

(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
2018年3月15日(15.03.2018)



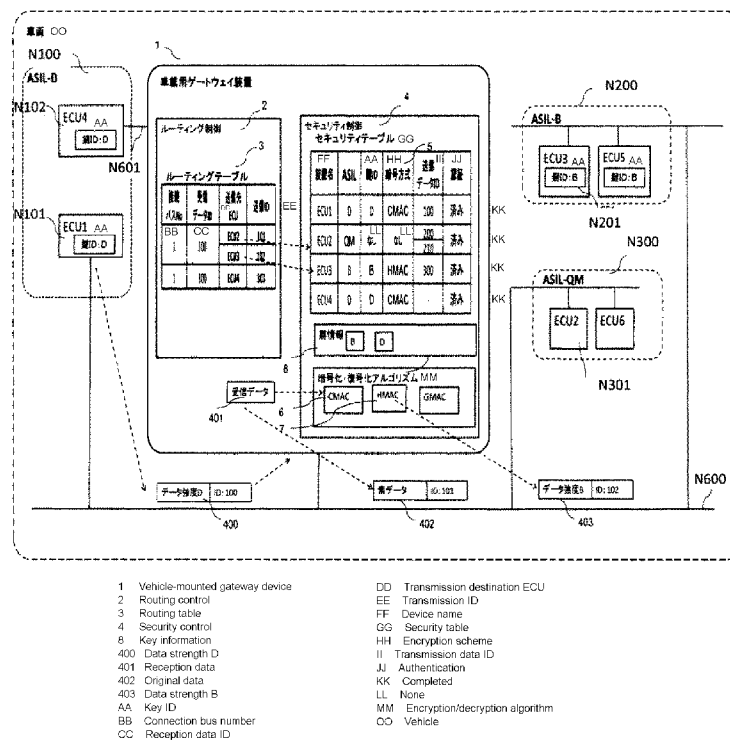
(10) 国際公開番号

WO 2018/047510 A1

- (51) 国際特許分類:
H04L 12/46 (2006.01) H04L 12/28 (2006.01)
- (21) 国際出願番号: PCT/JP2017/027366
- (22) 国際出願日: 2017年7月28日(28.07.2017)
- (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 2016-174561 2016年9月7日(07.09.2016) JP
- (71) 出願人: 日立オートモティブシステムズ株式会社(HITACHI AUTOMOTIVE SYSTEMS, LTD.) [JP/JP]; 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 Ibaraki (JP).
- (72) 発明者: 山本 尚幸 (YAMAMOTO Naoyuki); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP). 中西 一弘 (NAKANISHI Kazuhiro); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP).
- (74) 代理人: 戸田 裕二 (TODA Yuji); 〒1008220 東京都千代田区丸の内一丁目 6 番 1 号 株式会社日立製作所内 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, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) Title: PROCESSING DEVICE FOR MOUNTING IN VEHICLE

(54) 発明の名称: 車載用処理装置



(57) Abstract: The present invention provides a vehicle-mounted processing device capable of introducing security into a vehicle-mounted network in stages. According to the present invention, a communication device (receiving unit) of a vehicle-mounted gateway device 1 receives data 400 (first data) including an identifier (ID). A routing control unit 2 of the vehicle-mounted gateway device 1 identifies a transfer destination corresponding to the ID. A security control unit 4 of the vehicle-mounted gateway device 1 generates, from the data 400 (first data), data 402, 403 (second data) to be



DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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:

- 国際調査報告 (条約第21条(3))

transferred to the transfer destination, on the basis of safety level information (ASIL) indicating a safety level required for the transfer destination. A communication device (transmitting unit) of the vehicle-mounted gateway device 1 transmits the data 402, 403 (second data) to the transfer destination.

(57) 要約: 本発明は、車載ネットワークに段階的にセキュリティを導入することができる車載処理装置を提供する。本発明は、車載用ゲートウェイ装置1の通信装置(受信部)は、ID(識別子)を含むデータ400(第1データ)を受信する。車載用ゲートウェイ装置1のルーティング制御部2は、IDに対応する転送先を特定する。車載用ゲートウェイ装置1のセキュリティ制御部4は、転送先に要求される安全度を示すASIL(安全度情報)に基づいてデータ400(第1データ)から転送先に転送するデータ402、403(第2データ)を生成する。車載用ゲートウェイ装置1の通信装置(送信部)は、データ402、403(第2データ)を転送先へ送信する。

明 細 書

発明の名称：車載用処理装置

技術分野

[0001] 本発明は、車載用処理装置に関する。

背景技術

[0002] 車両システムの情報化の進展に従い、ネットワークのセキュリティリスクが増大している。実際に車両のネットワークに対し、攻撃することで走行に影響を与えるような脅威事例も発生し、外部からの攻撃に対して、自動車の制御システムを保護するセキュリティ機能が重要視されている。

[0003] 車両には、複数の電子制御装置（以降、ECUと呼ぶ）が搭載されており、装置間のネットワークは、主にCAN（Controller Area Network）の規格で構成されている。車載ネットワークにセキュリティ対策を適用する場合、CANフレーム送信ECUは、CANフレームの正当性を保証し、CANバスに接続された偽ECUからのリプレイ攻撃を防御するため、鍵を用いてCANフレームに認証コード（Message Authentication Code; MAC）を付与する方法が提案されている（例えば、特許文献1参照）。

