

(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
2022年8月25日(25.08.2022)



(10) 国際公開番号

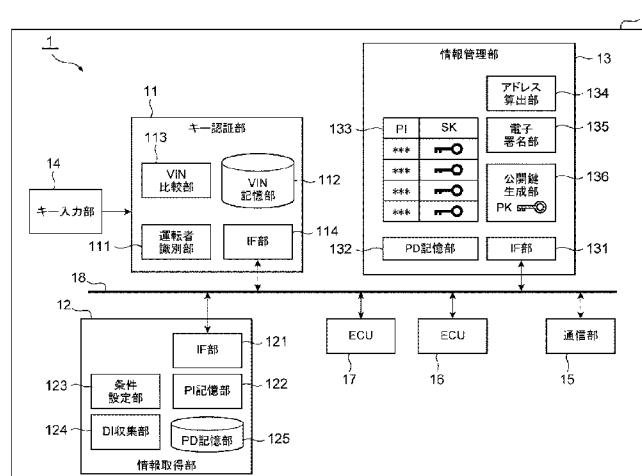
WO 2022/176240 A1

- (51) 国際特許分類:
G09C 1/00 (2006.01) *G06F 21/62* (2013.01)
G06F 21/32 (2013.01) *H04L 9/32* (2006.01)
- (21) 国際出願番号: PCT/JP2021/033001
- (22) 国際出願日: 2021年9月8日(08.09.2021)
- (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 2021-022213 2021年2月16日(16.02.2021) JP
- (71) 出願人: 日立 *A s t e m o* 株式会社(HITACHI *ASTEMO, LTD.*) [JP/JP]; 〒3128503 茨城県ひたちなか市高場2520番地 Ibaraki (JP).
- (72) 発明者: 山田 哲也 (YAMADA Tetsuya); 〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP). 清宮 大司(SEIMIYA Masashi); 〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP). 藤井 康広(FUJII Yasuhiro); 〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP).
- (74) 代理人: 特許業務法人平木国際特許事務所 (HIRAKI & ASSOCIATES); 〒1056232 東京都港区愛宕二丁目5-1 愛宕グリーンヒルズ MORIタワー32階 Tokyo (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,

(54) Title: INFORMATION MANAGEMENT SYSTEM

(54) 発明の名称: 情報管理システム

図2



- 11 ... Key verification unit
12 ... Information acquisition unit
13 ... Information management unit
14 ... Key input unit
15 ... Communication unit
17 ... ECU
111 ... Driver identification unit
112 ... VIN storage unit
113 ... VIN comparison unit
121 ... IF unit
122 ... PI storage unit
123 ... Condition setting unit
124 ... DI collection unit
125, 132 ... PD storage unit
134 ... Address calculation unit
135 ... Electronic signature unit
136 ... Public key generation unit
114, 121, 131 ... IF unit

(57) Abstract: The present disclosure provides an information management system which makes it possible to solve a problem pertaining to the handling of information related to each driver when a plurality of drivers drive one vehicle. An information management system 1 according to one embodiment of the present disclosure manages driver information DI pertaining to a driver of a vehicle V. The information management system 1 is equipped with a driver identification unit 111 for acquiring personal identification information PI for a driver, an information acquisition unit 12 for acquiring

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

添付公開書類:

一 国際調査報告 (条約第21条(3))

driver information DI which includes vehicle V travel information, and personal information storage units 125, 132 for storing personal information PD which associates the personal identification information PI and the driver information DI with one another.

(57) 要約: 本開示は、1台の車両を複数の運転者が運転する場合に、各々の運転者に係る情報の取り扱いに関する課題を解決することが可能な情報管理システムを提供する。本開示の一態様に係る情報管理システム1は、車両Vの運転者に関する運転者情報D1を管理する。情報管理システム1は、運転者の個人識別情報P1を取得する運転者識別部111と、車両Vの走行情報を含む運転者情報D1を取得する情報取得部112と、個人識別情報P1と運転者情報D1を関連付けた個別情報PDを記憶する個別情報記憶部125、132と、を備える。

明 細 書

発明の名称： 情報管理システム

技術分野

[0001] 本開示は、車両の運転者に関する情報を管理する情報管理システムに関する。

背景技術

[0002] 従来から車両に搭載される車載装置と、その車載装置とネットワークを介して通信を行うサーバとを備え、上記車両からプローブデータを収集するデータ収集システムが知られている（特許文献1、要約、請求項1等）。この従来のデータ収集システムにおいて、上記サーバは、データ収集条件決定部と、データ収集条件配信部と、プローブ受信処理部と、を備える。また、上記車載装置は、データ取得部と、収集データ絞込処理部と、プローブデータ送信部と、を備える。

[0003] 上記サーバのデータ収集条件決定部は、車両におけるプローブデータの収集頻度を含むデータ収集条件を決定する。また、上記サーバのデータ収集条件配信部は、上記データ収集条件決定部により決定されたデータ収集条件を車両に配信する。また、上記サーバのプローブ受信処理部は、車両から送信されるプローブデータを受信して記憶装置に蓄積する。

[0004] 上記車載装置のデータ取得部は、車両の周囲環境または状態に関するデータを取得する。また、上記車載装置の収集データ絞込処理部は、上記サーバから配信されたデータ収集条件に基づいて、上記データ取得部により取得されたデータからプローブデータを上記収集頻度ごとに抽出する。また、上記車載装置のプローブデータ送信部は、上記収集データ絞込処理部により上記収集頻度ごとに抽出されたプローブデータを上記サーバに送信する。

先行技術文献

特許文献

[0005] 特許文献1：特開2018-055191号公報

発明の概要

発明が解決しようとする課題

[0006] 上記従来のデータ収集システムによれば、車両で取得されたデータをサーバにおいて適切なデータ収集頻度で収集することができる（特許文献１、第０００８段落等）。しかしながら、この従来のデータ収集システムは、たとえばカーシェアリングなど、１台の車両を複数の運転者が運転する場合に、各々の運転者に係る情報の取り扱いに関する課題がある。

[0007] 本開示は、１台の車両を複数の運転者が運転する場合に、各々の運転者に係る情報の取り扱いに関する課題を解決することが可能な情報管理システムを提供する。

課題を解決するための手段

[0008] 本開示の一態様は、車両の運転者に関する運転者情報を管理する情報管理システムであって、前記運転者の個人識別情報を取得する運転者識別部と、前記車両の走行情報を含む前記運転者情報を取得する情報取得部と、前記個人識別情報と前記運転者情報を関連付けた個別情報を記憶する個別情報記憶部と、を備えることを特徴とする情報管理システムである。

発明の効果

[0009] 本開示の上記一態様によれば、１台の車両を複数の運転者が運転場合に、各々の運転者に係る情報の取り扱いに関する課題を解決することが可能な情報管理システムを提供することができる。

図面の簡単な説明

- [0010] [図１]本開示に係る情報管理システムの実施形態１を示すブロック図。
[図２]実施形態１に係る情報管理システムを搭載する車両のブロック図。
[図３]図２のキー入力部と無線通信を行う電子キーの一例を示すブロック図。
[図４]図２のキー入力部と無線通信を行うＰＤＡの一例を示すブロック図。
[図５]図２の情報管理システムによる処理の一例を示すフロー図。
[図６]実施形態２に係る情報管理システムを搭載する車両のブロック図。

[図7]図6の情報管理システムによる処理の一例を示すフロー図。

[図8]図6の情報管理システムによる処理の一例を示すフロー図。

[図9]図6の情報管理システムによる処理の一例を示すフロー図。

[図10]実施形態3に係る情報管理システムの運転者識別部のブロック図。

[図11]実施形態3に係る情報管理システムによる処理の一例を示すフロー図

。

発明を実施するための形態

[0011] 以下、図面を参照して本開示に係る情報管理システムの実施形態を説明する。

[0012] (実施形態1)

図1は、本開示に係る情報管理システムの実施形態1を示すブロック図である。図2は、実施形態1に係る情報管理システム1を搭載する車両Vのブロック図である。本実施形態の情報管理システム1は、車両Vの運転者に関する運転者情報を管理するシステムであり、たとえば、車両Vに搭載される車両システムである。車両Vは、たとえば、ガソリンエンジン車、ディーゼルエンジン車、ハイブリッド車、電気自動車、または、水素自動車である。

[0013] 車両Vは、図1に示すように、たとえば、無線通信回線RCL、無線基地局WBS、および有線通信回線WCLを介して、データセンタDCのサーバSや、分散型ネットワークDNを構成する複数のコンピュータPCに接続されている。分散型ネットワークDNを構成する複数のコンピュータPCは、P2P（ピアツーピア）ネットワーク方式のデータ通信を行う。

[0014] 情報管理システム1は、図2に示すように、たとえば、運転者識別部11を含むキー認証部11と、情報取得部12と、情報管理部13と、を備えている。また、情報管理システム1は、たとえば、車両Vに搭載されたキー入力部14、通信部15、複数の電子制御装置（ECU）16、17、および車載ネットワーク18を備えてもよい。また、情報管理システム1は、たとえば、図1に示すデータセンタDCのサーバSや、分散型ネットワークDNを構成するコンピュータPCなど、車両Vの外部の装置やネットワークを

含んでもよい。

[0015] 通信部 15 は、たとえば、無線通信回線 RCL を介して、車両 V の外部の無線基地局 WBS や通信機と通信可能な無線通信機を含む。ECU 16, 17 は、たとえば、車両 V のパワートレインや、先進運転支援システム (ADAS) や自動運転システム (ADS) を構成する各種のアクチュエータを制御するための電子制御装置である。車載ネットワーク 18 は、たとえば、コントローラ・エリア・ネットワーク (CAN) や、イーサネット (登録商標) などによって構成される。車両 V の他の一般的な構成については、図示および説明を省略する。

[0016] キー入力部 14 は、たとえば、車両 V のキーレスエントリーシステムを構成する電子キーや、車両 V のスマートエントリーシステムを構成するスマートキーまたは携帯情報端末との無線通信を行う。これにより、キー入力部 14 は、電子キー、スマートキー、または携帯情報端末から、車両識別番号 VIN を含む暗号化された情報を取得する。また、キー入力部 14 が取得する暗号化された情報は、たとえば、個人識別情報 PI を含んでいる。個人識別情報 PI は、たとえば、個人識別番号 PIN を含んでいる。キー入力部 14 は、電子キー、スマートキー、または携帯情報端末から取得した暗号化された情報を、たとえば、キー認証部 11 へ出力する。

[0017] 図 3 は、図 2 のキー入力部 14 と無線通信を行う電子キー 2 の一例を示すブロック図である。情報管理システム 1 は、たとえば、電子キー 2 を含んでもよい。電子キー 2 は、たとえば、アンテナ 21 と、マイクロコントローラ 22 と、操作ボタン 23 とを備えている。アンテナ 21 は、たとえば、キー入力部 14 との無線通信を行う。

[0018] マイクロコントローラ 22 は、たとえば、不揮発性のメモリ 221 と、入出力部 222 とを備える。メモリ 221 は、たとえば、暗号化された車両識別番号 VIN と、暗号化された個人識別情報 PI が記憶されている。入出力部 222 は、たとえば、操作ボタン 23 が押下されると、暗号化された車両識別番号 VIN および個人識別情報 PI をメモリ 221 から読み出して、ア

ンテナ 21 を介してキー入力部 14 へ送信する。

[0019] また、入出力部 222 は、アンテナ 21 を介してキー入力部 14 からリクエスト信号を受信すると、暗号化された車両識別番号 VIN および個人識別情報 PI をメモリ 221 から読み出す。さらに、入出力部 222 は、その暗号化された車両識別番号 VIN および個人識別情報 PI を、レスポンスコードとともに、アンテナ 21 を介してキー入力部 14 へ送信する。

[0020] 図 4 は、図 2 のキー入力部 14 と無線通信を行う携帯情報端末 3 の一例を示すブロック図である。以下では、携帯情報端末 3 を「PDA 3」と略称する。情報管理システム 1 は、たとえば、PDA 3 を含んでもよい。PDA 3 は、たとえば、スマートフォンまたはタブレット型コンピュータである。PDA 3 は、たとえば、通信部 31 と、マイクロコントローラ 32 と、入力部 33 とを備えている。

[0021] PDA 3 の通信部 31 は、たとえば、ブルートゥース（登録商標）などの近距離無線通信によって車両 V に搭載されたキー入力部 14 との無線通信を行う。なお、近距離無線通信のプロトコルは、ブルートゥース（登録商標）に限定されない。また、通信部 31 は、たとえば、無線通信回線 RCL、無線基地局 WBS、および通信網 CN を介して、車両 V の外部のデータセンタ DC に設置されたサーバ S との通信を行う。

[0022] 図 4 に示すように、データセンタ DC のサーバ S は、たとえば、キー管理ソフトウェア S1 と、ユーザデータベース S2 とを備えている。ユーザデータベース S2 には、たとえば、個人識別情報 PI および車両識別番号 VIN が、車両 V の運転者のユーザ ID と関連付けられて登録されている。

