

(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
2016 年 1 月 21 日(21.01.2016)



(10) 国際公開番号

WO 2016/009812 A1

- (51) 国際特許分類:
H04L 12/28 (2006.01)
- (21) 国際出願番号: PCT/JP2015/068452
- (22) 国際出願日: 2015 年 6 月 26 日(26.06.2015)
- (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 2014-144038 2014 年 7 月 14 日(14.07.2014) JP

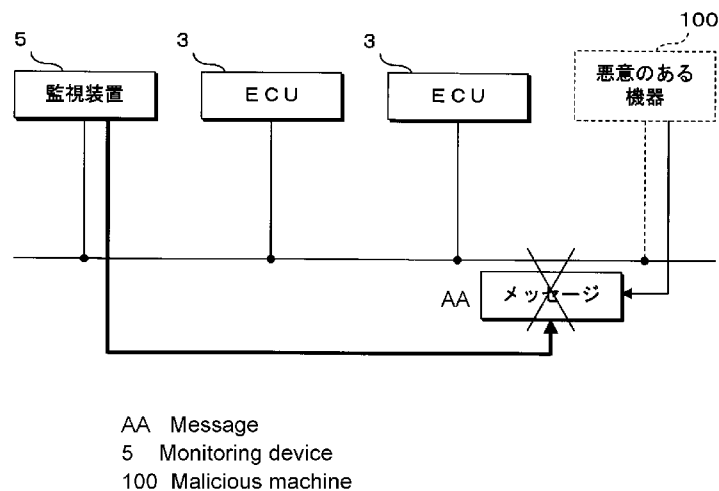
(71) 出願人: 国立大学法人名古屋大学(NATIONAL UNIVERSITY CORPORATION NAGOYA UNIVERSITY) [JP/JP]; 〒4648601 愛知県名古屋市千種区不老町 1 番 Aichi (JP). 株式会社オートネットワーク技術研究所(AUTONETWORKS TECHNOLOGIES, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町 1 番 1 4 号 Mie (JP). 住友電装株式会社(SUMITOMO WIRING SYSTEMS, LTD.) [JP/JP]; 〒5108503 三重県四日市市西末広町 1 番 1 4 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 3 3 号 Osaka (JP).

(72) 発明者: 高田 広章(TAKADA, Hiroaki); 〒4648601 愛知県名古屋市千種区不老町 1 番 国立大学法人名古屋大学内 Aichi (JP). 倉地 亮(KURACHI, Ryo); 〒4648601 愛知県名古屋市千種区不老町 1 番 国立大学法人名古屋大学内 Aichi (JP). 足立直樹(ADACHI, Naoki); 〒5108503 三重県四日市市西末広町 1 番 1 4 号 株式会社オートネットワーク技術研究所内 Mie (JP).

[続葉有]

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION CONTROL DEVICE AND METHOD FOR PREVENTING TRANSMISSION OF INVALID INFORMATION

(54) 発明の名称: 通信システム、通信制御装置及び不正情報送信防止方法



AA Message
5 Monitoring device
100 Malicious machine

(57) Abstract: The present invention offers a communication system, a communication control device and a method for preventing transmission of invalid information, capable of preventing misoperation of a communication device connected to a communication line, even if invalid information is transmitted to the common communication line. A plurality of ECUs 3 and a monitoring device 5 are connected to a common CAN bus. Each ECU 3 outputs, to the CAN bus, transmission frames having authentication information appended to data to be transmitted to other ECUs 3. The monitoring device 5 monitors the transmission of frames to the CAN bus, and when a frame is transmitted, obtains the frame and determines whether or not the authentication information contained in the obtained frame is valid. If the authentication information is not valid, then there is a possibility that the transmission frame is an invalid frame from a malicious machine 100, so the monitoring device 5 outputs an error frame to the CAN bus before the final bit of the EOF of the transmission frame is outputted to the CAN bus, and causes the ECU 3 to destroy the transmission frame.

(57) 要約:

[続葉有]

WO 2016/009812 A1



- (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, CL, CN,
CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG,
ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL,
IN, IR, IS, KE, KG, KN, KP, KR, 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))

共通の通信線に対して不正な情報送信がなされた場合であっても、この通信線に接続された通信装置の誤動作などを防止し得る通信システム、通信制御装置及び不正情報送信防止方法を提供する。共通のCANバスに対して複数のECU3と監視装置5とを接続する。各ECU3は、他のECU3へ送信すべきデータに認証情報を付した送信フレームをCANバスへ出力する。監視装置5は、CANバスに対するフレームの送信を監視しており、フレームの送信が行われた場合にはこれを取得して、取得したフレームに含まれる認証情報の正否を判定する。認証情報が正しいものでない場合、送信フレームが悪意のある機器100による不正なものである可能性があるため、監視装置5は、送信フレームのEOFの最終ビットがCANバスへ出力される前にエラーフレームをCANバスへ出力し、この送信フレームをECU3に破棄させる。

明 細 書

発明の名称：

通信システム、通信制御装置及び不正情報送信防止方法

技術分野

[0001] 本発明は、例えばＥＣＵ（Electronic Control Unit）などの複数の通信装置が共通の通信線で接続された通信システム、このシステムにおいて不正な情報送信を防止する通信制御装置及び不正情報送信防止方法に関する。

背景技術

[0002] 従来、車両に搭載された複数の通信装置間の通信には、ＣＡＮ（Controller Area Network）の通信プロトコルが広く採用されている。ＣＡＮの通信プロトコルでは、共通のＣＡＮバスに複数の通信装置が接続されるため、複数の通信装置が同時的に情報送信を行って衝突が発生した場合には、各通信装置にて調停処理（アービトレーション）が行われ、優先度の高い情報送信が実行される。アービトレーションを行うために、各通信装置は、ＣＡＮバスに送信信号の出力を行うと同時に、ＣＡＮバスの信号レベルの検出を行い、自らが出力した送信信号に対して、検出した信号の信号レベルがレセプブ（劣性値）からドミナント（優性値）に変化した場合、通信の衝突が発生したと判断し、送信処理を停止する。ＣＡＮバス上の信号はレセプブよりドミナントが優位であるため、通信の衝突が発生してもドミナントを出力した電子機器は送信処理を継続して行うことができる。

[0003] 特許文献１においては、分岐接続された２線式ＣＡＮ通信回路の分岐回路毎の異常診断を行う異常診断装置が提案されている。この異常診断装置は、ＣＡＮ通信線の各分岐回路とコネクタ接続される検査用の分岐回路と、該分岐回路を接続するジョイント回路を有する分岐接続回路と、各分岐回路をジョイント回路から切り離す分離手段と、前記分離手段で切り離された分岐回路の電位を測定する電位測定手段と、前記電位測定手段と前記分岐回路とを接続する接続手段と、前記電位測定手段と接続し、測定された電位より異常

判定を行う異常判定手段とを備えている。

先行技術文献

特許文献

[0004] 特許文献1：特開 2 0 1 0 － 1 1 1 2 9 5 号公報

発明の概要

発明が解決しようとする課題

[0005] 車両のCANバスには、悪意のある機器が接続される可能性がある。悪意のある機器は、例えばCANバスに対して不正な情報送信を繰り返し行うことによって、このCANバスに接続された他のECUを誤動作させる虞がある。

[0006] 本発明は、斯かる事情に鑑みてなされたものであって、その目的とするところは、共通の通信線に対して不正な情報送信がなされた場合であっても、この通信線に接続された通信装置の誤動作などを防止し得る通信システム、通信制御装置及び不正情報送信防止方法を提供することにある。

課題を解決するための手段

[0007] 本発明に係る通信システムは、複数の通信装置が共通の通信線を介して接続された通信システムにおいて、前記通信装置は、他の通信装置へ送信する情報に認証情報を付与する認証情報付与手段と、該認証情報付与手段により前記認証情報が付された送信情報を前記通信線へ出力し、該送信情報を他の通信装置へ送信する情報送信手段とを有し、前記通信線に接続され、前記通信線へ出力された送信情報を取得する取得手段、該取得手段が取得した送信情報に含まれる認証情報が正しいものであるか否かを判定する認証情報判定手段、及び、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に前記送信情報を前記通信装置に破棄させる情報破棄手段を有する通信制御装置を備え、前記通信制御装置の前記情報破棄手段は、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に所定の情報を前記通信線へ出力し、前記他の通信装置は、前記通信線より前記所定の

情報を受信した場合、前記通信装置から送信された前記送信情報を破棄するようにしてあることを特徴とする。

[0008] また、本発明に係る通信システムは、前記通信制御装置の情報破棄手段は、前記通信装置の情報送信手段が送信情報の全てを前記通信線へ出力し終える前に、前記所定の情報を前記通信線へ出力することにより、前記送信情報を破棄させるようにしてあることを特徴とする。

