

(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
2015 年 11 月 12 日(12.11.2015)



(10) 国際公開番号
WO 2015/170526 A1

- (51) 国際特許分類:
B60R 16/02 (2006.01) **G01M 17/007** (2006.01)
- (21) 国際出願番号: PCT/JP2015/059500
- (22) 国際出願日: 2015 年 3 月 26 日(26.03.2015)
- (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 2014-096112 2014 年 5 月 7 日(07.05.2014) JP
- (71) 出願人: 日立オートモティブシステムズ株式会社 (HITACHI AUTOMOTIVE SYSTEMS, LTD.) [JP/JP]; 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 Ibaraki (JP).
- (72) 発明者: 森田 伸義 (MORITA, Nobuyoshi); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP). 萱島 信

(KAYASHIMA, Makoto); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP). 伯田 恵輔 (HAKUTA, Keisuke); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP). 大和田 徹 (OWADA, Toru); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP).

(74) 代理人: 大賀 眞司, 外 (OHGA, Shinji et al.); 〒1400002 東京都品川区東品川二丁目 3 番 1 2 号 シーフォースクエア センタービルディング 1 6 階 サンネクスト国際特許事務所 Tokyo (JP).

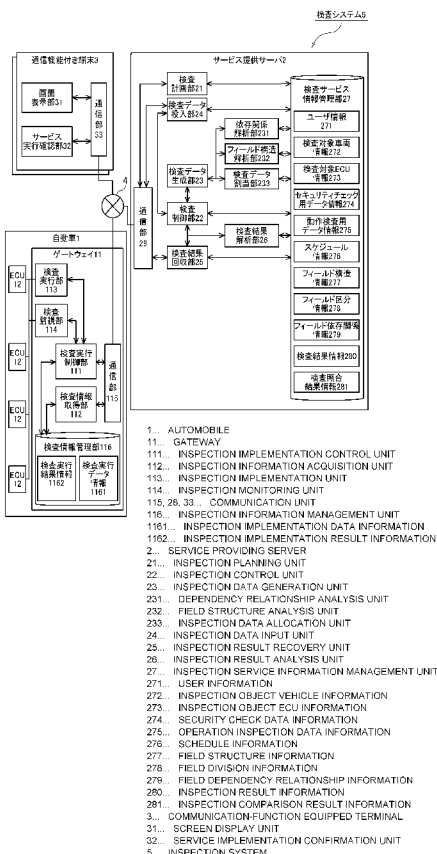
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN,

[続葉有]

(54) Title: INSPECTION DEVICE, INSPECTION SYSTEM, AND INSPECTION METHOD

(54) 発明の名称: 検査装置、検査システム及び検査方法

[図 1]



(57) Abstract: [Problem] To propose an inspection device, an inspection system, and an inspection method whereby the operation of a control device being used can be accurately inspected. [Solution] An inspection device for inspecting the operation of an ECU connected to a vehicle-mounted network is provided with an inspection implementation control unit that transmits two pieces of data including operation inspection data used for inspecting the operation of the ECU and security check data to the ECU, and that receives data outputted from the ECU, and is characterized in that the operation inspection data are data generated in advance on the basis of ECU design information, and that the security check data are data partially or entirely replacing the operation inspection data with random data.

(57) 要約: 【課題】運用時における制御装置の動作を正確に検査し得る検査装置、検査システム及び検査方法を提案する。【解決手段】車載ネットワークに接続された ECU の動作を検査する検査装置において、ECU の動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの 2 つのデータを ECU に送信し、ECU から出力されるデータを受信する検査実行制御部を備え、動作検査用データは、ECU の設計情報に基づいて予め生成されるデータであり、セキュリティチェック用データは、動作検査用データの一部又は全部をランダムデータに置き換えたデータであることを特徴とする。

WO 2015/170526 A1



IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

ロシア (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).

(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

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称： 検査装置、検査システム及び検査方法

技術分野

[0001] 本発明は、自動車に搭載された制御装置の動作を検査する検査装置、検査システム及び検査方法に関し、特に車載ネットワークに接続された制御装置の動作を検査する検査装置、検査システム及び検査方法に適用して好適なものである。

背景技術

[0002] 近年、自動車に搭載された複数の制御装置（Electronic Control Unit：ECU）を車載ネットワーク（Controller Area Network：CAN）に接続し、この車載ネットワークを介して、複数の制御装置を連携して動作させる技術が開発されている。

[0003] 複数のECUには、例えばエンジンの制御を行うエンジンECU、シフトチェンジの制御を行うトランスミッションECU及びブレーキ油圧の調整を行うブレーキECU等がある。そして特許文献1には、これら複数のECUが連携して動作する場合に連携動作の不具合を判断し、故障個所を特定する技術が開示されている。

[0004] 具体的に特許文献1には、車載ネットワークを介してECU間で送受信されるデータに基づいて、連係動作による不具合の発生を判断する不具合判断手段と、不具合の発生が判断されると、不具合に対応させて予め用意された検査診断プログラムを取得するプログラム取得手段と、検査診断プログラムを実行することによりECUに対して対応処理を実行させて、対応処理の実行によりECUから送信される情報に基づいて、故障個所を特定する故障個所特定手段とを備えた故障診断システムが開示されている。

先行技術文献

特許文献

[0005] 特許文献1：特許第4622177号公報

発明の概要

発明が解決しようとする課題

[0006] しかし特許文献 1 に記載の故障診断システムでは、予め用意された検査診断プログラムを用いて故障箇所を特定するものであり、検査診断プログラムは ECU の設計情報に基づいて、運用前に予め生成されるプログラムであることから、運用時において設計段階では想定されないデータが ECU に送信された場合に ECU が正常に動作するか否かを判断することはできない。

[0007] すなわち故障（機能不全）についてはその故障を特定することはできるが、動作はしているがその動作が正常であるのか異常であるのかを正確に判断することはできない。

[0008] 本発明は以上の点を考慮してなされたものであり、運用時における ECU の動作を正確に検査し得る検査装置、検査システム及び検査方法を提案する。

課題を解決するための手段

[0009] かかる課題を解決するために、本発明の検査装置においては、ECU の動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの 2 つのデータを ECU に送信し、ECU から出力されるデータを受信する検査実行制御部を備え、動作検査用データは、ECU の設計情報に基づいて予め生成されるデータであり、セキュリティチェック用データは、動作検査用データの一部又は全部をランダムデータに置き換えたデータであることを特徴とする。

[0010] またかかる課題を解決するために、本発明の検査システムにおいては、ECU の動作を検査するスケジュールを計画する検査計画部と、ECU の動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの 2 つのデータを生成する検査データ生成部と、計画されたスケジュールに従って、生成された 2 つのデータを外部に送信する検査制御部とを備えるサービス提供サーバと、サービス提供サーバから送信される動作検査用データ及びセキュリティチェック用データの 2 つのデータを受信した場合、

受信した2つのデータをECUに送信し、ECUから出力されるデータを受信した場合、受信したデータを含む検査実行結果情報をサービス提供サーバに送信するゲートウェイとを備え、動作検査用データは、ECUの設計情報に基づいて予め生成されるデータであり、セキュリティチェック用データは、動作検査用データの一部又は全部をランダムデータに置き換えたデータであることを特徴とする。

[0011] またかかる課題を解決するために、本発明の検査方法においては、検査計画部が、ECUの動作を検査するスケジュールを計画する第1のステップと、検査データ生成部が、ECUの動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの2つのデータを生成する第2のステップと、検査制御部が、計画されたスケジュールに従って、生成された2つのデータを外部に送信する第3のステップとを備え、ゲートウェイが、サービス提供サーバから送信される動作検査用データ及びセキュリティチェック用データの2つのデータを受信した場合、受信した2つのデータをECUに送信し、ECUから出力されるデータを受信した場合、受信したデータを含む検査実行結果情報をサービス提供サーバに送信する第4のステップとを備え、動作検査用データは、ECUの設計情報に基づいて予め生成されるデータであり、セキュリティチェック用データは、動作検査用データの一部又は全部をランダムデータに置き換えたデータであることを特徴とする。

発明の効果

[0012] 本発明によれば、運用時におけるECUの動作を正確に検査することができる。

図面の簡単な説明

[0013] [図1]本実施の形態における検査システムの全体構成図である。

[図2]ユーザ情報の論理構成図である。

[図3]検査対象車両情報の論理構成図である。

[図4]検査対象ECU情報の論理構成図である。

[図5]セキュリティチェック用データ情報の論理構成図である。

[図6]動作検査用データ情報の論理構成図である。

[図7]スケジュール情報の論理構成図である。

[図8]フィールド構造情報の論理構成図である。

[図9]フィールド区分情報の論理構成図である。

[図10]フィールド依存関係情報の論理構成図である。

[図11]検査結果情報の論理構成図である。

[図12]検査照合結果情報の論理構成図である。

[図13]検査実行データ情報の論理構成図である。

[図14]検査実行結果情報の論理構成図である。

[図15]データフレーム構造の構成図である。

[図16]スケジュール承認画面の画面構成図である。

[図17]スケジュール登録処理のフローチャートである。

[図18]通信機能付端末側のスケジュール登録処理のフローチャートである。

[図19]サービス提供サーバ側のスケジュール登録処理のフローチャートである。

[図20]E C U検査処理のフローチャートである。

[図21]通信機能付端末側のE C U検査処理のフローチャートである。

[図22]サービス提供サーバ側のE C U検査処理のフローチャートである。

[図23]自動車のゲートウェイ側のE C U検査処理のフローチャートである。

[図24]セキュリティチェック用データ生成処理のフローチャートである。

[図25]ゲートウェイが検査結果を解析する場合のE C U検査処理のフローチャートである。

発明を実施するための形態

[0014] 以下図面について、本発明の一実施の形態を詳述する。

[0015] (1) 全体構成

図1は、本実施の形態における検査システム5の全体構成を示す。検査システム5は、自動車1、サービス提供サーバ2及び通信機能付き端末3を備えて構成される。またこれら自動車1、サービス提供サーバ2及び通信機能

付き端末 3 は、通信網 4 を介して互いに通信可能に接続される。通信網 4 は、例えば携帯電話網又は無線 LAN (Local Area Network) である。

[0016] 自動車 1 は、ゲートウェイ 11 及び複数の ECU (Electronic Control Unit) 12 を備えて構成される。ゲートウェイ 11 と各 ECU 12 との間は、CAN (Controller Area Network) と呼ばれる車載ネットワークにより接続される。

[0017] ゲートウェイ 11 は、ここでは検査装置として機能する端末であり、検査実行制御部 111、検査情報取得部 112、検査実行部 113、検査監視部 114、通信部 115 及び検査情報管理部 116 を備えて構成される。

[0018] 検査実行制御部 111 は、通信部 115 を介して受信した検査実行データ情報 1161 を検査情報管理部 116 に格納し、また検査情報管理部 116 に格納した検査実行データ情報 1161 を取得して ECU 12 に送信する。検査実行データ情報 1161 には、動作検査用データ及びセキュリティチェック用データがある。

[0019] 動作検査用データとは、設計情報に基づいて、設計段階で予め生成される ECU 12 のテスト用のデータである。詳細については後述する (図 6)。またセキュリティチェック用データとは、実際の運用時において ECU 12 の動作が正常であるのか異常であるのかを検査及び診断するためのテスト用のデータである。詳細については後述する (図 5)。なおこれらをまとめて検査用データと呼ぶ場合がある。

[0020] 検査情報取得部 112 は、検査情報管理部 116 に格納されている検査実行結果情報 1162 を取得し、通信部 115 を介して、この検査実行結果情報 1162 をサービス提供サーバ 2 に送信する。検査実行部 113 は、検査実行制御部 111 からの検査実行要求に基づいて、動作検査用データ及びセキュリティチェック用データを ECU 12 に送信する。

[0021] 検査監視部 114 は、動作検査用データ及びセキュリティチェック用データに基づいて ECU 12 から出力されるデータを監視及び取得し、取得したデータを検査実行結果情報 1162 として検査情報管理部 116 に格納する

。

[0022] ECU12は、自動車1が備える各種機器を制御する制御装置である。ECU12には、例えばエンジンの制御を行うエンジンECU、シフトチェンジの制御を行うトランスミッションECU及びブレーキ油圧の調整を行うブレーキECU等がある。

[0023] サービス提供サーバ2は、検査計画部21、検査制御部22、検査データ生成部23、依存関係解析部231、フィールド構造解析部232、検査データ割当部233、検査データ投入部24、検査結果回収部25、検査結果解析部26及び検査サービス情報管理部27を備えて構成される。

[0024] 検査計画部21は、ECU12に対して実行する検査のスケジュールを計画し、計画したスケジュールを自動車1の利用者が所有する通信機能付き端末3に送信し、通信機能付き端末3において承認されたスケジュールを受信して、このスケジュールを検査サービス情報管理部27に格納する。

[0025] 検査制御部22は、検査データ生成部23、検査データ投入部24、検査結果回収部25及び検査結果解析部26の動作を統括的に制御する。

[0026] 検査データ生成部23は、依存関係解析部231、フィールド構造解析部232及び検査データ割当部233を用いてセキュリティチェック用データを生成し、生成したセキュリティチェック用データを検査サービス情報管理部27に格納する。

