

(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
2024年1月11日(11.01.2024)

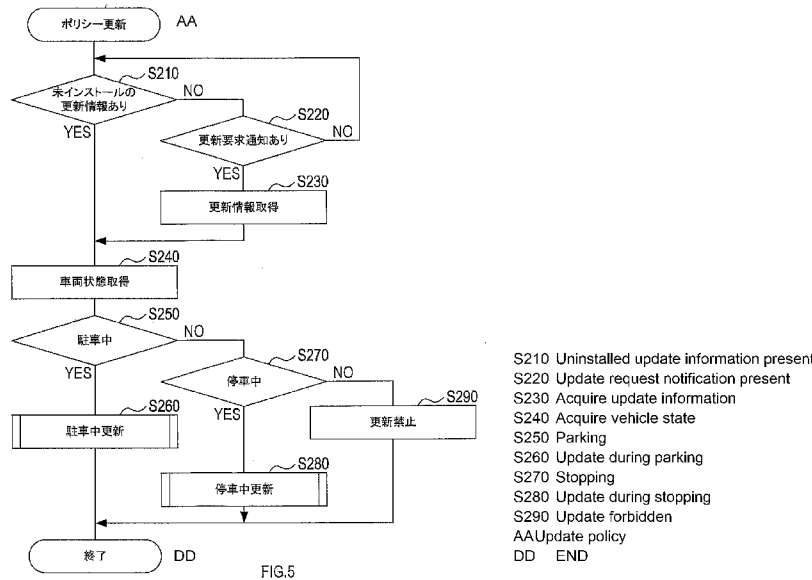


(10) 国際公開番号
WO 2024/009706 A1

- (51) 国際特許分類:
G06F 21/62 (2013.01) *H04L 12/28* (2006.01)
B60R 16/023 (2006.01)
- (21) 国際出願番号: PCT/JP2023/021939
- (22) 国際出願日: 2023年6月13日(13.06.2023)
- (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 2022-110649 2022年7月8日(08.07.2022) JP
- (71) 出願人: 株式会社デンソー (DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町1丁目1番地 Aichi (JP).
- (72) 発明者: 本谷 英之 (HONYA, Hideyuki); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP).
- (74) 代理人: 名古屋国際弁理士法人 (NAGOYA INTERNATIONAL IP FIRM); 〒4600003 愛知県名古屋市中区錦一丁目11番11号 名古屋インターシティ Aichi (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU,

(54) Title: VEHICLE-MOUNTED SYSTEM, ELECTRONIC CONTROL DEVICE, ACCESS AUTHORIZATION POLICY UPDATE METHOD, AND PROGRAM

(54) 発明の名称: 車載システム、電子制御装置、アクセス認可ポリシー更新方法、及びプログラム



(57) Abstract: Necessity determination units (S210-S220) determine whether an update required situation in which it is necessary to update an access authorization policy is in effect. State determination units (S240, S250, S270) determine whether a state of a vehicle on which a vehicle-mounted network is mounted is in a safe state where the access authorization policy can be safely updated. When the necessity determination units determine the necessary update situation and the state determination units determine the safe state, update execution units (S260, S280) update the access authorization policy.

LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

(57) 要約：要否判定部 (S 2 1 0 ~ S 2 2 0) は、アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定する。状態判定部 (S 2 4 0, S 2 5 0, S 2 7 0) は、車載ネットワークを搭載する車両の状態がアクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定する。更新実行部 (S 2 6 0, S 2 8 0) は、要否判定部にて要更新状況にあると判定され、かつ、状態判定部により、安全状態にあると判定された場合に、アクセス認可ポリシーの更新を実施する。

明 細 書

発明の名称：

車載システム、電子制御装置、アクセス認可ポリシー更新方法、及びプログラム

関連出願の相互参照

[0001] 本国際出願は、2022年7月8日に日本国特許庁に出願された日本国特許出願第2022-110649号に基づく優先権を主張するものであり、日本国特許出願第2022-110649号の全内容を本国際出願に参照により援用する。

技術分野

[0002] 本開示は、車両が持つリソースや情報へのアクセスを制御する技術に関する。

背景技術

[0003] 下記特許文献1には、携帯端末用オープンプラットフォームにおいて、サービスアプリケーションを介してシステムが持つリソースや情報へのアクセスを検出したときに、アクセス認可ポリシーを用いて、アクセスを制限する技術が記載されている。アクセス認可ポリシーは、「誰が」「何に対して」「何をするのか」を許可又は禁止することを規定する。

先行技術文献

特許文献

[0004] 特許文献1：特許第6124627号公報

発明の概要

[0005] 今後、車両に搭載される電子制御システム（以下、車載システム）において、サードパーティ製サービスアプリケーションが不特定多数搭載されることが想定される。このため、これら不特定多数のサービスアプリケーションからのアクセスを、アクセス認可ポリシーを用いて制限することが考えられ

る。なお、アクセス認可ポリシーは、アクセスの要求元となるサービスアプリケーションの信頼性、及びアクセス先となるリソースや情報の特性等に応じて設定される。また、様々なニーズに対応すべく、サービスアプリケーションの増加、変更、削除が頻繁に行われるのに伴って、アクセス認可ポリシーの更新頻度が増加することが予想される。

[0006] 車載システムにおけるアクセス認可ポリシーが更新されると、更新の前後でアクセスを許可／禁止する基準が変化することになるため、更新のタイミングによっては、予期しない作動又は不作為が誘発される可能性があった。

[0007] 本開示の1つの局面では、アクセス認可ポリシーの更新を安全に実施する技術を提供する。

[0008] 本開示の一態様は、車載システムであって、複数の機能ブロックと、連携制御部とを備える。複数の機能ブロックは、それぞれが車載ネットワークに接続された複数の電子制御装置のいずれか、又は前記車載ネットワークにリモート接続される外部装置に搭載され、それぞれに割り当てられた機能を実現するように構成される。連携制御部は、複数の機能ブロック間の連携を実現するように構成される。

[0009] 連携制御部は、アクセス制御部と、要否判定部と、状態判定部と、更新実行部と、を備える。

[0010] アクセス制御部は、複数の機能ブロックの一つである利用元ブロックから、複数の機能ブロックの他の一つである利用先ブロックへのアクセス要求を受け付ける。アクセス制御部は、機能ブロック間のアクセス権限を規定するアクセス認可ポリシーを用いて、利用先ブロックに対する利用元ブロックのアクセス権限の有無を判定する。アクセス制御部はアクセス権限が有ると判定した場合、アクセス要求を利用先ブロックに伝達するように構成される。

[0011] 要否判定部は、アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定するように構成される。状態判定部は、車載ネットワークを搭載する車両の状態がアクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定するように構成される。更新実行部は、要

否判定部にて要更新状況にあると判定され、かつ、状態判定部により、安全状態にあると判定された場合に、アクセス認可ポリシーの更新を実施するように構成される。

[0012] このような構成によれば、アクセス認可ポリシーの更新を安全に実施できる。

[0013] 本開示の一態様は、車両に搭載される電子制御装置である。電子制御装置は、アクセス制御部と、要否判定部と、状態判定部と、更新実行部とを備える。つまり、電子制御装置は、上記車載システムから複数の機能ブロックを除いた構成を有する。

[0014] このような構成によれば、アクセス認可ポリシーの更新を安全に実施できる。

[0015] 本開示の一態様は、車両に搭載された電子制御装置によって実施されるアクセス認可ポリシー更新方法である。アクセス認可ポリシーは、それぞれが決められた処理を実行するように構成された複数の機能ブロック間のアクセス権限を規定する。

[0016] アクセス認可ポリシー更新方法は、アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定することを含む。アクセス認可ポリシー更新方法は、車載ネットワークを搭載する車両の状態がアクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定することを含む。アクセス認可ポリシー更新方法は、要更新状況にあると判定され、かつ、安全状態にあると判定された場合に、アクセス認可ポリシーの更新を実施することを含む。

[0017] このような方法によれば、アクセス認可ポリシーの更新を安全に実施できる。

[0018] 本開示の一態様は、以下の機能をコンピュータに実現させるためのプログラムである。

[0019] プログラムがコンピュータに実現させる機能は、アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定する機能を含む。

アクセス認可ポリシーは、それぞれが決められた処理を実行するように構成された複数の機能ブロック間のアクセス権限を規定する。プログラムがコンピュータに実現させる機能は、車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定する機能を含む。プログラムがコンピュータに実現させる機能は、要更新状況にあると判定され、かつ、安全状態にあると判定された場合に、アクセス認可ポリシーの更新を実施する機能を含む。

[0020] このようなプログラムを実行することにより、上記アクセス認可ポリシー更新方法が実現され、その結果、アクセス認可ポリシーの更新を安全に実施できる。

図面の簡単な説明

[0021] [図1]モビリティサービス提供システムの構成を示すブロック図である。

[図2]プラットフォームの構成を示すブロック図である。

[図3]アクセス認可ポリシーの概略を示す説明図である。

[図4]アクセス制御部が実行するアクセス制限処理のフローチャートである。

[図5]ポリシー更新部が実行するポリシー更新処理のフローチャートである。

[図6]駐車中更新処理のフローチャートである。

[図7]停車中更新処理のフローチャートである。

発明を実施するための形態

[0022] 以下、図面を参照しながら、本開示の実施形態を説明する。

[0023] [1. 構成]

図1に示すように、本実施形態のモビリティサービス提供システム1は、車両に搭載される車載システム100と、クラウドサーバ200と、利用者端末300とを備える。車両は、手動運転機能に加えて自動運転機能を有していてもよい。車両は、走行駆動源として、エンジンと電動モータとを有するハイブリッド車両であってもよい。車両は、自動運転機能を有する車両とハイブリッド車両とに限らず、手動運転機能のみを備える車両であってもよいし、走行駆動源としてエンジンのみ又は電動モータのみを有する車両であ

ってもよい。以下では、車載システム１００を搭載する車両を、単に車両という。

[0024] 車載システム１００は、一つの電子制御装置（以下、ＥＣＵ）２と、複数のＥＣＵ３と、複数のＥＣＵ４と、車外通信装置５と、車内通信網６とを備える。ＥＣＵは、Electronic Control Unitの略である。

