

(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5月12日(12.05.2022)



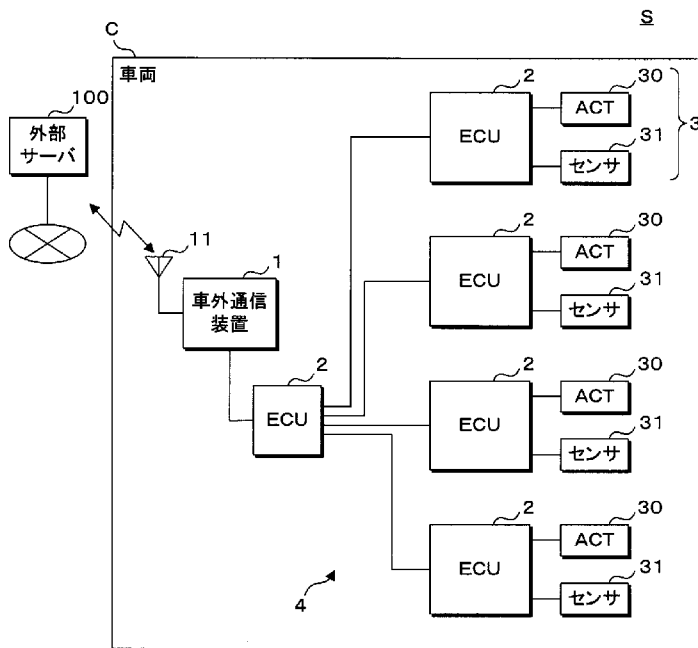
(10) 国際公開番号

WO 2022/097448 A1

- (51) 国際特許分類:
B60R 16/02 (2006.01) *G06F 21/57* (2013.01)
- (21) 国際出願番号: PCT/JP2021/038162
- (22) 国際出願日: 2021年10月15日(15.10.2021)
- (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 2020-184519 2020年11月4日(04.11.2020) JP
- (71) 出願人: 株式会社オートネットワーク技術研究所(AUTONETWORKS TECHNOLOGIES, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町1番14号 Mie (JP). 住友電装株式会社(SUMITOMO WIRING SYSTEMS, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町1番14号 Mie (JP). 住友電気工業株式会社(SUMITOMO ELECTRIC INDUSTRIES, LTD.) [JP/JP]; 〒5410041 大阪府大阪市中央区北浜四丁目5番33号 Osaka (JP).
- (72) 発明者: 相羽 慎一(AIBA, Shinichi); 〒5108503 三重県四日市市西末広町1番14号 株式会社オートネットワーク技術研究所内 Mie (JP).
- (74) 代理人: 河野 英仁, 外(KOHNO, Hideto et al.); 〒5400035 大阪府大阪市中央区釣鐘町二丁目4番3号 河野特許事務所 Osaka (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,

(54) Title: IN-VEHICLE ECU, PROGRAM, AND FAILSAFE METHOD

(54) 発明の名称: 車載ECU、プログラム及びフェールセーフ方法



- 1 External communication device
31 Sensor
100 External server
C Vehicle

(57) Abstract: The present invention provides an in-vehicle ECU installed onboard a vehicle, the in-vehicle ECU comprising a control unit that executes a plurality of applications and a verification unit that verifies each of the plurality of applications when the control unit executes the plurality of applications, wherein the control unit executes an application that has been positively verified by the verification unit, does not execute an application that has been negatively verified by the verification unit, and executes a failsafe process as a substitute for the negative application, and the failsafe process

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))

includes a process for specifying the negative application and outputting a substitute signal corresponding to the specified negative application.

(57) 要約: 車載ECUは、車両に搭載される車載ECUであって、複数のアプリケーションを実行する制御部と、前記制御部が複数のアプリケーションを実行するにあたり、前記複数のアプリケーションそれぞれの検証を行う検証部とを備え、前記制御部は、前記検証部による検証が肯定的なアプリケーションを実行し、前記検証部による検証が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、前記フェールセーフ処理は、前記否定的なアプリケーションを特定し、特定した前記否定的なアプリケーションに応じた代替信号を出力する処理を含む。

明 細 書

発明の名称：車載ECU、プログラム及びフェールセーフ方法 技術分野

[0001] 本開示は、車載ECU、プログラム及びフェールセーフ方法に関する。

本出願は、2020年11月4日出願の日本出願第2020-184519号に基づく優先権を主張し、前記日本出願に記載された全ての記載内容を援用するものである。

背景技術

[0002] 車両には、エンジン制御等のパワー・トレーン系、エアコン制御等のボディ系等の車載機器を制御するためのECU (Electronic Control Unit) が搭載されている。ECUは、MPU等の演算処理部、RAM等の書換可能な不揮発性の記憶部、及び他のECUと通信するための通信部を含み、記憶部に記憶した制御プログラムを読み込んで実行することにより、車載機器の制御を行う。当該制御プログラムを実行するにあたり、ECUの起動時に制御プログラムの完全性を検証し、当該検証に成功した場合にECUの起動（ブート）を許可するセキュアブート方法が、知られている（例えば特許文献1参照）。

[0003] 特許文献1は、制御プログラムの完全性の検証において、失敗回数が規定値を超えた場合は問題のある制御プログラム（ソフトウェア）を起動しないフェールセーフを行う。

先行技術文献

特許文献

[0004] 特許文献1：特開2020-144531号公報

発明の概要

[0005] 本開示の一態様に係る車載ECUは、車両に搭載される車載ECUであって、複数のアプリケーションを実行する制御部と、前記制御部が複数のアプリケーションを実行するにあたり、前記複数のアプリケーションそれぞれの

検証を行う検証部とを備え、前記制御部は、前記検証部による検証が肯定的なアプリケーションを実行し、前記検証部による検証が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、前記フェールセーフ処理は、前記否定的なアプリケーションを特定し、特定した前記否定的なアプリケーションに応じた代替信号を出力する処理を含む。

図面の簡単な説明

[0006] [図1]実施形態1に係る車載ECUを含む車載システムの構成を例示する模式図である。

[図2]車載ECUの物理構成を例示するブロック図である。

[図3]車載ECUの制御部に含まれる機能部を例示する機能ブロック図である。

[図4]代替信号テーブル（パターン情報）を例示する説明図である。

[図5]車載ECUの制御部の処理を例示するフローチャートである。

[図6]実施形態2（仮想環境）に係る車載ECUの論理構成を例示するブロック図である。

[図7]車載ECUの制御部に含まれる機能部を例示する機能ブロック図である。

[図8]動作環境テーブル（動作環境情報）を例示する説明図である。

[図9]車載ECUの制御部の処理を例示するフローチャートである。

発明を実施するための形態

[0007] [本開示が解決しようとする課題]

特許文献1のECUは、セキュアブートの検証結果により起動できなかったアプリケーションの代替を行う点が考慮されていないという問題点がある。

[0008] 本開示の目的は、起動できなかったアプリケーションの代替を行うことができる車載ECU等を提供する。

[0009] [本開示の効果]

本開示の一態様によれば、起動できなかったアプリケーションの代替を行う車載ECU等を提供することができる。

[0010] [本開示の実施形態の説明]

最初に本開示の実施態様を列挙して説明する。また、以下に記載する実施形態の少なくとも一部を任意に組み合わせてもよい。

[0011] (1) 本開示の一態様に係る車載ECUは、車両に搭載される車載ECUであって、複数のアプリケーションを実行する制御部と、前記制御部が複数のアプリケーションを実行するにあたり、前記複数のアプリケーションそれぞれの検証を行う検証部とを備え、前記制御部は、前記検証部による検証が肯定的なアプリケーションを実行し、前記検証部による検証が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、前記フェールセーフ処理は、前記否定的なアプリケーションを特定し、特定した前記否定的なアプリケーションに応じた代替信号を出力する処理を含む。

[0012] 本態様にあたっては、車載ECU (Electronic Control Unit) の制御部は、複数のアプリケーションに対する検証部の検証結果に基づき、複数のアプリケーションそれぞれの実行可否 (起動判定) を行うものであり、当該車載ECUにおいては、セキユアブートが行われるものとなる。当該セキユアブートの一端を担う検証部により否定的な検証結果となったアプリケーションを、制御部は実行しないため、車載ECUにおいて実行されるアプリケーションの適正性 (完全性) を担保することができる。更に、車載ECUの制御部は、否定的なアプリケーションに応じた代替信号を出力する処理を含むフェールセーフ処理を実行することにより、セキユアブートの検証結果により起動できなかったアプリケーションの代替を効率的に行うことができる。

[0013] (2) 本開示の一態様に係る車載ECUは、前記フェールセーフ処理を実行するためのフェールセーフプログラムは、書換不可の記憶領域に記憶されている。

[0014] 本態様にあたっては、車載ECUが備える記憶部において、フェールセー

フ処理を実行するためのフェールセーフプログラムは、書換不可の記憶領域に記憶されているため、例えば、車両内外から当該フェールセーフプログラムへの改竄等の攻撃（アタック）に対する堅牢性を向上させることができる。

[0015] （３）本開示の一態様に係る車載ＥＣＵは、前記書換不可の記憶領域には、前記アプリケーションの組み合わせと、前記代替信号に関する情報とが関連付けられたパターン情報が記憶されており、前記制御部による前記フェールセーフ処理は、前記パターン情報を参照して、特定した前記否定的なアプリケーションに応じた代替信号を出力する処理を含む。

[0016] 本態様にあたっては、車載ＥＣＵの制御部は複数のアプリケーションを実行するところ、検証部の検証結果によって、単一のアプリケーションのみが否定的な検証結果となる場合もあり、又は複数のアプリケーションが否定的な検証結果となる場合もある。これに対し、車載ＥＣＵの記憶領域に記憶されているパターン情報は、当該複数のアプリケーションにおける各アプリケーションの組み合わせと、当該組み合わせに関連付けられた代替信号に関する情報とを含む。当該アプリケーションの組み合わせは、２つ以上のアプリケーションの組み合わせに限定されず、単一のアプリケーションについても含む。従って、車載ＥＣＵの制御部は、特定したアプリケーションが単一の場合のみならず、複数である場合であっても、パターン情報を参照することにより、当該特定した単数又は複数のアプリケーションの組み合わせに応じた代替信号に関する情報を効率的に取得し、当該情報に基づき代替信号を出力することができる。

[0017] （４）本開示の一態様に係る車載ＥＣＵは、前記制御部による代替信号を出力する処理は、実行された肯定的なアプリケーションに対し代替信号を出力する処理を含む。