[0023] PDA 3 のマイクロコントローラ 32 は、たとえば、キー管理アプリケーション 321 と、メモリ 322 とを備える。キー管理アプリケーション 321 は、たとえば、マイクロコントローラ 32 のメモリに記憶されたプログラムであり、マイクロコントローラ 32 の中央処理装置（CPU）によって実行される。キー管理アプリケーション 321 は、たとえば、車両 V の運転者が入力部 33 を介して入力したユーザ ID を、通信部 31 を介してデータセ

ンタDCのサーバSへ送信する。

[0024] データセンタDCのサーバSのキー管理ソフトウェアS1は、サーバSの記憶装置に記憶され、サーバSのCPUによって実行される。キー管理ソフトウェアS1は、PDA3から送信された車両Vの運転者のユーザIDを、無線基地局WBSおよび通信網CNを介して受信する。すると、キー管理ソフトウェアS1は、受信したユーザIDに対応する車両識別番号VINと個人識別情報PIを、ユーザデータベースS2から読み出して暗号化する。さらに、キー管理ソフトウェアS1は、暗号化した車両識別番号VINと個人識別情報PIを、通信網CNおよび無線基地局WBSを介してPDA3へ送信する。

[0025] PDA3のキー管理アプリケーション321は、暗号化された車両識別番号VINおよび個人識別情報PIを、通信部31を介して受信し、メモリ322に記憶させる。さらに、キー管理アプリケーション321は、暗号化された車両識別番号VINおよび個人識別情報PIを、キー入力部14へ、PDA3の通信部31を介して送信する。

[0026] なお、PDA3のキー管理アプリケーション321を、データセンタDCのサーバSにインストールしてもよい。この場合、PDA3のマイクロコントローラ32は、たとえば、データセンタDCのサーバSから、暗号化された車両識別番号VINおよび個人識別情報PIの送信用の実行ファイルを受信して、メモリ322に記憶させる。これにより、PDA3のキー管理アプリケーション321を省略することができる。

[0027] 図2に示す情報管理システム1の各部の説明に戻る。キー認証部11は、たとえば、CPU、メモリ、タイマー、および入出力部を備えたマイクロコントローラまたはECUである。キー認証部11は、キー入力部14から出力された情報を入力として、車両Vと運転者の認証および識別を行う。キー認証部11は、たとえば、運転者識別部111と、VIN記憶部112と、VIN比較部113と、インターフェース部114と、を備えている。これらキー認証部11の各部は、たとえば、メモリに格納されたプログラムをC

PUによって実行することで実現される、キー認証部11の機能を表している場合がある。

[0028] 運転者識別部111は、たとえば、キー入力部14の出力である暗号化された情報を復号して平文化する。運転者識別部111は、さらに、平文化された情報から、個人識別番号PINを含む個人識別情報PIを抽出するとともに、車両識別番号VINを分離する。運転者識別部111は、平文化した情報から分離した車両識別番号VINを、VIN比較部113へ出力する。また、運転者識別部111は、平文化された情報から抽出した個人識別番号PINを含む個人識別情報PIを、インターフェース部114および車載ネットワーク18を介して情報取得部12および情報管理部13へ出力する。

[0029] VIN記憶部112は、たとえば、メモリによって構成され、車両Vに固有の車両識別番号VINが格納されている。VIN比較部113は、たとえば、運転者識別部111から入力された車両識別番号VINと、VIN記憶部112に格納された車両識別番号VINとを比較する。これらの車両識別番号VINが一致した場合、VIN比較部113は、インターフェース部114および車載ネットワーク18を介して、図示を省略する車両駆動用のECUに照合結果を送信する。これにより、車両Vのエンジンやモータなどの動力源を駆動させ、車両Vを走行させることが可能になる。

[0030] 以上のように、キー認証部11は、たとえば、キー入力部14の出力である暗号化された車両識別番号VINおよび個人識別情報PIを含む情報を、運転者識別部111によって復号して平文化する。これにより、キー認証部11は、車両Vの車両識別番号VINおよびその車両Vの運転者の個人識別情報PIを取得して、車両Vおよびその車両Vの運転者を認証および識別する。

[0031] 情報取得部12は、たとえば、CPU、メモリ、タイマー、および入出力部を備えたマイクロコントローラまたはECUである。情報取得部12は、車両Vの走行情報TIを含む運転者情報DIを取得する。情報取得部12は、たとえば、インターフェース部121と、PI記憶部122と、条件設定

部 1 2 3 と、D I 収集部 1 2 4 と、個別情報記憶部 1 2 5 とを備えている。
以下では、個別情報記憶部 1 2 5 を、「P D 記憶部 1 2 5」と略称する場合がある。これら情報取得部 1 2 の各部は、たとえば、メモリに格納されたプログラムを C P U によって実行することで実現される、情報取得部 1 2 の機能を表している場合がある。

[0032] インターフェース部 1 2 1 は、たとえば、車載ネットワーク 1 8 を介して、キー認証部 1 1、情報管理部 1 3、および通信部 1 5 との間で、データの送受信を行う。P I 記憶部 1 2 2 は、キー認証部 1 1 からインターフェース部 1 1 4、車載ネットワーク 1 8、およびインターフェース部 1 2 1 を介して入力された個人識別情報 P I を、一時的に記憶する。条件設定部 1 2 3 は、D I 収集部 1 2 4 によって収集する運転者情報 D I の種別、頻度、フォーマットなどの条件を設定する。

[0033] D I 収集部 1 2 4 は、条件設定部 1 2 3 によって設定された条件に従って、インターフェース部 1 2 1 および車載ネットワーク 1 8 を介して運転者情報 D I を収集する。ここで、運転者情報 D I は、少なくとも車両 V の走行情報 T I を含む。より具体的には、D I 収集部 1 2 4 は、たとえば、図示を省略する車載カメラ、車載センサ、全球測位衛星システムの受信機から出力された検出結果を、インターフェース部 1 2 1 を介して収集する。さらに、D I 収集部 1 2 4 は、たとえば、収集した車載カメラ等の検出結果を用いて、走行情報 T I を算出する。

[0034] P D 記憶部 1 2 5 は、たとえば、以下の表 1 に示すように、D I 収集部 1 2 4 によって収集された運転者情報 D I と、P I 記憶部 1 2 2 に記憶された車両 V の運転者の個人識別情報 P I とを関連付けた個別情報 P D を記憶する。車両 V の走行情報 T I は、たとえば、車両 V の運転者の運転傾向 D T を含む。運転者の運転傾向 D T は、たとえば、表 1 に示すような項目の記録日ごとの回数を含む。なお、表 1 に示す運転者の運転傾向 D T の項目は一例であり、特に限定はされない。

[0035]

[表1]

個別情報 P D					
個人識別情報 P I		運転者情報 D I			
***	走行情報 T I				...
	運転傾向 D T			...	...
	記録日	減速度超過回数 [回/日]	**	...	...
	***	操舵角速度超過回数 [回/日]	**	...	...
		加速度超過回数 [回/日]	**	...	...
		速度超過回数 [回/日]	**	...	...
		車間距離不足回数 [回/日]	**	...	...
		黄信号通過回数 [回/日]	**	...	...
		赤信号通過回数 [回/日]	**	...	...

[0036] 表 1 に示すような車両 V の運転者の運転傾向 D T を含む個別情報 P D は、たとえば、テレマティクス保険における保険料の算出に適用することができる。この場合、図 1 に示す車両 V の外部のデータセンタ D C に設置されるサーバ S は、たとえば、保険料計算ソフトウェア S 3 と、保険料計算データベース S 4 とを備えることができる。データセンタ D C のサーバ S による保険料の計算については、後述する。

[0037] また、車両 V の走行情報 T I は、運転者の運転傾向 D T の他に、車両 V の位置、走行経路、速度、加速度、角速度などの情報を含んでもよい。さらに、運転者情報 D I は、車両 V の走行情報 T I の他に、たとえば、シートの位置や角度、ミラーの位置や角度、照明、および空調などの運転者ごとの車両 V の設定や、車載インフォテインメントに関する嗜好などを含んでもよい。

[0038] 以上のように、情報取得部 1 2 は、たとえば、D I 収集部 1 2 4 により、車両 V の走行情報 T I を含む運転者情報 D I を取得する。さらに、情報取得部 1 2 は、たとえば、P D 記憶部 1 2 5 に記憶された個別情報 P D を、インターフェース部 1 2 1 および車載ネットワーク 1 8 を介して、必要に応じて情報管理部 1 3 へ出力する。

[0039] 情報管理部 1 3 は、たとえば、C P U、メモリ、タイマー、および入出力部を備えたマイクロコントローラまたは E C U である。情報管理部 1 3 は、前述のように個人識別情報 P I と運転者情報 D I とを関連付けた個別情報 P D を管理する。情報管理部 1 3 は、たとえば、インターフェース部 1 3 1 と

、個別情報記憶部 132 と、秘密鍵記憶部 133 と、アドレス算出部 134 と、電子署名部 135 と、公開鍵生成部 136 と、を備えている。

[0040] これら情報管理部 13 の各部は、たとえば、メモリに格納されたプログラムを CPU によって実行することで実現される、情報管理部 13 の機能を表している場合がある。また、以下では、個別情報記憶部 132 を、「PD 記憶部 132」と略称する場合がある。

[0041] インターフェース部 131 は、たとえば、車載ネットワーク 18 を介して、情報取得部 12 および通信部 15 との間で、データの送受信を行う。PD 記憶部 132 は、たとえば、メモリによって構成され、インターフェース部 131 および車載ネットワーク 18 を介して、情報取得部 12 の PD 記憶部 125 に記憶された個別情報 PD を取得して記憶する。なお、情報取得部 12 が PD 記憶部 125 を有しない場合、情報管理部 13 の PD 記憶部 132 は、情報取得部 12 から個別に取得した個人識別情報 P I と運転者情報 D I とを関連付けて、上記の表 1 に示すような個別情報 PD として記憶してもよい。

[0042] 秘密鍵記憶部 133 は、たとえば、ROM などの不揮発性メモリによって構成され、複数の個人識別情報 P I と複数の秘密鍵 S K とが 1 対 1 対応で関連付けられて記憶されている。すなわち、秘密鍵記憶部 133 は、1 つのアドレスに 1 つの秘密鍵 S K が 1 つの個人識別情報 P I に関連付けられて格納されている。本実施形態では、キー入力部 14 で取得された個人識別情報 P I と、情報取得部 12 で取得された運転者情報 D I により個別情報 PD を作成するが、秘密鍵記憶部 133 に格納された個人識別情報 P I と運転者情報 D I とを関連付けて個別情報 PD を作成してもよい。

[0043] 秘密鍵記憶部 133 に対する秘密鍵 S K の書き込みは、たとえば、以下のように行うことができる。情報管理システム 1 の生産工場で秘密鍵 S K の元となるシードを不揮発メモリに書き込み、情報管理部 13 に秘密鍵暗号計算ソフトウェアをインストールし、シードを入力して秘密鍵 S K を作成し、不揮発メモリに秘密鍵 S K を書き込み、該当するシードを削除する。秘密鍵暗

号計算ソフトウェアは、生産工場でシードを書き込む前にダウンロードして、秘密鍵SKの作成後に削除してもよい。

[0044] アドレス算出部134は、たとえば、PD記憶部132に記憶された個別情報PDに含まれる個人識別情報PIを入力とし、その個人識別情報PIに対応する秘密鍵SKが記憶された秘密鍵記憶部133のアドレスを出力する。

[0045] 電子署名部135は、たとえば、アドレス算出部134から出力された秘密鍵記憶部133のアドレスを参照して秘密鍵SKを取得するとともに、PD記憶部132から個別情報PDを取得する。ここで、個別情報PDは、たとえば、運転者情報DIの先頭に個人識別情報PIが付加された情報である。電子署名部135は、たとえば、ハッシュ関数を用いて、PD記憶部132から取得した個別情報PDのハッシュ値を算出する。さらに、電子署名部135は、算出したハッシュ値を、秘密鍵記憶部133から取得した秘密鍵SKを用いて暗号化する。これにより、電子署名部135は、RSA暗号方式による電子署名を作成することができる。

[0046] 公開鍵生成部136は、たとえば、アドレス算出部134から出力された秘密鍵記憶部133のアドレスを参照して秘密鍵SKを取得するとともに、取得した秘密鍵SKを用いて公開鍵PKを生成する。なお、秘密鍵記憶部133に格納された個々の運転者に固有の秘密鍵SKに対応する個々の公開鍵PKは、インターフェース部131、車載ネットワーク18、および通信部15を介して、個々の運転者の個別情報PDの送信先へ、事前に送信してもよい。

[0047] 情報管理部13は、電子署名部135によって電子署名が付された個別情報PDを、インターフェース部131、車載ネットワーク18、および通信部15を介して、車両Vの外部へ送信する。車両Vから送信された電子署名済みの個別情報PDは、たとえば、図1に示すように、無線通信回線RCLを介して無線基地局WBSへ送信される。無線基地局WBSによって受信された電子署名済みの個別情報PDは、たとえば、有線通信回線WCLを介し

てデータセンタDCのサーバSおよび分散型ネットワークDNを構成するコンピュータPCへ送信される。サーバSおよびコンピュータPCは、たとえば、情報管理システム1の情報管理部13から受信した電子署名が付された個別情報PDを、同じ情報管理部13によって生成された公開鍵PKによって認証する。

