(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10月8日(08.10.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/202886 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)　*B60R 16/02* (2006.01)
H04L 9/32 (2006.01)　*G06F 8/60* (2018.01)

(21) 国際出願番号：　PCT/JP2020/007013

(22) 国際出願日：　2020年2月21日(21.02.2020)

(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 2019-066887　2019年3月29日(29.03.2019)　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２５２０番地 Ibaraki (JP).

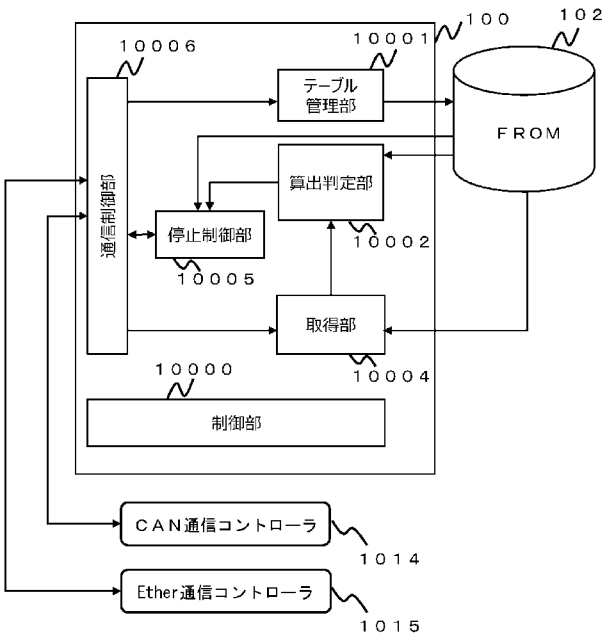
(72) 発明者: 寺岡　秀敏 (**TERAOKA, Hidetoshi**); 〒1008280 東京都千代田区丸の内一丁目６番６号 株式会社日立製作所内 Tokyo (JP). 矢野正 (**YANO, Masashi**); 〒3128503 茨城県ひたちなか市高場２５２０番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP).

(74) 代理人: 特許業務法人サンネクスト国際特許事務所(**SUNNEXT INTERNATIONAL PATENT OFFICE**); 〒1400002 東京都品川区東品川二丁目３番１２号 シーフォートスクエア センタービルディング１６階 Tokyo (JP).

(54) **Title:** COMPUTATION DEVICE AND ASSESSMENT METHOD

(54) 発明の名称： 演算装置、判定方法

［図7］



1014... CAN COMMUNICATION CONTROLLER
1015... Ether COMMUNICATION CONTROLLER
10000... CONTROL UNIT
10001... TABLE MANAGEMENT UNIT
10002... CALCULATION-ASSESSMENT UNIT
10004... ACQUISITION UNIT
10005... INTERRUPT CONTROL UNIT
10006... COMMUNICATION CONTROL UNIT

(57) **Abstract:** A computation device according to the present invention comprises: an external communication unit that is connected to a plurality of electronic control devices, the functions of the plurality of electronic control devices being respectively constituted by one or more electronic control devices, and receives, for each function, function constitution information including first identification information and first verification information for the one or more electronic control devices constituting the function; an acquisition unit for acquiring, from each of the plurality of electronic control

WO 2020/202886 A1

［続葉有］

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

devices, version information for software installed in the electronic control devices, and second identification information for the electronic control devices; a calculation unit that, for each function, uses the version information acquired by the acquisition unit for all electronic control devices constituting the function, and the second identification information for all electronic control devices constituting the function to create second verification information; and an assessment unit that, for each function, assesses whether the first verification information and the second verification information match.

(57) 要約:演算装置は、複数の電子制御装置と接続され、複数の電子制御装置は、1以上の電子制御装置によりそれぞれの機能を構成し、機能ごとに、機能を構成する1以上の電子制御装置の第1識別情報および第1検証情報を含む機能構成情報を受信する外部通信部と、複数の電子制御装置のそれぞれから、電子制御装置に搭載されたソフトウェアのバージョン情報および電子制御装置の第2識別情報を取得する取得部と、機能ごとに、機能を構成するすべての電子制御装置のバージョン情報であって取得部が取得したバージョン情報および機能を構成するすべての電子制御装置の第2識別情報を用いて第2検証情報を作成する算出部と、機能ごとに、第1検証情報および第2検証情報の整合を判定する判定部とを備える。

明　細　書

発明の名称 ： 演算装置、判定方法

技術分野

[0001]　本発明は、演算装置、および判定方法に関する。

背景技術

[0002]　近年、運転支援機能や自動運転技術の進展により、自動車用の電子制御装置（ＥＣＵ：Electric　Control　Unit）に搭載されるソフトウェアの規模が増大している。また、それに伴ってソフトウェア不具合に起因するリコールの回数だけでなく、１回あたりに対応が必要な台数も増加している。そのため、ＥＣＵに搭載されるソフトウェアを遠隔で更新する技術へのニーズが高まっている。ソフトウェアの更新が容易になることで、自動車を構成する各機能に対するハードウェアとソフトウェアの構成を管理することが課題となる。特許文献１には、複数の電子制御装置を備えた車両を特定するシステムであって、各車両に搭載された各電子制御装置の識別データ及び各電子制御装置間の接続状況を示す接続データをパターンとして記憶するパターン記憶手段と、任意の車両のパターンを前記パターン記憶手段に記憶されたパターンと照合する照合手段と、を有し、任意の車両のパターンと記憶された前記パターンとの同一性により前記任意の車両を特定することを特徴とする車両特定システムが開示されている。

先行技術文献

特許文献

[0003] 特許文献1：日本国特開２００４－２７６８２８号公報

発明の概要

発明が解決しようとする課題

[0004]　特許文献１に記載されている発明では、機能ごとの構成情報を確認できない。

課題を解決するための手段

[0005] 本発明の第１の態様による演算装置は、複数の電子制御装置と接続される演算装置であって、前記複数の電子制御装置は、１以上の前記電子制御装置によりそれぞれの機能を構成し、前記機能ごとに、前記機能を構成する１以上の前記電子制御装置の第１識別情報および第１検証情報を含む機能構成情報を受信する外部通信部と、前記複数の電子制御装置のそれぞれから、前記電子制御装置に搭載されたソフトウェアのバージョン情報および前記電子制御装置の第２識別情報を取得する取得部と、前記機能ごとに、前記機能を構成するすべての前記電子制御装置のバージョン情報であって前記取得部が取得したバージョン情報および前記機能を構成するすべての前記電子制御装置の前記第２識別情報を用いて第２検証情報を作成する算出部と、前記機能ごとに、前記第１検証情報および前記第２検証情報の整合を判定する判定部とを備える。

本発明の第２の態様による判定方法は、複数の電子制御装置と接続される演算装置が実行する判定方法であって、前記複数の電子制御装置は、１以上の前記電子制御装置によりそれぞれの機能を構成し、前記機能ごとに、前記機能を構成する１以上の前記電子制御装置の第１識別情報および第１検証情報を受信することと、前記複数の電子制御装置のそれぞれから、前記電子制御装置に搭載されたソフトウェアのバージョン情報および前記電子制御装置の第２識別情報を取得することと、前記機能ごとに、前記機能を構成するすべての前記電子制御装置のバージョン情報であって取得したバージョン情報および前記機能を構成するすべての前記電子制御装置の前記第２識別情報を用いて第２検証情報を作成することと、前記機能ごとに、前記第１検証情報および前記第２検証情報の整合を判定することとを含む。

発明の効果

[0006] 本発明によれば、機能ごとの構成情報を確認できる。

図面の簡単な説明

[0007] [図1]第１の実施の形態にかかる機能構成情報管理システムＳの構成を示す図

[図2]ゲートウェイ１０のハードウェア構成を示すブロック図

[図3]エンジン制御ＥＣＵ１３のハードウェア構成例を示すブロック図

[図4]エンジン制御ＥＣＵ１３上で動作する制御プログラム１３０の構成を示すブロック図

[図5]サーバ２の構成例を示すブロック図

[図6]機能構成情報６１の一例を示す図

[図7]ゲートウェイ１０で動作するゲートウェイプログラム１００の構成を示すブロック図

[図8]本実施の形態におけるテーブル検証情報６０４の検証を示す概念図

[図9]ＨＭＩ１２に表示される表示画面の一例を示す図

[図10]ゲートウェイ１０における検証処理を示すフローチャート

[図11]ゲートウェイ１０における復旧処理を示すフローチャート

[図12]ＥＣＵのソフトウェア更新の手順を示すシーケンス図

[図13]サーバ２における機能構成情報６１の登録画面の一例を示す図

[図14]変形例１における機能構成情報管理システムＳａの構成を示す図

[図15]変形例１における診断装置５の構成例を示すブロック図

[図16]変形例２における機能構成情報６４の一例を示す図

[図17]変形例３における機能構成情報６５の一例を示す図

[図18]第２の実施の形態における機能別バージョン情報９５１の一例を示す図

[図19]第２の実施の形態における機能構成情報６２の一例を示す図

[図20]第３の実施の形態における機能別バージョン情報９５２の一例を示す図

[図21]第３の実施の形態における機能構成情報６３の一例を示す図

[図22]第４の実施の形態における機能Ｄの機能構成情報６１ｃを示す図

[図23]第４の実施の形態における機能制限情報９１の一例を示す図

[図24]第４の実施の形態におけるゲートウェイ１０における機能制限処理を示すフローチャート

発明を実施するための形態

[0008] ―第１の実施の形態―

以下、図１～図１３を参照して、本発明に係る演算装置であるゲートウェイの第１の実施の形態に係る機能構成情報管理システムを説明する。

[0009] （システム構成）

図１は、第１の実施の形態にかかる機能構成情報管理システムＳの構成を示す図である。機能構成情報管理システムＳは車両１、およびサーバ２を備える。車両１とサーバ２は、アクセスネットワークや拠点を接続するインターネット３、および通信サービスプロバイダが提供するアクセスネットワーク４を介して接続される。

[0010] 車両１は、ゲートウェイ１０、通信モジュール１１、Ｈｕｍａｎ　Ｍａｃｈｉｎｅ　Ｉｎｔｅｒｆａｃｅ（ＨＭＩ）１２、および複数のＥＣＵ（電子制御装置）を備える。ゲートウェイ１０、通信モジュール１１、およびＨＭＩ１２は、車内ネットワーク１０ａにより接続される。

[0011] 車両１に備えられるＥＣＵは特に限定しないが、本実施の形態ではたとえばエンジン制御ＥＣＵ１３、ブレーキ制御ＥＣＵ１４、自動運転ＥＣＵ１５、および先進運転支援システム（ＡＤＡＳ）　ＥＣＵ１６を備える。ゲートウェイ１０とこれらのＥＣＵは、車内ネットワーク１０ｂにより接続される。ゲートウェイ１０と接続されるこれらのＥＣＵをまとめて、以下では「配下ＥＣＵ」と呼ぶ。

[0012] 車内ネットワーク１０ａおよび車内ネットワーク１０ｂは既知の通信規格、たとえばＣｏｎｔｒｏｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＣＡＮ）（登録商標）、Ｌｏｃａｌ　Ｉｎｔｅｒｃｏｎｎｅｃｔ　Ｎｅｔｗｏｒｋ（ＬＩＮ）、およびＦｌｅｘＲａｙ、Ｅｔｈｅｒｎｅｔ（登録商標）のいずれかを採用する。本実施の形態では、車内ネットワーク１０ｂはＣＡＮで、車内ネットワーク１０ａはＥｔｈｅｒｎｅｔで構成される。ただし車内ネットワーク１０ａおよび車内ネットワーク１０ｂは同一の通信規格を採用してもよい。また、図１では図示しないが、各種ＥＣＵなどの車両内の各構成要素は電力線で蓄電池に接続され、電力供給を受けている。

[0013] ゲートウェイ１０は、配下ＥＣＵ同士の通信データの中継、配下ＥＣＵのソフトウェア更新、および配下ＥＣＵに搭載されるソフトウェアの整合性確認を行う。ただし以下では、ソフトウェアの整合性確認を「検証」や「検証処理」とも呼ぶ。なお本実施の形態ではゲートウェイ１０はゲートウェイ１０自身のソフトウェア更新および整合性確認を行わないが、ゲートウェイ１０がゲートウェイ１０自身のソフトウェア更新および整合性確認を行ってもよい。なお本実施の形態では、「検証」と「整合」は同じ意味で用いる。

[0014] 通信モジュール１１は、ゲートウェイ１０、ＨＭＩ１２、および配下ＥＣＵとサーバ２との通信を中継する。ＨＭＩ１２は、車両１の乗員であるユーザへの情報提示やユーザからの入力を受け付けるための装置である。ＨＭＩ１２は、画面表示を行う表示装置および各種スイッチ等の入力装置、またはこれらを組み合わせたタッチパネル等により構成される。エンジン制御ＥＣＵ１３は、エンジンの制御を行う。ブレーキ制御ＥＣＵ１４は、ブレーキの制御を行う。自動運転ＥＣＵ１５は、自動運転時に環境の認識や車両の起動指示等を行う。ＡＤＡＳ　ＥＣＵ１６は、自動ブレーキなどの運転支援制御を行う。

[0015] サーバ２は機能構成情報６１をゲートウェイ１０に送信する。ゲートウェイ１０は、機能構成情報６１に基づいて車両１の機能構成を管理する。

[0016] （ゲートウェイのハードウェア構成）

図２は、ゲートウェイ１０のハードウェア構成を示すブロック図である。ゲートウェイ１０は、マイコン１０１、ＦＲＯＭ（ＦｌａｓｈＲＯＭ）１０２、ＣＡＮ用の通信Ｉ／Ｆ（インタフェース）１０４、およびＥｔｈｅｒｎｅｔ用の通信Ｉ／Ｆ１０５を備える。

[0017] マイコン１０１は、ＣＰＵ１０１１、ＳＲＡＭ１０１２、ＦＲＯＭ１０１３、ＣＡＮ通信コントローラ１０１４、およびＥｔｈｅｒ通信コントローラ１０１５を備える。マイコン１０１のＣＰＵ１０１１は、ＦＲＯＭ１０１３に格納されるプログラムを実行し、ゲートウェイ１０内の他の構成要素を制御するとともに、車内ネットワークにより接続された他の機器とデータ送受

信指示を行うなどしてゲートウェイ１０を機能させる。ただしＣＰＵ１０１１の代わりにＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）を用いてもよい。

[0018] ＦＲＯＭ１０２は、不揮発メモリであり、サーバ２から受信した情報が格納される。ＣＡＮ通信コントローラ１０１４は、ＣＡＮ通信用のインタフェースであり、マイコン１０１の指示に基づき車内ネットワーク１０ｂを介して、車内ネットワーク１０ｂに接続された配下ＥＣＵとの間でデータの送受信を行う。Ｅｔｈｅｒ通信コントローラ１０１５は、Ｅｔｈｅｒｎｅｔ通信用のインタフェースであり、マイコン１０１の指示に基づき車内ネットワーク１０ａを介して、車内ネットワーク１０ａに接続された機器との間でデータの送受信を行う。

[0019]（ＥＣＵの構成）

図３は、エンジン制御ＥＣＵ１３のハードウェア構成例を示すブロック図である。ただし本実施の形態においてソフトウェアが更新される対象となるＥＣＵはいずれも、少なくとも図３に示すハードウェア構成を備える。エンジン制御ＥＣＵ１３は、マイコン１３１、およびＣＡＮ用の通信Ｉ／Ｆ１３３を備える。

[0020] マイコン１３１は、ＣＰＵ１３１１、ＳＲＡＭ１３１２、ＦＲＯＭ１３１３、通信コントローラ１３１４、およびＩ／Ｏコントローラ１３１５を備える。マイコン１３１は、ＦＲＯＭ１３１３に格納される制御プログラムを実行し、エンジン制御ＥＣＵ１３内の他の構成要素やＩ／Ｏを介して接続されたセンサ／アクチュエータ１３２を制御するとともに、車内ネットワークで接続された他の機器とデータ送受信指示を行うなどしてエンジン制御を実施する。センサ／アクチュエータ１３２は、マイコン１３１の指示によってエンジン制御に必要となるデータを取得しつつ、エンジンの制御を実行する。

[0021] ＦＲＯＭ１３１３には、ＦＲＯＭ１３１３に格納される制御プログラムのバージョン情報も格納される。またＦＲＯＭ１３１３にはそのＥＣＵの種類や機能を特定する識別情報であるＥＣＵ　ＩＤも格納される。なおＥＣＵ

ＩＤは、「部品番号」や「型番」とも呼ばれる。ＥＣＵ　ＩＤは個々の製品を識別するための、いわゆる製造番号ではなく、ＥＣＵの故障時には同一のＥＣＵ　ＩＤを有する別の製品に交換が可能である。

[0022] 図４は、エンジン制御ＥＣＵ１３上で動作する制御プログラム１３０の構成を示すブロック図である。ただし本実施の形態においてソフトウェアが更新される対象となるＥＣＵはいずれも、少なくとも図４に示す制御プログラム１３０と同様の構成を備える。

[0023] ＥＣＵ１３の機能を実現する制御プログラム１３０は、マイコン１３１のＦＲＯＭ１３１３に格納されＣＰＵ１３１１で実行される。図４では、機能的なまとまりをブロックとして表現しており、各ブロックが複数に分割されてもよいし、いくつかのブロックが統合されてもよい。また制御プログラムは、１つのソフトウェアにより実現されてもよいし、２以上のソフトウェアの組合せにより実現されてもよい。

[0024] 制御プログラム１３０は、制御処理部１３００１、更新制御部１３００３、情報管理部１３００４、および通信制御部１３００５を備える。制御処理部１３００１は、Ｉ／Ｏコントローラ１３１５を制御し、センサ／アクチュエータ１３２を制御してエンジン制御を実施する。停止部１３００１１は、通信制御部１３００５を介してゲートウェイ１０からの停止指令や再開指令を受信し、機能の停止・再開制御を行う。

