

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02019/225257

発行日 令和3年4月22日 (2021.4.22)

(43) 国際公開日 令和1年11月28日 (2019.11.28)

(51) Int.Cl.	F I	テーマコード (参考)
HO4L 12/40 (2006.01)	HO4L 12/40 M	5K032
HO4L 12/28 (2006.01)	HO4L 12/28 200M	5K033

審査請求 未請求 予備審査請求 未請求 (全 48 頁)

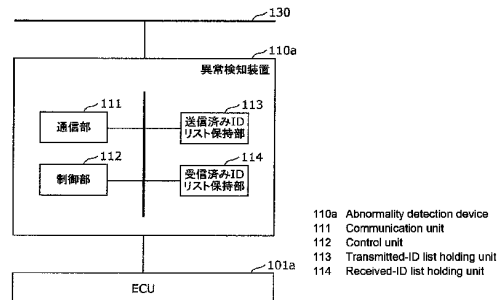
<p>出願番号 特願2019-537416 (P2019-537416)</p> <p>(21) 国際出願番号 PCT/JP2019/017014</p> <p>(22) 国際出願日 平成31年4月22日 (2019.4.22)</p> <p>(31) 優先権主張番号 特願2018-98855 (P2018-98855)</p> <p>(32) 優先日 平成30年5月23日 (2018.5.23)</p> <p>(33) 優先権主張国・地域又は機関 日本国 (JP)</p>	<p>(71) 出願人 514136668 パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ Panasonic Intellectual Property Corporation of America アメリカ合衆国 90503 カリフォルニア州, トーランス, スイート 200, マリナー アベニュー 20000</p> <p>(74) 代理人 100109210 弁理士 新居 広守</p> <p>(74) 代理人 100137235 弁理士 寺谷 英作</p>
---	--

最終頁に続く

(54) 【発明の名称】 異常検知装置、異常検知方法およびプログラム

(57) 【要約】

異常検知装置(110a)は、バス(130)とECU(101a)の間に配置され、ECU(101a)からメッセージを受信して当該メッセージをバス(130)へ送信し、バス(130)からメッセージを受信して当該メッセージをECU(101a)へ送信する通信部(111)と、通信部(111)がバス(130)から受信しECU(101a)へ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部(114)と、制御部(112)と、を備え、制御部(112)は、通信部(111)がバス(130)から受信したメッセージのIDが受信済みIDリストに存在しない場合に、当該IDを受信済みIDリストに追加し、通信部(111)がECU(101a)から受信したメッセージのIDが受信済みIDリストに存在する場合に、当該メッセージをバス(130)へ送信しない。



- 110a Abnormality detection device
- 111 Communication unit
- 112 Control unit
- 113 Transmitted-ID list holding unit
- 114 Received-ID list holding unit

【特許請求の範囲】**【請求項 1】**

複数の電子制御ユニットと、ネットワークバスと、異常検知装置から構成される車載ネットワークに配置される異常検知装置であって、

前記異常検知装置は、

前記ネットワークバスと前記複数の電子制御ユニットのうちのいずれかの第 1 電子制御ユニットの間に配置され、

前記第 1 電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークバスへ送信し、前記ネットワークバスからメッセージを受信して当該メッセージを前記第 1 電子制御ユニットへ送信する通信部と、

10

前記通信部が前記ネットワークバスから受信し前記第 1 電子制御ユニットへ送信したメッセージの ID のリストである受信済み ID リストを保持する受信済み ID リスト保持部と、

前記通信部および前記受信済み ID リスト保持部を制御する制御部と、を備え、

前記制御部は、

前記通信部が前記ネットワークバスから受信したメッセージの ID が前記受信済み ID リストに存在しない場合に、当該 ID を前記受信済み ID リストに追加し、

前記通信部が前記第 1 電子制御ユニットから受信したメッセージの ID が前記受信済み ID リストに存在する場合に、当該メッセージを前記ネットワークバスへ送信しないことを特徴とする、

20

異常検知装置。

【請求項 2】

前記制御部は、前記通信部が前記第 1 電子制御ユニットから受信したメッセージの ID が前記受信済み ID リストに存在する場合に、前記第 1 電子制御ユニットを前記ネットワークバスから隔離することを特徴とする、

請求項 1 記載の異常検知装置。

【請求項 3】

前記制御部は、前記通信部が前記複数の電子制御ユニットのうちの前記第 1 電子制御ユニットとは異なる第 2 電子制御ユニットから送信された異常な ID を示す異常 ID 情報を前記ネットワークバスから受信した場合に、前記受信済み ID リストから前記異常 ID 情報が示す ID を消去することを特徴とする、

30

請求項 1 または 2 に記載の異常検知装置。

【請求項 4】

前記受信済み ID リスト保持部は、前記受信済み ID リストに含まれる ID 毎のメッセージ受信回数を記録する領域を持ち、

前記制御部は、

前記通信部が前記ネットワークバスからメッセージを受信したとき、当該メッセージの ID について記録されるメッセージ受信回数を更新し、

前記車載ネットワークを搭載した車両のシャットダウン時に、前記受信済み ID リストに含まれる ID のうち、前記受信済み ID リスト保持部に記録されたメッセージ受信回数、または、当該メッセージ受信回数に基づくメッセージ受信頻度が所定の値以下となっている ID を不揮発性メモリに退避させ、

40

前記車両の起動時に、前記不揮発性メモリに退避させた前記 ID を前記受信済み ID リストに追加することを特徴とする、

請求項 1 ~ 3 のいずれか 1 項に記載の異常検知装置。

【請求項 5】

前記制御部は、前記車両の起動時に、前回の起動時から前記第 1 電子制御ユニットのファームウェア情報が変更されている場合に、前記不揮発性メモリに退避させた前記 ID を消去し、当該 ID を前記受信済み ID リストに追加しないことを特徴とする、

請求項 4 記載の異常検知装置。

50

【請求項 6】

前記異常検知装置は、さらに、前記通信部が前記第 1 電子制御ユニットから受信し前記ネットワークバスへ送信したメッセージの ID のリストである送信済み ID リストを保持する送信済み ID リスト保持部を備え、

前記制御部は、さらに、

前記送信済み ID リスト保持部を制御し、

前記通信部が前記第 1 電子制御ユニットから受信したメッセージの ID が前記送信済み ID リストに存在しない場合に、当該 ID を前記送信済み ID リストに追加し、

前記通信部が前記ネットワークバスから受信したメッセージの ID が前記送信済み ID リストに存在する場合、当該メッセージを前記第 1 電子制御ユニットへ送信しないことを特徴とする、

10

請求項 1 ~ 5 のいずれか 1 項に記載の異常検知装置。

【請求項 7】

前記送信済み ID リスト保持部は、前記送信済み ID リストに含まれる ID 毎のメッセージ送信回数を記録する領域を持ち、

前記制御部は、

前記通信部が前記第 1 電子制御ユニットからメッセージを受信したときに、当該メッセージの ID について記録されるメッセージ送信回数を更新し、

前記車載ネットワークを搭載した車両のシャットダウン時に、前記送信済み ID リストに含まれる ID のうち、前記送信済み ID リスト保持部に記録されたメッセージ送信回数、または、当該メッセージ送信回数に基づくメッセージ送信頻度が所定の値以下となっている ID を不揮発性メモリに退避させ、

20

前記車両の起動時に、前記不揮発性メモリに退避させた前記 ID を前記送信済み ID リストに追加することを特徴とする、

請求項 6 記載の異常検知装置。

【請求項 8】

前記制御部は、前記車両の起動時に、前回の起動時から前記第 1 電子制御ユニットのファームウェア情報に変更されている場合に、前記不揮発性メモリに退避させた前記 ID を消去し、当該 ID を前記送信済み ID リストに追加しないことを特徴とする、