[0004] また、ノードの負担を抑制しつつ、データ通信のセキュリティ性を高めることができる技術が開示されている（例えば、特許文献2参照）。特許文献2の車両用データ通信装置は、データを暗号化するか否かの暗号化情報をデータの送信側のノードを接続するバスとデータの受信側のノードを接続するバスとの組み合わせの単位で一元的に管理し、ノードは、データを復号化するか否かの復号化情報をデータの送信側のノードを接続するバスの単位で一元的に管理する。

先行技術文献

特許文献

[0005] 特許文献1：特許第5770602号公報

特許文献2：特開2013-201510号公報

発明の概要

発明が解決しようとする課題

- [0006] 現状の車両ネットワークのCANでは、ライン上に各ECUを接続していくことによるライン型のネットワークとなっている。CANフレームには送信元ECU及び宛先ECUの識別情報が含まれておらず、受信ECUにおいて、送信元の正しいECUからのデータであるか否かを単純に判断することはできない。
- [0007] 特許文献1に開示されるような技術では、車載ネットワークにセキュリティ対策を適用する場合、送信CANフレーム自体に変更が必要となり、全ECUの変更対応工数が大きくなる。
- [0008] 特許文献2に開示されるような技術では、バス毎にセキュリティ対策を行うことができるが、データを受信するECUはすべて復号化する機能を持つ必要があり、信頼性（安全性）が要求されるECUから段階的にセキュリティ機能を取り入れる事ができず、対応工数が大きくなる。
- [0009] 本発明の目的は、車載ネットワークに段階的にセキュリティを導入することができる車載処理装置を提供することにある。

課題を解決するための手段

- [0010] 上記目的を達成するために、本発明は、識別子を含む第1データを受信する受信部と、前記識別子に対応する転送先を特定するルーティング制御部と、前記転送先に要求される安全度を示す安全度情報に基づいて前記第1データから前記転送先に転送する第2データを生成するセキュリティ制御部と、前記第2データを前記転送先へ送信する送信部と、を備える。

発明の効果

- [0011] 本発明によれば、車載ネットワークに段階的にセキュリティを導入することができる。

上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。

図面の簡単な説明

[0012] [図1]本発明の一実施形態による車載用ゲートウェイ装置及び車載ネットワークシステムの構成並びに鍵配信の動作を説明するための図である。

[図2]本発明の一実施形態による車載用ゲートウェイ装置及び車載ネットワークシステムの構成並びに暗号鍵の付替え又は解除の動作を説明するための図である。

[図3]本発明の一実施形態による車載用ゲートウェイ装置のセキュリティテーブルの構成図である。

[図4]本発明の一実施形態による車載用ゲートウェイ装置のルーティングテーブルの構成図である。

[図5]本発明の一実施形態による車載用ゲートウェイ装置のフローチャートである。

[図6]本発明の一実施形態による車載用ゲートウェイ装置のハードウェア構成を示す図である。

発明を実施するための形態

[0013] 以下、図面を用いて、本発明の実施形態による車載用ゲートウェイ装置（車載処理装置）の構成及び動作について説明する。なお、各図において、同一符号は同一部分を示す。

[0014] （システム構成） 図1を用いて本発明の一実施形態による車載用ゲートウェイ装置及び車載ネットワークシステムの構成を説明する。

[0015] 図1の例では、車載ネットワークは、2つのバス（N600、N601）を備えている。バスN600（ライン）には、本発明の実施形態による車載用ゲートウェイ装置1、ECU1（N101）、ECU2（N301）、ECU3（N201）等が接続されている。一方、バスN601には、ECU4（N102）が接続されている。

[0016] 各ECUには、ISO（International Organization for Standardization）によって規定される自動車安全度水準ASIL（Automotive Safety Integrity Level）が割り当てられている。具体的には、ASILは、QM（Qual

ity Management)、A、B、C、D等の記号を用いて分類される。QM<A<B<C<Dの順で要求される安全度は大きくなる。

[0017] 図1の例では、破線N100内のECU1(N101)、ECU4(N102)に、最も高い安全度である「D」が割り当てられている。破線N200内のECU3(N201)、ECU5には、「B」が割り当てられている。破線N300内のECU2(N301)、ECU6には、最も低い安全度である「QM」が割り当てられている。

[0018] 車載用ゲートウェイ装置1は、データ転送先を判定するルーティング制御部2、CAN ID(識別子)と出力先(転送先)の対応づけを示すルーティングテーブル3、セキュリティの制御判定等をするセキュリティ制御部4、各装置の鍵情報管理、ECU間の認証情報、各ASIL情報及び暗号方式を示すセキュリティテーブル5、暗号化・復号化アルゴリズム6(図2)、鍵情報8を備える。

[0019] なお、車載用ゲートウェイ装置1は、図6に示すように、マイコン11(プロセッサ)、入出力ポートなどの入出力装置14、CANトランシーバなどの通信装置15等を備える。マイコン11は、揮発性メモリの一例であるSRAM12(Static Random Access Memory)と、不揮発性メモリの一例であるFLASH13(Flash Memory)を内蔵する。

[0020] FLASH13には、ルーティングテーブル3、セキュリティテーブル5、暗号化・復号化アルゴリズム6、7(プログラム)、鍵情報8等が記憶される。SRAM12には、演算に必要なデータ、演算結果などが一時的に記憶される。

[0021] ルーティングテーブル3は、図4に示すように、送信先ECUが接続されるバスを識別する番号を示す「接続バスNo」、受信データのIDを示す「受信データID」、受信データIDに対応する送信先のECUを示す「送信先ECU」、送信先へ送信するデータに割り当てるIDを示す「送信ID」等のフィールドを備える。

