

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7421856号
(P7421856)

(45)発行日 令和6年1月25日(2024.1.25)

(24)登録日 令和6年1月17日(2024.1.17)

(51)国際特許分類		F I		
G 0 8 G	1/09 (2006.01)	G 0 8 G	1/09	F
G 0 6 F	21/44 (2013.01)	G 0 6 F	21/44	
G 0 8 G	1/00 (2006.01)	G 0 8 G	1/00	D
		G 0 8 G	1/00	X

請求項の数 10 (全33頁)

(21)出願番号	特願2018-84204(P2018-84204)	(73)特許権者	514136668
(22)出願日	平成30年4月25日(2018.4.25)		パナソニック インテレクチュアル プロ
(65)公開番号	特開2019-40588(P2019-40588A)		パティ コーポレーション オブ アメリカ
(43)公開日	平成31年3月14日(2019.3.14)		Panasonic Intellec
審査請求日	令和2年11月27日(2020.11.27)		tual Property Corpo
審査番号	不服2022-14298(P2022-14298/J		ration of America
	1)		アメリカ合衆国 9 0 5 0 4 カリフォル
審判請求日	令和4年9月12日(2022.9.12)		ニア州, トーランス, スイート 4 5 0
(31)優先権主張番号	62/549,156	(74)代理人	100109210
(32)優先日	平成29年8月23日(2017.8.23)		弁理士 新居 広守
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100137235
			弁理士 寺谷 英作
		(74)代理人	100131417
			弁理士 道坂 伸一

最終頁に続く

(54)【発明の名称】 運転管理システム、車両、及び、情報処理方法

(57)【特許請求の範囲】

【請求項1】

1以上の認証サーバと、手動運転及び自動運転が切り替え可能な1以上の車両とを備える運転管理システムであって、

前記1以上の車両のそれぞれは、

前記1以上の認証サーバの少なくとも一の認証サーバと通信を行う第1通信部と、

前記車両内に設けられた車載ネットワークに接続する複数の電子制御装置と、

前記複数の電子制御装置のうちの前記車両の運転アシスト部に接続された1以上の電子制御装置が、前記車両の運転モードが自動運転される自動運転モードと手動運転される手動運転モードとの間で切り替わった時に発するメッセージに基づき、手動運転モードと自動運転モードとの切り替えを検知する検知部と、

前記検知部が検知した切り替えを示す情報、前記検知部が切り替えを検知した時刻及び当該車両を示す第1の識別子を含む第1トランザクションデータをブロックチェーンのトランザクションデータとして生成し、前記第1通信部を介して前記一の認証サーバに送信するトランザクションデータ生成部と、

を備え、

前記少なくとも一の認証サーバのそれぞれは、

前記1以上の車両のそれぞれと通信を行う第2通信部と、

前記1以上の車両の少なくとも一の車両から取得した前記第1トランザクションデータを含むトランザクションデータの正当性を判断する検証部と、

前記検証部により正当性が確認された前記トランザクションデータをブロックチェーンのブロックで記憶装置に記録する記録部とを備える、
運転管理システム。

【請求項 2】

前記記録部は、前記 1 以上の車両のそれぞれを一意に識別する第 2 の識別子を前記記憶装置に予め記録しており、

前記検証部は、前記第 1 トランザクションデータに含まれる前記第 1 の識別子が、前記第 2 の識別子に含まれているかと、前記第 1 トランザクションデータの正当性を検証し、
前記記録部は、

前記検証部により、前記第 1 の識別子が前記第 2 の識別子に含まれていることが確認され、かつ、前記第 1 トランザクションデータの正当性が確認された場合、前記第 1 トランザクションデータを前記記憶装置に記録する、

請求項 1 に記載の運転管理システム。

【請求項 3】

前記 1 以上の車両のそれぞれは、さらに、

情報の入力を受け付ける入力部を備え、

前記入力部は、入力された情報であって、切り替わった自動運転モードが継続されることが承認された旨を示す情報を前記トランザクションデータ生成部に送信し、

前記トランザクションデータ生成部は、前記入力された情報を含む第 2 トランザクションデータを生成し、前記第 1 通信部を介して前記一の認証サーバに送信する、

請求項 1 または 2 に記載の運転管理システム。

【請求項 4】

前記トランザクションデータ生成部は、前記検知部が検知した切り替えを示す情報が手動運転モードから自動運転モードに切り替えられたことを示す場合、前記検知部が検知した切り替えを示す情報、及び、当該車両を示す第 1 の識別子に加えて、前記自動運転モードにおける自動運転レベルを示す情報を含む前記第 1 トランザクションデータを生成し、前記第 1 通信部を介して前記一の認証サーバに送信する、

請求項 1 ~ 3 のいずれか 1 項に記載の運転管理システム。

【請求項 5】

前記トランザクションデータ生成部は、前記検知部が検知した切り替えを示す情報が手動運転モードから自動運転モードに切り替えられたことを示す場合、前記検知部が検知した切り替えを示す情報、及び、当該車両を示す第 1 の識別子に加えて、前記自動運転モードにおいて動作する運転アシスト機能を示す情報を含む前記第 1 トランザクションデータを生成し、前記第 1 通信部を介して前記一の認証サーバに送信する、

請求項 1 ~ 4 のいずれか 1 項に記載の運転管理システム。

【請求項 6】

前記 1 以上の車両のそれぞれは、さらに、

所定期間毎またはイベント毎に、当該車両の運転者に関する情報を示すセンサ情報を取得するセンサ部を備え、

前記センサ部は、取得した前記センサ情報を前記トランザクションデータ生成部に送信し、

前記トランザクションデータ生成部は、前記切り替えを示す情報、前記第 1 の識別子、及び前記センサ情報を含む第 1 トランザクションデータを生成し、前記第 1 通信部を介して前記一の認証サーバに送信する、

請求項 1 ~ 5 のいずれか 1 項に記載の運転管理システム。

【請求項 7】

前記記録部は、前記 1 以上の車両のそれぞれを一意に識別する第 2 の識別子を前記記憶装置に予め記録しており、

前記検証部は、前記第 1 トランザクションデータに含まれる前記第 1 の識別子が、前記第 2 の識別子に含まれていない場合、前記第 1 の識別子が前記第 2 の識別子に含まれてい

10

20

30

40

50

ない旨を通知する、

請求項 1 ~ 6 のいずれか 1 項に記載の運転管理システム。

【請求項 8】

前記自動運転モードは、前記車両が自動的に駐車する駐車モードを含む、
請求項 1 ~ 7 のいずれか 1 項に記載の運転管理システム。

【請求項 9】

1 以上の認証サーバと手動運転と自動運転とが切り替え可能な 1 以上の車両とを備える運転管理システムにおける一の車両であって、

前記 1 以上の認証サーバの少なくとも一の認証サーバと通信を行う第 1 通信部と、

前記一の車両内に設けられた車載ネットワークに接続する複数の電子制御装置と、

前記複数の電子制御装置のうちの前記一の車両の運転アシスト部に接続された 1 以上の電子制御装置が、前記車両の運転モードが自動運転される自動運転モードと手動運転される手動運転モードとの間で切り替わった時に発するメッセージに基づき、手動運転される手動運転モードと自動運転される自動運転モードとの切り替えを検知する検知部と、

前記検知部が検知した切り替えを示す情報、前記検知部が切り替えを検知した時刻及び当該車両を示す第 1 の識別子を含む第 1 トランザクションデータをブロックチェーンのトランザクションデータとして生成し、前記第 1 通信部を介して前記一の認証サーバに送信するトランザクションデータ生成部と、を備える、

車両。

【請求項 10】

1 以上の認証サーバと、手動運転と自動運転とが切り替え可能な 1 以上の車両とを備える運転管理システムにおける一の認証サーバの情報処理方法であって、

前記一の認証サーバが、

前記 1 以上の車両のそれぞれと通信を行う通信ステップと、

前記 1 以上の車両のうちの一の車両から取得した第 1 トランザクションデータであって前記一の車両内に設けられた車載ネットワークに接続する複数の電子制御装置のうちの前記車両の運転アシスト部に接続された 1 以上の電子制御装置が、前記車両の運転モードが自動運転される自動運転モードと手動運転される手動運転モードとの間で切り替わった時に発するメッセージに基づき、手動運転される手動運転モードと自動運転される自動運転モードとの切り替えを示す情報、手動運転される手動運転モードと自動運転される自動運転モードとが切り替わった時刻及び当該車両を示す第 1 の識別子を含む第 1 トランザクションデータを含むブロックチェーンのトランザクションデータの正当性を検証する検証ステップと、

前記検証ステップにおいて前記トランザクションデータの正当性が確認されると前記トランザクションデータをブロックチェーンのブロックで記憶装置に記録する記録ステップとを含む、

情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、運転管理システム、車両、及び、情報処理方法に関する。

【背景技術】

【0002】

近年、自動車の走行制御を自動的に行う自動運転システムの研究開発が盛んに行われている。自動運転システムでは、自動車の中に配置された電子制御装置（以下、ECU：Electronic Control Unit）が連携して、走行制御が行われる。

【0003】

また、自動運転システムでは、運転者が運転するすなわち運転者が自動車の走行制御を行う手動運転モードと自動車が自律走行するすなわち自動車の走行制御を自動的に行う自動運転モードとを切り替えることで、安全な走行を担保する。

10

20

30

40

50

【 0 0 0 4 】

例えば、特許文献 1 には、交通法規に基づいてあらかじめ定められた切り替え条件に合致するかどうかを判断して、手動運転モードから自動運転モードに切り替える技術が開示されている。

【 先行技術文献 】

【 特許文献 】

【 0 0 0 5 】

【 文献 】特開 2 0 1 7 - 6 1 3 2 0 号公報

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 6 】

ところで、自動運転モード中において、自動車事故があった場合、運転者に責任がなく自動車自体に問題がある。

【 0 0 0 7 】

しかしながら、特許文献 1 に開示される技術では、当該自動車事故があった場合、自動運転モード中の事故であったか、手動運転モード中の事故であったかを客観的に判断できない。そのため、自動運転システムを実現する自動運転機能に問題があるか否かを検証できず、自動運転機能の改善を図れない。この結果、より安全な自動運転システムの構築を行えないという問題にも繋がる。

【 0 0 0 8 】

本開示は、上述の事情を鑑みてなされたもので、車両における運転モードの切り替えを確実に管理することができる運転管理システム等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 】

【 0 0 0 9 】

本開示の一態様に係る運転管理システムは、1 以上の認証サーバと、手動運転及び自動運転が切り替え可能な 1 以上の車両とを備える運転管理システムであって、前記 1 以上の車両のそれぞれは、前記 1 以上の認証サーバの少なくとも一の認証サーバと通信を行う第 1 通信部と、前記車両内のネットワークに接続する複数の電子制御装置と、前記複数の電子制御装置のうちの 1 以上の電子制御装置が発するメッセージに基づき、手動運転される手動運転モードと自動運転される自動運転モードとの切り替えを検知する検知部と、前記検知部が検知した切り替えを示す情報及び当該車両を示す第 1 の識別子を含む第 1 トランザクションデータを生成し、前記第 1 通信部を介して前記一の認証サーバに送信するトランザクションデータ生成部と、備える。前記少なくとも一の認証サーバのそれぞれは、前記 1 以上の車両のそれぞれと通信を行う第 2 通信部と、前記 1 以上の車両の少なくとも一の車両から取得した前記第 1 トランザクションデータを含むトランザクションデータの正当性を判断する検証部と、前記検証部により正当性が確認された前記トランザクションデータを記憶装置に記録する記録部とを備える。

【 0 0 1 0 】

なお、これらの包括的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能な CD - ROM などの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