請求項 7 記載の異常検知装置。

30

【請求項 9】

複数の電子制御ユニットと、ネットワークバスと、異常検知装置から構成される車載ネットワークに配置される異常検知装置により実行される異常検知方法であって、

前記異常検知装置は、

前記ネットワークバスと前記複数の電子制御ユニットのうちのいずれかの第 1 電子制御ユニットの間に配置され、

前記第 1 電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークバスへ送信し、前記ネットワークバスからメッセージを受信して当該メッセージを前記第 1 電子制御ユニットへ送信する通信部と、

前記通信部が前記ネットワークバスから受信し前記第 1 電子制御ユニットへ送信したメッセージの ID のリストである受信済み ID リストを保持する受信済み ID リスト保持部と、を備え、

40

前記異常検知方法では、

前記通信部が前記ネットワークバスから受信したメッセージの ID が前記受信済み ID リストに存在しない場合に、当該 ID を前記受信済み ID リストに追加し、

前記通信部が前記第 1 電子制御ユニットから受信したメッセージの ID が前記受信済み ID リストに存在する場合に、当該メッセージを前記ネットワークバスへ送信しないことを特徴とする、

異常検知方法。

【請求項 10】

50

請求項 9 に記載の異常検知方法をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、車載ネットワーク等で用いられる異常検知装置等に関する。

【背景技術】

【0002】

電子化が進んだ自動車において、電子化が進んでいない自動車と比較すると、車載ネットワークの重要性は高くなっている。自動車には各種のシステムを制御する多数の電子制御ユニット (Electronic Control Unit、以下 ECU と表記する) が搭載されている。ECU は車載ネットワークに接続され、自動車の諸機能を実現するためにこの車載ネットワークを介して通信を行う。CAN (Controller Area Network) は、このような車載ネットワークの規格のひとつで、ISO 11898、ISO 11519 において規格化され標準的な技術として多くの国および地域で採用されている。

10

【0003】

CAN のプロトコルに準拠するネットワークは 1 台の車上で閉じた通信経路として構築可能である。しかしながら、自動車には外部からのアクセスが可能なネットワークが構築され、搭載されるのが珍しくない。例えば車載ネットワークには、ネットワークを流れる情報を自動車に搭載された各システムの診断に利用する目的で取り出すためのポートが設置されたり、無線 LAN を提供する機能を備えるカーナビゲーションシステムが接続されたりしている。車載ネットワークへの外部からのアクセスが可能になることで自動車のユーザにとっての利便性は向上し得るが、その一方で脅威も増大する。

20

【0004】

例えば、2013 年には、車載ネットワークの外部からの駐車支援機能等の悪用による不正な車両制御が可能であることが実証された。また、2015 年には特定の車種の遠隔からの不正制御が可能であることが実証され、この実証が発端となって当該車種のリコールに発展した。

【0005】

このような外部からのアクセスによる車両の不正制御は、自動車業界にとっては看過できない問題であり、車載ネットワークのセキュリティ対策は急務な状況にある。

30

【0006】

車載ネットワークへの攻撃の一手法としては、車載ネットワークに接続される ECU に外部からアクセスして乗っ取り、乗っ取った ECU から攻撃のためのメッセージ (以下では不正メッセージまたは異常メッセージともいう) を車載ネットワークに向けて送信させて自動車を不正に制御するものがある。

【0007】

このような攻撃に対し、非特許文献 1 では、車載ネットワークに送信されたメッセージから不正メッセージを検知する IDS (Intrusion Detection System) ECU と呼ばれるノードを車載ネットワークに追加し、IDSECUCU が不正なメッセージのハッシュ値をネットワークに送信し、このハッシュ値を各 ECU が送信したメッセージのハッシュ値と比較することで、不正なメッセージを送信する不正 ECU を特定し、車載ネットワークから遮断する方法を開示している。

40

【0008】

また、非特許文献 2 では、車載ネットワークでは同一の ID を持つメッセージを複数の ECU が送信しないという前提で、各 ECU が自身の送信する ID を持つメッセージを受信した際に、そのメッセージを不正メッセージとして遮断する方法を開示している。

【先行技術文献】

【非特許文献】

【0009】

50

【非特許文献1】Smart CAN cable, Another proposal of intrusion prevention system (IPS) for in-vehicle networks - LAC Co., Ltd., Symposium on Cryptography and Information Security, 2018.

【非特許文献2】A Method of Preventing Unauthorized Data Transmission in controller area network - Yokohama National University: Vehicular Technology Conference, 2012

【発明の概要】

【発明が解決しようとする課題】

【0010】

しかしながら、非特許文献1の方法では、車載ネットワーク内にIDSECUを追加するコストおよび、不正なメッセージのハッシュ値をネットワークに送ることによる、ネットワークのトラフィック量の増大が発生する。

【0011】

また、非特許文献2の方法では、不正メッセージの遮断を行うためにCANコントローラを改造する(例えば、各ECUが送信するメッセージのIDを予め記憶させておく)必要があり導入コストが大きい。

【0012】

そこで、本開示では上記課題を解決するために、車載ネットワークにおける異常を容易に検知できる異常検知装置等を提供する。

【課題を解決するための手段】

【0013】

上記課題を解決するために、本開示の一態様に係る異常検知装置は、複数の電子制御ユニットと、ネットワークバスと、異常検知装置から構成される車載ネットワークに配置される異常検知装置であって、前記異常検知装置は、前記ネットワークバスと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークバスへ送信し、前記ネットワークバスからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、前記通信部が前記ネットワークバスから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、前記通信部および前記受信済みIDリスト保持部を制御する制御部と、を備え、前記制御部は、前記通信部が前記ネットワークバスから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、当該メッセージを前記ネットワークバスへ送信しないことを特徴とする。

【0014】

なお、上記の包括的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラムまたはコンピュータ読取可能な記録ディスク等の記録媒体で実現されてもよく、システム、装置、方法、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。コンピュータ読み取り可能な記録媒体は、例えばCD-ROM (Compact Disc-Read Only Memory)等の不揮発性の記録媒体を含む。