[0009] また、本発明に係る通信システムは、前記通信装置及び前記通信制御装置が、鍵情報を共有し、前記通信装置の認証情報付与手段は、前記鍵情報に基づいて認証情報を生成して送信情報へ付与し、前記通信制御装置の前記認証情報判定手段は、前記鍵情報に基づいて前記送信情報に含まれる前記認証情報の判定を行うようにしてあることを特徴とする。

[0010] また、本発明に係る通信システムは、前記複数の通信装置が、それぞれ異なる前記鍵情報を有し、前記通信制御装置は、各通信装置の前記鍵情報を有していることを特徴とする。

[0011] また、本発明に係る通信制御装置は、複数の通信装置が接続された共通の通信線に接続され、前記通信線へ出力された送信情報を取得する取得手段と、該取得手段が取得した送信情報に含まれる認証情報が正しいものであるかを判定する認証情報判定手段と、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に前記送信情報を前記通信装置に破棄させる情報破棄手段とを備え、前記情報破棄手段は、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に所定の情報を前記通信線へ出力するようにしてあることを特徴とする。

[0012] また、本発明に係る不正情報送信防止方法は、複数の通信装置が共通の通信線を介して接続された通信システムにて、前記通信線に対する不正な情報送信を防止する不正情報送信防止方法であって、前記通信装置は、他の通信装置へ送信する情報に認証情報を付与して前記通信線へ出力し、前記通信線へ出力された送信情報を通信制御装置が取得し、取得した送信情報に含まれる認証情報が正しいものであるかを前記通信制御装置が判定し、前記認

証情報が正しいものでないと判定した場合に前記通信制御装置が所定の情報を前記通信線へ出力し、前記他の通信装置は、前記通信線より前記所定の情報を受信した場合、前記通信装置から送信された前記送信情報を破棄することを特徴とする。

[0013] 本発明においては、共通の通信線に対して複数の通信装置と通信制御装置とを接続する。各通信装置は、送信情報に認証情報を付与して通信線へ出力することにより、他の通信装置への情報送信を行う。なお本発明では、他の通信装置からの情報を受信した通信装置は、受信情報に含まれる認証情報の正否を判定する必要はない。

通信制御装置は、通信線に対する情報の送信を監視しており、情報の送信が行われた場合には送信情報を取得して、取得した情報に含まれる認証情報の正否を判定する。認証情報が正しいものであれば、通信制御装置は、この情報送信に対して何ら処理を行う必要はない。認証情報が正しいものでない場合、送信情報が悪意のある機器による不正なものである可能性があるため、通信制御装置は、通信装置に破棄させる処理を行う。

これにより、各通信装置では認証情報の正否を判定することなく、不正な情報が各通信装置にて受信されることを防止できる。

[0014] また本発明においては、送信情報を破棄させるため、通信装置が送信情報の全てを通信線へ出力し終える前に、通信制御装置が所定の情報を通信線へ出力する。これにより送信情報が正規のものではなくなり、各通信装置はこの情報の受信を中止するため、送信情報が破棄される。

[0015] また本発明においては、通信装置及び通信制御装置が鍵情報を共有し、認証情報の生成及び判定等の処理を行う。これにより、鍵情報を有していない悪意のある機器は認証情報を生成することができないため、通信制御装置がより確実に不正な情報送信を防止することができる。

[0016] また本発明においては、通信システムに含まれる複数の通信装置は、それぞれ異なる鍵情報を有する。これにより鍵情報の漏えいなどによる悪影響を低減することができる。各通信装置は、他の通信装置の送信情報に含まれる

認証情報の判定を行う必要がないため、他の通信装置の鍵情報を有している必要はない。これに対して通信制御装置は、送信情報の破棄を行う対象とすべき全ての通信装置についての鍵情報を有している。通信制御装置は、情報の送信元の通信装置に対応する鍵情報を用いて送信情報に含まれる認証情報の正否を判定する。

発明の効果

[0017] 本発明による場合は、通信装置が送信情報に付した認証情報に基づいて通信制御装置が送信情報の正否を判定し、送信情報が正しいものでない場合には通信制御装置がこの情報を通信装置に破棄させる構成とすることにより、悪意のある機器により共通の通信線に対して不正な情報送信がなされた場合であっても、送信された情報を破棄させることで通信装置が誤動作することを防止できる。

図面の簡単な説明

[0018] [図1]本実施の形態に係る通信システムの構成を示す模式図である。
[図2]E C Uの構成を示すブロック図である。
[図3]監視装置の構成を示すブロック図である。
[図4]鍵情報テーブルの構成を説明する模式図である。
[図5]本実施の形態に係る通信システムの監視処理の概要を説明するための模式図である。
[図6]各E C Uによる送信フレームの生成方法を説明するための模式図である。
[図7]E C Uが行う情報送信処理の手順を示すフローチャートである。
[図8]監視装置が行う監視処理の手順を示すフローチャートである。
[図9]監視装置が行う監視処理の手順を示すフローチャートである。
[図10]E C Uが行う情報受信処理の手順を示すフローチャートである。

発明を実施するための形態

[0019] <システム構成>

図1は、本実施の形態に係る通信システムの構成を示す模式図である。本

実施の形態に係る通信システムは、車両 1 に搭載された複数の ECU 3 と、1 つの監視装置 5 とを備えて構成されている。ECU 3 及び監視装置 5 は、車両 1 に敷設された共通の通信線を介して接続され、相互にデータを送受信することができる。本実施の形態においては、この通信線を CAN バスとし、ECU 3 及び監視装置 5 は、CAN プロトコルに従った通信を行う。ECU 3 は、例えば車両 1 のエンジンの制御を行うエンジン ECU、車体の電装品の制御を行うボディ ECU、ABS (Antilock Brake System) に関する制御を行う ABS-ECU、又は、車両 1 のエアバッグの制御を行うエアバッグ ECU 等のように、種々の電子制御装置であってよい。監視装置 5 は、車内ネットワークに対する不正なデータ送信を監視する装置である。監視装置 5 は、監視専用の装置として設けられてもよく、例えばゲートウェイなどの装置に監視の機能を付加した構成であってもよく、また例えばいずれか 1 つの ECU 3 に監視の機能を付加した構成であってもよい。

[0020] 図 2 は、ECU 3 の構成を示すブロック図である。なお図 2 においては、車両 1 に設けられた ECU 3 について、通信及び不正監視等に関するブロックを抜き出して図示してある。これらのブロックは各 ECU 3 に共通である。本実施の形態に係る ECU 3 は、処理部 31、記憶部 32 及び CAN 通信部 33 等を備えて構成されている。処理部 31 は、CPU (Central Processing Unit) 又は MPU (Micro-Processing Unit) 等の演算処理装置を用いて構成されている。処理部 31 は、記憶部 32 などに記憶されたプログラムを読み出して実行することにより、車両 1 に係る種々の情報処理又は制御処理等を行う。

[0021] 記憶部 32 は、フラッシュメモリ又は EEPROM (Electrically Erasable Programmable ROM) 等の不揮発性のメモリ素子を用いて構成されている。記憶部 32 は、処理部 31 が実行するプログラム、及び、これにより行われる処理に必要な種々のデータが記憶されている。なお記憶部 32 に記憶されるプログラム及びデータは、ECU 3 毎に異なる。また本実施の形態において記憶部 32 は、処理部 31 が行う認証情報の生成処理に用いられる鍵情報

3 2 a が記憶されている。本実施の形態においては C A N バスに複数の E C U 3 が接続されているが、各 E C U 3 が記憶部 3 2 に記憶する鍵情報 3 2 a は、それぞれ異なるものであってもよい。

[0022] C A N 通信部 3 3 は、C A N の通信プロトコルに従って、C A N バスを介した他の E C U 3 又は監視装置 5 との通信を行う。C A N 通信部 3 3 は、処理部 3 1 から与えられた送信用の情報を、C A N の通信プロトコルに従った送信信号に変換し、変換した信号を C A N バスへ出力することで他の E C U 3 又は監視装置 5 への情報送信を行う。C A N 通信部 3 3 は、C A N バスの電位をサンプリングすることによって、他の E C U 3 又は監視装置 5 が出力した信号を取得し、この信号を C A N の通信プロトコルに従って 2 値の情報に変換することで情報の受信を行い、受信した情報を処理部 3 1 へ与える。

[0023] 本実施の形態において E C U 3 の処理部 3 1 には、認証情報生成部 4 1 及び送信フレーム生成部 4 2 等が設けられている。認証情報生成部 4 1 及び送信フレーム生成部 4 2 は、ハードウェアの機能ブロックとして構成されるものであってもよく、ソフトウェアの機能ブロックとして構成されるものであってもよい。認証情報生成部 4 1 は、他の E C U 3 へ送信すべき情報と記憶部 3 2 の鍵情報 3 2 a とを用いて認証情報を生成する処理を行う。送信フレーム生成部 4 2 は、他の E C U 3 へ送信すべき情報及び認証情報生成部 4 1 が生成した認証情報を基に、本実施の形態における通信に適した送信用のフレーム（メッセージ）を生成する処理を行う。送信フレーム生成部 4 2 が生成した送信フレームを C A N 通信部 3 3 へ与えることにより、他の E C U 3 への情報送信を行うことができる。