[0025] ＥＣＵ２は、複数のＥＣＵ３を統括することにより、車両全体として連携がとれた制御を実現する。

[0026] ＥＣＵ３は、車両における機能によって分けられたドメイン毎に設けられ、主として、そのドメイン内に存在する複数のＥＣＵ４の制御を実行する。各ＥＣＵ３は、それぞれ個別に設けられた下層ネットワークを介して配下のＥＣＵ４と接続される。下層ネットワークは、例えば、Controller Area Network（以下、CAN）が用いられる。CANは登録商標である。ＥＣＵ３は、配下のＥＣＵ４に対するアクセス権限などを一元的に管理し利用者の認証等を行う機能を有する。ドメインは、例えば、パワートレイン、ボデー、シャシ、及びコックピット等である。

[0027] パワートレインのドメインに属するＥＣＵ３に接続されるＥＣＵ４は、例えば、エンジンを制御するＥＣＵ４、モータを制御するＥＣＵ４、及び、バッテリーを制御するＥＣＵ４等を含む。

[0028] ボデーのドメインに属するＥＣＵ３に接続されるＥＣＵ４は、例えば、エアコンを制御するＥＣＵ４、及びドアを制御するＥＣＵ４等を含む。

[0029] シャシドメインに属するＥＣＵ３に接続されるＥＣＵ４は、例えば、ブレーキを制御するＥＣＵ、及び、ステアリングを制御するＥＣＵ４等を含む。

[0030] コックピットのドメインに属するＥＣＵ３に接続されるＥＣＵ４は、例えば、メータやナビゲーションの表示を制御するＥＣＵ４、及び車両の乗員によって操作されるＨＭＩ装置７を制御するＥＣＵ４等を含む。ＨＭＩは、Human Machine Interfaceの略である。

[0031] 車外通信装置５は、広域無線通信網を介して、クラウドサーバ２００及び利用者端末３００等の車外装置との間でデータ通信を行う。

[0032] 車内通信網6は、CAN with Flexible Data Rate（以下、CAN FD）とイーサネットとを備える。イーサネットは登録商標である。CAN FDは、ECU2と各ECU3及び車外通信装置5とをバス接続する。イーサネットは、ECU2と各ECU3及び車外通信装置5との間を個別に接続する。ECU2は、使用するイーサネットを切り替えるイーサネットスイッチを備えてもよい。

[0033] ECU2は、CPU2a、ROM2b、及びRAM2c等を備えたマイクロコンピュータを中心に構成された電子制御装置である。マイクロコンピュータの各種機能は、CPU2aが非遷移的実体的記録媒体に格納されたプログラムを実行することにより実現される。この例では、ROM2bが、プログラムを格納した非遷移的実体的記録媒体に該当する。また、このプログラムの実行により、プログラムに対応する方法が実行される。なお、CPU2aが実行する機能の一部又は全部を、一つあるいは複数のIC等によりハードウェア的に構成してもよい。また、ECU2を構成するマイクロコンピュータの数は一つでも複数でもよい。

[0034] ECU3、ECU4、及び車外通信装置5は、いずれも、ECU2と同様に、CPU、ROM、及びRAM等を備えたマイクロコンピュータを中心に構成された電子制御装置である。また、ECU3、ECU4、及び車外通信装置5を構成するマイクロコンピュータの数は一つでも複数でもよい。

[0035] 以下では、ECU2、ECU3、ECU4、及び車外通信装置5を、特に区別しない場合は、車載装置2～5と称する。

[0036] [2. 機能構成]

車載システム100に属する車載装置2～5に搭載されるソフトウェアは、例えば、AUTOSARに沿って構築される。AUTOSARは、自動運転用のアーキテクチャであり、AUTomotive Open System Architectureの略である。AUTOSARは、種々のアプリケーションを実現するために実装されるソフトウェアコンポーネント（以下、SW-C）間の通信だけでなく、クラウドとの接続やセキュリティ等に関する機能も提供する。SW-Cは、

ある機能を実現するために部品化されたソフトウェアである。アプリケーションプログラムは、一つ以上のSW-Cを含む。なお、モビリティサービス提供システム1のソフトウェアは、必ずしもAUTSARに沿って構築される必要はない。

[0037] 車載装置2～5は、いずれも、プラットフォームを備える。プラットフォームは、ハードウェアに依存しない形式で記述されたSW-Cを実行する環境を提供する。

[0038] プラットフォームは、ランタイム環境（以下、RTE）と、基盤ソフトウェア（以下、BSW）とを備える。RTEは、SW-C同士、及びSW-CとBSWとの間をつなぐインタフェースである。BSWは、ハードウェアとSW-Cとをつなぐ階層であり、OS、ドライバ、ミドルウェア等を含む。BSWの機能は、細かいモジュールに分割される。各モジュールの機能は、Application Programming Interface（以下、API）を介してSW-Cに提供される。

[0039] 図2に示すように、車載装置2～5は、プラットフォーム上で動作するサービスアプリケーション（以下、サービスアプリ）の集合として、サービス系機能ブロック群21を備える。サービスアプリは、クライアントからリクエストを受け、処理し、結果を返すアプリケーションである。個々のサービスアプリは、一つ以上のSW-Cによって構成される。サービスアプリは、車載装置2～5のいずれかだけでなく、クラウドサーバ200等、車外通信装置5を介して車内通信網6にリモート接続される外部装置に実装されてもよい。

[0040] サービス系機能ブロック群21は、Original Equipment Manufacturer（以下、OEM）によって提供されるサービスアプリ（以下、OEMアプリ）を含む。OEMは、車両を製造した車両メーカーである。OEMアプリには、OEM自身によって開発されたアプリと、他ベンダーによって開発されたアプリとが存在してもよい。サービス系機能ブロック群21は、サードパーティによって提供されるサービスアプリ（以

下、3rdアプリ)を含んでもよい。サードパーティは、車両の所有者、及びOEM以外の第三者である。サードパーティとして、例えば、車両からデータを収集することによってサービスを提供するデータ活用業者が挙げられる。

[0041] プラットフォームは、制御系機能ブロック群22と、データ系機能ブロック群23と、APIゲートウェイ30とを備える。

[0042] 制御系機能ブロック群22は、車両の運動に関わる指令を受け付けるAPIを備え、APIが受け付けた指令を統括して、整合のとれた車両制御を実現するサービスアプリの集合である。制御系機能ブロック群22は、種々の指令を、該指令に基づく制御を実行する実体が存在する車載装置3～5に対して、車内通信網6を介して出力する。なお、制御系機能ブロック群22は、車両に依存しない形式で表現されているサービス系機能ブロック群21からの種々の指令(すなわち、APIアクセス要求)を、車両に依存した形式で表現された指令に変換する機能を有してもよい。

[0043] データ系機能ブロック群23は、車載装置2～5が有する車両データを扱うためのAPIを備えたサービスアプリの集合である。データ系機能ブロック群23は、各車載装置2～5から供給される、車両に依存した形式で表現された車両データを、車両に依存しない形式に抽象化して蓄積する機能を提供するAPIを有してもよい。データ系機能ブロック群23は、蓄積された車両データを、車外通信装置5を介してクラウドサーバ200にアップロードする機能を提供するAPIを有してもよい。

[0044] 以下では、制御系機能ブロック群22及びデータ系機能ブロック群23に属するサービスアプリが提供するAPIを、車両APIという。車両APIには、車外通信装置5を介してクラウドサーバ200等から後述するアクセス認可ポリシーを取得する機能を提供するAPIが含まれてもよい。車両APIには、車外通信装置5を介して利用者端末300と通信する機能を提供するAPIが含まれてもよい。車両APIには、車両に設けられたHMI装置7を介して乗員に対する情報提供及び乗員による入力操作の受付を行う機

能を提供するAPIが含まれてもよい。車両APIには、車両に設けられた乗員認識センサ8から乗員の有無の判定に必要な情報を取得する機能を提供するAPIが含まれてもよい。乗員認識センサ8は、車室内を撮影するカメラであってもよいし、座席に加わる荷重を検出する圧力センサであってもよい。

[0045] APIゲートウェイ30は、仮想機能バス（以下、VBF）の機能を利用して構成される。VBFは、SW-C間の通信、及びSW-CとBSWとの間の通信を、ハードウェアや通信プロトコル等を意識せず実現できるようにするミドルウェアであり、ソフトウェアバスともいう。SW-C間の通信とは、サービス系機能ブロック群21に属するサービスアプリ間で行う、SW-Cから他のSW-Cが提供するAPIへのアクセスである。SW-CとBSWとの間の通信とは、サービス系機能ブロック群21に属するサービスアプリと、制御系機能ブロック群22及びデータ系機能ブロック群23に属するサービスアプリとの間で行う、SW-Cから車両APIへのアクセスである。以下では、SW-Cとサービスアプリとが1対1で対応するものとして説明する。

[0046] サービスアプリは、制御系機能ブロック群22及びデータ系機能ブロック群23が提供する機能を利用する場合、車両APIへのアクセス要求であるAPIアクセス要求を送信する。APIアクセス要求は、利用元となるサービスアプリ（以下、利用元アプリ）のプロセスID、及び利用先となる車両API（以下、利用先API）を一意に識別する情報であるAPI-IDを少なくとも含む。

[0047] [3. アクセス制限機構]

APIゲートウェイ30は、サービス系機能ブロック群21、制御系機能ブロック群22、及びデータ系機能ブロック群23のいずれかが搭載される可能性がある、すべての車載装置2～5のプラットフォームが備える。

