(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5949732号
(P5949732)

(45)発行日　平成28年7月13日(2016.7.13)　(24)登録日　平成28年6月17日(2016.6.17)

(51)Int.Cl.		F I		
G06F 11/00	(2006.01)	G06F	9/06	630A
G06F 9/445	(2006.01)	G06F	9/06	610Q
G06F 21/12	(2013.01)	G06F	21/12	
B60R 16/02	(2006.01)	B60R	16/02	660U

請求項の数 7　(全 14 頁)

(21)出願番号　特願2013-245083(P2013-245083)
(22)出願日　平成25年11月27日(2013.11.27)
(65)公開番号　特開2015-103163(P2015-103163A)
(43)公開日　平成27年6月4日(2015.6.4)
審査請求日　平成27年12月24日(2015.12.24)

(73)特許権者　395011665
株式会社オートネットワーク技術研究所
三重県四日市市西末広町１番１４号
(73)特許権者　000183406
住友電装株式会社
三重県四日市市西末広町１番１４号
(73)特許権者　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(74)代理人　100114557
弁理士　河野　英仁
(74)代理人　100078868
弁理士　河野　登夫

最終頁に続く

(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

(57)【特許請求の範囲】
【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。
【発明の詳細な説明】
【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、車輌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】

本発明にあっては、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】ＥＣＵ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ＥＣＵ３０，３０，…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ＥＣＵ３０，３０，…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ＥＣＵ３０へ送信すると共に、ＥＣＵ３０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】
ＣＰＵ１１は、記憶部１３に記憶された一又は複数のプログラムをＲＡＭ１２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。ＣＰＵ１１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。ＲＡＭ１２は、ＳＲＡＭ（Static ＲＡＭ）又はＤＲＡＭ（Dynamic RAM）等のメモリ素子で構成され、ＣＰＵ１１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、ＣＰＵ１１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ＥＣＵ３０，３０，…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、ＥＣＵ３０との通信を行う。車内通信部１４は、ＣＰＵ１１から与えられた情報を対象のＥＣＵ３０へ送信すると共に、ＥＣＵ３０から受信した情報をＣＰＵ１１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、ＣＰＵ１１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ＣＰＵ３１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ＲＳ２３２Ｃ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、ＣＰＵ１１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ＣＰＵ１１へ与える。

【００３２】

図３はＥＣＵ３０の内部構成を説明するブロック図である。ＥＣＵ３０は、例えば、ＣＰＵ３１、ＲＡＭ３２、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】

ＣＰＵ３１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ＲＡＭ３２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、ＥＣＵ３０を本発明に係る制御装置として機能させる。ＲＡＭ３２は、ＳＲＡＭ又はＤＲＡＭ等のメモリ素子で構成され、ＣＰＵ３１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ＣＰＵ３１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、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、ＣＰＵ３１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ＣＰＵ３１へ与える。通信部３４は、上記通信規格だけなく、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、ＣＰＵ５１、ＲＯＭ５２、ＲＡＭ５３、記憶部５４、通信部５５等を備える。

【００３７】

ＣＰＵ５１は、ＲＯＭ５２に予め記憶された一又は複数のプログラムをＲＡＭ５３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。ＲＡＭ５３は、ＳＲＡＭ又はＤＲＡＭ等のメモリ素子で構成され、ＣＰＵ５１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（Ｓ１１：ＹＥＳ）、ＣＰＵ５１は、送信すべき更新データを記憶部５４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ＯＥＭ（Original Equipment Manufacturer）毎の電子署名を付与する（ステップＳ１２）。次いで、ＣＰＵ５１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ＥＣＵ３０を備える車両１のゲートウェイ１０へ通信部５５を通じて送信する（ステップＳ１３）。

【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、ＥＣＵ３０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ＥＣＵ３０を特定する構成としたが、サーバ装置５の記憶部５４にて、車両１の車両番号、ＥＣＵ３０のシリアル番号、ＥＣＵ３０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ＥＣＵ３０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１０の無線通信部１５にて受信した場合（ステップＳ２１）、ゲートウェイ１０のＣＰＵ１１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Ｓ２２）。ゲートウェイ１０は、認証局又は各ＯＥＭ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（Ｓ２２：ＮＯ）、ＣＰＵ１１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（Ｓ２２：ＹＥＳ）、ＣＰＵ１１は、車内通信部１４を通じて更新対象のＥＣＵ３０へ送信する（ステップＳ２３）。