【発明の効果】

【0015】

本開示によれば、車載ネットワークにおける異常を容易に検知できる。

【図面の簡単な説明】

【0016】

【図 1】図 1 は、実施の形態 1 における、車載ネットワークの全体構成図である。

【図 2】図 2 は、実施の形態 1 における、車載ネットワークの全体構成の変形例 1 を示す図である。

【図 3】図 3 は、実施の形態 1 における、車載ネットワークの全体構成の変形例 2 を示す図である。

【図 4】図 4 は、実施の形態 1 における、CAN プロトコルのデータフレームフォーマットを示す図である。

【図 5】図 5 は、実施の形態 1 における、車載ネットワークを構成する ECU が送信する ID の仕様を示す図である。

【図 6】図 6 は、実施の形態 1 における、IDSECUCU の構成図である。

10

【図 7】図 7 は、実施の形態 1 における、異常検知装置の構成図である。

【図 8】図 8 は、実施の形態 1 における、異常検知機能を有する ECU の構成図である。

【図 9】図 9 は、実施の形態 1 における、受信済み ID リストの一例を示す図である。

【図 10】図 10 は、実施の形態 1 における、送信済み ID リストの一例を示す図である。

【図 11】図 11 は、実施の形態 1 における、受信済み ID リストのアップデート処理のシーケンスを示す図である。

【図 12】図 12 は、実施の形態 1 における、受信済み ID リストを用いた異常検知処理のシーケンスを示す図である。

【図 13】図 13 は、実施の形態 1 における、送信済み ID リストのアップデート処理のシーケンスを示す図である。

20

【図 14】図 14 は、実施の形態 1 における、送信済み ID リストを用いた異常検知処理のシーケンスを示す図である。

【図 15】図 15 は、実施の形態 1 における、IDSECUCU が異常を検知した場合の処理シーケンスを示す図である。

【図 16】図 16 は、実施の形態 1 における、異常検知装置の全体処理のフローチャートである。

【図 17】図 17 は、実施の形態 1 における、受信済み ID リスト更新処理のフローチャートである。

【図 18】図 18 は、実施の形態 1 における、送信済み ID リスト更新処理のフローチャートである。

30

【図 19】図 19 は、実施の形態 1 における、受信済み ID リストによる異常検知処理のフローチャートである。

【図 20】図 20 は、実施の形態 1 における、受信済み ID リストによる異常検知処理の変形例のフローチャートである。

【図 21】図 21 は、実施の形態 1 における、送信済み ID リストによる異常検知処理のフローチャートである。

【図 22】図 22 は、実施の形態 1 における、異常検知装置が IDSECUCU から異常通知を受信した場合の処理のフローチャートである。

【図 23】図 23 は、実施の形態 1 における、異常検知装置の全体処理の変形例のフローチャートである。

40

【図 24】図 24 は、実施の形態 1 における、異常検知装置の車両シャットダウン時の処理のフローチャートである。

【図 25】図 25 は、実施の形態 1 における、低頻度受信済み ID の退避の処理のフローチャートである。

【図 26】図 26 は、実施の形態 1 における、低頻度送信済み ID の退避の処理のフローチャートである。

【図 27】図 27 は、実施の形態 1 における、異常検知装置の車両起動時の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】

50

【 0 0 1 7 】

本開示の異常検知装置は、複数の電子制御ユニットと、ネットワークバスと、異常検知装置から構成される車載ネットワークに配置される異常検知装置であって、前記異常検知装置は、前記ネットワークバスと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークバスへ送信し、前記ネットワークバスからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、前記通信部が前記ネットワークバスから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、前記通信部および前記受信済みIDリスト保持部を制御する制御部と、を備え、前記制御部は、前記通信部が前記ネットワークバスから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、当該メッセージを前記ネットワークバスへ送信しないことを特徴とする。

10

【 0 0 1 8 】

異常検知装置は、ネットワークバスから受信したメッセージのIDを受信済みIDリストに追加していく。つまり、異常検知装置は、複数のECUのうち、自身を介してネットワークバスと接続された第1ECU以外のECUがネットワークバスへ送信したメッセージのIDを受信済みIDリストに追加していく。一般的に、車載ネットワークにおける複数のECUのそれぞれは、同じIDを含むメッセージを送信しないという仕様になっていることが多い。この仕様のもとでは、受信済みIDリストは、第1ECUが送信しないメッセージのIDのリストとなる。これに対して、異常検知装置が第1ECUから受信したメッセージ（つまり、第1ECUが送信したメッセージ）のIDを受信済みIDリストに存在する場合、本来第1ECUが送信するはずのないメッセージを第1ECUが送信していることになる。つまり、第1ECUが異常なメッセージを送信していることがわかる。したがって、このような場合に、第1ECUからのメッセージをネットワークバスに送信しないようにすることで、異常なメッセージがネットワークバスに流れることを抑制できる。このように、車載ネットワーク内にIDS ECUを追加（つまり、ネットワークトラフィックおよびコストが増大）したり、各ECUが送信するメッセージのIDを予め記憶させておいたりすることなく、車載ネットワークにおける異常を容易に検知できる。また、正規メッセージがネットワークバスに流れる前に、攻撃者が不正メッセージをネットワークバスへ送信しない限り、誤検知をすることなく異常メッセージを遮断可能である。

20

30

【 0 0 1 9 】

また例えば、前記制御部は、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、前記第1電子制御ユニットを前記ネットワークバスから隔離してもよい。

【 0 0 2 0 】

この場合、第1ECUが不正なECUであるため、不正なECUをネットワークバスから隔離する（例えば、第1ECUから送信される全てのメッセージを異常検知装置において遮断してネットワークバスへ送信しないようにする）ことが可能となり、異常メッセージのみを遮断する場合と比べて、車載ネットワークに不正なECUが与える影響をより軽減できる。

40

【 0 0 2 1 】

また例えば、前記制御部は、前記通信部が前記複数の電子制御ユニットのうちの前記第1電子制御ユニットとは異なる第2電子制御ユニットから送信された異常なIDを示す異常ID情報を前記ネットワークバスから受信した場合に、前記受信済みIDリストから前記異常ID情報が示すIDを消去してもよい。

【 0 0 2 2 】

正規メッセージがネットワークバスに流れる前に、攻撃者が不正メッセージをネットワークバスへ送信する場合が考えられる。この場合、受信済みIDリストに不正メッセージ

50

に含まれるIDが追加されることになる。例えば、正規な第1ECUが送信するメッセージに含まれるIDが不正メッセージに含まれる場合、正規な第1ECUから送信される正規メッセージが不正メッセージであると判定されてしまう。つまり、以降は、正規メッセージがネットワークバスへ送信されず、攻撃者が第1ECUになりすまして不正メッセージがネットワークバスへ送信されることになる。これに対して、第2ECUとして例えばIDS ECU等が車載ネットワークに配置されることで、攻撃者が送信した不正メッセージを検知することが可能となる。したがって、正規メッセージがネットワークバスに流れる前に、攻撃者が不正メッセージをネットワークバスへ送信した場合（つまり、受信済みIDリストが汚染された場合）であっても、受信済みIDリストを修正して、受信済みIDリストに追加された不正メッセージに含まれるID（つまり第1ECUが送信するメッセージに含まれるID）を受信済みIDリストから消去することで、異常検知装置が正規メッセージを不正メッセージであると誤検知することを防止することが可能である。

10

20

30

40

50

【0023】

また例えば、前記受信済みIDリスト保持部は、前記受信済みIDリストに含まれるID毎のメッセージ受信回数を記録する領域を持ち、前記制御部は、前記通信部が前記ネットワークバスからメッセージを受信したとき、当該メッセージのIDについて記録されるメッセージ受信回数を更新し、前記車載ネットワークを搭載した車両のシャットダウン時に、前記受信済みIDリストに含まれるIDのうち、前記受信済みIDリスト保持部に記録されたメッセージ受信回数、または、当該メッセージ受信回数に基づくメッセージ受信頻度が所定の値以下となっているIDを不揮発性メモリに退避させ、前記車両の起動時に、前記不揮発性メモリに退避させた前記IDを前記受信済みIDリストに追加してもよい。

【0024】

メッセージ受信回数またはメッセージ受信頻度が所定の値以下となっているID（低頻度で受信されるメッセージに含まれるID）は、車両が起動した後、当該IDを含むメッセージがネットワークバスを流れるまでに時間を要する場合がある。つまり、当該IDを含む正規メッセージがネットワークバスを流れるまでに、攻撃者が当該IDを含む不正メッセージをネットワークバスへ送信して、受信済みIDリストに不正メッセージに含まれるIDが追加されてしまう（言い換えると、受信済みIDリストが不正なIDで汚染されてしまう）場合がある。これに対して、車両の起動時に、不揮発性メモリに退避させた低頻度で受信されるメッセージに含まれるIDを受信済みIDリストに追加することで、低頻度で受信されるメッセージが最初にネットワークバスに流れる前に攻撃者が不正メッセージを送信することによる受信済みIDリストの汚染を防ぐことが可能である。また、高頻度で受信されるメッセージの含まれるIDを不揮発性メモリに退避させないことで、その分メモリ容量を削減することが可能である。