[0048] また、コンピュータPCまたはそのユーザは、たとえば、認証済みの個別情報PDを、ブロックチェーンに登録してもよい。この場合、情報管理システム1の情報管理部13において、電子署名部135は、新しい個別情報PDのブロックを送信する際に、前の個別情報PDのブロックのハッシュ値を秘密鍵SKによって暗号化して、新しい個別情報PDのブロックの電子署名を作成する。これにより、コンピュータPCまたはそのユーザは、電子署名が付された個別情報PDを公開鍵PKによって認証するとともに、ブロックチェーンに登録することが可能になる。

[0049] また、情報管理部13は、情報取得部12によって取得された運転者情報DIのうち、電子署名を要しない情報については、インターフェース部131、車載ネットワーク18、および、通信部15を介して車両Vの外部へ電子署名を作成せずに送信する。また、電子署名部135は、車両Vの外部へ送信する個別情報PDを含む情報を、秘密鍵SKによって暗号化してもよい。

[0050] 以下、本実施形態の情報管理システム1の作用を説明する。図1に示すように、本実施形態の情報管理システム1は、たとえば、分散型ネットワークDNやデータセンタDCに接続され、車両VとデータセンタDCがデータやプログラムを相方向に送受信するようになっている。

[0051] データセンタDCから車両Vへのデータやプログラムの送信例として、ECUのプログラムを更新するFOTA (Firmware Over-The-Air)、カーナビゲーションシステムの地図データの更新、音楽データの配信などが挙げられる。また、車両VからデータセンタDCへのデータの送信例として、車両Vの部品の診断情報を送信する例が挙げられる。この場合、データセンタDC

は、たとえば、車両Vから受信した部品の診断情報を、カーディーラーに送信し、カーディーラーが部品の交換を行うなど、車両Vの部品管理を行うことができる。

[0052] また、保険業界においても、車両Vの走行情報T Iを利用する取り組みがある。車両Vの走行情報T Iを保険料に反映するテレマティクス保険は、車両Vの走行距離に基づいて保険料を算出する段階から、運転者の急ブレーキや急アクセルなど、運転者の運転傾向D Tに基づいて保険料を算出する段階へ移りつつある。また、テレマティクス保険においては、たとえば、大規模集合住宅の複数の居住者が車両Vを共有して利用する場合など、複数の運転者によるカーシェアリングを行う場合、運転者ごとに保険料を定めることが合理的である。

[0053] 1台の車両Vを複数の運転者が使用する場合に、運転者ごとにテレマティクス保険に適用するためには、運転者ごとに車両Vの走行情報T Iを収集し、収集した走行情報T Iを運転者が識別可能な状態で管理することが必要になる。また、車両Vから、運転者の運転傾向D Tを含む走行情報T Iを、運転者を識別可能な状態で、外部のデータセンタD Cに送信することが要求される。さらに、運転者ごとの走行情報T Iがブロックチェーンなどの分散型台帳によって管理される場合には、ブロックチェーンへの登録に対応することが求められる。

[0054] 前述のような課題に対し、本実施形態の情報管理システム1は、次のような処理を実行する。図5は、情報管理システム1による処理P 1の流れの一例を示すフロー図である。運転者が車両Vの起動スイッチをオンにしようすると、車両Vに搭載されたキー入力部1 4は、その運転者が所持する電子キー2またはP D A 3との通信を行う。これにより、キー入力部1 4は、電子キー2またはP D A 3から、暗号化された車両識別番号V I Nと、暗号化された個人識別情報P Iとを受信する。

[0055] すると、情報管理システム1は、たとえば、図5に示す処理P 1を開始して、キー情報の入力処理P 1 1を実行する。この処理P 1 1において、運転

者識別部 111 は、キー入力部 14 から、暗号化された車両識別番号 V I N と、暗号化された運転者の個人識別情報 P I を取得する。さらに、運転者識別部 111 は、前述のように、車両識別番号 V I N と個人識別情報 P I とを復号して平文化するとともに、車両識別番号 V I N と個人識別情報 P I とを分離して、車両識別番号 V I N と個人識別情報 P I をそれぞれ取得する。

[0056] さらに、V I N 比較部 113 は、キー入力部 14 から取得した車両識別番号 V I N と、V I N 記憶部 112 に記憶された車両識別番号 V I N とを比較し、これらが一致しない場合は、車両 V を起動させない。この場合、情報管理システム 1 は、図 5 に示す処理を終了する。ここでは、キー入力部 14 から取得した車両識別番号 V I N と、V I N 記憶部 112 に記憶された車両識別番号 V I N とが一致したものとする。次に、情報管理システム 1 は、たとえば、個人識別情報 P I の送信処理 P 12 を実行する。この処理 P 12 において、キー認証部 11 は、たとえば、車載ネットワーク 18 を介して個人識別情報 P I を送信する。

[0057] 次に、情報管理システム 1 は、たとえば、運転者情報 D I の取得処理 P 13 を実行する。この処理 P 13 において、情報取得部 12 は、たとえば、車載ネットワーク 18 を介して個人識別情報 P I を受信して、P I 記憶部 122 に記憶させる。さらに、情報取得部 12 は、条件設定部 123 によって設定された条件に従って、D I 収集部 124 によって運転者情報 D I を収集する。そして、情報取得部 12 は、個人識別情報 P I と運転者情報 D I とを関連付けた個別情報 P D を P D 記憶部 125 に記憶させる。

[0058] 次に、情報管理システム 1 は、たとえば、個別情報 P D の送信処理 P 14 を実行する。この処理 P 14 において、情報取得部 12 は、たとえば、車載ネットワーク 18 を介して個別情報 P D を送信する。

[0059] 次に、情報管理システム 1 は、たとえば、秘密鍵 S K の準備処理 P 15 を実行する。この処理 P 15 において、情報管理部 13 は、たとえば、インターフェース部 131 により、車載ネットワーク 18 を介して個別情報 P D を受信し、P D 記憶部 132 に記憶させる。さらに、情報管理部 13 は、たと

例えば、アドレス算出部134により、個別情報PDに含まれる個人識別情報PIに対応する秘密鍵SKが格納された、秘密鍵記憶部133のアドレスを算出して、電子署名部135へ出力する。

[0060] 次に、情報管理システム1は、たとえば、電子署名処理P16を実行する。この処理P16において、情報管理部13は、たとえば、電子署名部135により、アドレス算出部134から入力された秘密鍵記憶部133のアドレスを参照して、車両Vの現在の運転者の個人識別情報PIに対応する秘密鍵SKを取得する。さらに、この処理P16において、電子署名部135は、PD記憶部132から個別情報PDを取得する。そして、電子署名部135は、取得した秘密鍵SKを用いて個別情報PDに電子署名を行う。なお、個別情報PDの暗号化を行う場合は、個別情報PDの暗号化の後に電子署名を行ってもよい。

[0061] 次に、情報管理システム1は、たとえば、外部送信処理P17を実行する。この処理P17において、情報管理部13は、たとえば、インターフェース部131、車載ネットワーク18、および通信部15を介して、車両Vの外部へ電子署名を行った個別情報PDを送信する。以上により、図5に示す情報管理システム1の処理P1が終了する。

[0062] 車両Vから送信された電子署名済みの個別情報PDは、たとえば、図1に示す無線通信回線RCL、無線基地局WBS、および有線通信回線WCLを介して、データセンタDCのサーバSや、分散型ネットワークDNのコンピュータPCによって受信される。データセンタDCのサーバSは、たとえば、保険料計算ソフトウェアS3により、個別情報PDに含まれる個人識別情報PIに対応する公開鍵PKを用いて、受信した電子署名済みの個別情報PDを認証する。

[0063] サーバSの保険料計算ソフトウェアS3は、個別情報PDの認証後、保険料計算データベースS4に個別情報PDを登録する。ここで、個別情報PDは、前述の表1に示すように、車両Vの各々の運転者の個人識別情報PIと運転者情報DIとが関連付けられた情報である。また、前述のように、運転

者情報D Iは、各々の運転者の運転による車両Vの走行情報T Iを含み、走行情報T Iは、各々の運転者の運転傾向D Tを含む。

[0064] したがって、保険料計算ソフトウェアS 3は、保険料計算データベースS 4に登録された運転者ごとの個別情報P Dに基づいて、運転者ごとにリスクを適正に算出することができ、運転者ごとに適正な保険料を算出することが可能になる。これにより、たとえば、カーシェアリングなど、1台の車両Vを不特定多数の運転者が運転する場合でも、各運転者にテレマティクス保険を適用することが可能になる。

[0065] また、分散型ネットワークD Nを構成するコンピュータP Cは、たとえば、個別情報P Dに含まれる個人識別情報P Iに対応する公開鍵P Kを用いて、受信した電子署名済みの個別情報P Dを認証するとともに、ブロックチェーンに登録する。これにより、個別情報P Dの改ざんを防止することができ、分散型台帳による信頼性の高いデータベースを構築することが可能になる。

[0066] 以上のように、本実施形態の情報管理システム1は、車両Vの運転者に関する運転者情報D Iを管理するシステムである。情報管理システム1は、車両Vの運転者の個人識別情報P Iを取得する運転者識別部111と、車両Vの走行情報T Iを含む運転者情報D Iを取得する情報取得部12と、個人識別情報P Iと運転者情報D Iとを関連付けた個別情報P Dを記憶する個別情報記憶部125、132と、を備える。

[0067] このような構成により、本実施形態の情報管理システム1は、たとえば、複数の運転者が1台の車両Vを共有する場合でも、個人識別情報P Iに基づいて個々の運転者を識別可能な状態で、走行情報T Iを含む運転者情報D Iを収集することが可能になる。

[0068] また、本実施形態の情報管理システム1は、車両Vの外部と通信可能な通信部15と、個人識別情報P Iごとに固有の秘密鍵S Kが記憶された秘密鍵記憶部133と、個別情報P Dに関連付けられた個人識別情報P Iに固有の秘密鍵S Kを用いて個別情報P Dに電子署名を行う電子署名部135と、を

さらに備えている。また、通信部 15 は、電子署名が付された個別情報 P D を車両 V の外部へ送信する。

[0069] このような構成により、本実施形態の情報管理システム 1 は、たとえば、複数の運転者が 1 台の車両 V を共有する場合でも、他者によるなりすましを防止して、個別情報 P D が個々の運転者本人のものであることを担保することができる。また、個別情報 P D を、車両 V、データセンタ D C、および分散型ネットワーク D N などとの間で送受信する際に、個別情報 P D の改ざんを防止することができ、セキュアな環境で個別情報 P D を送受信することができる。

[0070] また、本実施形態の情報管理システム 1 において、運転者識別部 111 は、車両 V の電子キー 2 または運転者が所有する携帯情報端末 3 から送信される個人識別情報 P I を取得する。このような構成により、複数の運転者が 1 台の車両 V を使用する場合でも、運転者の識別を容易に行うことが可能になる。

[0071] また、本実施形態の情報管理システム 1 は、個々の個人識別情報 P I に固有の秘密鍵 S K に対応する公開鍵 P K を生成する公開鍵生成部 136 をさらに備えている。また、通信部 15 は、公開鍵 P K を外部へ送信する。このような構成により、情報管理システム 1 は、たとえば、分散型ネットワーク D N を構成する複数のコンピュータ P C へ公開鍵 P K を送信し、さらに、秘密鍵 S K によって電子署名が作成された個別情報 P D を送信することができる。そのため、公開鍵暗号方式を基本とする分散型台帳であるブロックチェーンに、個別情報 P D を登録することが可能になる。

[0072] 以上説明したように、本実施形態の情報管理システム 1 によれば、1 台の車両 V を複数の運転者が運転する場合に、個々の運転者の走行情報 T I を含む運転者情報 D I を独立して収集および出力することができる。また、本実施形態の情報管理システム 1 によれば、個々の運転者の識別に関するセキュリティを確保することができる。すなわち、本実施形態によれば、1 台の車両 V を複数の運転者が運転する場合に、各々の運転者に係る情報の取り扱い

に関する課題を解決することが可能な情報管理システム 1 を提供することができる。

[0073] (実施形態 2)

次に、本開示に係る情報管理システムの実施形態 2 について、図 1、図 3 および図 4 を援用し、図 6 から図 9 を参照して説明する。図 6 は、実施形態 2 に係る情報管理システム 1 を搭載する車両 V のブロック図である。情報管理システム 1 は、主に、秘密鍵記憶部 133 および電子署名部 135 を含むハードウェアセキュリティモジュール 137 を備える点で、前述の実施形態 1 の情報管理システム 1 と異なっている。以下では、ハードウェアセキュリティモジュールを、「HSM」と略称する場合がある。

[0074] また、本実施形態の情報管理システム 1 または車両 V は、キー認証部 11、情報取得部 12、通信部 15、および ECU 16、17 が、それぞれ、HSM によって構成された認証部 115、126、152、162、172 を備える点で、前述の実施形態 1 の情報管理システム 1 または車両 V と異なっている。また、本実施形態の情報管理システム 1 または車両 V は、たとえば、バッテリー電力供給部 19 を備えている。本実施形態の情報管理システム 1 および車両 V のその他の構成は、前述の実施形態 1 の情報管理システム 1 および車両 V と同様であるため、同様の部分には同一の符号を付して説明を省略する。