[0048] APIゲートウェイ30は、情報記憶部31と、アクセス制御部32と、車両判定部33と、乗車判定部34と、ポリシー更新部35とを備える。

- [0049] 情報記憶部 31 には、アクセス認可ポリシー 311 と、対応テーブル 312 と、利用者情報 313 とが記憶される。対応テーブル 312 は、RAM 2c に記憶されてもよい。アクセス認可ポリシー 311、利用者情報 313 は、ROM 2b に記憶されてもよい。但し、アクセス認可ポリシー 311、利用者情報 313 は、不揮発性の RAM 2c に記憶されてもよい。
- [0050] アクセス認可ポリシー 311 は、サービスアプリから車両 API へのアクセス権限の有無を判定するための情報の集合である。アクセス認可ポリシー 311 は、例えば、データ系機能ブロック群 23 に属するサービスアプリの機能を用いてクラウドサーバ 200 からダウンロードされて、情報記憶部 31 に記憶される。アクセス認可ポリシーは、図 3 に示すように、例えば、アプリ ID で特定される利用元アプリから、API-ID で特定される利用先 API へのアクセス権限の有無を定義した一覧表によって表される。
- [0051] アクセス認可ポリシー 311 は、例えば、セキュリティ保護資産として定義される属性である S、F、O、P の観点から考慮して設計されてもよい。S は、Safety の略であり、安全性に影響する API アクセスに対するアクセス制限を意味する。F は、Financial の略であり、企業もしくは個人の財産に影響する API アクセスに対するアクセス制限を意味する。O は、Operational の略であり、車両の操作性に影響する API アクセスに対するアクセス制限を意味する。P は、Privacy の略であり、プライバシー情報に影響する API アクセスに対するアクセス制限を意味する。
- [0052] 対応テーブル 312 は、オペレーティングシステム（以下、OS）におけるプログラムの実行単位であるプロセスに対して動的に割り当てられるプロセス ID と、そのプロセスで実行されるサービスアプリが有する固有のアプリ ID とを対応づける情報を含む。また、対応テーブル 312 は、個々の車両 API が有する固有の API-ID と、API の機能を実行する実体であるサービスアプリに割り当てられたプロセスのプロセス ID と、を対応づける情報を含む。対応テーブル 312 は、システムの起動時に、サービスア

り毎のプロセスが生成されるときに、OSによって生成される。

[0053] なお、アクセス認可ポリシー311と対応テーブル312とを組み合わせることで、一つのテーブルを生成してもよい。具体的には、対応テーブル312に示されるアプリIDとプロセスIDとの対応づけ、及びAPI-IDとプロセスIDとの対応付けを参照し、利用元アプリのプロセスIDから利用先APIのプロセスIDへのアクセス権限の有無を示すテーブルを生成してもよい。

[0054] 利用者情報313は、車両利用者によって任意に設定される情報である。例えば、利用者情報313は、車両利用者を識別する利用者IDに対応付けて、車両利用者への連絡先、例えば、所持する携帯端末の電話番号、メールアドレス等が記憶される。車両利用者は、車両の所有者であってもよいし、シェアカー等の車両を一時的に利用する利用者であってもよい。

[0055] アクセス制御部32は、APIアクセス要求を受け付けると、APIアクセス要求に示されたプロセスIDから、対応テーブル312を用いて利用元アプリのアプリIDを特定する。アクセス制御部32は、特定されたアプリIDと、APIアクセス要求に示された利用先APIのAPI-IDとに基づき、アクセス認可ポリシー311に従って、アクセス権限の有無を判定するアクセス制限処理を実行する。アクセス制限処理の詳細については後述する。

[0056] 車両判定部33は、ポリシー更新部35からの要求に従って車両状態及びバッテリー状態を判定して、判定結果をポリシー更新部35に提供する。具体的には、車両判定部33は、制御系機能ブロック群22が提供するAPIを利用して、車速、シフトレバー位置等の情報を取得することによって、車両状態が駐車中、停車中、走行中のいずれに該当するかを判定する。例えば、シフトレバー位置がパーキングである場合は駐車中と判定し、シフトレバー位置がパーキング以外である場合、車速の絶対値が所定値（例えば、1 km/h）未満であれば以下であれば停車中、所定値以上であれば走行中と判定する。また、車両判定部33は、制御系機能ブロック群22が提供するAPI

Ｉを利用して、バッテリー電圧を取得することによって、バッテリー状態が、通常状態にあるか、低電圧状態にあるかを判定する。低電圧状態は、ＡＰＩゲートウェイ３０としての機能を実現する処理を実行するマイクロコンピュータが、誤作動する可能性が、予め設定された許容値を超えて高くなるような電圧範囲にあることをいう。

[0057] 乗車判定部３４は、ポリシー更新部３５からの要求に従って、乗員の有無を判定して、判定結果をポリシー更新部３５に提供する。具体的には、乗車判定部３４は、制御系機能ブロック群２２が提供するＡＰＩを利用して、乗員認識センサ８の検知結果を取得して、乗員の有無を判定する。

[0058] ポリシー更新部３５は、アクセス認可ポリシーの更新が必要な状況が検出された場合に、車両判定部３３及び乗車判定部３４での判定結果に従ってアクセス認可ポリシーの更新を実行する。

[0059] [５．処理]

[５－１．アクセス制限処理]

アクセス制御部３２が実行するアクセス制限処理を、図４のフローチャートを用いて説明する。アクセス制限処理は、ＡＰＩゲートウェイ３０が起動すると繰り返し実行される。

[0060] Ｓ１１０では、アクセス制御部３２は、サービスアプリからＡＰＩアクセス要求を受け付けたか否かを判定し、ＡＰＩアクセス要求を受け付けていれば処理をＳ１２０に移行し、ＡＰＩアクセス要求を受け付けていなければ、同ステップを繰り返すことで待機する。

[0061] Ｓ１２０では、アクセス制御部３２は、ＡＰＩアクセス要求に示された情報に基づき、アクセス認可ポリシー３１１を参照して、ＡＰＩアクセス要求の要求元である利用元アプリが利用先ＡＰＩに対するアクセス権限を有するか否かを判定する。具体的には、アクセス制御部３２は、まず、対応テーブル３１２を用いて、ＡＰＩアクセス要求に示されたプロセスＩＤから利用元アプリのアプリＩＤを特定する。そして、アクセス制御部３２は、特定されたアプリＩＤと、ＡＰＩアクセス要求に示された利用先ＡＰＩのＡＰＩ－Ｉ

Dとに基づき、アクセス認可ポリシー 311を参照して、利用元アプリから利用先APIへのアクセス権限の有無を判定する。

[0062] 続くS130では、アクセス制御部32は、利用元アプリから利用先APIへのアクセス権限が有ると判定した場合は、処理をS140に移行し、アクセス権限が無いと判定した場合は処理をS150に移行する。

[0063] S140では、アクセス制御部32は、利用元アプリから利用先APIへのアクセスを許可し、すなわち、APIアクセス要求を利用先APIに伝達して処理を終了する。

[0064] S150では、アクセス制御部32は、利用元アプリから利用先APIへのアクセスを拒否し、すなわち、APIアクセス要求を破棄して、処理を終了する。

[0065] なお、S150では、単にAPIアクセス要求を破棄する代わりに、アクセス制御部32は、HMI装置7を介して、車両利用者へ当該アクセスの可否を確認してもよい。そして、アクセス制御部32は、HMI装置7を介して、当該アクセスを許可することを示す許可入力を受け付けた場合、処理をS140に移行し、当該アクセスを許可しないことを示す不許可入力を受け付けた場合、APIアクセス要求を破棄してもよい。

[0066] [5-2. ポリシー更新処理]

ポリシー更新部35が実行するポリシー更新処理を、図5のフローチャートを用いて説明する。ポリシー更新処理は、APIゲートウェイ30が起動すると繰り返し実行される。

[0067] S210では、ポリシー更新部35は、未インストールの更新情報が存在するか否かを判定する。ポリシー更新部35は、未インストールの更新情報が存在すると判定した場合、要更新状況であるとして、処理をS240に移行し、未インストールの更新情報が存在しないと判定した場合、処理をS220に移行する。

[0068] S220では、ポリシー更新部35は、アクセス認可ポリシーの更新要求が有るか否かを判定し、更新要求が有れば、要更新状況であるとして処理を

S 2 3 0に移行し、更新要求が無ければ処理をS 2 1 0に戻す。更新要求は、例えば、車載システム1 0 0に提供する新たなアクセス認可ポリシーがクラウドサーバ2 0 0にアップロードされていることを示すクラウドサーバ2 0 0から通知であってもよい。

[0069] S 2 3 0では、ポリシー更新部3 5は、車外通信装置5を介してアクセス認可ポリシーを取得する機能を提供するA P Iを用いて、クラウドサーバ2 0 0からアクセス認可ポリシーに更新情報を取得して、処理をS 2 4 0に進める。

[0070] S 2 4 0では、ポリシー更新部3 5は、車両判定部3 3を介して車両状態を取得する。

[0071] 続くS 2 5 0では、ポリシー更新部3 5は、取得した車両状態が駐車中であるか否かを判定する。ポリシー更新部3 5は、駐車中であると判定した場合、アクセス認可ポリシーの更新を安全に実行可能な安全状態であるとして、処理をS 2 6 0に移行し、駐車中ではないと判定した場合、処理をS 2 7 0に移行する。

[0072] S 2 6 0では、ポリシー更新部3 5は、駐車中更新処理を実行して処理を終了する。

[0073] S 2 7 0では、ポリシー更新部3 5は、取得した車両状態が停車中であるか否かを判定する。ポリシー更新部3 5は、停車中であると判定した場合、安全状態であるとして処理をS 2 8 0に移行し、停車中ではないと判定した場合、すなわち、走行中であれば、安全状態ではないとして、処理をS 2 9 0に移行する。

[0074] S 2 8 0では、ポリシー更新部3 5は、停車中更新処理を実行して処理を終了する。

[0075] S 2 9 0では、ポリシー更新部3 5は、更新を禁止して処理を終了する。更新を禁止された場合、更新情報は、削除されることなく、未インストールの更新情報として保持される。

[0076] [5 - 3 . 駐車中更新処理]

ポリシー更新部35が、S260で実行する駐車中更新処理を、図6のフローチャートを用いて説明する。

[0077] S300では、ポリシー更新部35は、乗車判定部34を介して乗車状態を取得する。

[0078] 続くS310では、ポリシー更新部35は、取得した乗車状態から車両利用者が乗車しているか否かを判定し、車両利用者が乗車していれば処理をS320に移行し、車両利用者が乗車していなければ処理をS350に移行する。