[0024] 図 3 は、監視装置 5 の構成を示すブロック図である。監視装置 5 は、処理部 5 1、記憶部 5 2 及び C A N 通信部 5 3 等を備えて構成されている。処理部 5 1 は、C P U 又は M P U 等の演算処理装置を用いて構成され、記憶部 5 2 に記憶されたプログラムを読み出して実行することにより、車両 1 の E C U 3 の挙動及び通信等を監視する処理を行う。

[0025] 記憶部 5 2 は、フラッシュメモリ又は E E P R O M 等のデータ書き換え可

能な不揮発性のメモリ素子を用いて構成されている。本実施の形態において記憶部52は、CANバスに接続された全てのECU3の鍵情報を含む鍵情報テーブル52aを記憶している。図4は、鍵情報テーブル52aの構成を説明する模式図である。監視装置5が記憶部52に記憶する鍵情報テーブル52aは、各ECU3を識別し得るIDと、ECU3が有する鍵情報とが対応付けられている。本実施の形態において各ECU3が送信する送信フレームには、IDが含まれている。各ECU3には予め又は複数のIDがそれぞれ割り当てられており、2つ以上のECU3に対して同一のIDが割り当てられることはないものとする。監視装置5は、ECU3の送信フレームに含まれるIDに基づいて、鍵情報テーブル52aから1つの鍵情報を取得することができる。

[0026] CAN通信部53は、CANの通信プロトコルに従って、CANバスを介したECU3との通信を行う。CAN通信部53は、処理部51から与えられた送信用の情報を、CANの通信プロトコルに従った送信信号に変換し、変換した信号をCANバスへ出力することでECU3への情報送信を行う。CAN通信部53は、CANバスの電位をサンプリングすることによって、ECU3が出力した信号を取得し、この信号をCANの通信プロトコルに従って2値の情報に変換することで情報の受信を行い、受信した情報を処理部51へ与える。

[0027] 本実施の形態において監視装置5の処理部51には、認証情報判定部61及び送信情報破棄処理部62等が設けられている。認証情報判定部61及び送信情報破棄処理部62は、ハードウェアの機能ブロックとして構成されるものであってもよく、ソフトウェアの機能ブロックとして構成されるものであってもよい。認証情報判定部61は、ECU3が送信した送信フレームに含まれる認証情報が正しいものであるか否かを判定する処理を行う。送信情報破棄処理部62は、不正な送信フレームを検出した場合に、各ECU3にこの送信フレームを破棄させるための処理を行う。

[0028] <監視処理>

本実施の形態に係る通信システムは、CANバスに対する不正な情報送信を監視する機能を有している。図5は、本実施の形態に係る通信システムの監視処理の概要を説明するための模式図である。車両1のCANバスに対しては、悪意のある機器100（図5において破線で示す）が不正に接続される可能性がある。悪意のある機器100は、例えば不正なメッセージをCANバスに対して送信する。不正なメッセージには、例えば正規のECU3を誤動作させるような制御指示又はセンサ検知結果等を含む可能性がある。本実施の形態に係る監視装置5は、CANバスに対するメッセージ送信を監視している。監視装置5は、CANバスに対してメッセージが送信された場合、このメッセージが正規のECU3が送信したものであるか否かを判定する。メッセージが不正なものであると判定した場合、監視装置5は、悪意のある機器100によるメッセージ送信が完了する前に（ECU3によるメッセージ受信が完了する前に）、CANバスに対して所定の信号を出力することによって、ECU3にこのメッセージを破棄させる。

[0029] 図6は、各ECU3による送信フレームの生成方法を説明するための模式図である。本実施の形態に係る通信システムにて送受信されるフレーム（メッセージ）には、CANヘッダ、データフィールド、認証情報、CRC（Cyclic Redundancy Check）フィールド、ACKフィールド及びEOF（End of Frame）を含んで構成されている。CANヘッダは、従来のCANプロトコルにおけるSOF（Start of Frame）、アービトレーションフィールド及びコントロールフィールド等を含むものであり、上述したECU3を識別し得るIDを含んでいる。データフィールドは、例えばECU3に対する制御指示又はセンサ検知結果等のように、ECU3間で授受すべき情報の本体が格納される。

[0030] CRCフィールド、ACKフィールド及びEOFは、従来のCANプロトコルにて用いられるものと同じであるため詳細な説明は省略する。CRCフィールドは、誤り検出を行うための情報を格納する。ACKフィールドは、このフレームを受信するECU3による受信応答のためのフィールドである

。E O Fは、フィールドの終了を示す特定のビット列である。

[0031] 本実施の形態に係るフレームには、従来のC A Nプロトコルと互換するものの、一部に認証情報を含んでいる。認証情報は、このフレームが正当なものであるか否かを監視装置5が判定するために用いられる情報である。E C U 3の認証情報生成部4 1は、送信フレームに含まれるC A Nヘッダ及びデータを、記憶部3 2に記憶した鍵情報3 2 aを用いて暗号化することにより認証情報を生成する。本実施の形態においては、例えばH M A C (S H A - 2 5 6)のアルゴリズムを用いて、5 1 2ビット程度の鍵情報3 2 aに基づき、2 5 6ビットのメッセージ認証符号(M A C)を生成する。E C U 3の送信フレーム生成部4 2は、認証情報生成部4 1が生成した2 5 6ビットのM A Cを認証情報として送信フレームに付し、C A N通信部3 3へ送信フレームを与えることで、他のE C U 3へのフレームの送信を行う。

[0032] なお本実施の形態において、図6に示したフレームを受信したE C U 3は、受信フレームに含まれる認証情報の正否を確認する必要はない。このため各E C U 3は、他のE C U 3と鍵情報を共有していない。

[0033] E C U 3のC A N通信部3 3は、送信フレームを構成する複数ビットの情報を、C A Nヘッダ側からE O Fまで順にC A Nバスへ出力する。監視装置5は、C A Nバスへ出力された情報を順次取得し、送信フレームのC R Cフィールドまでを取得した際に、C R Cフィールドの情報に基づく誤り検出を行う。送信フレームに誤りがない場合、監視装置5の認証情報判定部6 1は、送信フレームに含まれる認証情報の正否を判定する。認証情報判定部6 1は、受信済みのC A NヘッダからI Dを取得して記憶部5 2の鍵情報テーブル5 2 aを参照し、I Dに対応する鍵情報を取得する。認証情報判定部6 1は、取得した鍵情報と、受信済みのC A Nヘッダ及びデータフィールドとに基づき、E C U 3の認証情報生成部4 1と同じアルゴリズムにより認証情報を生成する。認証情報判定部6 1は、自らが生成した認証情報と、C A Nバスに送信された送信フレームに含まれる認証情報とを比較し、両認証情報が一致した場合にこの送信フレームが正当なものであると判定する。両認証情

報が一致しない場合、認証情報判定部 61 は、送信フレームが正当なものではないと判定する。なお認証情報判定部 61 は、送信フレームの CRC フィールドの最終ビットが CAN バスに出力されてから、EOF の最終ビットが CAN バスに出力されるまでの間に判定処理を完了する。

[0034] CAN バスに出力された送信フレームが正当なものではないと認証情報判定部 61 が判定した場合、監視装置 5 の送信情報破棄処理部 62 は、CAN バスに接続された ECU 3 にこの送信フレームを破棄させるための処理を行う。送信情報破棄処理部 62 は、この送信フレームの EOF の出力期間中に、CAN バスに対してエラーフレームを送信する。このエラーフレームにより、CAN バスに接続された全ての ECU 3 は、受信中の不正なフレームを破棄する。

[0035] <フローチャート>

以下、本実施の形態に係る通信システムの ECU 3 及び監視装置 5 が行う処理を、フローチャートを用いて説明する。図 7 は、ECU 3 が行う情報送信処理の手順を示すフローチャートである。ECU 3 の処理部 31 は、自らに与えられた ID 及びセンサの検知結果など他の ECU 3 へ送信すべき情報等に基づき、CAN ヘッダ及びデータフィールドを生成する（ステップ S1）。処理部 31 の認証情報生成部 41 は、記憶部 32 に記憶された鍵情報 32a を読み出す（ステップ S2）。認証情報生成部 41 は、ステップ S1 にて生成した CAN ヘッダ及びデータフィールドと、ステップ S2 にて読み出した鍵情報 32a とに基づいて、所定のアルゴリズムにより認証情報を生成する（ステップ S3）。処理部 31 は、CAN ヘッダ、データフィールド及び認証情報に対する誤り検出を行うための CRC フィールドを生成する（ステップ S4）。処理部 31 は、これまでに生成した CAN ヘッダ、データフィールド、認証情報及び CRC フィールドを結合して送信フレームを生成し（ステップ S5）、CAN 通信部 33 へ与える。

