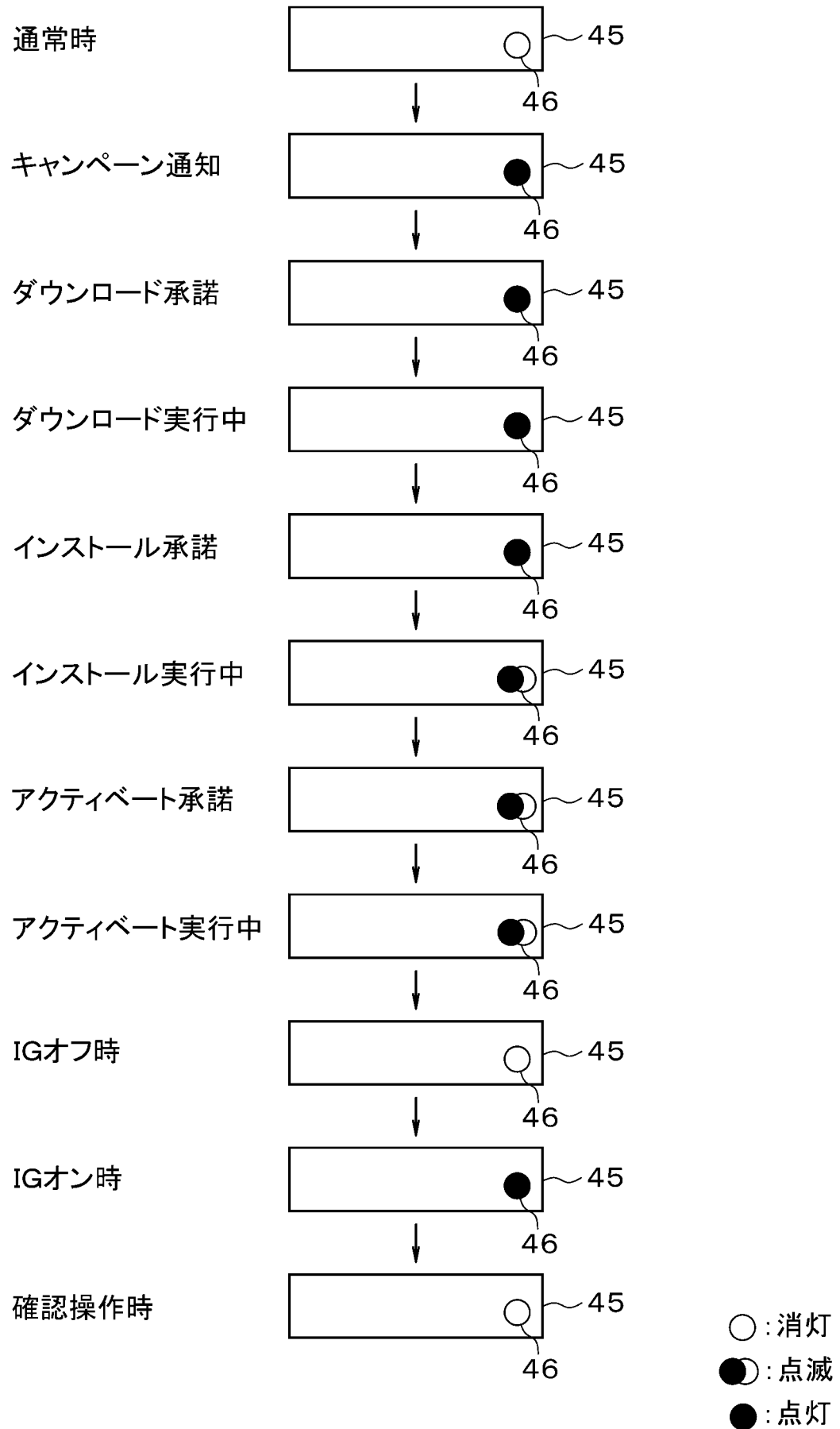
[図215]

Fig. 215



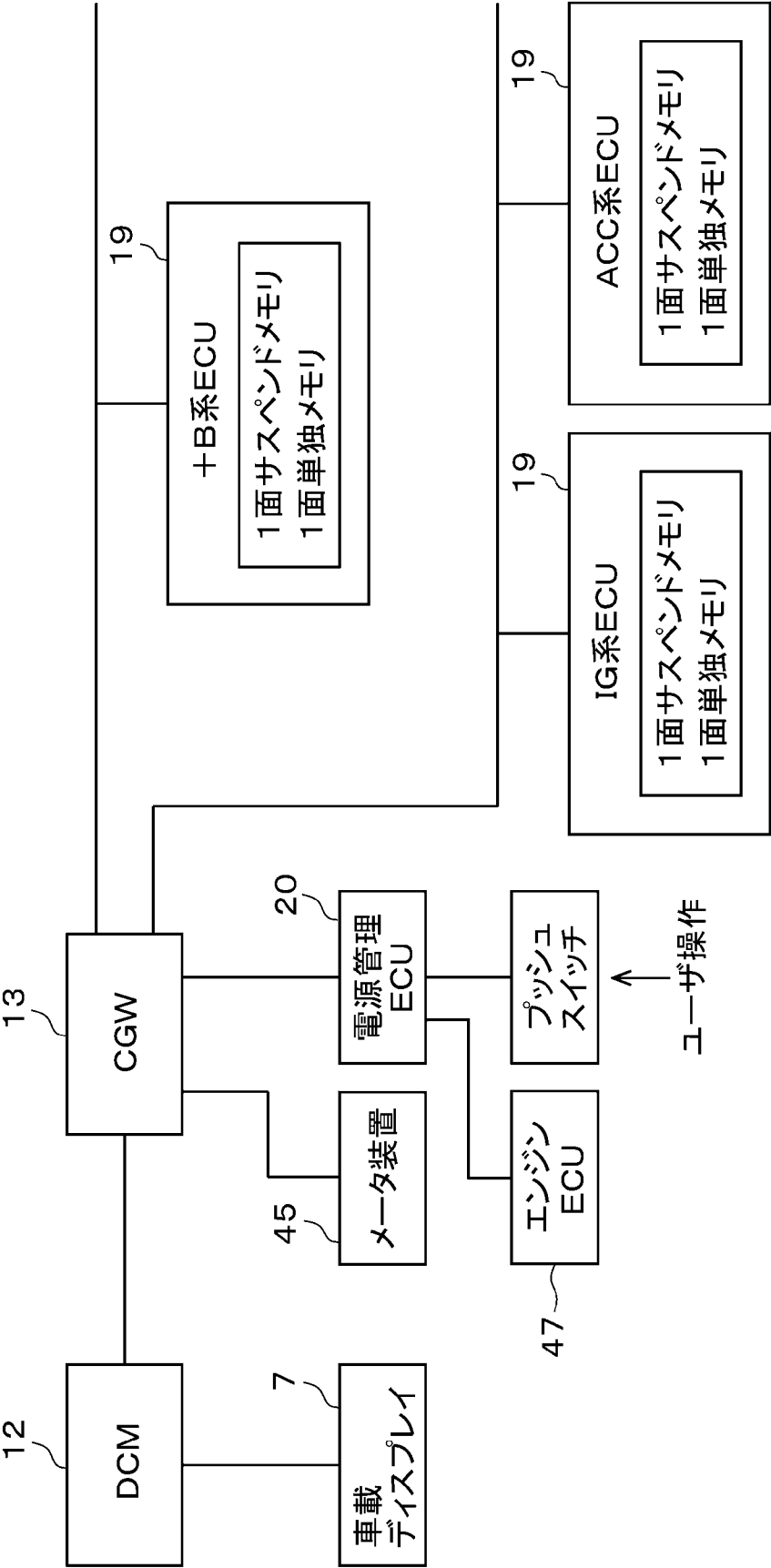
[図216]

Fig. 216



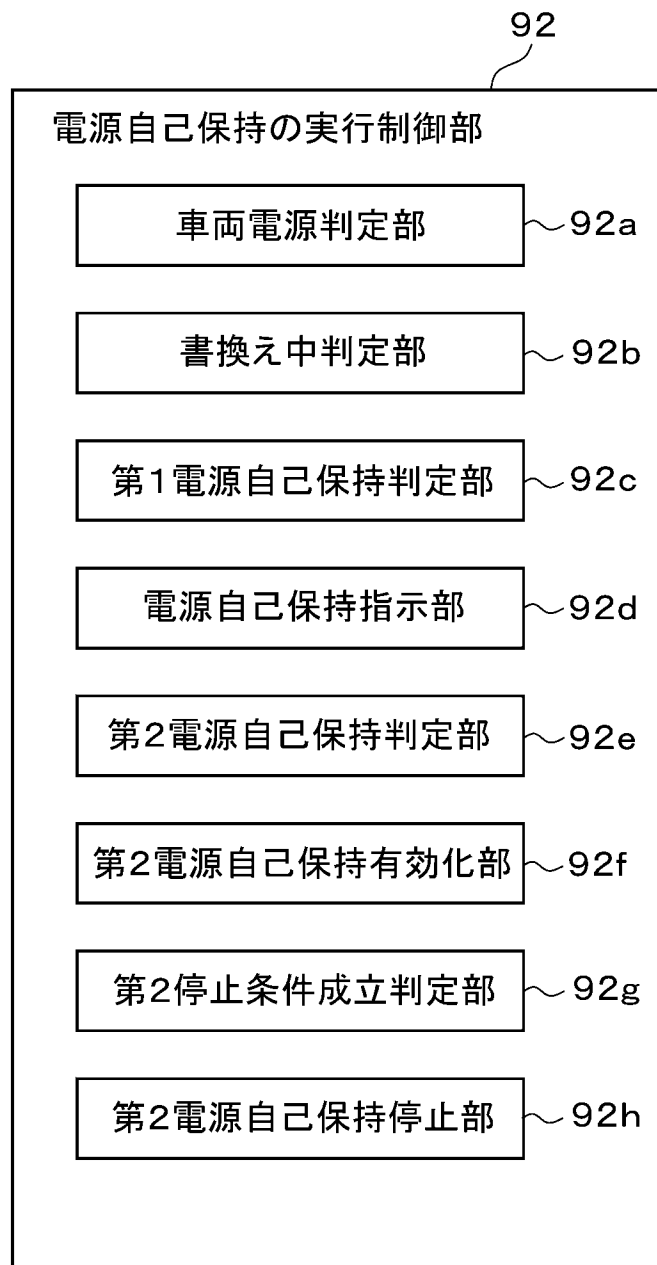
[図217]

Fig. 217



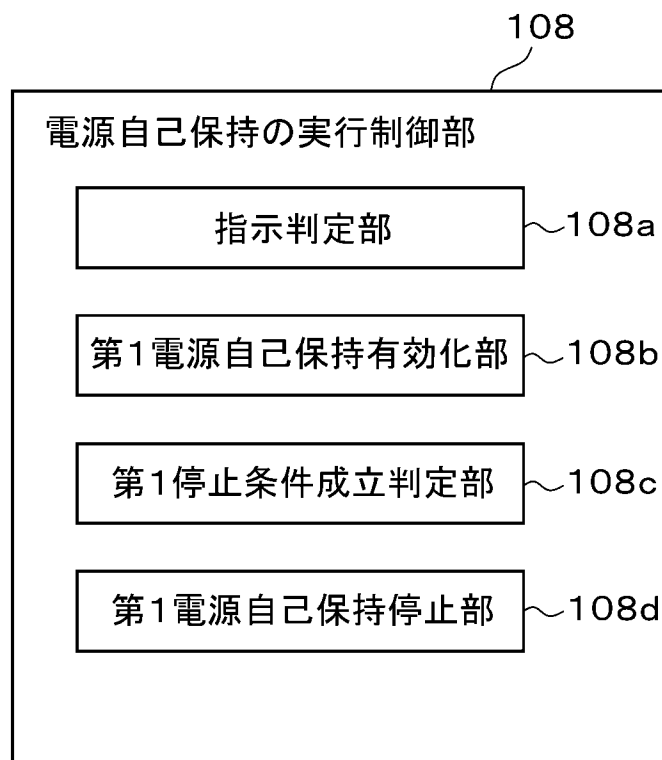
[図218]

Fig. 218



[図219]

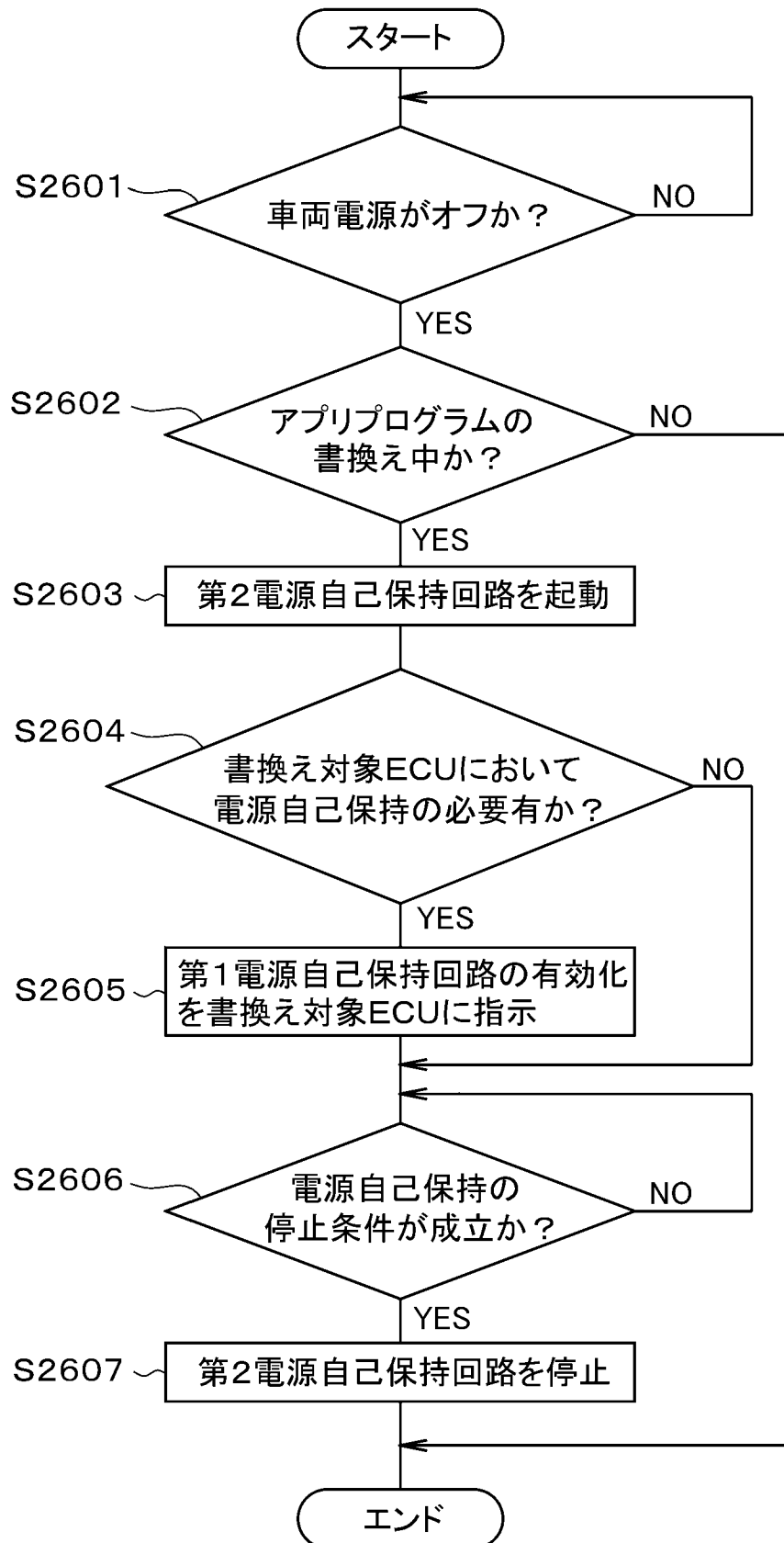
Fig. 219



[図220]

Fig. 220

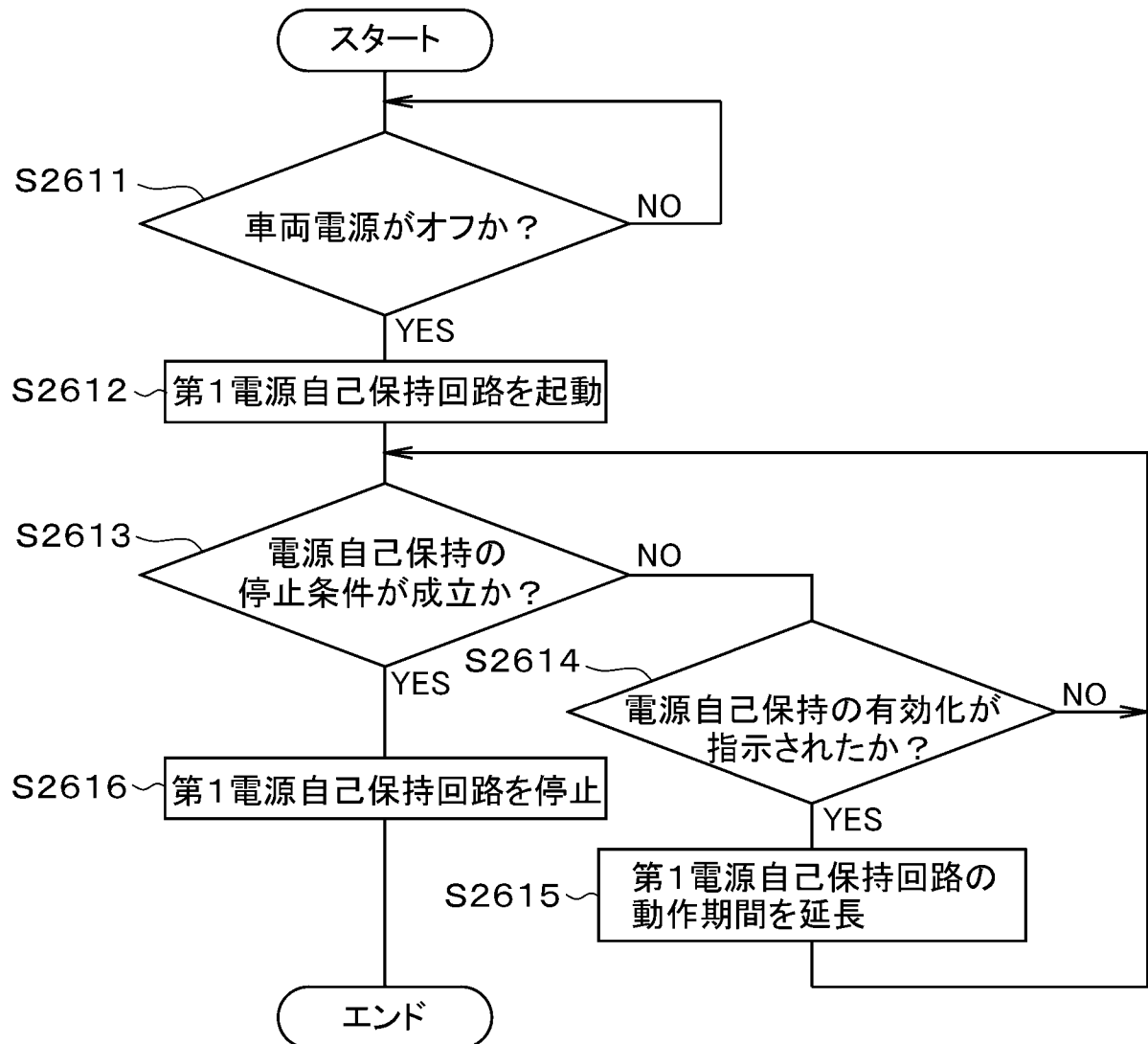
CGWにおける電源自己保持の実行制御処理



[図221]