[0079] S320では、ポリシー更新部35は、車両利用者に対して更新確認を通知済であるか否かを判定し、更新確認を通知済みであれば、処理をS340に移行し、更新確認を通知済みでなければ、処理をS330に移行する。

[0080] S330では、ポリシー更新部35は、HMI装置7を介して、アクセス認可ポリシーの更新の可否を確認する機能を提供するAPIを用いて、更新確認通知を送信して、処理を終了する。

[0081] S340では、ポリシー更新部35は、HMI装置7を介して、アクセス認可ポリシーの更新を許可する許可入力を受け付けたか否かを判定し、許可入力を受け付けていれば処理をS350に移行し、許可入力を受け付けていなければ処理を終了する。

[0082] S350では、ポリシー更新部35は、車両判定部33を介してバッテリー状態を取得する。

[0083] 続くS360では、ポリシー更新部35は、取得したバッテリー状態が低電圧状態であるか否かを判定し、低電圧状態であれば、処理をS370に移行し、低電圧状態でなければ、処理をS380に移行する。

[0084] S370では、ポリシー更新部35は、アクセス許可ポリシーの更新を限定的に行って処理を終了する。具体的には、アクセス認可ポリシーにおいて、アクセス権限ありからアクセス権限なしに変更されている部分についてのみインストールを実行する。更新された部分以外の更新情報は、未インストールの更新情報として保持される。

- [0085] S 3 5 0では、ポリシー更新部35は、バッテリー状態だけでなく、駐車中におけるアプリケーションの動作状況を取得してもよい。この場合、例えば、S 3 6 0では、駐車中に診断処理、又はプログラムの更新処理が実行されている場合は、低電圧状態であると判定された場合と同様に、S 3 7 0に移行し、アクセス認可ポリシーの更新を限定的に行ってもよい。
- [0086] S 3 8 0では、ポリシー更新部35は、更新情報の全てについてインストールを実行して、処理を終了する。この場合、未インストールの更新情報は存在しない状態となる。
- [0087] [5-4. 停車中更新処理]
- ポリシー更新部35が、S 2 8 0で実行する停車中更新処理を、図7のフローチャートを用いて説明する。
- [0088] S 4 0 0では、ポリシー更新部35は、乗車判定部34を介して乗車状態を取得する。
- [0089] 続くS 4 1 0では、ポリシー更新部35は、取得した乗車状態から車両利用者が乗車しているか否かを判定し、車両利用者が乗車していれば処理をS 4 2 0に移行し、車両利用者が乗車していなければ処理をS 4 6 0に移行する。
- [0090] S 4 2 0では、ポリシー更新部35は、車両利用者に対して更新確認を通知済であるか否かを判定し、更新確認を通知済みであれば、処理をS 4 4 0に移行し、更新確認を通知済みでなければ、処理をS 4 3 0に移行する。
- [0091] S 4 3 0では、ポリシー更新部35は、HMI装置7を介してアクセス認可ポリシーの更新の可否を確認する機能を提供するAPIを介して、更新確認通知を送信して、処理を終了する。
- [0092] S 4 4 0では、ポリシー更新部35は、HMI装置7を介して、アクセス認可ポリシーの更新を許可する許可入力を受け付けたか否かを判定し、許可入力を受け付けていれば処理をS 4 5 0に移行し、許可入力を受け付けていなければ処理を終了する。
- [0093] S 4 5 0では、ポリシー更新部35は、更新情報の全てについてインスト

ールを実行して、処理を終了する。この場合、未インストールの更新情報は存在しない状態となる。

[0094] S 4 6 0 では、ポリシー更新部 3 5 は、車両利用者に対して更新確認を通知済であるか否かを判定し、更新確認を通知済みであれば、処理を S 4 8 0 に移行し、更新確認を通知済みでなければ、処理を S 4 7 0 に移行する。

[0095] S 4 7 0 では、ポリシー更新部 3 5 は、車外通信装置 5 を介して利用者端末 3 0 0 にアクセス認可ポリシーの更新の可否を確認する通知を行う機能を提供する A P I を利用して、更新確認通知を送信して、処理を終了する。

[0096] S 4 8 0 では、ポリシー更新部 3 5 は、車外通信装置 5 を介して利用者端末 3 0 0 から、アクセス認可ポリシーの更新を許可する許可通知を受け付けたか否かを判定する。ポリシー更新部は、許可通知を受け付けていると判定した場合は処理を S 4 9 0 に移行し、許可通知を受け付けていないと判定した場合は処理を終了する。

[0097] S 4 9 0 では、ポリシー更新部 3 5 は、更新情報の全てについてインストールを実行して、処理を終了する。この場合、未インストールの更新情報は存在しない状態となる。

[0098] つまり、停車中更新処理では、車両利用者が乗車していれば、H M I 装置 7 を介して更新の可否を確認し、車両利用者が乗車していなければ、予め登録された利用者端末 3 0 0 を介して更新の可否を確認する。そして、更新許可の確認が得られた場合にのみアクセス許可ポリシーの更新（すなわち、更新情報のインストール）を実行する。

[0099] [6 . 用語の対応]

本実施形態におけるサービス系機能ブロック群 2 1、制御系機能ブロック群 2 2、及びデータ系機能ブロック群 2 3 が、本開示における複数の機能ブロックに相当する。A P I ゲートウェイ 3 0 が、本開示における連携制御部に相当する。S 2 1 0 ~ S 2 2 0 が、本開示における要否判定部に相当する。S 2 4 0、S 2 5 0、及び S 2 7 0 が、本開示における状態判定部に相当する。S 2 6 0、S 2 8 0 が、本開示における更新実行部に相当する。S 3

20～S330、S420～S430、及びS460～S470が、本開示における許可確認部に相当する。S340、S440、及びS480が、本開示における作動許可部に相当する。S300～S310、及びS400～S410が、本開示における乗員判定部に相当する。S430が、本開示における第1確認部に相当する。S470が、本開示における第2確認部に相当する。S350～S360が、本開示におけるバッテリー状態監視部に相当する。S370が、本開示における限定更新部に相当する。

[0100] [7. 効果]

以上詳述した実施形態によれば、以下の効果を奏する。

[0101] (a) クラウドサーバ200（すなわち、O u t - C a r）側で、アクセス認可ポリシーの更新情報が用意された場合、車載システム100では、車両状態が駐車中又は停車中のときに、アクセス認可ポリシーの更新を許可する。従って、アクセス認可ポリシーが切り替わることにより車両制御の内容に変化が生じたとしても、その変化が車両の移動中に生じることがないため、安全性を確保できる。

[0102] (b) 停車中の場合、車両利用者に対して更新の可否を確認し、更新許可が確認された場合に更新を実施する。つまり、信号待ち等で停車中の場合、直ぐに車両が動き出すことがない状況であるか否か、すなわち、更新に適した状況であるか否かを車両利用者に確認することで、より安全な状況でアクセス認可ポリシーの更新を実施できる。

[0103] (c) 停車中の場合、車両利用者への確認を行う際に、車両利用者が乗車していれば、H M I 装置7を用い、車両利用者が乗車していなければ、予め登録された利用者端末300を用いる。したがって、車両利用者の乗車状況に応じた的確な手段によって、車両利用者の意図を確認できる。

[0104] (d) 駐車中の場合、車両利用者が乗車していれば、車両が動き出す可能性があるため、停車中の場合と同様に車両利用者への確認を行う。また、車両利用者が乗車していなければ、車両が動き出す可能性が低いため、車両利用者への確認を省略して、アクセス認可ポリシーの更新を実行する。このよ

うに、車両利用者に対する確認が、確認が必要な状況にのみ行われるため、不必要な確認によって車両利用者を煩わせることを抑制できる。

[0105] (e) 駐車中の場合、自動的にバッテリーが充電されることがないため、バッテリー状態が低電圧状態にある場合は、更新情報の全部を認可ポリシーの更新に用いるのではなく、安全側に作用する更新情報についてのみ、認可ポリシーの更新に用いる。その後、駐車中以外の状態になり、バッテリーの充電が可能な状態になってから、残りの更新情報を、認可ポリシーの更新に用いる。従って、更新による電力消費を必要最小限とすることができ、また、更新中に電圧低下による誤作動（例えば、更新情報のビット誤り等）が生じることを抑制できる。

[0106] [8. 他の実施形態]

以上、本開示の実施形態について説明したが、本開示は上述の実施形態に限定されることなく、種々変形して実施することができる。

[0107] (a) 上述の実施形態では、更新要求を、クラウドサーバ200にアクセス認可ポリシーの更新情報が用意されたときに発生させているが、更新要求を発生させる契機は、更新情報が容易されたときに限定されない。例えば、異常が検出されたときに、アクセス認可ポリシーの更新要求を発生させてもよい。この場合、情報記憶部31に、異常時用のアクセス認可ポリシーを予め用意しておき、異常による更新要求が発生した場合には、アクセス認可ポリシーを正常時用から異常時用に切り替えてもよい。

[0108] (b) 上述の実施形態では、車両利用者への確認を行う際に、車両利用者が乗車していればHMI装置7を用いているが、乗車していない場合と同様に、利用者端末300を用いてもよい。

[0109] (c) 上述の実施形態では、車両状態が駐車中の場合、車両利用者が乗車しているときだけ、車両利用者への確認を行なっているが、車両利用者が乗車しているか否かに関わらず、常に、車両利用者への確認を行ってもよい。

[0110] (d) 上述の実施形態では、クラウドサーバ200から更新要求通知を受信した場合に、クラウドサーバ200からアクセス認可ポリシーの更新情報

を取得している。例えば、クラウドサーバ200から車載システム100に更新情報が自動的にダウンロードされ、更新情報のダウンロードが確認されると、車載システム100の内部で更新要求通知が発生するように構成されてもよい。この場合、図5におけるS230の処理は省略される。

[0111] (e) 上記実施形態では、車両状態等に応じたアクセス認可ポリシーの更新を、全てのAPIに適用しているが、センサやアクチュエータの動作を伴う制御系機能ブロック群22が提供するAPIに関するアクセス認可ポリシーについてだけ適用してもよい。この場合、データの取得等に用いるデータ系機能ブロック群23が提供するAPIに関するアクセス認可ポリシーについては、未インストールの更新情報があれば車両状態等に関係なく更新処理をしてもよい。