[0018] 本態様にあたっては、車載ＥＣＵの制御部は実行される複数のアプリケーションは、これらアプリケーション間にて、例えばプロセス間通信を行い協調動作又は依存動作を行う。これに対し、制御部による代替信号を出力する

処理は、当該代替信号を自ECU以外の他の車載ECUに出力する処理のみならず、自ECU（制御部）にて実行されるアプリケーション（検証結果が肯定的なアプリケーション）に対しても代替信号を出力する処理を含む。従って、自ECU（車載ECU）において実行されるべき複数のアプリケーションにおいて、これらアプリケーション間にて動作処理の依存性がある場合であっても、制御部は、実行された肯定的なアプリケーションに対し代替信号を出力する。従って、当該車載ECUにおける複数のアプリケーションに対する全体的又は包括的なフェールセーフ処理を行うことができる。

[0019] （５）本開示の一態様に係る車載ECUは、前記制御部は、仮想化オペレーティングシステムによって複数の仮想環境を生成し、前記複数のアプリケーションそれぞれは、前記複数の仮想環境のうちのいずれかの仮想環境を動作環境とするものであり、前記検証部は、複数の仮想環境それぞれの検証を行い、前記制御部は、前記検証部による検証が肯定的な仮想環境を生成し、前記検証部による検証が否定的な仮想環境は生成せず、該否定的な仮想環境を動作環境とするアプリケーションを代替する前記フェールセーフ処理を実行する。

[0020] 本態様にあたっては、車載ECUの制御部は、仮想化オペレーティングシステムによって複数の仮想環境を生成し、複数のアプリケーションそれぞれは、いずれかの仮想環境の上にて実行される。すなわち、複数のアプリケーションそれぞれは、CPU等の物理的なハードウェア環境にて動作するものでなく、仮想化オペレーティングシステムによって生成された仮想環境を動作環境として、実行される。これにより、単一の車載ECU（自ECU）において、生成した仮想環境と同数の仮想ECUを構成することができる。当該仮想環境は、アプリケーションを実行するためのプラットフォームとなるゲストOSを含むところ、検証部は当該仮想環境（ゲストOS）の検証を行い、制御部は、当該検証結果に基づき、肯定的な仮想環境は生成し、否定的な仮想環境は生成しない。従って、これら仮想環境（ゲストOS）それぞれに対する適正性（完全性）を担保することができる。否定的な仮想環境は生

成されないため、当該否定的な仮想環境を動作環境とするアプリケーションも実行されないものとなるが、これに対し、制御部は、否定的な仮想環境を動作環境とするアプリケーションを代替するフェールセーフ処理を実行する。従って、仮想化オペレーティングシステムによって生成された仮想環境（仮想ECU）を、動作環境としてアプリケーションを実行するように構成された車載ECUにおいても、セキュアブートの検証結果により起動できなかったアプリケーション（生成されなかった仮想環境を動作環境とするアプリケーション）の代替を、効率的に行うことができる。

[0021] （６）本開示の一態様に係る車載ECUは、前記フェールセーフ処理を実行するためのフェールセーフプログラムが記憶される書換不可の記憶領域には、前記仮想環境と、前記仮想環境を動作環境とする一つ以上のアプリケーションとが関連付けられた動作環境情報が記憶されており、前記制御部による前記フェールセーフ処理は、前記動作環境情報を参照して、前記否定的な仮想環境を動作環境とするアプリケーションを特定する処理を含む。

[0022] 本態様にあたっては、車載ECUの制御部は複数の仮想環境を生成し、生成されたそれぞれの仮想環境においては、単一又は複数のアプリケーションが実行されるところ、書換不可の記憶領域には、仮想環境と、仮想環境を動作環境とする一つ以上のアプリケーションとが関連付けられた動作環境情報が記憶されている。従って、車載ECUの制御部は、当該動作環境情報を参照することにより、否定的な検証結果のため生成しなかった仮想環境を動作環境とするアプリケーションを特定し、例えばパターン情報を参照することにより、特定したアプリケーションに応じた代替信号を出力する処理を効率的に行うことができる。

[0023] （７）本開示の一態様に係るプログラムは、車両に搭載され、複数のアプリケーションを実行するコンピュータに、前記複数のアプリケーションそれぞれの検証を行い、前記検証の結果が肯定的なアプリケーションを実行し、前記検証の結果が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、前記フェールセーフ処

理は、前記否定的なアプリケーションを特定し、特定した前記否定的なアプリケーションに応じた代替信号の出力を含む処理を実行させる。

[0024] 本態様にあっては、コンピュータを、起動できなかったアプリケーションの代替を行うことができる車載ECUとして機能させることができる。

[0025] (8) 本開示の一態様に係るフェールセーフ方法は、車両に搭載され、複数のアプリケーションを実行するコンピュータに、前記複数のアプリケーションそれぞれの検証を行い、前記検証の結果が肯定的なアプリケーションを実行し、前記検証の結果が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、前記フェールセーフ処理は、前記否定的なアプリケーションを特定し、特定した前記否定的なアプリケーションに応じた代替信号の出力を含む処理を実行させる。

[0026] 本態様にあっては、コンピュータを、起動できなかったアプリケーションの代替を行うことができる車載ECUとして機能させるフェールセーフ方法を提供することができる。

[0027] [本開示の実施形態の詳細]

本開示をその実施の形態を示す図面に基づいて具体的に説明する。本開示の実施形態に係る車載ECU2を、以下に図面を参照しつつ説明する。なお、本開示はこれらの例示に限定されるものではなく、請求の範囲によって示され、請求の範囲と均等の意味及び範囲内でのすべての変更が含まれることが意図される。

[0028] (実施形態1)

以下、実施の形態について図面に基づいて説明する。図1は、実施形態1に係る車載ECU2を含む車載システムの構成を例示する模式図である。図2は、車載ECU2の物理構成を例示するブロック図である。車載システムSは、車両Cに搭載される複数の車載ECU2及び、当該車載ECU2に接続される車載装置3を含む。

[0029] 複数の車載ECU2は、車両Cの全体を制御する統合的な車載ECU2(統合ECU)、及び当該統合的な車載ECU2と通信可能に接続され、車載

装置3と直接、接続される個別的な車載ECU2（個別ECU）を含むものであってもよい。統合的な車載ECU2は、車外通信装置1を介して、インターネット等の外部ネットワークに接続される外部サーバ100と、通信可能に接続されるものであってもよい。本実施形態において図示においては、統合的な車載ECU2と、複数の個別的な車載ECU2とは、スター状のネットワークトポロジーを形成する車載ネットワーク4によって通信可能に接続され、当該統合的な車載ECU2は、スター状のネットワークトポロジーの中心（センター）に位置して設けられている。更に、隣接する個々の個別的な車載ECU2同士が接続され、ループ状のネットワークトポロジーを構成し、双方向通信を可能として冗長化を図るものであってもよい。

[0030] 複数の個別的な車載ECU2は、車両Cにおける各エリアに配置され、イルミネーションランプ等のアクチュエータ30、及びセンサ等の車載装置3が、シリアルケーブル（じか線）等のワイヤーハーネスにて、直接接続されている。個別的な車載ECU2は、例えば、センサから出力された信号（入力信号）を取得（受信）し、取得した入力信号に基づき生成した要求信号を統合的な車載ECU2に送信する。個別的な車載ECU2は、統合的な車載ECU2から送信された制御信号に基づき、自ECUに直接、接続されたイルミネーションランプ等のアクチュエータ30の駆動制御を行う。個別的な車載ECU2は、当該個別的な車載ECU2に接続される複数の車載装置3間の通信、又は車載装置3と他の車載ECU2との通信を中継するゲートウェイ又はイーサスイッチ等の車載中継装置として機能する中継制御ECUであってよい。個別的な車載ECU2は、通信に関する中継に加え、蓄電装置5から出力された電力を分配及び中継し、自ECUに接続される車載装置3に供給する電力分配装置としても機能するPLB（Power Lan Box）であってよい。

[0031] 統合的な車載ECU2は、個別的な車載ECU2等、他の車載ECU2を介して中継された車載装置3からのデータに基づき、個々の車載装置3への制御信号を生成及び出力するものであり、例えばヴィークルコンピュータ等

の中央制御装置である。統合的な車載ECU2は、個別的な車載ECU2等、他の車載ECU2から出力（送信）される要求信号等の情報又はデータに基づき、当該要求信号の対象となるアクチュエータ30を制御するための制御信号を生成し、生成した制御信号を他の車載ECU2に出力（送信）する。本実施形態においては、統合的な車載ECU2（統合ECU）及び個別的な車載ECU2（個別ECU）により車載システムは構成されたとしたがこれに限定されない。車載システムは、例えばCAN（Controller Area Network）ゲートウェイ又はイーサスイッチ等の中継装置によってピアツーピアに接続された複数の車載ECU2によって構成されるものであってもよい。

[0032] 車載装置3は、例えばLiDAR（Light Detection and Ranging）、ライトセンサ、CMOSカメラ、赤外線センサ等の各種センサ31及び、ドアSW（スイッチ）、ランプSW等のスイッチ、ランプ、ドア開閉装置、モータ装置等のアクチュエータ30を含む。

[0033] 外部サーバ100は、例えばインターネット又は公衆回線網等の車外ネットワークに接続されているサーバ等のコンピュータであり、RAM（Random Access Memory）、ROM（Read Only Memory）又はハードディスク等による記憶部を備える。統合的な車載ECU2（統合ECU）は、車外通信装置1と通信可能に接続され、車外通信装置1を介して車外ネットワークを介して接続された外部サーバ100と通信し、外部サーバ100と、車両Cに搭載される他の車載ECU2又は車載装置3との間の通信を中継するものであってもよい。

[0034] 車外通信装置1は、車外通信部（図示せず）及び、統合的な車載ECU2（統合ECU）と通信するための入出力I/F（図示せず）を含む。車外通信部は、4G、LTE（Long Term Evolution／登録商標）、5G、Wi-Fi等の移動体通信のプロトコルを用いて無線通信をするための通信装置であり、車外通信部に接続されたアンテナ11を介して外部サーバ100とデータの送受信を行う。車外通信装置1と外部サーバ100との通信は、例えば公衆回線網又はインターネット等の外部ネットワークNを介して行われる。入