[0025] 更新制御部１３００３は、通信制御部１３００５を介してゲートウェイ１０からの動作指令やソフトウェアの更新に用いるデータを受信しソフトウェアの更新を制御する。情報管理部１３００４は、ＦＲＯＭ１３１３に格納されるソフトウェアのバージョン情報やＥＣＵ　ＩＤの読み出し、およびソフトウェアの更新に伴うバージョン情報の書き換えを行う。

[0026] 通信制御部１３００５は、更新制御部１３００３等の指示に従って、通信コントローラ１３１４を制御し、車内ネットワーク１０ｂに接続された機器と通信を行う。通信の際には、ＣＡＮフレームを解析・構成する。また通信制御部１３００５は、ＵＤＳ等の診断通信プロトコルに準拠したコマンドの

生成・解析を行う。

[0027]（機能と構成）

本実施の形態では、車両１が有する機能はある１つのＥＣＵにより、または複数のＥＣＵが協業することにより実現される。協業とは、連携して動作することを意味するが、必ずしも各ＥＣＵが協業する他のＥＣＵを認識する必要はなく、結果的に複数のＥＣＵがその機能の実現に関与していればよい。たとえばある機能Ｘがエンジン制御ＥＣＵ１３と、自動運転ＥＣＵ１５との協業により実現される場合には、本実施の形態では、エンジン制御ＥＣＵ１３および自動運転ＥＣＵ１５が機能Ｘを「構成する」と言う。また、エンジン制御ＥＣＵ１３および自動運転ＥＣＵ１５が機能Ｘを「実現する」とも言う。

[0028]（サーバの構成）

図５は、サーバ２の構成例を示すブロック図である。サーバ２は、ＣＰＵ２０１、主記憶部２０２、補助記憶部２０３、通信部２０４、入力部２０５、表示部２０６を備える。ＣＰＵ２０１は、補助記憶部２０３等に蓄積されたサーバ用プログラムを主記憶部２０２上で実行し機能構成管理情報の登録や配信の制御を行う。補助記憶部２０３は、機能構成管理情報や車両に配信するＥＣＵソフトウェア更新用のデータを記憶する。

[0029] 通信部２０４は、インターネットを介して車両１との間でデータの送受信を行う。入力部２０５は、サーバ２を操作するオペレータからの操作や入力情報を受け付ける。表示部２０６は、サーバ２を操作するオペレータに機能構成管理情報登録に関する情報を提供する。

[0030]（機能構成管理情報）

図６は、サーバ２で生成され、診断装置５やゲートウェイ１０のテーブル管理部１０００１が管理する機能構成情報６１の一例を示す図である。図６（ａ）は変更前の機能構成情報６１である機能構成情報６１ａを示し、図６（ｂ）は変更後の機能構成情報６１である機能構成情報６１ｂを示す。

[0031] 図６では、機能構成情報６１をテーブルとして管理し、機能毎の構成情報

を記録する場合の例が示されている。機能構成情報６１は複数のレコードを有する。機能構成情報６１の各レコードは、機能識別ＩＤ６０１、機能識別検証情報６０２、組み合わせテーブル６０３、組み合わせテーブル検証情報６０４、およびフラグ６０５のフィールドを備える。図６に示す例では、機能構成情報６１はＲ１１、Ｒ２１、およびＲ３１の３つのレコードを有するが、機能構成情報６１が有するレコードは１以上であればよく上限はない。また、機能識別検証情報６０２およびテーブル検証情報６０４のフィールドはサーバ２のＣＰＵ２０１による演算の結果が格納される。他のフィールドの情報は、オペレータにより入力される。

[0032] 機能識別ＩＤ６０１は、機能を構成するＥＣＵのハードウェアとソフトウェアの組み合わせを識別するための識別情報が格納されるフィールドである。ただしここで言う「ソフトウェア」とはバージョン番号も含んだ概念である。したがって機能識別ＩＤ６０１は、組み合わせテーブル６０３に登録されたＥＣＵ　ＩＤが変更された場合だけでなく、ソフトウェアのバージョンが変化した場合にも値が変更される。機能識別ＩＤ６０１はたとえば、機能を識別する文字列とＥＣＵ　ＩＤやバージョンの変化に対応する数字の組み合わせである。

[0033] 機能識別検証情報６０２は、機能識別ＩＤ６０１の完全性検証情報を格納する領域である。機能識別ＩＤ６０１の完全性検証情報は、たとえば、機能識別ＩＤ６０１のデジタル署名である。

[0034] 組み合わせテーブル６０３は、ＮＥＴ　ＩＤ６０３１、ＥＣＵ　ＩＤ６０３２、およびソフトウェアバージョン６０３３から構成される。組み合わせテーブル６０３には、機能識別ＩＤ６０１が示す機能に関連するＥＣＵのハードウェアとソフトウェアの組み合わせの情報が格納される。ＮＥＴ　ＩＤ６０３１には、車載ネットワーク上での当該ＥＣＵの識別情報を示すＩＤが格納される。車載ネットワーク１０ｂがＣＡＮの場合にはＮＥＴ　ＩＤ６０３１にはＣＡＮ　ＩＤが格納され、車載ネットワーク１０ｂがＥｔｈｅｒｎｅｔの場合にはＩＰアドレスやＭＡＣアドレスが格納される。ＮＥＴ　ＩＤ

６０３１にはネットワーク種別や、チャンネル番号など、不図示の情報が含まれてもよい。

[0035] ＥＣＵ　ＩＤ６０３２には、ＥＣＵの種類や機能を識別するための情報が格納される。ＥＣＵ　ＩＤ６０３２には、たとえばエンジン制御ＥＣＵ１３の種類や機能を示す識別情報である「エンジン」が格納される。ＥＣＵの識別情報としては部品番号などが利用されてもよい。すなわちＮＥＴ　ＩＤ６０３１はＥＣＵのネットワーク上の識別子であるのに対して、ＥＣＵ　ＩＤ６０３２はＥＣＵの種類を示す識別子である。また以下では、ＮＥＴ　ＩＤ６０３１を「第１識別情報」と呼ぶことがあり、ＥＣＵ　ＩＤ６０３２を「第２識別情報」と呼ぶことがある。

[0036] ソフトウェアバージョン６０３３は、ＥＣＵに搭載されたソフトウェアのバージョンを識別するための情報が格納されるフィールドである。なお以下では、ＥＣＵ　ＩＤ６０３２に格納される情報とソフトウェアバージョン６０３３に格納される情報とを合わせて「構成情報」とも呼ぶ。

[0037] 組み合わせテーブル検証情報６０４は、組み合わせテーブル６０３に登録された情報の完全性検証情報を格納する領域である。組み合わせテーブル検証情報６０４は、たとえば、機能識別ＩＤ６０１とＥＣＵ　ＩＤ６０３２、ソフトウェアバージョン６０３３を連結した値のデジタル署名である。

[0038] フラグ６０５は、組み合わせテーブル６０３に登録された情報と、配下ＥＣＵから収集した情報に矛盾がある場合に、機能識別ＩＤ６０１により示される機能の動作継続を許可するか否かを示す情報が格納される。継続動作を許可する場合には「動作許可」が格納され、動作許可を許容せず停止が必要な場合には「停止」が格納される。

[0039] 図６（ａ）のレコードＲ１は、機能識別ＩＤが”Ａ１”で示される機能Ａに関連する情報が格納されたレコードである。レコードＲ１の機能識別検証情報６０２のフィールドには「ａａａ」が格納され、ＮＥＴ　ＩＤ６０３１のフィールドには「７００」が格納され、ＥＣＵ　ＩＤ６０３２のフィールドにはエンジン制御ＥＣＵ１３であることを示す「エンジン」が格納され、

ソフトウェアバージョン６０３３のフィールドには「１．０．０．０」が格納され、組み合わせテーブル検証情報６０４のフィールドには「ｔａａａ」が格納され、フラグ６０５のフィールドには、不整合が発生した場合も当該機能の動作継続を許可する「動作許可」が格納されている。

[0040] 図６（ａ）のレコードＲ２は、機能識別ＩＤが”Ｂ１”で示される機能Ｂに関連する情報が格納されたレコードである。レコードＲ２の機能識別検証情報６０２のフィールドには「ｂｂｂ」が格納され、ＮＥＴ　ＩＤ６０３１のフィールドには「７０１」が格納され、ＥＣＵ　ＩＤ６０３２のフィールドにはブレーキ制御ＥＣＵ１４であることを示す「ブレーキ」が格納され、ソフトウェアバージョン６０３３のフィールドには「１．０．０．０」が格納され、組み合わせテーブル検証情報６０４のフィールドには「ｔｂｂｂ」が格納され、フラグ６０５のフィールドには、不整合が発生した場合は当該機能の動作停止が必要であることを示す「停止」が格納されている。

[0041] 図６（ａ）のレコードＲ３は、機能識別ＩＤが”Ｃ１”で示される機能Ｃに関連する情報が格納されたレコードである。レコードＲ３の機能識別検証情報６０２のフィールドには「ｃｃｃ」が格納される。機能Ｃを構成するＥＣＵは３つであるため、ＮＥＴ　ＩＤ６０３１のフィールドには「７００」「７０１」「７０２」がそれぞれ格納され、ＥＣＵ　ＩＤ６０３２のフィールドには「エンジン」「ブレーキ」「ＡＤＡＳ」がそれぞれ格納され、ソフトウェアバージョン６０３３のフィールドには「１．０．０．０」「１．０．０．０」「１．０．０．０」がそれぞれ格納される。レコードＲ３の組み合わせテーブル検証情報６０４のフィールドには「ｔｃｃｃ」が格納され、フラグ６０５のフィールドには、不整合が発生した場合は当該機能の動作停止が必要であることを示す「停止」が格納されている。

[0042] なおここでは、機能Ｃが３つのＥＣＵにより構成される例を示したが、前述のように１つの機能がいくつのＥＣＵにより構成されてもよく、１つの機能を構成するＥＣＵの数に上限はない。

[0043] 図６（ｂ）は図６（ｂ）に示す機能構成情報６１ａからエンジン制御ＥＣ

Ｕ１３のソフトウェアが更新された場合の更新後の機能構成情報６１である機能構成情報６１ｂを示す図である。具体的には図６（ｂ）ではエンジン制御ＥＣＵ１３のソフトウェアバージョンが「１．０．０．０」から「１．０．０．１」に更新された。図６（ｂ）に示すレコードＲ１２、Ｒ２２、およびＲ３２は、図６（ａ）に示すレコードＲ１１、Ｒ２１、およびＲ３１にそれぞれ対応する。

[0044] ソフトウェアの更新に伴って、図６（ｂ）のレコードＲ１２およびＲ３２に示すように、ＥＣＵ　ＩＤ６０３２が「エンジン」であるレコードのソフトウェアバージョン６０３３が「１．０．０．１」に更新されている。また、エンジン制御ＥＣＵ１３を構成要素に含むレコードＤ１０１ｂとレコードＤ１０３ｂの機能の機能識別ＩＤ６０１がそれぞれ”Ａ２”と”Ｃ２”に更新されている。このように、機能構成情報においては、機能実現に関連するＥＣＵの構成変更に伴い、機能識別ＩＤが更新する必要がある。

[0045]（ゲートウェイまたは診断装置のソフトウェア構成）

図７は、ゲートウェイ１０で動作するゲートウェイプログラム１００の構成を示すブロック図である。

[0046] ゲートウェイ１０の機能を実現するゲートウェイプログラム１００は、マイコン１０１のＦＲＯＭ１０１３に格納されＣＰＵ１０１１により実行される。図７では、機能的なまとまりをブロックとして表現しており、各ブロックが複数に分割されてもよいし、いくつかのブロックが統合されてもよい。また制御プログラムは、１つのソフトウェアにより実現されてもよいし、２以上のソフトウェアの組合せにより実現されてもよい。

[0047] ゲートウェイプログラム１００は、制御部１００００、テーブル管理部１０００１、算出判定部１００００２、取得部１００００４、停止制御部１００００５、および通信制御部１００００６を含む。制御部１００００は、テーブル管理部１００００１、算出判定部１００００２、取得部１００００４、停止制御部１００００５、および通信制御部１００００６を制御する。テーブル管理部１００００１は、ＦＲＯＭ１０１３に格納される機能構成情報６１を管理する。

[0048] 算出判定部１００００２は、取得部１００００４から取得した構成情報を用いて検証値を算出し、機能構成情報６１に含まれるテーブル検証情報６０４との整合を判定する。算出判定部１００００２は、判定の結果を停止制御部１００００５に出力する。検証値の算出方法はサーバ２と同様である。算出判定部１００００２が検証値の算出に用いる値、すなわちＥＣＵ　ＩＤとソフトウェアのバージョンがサーバ２が算出に用いた値と同じであれば、検証値とテーブル検証情報６０４は整合する。

[0049] 取得部１００００４は、テーブル管理部１００００１が管理する情報に基づいて、ＥＣＵからＥＣＵ　ＩＤやソフトウェアバージョンなどの構成情報を取得し、検証情報算出部に出力する。停止制御部１００００５は、テーブル管理部１００００１が管理する動作許可・停止を示すフラグと、算出判定部１０００００２の出力情報に基づいて、不整合が発生した機能の動作継続・停止制御を行う。

[0050] 通信制御部１００００６は、停止制御部１００００５等の指示に従って、ＣＡＮ通信コントローラ１０１４およびＥｔｈｅｒ通信コントローラ１０１５を制御し、車内ネットワーク１０ａおよび１０ｂに接続された機器と通信を行う。車内ネットワーク１０ａに接続された機器と通信する際には、通信制御部１００００７は、ＴＣＰ／ＩＰやＵＤＰ／ＩＰなどのパケットを解析・生成する。また車内ネットワーク１０ｂに接続された機器と通信する際には、通信制御部１００００６は、ＣＡＮフレームを解析・生成する。なお通信制御部１００００６は、通信モジュール１１を介して車両１の外部との通信が可能なので、「外部通信部」とも呼べる。

[0051]（検証）

図８は、本実施の形態におけるテーブル検証情報６０４の検証を示す概念図である。図８には以下の説明との対応関係を示すために便宜的にステップ番号を付与している。このステップ番号は後述するフローチャートのステップ番号とは対応しない。

[0052] サーバ２には予め秘密鍵ＳＫが格納され、ゲートウェイ１０には予め公開

鍵ＰＫが格納されている。サーバ２のＣＰＵ２０１は、あらかじめ定めたルールにしたがって、機能ごとに構成情報を繋げたビット列Ｘを作成する（Ｓ９０１）。たとえば図６に示したように機能Ａを構成するＥＣＵ「エンジン制御ＥＣＵ」だけの場合は、機能Ａのテーブル検証情報６０４を作成するために、ＣＰＵ２０１は「エンジン」を所定のルールによりたとえばＵＴＦ－８の文字コード番号に変換して「０ｘ８３４７１２３４５」を得て、バージョン番号「１．０．０．０」を所定のルールにより変換して「０ｘ１０００」を得る。そしてこの２つのビット列を連結して得られる「０ｘ８３４７１２３４５１０００」をビット列Ｘとする。

[0053] なお、ある機能が複数のＥＣＵから構成される場合には、ビット列Ｘを作成する際のビット列を並べる順番は、たとえばＮＥＴ　ＩＤが小さい順番に並べるなどのルールがあらかじめ定められている。

[0054] そしてＣＰＵ２０１は、そのビット列Ｘを対象とし、秘密鍵ＳＫを用いてデジタル署名Ｙを作成する（Ｓ９０２）。作成したデジタル署名Ｙは、機能構成情報６１のテーブル検証情報６０４として格納され、ゲートウェイ１０に送信される。デジタル署名Ｙの作成方式はあらかじめゲートウェイ１０と共有されている。

[0055] ゲートウェイ１０は、サーバ２から受信した機能構成情報６１を参照し、機能ごとにＥＣＵから構成情報を読み出し、あらかじめ定めたルールにしたがって検証値であるビット列Ｚを作成する（Ｓ９０３）。このビット列Ｚのルールは、サーバ２に格納されているビット列Ｘの作成ルールと同一である。そしてゲートウェイ１０は、機能構成情報６１に格納されたテーブル検証情報６０４、すなわちデジタル署名Ｙを公開鍵ＰＫを用いて復号化し、ビット列Ｘを得る（Ｓ９０４）。

[0056] 念のために記載すると、あらかじめ用意された秘密鍵ＳＫと公開鍵ＰＫの組合せが適切ならば、ゲートウェイ１０に接続されているＥＣＵの如何にかかわらず、ゲートウェイ１０において復号化されて得られるビット列Ｘはサーバ２において作成されたビット列Ｘと同一である。最後にゲートウェイ１

０は、ビット列Ｘとビット列Ｚが同一か否かを判断することで検証の合否を判断する（Ｓ９０５）。

[0057] ただしビット列Ｘを用いたデジタル署名Ｙの作成において、ビット列Ｘをそのまま用いずにビット列Ｘのハッシュ値やビット列Ｘとあらかじめ定めた値とのＸＯＲ値に対してデジタル署名Ｙを作成してもよい。また上述した説明におけるＳ９０３とＳ９０４は実行の順番を入れ替えてもよいし略同時に実行してもよい。なお以下では、ビット列Ｚを「検証値」とも呼ぶ。またビット列Ｚの比較対象は上述した通りビット列Ｘであるが、以下の説明では冗長な記載を避けるために、単に「ビット列Ｚとデジタル署名Ｙの整合を判定する」、または「検証値とテーブル検証情報６０４の整合を判定する」と記載する。

[0058] （車両側画面表示例）

図９は、ＨＭＩ１２に表示される表示画面の一例を示す図である。図９（ａ）に示す表示Ｇ１ａは、機能構成情報と実際の構成の不整合が検出されたことをユーザに示す画面例である。不整合により機能を停止させている場合は、さらに本画面に機能停止している旨の情報を表示してもよい。図９（ｂ）に示す表示Ｇ１ｂは、機能構成情報が不整合なため、機能の一部を停止したことをユーザに示す画面例である。