[0036] ECU 3 の CAN 通信部 33 は、送信フレームの CAN ヘッダから送信を開始する。CAN 通信部 33 は、送信フレームの未送信部分から 1 ビットを

取得し、この1ビットに応じた信号をCANバスへ出力する（ステップS6）。CAN通信部33は、例えばアービトレーションによる送信停止など、送信処理を中断する要因が発生したか否かを判定する（ステップS7）。中断要因が発生した場合（S7：YES）、CAN通信部33は、エラー処理などを行って（ステップS8）、情報送信処理を終了する。中断要因が発生していない場合（S7：NO）、CAN通信部33は、与えられた送信フレームの全ビットについて出力を完了したか否かを判定する（ステップS9）。全ビットの出力を完了していない場合（S9：NO）、CAN通信部33は、ステップS6へ処理を戻し、送信フレームの次のビットの出力を行う。全ビットの出力を完了している場合（S9：YES）、CAN通信部33は、情報送信処理を終了する。

[0037] 図8及び図9は、監視装置5が行う監視処理の手順を示すフローチャートである。監視装置5のCAN通信部53は、CANバスの電位を周期的にサンプリングしている。CAN通信部53は、CANバスの電位変化に基づき、CANバスに対する情報送信が開始されたか否かを判定する（ステップS21）。情報送信が開始されていない場合（S21：NO）、CAN通信部53は、情報送信が開始されるまで待機する。情報送信が開始された場合（S21：YES）、CAN通信部53は、CANバスの電位に基づいて送信フレームの1ビットを取得する（ステップS22）。CAN通信部53は、取得した1ビットがCRCフィールドの最終ビットに相当するものであるか否かを判定する（ステップS23）。CRCフィールドの最終ビットでない場合（S23：NO）、CAN通信部53は、ステップS22へ処理を戻し、送信フレームの各ビットの取得を繰り返して行う。CRCフィールドの最終ビットである場合（S23：YES）、CAN通信部53は、これまでに取得した情報を処理部51へ与える。

[0038] 処理部51は、CAN通信部53から与えられた情報（送信フレーム）を基に、CRCフィールドの判定を行う（ステップS24）。処理部51は、送信フレームのCANヘッダ～認証情報に基づいて算出したCRCと、送信

フレームのCRCフィールドに格納されたCRCとの値を比較することで、送信フレームに誤りがあるか否かを判定する（ステップS25）。送信フレームに誤りがある場合（S25：YES）、処理部51は、処理を終了する。なおCRCフィールドに基づいて送信フレームに誤りがあると判断される場合、他のECU3においても同様の判断がなされ、この送信フレームは各ECU3において破棄される。

[0039] 送信フレームに誤りがない場合（S25：NO）、処理部51の認証情報判定部61は、送信フレームのCANヘッダに含まれるIDを取得する（ステップS26）。認証情報判定部61は、取得したIDを基に記憶部52の鍵情報テーブル52aを参照し、IDに対応する鍵情報を取得する（ステップS27）。認証情報判定部61は、取得した送信フレームのCANヘッダ及びデータフィールドと、ステップS27にて取得した鍵情報とに基づいて、所定のアルゴリズムにより認証情報を生成する（ステップS28）。認証情報判定部61は、送信フレームから認証情報を取得し（ステップS29）、取得した認証情報と、ステップS28にて生成した認証情報とが一致するか否かを判定する（ステップS30）。両認証情報が一致する場合（S30：YES）、処理部51は、処理を終了する。両認証情報が一致しない場合（S30：NO）、処理部51の送信情報破棄処理部62は、CAN通信部53にてエラーフレームをCANバスへ出力し（ステップS31）、処理を終了する。

[0040] 図10は、ECU3が行う情報受信処理の手順を示すフローチャートである。ECU3のCAN通信部33は、まず、CANバスに対して出力された送信フレームを1ビットずつ取得していき、送信フレームのCANヘッダからACKフィールドまでの受信処理を行う（ステップS41）。なお図示は省略するが、ECU3は、CRCフィールドまで受信した際に誤りの有無を検知する処理を行う。

[0041] その後、CAN通信部33は、CANバスに対して出力された送信フレームのEOFの1ビットを取得する（ステップS42）。CAN通信部33は

、取得した1ビットがE O Fではなく監視装置5が出力したエラーフレームであるか否かを判定する（ステップS 4 3）。エラーフレームである場合（S 4 3 : Y E S）、C A N通信部3 3は、これまでに受信したフレームを破棄して（ステップS 4 4）、受信処理を終了する。

[0042] エラーフレームでない場合（S 4 3 : N O）、C A N通信部3 3は、E O Fの受信を完了したか否かを判定する（ステップS 4 5）。E O Fの受信を完了していない場合（S 4 5 : N O）、C A N通信部3 3は、ステップS 4 2へ処理を戻し、E O Fの受信を継続する。E O Fの受信を完了した場合（S 4 5 : Y E S）、処理部3 1は、C A N通信部3 3が受信したフレームのデータフィールドから必要なデータを取得し（ステップS 4 6）、取得したデータに応じた処理を行って（ステップS 4 7）、処理を終了する。

[0043] <まとめ>

以上の構成の本実施の形態に係る通信システムは、共通のC A Nバスに対して複数のE C U 3と監視装置5とを接続する。各E C U 3は、他のE C U 3へ送信すべきデータに認証情報を付した送信フレームをC A N通信部3 3にてC A Nバスへ出力することにより、他のE C U 3への情報送信を行う。なお本実施の形態においては、他のE C U 3からのフレームを受信したE C U 3は、受信フレームに含まれる認証情報の正否を判定する必要はない。監視装置5は、C A Nバスに対するフレームの送信を監視しており、フレームの送信が行われた場合にはこれを取得して、取得したフレームに含まれる認証情報の正否を判定する。認証情報が正しいものであれば、監視装置5は、このフレームに対して何ら処理を行う必要はない。認証情報が正しいものではない場合、送信フレームが悪意のある機器1 0 0による不正なものである可能性があるため、監視装置5は、この送信フレームをE C U 3に破棄させる処理を行う。これにより、各E C U 3では認証情報の正否を判定することなく、不正なフレームが各E C U 3にて受信されることを防止できる。

[0044] また本実施の形態においては、各E C U 3に送信フレームを破棄させるため、送信フレームのE O Fの最終ビットがC A Nバスへ出力される前に、監

視装置 5 がエラーフレームを C A N バスへ出力する。これにより各 E C U 3 は、この送信フレームの受信を中止し、送信フレームが破棄される。

[0045] また本実施の形態においては、監視装置 5 と E C U 3 とが鍵情報を共有し、認証情報の生成及び判定を行う。これにより鍵情報を有していない悪意のある機器 1 0 0 は認証情報を生成することができないため、不正なフレームの送信を監視装置 5 がより確実に防止することができる。

[0046] また本実施の形態においては、C A N バスに接続された複数の E C U 3 は、それぞれ異なる鍵情報を有している。これにより鍵情報の漏えいなどによる悪影響を低減することができる。各 E C U 3 は、他の E C U 3 の送信フレームに含まれる認証情報の正否を判定する必要があるため、他の E C U 3 の鍵情報を有している必要はない。これに対して監視装置 5 は、全ての E C U 3 についての鍵情報を有しており、記憶部 5 2 に鍵情報テーブル 5 2 a として管理している。監視装置 5 は、送信フレームに含まれる I D に基づいて送信元の E C U 3 を判別し、対応する鍵情報を鍵情報テーブル 5 2 a から読み出して、送信フレームに含まれる認証情報の正否を判定することができる。

[0047] なお本実施の形態においては、E C U 3 及び監視装置 5 が C A N のプロトコルに従った通信を行う構成としたが、これに限るものではなく、C A N 以外のプロトコルによる通信を行う構成としてもよい。また本実施の形態においては、車両 1 に搭載された通信システムを例に説明を行ったが、通信システムは車両 1 に搭載されるものに限らず、例えば飛行機又は船舶等の移動体に搭載されるものであってよく、また例えば移動体ではなく工場、オフィス又は学校等に設置されるものであってもよい。また本実施の形態にて示したフレームの構成は、一例であって、これに限るものではない。また通信システム中に監視装置 5 を設けるのではなく、いずれか 1 つの E C U 3 が本実施の形態に係る監視装置 5 の監視機能を備える構成であってもよい。また E C U 3 及び監視装置 5 の間での鍵情報の共有方法は、どのような方法を採用してもよい。また E C U 3 及び監視装置 5 が鍵情報を用いて行う暗号処理は、どのようなアルゴリズムのものであってもよい。また認証情報の生成処理及

び送信フレーム破棄の処理等を処理部 5 1 が行う構成としたが、これに限るものではなく、その一部又は全部の処理を C A N 通信部 5 3 が行う構成としてもよい。