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

[0035] 車載 E C U 2 (統合 E U C、個別 E C U) は、制御部 2 0、記憶部 2 1、入出力 I / F 2 2、車内通信部 2 3 及び検証部 2 4 を含む。制御部 2 0 は、C P U (Central Processing Unit) 又は M P U (Micro Processing Unit) 等により構成してあり、記憶部 2 1 に予め記憶された制御プログラム及びデータを読み出して実行することにより、種々の制御処理及び演算処理等を行うようにしてある。制御部 2 0 は、C P U 等のソフトウェア処理を行うソフトウェア処理部のみに限定されず、F P G A、A S I C 又は S O C 等のハードウェア処理にて種々の制御処理及び演算処理等を行うハードウェア処理部を含むものであってもよい。

[0036] 記憶部 2 1 は、R A M (Random Access Memory) 等の揮発性のメモリ素子又は、R O M (Read Only Memory)、E E P R O M (Electrically Erasable Programmable ROM) 若しくはフラッシュメモリ等の不揮発性のメモリ素子、又は、これら記憶デバイスの組み合わせにより構成してあり、制御プログラム及び処理時に参照するデータが予め記憶してある。当該制御プログラムは、例えば、各種の車載装置 3 を制御するためのアプリケーション、又は L i D A R 又は C M O S カメラからの出力データに基づき自動化運転を行うための物標認識を行うアプリケーション等の複数のアプリケーションを含む。これら複数のアプリケーションは、記憶部 2 1 に含まれ、R A M 等により構成される書込み可能な記憶領域に記憶されているものであってもよい。記憶部 2 1 は、R O M 等により構成される書込み不可な記憶領域を含み、当該書込み不可な記憶領域には、後述するフェールセーフプログラム、代替信号テーブ

ル 2 1 1 等のフェールセーフ処理に必要なプログラム及びデータが記憶されている。

[0037] 入出力 I / F 2 2 は、車外通信装置 1 の入出力 I / F 2 2 と同様に、例えばシリアル通信するための通信インターフェイスである。入出力 I / F 2 2 及びシリアルケーブル等のワイヤーハーネスを介して、車載 ECU 2 は、車外通信装置 1 と通信可能に接続される。

[0038] 車内通信部 2 3 は、例えば CAN (Controller Area Network) 又はイーサネット (Ethernet/登録商標) の通信プロトコルを用いた入出力インターフェイスであり、制御部 2 0 は、車内通信部 2 3 を介して車載ネットワーク 4 に接続されている他の車載 ECU 2 と相互に通信する。

[0039] 検証部 2 4 は、例えば HSM (Hardware Security Module) であり、CPU 等で構成される制御部 2 0 とは別デバイス又は別モジュールとして構成されている。HSM にて構成される検証部 2 4 は、車載 ECU 2 (自 ECU) が起動 (ブート) される際に行われるセキュアブート処理の一端を担うものであり、記憶部 2 1 に記憶されている複数のアプリケーション等、車載 ECU 2 の起動において実行されるソフトウェアの適正性 (完全性) 又は健全性を検証する機能モジュールである。検証部 2 4 は、例えば、暗号処理用のプロセッサを含み、例えば CMAC (Cipher-based Message Authentication Code) 等の暗号アルゴリズムを用いて、検証対象となるアプリケーション等のソフトウェアの適正性 (完全性) を検証する。検証部 2 4 は、車載 ECU 2 の起動時に行われるセキュアブート処理 (セキュアブートシーケンス) において、検証対象となる複数のアプリケーションそれぞれの適正性 (完全性) を検証し、アプリケーションそれぞれに対する検証結果を出力する。当該検証結果は、アプリケーションが正当である旨を示す肯定的検証結果、又はアプリケーションが例えば改竄等され不正である旨を示す否定的検証結果を含む。

[0040] 図 3 は、車載 ECU 2 の制御部 2 0 に含まれる機能部を例示する機能ブロック図である。車載 ECU 2 の制御部 2 0 は、記憶部 2 1 に記憶されている

制御プログラムを実行することにより、取得部 201、アプリ起動判定部 202、フェールセーフ部 203、及び出力部 204 として機能し、これら機能部が連関することにより、フェールセーフ処理が行われる。すなわち、制御部 20 は、セキュアブート処理（セキュアブートシーケンス）にてアプリケーションの検証を行う検証部 24 と協働することにより、当該フェールセーフ処理を行うものとなる。

[0041] フェールセーフ処理を制御部 20 に実行させるためのフェールセーフプログラムは、記憶部 21 における（含まれる）書換不可の記憶領域に記憶されているものであってもよい。書換不可の記憶領域にフェールセーフプログラムを記憶することにより、例えば、車両 C 内外から当該フェールセーフプログラムへの改竄等の攻撃（アタック）に対する堅牢性を向上させることができる。

[0042] フェールセーフ処理を行う車載 ECU 2 の制御部 20（各機能部）は、検証部 24 から取得した検証結果に基づき、適正性（完全性）が検証されたアプリケーションを実行する。制御部 20（は、検証適正性（完全性）が検証されなかったアプリケーションについては実行することなく、当該実行しなかったアプリケーションを代替するための代替信号（フェールセーフ値）を出力する。

[0043] 取得部 201 は、セキュアブート処理の一環として行われた検証部 24 による検証の結果（検証結果）を、当該検証部 24 から取得する。検証部 24 から出力される検証結果には、アプリケーションそれぞれに対する検証結果が肯定的な結果であるか、又は否定的な結果であるかが、含まれている。肯定的な結果である場合、当該肯定的なアプリケーションに対する改竄等の不正処理は行われおらず、当該アプリケーションの適正性（完全性）が保証されるものとなる。否定的な結果である場合、当該否定的なアプリケーションに対し改竄等の不正処理が行われた蓋然性があり、当該アプリケーションの適正性（完全性）が否定されるものとなる。取得部 201 は、取得した検証結果を、アプリ起動判定部 202 及びフェールセーフ部 203 に出力する。

[0044] アプリ起動判定部202は、検証結果に基づき、個々のアプリケーションの実行（起動）の可否を判定し、実行が可能（肯定的な検証結果）であるアプリケーションを実行する。当該アプリケーションを実行することにより、アプリケーションに対応したプロセス又はスレッドが生成される。アプリ起動判定部202は、肯定的なアプリケーションは実行（起動）し、否定的なアプリケーションは実行（起動）しない。実行されるアプリケーションの適正性（完全性）は保証されているため、複数のアプリケーションが実行される車載ECU2において、当該車載ECU2の健全性を担保することができる。

[0045] フェールセーフ部203は、検証結果に基づき、検証結果が否定的なアプリケーションを特定する。検証部24から出力される検証結果には、複数のアプリケーションそれぞれに対する肯定的検証結果又は否定的検証結果が含まれている。又は、当該検証結果には、肯定的な検証結果のアプリケーションに関する情報のみが含まれる場合であっても、フェールセーフ部203は、記憶部21に記憶されている複数のアプリケーションとの対比（差分）を行うことにより、否定的な検証結果のアプリケーションを特定することができる。否定的なアプリケーションの特定においては、否定的なアプリケーションが皆無な場合、否定的なアプリケーションが一つである場合、又は否定的なアプリケーションが複数である場合に大別される。これら各場合において、当該否定的なアプリケーションの組み合わせが、特定されるものとなる。すなわち、当該否定的なアプリケーションの組み合わせは、2つ以上のアプリケーションの組み合わせに限定されず、単一のアプリケーション、又は否定的なアプリケーションが無い旨についても、含まれる。

[0046] フェールセーフ部203は、特定した否定的なアプリケーションの組み合わせに基づき、例えば、記憶部21に記憶されているパターン情報を参照し、実行しなかった当該否定的なアプリケーションを代替するための代替信号（フェールセーフ値）を生成する。パターン情報は、例えばテーブル形式のデータ（代替信号テーブル211）として、フェールセーフプログラムと同

様に記憶部 21 に含まれる書換不可の記憶領域に記憶されているものであってもよい。

[0047] 図 4 は、代替信号テーブル 211（パターン情報）を例示する説明図である。代替信号テーブル 211 は、管理項目として、車載 ECU 2 の制御部 20 が実行するアプリケーションそれぞれの名称の項目、及び代替信号のバターンの項目を含む。車載 ECU 2 の制御部 20 が実行するアプリケーションそれぞれの名称の項目に対し、個々のアプリケーションが、肯定的な検証結果（○にて図示）であるか、否定的な検証結果（×にて図示）であるかを示す値が格納される。代替信号テーブル 211 には、全アプリケーションが肯定的（○）又は否定的（×）である場合における、全ての組み合わせパターン（全網羅パターン）が含まれている。当該個々の組み合わせが、検証結果が否定的なアプリケーションの組み合わせそれぞれに相当する。当該組み合わせは、2 つ以上のアプリケーションの組み合わせに限定されず、単一のアプリケーションについても含む。

[0048] 代替信号のバターンの項目には、当該組み合わせ（否定的なアプリケーションの組み合わせ）に対応する代替信号パターンが、格納されている。代替信号パターンは、例えば、予め定義されている値（フェールセーフ値）によって、示されるものであってもよい。

[0049] フェールセーフ部 203 は、検証結果に基づき特定した否定的なアプリケーションに基づき当該否定的なアプリケーションを特定し、パターン情報（代替信号テーブル 211）を参照することにより、特定したアプリケーションの組み合わせに応じた代替信号パターン（フェールセーフ値）を導出（抽出）する。

[0050] フェールセーフ部 203 は、導出した代替信号パターン（フェールセーフ値）に基づき、代替信号を生成し、出力部 204 に出力する。フェールセーフ部 203 は、代替信号パターン（フェールセーフ値）に基づき代替信号を生成するにあたり、代替対象となるアプリケーションが正常動作していた際に出したデータに基づき、当該代替信号を生成するものであってもよい。

又は、代替対象となるアプリケーションの機能仕様等に基づき予め定められた信号を、代替信号として生成するものであってもよい。又は、フェールセーフ部203は、導出した代替信号パターン（フェールセーフ値）を、車外通信装置1を介して外部サーバ100に送信し、当該代替信号パターン（フェールセーフ値）に基づき外部サーバ100が生成した代替信号を取得することにより、当該代替信号として生成するものであってもよい。

[0051] 出力部204は、フェールセーフ部203が生成した代替信号を、車内通信部23を介して他の車載ECU2に出力する。又は、出力部204は、フェールセーフ部203が生成した代替信号を、自ECUにて実行されたアプリケーション（実行中のアプリケーション）に対し、例えばプロセス間通信を行うことにより、当該アプリケーションのプロセスに出力（送信）するものであってもよい。