【００４７】

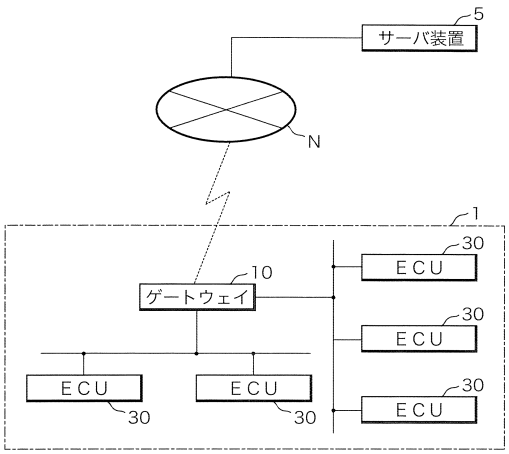
ゲートウェイ１０から送信される更新データをＥＣＵ３０の通信部３４にて受信した場合（ステップＳ２４）、ＥＣＵ３０のＣＰＵ３１は、受信した更新データに含まれる更新制御プログラムをＲＡＭ３２に読み込んで実行し、記憶部３３に記憶されている制御プログラムを更新する処理（リプログラミング）を実行する（ステップＳ２５）。

【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Ｓ２７で算出したダイジェスト値を通信部３４を通じてゲートウェイ１０へ送信する（ステップＳ２９）。また、自装置が正常に動作しなかった場合（Ｓ２８：ＮＯ）、ＣＰＵ３１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１０のＣＰＵ１１は、ＥＣＵ３０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１４にて受信した場合（ステップＳ３０）、受信したダイジェスト値を暗号化し（ステップＳ３１）、暗号化したダイジェスト値を無線通信部１５を通じてサーバ装置５へ送信する（ステップＳ３２）。
【００５３】
なお、本実施の形態では、ＥＣＵ３０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１０へ送信する構成としたが、ＥＣＵ３０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１０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１０は、ＥＣＵ３０から正常に動作する旨の返答を受信したとき、ステップＳ２１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ＣＰＵ５１は、車両１のゲートウェイ１０から送信される暗号化済みのダイジェスト値を通信部５５にて受信した場合（ステップＳ４１）、暗号化済みのダイジェスト値を復号する（ステップＳ４２）。なお、ゲートウェイ１０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。

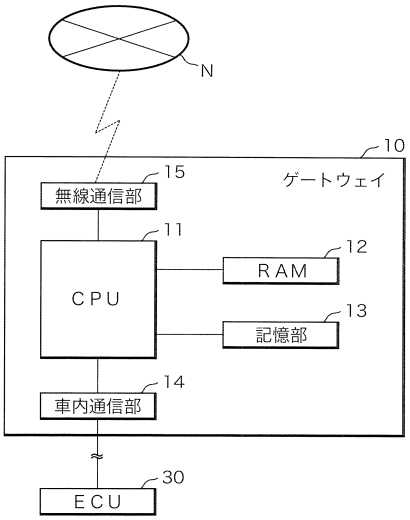
【００５５】
次いで、サーバ装置５のＣＰＵ５１は、復号したダイジェスト値と、記憶部５４に予め記憶してある期待値とを比較し（ステップＳ４３）、両者が一致するか否かを判断する（ステップＳ４４）。
【００５６】
両者が一致すると判断した場合（Ｓ４４：ＹＥＳ）、ＣＰＵ５１は、更新対象のＥＣＵ３０において制御プログラムの更新が正常に終了したと判定する（ステップＳ４５）。また、両者が一致しないと判断した場合（Ｓ４４：ＮＯ）、ＣＰＵ５１は、ＥＣＵ３０における制御プログラムの更新が正常でなかったと判定する（ステップＳ４６）。
【００５７】
ＥＣＵ３０における制御プログラムの更新が正常でなかった場合、サーバ装置５は、記憶部５４に記憶してある更新データをＥＣＵ３０へ再送する構成としてもよい。
【００５８】
また、ＥＣＵ３０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ＥＣＵ３０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してもよい。
【００５９】
更に、ＥＣＵ３０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１０を介してＥＣＵ３０へ送信し、ＥＣＵ３０の記憶部３３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５４、ゲートウェイ１０の記憶部１３、及びＥＣＵ３０の記憶部３３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ＥＣＵ３０が受信した場合、自身の記憶部３３、ゲートウェイ１０の記憶部１３、及びサーバ装置５の記憶部５４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１０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ＥＣＵ３０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、特許請求の範囲によって示され、特許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