[0075] 情報管理部 13 の HSM 137 は、前述の実施形態 1 と同様の秘密鍵記憶部 133、アドレス算出部 134、電子署名部 135、および公開鍵生成部 136 を含む。HSM 137 は、たとえば、すべての暗号化処理を 1 つのチップで行うワンチップ構成であり、分解困難な一体型の構成であり、真正乱数生成機能が搭載されたハードウェアであり、秘密鍵 SK、公開鍵 PK、および共通鍵 CK などの電子鍵を安全に保管する。

[0076] このように、本実施形態の情報管理システム 1 は、秘密鍵記憶部 133 および電子署名部 135 を含むハードウェアセキュリティモジュール 137 を備える。このような構成により、複数の運転者が 1 台の車両 V を使用する場

合に、個々の運転者に固有の秘密鍵SKを、HSM137に含まれる秘密鍵記憶部133にセキュアに格納して、秘密鍵SKの漏洩をより確実に防止することができる。したがって、本実施形態の情報管理システム1によれば、前述の実施形態1と同様の効果を奏することができるだけでなく、運転者の識別におけるセキュリティを確保することが可能になる。

[0077] HSM137は、さらに、認証部138を含む。認証部138は、たとえば、メッセージ認証に使用される共通鍵CKが格納されている。すなわち、HSM137は、前述の秘密鍵記憶部133、アドレス算出部134、電子署名部135、および公開鍵生成部136による電子署名だけでなく、認証部138によるメッセージ認証を行うことが可能である。HSM137は、たとえば、データとともに入力される指示に応じて、データに電子署名を行うか、データのメッセージ認証を行うか、いずれかを選択することができる。

[0078] また、キー認証部11、情報取得部12、通信部15、およびECU16、17の認証部115、126、152、162、172は、情報管理部13のHSM137と同様にハードウェアセキュリティモジュールによって構成されている。また、これらの認証部115、126、152、162、172は、HSM137の認証部138と同様の構成を備えている。ただし、これらの認証部115、126、152、162、172は、HSM137とは異なり、秘密鍵記憶部133、アドレス算出部134、電子署名部135、および公開鍵生成部136を有しない。

[0079] 各々の認証部115、126、138、152、162、172は、車載ネットワーク18に送信するデータと共通鍵CKを元に、ハッシュ関数を用いてMAC値を算出する。また、各々の認証部115、126、138、152、162、172は、車載ネットワーク18からデータとMAC値を受信し、受信したデータと共通鍵CKを元にMAC値を算出し、算出したMAC値と受信したMAC値とを比較する。そして、算出したMAC値と受信したMAC値とが一致していれば、認証が成功する。これにより、車載ネット

ワーク 18 を介して送受信されるデータの改ざんを防止して、キー認証部 11、情報取得部 12、情報管理部 13、通信部 15、および ECU 16, 17 の間で、セキュアな通信を行うことが可能になる。

[0080] バッテリ電力供給部 19 は、たとえば、マイクロコントローラまたは ECU によって構成され、車両 V の起動スイッチがオフにされたときに、車両 V に搭載されたバッテリーから、情報取得部 12 および情報管理部 13 への電力の供給と停止を制御する。

[0081] 本実施形態の情報管理システム 1 は、車両 V の起動スイッチがオンまたはオフにされたときに、個別情報記憶部 125, 132 に記憶された個別情報 PD を消去する点で、前述の実施形態 1 の情報管理システム 1 と異なっている。以下、本実施形態の情報管理システム 1 による処理について説明する。

[0082] 図 7 は、本実施形態の情報管理システム 1 による処理 P2 の一例を示すフロー図である。情報管理システム 1 は、図 7 に示す処理 P2 を開始すると、図 5 に示す実施形態 1 のキー情報の入力処理 P11、個人識別情報 P1 の送信処理 P12、および運転者情報 DI の取得処理 P13 と同様の処理 P21, P22, P23 を実行する。次に、情報管理システム 1 は、たとえば、バッテリー電力供給部 19 により、車両 V の起動スイッチがオフか否かを判定する処理 P24 を実行する。

[0083] この処理 P24 において、たとえば、起動スイッチがオフではない（NO）と判定されると、情報管理システム 1 は、車両 V の起動スイッチがオンになったとき、または前回の外部送信処理 P29 の終了時から、所定時間 t_s が経過したか否かの判定処理 P25 を実行する。この処理 P25 において、所定時間 t_s が経過していない（NO）と判定されると、情報管理システム 1 は、再度、運転者情報 DI の取得処理 P23 を実行する。

[0084] 一方、この処理 P25 において、所定時間 t_s が経過した（YES）と判定されると、情報管理システム 1 は、図 5 に示す実施形態 1 の個別情報 PD の送信処理 P14、秘密鍵 SK の準備処理 P15、電子署名処理 P16、および外部送信処理 P17 と同様の処理 P26, P27, P28, P29 を実

行する。これにより、車両Vの起動スイッチがオフにされるまで、個別情報PDが定期的に車両Vの外部へ送信される。

[0085] 一方、前述の処理P24において、車両Vの起動スイッチがオフである（YES）と判定されると、情報管理システム1は、たとえば、バッテリー電力供給部19により、車両Vのバッテリーから、情報取得部12および情報管理部13へ電力を供給する処理P2Aを実行する。

[0086] さらに、情報管理システム1は、たとえば、情報取得部12および情報管理部13により、PD記憶部125、132に記憶された個別情報PDを消去する処理P2Bを実行する。その後、情報管理システム1は、たとえば、バッテリー電力供給部19により、車両のバッテリーから情報取得部12および情報管理部13への電力の供給を停止する処理P2Cを実行して、図7に示す処理P2を終了する。

[0087] 以上のように、図7に示す例において、情報管理システム1は、車両Vの起動スイッチがオフにされたときに、個別情報記憶部125、132に記憶された個別情報PDを消去する。これにより、複数の運転者が1台の車両Vを使用する場合に、各運転者の個別情報PDが他の運転者に知られることを防止して、各運転者のプライバシーを保護することができる。

[0088] 図8は、本実施形態の情報管理システム1による別の処理P3の一例を示すフロー図である。情報管理システム1は、図8に示す処理P3を開始すると、図5に示す実施形態1のキー情報の入力処理P11、個人識別情報PIの送信処理P12、および運転者情報DIの取得処理P13と同様の処理P31、P32、P33を実行する。次に、情報管理システム1は、たとえば、バッテリー電力供給部19により、車両Vの起動スイッチがオフか否かを判定する処理P34を実行する。

[0089] この処理P34において、たとえば、起動スイッチがオフではない（NO）と判定されると、情報管理システム1は、再度、運転者情報DIの取得処理P33を実行する。一方、この処理P34において、たとえば、起動スイッチがオフである（YES）と判定されると、情報管理システム1は、たと

例えば、バッテリー電力供給部 19 により、車両 V のバッテリーから、情報取得部 12 および情報管理部 13 へ電力を供給する処理 P35 を実行する。

[0090] 次に、情報管理システム 1 は、図 5 に示す実施形態 1 の個別情報 PD の送信処理 P14、秘密鍵 SK の準備処理 P15、電子署名処理 P16、および外部送信処理 P17 と同様の処理 P36, P37, P38, P39 を実行する。これにより、車両 V の起動スイッチのオフ時に、個別情報 PD が車両 V の外部へ送信される。

[0091] その後、情報管理システム 1 は、たとえば、情報取得部 12 および情報管理部 13 により、PD 記憶部 125, 132 に記憶された個別情報 PD を消去する処理 P3A を実行する。その後、情報管理システム 1 は、たとえば、バッテリー電力供給部 19 により、車両 V のバッテリーから情報取得部 12 および情報管理部 13 への電力の供給を停止する処理 P3B を実行して、図 8 に示す処理 P3 を終了する。

[0092] 以上のように、図 8 に示す例において、情報管理システム 1 は、車両 V の起動スイッチがオフにされたときに、個別情報記憶部 125, 132 に記憶された個別情報 PD を消去するが、その個別情報 PD の消去前に、通信部 15 を介して車両 V の外部へ個別情報 PD を送信する。これにより、複数の運転者が 1 台の車両 V を使用する場合に、各運転者のプライバシーを保護することができるだけでなく、車両 V の起動スイッチがオフにされるまでの運転者の個別情報 PD を車両 V の外部へ送信することが可能になる。

[0093] 図 9 は、本実施形態の情報管理システム 1 による別の処理 P4 の一例を示すフロー図である。情報管理システム 1 は、図 9 に示す処理 P4 を開始すると、図 5 に示す実施形態 1 のキー情報の入力処理 P11 および個人識別情報 PI の送信処理 P12 と同様の処理 P41, P42 を実行する。次に、情報管理システム 1 は、たとえば、情報管理部 13 により、車両 V の外部へ送信がされていない未出力の個別情報 PD が PD 記憶部 125 または PD 記憶部 132 に記憶されているか否かを判定する処理 P43 を実行する。

[0094] この処理 P43 において、たとえば、PD 記憶部 125 または PD 記憶部

132に個別情報PDが記憶されておらず、未出力のデータがない（NO）と判定されると、情報管理システム1は、図5に示す運転者情報D1の取得処理P13と同様の処理P44を実行する。次に、情報管理システム1は、たとえば、バッテリー電力供給部19により、車両Vの起動スイッチがオフであるか否かを判定する処理P45を実行する。

[0095] この処理P45において、たとえば、起動スイッチがオフではない（NO）と判定されると、情報管理システム1は、再度、運転者情報D1の取得処理P44を実行する。一方、この処理P45において、起動スイッチがオフである（YES）と判定されると、情報管理システム1は、たとえば、バッテリー電力供給部19により、車両Vのバッテリーから、情報取得部12および情報管理部13へ電力を供給する処理P46を実行する。

[0096] 次に、情報管理システム1は、たとえば、情報取得部12または情報管理部13により、PD記憶部125またはPD記憶部132の不揮発性記憶領域に個別情報PDを記憶させて保存する処理P47を実行する。その後、情報管理システム1は、たとえば、バッテリー電力供給部19により、車両Vのバッテリーから情報取得部12および情報管理部13への電力の供給を停止する処理P48を実行して、図9に示す処理P4を終了する。

[0097] その後、たとえば、車両Vの起動スイッチが再びオンにされると、情報管理システム1は、再度、キー情報の入力処理P41および個人識別情報P1の送信処理P42を実行する。ここでは、PD記憶部125またはPD記憶部132の不揮発性記憶領域には、前回の個別情報PDが、車両Vの外部へ未出力の状態で記憶されている。そのため、情報管理システム1は、前述の処理P43において、未出力のデータがある（YES）と判定する。

[0098] すると、情報管理システム1は、図5に示す実施形態1の個別情報PDの送信処理P14、秘密鍵SKの準備処理P15、電子署名処理P16、および外部送信処理P17と同様の処理P49、P4A、P4B、P4Cを実行する。これにより、車両Vの起動スイッチがオンにされたときに、車両Vの外部へ未出力であった前回の個別情報PDが車両Vの外部へ送信される。

[0099] その後、情報管理システム 1 は、たとえば、情報取得部 1 2 および情報管理部 1 3 により、P D 記憶部 1 2 5, 1 3 2 に記憶された個別情報 P D を消去する処理 P 4 D を実行する。次に、情報管理システム 1 は、新たに運転者情報 D 1 の取得処理 P 4 4 を実行する。

[0100] 以上のように、図 9 に示す例において、情報管理システム 1 は、車両 V の起動スイッチがオフにされたときに、個別情報記憶部 1 2 5, 1 3 2 の不揮発性記憶領域に個別情報 P D を記憶させる。また、情報管理システム 1 は、車両 V の起動スイッチがオンにされたときに、個別情報記憶部 1 2 5, 1 3 2 の不揮発性記憶領域に記憶された個別情報 P D を、通信部 1 5 を介して車両 V の外部へ送信してから消去する。

[0101] このような構成により、複数の運転者が 1 台の車両 V を使用する場合に、前回の車両 V の起動スイッチがオフにされるまでの運転者の個別情報 P D を、次に車両 V の起動スイッチがオンにされたときに、車両 V の外部へ送信することができる。さらに、各運転者の個別情報 P D が他の運転者に知られることを防止して、各運転者のプライバシーを保護することができる。

[0102] 以上説明したように、本実施形態の情報管理システム 1 によれば、複数の運転者が 1 台の車両 V を使用する場合に、秘密鍵 S K をセキュアに保管して運転者の識別のセキュリティを確保することができる。また、本実施形態の情報管理システム 1 によれば、複数の運転者が 1 台の車両 V を使用する場合に、各運転者のプライバシーを保護することができる。したがって、本実施形態によれば、1 台の車両 V を複数の運転者が運転する場合に、各々の運転者に係る情報の取り扱いに関する課題を解決することが可能な情報管理システム 1 を提供することができる。

[0103] (実施形態 3)

次に、本開示に係る情報管理システムの実施形態 3 について、図 1、図 3、図 4 および図 6 を援用し、図 1 0 および図 1 1 を参照して説明する。図 1 0 は、図 6 に示す車両 V の車載ネットワーク 1 8 に接続される運転者識別部 (生体認証部) 1 A のブロック図である。本実施形態の情報管理システム 1