【 発明の効果 】

【 0 0 1 1 】

本開示によれば、車両における運転モードの切り替えを確実に管理することができる。

【 図面の簡単な説明 】

【 0 0 1 2 】

【 図 1 】 実施の形態に係る運転管理システムの構成の一例を示した図である。

【 図 2 】 実施の形態に係る車両が有する車載ネットワークシステムの全体構成の一例を示す図である。

10

20

30

40

50

【図 3】実施の形態に係るヘッドユニットの機能構成の一部を示す図である。

【図 4】実施の形態に係るゲートウェイの機能構成を示すブロック図である。

【図 5】実施の形態に係る認証サーバの機能構成を示すブロック図である。

【図 6 A】ブロックチェーンのデータ構造を示す説明図である。

【図 6 B】トランザクションデータのデータ構造を示す説明図である。

【図 7】実施の形態に係るカーメーカサーバの機能構成を示すブロック図である。

【図 8 A】実施の形態におけるカーメーカサーバと認証サーバとの間の登録処理を示すシーケンス図である。

【図 8 B】図 8 A に示すステップ S 1 0 4 の詳細処理を示すフローチャートである。

【図 9 A】実施の形態に係る車両と認証サーバとの間の第 1 検証処理を示すシーケンス図である。

10

【図 9 B】図 9 A に示すステップ S 2 0 1 の詳細処理を示すフローチャートである。

【図 9 C】図 9 A に示すステップ S 2 0 5 の詳細処理を示すフローチャートである。

【図 1 0 A】実施の形態 1 に係る車両と認証サーバとの間の第 2 検証処理を示すシーケンス図である。

【図 1 0 B】図 1 0 A に示すステップ S 2 0 9 の詳細処理を示すフローチャートである。

【図 1 0 C】図 1 0 A に示すステップ S 2 1 3 の詳細処理を示すフローチャートである。

【図 1 0 D】図 1 0 A に示すステップ S 2 1 5 の詳細処理を示すフローチャートである。

【図 1 1】実施の形態に係る車両で表示される画面表示の一例を示す図である。

【図 1 2】実施の形態に係る車両で表示される画面表示の一例を示す図である。

20

【図 1 3】実施の形態の変形例に係る認証サーバの機能構成を示すブロック図である。

【図 1 4】実施の形態の変形例に係るカーメーカサーバと認証サーバとの間の登録処理を示すシーケンス図である。

【図 1 5】実施の形態の変形例に係る認証サーバが第 3 トランザクションデータを記録する際に用いるデータ構造の一例である。

【図 1 6】実施の形態の変形例に係る車両と認証サーバとの間の第 1 検証処理を示すシーケンス図である。

【図 1 7】実施の形態の変形例に係る認証サーバが第 1 トランザクションデータを記録する際に用いるデータ構造の一例である。

【発明を実施するための形態】

30

【0 0 1 3】

本開示の一態様に係る運転管理システムは、1 以上の認証サーバと、手動運転及び自動運転が切り替え可能な 1 以上の車両とを備える運転管理システムであって、前記 1 以上の車両のそれぞれは、前記 1 以上の認証サーバの少なくとも一の認証サーバと通信を行う第 1 通信部と、前記車両内のネットワークに接続する複数の電子制御装置と、前記複数の電子制御装置のうちの 1 以上の電子制御装置が発するメッセージに基づき、手動運転される手動運転モードと自動運転される自動運転モードとの切り替えを検知する検知部と、前記検知部が検知した切り替えを示す情報及び当該車両を示す第 1 の識別子を含む第 1 トランザクションデータを生成し、前記第 1 通信部を介して前記一の認証サーバに送信するトランザクションデータ生成部と、備える。前記少なくとも一の認証サーバのそれぞれは、前記 1 以上の車両のそれぞれと通信を行う第 2 通信部と、前記 1 以上の車両の少なくとも一の車両から取得した前記第 1 トランザクションデータを含むトランザクションデータの正当性を判断する検証部と、前記検証部により正当性が確認された前記トランザクションデータを記憶装置に記録する記録部とを備える。

40

【0 0 1 4】

これにより、車両における運転モードの切り替えの履歴を記憶装置に記録することができるので、車両における運転モードの切り替えを確実に管理することができる。

【0 0 1 5】

また、例えば、前記記録部は、前記 1 以上の車両のそれぞれを一意に識別する第 2 の識別子を前記記憶装置に予め記録しており、前記検証部は、前記第 1 トランザクションデー

50

タに含まれる前記第1の識別子が、前記第2の識別子に含まれているかと、前記第1トランザクションデータの正当性を検証し、前記記録部は、前記検証部により、前記第1の識別子が前記第2の識別子に含まれていることが確認され、かつ、前記第1トランザクションデータの正当性が確認された場合、前記第1トランザクションデータを前記記憶装置に記録するとしてもよい。

【0016】

また、例えば、前記1以上の車両のそれぞれは、さらに、情報の入力を受け付ける入力部を備え、前記入力部は、入力された情報であって、切り替わった自動運転モードが継続されることが承認された旨を示す情報を前記トランザクションデータ生成部に送信し、前記トランザクションデータ生成部は、前記入力された情報を含む第2トランザクションデータを生成し、前記第1通信部を介して前記一の認証サーバに送信するとしてもよい。

10

【0017】

また、例えば、前記トランザクションデータ生成部は、前記検知部が検知した切り替えを示す情報が手動運転モードから自動運転モードに切り替えられたことを示す場合、前記検知部が検知した切り替えを示す情報、及び、当該車両を示す第1の識別子に加えて、前記自動運転モードにおける自動運転レベルを示す情報を含む前記第1トランザクションデータを生成し、前記第1通信部を介して前記一の認証サーバに送信するとしてもよい。

【0018】

また、例えば、前記トランザクションデータ生成部は、前記検知部が検知した切り替えを示す情報が手動運転モードから自動運転モードに切り替えられたことを示す場合、前記検知部が検知した切り替えを示す情報、及び、当該車両を示す第1の識別子に加えて、前記自動運転モードにおいて動作する運転アシスト機能を示す情報を含む前記第1トランザクションデータを生成し、前記第1通信部を介して前記一の認証サーバに送信するとしてもよい。

20

【0019】

また、例えば、前記1以上の車両のそれぞれは、さらに、所定期間毎またはイベント毎に、当該車両の運転者に関する情報を示すセンサ情報を取得するセンサ部を備え、前記センサ部は、取得した前記センサ情報を前記トランザクションデータ生成部に送信し、前記トランザクションデータ生成部は、前記切り替えを示す情報、前記第1の識別子、及び前記センサ情報を含む第1トランザクションデータを生成し、前記第1通信部を介して前記一の認証サーバに送信するとしてもよい。

30

【0020】

また、例えば、前記記録部は、前記1以上の車両のそれぞれを一意に識別する第2の識別子を前記記憶装置に予め記録しており、前記検証部は、前記第1トランザクションデータに含まれる前記第1の識別子が、前記第2の識別子に含まれていない場合、前記第1の識別子が前記第2の識別子に含まれていない旨を通知するとしてもよい。

【0021】

また、例えば、前記トランザクションデータ生成部は、さらに、前記第1トランザクションデータを含むトランザクションデータを、ブロックチェーンのトランザクションデータとして生成し、前記記録部は、前記第1トランザクションデータを含むトランザクションデータをブロックチェーンのトランザクションデータとして記録するとしてもよい。

40

【0022】

以下、図面を参照しながら、実施の形態について説明する。なお、以下で説明する実施の形態は、いずれも本開示の一具体例を示す。つまり、以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置及び接続形態、ステップ、ステップの順序などは、本開示の一例であり、本開示を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素は、本開示の課題を達成するために必ずしも必要ではないが、より好ましい形態を構成する構成要素として説明される。

【0023】

50

(実施の形態)

[1.1 システム構成]

まず、本開示のシステム構成について説明する。

【 0024 】

本開示の運転管理システムは、車両における自動運転モードと手動運転モードとの間の切り替えである運転モードの切り替えを確実に管理する。以下では、図面を参照しながら実施の形態における運転管理システム等の説明を行う。

【 0025 】

[1.1.1 運転管理システム10の全体構成]

図1は、本実施の形態に係る運転管理システムの構成の一例を示した図である。

10

【 0026 】

運転管理システム10は、1以上の認証サーバと、手動運転及び自動運転が切り替え可能な1以上の車両とを備える。本実施の形態では、運転管理システム10は、図1に示すように、例えば、車両100a、100b、100cと、認証サーバ200a、200b、200cと、カーメーカサーバ300とを備える。これらは、車両100a等及び認証サーバ200a等と、認証サーバ200a等同士、カーメーカサーバ300と認証サーバ200a等とは、ネットワークNで接続されている。また、認証サーバ200a、200b、200cは記憶装置201a、201b、201cと接続する。認証サーバ200a等は、記憶装置201a等とネットワークNを介して接続されていてもよいし、内部に記憶装置201aを備えてもよい。記憶装置201aは、ブロックチェーンのトランザクション及びブロックが電子的に記録される。

20

【 0027 】

[1.1.2 車両100aの構成]

車両100a等は、例えば手動運転と自動運転とが切り替え可能な自動車であるが、これに限られない。車両100a等は、手動運転と自動運転とが切り替え可能な自動二輪車、船舶等であってもよい。つまり、車両100a等は、運転者が車両の走行制御を行う手動運転モードと車両が自律走行するすなわち自動車の走行制御を自動的に行う自動運転モードとを切り替えることができればよい。また、車両100a等は、車両100a内のネットワークに複数のECUが接続されており、自動運転モードにおいて、複数のECUが連携して、車両100aの走行制御を自動的に行うものであればよい。

30

【 0028 】

図2は、本実施の形態に係る車両100aが有する車載ネットワークシステムの全体構成の一例を示す図である。車両100b、100cも同様の構成であるため、車両100aを例に挙げて説明する。

【 0029 】

複数の電子制御装置は、車両100a等内のネットワークで接続されている。より具体的には、複数の電子制御装置であるECU111、ECU121、ECU131、ECU141、ECU151、及びゲートウェイ101が車載ネットワークで接続されている。ここで、車載ネットワークはCANであってもよいし、Ethernet(登録商標)であってもよいし、CANとEthernet(登録商標)とが混在したものであってもよい。なお、車載ネットワークがEthernet(登録商標)を含む場合でも、ブロードキャストでメッセージが送信されるとしてもよい。

40

【 0030 】

車載ネットワークには、例えば、エンジン110、バッテリー130、及び、図示しないモータなどの燃料の制御に関連する駆動系のECUが接続されている。図2に示す例では、車載ネットワークには、エンジン110用のECU111、バッテリー130用のECU131が接続されている。

【 0031 】

また、車載ネットワークには、運転アシスト部120、並びに、図示しない自動ブレーキ、車線維持、車間距離機能、衝突防止機能、及び、エアバッグなどの安全快適機能系E

50

ＣＵが接続されている。図２に示す例では、車載ネットワークには、運転アシスト部１２０用のＥＣＵ１２１が接続されている。本実施の形態では、運転アシスト部１２０用のＥＣＵ１２１は、例えば、運転アシスト部１２０の運転アシスト機能がＯＮになり、車両１００ａの運転モードが自動運転モードと手動運転モードとの間で切り替わった時にその旨を示すメッセージを送信する。なお、運転アシスト部１２０用のＥＣＵ１２１は、定期的には送信しているメッセージに車両１００ａの運転モードが自動運転モードと手動運転モードとの間で切り替わったこと示す情報を含めてもよい。

【００３２】

また、車載ネットワークには、ヘッドユニット１４０などインフォテインメント系ＥＣＵが接続されている。図２に示す例では、車載ネットワークには、ヘッドユニット１４０用のＥＣＵ１４１が接続されている。なお、ヘッドユニット１４０用のＥＣＵ１４１がなく、ヘッドユニット１４０がＥＣＵ１４１を介さず車載ネットワークに直接接続されていてもよい。本実施の形態では、ヘッドユニットは後述する表示部及び入力部を有し、車両１００ａに搭乗している運転者等のユーザに対し、画面の表示及び情報入力を受け付ける機能を有する。

10

【００３３】

図３は、本実施の形態に係るヘッドユニット１４０の機能構成の一部を示す図である。図３に示すように、ヘッドユニット１４０は、表示部１４１１と入力部１４１２とを有する。

【００３４】

表示部１４１１は、認証サーバ２００ａ等の一から送信された画面情報に示される画面をユーザに表示する。本実施の形態では、表示部１４１１は、自動運転モードに切り替わったことを通知し、かつ、自動運転モードを継続するか否かをユーザに確認するための画面を表示する。

20

【００３５】

入力部１４１２は、情報の入力を受け付ける。入力部１４１２は、ユーザにより入力された情報であって、切り替わった自動運転モードが継続されることが承認された旨を示す情報をゲートウェイ１０１に送信する。具体的には、入力部１４１２は、表示部１４１１により表示された画面において、切り替わった自動運転モードを継続することの承認または確認を示す情報である確認情報がユーザにより入力される。そして、入力部１４１２は、入力された確認情報を、ゲートウェイ１０１またはゲートウェイ１０１を介して認証サーバ２００ａ等に送信する。

30

【００３６】

また、車載ネットワークには、認証サーバ２００ａ等と通信する通信機能を有する通信部１５０など通信系ＥＣＵが接続されている。図２に示す例では、車載ネットワークには、通信部１５０用のＥＣＵ１５１が接続されている。

【００３７】

なお、上述したＥＣＵ１１１～ＥＣＵ１５１は、それぞれが接続する部品と一体すなわち１つの部品で構成されるときもよい。例えば、エンジン１１０とこれに接続されるｅＥＣＵ１１１とが一体すなわち１つの部品として構成されてもよい。他のＥＣＵも同様である。

40

【００３８】

このような複数の電子制御装置すなわちＥＣＵ１１１～ＥＣＵ１５１は、接続されたものの状態等を取得し、定期的または非定期的に得た状態等を示すメッセージを送信する。例えば、ＥＣＵ１１１は、エンジン１１０の回転数を状態等として取得し、定期的に回転数を示すメッセージを送信する。また、例えばＥＣＵ１２１は、上述したように、運転アシスト部１２０の運転アシスト機能がＯＮになった時にメッセージを送信する。

【００３９】

次に、車載ネットワークに接続されているゲートウェイ１０１について説明する。

【００４０】

50

[1 . 1 . 3 ゲートウェイ 1 0 1 の構成]

図 4 は、本実施の形態に係るゲートウェイ 1 0 1 の機能構成を示すブロック図である。

【 0 0 4 1 】

ゲートウェイ 1 0 1 は、車両 1 0 0 a 等に搭載され、図 4 に示すように、検知部 1 1 0 1 と、トランザクションデータ生成部 1 1 0 2 と、第 1 通信部 1 1 0 3 とを備える。以下、各構成要素について説明する。

