

(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 6 月 4 日(04.06.2015)



(10) 国際公開番号

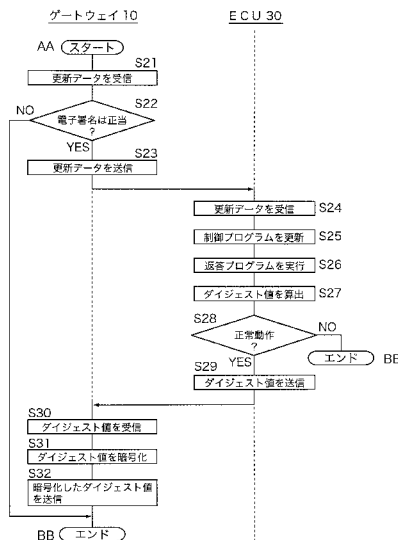
WO 2015/080108 A1

- (51) 国際特許分類:
G06F 11/00 (2006.01) G06F 9/445 (2006.01)
B60R 16/02 (2006.01)
- (21) 国際出願番号: PCT/JP2014/081139
- (22) 国際出願日: 2014 年 11 月 26 日(26.11.2014)
- (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 2013-245083 2013 年 11 月 27 日(27.11.2013) JP
- (71) 出願人: 株式会社オートネットワーク技術研究所 (AUTONETWORKS TECHNOLOGIES, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町 1 番 1 4 号 Mie (JP). 住友電装株式会社(SUMITOMO WIRING SYSTEMS, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町 1 番 1 4 号 Mie (JP). 住友電気工業株式会社(SUMITOMO ELECTRIC INDUSTRIES, LTD.) [JP/JP]; 〒5410041 大阪府大阪市中央区北浜四丁目 5 番 3 3 号 Osaka (JP).
- (72) 発明者: 足立 直樹(ADACHI, Naoki); 〒5108503 三重県四日市市西末広町 1 番 1 4 号 株式会社オートネットワーク技術研究所内 Mie (JP). 宇佐美 彰規(USAMI, Akinori); 〒5108503 三重県四日市市西末広町 1 番 1 4 号 株式会社オートネットワーク技術研究所内 Mie (JP). 渡部 正志(WATANABE, Masashi); 〒5108503 三重県四日市市西末広町 1 番 1 4 号 株式会社オートネットワーク技術研究所内 Mie (JP). 野田 哲矢(NODA, Tetsuya); 〒5108503 三重県四日市市西末広町 1 番

[続葉有]

(54) Title: PROGRAM UPDATE SYSTEM AND PROGRAM UPDATE METHOD

(54) 発明の名称: プログラム更新システム及びプログラム更新方法



10 Gateway
AA Start
S21, S24 Receive update data
S22 Digital signature legitimate?
S23 Transmit update data
S25 Update control program
S26 Execute response program
S27 Compute digest value
S28 Normal operation?
S29 Transmit digest value
S30 Receive digest value
S31 Encrypt digest value
S32 Transmit encrypted digest value
BB End

(57) Abstract: Provided are a program update system and program update method capable of verifying the legitimacy of an update of a program executed on a vehicle side. A vehicle-external device stores, as update data necessary for updating a control program which is stored in a control device, update data including: an update control program for the control device to be updated; and a computer program which implements a means for computing a digest value relating to the update control program, a means for determining whether an operation of the updated control device is normal, and a means for returning the result of the determination. The control device receives via a relay device the update data transmitted from the vehicle-external device, updates the control program by the update control program which is included in the received update data, executes the computer program, determines whether the operation after the update is normal, and returns the result of the determination to the relay device.

(57) 要約: 車両側で実行されたプログラムの更新の正当性を検証できるプログラム更新システム及びプログラム更新方法の提供。車外装置は、制御装置に記憶された制御プログラムを更新するために必要な更新データとして、更新対象の制御装置に対する更新制御プログラムと、更新制御プログラムに係るダイジェスト値を算出する手段、更新後の制御装置の動作が正常であるか否かを判定する手段、及び判定結果を返答する手段を実現するコンピュータプログラムとを含む更新データを記憶してあり、制御装置は、車外装置から送信される更新データを中継装置を介して受信し、受信した更新データに含まれる更新制御プログラムにより制御プログラムを更新すると共に、前記コンピュータプログラムを実行して更新後の動作が正常であるか否かを判定して、その判定結果を中継装置に返答する。

WO 2015/080108 A1



1 4 号 株式会社オートネットワーク技術研
究所内 Mie (JP).

(74) 代理人: 河野 英仁, 外 (KOHNO, Hideto et al.);
〒5400035 大阪府大阪市中央区釣鐘町二丁目 4
番 3 号 河野特許事務所 Osaka (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, 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.

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

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：プログラム更新システム及びプログラム更新方法 技術分野

[0001] 本発明は、車両側で実行されたプログラムの更新の正当性を検証するプログラム更新システム及びプログラム更新方法に関する。

背景技術

[0002] 近年、自動車の分野においては、車両の高機能化が益々進んでおり、多種多様な機器が車両に搭載され、これら車載機器を制御するための制御装置、所謂ＥＣＵ（Electronic Control Unit）が多数搭載されている。例えば、乗員によるスイッチ操作などに応じて車内照明やヘッドライトの点灯／消灯、及び警報器の吹鳴等の制御を行うボディ系ＥＣＵ、運転席近傍に配設されるメータ類の動作を制御するメータ系ＥＣＵ、並びにカーナビゲーション装置等の制御を行うナビ系ＥＣＵなどの種々のＥＣＵが車両には搭載されている。

[0003] 一般的にＥＣＵは、マイクロコンピュータ等の演算処理装置によって構成されており、ＲＯＭ（Read Only Memory）に記憶した制御プログラムを読み込んで実行することにより、車載機器の制御が実現されている。制御プログラムは、同じ車種でも、車両が運用される仕向け地や搭載機能によって異なることがあり、仕向け地や搭載機能に合わせて制御プログラムを書換えたり、制御プログラムのバージョンアップに対応して、旧バージョンの制御プログラムを新たなバージョンの制御プログラムに書換えたりする必要がある。

[0004] 特許文献１には、車両に搭載された自動車制御装置において、無線通信により受信したデータが自己の装置宛に送信されたデータであると確認できた場合、不揮発性メモリに記憶されているデータを、受信したデータに書換える自動車用制御装置が開示されている。

先行技術文献

特許文献

[0005] 特許文献1：特開平05－195859号公報

発明の概要

発明が解決しようとする課題

[0006] しかしながら、車載機器の制御プログラムを追加又は更新できる構成とした場合、悪意の第三者が作成したプログラムが追加されて実行される虞がある。これにより、例えば車内ネットワークにて送受信される情報が不正なプログラムによって外部へ漏洩するなどの虞がある。

[0007] 本発明は、斯かる事情に鑑みてなされたものであり、車両側で実行されたプログラムの更新の正当性を検証できるプログラム更新システム及びプログラム更新方法を提供することを目的とする。