は、主に、図 6 に示すキー認証部 1 1 の運転者識別部 1 1 1 に換えて、図 1 0 に示す運転者識別部 1 A を備える点で、前述の実施形態 2 の情報管理システム 1 と異なっている。本実施形態の情報管理システム 1 のその他の構成は、前述の実施形態 2 の情報管理システム 1 と同様であるので、同様の部分には同一の符号を付して説明を省略する。

[0104] 図 1 0 に示すように、運転者識別部 1 A は、たとえば、インターフェース部 1 A 1 と、認証部 1 A 2 と、認証情報取得部 1 A 3 と、認証情報記憶部 1 A 4 と、登録部 1 A 5 と、照合部 1 A 6 とを備えている。

[0105] インターフェース部 1 A 1 は、たとえば、車載ネットワーク 1 8 に接続され、車載ネットワーク 1 8 へ情報を送信するとともに、車載ネットワーク 1 8 から情報を受信する。認証部 1 A 2 は、キー認証部 1 1、情報取得部 1 2、情報管理部 1 3 等が備える認証部 1 1 5、1 2 6、1 3 8 と同様の構成であり、インターフェース部 1 A 1 を介して送受信される情報のメッセージ認証を行う。

[0106] 認証情報取得部 1 A 3 は、車両 V の運転者の生体情報 B 1 を取得するセンサである。生体情報 B 1 は、たとえば、指紋情報、指静脈情報、手のひら静脈情報、顔画像情報、虹彩画像情報などを含む。本実施形態において、認証情報取得部 1 A 3 は、たとえば、運転者の顔画像を撮影するカメラなどの撮像部である。なお、認証情報取得部 1 A 3 は、指紋センサなど、その他のセンサであってもよい。

[0107] 認証情報記憶部 1 A 4 は、たとえば、不揮発性のメモリによって構成され、運転者の個人識別情報 P 1 と、顔画像に基づくデータなどの生体情報 B 1 とを関連付けて記憶する。登録部 1 A 5 は、認証情報取得部 1 A 3 によって取得された生体情報 B 1 を個人識別情報 P 1 と関連付けて認証情報記憶部 1 A 4 に記憶させて登録する。なお、個々の生体情報 B 1 に対しては、少なくとも車両 V 内で固有の個人識別情報 P 1 が関連付けられる。

[0108] 照合部 1 A 6 は、認証情報取得部 1 A 3 によって取得された生体情報 B 1 と、認証情報記憶部 1 A 4 に記憶された生体情報 B 1 とを照合する。照合部

1 A 6 は、認証情報取得部 1 A 3 によって取得された生体情報 B 1 と、認証情報記憶部 1 A 4 に記憶された生体情報 B 1 とが合致する場合、認証情報記憶部 1 A 4 からその生体情報 B 1 に関連付けられた個人識別情報 P 1 を取得する。

[0109] 照合部 1 A 6 は、認証情報記憶部 1 A 4 から取得した個人識別情報 P 1 を、たとえば、情報取得部 1 2 または秘密鍵記憶部 1 3 3 へ送信する。本実施形態では、図 3 に示す電子キー 2 や、図 4 に示す P D A 3 は、たとえば、車両識別番号 V I N のみをキー認証部 1 1 へ送信する。また、本実施形態では、図 6 に示すキー認証部 1 1 は、車両識別番号 V I N の認証を行うだけでよい、ため、運転者識別部 1 1 1 を有しない。

[0110] 以下、本実施形態の情報管理システム 1 の作用を説明する。図 1 1 は、本実施形態の情報管理システム 1 の処理 P 5 の流れの一例を示すフロー図である。

[0111] 運転者が車両 V の起動スイッチをオンにしようとする、と、車両 V に搭載されたキー入力部 1 4 は、その運転者が所持する電子キー 2 または P D A 3 との通信を行う。これにより、キー入力部 1 4 は、電子キー 2 または P D A 3 から、暗号化された車両識別番号 V I N を受信する。すると、情報管理システム 1 は、たとえば、図 1 1 に示す処理 P 5 を開始して、キー情報の入力処理 P 5 1 を実行する。

[0112] この処理 P 5 1 において、V I N 比較部 1 1 3 は、キー入力部 1 4 から、暗号化された車両識別番号 V I N を取得し、取得した車両識別番号 V I N を復号して平文化する。さらに、V I N 比較部 1 1 3 は、キー入力部 1 4 から取得した車両識別番号 V I N と、V I N 記憶部 1 1 2 に記憶された車両識別番号 V I N とを比較し、これらが一致しない場合は車両 V を起動させない。この場合、情報管理システム 1 は、図 1 1 に示す処理を終了する。

[0113] ここでは、キー入力部 1 4 から取得した車両識別番号 V I N と、V I N 記憶部 1 1 2 に記憶された車両識別番号 V I N とが一致したものとする。次に、情報管理システム 1 は、たとえば、生体情報取得処理 P 5 2 を実行する。

この処理 P 5 2 において、運転者識別部 1 A は、たとえば、認証情報取得部 1 A 3 によって運転者の生体情報 B 1 を取得する。より具体的には、たとえば、認証情報取得部 1 A 3 としての撮像部は、運転者の顔を撮影して顔画像を取得する。

[0114] 次に、情報管理システム 1 は、照合処理 P 5 3 を実行する。この処理 P 5 3 において、運転者識別部 1 A は、たとえば、照合部 1 A 6 により、認証情報取得部 1 A 3 によって取得された生体情報 B 1 と、認証情報記憶部 1 A 4 に記憶された生体情報 B 1 とを照合する。これらが合致しない場合、情報管理システム 1 は、たとえば、登録部 1 A 5 によって、認証情報取得部 1 A 3 によって取得された生体情報 B 1 を固有の個人識別情報 P 1 と関連付けて認証情報記憶部 1 A 4 に記憶させて登録する。

[0115] 一方、認証情報取得部 1 A 3 によって取得された生体情報 B 1 と、認証情報記憶部 1 A 4 に記憶された生体情報 B 1 とが合致すると、照合部 1 A 6 は、その生体情報 B 1 に関連付けられた個人識別情報 P 1 を認証情報記憶部 1 A 4 から取得する。次に、情報管理システム 1 は、個人識別情報 P 1 の送信処理 P 5 4 を実行する。

[0116] この処理 P 5 4 において、情報管理システム 1 は、たとえば、照合部 1 A 6 によって取得された個人識別情報 P 1 を、インターフェース部 1 A 1 および車載ネットワーク 1 8 を介して、情報取得部 1 2 および情報管理部 1 3 へ送信する。その後、情報管理システム 1 は、図 5 に示す実施形態 1 の運転者情報 D 1 の取得処理 P 1 3、個別情報 P D の送信処理 P 1 4、秘密鍵 S K の準備処理 P 1 5、電子署名処理 P 1 6、および外部送信処理 P 1 7 と同様の処理 P 5 5、P 5 6、P 5 7、P 5 8、P 5 9 を実行する。これにより、車両 V の個別情報 P D が車両 V の外部へ送信される。

[0117] 以上のように、本実施形態の情報管理システム 1 において、運転者識別部 1 A は、運転者の生体情報 B 1 を取得する認証情報取得部 1 A 3 と、生体情報 B 1 と個人識別情報 P 1 とを関連付けて記憶する認証情報記憶部 1 A 4 と、認証情報取得部 1 A 3 によって取得された生体情報 B 1 と認証情報記憶部

1 A 4 に記憶された生体情報 B I とを照合する照合部 1 A 6 と、を備えている。照合部 1 A 6 は、認証情報取得部 1 A 3 によって取得された生体情報 B I と認証情報記憶部 1 A 4 に記憶された生体情報 B I とが合致する場合に、合致した生体情報 B I に関連付けられた個人識別情報 P I を認証情報記憶部 1 A 4 から取得する。

[0118] このような構成により、本実施形態の情報管理システム 1 によれば、電子キー 2 または P D A 3 から個人識別情報 P I を取得することなく、実施形態 2 の情報管理システム 1 と同様の効果を奏することができる。

[0119] 以上、図面を用いて本開示に係る情報管理システムの実施形態を詳述してきたが、具体的な構成はこの実施形態に限定されるものではなく、本開示の要旨を逸脱しない範囲における設計変更等があっても、それらは本開示に含まれるものである。

[0120] たとえば、前述の実施形態では、情報管理システムの運転者識別部と、情報取得部と、情報管理部とを、個別の E C U またはマイクロコントローラによって構成する例を説明した。しかし、情報管理システムは、たとえば、1 つのマイクロコントローラによって構成することも可能である。また、情報管理システムを車両に搭載される車両制御装置の一部として構成してもよい。

符号の説明

- [0121] 1 情報管理システム
- 1 1 1 運転者識別部
- 1 2 情報取得部
- 1 2 5 P D 記憶部（個別情報記憶部）
- 1 3 2 P D 記憶部（個別情報記憶部）
- 1 3 3 秘密鍵記憶部
- 1 3 5 電子署名部
- 1 3 6 公開鍵生成部
- 1 3 7 H S M（ハードウェアセキュリティモジュール）

1 5 通信部
1 A 運転者識別部
1 A 3 認証情報取得部
1 A 4 認証情報記憶部
1 A 6 照合部
2 電子キー
3 P D A（携帯情報端末）
B I 生体情報
D I 運転者情報
P D 個別情報
P I 個人識別情報
P K 公開鍵
S K 秘密鍵
T I 走行情報
V 車両

請求の範囲

- [請求項1] 車両の運転者に関する運転者情報を管理する情報管理システムであって、
前記運転者の個人識別情報を取得する運転者識別部と、
前記車両の走行情報を含む前記運転者情報を取得する情報取得部と、
、
前記個人識別情報と前記運転者情報を関連付けた個別情報を記憶する個別情報記憶部と、
を備えることを特徴とする情報管理システム。
- [請求項2] 前記車両の外部と通信可能な通信部と、
前記個人識別情報ごとに固有の秘密鍵が記憶された秘密鍵記憶部と、
、
前記個別情報に関連付けられた前記個人識別情報に固有の前記秘密鍵を用いて前記個別情報に電子署名を行う電子署名部と、をさらに備え、
前記通信部は、前記電子署名が付された前記個別情報を前記車両の外部へ送信することを特徴とする請求項1に記載の情報管理システム。
- [請求項3] 前記秘密鍵記憶部および前記電子署名部を含むハードウェアセキュリティモジュールを備えることを特徴とする請求項2に記載の情報管理システム。
- [請求項4] 前記車両の起動スイッチがオフにされたときに、前記個別情報記憶部に記憶された前記個別情報を消去することを特徴とする請求項2に記載の情報管理システム。
- [請求項5] 前記個別情報の消去前に、前記通信部を介して前記車両の外部へ前記個別情報を送信することを特徴とする請求項4に記載の情報管理システム。
- [請求項6] 前記車両の起動スイッチがオフにされたときに、前記個別情報記憶

部の不揮発性記憶領域に前記個別情報を記憶させ、

前記車両の起動スイッチがオンにされたときに、前記個別情報記憶部の前記不揮発性記憶領域に記憶された前記個別情報を、前記通信部を介して前記車両の外部へ送信してから消去することを特徴とする請求項 2 に記載の情報管理システム。

[請求項7] 前記運転者識別部は、前記車両の電子キーまたは前記運転者が所有する携帯情報端末から送信される前記個人識別情報を取得することを特徴とする請求項 1 に記載の情報管理システム。

[請求項8] 前記運転者識別部は、前記運転者の生体情報を取得する認証情報取得部と、前記生体情報と前記個人識別情報とを関連付けて記憶する認証情報記憶部と、前記認証情報取得部によって取得された前記生体情報と前記認証情報記憶部に記憶された前記生体情報とを照合する照合部と、を備え、