符号の説明

- [0048]
- 1 車両
 - 3 ECU
 - 5 監視装置
 - 3 1 処理部
 - 3 2 記憶部
 - 3 2 a 鍵情報
 - 3 3 C A N 通信部
 - 4 1 認証情報生成部
 - 4 2 送信フレーム生成部
 - 5 1 処理部
 - 5 2 記憶部
 - 5 2 a 鍵情報テーブル
 - 5 3 C A N 通信部
 - 6 1 認証情報判定部
 - 6 2 送信情報破棄処理部
 - 1 0 0 悪意のある機器

請求の範囲

- [請求項1] 複数の通信装置が共通の通信線を介して接続された通信システムにおいて、
- 前記通信装置は、
- 他の通信装置へ送信する情報に認証情報を付与する認証情報付与手段と、
- 該認証情報付与手段により前記認証情報が付された送信情報を前記通信線へ出力し、該送信情報を他の通信装置へ送信する情報送信手段と
- を有し、
- 前記通信線に接続され、前記通信線へ出力された送信情報を取得する取得手段、該取得手段が取得した送信情報に含まれる認証情報が正しいものであるか否かを判定する認証情報判定手段、及び、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に前記送信情報を前記通信装置に破棄させる情報破棄手段を有する通信制御装置を備え、
- 前記通信制御装置の前記情報破棄手段は、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に所定の情報を前記通信線へ出力し、
- 前記他の通信装置は、前記通信線より前記所定の情報を受信した場合、前記通信装置から送信された前記送信情報を破棄するようにしてあること
- を特徴とする通信システム。
- [請求項2] 前記通信制御装置の情報破棄手段は、前記通信装置の情報送信手段が送信情報の全てを前記通信線へ出力し終える前に、前記所定の情報を前記通信線へ出力することにより、前記送信情報を破棄させるようにしてあること
- を特徴とする請求項1に記載の通信システム。

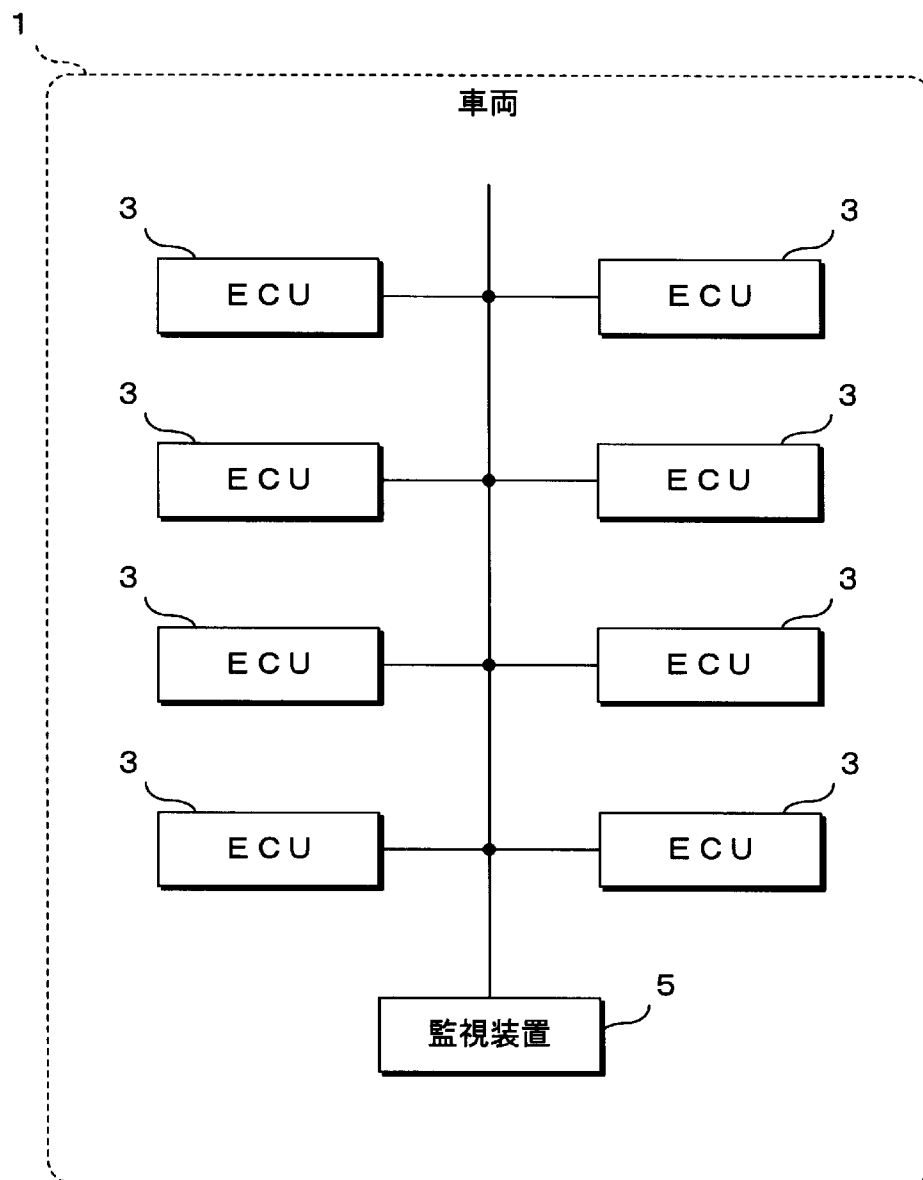
- [請求項3] 前記通信装置及び前記通信制御装置は、鍵情報を共有し、
前記通信装置の認証情報付与手段は、前記鍵情報に基づいて認証情報を生成して送信情報へ付与し、
前記通信制御装置の前記認証情報判定手段は、前記鍵情報に基づいて前記送信情報に含まれる前記認証情報の判定を行うようにしてあること
を特徴とする請求項1又は請求項2に記載の通信システム。
- [請求項4] 前記複数の通信装置は、それぞれ異なる前記鍵情報を有し、
前記通信制御装置は、各通信装置の前記鍵情報を有していること
を特徴とする請求項3に記載の通信システム。
- [請求項5] 複数の通信装置が接続された共通の通信線に接続され、
前記通信線へ出力された送信情報を取得する取得手段と、
該取得手段が取得した送信情報に含まれる認証情報が正しいものであるか否かを判定する認証情報判定手段と、
前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に前記送信情報を前記通信装置に破棄させる情報破棄手段と
を備え、
前記情報破棄手段は、前記認証情報が正しいものでないと前記認証情報判定手段が判定した場合に所定の情報を前記通信線へ出力するようにしてあること
を特徴とする通信制御装置。
- [請求項6] 複数の通信装置が共通の通信線を介して接続された通信システムにて、前記通信線に対する不正な情報送信を防止する不正情報送信防止方法であって、
前記通信装置は、他の通信装置へ送信する情報に認証情報を付与して前記通信線へ出力し、
前記通信線へ出力された送信情報を通信制御装置が取得し、
取得した送信情報に含まれる認証情報が正しいものであるか否かを