課題を解決するための手段

[0008] 本発明に係るプログラム更新システムは、車載機器を制御するための制御プログラムを記憶する記憶手段と、前記制御プログラムを読み出して実行する実行手段とを備える複数の制御装置、該複数の制御装置に車内通信線を介して接続された中継装置、及び該中継装置に車外通信網を介して接続され、前記制御プログラムを更新するために必要な更新データを記憶する車外装置を含み、該車外装置から前記更新データを前記中継装置へ送信し、該中継装置が受信した前記更新データに基づき、前記制御装置の記憶手段に記憶された制御プログラムを更新するシステムにおいて、前記更新データは、更新対象の制御装置に対する更新制御プログラムと、該更新制御プログラムに係るダイジェスト値を算出する手段、更新後の前記制御装置の動作が正常であるか否かを判定する手段、及び該判定する手段の判定結果を前記中継装置に返答する手段を実現するコンピュータプログラムとを含み、前記中継装置は、前記車外装置から受信した前記更新データを前記更新対象の制御装置へ送信する手段を備え、前記制御装置は、前記中継装置から送信された前記更新データを受信する手段と、受信した前記更新データに含まれる前記更新制御プログラムにより前記記憶手段に記憶された制御プログラムを更新する手段とを備え、前記制御装置は、前記更新データに含まれる前記コンピュータプロ

グラムを実行して更新後の動作が正常であるか否かを判定し、その判定結果を前記中継装置に返答することを特徴とする。

[0009] 本発明に係るプログラム更新システムは、前記中継装置は、前記車内通信線を介して接続された各制御装置を識別する装置識別情報、及び各制御装置の記憶手段に記憶された制御プログラムを識別するプログラム識別情報を記憶する手段と、更新対象の制御プログラムを記憶する制御装置の装置識別情報、及び前記制御プログラムのプログラム識別情報を前記車外装置へ送信する手段とを備え、前記車外装置は、前記中継装置から送信された装置識別情報及びプログラム識別情報を受信する手段と、受信した装置識別情報及びプログラム識別情報に基づき、前記中継装置へ送信すべき更新データを特定する手段と、特定した更新データを前記中継装置へ送信する際、前記装置識別情報及びプログラム識別情報を付加する手段とを備えることを特徴とする。

[0010] 本発明に係るプログラム更新システムは、前記中継装置は、前記更新制御プログラムに係るダイジェスト値を取得する手段と、取得したダイジェスト値を暗号化する手段と、暗号化したダイジェスト値を前記車外装置へ送信する手段とを備え、前記車外装置は、前記中継装置から送信された暗号化済みのダイジェスト値を受信する手段と、受信したダイジェスト値を復号する手段と、復号したダイジェスト値を予め記憶してある期待値と比較する手段と比較した結果に基づき、前記制御装置における更新後の制御プログラムの正当性を判断する手段とを備えることを特徴とする。

[0011] 本発明に係るプログラム更新システムは、前記車外装置は、更新後の制御プログラムが正当でないと判断した場合、記憶してある更新データ及び前記コンピュータプログラムを前記中継装置を介して前記制御装置へ再送信する手段を備えることを特徴とする。

[0012] 本発明に係るプログラム更新システムは、前記車外装置は、更新後の制御プログラムが正当でないと判断した場合、前記制御プログラムの実行を停止すべき旨を前記中継装置を介して前記制御装置へ通知する手段を備え、前記制御装置は、前記制御プログラムの実行を停止すべき旨の通知を前記車外装

置から受信した場合、前記制御プログラムの実行を停止する手段を備えることを特徴とする。

[0013] 本発明に係るプログラム更新システムは、前記車外装置、前記中継装置及び前記制御装置の少なくとも1つは、更新前の制御プログラムを保持する手段を備え、前記車外装置は、更新後の制御プログラムが正当でないと判断した場合、更新前の制御プログラムに戻すべき旨を前記中継装置を介して前記制御装置へ通知する手段を備え、前記制御装置は、更新前の制御プログラムに戻すべき旨の通知を前記中継装置を介して受信した場合、更新前の制御プログラムを取得する手段と、前記記憶手段に記憶された更新後の制御プログラムを、取得した更新前の制御プログラムに戻す手段とを備えることを特徴とする。

[0014] 本発明に係るプログラム更新方法は、車載機器を制御するための制御プログラムを記憶する記憶手段と、前記制御プログラムを読み出して実行する実行手段とを備える制御装置に対し、車外装置は、前記制御プログラムを更新するために必要な更新データを前記制御装置に接続された中継装置へ送信し、該中継装置が受信した前記更新データに基づき、前記制御装置の記憶手段に記憶された制御プログラムを更新する方法において、前記更新データは、更新対象の制御装置に対する更新制御プログラムと、該更新制御プログラムに係るダイジェスト値を算出する手段、更新後の前記制御装置の動作が正常であるか否かを判定する手段、及び該判定する手段の判定結果を前記中継装置に返答する手段を実現するコンピュータプログラムとを含み、前記中継装置は、前記車外装置から受信した前記更新データを前記更新対象の制御装置へ送信し、前記制御装置は、前記中継装置から送信された前記更新データを受信し、受信した前記更新データに含まれる前記更新制御プログラムにより前記記憶手段に記憶された制御プログラムを更新し、前記更新データに含まれる前記コンピュータプログラムを実行して更新後の動作が正常であるか否かを判定し、その判定結果を前記中継装置に返答することを特徴とする。

[0015] 本発明にあつては、車外装置は、制御装置に記憶された制御プログラムを

更新するために必要な更新データとして、更新対象の制御装置に対する更新制御プログラムと、更新制御プログラムに係るダイジェスト値を算出する手段、更新後の制御装置の動作が正常であるか否かを判定する手段、及び判定結果を返答する手段を実現するコンピュータプログラムとを含む更新データを記憶しており、中継装置を介して、制御装置へ更新データを送信する。制御装置では、受信した更新データに含まれる更新制御プログラムに基づき制御プログラムを更新すると共に、更新データに含まれるコンピュータプログラムを実行することによって、更新後の動作が正常であるか否かを判定して中継装置へ返答する。

本発明では、制御プログラムを更新する更新データに上記コンピュータプログラムを実装できるので、事前に制御装置内に実装しておく場合と比較して、上記コンピュータプログラムの改竄が困難となる。また、中継装置又は中継装置に通信可能に接続された車外装置において、更新制御プログラムのダイジェスト値の正当性を検証することにより、更新された制御プログラムの正当性が担保される。

[0016] 本発明では、中継装置が制御装置の装置識別情報、及び制御プログラムのプログラム識別情報を管理しているので、車外装置は、中継装置から更新対象の制御装置の装置識別情報、及び制御プログラムのプログラム識別情報を取得することにより、更新対象を特定することができる。

[0017] 本発明では、中継装置は、制御装置から送信されたダイジェスト値を暗号化して車外装置へ送信するので、ダイジェスト値を送信する通信経路の途中で改竄されることが防止される。

[0018] 本発明では、更新後の制御プログラムが正当でないと判断した場合、更新データ及び前記コンピュータプログラムを再送信するので、ビット欠け等に伴う制御プログラムの不具合が防止される。

[0019] 本発明では、更新後の制御プログラムが正当でないと判断した場合、制御プログラムの実行を停止するので、改竄された制御プログラムにより車載機器が動作することを防止する。

[0020] 本発明では、更新後の制御プログラムが正当でないと判断した場合、更新前の制御プログラムに戻すので、少なくとも更新前の制御装置の動作を担保することができる。

