(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7111030号
(P7111030)

(45)発行日　令和4年8月2日(2022.8.2)

(24)登録日　令和4年7月25日(2022.7.25)

(51)国際特許分類
Ｂ６０Ｒ　16/02　(2006.01)

ＦＩ
Ｂ６０Ｒ　16/02　６６０Ｕ
Ｂ６０Ｒ　16/02　６６０Ｗ

請求項の数　7　（全15頁）

(21)出願番号　特願2019-38882(P2019-38882)
(22)出願日　平成31年3月4日(2019.3.4)
(65)公開番号　特開2020-142565(P2020-142565A)
(43)公開日　令和2年9月10日(2020.9.10)
審査請求日　令和3年6月25日(2021.6.25)

(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
(72)発明者　小林 拓也

最終頁に続く

(54)【発明の名称】　車載更新装置、更新処理プログラム及び、プログラムの更新方法

(57)【特許請求の範囲】
【請求項１】
車外の外部サーバから送信される更新プログラムを取得し、車両に搭載される車載制御装置のプログラムを更新するための処理を行う車載更新装置であって、
記憶部と、制御部とを備え、
前記記憶部には、取得した前記更新プログラムが記憶され、
前記制御部は、取得した前記更新プログラムの前記車載制御装置への送信を制御するものであり、
前記制御部は、前記車両の停止により、前記送信が中断され、
前記中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、
比較結果に基づいて前記記憶部に記憶されている前記更新プログラムの正当性に関し、前記中断の間に前記更新プログラムが変更されたか否かを判定する
車載更新装置。
【請求項２】
前記中断の前後における前記導出値それぞれが異なる場合は、
前記制御部は、前記記憶部に記憶されている前記更新プログラムが不正であると判定し、
前記外部サーバから前記更新プログラムを最初から取得する
請求項１に記載の車載更新装置。
【請求項３】

前記中断の前後における前記導出値それぞれが同一である場合は、
前記制御部は、前記記憶部に記憶されている前記更新プログラムが正当であると判定し、
中断ポイントから前記送信を再開する
請求項１又は請求項２に記載の車載更新装置。
【請求項４】
前記中断ポイントは、取得した前記更新プログラムに含まれるチェックポイントに基づいて導出される
請求項３に記載の車載更新装置。
【請求項５】
前記更新プログラムの最後のブロックが前記車載制御装置に送信された後、前記制御部は前記記憶部に記憶されている前記更新プログラムを前記記憶部から消去する
請求項１から請求項４のいずれか１項に記載の車載更新装置。
【請求項６】
コンピュータに、
車外の外部サーバから送信される更新プログラムを取得し、
取得した該更新プログラムを記憶部に記憶し、
前記更新プログラムを車載制御装置へ送信し、
前記送信の中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、
比較結果に基づいて前記記憶部に記憶されている前記更新プログラムの正当性に関し、前記中断の間に前記更新プログラムが変更されたか否かを判定する
処理を実行させる更新処理プログラム。
【請求項７】
車外の外部サーバから送信される更新プログラムを取得し、
取得した該更新プログラムを記憶部に記憶し、
前記更新プログラムを車載制御装置へ送信し、
前記送信の中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、
比較結果に基づいて前記記憶部に記憶されている前記更新プログラムの正当性に関し、前記中断の間に前記更新プログラムが変更されたか否かを判定する
プログラムの更新方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、車載更新装置、更新処理プログラム及び、プログラムの更新方法に関する。
【背景技術】
【０００２】
車両には、エンジン制御等のパワー・トレーン系、エアコン制御等のボディ系統の車載機器を制御するための車載制御装置、例えば車載ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）が搭載されている。車載制御装置は、ＭＰＵ（Ｍｉｃｒｏ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）等の演算処理部、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）等の書き換え可能な不揮発性の記憶部、及び他の車載制御装置と通信するための通信部を含み、記憶部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、車載機器の制御を行う。更に車両には、無線通信の機能を備えた中継装置（車載更新装置）が実装されている。中継装置は、車外のネットワークに接続されている外部サーバ等のプログラム提供装置と通信し、当該プログラム提供装置から車載制御装置の制御プログラムをダウンロード（受信）する。ダウンロードされたプログラムは中継装置の記憶部に記憶される。記憶部に記憶されたプログラムは当該車載制御装置へと送信され、当該車載制御装置の制御プログラムは更新（リプログラミング、リプロ）される。（特許文献１参照）
【先行技術文献】

【特許文献】
【０００３】
【文献】特開２０１７－９７８５１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
車載更新装置が外部サーバからプログラムを取得し、プログラムがリプロ対象となる車載制御装置に送信されるまでの間にリプログラミングが中断されると、中断の間に車載更新装置の記憶部に記憶されているプログラムは改竄され、不正なプログラムとなるおそれがある。しかしながら、特許文献１は、前述の中断が生じた場合における車載更新装置の記憶部に記憶されているプログラムの正当性に関する点が考慮されていない。
【０００５】
本開示は斯かる事情に鑑みてなされたものであり、その目的とするところは、車載更新装置の記憶部に記憶されているプログラムの正当性を担保することができる車載更新装置等を提供することにある。
【課題を解決するための手段】
【０００６】
本開示の一態様に係る車載更新装置は、車外の外部サーバから送信される更新プログラムを取得し、車両に搭載される車載制御装置のプログラムを更新するための処理を行う車載更新装置であって、記憶部と、制御部とを備え、前記記憶部には、取得した前記更新プログラムが記憶され、前記制御部は、取得した前記更新プログラムの前記車載制御装置への送信を制御するものであり、前記制御部は、前記車両の停止により、前記送信が中断され、前記中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、比較結果に基づいて前記記憶部に記憶されている前記更新プログラムの正当性に関し、前記中断の間に前記更新プログラムが変更されたか否かを判定する。
【発明の効果】
【０００７】
本開示の一態様によれば、車載更新装置の記憶部に記憶されているプログラムの正当性を担保することができる車載更新装置を提供できる。
【図面の簡単な説明】
【０００８】
【図１】実施形態１に係る車載更新システムの構成を示す模式図である。
【図２】実施形態１に係る車載更新装置等の構成を示すブロック図である。
【図３】車載更新装置の制御部の処理を例示するフローチャートである。
【図４】プログラム提供装置、車載更新装置、及び車載制御装置の間で送受信される通信信号及び更新プログラムを示すシーケンス図である。
【発明を実施するための形態】
【０００９】
[本開示の実施形態の説明]
最初に本開示の実施態様を列挙して説明する。また、以下に記載する実施形態の少なくとも一部を任意に組み合わせてもよい。
【００１０】
（１）本開示の一態様に係る車載更新装置は、車外の外部サーバから送信される更新プログラムを取得し、車両に搭載される車載制御装置のプログラムを更新するための処理を行う車載更新装置であって、記憶部と、制御部とを備え、前記記憶部には、取得した前記更新プログラムが記憶され、前記制御部は、取得した前記更新プログラムの前記車載制御装置への送信を制御するものであり、前記制御部は、前記車両の停止により、前記送信が中断され、前記中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、比較結果に基づいて前記記憶部に記憶されてい