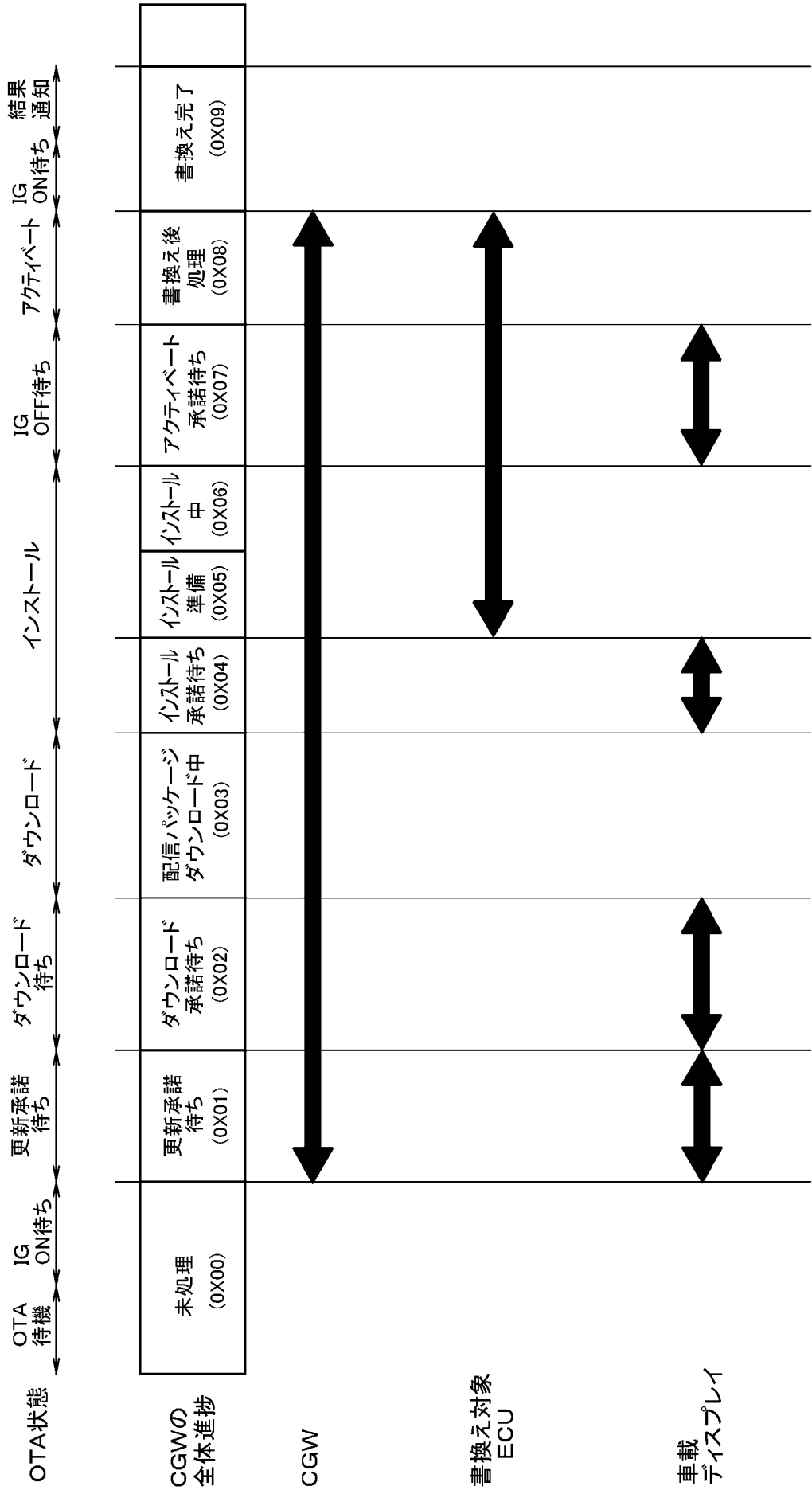
Fig. 221

書換え対象ECUにおける電源自己保持の実行制御処理



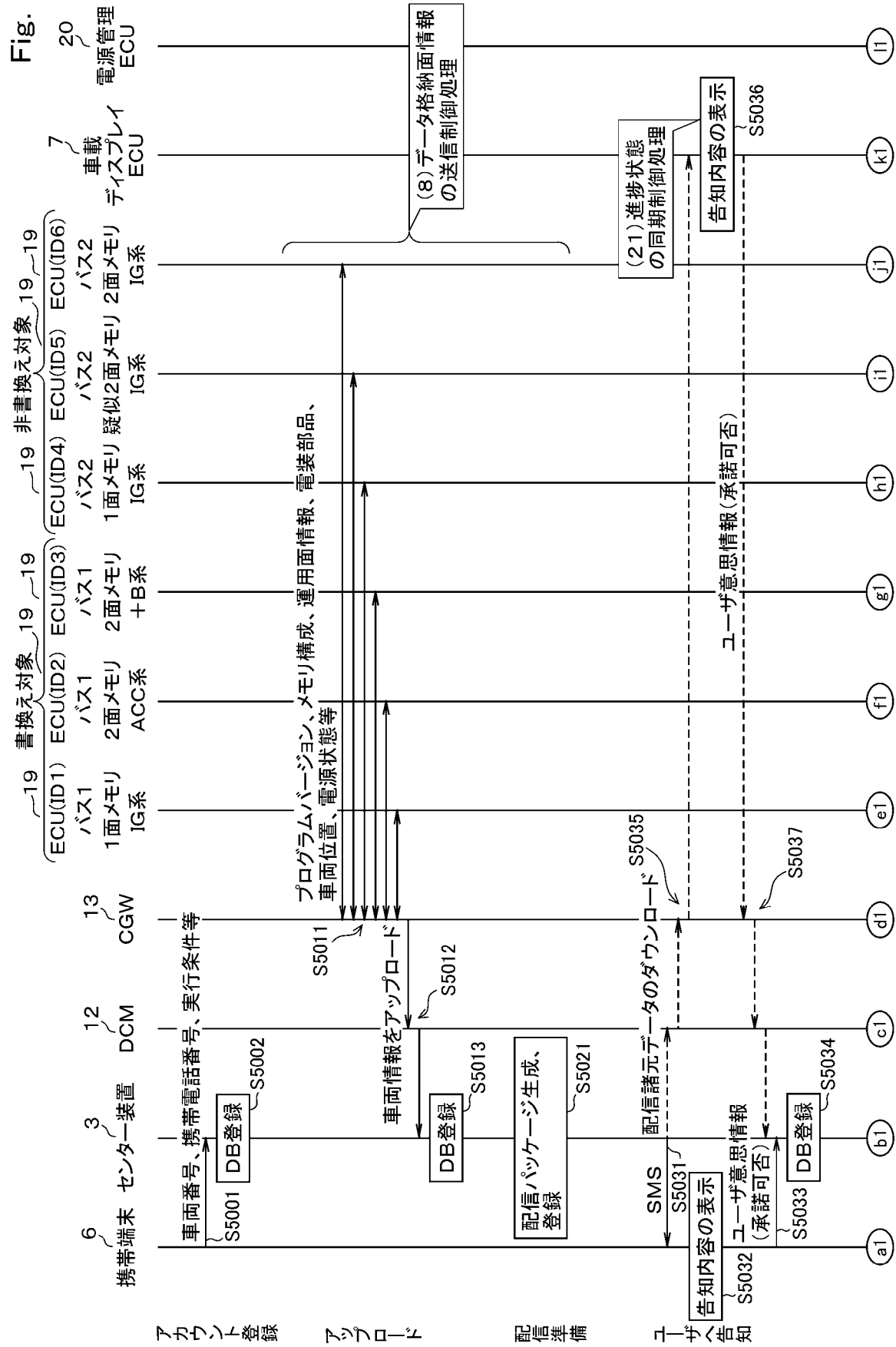
[図222]

Fig. 222



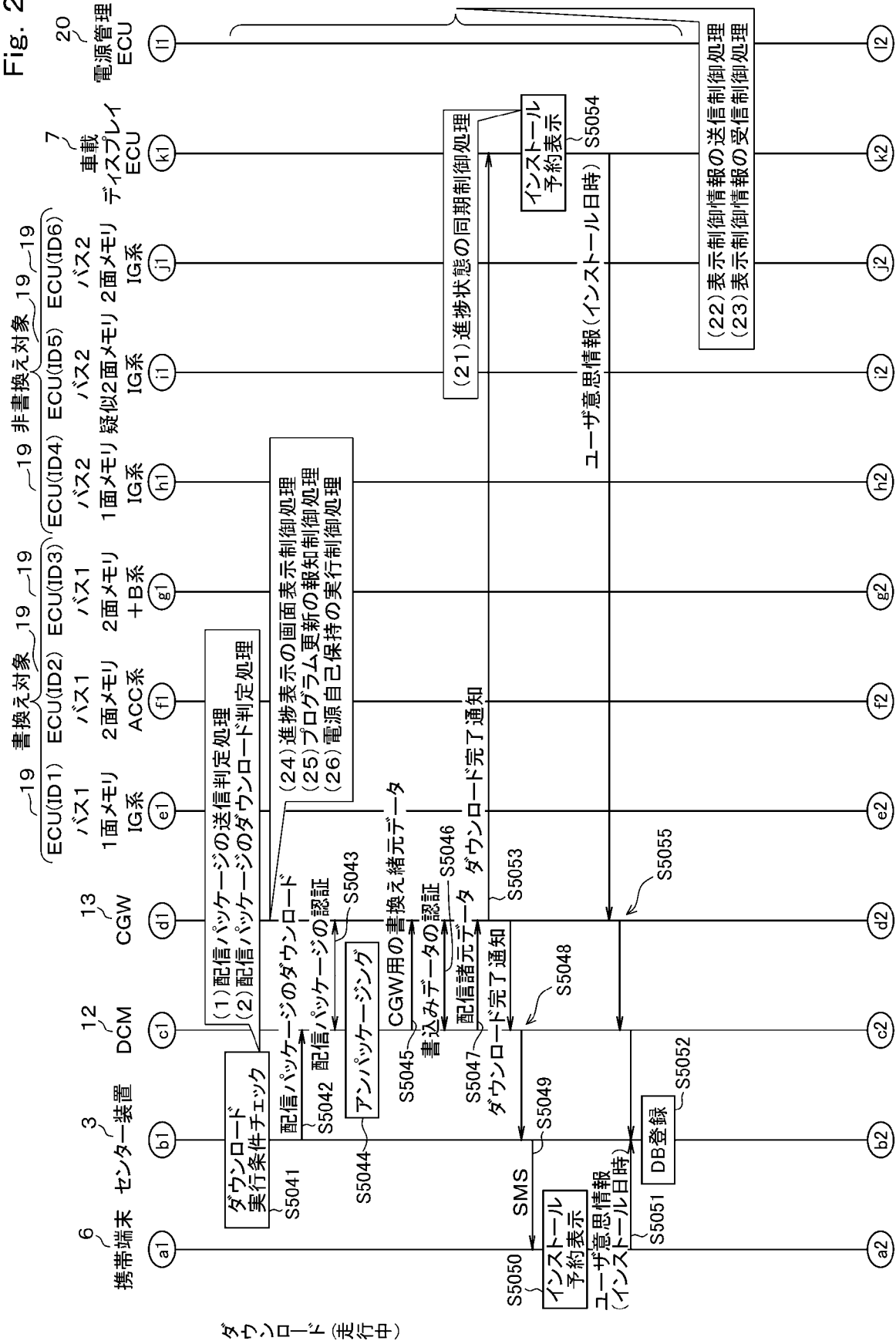
[図223]

Fig. 223



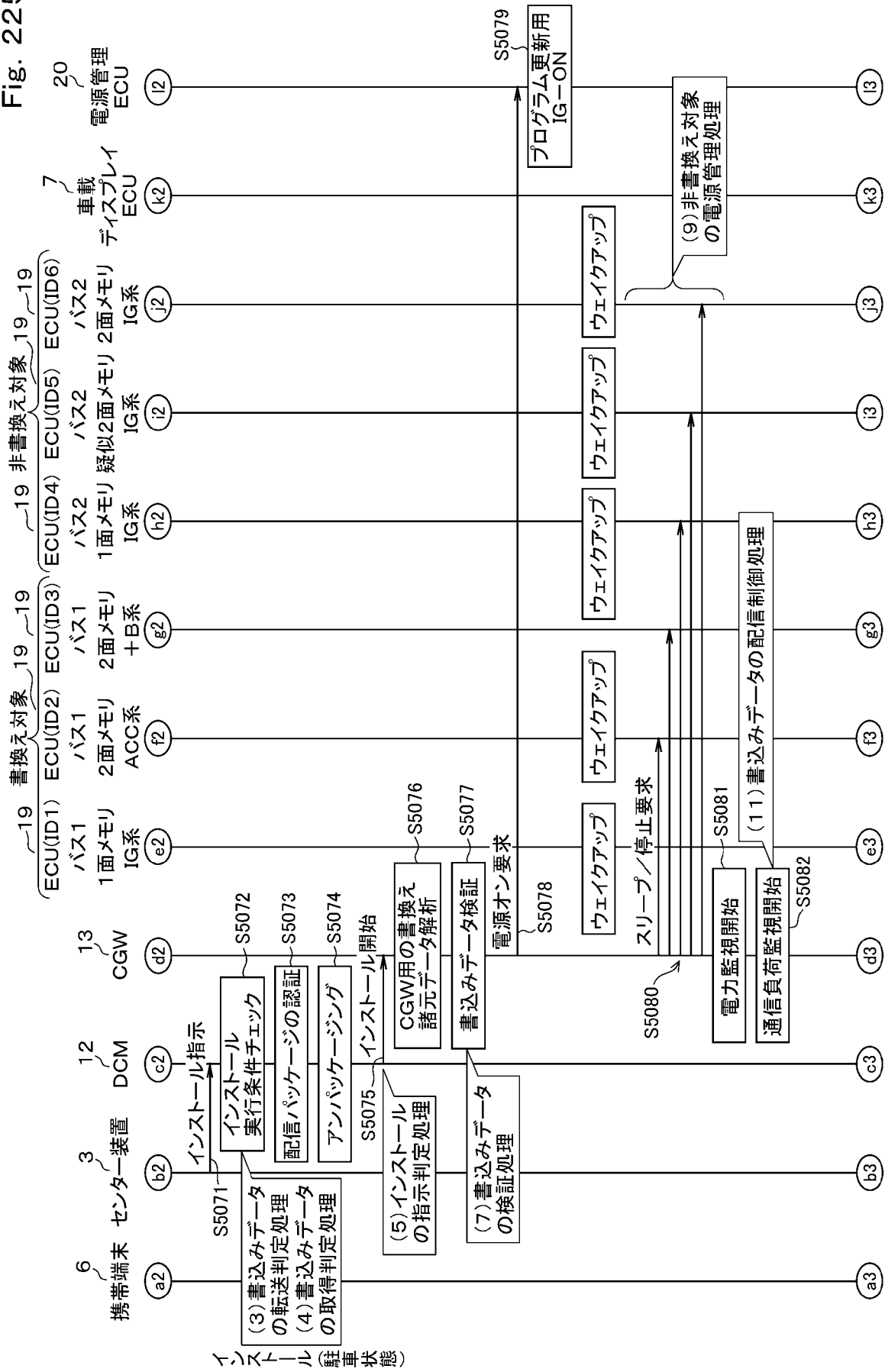
[図224]

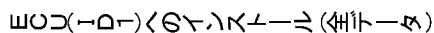
Fig. 224



[図225]