[0027] 検査データ投入部24は、検査の実行を通知するお知らせを自動車1の利用者が所有する通信機能付き端末3に送信し、検査サービス情報管理部27からセキュリティチェック用データ及び動作検査用データを取得して検査対象の自動車1に送信する。

[0028] 検査結果回収部25は、ゲートウェイ11から検査完了通知を受信すると、検査実行結果情報1162の回収要求をゲートウェイ11に送信し、ゲートウェイ11から回収した検査実行結果情報1162を検査サービス情報管理部27に格納する。

[0029] 検査結果解析部26は、検査サービス情報管理部27から検査結果情報2

８０及び検査照合結果情報２８１を取得し、両者を比較して、ＥＣＵ１２から出力された信号が異常であるか否かを解析する。

[0030] 検査サービス情報管理部２７は、サービス提供サーバ２の動作に必要な各種情報（２７１～２８１）を備える。各種情報の詳細については後述する（図２～図１４）。

[0031] 通信機能付き端末３は、画面表示部３１、サービス実行確認部３２及び通信部３３を備えて構成される。画面表示部３１は、サービス提供サーバ２により計画された検査のスケジュールを表示画面に表示し、またサービス提供サーバ２により解析された検査結果を表示画面に表示する。サービス実行確認部３２は、表示画面に表示された検査のスケジュールについて、編集及び承認の処理を実行する。

[0032] （２）テーブル構成

以下図２～図１２を参照して、サービス提供サーバ２の検査サービス情報管理部２７に格納されている各種情報について説明する。

[0033] 図２は、ユーザ情報２７１の論理構成を示す。ユーザ情報２７１は、ユーザＩＤ欄２７１１、ユーザＰＡＳＳ欄２７１２及びユーザ名欄２７１３から構成される。ユーザＩＤ欄２７１１には、検査システム５を利用するユーザの識別情報が格納され、ユーザＰＡＳＳ欄２７１２には、ユーザのパスワードが格納される。またユーザ名欄２７１３には、ユーザ名が格納される。

[0034] 図３は、検査対象車両情報２７２の論理構成を示す。検査対象車両情報２７２は、ユーザＩＤ欄２７２１、ＶＩＮ（Vehicle Identification Number）欄２７２２、メーカー欄２７２３、車種欄２７２４、車色欄２７２５及び車両ナンバ欄２７２６から構成される。

[0035] ユーザＩＤ欄２７２１には、ユーザの識別情報が格納され、ＶＩＮ欄２７２２には、検査対象の自動車１を識別する識別情報が格納される。またメーカー欄２７２３には、自動車１のメーカー名が格納され、車種欄２７２４には、自動車１の車種が格納され、車色欄２７２５には、自動車１の色が格納される。また車両ナンバ欄２７２６には、自動車１の車両ナンバが格納される。

- [0036] 図4は、検査対象ECU情報273の論理構成を示す。検査対象ECU情報273は、車種欄2731、ECU-ID欄2732、ECU名欄2733、検査対象フラグ欄2734、検査期限欄2735及びCAN-ID欄2736から構成される。
- [0037] 車種欄2731には、検査対象の自動車1の車種が格納され、ECU-ID欄2732には、検査対象のECU12を識別する識別情報が格納される。またECU名欄2733には、ECU名が格納され、検査対象フラグ欄2734には、検査対象であるか否かの情報が格納され、例えば「対象」又は「非対象」が格納される。
- [0038] また検査期限欄2735には、検査の期限が格納され、CAN-ID欄2736には、検査対象のECU12が接続しているCANの識別情報が格納される。
- [0039] 図5は、セキュリティチェック用データ情報274の論理構成を示す。セキュリティチェック用データ情報274は、検査ID欄2741、ECU-ID欄2742、CAN-ID欄2743及び検査データ欄2744から構成される。
- [0040] 検査ID欄2741には、検査対象のECU12ごとに割り当てられたセキュリティチェック用データを用いた検査を識別する識別情報が格納され、ECU-ID欄2742には、セキュリティチェック用データを用いた検査の対象となるECU12を識別する識別情報が格納される。
- [0041] またCAN-ID欄2743には、検査対象のECU12が接続しているCANの識別情報が格納され、検査データ欄2744には、検査用データが格納され、例えばCANプロトコルのデータフィールドに該当するデータが格納される。
- [0042] 図6は、動作検査用データ情報275の論理構成を示す。動作検査用データ情報275は、セキュリティチェック用データ情報274と同様、検査ID欄2751、ECU-ID欄2752、CAN-ID欄2753及び検査データ欄2754から構成される。

- [0043] 検査ＩＤ欄２７５１には、検査対象のＥＣＵ１２ごとに割り当てられた動作検査用データを用いた検査を識別する識別情報が格納され、ＥＣＵ－ＩＤ欄２７５２には、動作検査用データを用いた検査の対象となるＥＣＵ１２を識別する識別情報が格納される。
- [0044] またＣＡＮ－ＩＤ欄２７５３には、検査対象のＥＣＵ１２が接続しているＣＡＮの識別情報が格納され、検査データ欄２７５４には、検査用データが格納され、例えばＣＡＮプロトコルのデータフィールドに該当するデータが格納される。
- [0045] 図７は、スケジュール情報２７６の論理構成を示す。スケジュール情報２７６は、ＶＩＮ欄２７６１、日時欄２７６２及び検査ＩＤ欄２７６３から構成される。ＶＩＮ欄２７６１には、検査対象の自動車１を識別する識別情報が格納される。
- [0046] 日時欄２７６２には、検査対象の自動車１の利用者が承認した検査日時が格納され、検査ＩＤ欄２７６３には、自動車１に対して実行する検査を識別する識別情報が格納される。
- [0047] 図８は、フィールド構造情報２７７の論理構成を示す。フィールド構造情報２７７は、車種欄２７７１、ＣＡＮ－ＩＤ欄２７７２、詳細フィールドＩＤ欄２７７３、区分ＩＤ欄２７７４及びビット数欄２７７５から構成される。
- [0048] 車種欄２７７１には、検査対象の自動車１の車種が格納され、ＣＡＮ－ＩＤ欄２７７２には、検査対象のＥＣＵ１２が接続しているＣＡＮの識別情報が格納される。
- [0049] また詳細フィールドＩＤ欄２７７３には、ＥＣＵ１２のアプリケーションの設計情報に基づいて、ＣＡＮプロトコルのデータフィールドをより詳細に分類した意味を持つ区分を識別する識別情報が格納され、区分ＩＤ欄２７７４には、ＥＣＵ１２のアプリケーションの設計情報に基づいてデータの持つ意味を識別する識別情報が格納される。
- [0050] 例えば区分ＩＤ欄２７７４には、「有効桁、可変データ、予約データ、ダ

ミーデータ、チェックサム等」の区分を識別するための固有値が格納される。ビット数欄 2775 には、詳細フィールド ID に割り当てられているビット数が格納される。

[0051] 図 9 は、フィールド区分情報 278 の論理構成を示す。フィールド区分情報 278 は、区分 ID 欄 2781 及び区分名称欄 2782 から構成される。区分 ID 欄 2781 には、CAN プロトコルのデータフィールドで用いられるデータの種別を識別する識別情報が格納される。

[0052] また区分名称欄 2782 には、区分 ID に対応する CAN プロトコルのデータフィールドで用いられるデータの種類の名称が格納される。例えばデータの種類の名称は、「有効桁、可変データ、予約データ、ダミーデータ、チェックサム等」のように区分してもよい。

[0053] 図 10 は、フィールド依存関係情報 279 の論理構成を示す。フィールド依存関係情報 279 は、車種欄 2791、CAN-ID 欄 2792 及び詳細フィールドの依存関係欄 2793 から構成される。車種欄 2791 には、検査対象の自動車 1 の識別情報が格納され、CAN-ID 欄 2792 には、検査対象の ECU 12 が接続している CAN の識別情報が格納される。

[0054] 詳細フィールドの依存関係欄 2793 には、ECU 12 のアプリケーションの設計情報における分岐処理の条件や関数呼び出しの引数としての使われ方等に基づいて ECU 12 のアプリケーションにおける詳細フィールド ID (図 8) の処理依存の関係を示す情報が格納され、例えば詳細フィールド ID (図 8) の A1 と A2 とに依存関係がある場合には「&」を用いて「A1 & A2」が格納される。

[0055] 図 11 は、検査結果情報 280 の論理構成を示す。検査結果情報 280 は、VIN 欄 2801、検査結果欄 2802 及び実施検査 ID 欄 2803 から構成される。VIN 欄 2801 には、検査対象の自動車 1 を識別する識別情報が格納され、検査結果欄 2802 には、実行された検査の結果がログファイルとして格納される。また実施検査 ID 欄 2803 には、自動車 1 に対して実行した検査を識別する識別情報が格納される。

[0056] 図 1 2 は、検査照合結果情報 2 8 1 の論理構成を示す。検査照合結果情報 2 8 1 は、車種欄 2 8 1 1、CAN-ID 欄 2 8 1 2、実施検査データ欄 2 8 1 3、予想出力データ欄 2 8 1 4 及び判定結果欄 2 8 1 5 から構成される。

[0057] 車種欄 2 8 1 1 には、検査対象の自動車 1 の車種が格納され、CAN-ID 欄 2 8 1 2 には、検査対象の ECU 1 2 が接続している CAN の識別情報が格納される。

[0058] また実施検査データ欄 2 8 1 3 には、ECU 1 2 に送信した検査用データが格納され、予想出力データ欄 2 8 1 4 には、実施した検査用データを ECU 1 2 に送信した結果、ECU 1 2 が出力すると予想されるデータが格納される。

[0059] また判定結果欄 2 8 1 5 には、予想出力データと、検査結果（図 1 1）のログファイルに格納されている出力データとを比較して判定した結果が格納され、例えば出力データが予想出力データの範囲内である場合には「異常なし」が格納され、範囲外である場合には「異常あり」が格納される。

[0060] 次いで以下図 1 3 及び図 1 4 を参照して、自動車 1 の検査情報管理部 1 1 6 に格納されている各種情報について説明する。

[0061] 図 1 3 は、検査実行データ情報 1 1 6 1 の論理構成を示す。検査実行データ情報 1 1 6 1 は、実行順欄 1 1 6 1 1、検査 ID 欄 1 1 6 1 2、CAN-ID 欄 1 1 6 1 3、検査データ欄 1 1 6 1 4 及び進捗状況欄 1 1 6 1 5 から構成される。

[0062] 実行順欄 1 1 6 1 1 には、検査データ欄 1 1 6 1 4 に格納されている検査用データを ECU 1 2 に送信する順序が格納され、検査 ID 欄 1 1 6 1 2 には、ECU 1 2 ごとに紐付けられた動作検査用データ又はセキュリティチェック用データを識別する識別情報が格納される。

[0063] また CAN-ID 欄 1 1 6 1 3 には、検査対象の ECU 1 2 が接続している CAN の識別情報が格納され、検査データ欄 1 1 6 1 4 には、ECU 1 2 に送信する検査用データ（動作検査用データ又はセキュリティチェック用デ

ータ)が格納される。

[0064] また進捗状況欄 1 1 6 1 5 には、検査データ欄 1 1 6 1 4 に格納されている検査用データを用いた検査が完了したか否かの情報が格納され、例えば検査用データを ECU 1 2 に送信し、ECU 1 2 から出力されるデータを取得したタイミングで「完了」が格納される。

[0065] 図 1 4 は、検査実行結果情報 1 1 6 2 の論理構成を示す。検査実行結果情報 1 1 6 2 は、検査 ID 欄 1 1 6 2 1 及び検査結果欄 1 1 6 2 2 から構成される。検査 ID 欄 1 1 6 2 1 には、ECU ごとに紐付けられた動作検査用データ又はセキュリティチェック用データを識別する識別情報が格納される。

[0066] また検査結果欄 1 1 6 2 2 には、検査実行部 1 1 3 が検査データ欄 1 1 6 1 4 に格納されている検査用データを ECU 1 2 に送信し、ECU 1 2 から出力されたデータが格納され、例えば「日付、ECU 1 2 に送信した検査用データ、ECU 1 2 から出力されたデータ」等を記録したログファイルが格納される。

[0067] (3) データ構造

図 1 5 は、データフレーム構造を示す。このデータフレーム構造は、国際標準化機構の ISO 15031 により規定されている。

[0068] SOF (Start Of Frame) フィールドは、データフレームの開始を示すフィールドであり、アービトレーションフィールドは、送信先を示す ID (Identifier) 及び RTR (Remote Transmission Request) から構成され、フレームの優先順位を示すフィールドである。コントローラフィールドは、予約ビット及びデータのバイト数を示すフィールドである。

[0069] なおアービトレーションフィールドを構成する ID は、本実施の形態においては CAN-ID であり、CAN-ID により、後述するデータフィールドの構造 (区分) が定められている。

[0070] データフィールドは、データ本体を格納するフィールドである。本実施の形態においては、このデータフィールドの一部又は全部にランダムデータを格納することにより、セキュリティチェック用データを生成している。なお

セキュリティチェック用データは、サービス提供サーバ２の検査データ生成部２３により生成される。

[0071] セキュリティチェック用データの生成処理の詳細については後述するが（図２４）、ここで簡単に説明すると、検査データ生成部２３により、まずデータフィールドの構造（区分）を解析し、例えば４つに区分されているという解析結果を得る。次に各区分の依存関係を解析し、最後に依存関係に基づいて、検査効率の良い何れかの区分にランダムデータを格納してセキュリティチェック用データを生成する。