る前記更新プログラムの正当性を判定する。
【００１１】
本態様にあたっては、記憶部に記憶された更新プログラムの車載制御装置への送信が中断された後に再開されるにあたって、制御部は記憶部に記憶された更新プログラムの正当性を判定する。従って、前記送信を再開する際に、記憶部に記憶されている更新プログラムの正当性を担保することができる。例えば、中断の間に更新プログラムが不正に変更されていないことを担保できる。
【００１２】
（２）本開示の一態様に係る車載更新装置は、前記中断の前後における前記導出値それぞれが異なる場合は、前記制御部は、前記記憶部に記憶されている前記更新プログラムが不正であると判定し、前記外部サーバから前記更新プログラムを最初から取得する。
【００１３】
本態様にあたっては、制御部は、記憶部に記憶されている更新プログラムを不正と判定した場合に、外部サーバから更新プログラムを最初から取得して車載制御装置の更新を再開する。従って、不正な更新プログラムが車載制御装置へと送信されることを防止することができる。
【００１４】
（３）本開示の一態様に係る車載更新装置は、前記中断の前後における前記導出値それぞれが同一である場合は、前記制御部は、前記記憶部に記憶されている前記更新プログラムが正当であると判定し、中断ポイントから前記送信を再開する。
【００１５】
本態様にあたっては、制御部は、記憶部に記憶されている更新プログラムを正当と判断した場合に、記憶部に記憶されている更新プログラムを用いて車載制御装置の更新を再開する。従って、記憶部に記憶されている更新プログラムの適正性を担保したうえで、更新プログラムを再度取得することを不要とし、取得するための通信コスト及び処理時間を削減することができる。
【００１６】
（４）本開示の一態様に係る車載更新装置は、前記中断ポイントは、取得した前記更新プログラムに含まれるチェックポイントに基づいて導出される。
【００１７】
本態様にあたっては、更新プログラムに含まれるチェックポイントから導出される中断ポイントから、車載制御装置の更新が再開される。従って、効率的に更新が再開される。
【００１８】
（５）本開示の一態様に係る車載更新装置は、前記更新プログラムが前記車載制御装置に送信された後、前記制御部は前記記憶部に記憶されている前記更新プログラムを前記記憶部から消去する。
【００１９】
本態様にあたっては、更新プログラムが車載制御装置に送信された後、記憶部に記憶されている更新プログラムが消去されるので、記憶部が更新プログラムによって圧迫されることを防止することができる。
【００２０】
（６）本開示の一態様に係る更新処理プログラムは、コンピュータに、車外の外部サーバから送信される更新プログラムを取得し、取得した該更新プログラムを記憶部に記憶し、前記更新プログラムを車載制御装置へ送信し、前記送信の中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、比較結果に基づいて前記記憶部に記憶されている前記更新プログラムの正当性を判定する処理を実行させる。
【００２１】
本態様にあたっては、コンピュータを、本開示の一態様の車載更新装置として機能させることができる。