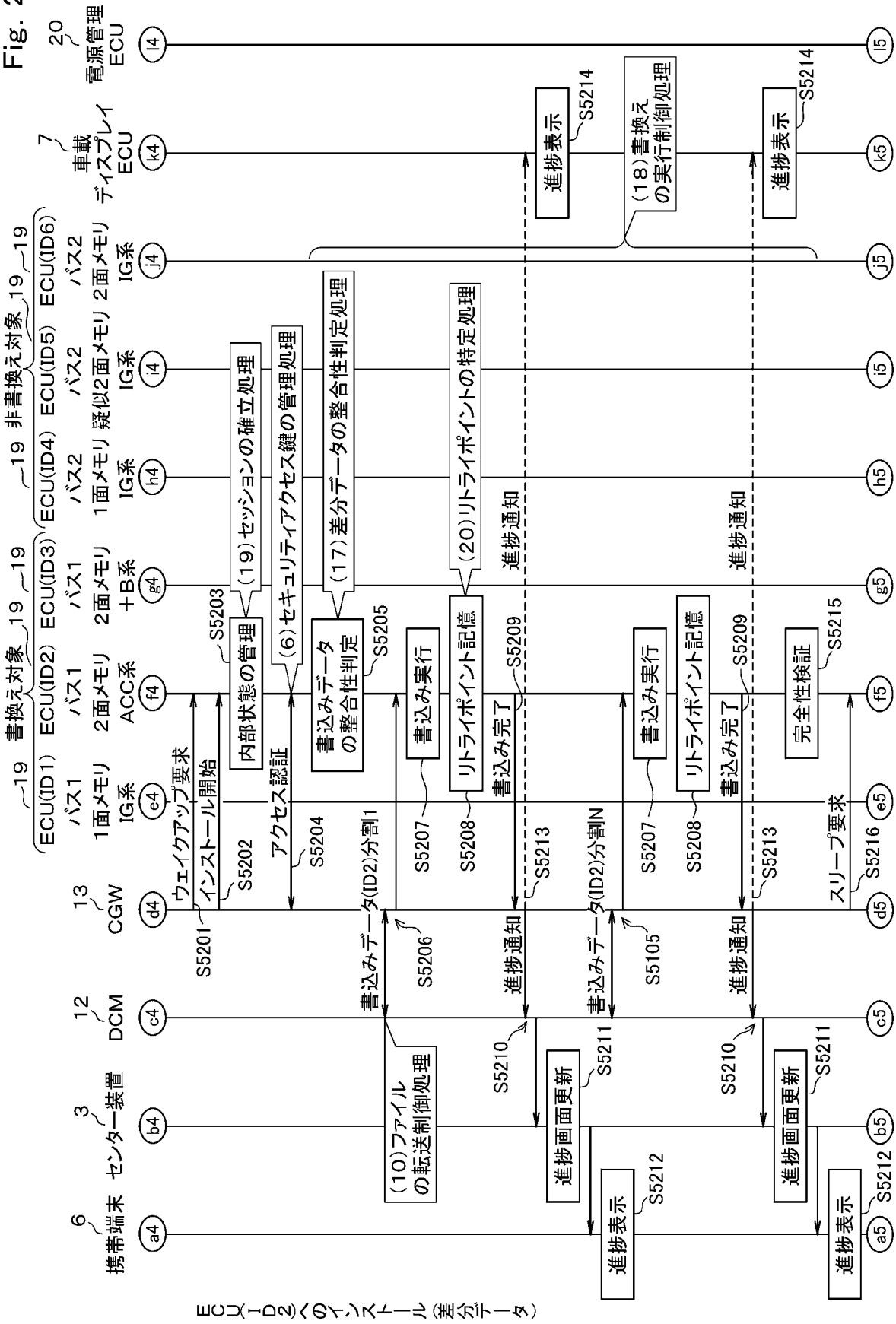
Fig. 225



226
Fi. 226

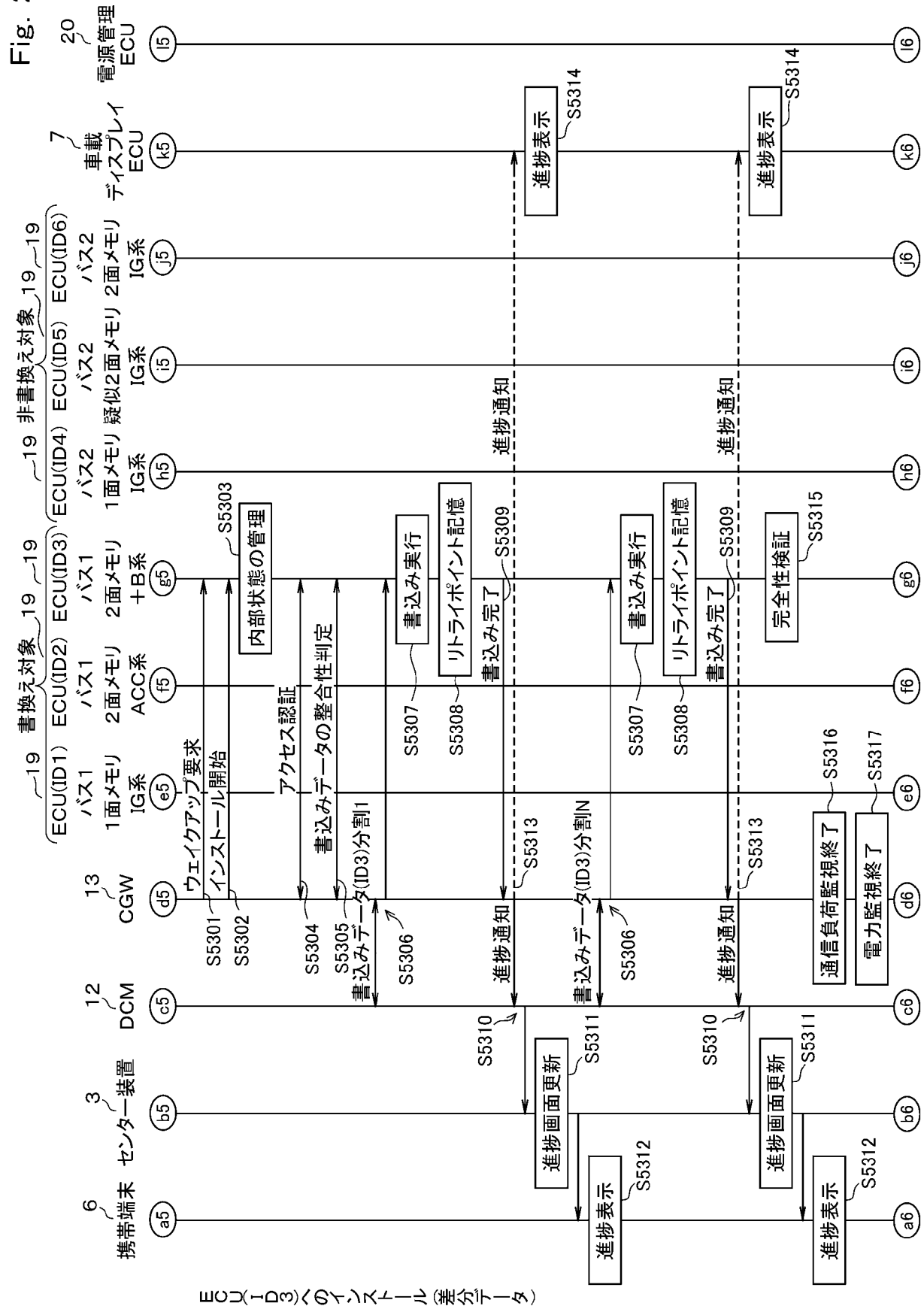
[図227]

Fig. 227



[図228]

Fig. 228



[図229]

Fig. 229

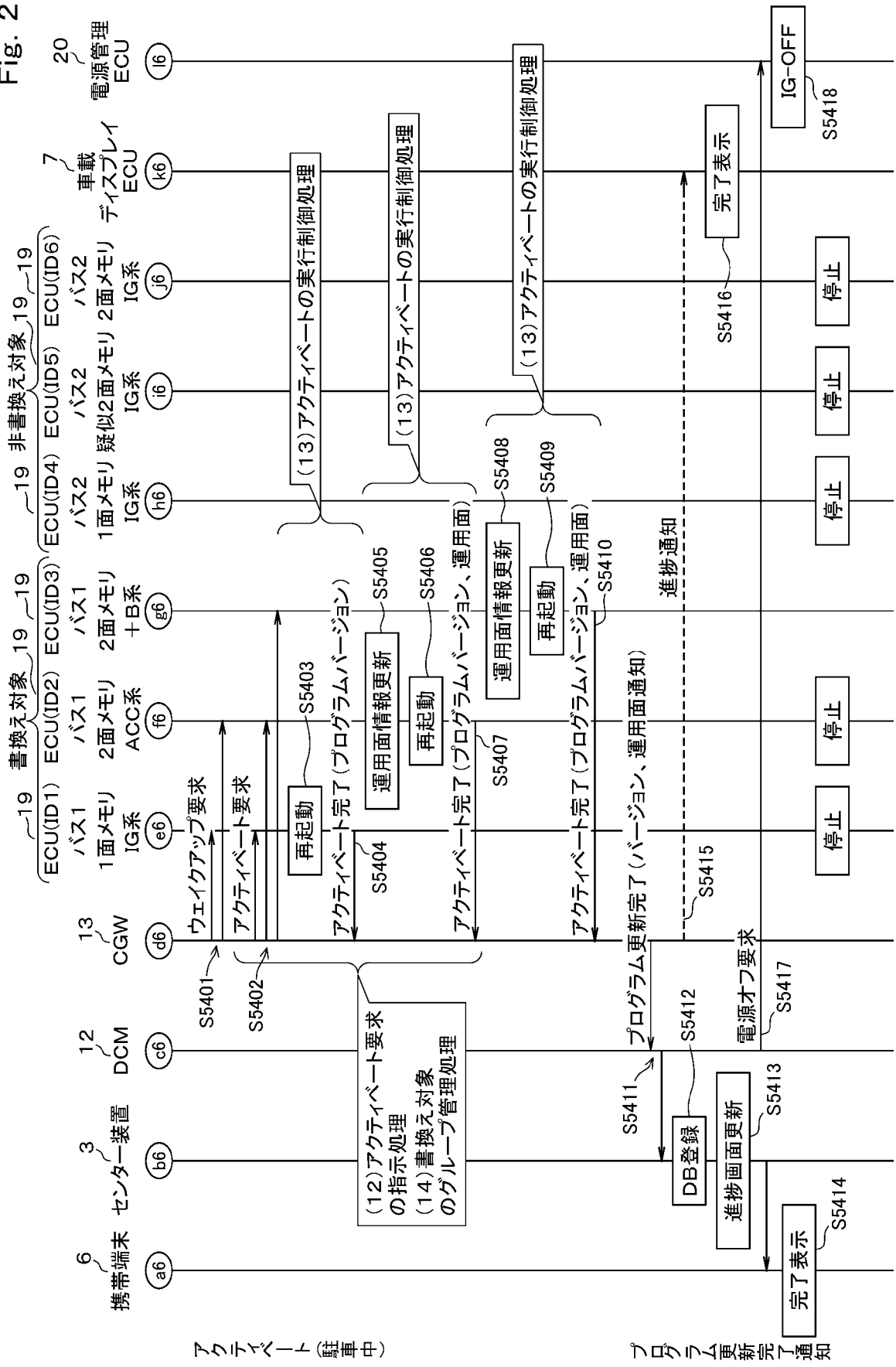
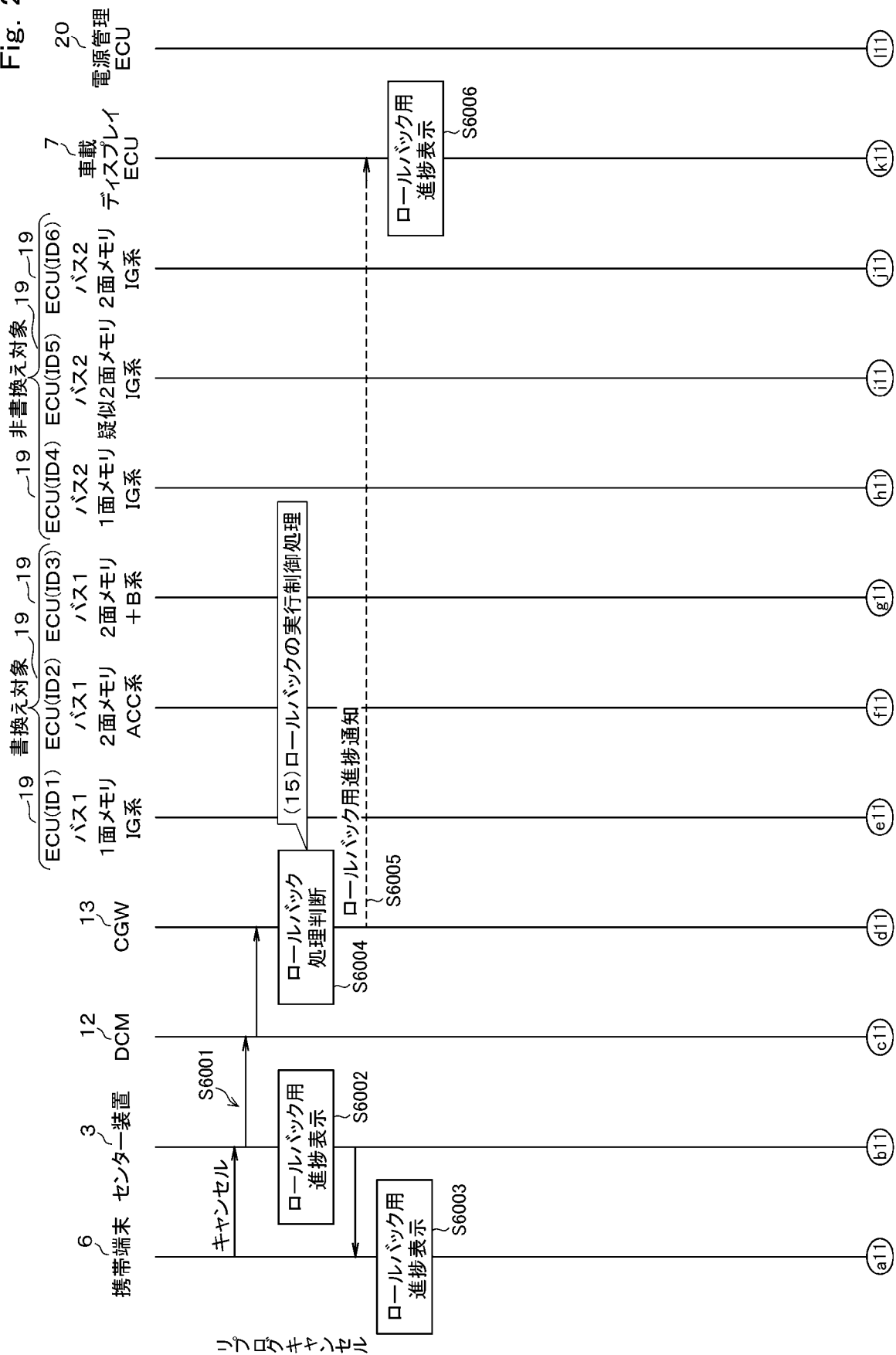
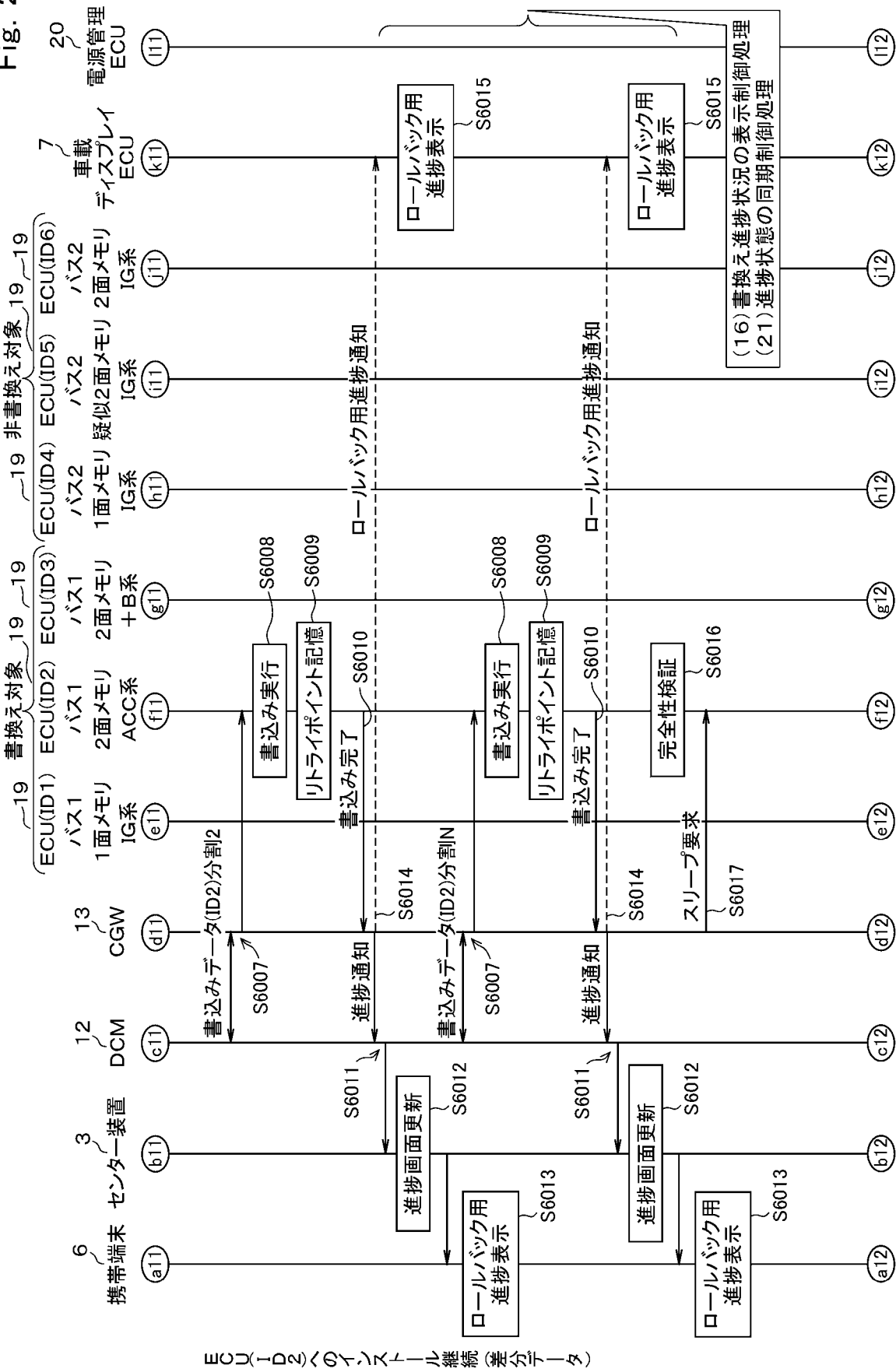