[0072] またＣＲＣフィールドは、データフレームの誤りをチェックするフィールドである。またＡＣＫフィールドは、正常に受信した確認の合図を示すフィールドであり、ＥＯＦ（End Of Frame）フィールドは、データフレームの終了を示すフィールドである。

[0073] （４）画面構成

図１６は、通信機能付き端末３の画面表示部３１により表示される画面構成を示す。この画面は、検査のスケジュールがサービス提供サーバ２から通信機能付き端末３に送信された場合に通信機能付き端末３において編集又は承認する際の画面である。

[0074] ユーザ名領域３１１には、検査対象の自動車１の利用者として登録されているユーザ名が表示される。このユーザ名は、ユーザ名欄２７１３に格納されているユーザ名から取得される。メーカー領域３１２には、検査対象の自動車１のメーカー名が表示される。このメーカー名は、メーカー欄２７２３に格納されているメーカー名から取得される。

[0075] また車種領域３１３には、検査対象の自動車１の車種が表示される。この車種は、車種欄２７２４に格納されている車種から取得される。車色領域３１４には、検査対象の自動車１の車色が表示される。この車色は、車色欄２７２５に格納されている車色から取得される。車両ナンバ領域３１５には、検査対象の自動車１の車両ナンバが表示される。この車両ナンバは、車両ナンバ欄２７２６に格納されている車両ナンバから取得される。

[0076] また検査日時領域 3 1 6 には、検査計画部 2 1 が作成したスケジュールが編集可能に表示される。実施期限領域 3 1 7 には、検査の期限が表示される。この検査の期限は、検査期限欄 2 7 3 5 に格納されている検査の期限から取得される。また登録承認ボタン 3 1 8 は、検査日時領域 3 1 6 に表示される検査日時で検査が実行されることを承認する際に押下するためのボタンである。

[0077] (5) フローチャート

図 1 7 は、スケジュール登録処理の処理手順を示す。このスケジュール登録処理は、サービス提供サーバ 2 及び通信機能付き端末 3 により実行される。

[0078] まずサービス提供サーバ 2 の検査計画部 2 1 は、検査の承認依頼の通知を送信する (S P 1)。この検査の承認依頼の通知は、ID 及びパスワードの送信を要求する通知である。通信機能付き端末 3 のサービス実行確認部 3 2 は、この検査の承認依頼の通知を受信すると、利用者が入力した ID 及びパスワードをサービス提供サーバ 2 に送信する (S P 2)。

[0079] 次に検査計画部 2 1 は、ID 及びパスワードを受信すると、ユーザ情報 2 7 1 を参照して ID 及びパスワードの認証処理を実行する (S P 3)。そして検査計画部 2 1 は、認証処理により ID 及びパスワードを認証すると、検査対象車両情報 2 7 2 及び検査対象 ECU 情報 2 7 3 を参照して一又は複数の検査のスケジュールを作成し、作成したスケジュールの承認依頼の通知を通信機能付き端末 3 に送信する (S P 4)。

[0080] このスケジュールの承認依頼の通知は、ユーザ情報 2 7 1、検査対象車両情報 2 7 2 及び検査対象 ECU 情報 2 7 3 に含まれる各種情報とともにスケジュールを表示することを指示する通知である。画面表示部 3 1 は、スケジュールの承認依頼の通知を受信すると、この通知に含まれる各種情報とともにスケジュールを表示画面に表示する (S P 5)。なおここで表示される表示画面は、図 1 6 で説明した表示画面である。

[0081] サービス実行確認部 3 2 は、必要に応じてスケジュールを編集した後 (S

P 6)、登録承認ボタン 3 1 8 の押下によりスケジュールを承認する (S P 7)。そしてサービス実行確認部 3 2 は、承認したスケジュールをサービス提供サーバ 2 に送信する (S P 8)。検査計画部 2 1 は、通信機能付き端末 3 からのスケジュールを受信すると、このスケジュールをスケジュール情報 2 7 6 に格納する (S P 9)。

[0082] そして検査計画部 2 1 は、スケジュールを格納して登録が完了したことを通知する登録完了通知を送信する (S P 1 0)。画面表示部 3 1 は、登録完了通知を受信すると、登録が完了したことを示す登録完了画面を表示して (S P 1 1)、このスケジュール登録処理を終了する。

[0083] 図 1 8 は、通信機能付き端末 3 側のスケジュール登録処理の詳細な処理手順を示す。ここでは、図 1 7 のスケジュール登録処理において通信機能付き端末 3 が実行する処理の詳細な処理手順について説明する。

[0084] 通信機能付き端末 3 のサービス実行確認部 3 2 は、検査承認依頼待ちの状態において (S P 1 0 1)、サービス提供サーバ 2 から送信された検査の承認依頼の通知を受信したか否かを判断する (S P 1 0 2)。サービス実行確認部 3 2 は、ステップ S P 1 0 2 の判断で否定結果を得ると、ステップ S P 1 0 1 に移行して待機状態となる。

[0085] これに対し、サービス実行確認部 3 2 は、ステップ S P 1 0 2 の判断で肯定結果を得ると、ID 及びパスワードをサービス提供サーバ 2 に送信し、その後サービス提供サーバ 2 からのスケジュールの承認依頼の通知を受信すると、各種情報とともにスケジュールを表示画面に表示する (S P 1 0 3)。

[0086] サービス実行確認部 3 2 は、利用者の編集操作によりスケジュールの編集が指示されたか否かを判断する (S P 1 0 4)。サービス実行確認部 3 2 は、ステップ S P 1 0 4 の判断で否定結果を得ると、ステップ S P 1 0 6 に移行し、肯定結果を得るとスケジュールを編集する (S P 1 0 5)。

[0087] 次いでサービス実行確認部 3 2 は、実施期限領域 3 1 7 に表示された実施期限の範囲内でスケジュールを編集し、登録承認ボタン 3 1 8 の押下によりスケジュールを承認する。そしてサービス実行確認部 3 2 は、承認したスケ

ジュールをサービス提供サーバ2に送信する（SP106）。

[0088] サービス実行確認部32は、スケジュールの登録完了待ちの状態において（SP107）、登録完了通知を受信したか否かを判断する（SP108）。サービス実行確認部32は、ステップSP108の判断で否定結果を得ると、ステップSP107に移行する。これに対し、サービス実行確認部32は、ステップSP108の判断で肯定結果を得ると、登録完了画面を表示画面に表示して（SP109）、このスケジュール登録処理を終了する。

[0089] 図19は、サービス提供サーバ2側のスケジュール登録処理の詳細な処理手順を示す。ここでは、図17のスケジュール登録処理においてサービス提供サーバ2が実行する処理の詳細な処理手順について説明する。

[0090] サービス提供サーバ2の検査計画部21は、通信機能付き端末3から送信されたID及びパスワードの認証処理を終了すると、検査対象ECU情報273を参照して、「検査期限」内で一又は複数のスケジュールを作成する（SP111）。

[0091] 次に検査計画部21は、ユーザ情報271及び検査対象車両情報272を取得し（SP112）、作成したスケジュールとともにユーザ情報271等を通信機能付き端末3に送信する（SP113）。次に検査計画部21は、通信機能付き端末3において承認されたスケジュールの受信待ちの状態において（SP114）、承認されたスケジュールを受信したか否かを判断する（SP115）。

[0092] 検査計画部21は、ステップSP115の判断で否定結果を得ると、ステップSP114に移行する。これに対し、検査計画部21は、ステップSP115の判断で肯定結果を得ると、受信したスケジュールをスケジュール情報276に格納する（SP116）。そして検査計画部21は、登録完了通知を通信機能付き端末3に送信して（SP117）、このスケジュール登録処理を終了する。

[0093] 図20は、ECU検査処理の一連の処理手順を示す。このECU検査処理は、自動車1のゲートウェイ11、サービス提供サーバ2及び通信機能付き

端末 3 により実行される。

- [0094] まずサービス提供サーバ 2 の検査制御部 2 2 は、定期的又は不定期にスケジュール情報 2 7 6 を参照して、検査予定の「日時」を取得することによりスケジュールをチェックする (S P 2 1)。次いで検査制御部 2 2 は、対象となる検査があるか否かを判断し (S P 2 2)、否定結果を得るとステップ S P 2 1 に戻り、肯定結果を得るとステップ S P 2 3 に移行する。
- [0095] 次いで検査制御部 2 2 は、検査データ投入部 2 4 により検査実施通知を通信機能付き端末 3 に送信する (S P 2 3)。画面表示部 3 1 は、検査実施通知を受信すると、リマインダ画面を表示する (S P 2 4)。一方で検査データ投入部 2 4 は、セキュリティチェック用データ情報 2 7 4 及び動作検査用データ情報 2 7 5 から検査用データを取得し、取得した検査用データを検査対象の自動車 1 のゲートウェイ 1 1 に送信する (S P 2 5)。
- [0096] ゲートウェイ 1 1 の検査実行制御部 1 1 1 は、検査データを受信すると、受信した検査用データを検査実行データ情報 1 1 6 1 に格納する (S P 2 6)。次いで検査実行制御部 1 1 1 は、自動車 1 の車両状態を確認し (S P 2 7)、自動車 1 がスタンバイ状態でない場合 (S P 2 8 : N)、検査可能な状態でないと判断してステップ S P 2 7 に移行する。
- [0097] なおスタンバイ状態とは、自動車 1 が停止状態であって、かつ、一定時間が経過した状態であることをいう。検査実行制御部 1 1 1 は、自動車 1 がスタンバイ状態である場合 (S P 2 8 : Y)、検査実行データ情報 1 1 6 1 に格納した検査用データを取得し、検査実行部 1 1 3 により取得した検査用データを E C U 1 2 に送信する (S P 2 9)。
- [0098] 次いで検査実行制御部 1 1 1 は、検査監視部 1 1 4 により E C U 1 1 4 から出力されるデータを取得し、具体的にはパケットをキャプチャして (S P 3 0)、キャプチャしたパケットを検査実行結果情報 1 1 6 2 に格納する。
- [0099] 次いで検査実行制御部 1 1 1 は、E C U 1 2 に送信すべき検査用データが検査実行データ情報 1 1 6 1 に残っていないか確認し (S P 3 1)、残っている場合にはステップ S P 2 8 に移行し、残っていない場合にはステップ S

P 3 2 に移行する。なお一定期間が経過しても検査が完了していない場合には、サービス提供サーバ 2 に警告を通知するとしてもよい。

[0100] 検査実行制御部 1 1 1 は、E C U 1 2 に送信すべき検査用データが残っていない場合には検査が完了したことを示す検査結果完了通知をサービス提供サーバ 2 に送信する (S P 3 2)。サービス提供サーバ 2 の検査制御部 2 2 は、検査結果完了通知を受信すると、検査結果回収部 2 5 により検査結果回収依頼の通知をゲートウェイ 1 1 に送信する (S P 3 3)。

[0101] ゲートウェイ 1 1 の検査情報取得部 1 1 2 は、検査結果回収依頼の通知を受信すると、検査実行結果情報 1 1 6 2 を取得し (S P 3 4)、取得した検査実行結果情報 1 1 6 2 をサービス提供サーバ 2 に送信する (S P 3 5)。サービス提供サーバ 2 の検査結果回収部 2 5 は、検査実行結果情報 1 1 6 2 を受信すると、検査結果情報 2 8 0 に格納する (S P 3 6)。

[0102] 次に検査結果解析部 2 6 は、検査結果情報 2 8 0 及び検査照合結果情報 2 8 1 を参照して、E C U 1 2 から実際に出力された出力結果と、予測される出力結果とを比較することにより検査結果情報を解析し (S P 3 7)、解析結果を判定し (S P 3 8)、判定結果を検査照合結果情報 2 8 1 に格納する。

[0103] そして検査制御部 2 2 は、判定結果を通信機能付き端末 3 に送信する (S P 3 9)。なお判定結果は通信機能付き端末 3 以外にもディーラや自動車メーカー等に送信するとしてもよい。通信機能付き端末 3 の画面表示部 3 1 は、判定結果を受信すると、検査結果として表示画面に表示する (S P 4 0)。以上により E C U 検査処理の一連の処理が終了する。

[0104] 図 2 1 は、通信機能付き端末 3 側の E C U 検査処理の詳細な処理手順を示す。ここでは、図 2 0 の E C U 検査処理において通信機能付き端末 3 が実行する処理の詳細な処理手順について説明する。

[0105] 通信機能付き端末 3 のサービス実行確認部 3 2 は、検査実施通知待ちの状態において (S P 2 0 1)、サービス提供サーバ 2 から送信される検査実施通知を受信したか否かを判断する (S P 2 0 2)。サービス実行確認部 3 2

は、ステップＳＰ２０２の判断で否定結果を得ると、ステップＳＰ２０１に移行する。

[0106] これに対し、サービス実行確認部３２は、ステップＳＰ２０２の判断で肯定結果を得ると、リマインダ画面を表示画面に表示する（ＳＰ２０３）。次いでサービス実行確認部３２は、サービス提供サーバ２から送信される判定結果を受信したか否かを判断する（ＳＰ２０４）。サービス実行確認部３２は、ステップＳＰ２０４の判断で否定結果を得ると、判定結果を受信するまで待機する。