発明の効果

[0021] 本願によれば、制御プログラムを更新する更新データに、更新制御プログラムに係るダイジェスト値を算出する手段、更新後の動作が正常であるか否かを判定する手段、及び判定結果を前記中継装置に返答する手段を実現するコンピュータプログラムを実装するので、事前に制御装置内に実装しておく場合と比較して、上記コンピュータプログラムを改竄することが困難となる。また、更新データの配信側にて上記コンピュータプログラムを作成することができるため、更新する都度、ダイジェスト値に対する期待値を変更することができ、改竄及びなりすましを防止することができる。

[0022] また、中継装置又は中継装置に通信可能に接続された車外装置において、制御装置から出力されるダイジェスト値を検証することにより、上記コンピュータプログラムの正常動作を確認することができ、更新された制御プログラムの正当性を担保することができる。

図面の簡単な説明

[0023] [図1]本実施の形態に係るプログラム更新システムの構成を示す模式図である。

[図2]ゲートウェイの内部構成を示すブロック図である。

[図3]E C Uの内部構成を説明するブロック図である。

[図4]サーバ装置の内部構成を説明するブロック図である。

[図5]サーバ装置が実行する処理の手順を示すフローチャートである。

[図6]車両にて実行される処理の手順を示すフローチャートである。

[図7]ダイジェスト値を検証する処理の手順を示すフローチャートである。

発明を実施するための形態

[0024] 以下、本発明をその実施の形態を示す図面に基づいて具体的に説明する。

図1は本実施の形態に係るプログラム更新システムの構成を示す模式図で

ある。図において一点鎖線で示す 1 は車両であり、車両 1 には、ゲートウェイ 10 及び複数の ECU 30, 30, …等が搭載されている。車両 1 には、共通の通信線にバス接続された複数の ECU 30, 30, …による通信グループが複数存在し、通信グループ間の通信をゲートウェイ 10 が中継している。このためゲートウェイ 10 には、複数の通信線が接続されている。また、ゲートウェイ 10 は、公衆携帯電話網などの広域無線網 N に通信可能に接続され、広域無線網 N を通じてサーバ装置 5 などの車外装置から受信した情報を ECU 30 へ送信すると共に、ECU 30 から取得した情報を広域無線網 N を介して車外装置へ送信する。

[0025] なお、本実施の形態では、ゲートウェイ 10 が直接的に車外装置と通信を行う構成としたが、ゲートウェイ 10 に通信装置を接続し、接続した通信装置を通じて車外装置と通信を行う構成としてもよい。ゲートウェイ 10 に接続される通信装置には、例えば、ユーザが所持する携帯電話機、スマートフォン、タブレット型端末、ノート PC (Personal Computer) 等の装置が含まれる。

[0026] 図 2 はゲートウェイ 10 の内部構成を示すブロック図である。ゲートウェイ 10 は、CPU (Central Processing Unit) 11、RAM (Random Access Memory) 12、記憶部 13、車内通信部 14、及び無線通信部 15 等を備えて構成されている。

[0027] CPU 11 は、記憶部 13 に記憶された一又は複数のプログラムを RAM 12 に読み出して実行することにより、ゲートウェイ 10 を本発明に係る中継装置として機能させる。CPU 11 は、例えば時分割などで複数のプログラムを切り替えて実行することにより、複数のプログラムを並列的に実行することができる。RAM 12 は、SRAM (Static RAM) 又は DRAM (Dynamic RAM) 等のメモリ素子で構成され、CPU 11 が実行するプログラム及び実行に必要なデータ等が一時的に記憶される。

[0028] 記憶部 13 は、フラッシュメモリ若しくは EEPROM (Electrically Erasable Programmable Read Only Memory) 等の不揮発性のメモリ素子、又は

、ハードディスクなどの磁気記憶装置等を用いて構成されている。記憶部 13 は、CPU 11 が実行するプログラム及び実行に必要なデータ等を記憶する記憶領域を有する。

[0029] 車内通信部 14 には、車両 1 内に配設された通信線を介して複数の ECU 30, 30, …が接続されている。車内通信部 14 は、例えば CAN (Controller Area Network)、LIN (Local Interconnect Network)、Ethernet (登録商標)、又は MOST (Media Oriented Systems Transport) 等の規格に応じて、ECU 30 との通信を行う。車内通信部 14 は、CPU 11 から与えられた情報を対象の ECU 30 へ送信すると共に、ECU 30 から受信した情報を CPU 11 へ与える。車内通信部 14 は、上記通信規格だけでなく、車載ネットワークで用いられる他の通信規格によって通信してもよい。

[0030] 無線通信部 15 は、例えばアンテナ及びその通信に関する処理を実行する付属回路を用いて構成され、公衆携帯電話網等の広域無線網 N に接続して通信処理を実行する機能を有する。無線通信部 15 は、図に示していない基地局により形成される広域無線網 N を介して、CPU 11 から与えられた情報をサーバ装置 5 等の車外装置へ送信すると共に、車外装置から受信した情報を CPU 31 へ与える。

[0031] なお、ゲートウェイ 10 は、無線通信部 15 に代えて、上述した通信装置を接続するための有線通信部を備える構成であってもよい。この有線通信部は、USB (Universal Serial Bus) 又は RS 232C 等の規格に応じた通信ケーブルを介して通信装置を接続するコネクタを有し、通信ケーブルを介して接続された通信装置と通信を行う。有線通信部は、CPU 11 から与えられた情報を無線通信により広域無線網 N に接続された車外装置へ送信すると共に、広域無線網 N を通じて車外装置から受信した情報を CPU 11 へ与える。

[0032] 図 3 は ECU 30 の内部構成を説明するブロック図である。ECU 30 は、例えば、CPU 31、RAM 32、記憶部 33、通信部 34 等を備え、図

に示していない各種車載機器の制御を行う。

[0033] CPU 31は、記憶部33に予め記憶された一又は複数のプログラムをRAM 32に読み出して実行することにより、上述した各ハードウェアの動作を制御し、ECU 30を本発明に係る制御装置として機能させる。RAM 32は、SRAM又はDRAM等のメモリ素子で構成され、CPU 31が実行するプログラム及び実行に必要なデータ等が一時的に記憶される。

[0034] 記憶部33は、フラッシュメモリ若しくはEEPROM等の不揮発性のメモリ素子、又は、ハードディスクなどの磁気記憶装置等を用いて構成されている。記憶部33が記憶する情報には、例えば、制御対象である車載装置を制御するための処理をCPU 31に実行させるためのコンピュータプログラム（以下、制御プログラムという）が含まれる。

[0035] 通信部34には、車両1内に配設された通信線を介してゲートウェイ10が接続されている。通信部34は、例えばCAN（Controller Area Network）又はLIN（Local Interconnect Network）、Ethernet（登録商標）、又はMOST（Media Oriented Systems Transport）等の規格に応じて、ゲートウェイ10との通信を行う。通信部34は、CPU 31から与えられた情報をゲートウェイ10へ送信すると共に、ゲートウェイ10から受信した情報をCPU 31へ与える。通信部34は、上記通信規格だけでなく、車載ネットワークで用いられる他の通信規格によって通信してもよい。

[0036] 図4はサーバ装置5の内部構成を説明するブロック図である。サーバ装置5は、例えば、CPU 51、ROM 52、RAM 53、記憶部54、通信部55等を備える。

[0037] CPU 51は、ROM 52に予め記憶された一又は複数のプログラムをRAM 53に読み出して実行することにより、上述した各ハードウェアの動作を制御し、サーバ装置5を本発明に係る車外装置として機能させる。RAM 53は、SRAM又はDRAM等のメモリ素子で構成され、CPU 51が実行するプログラム及び実行に必要なデータ等が一時的に記憶される。