【００２２】
（７）本開示の一態様に係るプログラムの更新方法は、車外の外部サーバから送信される更新プログラムを取得し、取得した該更新プログラムを記憶部に記憶し、前記更新プログラムを車載制御装置へ送信し、前記送信の中断の前後における前記記憶部に記憶されている前記更新プログラムに基づいて導出される導出値それぞれを比較し、比較結果に基づいて前記記憶部に記憶されている前記更新プログラムの正当性を判定する。
【００２３】
本態様にあたっては、記憶部に記憶された更新プログラムの車載制御装置への送信が中断された後に再開されるにあたって、記憶部に記憶された更新プログラムの正当性が判定される。従って、前記送信を再開する際に、記憶部に記憶されている更新プログラムの正当性を担保することができるプログラムの更新方法を提供することができる。
【００２４】
[本開示の実施形態の詳細]
本開示をその実施形態を示す図面に基づいて具体的に説明する。本開示の実施形態に係る車載更新装置２を、以下に図面を参照しつつ説明する。なお、本開示はこれらの例示に限定されるものではなく、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すべての変更が含まれることが意図される。
【００２５】
（実施形態１）
以下、実施の形態について図面に基づいて説明する。図１は、実施形態１に係る車載更新システムＳの構成を示す模式図である。図２は、実施形態１に係る車載更新装置２等の構成を示すブロック図である。車載更新システムＳは、車両Ｃに搭載された車外通信装置１及び車載更新装置２を含み、車外ネットワークＮを介して接続されたプログラム提供装置Ｓ１から取得したプログラム又はデータを、車両Ｃに搭載されている車載制御装置３に送信する。
【００２６】
プログラム提供装置Ｓ１は、例えばインターネット又は公衆回線網等の車外ネットワークＮに接続されているサーバ等のコンピュータであり、ＲＡＭ、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）又はハードディスク等による記憶部Ｓ１１を備え、車外の外部サーバに相当する。プログラム提供装置Ｓ１の記憶部Ｓ１１には、車載制御装置３の製造メーカ等によって作成された当該車載制御装置３を制御するためのプログラム又はデータが保存されている。当該プログラム又はデータは、更新プログラムとして、後述のごとく車両Ｃに送信され、車両Ｃに搭載されている車載制御装置３のプログラム又はデータを更新するために用いられる。このように構成されたプログラム提供装置Ｓ１（外部サーバ）は、ＯＴＡ（Ｏｖｅｒ Ｔｈｅ Ａｉｒ）サーバとも称される。車両Ｃに搭載される車載制御装置３は、プログラム提供装置Ｓ１から無線通信により送信された更新プログラムを取得し、当該更新プログラムが実行するプログラムとして適用されることにより、自制御装置が実行するプログラムを更新（リプロ）することができる。
【００２７】
以降、プログラムは、車載制御装置３が処理を行うための制御構文等を含むプログラムコード及び、当該プログラムコードを実行するにあたり参照するデータが記載される外部ファイルを含むものとして説明する。更新プログラムの送信時において、これらプログラムコード及びデータが記載される外部ファイルは、例えば暗号化されたアーカイブファイルとして、プログラム提供装置Ｓ１から送信される。
【００２８】
車両Ｃには、車外通信装置１、車載更新装置２、表示装置５、ＩＧ（イグニッション）スイッチ６、及び種々の車載機器を制御するための複数の車載制御装置３が搭載されている。車外通信装置１と車載更新装置２とは、例えばシリアルケーブル等のハーネスにより通信可能に接続されている。車載更新装置２及び車載制御装置３は、ＣＡＮ（Ｃｏｎｔｒｏｌ Ａｒｅａ Ｎｅｔｗｏｒｋ／登録商標）又はＥｔｈｅｒｎｅｔ（登録商標）等の通信

プロトコルに対応した車内ＬＡＮ４によって通信可能に接続されている。

【００２９】

車外通信装置１は、車外通信部１１及び、車載更新装置２と通信するための入出力Ｉ／Ｆ（インターフェイス）１２を含む。車外通信部１１は、３Ｇ、ＬＴＥ、４Ｇ、ＷｉＦｉ等の移動体通信のプロトコルを用いて無線通信をするための通信装置であり、車外通信部１１に接続されたアンテナ１３を介してプログラム提供装置Ｓ１とデータの送受信を行う。車外通信装置１とプログラム提供装置Ｓ１との通信は、例えば公衆回線網又はインターネット等の外部ネットワークを介して行われる。

【００３０】

入出力Ｉ／Ｆ１２は、車外通信装置１と車載更新装置２とが、例えばシリアル通信をするための通信インターフェイスである。車外通信装置１と車載更新装置２とは、入出力Ｉ／Ｆ１２及び車載更新装置２が備えている入出力Ｉ／Ｆ２４に接続されたシリアルケーブル等のハーネスを介して相互に通信する。本実施形態では、車外通信装置１は、車載更新装置２と別装置とし、入出力Ｉ／Ｆ１２等によってこれら装置を通信可能に接続しているが、これに限定されない。車外通信装置１は、車載更新装置２の一構成部位として、車載更新装置２に内蔵されるものであってもよい。

【００３１】

車載更新装置２は、制御部２０、記憶部２１及び車内通信部２３を含む。車載更新装置２は、車外通信装置１が無線通信によってプログラム提供装置Ｓ１から受信した更新プログラムを、車外通信装置1から取得し、車内ＬＡＮ４を介して当該更新プログラムを所定（更新対象）の車載制御装置３に送信するように構成されている。車載更新装置２は、例えば、制御系の車載制御装置３、安全系の車載制御装置３及び、ボディ系の車載制御装置３等の複数の系統のセグメントを統括し、これらセグメント間での車載制御装置３同士の通信を中継するゲートウェイ（中継器）である。又は、車載更新装置２は、車両Ｃ全体をコントロールするボディＥＣＵの一機能部として構成されるものであってもよい。

【００３２】

制御部２０は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）又はＭＰＵ等により構成してあり、記憶部２１に予め記憶された制御プログラム及びデータを読み出して実行することにより、種々の制御処理及び演算処理等を行うようにしてある。制御部２０は、車内通信部２３を介して車載制御装置３へと更新プログラムを送信する。制御部２０は、記憶部２１に記憶されている更新プログラムを基にした導出値の導出、及び導出された導出値を比較して記憶部２１に記憶されている更新プログラムの正当性の判定を行う。制御部２０は、記憶部２１に記憶されている更新プログラムの消去を行う。

【００３３】

記憶部２１は、ＲＡＭ等の揮発性のメモリ素子又は、ＲＯＭ、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）若しくはフラッシュメモリ等の不揮発性のメモリ素子により構成してあり、制御プログラム及び処理時に参照するデータがあらかじめ記憶されてある。記憶部２１に記憶された制御プログラムは、車載更新装置２が読み取り可能な記録媒体２２から読み出された制御プログラムを記憶したものであってもよい。また、図示しない通信網に接続されている図示しない外部コンピュータから制御プログラムをダウンロードし、記憶部２１に記憶させたものであってもよい。詳細は後述するが、記憶部２１には、導出値を導出するためのプログラム又はデータが記憶されており、プログラム提供装置Ｓ１から取得した更新プログラムが記憶される。