前記通信制御装置が判定し、

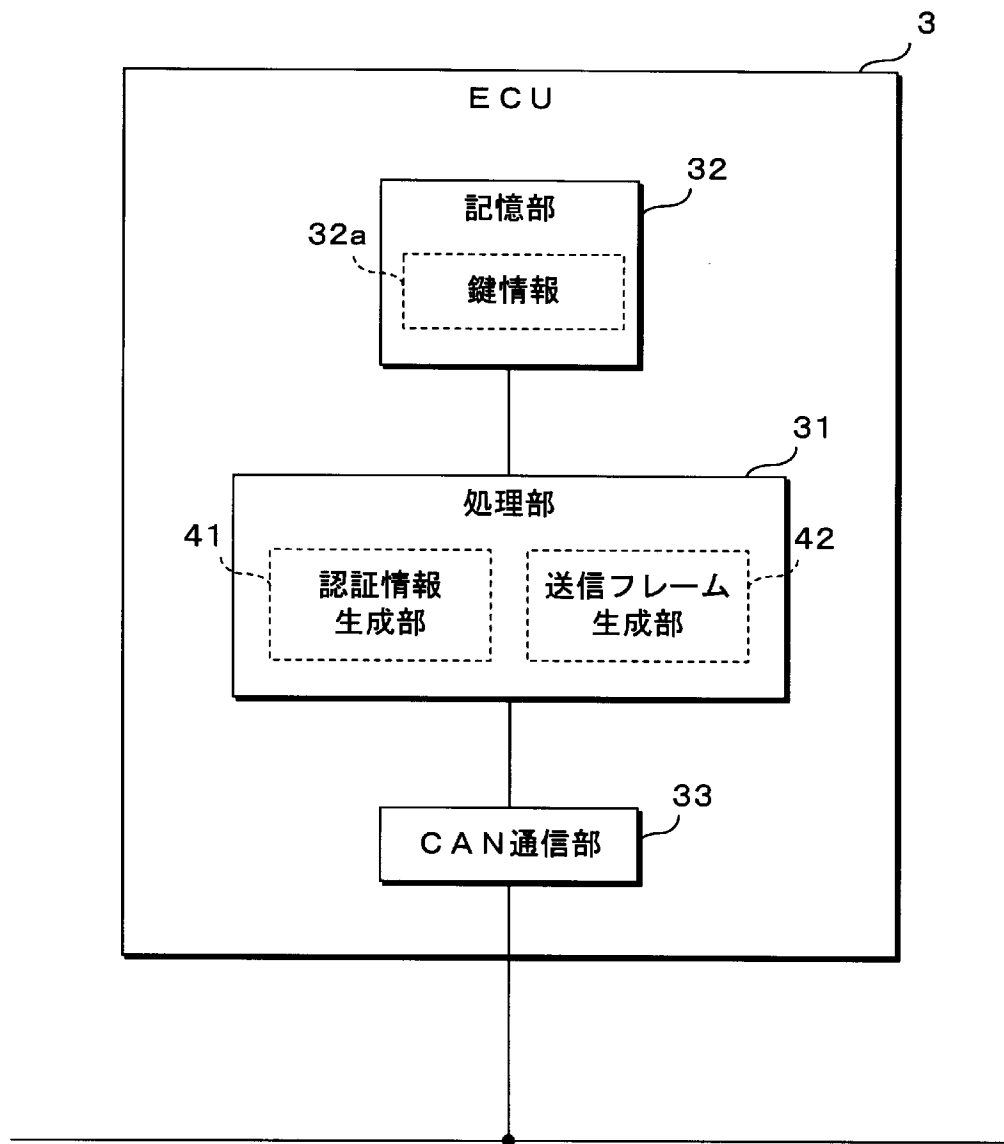
前記認証情報が正しいものでないと判定した場合に前記通信制御装置が所定の情報を前記通信線へ出力し、

前記他の通信装置は、前記通信線より前記所定の情報を受信した場合、前記通信装置から送信された前記送信情報を破棄することを特徴とする不正情報送信防止方法。

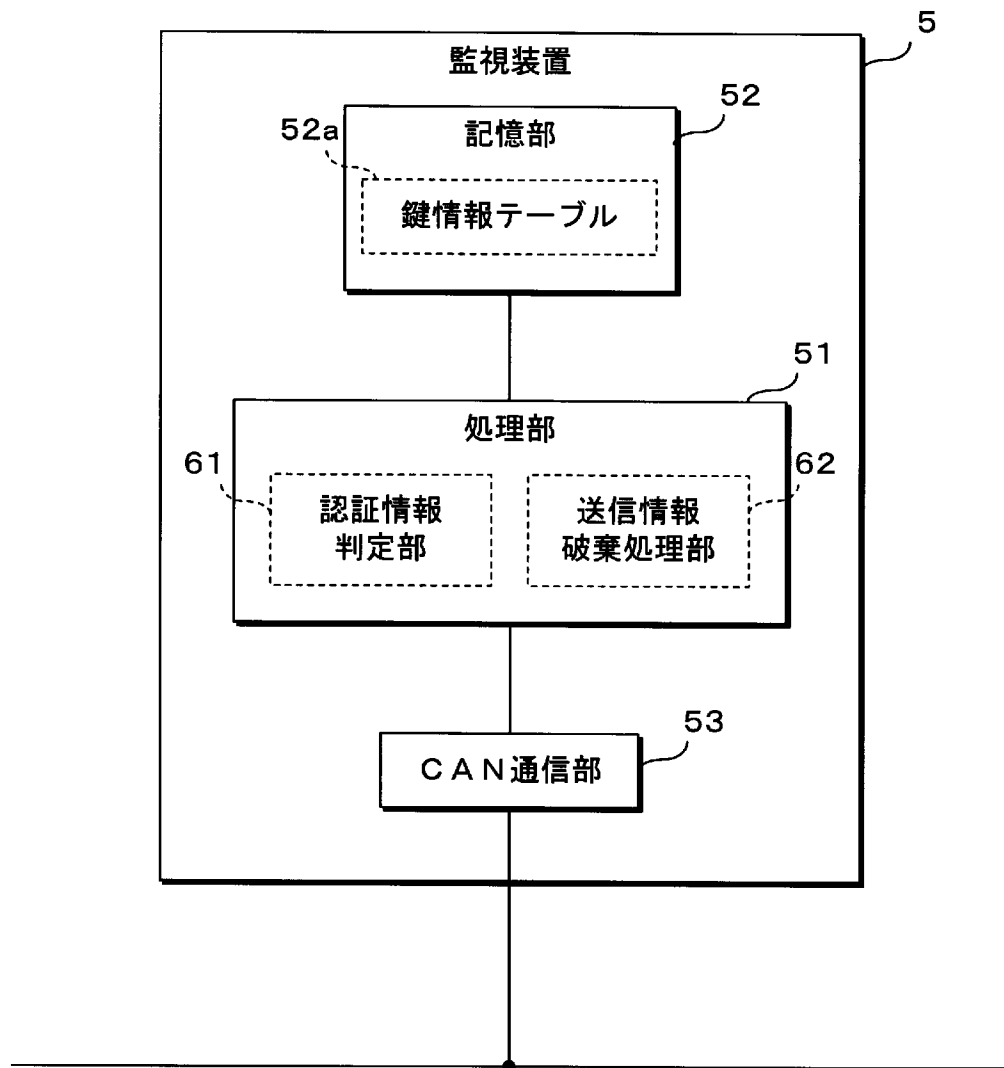
[図1]



[図2]



[図3]

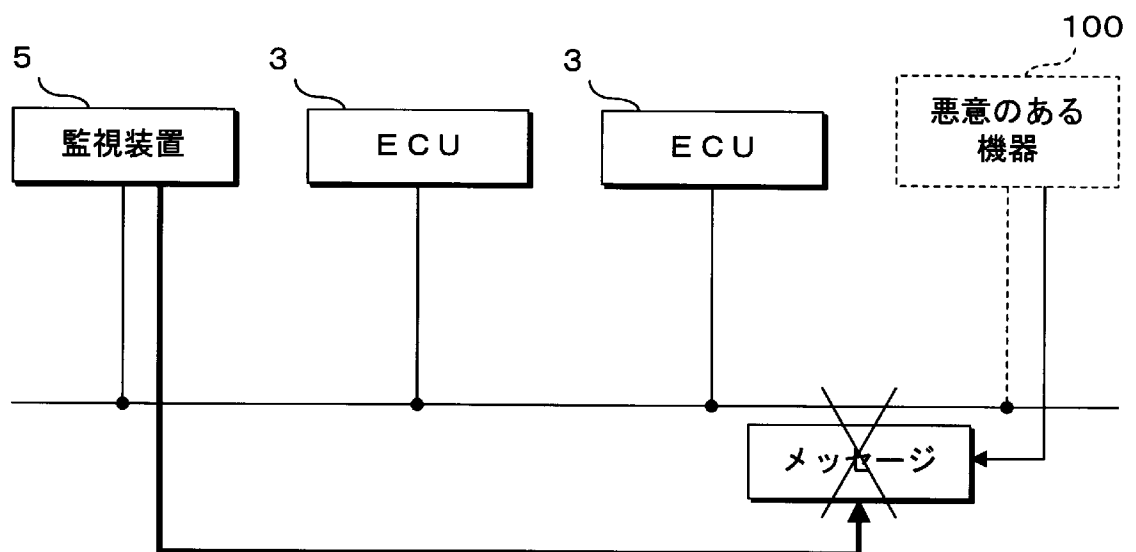


[図4]