[0038] 記憶部54は、フラッシュメモリ若しくはEEPROM等の不揮発性のメ

メモリ素子、又は、ハードディスクなどの磁気記憶装置等を用いて構成されている。記憶部54が記憶する情報には、例えば、車両1に搭載されたECU30が実行する制御プログラムを更新するために必要な更新データが含まれる。更新データには、更新対象のECU30が記憶する制御プログラムの一部又は全部を書き換えるための制御を実行させる更新制御プログラムが含まれている。

[0039] また、更新データには、制御プログラムを更新したECU30に実行させるべきコンピュータプログラム（以下、返答プログラムという）が記憶されている。返答プログラムは、ECU30を、更新制御プログラムに係るダイジェスト値を算出する手段、更新後の動作が正常であるか否かを判定する手段、及びその判定結果をゲートウェイ10へ返答する手段として機能させるコンピュータプログラムとして構成されている。

[0040] 通信部55は、例えば通信に関する処理を実行する処理回路を含み、公衆携帯電話網等の広域無線網Nに接続して通信処理を実行する機能を有する。通信部55は、CPU51から与えられた情報を広域無線網Nを介して外部の装置へ送信すると共に、広域無線網Nを介して受信した情報をCPU51へ与える。

[0041] 以下、制御プログラムの更新手順について説明する。

図5はサーバ装置5が実行する処理の手順を示すフローチャートである。サーバ装置5の記憶部54には、車両1側のECU30が実行する制御プログラムを更新するための更新データ（リプロデータ）が制御プログラムのバージョン番号に対応付けられて記憶されているものとする。サーバ装置5のCPU51は、車両1の車両番号、更新対象のECU30のシリアル番号、及び更新対象の制御プログラムのバージョン番号が添付された更新データのリクエストを、車両1のゲートウェイ10から受信したか否かを判断する（ステップS11）。リクエストを受信していない場合（S11：NO）、CPU51は、車両1のゲートウェイ10からリクエストを受信するまで待機する。

- [0042] リクエストを受信した場合（S 1 1 : Y E S）、C P U 5 1 は、送信すべき更新データを記憶部 5 4 から読み出し、読み出した更新データに対して認証局（CA : Certification Authority）又は O E M（Original Equipment Manufacturer）毎の電子署名を付与する（ステップ S 1 2）。次いで、C P U 5 1 は、上述した更新制御プログラム及び返答プログラムを含み、電子署名を付与した更新データを更新対象の E C U 3 0 を備える車両 1 のゲートウェイ 1 0 へ通信部 5 5 を通じて送信する（ステップ S 1 3）。
- [0043] なお、図 5 に示す処理手順では、更新データのリクエストに添付されている車両番号、E C U 3 0 のシリアル番号、及び制御プログラムのバージョン番号を参照して、更新対象の E C U 3 0 を特定する構成としたが、サーバ装置 5 の記憶部 5 4 にて、車両 1 の車両番号、E C U 3 0 のシリアル番号、E C U 3 0 にインストールされている制御プログラムのバージョン番号を互いに関連付けて記憶しておき、サーバ装置 5 側から更新対象の E C U 3 0 を指定する構成としてもよい。
- [0044] 図 6 は車両 1 にて実行される処理の手順を示すフローチャートである。サーバ装置 5 から送信される更新データをゲートウェイ 1 0 の無線通信部 1 5 にて受信した場合（ステップ S 2 1）、ゲートウェイ 1 0 の C P U 1 1 は、受信した更新データに係る電子署名が正当であるか否かを判断する（ステップ S 2 2）。ゲートウェイ 1 0 は、認証局又は各 O E M から電子証明書を予め取得しておくことにより、その電子証明書を用いて電子署名が正当であるか否かを判断することができる。
- [0045] サーバ装置 5 から受信した更新データの電子署名が正当でないと判断した場合（S 2 2 : N O）、C P U 1 1 は、本フローチャートによる処理を終了する。
- [0046] サーバ装置 5 から受信した更新データの電子署名が正当であると判断した場合（S 2 2 : Y E S）、C P U 1 1 は、車内通信部 1 4 を通じて更新対象の E C U 3 0 へ送信する（ステップ S 2 3）。
- [0047] ゲートウェイ 1 0 から送信される更新データを E C U 3 0 の通信部 3 4 に

て受信した場合（ステップS24）、ECU30のCPU31は、受信した更新データに含まれる更新制御プログラムをRAM32に読み込んで実行し、記憶部33に記憶されている制御プログラムを更新する処理（リプログラミング）を実行する（ステップS25）。

[0048] 制御プログラムの更新には、例えば、OSGi（Open Services Gateway initiative）の技術を採用することができる。OSGiは、バンドルと呼ばれるプログラムの動的な追加及び実行等を管理するシステムであり、バンドルの実行基盤であるOSGiフレームワークがCPU31にて動作するように構成されている。なお、OSGiは既存の技術であるため、詳細な説明は省略する。また、CPU31は、OSGi以外の技術を採用して制御プログラムの更新を行ってもよい。

[0049] 制御プログラムの更新が完了した場合、ECU30のCPU31は、更新データに含まれる返答プログラムをRAM32に読み込んで実行し（ステップS26）、ECU30を、更新制御プログラムに係るダイジェスト値を算出する手段、更新後の動作が正常であるか否かを判定する手段、及びその判定結果をゲートウェイ10へ送信する手段として機能させる。

[0050] 返答プログラムを実行したECU30のCPU31は、更新制御プログラムについてダイジェスト値を算出する（ステップS27）。CPU31が算出するダイジェスト値は、既知のハッシュ関数によって求めたダイジェスト値（ハッシュ値）であってもよく、MD5などのその他のアルゴリズムによって求めたダイジェスト値であってもよい。また、更新制御プログラムが、複数のプログラムからなるプログラム群により構成されている場合、予め定めたプログラムのみからダイジェスト値を算出してもよい。更新後の制御プログラムを含めてダイジェスト値を算出してもよい。なお、ダイジェスト値を算出する範囲は返答プログラムにより規定されているものとする。

[0051] 次いで、CPU31は、ECU30の基本機能を動作させ、自装置（ECU30自身）が正常に動作するか否かを判定する（ステップS28）。自装置が正常に動作すると判定した場合（S28：YES）、CPU31は、そ

の判定結果と共に、ステップS 2 7で算出したダイジェスト値を通信部3 4を通じてゲートウェイ1 0へ送信する（ステップS 2 9）。また、自装置が正常に動作しなかった場合（S 2 8：NO）、CPU 3 1は、本フローチャートによる処理を終了する。

[0052] ゲートウェイ1 0のCPU 1 1は、ECU 3 0から送信される判定結果及びダイジェスト値を車内通信部1 4にて受信した場合（ステップS 3 0）、受信したダイジェスト値を暗号化し（ステップS 3 1）、暗号化したダイジェスト値を無線通信部1 5を通じてサーバ装置5へ送信する（ステップS 3 2）。