[0022] セキュリティテーブル5は、図3に示すように、「装置名」、自動車安全

度水準を示す「A S I L」、暗号鍵を識別する I D を示す「鍵 I D」、「暗号方式」、装置名が示す E C U が送信するデータの I D を示す「送信データ I D」、チャレンジアンドレスポンスによる認証の結果を示す「認証」等のフィールドを備える。換言すれば、F L A S H 1 3（記憶装置）は、装置名（転送先）、及び装置名（転送先）に対応する A S I L（安全度情報）の組合せを記憶する。

[0023] 車載用ゲートウェイ装置 1 のセキュリティ制御部 4（マイコン 1 1）は、F L A S H 1 3（記憶装置）から転送先に対応する A S I L（安全度情報）を読み出し、読み出した A S I L に応じて、転送先に転送するデータの暗号強度を設定する。これにより、転送前のデータの暗号強度にかかわらず転送先の A S I L に応じて転送するデータの暗号強度が決まる。動作の詳細については、図 5 を用いて後述する。

[0024] また、F L A S H 1 3（記憶装置）は、A S I L（安全度情報）、及び A S I L に対応する暗号方式の組合せを記憶する。

[0025] 車載用ゲートウェイ装置 1 のセキュリティ制御部 4（マイコン 1 1）は、F L A S H 1 3（記憶装置）から A S I L（安全度情報）に対応する暗号方式を読み出し、読み出した暗号方式を用いて、転送先に転送するデータの暗号強度を設定する。これにより、転送先では、A S I L に対応する暗号方式の復号のみを行えばよい。詳細については、図 5 を用いて後述する。

[0026] さらに、F L A S H 1 3（記憶装置）は、A S I L（安全度情報）、及び A S I L に対応する暗号鍵の情報を示す鍵 I D（暗号鍵情報）の組合せを記憶する。

[0027] 車載用ゲートウェイ装置 1 のセキュリティ制御部 4（マイコン 1 1）は、F L A S H 1 3（記憶装置）から A S I L（安全度情報）に対応する鍵 I D を読み出し、読み出した鍵 I D が示す暗号鍵を転送先に配信する。これにより、転送先では、A S I L に応じた暗号鍵を用いてデータを復号化することができる。

[0028] なお、図 3 に示す C M A C（Cipher-based MAC）は、ブロック暗号に基づくメッ

セージ認証符号アルゴリズムである。また、図3に示すHMAC (Hash-based Message Authentication Code)は、メッセージ認証符号 (MAC; Message Authentication Code) の一つであり、秘密鍵とメッセージ (データ) とハッシュ関数をもとに計算される。CMACの暗号強度は、HMACの暗号強度よりも大きい。

[0029] (暗号鍵の配信)

次に、図1を用いて、ASIL毎に車載用ゲートウェイ装置1が各ECUへ鍵配信を行う例を説明する。

[0030] 車載用ゲートウェイ装置1のルーティングテーブル3には、セキュリティを必要とするECU1 (N101)、ECU3 (N201) 等へ鍵情報を送信するため送信IDを準備する。図1の例では、ルーティングテーブル3の第3レコードにおいて、送信先「ECU1」に送信ID「600」が割り当てられている。また、ルーティングテーブル3の第4レコードにおいて、送信先「ECU3」に送信ID「610」が割り当てられている。

[0031] セキュリティテーブル5には、各ECUに対応したASIL毎の鍵情報を準備する。図1の例では、セキュリティテーブル5の第1レコードにおいて、装置名「ECU1」に、鍵ID「D」が割り当てられている。また、セキュリティテーブルの第3レコードにおいて、装置名「ECU3」に鍵ID「B」が割り当てられている。ここで、鍵IDは、暗号鍵を識別する識別子である。

[0032] 車載用ゲートウェイ装置1は、各ECUとチャレンジ&レスポンスによるECU機器認証を行う。車載用ゲートウェイ装置1は、各ECUと認証が成功した場合に、セキュリティテーブル5で解決したASIL毎の鍵情報8を各ECUへ配信する。車載用ゲートウェイ装置1は、受信データID毎に周期の監視を行う。周期を逸脱して受信したIDのデータは不正データとし破棄する。

[0033] 車載用ゲートウェイ装置1は、各ECUへ配信した鍵を用いてフレーム受信及びフレーム送信時MACの解決を行い、各ECUとの暗号化の調停を行う。このフレーム調停 (暗号鍵の付替え又は解除) は、図2を用いて説明する。

[0034] (暗号鍵の付替え又は解除)

次に、図2を用いて本発明の一実施形態による車載用ゲートウェイ装置及び車載ネットワークの暗号鍵の付替え又は解除の動作を説明する。

[0035] ECU1(N101)からECU2(N301)及びのECU3(N201)へデータを渡したい場合、ECU1(N101)で、CANフレームの暗号化をしている為、受信側のECUはデータを受信してもそのままデータを扱う事ができない。そこで車載用ゲートウェイ装置1はECU1(N101)からの受信データ401をルーティングテーブル3及びセキュリティテーブル5から解決し、復号化アルゴリズム6によりデータ復号化をする。

[0036] ルーティングテーブル3の送信先ECUに見合った暗号化アルゴリズム6により鍵情報8を指定して、データ暗号化する事でデータ強度B(403)とし、送信IDを付け替えて送信する。セキュリティテーブル5の送信先ECUのASILがQMの場合は、暗号化せずに素データ402として、送信IDを付け替えて送信する。