【 0 0 4 2 】

< 検知部 1 1 0 1 >

検知部 1 1 0 1 は、複数の電子制御装置のうちの 1 以上の電子制御装置が発するメッセージに基づき、手動運転される手動運転モードと自動運転される自動運転モードとの切り替えを検知する。図 2 に示す例では、検知部 1 1 0 1 は、車載ネットワークに接続している ECU 1 2 1 が送信するメッセージから、運転アシスト部 1 2 0 のアシスト機能の切り替えとして運転モードの切り替えを検知する。ここで、運転モードの切り替えには、手動運転モードから自動運転モードに切り替わったこと、または、自動運転モードから手動運転モードに切り替わったことが含まれる。

10

【 0 0 4 3 】

より具体的には、検知部 1 1 0 1 は、車載ネットワークに接続している ECU 1 2 1 が送信するメッセージから、手動運転中に自動運転の機能が ON になったことを検知した場合、手動運転モードから自動運転モードに切り替わったと検知してもよい。また、検知部 1 1 0 1 は、車載ネットワークに接続している ECU 1 2 1 が送信するメッセージから、自動運転中に運転者により手動運転が行われたことを検知した場合、自動運転モードから手動運転モードに切り替わったと検知してもよい。

20

【 0 0 4 4 】

また、検知部 1 1 0 1 は、運転アシスト部 1 2 0 のアシスト機能の切り替えとして、自動駐車機能により車両 1 0 0 a 等が自動的に駐車する駐車モードに切り替わったことなどを検知してもよい。

【 0 0 4 5 】

なお、運転アシスト部 1 2 0 のアシスト機能の切り替えがあったか否かを検知する検知方法としてはいくつか挙げられる。例えば、検知部 1 1 0 1 は、車載ネットワークに接続している、運転アシスト部 1 2 0 用の ECU 1 2 1 が送信するメッセージから運転アシスト部 1 2 0 のアシスト機能の切り替えがあったか否かを検知してもよい。また、検知部 1 1 0 1 は、車両 1 0 0 a 等の車外に搭載されるセンサ（不図示）の情報またはセンサ用の ECU が送信するメッセージから運転アシスト部 1 2 0 のアシスト機能の切り替えがあったか否かを検知してもよい。

30

【 0 0 4 6 】

本実施の形態では、検知部 1 1 0 1 は、運転アシスト部 1 2 0 のアシスト機能の切り替えを検知した場合、当該切り替えを示す情報である切り替え情報をトランザクションデータ生成部 1 1 0 2 へ送信する。そして、切り替え情報は、手動運転モードと自動運転モードとの切り替えを示す情報などを含む。

【 0 0 4 7 】

< トランザクションデータ生成部 1 1 0 2 >

トランザクションデータ生成部 1 1 0 2 は、検知部 1 1 0 1 が検知した切り替え情報及び当該車両を示す第 1 の識別子を含む第 1 トランザクションデータを生成する。トランザクションデータ生成部 1 1 0 2 は、生成した第 1 トランザクションデータを、第 1 通信部 1 1 0 3 を介して認証サーバ 2 0 0 a 等の一に送信する。また、トランザクションデータ生成部 1 1 0 2 は、第 1 トランザクションデータをブロックチェーンのトランザクションデータとして生成する。

40

【 0 0 4 8 】

本実施の形態では、トランザクションデータ生成部 1 1 0 2 は、検知部 1 1 0 1 から取得した切り替え情報から、ブロックチェーンのトランザクションデータである第 1 トラン

50

ザクションデータを生成する。ここで、切り替え情報が運転モードの切り替えを示す情報であるとする。この場合、第1トランザクションデータには、運転モードの切り替えを示す切り替え情報と、切り替わった時刻と、車両100a等を示す第1の識別子と、これらを含む情報に対する署名とが含まれる。

【0049】

ここで、当該署名を生成するために必要な署名鍵は、あらかじめゲートウェイ101が保持してもよい。また、当該署名を生成するために必要な署名鍵は、ヘッドユニット140の入力部1412に入力された秘密情報を基に生成されてもよい。

【0050】

なお、運転モードの切り替えを示す切り替え情報は、自動運転モードから手動運転モードに切り替わったことを示す情報でもよいし、手動運転モードから自動運転モードに切り替わったことを示す情報でもよい。また、当該切り替え情報は、運転モードの切り替え以外である運転アシスト部120のアシスト機能の切り替えを示す情報でもよい。この場合、切り替え情報に、運転アシスト部120が有するアシスト機能のうちどの運転アシスト機能が切り替わった運転アシスト機能として用いられているかを示す情報をさらに含めてもよい。

10

【0051】

また、トランザクションデータ生成部1102は、ヘッドユニット140から取得した確認情報から、ブロックチェーンのトランザクションデータすなわち後述する確認情報を含む第2トランザクションデータを生成して、第1通信部1103を介して認証サーバ200a等に送信するとしてもよい。トランザクションデータ生成部1102は、確認情報を含む第2トランザクションデータを、例えば、ユーザの承諾情報を含めて生成してもよい。この承諾情報は、例えば、手動運転モードから自動運転モードに切り替わったことを確認し、当該自動運転モードを継続することをユーザが承諾したことを示す情報である。

20

【0052】

<第1通信部1103>

第1通信部1103は、1以上の認証サーバ200a等の少なくとも一の認証サーバと通信を行う。より具体的には、第1通信部1103は、車載システムに接続されている通信部150を介して認証サーバ200a等のうち少なくとも一と通信を行う通信インタフェースである。この通信は、T L S (Transport Layer Security) によりなされてもよい。その場合、T L S 通信用の暗号鍵は通信部150または第1通信部1103で保持してもよい。

30

【0053】

次に、認証サーバ200a等について説明する。

【0054】

[1.1.4 認証サーバ200aの構成]

図5は、本実施の形態に係る認証サーバ200aの機能構成を示すブロック図である。認証サーバ200b、200cも同様の構成であるため、認証サーバ200aを例に挙げて説明する。

【0055】

認証サーバ200aは、図5に示すように、画面生成部211と、トランザクションデータ検証部212と、トランザクションデータ生成部213と、ブロック生成部214と、同期部215と、記録部216と、第2通信部217とを備える。認証サーバ200aは、プロセッサがメモリを用いて所定のプログラムを実行することで実現され得る。以下、各構成要素について説明する。

40

【0056】

<画面生成部211>

画面生成部211は、車両100a等から取得した第1トランザクションデータに含まれる切り替え情報により、運転モードが手動運転モードから自動運転モードに切り替わったと判断された場合、ユーザに表示するための画面を生成する。例えば、画面生成部21

50

1 は、車両 100 a 等の搭乗者であるユーザに、運転モードが自動運転モードに切り替わったことを通知し、かつ、自動運転モードを継続するか否かをユーザに確認するための画面を生成する。

【0057】

そして、画面生成部 211 は、生成した画面を示す画面情報を第 2 通信部 217 を介し車両 100 a 等のゲートウェイ 101 に送信する。

【0058】

<トランザクションデータ検証部 212 >

トランザクションデータ検証部 212 は、検証部の一例であり、1 以上の車両の少なくとも一の車両 100 a から取得した第 1 トランザクションデータを含むトランザクションデータの正当性を検証する。例えば、トランザクションデータ検証部 212 は、第 1 トランザクションデータに含まれる第 1 の識別子が、第 2 の識別子に含まれているかと、第 1 トランザクションデータの正当性とを検証する。トランザクションデータ検証部 212 は、第 1 トランザクションデータに含まれる第 1 の識別子が、第 2 の識別子に含まれていない場合、第 2 通信部 217 を介して、第 1 の識別子が第 2 の識別子に含まれていない旨を通知する。

【0059】

本実施の形態では、トランザクションデータ検証部 212 は、車両 100 a 等から取得した第 1 トランザクションデータの正当性を検証する。

【0060】

具体的には、トランザクションデータ検証部 212 は、車両 100 a 等から第 1 トランザクションデータを取得すると、第 1 トランザクションデータに含まれる署名すなわち認証情報が正当であるかを検証する。また、トランザクションデータ検証部 212 は、第 1 トランザクションデータを取得すると、第 1 の識別子が正当であるかを検証する。より詳細には、トランザクションデータ検証部 212 は、第 1 トランザクションデータに含まれる第 1 の識別子が、記録部 216 に予め記録されている正規の車両を示す第 2 の識別子に含まれるかを検証する。これにより、第 1 トランザクションデータに含まれる第 1 の識別子に示される車両が、正規に登録された、手動運転と自動運転とが切り替え可能な車両であるかを検証することができる。

【0061】

トランザクションデータ検証部 212 は、検証した結果、取得した第 1 トランザクションデータの正当性を確認した場合には、記録部 216 に第 1 トランザクションデータを記録させ、同期部 215 に第 1 トランザクションデータを通知させる。

【0062】

トランザクションデータ検証部 212 は、同様に、車両 100 a 等から取得した第 2 トランザクションデータの正当性を検証する。トランザクションデータ検証部 212 は、検証した結果、第 2 トランザクションデータの正当性を確認した場合、記録部 216 に第 2 トランザクションデータを記録させ、同期部 215 に第 2 トランザクションデータを通知すればよい。

【0063】

また、トランザクションデータ検証部 212 は、同様に、カーメーカーサーバ 300 から取得した第 3 トランザクションデータの正当性を検証する。トランザクションデータ検証部 212 は、検証した結果、第 3 トランザクションデータの正当性を確認した場合、記録部 216 に第 3 トランザクションデータを記録させ、同期部 215 に第 3 トランザクションデータを通知すればよい。

【0064】

なお、第 2 トランザクションデータ及び第 3 トランザクションデータの詳細は後述する。

【0065】

<トランザクションデータ生成部 213 >

トランザクションデータ生成部 213 は、車両 100 a 等から確認情報を取得した場合

10

20

30

40

50

には、当該確認情報を含む第2トランザクションデータを生成してもよい。この場合、トランザクションデータ生成部213は、当該確認情報を含む第2トランザクションデータに、さらにユーザの承諾情報を含めて生成してもよい。この承諾情報は、例えば、手動運転モードから自動運転モードに切り替わったことを確認し、当該自動運転モードを継続することをユーザが承諾または確認したことを示す情報である。

【0066】

なお、このような第2トランザクションデータは、トランザクションデータ生成部213が生成する場合に限らず、上述したように、車両100a等のゲートウェイ101により生成されてもよい。ゲートウェイ101により生成される第2トランザクションデータは、車両100a等からトランザクションデータ生成部213により取得されてもよいし、ブロック生成部214により取得されてもよい。

10

【0067】

<ブロック生成部214>

ブロック生成部214は、複数の認証サーバの間でコンセンサスアルゴリズムを実行する。コンセンサスアルゴリズムは、PBFT (Practical Byzantine Fault Tolerance) とよばれるコンセンサスアルゴリズムを用いてもよいし、その他の公知のコンセンサスアルゴリズムを用いても良い。本実施の形態では、ブロック生成部214は、認証サーバ200a、認証サーバ200b及び認証サーバ200cの間でコンセンサスアルゴリズムを実行する。

【0068】

ブロック生成部214は、まず、一以上のトランザクションデータを含むブロックチェーンのブロックを生成する。そして、ブロック生成部214は、コンセンサスアルゴリズムで合意形成ができた場合、記録部216に記録させる。ブロック生成部214により生成されたブロックは、記録部216に記録されているブロックチェーンに接続されて記録される。

20

【0069】

ここで、ブロックチェーンのデータ構造と、トランザクションデータのデータ構造とについて説明する。

【0070】

図6Aは、ブロックチェーンのデータ構造を示す説明図である。

30

【0071】

ブロックチェーンは、その記録単位であるブロックがチェーン(鎖)上に接続されたものである。それぞれのブロックは、複数のトランザクションデータと、直前のブロックのハッシュ値とを有している。具体的には、ブロックB2には、その前のブロックB1のハッシュ値が含まれている。そして、ブロックB2に含まれる複数のトランザクションデータと、ブロックB1のハッシュ値とから演算されたハッシュ値が、ブロックB2のハッシュ値として、ブロックB3に含められる。このように、前のブロックの内容をハッシュ値として含めながら、ブロックをチェーン状に接続することで、接続されたトランザクションデータの改ざんを有効に防止する。

【0072】

仮に過去のトランザクションデータが変更されると、ブロックのハッシュ値が変更前と異なる値になり、改ざんしたブロックを正しいものとみせかけるには、それ以降のブロックすべてを作り直さなければならず、この作業は現実的には非常に困難である。

40

【0073】

本実施の形態では、各トランザクションデータは、切り替え情報を含む第1トランザクションデータ、ユーザの確認情報を含む第2トランザクションデータ、及び、後述する正規の車両の登録に関する第3トランザクションデータなどである。

【0074】

図6Bは、トランザクションデータのデータ構造を示す説明図である。

【0075】

50

図 6 B に示されるトランザクションデータ D 1 は、例えば運転モードの切り替えを示す切り替え情報を含む第 1 トランザクションデータの一例である。トランザクションデータ D 1 は、保持者を示すアドレス P 1 と、提供先を示すアドレス P 2 と、アドレス P 1 及び P 2 のハッシュ値に対して、保持者の署名鍵で署名することで生成される電子署名 P 3 とを含んでいる。なお、新たにトランザクションデータが生成されるときにトランザクションデータは、アドレス P 1 が空欄となる。

【 0 0 7 6 】

< 同期部 2 1 5 >

同期部 2 1 5 は、複数の認証サーバの間でブロックチェーンのブロックの同期、及び、トランザクションデータの同期を行う。複数の認証サーバでは、peer to peer でブロックチェーンのトランザクションデータの同期が行われ、記録部 2 1 6 に記録される。