[0053] なお、本実施の形態では、ECU 3 0において更新制御プログラムのダイジェスト値を算出し、自装置が正常に動作すると判定した場合、算出したダイジェスト値をゲートウェイ1 0へ送信する構成としたが、ECU 3 0では、更新後の制御プログラムによって自装置が正常に動作するか否かの判定を行い、その判定結果をゲートウェイ1 0に返答する処理のみを実行してもよい。この場合、ゲートウェイ1 0は、ECU 3 0から正常に動作する旨の返答を受信したとき、ステップS 2 1で受信した更新データに含まれる更新制御プログラムからダイジェスト値を算出し、算出したダイジェスト値を暗号化した上でサーバ装置5へ送信する構成とすればよい。

[0054] 図7はダイジェスト値を検証する処理の手順を示すフローチャートである。サーバ装置5のCPU 5 1は、車両1のゲートウェイ1 0から送信される暗号化済みのダイジェスト値を通信部5 5にて受信した場合（ステップS 4 1）、暗号化済みのダイジェスト値を復号する（ステップS 4 2）。なお、ゲートウェイ1 0にてダイジェスト値を暗号化し、サーバ装置5にて暗号化済みのダイジェスト値を復号する手法には、公開鍵暗号方式等の既知の手法を用いることができる。

[0055] 次いで、サーバ装置5のCPU 5 1は、復号したダイジェスト値と、記憶部5 4に予め記憶してある期待値とを比較し（ステップS 4 3）、両者が一致するか否かを判断する（ステップS 4 4）。

- [0056] 両者が一致すると判断した場合（S 4 4 : Y E S）、C P U 5 1 は、更新対象の E C U 3 0 において制御プログラムの更新が正常に終了したと判定する（ステップ S 4 5）。また、両者が一致しないと判断した場合（S 4 4 : N O）、C P U 5 1 は、E C U 3 0 における制御プログラムの更新が正常でなかったと判定する（ステップ S 4 6）。
- [0057] E C U 3 0 における制御プログラムの更新が正常でなかった場合、サーバ装置 5 は、記憶部 5 4 に記憶してある更新データを E C U 3 0 へ再送する構成としてもよい。
- [0058] また、E C U 3 0 における制御プログラムの更新が正常でなかった場合、制御プログラムの配信元が意図しない動作が E C U 3 0 にて実行される虞があるので、制御プログラムの停止を指示する通知をサーバ装置 5 から車両 1 側に通知し、制御プログラムを停止させる構成としてもよい。
- [0059] 更に、E C U 3 0 における制御プログラムの更新が正常でなかった場合、サーバ装置 5 は、更新前の制御プログラムに戻すべき旨の通知をゲートウェイ 1 0 を介して E C U 3 0 へ送信し、E C U 3 0 の記憶部 3 3 に記憶された更新後の制御プログラムを更新前の制御プログラムに戻すようにしてもよい。なお、更新前の制御プログラムは、サーバ装置 5 の記憶部 5 4、ゲートウェイ 1 0 の記憶部 1 3、及び E C U 3 0 の記憶部 3 3 の何れかで保持されていればよい。サーバ装置 5 から送信される前記通知を E C U 3 0 が受信した場合、自身の記憶部 3 3、ゲートウェイ 1 0 の記憶部 1 3、及びサーバ装置 5 の記憶部 5 4 の何れかから更新前の制御プログラムを取得し、更新後の制御プログラムを更新前の制御プログラムに書き換えることによって、元に戻すことが可能である。
- [0060] 以上のように、本願では、制御プログラムを更新する更新データに、制御プログラムのダイジェスト値を算出する処理、自装置が正常に動作するか否かを判定する処理、及び正常に動作する場合にダイジェスト値をゲートウェイ 1 0 へ送信する処理を実行させるコンピュータプログラム（返答プログラム）を実装できるので、事前に E C U 3 0 内に返答プログラムを実装してお

く場合と比較して、返答プログラムを改竄することが困難となる。また、更新データの配信側にて返答プログラムを作成することができるため、更新する都度、ダイジェスト値に対する期待値を変更することができ、改竄及びなりすましを防止することができる。

[0061] 今回開示された実施の形態は、全ての点で例示であって、制限的なものではないと考えられるべきである。本発明の範囲は、上述した意味ではなく、請求の範囲によって示され、請求の範囲と均等の意味及び範囲内での全ての変更が含まれることが意図される。

符号の説明

- [0062]
- 1 車両
 - 10 ゲートウェイ
 - 11 CPU
 - 12 RAM
 - 13 記憶部
 - 14 車内通信部
 - 15 無線通信部
 - 30 ECU
 - 31 CPU
 - 32 RAM
 - 33 記憶部
 - 34 通信部
 - 5 サーバ装置
 - 51 CPU
 - 52 ROM
 - 53 RAM
 - 54 記憶部
 - 55 通信部

請求の範囲

[請求項1]

車載機器を制御するための制御プログラムを記憶する記憶手段と、
前記制御プログラムを読み出して実行する実行手段と
を備える複数の制御装置、
該複数の制御装置に車内通信線を介して接続された中継装置、及び
該中継装置に車外通信網を介して接続され、前記制御プログラムを
更新するために必要な更新データを記憶する車外装置を含み、
該車外装置から前記更新データを前記中継装置へ送信し、該中継装
置が受信した前記更新データに基づき、前記制御装置の記憶手段に記
憶された制御プログラムを更新するシステムにおいて、
前記更新データは、
更新対象の制御装置に対する更新制御プログラムと、
該更新制御プログラムに係るダイジェスト値を算出する手段、
更新後の前記制御装置の動作が正常であるか否かを判定する手
段、及び
該判定する手段の判定結果を前記中継装置に返答する手段
を実現するコンピュータプログラムと
を含み、
前記中継装置は、
前記車外装置から受信した前記更新データを前記更新対象の制御装
置へ送信する手段
を備え、
前記制御装置は、
前記中継装置から送信された前記更新データを受信する手段と、
受信した前記更新データに含まれる前記更新制御プログラムにより
前記記憶手段に記憶された制御プログラムを更新する手段と
を備え、
前記制御装置は、前記更新データに含まれる前記コンピュータプロ

グラムを実行して更新後の動作が正常であるか否かを判定し、その判定結果を前記中継装置に返答する

ことを特徴とするプログラム更新システム。

[請求項2]

前記中継装置は、

前記車内通信線を介して接続された各制御装置を識別する装置識別情報、及び各制御装置の記憶手段に記憶された制御プログラムを識別するプログラム識別情報を記憶する手段と、

更新対象の制御プログラムを記憶する制御装置の装置識別情報、及び前記制御プログラムのプログラム識別情報を前記車外装置へ送信する手段と

を備え、

前記車外装置は、

前記中継装置から送信された装置識別情報及びプログラム識別情報を受信する手段と、

受信した装置識別情報及びプログラム識別情報に基づき、前記中継装置へ送信すべき更新データを特定する手段と、

特定した更新データを前記中継装置へ送信する際、前記装置識別情報及びプログラム識別情報を付加する手段と

を備えることを特徴とする請求項1に記載のプログラム更新システム。

[請求項3]

前記中継装置は、

前記更新制御プログラムに係るダイジェスト値を取得する手段と、

取得したダイジェスト値を暗号化する手段と、

暗号化したダイジェスト値を前記車外装置へ送信する手段と

を備え、

前記車外装置は、

前記中継装置から送信された暗号化済みのダイジェスト値を受信する手段と、

受信したダイジェスト値を復号する手段と、
復号したダイジェスト値を予め記憶してある期待値と比較する手段
と
比較した結果に基づき、前記制御装置における更新後の制御プログラムの正当性を判断する手段と
を備えることを特徴とする請求項 1 又は請求項 2 に記載のプログラム更新システム。