【0025】

また例えば、前記制御部は、前記車両の起動時に、前回の起動時から前記第1電子制御ユニットのファームウェア情報が変更されている場合に、前記不揮発性メモリに退避させた前記IDを消去し、当該IDを前記受信済みIDリストに追加しなくてもよい。

【0026】

第1ECUのファームウェアアップデートに伴い第1ECUのファームウェア情報が変更された場合、第1ECUから送信されるメッセージに含まれるIDの仕様が変更されることがある。したがって、この場合に、不揮発性メモリに退避させたIDを消去し、当該IDを受信済みIDリストに追加しないようにすることで、仕様が変更されたIDが原因で発生する正常メッセージの誤遮断を防止することが可能である。

【0027】

また例えば、前記異常検知装置は、さらに、前記通信部が前記第1電子制御ユニットから受信し前記ネットワークバスへ送信したメッセージのIDのリストである送信済みIDリストを保持する送信済みIDリスト保持部を備え、前記制御部は、さらに、前記送信済みIDリスト保持部を制御し、前記通信部が前記第1電子制御ユニットから受信したメッ

ページのIDが前記送信済みIDリストに存在しない場合に、当該IDを前記送信済みIDリストに追加し、前記通信部が前記ネットワークバスから受信したメッセージのIDが前記送信済みIDリストに存在する場合、当該メッセージを前記第1電子制御ユニットへ送信しなくてもよい。

【0028】

異常検知装置は、第1ECUから受信したメッセージのIDを送信済みIDリストに追加していく。車載ネットワークにおける複数のECUのそれぞれは、同じIDを含むメッセージを送信しないという仕様のもとでは、送信済みIDリストは、複数のECUのうちの第1ECU以外のECU等が送信しないメッセージのIDのリストとなる。これに対して、異常検知装置がネットワークバスから受信したメッセージ（つまり、第1ECU以外のECUが送信したメッセージ）のIDが送信済みIDリストに存在する場合、本来第1ECU以外のECU等が送信するはずのないメッセージを第1ECU以外のECU等が送信していることになる。つまり、第1ECU以外のECU等が異常なメッセージを送信していることがわかる。したがって、このような場合に、第1ECU以外のECU等からのメッセージを第1ECUに送信しないようにすることで、異常なメッセージが第1ECUに送信されることを抑制できる。このように車載ネットワーク内にIDSECUを追加（つまり、ネットワークトラフィックおよびコストが増大）したり、各ECUが送信するメッセージのIDを予め記憶させておいたりすることなく、車載ネットワークにおける異常を容易に検知できる。また、正規メッセージがネットワークバスに流れる前に、攻撃者が不正メッセージをネットワークバスへ送信しない限り、誤検知をすることなく異常メッセージを検知可能である。

10

20

【0029】

また例えば、前記送信済みIDリスト保持部は、前記送信済みIDリストに含まれるID毎のメッセージ送信回数を記録する領域を持ち、前記制御部は、前記通信部が前記第1電子制御ユニットからメッセージを受信したときに、当該メッセージのIDについて記録されるメッセージ送信回数を更新し、前記車載ネットワークを搭載した車両のシャットダウン時に、前記送信済みIDリストに含まれるIDのうち、前記送信済みIDリスト保持部に記録されたメッセージ送信回数、または、当該メッセージ送信回数に基づくメッセージ送信頻度が所定の値以下となっているIDを不揮発性メモリに退避させ、前記車両の起動時に、前記不揮発性メモリに退避させた前記IDを前記送信済みIDリストに追加してもよい。

30

【0030】

メッセージ送信回数またはメッセージ送信頻度が所定の値以下となっているID（低頻度で第1ECUから送信されるメッセージに含まれるID）は、車両が起動した後、当該IDを含むメッセージを異常検知装置が第1ECUから受信するまでに時間を要する場合がある。つまり、当該IDを含む正規メッセージを異常検知装置が受信するまでに、攻撃者が第1ECUを攻撃して不正な第1ECUから不正メッセージを異常検知装置へ送信して、送信済みIDリストに不正メッセージに含まれるIDが追加されてしまう（言い換えると、送信済みIDリストが不正なIDで汚染されてしまう）場合がある。これに対して、車両の起動時に、不揮発性メモリに退避させた低頻度で送信されるメッセージに含まれるIDを送信済みIDリストに追加することで、低頻度で送信されるメッセージを異常検知装置が受信する前に攻撃者が不正メッセージを送信することによる送信済みIDリストの汚染を防ぐことが可能である。また、高頻度で送信されるメッセージに含まれるIDを不揮発性メモリに退避させないことで、その分メモリ容量を削減することが可能である。

40

【0031】

また例えば、前記制御部は、前記車両の起動時に、前回の起動時から前記第1電子制御ユニットのファームウェア情報が変更されている場合に、前記不揮発性メモリに退避させた前記IDを消去し、当該IDを前記送信済みIDリストに追加しなくてもよい。

【0032】

第1ECUのファームウェアアップデートに伴い第1ECUのファームウェア情報が変

50

更された場合、第1 ECUから送信されるメッセージに含まれるIDの仕様が変更されることがある。したがって、この場合に、不揮発性メモリに退避させたIDを消去し、当該IDを送信済みIDリストに追加しないようにすることで、仕様が変更されたIDによる正常メッセージの誤遮断の防止が可能である。

【0033】

本開示の異常検知方法は、複数の電子制御ユニットと、ネットワークバスと、異常検知装置から構成される車載ネットワークに配置される異常検知装置により実行される異常検知方法であって、前記異常検知装置は、前記ネットワークバスと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークバスへ送信し、前記ネットワークバスからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、前記通信部が前記ネットワークバスから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、を備え、前記異常検知方法では、前記通信部が前記ネットワークバスから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、当該メッセージを前記ネットワークバスへ送信しないことを特徴とする。

10

【0034】

これにより、車載ネットワークにおける異常を容易に検知できる異常検知方法を提供できる。

20

【0035】

本開示のプログラムは、上記の異常検知方法をコンピュータに実行させるプログラムである。

【0036】

これにより、車載ネットワークにおける異常を容易に検知できるプログラムを提供できる。

【0037】

以下、実施の形態に係る異常検知装置について、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本開示の一具体例を示すものである。したがって、以下の実施の形態で示される数値、構成要素、構成要素の配置および接続形態、並びに、ステップ(工程)およびステップの順序等は、一例であって本開示を限定するものではない。

30

【0038】

また、以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。各図は模式図であり、必ずしも厳密に図示されたものではない。

【0039】

また、以下に含まれるCANおよび異常検知装置に関する説明は、本開示の理解の一助を主な趣旨とするものであり、この説明のうち請求項に含まれない事項については、本開示を限定する趣旨で記載されるものではない。

40

【0040】

(実施の形態1)

[1-1. 車載ネットワーク構成]

図1は、車載ネットワーク100の全体構成図である。なお、図1には、車載ネットワーク100を搭載し車両10を示している。車両10は、その内部に車載ネットワーク100を持つ。車両10は、例えば自動車である。

【0041】

車載ネットワーク100は、複数のECUと、ネットワークバスと、異常検知装置から構成される。例えば、図1に示す例では、車載ネットワーク100は、複数のECUのそれぞれに対応するように設けられた複数の異常検知装置を備える。例えば、車載ネットワ