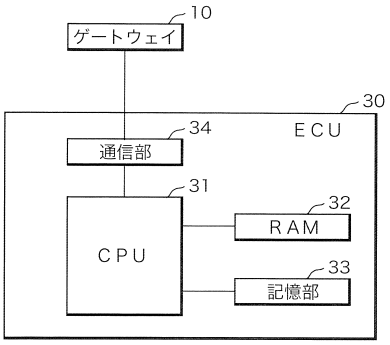
【図１】



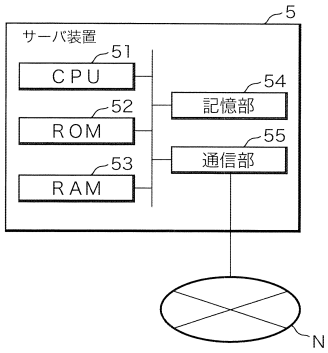
【図２】



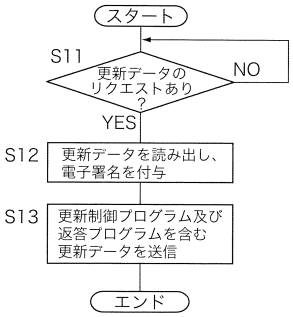
【図３】


10
ゲートウェイ
30
ECU
34
通信部
31
CPU
32
RAM
33
記憶部

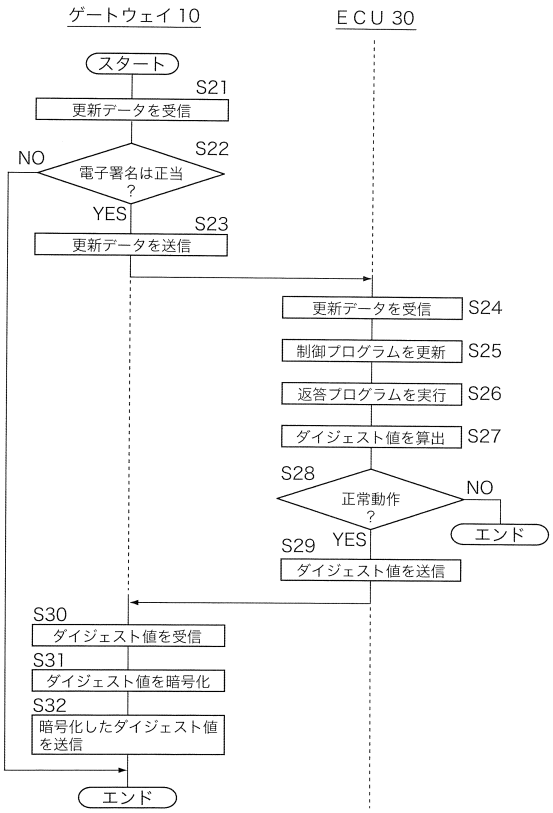
【図４】


5
サーバ装置
51
CPU
52
ROM
53
RAM
54
記憶部
55
通信部
N

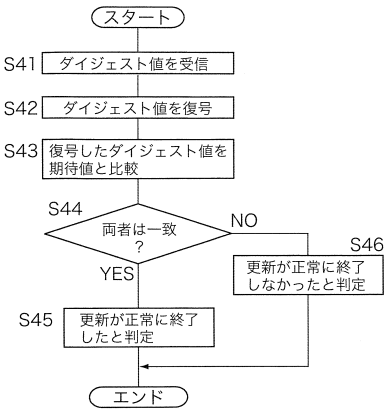
【図５】


スタート
S11
更新データの
リクエストあり
？
NO
YES
S12
更新データを読み出し、
電子署名を付与
S13
更新制御プログラム及び
返答プログラムを含む
更新データを送信
エンド

【図６】


ゲートウェイ 10
ECU 30
スタート
S21
更新データを受信
NO
S22
電子署名は正当
？
YES
S23
更新データを送信
更新データを受信
S24
制御プログラムを更新
S25
返答プログラムを実行
S26
ダイジェスト値を算出
S27
S28
正常動作
？
NO
エンド
YES
S29
ダイジェスト値を送信
S30
ダイジェスト値を受信
S31
ダイジェスト値を暗号化
S32
暗号化したダイジェスト値
を送信
エンド

【図７】


スタート
S41
ダイジェスト値を受信
S42
ダイジェスト値を復号
S43
復号したダイジェスト値を
期待値と比較
S44
両者は一致
？
NO
S46
更新が正常に終了
しなかったと判定
YES
S45
更新が正常に終了
したと判定
エンド

フロントページの続き

(72)発明者　足立　直樹
三重県四日市市西末広町１番１４号　株式会社オートネットワーク技術研究所内
(72)発明者　宇佐美　彰規
三重県四日市市西末広町１番１４号　株式会社オートネットワーク技術研究所内
(72)発明者　渡部　正志
三重県四日市市西末広町１番１４号　株式会社オートネットワーク技術研究所内
(72)発明者　野田　哲矢
三重県四日市市西末広町１番１４号　株式会社オートネットワーク技術研究所内

審査官　漆原　孝治

(56)参考文献　特開２０１１－００３０２０（ＪＰ，Ａ）
特開２００４－３２６６８９（ＪＰ，Ａ）
特開２００３－０１９９３１（ＪＰ，Ａ）
特開２０１３－１３７７２９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１１／００
Ｂ６０Ｒ　１６／０２
Ｇ０６Ｆ　９／４４５
Ｇ０６Ｆ　２１／１２