[0107] これに対し、サービス実行確認部３２は、ステップＳＰ２０４の判断で肯定結果を得ると、画面表示部３１により検査結果を表示画面に表示して（ＳＰ２０５）、このＥＣＵ検査処理を終了する。

[0108] 図２２は、サービス提供サーバ２側のＥＣＵ検査処理の詳細な処理手順を示す。ここでは、図２０のＥＣＵ検査処理においてサービス提供サーバ２が実行する処理の詳細な処理手順について説明する。

[0109] サービス提供サーバ２の検査データ投入部２４は、検査制御部２２からの指示により定期的又は不定期にスケジュール情報２７６を参照して、検査予定の「日時」を取得することによりスケジュールをチェックする（ＳＰ２１１）。そして検査データ投入部２４は、実施すべき検査があるか否かを判断する（ＳＰ２１２）。

[0110] 検査データ投入部２４は、ステップＳＰ２１２の判断で否定結果を得ると、ステップＳＰ２１１に移行する。これに対し、検査データ投入部２４は、ステップＳＰ２１２の判断で肯定結果を得ると、検査実施通知を通信機能付き端末３に送信する（ＳＰ２１３）。

[0111] 次いで検査データ投入部２４は、セキュリティチェック用データ情報２７４及び動作検査用データ情報２７５から検査用データを取得し、この検査用データを検査対象の自動車１のゲートウェイ１１に送信する（ＳＰ２１４）。

[0112] 次いで検査制御部２２は、検査結果完了通知待ちの状態において（ＳＰ２

15)、ゲートウェイ11から送信される検査結果完了通知を受信したか否かを判断する(S P 2 1 6)。検査制御部22は、ステップS P 2 1 6の判断で否定結果を得ると、ステップS P 2 1 5に移行する。

[0113] これに対し、検査制御部22は、ステップS P 2 1 6の判断で否定結果を得ると、検査結果回収部25により検査結果回収依頼の通知をゲートウェイ11に送信する(S P 2 1 7)。次いで検査結果回収部25は、検査結果回収待ちの状態において(S P 2 1 8)、ゲートウェイ11から送信される検査実行結果情報1162を受信したか否かを判断する(S P 2 1 9)。

[0114] 検査結果回収部25は、ステップS P 2 1 9の判断で否定結果を得ると、ステップS P 2 1 8に移行する。これに対し、検査結果回収部25は、ステップS P 2 1 9の判断で肯定結果を得ると、受信した検査実行結果情報1162を検査結果情報280に格納する。

[0115] そして検査結果解析部26は、検査結果情報280及び検査照合結果情報281を参照して、ECU12から実際に出力された出力結果と、予想される出力結果とを比較することにより検査結果を解析し(S P 2 2 0)、予想通りの出力結果である場合には異常なし、予想通りの出力結果でない場合には異常ありと判定する(S P 2 2 1)。

[0116] そして検査制御部22は、判定結果を通信機能付き端末3に送信して(S P 2 2 2)、このECU検査処理を終了する。

[0117] 図23は、自動車1のゲートウェイ11側のECU検査処理の詳細な処理手順を示す。ここでは、図20のECU検査処理においてゲートウェイ11が実行する処理の詳細な処理手順について説明する。

[0118] ゲートウェイ11の検査実行制御部111は、サービス提供サーバ2からの処理依頼待ちの状態において(S P 2 3 1)、処理依頼があるか否かを判断する(S P 2 3 2)。検査実行制御部111は、ステップS P 2 3 2の判断で否定結果を得ると、ステップS P 2 3 1に移行し、肯定結果を得ると、処理内容を判定する(S P 2 3 3)。

[0119] 検査実行制御部111は、処理内容が検査実施依頼である場合、すなわち

サービス提供サーバ2から検査用データを受信した場合、受信した検査用データを検査実行データ情報1161に格納する（SP234）。次いで検査実行制御部111は、自動車1の車両状態を確認し（SP235）、自動車1がスタンバイ状態であるか否かを判断する（SP236）。

[0120] 検査実行制御部111は、自動車1がスタンバイ状態である場合（SP236：Y）、検査実行部113により、検査実行データ情報1161の「CAN-ID」と、「検査データ」とに基づいてCANプロトコルに合わせたメッセージを生成し、生成したメッセージをECU12に送信する（SP237）。

[0121] 次いで検査実行制御部111は、検査監視部114によりECU12から出力されるデータを取得し、具体的にはパケットをキャプチャして、検査実行結果情報1162に格納する（SP238）。次いで検査実行制御部111は、検査実行データ情報1161の「進捗状況」を「完了」に更新する（SP239）。

[0122] 次いで検査実行制御部111は、検査実行データ情報1161の「進捗状況」を参照して、「完了」になっていない項目があるか否かを確認することにより、ECU12に送信すべき検査用データが検査実行データ情報1161に残っていないか確認する（SP240）。

[0123] 検査実行制御部111は、ステップSP240の判断で否定結果を得ると、ステップSP236に移行し、肯定結果を得ると、検査結果完了通知をサービス提供サーバ2に送信して（SP243）、このECU検査処理を終了する。

[0124] ステップSP236に戻り、自動車1がスタンバイ状態でない場合（SP236：N）、スタンバイ状態になるまで待機してもよいが、ここでは検査を一時的に停止し（SP241）、停止したことを示す一時停止通知をサービス提供サーバ2に送信して（SP243）、このECU検査処理を終了する。

[0125] ステップSP233に戻り、検査実行制御部111は、処理内容が検査結

果回収依頼である場合、すなわちサービス提供サーバ2から検査結果回収依頼の通知を受信した場合、検査情報取得部112により検査実行結果情報1162を取得し（SP242）、この検査実行結果情報1162をサービス提供サーバ2に送信して（SP243）、このECU検査処理を終了する。

[0126] 図24は、セキュリティチェック用データ生成処理の処理手順を示す。このセキュリティチェック用データ生成処理は、ECU検査処理時（図20）又はECU検査処理前の任意のタイミングで、サービス提供サーバ2により実行される。

[0127] まずサービス提供サーバ2の検査データ生成部23は、検査対象ECU情報273を参照して、「検査対象フラグ」が「対象」である「ECU-ID」を検査対象のECU-IDとして取得する（SP31）。次いで検査データ生成部23は、検査対象として特定したECU-IDに対応付けられている「CAN-ID」を取得する（SP32）。

[0128] 次いで検査データ生成部23は、フィールド構造解析部232により、フィールド構造情報277を参照して、ステップSP32で取得したCAN-IDに対応付けられている「詳細フィールドID」及び「ビット数」を取得することにより、データフィールド（図15）のフィールド構造を解析する（SP33）。

[0129] 例えばフィールド構造解析部232は、フィールド構造情報277を参照して、ステップSP32で取得したCAN-IDが「0×7E0」である場合、「0×7E0」のCAN-IDに対応付けられている「A1」、「A2」、「A3」、「A4」の詳細フィールドIDを取得する。

[0130] またフィールド構造解析部232は、これら「A1」～「A4」の詳細フィールドIDに対応付けられている「8bit」、「8bit」、「16bit」、「32bit」の各ビット数を取得する。この結果、フィールド構造解析部232は、データフィールドの構造は「A1」～「A4」の4つに区分されており、各区分はそれぞれ「8bit」、「8bit」、「16bit」、「32bit」であるとする解析結果を得ることができる。

- [0131] なおフィールド構造解析部232は、フィールド構造情報277を参照して、「A1」～「A4」の詳細フィールドIDに対応付けられている「D1」、「D2」、「D2」、「D4」の区分IDを取得し、フィールド区分情報278を参照して、「D1」、「D2」、「D4」に対応付けられている「有効桁」、「可変データ」、「ダミー」の区分名称を取得することにより、「A1」～「A4」に格納されるデータが示す意味を解析することができる。
- [0132] 次いで検査データ生成部23は、依存関係解析部231により、フィールド依存関係情報279を参照して、ステップSP32で取得したCAN-IDに対応付けられている「詳細フィールドの依存関係」を取得する（SP34）。
- [0133] 例えば依存関係解析部231は、フィールド依存関係情報279を参照して、ステップSP32で取得したCAN-IDが「0×7E0」である場合、「0×7E0」のCAN-IDに対応付けられている{A1、(A2&A3)、A4}という依存関係を取得する。この場合、「A2」の区分に格納されるデータと、「A3」の区分に格納されるデータとの間に依存関係がある。
- [0134] 次いで検査データ生成部23は、検査データ割当部233により、ステップSP33で取得した「ビット数」と、ステップSP34で取得した「詳細フィールドの依存関係」とに基づいて、ランダムデータの割当て数を決定する（SP35）。
- [0135] 例えば検査データ生成部23は、全部で64ビットあるデータフィールドの全てにランダムなデータを割り当てるのではなく、検査効率の観点から、データフィールドのなかでもより効果的な検査を実現し得る位置にランダムデータを割り当てる。ここでは検査データ生成部23は、「A2」及び「A3」に依存関係があり、「A2」及び「A3」はそれぞれ「8bit」及び「16bit」であるから、ランダムデータの割当て数を24bitに決定する。
- [0136] なお検査データ生成部23は、上記のとおり依存関係単位でランダムデー

タの割当て数を決定してもよいし、フィールド区分情報 278 の「区分 I D」の特徴に合わせて優先度に応じてランダムデータの割当て数を決定してもよい。例えば「A 1」にランダムデータを割り当てて、「A 2」～「A 4」には固定データを割り当てるようにしてもよい。

[0137] 次いで検査データ生成部 23 は、検査データ割当部 233 により、ステップ S P 35 で決定したデータの割当て数に基づいて、ランダムデータを使用する範囲を決定し、検査用データを生成する（S P 36）。そして検査データ生成部 23 は、生成したデータをセキュリティチェック用データ情報 274 に格納する（S P 37）。

[0138] 次いで検査データ生成部 23 は、ステップ S P 34 で取得した依存関係のうち、検査用データが生成されていない依存関係が残っていないか判断する（S P 38）。検査データ生成部 23 は、ステップ S P 38 の判断で否定結果を得ると、ステップ S P 36 に移行し、肯定結果を得ると、このセキュリティチェック用データ生成処理を終了する。

[0139] （6）本実施の形態による効果

以上のように本実施の形態における検査システム 5 によれば、E C U 12 の設計段階で予め用意される動作検査用データに加えて、E C U 12 の設計段階では E C U 12 が受信することを想定していないセキュリティチェック用データを E C U 12 に送信し、E C U 12 から出力されるデータが正常な範囲内であるか否かを判断するようにしたので、運用時における E C U 12 の動作を正確に検査することができる。

[0140] （7）他の実施の形態

上記説明してきた本実施の形態においては、サービス提供サーバ 2 の検査結果解析部 26 が検査結果情報 280 及び検査照合結果情報 281 を参照して、検査結果情報 280 を解析し、解析結果を判定するとしたが（図 20：S P 37 及び S P 38）、これに限らず、自動車 1 のゲートウェイ 11 が検査結果解析部 26 及び検査照合結果情報 281 を備え、ゲートウェイ 11 が検査結果解析部 26 により、検査実行データ情報 1161 及び検査照合結果

情報 2 8 1 を参照して、検査実行データ情報 1 1 6 1 を解析し、解析結果を判定するとしてもよい。

[0141] 図 2 5 は、他の実施の形態における E C U 検査処理の処理手順を示す。他の実施の形態における E C U 検査処理は、ゲートウェイ 1 1 が検査結果を解析し (S P 3 1 A) 、解析結果を判定する (S P 3 2 A) 点及びゲートウェイ 1 1 が判定結果を取得して (S P 3 6 A) 、サービス提供サーバ 2 (又は直接通信機能付き端末 3) に送信する (S P 3 7 A) 点で、上記説明してきた本実施の形態における E C U 検査処理 (図 2 0) と異なる。

符号の説明

- [0142] 1 自動車
2 サービス提供サーバ
3 通信機能付き端末
4 通信網
5 検査システム

請求の範囲

- [請求項1] 車載ネットワークに接続されたＥＣＵの動作を検査する検査装置において、
- 前記ＥＣＵの動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの２つのデータを前記ＥＣＵに送信し、前記ＥＣＵから出力されるデータを受信する検査実行制御部を備え、
- 前記動作検査用データは、
- 前記ＥＣＵの設計情報に基づいて予め生成されるデータであり、
- 前記セキュリティチェック用データは、
- 前記動作検査用データの一部又は全部をランダムデータに置き換えたデータである
- ことを特徴とする検査装置。
- [請求項2] 前記検査実行制御部は、
- 前記動作検査用データ及び前記セキュリティチェック用データを外部端末から受信し、前記ＥＣＵから出力されたデータを含む検査実行結果情報を前記外部端末に送信する
- ことを特徴とする請求項１に記載の検査装置。
- [請求項3] 前記セキュリティチェック用データを前記ＥＣＵに送信した場合に前記ＥＣＵから出力されると予想される予想出力データを備え、
- 前記検査実行制御部は、
- 前記ＥＣＵから出力されたデータと、前記予想出力データとを比較することにより前記ＥＣＵから出力されたデータを解析し、解析結果に基づいて、前記ＥＣＵの動作が正常であるか否かを判定することにより、前記ＥＣＵの動作を検査する
- ことを特徴とする請求項１に記載の検査装置。
- [請求項4] 前記検査実行制御部は、
- 前記ＥＣＵの動作の検査結果を外部端末に送信する