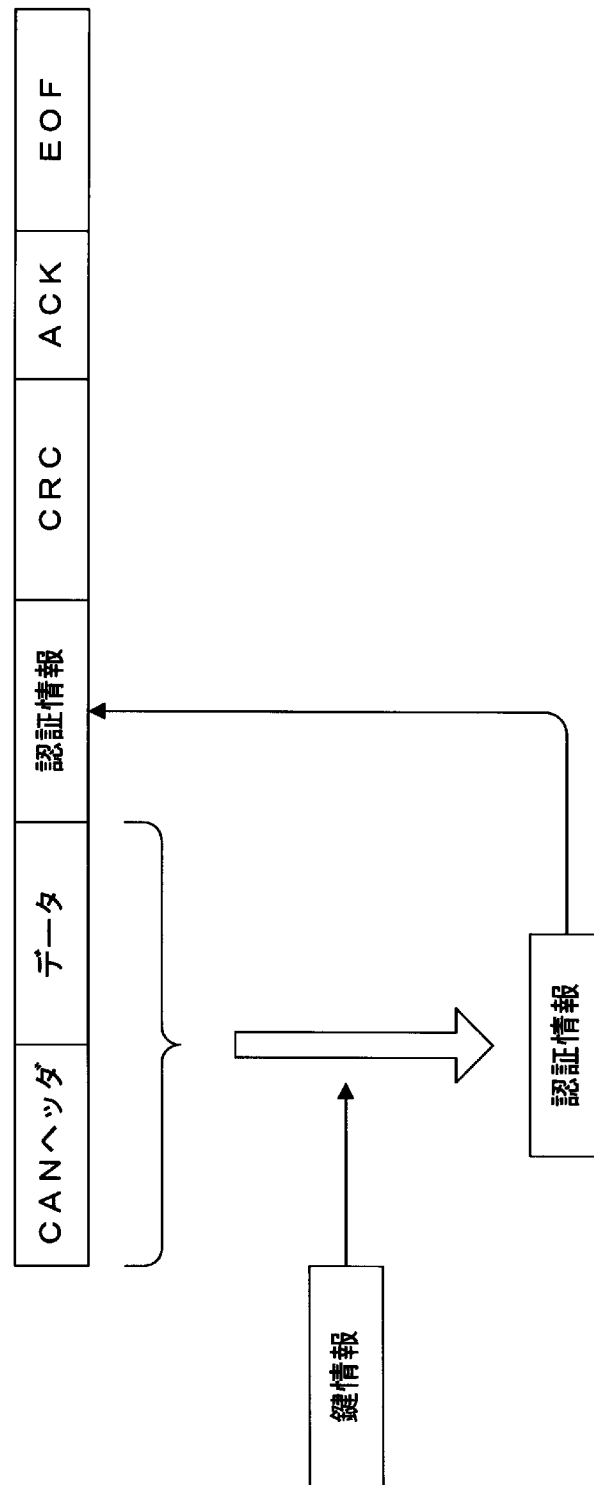
鍵情報テーブル

I D	鍵情報
E C U a	鍵 A
E C U b	鍵 B
E C U c	鍵 C
⋮	⋮

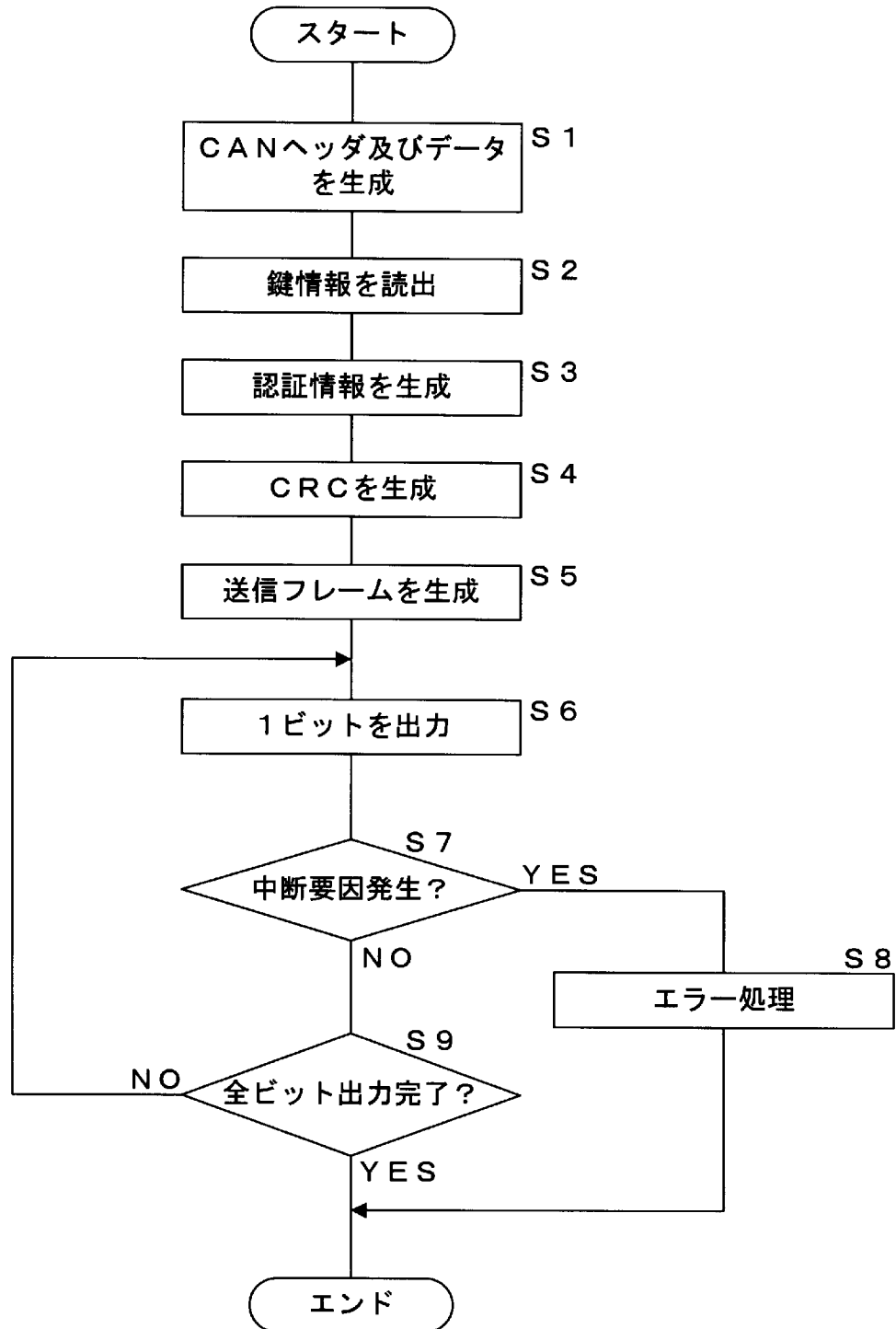
[図5]



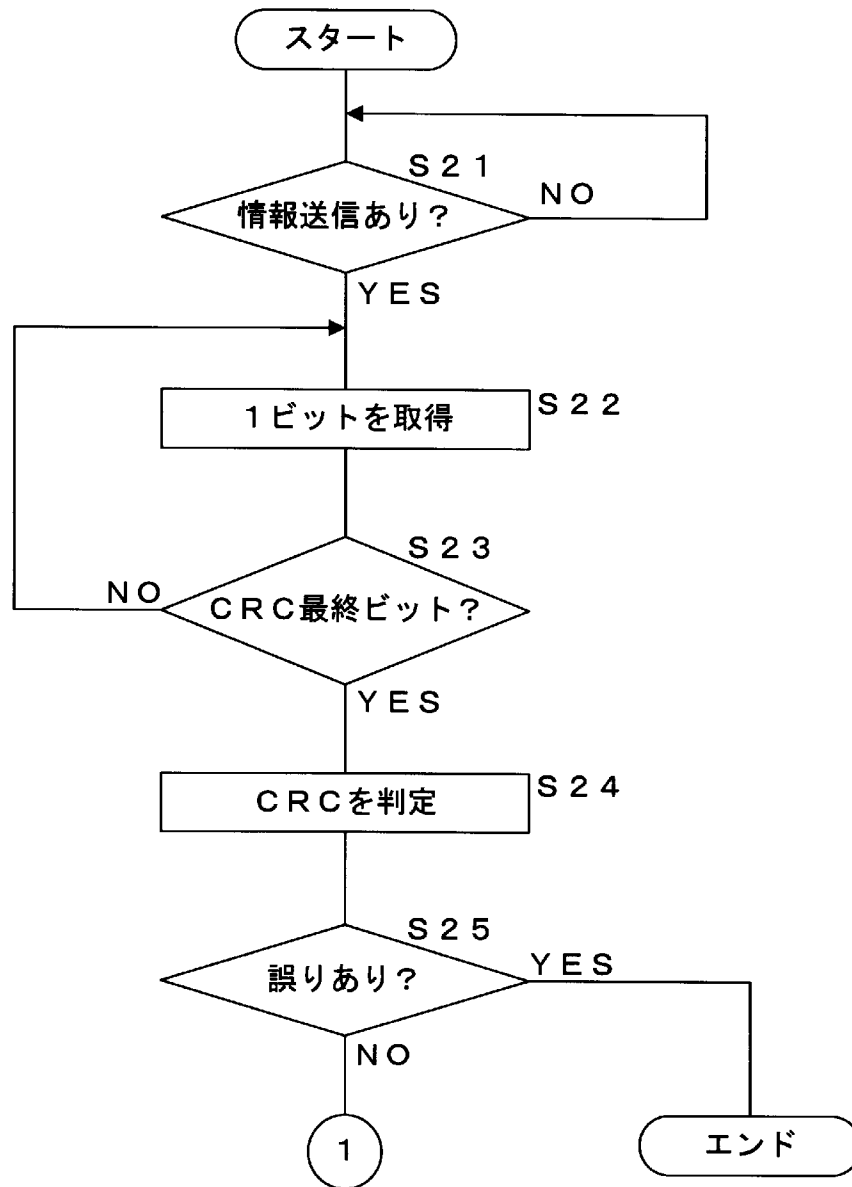
[図6]