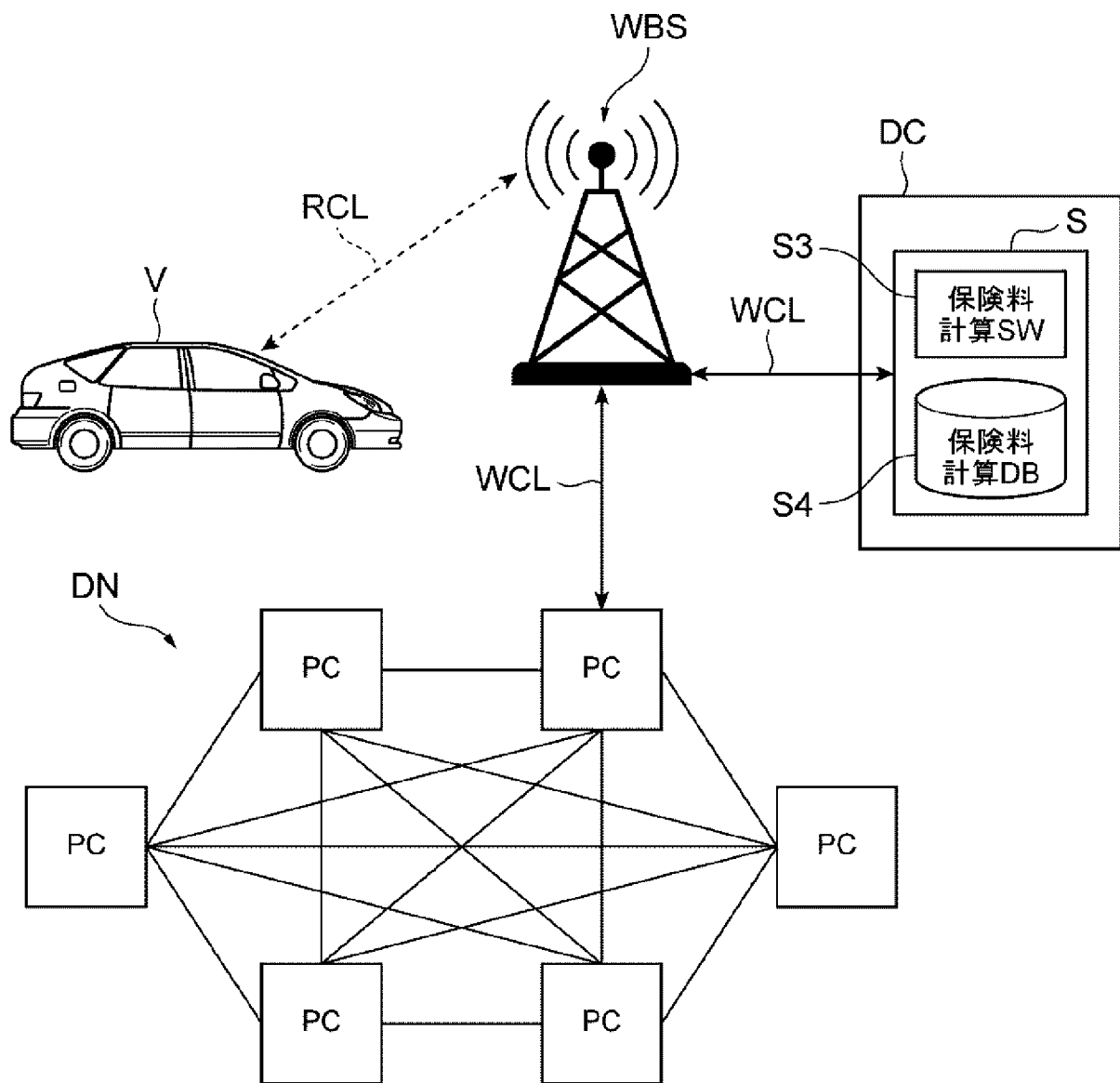
前記照合部は、前記認証情報取得部によって取得された前記生体情報と前記認証情報記憶部に記憶された前記生体情報とが合致する場合に、合致した前記生体情報に関連付けられた前記個人識別情報を前記認証情報記憶部から取得することを特徴とする請求項 1 に記載の情報管理システム。

[請求項9] 個々の前記個人識別情報に固有の前記秘密鍵に対応する公開鍵を生成する公開鍵生成部をさらに備え、

前記通信部は、前記公開鍵を外部へ送信することを特徴とする請求項 2 に記載の情報管理システム。

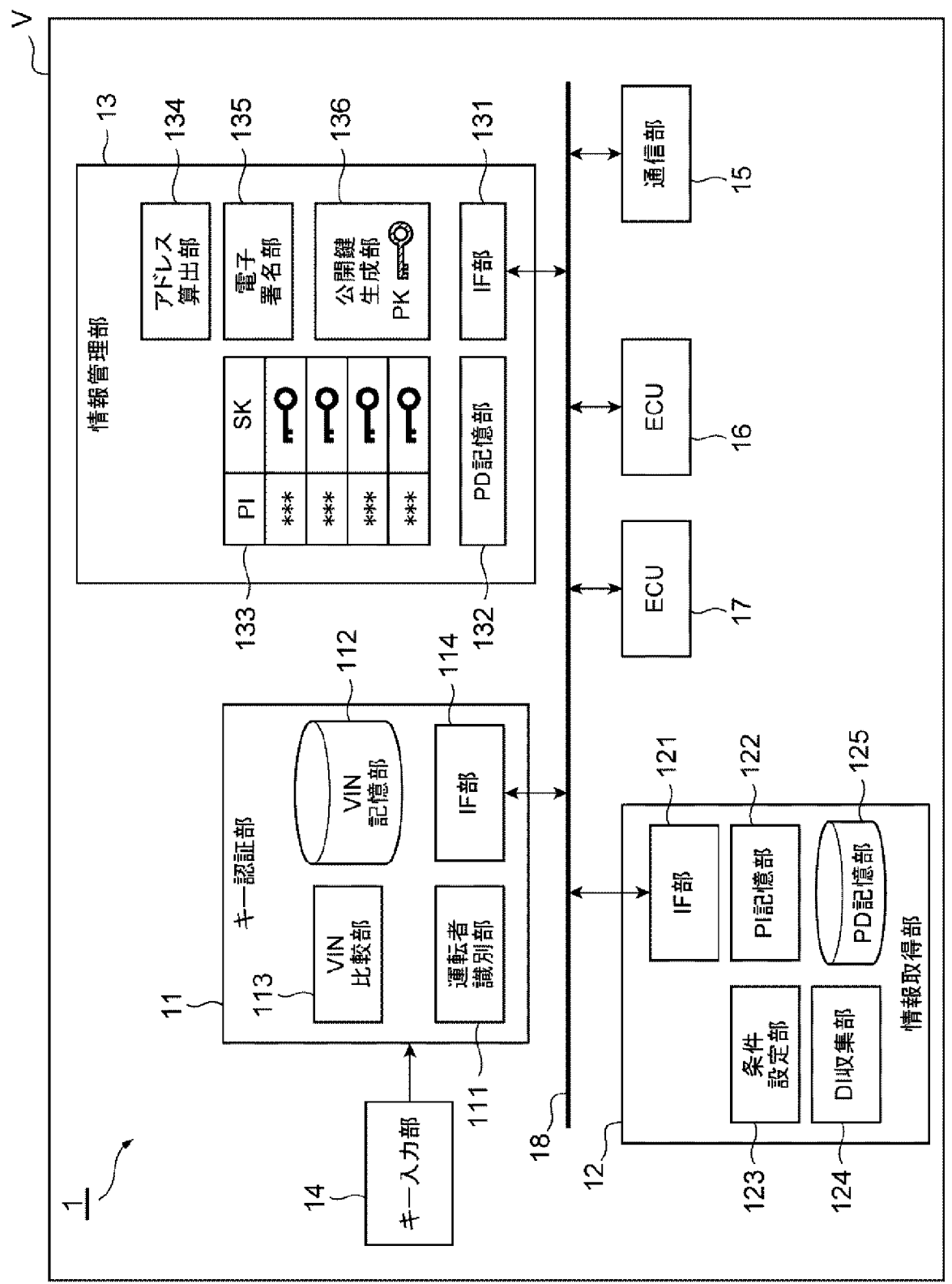
[図1]

図 1



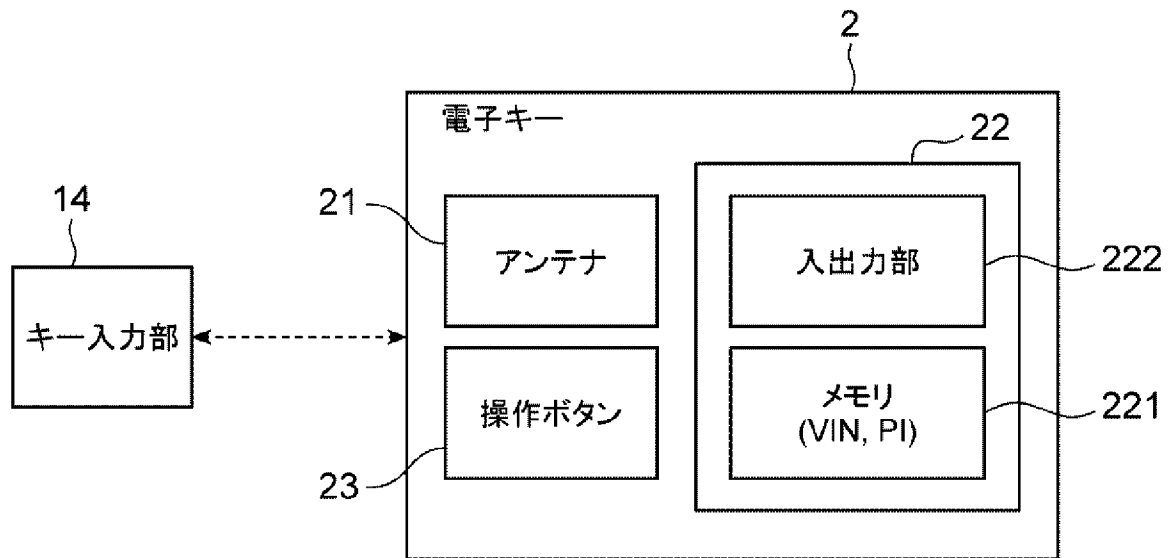
[図2]

図 2



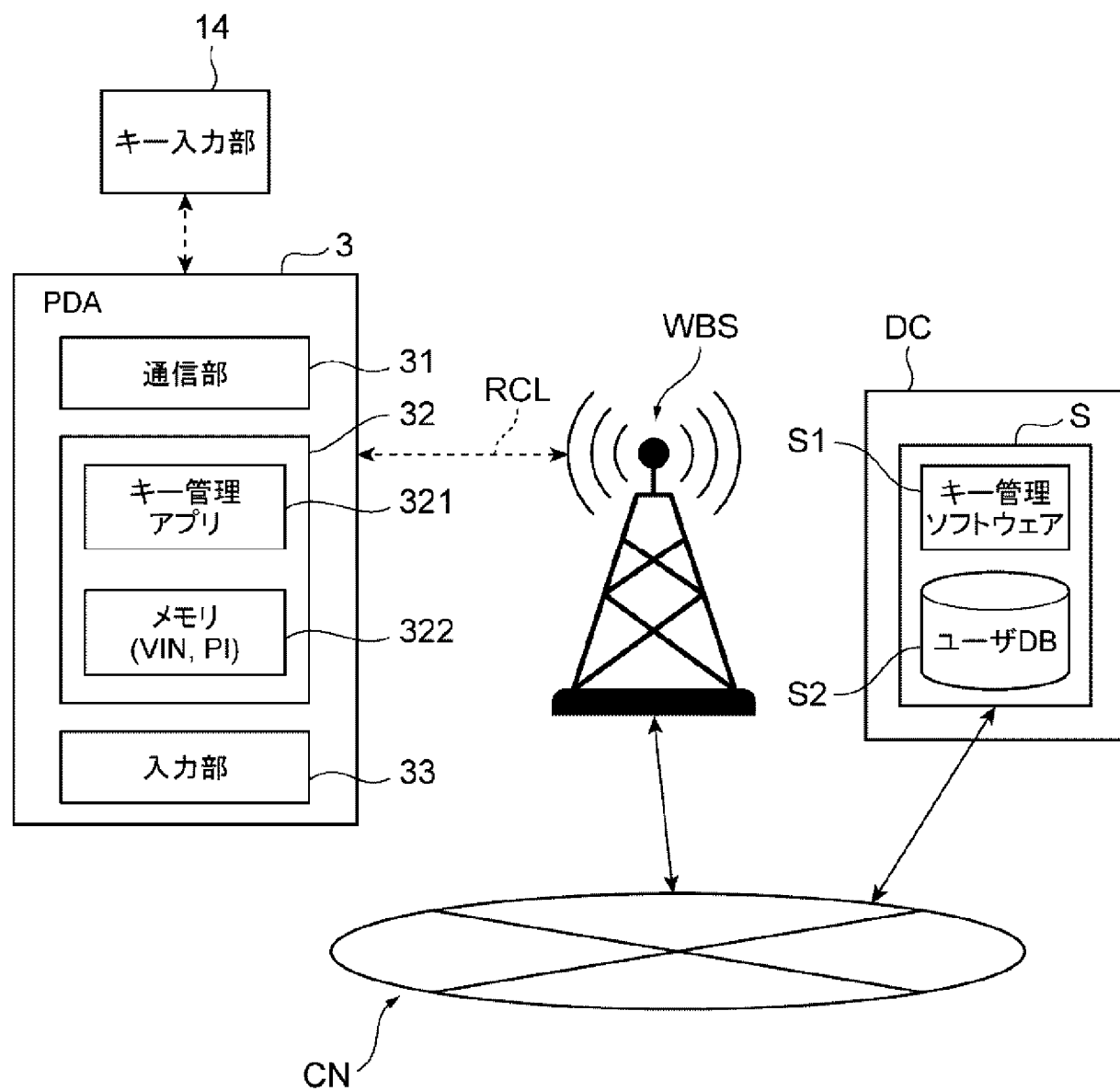
[図3]