ことを特徴とする請求項3に記載の検査装置。

[請求項5]

前記検査実行制御部は、

前記E C Uを備える自動車の車両状態を確認し、車両状態がスタンバイ状態である場合に限って、前記動作検査用データ及び前記セキュリティチェック用データの2つのデータを前記E C Uに送信する

ことを特徴とする請求項1に記載の検査装置。

[請求項6]

車載ネットワークに接続されたE C Uの動作を検査する検査システムにおいて、

前記E C Uの動作を検査するスケジュールを計画する検査計画部と、

前記E C Uの動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの2つのデータを生成する検査データ生成部と、

前記計画されたスケジュールに従って、前記生成された2つのデータを外部に送信する検査制御部とを備えるサービス提供サーバと、

前記サービス提供サーバから送信される前記動作検査用データ及び前記セキュリティチェック用データの2つのデータを受信した場合、受信した2つのデータを前記E C Uに送信し、前記E C Uから出力されるデータを受信した場合、受信したデータを含む検査実行結果情報を前記サービス提供サーバに送信するゲートウェイとを備え、

前記動作検査用データは、

前記E C Uの設計情報に基づいて予め生成されるデータであり、

前記セキュリティチェック用データは、

前記動作検査用データの一部又は全部をランダムデータに置き換えたデータである

ことを特徴とする検査システム。

[請求項7]

前記サービス提供サーバは、

前記セキュリティチェック用データを前記E C Uに送信した場合に

前記E C Uから出力されると予想される予想出力データを備え、

前記ゲートウェイから送信された前記検査実行結果情報を受信した場合、受信した前記検査実行結果情報に含まれる前記E C Uから出力されたデータと、前記予想出力データとを比較することにより前記E C Uから出力されたデータを解析し、解析結果に基づいて、前記E C Uの動作が正常であるか否かを判定することにより、前記E C Uの動作を検査する検査結果解析部を備える

ことを特徴とする請求項6に記載の検査システム。

[請求項8]

前記サービス提供サーバは、

前記E C Uが所属する車載ネットワークの識別情報であるC A N－I Dと、前記セキュリティチェック用データが格納されるデータフィールドの構成要素である複数の詳細フィールドとの対応関係を示すフィールド構造情報と、

前記C A N－I Dと、前記詳細フィールドの依存関係との対応関係を示すフィールド依存関係情報とを備え、

前記検査データ生成部は、

前記セキュリティチェック用データを生成する際、

前記フィールド構造情報を参照して、前記詳細フィールドの構造を解析し、前記詳細フィールドの区分を特定し、前記フィールド依存関係情報を参照して、前記詳細フィールドの区分の依存関係を特定し、特定した前記詳細フィールドの区分及び区分の依存関係に基づいて、前記詳細フィールドのうちの何れか又は全てにランダムデータを割り当てて格納することにより、前記セキュリティチェック用データを生成する

ことを特徴とする請求項6に記載の検査システム。

[請求項9]

通信機能付き端末を備え、

前記サービス提供サーバは、

前記検査結果を前記通信機能付き端末に送信する

ことを特徴とする請求項6に記載の検査システム。

[請求項10]

車載ネットワークに接続されたE C Uの動作を検査する検査方法において、

検査計画部が、前記E C Uの動作を検査するスケジュールを計画する第1のステップと、

検査データ生成部が、前記E C Uの動作を検査するために用いられる動作検査用データ及びセキュリティチェック用データの2つのデータを生成する第2のステップと、

検査制御部が、前記計画されたスケジュールに従って、前記生成された2つのデータを外部に送信する第3のステップとを備え、

ゲートウェイが、サービス提供サーバから送信される前記動作検査用データ及び前記セキュリティチェック用データの2つのデータを受信した場合、受信した2つのデータを前記E C Uに送信し、前記E C Uから出力されるデータを受信した場合、受信したデータを含む検査実行結果情報を前記サービス提供サーバに送信する第4のステップとを備え、

前記動作検査用データは、

前記E C Uの設計情報に基づいて予め生成されるデータであり、

前記セキュリティチェック用データは、

前記動作検査用データの一部又は全部をランダムデータに置き換えたデータである

ことを特徴とする検査方法。

[請求項11]

前記サービス提供サーバは、

前記セキュリティチェック用データを前記E C Uに送信した場合に前記E C Uから出力されると予想される予想出力データを備え、

検査結果解析部が、前記ゲートウェイから送信された前記検査実行結果情報を受信した場合、受信した前記検査実行結果情報に含まれる前記E C Uから出力されたデータと、前記予想出力データとを比較す

ることにより前記E C Uから出力されたデータを解析し、解析結果に基づいて、前記E C Uの動作が正常であるか否かを判定することにより、前記E C Uの動作を検査する第5のステップを備える

ことを特徴とする請求項10に記載の検査方法。

[請求項12]

前記サービス提供サーバは、

前記E C Uが所属する車載ネットワークの識別情報であるC A N－I Dと、前記セキュリティチェック用データが格納されるデータフィールドの構成要素である複数の詳細フィールドとの対応関係を示すフィールド構造情報と、

前記C A N－I Dと、前記詳細フィールドの依存関係との対応関係を示すフィールド依存関係情報とを備え、

前記検査データ生成部が、前記セキュリティチェック用データを生成する際、

前記フィールド構造情報を参照して、前記詳細フィールドの構造を解析し、前記詳細フィールドの区分を特定し、前記フィールド依存関係情報を参照して、前記詳細フィールドの区分の依存関係を特定し、特定した前記詳細フィールドの区分及び区分の依存関係に基づいて、前記詳細フィールドのうちの何れか又は全てにランダムデータを割り当てて格納することにより、前記セキュリティチェック用データを生成する第6のステップを備える

ことを特徴とする請求項10に記載の検査方法。

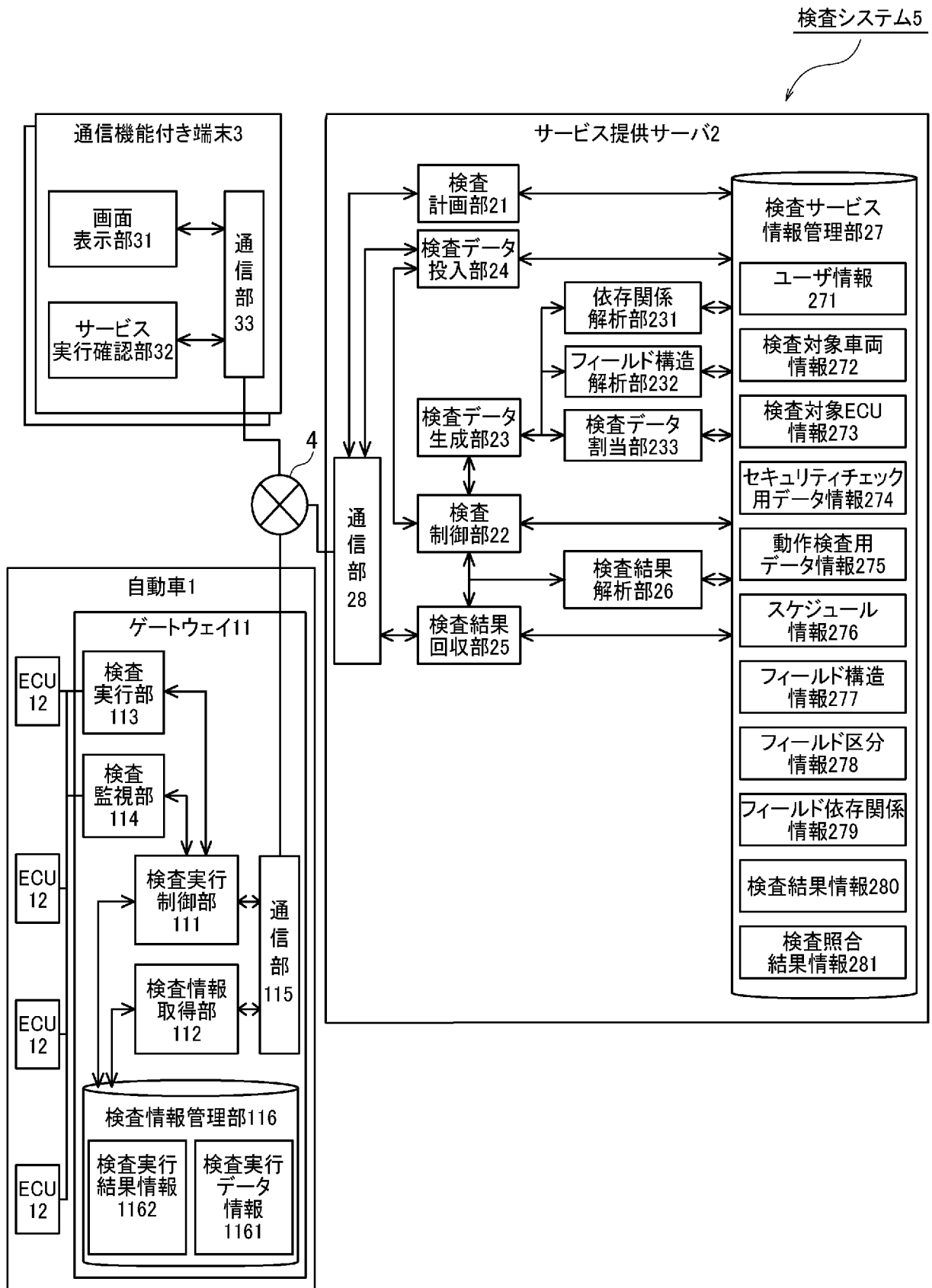
[請求項13]

前記サービス提供サーバが、前記検査結果を通信機能付き端末に送信する第7のステップを備える

ことを特徴とする請求項10に記載の検査方法。

[図1]

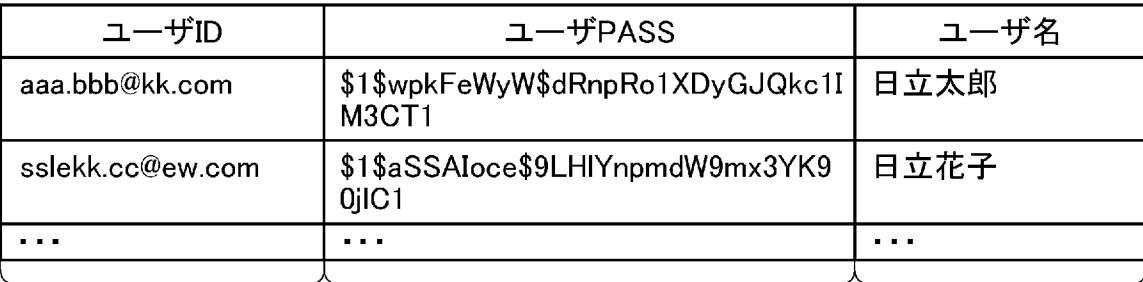
図 1



[図2]

図 2

ユーザ情報271



ユーザID	ユーザPASS	ユーザ名
aaa.bbb@kk.com	\$1\$wPkFeWyW\$dRnpRo1XDyGJQkc1IM3CT1	日立太郎
sslekk.cc@ew.com	\$1\$aSSAloce\$9LHIYnpmdW9mx3YK90jIC1	日立花子
...	...	...

2711 2712 2713

[図3]

図 3

検査対象車両情報272



ユーザID	VIN	メーカー	車種	車色	車両ナンバ
aaa.bbb@kk.com	1FALP45D9RF158493	メーカーA	車種A	青	徳島500-か08-73
	...	...	...	...	...
sslekk.cc@ew.com	1HD1CAP1APY999FE9	メーカーB	車種B	白	品川500-は34-55
...	...	...	...	...	...

2721 2722 2723 2724 2725 2726

[図4]

図 4

検査対象ECU情報273



車種	ECU-ID	ECU名	検査対象 フラグ	検査期限	CAN-ID
車種A	ECU-1	エンジン ECU	対象	{2014/02/20/0:00、 2014/02/27/23:59}	{0x3C4、 0xA30、...}
車種A	ECU-2	オーディオ ECU	非対象	{一、一}	...
車種A	ECU-3	ブレーキ ECU	対象	{2014/02/10/0:00、 2014/02/18/23:59}	...
...	...	...	...	...	...