[0052] 出力部204から出力（送信）された代替信号を取得（受信）した他の車載ECU2、又は自ECUにて実行中のアプリケーションは、当該代替信号に基づき、所定の処理を行う。これにより、セキュアブートの検証結果により起動できなかったアプリケーションの代替を効率的に行うことができる。当該所定の処理は、例えば、機能を一部限定した縮退運転を行う処理、又は車両Cを適切に停止状態に遷移させる処理を含むものであってもよい。

[0053] 本実施形態において、取得部201、アプリ起動判定部202フェールセーフ部203、及び出力部204は、車載ECU2の制御部20における機能部として説明したが、これに限定されない。これら機能部における一部の機能部、又は単一の機能部における処理の一部は、車載ECU2と通信可能に接続される外部サーバ100等のクラウドサーバ、又は、制御部20とは別体で構成される検証部24が担うものであってもよい。制御部20は、これら外部サーバ100又は検証部24と協働して、当該機能部による一連の処理を行うものであってもよい。

[0054] 図5は、車載ECU2の制御部20の処理を例示するフローチャートである。車載ECU2の制御部20は、例えば、車両Cが停止状態（IGスイッ

チがオフ)から起動状態(IGスイッチがオン)に状態遷移するにあたり、車載ECU2(自ECU)が起動(ブート)される際に行われるセキュアブート処理(セキュアブートシーケンス)に基づき、以下の処理を行う。

[0055] セキュアブート処理において最初に行われるのは、検証部24によるアプリケーションそれぞれに対する検証である。当該検証部24は、例えばHSM(Hardware Security Module)であり、CPU等で構成される制御部20とは別デバイス又は別モジュールとして構成されている。車載ECU2の制御部20による一連の処理は、検証部24によるアプリケーションそれぞれに対する検証の処理後に行われる。

[0056] 車載ECU2の制御部20は、検証部24から検証結果を取得する(S101)。検証部24から出力される検証結果には、アプリケーションそれぞれに対する検証結果が肯定的な結果であるか、又は否定的な結果であるかが、含まれている。肯定的な結果である場合、肯定的なアプリケーションに対する改竄等の不正処理は行われおらず、当該アプリケーションの適正性(完全性)が保証されるものとなる。否定的な結果である場合、否定的なアプリケーションに対し改竄等の不正処理が行われた蓋然性があり、当該アプリケーションの適正性(完全性)が否定されるものとなる。車載ECU2の制御部20は、検証結果を参照することにより、各アプリケーションの検証結果が肯定的であるか否定的であるかを把握することができる。

[0057] 車載ECU2の制御部20は、取得した検証結果に基づき、肯定的な検証結果のアプリケーションを実行(起動)する(S102)。車載ECU2の制御部20は、検証結果に基づき、肯定的な検証結果のアプリケーションを実行可能なアプリケーションとして特定(判定)し、当該アプリケーションを実行する。アプリケーションを実行することにより、当該アプリケーションに対応したプロセス又はスレッドが生成される。

[0058] 車載ECU2の制御部20は、取得した検証結果に基づき、否定的な検証結果のアプリケーションを特定する(S103)。車載ECU2の制御部20は、取得した検証結果に基づき、否定的な検証結果のアプリケーションを実

行不可なアプリケーションとして特定（判定）し、当該アプリケーションは実行しない。

[0059] 車載ＥＣＵ２の制御部２０は、否定的な検証結果のアプリケーションに対応する代替信号を生成する（Ｓ１０４）。車載ＥＣＵ２の制御部２０は、例えば、記憶部２１に記憶されている代替信号テーブル２１１を参照して、特定したアプリケーションの組み合わせに対応する代替信号パターン（フェールセーフ値）を導出する。車載ＥＣＵ２の制御部２０は、導出した代替信号パターン（フェールセーフ値）に基づき、代替信号を生成する。

[0060] 車載ＥＣＵ２の制御部２０は、生成した代替信号を出力する（Ｓ１０５）。車載ＥＣＵ２の制御部２０は、生成した代替信号を、他の車載ＥＣＵ２、又は自ＥＣＵにて実行中のアプリケーションに出力（送信）する。代替信号を取得（受信）した他の車載ＥＣＵ２、又は自ＥＣＵにて実行中のアプリケーションは、当該代替信号に基づき、縮退運転を行う処理、又は車両Ｃを適切に停止状態に遷移させる処理等、所定の処理を行うものであってもよい。

[0061] 本実施形態によれば、セキュアブートの一端を担う検証部２４により否定的な検証結果となったアプリケーションは、車載ＥＣＵ２の制御部２０によって実行（起動）されないため、車載ＥＣＵ２としての健全性を担保することができる。更に、車載ＥＣＵ２の制御部２０は、否定的なアプリケーションに応じた代替信号を出力する処理を含むフェールセーフ処理を実行することにより、セキュアブートの検証結果により実行（起動）できなかったアプリケーションがある場合であっても、当該実行されなかったアプリケーションの代替を効率的に行うことができる。

[0062] （実施形態２）

図６は、実施形態２（仮想環境）に係る車載ＥＣＵ２の論理構成を例示するブロック図である。実施形態２の車載ＥＣＵ２は、アプリケーションを仮想環境上で実行する点で、実施形態１と異なる。実施形態２の車載ＥＣＵ２は、実施形態１の車載ＥＣＵ２と同様に、制御部２０、記憶部２１、入出力Ｉ／Ｆ２２、車内通信部２３及び検証部２４を含む。すなわち、実施形態１

の車載ECU2と実施形態2の車載ECU2のハードウェア構成は、同様の構成である。本実施形態における図示にて、実施形態2の車載ECU2の論理構成を例示するものであり、制御部20等によるハードウェア層（物理基盤）を最下層とし、仮想環境にて実行されるアプリケーション、フェールセーフプログラム、及び仮想環境管理プログラム等によるソフトウェア層を最上層とした階層構造を例示するブロック図である。

[0063] 車載ECU2の記憶部21には、例えば、Hypervisor又はVMware等の仮想オペレーティングシステムが記憶されており、車載ECU2の制御部20は、仮想オペレーティングシステムを用いて起動することにより、仮想オペレーティングシステム上にて複数の仮想環境を構築することができる。仮想化の方式は、本実施形態の図示のように仮想オペレーティングシステムによって直接的に制御部20等のハードウェアリソースにアクセスするハイパーバイザー方式、又は仮想オペレーティングシステムとハードウェアリソースとの間にLinux（登録商標）等のオペレーティングシステムが介在するホストOS方式であってもよい。

[0064] 仮想オペレーティングシステムを用いて起動した車載ECU2は、仮想オペレーティングシステムの機能により、複数の仮想環境を構築ことができ、複数の仮想環境には、車載ECU2が備える制御部20等のハードウェアリソースが割り当てられる。これらハードウェアリソースが割り当てられた仮想環境夫々は、仮想的な制御部20（仮想制御部）、記憶部21（仮想記憶部）及び車内通信部23（仮想車内通信部）を備えるものとなり、仮想ECU2051として機能する。制御部20とは別個のデバイである検証部24は、仮想オペレーティングシステムによる仮想化の対象外となり、当該検証部24は、いずれかの仮想ECU2051、又は個々の仮想ECU2051と通信するものとなる。

[0065] 仮想ECU2051夫々の仮想記憶部夫々には、例えばUbuntu（登録商標）等のゲストOS（Operation System）が記憶され、仮想ECU2051夫々はゲストOSを起動し、当該ゲストOSの上でアプリケーションを

実行する。当該ゲストOSは、個々の仮想ECU2051に応じて、異なる種類のOSであってもよい。上述のごとく仮想記憶部の実体は、仮想ECU2051夫々割り当てられた記憶部21の記憶領域であるため、ゲストOSも仮想オペレーティングシステムと同様に記憶部21に記憶されていることは、言うまでもない。

[0066] 仮想オペレーティングシステムを用いて起動した車載ECU2の制御部20は、構築したいずれかの仮想環境（仮想ECU2051）のうちの一つの仮想ECU2051にて、全ての仮想環境を管理するプログラム（仮想環境管理プログラム）を実行する。すなわち、仮想環境管理プログラムを実行する仮想ECU2051は、仮想オペレーティングシステムのコントロールパネルとして機能する。フェールセーフ処理を実行させるためのフェールセーフプログラムは、当該コントロールパネルとして機能する仮想ECU2051（仮想環境）にて実行されるものであってもよい。当該フェールセーフプログラムを実行する仮想ECU2051は、検証部24と通信し、セキュアブート処理にて検証部24が行った検証結果を、当該検証部24より取得する。

[0067] 図7は、車載ECU2の制御部20に含まれる機能部を例示する機能ブロック図である。車載ECU2の制御部20は、記憶部21に記憶されている制御プログラムを実行することにより、実施形態1と同様に取得部201、アプリ起動判定部202、フェールセーフ部203、及び出力部204として機能し、更に仮想環境生成判定部205として機能し、フェールセーフ処理を行う。本実施形態における図示において、フェールセーフ処理を行うためのフェールセーフプログラムは、例えば、仮想オペレーティングシステムのコントロールパネルとして機能する仮想ECU2051（仮想環境）の制御部20（仮想制御部）、記憶部21（仮想記憶部）及び車内通信部23（仮想車内通信部）を用いて、実行されるものとなる。すなわち、本実施形態において図示される取得部201等の各機能部は、仮想ECU2051（仮想環境）の制御部20（仮想制御部）がフェールセーフプログラムを実行す

ることにより、構成されるものとなる。

[0068] 実施形態2の検証部24は、実施形態1の検証部24と同様にアプリケーションそれぞれに対する検証を行うと共に、仮想環境それぞれを生成するにあたり起動されるゲストOSそれぞれに対する検証を行い、当該検証の結果（検証結果）を取得部201に出力する。従って、当該検証結果には、アプリケーションそれぞれの検証結果（肯定的又は否定的）、及びゲストOSそれぞれの検証結果（肯定的又は否定的）が、含まれる。

[0069] 取得部201は、検証部24から取得した検証結果を、仮想環境生成判定部205、アプリ起動判定部202、及びフェールセーフ部203に出力する。

[0070] 仮想環境生成判定部205は、検証結果に基づき、肯定的な検証結果のゲストOSは起動して当該肯定的なゲストOSによる仮想環境を生成し、否定的な検証結果のゲストOSは起動せず当該否定的なゲストOSによる仮想環境を生成しない。従って、これら仮想環境（ゲストOS）それぞれに対する適正性（完全性）を担保することができる。