50

ーク100は、複数のECUとして、ECU101a、101b、101c、101d、101eおよび101fとバス130（ネットワークバス）と異常検知装置110a、110b、110c、110d、110eおよび110fとから構成される。ECU101aとバス130は、異常検知装置110aを間に介して接続され、通信を行う。ECU101bとバス130は、異常検知装置110bを間に介して接続され、通信を行う。ECU101cとバス130は、異常検知装置110cを間に介して接続され、通信を行う。ECU101dとバス130は、異常検知装置110dを間に介して接続され、通信を行う。ECU101eとバス130は、異常検知装置110eを間に介して接続され、通信を行う。ECU101fとバス130は、異常検知装置110fを間に介して接続され、通信を行う。例えば、異常検知装置110aに着目すると、異常検知装置110aは、バス130と複数のECUのうちのいずれかの第1ECU（ここではECU101a）の間に配置される。ECU101aがバス130へ向けてメッセージを送信する際、および、ECU101aがバス130からメッセージが受信する際に、異常検知装置110aを介してメッセージの送受信が行われる。

10

【0042】

車載ネットワーク100では、例えばCAN（Controller Area Network）プロトコルに従って通信が行われる。

【0043】

車載ネットワーク100を構成するECU101a、101b、101c、101d、101eおよび101fとしては、例えば、ステアリング、ブレーキ、エンジン、ドアまたはウィンドウ等に関連したECUがあり、これらのECUは、走行制御やインストルメントパネルの制御等の車両10の各種制御を行う。

20

【0044】

ECUは、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM（Read Only Memory）、RAM（Random Access Memory）等であり、プロセッサにより実行されるプログラムを記憶することができる。例えばプロセッサが、プログラムに従って動作することにより、ECUは各種機能を実現することになる。ECUは、例えば、CANプロトコルに従って車載ネットワークにおけるネットワークバスを介してメッセージの送受信を行う。

30

【0045】

各ECUは、ネットワークバスに対して、CANのプロトコルに従ったメッセージを送受信する。例えば、ネットワークバスから他のECUが送信したメッセージを受信し、また、他のECUに送信したい内容を含むメッセージを生成してバスに送信する。具体的には、各ECUは、受信したメッセージの内容に応じた処理を行い、また、ECUに接続されている機器、センサ等の状態を示すメッセージもしくは他のECUへの指示値（制御値）等のメッセージを生成して送信する。

【0046】

異常検知装置の詳細については後述する。

【0047】**[1-2. 車載ネットワーク構成（変形例1）]**

図2は、車載ネットワーク100の全体構成の変形例1を示す図である。図1の車載ネットワーク100では、全てのECUに異常検知装置が接続されていたが、図2の車載ネットワーク100は、一部のECUには異常検知装置が接続されていない場合の一例である。つまり、車載ネットワーク100における複数のECUには、異常検知装置を介さずにバス130に接続されるECUが含まれていてもよい。

40

【0048】

図2において、具体的にはECU101cおよび101eには異常検知装置が接続されずに直接バス130に接続されている。図2に示すように、異常検知装置は必ずしも全てのECUに接続する必要はない。例えば、車両の安全性に大きな影響を及ぼす可能性の高

50

い走行制御に関わるECUとバス130との間のみ異常検知装置を接続することでコストダウンを図ってもよい。

【0049】

[1-3. 車載ネットワーク構成(変形例2)]

図3は、車載ネットワーク100の全体構成の変形例2を示す図であり、図1および図2の車載ネットワーク100に対して、異常検知機能を持ったノードが存在する。以後、異常検知機能を持ったノードをIDSECUとも表記する。図3において、IDSECU120は、バス130を流れるメッセージの異常検知を行い、異常を検知した際はその情報を車載ネットワーク内の異常検知装置110a、110b、110d、110fに通知する。IDSECU120を、異常検知装置を介してバス130に接続されたECU(第1ECU)と区別するために、第2ECUとも呼ぶ。

10

【0050】

[1-4. CANメッセージのフォーマット]

図4は、CANプロトコルのデータフレームのフォーマットを示す図である。ここではCANプロトコルにおける標準IDフォーマットにおけるデータフレームを示している。データフレームは、Start Of Frame(SOF)、IDフィールド、Remote Transmission Request(RTR)、Identifier Extension(IDE)、予約ビット(r)、データレングスコード(DLC)、データフィールド、CRCシーケンス、CRCデリミタ(DEL)、Acknowledgementスロット(ACK)、ACKデリミタ(DEL)、および、エンドオブフレーム(EOF)から構成される。IDフィールドには、各ECUが送信するメッセージに固有のIDが格納される。

20

【0051】

[1-5. ECUの送信IDの仕様]

図5は、車載ネットワーク100を構成するECUが送信するIDの仕様を示す図である。

【0052】

本実施の形態の車載ネットワーク100では、図5に示すように、同じIDのメッセージを複数のECUが送信しないものとする。例えば、エンジンECUが送信する「0x13」というIDを含むメッセージを、ブレーキECUまたはドア制御ECUは送信しない。同じIDのメッセージを複数のECUが送信しない、という仕様はCANを用いた通信において一般的である。異常検知装置は、この仕様を利用することで、車載ネットワーク100における異常を容易に検知することを可能としている。

30

【0053】

[1-6. IDSECUの構成]

図6は、IDSECU120の構成図である。IDSECU120は、CANメッセージの送受信を行う通信部121と、受信したメッセージの異常検知を行う異常検知部122を持つECUであって、複数のECUのうちの第1ECU(例えば、ECU101a、ECU101b、ECU101dおよびECU101f)とは異なる第2ECUである。

【0054】

通信部121は、バス130に流れるメッセージを受信し、また、バス130に流れるメッセージに含まれる異常なIDを示す異常ID情報をバス130へ送信する。

40

【0055】

異常検知部122は、通信部121が受信したバス130に流れるメッセージの異常検知を行う。例えば、IDSECU120は、異常を判定するための判定ルールを保持しており、異常検知部122は、バス130から受信するメッセージを判定ルールに照らし合わせることで、メッセージの異常検知を行う。具体的には、異常検知部122は、判定ルールに基づいて、バス130を流れるメッセージの送信周期に異常があったり、バス130を流れるメッセージに含まれる指示値に異常があったりした場合に、当該メッセージを異常と検知する。

50

【 0 0 5 6 】

I D S E C U 1 2 0 は、通信部 1 2 1 で受信したメッセージを、異常検知部 1 2 2 で異常と検知した場合、そのメッセージに含まれる異常な I D を示す異常 I D 情報を通信部 1 2 1 からバス 1 3 0 を介して車載ネットワーク 1 0 0 内の異常検知装置（図 3 に示す例では、異常検知装置 1 1 0 a、1 1 0 b、1 1 0 d および 1 1 0 f）に送信する。これにより、各異常検知装置は、異常な I D を認識することができる。

【 0 0 5 7 】

[1 - 7 . 異常検知装置の構成]

図 7 は、異常検知装置 1 1 0 a の構成図である。図 7 には、異常検知装置 1 1 0 a の他に、異常検知装置 1 1 0 a に直接接続された E C U 1 0 1 a およびバス 1 3 0 も示されている。本実施の形態では、複数の異常検知装置のうち異常検知装置 1 1 0 a に着目して説明する。

10

【 0 0 5 8 】

異常検知装置 1 1 0 a は、バス 1 3 0 と E C U 1 0 1 a の間に配置される。

【 0 0 5 9 】

異常検知装置 1 1 0 a は、通信部 1 1 1、制御部 1 1 2、送信済み I D リスト保持部 1 1 3 および受信済み I D リスト保持部 1 1 4 を備える。異常検知装置 1 1 0 a は、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM、RAM 等であり、プロセッサにより実行されるプログラムを記憶することができる。例えば、プロセッサが、プログラムに従って動作することにより、異常検知装置 1 1 0 a は制御部 1 1 2 を実現することになる。通信部 1 1 1 は、例えば通信回路により実現される。送信済み I D リスト保持部 1 1 3 および受信済み I D リスト保持部 1 1 4 は、例えばメモリにより実現される。