【００３４】

車内通信部２３は、ＣＡＮ（登録商標）、又はＥｔｈｅｒｎｅｔ（登録商標）等の通信プロトコルを用いた入出力インターフェイスであり、制御部２０は、車内通信部２３を介して車内ＬＡＮ４に接続されている車載制御装置３又は他の中継装置等の車載機器と相互に通信する。車内通信部２３は、複数個（図面上では３つ）設けられており、車内通信部２３それぞれに、車内ＬＡＮ４を構成する通信線が接続されている。このように車内通信

部２３を複数個設けることにより、車内ＬＡＮ４は複数のセグメントに分けられ、各セグメントそれぞれに車載制御装置３が、当該車載制御装置３の機能（制御系機能、安全系機能、ボディ系機能）に応じて接続される。

【００３５】

車載制御装置３は、制御部３０、記憶部３１及び車内通信部３２を含む。記憶部３１は、ＲＡＭ等の揮発性メモリ素子又は、ＲＯＭ、ＥＥＰＲＯＭ若しくはフラッシュメモリ等の不揮発性のメモリ素子により構成してあり、車載制御装置３のプログラム又はデータが記憶されてある。このプログラム又はデータが、車載更新装置２から送信される更新プログラムによって更新される対象である。

【００３６】

記憶部３１は、第１記憶領域（第１面）３１１及び第２記憶領域（第２面）３１２を含む。記憶部３１には、現状において車載制御装置３が実行（適用）しているプログラム（現バージョン）及び、現バージョンの以前に適用されていたプログラム（旧バージョン）の２つのプログラムが記憶されている。これら現バージョンのプログラムと、旧バージョンのプログラムとは、第１記憶領域３１１又は第２記憶領域３１２のいずれかの記憶領域に分かれて、記憶されている。すなわち、第１記憶領域３１１に現バージョンのプログラムが記憶されている場合、第２記憶領域３１２に旧バージョンのプログラムが記憶されている。第１記憶領域３１１に旧バージョンのプログラムが記憶されている場合、第２記憶領域３１２に現バージョンのプログラムが記憶されている。このように現バージョン及び旧バージョンの２つのプログラムを、いわゆる２面持ちとして記憶することにより、万が一現バージョンのプログラムに問題が生じた場合であっても、制御部３０は、以前に適用して正常に動作していた旧バージョンのプログラムを読み込み実行する（切替える）ことで、車載制御装置３の信頼性を担保することができる。

【００３７】

記憶部３１には、現バージョン及び旧バージョンの２つのプログラムそれぞれのバージョンに関する情報、及び現在実行（適用）しているプログラムが記憶されている領域（動作面）に関する情報が記憶されている。すなわち、現状において第１記憶領域（第１面）３１１に記憶されているプログラムを実行している場合、記憶部３１には、動作面は第１記憶領域（第１面）３１１であると記憶される。現状において第２記憶領域（第２面）３１２に記憶されているプログラムを実行している場合、記憶部３１には、動作面は第２記憶領域（第２面）３１２であると記憶される。記憶部３１には、プログラム（現バージョン及び旧バージョン）のバージョン情報及び動作面に関する情報が記憶される。

【００３８】

制御部３０は、ＣＰＵ又はＭＰＵ等により構成してあり、記憶部３１（動作面）に記憶されたプログラム及びデータを読み出し実行して制御処理等を行い、当該車載制御装置３を含む車載機器又はアクチュエータ等が制御される。

【００３９】

車載制御装置３の制御部３０は、車載更新装置２から送信される更新プログラムを、車内通信部３２を介して受信し、当該更新プログラムを取得する。従って、車載制御装置３の制御部３０は、プログラム提供装置Ｓ１から送信された更新プログラムを、車外通信装置１及び車載更新装置２を介して取得する。制御部３０は、取得した更新プログラムを、動作面でない記憶領域（第１記憶領域３１１又は第２記憶領域３１２）に記憶する。すなわち、制御部３０は、車載更新装置２から送信された更新プログラムを取得するにあたり、当該取得の準備処理として、動作面でない記憶領域（非動作面）に記憶されているプログラムを消去する。通常、動作面でない記憶領域に記憶されているプログラムは、現バージョンのプログラムの以前に実行された旧バージョンのプログラムであるため、制御部３０は車載制御装置３における車載装置への制御機能を停止させることなく、当該旧バージョンのプログラムを消去し、車載更新装置２から送信さえた更新プログラムを、当該非動作面に記憶する。

【００４０】

詳細は後述するが、車載更新装置２によるプログラム提供装置Ｓ１からの更新プログラムの取得、及び車載更新装置２から車載制御装置３への更新プログラムの送信は、当該更新プログラムを、例えば所定のデータサイズで分割したブロック単位で行われる。取得及び送信されるブロックそれぞれには、当該ブロックを個々に識別するためのブロックＩＤが付与されており、車載更新装置２の制御部２０は、取得及び送信したブロックＩＤを記憶部２１に記憶することにより、ブロックＩＤをチェックポイントとして用いて前回の更新プログラムの取得及び送信が中断された中断ポイントを特定することができる。車載制御装置３の制御部３０が、受信したブロックＩＤを記憶部３１に記憶してもよい。

【００４１】

車載制御装置３の制御部３０は、更新プログラムの受信を正常終了、すなわち分割されたすべてのブロックの受信を正常終了した後、動作面の切替えを行い、受信した更新プログラムを現バージョンのプログラムとして適用して実行する。制御部３０は、更新プログラムの受信を正常終了し、動作面の切替えを正常に行った場合、プログラムの更新が完了（正常終了）したことを記憶部３１に記憶し、更に車載更新装置２に送信（通知）する。

【００４２】

車載制御装置３の制御部３０は、更新プログラムへの切替えが失敗した場合、ロールバック処理、すなわち更新プログラムの前バージョン（旧バージョン）のプログラムが記憶されている非動作面の記憶領域を、動作面の記憶領域として切替え（ロールバック）、当該前バージョンのプログラムを実行（適用）する。制御部３０は、更新プログラムへの切替えが失敗した場合、更新が失敗（異常終了）したことを記憶部３１に記憶し、更に車載更新装置２に送信（通知）してもよい。