[0112] (f) 本開示に記載の車載装置2～5及びその手法は、コンピュータプログラムにより具体化された一つ乃至は複数の機能を実行するようにプログラムされたプロセッサ及びメモリを構成することによって提供された専用コンピュータにより、実現されてもよい。あるいは、本開示に記載の車載装置2～5及びその手法は、一つ以上の専用ハードウェア論理回路によってプロセッサを構成することによって提供された専用コンピュータにより、実現されてもよい。もしくは、本開示に記載の車載装置2～5及びその手法は、一つ乃至は複数の機能を実行するようにプログラムされたプロセッサ及びメモリと一つ以上のハードウェア論理回路によって構成されたプロセッサとの組み合わせにより構成された一つ以上の専用コンピュータにより、実現されてもよい。また、コンピュータプログラムは、コンピュータにより実行されるインストラクションとして、コンピュータ読み取り可能な非遷移有形記録媒体に記憶されてもよい。車載装置2～5に含まれる各部の機能を実現する手法には、必ずしもソフトウェアが含まれている必要はなく、その全部の機能が、一つあるいは複数のハードウェアを用いて実現されてもよい。

[0113] (g) 上記実施形態における1つの構成要素が有する複数の機能を、複数の構成要素によって実現したり、1つの構成要素が有する1つの機能を、複

数の構成要素によって実現したりしてもよい。また、複数の構成要素が有する複数の機能を、1つの構成要素によって実現したり、複数の構成要素によって実現される1つの機能を、1つの構成要素によって実現したりしてもよい。また、上記実施形態の構成の一部を省略してもよい。また、上記実施形態の構成の少なくとも一部を、他の上記実施形態の構成に対して付加又は置換してもよい。

[0114] (h) 上述した車載システム100の他、当該車載システム100を構成要素とするシステム、当該車載システム100としてコンピュータを機能させるためのプログラム、このプログラムを記録した半導体メモリ等の非遷移的実体的記録媒体など、種々の形態で本開示を実現することもできる。

[0115] [9. 本明細書が開示する技術思想]

[項目1]

それぞれが車載ネットワークに接続された複数の電子制御装置のいずれか、又は前記車載ネットワークにリモート接続される外部装置に搭載され、それぞれが決められた処理を実行するように構成された複数の機能ブロックと、

前記複数の機能ブロック間の連携を実現するように構成された連携制御部と、

を備え、

前記連携制御部は、

前記複数の機能ブロックの一つである利用元ブロックから、前記複数の機能ブロックの他の一つである利用先ブロックへのアクセス要求を受け付けると、前記機能ブロック間のアクセス権限を規定するアクセス認可ポリシーを用いて、前記利用先ブロックに対する前記利用元ブロックの前記アクセス権限の有無を判定し、前記アクセス権限が有ると判定した場合、前記アクセス要求を前記利用先ブロックに伝達するように構成されたアクセス制御部と、

前記アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定するように構成された要否判定部と、

前記車載ネットワークを搭載する車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定するように構成された状態判定部と、

前記要否判定部にて前記要更新状況にあると判定され、かつ、前記状態判定部により、前記安全状態にあると判定された場合に、前記アクセス認可ポリシーの更新を実施するように構成された更新実行部と、

を備える、車載システム。

[0116] [項目 2]

項目 1 に記載の車載システムであって、

前記更新実行部は、

前記アクセス認可ポリシーの更新を実施することについて車両利用者の許可があるか否かを確認するように構成された許可確認部と、

前記許可確認部により前記車両利用者の許可が確認された場合に、前記更新実行部の作動を許可するように構成された作動許可部と、

を更に備える、車載システム。

[0117] [項目 3]

項目 2 に記載の車載システムであって、

前記許可確認部は、前記要否判定部にて前記要更新状況にあると判定され、かつ、前記状態判定部により前記安全状態にあると判定された場合に、前記車両利用者の許可があるか否かを確認するように構成された

車載システム。

[0118] [項目 4]

項目 2 又は項目 3 に記載の車載システムであって、

前記更新実行部は、

前記車両に乗車している乗員の有無を判定するように構成された乗員判定部を更に備え、

前記許可確認部は、

前記乗員判定部にて乗員があると判定された場合、前記車両に装備された

H M I 装置を介して、前記車両利用者の許可を確認するように構成された第 1 確認部と、

前記乗員判定部にて乗員がないと判定された場合、予め登録された利用者端末を介して、前記車両利用者の許可を確認するように構成された第 2 確認部と、

を備える、車載システム。

[0119] [項目 5]

項目 1 から項目 4 までのいずれか 1 項に記載の車載システムであって、
前記更新実行部は、

前記車両に搭載されたバッテリーの状態を監視するように構成されたバッテリー状態監視部と、

前記バッテリーの状態が、当該更新実行部の作動が不安定となる可能性がある低電圧状態である場合、前記アクセス認可ポリシーの更新を部分的に実施する限定更新部と、

を更に備える、車載システム。

[0120] [項目 6]

項目 1 から項目 5 までのいずれか 1 項に記載の車載システムであって、
前記安全状態は、前記車両が駐車中又は停車中の状態である
車載システム。

[0121] [項目 7]

項目 1 から項目 6 までのいずれか 1 項に記載の車載システムであって、
前記要否判定部は、前記アクセス認可ポリシーの更新情報が存在する場合に、前記要更新状況であると判定する
車載システム。

[0122] [項目 8]

項目 1 から項目 7 までのいずれか 1 項に記載の車載システムであって、
前記要否判定部は、前記車両の異常を検出した場合に、前記要更新状況であると判定する

車載システム。

[0123] [項目 9]

車両に搭載される電子制御装置であって、

それぞれが決められた処理を実行するように構成された複数の機能ブロックの一つである利用元ブロックから、前記複数の機能ブロックの他の一つである利用先ブロックへのアクセス要求を受け付けると、前記複数の機能ブロック間のアクセス権限を規定するアクセス認可ポリシーを用いて、前記利用先ブロックに対する前記利用元ブロックの前記アクセス権限の有無を判定し、前記アクセス権限が有ると判定した場合、前記アクセス要求を前記利用先ブロックに伝達するように構成されたアクセス制御部と、

前記アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定するように構成された要否判定部と、

前記車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定するように構成された状態判定部と、

前記要否判定部にて前記要更新状況にあると判定され、かつ、前記状態判定部により、前記安全状態にあると判定された場合に、前記アクセス認可ポリシーの更新を実施するように構成された更新実行部と、

を備える、電子制御装置。

[0124] [項目 10]

項目 9 に記載の電子制御装置であって、

前記要否判定部は、前記アクセス認可ポリシーの更新情報が存在する第 1 の状況である場合、及び前記車両の異常を検出した第 2 の状況である場合に、前記要更新状況であると判定するように構成され、

前記更新実行部は、前記第 1 の状況である場合、当該電子制御装置が接続された車載ネットワークにリモート接続される外部装置から取得する更新情報を用いて正常時用のアクセス認可ポリシーを更新し、前記第 2 の状況である場合、前記正常時用のアクセス認可ポリシーとは別に用意されている異常時用のアクセス認可ポリシーに切り替えて使用するよう構成された

電子制御装置。

[0125] [項目 1 1]

車両に搭載された電子制御装置によって実施され、それぞれが決められた処理を実行するように構成された複数の機能ブロック間のアクセス権限を規定したアクセス認可ポリシーを更新するアクセス認可ポリシー更新方法であって、

前記アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定すること、

前記車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定すること、

前記要更新状況にあると判定され、かつ、前記安全状態にあると判定された場合に、前記アクセス認可ポリシーの更新を実施すること、

を含む、アクセス認可ポリシー更新方法。

[0126] [項目 1 2]

車両に搭載されたコンピュータに、

それぞれが決められた処理を実行するように構成された複数の機能ブロック間のアクセス権限を規定したアクセス認可ポリシーについて、前記アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定する機能、

前記車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定する機能、

前記要更新状況にあると判定され、かつ、前記安全状態にあると判定された場合に、前記アクセス認可ポリシーの更新を実施する機能、

を実現させるためのプログラム。

請求の範囲

[請求項1]

それぞれが車載ネットワークに接続された複数の電子制御装置（２～５）のいずれか、又は前記車載ネットワークにリモート接続される外部装置（２００）に搭載され、それぞれが決められた処理を実行するように構成された複数の機能ブロック（２１～２３）と、

前記複数の機能ブロック間の連携を実現するように構成された連携制御部（３０）と、

を備え、

前記連携制御部は、

前記複数の機能ブロックの一つである利用元ブロックから、前記複数の機能ブロックの他の一つである利用先ブロックへのアクセス要求を受け付けると、前記機能ブロック間のアクセス権限を規定するアクセス認可ポリシーを用いて、前記利用先ブロックに対する前記利用元ブロックの前記アクセス権限の有無を判定し、前記アクセス権限があると判定した場合、前記アクセス要求を前記利用先ブロックに伝達するように構成されたアクセス制御部（３２）と、

前記アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定するように構成された要否判定部（３５：Ｓ２１０～Ｓ２２０）と、

前記車載ネットワークを搭載する車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定するように構成された状態判定部（３５：Ｓ２４０，Ｓ２５０，Ｓ２７０）と、

前記要否判定部にて前記要更新状況にあると判定され、かつ、前記状態判定部により、前記安全状態にあると判定された場合に、前記アクセス認可ポリシーの更新を実施するように構成された更新実行部（３５：Ｓ２６０，Ｓ２８０）と、