[0059] 図９（ｃ）に示す表示Ｇ１ｃは、機能構成情報が不整合で対策できないため、回復のためにディーラに連絡することをユーザに促す画面例である。図９（ｄ）に示す表示Ｇ１ｄは、機能構成情報の不整合が回復され、機能の一部が普及したことをユーザに示す画面例である。

[0060] （確認シーケンス）

図１０は、ゲートウェイ１０における検証処理を示すフローチャートである。図１０に示す処理は、車両１のイグニッションスイッチがオンにされると実行される。なおゲートウェイ１０は、イグニッションスイッチと信号線で接続されてイグニッションスイッチからオン／オフの状態を示す信号を直接受信してもよいし、イグニッションスイッチと接続される不図示のＥＣＵ

から動作指令信号をうけて動作を開始してもよい。

[0061] まず制御部１００００は、最初に処理対処のレコードｘを１に設定する（Ｓ１０１）。機能構成情報６１が図６（ａ）に示すものの場合は、Ｘ＝１の場合にはレコードＲ１１が読み込まれ、Ｘ＝２の場合にはレコードＲ２１が読み込まれる。後述するＳ１１２の判断により、ゲートウェイプログラム１００は、機能構成情報６１に格納されたレコードの数だけＳ１０３～Ｓ１１１の処理を繰り返す。

[0062] 制御部１００００は、機能構成情報６１における処理対象レコードｘのＮＥＴ　ＩＤを読み出し、取得部１００００４にそのＮＥＴ　ＩＤを有するＥＣＵからの構成情報の読み出しを指示する（Ｓ１０３）。取得部１００００４は、通信制御部１００００６を介して、ＥＣＵから構成情報、すなわちＥＣＵＩＤとソフトウェアバージョンの組合せを読み出し、算出判定部１００００２に読み出した構成情報を渡す（Ｓ１０４）。なお図６（ａ）に示すレコードＲ３１のようにＮＥＴ　ＩＤが複数存在する場合には、そのすべてのＮＥＴ　ＩＤに対して構成情報を読み出す。算出判定部１００００２は、受信した構成情報を用いて検証情報を算出する（Ｓ１０５）。

[0063] 算出判定部１００００２は、機能構成情報６１の処理対処のレコードｘにおけるテーブル検証情報６０４を読みだし、Ｓ１０５において算出した検証値との整合を判断する（Ｓ１０６）。算出判定部１００００２は、検証値とテーブル検証情報６０４が整合すると判断する場合は（Ｓ１０７：ＹＥＳ）、Ｓ１１２に進んで制御部１００００が未確認のレコード有無を確認する。制御部１００００は、未確認のレコードがないと判断する場合は（Ｓ１１２：ＮＯ）、確認済みレコードの不整合の有無を確認する。制御部１００００は、不整合が全くない、すなわち機能構成情報６１の全レコードについて算出判定部１００００２が算出する検証値と機能構成情報６１から読み出したテーブル検証情報６０４が整合すると判断する場合は（Ｓ１１３：ＮＯ）は、処理を終了する。

[0064] 制御部１００００は、不整合がある、すなわち機能構成情報６１のいずれ

かのレコードにおいて算出判定部１００００２が算出する検証値と機能構成情報６１から読み出したテーブル検証情報６０４が整合しないと判断する場合は（Ｓ１１３：ＹＥＳ）、ＨＭＩに図９の画面Ｇ１ａの表示を指示し（Ｓ１１４）、処理を終了する。未確認のレコードがある場合（Ｓ１１２：ＹＥＳ）は、制御部１００００は処理対象レコードｘを次のレコードに更新して（Ｓ１１５）、Ｓ１０３に戻る。

[0065] 制御部１００００は、整合しないと判断する場合（Ｓ１０７：ＮＯ）、バージョン情報が整合しない旨の故障コード、すなわちＤＴＣ（diagnostic trouble code）コードを記録する（Ｓ１０８）。停止制御部１００００５は、制御部１００００から処理対象レコードＸと比較結果を受信し、機能構成情報６１から該当レコードのフラグ６０５を読み出す（Ｓ１０９）。停止制御部１００００５は、読み出したフラグ６０５が「動作許可」の場合（Ｓ１１０：ＹＥＳ）は、何もせずに処理を継続する。読み出したフラグ６０５が「動作許可」ではない場合（Ｓ１１０：ＮＯ）は、通信制御部１００００６を介して、機能構成情報６１の処理対象レコードＸに登録された関連ＥＣＵに当該機能の停止を指示する（Ｓ１１１）。以上が図１０の説明である。

[0066] （不整合時の復旧シーケンス）

図１１は、ゲートウェイ１０における復旧処理を示すフローチャートである。図１１に示す処理は、図１０に示す処理の完了後であって、機能構成情報６１のいずれかのレコードに不整合がある場合に実行される。ただし図１１に示す処理は必ずしも図１０に示す処理の完了を待機してから開始しなくてもよく、たとえばＳ１０７において否定判断がされた際にＳ１０８と並列に実行を開始してもよい。

[0067] 制御部１００００は、最初に機能構成情報が不整合である情報を含む構成情報をサーバ２に送信する（Ｓ２０１）。サーバ２は、ゲートウェイ１０から受信した構成情報に基づき、次の３つのいずれかの応答を送信する。第１の応答は機能構成情報６１の更新指示、第２の応答はＥＣＵのソフトウェア更新指示、第３の応答は機能構成情報６１およびＥＣＵのソフトウェアの更

新指示である。サーバ２はたとえば、機能構成情報６１の更新日時やＥＣＵのソフトウェアの更新日時、ソフトウェアのバージョン番号に基づき第１～第３の応答のいずれにするかを選択する。ただしサーバ２は更新指示を含めない応答を返してもよい。

[0068] 制御部１００００はサーバ２からの応答を受信すると（Ｓ２０２）、その中に更新指示が含まれるかを判定する。制御部１００００は、更新指示が含まれないと判断する場合は（Ｓ２０３：ＮＯ）、ＨＭＩ１２に図９（ｃ）に示す画面Ｇ１ｃの表示を指示し（Ｓ２０４）、図１１に示す処理を終了する。制御部１００００は、応答に更新指示が含まれると判断する場合は、サーバ２からの応答に機能構成情報６１の更新指示が含まれるかどうかを判定する。制御部１００００は、機能構成情報６１の更新指示が含まれると判断する場合は（Ｓ２０５：ＹＥＳ）、機能構成情報６１を更新する（Ｓ２０６）。

[0069] 次に制御部１００００は、サーバ２からの応答にＥＣＵのソフトウェア更新指示が含まれるか否かを判定する。制御部１００００は、ＥＣＵのソフトウェア更新指示が含まれないと判断する場合は（Ｓ２０７：ＮＯ）、機能を停止していたＥＣＵに機能復旧を指示し（Ｓ２０９）、ＨＭＩ１２に図９（ｄ）に示す画面Ｇ１ｄの表示を指示（Ｓ２１０）して、図１１に示す処理を終了する。制御部１００００は、ＥＣＵのソフトウェア更新指示が含まれると判断する場合は（Ｓ２０７：ＹＥＳ）、ＥＣＵのソフトウェア更新処理を実行（Ｓ２０８）する。そして制御部１００００は、ソフトウェア更新が完了すると、機能を停止していたＥＣＵに機能復旧を指示し（Ｓ２０９）、ＨＭＩ１２に図９（ｄ）に示す画面Ｇ１ｄの表示を指示（Ｓ２１０）して、図１１に示す処理を終了する。

[0070]（ソフトウェア更新シーケンス）

図１２は、ＥＣＵのソフトウェア更新の手順を示すシーケンス図である。なお図１２では処理の一例としてエンジン制御ＥＣＵ１３をソフトウェア更新の処理対象として説明するが、以下に説明するシーケンスは処理対象のＥ

ＣＵによらず共通である。

[0071] ゲートウェイ１０は、最初に更新対象であるエンジン制御ＥＣＵ１３からＥＣＵ　ＩＤとソフトウェアバージョンを読み出す（Ｓ２０８１）。ゲートウェイ１０は、次に収集したＥＣＵ　ＩＤとソフトウェアバージョン、すなわち構成情報をサーバに送信する（Ｓ２０８２）。サーバ２は、受信した構成情報をもとに、当該車両のソフトウェア更新有無を判断し、その結果としての更新情報をゲートウェイ１０に送信する（Ｓ２０８３）。次に、ゲートウェイ１０は、サーバ２から更新に必要なデータをダウンロードする（Ｓ２０８４）。更新に必要なデータには、新しいソフトウェアや、更新後の機能構成情報６１が含まれる。

[0072] 次に、ゲートウェイ１０は、更新対象のエンジン制御ＥＣＵ１３を制御してエンジン制御ＥＣＵ１３のソフトウェアを更新する（Ｓ２０８５）。ゲートウェイ１０は、更新が完了すると機能構成情報６１を更新する（Ｓ２０８６）。

[0073] なお、図１１のＳ２０８におけるソフトウェア更新処理では、Ｓ２０８１～Ｓ２０８３は、図１１のＳ２０１で実施済みのため実施を省略できる。またゲートウェイ１０は、ダウンロードしたデータに機能構成情報６１が含まれない場合は、Ｓ２０８６は実施しなくてよい。

[0074] （サーバ側画面表示例）

図１３は、サーバ２における機能構成情報６１の登録画面の一例を示す図である。登録画面Ｇ２は、サーバ２の表示部２０６に表示される。機能構成情報６１の登録画面Ｇ２は、対象機能Ｇ２１、機能識別ＩＤ　Ｇ２２、機能実現ＥＣＵ　Ｇ２３、不整合時動作Ｇ２４、登録ボタンＧ２５、および行追加ボタンＧ２６から構成される。

[0075] 対象機能Ｇ２１は、緊急ブレーキ機能などの管理対象の機能を識別する情報を設定する領域であり、本例では符号Ｇ２１ａに示すように「機能Ｃ」が設定されている。機能識別ＩＤ　Ｇ２２は、管理対象の構成を一意に識別するための識別情報を設定する領域であり、本例では符号Ｇ２２ａに示すよう

に「Ｃ１」が設定されている。

[0076] 関連ＥＣＵ　Ｇ２３は、対象機能Ｇ２１を実現するＥＣＵを一意に特定するための情報を設定する領域であり、ＮＥＴ　ＩＤ、ＥＣＵ　ＩＤ、ソフトウェアバージョンで構成される。本例では、符号Ｇ２３ａ～Ｇ２３ｃで示す３つのＥＣＵにより機能Ｃが実現されることが示されている。符号Ｇ２３ａに示すＥＣＵは、ＮＥＴ　ＩＤが「７００」、ＥＣＵ　ＩＤが「エンジン」、ソフトウェアバージョンが「１．０．０．０」である。符号Ｇ２３ｂに示すＥＣＵは、ＮＥＴ　ＩＤが「７０１」、ＥＣＵ　ＩＤが「ブレーキ」、ソフトウェアバージョンが「１．０．０．０」である。符号Ｇ２３ｃに示すＥＣＵは、ＮＥＴ　ＩＤが「７０２」、ＥＣＵ　ＩＤが「ＡＤＡＳ」、ソフトウェアバージョンが「１．０．０．０」である。

[0077] 不整合時動作Ｇ２４は、対象機能Ｇ２１に示す機能の構成情報に不整合を検出した場合の当該機能の動作を設定する領域絵であり、本例では符号Ｇ２４ａに示すように「停止」が設定されている。登録ボタンＧ２５は入力した情報をサーバ２に登録するためのボタンであり、オペレータがこのボタンを押すと機能識別検証情報６０２およびテーブル検証情報６０４のフィールドの値がＣＰＵ２０１によって算出される。行追加ボタンＧ２６は、機能実現ＥＣＵの入力欄を増加させるためのボタンである。

[0078] 上述した第１の実施の形態によれば、次の作用効果が得られる。

（１）ゲートウェイ１０は、複数のＥＣＵと接続される。複数のＥＣＵのそれぞれは、１以上のＥＣＵによりそれぞれの機能を構成する。ゲートウェイ１０は、機能ごとに、機能を構成する１以上のＥＣＵの第１識別情報、すなわちＮＥＴ　ＩＤ６０３１および第１検証情報、すなわちテーブル検証情報６０４を含む機能構成情報６１を受信する外部通信部、すなわち通信制御部１０００６と、複数のＥＣＵのそれぞれから、ＥＣＵに搭載されたソフトウェアバージョン６０３３およびＥＣＵの第２識別情報、すなわちＥＣＵ　ＩＤ６０３２を取得する取得部１００００４と、機能ごとに、機能を構成するすべてのＥＣＵのバージョン情報であって取得部が取得したソフトウェアバー

ジョン６０３３および機能を構成するすべてのＥＣＵの第２識別情報、すなわちＥＣＵ　ＩＤ６０３２を用いて第２検証情報、すなわちビット列Ｚを算出する算出判定部１００００２と、機能ごとに、第１検証情報および第２検証情報の整合を判定する算出判定部１００００２とを備える。そのためゲートウェイ１０は、ゲートウェイ１０に接続されるＥＣＵが構成する全ての機能について、機能ごとの構成情報を確認することができる。

[0079] ある機能が複数のＥＣＵにより構成される場合には、それら複数のＥＣＵに搭載されるソフトウェアのバージョンは、意図された通りの組合せであることが望ましい。たとえば事前に検証されていない組合せでは動作が保証できない場合があるからである。また、ソフトウェアの更新は無線通信を介して実行することも可能なので、専門店に持ち込んでソフトウェアを更新する場合に比べれば、ソフトウェアのバージョンの組合せが予定していないものになる可能性が高まる。また、ＥＣＵが故障した際に同一の型番の他のＥＣＵと交換し、そのＥＣＵのソフトウェアのバージョンが交換前のＥＣＵと一致していないことも起こりうる。このような場合に、本実施の形態で示した検証処理を行うことで、機能ごとの構成情報を確認し、問題の発見や問題がないことの確認が可能となる。

[0080] （２）第１識別情報とは、ＥＣＵのネットワーク上の識別子、すなわちＮＥＴ　ＩＤ６０３１である。第２識別情報とは、ＥＣＵの種類を示す識別子、すなわちＥＣＵ　ＩＤ６０３２である。

[0081] （３）機能構成情報６１には、機能ごとに不整合時の実行を許可または拒否を示すフラグ６０５が含まれる。停止制御部１００００５は、算出判定部１００００２により第１検証情報と第２検証情報とが整合しないと判断されると、整合しないと判定された第２検証情報に関する機能であって、機能構成情報におけるフラグが不整合時に実行を拒否することを示すフラグを有する機能を停止させる。そのためゲートウェイ１０は、フラグ６０５の設定に応じて不整合時に機能を停止させることができる。

[0082] （４）制御部１００００は、算出判定部１００００２により第１検証情報と第

２検証情報とが整合しないと判断されると、Ｅｔｈｅｒ通信コントローラ１０１５から受ける指令に基づき、機能構成情報６１およびＥＣＵのソフトウェアの少なくとも一方を更新する。そのためゲートウェイ１０は、不整合時に機能構成情報６１およびＥＣＵのソフトウェアの少なくとも一方を更新できる。

[0083] （５）制御部１００００は、算出判定部１００００２により第１検証情報と第２検証情報とが整合しないと判断されると、不整合が生じたことを故障コードとして記憶部であるＦＲＯＭ１０２に記録する。そのため、ＦＲＯＭ１０２を参照することで不整合の発生を事後的に確認できる。

[0084] （６）制御部１００００は、算出判定部１００００２により第１検証情報と第２検証情報とが整合しないと判断されると、不整合が生じたことを表示部、すなわちＨＭＩ１２に表示させる。そのため車両１の乗員は不整合の発生をＨＭＩ１２の表示により知ることができる。

[0085] （７）ゲートウェイ１０は車両１に搭載される。取得部１００００４、および算出判定部１００００２は、車両１のイグニッションスイッチがオンにされると動作を開始する。そのため、車両１の起動時に動作することで、車両１が走行を開始する前に、または車両１が低速で走行している間にソフトウェアの不整合を検出できる。

[0086] （変形例１）

各機能の構成情報の確認は、ゲートウェイ１０以外の装置が実現してもよい。たとえば車両１に接続可能な診断装置により実行してもよい。

[0087] 図１４は変形例１における機能構成情報管理システムＳａの構成を示す図である。図１４では、診断装置５が追加されている点が第１の実施の形態と異なる。本変形例では、サーバ２が送信する機能構成情報６１は診断装置５が受信する。診断装置５とゲートウェイ１０は、ＯＢＤ２などの汎用コネクタ６００を介して接続される。なお図１４では通信モジュール１１とサーバ２は接続されていないが、ＥＣＵのソフトウェアを更新する際には、第１の実施の形態と同様に通信モジュール１１はサーバ２と通信を行う。

[0088]（診断装置の構成）

図１５は、診断装置５の構成例を示すブロック図である。診断装置５は、ＣＰＵ５０１、主記憶部５０２、補助記憶部５０３、第１通信部５０４、第２通信部５０５、入力部５０６、および表示部５０７を備える。ＣＰＵ５０１は、補助記憶部５０３等に蓄積されたプログラムを主記憶部５０２上で実行し機能構成管理の制御を行う。補助記憶部５０３は、機能構成管理情報や車両に配信するＥＣＵソフトウェア更新用のデータを記憶する。

[0089] 第１通信部５０４は、インターネット３を介してサーバ２との間でデータの送受信を行う。第２通信部５０５は、車両１との間でデータの送受信を行う。入力部５０６は、診断装置５を操作するオペレータからの操作や入力情報を受け付ける。表示部５０７は、診断装置５を操作するオペレータに機能構成管理情報を表示する。

[0090]（動作）

本変形例では、オペレータが入力部５０６から動作指示を与えることで図１０に示した検証処理が開始される。本変形例ではゲートウェイ１０は、診断装置５の動作指令に基づき各ＥＣＵとの通信を仲介する。その他の動作は第１の実施の形態と同様である。