Fig. 230



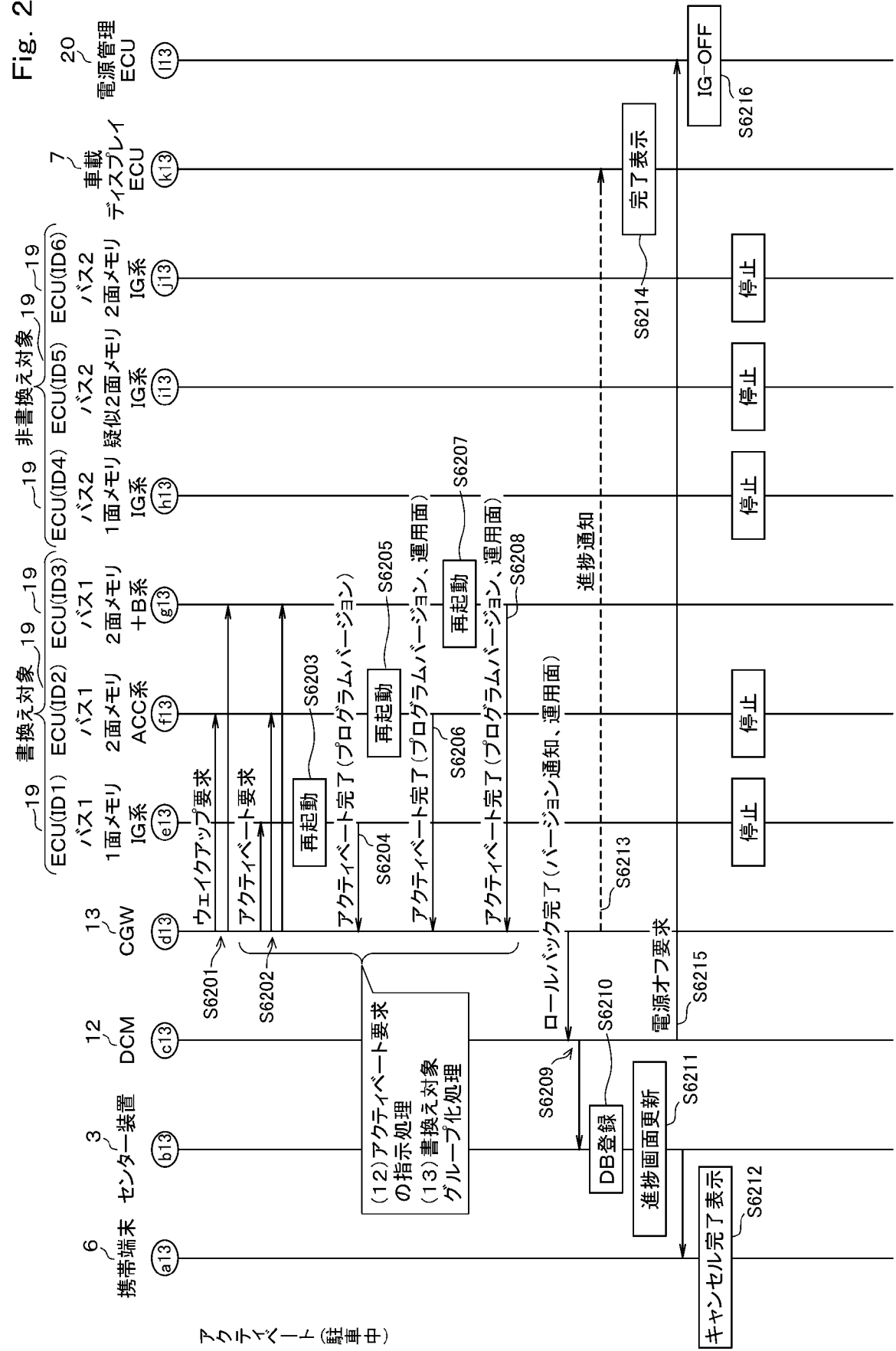
[図 231]

Fig. 231

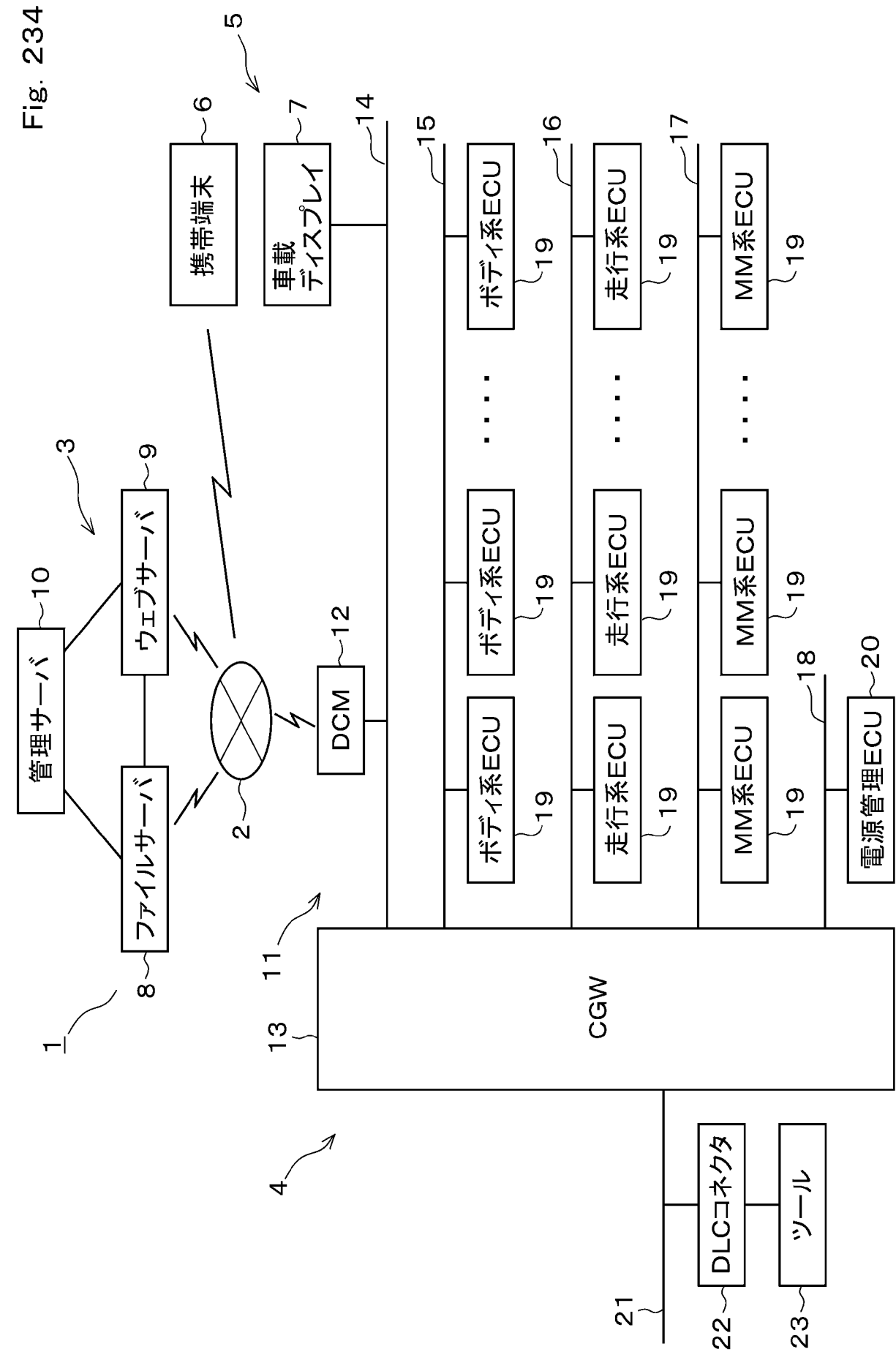


[図233]

Fig. 233

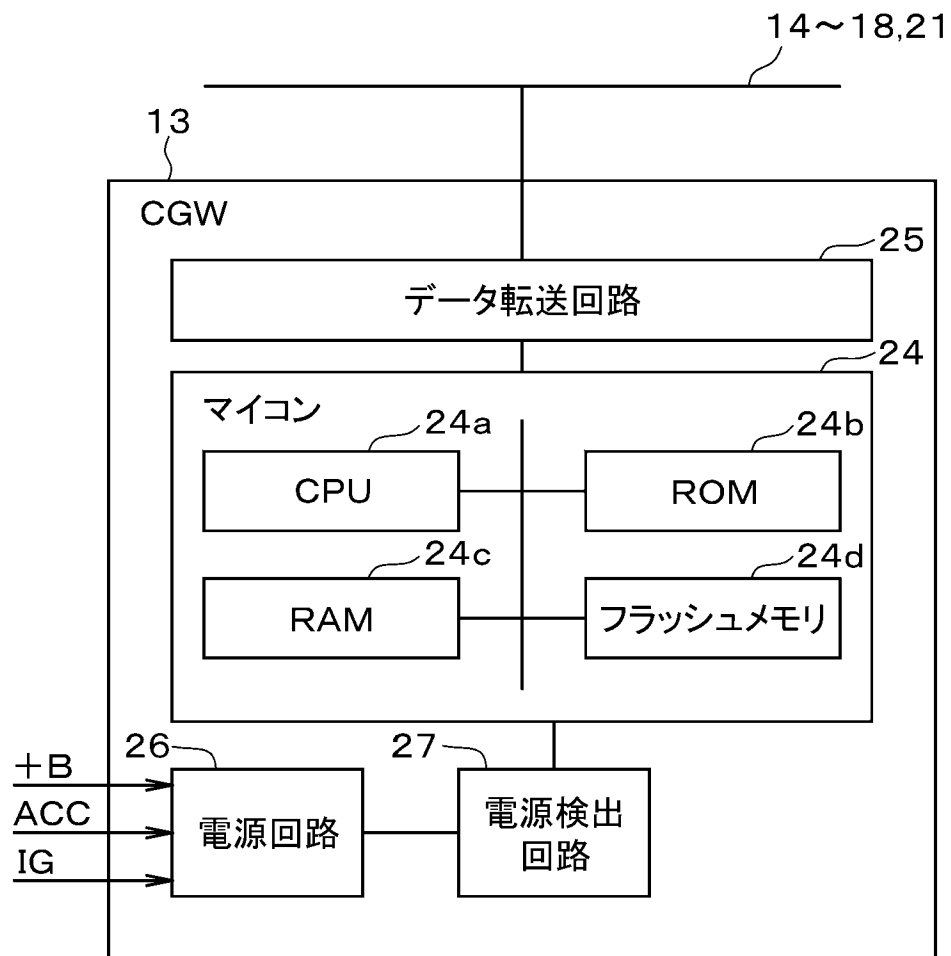


[図234]



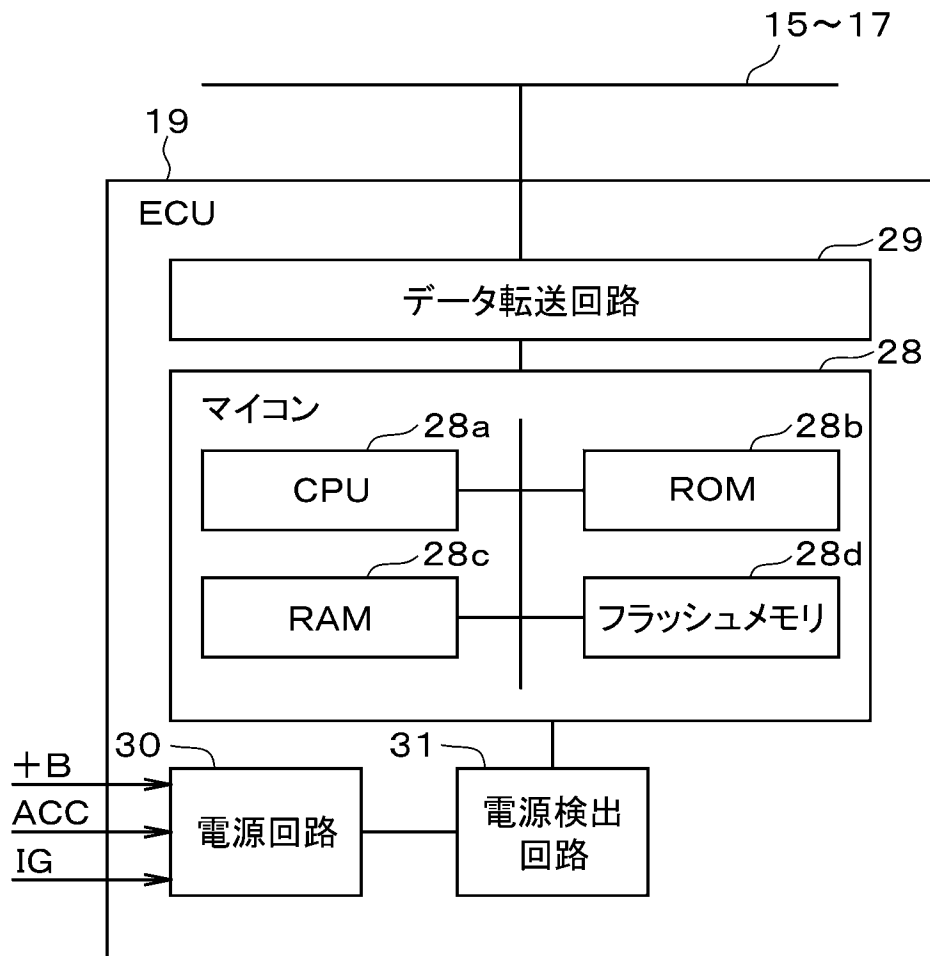
[図235]

Fig. 235



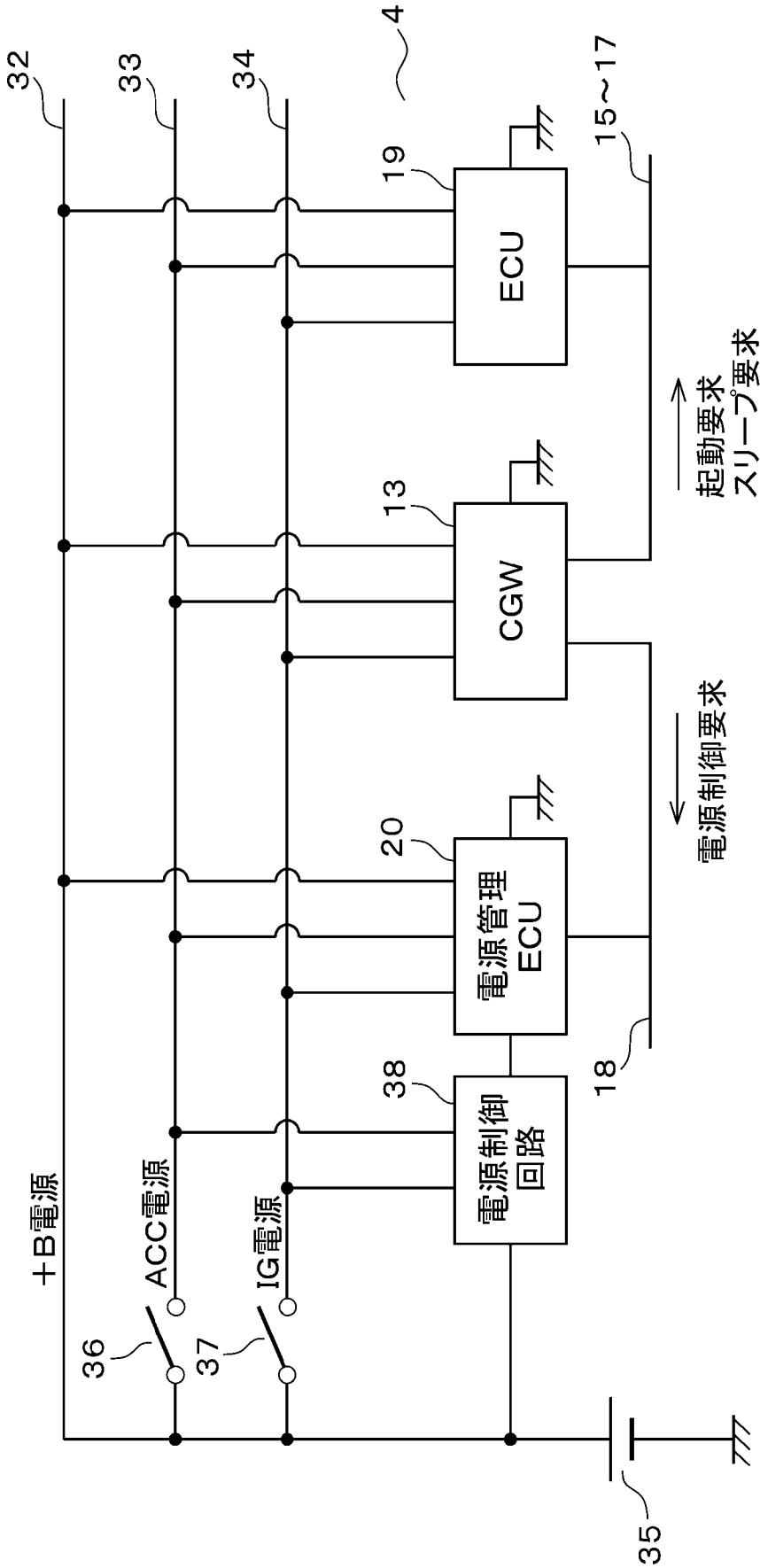
[図236]

Fig. 236

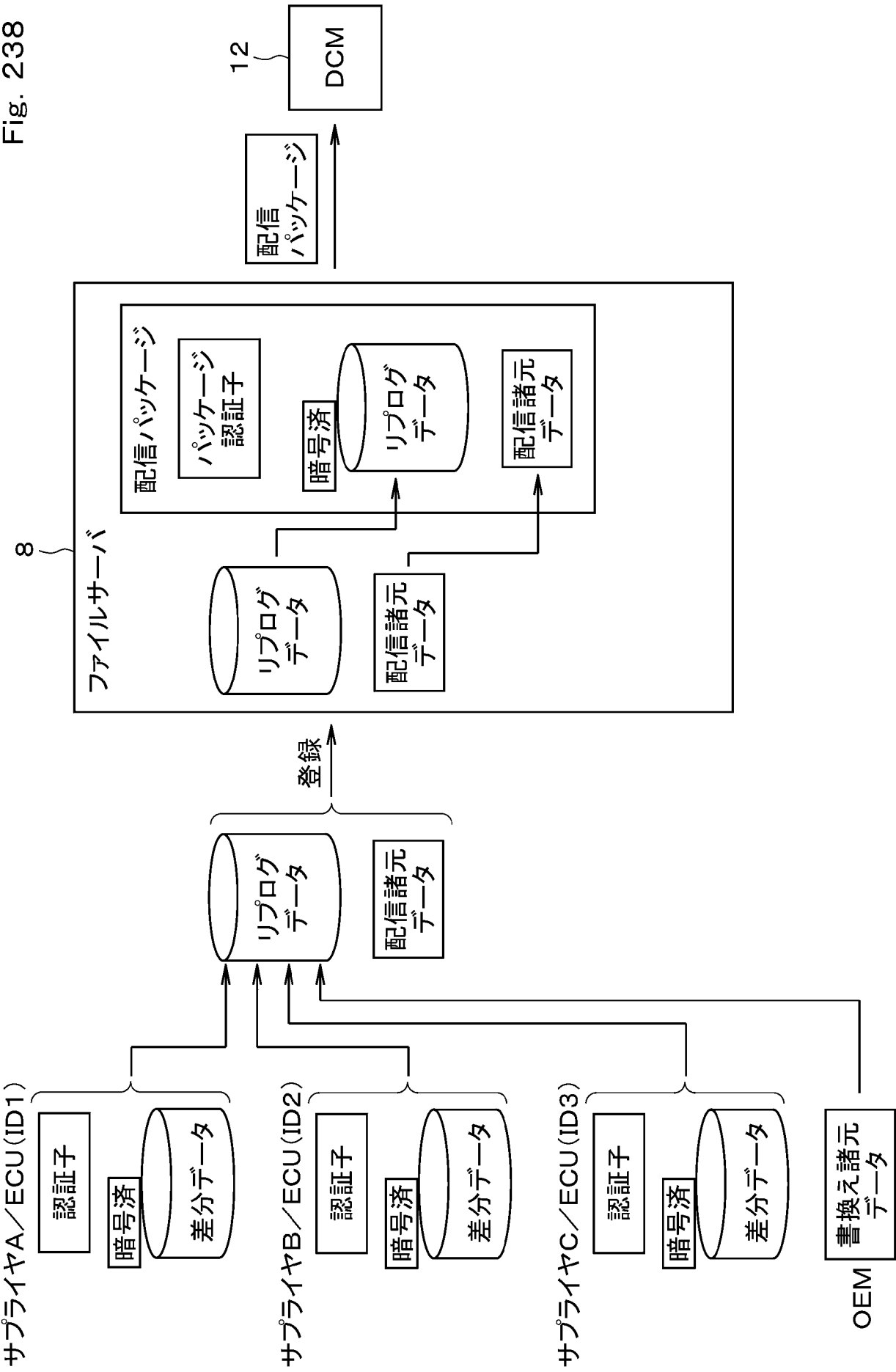


[図237]