[0037] 次に、図5を用いて、車載用ゲートウェイ装置1の動作を詳細に説明する。ここでは、図2に示すECU1が、暗号化したデータ強度Dのデータ400(CANフレーム)を、バスN601を介して送信したと仮定する。なお、データ400に含まれるID(識別子)は「100」である。データ400(第1データ)は、鍵IDである「D」が示す暗号鍵(第1暗号鍵)を用いて暗号化されている。

[0038] 車載用ゲートウェイ装置1は、データ400を受信する(S1)。ここで、車載用ゲートウェイ装置1の通信装置15は、ID(識別子)を含むデータ400を受信する受信部として機能する。

[0039] 車載用ゲートウェイ装置1は、受信したデータ400(受信データ401)が転送の対象であるか否かを判定する(S2)。

[0040] 詳細には、車載用ゲートウェイ装置1は、ルーティングテーブル3から「受信データID」フィールドの値がデータ400のID「100」と一致するレコードを検索する。車載用ゲートウェイ装置1は、検索によりヒットし

たレコードの「送信先 ECU」フィールドの値が自身でない場合（S2：YES）、S3へ処理を進め、検索によりヒットしたレコードの「送信先 ECU」フィールドの値が自身である場合又は検索条件を満たすレコードがない場合（S2：NO）、処理を終了する。

[0041] 図5に示すルーティングテーブル3では、検索により第1レコードがヒットする。車載用ゲートウェイ装置1は、ルーティングテーブル3の第1レコードの「送信先 ECU」フィールドD1の値から送信先 ECUが ECU2、ECU3であり、受信したデータ400は転送の対象であると判定する。なお、車載用ゲートウェイ装置1は、ルーティングテーブル3の第1レコードの「送信 ID」フィールドから送信するデータの IDが 101、102であることを特定する。

[0042] ここで、車載用ゲートウェイ装置1のマイコン11は、データ400に含まれる ID（識別子）に対応する転送先を特定するルーティング制御部2として機能する。

[0043] 続いて、車載用ゲートウェイ装置1は、データ400を送信した ECU1の ASILと送信先の ECU2、ECU3の ASILが異なるか否かをそれぞれ判定する（S3）。

[0044] まず、車載用ゲートウェイ装置1は、セキュリティテーブル5を参照し、データ400を送信した ECU1の ASILを特定する。具体的には、車載用ゲートウェイ装置1は、セキュリティテーブル5から「送信データ ID」フィールドの値がデータ400の ID「100」と一致するレコードを検索する。図5に示すセキュリティテーブル5では、第1レコードがヒットする。車載用ゲートウェイ装置1は、セキュリティテーブル5の第1レコードの「ASIL」フィールドD2の値からデータ400を送信した ECU1の ASILが「D」であることを特定する。

[0045] 次に、車載用ゲートウェイ装置1は、セキュリティテーブル5を参照し、転送先の ECU2、ECU3の ASILを特定する。具体的には、車載用ゲートウェイ装置1は、セキュリティテーブル5から「装置名」フィールドの

値が、ECU2、ECU3のデータをそれぞれ検索する。図5に示すセキュリティテーブル5では、第2レコード、第3レコードがそれぞれヒットする。

[0046] 車載用ゲートウェイ装置1は、セキュリティテーブル5の第2レコードの「ASIL」フィールドD2の値から送信先のECU2のASILが「QM」であることを特定する。

同様に、車載用ゲートウェイ装置1は、セキュリティテーブル5の第3レコードの「ASIL」フィールドD2の値から送信先のECU3のASILが「B」であることを特定する。

[0047] これにより、車載用ゲートウェイ装置1は、データ400を送信したECU1のASILと送信先のECU2、ECU3のASILがそれぞれ異なると判定する（S3：YES）。

[0048] 車載用ゲートウェイ装置1は、セキュリティテーブル5の第1レコードの「暗号方式」フィールドの値からECU1が「CMAC」でデータ400を暗号化したことを特定し、受信したデータ400を暗号方式「CMAC」で復号化する（S4）。

[0049] 車載用ゲートウェイ装置1は、送信先（転送先）のECUのASILが「QM」以外であるか否かを判定する（S5）。図5の例では、送信先のECU2のASILは「QM」であるため、車載用ゲートウェイ装置1は、S4で復号化したデータ400から平文の素データ402（CANフレーム）を生成して送信する（S7）。また、送信先のECU3のASILは「B」であるため、車載用ゲートウェイ装置1は、S4で復号化したデータ400をセキュリティテーブル5の第3レコードの「鍵ID」フィールドの値「B」が示す暗号鍵を用いて、S4で復号化したデータ400を「暗号方式」フィールドの値「HMAC」で暗号化し（S6）、データ強度Bのデータ403（CANフレーム）を生成して送信する（S7）。

[0050] 換言すれば、車載用ゲートウェイ装置1のマイコン11は、転送先に要求される安全度を示すASIL（安全度情報）に基づいてデータ400（第1

データ)から転送先に転送するデータ402、403(第2データ)を生成するセキュリティ制御部4として機能する。また、車載用ゲートウェイ装置1の通信装置15は、データ402、403(第2データ)を転送先へ送信する送信部として機能する。

[0051] 詳細には、マイコン11(セキュリティ制御部4)は、転送先のASIL(安全度情報)に応じてデータ402、403(第2データ)の暗号強度を設定する。具体的には、マイコン11(セキュリティ制御部4)は、転送先のASIL(安全度情報)に応じてデータ400(第1データ)の暗号鍵を交換する又はデータ400の暗号化を解除することにより、データ402、403(第2データ)を生成する。