を備える、車載システム。

- [請求項2] 請求項1に記載の車載システムであって、
前記更新実行部は、
前記アクセス認可ポリシーの更新を実施することについて車両利用
者の許可があるか否かを確認するように構成された許可確認部（35
：S320～S330，S420～S430，S460～S470）
と、
前記許可確認部により前記車両利用者の許可が確認された場合に、
前記更新実行部の作動を許可するように構成された作動許可部（35
：S340，S440，S480）と、
を更に備える、車載システム。
- [請求項3] 請求項2に記載の車載システムであって、
前記許可確認部は、前記要否判定部にて前記要更新状況にあると判
定され、かつ、前記状態判定部により前記安全状態にあると判定され
た場合に、前記車両利用者の許可があるか否かを確認するように構成
された
車載システム。
- [請求項4] 請求項2に記載の車載システムであって、
前記更新実行部は、
前記車両に乗車している乗員の有無を判定するように構成された乗
員判定部（35：S300～S310，S400～S410）を更に
備え、
前記許可確認部は、
前記乗員判定部にて乗員があると判定された場合、前記車両に装備
されたHMI装置（7）を介して、前記車両利用者の許可を確認する
ように構成された第1確認部（35：S430）と、
前記乗員判定部にて乗員がないと判定された場合、予め登録された
利用者端末（300）を介して、前記車両利用者の許可を確認するよ
うに構成された第2確認部（35：S470）と、

を備える、車載システム。

[請求項5]

請求項1に記載の車載システムであって、

前記更新実行部は、

前記車両に搭載されたバッテリーの状態を監視するように構成された
バッテリー状態監視部（35：S350～S360）と、

前記バッテリーの状態が、当該更新実行部の作動が不安定となる可能性
がある低電圧状態である場合、前記アクセス認可ポリシーの更新を
部分的に実施する限定更新部（35：S370）と、

を更に備える、車載システム。

[請求項6]

請求項1から請求項5までのいずれか1項に記載の車載システムで
あって、

前記安全状態は、前記車両が駐車中又は停車中の状態である
車載システム。

[請求項7]

請求項1から請求項5までのいずれか1項に記載の車載システムで
あって、

前記要否判定部は、前記アクセス認可ポリシーの更新情報が存在す
る場合に、前記要更新状況であると判定する

車載システム。

[請求項8]

請求項1から請求項5までのいずれか1項に記載の車載システムで
あって、

前記要否判定部は、前記車両の異常を検出した場合に、前記要更新
状況であると判定する

車載システム。

[請求項9]

車両に搭載される電子制御装置であって、

それぞれが決められた処理を実行するように構成された複数の機能
ブロックの一つである利用元ブロックから、前記複数の機能ブロック
の他の一つである利用先ブロックへのアクセス要求を受け付けると、
前記複数の機能ブロック間のアクセス権限を規定するアクセス認可ポ

リシーを用いて、前記利用先ブロックに対する前記利用元ブロックの前記アクセス権限の有無を判定し、前記アクセス権限が有ると判定した場合、前記アクセス要求を前記利用先ブロックに伝達するように構成されたアクセス制御部（32）と、

前記アクセス認可ポリシーの更新を実施する必要がある要更新状況にあるか否かを判定するように構成された要否判定部（35：S210～S220）と、

前記車両の状態が前記アクセス認可ポリシーの更新を安全に実施可能な安全状態にあるか否かを判定するように構成された状態判定部（35：S240，S250，S270）と、

前記要否判定部にて前記要更新状況にあると判定され、かつ、前記状態判定部により、前記安全状態にあると判定された場合に、前記アクセス認可ポリシーの更新を実施するように構成された更新実行部（35：S260，S280）と、

を備える、電子制御装置。

[請求項10]

請求項9に記載の電子制御装置であって、

前記要否判定部は、前記アクセス認可ポリシーの更新情報が存在する第1の状況である場合、及び前記車両の異常を検出した第2の状況である場合に、前記要更新状況であると判定するように構成され、

前記更新実行部は、前記第1の状況である場合、当該電子制御装置が接続された車載ネットワークにリモート接続される外部装置（200）から取得する更新情報を用いて正常時用のアクセス認可ポリシーを更新し、前記第2の状況である場合、前記正常時用のアクセス認可ポリシーとは別に用意されている異常時用のアクセス認可ポリシーに切り替えて使用するよう構成された

電子制御装置。

[請求項11]

車両に搭載された電子制御装置によって実施され、それぞれが決められた処理を実行するように構成された複数の機能ブロック（21～

23) 間のアクセス権限を規定したアクセス認可ポリシーを更新する
アクセス認可ポリシー更新方法であって、

前記アクセス認可ポリシーの更新を実施する必要がある要更新状況
にあるか否かを判定すること (S 210 ~ S 220)、

前記車両の状態が前記アクセス認可ポリシーの更新を安全に実施可
能な安全状態にあるか否かを判定すること (S 240, S 250, S
270)、

前記要更新状況にあると判定され、かつ、前記安全状態にあると判
定された場合に、前記アクセス認可ポリシーの更新を実施すること (S
260, S 280)、

を含む、アクセス認可ポリシー更新方法。

[請求項12]

車両に搭載されたコンピュータに、

それぞれが決められた処理を実行するように構成された複数の機能
ブロック (21 ~ 23) 間のアクセス権限を規定したアクセス認可ポ
リシーについて、前記アクセス認可ポリシーの更新を実施する必要が
ある要更新状況にあるか否かを判定する機能 (S 210 ~ S 220)
、

前記車両の状態が前記アクセス認可ポリシーの更新を安全に実施可
能な安全状態にあるか否かを判定する機能 (S 240, S 250, S
270)、

前記要更新状況にあると判定され、かつ、前記安全状態にあると判
定された場合に、前記アクセス認可ポリシーの更新を実施する機能 (S
260, S 280)、

を実現させるためのプログラム。

[図1]

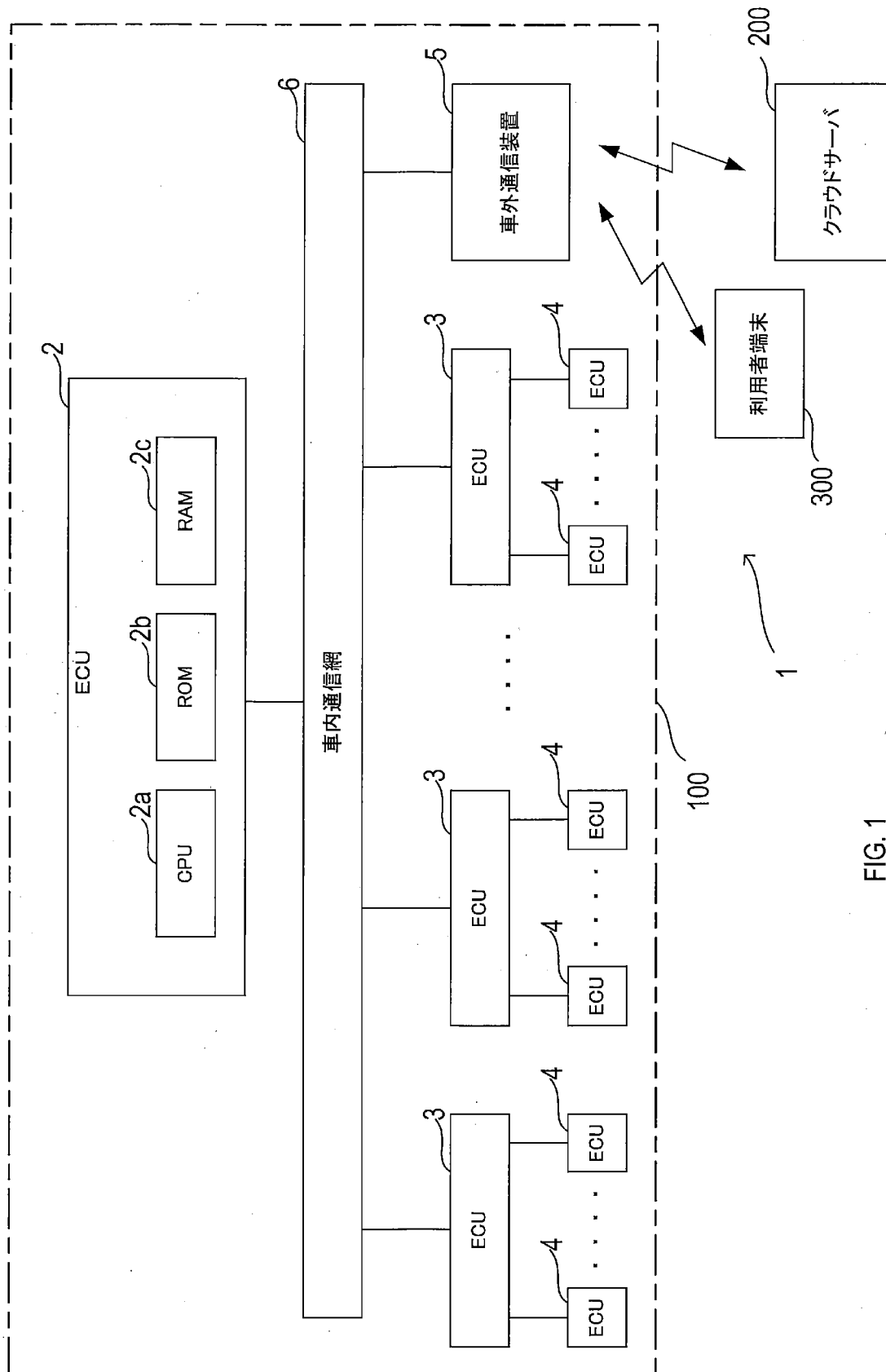


FIG. 1

[図2]