Fig. 237

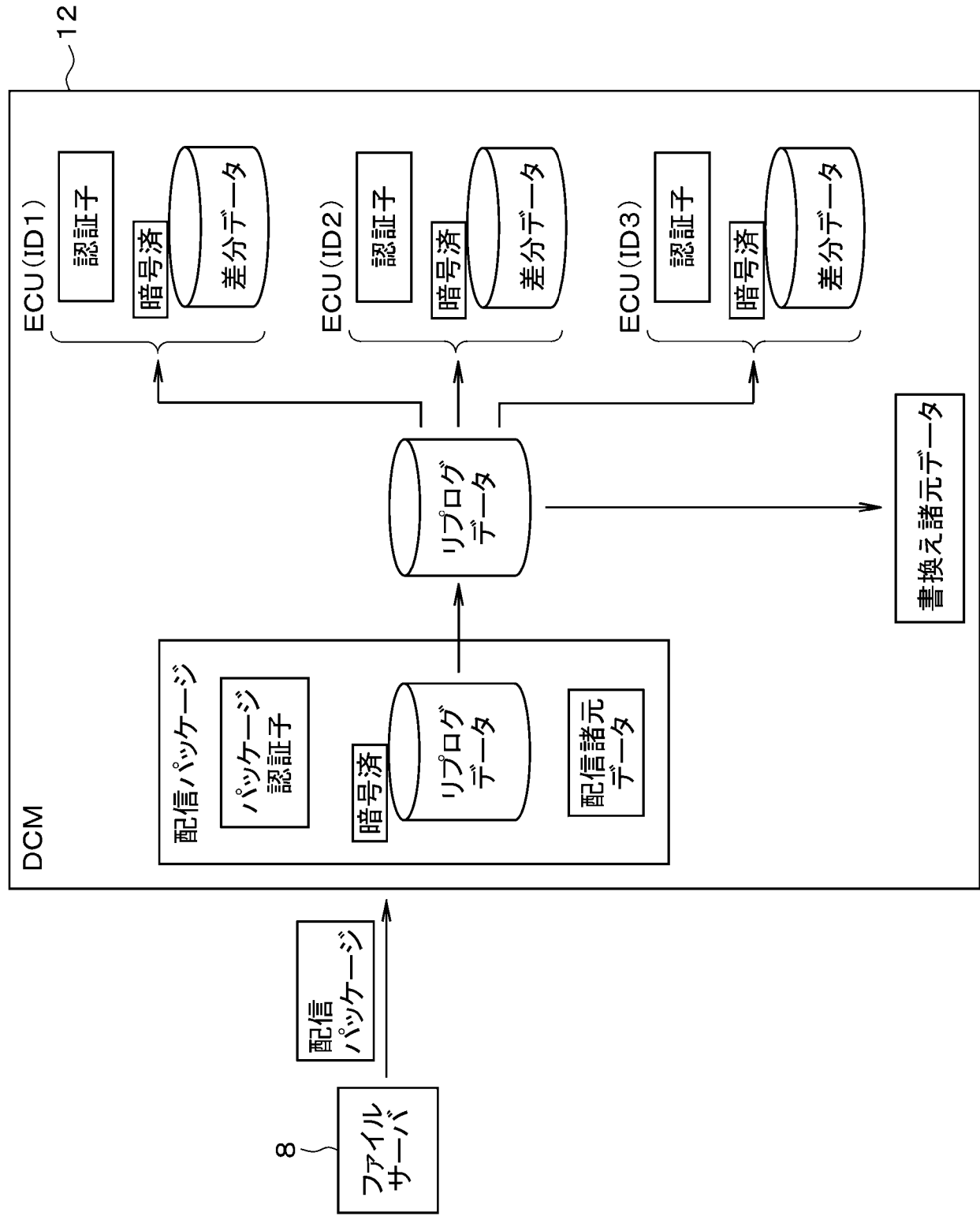


[図238]



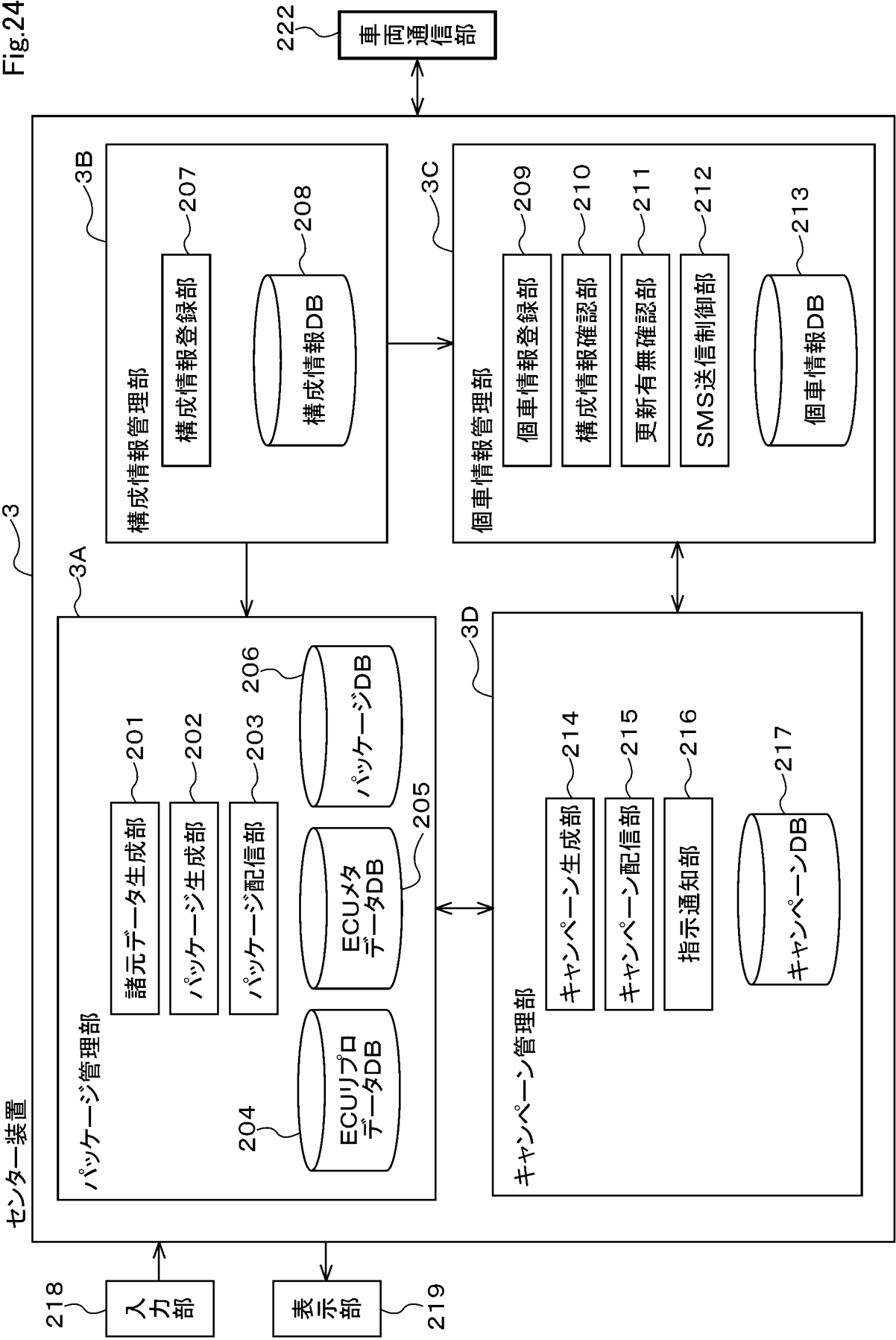
[図239]

Fig. 239



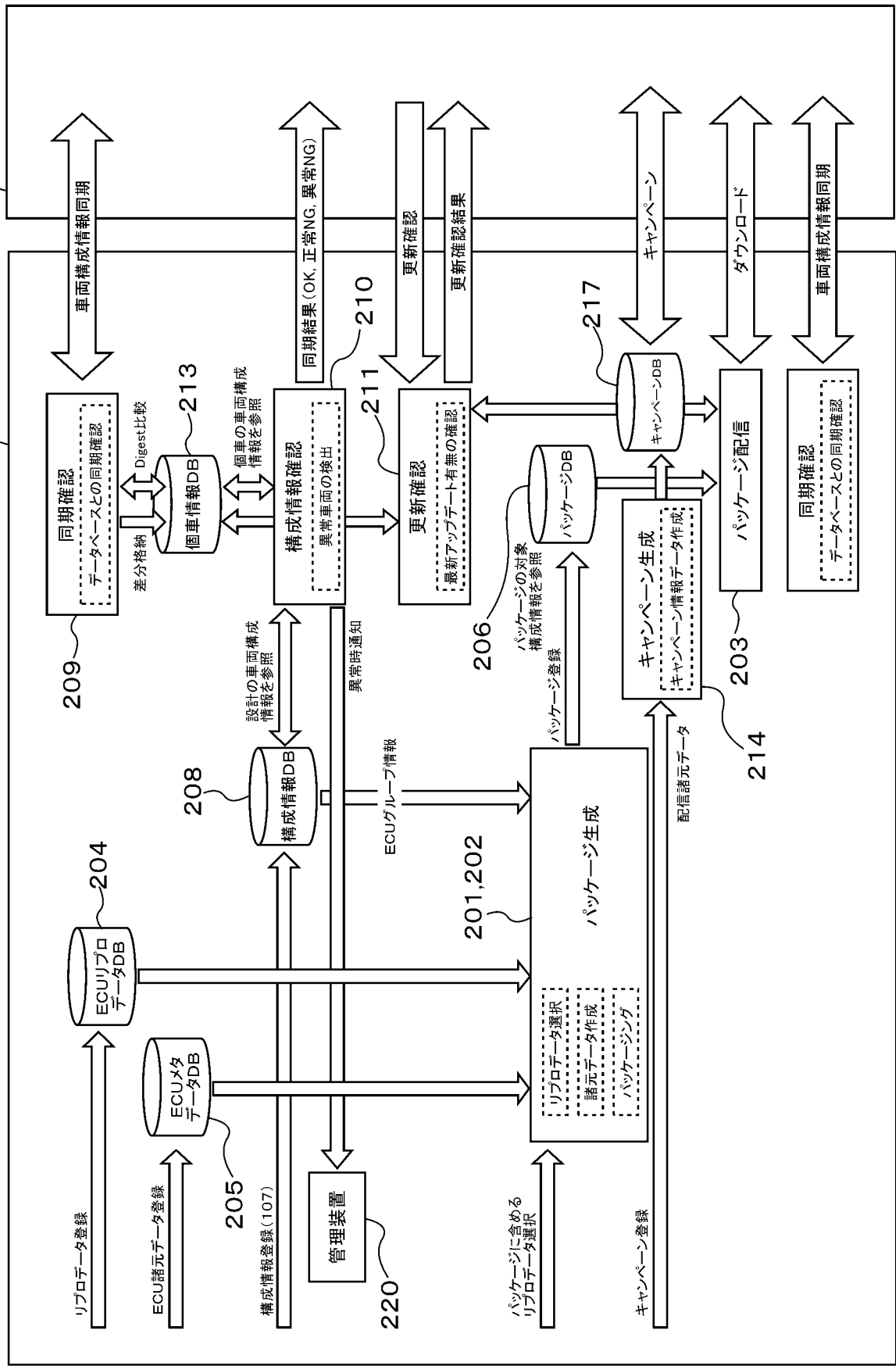
[図240]

Fig.240

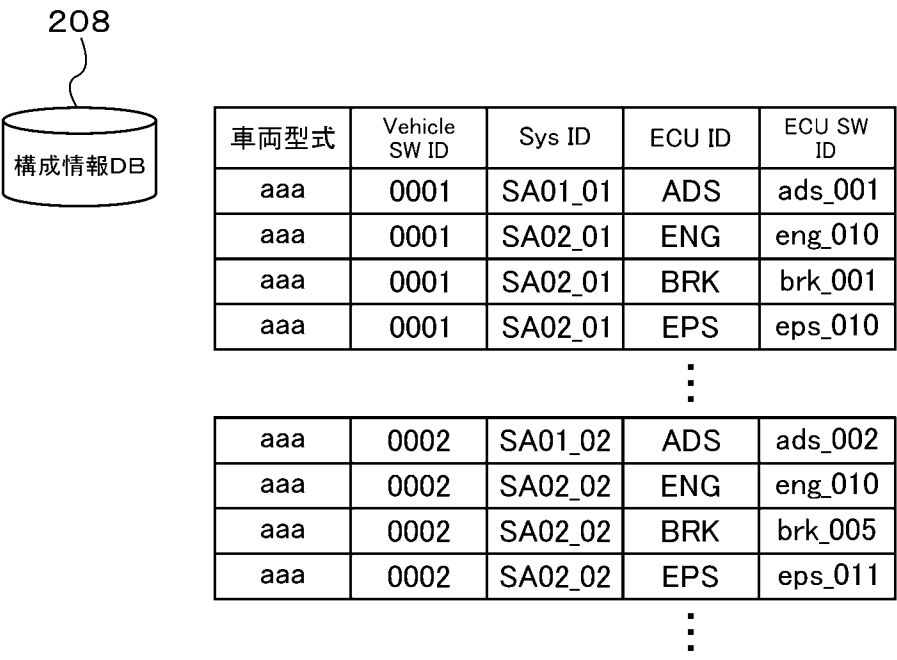


[図241]

Fig.241

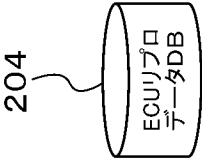


[図242]
Fig.242



[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

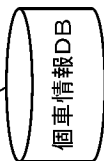
[図244]

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



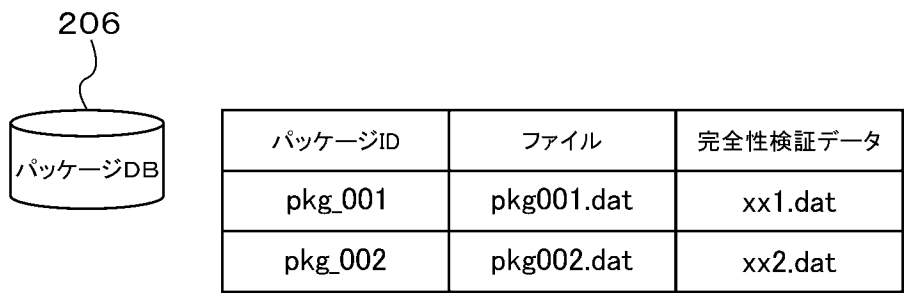
[図245]

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	リブ羅斯テータス
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
: :									

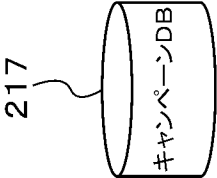
[図246]

Fig.246



[図247]

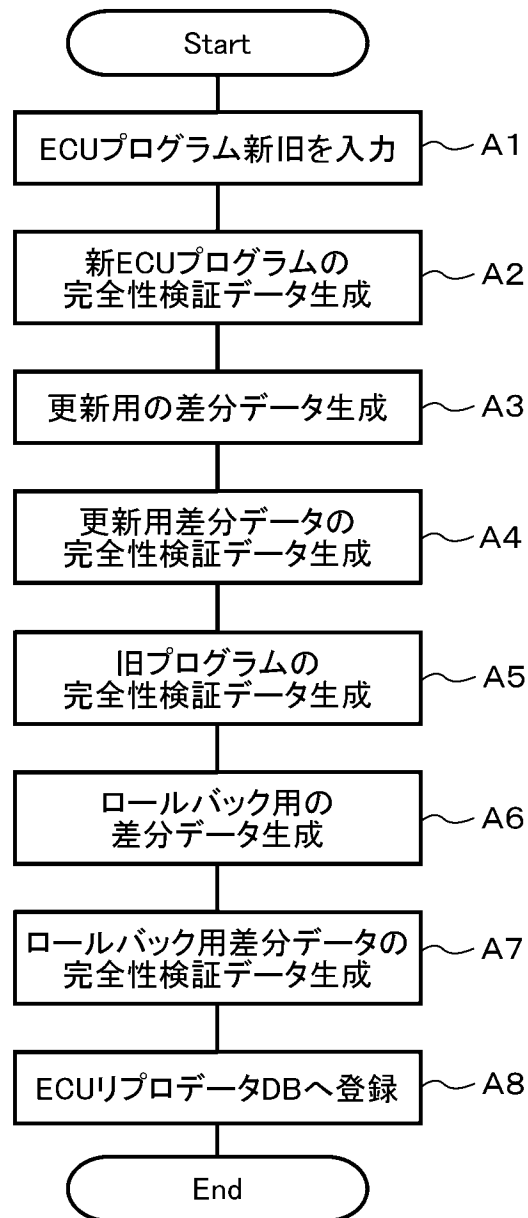
Fig.247



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	...	...