図 3



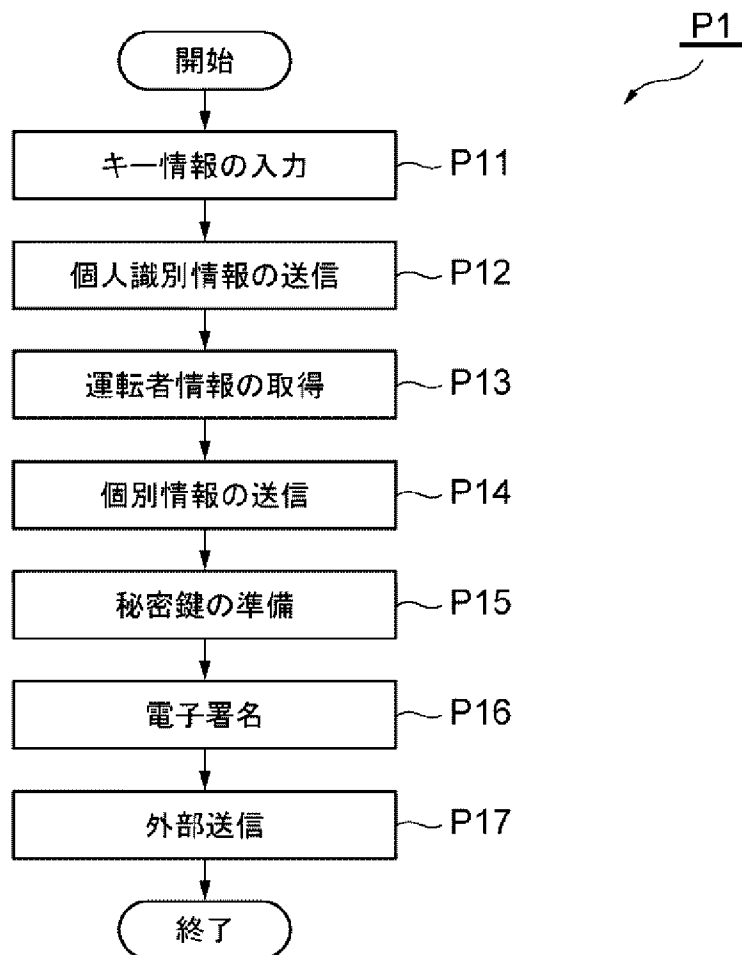
[図4]

図 4



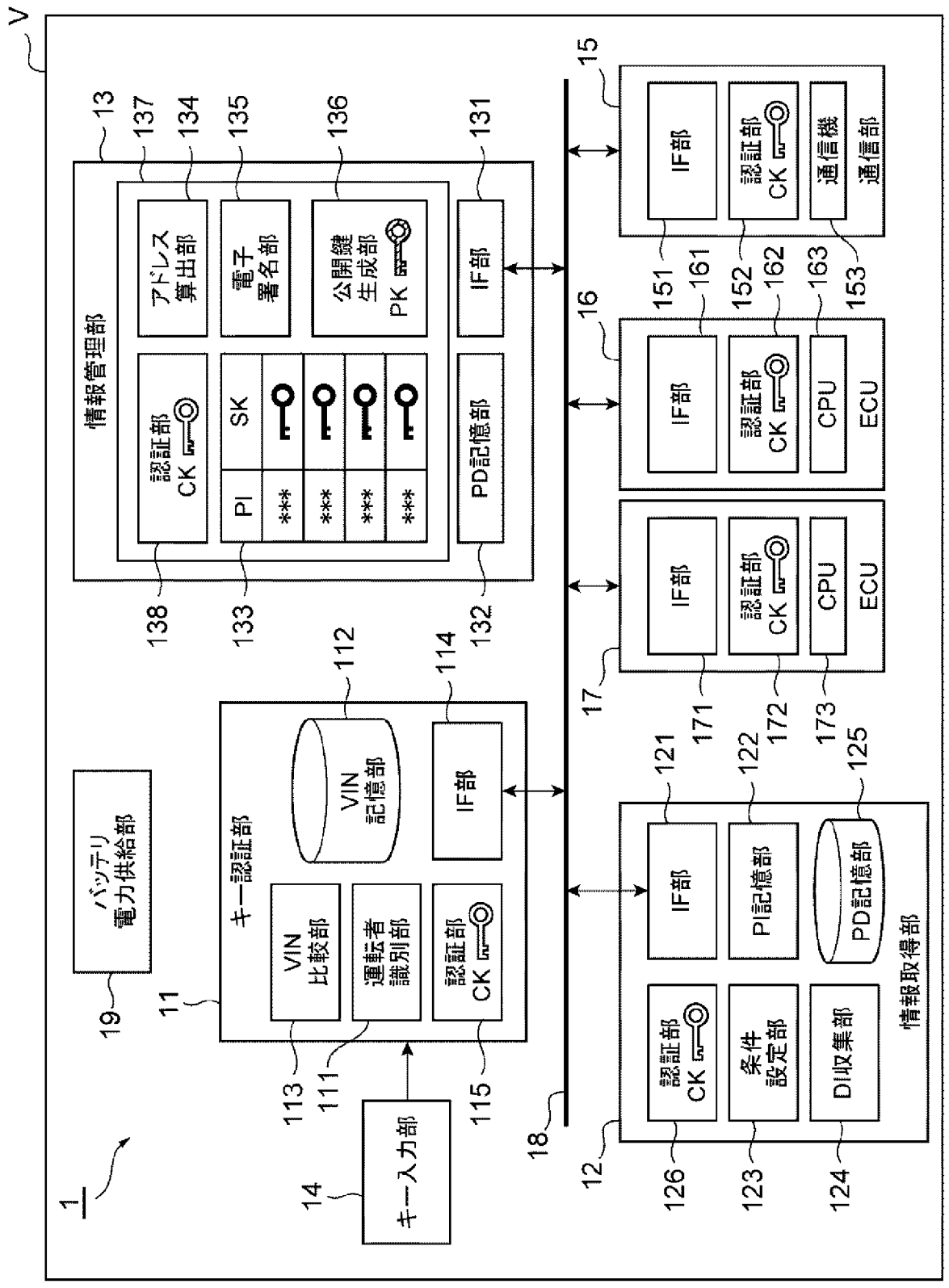
[図5]

図 5



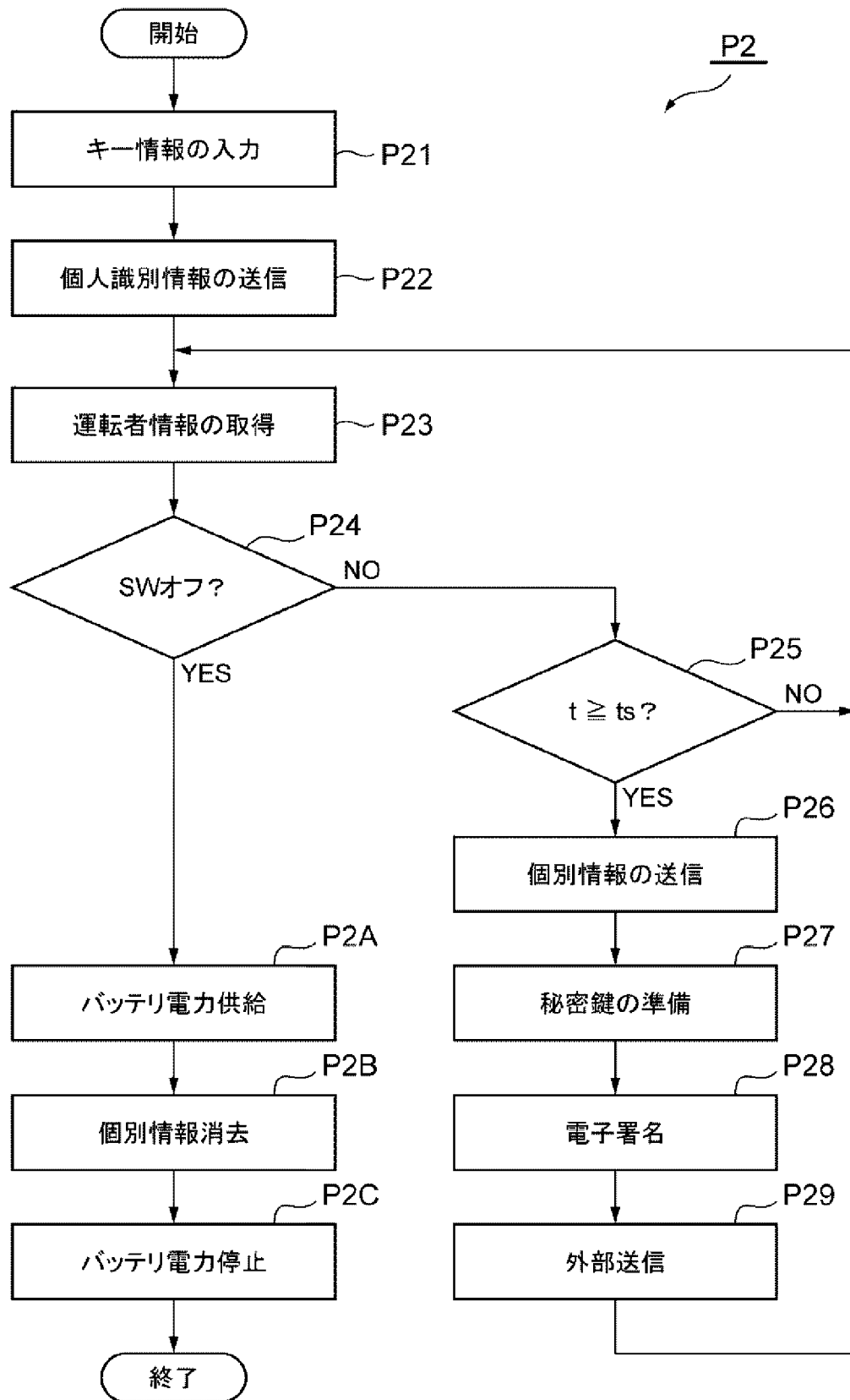
[図6]

図 6



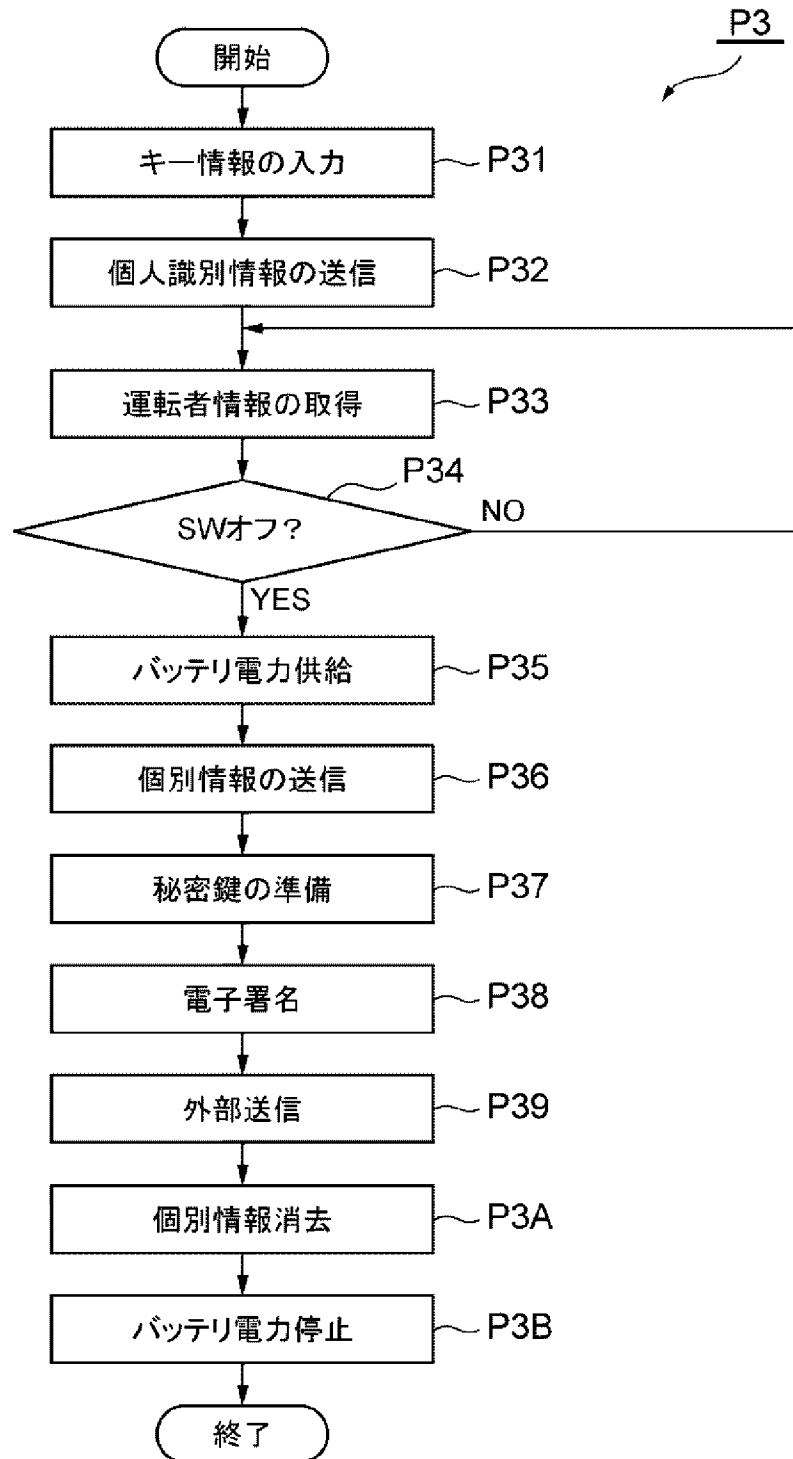
[図7]