[0052] 例えば、マイコン11(セキュリティ制御部4)は、転送先のASIL(安全度情報)に応じて、第1暗号鍵(鍵ID=D)を用いてデータ400(第1データ)を復号化し、第1暗号鍵と異なる第2暗号鍵(鍵ID=B)を用いて暗号化することにより、データ400の暗号鍵を交換し、転送先のASILが最も低い安全度を示す場合、第1暗号鍵(鍵ID=D)を用いてデータ400を復号化することにより、データ400の暗号化を解除する。これにより、転送先のASILに応じて、転送先毎にセキュリティを導入できる。

[0053] ECU2(N301)は、暗号化されていない素データ402を受信し、受信した素データ402を用いて、所定の処理を行う。一方、ECU3(N201)は、車載用ゲートウェイ装置1から配信された鍵ID「B」に対応する暗号鍵を用いて、暗号化されたデータ強度Bのデータ403を復号化し、復号化したデータを用いて所定の処理を行う。

[0054] このようにして、ECU2(N301)は、素データ402を復号化なしでデータ受信のみでデータを取り扱う。ECU3(N201)は、データ受信時にデータ強度Bのデータ403を対象アルゴリズム(HMAC)で復号化しデータを取り扱う。

[0055] 以上説明したように、本実施形態によれば、車載ネットワークに段階的に

セキュリティを導入することができる。具体的には、セキュリティ機能対応 ECU（復号機能あり）と従来 ECU（復号機能なし）との混在を許容する事で、セキュリティ導入を容易とする。

また従来 ECU には、変更工数をかけずに、ネットワークにセキュリティ機能をいれる事ができる。ゲートウェイで認証や鍵管理を行う為、ゲートウェイでセキュリティ機能の一元管理がでるので早急な事故対応を可能とする。

[0056] なお、本発明は上記した実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上述した実施形態は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施形態の構成の一部を他の実施形態の構成に置き換えることが可能であり、また、ある実施形態の構成に他の実施形態の構成を加えることも可能である。また、各実施形態の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

[0057] 上記実施形態では、ルーティングテーブル 3 及びセキュリティテーブル 5 の各フィールドには予め値が格納されているが、各 ECU から指定して登録するようにしてもよい。

[0058] また、上記の各構成、機能等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサ（マイコン）がそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、SSD（Solid State Drive）等の記録装置、または、ICカード、SDカード、DVD等の記録媒体に置くことができる。

[0059] なお、本発明の実施形態は、以下の態様であってもよい。

[0060] （１）他の車載処理装置と接続された車載処理装置において、前記他の車載処理装置の安全度情報が格納された記憶部と、前記他の車載処理装置に送信されるデータを前記他の車載処理装置の安全度情報に基づいて処理する送

信データ処理部と、前記送信用データ処理部で処理されたデータを前記他の車載処理装置へ送信する送信部と、を備える、車載処理装置。

[0061] (2) 前記送信データ処理部は、前記他の車載処理装置に送信されるデータを暗号化する暗号化部である、(1)に記載の車載処理装置。

[0062] (3) 前記暗号化部は、前記データを暗号化する際の暗号化レベルを、前記安全度情報に基づいて設定する(2)に記載の車載処理装置。

[0063] (4) (1)に記載の車載処理装置において、前記暗号化部は、他の車載用ゲートウェイ装置から送信されたデータに付与された識別番号に基づいて、前記データを処置する他の車載用ゲートウェイ装置を特定した後、前記他の車載処理装置の情報と前記安全度情報とを、照合して、前記データを送信する際の暗号化レベルを設定する。

[0064] (5) (1)に記載の車載処理装置において、複数の車載用ゲートウェイ装置の少なくとも1つは、車載処理装置である。

[0065] (6) (1)に記載の車載処理装置において、複数の車載処理装置の少なくとも1つは、ECUである。

[0066] (7) (1)に記載の車載処理装置に暗号レベルが複数割り当てられ暗号レベルと、出力先車載装置が対応づけられた設定テーブルを有するゲートウェイ装置。

[0067] (8) (1)に記載の車載処理装置に安全度が複数割り当てられ安全度レベルと、暗号レベルが対応づけられた設定テーブルを有するゲートウェイ装置。

[0068] (9) (1)に記載の車載処理装置に暗号方式が複数割り当てられ暗号方式と、暗号レベルが対応づけられた設定テーブルを有するゲートウェイ装置。

符号の説明

- [0069] 1 車載用ゲートウェイ装置
2 ルーティング制御(部)
3 ルーティングテーブル

- 4 セキュリティ制御（部）
- 5 セキュリティテーブル
- 6 暗号化・復号化アルゴリズム（CMAC）
- 7 暗号化・復号化アルゴリズム（HMAC）
- 8 鍵情報
- 1 1 マイコン
- 1 2 SRAM
- 1 3 FLASH
- 1 4 入出力装置
- 1 5 通信装置
- 1 0 0 安全度ASIL-DのECU
- N 1 0 1 ECU 1
- N 1 0 2 ECU 4
- N 2 0 0 安全度ASIL-BのECU
- N 2 0 1 ECU 3
- N 2 0 2 ECU 5
- N 3 0 0 安全度ASIL-QMのECU
- N 3 0 1 ECU 2
- N 3 0 2 ECU 6
- 4 0 0 データ強度Dのデータ
- 4 0 1 受信データ
- 4 0 2 素データ
- 4 0 3 データ強度Bのデータ
- 5 0 1 鍵情報B
- 5 0 2 鍵情報D