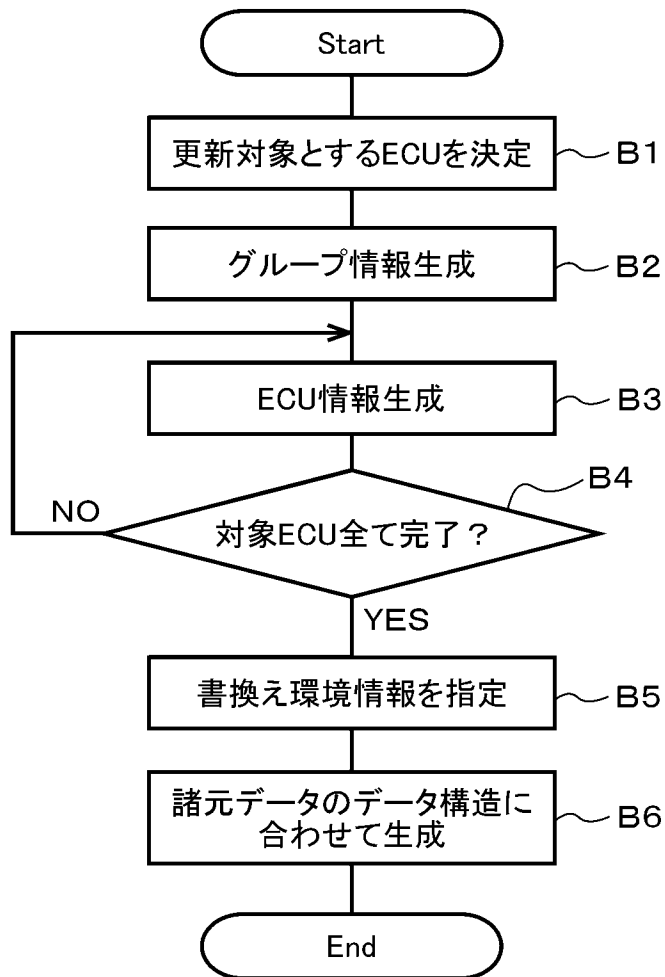
[図248]

Fig.248



[図249]

Fig.249



[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
	バッテリー負荷(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]

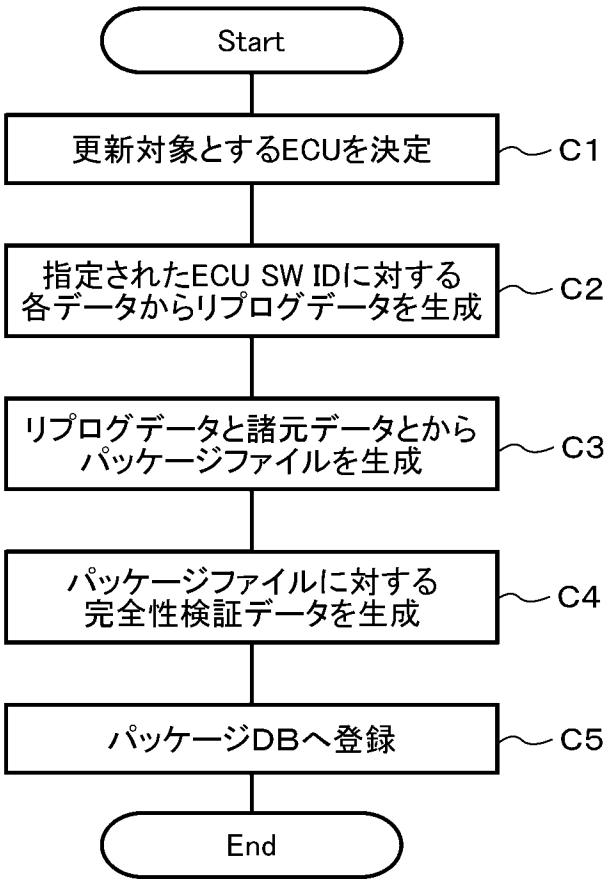
Fig.251

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%

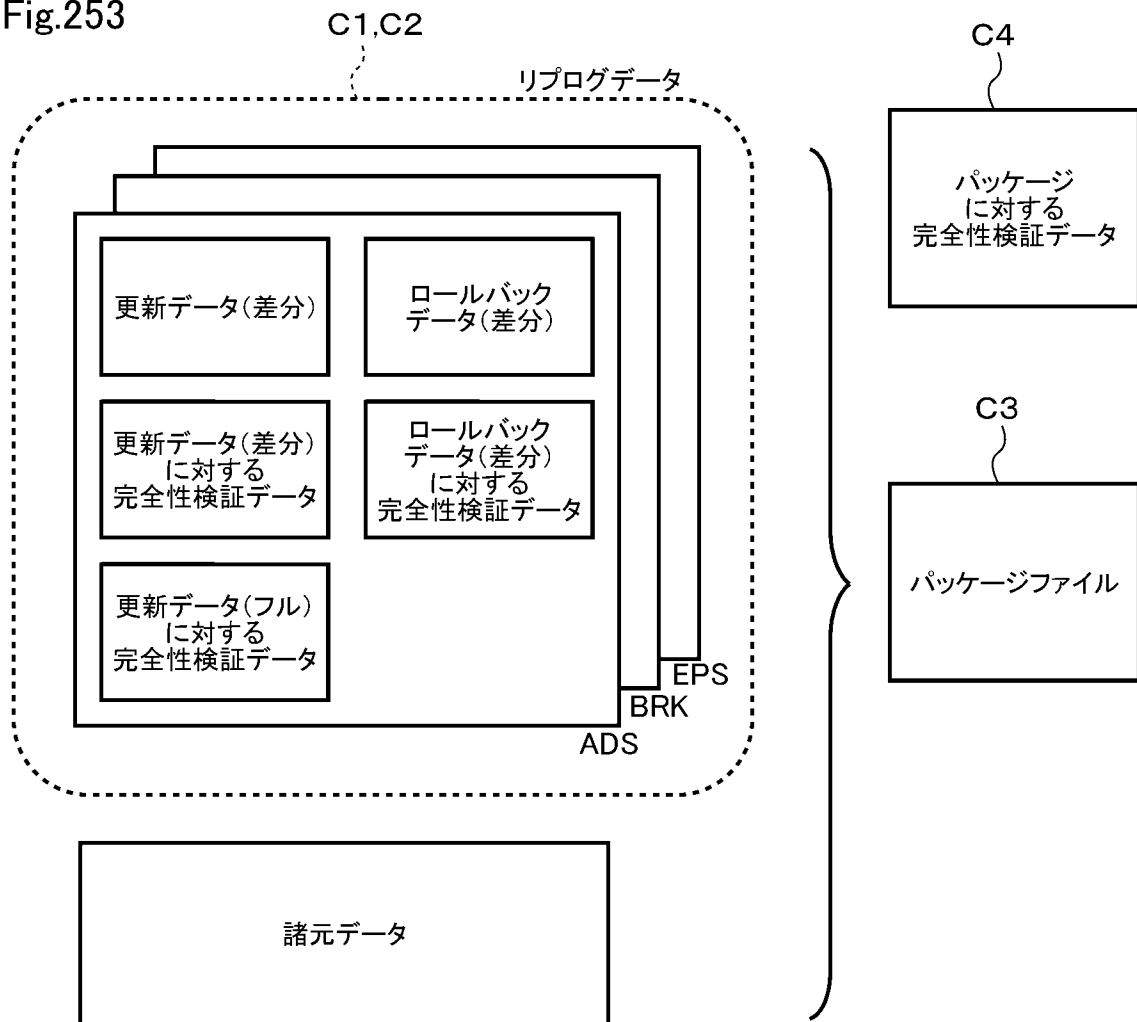
[図252]

Fig.252



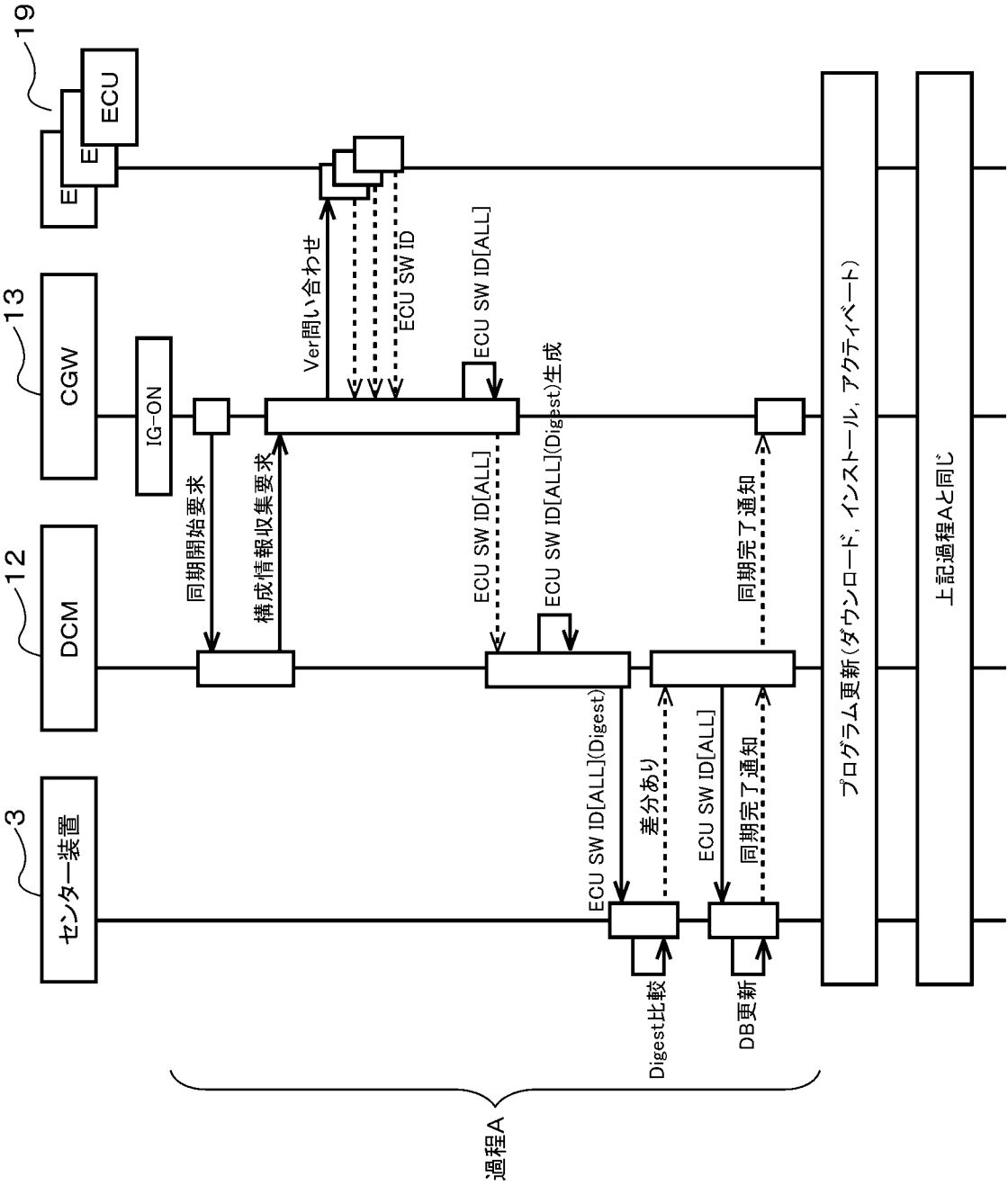
[図253]

Fig.253



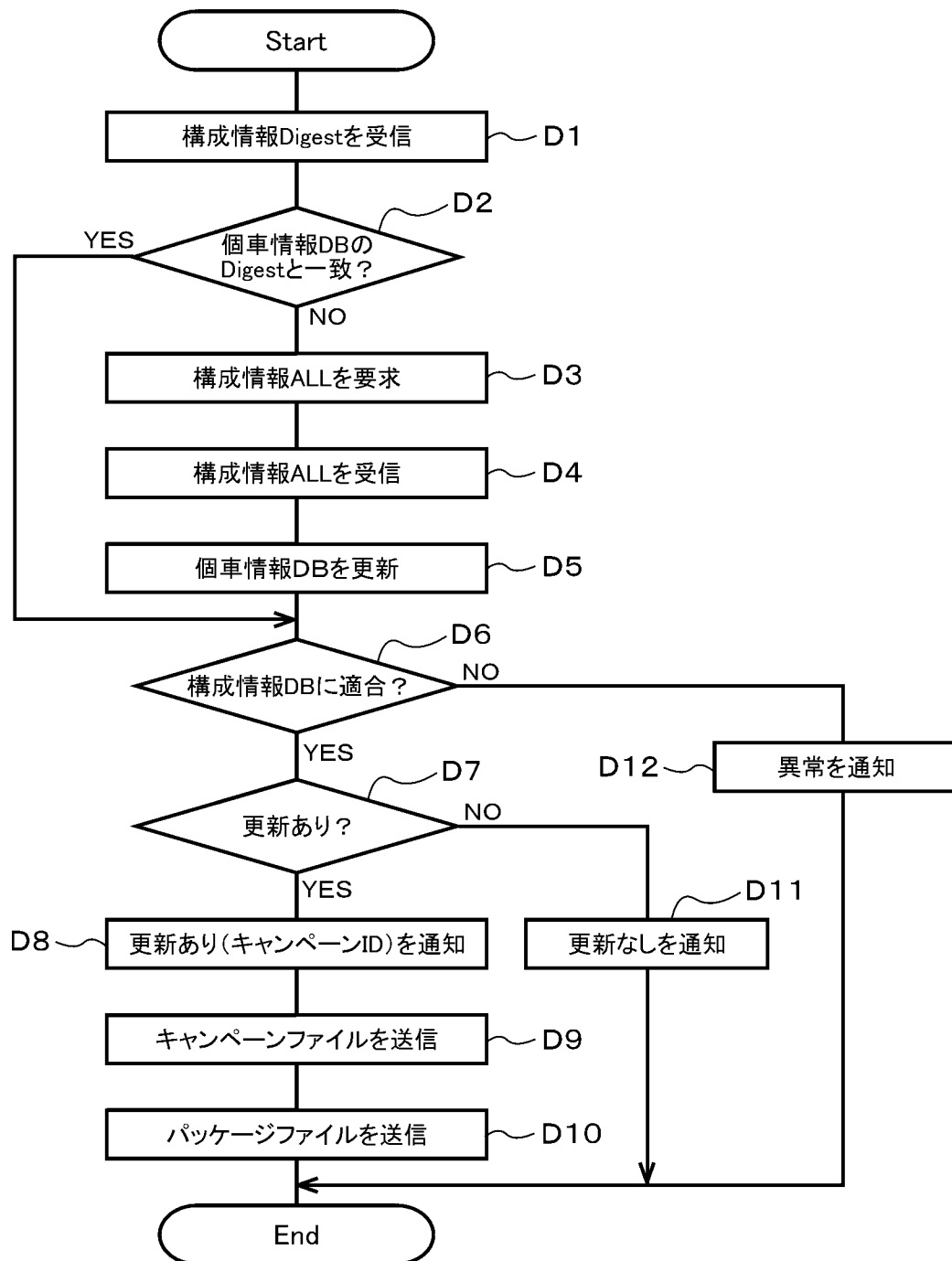
[図254]

Fig.254



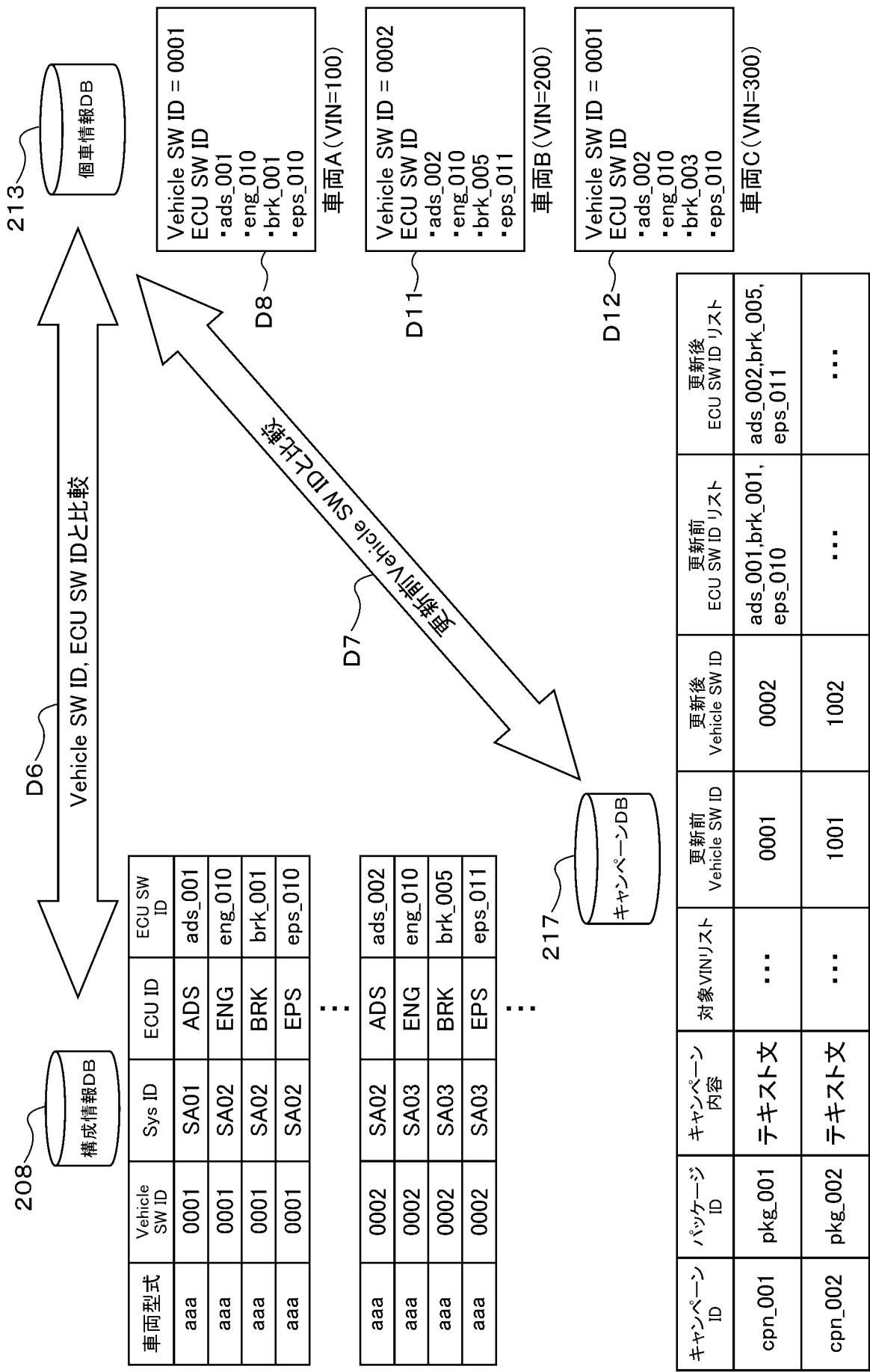
[図255]