[請求項4]

前記車外装置は、
更新後の制御プログラムが正当でないと判断した場合、記憶してある更新データ及び前記コンピュータプログラムを前記中継装置を介して前記制御装置へ再送信する手段
を備えることを特徴とする請求項 3 に記載のプログラム更新システム。

[請求項5]

前記車外装置は、
更新後の制御プログラムが正当でないと判断した場合、前記制御プログラムの実行を停止すべき旨を前記中継装置を介して前記制御装置へ通知する手段
を備え、
前記制御装置は、
前記制御プログラムの実行を停止すべき旨の通知を前記車外装置から受信した場合、前記制御プログラムの実行を停止する手段
を備えることを特徴とする請求項 3 に記載のプログラム更新システム。

[請求項6]

前記車外装置、前記中継装置及び前記制御装置の少なくとも 1 つは、更新前の制御プログラムを保持する手段を備え、
前記車外装置は、
更新後の制御プログラムが正当でないと判断した場合、更新前の制御プログラムに戻すべき旨を前記中継装置を介して前記制御装置へ通

知する手段

を備え、

前記制御装置は、

更新前の制御プログラムに戻すべき旨の通知を前記中継装置を介して受信した場合、更新前の制御プログラムを取得する手段と、

前記記憶手段に記憶された更新後の制御プログラムを、取得した更新前の制御プログラムに戻す手段と

を備えることを特徴とする請求項3に記載のプログラム更新システム。

[請求項7]

車載機器を制御するための制御プログラムを記憶する記憶手段と、前記制御プログラムを読み出して実行する実行手段とを備える制御装置に対し、車外装置は、前記制御プログラムを更新するために必要な更新データを前記制御装置に接続された中継装置へ送信し、該中継装置が受信した前記更新データに基づき、前記制御装置の記憶手段に記憶された制御プログラムを更新する方法において、

前記更新データは、

更新対象の制御装置に対する更新制御プログラムと、

該更新制御プログラムに係るダイジェスト値を算出する手段、

更新後の前記制御装置の動作が正常であるか否かを判定する手段、及び

該判定する手段の判定結果を前記中継装置に返答する手段

を実現するコンピュータプログラムと

を含み、

前記中継装置は、

前記車外装置から受信した前記更新データを前記更新対象の制御装置へ送信し、

前記制御装置は、

前記中継装置から送信された前記更新データを受信し、

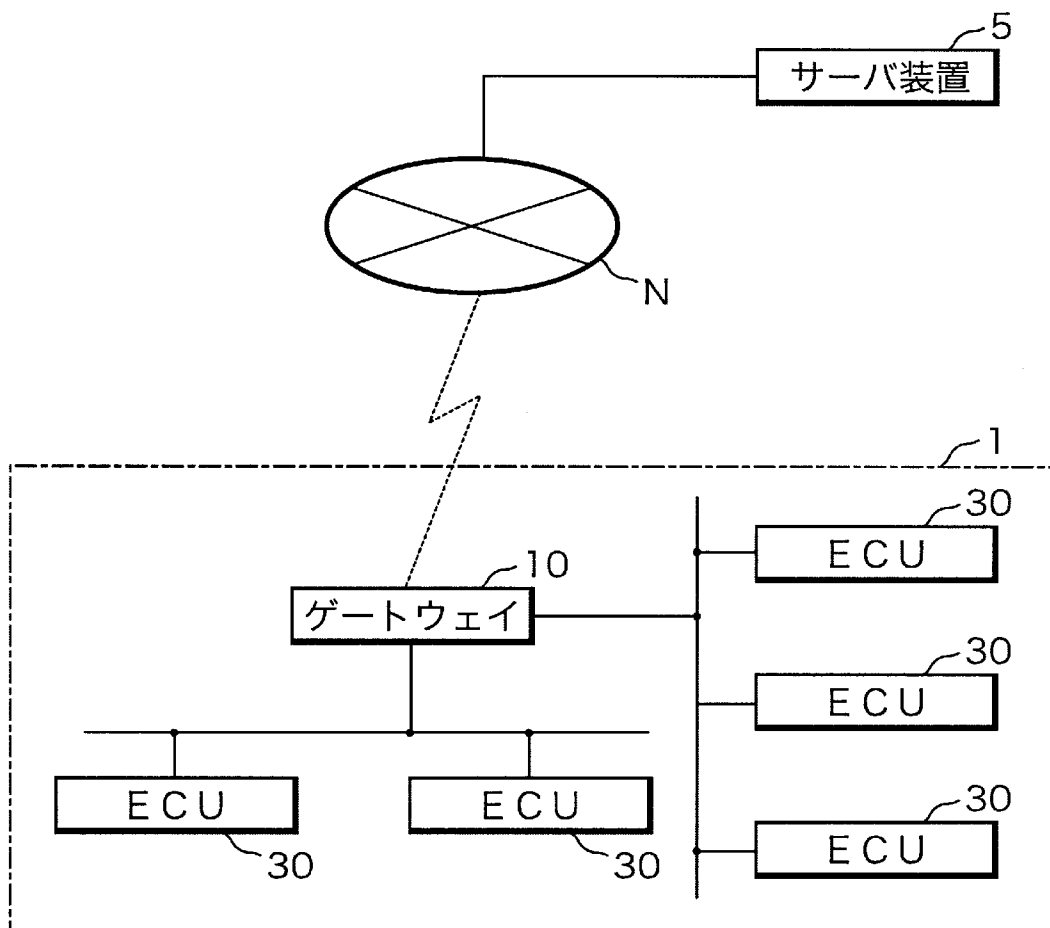
受信した前記更新データに含まれる前記更新制御プログラムにより
前記記憶手段に記憶された制御プログラムを更新し、