10

【 0 0 7 7 】

例えば、トランザクションデータ検証部 2 1 2 により、車両 1 0 0 a から取得した第 1 トランザクションデータの正当性が検証されると、同期部 2 1 5 は、他の認証サーバ 2 0 0 b 及び 2 0 0 c に第 1 トランザクションデータの複製を転送する。これにより、検証済みの第 1 トランザクションデータを他の認証サーバ 2 0 0 b 及び 2 0 0 c の記録部 2 1 6 に記録させることができる。また、同期部 2 1 5 は、他の認証サーバ 2 0 0 b 及び 2 0 0 c から第 1 トランザクションデータを取得したら、取得した第 1 トランザクションデータを記録部 2 1 6 に記録させる。なお、第 2 トランザクションデータ及び第 3 トランザクションデータの場合も同様であるので、説明は省略する。

20

【 0 0 7 8 】

< 記録部 2 1 6 >

記録部 2 1 6 は、第 1 トランザクションデータと、第 2 トランザクションデータと、第 3 トランザクションデータとをブロックチェーンのブロックで記憶装置 2 0 1 a に記録する。なお、当該記憶装置 2 0 1 a は、記録部 2 1 6 の内部に構成されていてもよいし、図 1 に示すように、認証サーバ 2 0 0 a の外部に構成されていてもよい。

【 0 0 7 9 】

本実施の形態では、記録部 2 1 6 は、トランザクションデータ検証部 2 1 2 により正当性が確認された例えば第 1 トランザクションデータと、第 2 トランザクションデータと、第 3 トランザクションデータとを含むトランザクションデータを記憶装置 2 0 1 a に記録する。記録部 2 1 6 は、第 1 トランザクションデータと、第 2 トランザクションデータと、第 3 トランザクションデータとを含むトランザクションデータをブロックチェーンのトランザクションデータとして記録する。

30

【 0 0 8 0 】

ここで、記録部 2 1 6 は、1 以上の車両のそれぞれを一意に識別する第 2 の識別子を記憶装置 2 0 1 a に予め記録していてもよい。予め記録される第 2 の識別子により示される車両は、例えば、カーメカなどが認定し、手動運転と自動運転とが切り替え可能な正規の車両であって動作保証のある車両である。

【 0 0 8 1 】

より具体的には、記録部 2 1 6 は、トランザクションデータ検証部 2 1 2 により、第 1 の識別子が第 2 の識別子に含まれていることが確認され、かつ、第 1 トランザクションデータの正当性が確認された場合、第 1 トランザクションデータを記憶装置 2 0 1 a に記録してもよい。これにより、正規の車両において運転モードが切り替わったことが記憶装置 2 0 1 a に確実に記録される。

40

【 0 0 8 2 】

< 第 2 通信部 2 1 7 >

第 2 通信部 2 1 7 は、車両 1 0 0 a 等、及び、カーメカサーバ 3 0 0 と通信を行う通信インタフェースである。この通信は、T L S によりなされてもよい。その場合、T L S 通信の暗号鍵は第 2 通信部 2 1 7 が保持してもよい。

【 0 0 8 3 】

50

本実施の形態では、第2通信部217は、1以上の車両100a等のそれぞれと通信を行う。第2通信部217は、トランザクションデータ検証部212により、第1の識別子が第2の識別子に含まれていないことが確認され、かつ、第1トランザクションデータの正当性が確認された場合、第1の識別子が第2の識別子に含まれていない旨を通知する。これにより、当該車両が非正規であったり、運転モードの切り替えを含む運転アシスト部120のアシスト機能の切り替えが不正であったりすることを判断することができる。

【0084】

次に、カーメーカサーバ300について説明する。

【0085】

[1.1.5 カーメーカサーバ300の構成]

図7は、本実施の形態に係るカーメーカサーバ300の機能構成を示すブロック図である。

【0086】

カーメーカサーバ300は、図7に示すように、入力部311と、トランザクションデータ生成部312と、第3通信部313とを備える。カーメーカサーバ300は、プロセッサがメモリを用いて所定のプログラムを実行することで実現され得る。以下、各構成要素について説明する。

【0087】

<入力部311>

入力部311は、カーメーカで管理している車両であって手動運転と自動運転とが切り替え可能な正規の車両に関する入力を受け付け、トランザクションデータ生成部312へ送信する。より具体的には、入力部311は、カーメーカで管理している複数の正規の車両それぞれを一意に識別する第2の識別子の入力を受け付ける。そして、入力部311は、入力された第2の識別子をトランザクションデータ生成部312へ送信する。

【0088】

<トランザクションデータ生成部312>

トランザクションデータ生成部312は、入力部311から取得した第2の識別子を含み正規の車両を登録する旨を示す第3トランザクションデータをブロックチェーンのトランザクションデータとして生成する。

【0089】

本実施の形態では、トランザクションデータ生成部312は、正規の車両を登録する旨を示す第3トランザクションデータを、第2の識別子とカーメーカサーバ300の署名とを含めて生成する。なお、署名は、認証情報の一例であるので、カーメーカサーバ300が入力するパスワードが得られる場合には、当該パスワードのハッシュ値であってもよいし、当該パスワードから生成した署名鍵を用いて生成されてもよい。

【0090】

<第3通信部313>

第3通信部313は、車両100a等、及び、認証サーバ200a等との通信を行う通信インタフェースである。この通信は、TLSとしてもよい。この通信は、TLSによりなされてもよい。その場合、TLS通信用の暗号鍵は第3通信部313で保持するとしてもよい。

【0091】

[1.2 動作等]

以下、以上のように構成された運転管理システム10の処理動作について説明する。

【0092】

[1.2.1 カーメーカサーバ300と認証サーバ200a等との間の登録処理]

まず、認証サーバ200a等に、手動運転と自動運転とが切り替え可能な正規の車両を一意に識別する第2の識別子を登録する登録処理について説明する。ここでは、カーメーカサーバ300から認証サーバ200a等のうちの一の認証サーバ200aに第2の識別子を含む第3トランザクションデータを送信する場合について説明する。

10

20

30

40

50

【 0 0 9 3 】

図 8 A は、本実施の形態に係るカーメーカサーバ 3 0 0 と認証サーバ 2 0 0 a 等との間の登録処理を示すシーケンス図である。図 8 B は、図 8 A に示すステップ S 1 0 4 の詳細処理を示すフローチャートである。

【 0 0 9 4 】

まず、ステップ S 1 0 1 において、カーメーカサーバ 3 0 0 は、手動運転と自動運転とが切り替え可能な正規の車両を示す第 2 の識別子を取得する。

【 0 0 9 5 】

次に、ステップ S 1 0 2 において、カーメーカサーバ 3 0 0 は、取得した正規の車両を示す第 2 の識別子を含む第 3 トランザクションデータを生成する。本実施の形態では、第 3 トランザクションデータは、例えば、第 2 の識別子とカーメーカサーバ 3 0 0 の署名などの認証情報とを含めて生成される。

10

【 0 0 9 6 】

次に、ステップ S 1 0 3 において、カーメーカサーバ 3 0 0 は生成した第 3 トランザクションデータを認証サーバ 2 0 0 a に送信する。なお、図 8 A では、カーメーカサーバ 3 0 0 は、生成した第 3 トランザクションデータを認証サーバ 2 0 0 a に送信する例が示されているが、これに限らない。認証サーバ 2 0 0 a 等のうちのいずれかの認証サーバに送信すればよい。

【 0 0 9 7 】

次に、ステップ S 1 0 4 において、認証サーバ 2 0 0 a は、取得した第 3 トランザクションデータの検証を行い、成功した場合に、記録部 2 1 6 に第 3 トランザクションデータを記録させて、ステップ S 1 0 6 に進む。

20

【 0 0 9 8 】

ここで、ステップ S 1 0 4 の詳細処理について、図 8 B を用いて説明する。すなわち、認証サーバ 2 0 0 a は、まず、取得した第 3 トランザクションデータの検証を行い、成功したか否かを確認する (S 1 0 4 1)。より詳細には、認証サーバ 2 0 0 a は、第 3 トランザクションデータに含まれる第 2 の識別子が正当であるかと、第 3 トランザクションデータに含まれるカーメーカサーバ 3 0 0 の署名が正当であることを検証する。つまり、認証サーバ 2 0 0 a は、第 2 の識別子及び署名が正当であるか否かを確認する。ステップ S 1 0 4 1 において、認証サーバ 2 0 0 a は、第 2 の識別子及び署名が正当であることを確認し、第 3 トランザクションデータの検証が成功した場合 (S 1 0 4 1 で Y)、記録部 2 1 6 に第 3 トランザクションデータを記録させて (S 1 0 4 2)、ステップ S 1 0 6 に進む。なお、ステップ S 1 0 4 1 において、認証サーバ 2 0 0 a は、第 3 トランザクションデータの検証が成功しなかった場合 (S 1 0 4 1 で N)、カーメーカサーバ 3 0 0 にその旨を通知し (S 1 0 4 3)、登録処理を終了する。

30

【 0 0 9 9 】

次に、ステップ S 1 0 6 において、認証サーバ 2 0 0 a は、取得した第 3 トランザクションデータの複製を、他の認証サーバ 2 0 0 b、2 0 0 c に転送する。なお、他の認証サーバ 2 0 0 b、2 0 0 c においても、転送され取得した第 3 トランザクションデータを検証する。この検証処理は、図 8 B で説明した処理と同様である。

40

【 0 1 0 0 】

次に、ステップ S 1 0 7 において、認証サーバ 2 0 0 a と認証サーバ 2 0 0 b と認証サーバ 2 0 0 c とは、コンセンサスアルゴリズムを実行する。コンセンサスアルゴリズムを実行することで、認証サーバ 2 0 0 a と認証サーバ 2 0 0 b と認証サーバ 2 0 0 c とが取得した第 3 トランザクションデータが正当なトランザクションデータであると検証される。認証サーバ 2 0 0 a、2 0 0 b 及び 2 0 0 c は、検証済みの第 3 トランザクションデータを含むブロックの生成を行う。これにより、手動運転と自動運転とが切り替え可能な正規の車両を示す第 2 の識別子を含む第 3 トランザクションデータのブロックが生成されるので、ブロックチェーンを参照することで正規の車両であるかの判断ができる。

【 0 1 0 1 】

50

[1 . 2 . 2 車両 1 0 0 a と認証サーバ 2 0 0 a 等との間の検証処理]

続いて、車両 1 0 0 a において運転モードの切り替えが検知され、車両 1 0 0 a と認証サーバ 2 0 0 a 等との間で当該切り替えを検証する処理について説明する。ここでは、車両 1 0 0 a から認証サーバ 2 0 0 a 等のうちの一の認証サーバ 2 0 0 a に、当該切り替えを示す切り替え情報と車両 1 0 0 a の第 1 の識別子を含む第 1 トランザクションデータを送信する場合について説明する。

【 0 1 0 2 】

図 9 A は、本実施の形態に係る車両 1 0 0 a と認証サーバ 2 0 0 a 等との間の第 1 検証処理を示すシーケンス図である。図 9 B は、図 9 A に示すステップ S 2 0 1 の詳細処理を示すフローチャートである。図 9 C は、図 9 A に示すステップ S 2 0 5 の詳細処理を示すフローチャートである。ここで、第 1 検証処理を、車両 1 0 0 a において運転モードの切り替えが検知され、当該切り替えを示す切り替え情報を含む第 1 トランザクションデータが検証されるまでの処理として説明する。

10

【 0 1 0 3 】

まず、ステップ S 2 0 1 において、車両 1 0 0 a のゲートウェイ 1 0 1 は、車両 1 0 0 a において運転モードの切り替えが行われたことを検知する。

【 0 1 0 4 】

ここで、ステップ S 2 0 1 の詳細処理について、図 9 B を用いて説明する。すなわち、車両 1 0 0 a のゲートウェイ 1 0 1 は、まず、車載ネットワークに接続している運転アシスト部 1 2 0 用の E C U 1 2 1 が送信するメッセージから、運転アシスト部 1 2 0 のアシスト機能の切り替えとして運転モードの切り替えを検知したかを確認する (S 2 0 1 1) 。ステップ S 2 0 1 1 において、ゲートウェイ 1 0 1 は、運転モードの切り替えを検知した場合 (S 2 0 1 1 で Y) 、ステップ S 2 0 3 に進む。なお、ステップ S 2 0 1 1 において、ゲートウェイ 1 0 1 は、運転モードの切り替えを検知しなかった場合 (S 2 0 1 1 で N) 、第 1 検証処理を終了する。

20

【 0 1 0 5 】

次に、ステップ S 2 0 3 において、車両 1 0 0 a のゲートウェイ 1 0 1 は、運転モードの切り替えを示す切り替え情報と車両 1 0 0 a を示す第 1 の識別子を含む第 1 トランザクションデータを生成する。本実施の形態では、第 1 トランザクションデータは、例えば、切り替え情報及び第 1 の識別子と、当該切り替え情報及び第 1 の識別子を含む情報に対する署名などの認証情報とを含めて生成される。

30

【 0 1 0 6 】

次に、ステップ S 2 0 4 において、車両 1 0 0 a のゲートウェイ 1 0 1 は、生成した第 1 トランザクションデータを認証サーバ 2 0 0 a に送信する。なお、図 9 A では、車両 1 0 0 a は、生成した第 1 トランザクションデータを認証サーバ 2 0 0 a に送信する例が示されているが、これに限らない。認証サーバ 2 0 0 a 等のうちのいずれの認証サーバに送信してもよい。