Fig.255



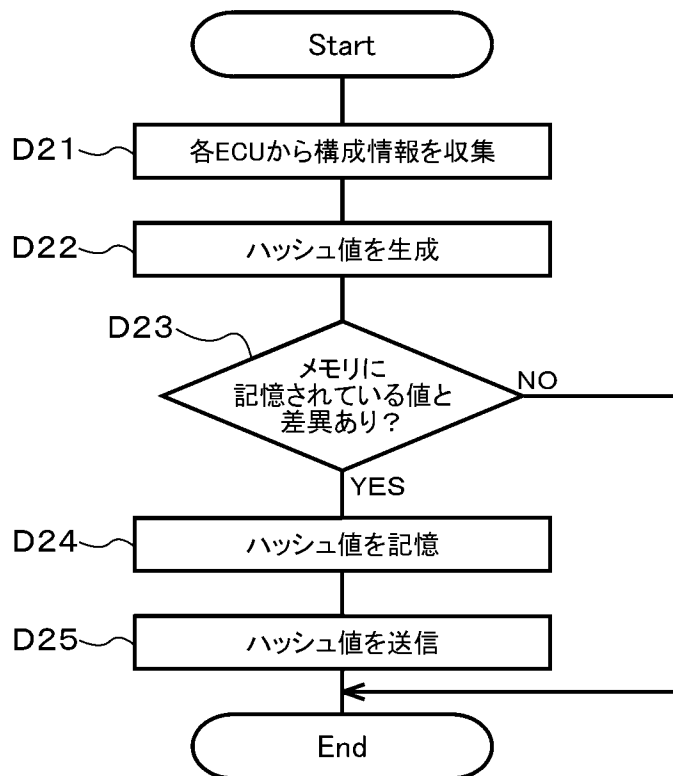
[図256]

Fig.256



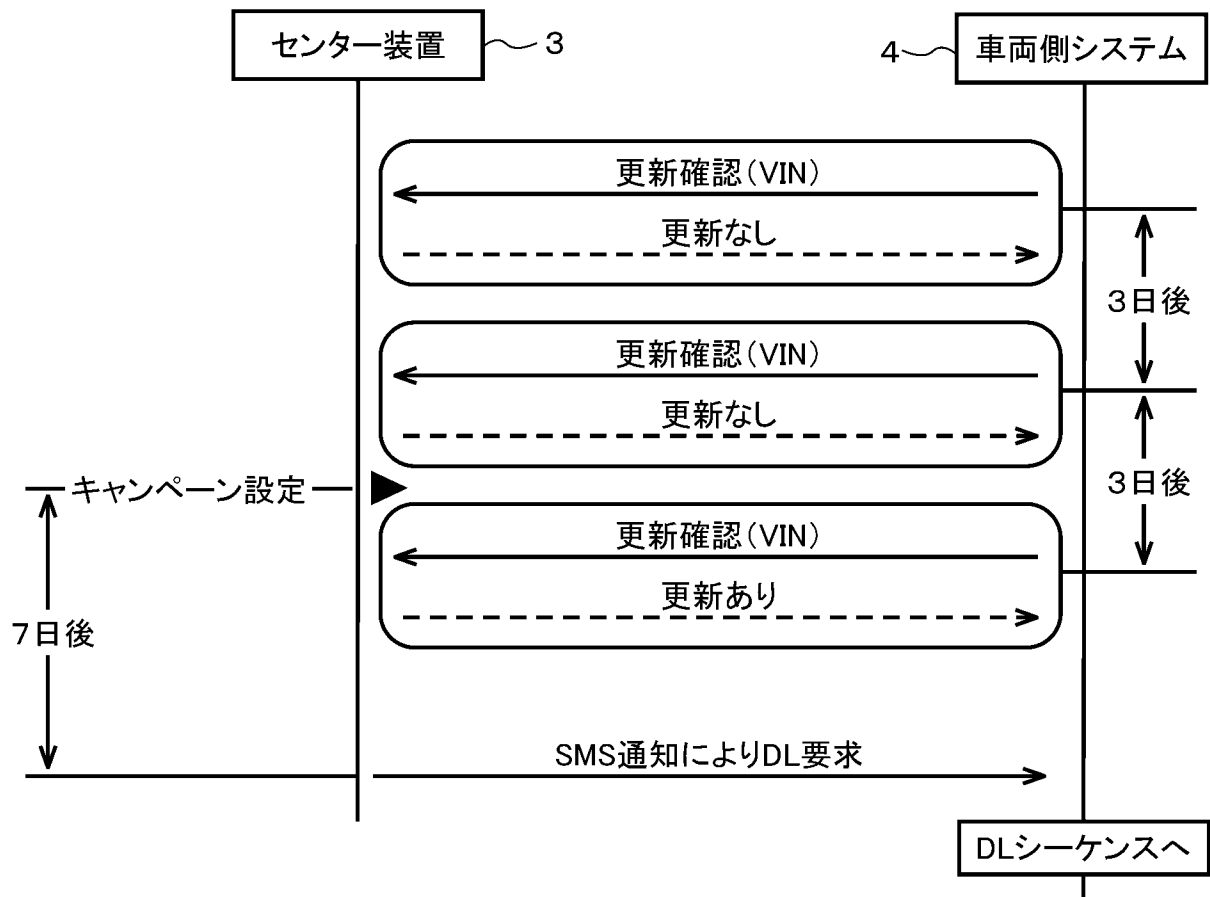
[図257]

Fig.257



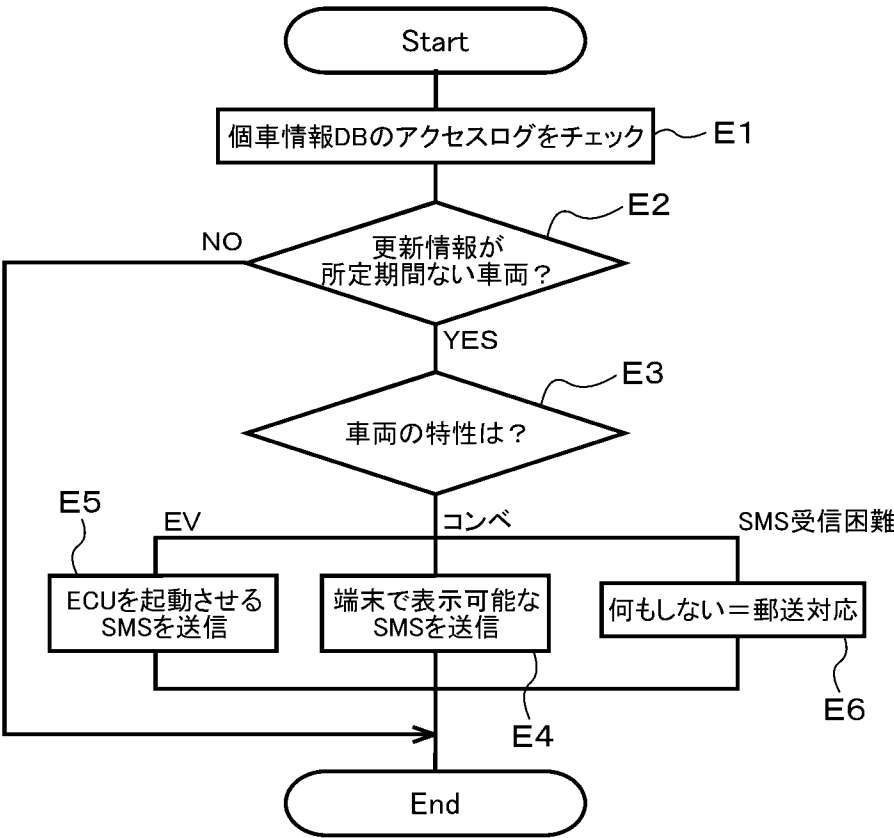
[図258]

Fig.258



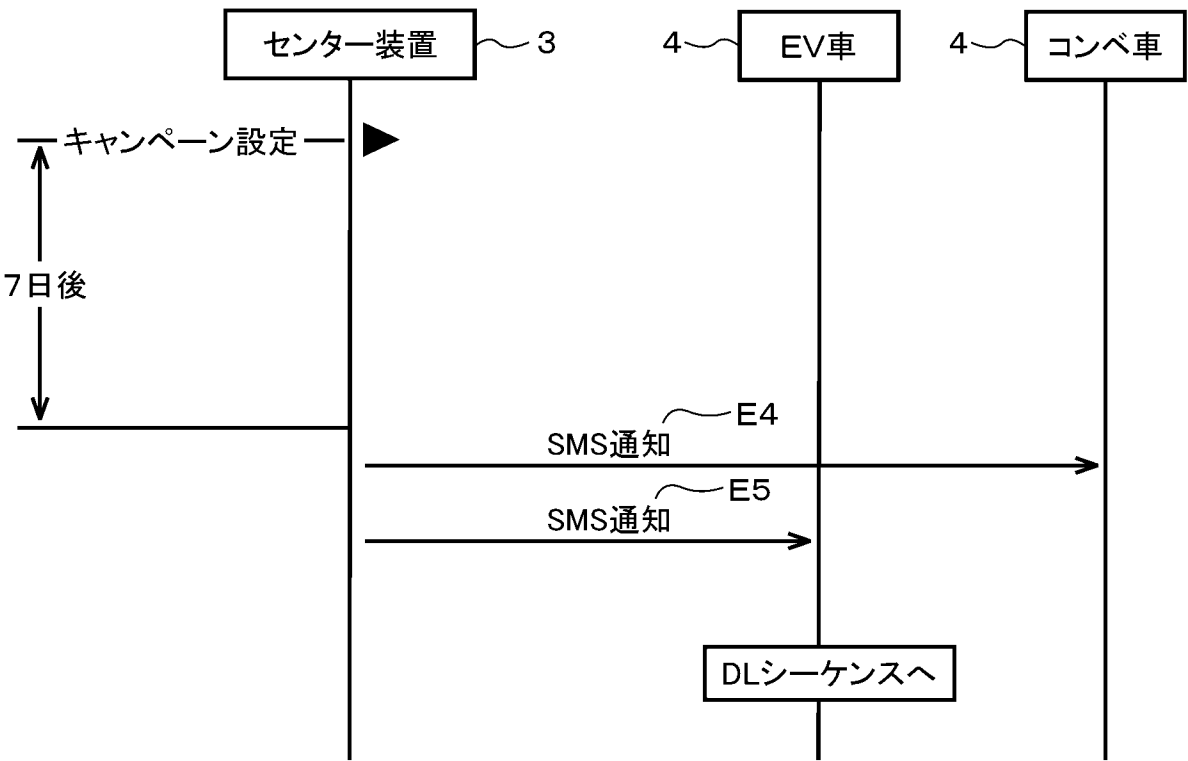
[図259]

Fig.259



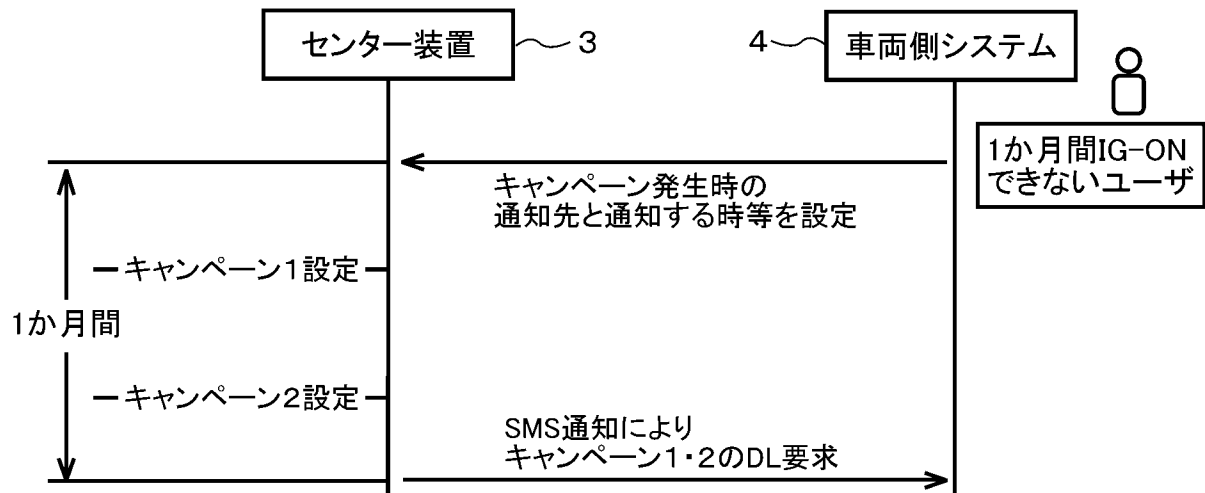
[図260]

Fig.260



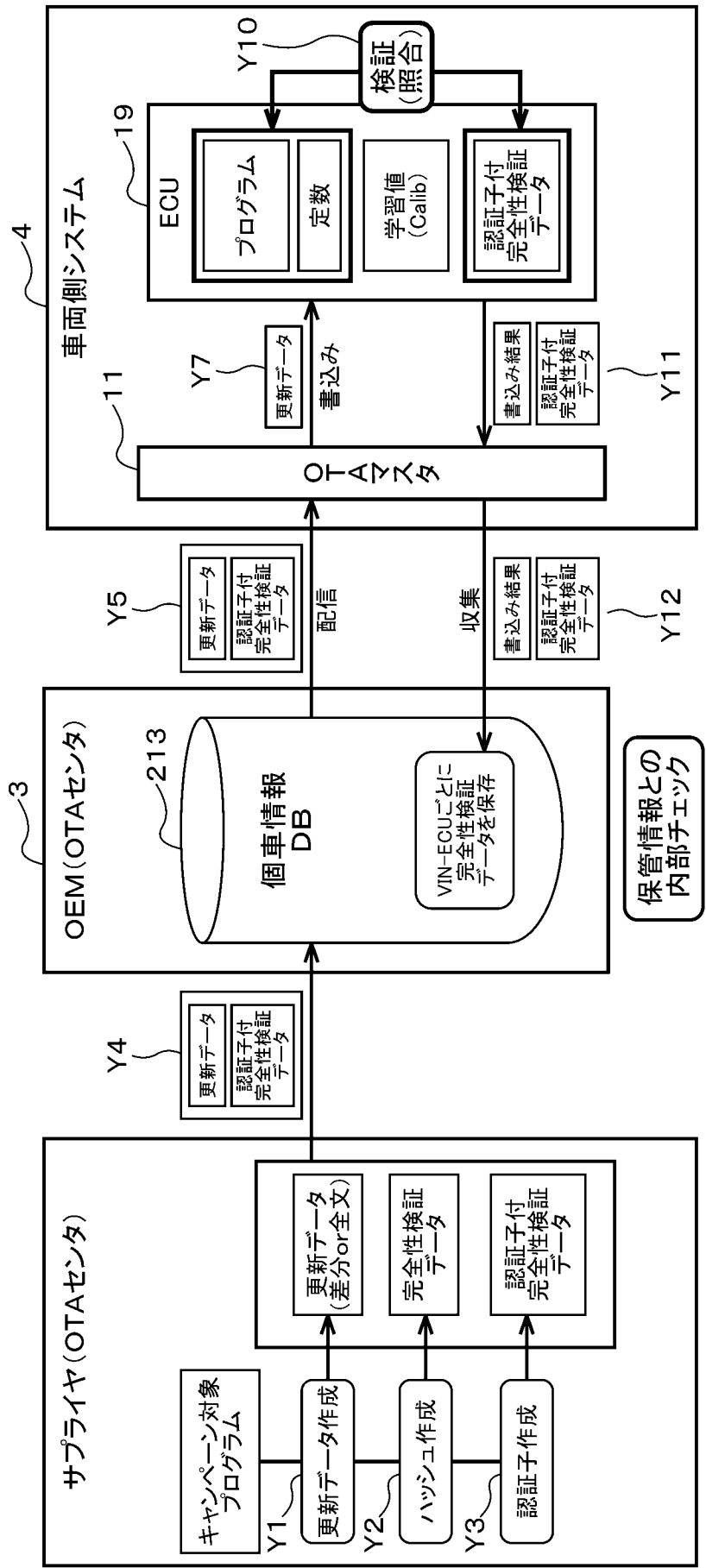
[図261]

Fig.261



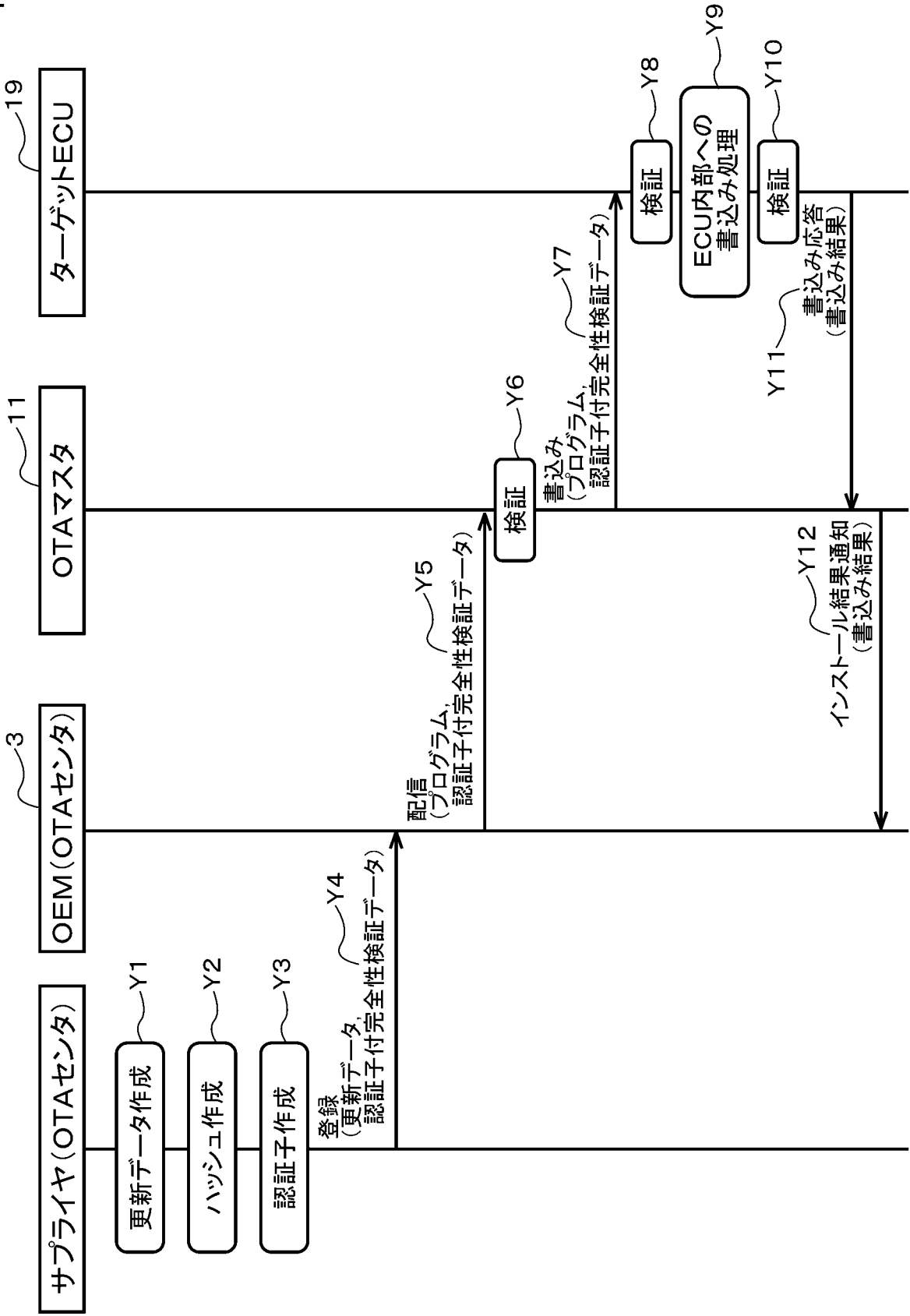
[図262]