[0091]（変形例２）

上述した第１の実施の形態では、機能構成情報６１にＥＣＵ　ＩＤ６０３２およびソフトウェアバージョン６０３３も含まれた。しかしゲートウェイ１０は検証処理も含めて特にＥＣＵ　ＩＤ６０３２およびソフトウェアバージョン６０３３を必要としないので、機能構成情報６１にＥＣＵ　ＩＤ６０３２およびソフトウェアバージョン６０３３を含めなくてもよい。

[0092] 図１６は変形例１における機能構成情報６４の一例を示す図である。機能構成情報６４では組合せテーブル６０３がＮＥＴ　ＩＤ６０３１のみで構成される。本変形例においてもゲートウェイ１０の動作は第１の実施の形態と同様である。前述のように、第１の実施の形態においてゲートウェイ１０は、サーバ２から受信した機能構成情報６１に記載されたＥＣＵ　ＩＤ６０３

４および機能バージョン６０３５を参照する機会がなかった。そのため、機能構成情報６４からＥＣＵ　ＩＤ６０３４および機能バージョン６０３５が削除されても何ら影響がないためである。

[0093]（変形例３）

上述した第１の実施の形態では、機能構成情報６１にＮＥＴ　ＩＤ６０３１およびソフトウェアバージョン６０３３も含まれた。しかし機能構成情報６１にＮＥＴ　ＩＤ６０３１およびソフトウェアバージョン６０３３を含めなくてもよい。

[0094] 図１７は変形例３における機能構成情報６５の一例を示す図である。機能構成情報６５では組合せテーブル６０３がＥＣＵ　ＩＤ６０３２のみで構成される。本変形例ではゲートウェイ１０の図１０のＳ１０３～Ｓ１０５を次のように変更する。すなわちゲートウェイ１０は、接続されている全てのＥＣＵに対してＥＣＵ　ＩＤとソフトウェアのバージョンを問い合わせるメッセージを送信する。そして、機能構成情報６５に記載された機能ごとに、取得したＥＣＵ　ＩＤとソフトウェアのバージョンを用いて検証情報、すなわち図８のビット列Ｚを作成する。

[0095] 第１の実施の形態ではゲートウェイ１０は、機能ごとに機能を構成するＥＣＵを特定して問い合わせを行うためにＮＥＴ　ＩＤ６０３１を利用していた。しかし本変形例では機能構成情報６５にＮＥＴ　ＩＤ６０３１が含まれないので、接続されているＥＣＵの全てに問い合わせを行う。本変形例では、機能構成情報６５においてそれぞれの機能を構成するＥＣＵはＥＣＵ　ＩＤ６０３２により特定されるので、ゲートウェイ１０は問い合わせに対する回答として得られるＥＣＵ　ＩＤとバージョン情報を用いて、機能ごとにビット列Ｚを作成できる。

[0096]（変形例４）

上述した第１の実施の形態では、機能構成情報６１にフラグ６０５が含まれた。しかし機能構成情報６１にフラグ６０５を含めなくてもよい。この場合にはゲートウェイ１０は、図１０のＳ１１０において一律に動作を許可す

る、または一律に動作を許可しない構成とする。さらにこの場合に、動作を停止させる代わりに機能を制限してもよい。機能の制限とは、処理能力を低下させることや実現する機能の種類を減少させることである。

[0097] 本変形例によれば次の作用効果が得られる。

（８）停止制御部１００００５は、算出判定部１００００２により第１検証情報と第２検証情報とが整合しないと判断されると、整合しないと判定された第２検証情報に関する機能を停止、または機能を制限させる。そのため、ソフトウェアの不整合が検出された機能を一律に停止、または機能を制限させることができる。

[0098]（変形例５）

上述した第１の実施の形態では、公開鍵暗号方式を利用してサーバ２とゲートウェイ１０の間で情報の検証を行った。しかし検証の方式は特に限定されず既知の様々な手法に置き換えることや既知の手法を組み合わせることも本発明の範囲に含まれる。たとえば同じ公開鍵暗号方式であっても、サーバ２では秘密鍵ＳＫによる暗号化を行いゲートウェイ１０では公開鍵ＰＫによる複合化を行うことで検証を行ってもよい。また公開鍵暗号方式の代わりに対称暗号方式を利用してもよいし、メッセージ認証コードやソルトを利用してもよい。

[0099]（変形例６）

サーバ２からのゲートウェイ１０への応答に復旧可否フラグを含めてもよい。その場合はゲートウェイ１０の制御部１００００は、図１１のステップＳ２０９において、復旧可否フラグにより復旧させてもよい旨のフラグが設定されているＥＣＵに対してのみ機能の復旧を指示する。

[0100]（変形例７）

第１の実施の形態では特に説明しなかったが、ゲートウェイ１０は機能識別検証情報６０２もテーブル検証情報６０４と同様に検証を行ってもよい。この場合はゲートウェイ１０は、たとえば図１０のＳ１０８の直前に機能識別検証情報６０２の検証を行い、検証に成功するとＳ１１２に進み、検証に

失敗するとＳ１０８に進む。本変形例によれば、機能識別ＩＤ６０１を検証できる。

[0101]（変形例８）

サーバ２は、テーブル検証情報６０４の算出に機能識別ＩＤ６０１およびＮＥＴ　ＩＤ６０３１の少なくとも一方をさらに利用してもよい。この場合にはゲートウェイ１０も検証処理において同様の算出を行う。

[0102]（変形例９）

上述した第１の実施の形態では、ゲートウェイ１０は車両１のイグニッションスイッチがオンにされると検証処理を開始した。しかしゲートウェイ１０は、外部から動作指令を受けて検証処理を開始してもよい。たとえばゲートウェイ１０は、通信モジュール１１を介して車両１の外部から動作指令を受けてもよいし、車両１に搭載されるＥＣＵなどから動作指令を受けて動作を開始してもよい。

[0103]（変形例１０）

上述した第１の実施の形態では、機能構成情報６１はオペレータが入力した情報に基づきサーバ２により作成された。しかしあらかじめオペレータが機能構成情報６１を作成し、オペレータが機能構成情報６１そのものをサーバ２の補助記憶部２０３に格納してもよい。

[0104]－第２の実施の形態－

図１８～図１９を参照して、本発明に係る演算装置であるゲートウェイの第２の実施の形態を説明する。以下の説明では、第１の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第１の実施の形態と同じである。本実施の形態では、主に、機能毎にＥＣＵ内でソフトウェアのバージョンを管理する点で、第１の実施の形態と異なる。また本実施の形態では機能構成情報に格納される情報が第１の実施の形態と異なる。

[0105]　図１８は第２の実施の形態において各ＥＣＵに格納される機能別バージョン情報９５１の一例を示す図である。図１８ではエンジン制御ＥＣＵ１３を

具体例として使用し、図１８（ａ）はエンジン制御ＥＣＵ１３の更新前の機能別バージョン情報９５１ａを示し、図１８（ｂ）はエンジン制御ＥＣＵ１３の更新後の機能別バージョン情報９５１ｂを示す。エンジン制御ＥＣＵ１３は、機能Ａおよび機能Ｃの実現に寄与している。そのため、エンジン制御ＥＣＵ１３に保存される機能別バージョン情報９５１は、図１８（ａ）に示すようにソフトウェアバージョンである「１．０．０．０」と、機能Ａバージョンである「１」と、機能Ｃバージョンである「１」とから構成される。機能別バージョン情報９５０はソフトウェアの更新に伴い更新される。

[0106] 図１８（ｂ）に示す更新後の機能別バージョン情報９５１ｂでは、ソフトウェアバージョンが「１．０．１．０」に更新され、機能Ａバージョンが「２」に更新されている。しかし機能Ｃに関する更新は行われなかったので、機能Ｃバージョンは「１」から変更がない。

[0107] 図１９は、本実施の形態における機能構成情報６２の一例を示す図である。図１９（ａ）は更新前の機能構成情報６２ａを示す図、図１９（ｂ）は更新後の機能構成情報６２ｂを示す図である。図１９（ａ）に示す例ではＲ４１、Ｒ５１、およびＲ６１のレコードが含まれ、図１９（ｂ）に示す例ではＲ４２、Ｒ５２、およびＲ６２のレコードが含まれる。本実施の形態における機能構成情報６２と第１の実施の形態における機能構成情報６１とを比較すると、機能構成情報６１におけるソフトウェアバージョン６０３３のフィールドが削除され、その代わりにＤＩＤ６０３４と機能バージョン６０３５のフィールドが追加される。

[0108] ＤＩＤ６０３４には、ＥＣＵから機能毎のバージョンを読み出す際に用いる識別情報が格納される。ＤＩＤ６０３４はバージョン情報の読み出しのために設定された機能の識別情報である。ＤＩＤ６０３４は、図１９に示すように全ＥＣＵに共通して機能と１：１で対応してもよいし、ＥＣＵごとにＤＩＤと機能との対応を異ならせてもよい。たとえば図１９では、レコードＲ６１では３つのＥＣＵが共通するＤＩＤ６０３４である「Ｆ００３」により機能Ｃのバージョン情報が読み出されることが示されている。

[0109] 図１９（ａ）と図１９（ｂ）を比較すると、レコードＲ４１とレコードＲ４２は相違するが、レコードＲ５１およびレコードＲ６１は、レコードＲ５２およびレコードＲ６２と同一である。これは、ソフトウェアのバージョン情報そのものは機能構成情報６２に格納せず、各ソフトウェアの各機能のバージョン情報のみを機能構成情報６２に格納しているためである。

[0110] （その他の相違点）

本実施の形態では、それぞれのＥＣＵはゲートウェイ１０からＤＩＤ６０３４とともにソフトウェアのバージョン情報の問い合わせを受けると、次の動作を行う。すなわちＥＣＵは、ＦＲＯＭ１３１３に格納されている機能構成情報６２を参照して、受信したＤＩＤ６０３４に対応する機能のバージョン情報を返す。

[0111] ゲートウェイ１０は、図１０のＳ１０４において、機能構成情報６２に格納されているＮＥＴ　ＩＤのＥＣＵに対してＤＩＤ６０３４とともにバージョン情報の問い合わせを行う。たとえばゲートウェイ１０は、処理対象レコードＸ＝１の場合には、ＮＥＴ　ＩＤが「７００」のＥＣＵに対して「Ｆ００１」のＤＩＤ６０３４とともにバージョン情報の問い合わせを行う。

[0112] 本実施の形態では、サーバ２は、ＥＣＵ　ＩＤ６０３２、および機能バージョン６０３５を用いてビット列Ｘを作成し、そのデジタル署名であるテーブル検証情報６０４を作成する。ゲートウェイ１０はＥＣＵ　ＩＤ６０３２、および機能バージョン６０３５を用いてビット列Ｚを作成し、テーブル検証情報６０４を検証する。

[0113] 以上のように、機能毎にＥＣＵ内で関連するソフトウェア部分のバージョン情報を管理することによって、ソフトウェア更新時の機能構成情報への影響低減を図り、機能構成情報６２の変更箇所を減らすことができる。

[0114] （第２の実施の形態の変形例）

サーバ２は、ビット列Ｘの作成においてさらにＤＩＤ６０３４の値を用いてもよい。この場合にはゲートウェイ１０もビット列Ｚの作成においてＤＩＤ６０３４の値を用いる。

[0115] ―第３の実施の形態―

図２０～図２１を参照して、本発明に係る演算装置であるゲートウェイの第３の実施の形態を説明する。以下の説明では、第２の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第２の実施の形態と同じである。本実施の形態では、主に、機能構成情報に格納される情報が第２の実施の形態と異なる。

[0116] 図２０は本実施の形態において各ＥＣＵに格納される機能別バージョン情報９５２の一例を示す図である。図２０ではエンジン制御ＥＣＵ１３を具体例として使用し、図２０（ａ）はエンジン制御ＥＣＵ１３の更新前の機能別バージョン情報９５２ａを示し、図２０（ｂ）はエンジン制御ＥＣＵ１３の更新後の機能別バージョン情報９５２ｂを示す。

[0117] 機能別バージョン情報９５２は６バイトで構成され、先頭から、ブートローダ、ＢＳＷ、ＡＳＷ、キャリブレーションデータ、機能Ａ、機能Ｃのそれぞれのソフトウェアのバージョンを一意に識別する情報を示す。機能別バージョン情報９５２の各桁の値は、それぞれ対象とする部分のソフトウェアの更新にともない更新される。なお図２０では説明のために各桁に対応する情報を記載しているが、実際には機能別バージョン情報９５２には６バイトの値のみから構成される。

[0118] 図２０（ａ）に示す更新前の機能別バージョン情報９５２ａは、「１，１，１，１，１，１」である。図２０（ｂ）に示す更新後の機能別バージョン情報９５２ｂは、機能Ａに関連する部分が更新されているため、機能Ａに該当する識別情報が「２」に更新され、機能Ａを含むアプリケーション全体のソフトウェアを示すＡＳＷの識別情報が「２」に更新されている。

[0119] 図２１は、本実施の形態における機能構成情報６３の一例を示す図である。図２１（ａ）は更新前の機能構成情報６３ａを示す図、図２１（ｂ）は更新後の機能構成情報６３ｂを示す図である。図２１（ａ）に示す例ではＲ７１、Ｒ８１、およびＲ９１のレコードが含まれ、図２１（ｂ）に示す例ではＲ７２、Ｒ８２、およびＲ９２のレコードが含まれる。本実施の形態におけ

る機能構成情報６３と第２の実施の形態における機能構成情報６２とを比較すると、機能構成情報６２におけるＤＩＤ６０３４の代わりにマスク６０３６のフィールドが追加されている。

[0120] マスク６０３６は、当該機能の識別情報が機能別バージョン情報９５２の先頭から何バイト目に相当するかを示す識別情報である。ゲートウェイ１０は、機能別バージョン情報９５２をＥＣＵから読み出したのちにマスク６０３６を利用することで、読み出した機能別バージョン情報９５２から、当該機能に関する識別情報を特定する。ただしゲートウェイ１０がＥＣＵに対してソフトウェアの機能別バージョン情報９５２の要求とともにマスク６０３６の値を送信し、ＥＣＵが機能別バージョン情報９５２のうちマスク６０３６に該当するビットの値だけを返してもよい。

[0121] 図２１（ａ）と図２１（ｂ）とを比較すると、レコードＲ１とレコードＲ７２は相違するが、レコードＲ８１およびレコードＲ９１は、レコードＲ８２およびレコードＲ９２と同一である。これは、ソフトウェアのバージョン情報そのものは機能構成情報６３に格納せず、各ソフトウェアの各機能のバージョン情報のみを機能構成情報６３に格納しているためである。

[0122] その他の点は第２の実施の形態と同様なので説明を省略する。

[0123] 以上のように、機能毎にＥＣＵ内で関連するソフトウェア部分のバージョンを管理することによって、ソフトウェア更新時の機能構成情報への影響低減を図り、不要な変更を減らすことができる。

[0124] ―第４の実施の形態―

図２２～図２４を参照して、本発明に係る演算装置であるゲートウェイの第３の実施の形態を説明する。以下の説明では、第２の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第２の実施の形態と同じである。本実施の形態では、主に、テーブル検証情報が不一致の場合の振る舞いが第１の実施の形態と異なる。

[0125] 図２２は機能Ｄの機能構成情報６１ｃを示す図、図２３は機能Ｄの機能制限情報９１を示す図である。

[0126] 図２２のレコードＲ４は、機能識別ＩＤが”Ｄ２”で示される機能Ｄに関連する情報が格納されたレコードである。レコードＲ４の機能識別検証情報６０２のフィールドには「ｄｚｚｚ」が格納される。機能Ｄを構成するＥＣＵは３つであるため、ＮＥＴ　ＩＤ６０３１のフィールドには「７０１」「７０２」「７０３」がそれぞれ格納され、ＥＣＵ　ＩＤ６０３２のフィールドには「ブレーキ」「ＡＤＡＳ」「カメラ」がそれぞれ格納され、ソフトウェアバージョン６０３３のフィールドには「１．０．０．０」「１．０．０．１」「１．０．０．０」がそれぞれ格納される。レコードＲ４のテーブル検証情報６０４のフィールドには「ｔｄｄｄ」が格納され、フラグ６０５のフィールドには、不整合が発生した場合は当該機能の動作制限が必要であることを示す「制限」が格納されている。ここで、当該機能の動作制限とは、機能を停止するのではなく、機能の一部を継続して動作させることをいう。すなわち本実施の形態では、フラグ６０５のフィールドには、「停止」および「制限」のいずれかが格納され、「動作許可」という値が格納されることはない。

[0127] 図２３は、フラグ６０５のフィールドが「制限」の場合に参照する機能制限情報９１の一例を示す図であり、機能構成情報６１ｃと同様に管理される。図２３のレコードＲ４１は、機能Ｄに関連する機能制限情報が格納されたレコードである。レコードＲ４１の機能６００のフィールドには「Ｄ」が格納され、機能Ｄを構成するＥＣＵは３つであるため、バージョン不一致ＥＣＵ　ＩＤ６０３８のフィールドには「ブレーキ」「ＡＤＡＳ」「カメラ」がそれぞれ格納され、制限内容６０３７のフィールドには「警告のみ動作」「機能全停止」「機能全停止」が格納される。

[0128] 図２３に例示した内容について、機能Ｄが自動ブレーキ機能の場合を例に以下説明する。機能Ｄの自動ブレーキ機能は、「ブレーキ」「ＡＤＡＳ」「カメラ」のＩＤを有する３つのＥＣＵが連携して機能が実現される。また、自動ブレーキ機能は、ブレーキをかけるべき障害物の検知と障害物が接近した場合のドライバへの警告、ブレーキと３つの基本機能から構成される。本