【００４３】

表示装置５は、例えばカーナビゲーションのディスプレイ等のＨＭＩ（Ｈｕｍａｎ　Ｍａｃｈｉｎｅ　Ｉｎｔｅｒｆａｃｅ）装置である。表示装置５は、車載更新装置２の入出力Ｉ／Ｆ２４とシリアルケーブル等のハーネスにより通信可能に接続されている。表示装置５には、車載更新装置２の制御部２０から入出力Ｉ／Ｆ２４を介して出力されたデータ又は情報が表示される。表示装置５と車載更新装置２との接続形態は入出力Ｉ／Ｆ２４による接続形態に限定されず、表示装置５と車載更新装置２とは、車内ＬＡＮ４を介した接続形態であってもよい。

【００４４】

ＩＧスイッチ６は、車両Ｃのエンジン等の原動機（図示せず）の動作状態を切替えるスイッチである。例えばユーザはＩＧスイッチ６をオフからオンへ切替えて車両Ｃを起動し、車両Ｃの走行を開始する。その後、車両Ｃの走行を終えてユーザはＩＧスイッチ６をオンからオフへ切り替え、車両を停止する。ＩＧスイッチ６は、車載更新装置２の入出力Ｉ／Ｆ２４とシリアルケーブル等のハーネスにより通信可能に接続されている。入出力Ｉ／Ｆ２４を介して、車載更新装置２の制御部２０にＩＧスイッチ６の切替状態（オン又はオフ）が通知される。例えば、車載更新装置２の制御部２０には、入出力Ｉ／Ｆ２４を介して、ＩＧスイッチ６のオン又はオフを示す信号がＩＧスイッチ６から入力されている。ＩＧスイッチ６と車載更新装置２との接続形態は入出力Ｉ／Ｆ２４による接続形態に限定されず、ＩＧスイッチ６と車載更新装置２とは、車内ＬＡＮ４を介した接続形態であってもよい。

【００４５】

図３は、車載更新装置２の制御部２０の処理を例示するフローチャートである。図４はプログラム提供装置Ｓ１、車載更新装置２、及び車載制御装置３の間で送受信される通信信号及び更新プログラムを示すシーケンス図である。車載更新装置２の制御部２０は、車両Ｃが起動状態（ＩＧスイッチがオン）である場合、車外通信装置１を介してプログラム提供装置Ｓ１と定期的又は非定期的に通信し、更新すべきプログラム又はデータ、すなわち更新プログラムがプログラム提供装置Ｓ１に用意されている場合、以下の処理を行う。又は、制御部２０は、車外通信装置１を介して取得したプログラム提供装置Ｓ１からの更新通知に基づいて、以下の処理を行ってもよい。制御部２０は、更新通知を表示装置５に

表示させ、表示装置５が備えるタッチパネル等の入力端末を介して車両Ｃの操作者から入力された更新の承認に基づいて、以下の処理を行ってもよい。

【００４６】

車載更新装置２の制御部２０は、プログラム提供装置Ｓ１から更新情報が通知されると、プログラム提供装置Ｓ１に更新プログラムの送信を要求する。制御部２０は、プログラム提供装置Ｓ１から更新プログラムをブロック単位で取得（受信）し（Ｓ１１）、取得した更新プログラムをブロック単位で車載制御装置３へと送信する。詳しくは、制御部２０は、車外通信装置１を介して更新プログラムをブロック単位で取得し、取得した更新プログラムは記憶部２１に記憶される。記憶部２１に記憶された更新プログラムは、制御部２０により車内ＬＡＮ４を介してブロック単位で車載制御装置３へと送信される。取得する更新プログラムは、例えば共通鍵方式、又は公開鍵方式による暗号化等の秘匿化処理が施されていてもよい。暗号化された更新プログラムは記憶部２１に記憶され、制御部２０によって復号される。復号された更新プログラムは記憶部２１に記憶され、制御部２０によってブロック単位で車載制御装置３へと送信される。

【００４７】

車載更新装置２の制御部２０は、更新プログラムを所定のデータサイズで分割したブロック単位で車載制御装置３へと送信する。又は、制御部２０は、更新プログラムに含まれるセパレータを抽出し、当該セパレータに基づいて、更新プログラムを分割しブロックとしてもよい。制御部２０は、同様にして分割されたブロック単位で更新プログラムを取得する。ブロックにはブロックそれぞれを識別するためのブロックＩＤが付与される。制御部２０は、取得及び送信したブロックのブロックＩＤを記憶部２１に記憶する。

【００４８】

車載更新装置２の制御部２０は、送信したブロックが、最後のブロックか否かを判定する。制御部２０は、例えば、更新プログラムを所定のデータサイズで分割してブロック化するにあたり、生成されるブロックの個数を確定する。当該確定したブロックの個数が、ブロックＩＤの末尾の番号となり、制御部２０は、今回送信するブロックのブロックＩＤが末尾の番号であるか否かにより、更新プログラムの送信を完了させるにあたり最後のブロックであるか否かを判定する。

【００４９】

送信したブロックが最後のブロックでない場合、車載更新装置２の制御部２０は、前回送信したブロックのブロックＩＤの次の順番となるブロックＩＤのブロックを送信する。制御部２０は、所定のデータサイズで分割された更新プログラムのブロックを、更新対象の車載制御装置３に順次送信する。

【００５０】

車載更新装置２から送信された更新プログラムのブロックを受信した更新対象の車載制御装置３は、当該ブロックを非動作面の記憶領域（第１記憶領域３１１又は第２記憶領域３１２）に記憶する。車載制御装置３は、受信したブロックのブロックＩＤを記憶部３１に記憶してもよい。