前記更新データに含まれる前記コンピュータプログラムを実行して
更新後の動作が正常であるか否かを判定し、

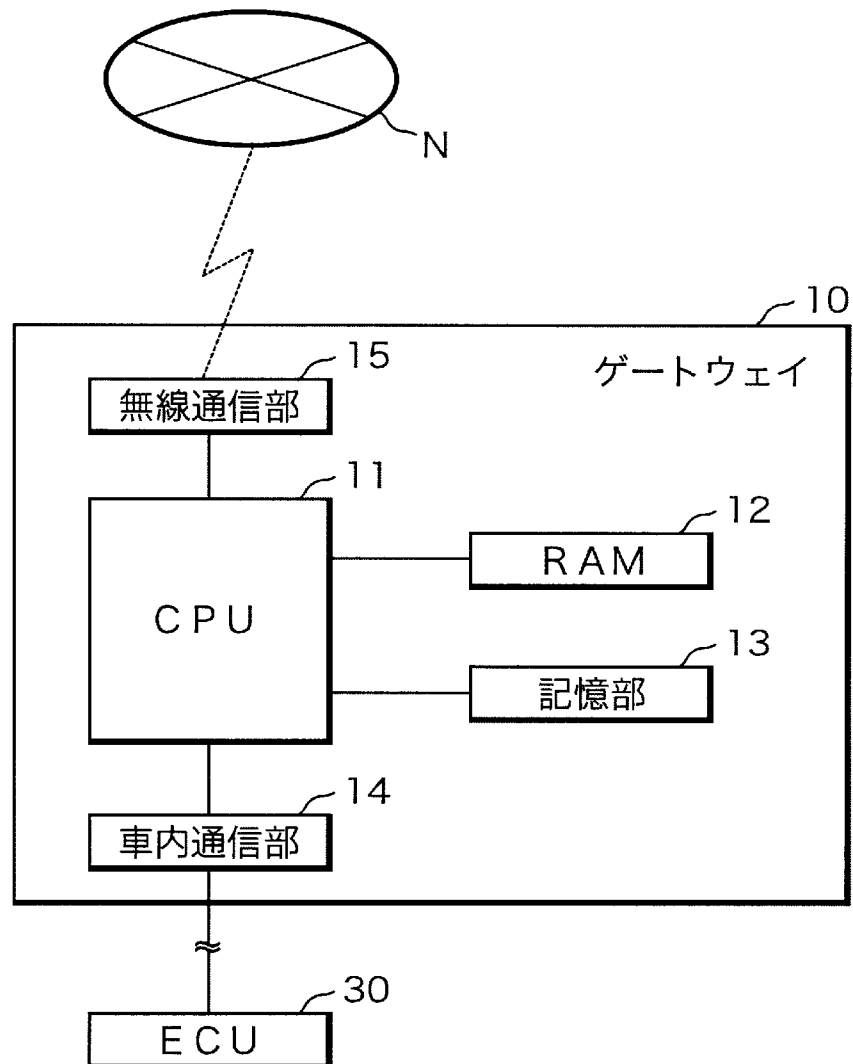
その判定結果を前記中継装置に返答する

ことを特徴とするプログラム更新方法。

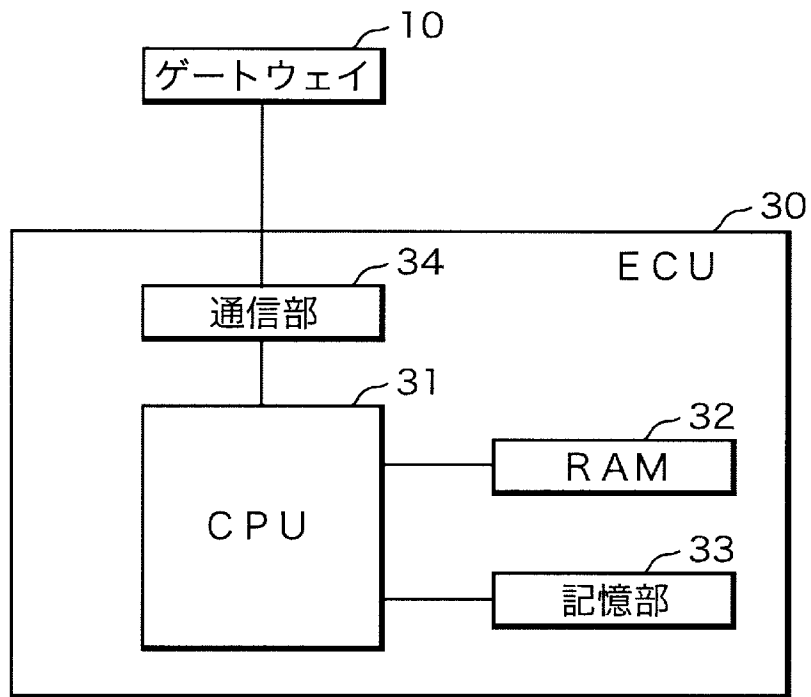
[図1]



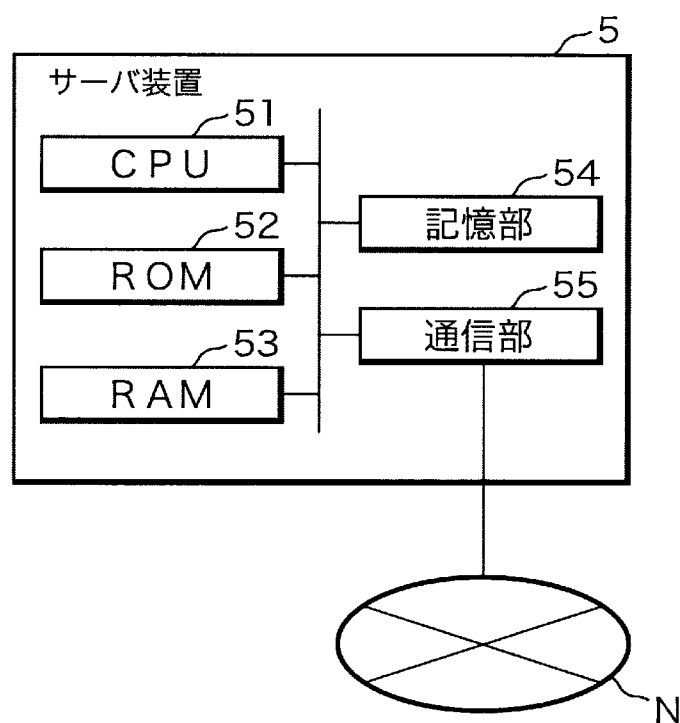
[図2]



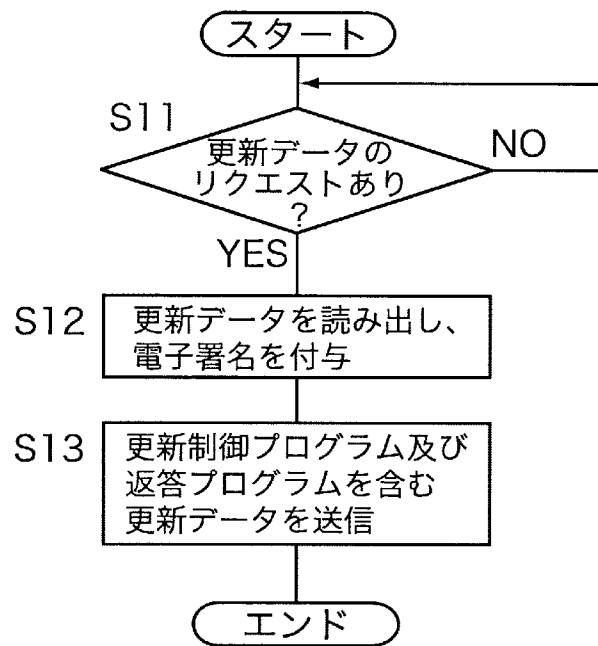
[図3]