20

【 0 0 6 0 】

通信部 1 1 1 は、E C U 1 0 1 a からメッセージを受信して当該メッセージをバス 1 3 0 へ送信し、バス 1 3 0 からメッセージを受信して当該メッセージを E C U 1 0 1 a へ送信する通信回路である。通信部 1 1 1 は、バス 1 3 0 から E C U 1 0 1 a へ送信されるメッセージおよび、E C U 1 0 1 a からバス 1 3 0 へ送信されるメッセージを中継する機能を持つ。

【 0 0 6 1 】

送信済み I D リスト保持部 1 1 3 は、通信部 1 1 1 が E C U 1 0 1 a から受信しバス 1 3 0 へ送信したメッセージの I D のリストである送信済み I D リストを保持する。送信済み I D リストについては後述する。

30

【 0 0 6 2 】

受信済み I D リスト保持部 1 1 4 は、通信部 1 1 1 がバス 1 3 0 から受信し E C U 1 0 1 a へ送信したメッセージの I D のリストである受信済み I D リストを保持する。受信済み I D リストについては後述する。

【 0 0 6 3 】

制御部 1 1 2 は、通信部 1 1 1、送信済み I D リスト保持部 1 1 3 および受信済み I D リスト保持部 1 1 4 を制御する。制御部 1 1 2 は、以下の処理を行う（それぞれ詳細は後述する）。

40

【 0 0 6 4 】

制御部 1 1 2 は、通信部 1 1 1 がバス 1 3 0 から受信したメッセージの I D が受信済み I D リストに存在しない場合に、当該 I D を受信済み I D リストに追加する。また、制御部 1 1 2 は、通信部 1 1 1 が E C U 1 0 1 a から受信したメッセージの I D が受信済み I D リストに存在する場合に、当該メッセージをバス 1 3 0 へ送信しない。例えば、制御部 1 1 2 は、通信部 1 1 1 が E C U 1 0 1 a から受信したメッセージの I D が受信済み I D リストに存在する場合に、E C U 1 0 1 a をバス 1 3 0 から隔離する。

【 0 0 6 5 】

また、制御部 1 1 2 は、通信部 1 1 1 が複数の E C U のうちの他の E C U（具体的には

50

IDS ECU 120) から送信された異常な ID を示す異常 ID 情報をバス 130 から受信した場合に、受信済み ID リストから異常 ID 情報が示す ID を消去する。

【0066】

また、制御部 112 は、通信部 111 がバス 130 からメッセージを受信したとき、当該メッセージの ID について記録されるメッセージ受信回数を更新する。また、制御部 112 は、車載ネットワーク 100 を搭載した車両 10 のシャットダウン時に、受信済み ID リストに含まれる ID のうち、受信済み ID リスト保持部 114 に記録されたメッセージ受信回数、または、当該メッセージ受信回数に基づくメッセージ受信頻度が所定の値以下となっている ID を不揮発性メモリに退避させ、車両 10 の起動時に、不揮発性メモリに退避させた ID を受信済み ID リストに追加する。また、制御部 112 は、車両 10 の起動時に、前回の起動時から ECU 101 a のファームウェア情報が変更されている場合に、不揮発性メモリに退避させた ID を消去し、当該 ID を受信済み ID リストに追加しない。

10

【0067】

また、制御部 112 は、ECU 101 a から受信したメッセージの ID が送信済み ID リストに存在しない場合に、当該 ID を送信済み ID リストに追加する。また、制御部 112 は、通信部 111 がバス 130 から受信したメッセージの ID が送信済み ID リストに存在する場合、当該メッセージを ECU 101 a へ送信しない。

【0068】

また、制御部 112 は、通信部 111 が ECU 101 a からメッセージを受信したときに、当該メッセージの ID について記録されるメッセージ送信回数を更新する。また、制御部 112 は、車載ネットワーク 100 を搭載した車両 10 のシャットダウン時に、送信済み ID リストに含まれる ID のうち、送信済み ID リスト保持部 113 に記録されたメッセージ送信回数、または、当該メッセージ送信回数に基づくメッセージ送信頻度が所定の値以下となっている ID を不揮発性メモリに退避させ、車両 10 の起動時に、不揮発性メモリに退避させた ID を送信済み ID リストに追加する。制御部 112 は、車両 10 の起動時に、前回の起動時から ECU 101 a のファームウェア情報が変更されている場合に、不揮発性メモリに退避させた ID を消去し、当該 ID を送信済み ID リストに追加しない。

20

【0069】

なお、異常検知装置 110 b、110 c、110 d、110 e および 110 f は、異常検知装置 110 a と同様の構成であり、異常検知装置 110 a と同様のことが言えるため説明は省略する。ただし、異常検知装置 110 b、110 c、110 d、110 e および 110 f に接続される ECU はそれぞれ ECU 101 b、101 c、101 d、101 e および 101 f である点が異なる。

30

【0070】

[1 - 8 . 異常検知機能を有する ECU の構成]

図 8 は、異常検知機能を有する ECU 101 g の構成図である。図 8 において、ECU 101 g は、図 7 に示した異常検知装置 110 a を ECU に実装した場合の構成を示している。具体的には、異常検知装置 110 a が有する機能を異常検知部 110 g として示し、ECU 101 a が有する車両制御等に関する処理を行う機能を ECU 処理部 115 として示している。この場合、異常検知部 110 g (異常検知装置 110 a に対応) は、バス 130 と ECU 処理部 115 (ECU 101 a に対応) の間に配置されることになる。図 8 に示すように、異常検知機能は ECU に直接実装されてもよい。

40

【0071】

[1 - 9 . 受信済み ID リスト例]

図 9 は、受信済み ID リストの一例を示す図である。受信済み ID リストは、受信済み ID リスト保持部 114 に保持される。受信済み ID リスト保持部 114 は、異常検知装置 110 a に接続された ECU 101 a が受信したメッセージの ID、受信済み ID リストに含まれる ID 毎のメッセージ受信回数を記録する領域を持つ。言い換えると、受信済

50

みIDリストには、例えば、異常検知装置110aに接続されたECU101aが受信したメッセージのID、そのIDを持つメッセージの車両10の起動時からのメッセージ受信回数、および、メッセージ受信回数に基づくメッセージ受信頻度（例えば最近1分間の受信回数）が含まれる。なお、ECU101aが受信したメッセージとは、異常検知装置110aがバス130から受信して、異常検知装置110aがECU101aへ送信したメッセージのことである。制御部112は、受信済みIDリスト保持部114を制御することで、受信済みIDリストに含まれるこれらの情報を更新する。具体的には、制御部112は、通信部111がバス130からメッセージを受信して当該メッセージをECU101aへ送信したときに当該メッセージに含まれるIDを受信済みIDリストに追加する。また、制御部112は、メッセージに含まれるIDごとにメッセージをECU101aへ送信した回数を車両10の起動時からカウントすることで、IDごとにECU101aがメッセージを受信した受信回数を更新する。また、制御部112は、例えば、1分ごとに最近1分間の受信回数を更新する。

10

20

30

40

50

【0072】

図9では、IDとして0x25、0x27、0x89のメッセージのそれぞれについて、受信回数および最近1分間の受信回数が受信済みIDリスト保持部114に保持されていることを示している。

【0073】

なお、図9では最近1分間の受信回数が見られているが、最近30分間もしくは最近1時間等の受信回数、または、車両起動時からの受信回数を車両起動時間で割った回数等が保持されるように受信済みIDリスト保持部114を構成してもよい。

【0074】

[1-10. 送信済みIDリスト例]