【 0 1 0 7 】

次に、ステップ S 2 0 5 において、認証サーバ 2 0 0 a は、取得した第 1 トランザクションデータの検証を行い、成功した場合に、記録部 2 1 6 に第 1 トランザクションデータを記録させて、ステップ S 2 0 7 に進む。

40

【 0 1 0 8 】

ここで、ステップ S 2 0 5 の詳細処理について、図 9 C を用いて説明する。すなわち、認証サーバ 2 0 0 a は、まず、取得した第 1 トランザクションデータの検証を行い、成功したか否かを確認する (S 2 0 5 1) 。より詳細には、認証サーバ 2 0 0 a は、第 1 トランザクションデータに含まれる第 1 の識別子が記録部 2 1 6 に予め記録されている正規の車両を示す第 2 の識別子に含まれており正当であるかと、第 1 トランザクションデータに含まれる署名が正当であるかを確認する。つまり、認証サーバ 2 0 0 a は、第 1 の識別子及び署名がいずれも正当であるか否かを確認する。ステップ S 2 0 5 1 において、認証サーバ 2 0 0 a は、第 1 の識別子及び署名が正当であることを確認し、第 1 トランザクシ

50

ョンデータの検証が成功した場合（S 2 0 5 1でY）、記録部 2 1 6 に第 1 トランザクションデータを記録させて（S 2 0 5 2）、ステップ S 2 0 7 に進む。なお、ステップ S 2 0 5 1 において、認証サーバ 2 0 0 a は、第 1 トランザクションデータの検証が成功しなかった場合（S 2 0 5 1でN）、車両 1 0 0 a のゲートウェイ 1 0 1 にその旨を通知し（S 2 0 5 3）、第 1 検証処理を終了する。なお、認証サーバ 2 0 0 a は、車両 1 0 0 a だけでなく、カーメーカサーバ 3 0 0 にその旨を通知後に、第 1 検証処理を終了してもよい。これにより、カーメーカサーバ 3 0 0 は、不正な車両 1 0 0 a を検知したことを知ることができる。

【 0 1 0 9 】

次に、ステップ S 2 0 7 において、認証サーバ 2 0 0 a は、取得した第 1 トランザクションデータの複製を、他の認証サーバ 2 0 0 b、2 0 0 c に転送する。他の認証サーバ 2 0 0 b、2 0 0 c でも転送され取得した第 1 トランザクションデータを検証する。この検証処理は、図 9 C で説明した処理と同様である。

10

【 0 1 1 0 】

次に、ステップ S 2 0 8 において、認証サーバ 2 0 0 a と認証サーバ 2 0 0 b と認証サーバ 2 0 0 c とは、コンセンサスアルゴリズムを実行する。コンセンサスアルゴリズムを実行することで、認証サーバ 2 0 0 a と認証サーバ 2 0 0 b と認証サーバ 2 0 0 c とが取得した第 1 トランザクションデータが正当なトランザクションデータであると検証される。認証サーバ 2 0 0 a、2 0 0 b 及び 2 0 0 c は、検証済みの第 1 トランザクションデータを含むブロックの生成を行う。

20

【 0 1 1 1 】

次に、第 1 検証処理に続く第 2 検証処理について説明する。

【 0 1 1 2 】

図 1 0 A は、本実施の形態に係る車両 1 0 0 a と認証サーバ 2 0 0 a 等との間の第 2 検証処理を示すシーケンス図である。図 1 0 B は、図 1 0 A に示すステップ S 2 0 9 の詳細処理を示すフローチャートである。図 1 0 C は、図 1 0 A に示すステップ S 2 1 3 の詳細処理を示すフローチャートである。図 1 0 D は、図 1 0 A に示すステップ S 2 1 5 の詳細処理を示すフローチャートである。第 2 検証処理は、運転モードの切り替えを示す第 1 トランザクションデータが記録される第 1 検証処理に続いて行われる。より詳細には、第 2 検証処理は、第 1 検証処理後において、手動運転モードから自動運転モードへの運転モードの切り替わりを継続することをユーザが確認したことを含む第 2 トランザクションデータが検証されるまでの処理である。

30

【 0 1 1 3 】

まず、ステップ S 2 0 9 において、認証サーバ 2 0 0 a は、第 1 トランザクションデータに含まれる運転モードの切り替えの判定を行う。

【 0 1 1 4 】

ここで、ステップ S 2 0 9 の詳細処理について、図 1 0 B を用いて説明する。すなわち、認証サーバ 2 0 0 a は、まず、切り替えられた運転モードが、自動運転モードであるか手動運転モードであるかを確認する（S 2 0 9 1）。より詳細には、認証サーバ 2 0 0 a は、ブロック生成済みの第 1 トランザクションデータに含まれる切り替え情報が示す切り替えられた運転モードが、自動運転モードであるか手動運転モードであるかを確認する。ステップ S 2 0 9 1 において、認証サーバ 2 0 0 a は、切り替えられた運転モードが、自動運転モードである場合（S 2 0 9 1 で自動運転モード）、自動運転モード切り替え画面を生成し（S 2 0 9 2）、ステップ S 2 1 2 に進む。なお、ステップ S 2 0 9 1 において、認証サーバ 2 0 0 a は、切り替えられた運転モードが、手動運転モードである場合（S 2 0 9 1 で手動運転モード）、手動運転モード切り替え画面を生成し（S 2 0 9 3）、ステップ S 2 1 2 に進む。

40

【 0 1 1 5 】

次に、ステップ S 2 1 2 において、認証サーバ 2 0 0 a は、ステップ S 2 0 9 で生成した画面を示す画面情報を、車両 1 0 0 a に送信する。

50

【0116】

次に、ステップS213において、車両100aは、認証サーバ200aから取得した画面を表示する。本実施の形態では、車両100aは、当該画面を、ヘッドユニット140で表示する。

【0117】

ここで、ステップS213の詳細処理について、図10Cを用いて説明する。すなわち、車両100aは、まず、認証サーバ200aから取得した画面が、自動運転モード切り替え画面であるか手動運転モード切り替え画面であるかを確認する(S2131)。ステップS2131において、車両100aは、認証サーバ200aから取得した画面が、自動運転モード切り替え画面である場合(S2131で自動運転モード切り替え画面)、自動運転モード切り替え画面を表示する(S2132)。本実施の形態では、自動運転モード切り替え画面は、例えば図11に示すような画面である。ここで、図11は、本実施の形態に係る車両100aで表示される画面表示の一例を示す図である。図11では、「手動運転モードへの切り替えが検出されました。自動運転モードを継続しますか?」といった画面表示の例が示されている。すなわち、図11には、車両100aにおいて運転モードが自動運転モードに切り替わったことと、切り替わった自動運転モードをそのまま継続するかをユーザに確認する(または承認させる)ための画面表示の一例が示されている。そして、図11に示す画面において、ユーザが「はい」を選択すると、切り替わった自動運転モードをそのまま継続することをユーザが確認または承認したことになる。一方、図11に示す画面において、ユーザが「いいえ」を選択すると、ユーザが当該自動運転モードの切り替わりをそのまま継続することを承認しないことになる。すなわち、ステップS2133において、車両100aは、ユーザの承認を示す入力があったか否かを確認し、ユーザの承認を示す入力があれば(S2133でY)、ステップS214に進む。一方、ユーザの承認を示す入力がなければ(S2133でN)、第2検証処理を終了する。

【0118】

なお、ステップS2131において、車両100aは、認証サーバ200aから取得した画面が、手動運転モード切り替え画面である場合(S2131で手動運転モード切り替え画面)、手動運転モード切り替え画面を表示し(S2134)第2検証処理を終了する。

【0119】

本実施の形態では、手動運転モード切り替え画面は、例えば図12に示すような画面である。ここで、図12は、本実施の形態に係る車両100aで表示される画面表示の一例を示す図である。図12では、「手動運転モードへの切り替えが検出されました。」といった画面表示の例が示されている。すなわち、図12には、車両100aにおいて運転モードが手動運転モードに切り替わったことをユーザに通知するための画面表示の一例が示されている。図12に示す画面が表示されるときには、ユーザは手動運転中であるため、図12に示す画面には、ユーザに対して選択させるものは表示されない。

【0120】

次に、ステップS214において、ユーザの確認または承認を示す入力を示す確認情報を含む第2トランザクションデータを生成して、認証サーバ200aに送信する。ユーザの確認または承認を示す入力を示す確認情報とは、例えば図11に示される「はい」を示す情報であってもよいし、切り替わった自動運転モードをそのまま継続することを承認(確認)したことを示す情報であってもよい。

【0121】

次に、ステップS215において、認証サーバ200aは、取得した第2トランザクションデータの検証を行い、成功した場合に、記録部216に第2トランザクションデータを記録させて、ステップS217に進む。

【0122】

ここで、ステップS215の詳細処理について、図10Dを用いて説明する。すなわち、認証サーバ200aは、まず、取得した第2トランザクションデータの検証を行い、成功したか否かを確認する(S2151)。より詳細には、認証サーバ200aは、第2ト

10

20

30

40

50

ランザクションデータに含まれる署名が正当であることを検証する。ステップ S 2 1 5 1 において、認証サーバ 2 0 0 a は、署名が正当であることを確認し、第 2 トランザクションデータの検証が成功した場合 (S 2 1 5 1 で Y)、記録部 2 1 6 に第 2 トランザクションデータを記録させて (S 2 1 5 2)、ステップ S 2 1 7 に進む。なお、ステップ S 2 1 5 1 において、認証サーバ 2 0 0 a は、第 2 トランザクションデータの検証が成功しなかった場合 (S 2 1 5 1 で N)、車両 1 0 0 a のゲートウェイ 1 0 1 にその旨を通知し (S 2 1 5 3)、第 2 検証処理を終了する。

【 0 1 2 3 】

次に、ステップ S 2 1 7 において、認証サーバ 2 0 0 a は、取得した第 2 トランザクションデータの複製を、他の認証サーバ 2 0 0 b、2 0 0 c に転送する。なお、他の認証サーバ 2 0 0 b、2 0 0 c においても、転送され取得した第 2 トランザクションデータを検証する。この検証処理は、図 1 0 D で説明した処理と同様である。

10

【 0 1 2 4 】

次に、ステップ S 2 1 8 において、認証サーバ 2 0 0 a と認証サーバ 2 0 0 b と認証サーバ 2 0 0 c とは、コンセンサスアルゴリズムを実行する。コンセンサスアルゴリズムを実行することで、認証サーバ 2 0 0 a と認証サーバ 2 0 0 b と認証サーバ 2 0 0 c とが取得した第 2 トランザクションデータが正当なトランザクションデータであることが検証され。認証サーバ 2 0 0 a、2 0 0 b 及び 2 0 0 c は、検証済みの第 2 トランザクションデータを含むブロックの生成を行う。

【 0 1 2 5 】

20

[1 . 3 実施の形態の効果]

以上のように、本実施の形態に係る運転管理システム 1 0 等によれば、車両における運転モードの切り替えすべての履歴を記憶装置に記録することができるので、車両における運転モードの切り替えを確実に管理することができる。また、本実施の形態に係る運転管理システム 1 0 等によれば、手動運転モードから自動運転モードへ運転モードが切り替わった場合、切り替わった自動運転モードをそのまま継続することをユーザが承認または確認したことも履歴として記録する。このようにして、本実施の形態に係る運転管理システムは、車両における運転モードの切り替えを確実に管理することができる。

【 0 1 2 6 】

それにより、車両の故障または事故などの問題が発生した場合に、問題が発生した時点において車両が自動運転モードであったのか手動運転モードであったのかが客観的に判断できる。このため、自動運転システムを実現する自動運転機能に異常などの問題があったかの検証を確実に行うことができるので、自動運転機能に問題があった場合に自動運転機能の改善を行うことができる。よって、自動運転モード中の自動車事故をより抑制することができるので、より安全な自動運転システムを構築することができる。

30

【 0 1 2 7 】

さらに、本実施の形態に係る運転管理システム 1 0 等によれば、自動運転モード中の自動車事故または故障であったかを客観的に判断できるので、運転者に責任がないことがわかる。この結果、自動車事故または故障による補償等を、カーメーカ及び / または保険会社に求めることができる。

40

【 0 1 2 8 】

また、本実施の形態に係る運転管理システム 1 0 等によれば、改ざんが困難であるブロックチェーンにより車両における運転モードの切り替えのすべての履歴を管理するので、車両における運転モードの切り替えのすべての履歴が改ざんされずに後からでも確実に確認することができる。よって、自動運転システムを実現する自動運転機能に異常などの問題があったかの検証を確実にを行い、自動運転機能に問題があった場合に自動運転機能の改善を行うことができる。それにより、自動運転モード中の自動車事故をより抑制することができ、より安全な自動運転システムを構築することができる。

【 0 1 2 9 】

(変形例)

50

上記の実施の形態では、改ざんが困難であるブロックチェーンにより車両における運転モードの切り替えを含む運転アシスト部 120 のアシスト機能の切り替えを管理する運転管理システム 10 について説明したが、これに限らない。ブロックチェーンを用いずに運転モードの切り替えを含む運転アシスト部 120 のアシスト機能の切り替えを管理してもよい。以下、この場合を変形例として、上記の実施の形態と異なる点を中心に説明する。

【0130】

[1.4. システム構成]