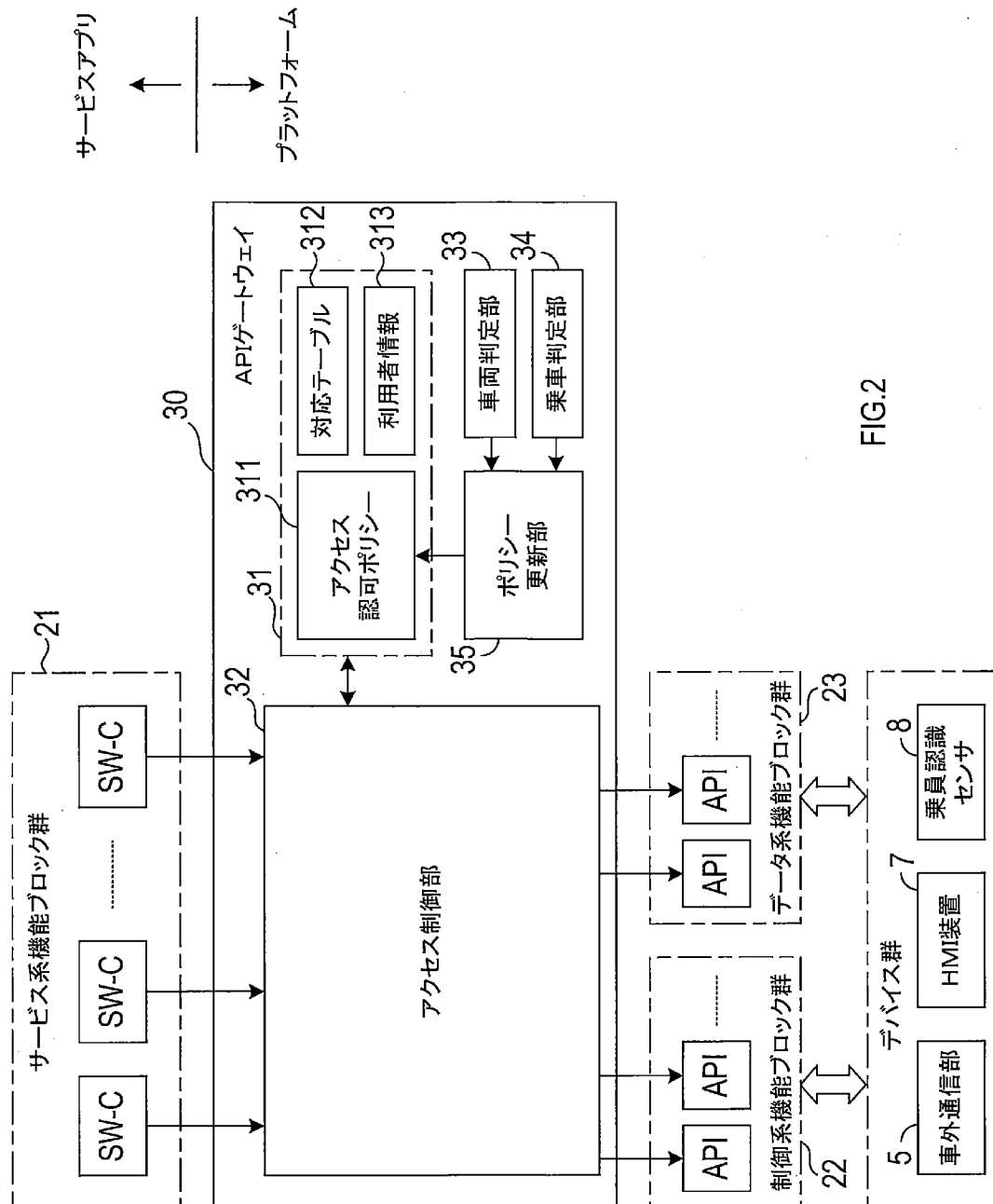


FIG.2

[図3]

アクセス認可ポリシー					
		利用元アプリ			
		S1	S2	S3	S4
利用 先 A P I	P1	○	×	×	×
	P2	○	×	○	○
	P3	○	○	○	○
	P4	○	×	×	○

○ : 権限有り(許可)

× : 権限無し(禁止)

FIG.3

[図4]

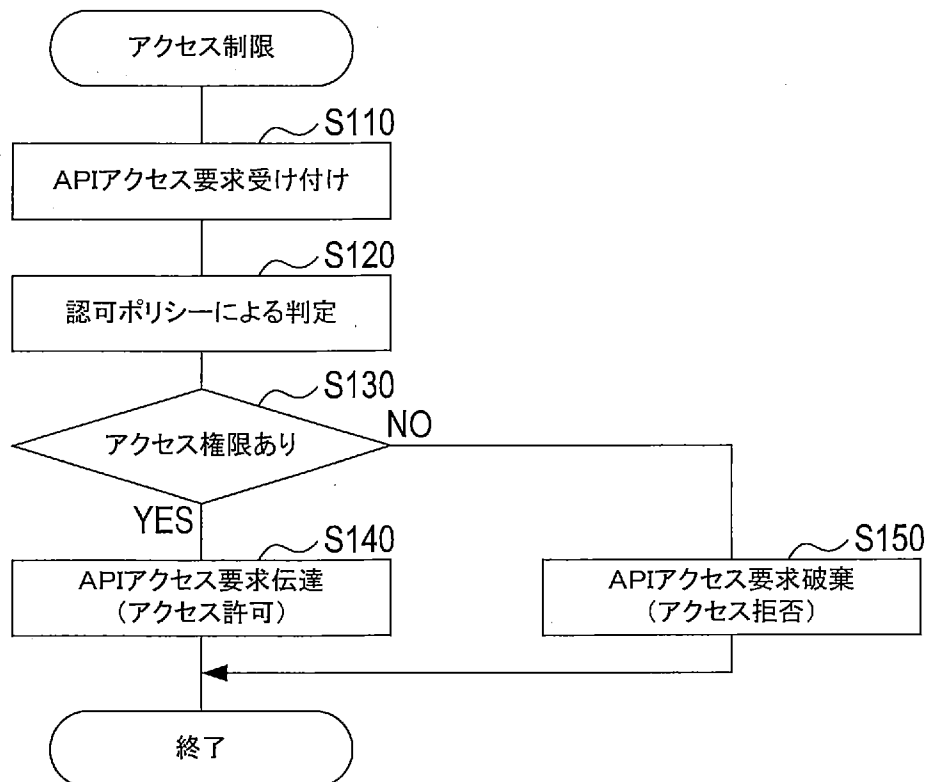


FIG.4

[図5]

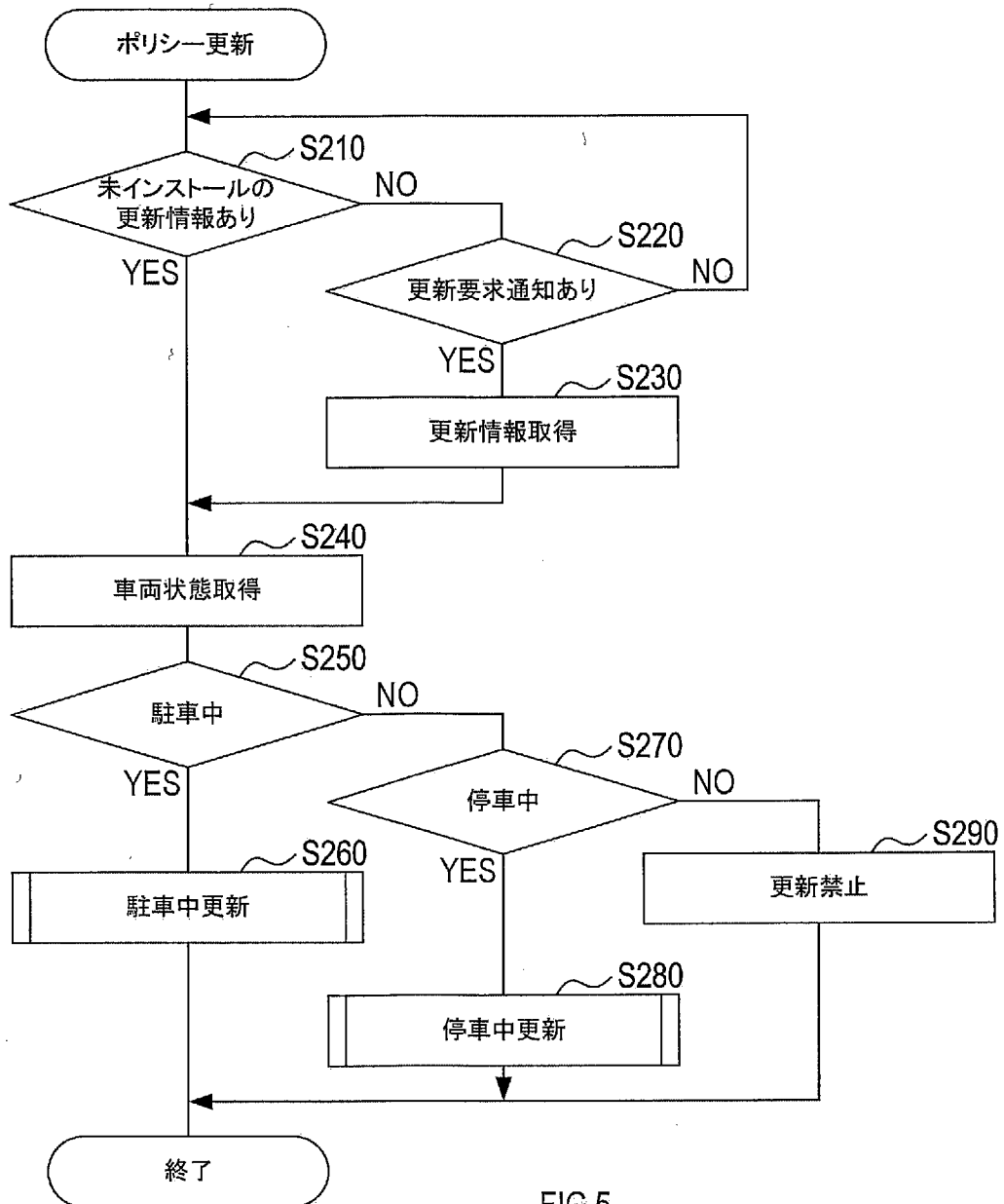


FIG.5

[図6]