2731 2732 2733 2734 2735 2736

[図5]

図 5

セキュリティチェック用データ情報274

検査ID	ECU-ID	CAN-ID	検査データ
ST-1	ECU-1	0x7E0	{0x1DC320、・・・}
		0x7E8	{0x1FA220、・・・}
		...	...
ST-2	ECU-3	...	...
...	...	...	...
2741		2742	2743 2744

[図6]

図 6

動作検査用データ情報275

検査ID	ECU-ID	CAN-ID	検査データ
OT-1	ECU-1	0x7E0	{0x2B3CF0、・・・}
		0x7E8	{0x1A3DE0、・・・}
		...	...
OT-2	ECU-3	...	...
...	...	...	...
2751		2752	2753 2754

[図7]

図 7

スケジュール情報276

VIN	日時	検査ID
1FALP45D9RF158493	2014/02/20/20:00	{OT-1、ST-1}
1HD1CAP1APY999FE9	2014/02/24/23:00	{OT-2、ST-2}
...	...	...
2761		2762 2763

[図8]

図 8

フィールド構造情報277

車種	CAN-ID	詳細フィールドID	区分ID	ビット数
車種A	0x7E0	A1	D1	8bit
車種A	0x7E0	A2	D2	8bit
車種A	0x7E0	A3	D2	16bit
車種A	0x7E0	A4	D4	32bit
車種A	0x9C0	A1	D1	8bit
...	...	...	...	...
2771		2772	2773	2774

[図9]

図 9

フィールド区分情報278

区分ID	区分名称
D1	有効桁
D2	可変データ
D3	予約
D4	ダミー
D5	チェックサム
...	...
2781	

[図10]

図 10

フィールド依存関係情報279

車種	CAN-ID	詳細フィールドの依存関係
車種A	0x7E0	{A1、(A2 & A3)、A4}
車種A	0x9C0	{A1,...}
...	...	...
2791		2792

[図11]

図 11

検査結果情報280

VIN	検査結果	実施検査ID
1FALP45D9RF158493	aaa.log	{OT-1、ST-1}
1HD1CAP1APY999FE9	bbb.log	{OT-2、ST-2}
...	...	...

2801
2802
2803

[図12]

図 12

検査照合結果情報281

車種	CAN-ID	実施検査データ	予想出力データ	判定結果
車種A	0x7E0	{0x1DC320、...}	0x102DF583C34A5 B0003A023C1010	異常なし
車種A	0x7E8	{0x1FA220、...}	0x1C347BA3C3920 D5183ACBAC0F13	異常なし
...	...	...	...	...

2811
2812
2813
2814
2815

[図13]

図 13

検査実行データ情報1161

実行順	検査ID	CAN-ID	検査データ	進捗状況
1	OT-1	0x7E0	{0x1DC320、...}	完了
2	OT-1	0x7E8	{0x1FA220、...}	—
...	...	...	...	...

11611
11612
11613
11614
11615

[図14]

図 14

検査実行結果情報1162

検査ID	検査結果
{OT-1、ST-1}	aaa.log
...	...

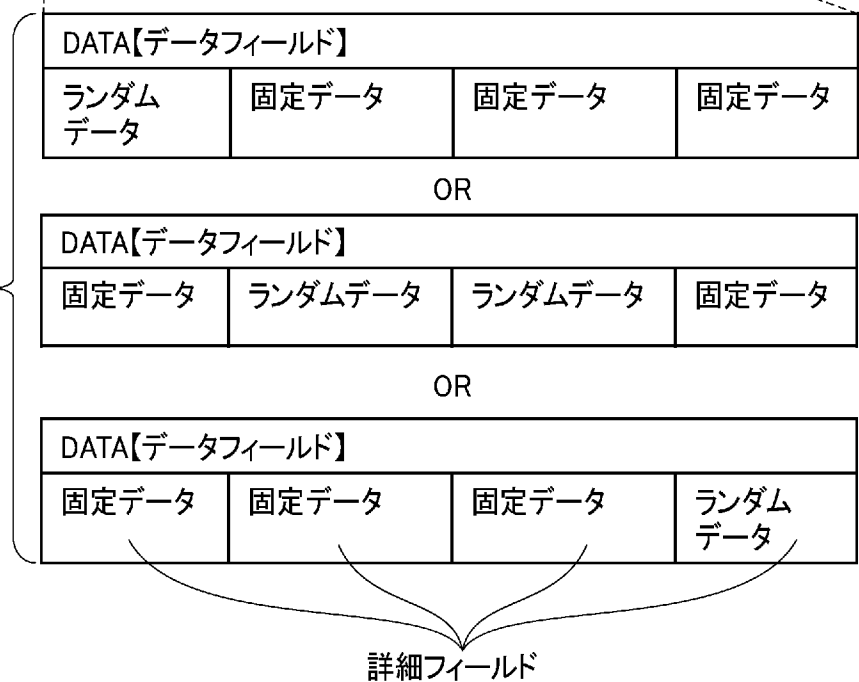
11621
11622

[図15]

図 15

SOF	アービトレーション		コントローラ			データ	CRC		ACK		EOF
SOF 1bit	ID 11bit	RTR 1bit	IDE 1bit	R0 1bit	DLC 4bit	DATA 64bit	CRC シーケンス 15bit	CRC デリミタ 1bit	ACK スロット 1bit	ACK デリミタ 1bit	EOF 7bit

詳細フィールドの依存関係に合わせて、ランダムデータを使用する範囲を変更する



[図16]

図 16

ユーザ名 311 日立太郎

メーカー 312 メーカーA

車種 313 車種A

車色 314 青

車両ナンバ 315 徳島500-か08-73

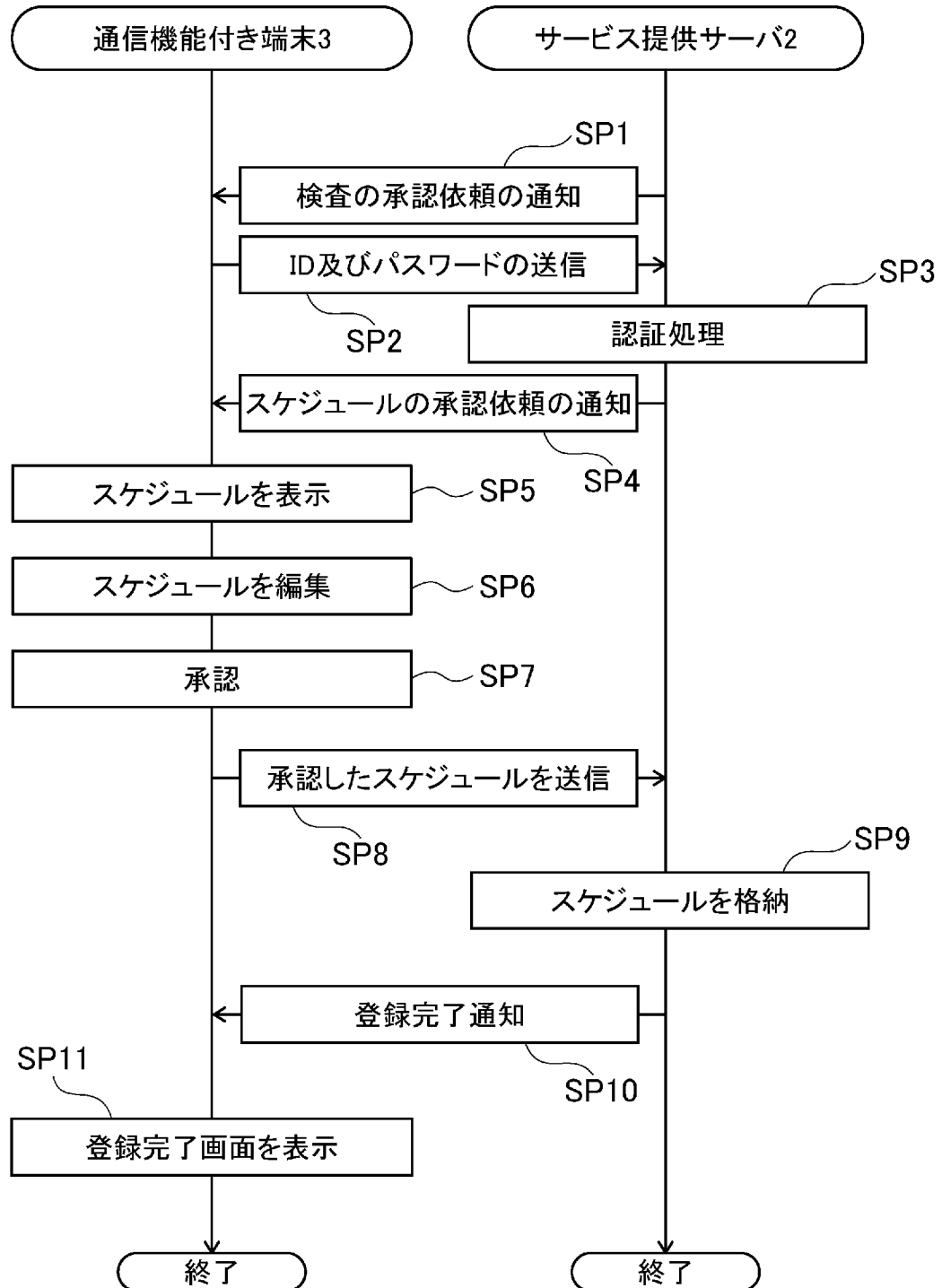
検査日時 316 2014/02/20/0:00

317 実施期限:2014/02/27/24:00

318 登録承認ボタン

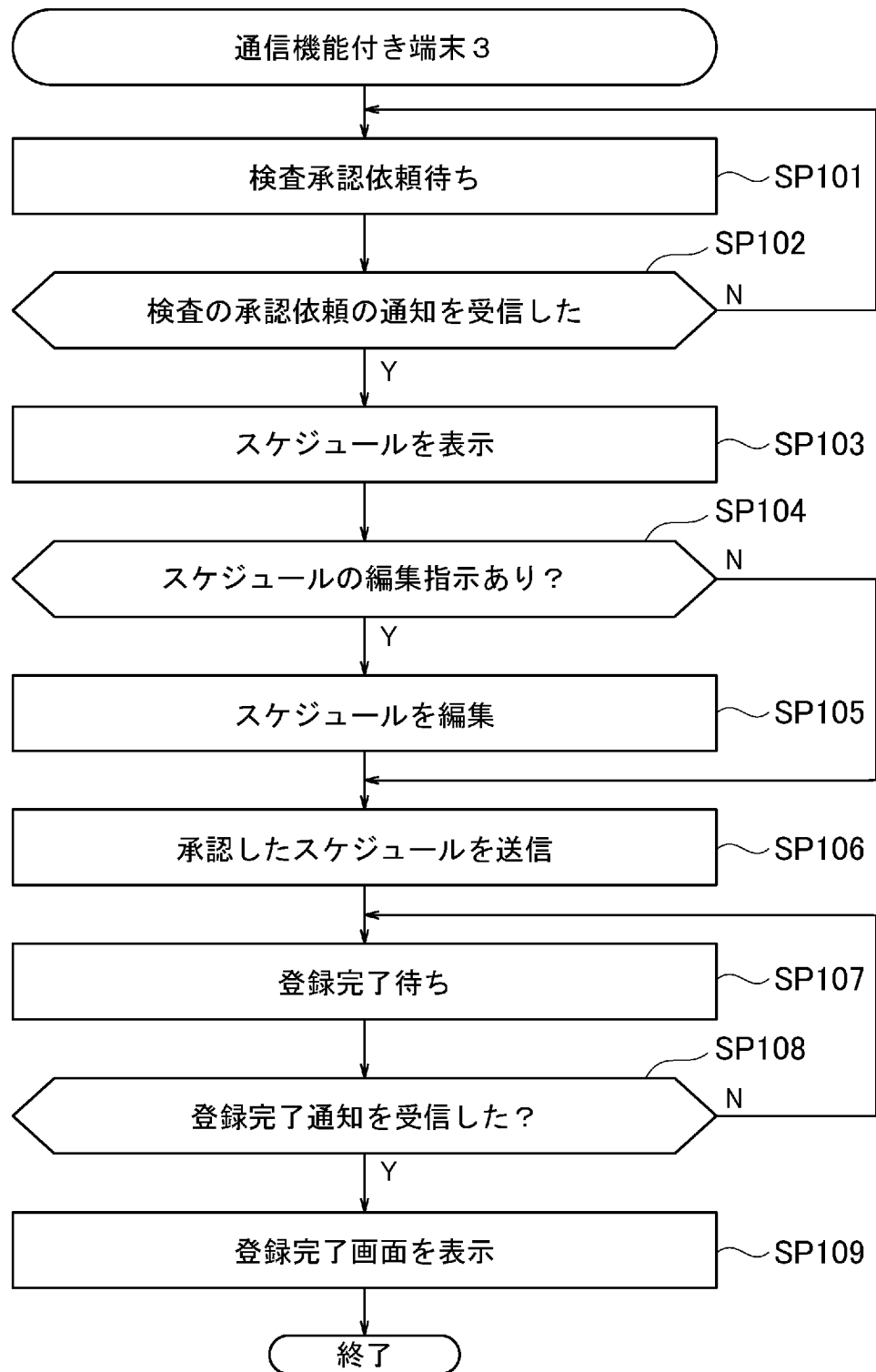
[図17]