本変形例の運転管理システム 10 は、上記の実施の形態と同様に、運転モードの切り替えを含む運転アシスト部 120 のアシスト機能の切り替えされたことを履歴として記録する。また、本変形例の運転管理システム 10 は、上記の実施の形態と同様に、手動運転モードから自動運転モードへの切り替えであれば自動運転モードを継続することをユーザに確認したことも履歴として記録する。

10

【0131】

本変形例の運転管理システム 10 は、例えば、図 1 に示す車両 100 a、100 b、100 c などの 1 以上の車両と、図 13 に示す認証サーバ 200 A などの 1 以上の認証サーバと、カーメーカサーバ 300 とを備える。なお、車両 100 a 等は、上記の実施の形態と比較して、第 1 トランザクションデータ及び第 2 トランザクションデータをブロックチェーンではないトランザクションデータとして生成する点のみが異なり、他は同様である。また、カーメーカサーバ 300 は、上記の実施の形態と比較して、第 3 トランザクションデータをブロックチェーンではないトランザクションデータとして生成する点のみが異なり、他は同様である。認証サーバ 200 A については、後述する。

20

【0132】

[1.4.1 認証サーバ 200 A の構成]

図 13 は、実施の形態の変形例に係る認証サーバ 200 A の機能構成を示すブロック図である。図 5 と同様の要素には同一の符号を付しており、詳細な説明は省略する。

【0133】

図 13 に示す認証サーバ 200 A は、上記の実施の形態に係る認証サーバ 200 a に対して、トランザクションデータ生成部 213 A の構成が異なり、ブロック生成部 214 が無い点で異なる。

【0134】

トランザクションデータ生成部 213 A は、車両 100 a 等から確認情報を取得した場合、ブロックチェーンではないトランザクションデータである第 2 トランザクションデータを生成してもよい。その他は、同様であるので説明を省略する。

30

【0135】

[1.5 動作等]

以下、以上のように構成された本変形例の運転管理システム 10 の処理動作について説明する。

【0136】

[1.5.1 カーメーカサーバ 300 と認証サーバ 200 A との間の登録処理]

まず、認証サーバ 200 A において手動運転と自動運転とが切り替え可能な正規の車両を一意に識別する第 2 の識別子を登録する登録処理について説明する。ここでは、カーメーカサーバ 300 から、認証サーバ 200 A に第 2 の識別子を含む第 3 トランザクションデータを送信する場合について説明する。

40

【0137】

図 14 は、実施の形態の変形例に係るカーメーカサーバ 300 と認証サーバ 200 A 等との間の登録処理を示すシーケンス図である。なお、図 8 A 等と同様の要素には同一の符号を付しており、詳細な説明は省略する。図 15 は、実施の形態の変形例に係る認証サーバ 200 A が第 3 トランザクションデータを記録する際に用いるデータ構造の一例である。

【0138】

まず、ステップ S101 において、カーメーカサーバ 300 は、手動運転と自動運転と

50

が切り替え可能な正規の車両を示す第2の識別子を取得する。

【0139】

次に、ステップS102において、カーメーカサーバ300は、取得した正規の車両を示す第2の識別子を含む第3トランザクションデータを生成する。ここで、第3トランザクションデータは、ブロックチェーンとして記録されないトランザクションデータである。

【0140】

次に、ステップS103において、カーメーカサーバ300は、生成した第3トランザクションデータを認証サーバ200Aに送信する。

【0141】

次に、ステップS104Aにおいて、認証サーバ200Aは、取得した第3トランザクションデータの検証を行い、成功した場合に、ステップS104Bに進む。なお、ステップS104Aの詳細処理については、図8Bで説明した通りであるのでここでの説明は省略する。

10

【0142】

次に、ステップS104Bにおいて、認証サーバ200Aは、記録部216に第3トランザクションデータを記録させる。より具体的には、認証サーバ200Aは、例えば図15に示すように、登録処理すなわち登録を示す取引において、取得した第2の識別子で示される車両の種別が、手動運転及び自動運転を切り替え可能な正規の自動車であることを記憶装置201Aに記録する。このようにして、認証サーバ200Aは、ブロックチェーンではない第3トランザクションデータを記憶装置201Aに記録する。

20

【0143】

[1.5.2 車両100aと認証サーバ200Aとの間の検証処理]

続いて、車両100aにおいて運転モードの切り替えが検知され、車両100aと認証サーバ200Aとの間で当該切り替えを検証する処理について説明する。ここでは、車両100aから、認証サーバ200Aに、当該切り替えを示す切り替え情報と車両100aの第1の識別子を含む第1トランザクションデータを送信する場合について説明する。

【0144】

図16は、実施の形態の変形例に係る車両100aと認証サーバ200Aとの間の第1検証処理を示すシーケンス図である。なお、図9A等と同様の要素には同一の符号を付しており、詳細な説明は省略する。図17は、実施の形態の変形例に係る認証サーバ200Aが第1トランザクションデータを記録する際に用いるデータ構造の一例である。ここでも、第1検証処理を、車両100aにおいて運転モードの切り替えが検知され、当該切り替えを示す切り替え情報を含む第1トランザクションデータが検証されるまでの処理として説明する。

30

【0145】

まず、ステップS201において、車両100aのゲートウェイ101は、車両100aにおいて運転モードの切り替えが行われたことを検知する。ステップS201の詳細処理については、図9Bで説明した通りであるのでここでの説明は省略する。

【0146】

次に、ステップS203において、車両100aのゲートウェイ101は、運転モードの切り替えを示す切り替え情報と車両100aを示す第1の識別子とを含む第1トランザクションデータを生成する。本変形例でも、第1トランザクションデータは、例えば、切り替え情報及び第1の識別子と、当該切り替え情報及び当該第1の識別子を含む情報に対する署名などの認証情報とを含めて生成される。

40

【0147】

次に、ステップS204において、車両100aのゲートウェイ101は、生成した第1トランザクションデータを認証サーバ200Aに送信する。

【0148】

次に、ステップS205Aにおいて、認証サーバ200Aは、取得した第1トランザクションデータの検証を行い、成功した場合に、ステップS205Bに進む。なお、ステッ

50

プ S 2 0 5 B の詳細処理については、図 9 C で説明した通りであるのでここでの説明は省略する。

【 0 1 4 9 】

次に、ステップ S 2 0 5 B において、認証サーバ 2 0 0 A は、記録部 2 1 6 に第 1 トランザクションデータを記録させる。より具体的には、認証サーバ 2 0 0 A は、例えば図 1 7 に示すように、取得した第 1 の識別子で示される車両における運転モードの切り替えを示す取引において、手動運転モードに切り替わったか自動運転モードに切り替わったかを記憶装置 2 0 1 A に記録する。また、認証サーバ 2 0 0 A は、例えば図 1 7 に示すように、運転モードの切り替えを示す取引において、自動運転モードに切り替わった場合ユーザの承認があるか否かについてさらに記憶装置 2 0 1 A に記録する。このようにして、認証サーバ 2 0 0 A は、第 1 トランザクションデータを記憶装置 2 0 1 A に記録する。

10

【 0 1 5 0 】

なお、第 1 検証処理に続く第 2 検証処理についても、同様に、認証サーバ 2 0 0 A は、ブロックチェーンを利用しないデータ構造を用いて、第 3 トランザクションデータを記憶装置 2 0 1 A に記録する。

【 0 1 5 1 】

[2 . その他変形例]

以上、本開示を上記の実施の形態及び変形例に基づいて説明してきたが、本開示は、上記各実施の形態に限定されないのももちろんである。以下のような場合も本開示に含まれる。

20

【 0 1 5 2 】

(1) 上記の実施の形態では、認証サーバとカーメーカサーバは別の装置として説明したが、認証サーバとカーメーカサーバとが同一の装置で構成されていてもよい。

【 0 1 5 3 】

(2) 上記の実施の形態及び変形例では、認証サーバは、運転モードの切り替えでエラーを検知した場合、車両に通知するが、カーメーカサーバにも通知するとしてもよい。

【 0 1 5 4 】

(3) 上記の実施の形態における認証サーバが管理するブロックチェーンはカーメーカサーバから参照できるとしてもよい。また、当該ブロックチェーンは、カーメーカだけでなく、保険会社のサーバ (不図示) から参照できるとしてもよい。

30

【 0 1 5 5 】

(4) 上記の実施の形態及び変形例では、車両 1 0 0 a 等のゲートウェイ 1 0 1 は運転モードの切り替えを検知し、当該切り替えを示す切り替え情報と当該車両 1 0 0 a 等を示す第 1 の識別子を含む第 1 トランザクションデータを送信しているが、これに限らない。当該ゲートウェイ 1 0 1 は、第 1 トランザクションデータを、運転アシスト部 1 2 0 で動作している機能及び / または運転アシスト部 1 2 0 の E C U 1 2 1 を示す識別子も含めて生成してもよい。これにより、自動運転モードにおいて運転アシスト部 1 2 0 どの機能が動作しているときに車両 1 0 0 a 等が問題すなわち自動運転機能が異常になったかなどを容易に検証することも可能となる。また、車両 1 0 0 a 等が問題すなわち自動運転機能が異常になったとき、運転アシスト部 1 2 0 の E C U 1 2 1 の識別子により、対応している運転アシスト部 1 2 0 で動作する機能の特定も容易に行うことができる。

40

【 0 1 5 6 】

(5) 上記の実施の形態及び変形例では、車両 1 0 0 a 等のゲートウェイ 1 0 1 は、運転モードの切り替えを検知していたが、これに限らない。車両 1 0 0 a 等が有する車載ネットワーク内のいずれの E C U またはすべての E C U に同様の機能があり、運転モードの切り替えを検知するとしてもよい。

【 0 1 5 7 】

(6) 上記の実施の形態及び変形例では、手動運転モードから自動運転モードに切り替わったことを検知したときに、車両 1 0 0 a 等のヘッドユニット 1 4 0 に運転者等のユーザに対して画面の表示を行わせ、ユーザによる情報入力をさせていたが、これに限らない

50

。手動運転モードから自動運転モードに切り替わったことを検知したときに、音声によりユーザに対して通知及び自動運転モードの継続の確認を行い、ユーザの音声により情報入力させるとしてもよい。

【 0 1 5 8 】

(7) 上記の実施の形態及び変形例では、カーメカサーバは車両を示す第 1 の識別子を取得しているが、これに限らない。カーメカサーバは、当該第 1 の識別子に加えて当該車両に搭載されている運転アシスト機能または自動運転機能も取得するとしてもよい。これにより、認証サーバが受信した第 2 トランザクションデータに含まれる運転アシスト機能または自動運転機能とカーメカサーバから取得した運転アシスト機能または自動運転機能が一致しているかの検証をすることも可能となる。

10

【 0 1 5 9 】

(8) 上記の実施の形態及び変形例では、車両 1 0 0 a 等のゲートウェイ 1 0 1 は、運転モードの切り替えを検知し、認証サーバに送信していたが、運転モードの切り替えを示す切り替え情報以外に、当該車両 1 0 0 a 等が有する車載ネットワーク上に送信されるメッセージを送信するとしてもよい。これにより、認証サーバに記録されている第 1 トランザクションデータを含むトランザクションデータを参照し、当該車載ネットワーク上のメッセージを確認することで、運転モードの切り替えを検出することが可能となる。また、手動運転モード中のどのタイミングで自動運転モードに切り替えたかの確認もすることができる。

【 0 1 6 0 】

20

(9) 上記実施の形態及び変形例では、車両 1 0 0 a 等のゲートウェイ 1 0 1 は、運転モードの切り替えを検知し、当該切り替えを示す切り替え情報と第 1 の識別子とを含む第 1 トランザクションデータを認証サーバに送信しているが、これに限らない。当該ゲートウェイ 1 0 1 は、第 1 トランザクションデータに、当該車両 1 0 0 a に搭載されている自動運転機能または自動運転モードで実行されている自動運転レベルをさらに含めて送信するとしてもよい。

【 0 1 6 1 】

より具体的には、トランザクションデータ生成部 1 1 0 2 は、検知部 1 1 0 1 が検知した切り替えを示す情報が手動運転モードから自動運転モードに切り替えられたことを示す場合、検知部 1 1 0 1 が検知した切り替えを示す情報、及び、当該車両を示す第 1 の識別子に加えて、自動運転モードにおける自動運転レベルを示す情報を含む第 1 トランザクションデータを生成し、第 1 通信部 1 1 0 3 を介して一の認証サーバに送信してもよい。なお、この場合、図 1 0 A 等を示すステップ S 2 1 2 及び S 2 1 3 において、運転者に自動運転モードを継続するか否かをユーザに確認するための画面を作成し表示する際に、さらに、自動運転レベルも確認するとしてもよい。また、自動運転レベルは、0 ~ 5 までである。レベル 0 では、運転者がすべてを操作することを示し、レベル 1 では、自動運転システムがステアリング操作、加減速のどちらかを支援する運転支援を行うことを示す。レベル 2 では、自動運転システムがステアリング操作、加減速のどちらも支援する運転支援を行うことを示す。レベル 3 では、特定の場所で自動運転システムが全てを操作し、緊急時は運転者が操作するといった自動運転を行うことを示す。レベル 4 では、特定の場所で自動運転システムが全てを操作するといった自動運転を行うことを示す。レベル 5 では、場所の限定なく自動運転システムが全てを操作する完全自動運転を行うことを示す。