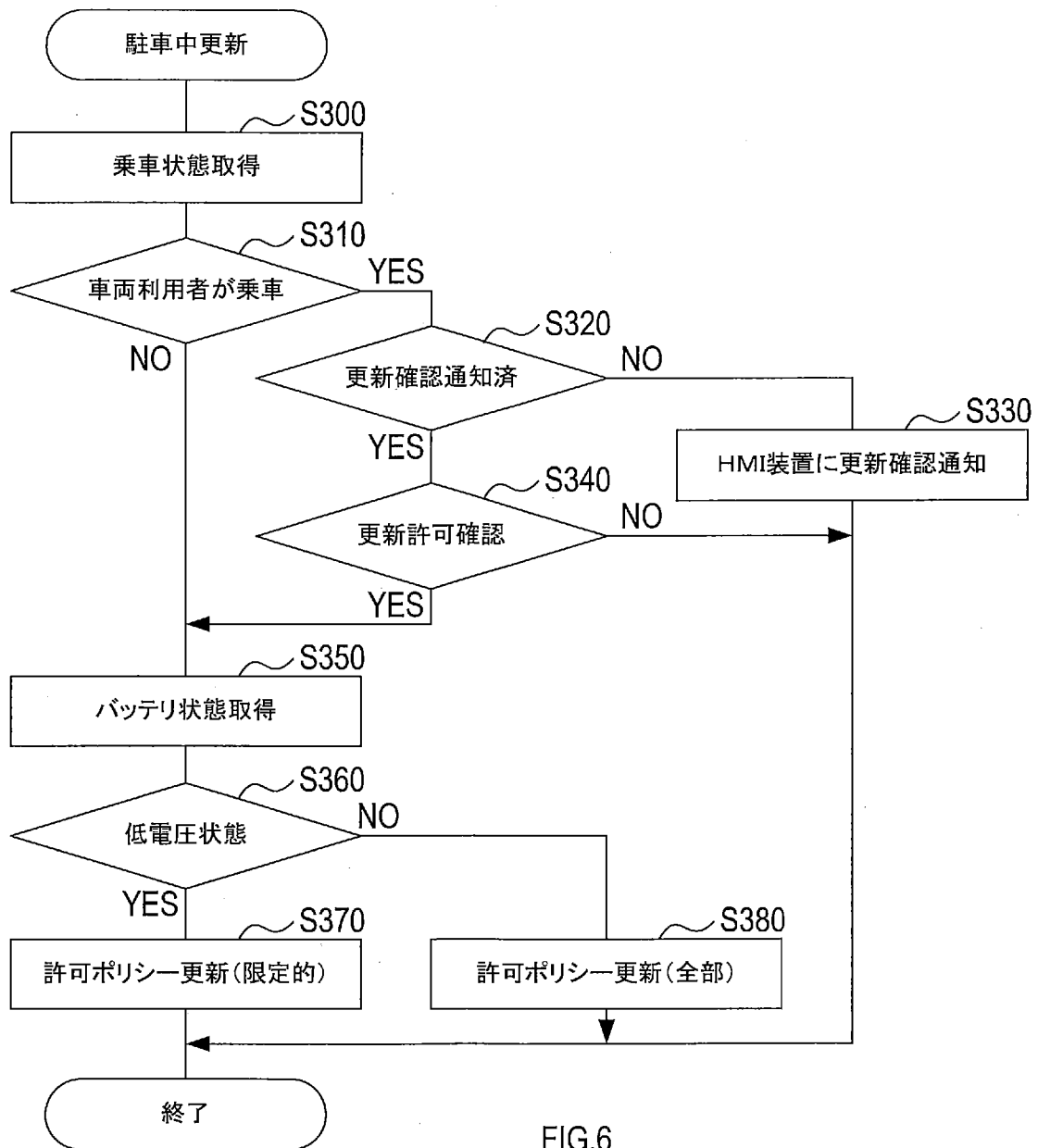


FIG.6

[図7]

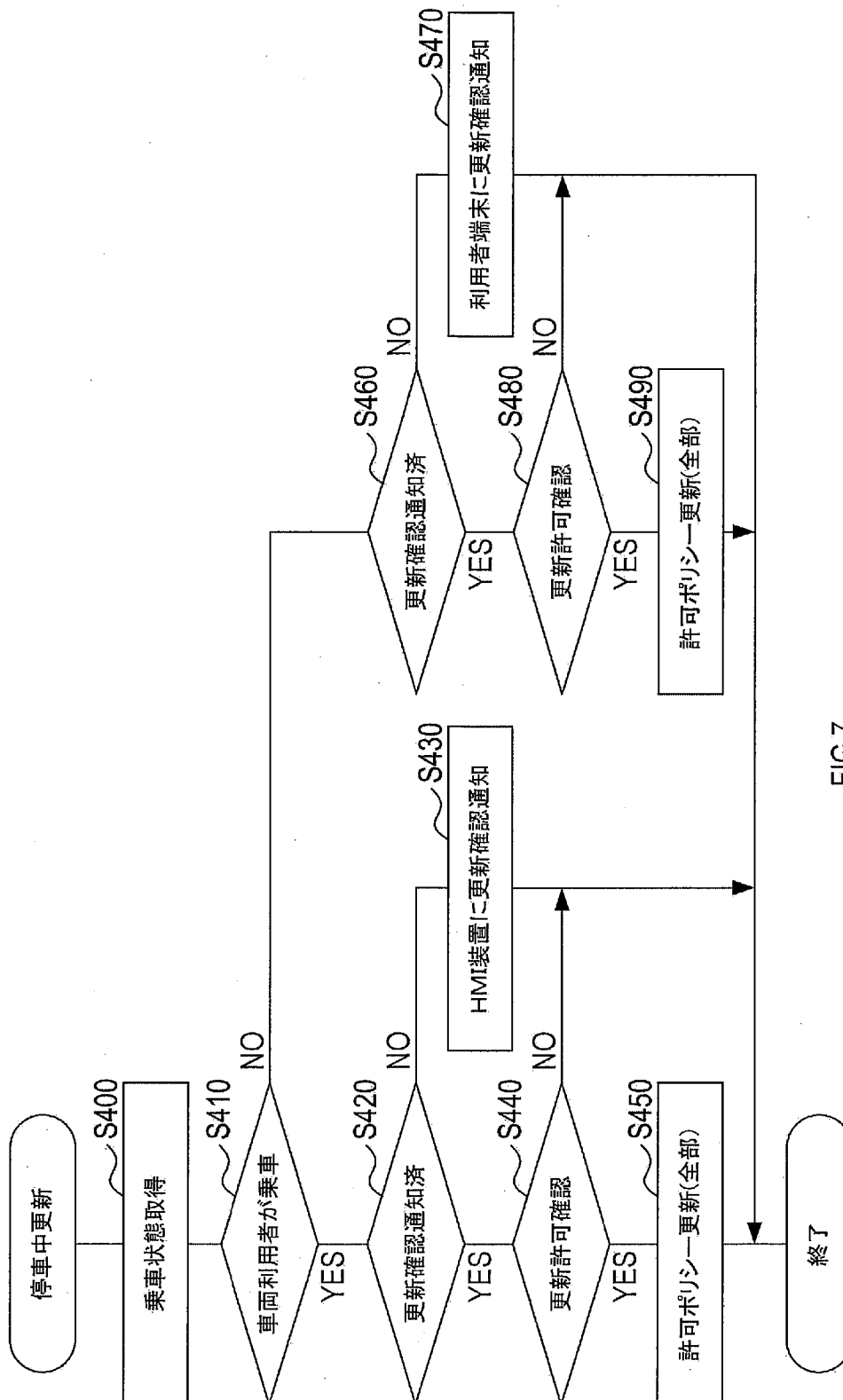


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/021939

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(2013.01)i; **B60R 16/023**(2006.01)i; **H04L 12/28**(2006.01)i
 FI: G06F21/62 318; H04L12/28 100A; B60R16/023 P; H04L12/28 200Z

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)

G06F21/62; B60R16/023; H04L12/28

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 1971-2023
 Registered utility model specifications of Japan 1996-2023
 Published registered utility model applications of Japan 1994-2023

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-193572 A (HITACHI, LTD.) 21 August 2008 (2008-08-21)	1-12
A	WO 2022/069106 A1 (VALEO COMFORT AND DRIVING ASSISTANCE) 07 April 2022 (2022-04-07)	1-12
A	JP 2014-134483 A (CLARION CO., LTD.) 24 July 2014 (2014-07-24)	1-12

☐ 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

27 July 2023

Date of mailing of the international search report

08 August 2023

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/JP2023/021939

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
JP	2008-193572	A	21 August 2008	US	2008/0219274	A1	
				EP	1956794	A2	
				KR	10-2008-0074052	A	
				CN	101242380	A	

WO	2022/069106	A1	07 April 2022	EP	3979584	A1	

JP	2014-134483	A	24 July 2014	US	2014/0200745	A1	
				EP	2755201	A2	
				CN	103921727	A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/62(2013.01)i; B60R 16/023(2006.01)i; H04L 12/28(2006.01)i FI: G06F21/62 318; H04L12/28 100A; B60R16/023 P; H04L12/28 200Z										
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）） G06F21/62; B60R16/023; H04L12/28										
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 - 2023年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2023年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2023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 - 2023年	日本国実用新案登録公報	1996 - 2023年	日本国登録実用新案公報	1994 - 2023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 - 2023年									
日本国実用新案登録公報	1996 - 2023年									
日本国登録実用新案公報	1994 - 2023年									
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）										
C. 関連すると認められる文献										
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号								
A	JP 2008-193572 A（株式会社日立製作所）21.08.2008（2008 - 08 - 21）	1-12								
A	WO 2022/069106 A1（VALEO COMFORT AND DRIVING ASSISTANCE）07.04.2022（2022 - 04 - 07）	1-12								
A	JP 2014-134483 A（クラリオン株式会社）24.07.2014（2014 - 07 - 24）	1-12								
☐ 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。										
<table border="0"> <tr> <td> * 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “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 </td> <td> “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 </td> </tr> </table>			* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “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						
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “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 27.07.2023		国際調査報告の発送日 08.08.2023								
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） 岸野 徹 5S 3983 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/JP2023/021939

引用文献			公表日	パテントファミリー文献			公表日
JP	2008-193572	A	21.08.2008	US	2008/0219274	A1	
				EP	1956794	A2	
				KR	10-2008-0074052	A	
				CN	101242380	A	
WO	2022/069106	A1	07.04.2022	EP	3979584	A1	
JP	2014-134483	A	24.07.2014	US	2014/0200745	A1	
				EP	2755201	A2	
				CN	103921727	A	