図 17



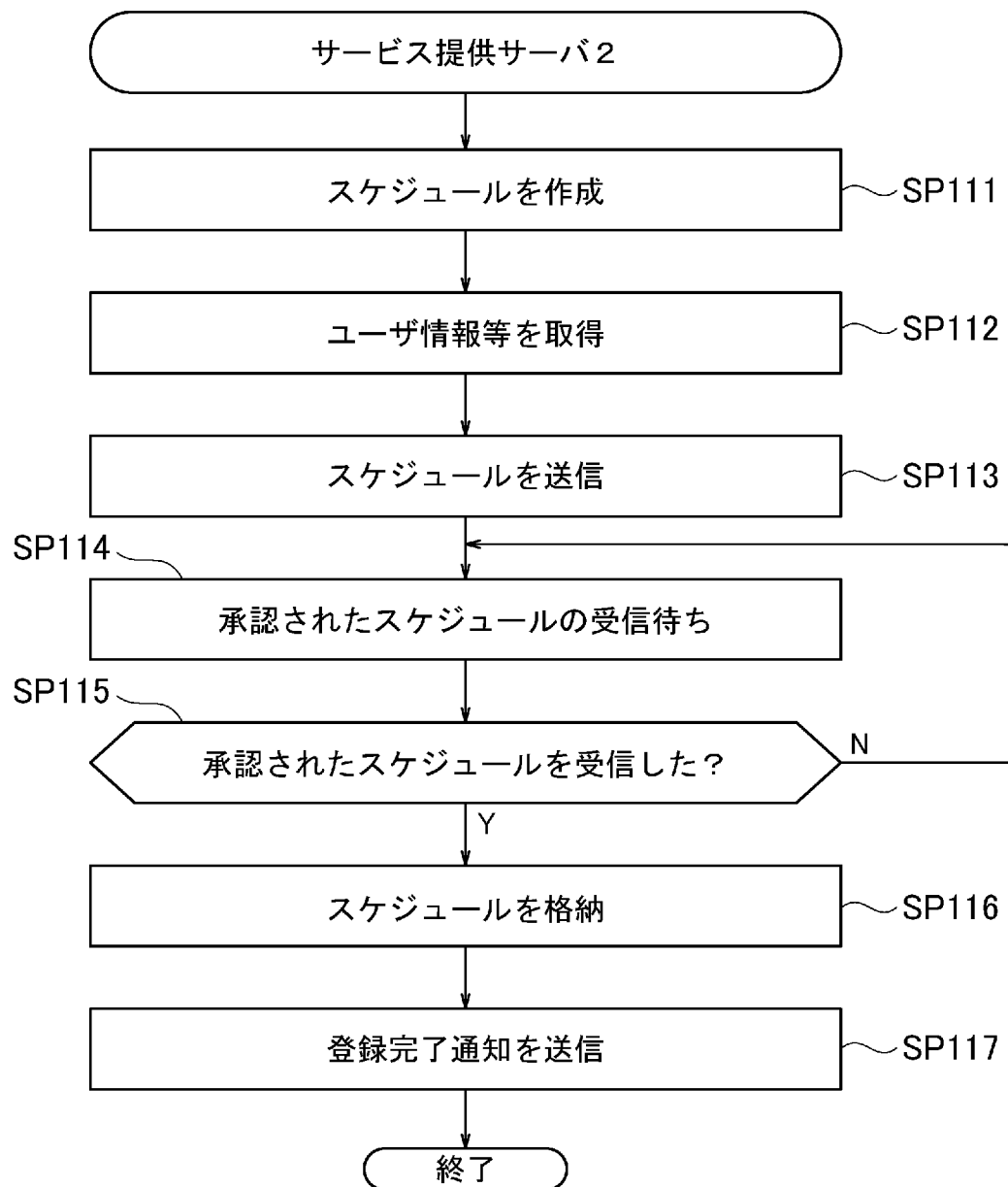
[図18]

図 18



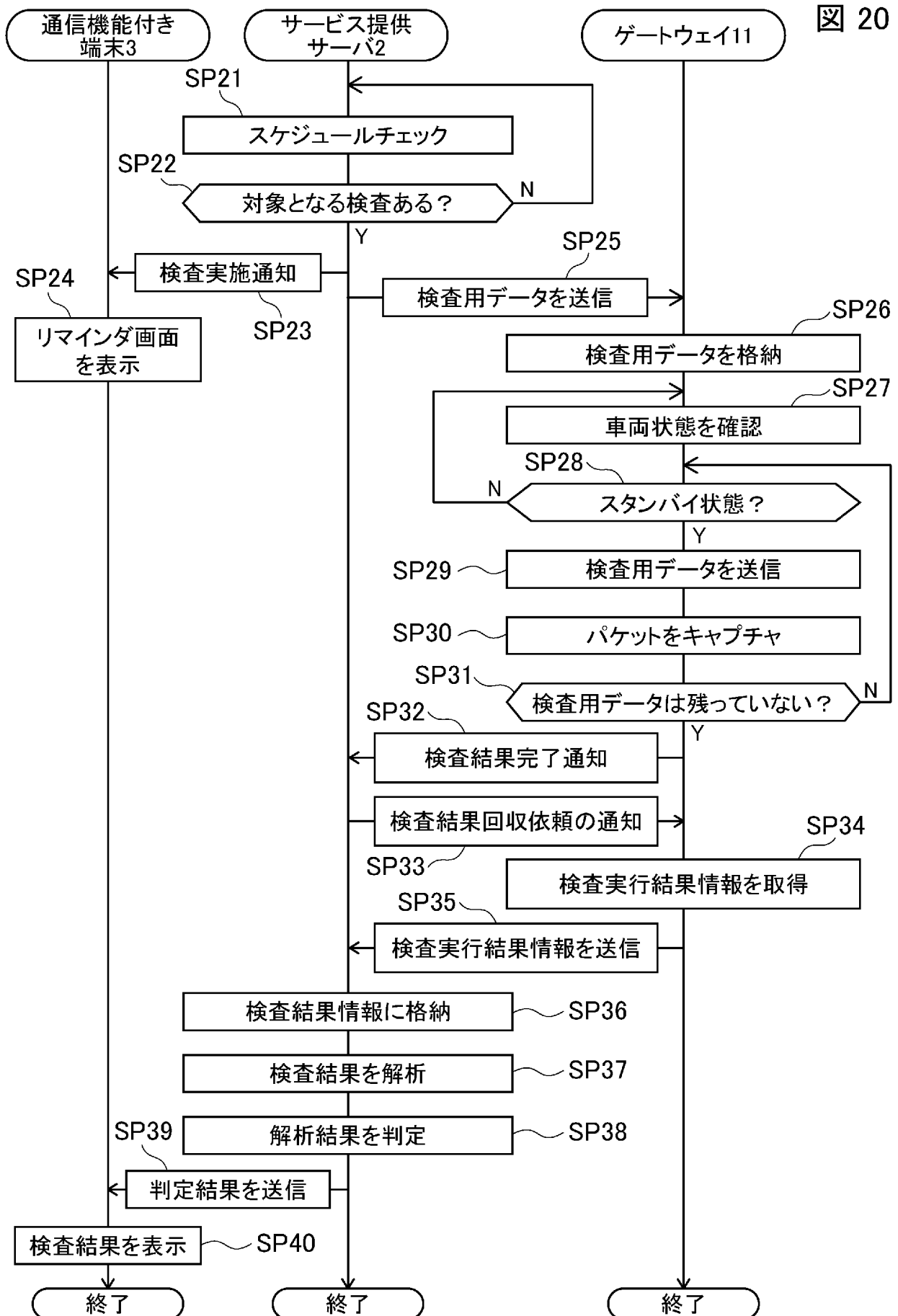
[図19]

図 19



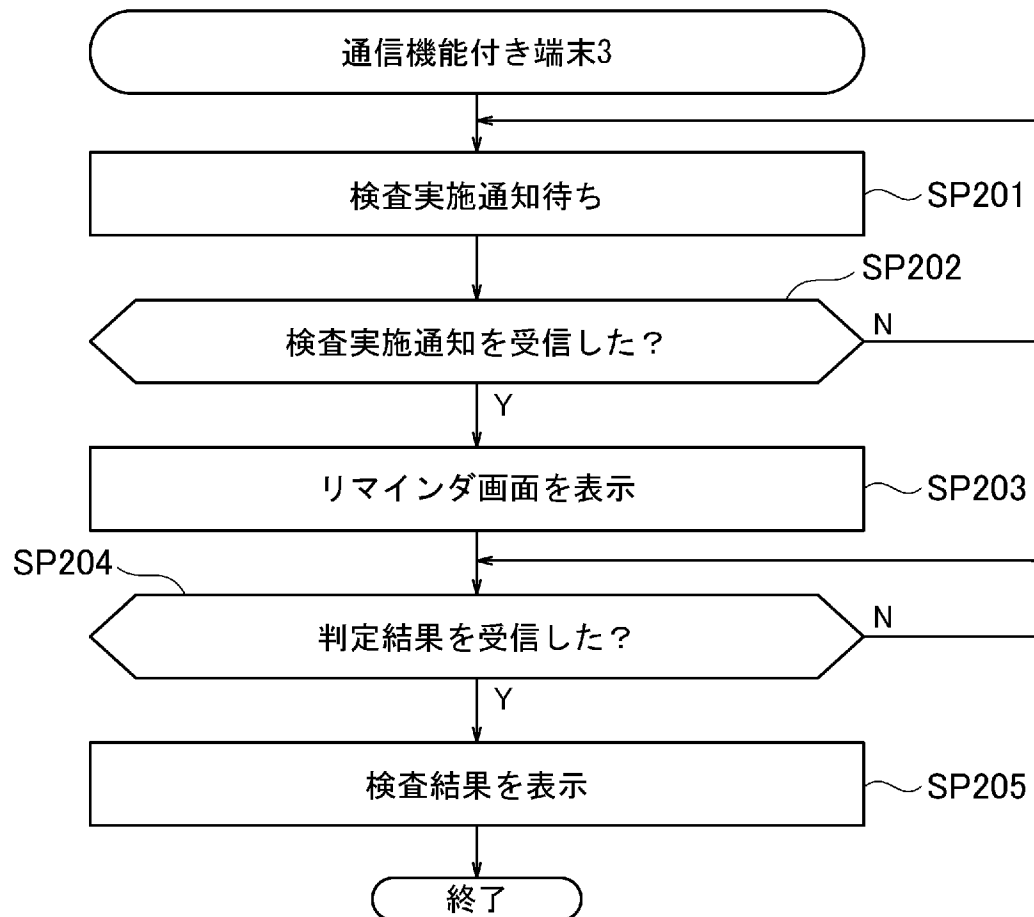
[図20]

図 20



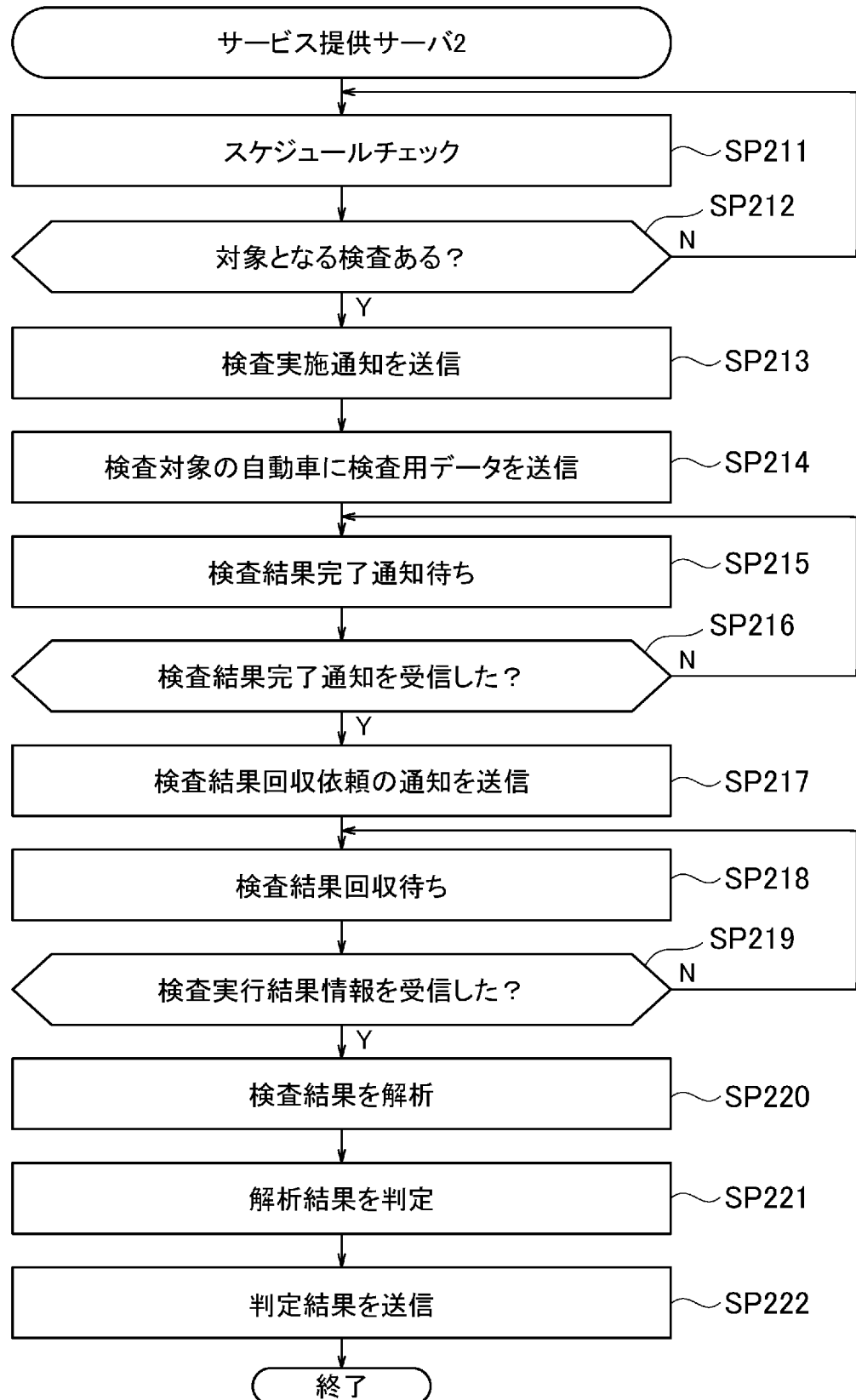
[図21]