Fig.262



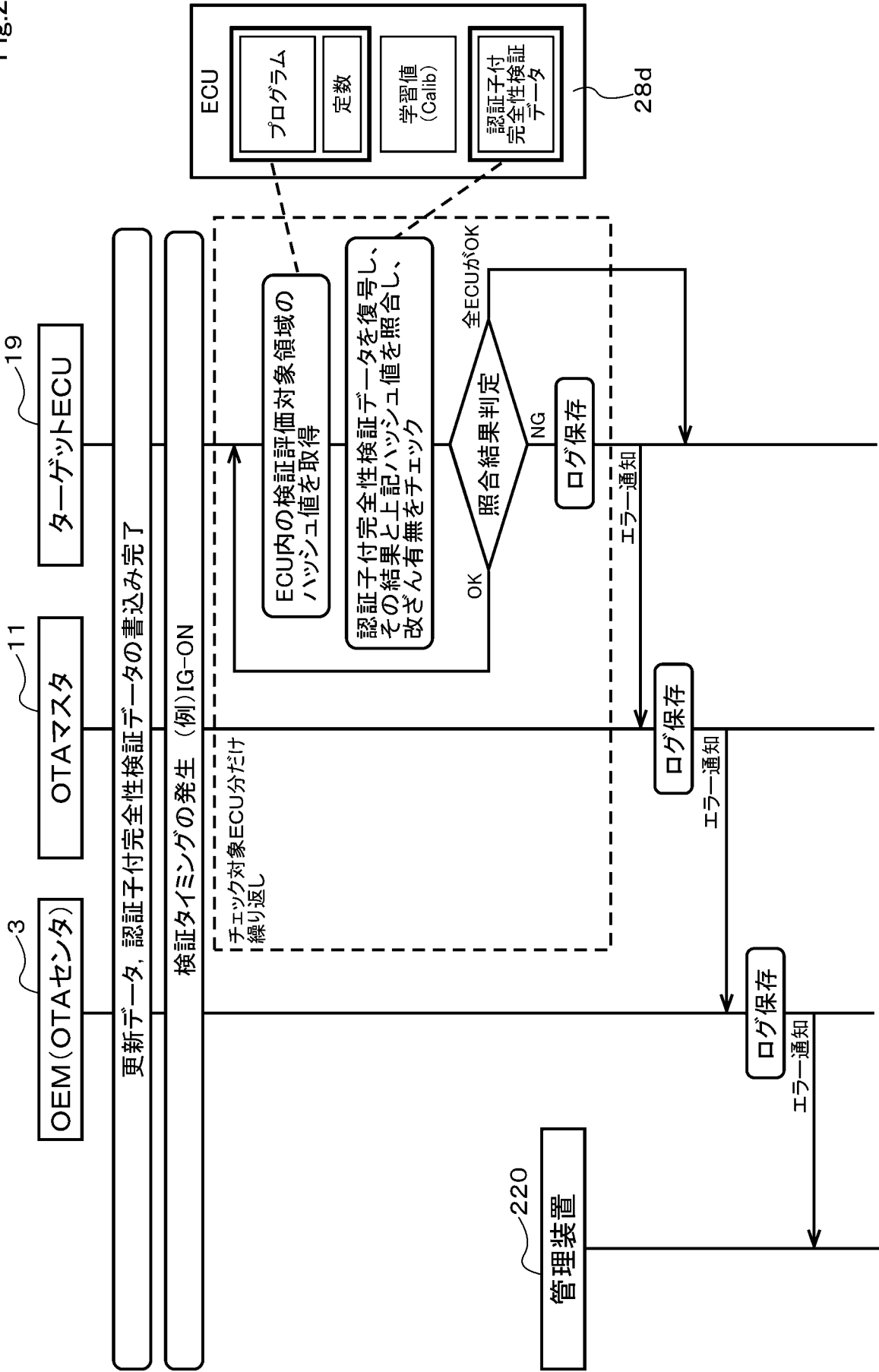
[図263]

Fig.263



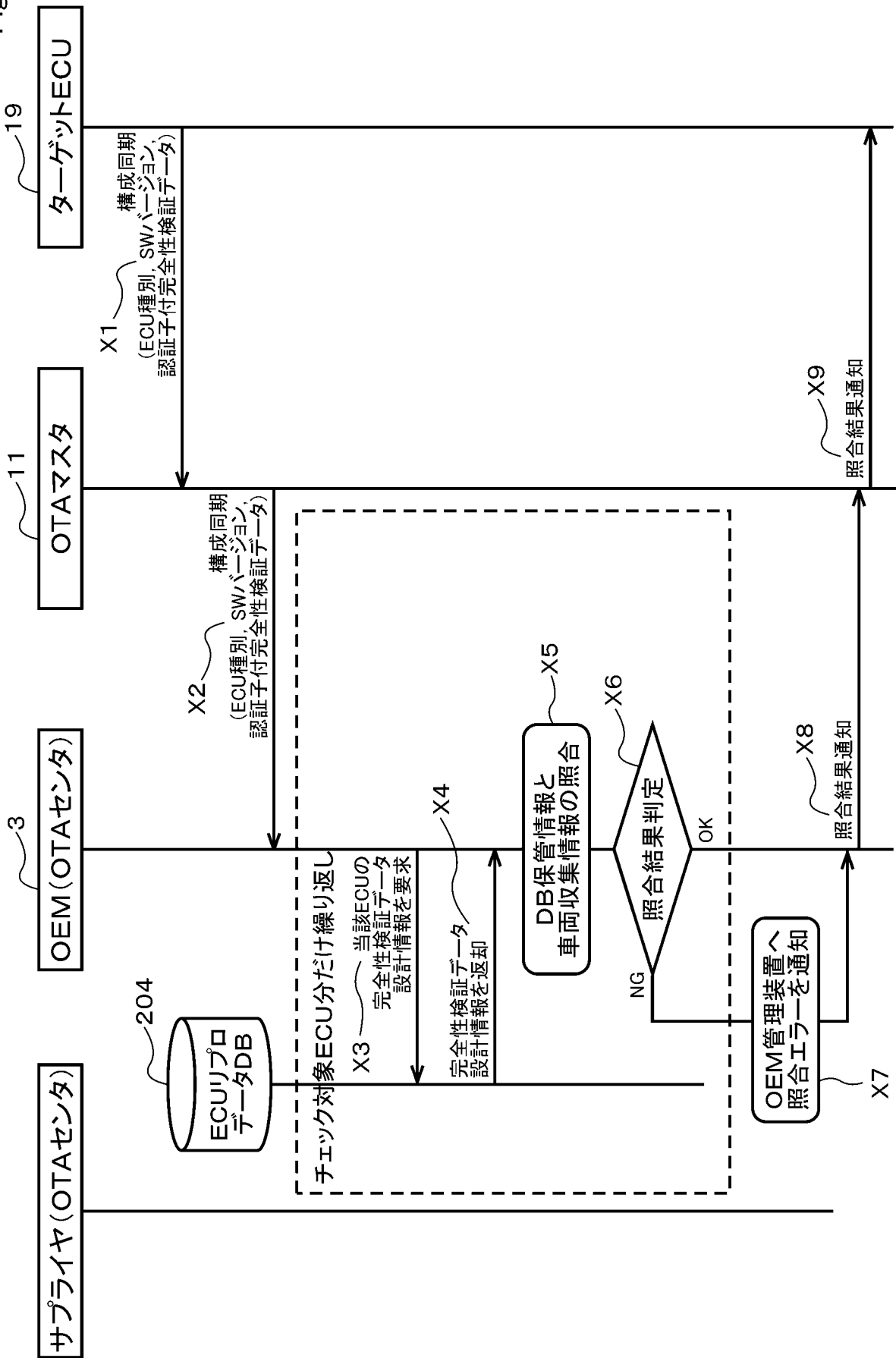
[図264]

Fig.264



[図265]

Fig.265



[図266]

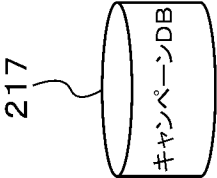
Fig.266



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]

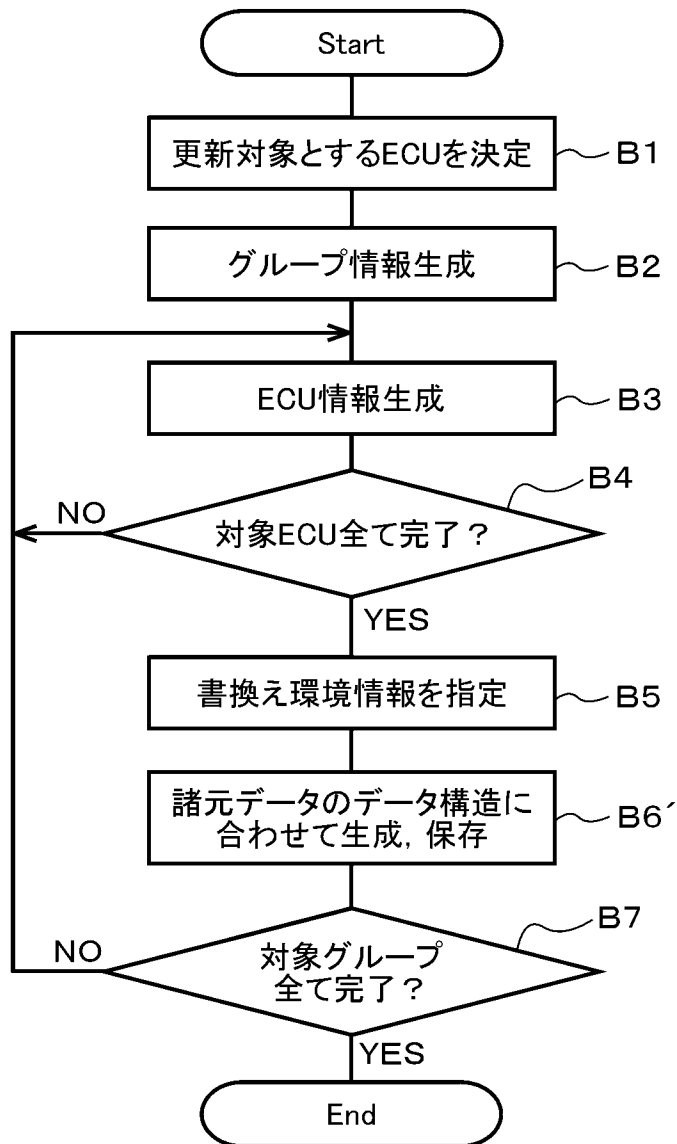
Fig.267



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	...	...

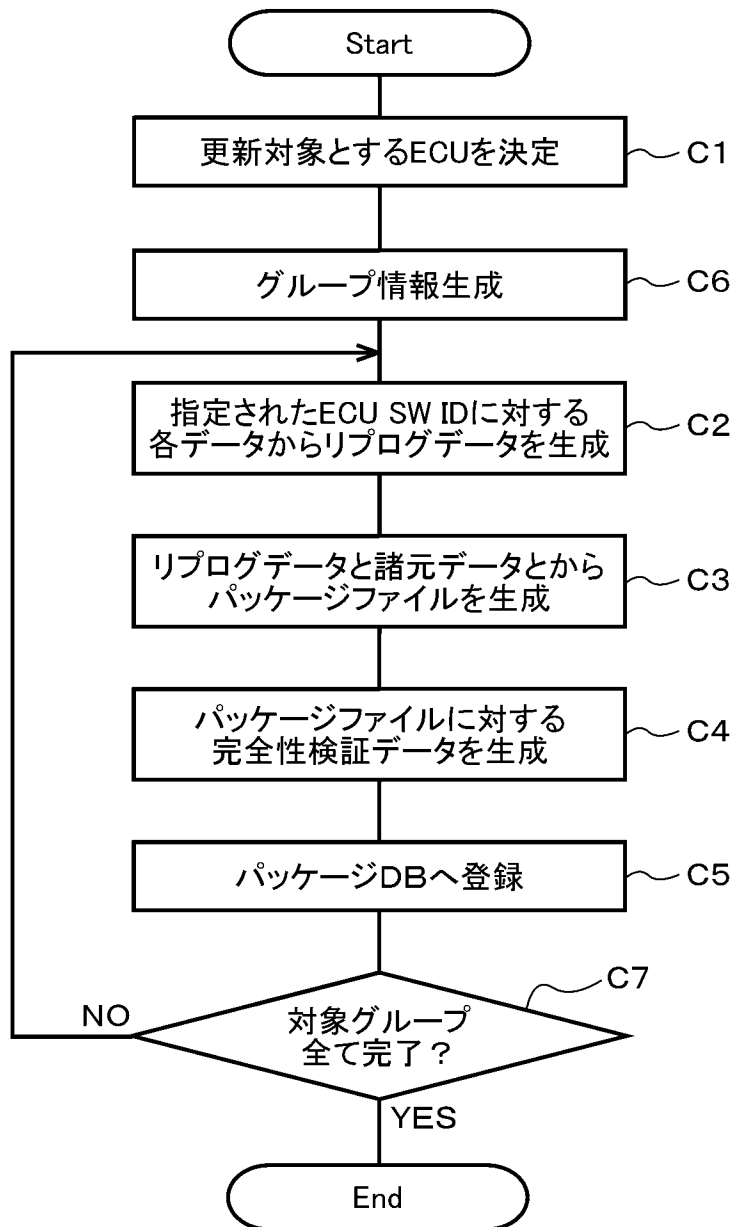
[図268]

Fig.268



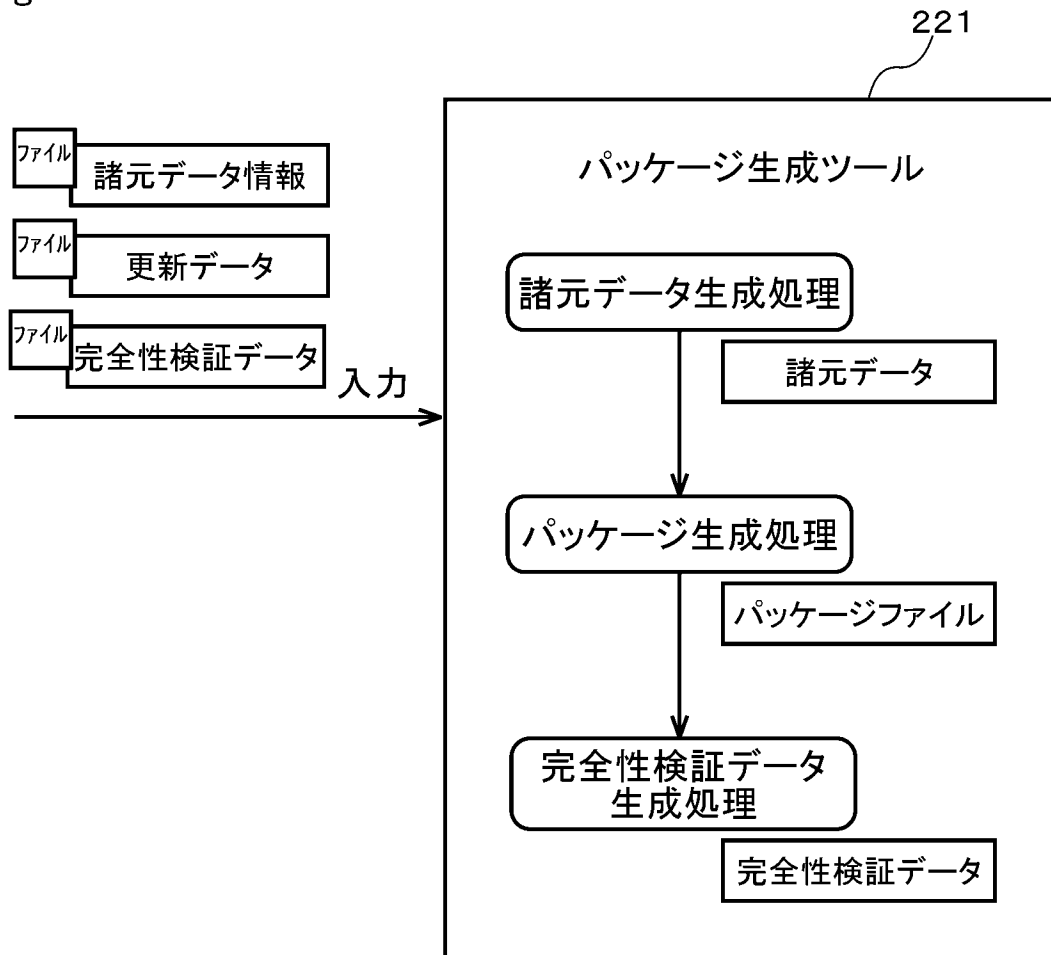
[図269]

Fig.269



[図270]

Fig.270



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/030945

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.
Y	JP 2012-091754 A (HONDA MOTOR CO., LTD.) 17 May 2012, paragraphs [0017]-[0036], [0058]-[0104], [0117]-[0124] (Family: none)	1-10
Y	JP 2016-218932 A (KYOCERA CORP.) 22 December 2016, paragraphs [0015]-[0016], [0044], [0062] & US 2018/0150290 A1, paragraphs [0024]-[0025], [0052], [0070] & WO 2016/190377 A1	1-10



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

"I" 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
15 October 2019 (15.10.2019)

Date of mailing of the international search report
21 October 2019 (21.10.2019)

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/JP2019/030945

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2012/017719 A1 (HONDA MOTOR CO., LTD.) 09 February 2012, paragraphs [0075] & US 2013/0197712 A1, paragraph [0104] & EP 2602157 A1 & CN 103052539 A	7-8

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
Y	JP 2012-091754 A（本田技研工業株式会社）2012.05.17, 段落[0017]-[0036], [0058]-[0104], [0117]-[0124]（ファミリーなし）	1-10
Y	JP 2016-218932 A（京セラ株式会社）2016.12.22, 段落[0015]-[0016], [0044], [0062] & US 2018/0150290 A1, 段落[0024]-[0025], [0052], [0070] & WO 2016/190377 A1	1-10

☒ 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

15.10.2019

国際調査報告の発送日

21.10.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

多胡 滋

5B

3562

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	WO 2012/017719 A1 (本田技研工業株式会社) 2012. 02. 09, 段落[0075] & US 2013/0197712 A1, 段落[0104] & EP 2602157 A1 & CN 103052539 A	7 - 8