機能構成において、「ブレーキ」ＥＣＵのバージョンが不一致の場合は、カメラやＡＤＡＳ　ＥＣＵは正常に動作できるため、基本機能のうち障害物の検知とドライバへの警告は問題なく実現でき、これらの機能は動作させることが好ましい。一方で、「カメラ」や「ＡＤＡＳ」ＥＣＵのバージョンが不一致の場合は、障害物の検知や警告にも問題がある可能性があるため、自動ブレーキ機能の全停止が好ましい。以上により、テーブル検証情報６０４が不一致の場合でも有用な機能を動作させることが可能になる。

[0129] 図２４は、ゲートウェイ１０における機能制限処理を示すフローチャートである。本処理は、図１０の処理Ｓ１１１を置き換えることで実現する。まず停止制御部１０００５は、フラグが「停止」であるか否かを判定し、「停止」の場合（Ｓ１２１のＹＥＳ）は関連ＥＣＵに停止を指示する（Ｓ１１１）。フラグが「停止」でない、すなわち「機能制限」の場合（Ｓ１２１のＮＯ）は、機能制限情報９１の機能Ｄのレコード Ｒ４１を読み出す（Ｓ１２２）。

[0130] 次にゲートウェイ１０はＥＣＵごとに、ＥＣＵから取得したバージョンと機能構成情報６１ｃのバージョンを比較し、相違を確認する（Ｓ１２３）。ゲートウェイ１０は、バージョンが一致すると判断する場合は、何もしない（Ｓ１２４のＹＥＳ）。ゲートウェイ１０は、バージョンが不一致と判断する場合（Ｓ１２４のＮＯ）は、機能制限情報９１の制限内容６０３７に規定された内容に従って、機能の一部を制限する（Ｓ１２５）。次に、ゲートウェイ１０バージョンを比較していないＥＣＵが存在するか否かを判断し（Ｓ１２６）、すべてのバージョンの比較が完了している場合は処理を終了する（Ｓ１２６のＮＯ）。ゲートウェイ１０は、バージョン未比較のＥＣＵがあると判断する場合（Ｓ１２６のＮＯ）は、Ｓ１２３に戻って処理を繰り返す。

[0131] 以上説明した第４の実施の形態では、次の作用効果が得られる。

（９）停止制御部１０００５は、算出判定部１０００２により第１検証情報と第２検証情報とが整合しないと判断されると、整合しないと判定された第

２検証情報に関する機能であって、フラグが不整合時に実行を許可することを示すフラグを有する機能について、機能制限情報９１を参照して、バージョン情報が一致しない第２識別情報に基づき機能を制限するか否かを決定する。そのため、テーブル検証情報が不一致の場合でも有用な機能を動作させることが可能になる。

[0132] なお、本発明は上記した実施例に限定されるものではなく、様々な変形例が含まれる。たとえば、上記した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施例の構成の一部を他の実施例の構成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることや各処理における処理の順番を入れ替えることも可能である。たとえば、本実施の形態１では機能構成情報管理装置はゲートウェイ１０であるとしたが、通信モジュール１１やＨＭＩ１２が機能構成情報管理装置であってもよい。また、専用の装置を設けてもよい。

[0133] 上述した各実施の形態および変形例において、機能ブロックの構成は一例に過ぎない。別々の機能ブロックとして示したいくつかの機能構成を一体に構成してもよいし、１つの機能ブロック図で表した構成を２以上の機能に分割してもよい。また各機能ブロックが有する機能の一部を他の機能ブロックが備える構成としてもよい。

[0134] 上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、たとえば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するソフトウェアを解釈し、実行することによりソフトウェアで実現してもよい。

[0135] また、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。実際には殆ど全ての構成が相互に接続されていると考えてもよい。

[0136] 上記では、種々の実施の形態および変形例を説明したが、本発明はこれらの内容に限定されるものではない。本発明の技術的思想の範囲内で考えられるその他の態様も本発明の範囲内に含まれる。

[0137] 次の優先権基礎出願の開示内容は引用文としてここに組み込まれる。

日本国特許出願２０１９－６６８８７（２０１９年３月２９日出願）

符号の説明

[0138] １…車両

５…診断装置

６…機能構成情報

１０…ゲートウェイ

６１、６２、６３、６４、６５…機能構成情報

６０４…テーブル検証情報

６０５…フラグ

６０３１…ＮＥＴ　ＩＤ

６０３２…ＥＣＵ　ＩＤ

１０００２…算出判定部

１０００５…停止制御部

請求の範囲

[請求項1] 複数の電子制御装置と接続される演算装置であって、

前記複数の電子制御装置は、１以上の前記電子制御装置によりそれぞれの機能を構成し、

前記機能ごとに、前記機能を構成する１以上の前記電子制御装置の第１識別情報および第１検証情報を含む機能構成情報を受信する外部通信部と、

前記複数の電子制御装置のそれぞれから、前記電子制御装置に搭載されたソフトウェアのバージョン情報および前記電子制御装置の第２識別情報を取得する取得部と、

前記機能ごとに、前記機能を構成するすべての前記電子制御装置のバージョン情報であって前記取得部が取得したバージョン情報および前記機能を構成するすべての前記電子制御装置の前記第２識別情報を用いて第２検証情報を算出する算出部と、

前記機能ごとに、前記第１検証情報および前記第２検証情報の整合を判定する判定部とを備える演算装置。

[請求項2] 請求項１に記載の演算装置において、

前記第１識別情報とは、前記電子制御装置のネットワーク上の識別子であり、

前記第２識別情報とは、前記電子制御装置の種類を示す識別子である演算装置。

[請求項3] 請求項１に記載の演算装置において、

前記第１識別情報および前記第２識別情報は、前記電子制御装置の種類を示す識別子である演算装置。

[請求項4] 請求項１に記載の演算装置において、

前記判定部により前記第１検証情報と前記第２検証情報とが整合しないと判断されると、整合しないと判定された前記第２検証情報に関する前記機能を停止または制限させる停止制御部をさらに備える演算

装置。

[請求項5] 請求項１に記載の演算装置において、

前記機能構成情報には、前記機能ごとに不整合時の実行を許可または拒否を示すフラグが含まれ、

前記判定部により前記第１検証情報と前記第２検証情報とが整合しないと判断されると、整合しないと判定された前記第２検証情報に関する前記機能であって、前記機能構成情報における前記フラグが不整合時に実行を拒否することを示すフラグを有する機能を停止させる停止制御部をさらに備える演算装置。

[請求項6] 請求項５に記載の演算装置において、

前記停止制御部は、前記判定部により前記第１検証情報と前記第２検証情報とが整合しないと判断されると、整合しないと判定された前記第２検証情報に関する前記機能であって、前記フラグが不整合時に実行を許可することを示すフラグを有する機能について、前記バージョン情報が一致しない前記第２識別情報に基づき前記機能を制限するか否かを決定する演算装置。

[請求項7] 請求項１に記載の演算装置において、

前記判定部により前記第１検証情報と前記第２検証情報とが整合しないと判断されると、前記外部通信部から受ける指令に基づき、前記機能構成情報および前記電子制御装置のソフトウェアの少なくとも一方を更新する更新制御部をさらに備える演算装置。

[請求項8] 請求項１に記載の演算装置において、

前記判定部により前記第１検証情報と前記第２検証情報とが整合しないと判断されると、不整合が生じたことを記憶部に記録する制御部をさらに備える演算装置。

[請求項9] 請求項１に記載の演算装置において、

前記判定部により前記第１検証情報と前記第２検証情報とが整合しないと判断されると、不整合が生じたことを表示部に表示させる制御

部をさらに備える演算装置。

[請求項10] 請求項１に記載の演算装置において、

前記演算装置は車両に搭載され、

前記取得部、前記算出部、および前記判定部は、前記車両のイグニッションスイッチがオンにされると動作を開始する演算装置。

[請求項11] 請求項１に記載の演算装置において、

前記取得部、前記算出部、および前記判定部は、外部から動作指令を受けると動作を開始する演算装置。

[請求項12] 複数の電子制御装置と接続される演算装置が実行する判定方法であって、

前記複数の電子制御装置は、１以上の前記電子制御装置によりそれぞれの機能を構成し、

前記機能ごとに、前記機能を構成する１以上の前記電子制御装置の第１識別情報および第１検証情報を受信することと、

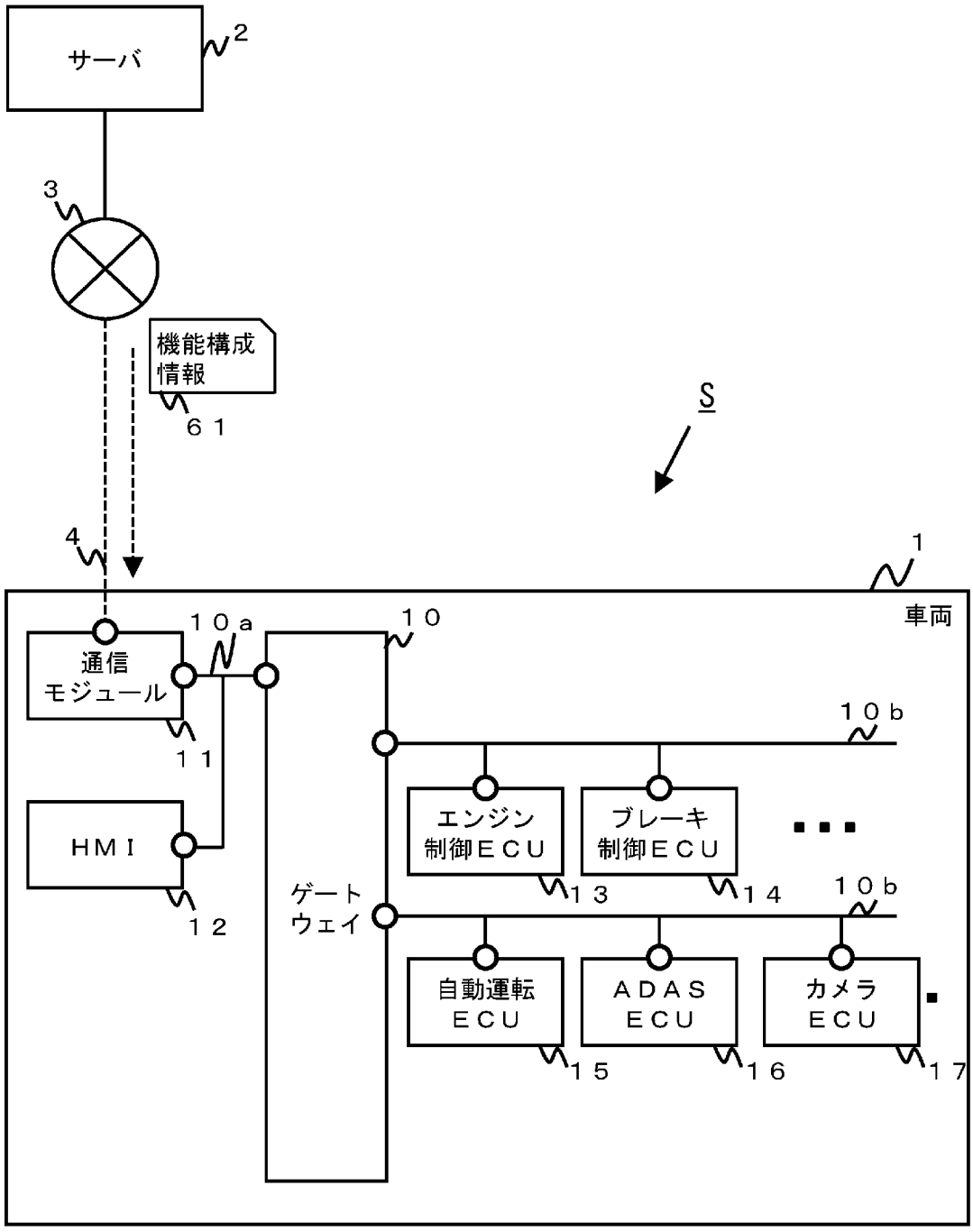
前記複数の電子制御装置のそれぞれから、前記電子制御装置に搭載されたソフトウェアのバージョン情報および前記電子制御装置の第２識別情報を取得することと、

前記機能ごとに、前記機能を構成するすべての前記電子制御装置のバージョン情報であって取得したバージョン情報および前記機能を構成するすべての前記電子制御装置の前記第２識別情報を用いて第２検証情報を作成することと、

前記機能ごとに、前記第１検証情報および前記第２検証情報の整合を判定することとを含む判定方法。

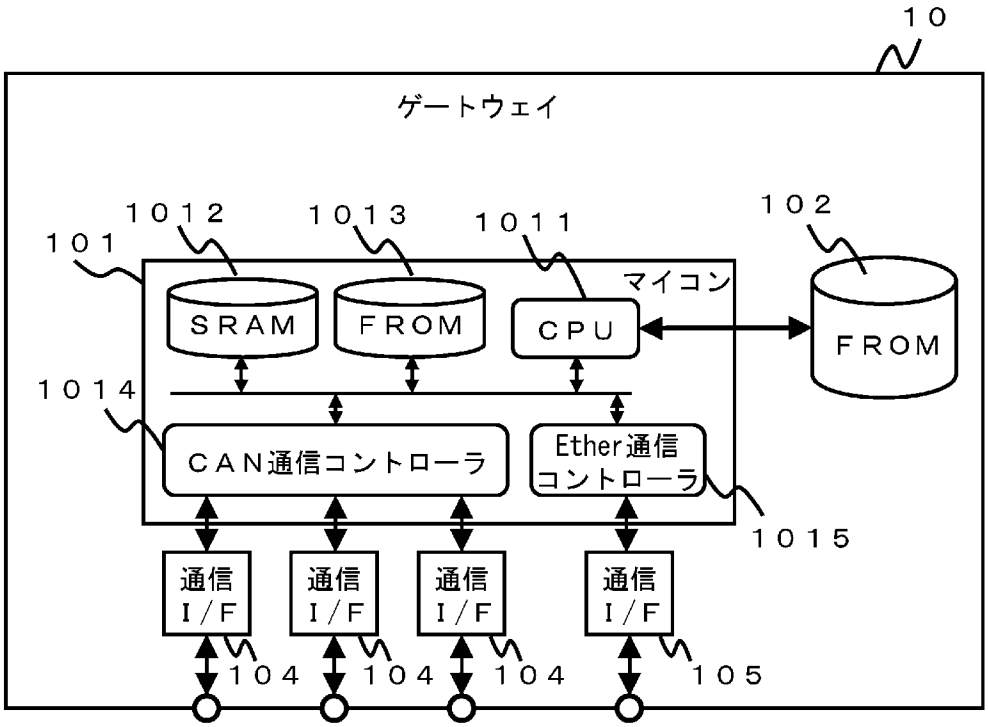
[図1]

図１


サーバ
2
3
機能構成
情報
６１
S
4
1
車両
１０a
１０
通信
モジュール
１１
１０b
エンジン
制御ＥＣＵ
１３
ブレーキ
制御ＥＣＵ
１４
HMI
１２
ゲート
ウェイ
１０b
自動運転
ＥＣＵ
１５
ＡＤＡＳ
ＥＣＵ
１６
カメラ
ＥＣＵ
１７

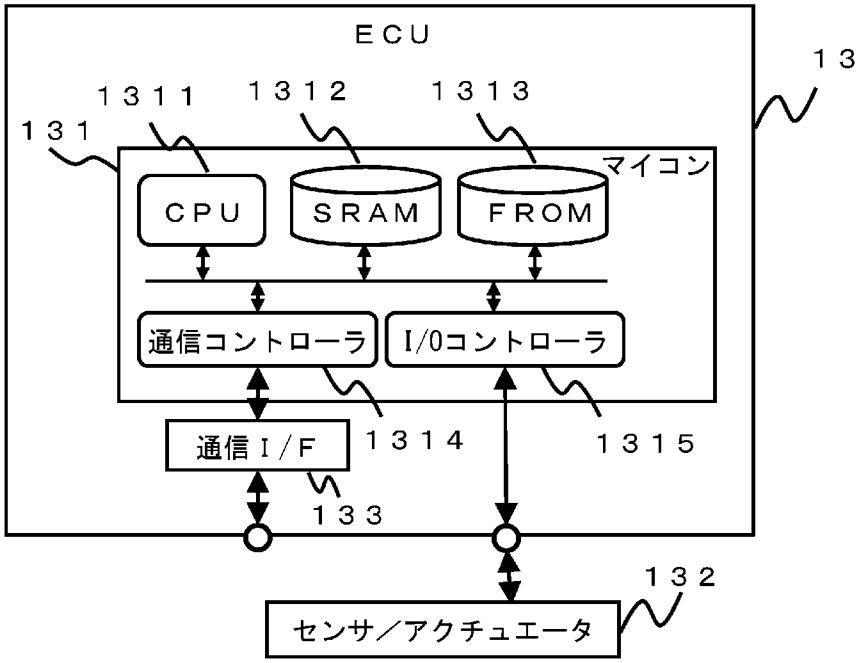
[図2]

図２


１０
ゲートウェイ
１０１
１０１２
１０１３
１０１１
１０２
マイコン
SRAM
FROM
CPU
FROM
１０１４
CAN通信コントローラ
Ether通信
コントローラ
１０１５
通信
I/F
通信
I/F
通信
I/F
通信
I/F
１０４
１０４
１０４
１０５