図 21



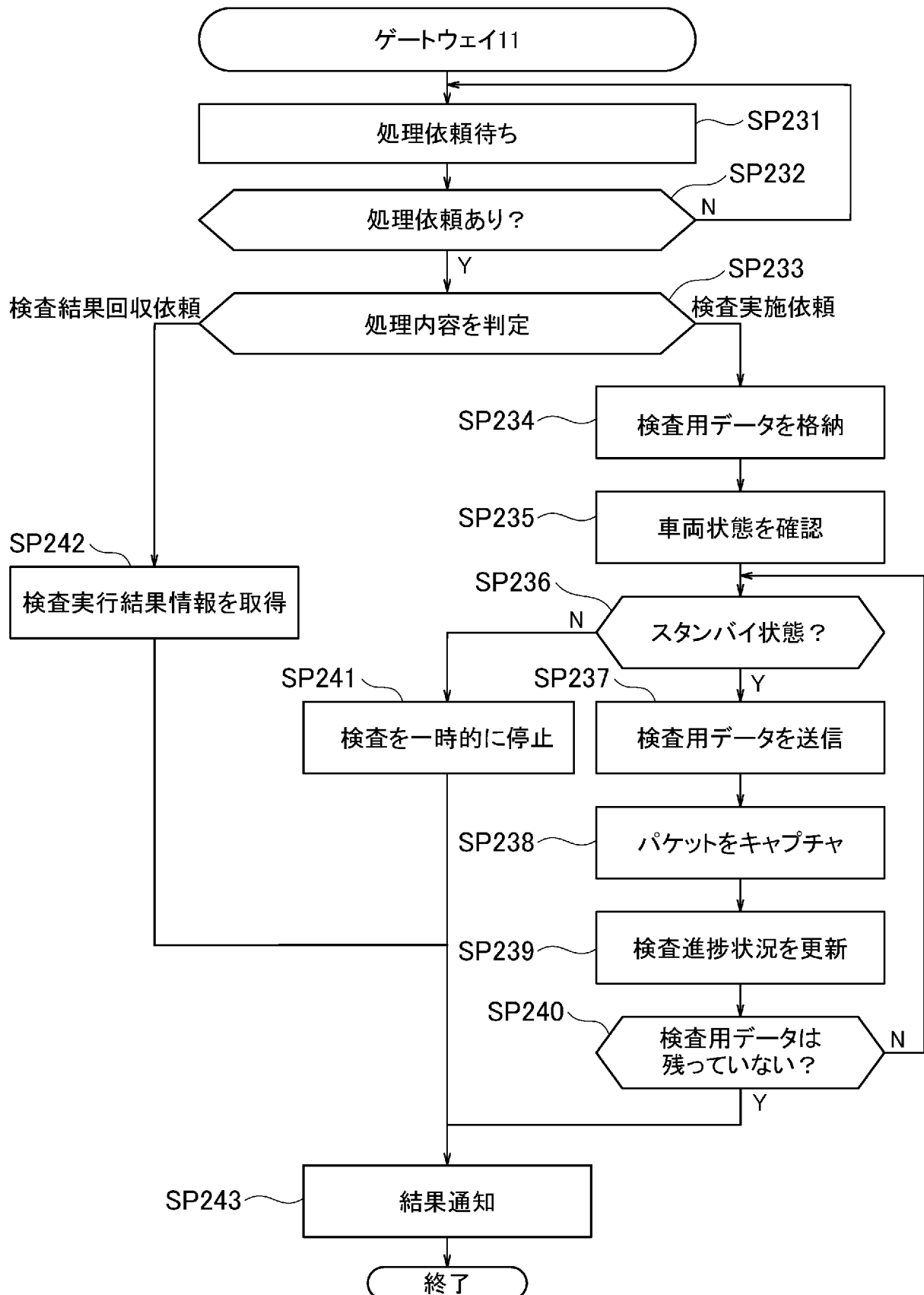
[図22]

図 22



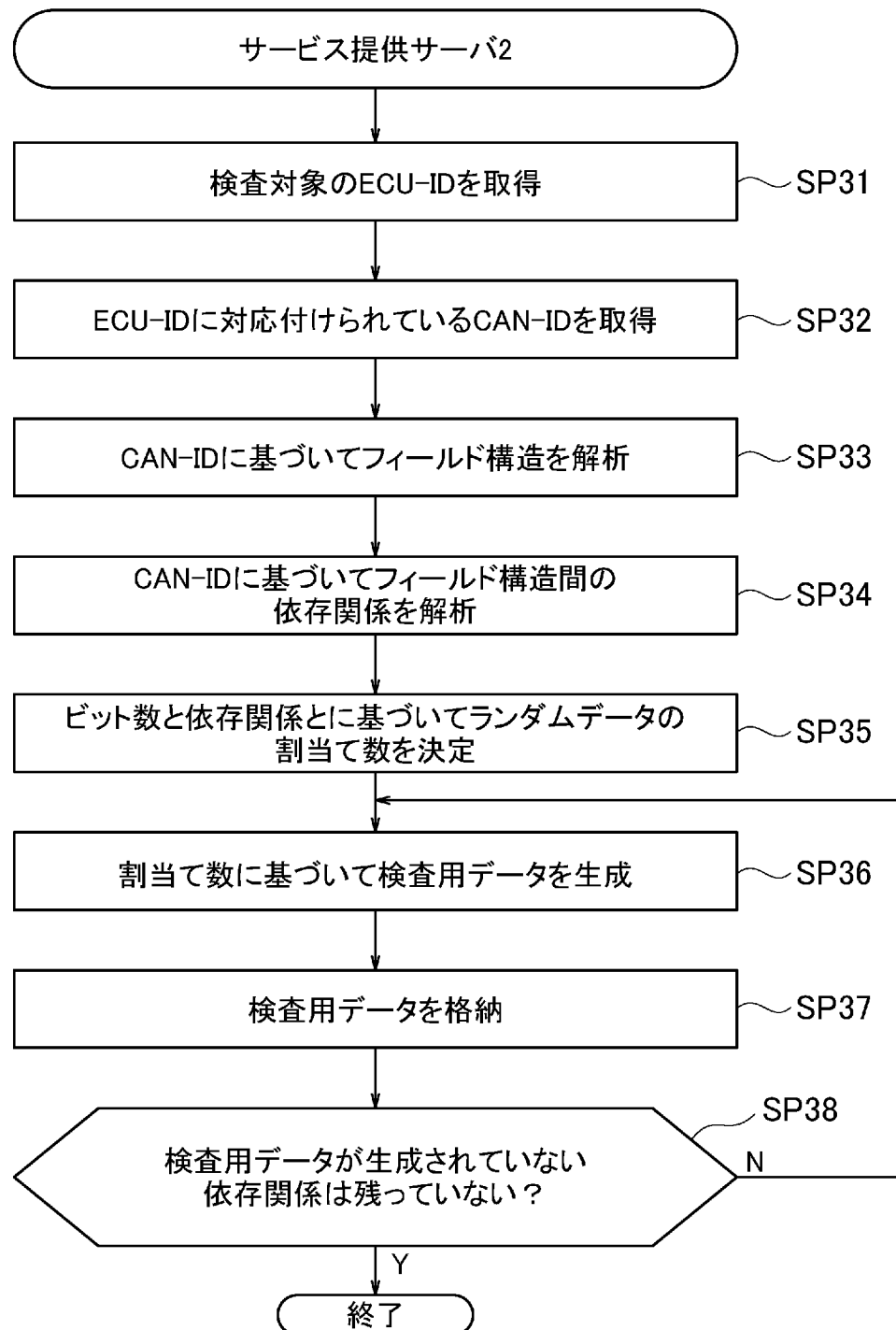
[図23]

図 23



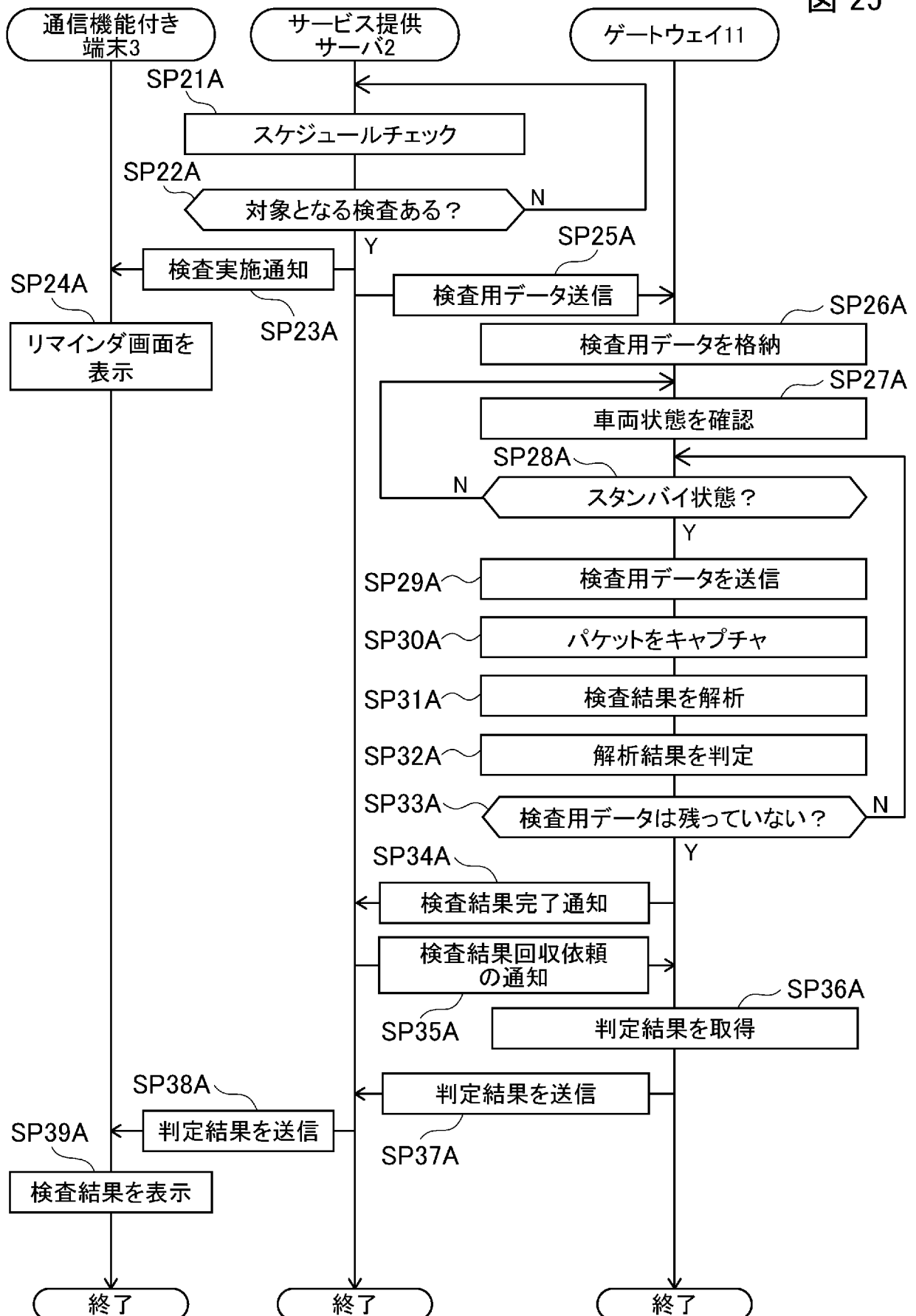
[図24]

図 24



[図25]

図 25



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/059500

A. CLASSIFICATION OF SUBJECT MATTER

B60R16/02(2006.01)i, G01M17/007(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)

B60R16/02, G01M17/007

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-019931 A (Denso Corp.), 21 January 2003 (21.01.2003), entire text; all drawings & US 2003/0009271 A1 & DE 10230351 A1	1-13
A	JP 2007-099145 A (Denso Corp.), 19 April 2007 (19.04.2007), entire text; all drawings & US 2007/0083304 A1 & EP 1826946 A2	1-13

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

☐ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search
27 May 2015 (27.05.15)

Date of mailing of the international search report
09 June 2015 (09.06.15)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. B60R16/02(2006.01)i, G01M17/007(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. B60R16/02, G01M17/007

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	1971-2015年
日本国実用新案登録公報	1996-2015年
日本国登録実用新案公報	1994-2015年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2003-019931 A（株式会社デンソー）2003.01.21, 全文, 全図 & US 2003/0009271 A1 & DE 10230351 A1	1-13
A	JP 2007-099145 A（株式会社デンソー）2007.04.19, 全文, 全図 & US 2007/0083304 A1 & EP 1826946 A2	1-13

☐ 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

27.05.2015

国際調査報告の発送日

09.06.2015

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

前田 浩

3 D

2943

電話番号 03-3581-1101 内線 3341