[0071] アプリ起動判定部202は、検証結果に基づき、肯定的な検証結果のゲストOSによる仮想環境を動作環境とし、かつ肯定的な検証結果のアプリケーションを実行（起動）する。否定的な仮想環境は生成されないため、当該否定的な仮想環境を動作環境とするアプリケーションも実行されないものとなる。すなわち、アプリケーション自体の検証結果は肯定的であっても、当該アプリケーションの動作環境となる仮想環境のゲストOSが否定的な検証結果である場合は、当該肯定的アプリケーションは、実行されないものとなる。

[0072] アプリ起動判定部202は、当該否定的な仮想環境を動作環境とするアプリケーションを特定するにあたり、仮想環境（ゲストOS）と、仮想環境を動作環境とする一つ以上のアプリケーションとが関連付けられた動作環境情報を参照して、当該アプリケーションを特定するものであってもよい。当該動作環境情報は、例えばテーブル形式のデータ（動作環境テーブル212）

として、代替信号テーブル 2 1 1 と同様に記憶部 2 1 に含まれる書換不可の記憶領域に記憶されているものであってもよい。

[0073] 図 8 は、動作環境テーブル 2 1 2（動作環境情報）を例示する説明図である。動作環境テーブル 2 1 2 は、管理項目として、アプリケーション名称の項目、及び仮想環境（ゲスト OS）を含む。アプリケーション名称の項目には、車載 ECU 2 にて実行される複数のアプリケーションの名称が格納される。仮想環境（ゲスト OS）の項目には、対応するアプリケーション（同じレコードに格納されるアプリケーション）の動作環境となる仮想環境（ゲスト OS）の名称が格納される。

[0074] アプリ起動判定部 2 0 2 は、動作環境テーブル 2 1 2 を参照することにより、仮想環境（ゲスト OS）と、当該仮想環境を動作環境とするアプリケーションとの関連性を取得することができる。アプリ起動判定部 2 0 2 は、検証結果に基づき、肯定的な検証結果のゲスト OS を特定し、動作環境テーブル 2 1 2 を参照することにより、当該特定したゲスト OS の仮想環境を動作環境とするアプリケーションを特定する。特定されたアプリケーションにおいて、更に肯定的な検証結果のアプリケーションを、実行可能なアプリケーションとして特定する。アプリ起動判定部 2 0 2 は、特定した実行可能なアプリケーションを、これらアプリケーションの動作環境となる仮想環境（ゲスト OS）にて実行する。

[0075] フェールセーフ部 2 0 3 は、実行不可なアプリケーションを特定し、当該特定した実行不可なアプリケーションに対応する代替信号を生成する。フェールセーフ部 2 0 3 は、検証結果に基づき否定的な検証結果のゲスト OS を特定し、動作環境テーブル 2 1 2 を参照することにより、当該否定的な検証結果のゲスト OS の仮想環境を動作環境とするアプリケーションを特定する。フェールセーフ部 2 0 3 は、特定したアプリケーション（否定的なゲスト OS の仮想環境を動作環境とするアプリケーション）と、検証結果に含まれる否定的な検証結果のアプリケーションに基づき、実施形態 1 と同様に実行不可なアプリケーションの組み合わせを特定する。

- [0076] フェールセーフ部203は、実施形態1と同様に代替信号テーブル211を参照して、実行不可なアプリケーションの組み合わせに対応する代替信号パターン（フェールセーフ値）を導出する。フェールセーフ部203は、実施形態1と同様に導出した代替信号パターン（フェールセーフ値）に基づき、代替信号を生成し、出力部204に出力する。
- [0077] 出力部204は、実施形態1と同様にフェールセーフ部203が生成した代替信号を、他の車載ECU2、又は自ECUにて実行中のアプリケーションに出力（送信）する。
- [0078] 図9は、車載ECU2の制御部20の処理を例示するフローチャートである。車載ECU2の制御部20は、例えば、車両Cが停止状態（IGスイッチがオフ）から起動状態（IGスイッチがオン）に状態遷移するにあたり、車載ECU2（自ECU）が起動（ブート）される際に行われるセキュアブート処理（セキュアブートシーケンス）に基づき、以下の処理を行う。当該処理（フェールセーフ処理）を実行させるためのフェールセーフプログラムが、仮想オペレーティングシステムのコントロールパネルとして機能する仮想ECU2051（仮想環境）にて実行される場合、制御部20は、当該仮想ECU2051の制御部20（仮想制御部）に相当する。
- [0079] 実施形態2の検証部24は、アプリケーションのみならず、仮想環境を生成するにあたり起動されるゲストOSについても検証する。車載ECU2の制御部20による一連の処理は、検証部24によるゲストOS及びアプリケーションそれぞれに対する検証の処理後に行われる。
- [0080] 車載ECU2の制御部20は、検証部24から検証結果を取得する（S201）。車載ECU2の制御部20は、実施形態1のS101と同様にS201の処理を行う。検証部24から出力される検証結果は、アプリケーションそれぞれの検証結果（肯定的又は否定的）、及びゲストOSそれぞれの検証結果（肯定的又は否定的）が含まれており、車載ECU2の制御部20は、アプリケーション及びゲストOSの検証結果を取得することができる。
- [0081] 車載ECU2の制御部20は、取得した検証結果に基づき、肯定的な検証

結果のゲストOSを起動して仮想環境を生成する（S202）。車載ECU2の制御部20は、検証結果に基づき、肯定的な検証結果のゲストOSは起動し、当該肯定的なゲストOSによる仮想環境を生成する。車載ECU2の制御部20は、否定的な検証結果のゲストOSは起動せず、当該否定的なゲストOSによる仮想環境を生成しない。

[0082] 車載ECU2の制御部20は、取得した検証結果に基づき、肯定的な検証結果のゲストOSによる仮想環境を動作環境とし、肯定的な検証結果のアプリケーションを実行（起動）する（S203）。車載ECU2の制御部20は、検証結果に基づき肯定的な検証結果のゲストOSを特定し、動作環境テーブル212を参照することにより、当該特定したゲストOSの仮想環境を動作環境とするアプリケーションを特定する。制御部20は、更に、特定されたアプリケーションにおいて肯定的な検証結果のアプリケーションを、実行可能なアプリケーションとして特定する。すなわち、肯定的な検証結果のゲストOSによる仮想環境を動作環境とするアプリケーションであって、更に肯定的な検証結果のアプリケーションが、実行可能なアプリケーションとして特定される。車載ECU2の制御部20は、当該特定したアプリケーションを、対応するそれぞれの仮想環境にて実行させる。

[0083] 車載ECU2の制御部20は、取得した検証結果に基づき、否定的な検証結果のゲストOSを特定する（S204）。検証結果には、ゲストOSそれぞれの検証結果が含まれており、車載ECU2の制御部20は、取得した検証結果に基づき否定的な検証結果のゲストOSを特定する。

[0084] 車載ECU2の制御部20は、取得した検証結果及び特定した否定的な検証結果のゲストOSに基づき、実行不可なアプリケーションを特定する（S205）。実行不可なアプリケーションは、否定的な検証結果のゲストOSによる仮想環境を動作環境とするアプリケーション、及び否定的な検証結果のアプリケーションである。車載ECU2の制御部20は、例えば、記憶部21に記憶されている動作環境テーブル212を参照し、否定的な検証結果のゲストOSによる仮想環境を動作環境とする単一又は複数のアプリケーシ

ョンを特定する。車載ECU2の制御部20は、動作環境テーブル212を参照して特定したアプリケーション（否定的な検証結果のゲストOSによる仮想環境を動作環境とするアプリケーション）、及び検証結果に含まれる否定的な検証結果のアプリケーションに基づき、実施形態1と同様に実行不可なアプリケーションの組み合わせを特定する。

[0085] 車載ECU2の制御部20は、実行不可なアプリケーションに対応する代替信号を生成する（S206）。車載ECU2の制御部20は、実施形態1の処理S104と同様に代替信号テーブル211を参照して、実行不可なアプリケーションの組み合わせに対応する代替信号パターン（フェールセーフ値）を導出する。

[0086] 車載ECU2の制御部20は、生成した代替信号を出力する（S207）。車載ECU2の制御部20は、実施形態1の処理S105と同様に生成した代替信号を、他の車載ECU2、又は自ECUにて実行中のアプリケーションに出力（送信）する。

[0087] 本実施形態においては、否定的な検証結果となった仮想OSによる仮想環境は生成されないため、当該否定的な仮想環境を動作環境とするアプリケーションも実行されないものとなる。これに対し、制御部20は、否定的な仮想環境を動作環境とするアプリケーションを代替する代替信号を生成及び出力するフェールセーフ処理を実行する。従って、仮想化オペレーティングシステムによって生成された仮想環境（仮想ECU2051）を、動作環境としてアプリケーションを実行するように構成された車載ECU2においても、セキュアブートの検証結果により起動できなかったアプリケーション（生成されなかった仮想環境を動作環境とするアプリケーション）の代替を、効率的に行うことができる。

[0088] 今回開示された実施形態はすべての点で例示であって、制限的なものではないと考えられるべきである。本発明の範囲は、上記した意味ではなく、請求の範囲によって示され、請求の範囲と均等の意味及び範囲内でのすべての変更が含まれることが意図される。

符号の説明

- [0089] C 車両
- S 車載システム
- 1 0 0 外部サーバ
- 1 車外通信装置
- 1 1 アンテナ
- 2 車載 E C U
- 2 0 制御部
- 2 0 1 取得部
- 2 0 2 アプリ起動判定部
- 2 0 3 フェールセーフ部
- 2 0 4 出力部
- 2 0 5 仮想環境生成判定部
- 2 0 5 1 仮想 E C U
- 2 1 記憶部
- 2 1 1 代替信号テーブル
- 2 1 2 動作環境テーブル
- 2 2 入出力 I / F
- 2 3 車内通信部
- 2 4 検証部
- 3 車載装置
- 3 0 アクチュエータ (A C T)
- 3 1 センサ
- 4 車載ネットワーク