請求の範囲

- [請求項1] 識別子を含む第1データを受信する受信部と、
前記識別子に対応する転送先を特定するルーティング制御部と、
前記転送先に要求される安全度を示す安全度情報に基づいて前記第1データから前記転送先に転送する第2データを生成するセキュリティ制御部と、
前記第2データを前記転送先へ送信する送信部と、
を備えることを特徴とする車載処理装置。
- [請求項2] 請求項1に記載の車載処理装置であって、
前記セキュリティ制御部は、
前記転送先の前記安全度情報に応じて前記第2データの暗号強度を設定する ことを特徴とする車載処理装置。
- [請求項3] 請求項2に記載の車載処理装置であって、
前記第1データは、
暗号化されており、
前記セキュリティ制御部は、
前記転送先の前記安全度情報に応じて前記第1データの暗号鍵を交換する又は前記第1データの暗号化を解除することにより、前記第2データを生成する
ことを特徴とする車載処理装置。
- [請求項4] 請求項3に記載の車載処理装置であって、
前記第1データは、
第1暗号鍵を用いて暗号化されており、
前記セキュリティ制御部は、
前記転送先の前記安全度情報に応じて、前記第1暗号鍵を用いて前記第1データを復号化し、前記第1暗号鍵と異なる第2暗号鍵を用いて暗号化することにより、前記第1データの暗号鍵を交換し、
前記転送先の前記安全度情報が最も低い前記安全度を示す場合、前

記第 1 暗号鍵を用いて前記第 1 データを復号化することにより、前記第 1 データの暗号化を解除する

ことを特徴とする車載処理装置。

[請求項5]

請求項 2 に記載の車載処理装置であって、

前記転送先、及び前記転送先に対応する前記安全度情報の組合せを記憶する記憶装置を備え、

前記セキュリティ制御部は、

前記記憶装置から前記転送先に対応する前記安全度情報を読み出し、読み出した前記安全度情報に応じて、前記第 2 データの暗号強度を設定する

ことを特徴とする車載処理装置。

[請求項6]

請求項 5 に記載の車載処理装置であって、

前記記憶装置は、

前記安全度情報、及び前記安全度情報に対応する暗号方式の組合せを記憶し、

前記セキュリティ制御部は、

前記記憶装置から前記安全度情報に対応する前記暗号方式を読み出し、読み出した前記暗号方式を用いて、前記第 2 データの暗号強度を設定する

ことを特徴とする車載処理装置。

[請求項7]