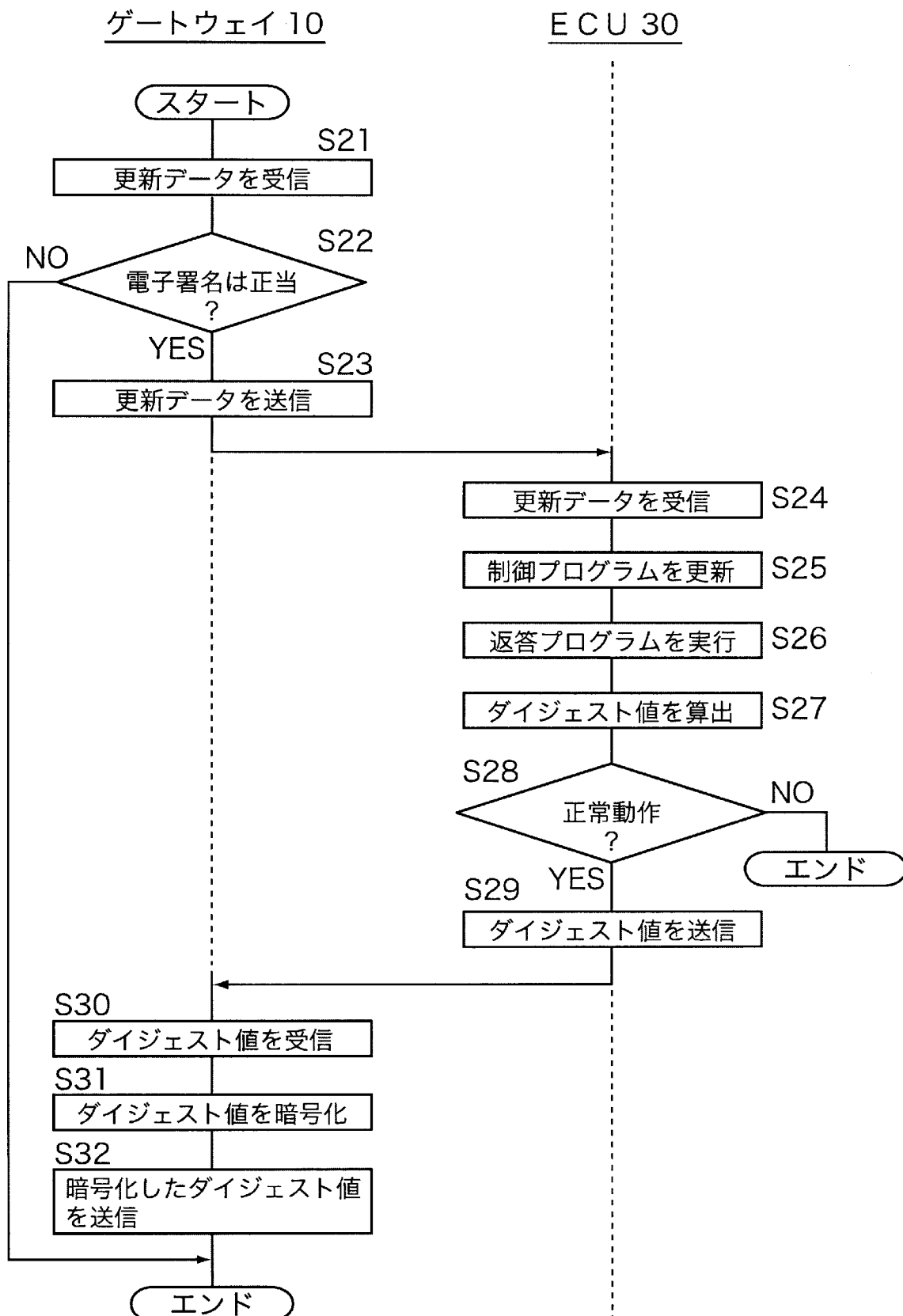
[図4]



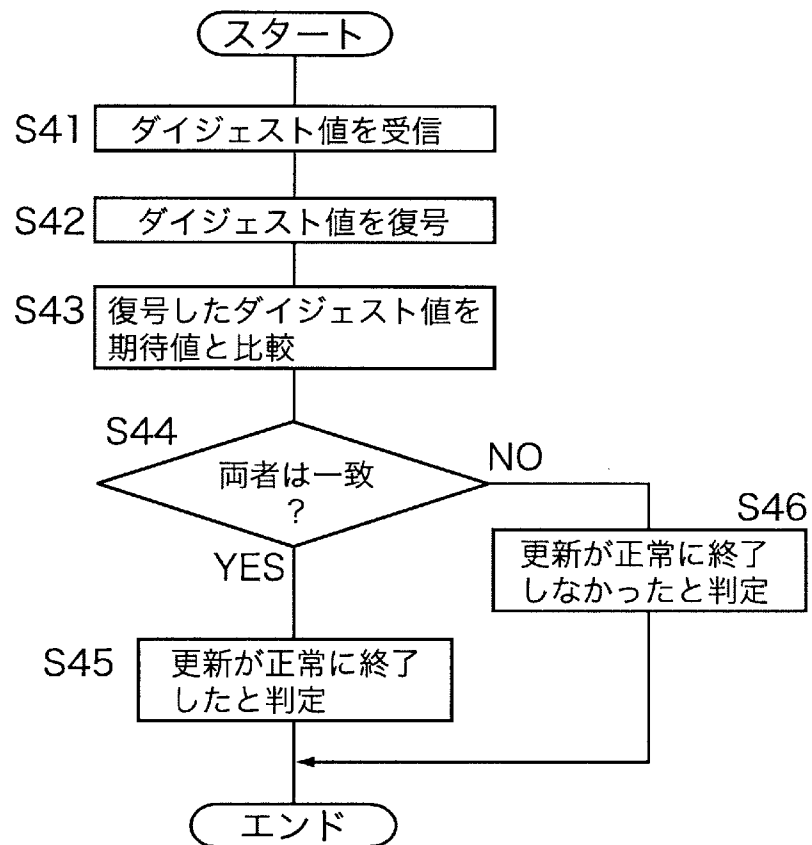
[図5]



[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/081139

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/00(2006.01)i, B60R16/02(2006.01)i, G06F9/445(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)

G06F11/00, B60R16/02, G06F9/445

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 2011-003020 A (Toyota InfoTechnology Center, Co., Ltd.), 06 January 2011 (06.01.2011), paragraphs [0009] to [0016] (Family: none)	1-7
A	JP 2004-326689 A (Nissan Motor Co., Ltd.), 18 November 2004 (18.11.2004), claim 2; paragraphs [0011] to [0013], [0017], [0022] to [0027]; fig. 1 (Family: none)	1-7
A	JP 2003-019931 A (Denso Corp.), 21 January 2003 (21.01.2003), paragraphs [0034], [0048] to [0050]; fig. 1, 3 & US 2003/0009271 A1 & DE 10230351 A1	1-7

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
07 January 2015 (07.01.15)

Date of mailing of the international search report
20 January 2015 (20.01.15)

Name and mailing address of the ISA/
Japan Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/081139

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2013-137729 A (Autonetworks Technologies, Ltd.), 11 July 2013 (11.07.2013), paragraphs [0043] to [0052] (Family: none)	2

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F11/00(2006.01)i, B60R16/02(2006.01)i, G06F9/445(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. G06F11/00, B60R16/02, G06F9/445

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 2011-003020 A（株式会社トヨタ I T開発センター）2011.01.06, 段落【0009】－【0016】，（ファミリーなし）	1-7
A	JP 2004-326689 A（日産自動車株式会社）2004.11.18, 請求項2, 段落【0011】－【0013】，段落【0017】，段落【0022】－【0027】，第1図，（ファミリーなし）	1-7
A	JP 2003-019931 A（株式会社デンソー）2003.01.21, 段落【0034】，段落【0048】－【0050】，第1図，第3図 & US 2003/0009271 A1 & DE 10230351 A1	1-7

☒ 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

07.01.2015

国際調査報告の発送日

20.01.2015

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）

坂庭 剛史

5 B

5881

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
A	JP 2013-137729 A (株式会社オートネットワーク技術研究所) 2013.07.11, 段落【0043】－【0052】, (ファミリーなし)	2