請求の範囲

- [請求項1] 車両に搭載される車載ECUであって、
 複数のアプリケーションを実行する制御部と、
 前記制御部が複数のアプリケーションを実行するにあたり、前記複数のアプリケーションそれぞれの検証を行う検証部とを備え、
 前記制御部は、
 前記検証部による検証が肯定的なアプリケーションを実行し、
 前記検証部による検証が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、
 、
 前記フェールセーフ処理は、
 前記否定的なアプリケーションを特定し、
 特定した前記否定的なアプリケーションに応じた代替信号を出力する処理を含む
 車載ECU。
- [請求項2] 前記フェールセーフ処理を実行するためのフェールセーフプログラムは、書換不可の記憶領域に記憶されている
 請求項1に記載の車載ECU。
- [請求項3] 前記書換不可の記憶領域には、前記アプリケーションの組み合わせと、前記代替信号に関する情報とが関連付けられたパターン情報が記憶されており、
 前記制御部による前記フェールセーフ処理は、前記パターン情報を参照して、特定した前記否定的なアプリケーションに応じた代替信号を出力する処理を含む
 請求項2に記載の車載ECU。
- [請求項4] 前記制御部による代替信号を出力する処理は、実行された肯定的なアプリケーションに対し代替信号を出力する処理を含む
 請求項1から請求項3のいずれか1項に記載の車載ECU。

- [請求項5] 前記制御部は、仮想化オペレーティングシステムによって複数の仮想環境を生成し、
- 前記複数のアプリケーションそれぞれは、前記複数の仮想環境のうちのいずれかの仮想環境を動作環境とするものであり、
- 前記検証部は、複数の仮想環境それぞれの検証を行い、
- 前記制御部は、
- 前記検証部による検証が肯定的な仮想環境を生成し、
- 前記検証部による検証が否定的な仮想環境は生成せず、該否定的な仮想環境を動作環境とするアプリケーションを代替する前記フェールセーフ処理を実行する
- 請求項1から請求項4のいずれか1項に記載の車載ECU。
- [請求項6] 前記フェールセーフ処理を実行するためのフェールセーフプログラムが記憶される書換不可の記憶領域には、前記仮想環境と、前記仮想環境を動作環境とする一つ以上のアプリケーションとが関連付けられた動作環境情報が記憶されており、
- 前記制御部による前記フェールセーフ処理は、前記動作環境情報を参照して、前記否定的な仮想環境を動作環境とするアプリケーションを特定する処理を含む
- 請求項5に記載の車載ECU。
- [請求項7] 車両に搭載され、複数のアプリケーションを実行するコンピュータに、
- 前記複数のアプリケーションそれぞれの検証を行い、
- 前記検証の結果が肯定的なアプリケーションを実行し、
- 前記検証の結果が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、
- 前記フェールセーフ処理は、
- 前記否定的なアプリケーションを特定し、
- 特定した前記否定的なアプリケーションに応じた代替信号の出力を

含む

処理を実行させるプログラム。

[請求項8]