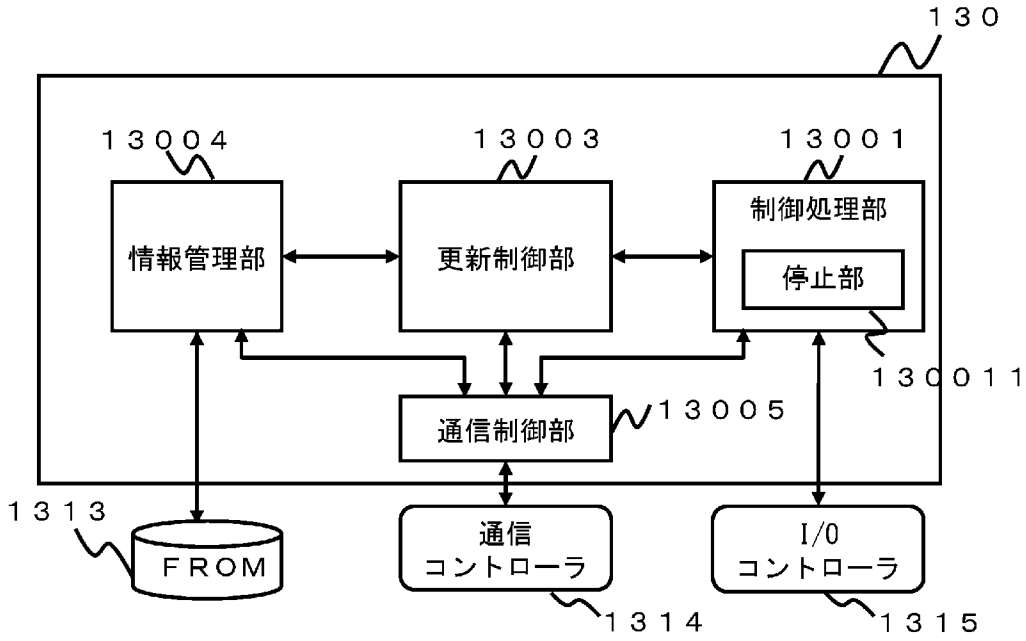
[図3]

図３


ＥＣＵ
１３
１３１１
１３１２
１３１３
１３１
マイコン
ＣＰＵ
ＳＲＡＭ
ＦＲＯＭ
通信コントローラ
Ｉ/Ｏコントローラ
通信Ｉ／Ｆ
１３１４
１３１５
１３３
１３２
センサ／アクチュエータ

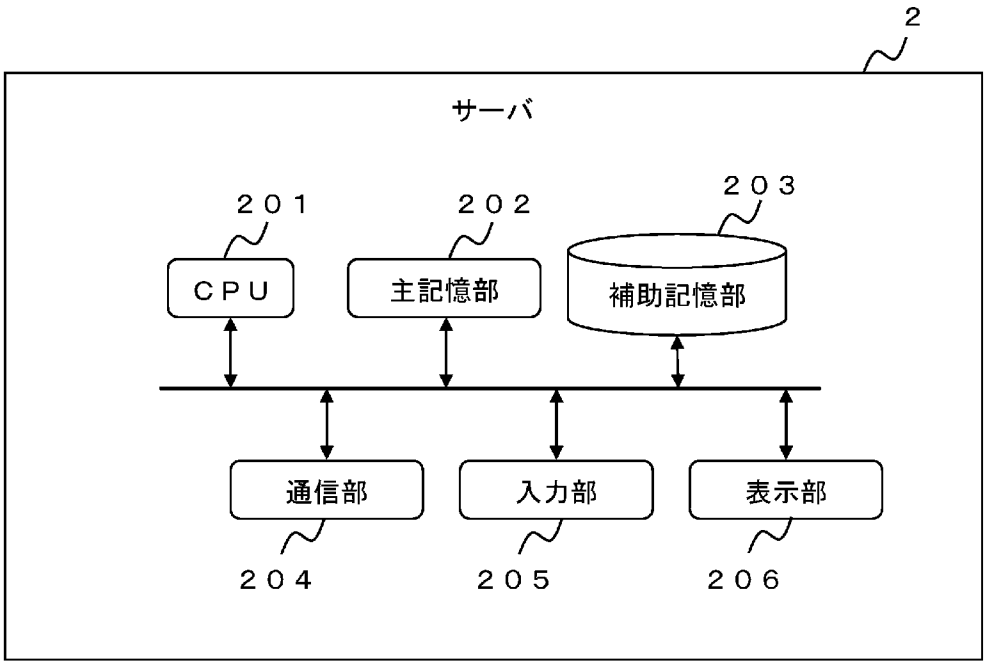
[図4]

図４


１３０
１３００４
１３００３
１３００１
情報管理部
更新制御部
制御処理部
停止部
１３００１１
１３００５
通信制御部
１３１３
ＦＲＯＭ
通信
コントローラ
１３１４
I/O
コントローラ
１３１５

[図5]

図５



[図6]

図６

６１ａ

６０１ 機能識別ID	６０２ 機能識別検証情報	６０３ 組み合わせテーブル ６０３１ NET ID	６０３２ ECU ID	６０３３ ソフトウェアバージョン	６０４ テーブル検証情報	６０５ フラグ	
A1	aaa	700	エンジン	1.0.0.0	taaa	動作許可	R１１
B1	bbb	701	ブレーキ	1.0.0.0	tbbb	停止	R２１
C1	ccc	700	エンジン	1.0.0.0	tccc	停止	R３１
		701	ブレーキ	1.0.0.0			
		702	ADAS	1.0.0.1			

（ａ）

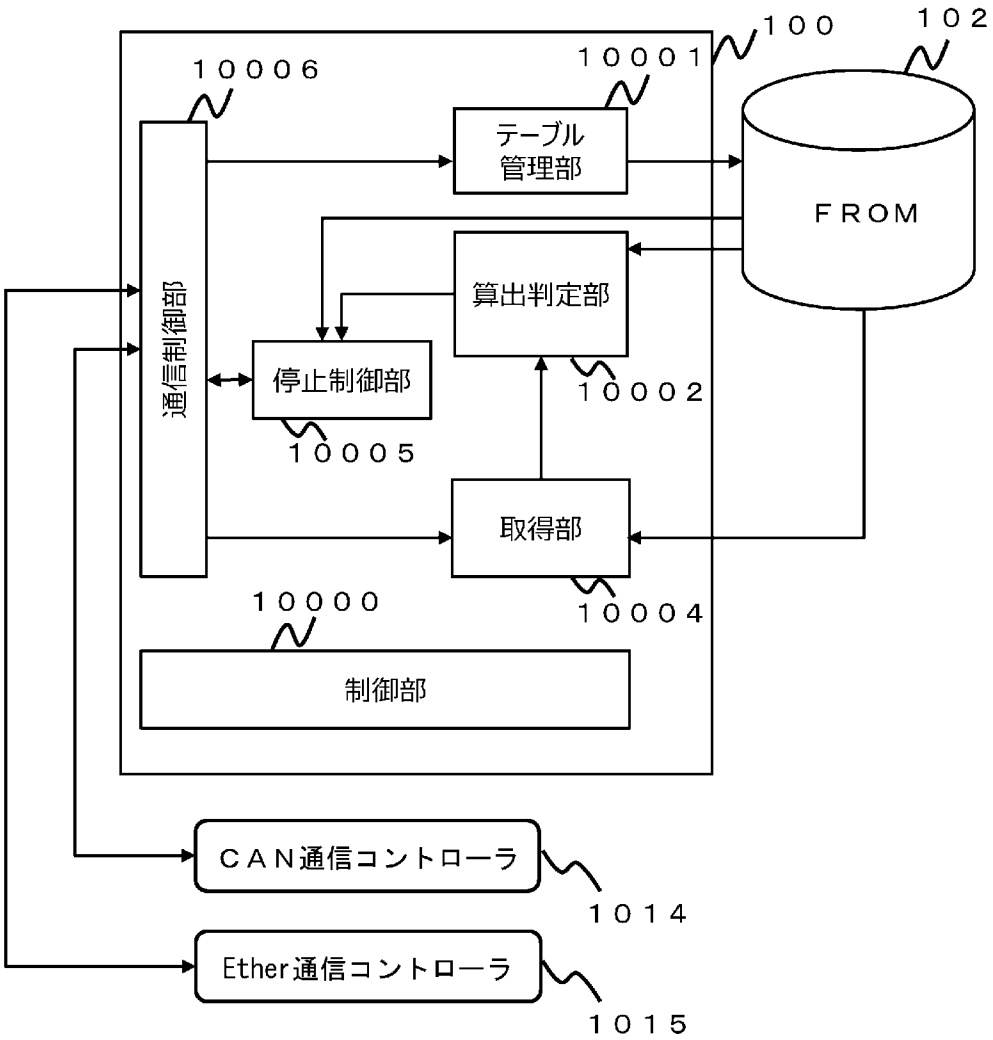
６１ｂ

６０１ 機能識別ID	６０２ 機能識別検証情報	６０３ 組み合わせテーブル ６０３１ NET ID	６０３２ ECU ID	６０３３ ソフトウェアバージョン	６０４ テーブル検証情報	６０５ フラグ	
A2	azzz	700	エンジン	1.0.0.1	taab	動作許可	R１２
B1	bbb	701	ブレーキ	1.0.0.0	tbbb	停止	R２２
C2	czzz	700	エンジン	1.0.0.1	tccd	停止	R３２
		701	ブレーキ	1.0.0.0			
		702	ADAS	1.0.0.1			

（ｂ）

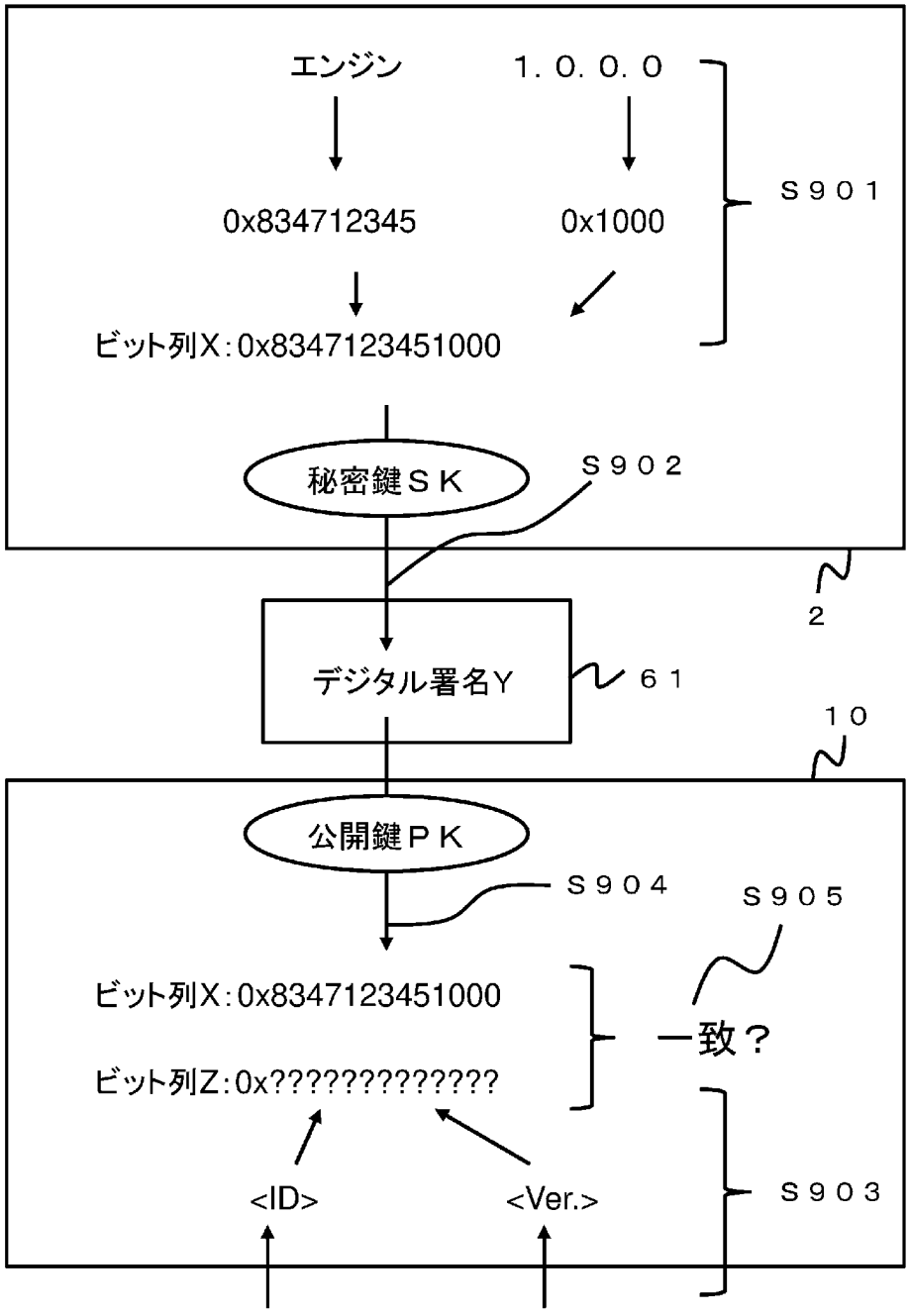
[図7]

図７


１００
１０２
１０００６
１０００１
テーブル
管理部
ＦＲＯＭ
通信制御部
算出判定部
停止制御部
１０００２
１０００５
取得部
１０００４
１０００
制御部
ＣＡＮ通信コントローラ
１０１４
Ether通信コントローラ
１０１５

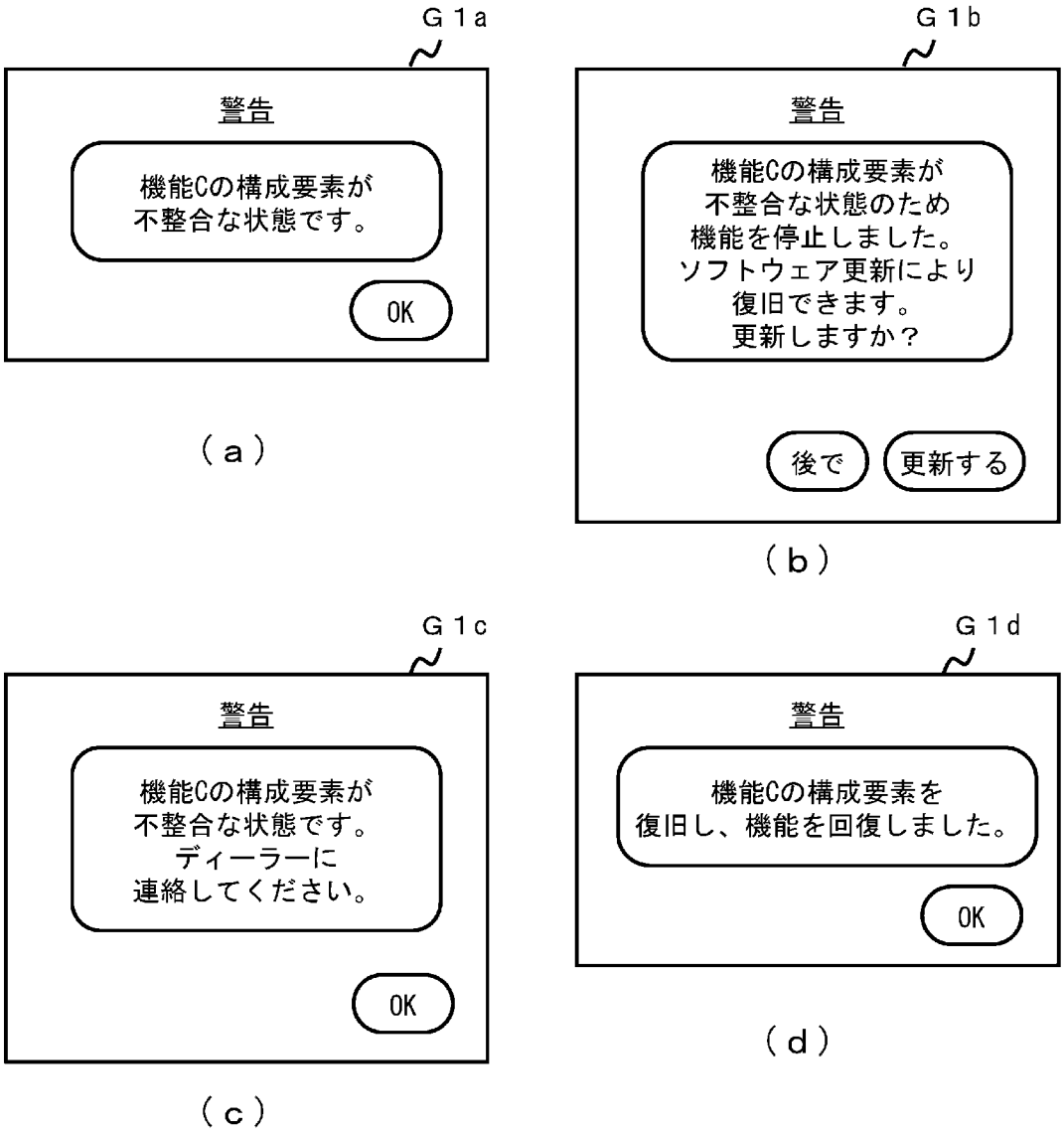
[図8]

図８


エンジン
1．0．0．0
0x834712345
0x1000
ビット列X：0x8347123451000
Ｓ９０１
秘密鍵ＳＫ
Ｓ９０２
2
デジタル署名Y
６１
１０
公開鍵ＰＫ
Ｓ９０４
Ｓ９０５
ビット列X：0x8347123451000
ビット列Z：0x????????????
一致？
<ID>
<Ver.>
Ｓ９０３