30

40

【 0 1 6 2 】

また、トランザクションデータ生成部 1 1 0 2 は、検知部 1 1 0 1 が検知した切り替えを示す情報が手動運転モードから自動運転モードに切り替えられたことを示す場合、検知部 1 1 0 1 が検知した切り替えを示す情報、及び、当該車両を示す第 1 の識別子に加えて、自動運転モードにおいて動作する運転アシスト機能を示す情報を含む第 1 トランザクションデータを生成し、第 1 通信部 1 1 0 3 を介して一の認証サーバに送信してもよい。

【 0 1 6 3 】

(1 0) 上記実施の形態及び変形例では、車両 1 0 0 a 等のゲートウェイ 1 0 1 は、運

50

転モードの切り替えを検知し、当該切り替えを示す切り替え情報と第1の識別子とを含む第1トランザクションデータを認証サーバに送信しているが、これに限らない。当該ゲートウェイ101は、第1トランザクションデータに、当該車両100aに搭載されるセンサから取得したセンサ情報をさらに含めて送信してもよい。ここで、センサ情報は、運転者の状態を含む車両100aの運転者に関する情報である。

【0164】

より具体的には、1以上の車両のそれぞれは、さらに、所定期間毎またはイベント毎に、当該車両の運転者に関する情報を示すセンサ情報を取得するセンサ部を備え、当該センサ部は、取得したセンサ情報をトランザクションデータ生成部1102に送信し、トランザクションデータ生成部1102は、切り替えを示す情報、第1の識別子、及びセンサ情報を含む第1トランザクションデータを生成し、第1通信部1103を介して一の認証サーバに送信してもよい。

10

【0165】

例えば、センサ部は、車両100a等内に設置されたカメラでもよい。この場合、センサ情報は、カメラが撮影した運転者の画像、動画又は虹彩情報を含むとしてもよい。また、例えば、センサ部は、車両100a等内に設置されたミリ波レーダであってもよい。この場合、センサ情報は、ミリ波により取得した運転者の心拍を示す情報を含むとしてもよい。

【0166】

(11)上記の実施の形態および変形例における各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAMまたはハードディスクユニットには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

20

【0167】

(12)上記の実施の形態および変形例における各装置は、構成する構成要素の一部または全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

30

【0168】

また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又はすべてを含むように1チップ化されてもよい。

【0169】

また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)又は、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。

40

【0170】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

【0171】

(13)上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なI

50

Cカードまたは単体のモジュールから構成されているとしてもよい。前記ICカードまたは前記モジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ICカードまたは前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ICカードまたは前記モジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【0172】

(14) 本開示は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

10

【0173】

また、本開示は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(登録商標) Disc)、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

【0174】

また、本開示は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

20

【0175】

また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

【0176】

また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0177】

(15) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

30

【産業上の利用可能性】

【0178】

本開示は、運転管理システム、車両、及び、運転管理システムの情報処理方法に利用でき、特に自動車などの車両において運転モードの切り替えを確実に管理する運転管理システム、車両、及び、運転管理システムの情報処理方法に利用できる。

【符号の説明】

【0179】

100 a、100 b、100 c 車両

101 ゲートウェイ

110 エンジン

40

111、121、131、141、151 ECU

120 運転アシスト部

130 バッテリー

140 ヘッドユニット

150 通信部

200 a、200 A、200 b、200 c 認証サーバ

211 画面生成部

212 トランザクションデータ検証部

213、213 A トランザクションデータ生成部

214 ブロック生成部

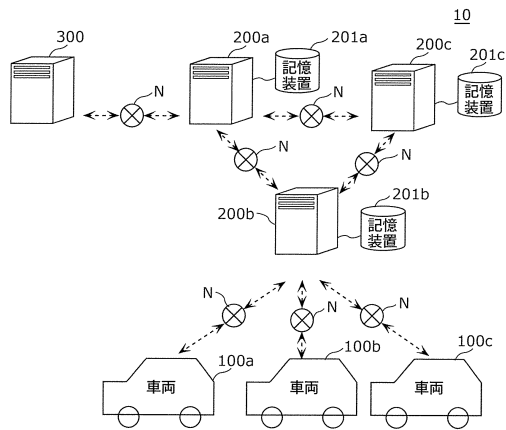
50

- 2 1 5 同期部
- 2 1 6 記録部
- 2 1 7 第2通信部
- 3 0 0 カーメーカサーバ
- 3 1 1 入力部
- 3 1 2 トランザクションデータ生成部
- 3 1 3 第3通信部
- 1 1 0 1 検知部
- 1 1 0 2 トランザクションデータ生成部
- 1 1 0 3 第1通信部
- 1 4 1 1 表示部
- 1 4 1 2 入力部