車両に搭載され、複数のアプリケーションを実行するコンピュータに、

前記複数のアプリケーションそれぞれの検証を行い、

前記検証の結果が肯定的なアプリケーションを実行し、

前記検証の結果が否定的なアプリケーションは実行せず、前記否定的なアプリケーションを代替するフェールセーフ処理を実行し、

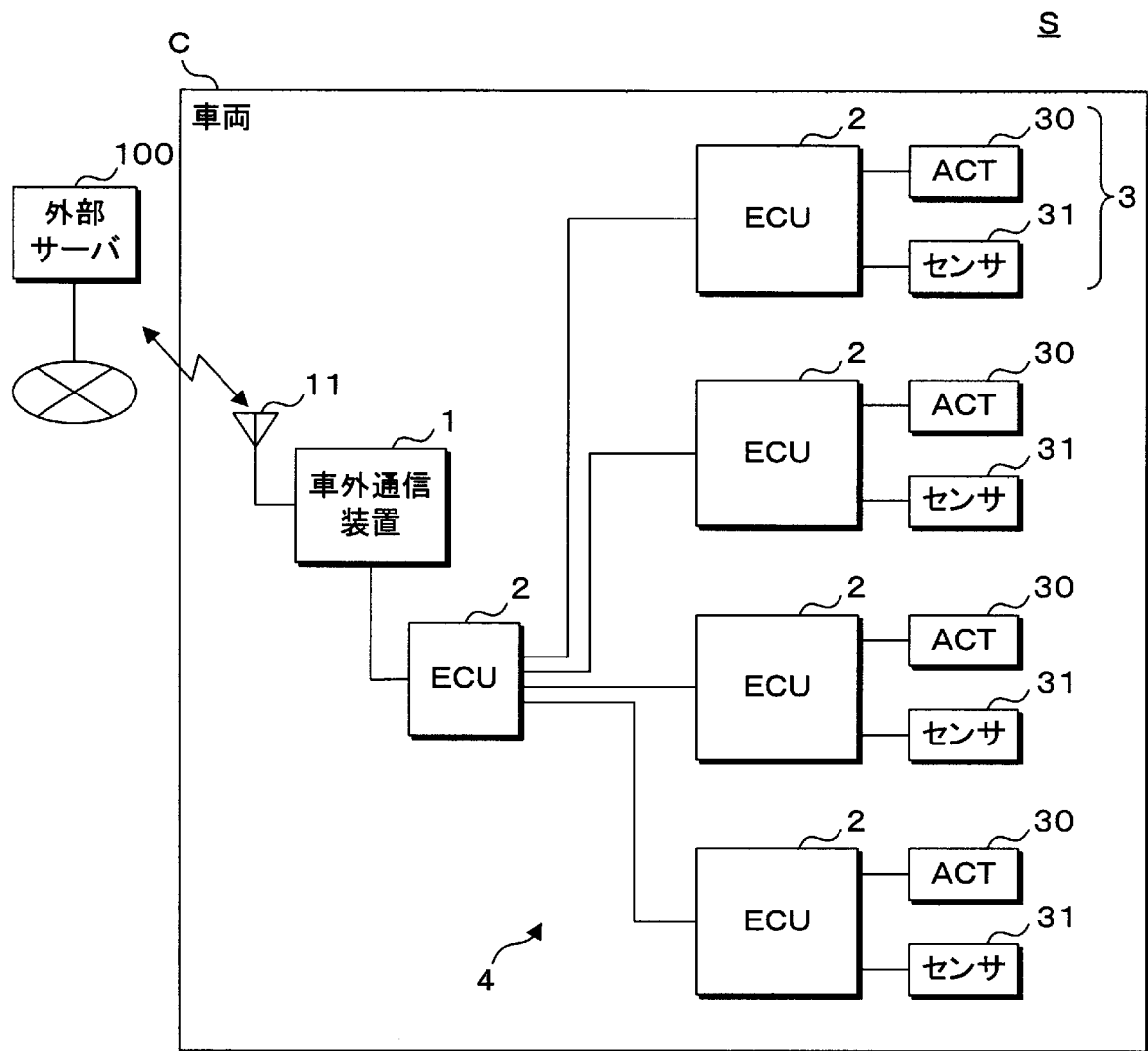
前記フェールセーフ処理は、

前記否定的なアプリケーションを特定し、

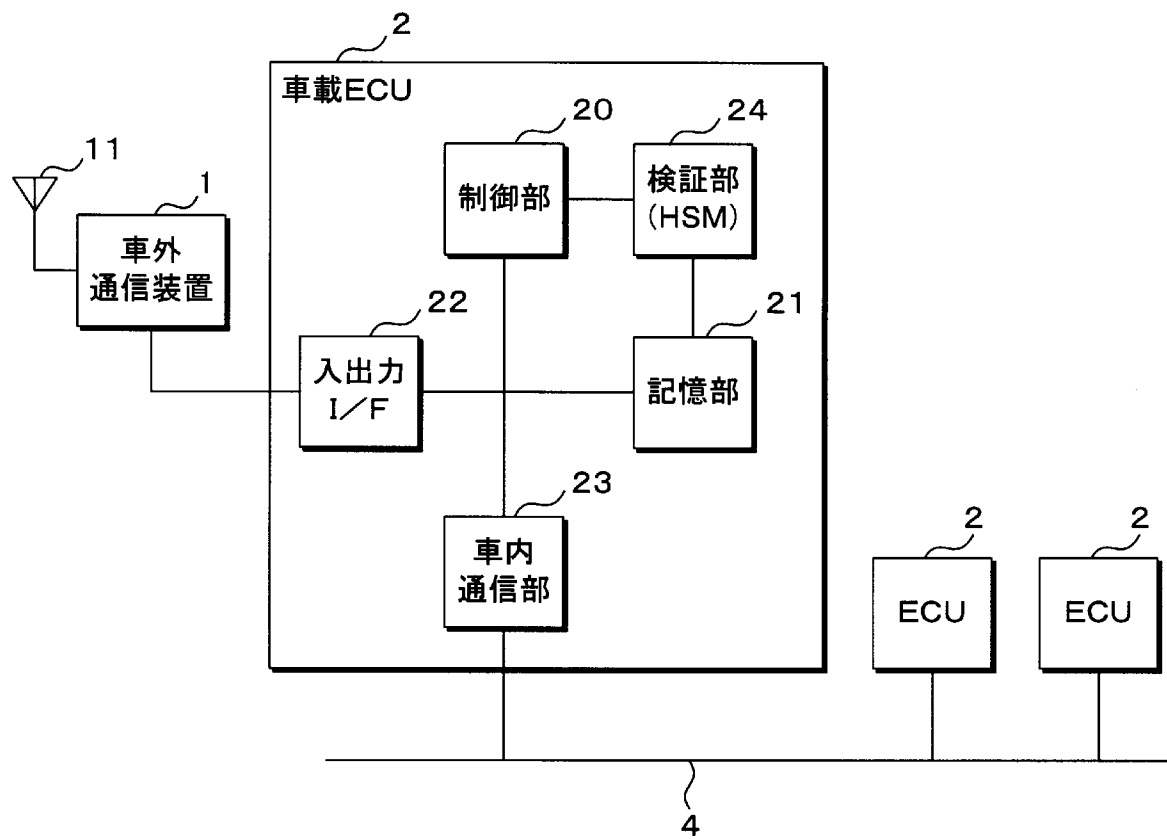
特定した前記否定的なアプリケーションに応じた代替信号の出力を含む

処理を実行させるフェールセーフ方法。

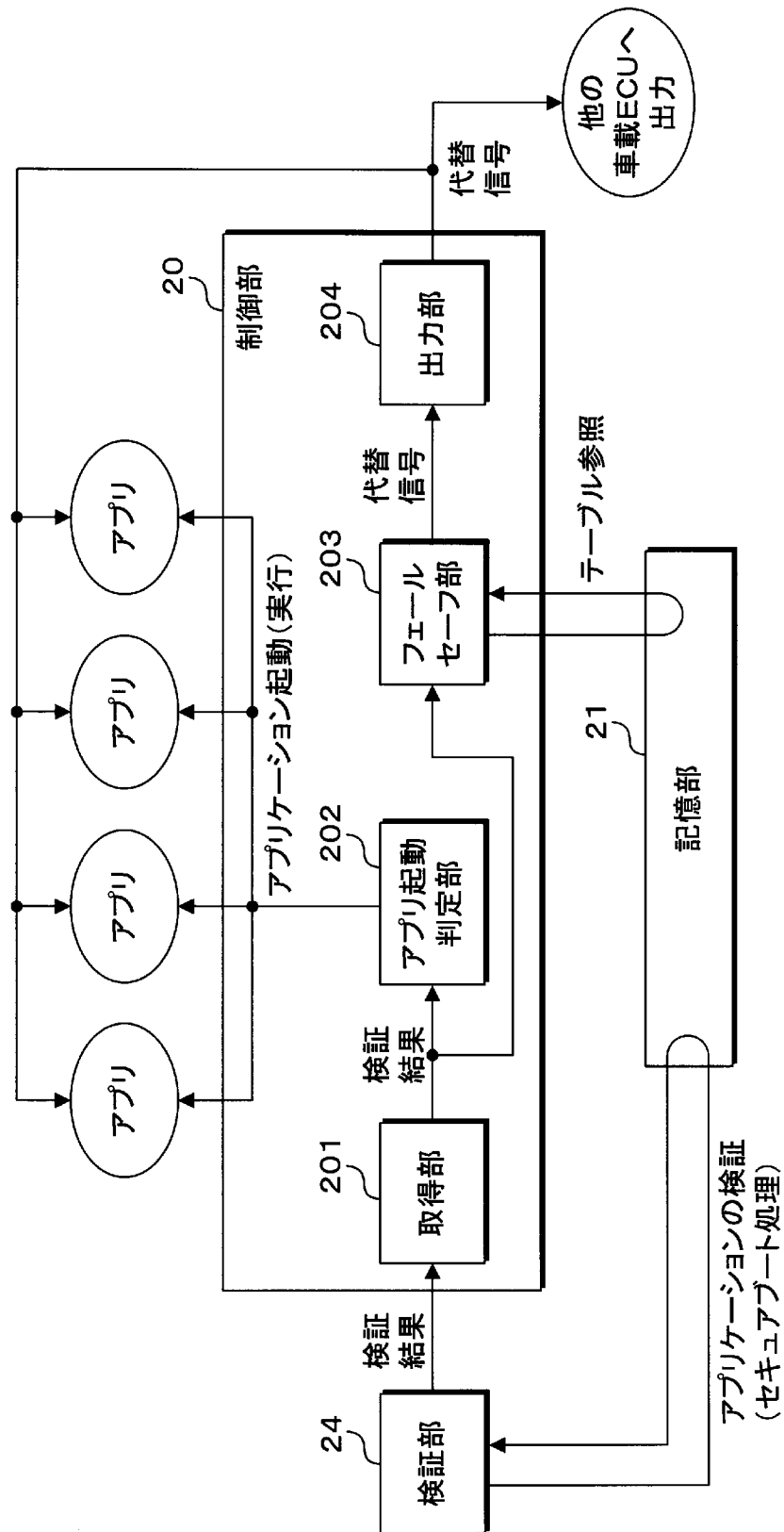
[図1]



[図2]



[図3]



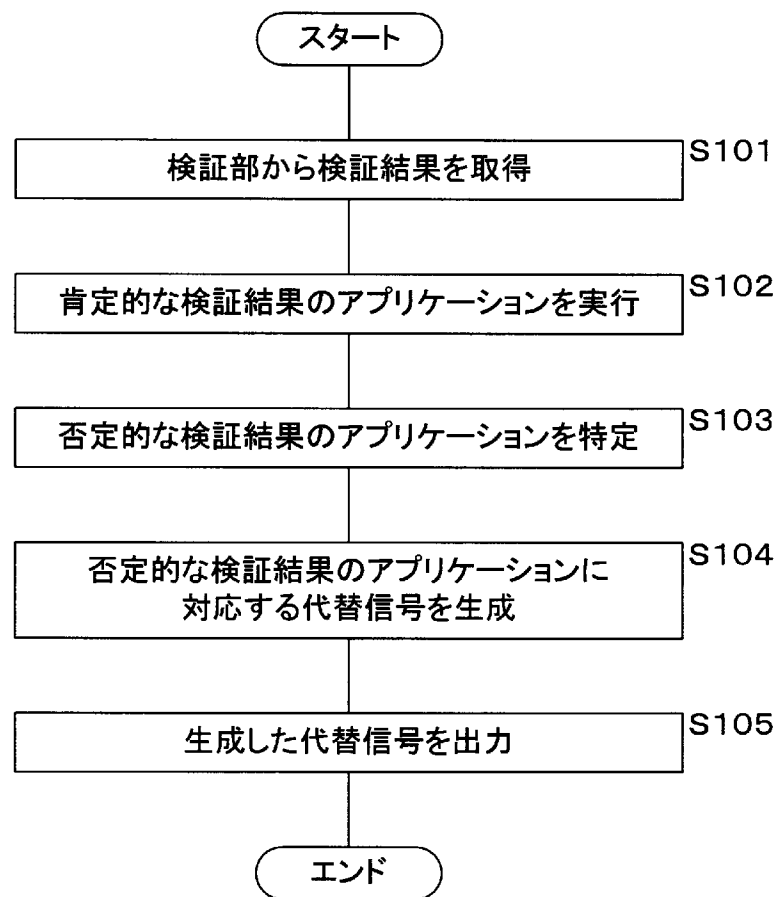
[図4]

211

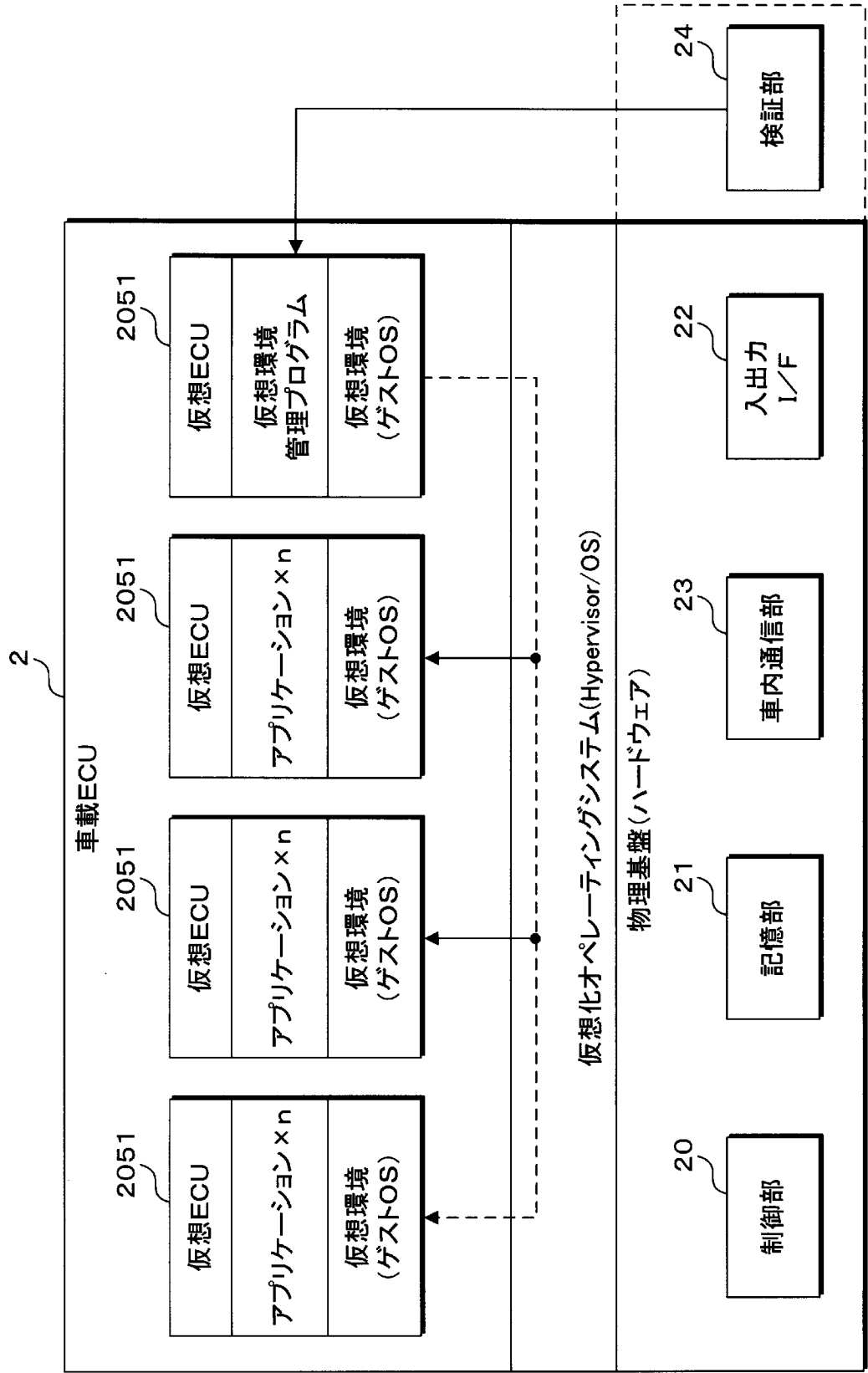
application-1	application-2	application-3	application-4	...	application-X	代替信号パターン
○	○	○	×	○	○	001
○	○	×	×	×	×	002
○	×	×	×	×	×	003
×	○	○	○	○	○	004
×	○	○	×	○	○	005
×	○	×	×	×	×	006
・	・	・	・	・	・	・
・	・	・	・	・	・	・