請求項 6 に記載の車載処理装置であって、

前記記憶装置は、

前記安全度情報、及び前記安全度情報に対応する暗号鍵の情報を示す暗号鍵情報の組合せを記憶し、

前記セキュリティ制御部は、

前記記憶装置から前記安全度情報に対応する前記暗号鍵情報を読み出し、読み出した前記暗号鍵情報が示す暗号鍵を前記転送先に配信する

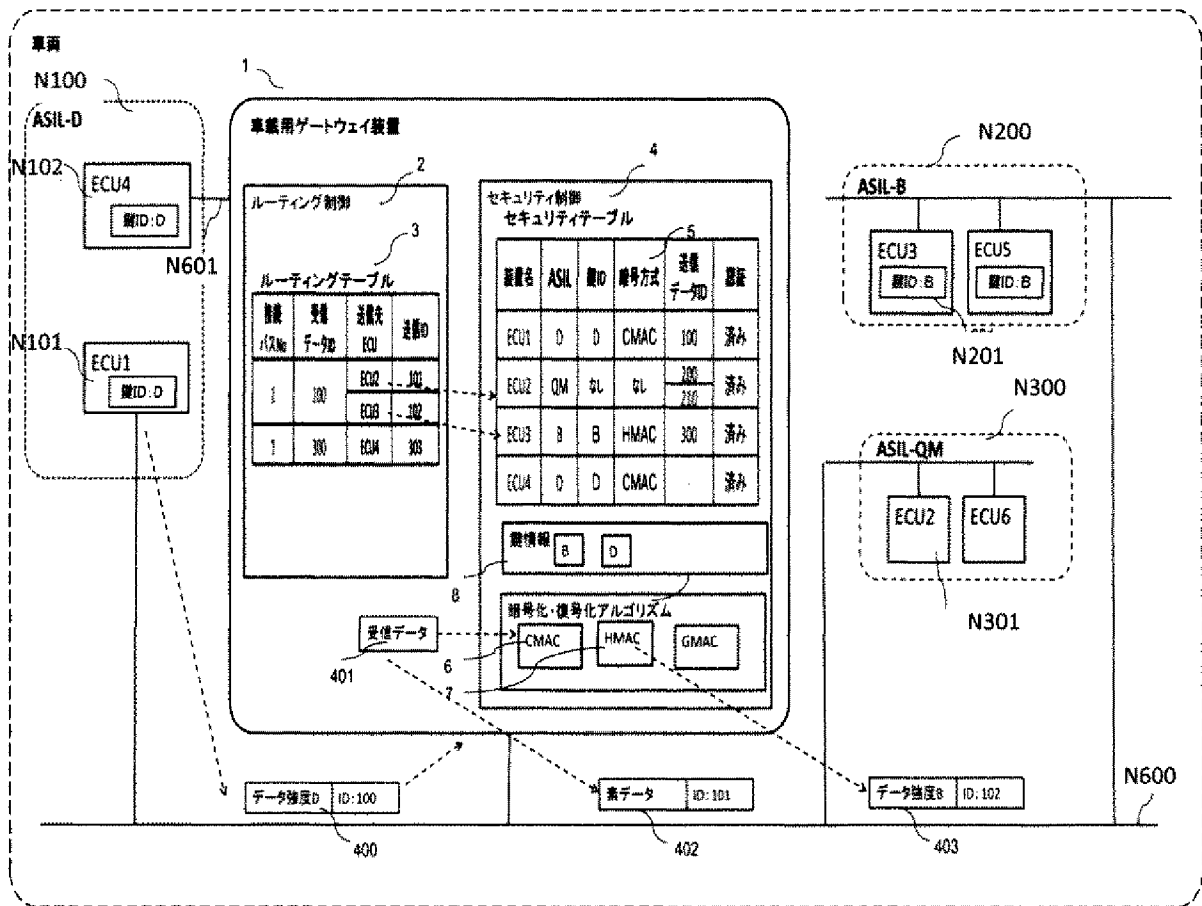
ことを特徴とする車載処理装置。

[請求項8] 請求項1に記載の車載処理装置であって、
前記安全度情報は、
自動車安全度水準ASILである
ことを特徴とする車載処理装置。

[請求項9] 第1の車載処理装置、第2の車載処理装置、及び第3の車載処理装置を含む車載システムであって、
第1の車載処理装置は、
識別子を含む第1データを送信し、
前記第2の車載処理装置は、
前記第1データを受信する受信部と、
前記識別子に対応する転送先を特定するルーティング制御部と、
前記転送先に要求される安全度を示す安全度情報に基づいて前記第1データから前記転送先に転送する第2データを生成するセキュリティ制御部と、
前記第2データを前記転送先である前記第3の車載処理装置へ送信する送信部と、を備え、
前記第3の車載処理装置は、
前記第2データを受信し、受信した前記第2データを用いて所定の処理を行う
ことを特徴とする車載システム。

Figure 1 is a block diagram of a vehicle system architecture. The system is divided into three main sections: N100 (left), N200 (top right), and N300 (bottom right). N100 contains ECU4 and ECU1. N200 contains ECU3 and ECU5. N300 contains ECU2 and ECU6. A central '車載用ゲートウェイ装置' (Vehicle Gateway Device) is connected to all ECUs. This device includes a 'ルーティング制御' (Routing Control) block with a 'ルーティングテーブル' (Routing Table) and a 'セキュリティ制御' (Security Control) block with a 'セキュリティテーブル' (Security Table). The routing table lists destinations (ECU1-ECU6) and their corresponding gateway addresses. The security table lists ECUs, their ASIL levels, IDs, communication methods, and security levels. A '登録情報' (Registration Information) block shows 'D' and 'B' entries. Below the gateway device, two boxes labeled 501 and 502 contain '鍵ID-D' (Key ID-D) and '600', and '鍵ID-B' (Key ID-B) and '610' respectively. Dashed lines connect the 'D' and 'B' entries in the registration information block to these key ID boxes. The entire system is connected to a common bus labeled N600.

[図2]



[図3]

5

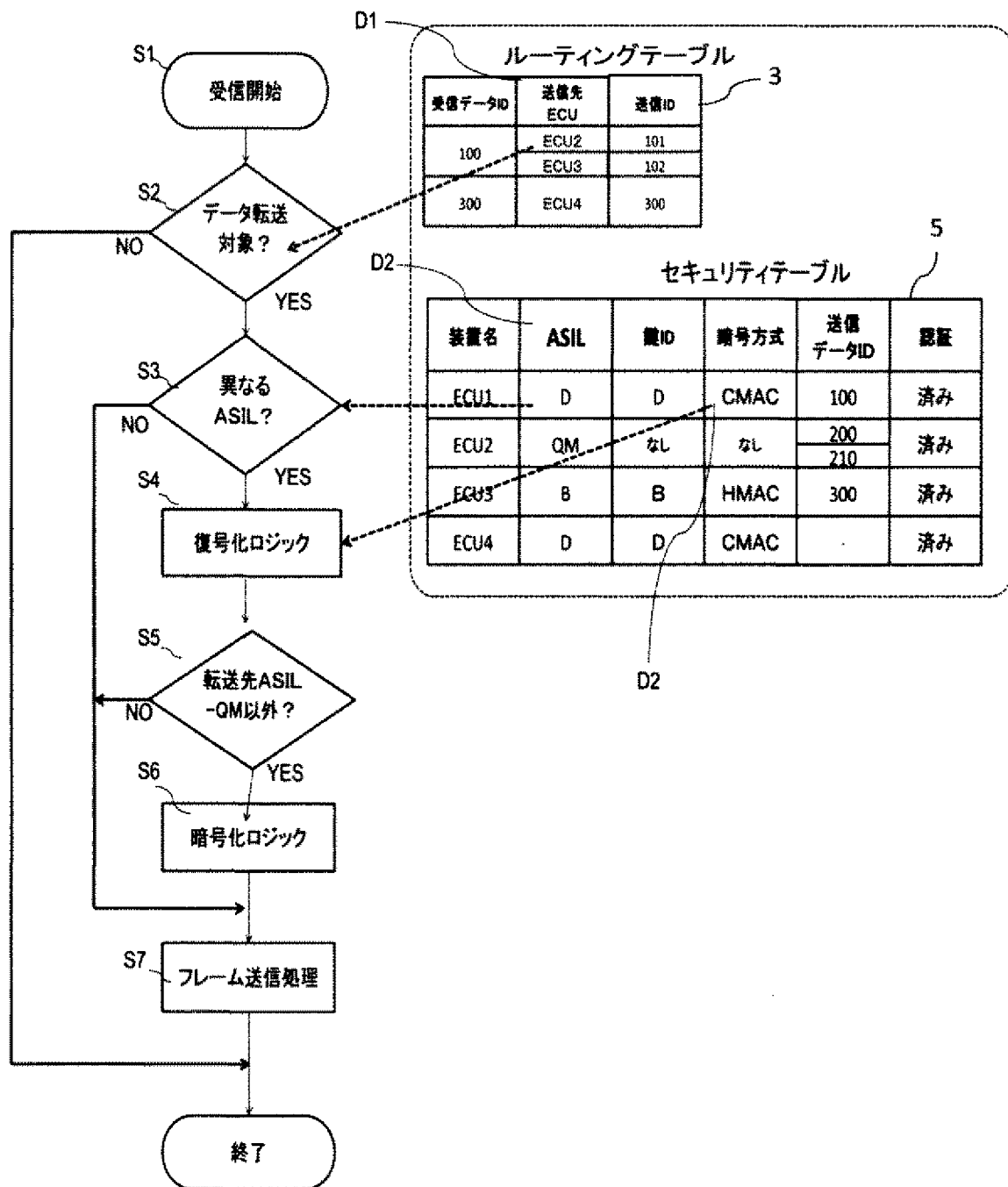
装置名	ASIL	鍵ID	暗号方式	送信データID	認証
ECU1	D	D	CMAC	100	済み
ECU2	QM	なし	なし	200 210	済み
ECU3	B	B	HMAC	300	済み
ECU4	D	D	CMAC	-	済み