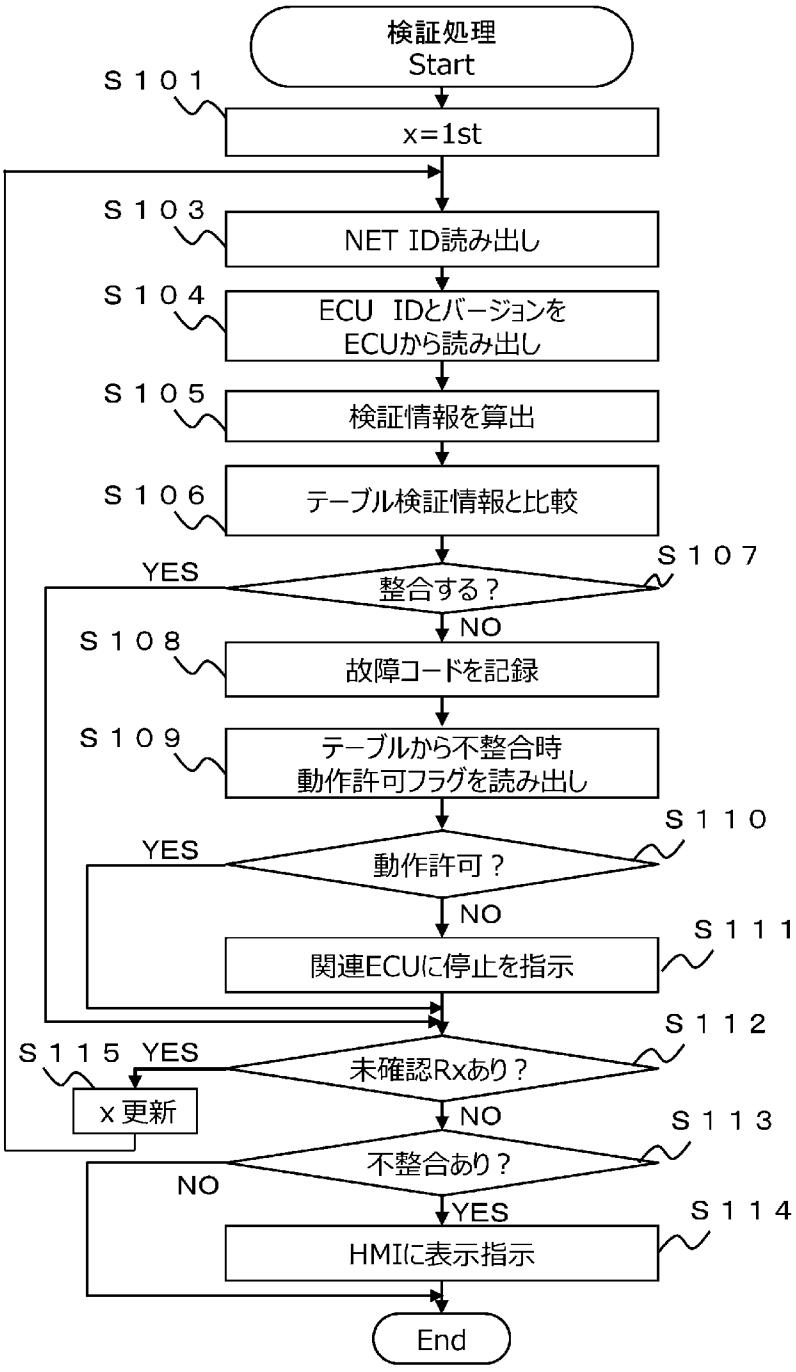
[図9]

図９


Ｇ１a
警告
機能Cの構成要素が
不整合な状態です。
OK
（ａ）
Ｇ１b
警告
機能Cの構成要素が
不整合な状態のため
機能を停止しました。
ソフトウェア更新により
復旧できます。
更新しますか？
後で
更新する
（ｂ）
Ｇ１c
警告
機能Cの構成要素が
不整合な状態です。
ディーラーに
連絡してください。
OK
（ｃ）
Ｇ１d
警告
機能Cの構成要素を
復旧し、機能を回復しました。
OK
（ｄ）

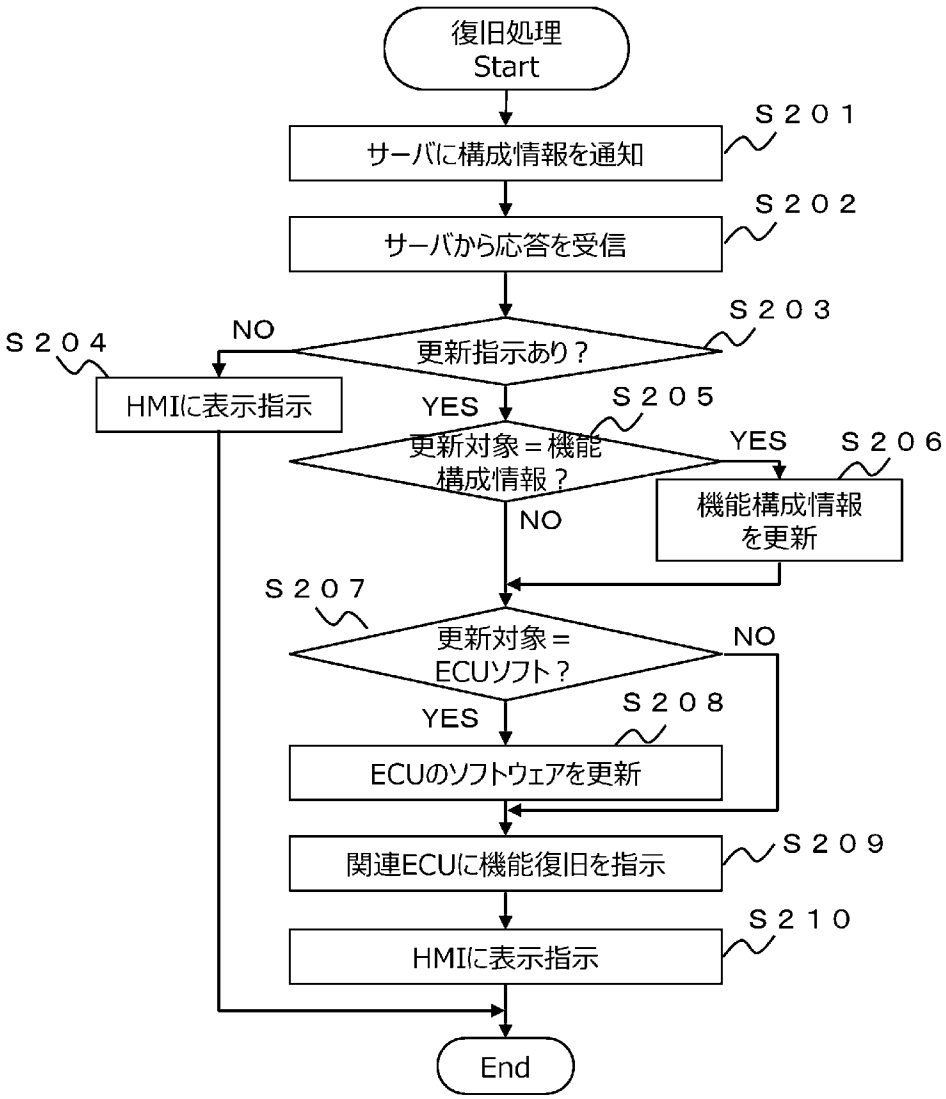
[図10]

図１０


検証処理
Start
S１０１
x=1st
S１０３
NET ID読み出し
S１０４
ECU IDとバージョンを
ECUから読み出し
S１０５
検証情報を算出
S１０６
テーブル検証情報と比較
S１０７
整合する？
YES
NO
S１０８
故障コードを記録
S１０９
テーブルから不整合時
動作許可フラグを読み出し
S１１０
動作許可？
YES
NO
S１１１
関連ECUに停止を指示
S１１２
未確認Rxあり？
S１１５ YES
NO
x 更新
S１１３
不整合あり？
NO
YES
S１１４
HMIに表示指示
End

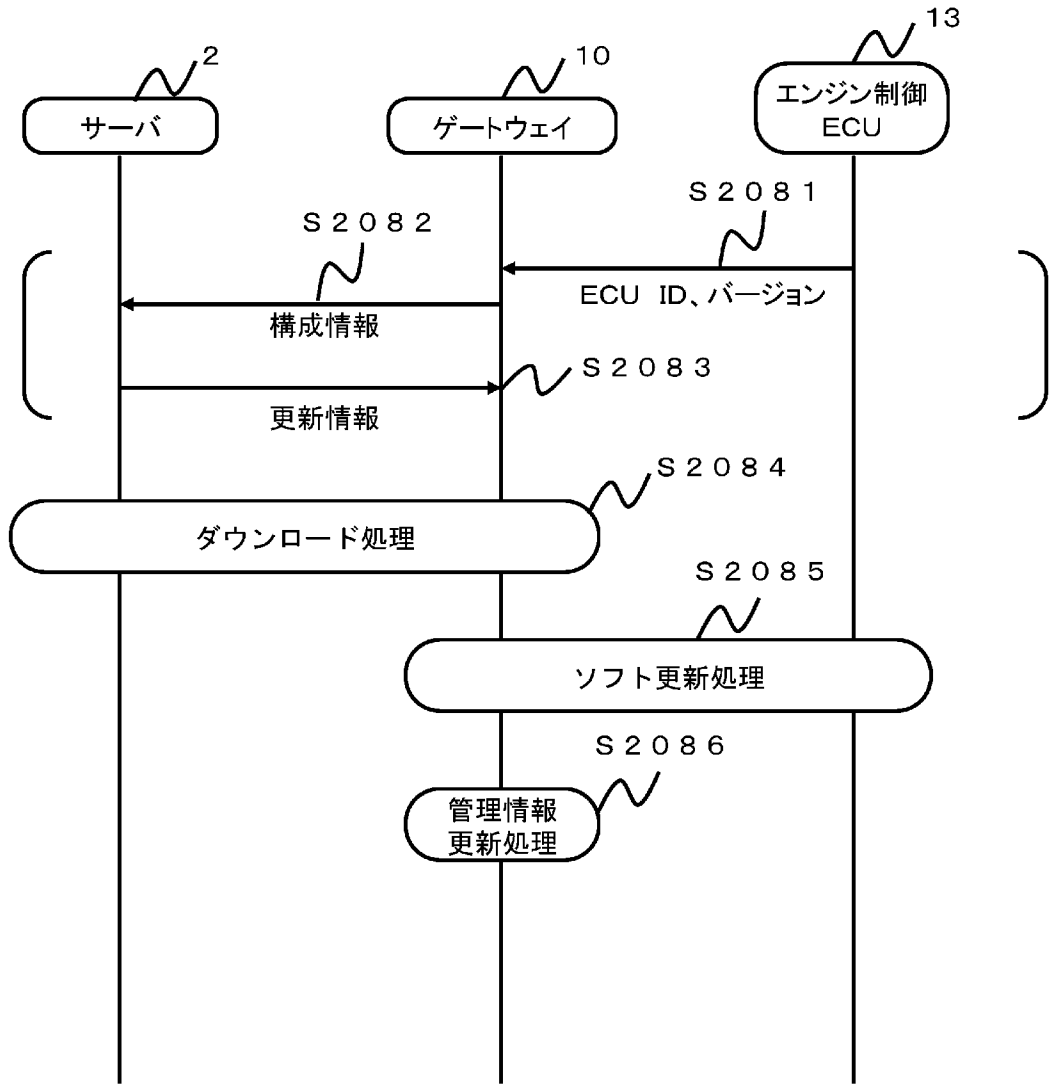
[図11]

図１１


復旧処理
Start
サーバに構成情報を通知
Ｓ２０１
サーバから応答を受信
Ｓ２０２
更新指示あり？
Ｓ２０３
NO
Ｓ２０４
HMIに表示指示
YES
更新対象＝機能
構成情報？
Ｓ２０５
YES
Ｓ２０６
機能構成情報
を更新
NO
Ｓ２０７
更新対象＝
ECUソフト？
NO
YES
Ｓ２０８
ECUのソフトウェアを更新
関連ECUに機能復旧を指示
Ｓ２０９
HMIに表示指示
Ｓ２１０
End

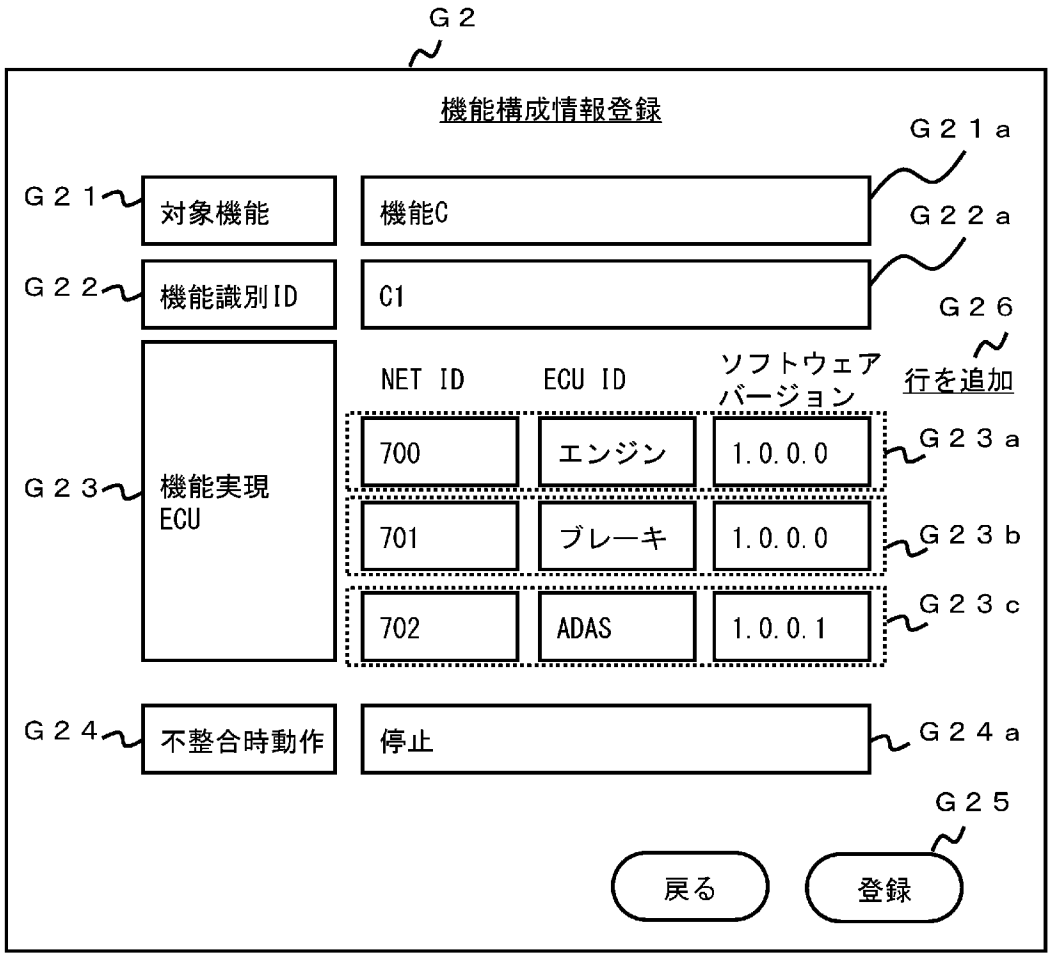
[図12]

図１２


2
サーバ
10
ゲートウェイ
13
エンジン制御
ECU
Ｓ２０８１
ECU ID、バージョン
Ｓ２０８２
構成情報
Ｓ２０８３
更新情報
Ｓ２０８４
ダウンロード処理
Ｓ２０８５
ソフト更新処理
Ｓ２０８６
管理情報
更新処理

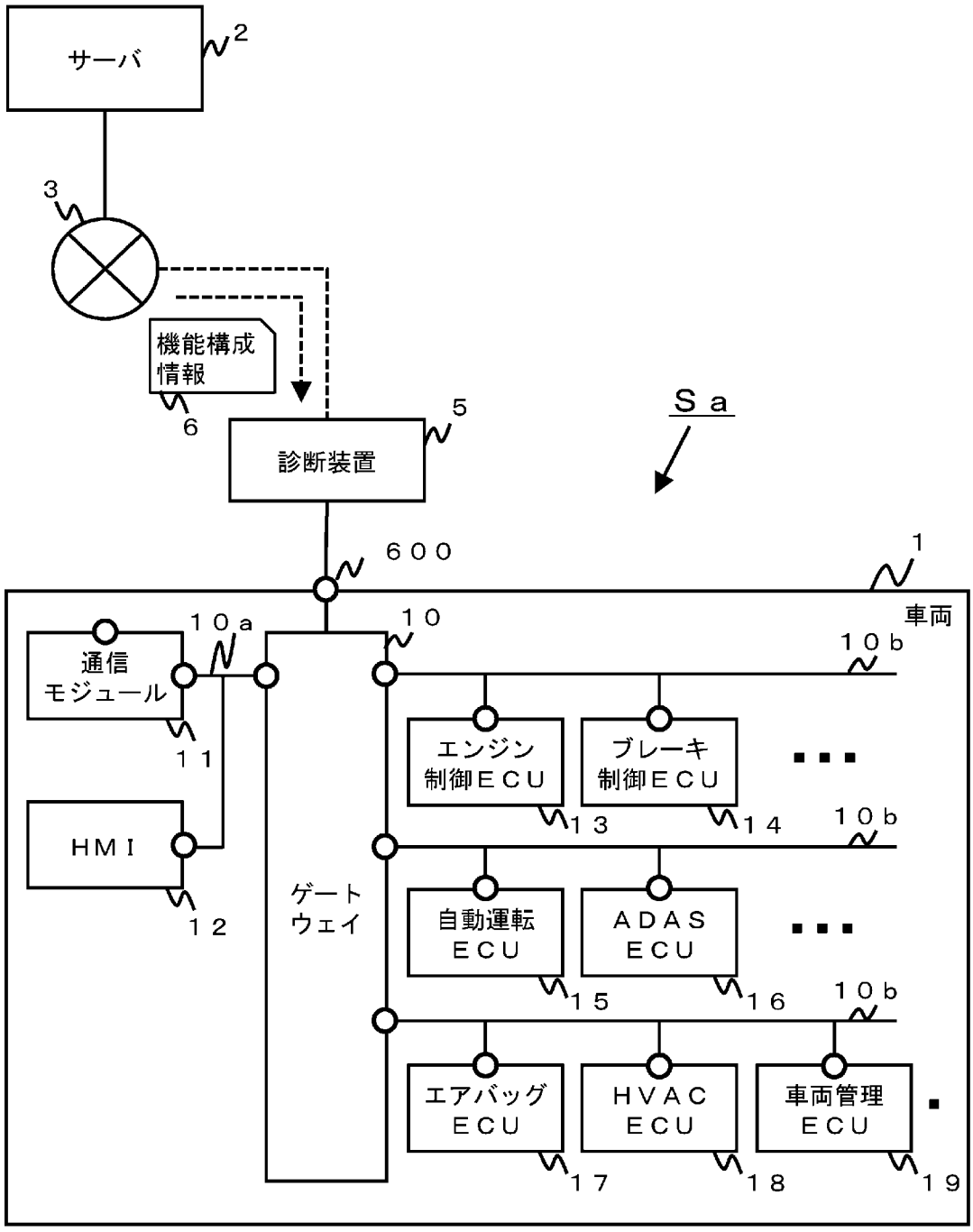
[図13]