○: 肯定的な検証結果／実行(起動)可能
 ×: 否定的な検証結果／実行(起動)不可

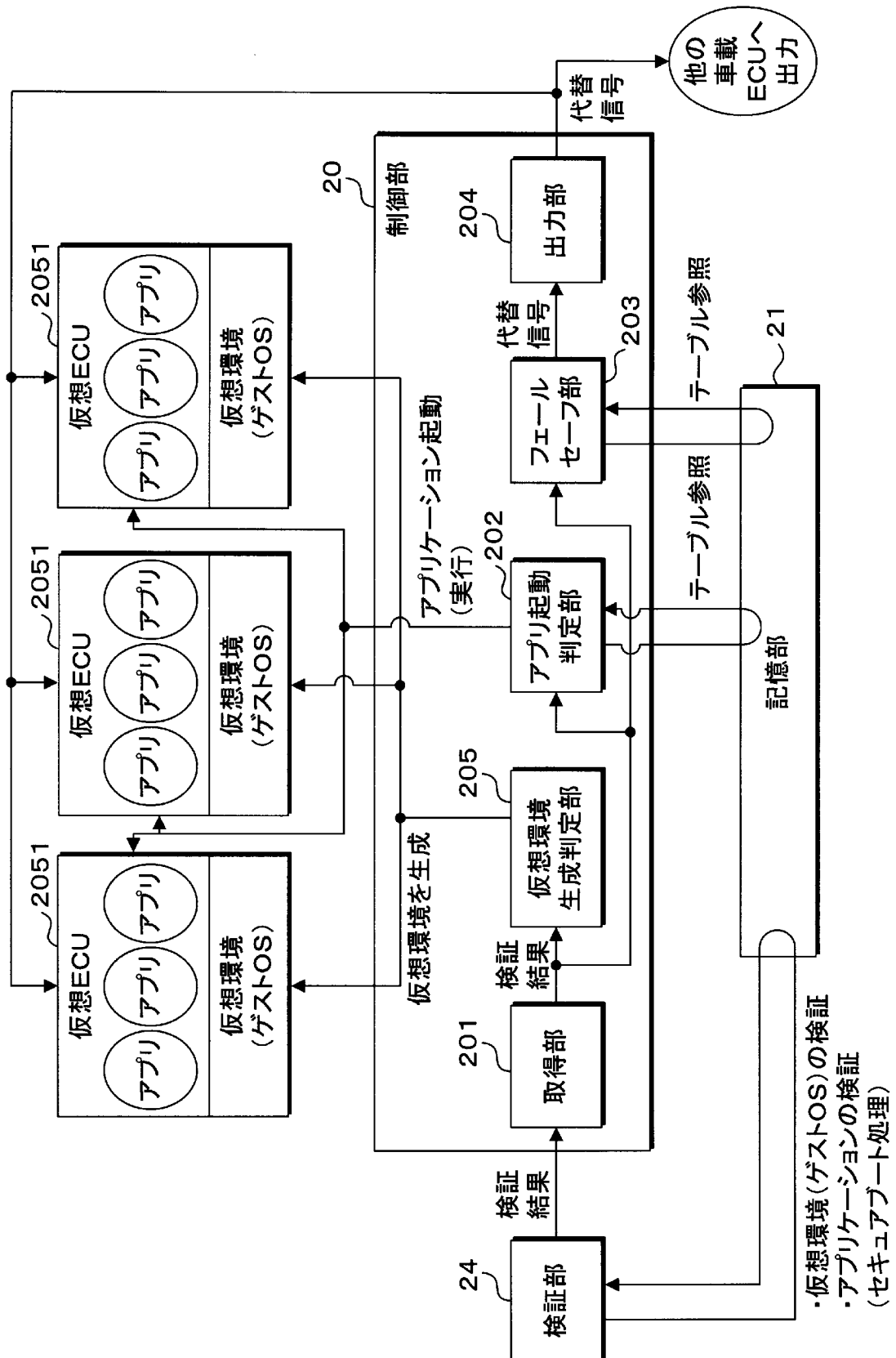
[図5]



[図6]



[図7]

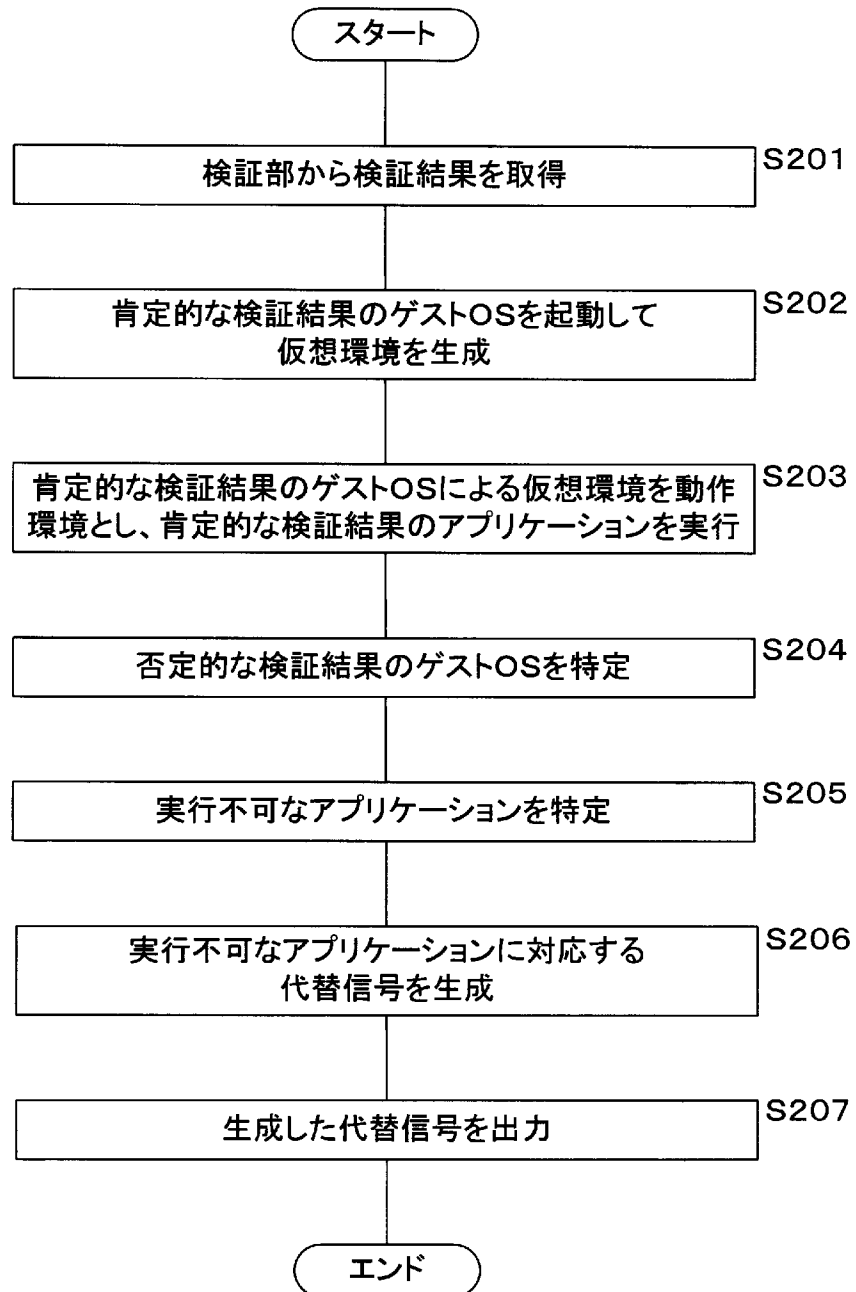


[図8]

212

アプリケーション	仮想環境(ゲストOS)
Application-1	OS-1
Application-2	OS-1
Application-3	OS-1
Application-4	OS-2
Application-5	OS-2
Application-6	OS-2
Application-7	OS-2
Application-8	OS-3
Application-9	OS-3
Application-10	OS-3
Application-11	OS-4
.	.

[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/038162

A. CLASSIFICATION OF SUBJECT MATTER <i>B60R 16/02</i> (2006.01)i; <i>G06F 21/57</i> (2013.01)i FI: B60R16/02 660W; G06F21/57 350 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) B60R16/02; G06F21/57 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.
Y	JP 2020-144531 A (TOYOTA MOTOR CORP.) 10 September 2020 (2020-09-10) paragraphs [0030]-[0073], fig. 1-5	1-8
Y	JP 6-33828 A (DENSO CORP.) 08 February 1994 (1994-02-08) paragraphs [0001]-[0004]	1-8
Y	WO 2010/097936 A1 (TOYOTA MOTOR CORP.) 02 September 2010 (2010-09-02) paragraphs [0020]-[0091], fig. 1-4	3-6
Y	JP 2020-173560 A (AUTONETWORKS TECHNOLOGIES, LTD.) 22 October 2020 (2020-10-22) paragraphs [0037]-[0056], fig. 1-3	5-6
☐ 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 14 December 2021		Date of mailing of the international search report 28 December 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/JP2021/038162

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2020-144531	A	10 September 2020	US 2020/0285749 A1 paragraphs [0014]-[0089], fig. 1-5 EP 3706387 A1	
JP	6-33828	A	08 February 1994	(Family: none)	
WO	2010/097936	A1	02 September 2010	US 2011/0202231 A1 paragraphs [0034]-[0105], fig. 1-4 EP 2402199 A1 CN 102271951 A	
JP	2020-173560	A	22 October 2020	WO 2020/208952 A1 paragraphs [0037]-[0056], fig. 1-3	

A. 発明の属する分野の分類（国際特許分類（IPC）） B60R 16/02(2006.01)i; G06F 21/57(2013.01)i FI: B60R16/02 660W; G06F21/57 350														
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）） B60R16/02; G06F21/57														
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												
Y	JP 2020-144531 A（トヨタ自動車株式会社）10.09.2020（2020 - 09 - 10） 段落[0030] - [0073], 図1 - 図5	1-8												
Y	JP 6-33828 A（日本電装株式会社）08.02.1994（1994 - 02 - 08） 段落[0001] - [0004]	1-8												
Y	WO 2010/097936 A1（トヨタ自動車株式会社）02.09.2010（2010 - 09 - 02） 段落[0020] - [0091], 図1 - 図4	3-6												
Y	JP 2020-173560 A（株式会社オートネットワーク技術研究所）22.10.2020（2020 - 10 - 22） 段落[0037] - [0056], 図1 - 図3	5-6												
☐ 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</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</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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></td> </tr> </table>			* 引用文献のカテゴリー	“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	“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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													
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 14.12.2021	国際調査報告の発送日 28.12.2021													
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） 菅 和幸 3Q 4547 電話番号 03-3581-1101 内線 3339													

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/JP2021/038162

引用文献			公表日	パテントファミリー文献	公表日
JP	2020-144531	A	10.09.2020	US 2020/0285749 A1 段落[0014]－[0089], 図1 －図5 EP 3706387 A1	
JP	6-33828	A	08.02.1994	(ファミリーなし)	
WO	2010/097936	A1	02.09.2010	US 2011/0202231 A1 段落[0034]－[0105], 図1 －図4 EP 2402199 A1 CN 102271951 A	
JP	2020-173560	A	22.10.2020	WO 2020/208952 A1 段落[0037]－[0056], 図1 －図3	