図 7



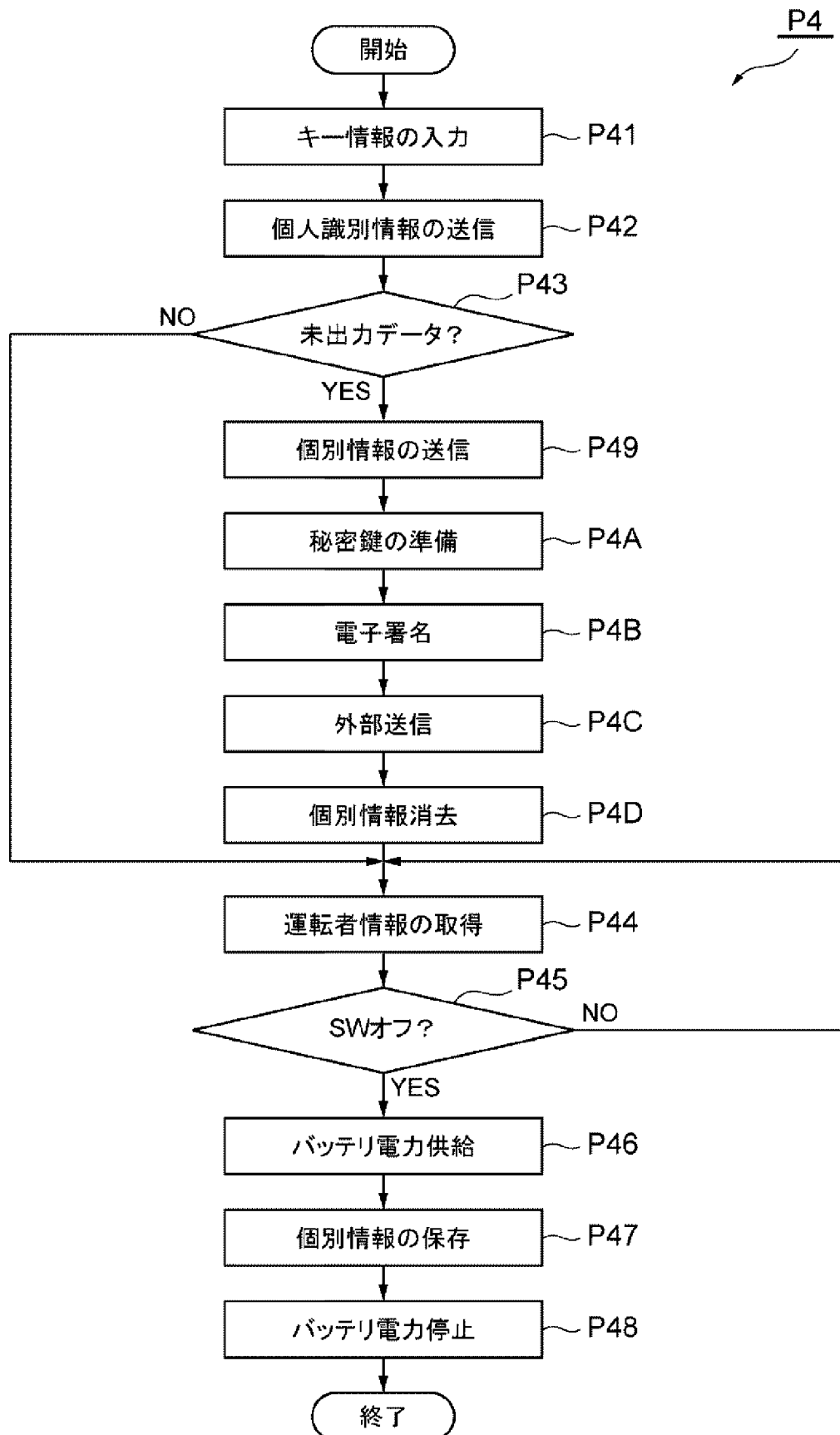
[図8]

図 8



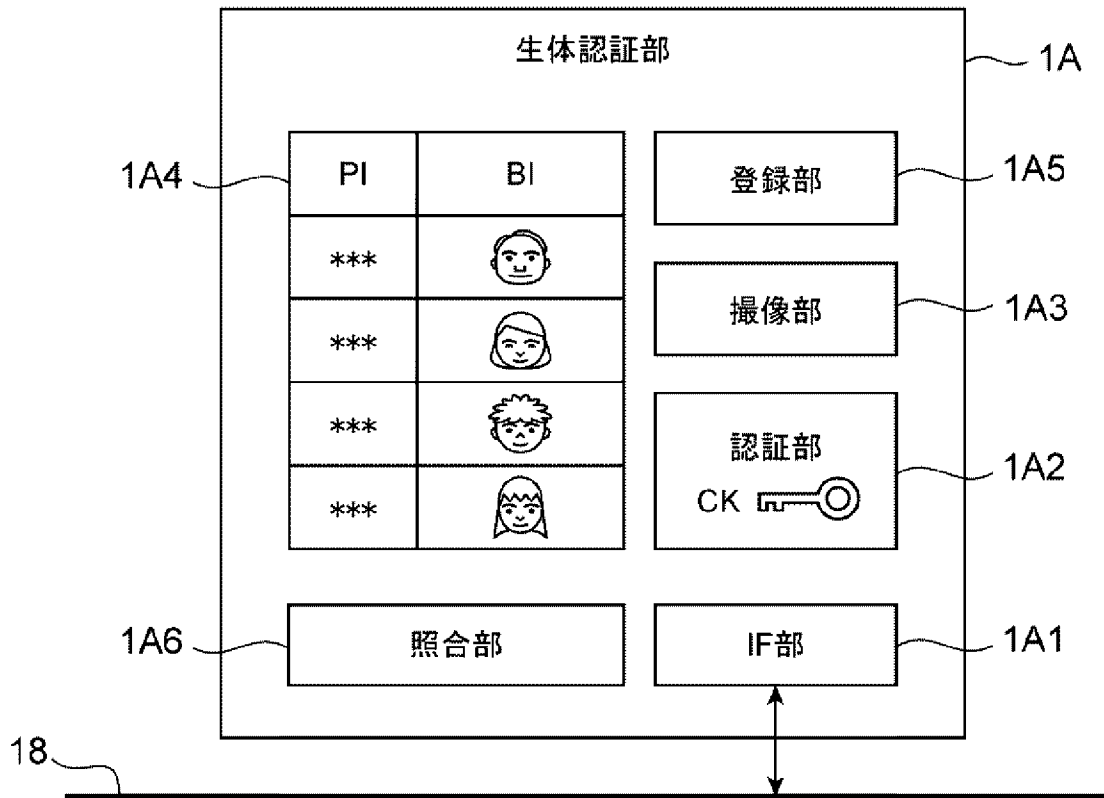
[図9]

図 9



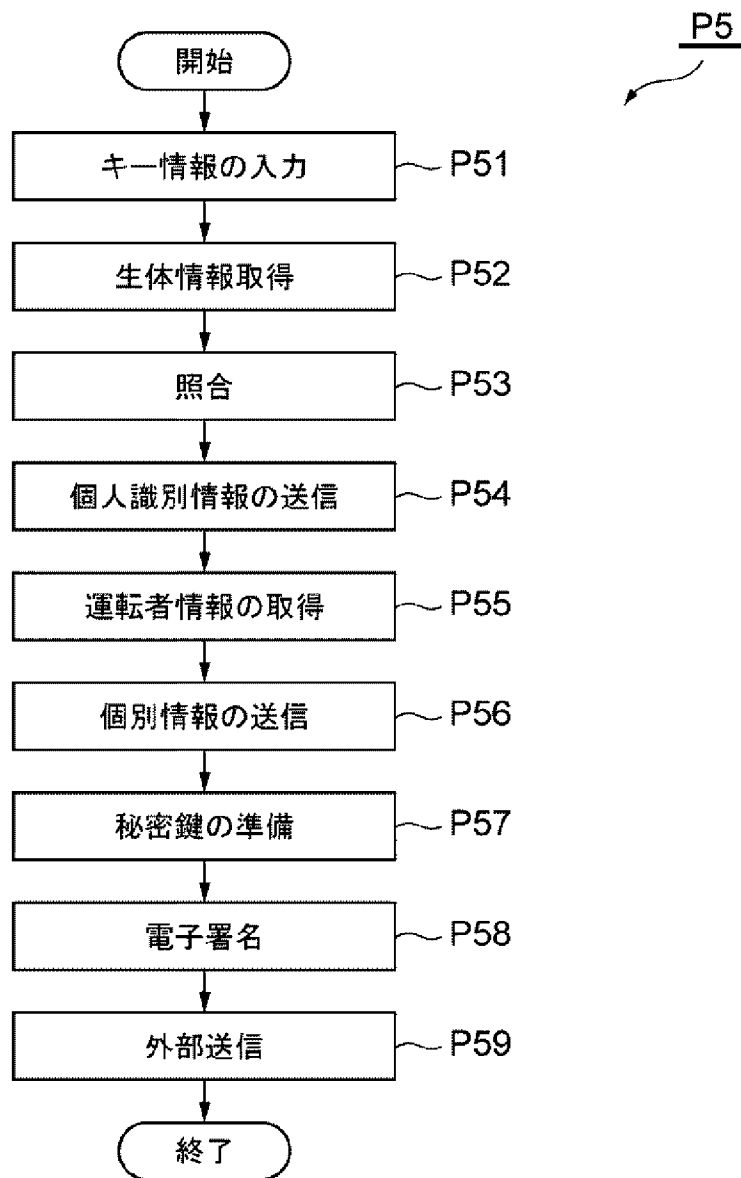
[図10]

図 10



[図11]

図 1 1



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/033001

A. CLASSIFICATION OF SUBJECT MATTER*G09C 1/00*(2006.01)i; *G06F 21/32*(2013.01)i; *G06F 21/62*(2013.01)i; *H04L 9/32*(2006.01)i

FI: G06F21/62 345; H04L9/32 200B; G06F21/32; G09C1/00 640E

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G09C1/00; G06F21/32; G06F21/62; H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2021
 Registered utility model specifications of Japan 1996-2021
 Published registered utility model applications of Japan 1994-2021

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.
X	JP 2014-235609 A (HORIBA LTD) 15 December 2014 (2014-12-15) claims 1, 3, 5	1, 7
A	claims 1, 3, 5, paragraphs [0087]-[0099], [0106], fig. 11-12	2-6, 8-9
X	JP 2009-169486 A (SEIKO EPSON CORP) 30 July 2009 (2009-07-30) paragraphs [0022]-[0073]	1, 8
A		2-7, 9
A	JP 2005-303615 A (NIPPON TELEGR & TELEPH CORP <NTT>) 27 October 2005 (2005-10-27) claims 1, 2, 4	1-9
A	JP 2020-17805 A (KDDI CORP) 30 January 2020 (2020-01-30) claim 1	1-9

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

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

19 November 2021

Date of mailing of the international search report

30 November 2021

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/033001

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2014-235609	A	15 December 2014	CN 104217470 A KR 10-2014-0142135 A	
JP	2009-169486	A	30 July 2009	(Family: none)	
JP	2005-303615	A	27 October 2005	(Family: none)	
JP	2020-17805	A	30 January 2020	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G09C 1/00(2006.01)i; G06F 21/32(2013.01)i; G06F 21/62(2013.01)i; H04L 9/32(2006.01)i FI: G06F21/62 345; H04L9/32 200B; G06F21/32; G09C1/00 640E										
B. 調査を行った分野										
調査を行った最小限資料（国際特許分類（IPC）） G09C1/00; G06F21/32; G06F21/62; H04L9/32										
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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2021年</td> </tr> </table>			日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2021年	日本国実用新案登録公報	1996-2021年	日本国登録実用新案公報	1994-2021年
日本国実用新案公報	1922-1996年									
日本国公開実用新案公報	1971-2021年									
日本国実用新案登録公報	1996-2021年									
日本国登録実用新案公報	1994-2021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								
X	JP 2014-235609 A（株式会社堀場製作所） 15.12.2014（2014-12-15）	1, 7								
A	請求項1, 3, 5 請求項1, 3, 5, 段落[0087]-[0099], [0106], 図11-12	2-6, 8-9								
X	JP 2009-169486 A（セイコーエプソン株式会社） 30.07.2009（2009-07-30）	1, 8								
A	段落[0022]-[0073]	2-7, 9								
A	JP 2005-303615 A（日本電信電話株式会社） 27.10.2005（2005-10-27）	1-9								
A	請求項1, 2, 4									
A	JP 2020-17805 A（KDDI株式会社） 30.01.2020（2020-01-30）	1-9								
A	請求項1									
☐ 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、一般的な技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの “&” 同一パテントファミリー文献										
国際調査を完了した日 19.11.2021	国際調査報告の発送日 30.11.2021									
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 宮司 卓佳 5S 9555 電話番号 03-3581-1101 内線 3546									

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2021/033001

引用文献			公表日	パテントファミリー文献			公表日
JP	2014-235609	A	15.12.2014	CN	104217470	A	
				KR	10-2014-0142135	A	
JP	2009-169486	A	30.07.2009	(ファミリーなし)			
JP	2005-303615	A	27.10.2005	(ファミリーなし)			
JP	2020-17805	A	30.01.2020	(ファミリーなし)			