【００５１】

ブロック単位での更新プログラムの取得及び送信を順次行っている間に、車両Ｃが停止した、すなわちＩＧスイッチがオフとなった場合（Ｓ１２：ＹＥＳ）、当該ブロック単位の更新プログラムの取得及び送信は中断される。そして、車載更新装置２の記憶部２１には、更新プログラムと最後に取得及び送信したブロックのブロックＩＤの情報とが残っている。

【００５２】

車載更新装置２の制御部２０は、記憶されたブロックＩＤを更新プログラムの取得及び送信のチェックポイントとして用い、該チェックポイントに基づいて更新プログラムの取得及び送信が中断された中断ポイントを導出することができる。

【００５３】

更新プログラムは、複数のチェックポイント及び、当該更新プログラムのファイルの終

端を示す情報を示すＥＯＦ（Ｅｎｄ　Ｏｆ　Ｆｉｌｅ）が含まれていてもよい。制御部２０は、ＥＯＦから当該ファイルの先頭に遡ってチェックポイントを検出し、最初に検出（確認）されたチェックポイントに基づいて中断ポイントを導出するものあってもよい。チェックポイントは、例えば所定の文字コード、又は当該ファイル内でのセグメントを分割するセパレータを用いるものであってもよい。中断ポイントの導出はチェックポイントに基づく導出に限らず、制御部２０がプログラム提供装置Ｓ１と通信し、中断ポイントの導出を行ってもよい。

【００５４】

車載更新装置２の制御部２０は、車両Ｃの停止後に車載更新装置２の蓄電装置（図示せず）に蓄えられている電気を用いて、記憶部２１に記憶されている更新プログラムに基づいて第１導出値を導出する（Ｓ１３）。すなわち第１導出値は、更新プログラムの取得及び送信の中断前に記憶部２１に記憶されている更新プログラムに基づいて導出される導出値である。導出された第１導出値は、記憶部２１に記憶される。第１導出値は、例えば、ハッシュ値、又はＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ、メッセージ認証コード）値である。ハッシュ値である第１導出値は、記憶部２１に記憶されている更新プログラムに基づいて、記憶部２１に記憶されているハッシュ関数を用いて導出される。ＭＡＣ値である第１導出値は、記憶部２１に記憶されている更新プログラムに基づいて、記憶部２１に記憶されている共通鍵（共有鍵）及びＭＡＣアルゴリズムを用いて導出される。導出値の導出は制御部２０による導出に限らず、車載更新装置２が制御部２０と通信可能に接続された専用のプロセッサを備え、該プロセッサが導出値を導出してもよい。

【００５５】

車両Ｃが停止状態、すなわちＩＧスイッチがオンでない場合（Ｓ１４：ＮＯ）、車載更新装置２の制御部２０は再度Ｓ１４の判定を行うべくループ処理を行う。当該ループ処理を行うにあたって、制御部２０は、所定時間の待機処理（スリープ）を実行してもよい。

【００５６】

車両Ｃが再び起動状態、すなわちＩＧスイッチがオンとなる場合（Ｓ１４：ＹＥＳ）、車載更新装置２の制御部２０は、記憶部２１に記憶されている更新プログラムに基づいて第２導出値を導出する（Ｓ１５）。すなわち第２導出値は、更新プログラムの取得及び送信の中断後に記憶部２１に記憶されている更新プログラムに基づいて導出される。導出された第２導出値は、記憶部２１に記憶される。第２導出値は、前述の第１導出値と同じ方法で導出される導出値であり、例えば、ハッシュ値、又はＭＡＣ値である。

【００５７】

車載更新装置２の制御部２０は、記憶部２１に記憶されている第１導出値と第２導出値とを比較し、同じ値であるかを判定する（Ｓ１６）。第１導出値と第２導出値とが同一である場合、制御部２０は、記憶部２１に記憶されている更新プログラムが正当であると判定する。すなわち、記憶部２１に記憶されている更新プログラムは改竄等により変更されていないと判定される。中断の前後における記憶部２１に記憶されている更新プログラムに基づいて導出された導出値（第１導出値及び第２導出値）を比較することで、送信の再開前に記憶部２１に記憶されている更新プログラムの適正性を判定できる。

【００５８】

第１導出値と第２導出値とが同一である場合（Ｓ１６：ＹＥＳ）、制御部２０は、前述の中断ポイントから、更新（更新プログラムの取得及び送信）を再開する（Ｓ１７）。詳しくは、制御部２０は、プログラム提供装置Ｓ１へ、前回（中断前）の更新プログラムの取得において、最後に取得したブロックＩＤの次の順番となるブロックからの送信を要求し、ブロック単位での更新プログラムの取得を再開する。取得した更新プログラムは記憶部２１に記憶される。記憶部２１に記憶された更新プログラムは車載制御装置３へとブロック単位で送信される。又は、制御部２０は、前回の更新プログラムの送信において、最後に送信したブロックのブロックＩＤの次の順番となるブロックを車載制御装置３へと送信し、車載制御装置３へのブロック単位での更新プログラムの送信を再開する。すなわち

、車載制御装置３の更新を再開する。

【００５９】

中断ポイントから更新を再開することにより、前回の更新プログラムの取得及び送信において既に取得及び送信しているブロックを再度取得及び送信する処理を不要とし、更新の再開から完了までに要する所要時間の短縮、及び車内ＬＡＮ４におけるトラフィックが増加することを抑制できる。