図１３


Ｇ２
機能構成情報登録
Ｇ２１ａ
Ｇ２１
対象機能
機能C
Ｇ２２ａ
Ｇ２２
機能識別ID
C1
Ｇ２６
行を追加
NET ID
ECU ID
ソフトウェア
バージョン
Ｇ２３
機能実現
ECU
700
エンジン
1.0.0.0
Ｇ２３ａ
701
ブレーキ
1.0.0.0
Ｇ２３ｂ
702
ADAS
1.0.0.1
Ｇ２３ｃ
Ｇ２４
不整合時動作
停止
Ｇ２４ａ
Ｇ２５
戻る
登録

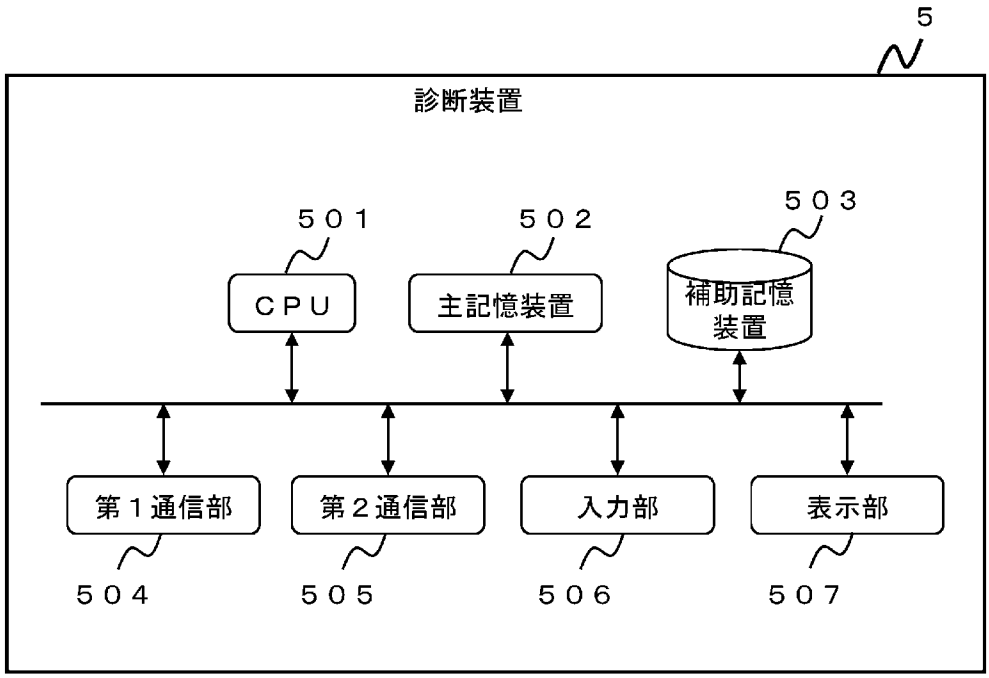
[図14]

図１４


サーバ
2
3
機能構成
情報
6
診断装置
5
Ｓａ
６００
1
車両
１０ａ
１０
１０ｂ
通信
モジュール
１１
エンジン
制御ＥＣＵ
１３
ブレーキ
制御ＥＣＵ
１４
ＨＭＩ
１２
ゲート
ウェイ
自動運転
ＥＣＵ
１５
ＡＤＡＳ
ＥＣＵ
１６
エアバッグ
ＥＣＵ
１７
ＨＶＡＣ
ＥＣＵ
１８
車両管理
ＥＣＵ
１９

[図15]

図１５


5
診断装置
５０１
５０２
５０３
ＣＰＵ
主記憶装置
補助記憶装置
第１通信部
第２通信部
入力部
表示部
５０４
５０５
５０６
５０７

[図16]

図１６

６４

６０１ 機能識別ID	６０２ 機能識別検証情報	６０３ 組み合わせテーブル ６０３１ NET ID	６０４ テーブル検証情報	６０５ フラグ
A1	aaa	700	taaa	動作許可
B1	bbb	701	tbbb	停止
C1	ccc	700	tccc	停止
		701		
		702		

[図17]

図１７

６５

６０１ 機能識別ID	６０２ 機能識別検証情報	６０３ 組み合わせテーブル ６０３２ ECU ID	６０４ テーブル検証情報	６０５ フラグ
A1	aaa	エンジン	taaa	動作許可
B1	bbb	ブレーキ	tbbb	停止
C1	ccc	エンジン	tccc	停止
		ブレーキ		
		ADAS		

[図18]

図１８

９５１ａ

ソフトウェアバージョン	1.0.0.0
機能Aバージョン	1
機能Cバージョン	1

（ａ）

９５１ｂ

ソフトウェアバージョン	1.0.1.0
機能Aバージョン	2
機能Cバージョン	1

（ｂ）

[図19]

図１９

６２ａ

機能識別ID	機能識別検証情報	組み合わせテーブル				テーブル検証情報	フラグ	
				６０３４	６０３５			
		NET ID	ECU ID	DID	機能バージョン			
A1	aaa	700	エンジン	F001	1	taaa	動作許可	R４１
B1	bbb	701	ブレーキ	F002	1	tbbb	停止	R５１
C1	ccc	700	エンジン	F003	1	tccc	停止	R６１
		701	ブレーキ	F003	1			
		702	ADAS	F003	1			

（ａ）

６２ｂ

機能識別ID	機能識別検証情報	組み合わせテーブル				テーブル検証情報	フラグ	
				６０３４	６０３５			
		NET ID	ECU ID	DID	機能バージョン			
A2	azzz	700	エンジン	F001	2	taaB	動作許可	R４２
B1	bbb	701	ブレーキ	F002	1	tbbb	停止	R５２
C1	ccc	700	エンジン	F003	1	tccC	停止	R６２
		701	ブレーキ	F003	1			
		702	ADAS	F003	1			

（ｂ）

[図20]

図２０

９５２ａ

ブートローダ	BSW	ASW	キャリブ	機能A	機能C
1.	1.	1.	1.	1.	1.

（ａ）

９５２ｂ

ブートローダ	BSW	ASW	キャリブ	機能A	機能C
1.	1.	2.	1.	2.	1.

（ｂ）

[図21]

図２１

６３ａ

機能識別ID	機能識別検証情報	組み合わせテーブル				テーブル検証情報	フラグ	
				６０３６	６０３５			
		NET ID	ECU ID	マスク	機能バージョン			
A1	aaa	700	エンジン	4	1	taaa	動作許可	R７１
B1	bbb	701	ブレーキ	4	1	tbbb	停止	R８１
C1	ccc	700	エンジン	5	1	tccc	停止	R９１
		701	ブレーキ	5	1			
		702	ADAS	4	1			

（ａ）

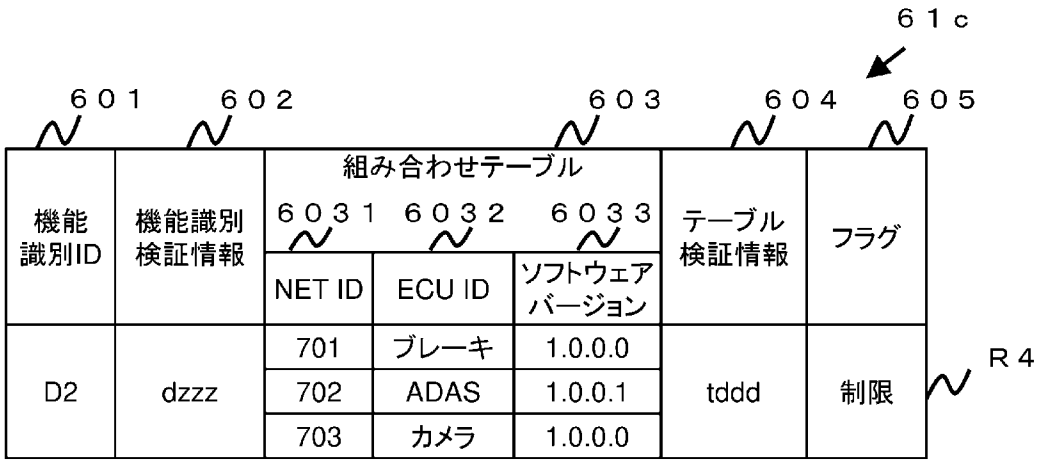
６３ｂ

機能識別ID	機能識別検証情報	組み合わせテーブル				テーブル検証情報	フラグ	
				６０３６	６０３５			
		NET ID	ECU ID	マスク	機能バージョン			
A2	aaa	700	エンジン	4	2	taab	動作許可	R７２
B1	bbb	701	ブレーキ	4	1	tbbb	停止	R８２
C1	ccc	700	エンジン	5	1	tccc	停止	R９２
		701	ブレーキ	5	1			
		702	ADAS	4	1			

（ｂ）

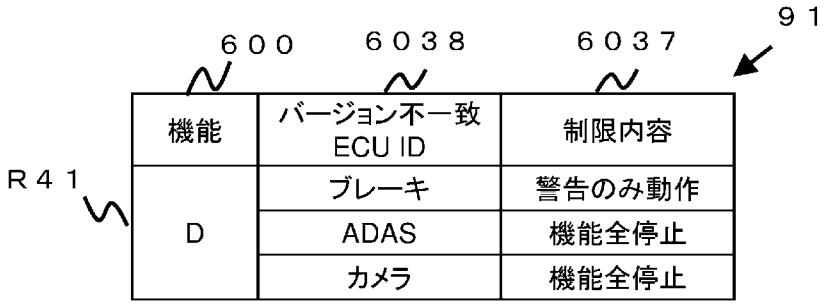
[図22]

図２２



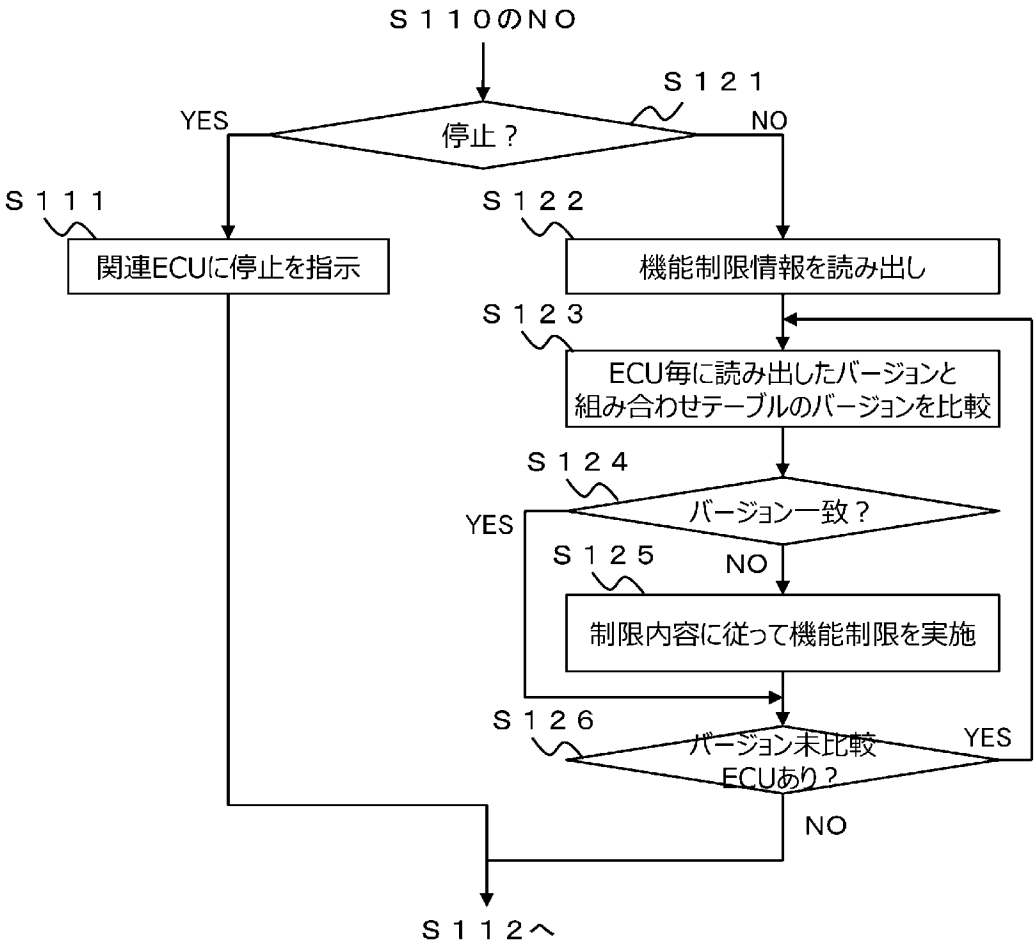
[図23]

図２３



[図24]

図２４


Ｓ１１０のＮＯ
Ｓ１２１
停止？
YES
NO
Ｓ１１１
関連ECUに停止を指示
Ｓ１２２
機能制限情報を読み出し
Ｓ１２３
ECU毎に読み出したバージョンと
組み合わせテーブルのバージョンを比較
Ｓ１２４
バージョン一致？
YES
Ｓ１２５
NO
制限内容に従って機能制限を実施
Ｓ１２６
バージョン未比較
ECUあり？
YES
NO
Ｓ１１２へ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/007013

A. CLASSIFICATION OF SUBJECT MATTER
G09C 1/00(2006.01)i; H04L 9/32(2006.01)i; B60R 16/02(2006.01)i; G06F 8/60(2018.01)i
FI: G06F8/60; B60R16/02 660U; G09C1/00 640E; H04L9/00 675B
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)
G09C1/00; H04L9/32; B60R16/02; G06F8/60

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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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 2016-188016 A (HONDA MOTOR CO., LTD.) 04.11.2016 (2016-11-04) claim 1, paragraphs [0021]-[0082], [0119], fig. 1-5	1-12
Y	WO 2015/011840 A1 (HITACHI, LTD.) 29.01.2015 (2015-01-29) paragraphs [0040], [0044], [0048], [0062]-[0063], fig. 6, 9-14	1-12
Y	WO 2016/147766 A1 (HITACHI AUTOMOTIVE SYSTEMS, LTD.) 22.09.2016 (2016-09-22) paragraphs [0091]-[0093]	2
Y	JP 2009-199497 A (PANASONIC CORP.) 03.09.2009 (2009-09-03) paragraphs [0038]-[0040]	4-6, 10
Y	JP 2018-124749 A (KYOCERA DOCUMENT SOLUTIONS INC.) 09.08.2018 (2018-08-09) paragraph [0040]	9

☐ 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	Date of mailing of the international search report
06 April 2020 (06.04.2020)	21 April 2020 (21.04.2020)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application no.
PCT/JP2020/007013

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2016-188016 A	04 Nov. 2016	US 2018/0081671 A1 claim 1, paragraphs [0036]-[0099], [0144], fig. 1-5 WO 2016/158547 A1 DE 112016000992 T CN 107531198 A	
WO 2015/011840 A1	29 Jan. 2015	(Family: none)	
WO 2016/147766 A1	22 Sep. 2016	US 2018/0018160 A1 paragraphs [0133]-[0136] JP 2016-170740 A EP 3273350 A1 CN 107077395 A	
JP 2009-199497 A	03 Sep. 2009	(Family: none)	
JP 2018-124749 A	09 Aug. 2018	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/007013

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G09C 1/00(2006.01)i; H04L 9/32(2006.01)i; B60R 16/02(2006.01)i; G06F 8/60(2018.01)i
FI: G06F8/60; B60R16/02 660U; G09C1/00 640E; H04L9/00 675B

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））

G09C1/00; H04L9/32; B60R16/02; G06F8/60

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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 2016-188016 A (本田技研工業株式会社) 04.11.2016 (2016-11-04) 請求項1,[0021]-[0082],[0119],図1-5	1-12
Y	WO 2015/011840 A1 (株式会社日立製作所) 29.01.2015 (2015-01-29) [0040],[0044],[0048],[0062]-[0063],図6,9-14	1-12
Y	WO 2016/147766 A1 (日立オートモティブシステムズ株式会社) 22.09.2016 (2016-09-22) [0091]-[0093]	2
Y	JP 2009-199497 A (パナソニック株式会社) 03.09.2009 (2009-09-03) [0038]-[0040]	4-6,10
Y	JP 2018-124749 A (京セラドキュメントソリューションズ株式会社) 09.08.2018 (2018-08-09) [0040]	9

☐ 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抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
06.04.2020	21.04.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
山本　俊介 5B 5087
電話番号 03-3581-1101 内線 3545

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/007013

引用文献	公表日	パテントファミリー文献	公表日
JP 2016-188016 A	04.11.2016	US 2018/0081671 A1 Claiml,[0036]-[0099], [0144],FIGs.1-5 WO 2016/158547 A1 DE 112016000992 T CN 107531198 A	
WO 2015/011840 A1	29.01.2015	（ファミリーなし）	
WO 2016/147766 A1	22.09.2016	US 2018/0018160 A1 [0133]-[0136] JP 2016-170740 A EP 3273350 A1 CN 107077395 A	
JP 2009-199497 A	03.09.2009	（ファミリーなし）	
JP 2018-124749 A	09.08.2018	（ファミリーなし）	