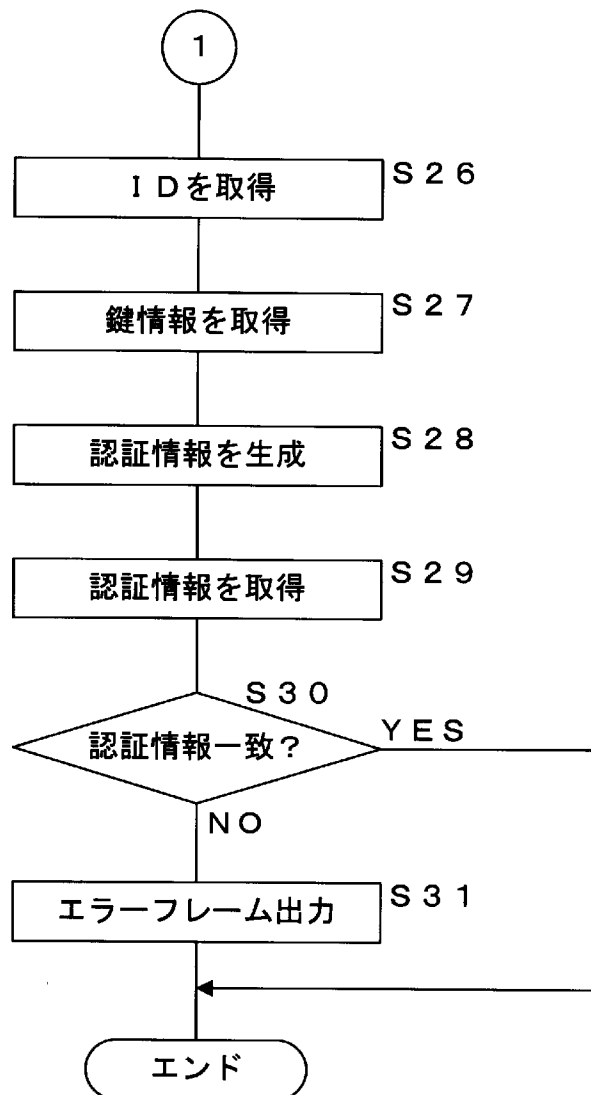
[図7]



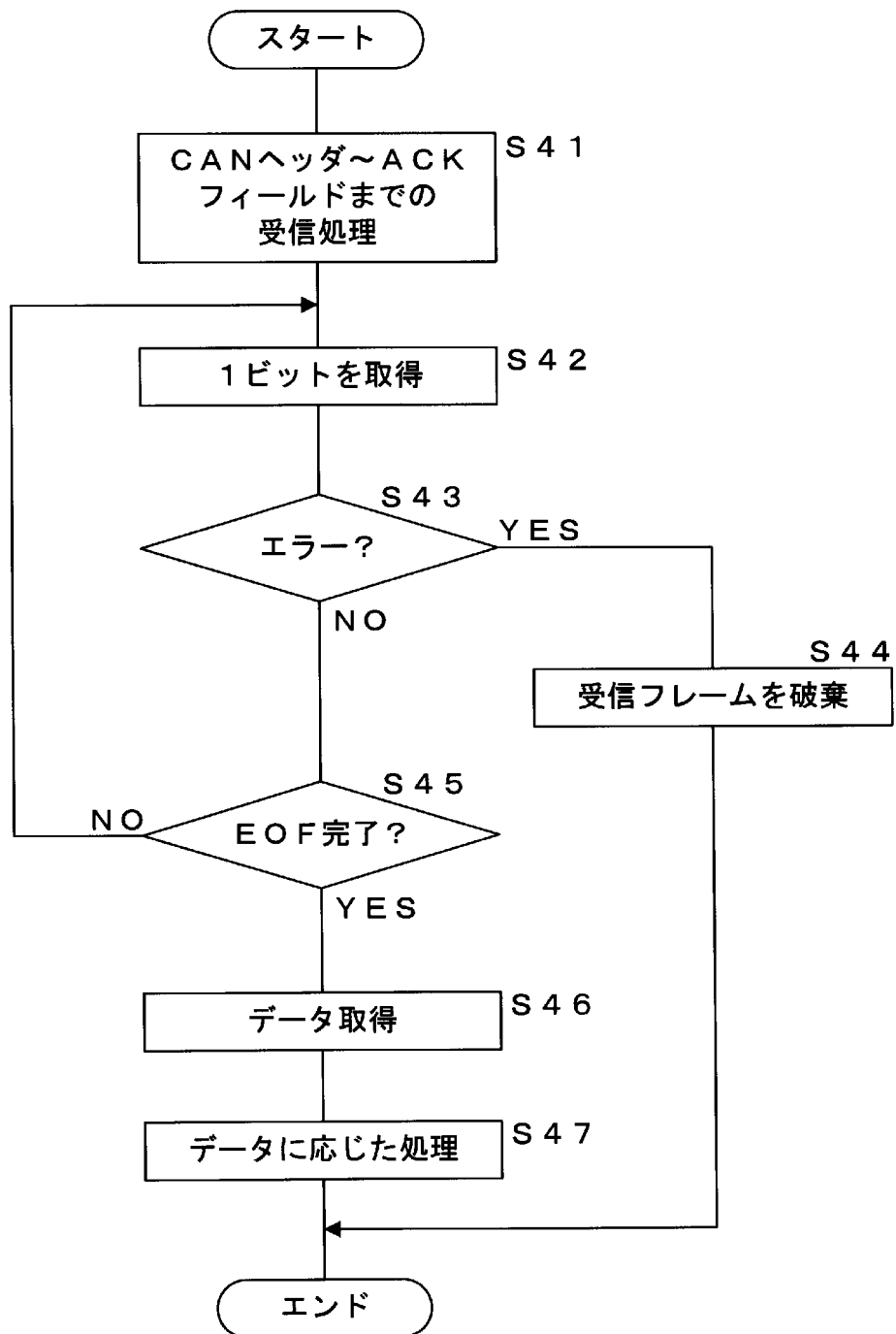
[図8]



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/068452

A. CLASSIFICATION OF SUBJECT MATTER

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)

H04L12/28

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	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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	WO 2013/175633 A1 (Toyota Motor Corp.), 28 November 2013 (28.11.2013), paragraphs [0035] to [0037], [0048] to [0055], [0073] to [0075]; fig. 2, 7 (Family: none)	1-6
Y	JP 2013-131907 A (Toyota Motor Corp.), 04 July 2013 (04.07.2013), paragraphs [0049] to [0056], [0085]; fig. 6, 7 & US 2015/0066239 A1 & WO 2013/093591 A1 & CN 104012065 A	1, 3-6
Y	JP 2007-67812 A (Fujitsu Ten Ltd.), 15 March 2007 (15.03.2007), paragraphs [0012] to [0014]; fig. 1 (Family: none)	1, 3-6

☒ 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 August 2015 (14.08.15)

Date of mailing of the international search report
01 September 2015 (01.09.15)

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/JP2015/068452

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Masato HATA, "How to Stop Unauthorized Transmission in Controller Area Network", CSS2011 Computer Security Symposium 2011 Ronbunshu Heisai Anti-Malware Engineering Workshop 2011, IPSJ Symposium Series, vol.2011, no.3 [CD-ROM], vol.2011, Outline, 1. Introduction	2

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. 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. H04L12/28

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	1971-2015年
日本国実用新案登録公報	1996-2015年
日本国登録実用新案公報	1994-2015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	WO 2013/175633 A1（トヨタ自動車株式会社）2013.11.28, 段落 [0035] ~ [0037]、[0048] ~ [0055]、段落 [0073] ~ [0075]、第2図、第7図（ファミリーなし）	1-6
Y	JP 2013-131907 A（トヨタ自動車株式会社）2013.07.04, 段落 [0049] ~ [0056]、[0085]、第6、7図 & US 2015/0066239 A1 & WO 2013/093591 A1 & CN 104012065 A	1、3-6
Y	JP 2007-67812 A（富士通テン株式会社）2007.03.15, 段落 [0012] ~ [0014]、第1図（ファミリーなし）	1、3-6

☒ 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。

* 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

14.08.2015

国際調査報告の発送日

01.09.2015

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）

大石 博見

5 X

4185

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
Y	畑 正人 Masato Hata, 不正送信阻止: CANではそれが可能である How to Stop Unauthorized Transmission in Controller Area Network, C S S 2 0 1 1 コンピュータセキュリティシンポジウム 2 0 1 1 論文集 併催 マルウェア対策研究人材育成ワークショップ 2 0 1 1 情報処理学会シンポジウムシリーズ V o 1 . 2 0 1 1 N o . 3 [C D - R O M] , 第 2011 巻, あらまし、1. はじめに	2