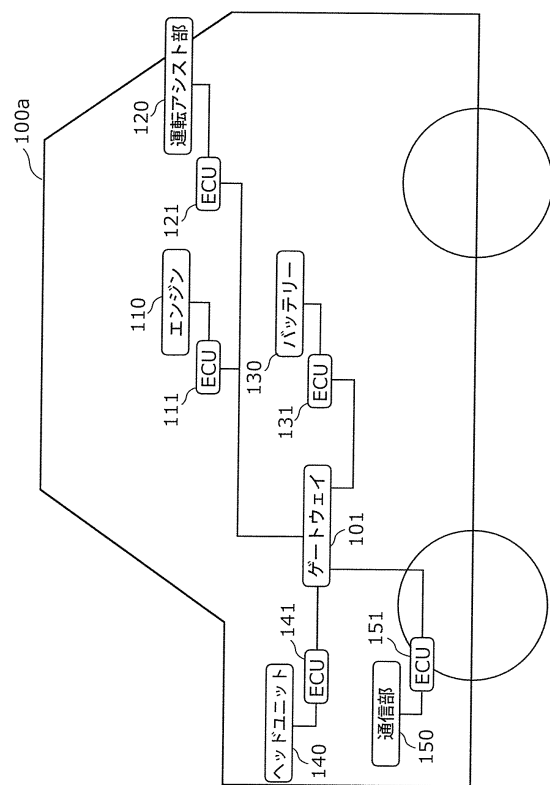
10

【図面】

【図1】



【図2】



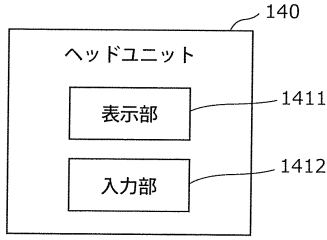
20

30

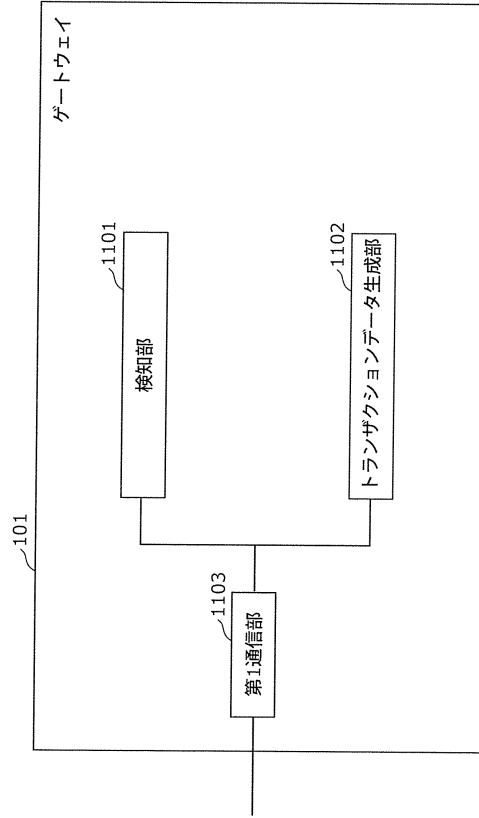
40

50

【図3】



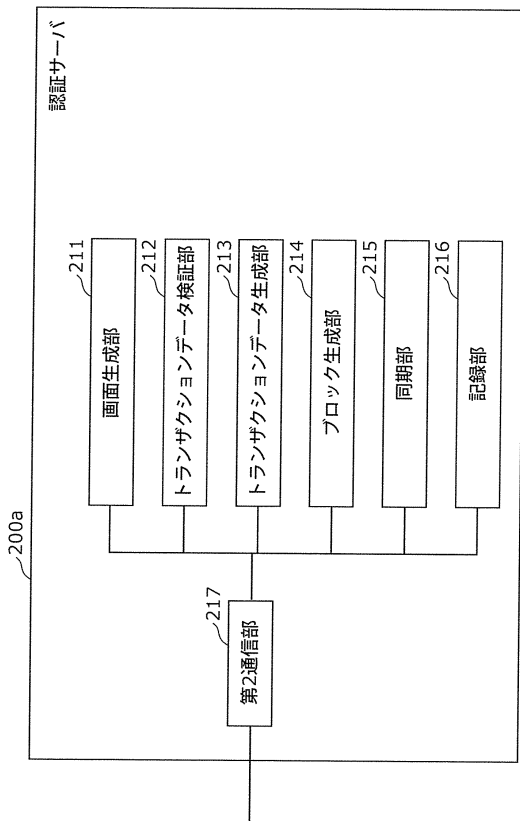
【図4】



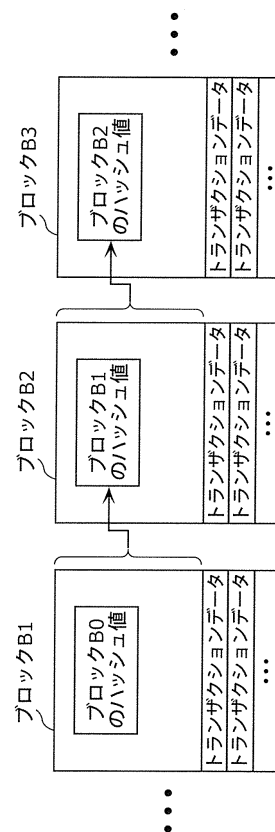
10

20

【図5】



【図6A】

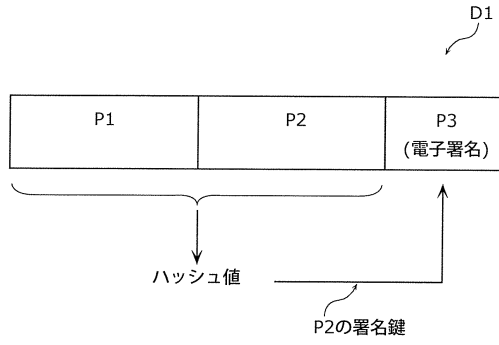


30

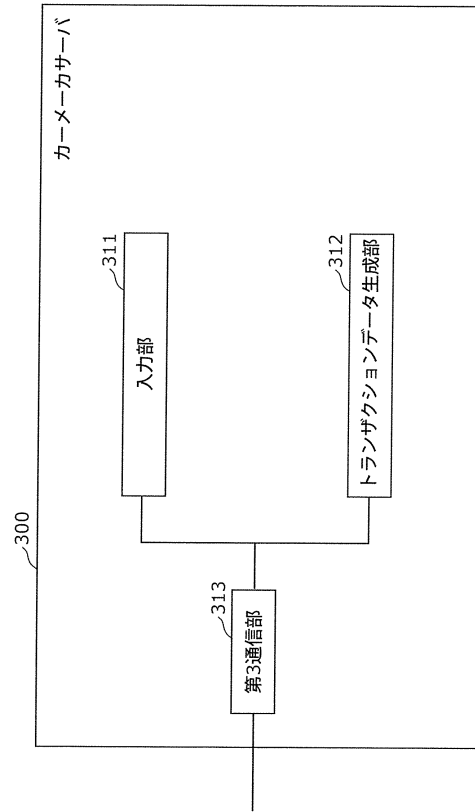
40

50

【図 6 B】



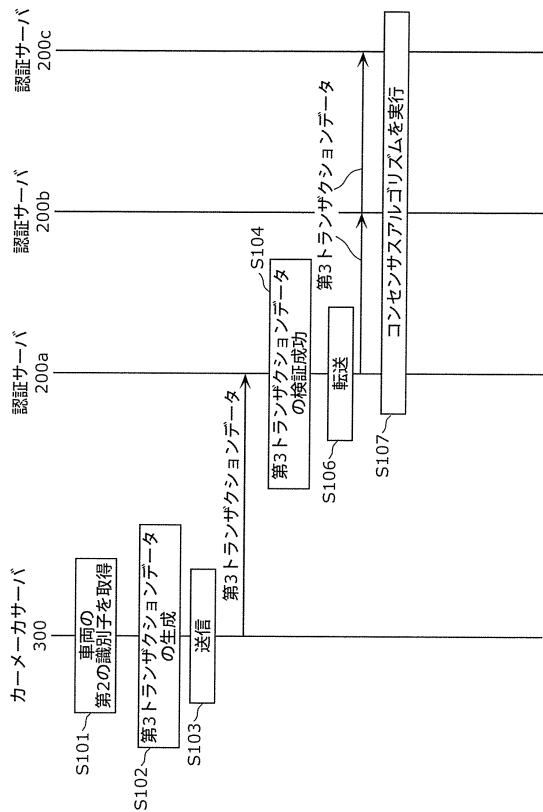
【図 7】



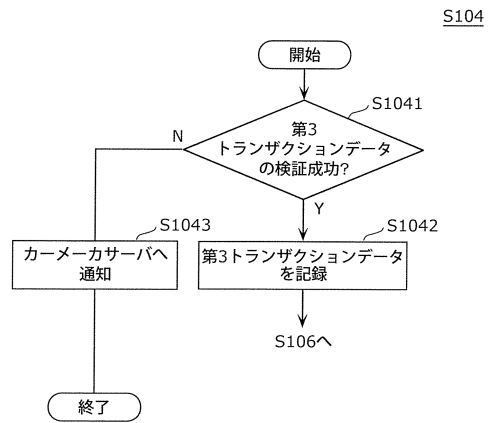
10

20

【図 8 A】



【図 8 B】

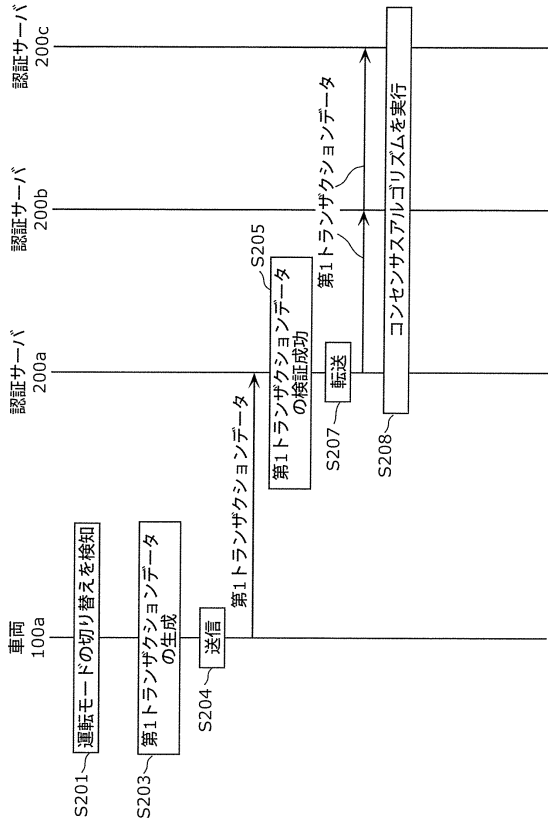


30

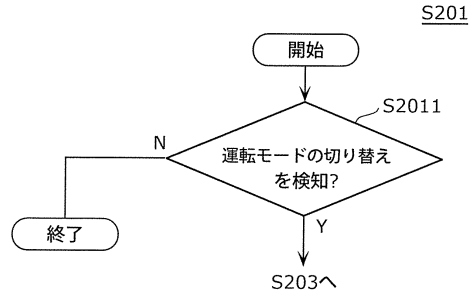
40

50

【図 9 A】



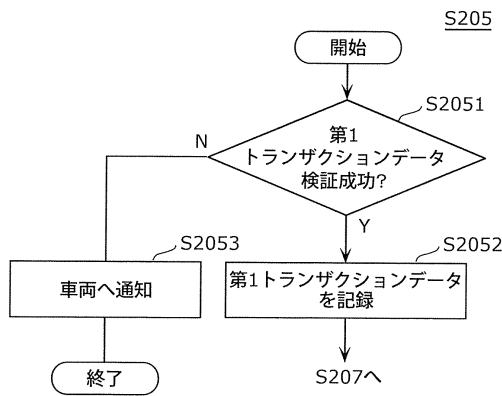
【図 9 B】



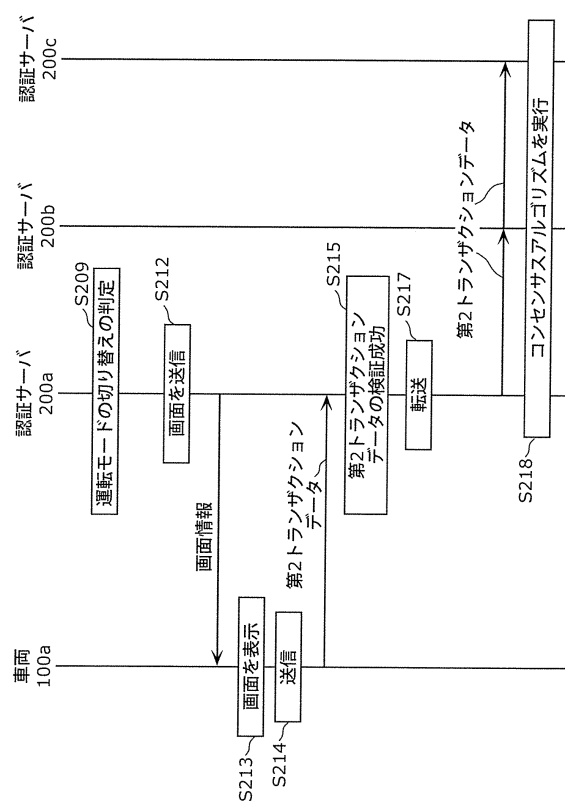
10

20

【図 9 C】



【図 10 A】

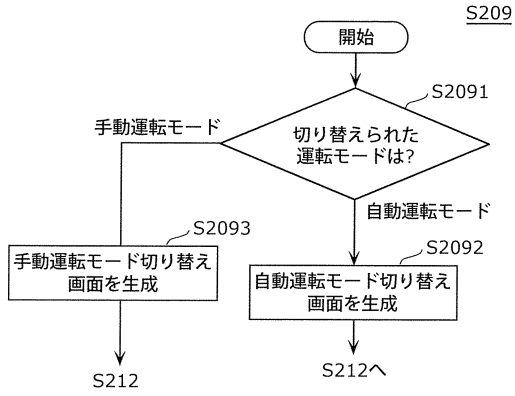


30

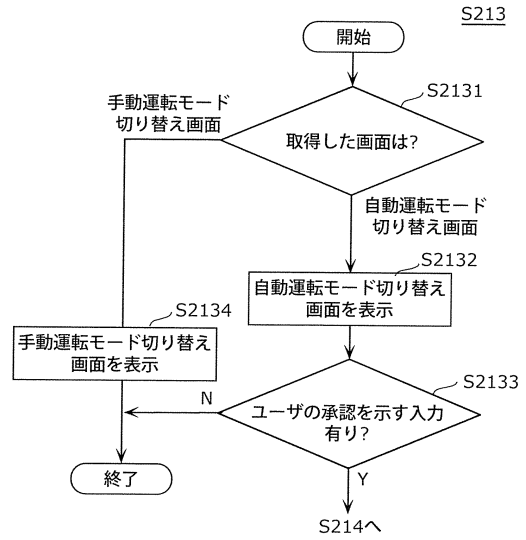
40

50

【図10B】

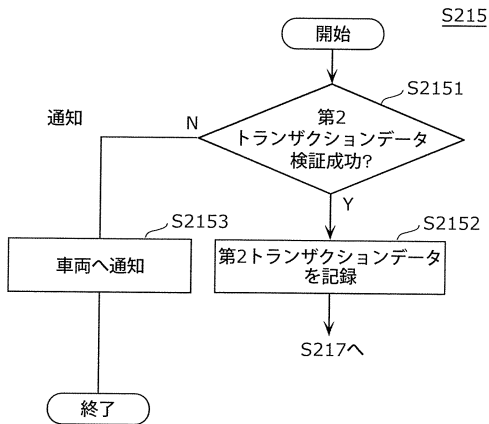


【図10C】

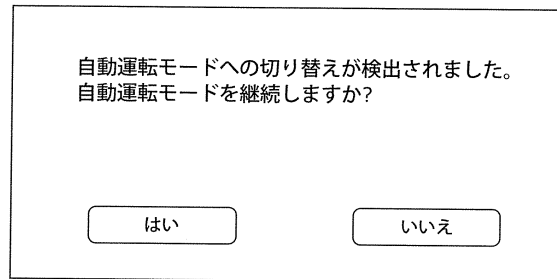


10

【図10D】



【図11】



20

30

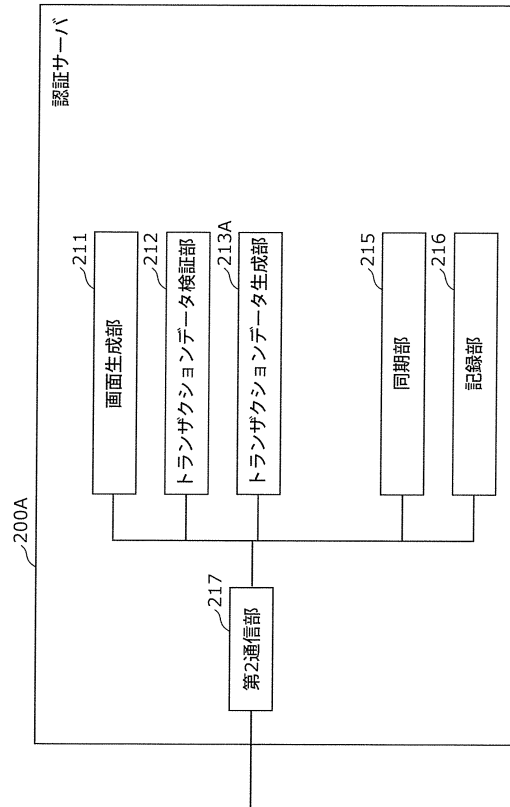
40

50

【 図 1 2 】

手動運転モードへの切り替えが検出されました。

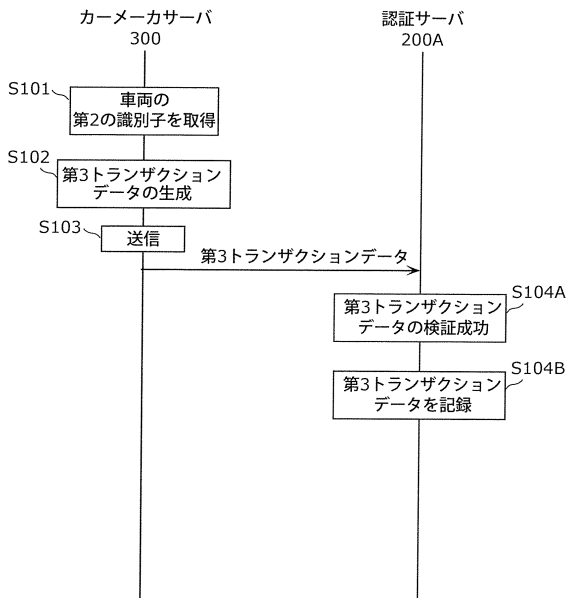
【 図 1 3 】



10

20

【 図 1 4 】



【 図 1 5 】

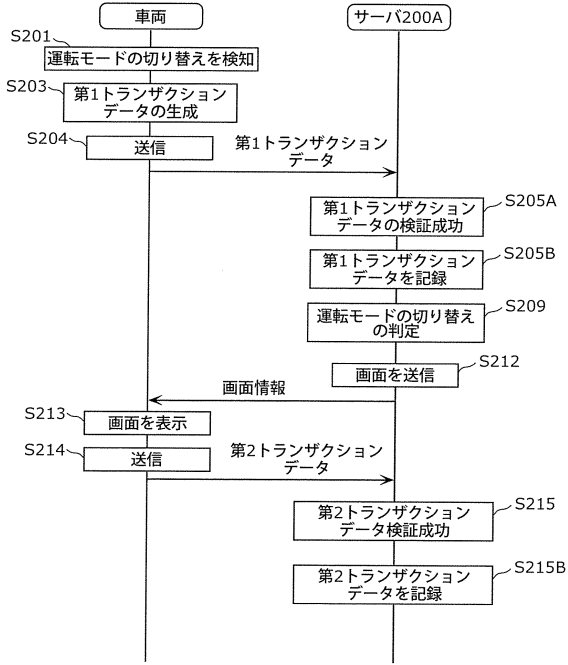
第2の識別子	取引	車両種別
100a	登録	自動車
100b	登録	自動車
....

30

40

50

【図16】



【図17】

第1の識別子	取引	運転モード	ユーザ承認の有無
100a	運転モードの切り替え	手動運転モード	—
100b	運転モードの切り替え	自動運転モード	有り
....

10

20

30

40

50

フロントページの続き

- (72)発明者 海上 勇二
大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内
- (72)発明者 添田 純一郎
大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内
- (72)発明者 大森 基司
大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内

合議体

審判長 山本 信平

審判官 中尾 麗

審判官 青木 良憲

- (56)参考文献 米国特許出願公開第 2 0 1 3 / 0 3 0 4 5 1 4 (U S , A 1)
特表 2 0 1 6 - 5 0 3 7 4 0 (J P , A)
特開 2 0 1 5 - 2 1 9 1 2 8 (J P , A)
特開 2 0 1 3 - 1 9 3 5 9 8 (J P , A)
特開 2 0 1 3 - 2 5 0 6 4 0 (J P , A)
国際公開第 2 0 1 6 / 0 8 0 0 7 0 (W O , A 1)
森岡剛, 自動車、ブロックチェーン、そして決済, Infcurion Insight, 日本, 株式会社インフキュリオン, 2016年01月15日, <https://insight.infcurion.com/fintech/auto-blockchain-and-payment/>
佐古和恵, 履歴蓄積システムとしてのブロックチェーン、その原理動作に迫る, 日経XTECH, 日本, 株式会社日経BP, 2016年08月22日, <https://xtech.nikkei.com/it/atcl/column/16/062400138/081200005/>
- (58)調査した分野 (Int.Cl., DB名)
B60W 10/00-10/30
B60W 30/00-60/00
G08G 1/00-99/00
G06F 21/30-21/46