[図4]

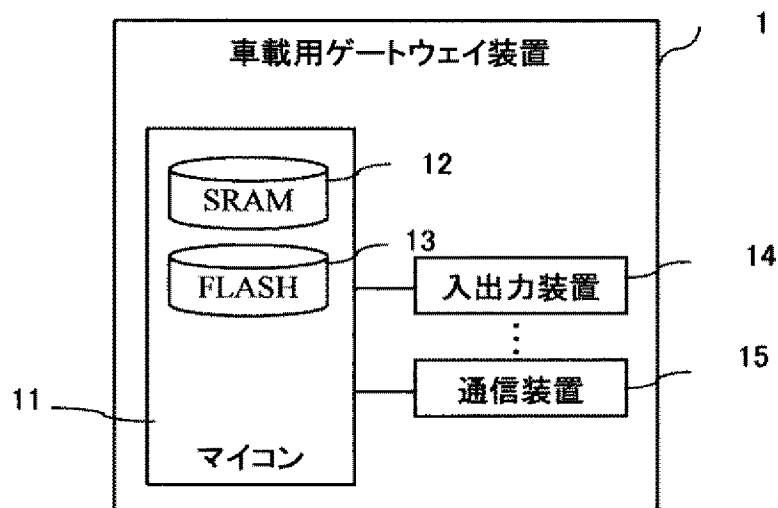
3

接続 バスNo	受信 データID	送信先 ECU	送信ID
1	100	ECU2	101
		ECU3	102
1	300	ECU4	303
1	マスタGW	ECU1	600
1	マスタGW	ECU3	610
2	マスタGW	ECU4	601

[図5]



[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/027366

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/46(2006.01)i, H04L12/28(2006.01)i

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)

H04L12/46, H04L12/28

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

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 2004-343626 A (Sumitomo Electric Industries, Ltd.), 02 December 2004 (02.12.2004), paragraphs [0030] to [0047], [0049], [0053] (Family: none)	1-7, 9
X	JP 2014-204315 A (Denso Corp.), 27 October 2014 (27.10.2014), fig. 4 (Family: none)	1, 2, 5, 8, 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
02 October 2017 (02.10.17)

Date of mailing of the international search report
10 October 2017 (10.10.17)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/027366

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2010-98626 A (Hitachi Automotive Systems, Ltd.), 30 April 2010 (30.04.2010), entire text; all drawings & US 2010/0098095 A1 entire text; all drawings & EP 2178257 A1	1-9
A	JP 2014-174778 A (Hitachi Automotive Systems, Ltd.), 22 September 2014 (22.09.2014), entire text; all drawings & US 2015/0326529 A1 entire text; all drawings & WO 2014/141518 A1	1-9
A	JP 2016-134834 A (Toyota Motor Corp.), 25 July 2016 (25.07.2016), entire text; all drawings (Family: none)	1-9

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L12/46(2006.01)i, H04L12/28(2006.01)i

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))

Int.Cl. H04L12/46, 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

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017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 2004-343626 A (住友電気工業株式会社) 2004. 12. 02, 段落 [0030] - [0047], [0049], [0053] (ファミリーなし)	1-7, 9
X	JP 2014-204315 A (株式会社デンソー) 2014. 10. 27, 図 4 (ファミリーなし)	1, 2, 5, 8, 9

☒ 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矛盾するものではなく、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

02. 10. 2017

国際調査報告の発送日

10. 10. 2017

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

上田 翔太

5 X

4449

電話番号 03-3581-1101 内線 3596

C (続き) . 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 2010-98626 A (日立オートモティブシステムズ株式会社) 2010.04.30, 全文、全図 & US 2010/0098095 A1, 全文、全図 & EP 2178257 A1	1-9
A	JP 2014-174778 A (日立オートモティブシステムズ株式会社) 2014.09.22, 全文、全図 & US 2015/0326529 A1, 全文、全図 & WO 2014/141518 A1	1-9
A	JP 2016-134834 A (トヨタ自動車株式会社) 2016.07.25, 全文、全図 (ファミリーなし)	1-9