【００６０】

車載更新装置２の制御部２０は、入出力Ｉ／Ｆ２４を介して、更新再開の通知を表示装置５に表示させ、車両Ｃの操作者に更新再開を報知する（Ｓ１８）。

【００６１】

第１導出値と第２導出値とが異なる場合（Ｓ１６：ＮＯ）、車載更新装置２の制御部２０は、記憶部２１に記憶されている更新プログラムが不正であると判定する。すなわち、記憶部２１に記憶されている更新プログラムは改竄等により不正に変更されたと判定される。従って、制御部２０は、正当な更新プログラムの送信のために、プログラム提供装置Ｓ１から更新プログラムを最初から取得する（Ｓ１６１）。詳しくは、制御部２０は、プログラム提供装置Ｓ１へ、最初のブロックＩＤを備えるブロックからの更新プログラムの送信を要求する。制御部２０は、プログラム提供装置Ｓ１からブロック単位で更新プログラムを取得し、取得した更新プログラムを記憶部２１に記憶する。記憶部２１に記憶されている更新プログラムは、ブロック単位で車載制御装置３へと送信される。最初から更新プログラムを取得することにより、不正に変更された更新プログラムが車載制御装置３へと送信されることを防止することができる。

【００６２】

車載更新装置２の制御部２０は、車両Ｃの停止中に更新プログラムが不正に変更されたことを入出力Ｉ／Ｆ２４を介して、表示装置５に表示し、車両Ｃの操作者に報知する（Ｓ１６２）。制御部２０は、更新プログラムを最初から取得することを表示装置５に表示させ、車両Ｃの操作者に報知してもよい。制御部２０は、記憶されている更新プログラムが不正に変更されたことをプログラム提供装置Ｓ１に送信（通知）してもよい。

【００６３】

送信した更新プログラムのブロックが最後のブロックである場合、車載更新装置２の制御部２０は、最後のブロックを送信することにより、車載制御装置３への更新プログラムの送信を終了する（Ｓ１９）。取得した更新プログラムを送信するので、最後のブロックを送信する前に、更新プログラムの取得が終了していることは言うまでもない。制御部２０は当該車載制御装置３の更新が完了したことを、記憶部２１に記憶する。図３においては省略しているが、更新プログラムの送信が終了する前に再び車両Ｃが停止状態（ＩＧスイッチ６がオフ）になった場合、Ｓ１３の処理を行う。

【００６４】

車載制御装置３は、車載更新装置２から送信された最後のブロックを受信した後、自制御装置の更新が完了したことを記憶部３１に記憶する。車載制御装置３は、最後のブロックを受信し、受信を完了した更新プログラムへの切替え、すなわち動作面を更新プログラムが記憶されている記憶領域に切り替えた後、更新プログラムへの切替えが完了したこと（更新完了）を車載更新装置２に送信（通知）する。車載更新装置２の制御部２０は、更新対象の車載制御装置３が更新プログラムへの切替えを完了したことを、記憶部２１に記憶してもよい。制御部２０は、更新対象の車載制御装置３の更新完了を、プログラム提供装置Ｓ１に送信（通知）する。制御部２０は、更新対象の車載制御装置３の更新完了を入出力Ｉ／Ｆ２４を介して表示装置５に表示させ、車両Ｃの操作者に報知してもよい。

【００６５】

制御部２０は、更新プログラムの送信が終了した後、記憶部２１に記憶されている更新プログラムを消去する（Ｓ２０）。更新プログラムの消去により、記憶部２１が更新プログラムによって圧迫されることを防止できる。

【００６６】

更新プログラムの取得又は送信の間、車両Ｃが起動状態である、すなわちＩＧスイッチがオフでない場合（Ｓ１２：ＮＯ）、制御部２０は再度Ｓ１２の判定を行うべくループ処理を行う。該ループ処理の間、制御部２０は更新プログラムの取得及び送信を継続し、更新プログラムの送信が完了した場合、制御部２０はＳ２０の処理を行ってもよい。

【００６７】

今回開示された実施形態はすべ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。本開示の範囲は、上記した意味ではなく、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すべての変更が含まれることが意図される。