図10は、送信済みIDリストの一例を示す図である。送信済みIDリストは、送信済みIDリスト保持部113に保持される。送信済みIDリスト保持部113は、異常検知装置110aに接続されたECU101aが送信したメッセージのID、送信済みIDリストに含まれるID毎のメッセージ送信回数を記録する領域を持つ。言い換えると、送信済みIDリストは、異常検知装置110aに接続されたECU101aが送信したメッセージのID、そのIDを持つメッセージの車両10の起動時からのメッセージ送信回数、および、メッセージ送信回数に基づくメッセージ送信頻度（例えば最近1分間の送信回数）が含まれる。なお、ECU101aが送信したメッセージとは、異常検知装置110aがECU101aから受信して、異常検知装置110aがバス130へ送信したメッセージのことである。制御部112は、送信済みIDリスト保持部113を制御することで、送信済みIDリストに含まれるこれらの情報を更新する。具体的には、制御部112は、通信部111がECU101aからメッセージを受信して当該メッセージをバス130へ送信したときに当該メッセージに含まれるIDを送信済みIDリストに追加する。また、制御部112は、メッセージに含まれるIDごとにメッセージをバス130へ送信した回数を車両10の起動時からカウントすることで、IDごとにECU101aがメッセージを送信した送信回数を更新する。また、制御部112は、例えば、1分ごとに最近1分間の送信回数を更新する。

【0075】

図10では、IDとして0x253、0x272、0x349のメッセージのそれぞれについて、送信回数および最近1分間の送信回数が送信済みIDリスト保持部113に保持されていることを示している。

【0076】

なお、図10では最近1分間の送信回数が見られているが、最近30分間または最近1時間等の送信回数等が保持されるように送信済みIDリスト保持部113を構成してもよい。

【0077】

[1-11. 受信済みIDリストのアップデート処理シーケンス]

図 1 1 は、受信済み I D リストのアップデート処理のシーケンスを示す図である。図 1 1 では異常検知装置 1 1 0 a が、受信済み I D リストに存在しない I D のメッセージをバス 1 3 0 から受信した場合の受信済み I D リストのアップデート処理のシーケンスの一例である。

【 0 0 7 8 】

ステップ S 1 1 1 では、バス 1 3 0 から異常検知装置 1 1 0 a にメッセージが送信される。

【 0 0 7 9 】

ステップ S 1 1 2 では、異常検知装置 1 1 0 a がバス 1 3 0 から受信したメッセージの I D を読み出す。

【 0 0 8 0 】

ステップ S 1 1 3 では、異常検知装置 1 1 0 a は、ステップ S 1 1 2 で読み出した I D が受信済み I D リストに存在するか否かを確認し、読み出した I D が受信済み I D リストに存在していないと判断する場合、受信済み I D リストに、読み出した I D を追加する。

【 0 0 8 1 】

ステップ S 1 1 4 では、異常検知装置 1 1 0 a がバス 1 3 0 から受信したメッセージを E C U 1 0 1 a に転送する。

【 0 0 8 2 】

このようにして、異常検知装置 1 1 0 a は、バス 1 3 0 から受信したメッセージの I D を受信済み I D リストに追加していく。つまり、異常検知装置 1 1 0 a は、複数の E C U のうち、自身を介してバス 1 3 0 と接続された E C U 1 0 1 a 以外の E C U がバス 1 3 0 へ送信したメッセージの I D を受信済み I D リストに追加していく。車載ネットワーク 1 0 0 における複数の E C U のそれぞれは、同じ I D を含むメッセージを送信しないという仕様のもとでは、受信済み I D リストは、E C U 1 0 1 a が送信しないメッセージの I D のリストとなる。

【 0 0 8 3 】

[1 - 1 2 . 受信済み I D リストによる異常検知処理シーケンス]

図 1 2 は、受信済み I D リストを用いた異常検知処理のシーケンスを示す図である。図 1 2 では、受信済み I D リストにある I D のメッセージ（つまり、E C U 1 0 1 a が送信しないメッセージ）を E C U 1 0 1 a が送信した場合のシーケンスの一例である。

【 0 0 8 4 】

ステップ S 1 2 1 では、E C U 1 0 1 a から異常検知装置 1 1 0 a にメッセージが送信される。これにより、異常検知装置 1 1 0 a は、E C U 1 0 1 a から送信されたメッセージを受信する。

【 0 0 8 5 】

ステップ S 1 2 2 では、異常検知装置 1 1 0 a が受信したメッセージの I D を読み出す。

【 0 0 8 6 】

ステップ S 1 2 3 では、異常検知装置 1 1 0 a は、ステップ S 1 2 2 で読み出した I D が受信済み I D リストに存在するか否かを確認し、読み出した I D が受信済み I D リストに存在していると判断する。この場合、本来 E C U 1 0 1 a が送信するはずのないメッセージを E C U 1 0 1 a が送信していることになる。つまり、E C U 1 0 1 a が異常なメッセージを送信していることがわかる。

【 0 0 8 7 】

ステップ S 1 2 4 では、異常検知装置 1 1 0 a は、E C U 1 0 1 a が送信したメッセージをバス 1 3 0 へ送信することを中止する。このような場合に、E C U 1 0 1 a からのメッセージをバス 1 3 0 に送信しないようにすることで、異常なメッセージがバス 1 3 0 に流れることを抑制できる。

【 0 0 8 8 】

ステップ S 1 2 5 では、異常検知装置 1 1 0 a は、E C U 1 0 1 a が異常であることを

10

20

30

40

50

バス130に送信し、バス130に接続されたECU101a以外の各ノードにECU101aが異常であることを通知する。例えば、ECU101aに異常があることをECU101a以外の各ノードが認識することで、各ノードは、ECU101aの機能に応じて適切な処理ができる。例えば、ECU101aが車両10の走行に関するECUである場合、各ノードは、車両10を停止させるような処理をすることができる。

【0089】

ステップS126では、異常検知装置110aは、ECU101aが異常であるという通知をECU101a自身に送信する。ECU101aが自身に異常があることを認識することで、ECU101aは、ECU101aの異常の程度にもよるが、例えばフェイルセーフ機能を起動させることができる。

10

【0090】

[1-13.送信済みIDリストのアップデート処理シーケンス]

図13は、送信済みIDリストのアップデート処理のシーケンスを示す図である。図13では、送信済みIDリストに存在しないIDを異常検知装置110aが自身に接続されたECU101aから受信した場合の送信済みIDリストのアップデート処理のシーケンスの一例である。

【0091】

ステップS131では、ECU101aから異常検知装置110aへメッセージが送信される。

20

【0092】

ステップS132では、ECU101aが送信したメッセージを異常検知装置110aが受信し、IDを読み出す。

【0093】

ステップS133では、異常検知装置110aは、ステップS132で読み出したIDが送信済みIDリストに存在するか否かを確認し、読み出したIDが送信済みIDリストに存在していないと判断する場合、送信済みIDリストに、読み出したIDを追加する。

【0094】

ステップS134では、異常検知装置110aがECU101aから受信したメッセージをバス130に転送する。

30

【0095】

このようにして、異常検知装置110aは、ECU101aから受信したメッセージのIDを送信済みIDリストに追加していく。つまり、異常検知装置110aは、複数のECUのうち、自身を介してバス130と接続されたECU101aがバス130へ送信したメッセージのIDを送信済みIDリストに追加していく。車載ネットワーク100における複数のECUのそれぞれは、同じIDを含むメッセージを送信しないという仕様のもとでは、送信済みIDリストは、ECU101a以外のECU等が送信しないメッセージのIDのリストとなる。

【0096】

[1-14.送信済みIDリストによる異常検知処理シーケンス]

図14は、送信済みIDリストを用いた異常検知処理のシーケンスを示す図である。図14では、送信済みIDリストに存在するIDのメッセージ(つまり、ECU101a以外のECU等が送信しないメッセージ)がバス130に送信された場合のシーケンスである。