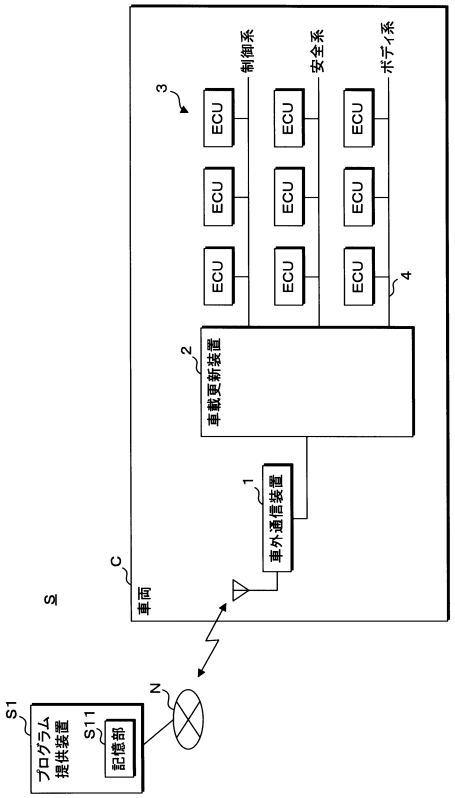
【符号の説明】

【００６８】

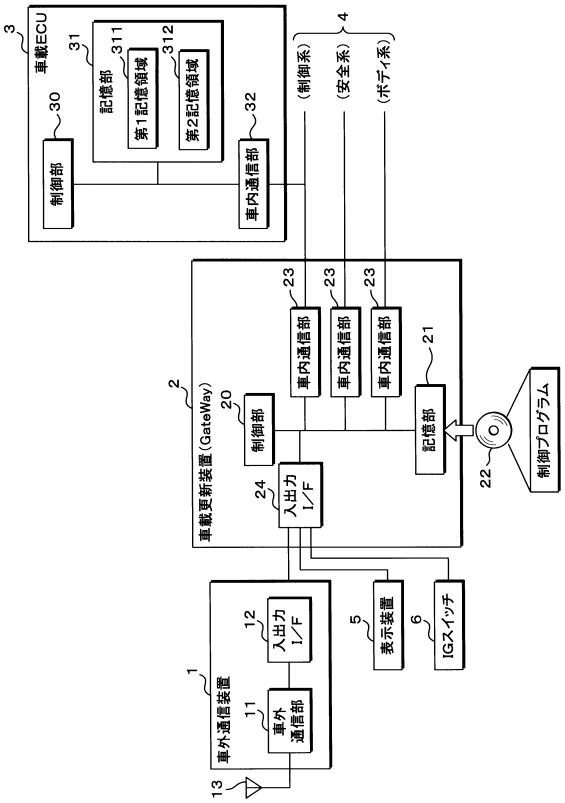
Ｃ　車両
Ｓ　車載更新システム
Ｓ１　プログラム提供装置（外部サーバ）
Ｓ１１　記憶部
１　車外通信装置
１１　車外通信部
１２　入出力Ｉ／Ｆ
１３　アンテナ
２　車載更新装置
２０　制御部
２１　記憶部
２２　記録媒体
２３　車内通信部
２４　入出力Ｉ／Ｆ
３　車載制御装置
３０　制御部
３１　記憶部
３１１　第１記憶領域
３１２　第２記憶領域
３２　車内通信部
４　車内ＬＡＮ
５　表示装置
６　ＩＧスイッチ
Ｎ　車外ネットワーク

【図面】

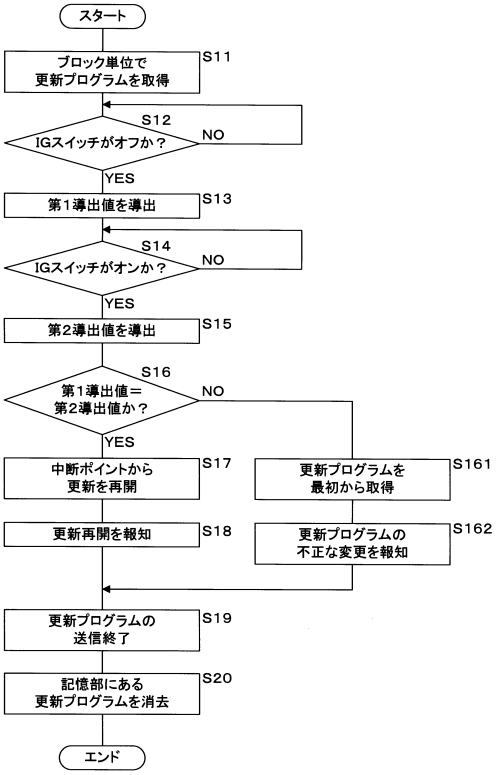
【図１】


S
C
車両
1
車外通信装置
2
車載更新装置
3
4
制御系
安全系
ボディ系
ECU
N
S1
プログラム提供装置
S11
記憶部

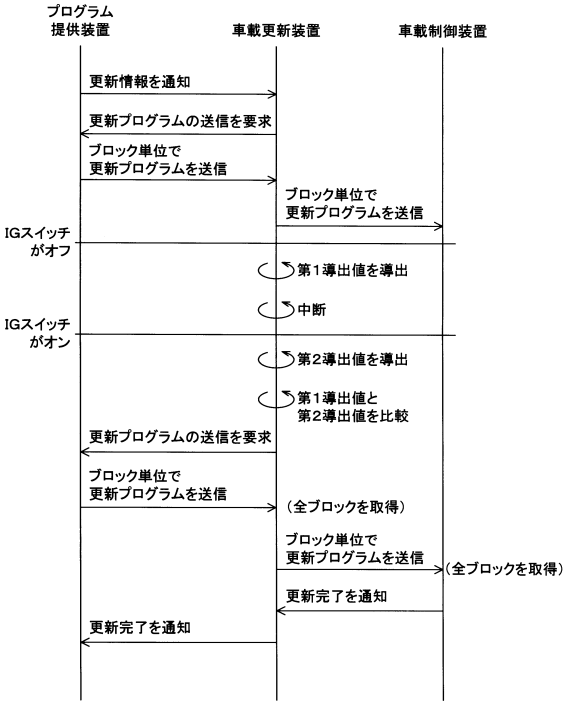
【図２】


3
車載ECU
30
制御部
31
記憶部
311
第1記憶領域
312
第2記憶領域
32
車内通信部
4
(制御系)
(安全系)
(ボディ系)
2
車載更新装置(GateWay)
20
制御部
23
車内通信部
21
記憶部
22
制御プログラム
24
入出力I/F
1
車外通信装置
12
入出力I/F
11
車外通信部
13
5
表示装置
6
IGスイッチ

【図３】


スタート
ブロック単位で
更新プログラムを取得
S11
S12
IGスイッチがオフか？
NO
YES
第１導出値を導出
S13
S14
IGスイッチがオンか？
NO
YES
第２導出値を導出
S15
S16
第１導出値＝
第２導出値か？
NO
YES
中断ポイントから
更新を再開
S17
更新プログラムを
最初から取得
S161
更新再開を報知
S18
更新プログラムの
不正な変更を報知
S162
更新プログラムの
送信終了
S19
記憶部にある
更新プログラムを消去
S20
エンド

【図４】


プログラム
提供装置
車載更新装置
車載制御装置
更新情報を通知
更新プログラムの送信を要求
ブロック単位で
更新プログラムを送信
ブロック単位で
更新プログラムを送信
IGスイッチ
がオフ
第１導出値を導出
中断
IGスイッチ
がオン
第２導出値を導出
第１導出値と
第２導出値を比較
更新プログラムの送信を要求
ブロック単位で
更新プログラムを送信
（全ブロックを取得）
ブロック単位で
更新プログラムを送信
（全ブロックを取得）
更新完了を通知
更新完了を通知

フロントページの続き

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　佐々木 智洋

(56)参考文献　特開２００７－０１１７３４（ＪＰ，Ａ）
特開２０１１－００３０２０（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｂ６０Ｒ　１６／０２
Ｇ０６Ｆ　１３／００