40

【0097】

ステップS141では、バス130から異常検知装置110aにメッセージが送信される。これにより、異常検知装置110aは、バス130からのメッセージを受信する。

【0098】

ステップS142では、異常検知装置110aが受信したメッセージのIDを読み出す。

【0099】

50

ステップS 1 4 3では、異常検知装置 1 1 0 aは、ステップS 1 4 2で読み出したIDが送信済みIDリストに存在するか否かを確認し、読み出したIDが送信済みIDリストに存在していると判断する。この場合、本来ECU 1 0 1 a以外のECU等が送信するはずのないメッセージをECU 1 0 1 a以外のECU等が送信していることになる。つまり、ECU 1 0 1 a以外のECU等が異常なメッセージを送信していることがわかる。

【 0 1 0 0 】

ステップS 1 4 4では、異常検知装置 1 1 0 aは、バス 1 3 0が送信したメッセージをECU 1 0 1 aへ送信することを中止している。このような場合に、ECU 1 0 1 a以外のECU等からのメッセージをECU 1 0 1 aに送信しないようにすることで、異常なメッセージがECU 1 0 1 aに送信されることを抑制できる。

10

【 0 1 0 1 】

ステップS 1 4 5では、異常検知装置 1 1 0 aは、車載ネットワーク 1 0 0に異常なECU等が存在することをECU 1 0 1 aに通知している。例えば、異常なECU等は、ECU 1 0 1 aが送信するメッセージに含まれるIDを使って不正メッセージを送信しているため、ECU 1 0 1 aになりすまそうとしている可能性がある。このため、ECU 1 0 1 aは、自身が有する機能に応じて適切な処理ができる。例えば、ECU 1 0 1 aが車両 1 0の走行に関するECUである場合、ECU 1 0 1 aは、車両 1 0を停止させるような処理をすることができる。

【 0 1 0 2 】

ステップS 1 4 6では、異常検知装置 1 1 0 aは、車載ネットワーク 1 0 0に異常なECU等が存在することをバス 1 3 0に通知する。つまり、異常検知装置 1 1 0 aは、バス 1 3 0に接続されたECU 1 0 1 a以外のECU 1 0 1 b、1 0 1 c、1 0 1 d、1 0 1 e、1 0 1 fにその旨を通知する。これにより、各ECUは、ECU 1 0 1 aが有する機能に応じて適切な処理ができる。

20

【 0 1 0 3 】

[1 - 1 5 . I D S E C Uが異常を検知した場合のシーケンス]

図 1 1から図 1 4では、送信済みIDリストに含まれるIDおよび受信済みIDリストに含まれるIDが正規なIDであるとして説明した。基本的には、車両 1 0が起動してすぐに各ECUからのメッセージの送信が開始され、送信済みIDリストおよび受信済みIDリストには、すぐに正規のIDが追加されることになるためである。

30

【 0 1 0 4 】

しかし、車両 1 0が起動した後、送信済みIDリストおよび受信済みIDリストに正規のIDが追加される前に、攻撃者によって攻撃を受けて異常なIDが送信済みIDリストまたは受信済みIDリストに追加される場合も考えられる。

【 0 1 0 5 】

以下では、正規のIDが追加される前に、異常なID（例えばECU 1 0 1 aが送信する正規のメッセージに含まれるID）が異常検知装置 1 1 0 aの受信済みIDリストに追加された場合の処理について説明する。

【 0 1 0 6 】

図 1 5は、IDSECU 1 2 0が異常を検知した場合の処理のシーケンスを示す図である。図 1 5では、図 3に示すように、車載ネットワーク 1 0 0にIDSECU 1 2 0が存在する場合に、IDSECU 1 2 0が異常を検知した場合の処理のシーケンスの一例である。IDSECU 1 2 0が異常を検知した場合は、検知した異常なメッセージに含まれる異常なIDを異常検知装置 1 1 0 aが保持する受信済みIDリストから消去する。

40

【 0 1 0 7 】

ステップS 1 5 1では、バス 1 3 0からIDSECU 1 2 0へメッセージが送信される。

【 0 1 0 8 】

ステップS 1 5 2では、IDSECU 1 2 0が受信したメッセージの異常判定を行い、受信したメッセージは異常と判定する。

50

【0109】

ステップS153では、IDSEC U120は、異常と判定したメッセージの異常なIDを示す異常ID情報をバス130へ送信する。

【0110】

ステップS154では、バス130に送信された、IDSEC U120で異常と判定されたメッセージについての異常ID情報を、バス130に接続された異常検知装置110aは受信する。なお、IDSEC U120で異常と判定されたメッセージについての異常ID情報は、バス130に接続された全ての異常検知装置、すなわち、異常検知装置110a、110b、110d、110fに通知される。

【0111】

ステップS155では、異常検知装置110aが受信済みIDリストから、IDSEC U120で異常と判定されたメッセージのID（つまり、異常ID情報が示すID）を消去する。

【0112】

このように、正規メッセージがバス130に流れる前に、攻撃者が不正メッセージをバス130へ送信した場合であっても、受信済みIDリストを修正して、受信済みIDリストに追加された不正メッセージに含まれるID（例えばECU101aが送信するメッセージに含まれるID）を受信済みIDリストから消去することで正規メッセージ（例えば正規なECU101aが送信するメッセージ）を不正メッセージであると異常検知装置110aが誤検知することを防止することが可能である。すなわち、正規なECU101aが送信するメッセージに含まれるIDが受信済みIDリストに存在しなくなるため、正規なECU101aからバス130へのメッセージの送信が可能となる。

【0113】

[1-16. 異常検知装置の全体処理フロー]

図16は、実施の形態1における異常検知装置110aの全体処理のフローチャートである。異常検知装置110aは、異常検知装置110aに接続されるECU101aとバス130間で送受信されるメッセージを受信し、メッセージがバス130からECU101aへ送信されたものか、ECU101aからバス130へ送信されたものかに応じて受信済みIDリストまたは送信済みIDリストの更新とメッセージの異常判定を行い、異常を検知した場合はECU101aまたはバス130へのメッセージの転送を中止する。

【0114】

ステップS161では、異常検知装置110aがバス130または、異常検知装置110aに接続されたECU101aからメッセージを受信する。

【0115】

ステップS162では、異常検知装置110aは、受信したメッセージがECU101aから送信されたメッセージか、バス130から送信されたメッセージかを判定する。例えば、異常検知装置110aは、ECU101aに接続された入出力端子と、バス130に接続された入出力端子を有し、どちらの入出力端子からメッセージを受信したかに応じて上記判定を行ってもよい。

【0116】

ステップS163およびS164は、受信したメッセージがバス130から送信された場合（ステップS162で「バス」の場合）の処理であり、異常検知装置110aは、受信済みIDリストの更新処理および、送信済みIDリストによる異常検知処理を行う。

【0117】

ステップS165およびステップS166は、受信したメッセージがECU101aから送信された場合（ステップS162で「ECU」の場合）の処理であり、異常検知装置110aは、送信済みIDリスト更新処理および、受信済みIDリストによる異常検知処理を行う。

【0118】

ステップS163は、図17を用いて後述し、ステップS164は、図21を用いて後

10

20

30

40

50

述し、ステップS 1 6 5は、図 1 8を用いて後述し、ステップS 1 6 6は、図 1 9および図 2 0を用いて後述する。

【 0 1 1 9 】

[1 - 1 7 . 受信済み I D リスト更新処理フロー]

図 1 7は、受信済み I D リスト更新処理のフローチャートである。図 1 7は、図 1 6のステップS 1 6 3の受信済み I D リスト更新処理の詳細な処理フローである。異常検知装置 1 1 0 aは、バス 1 3 0からメッセージが送信された際に、受信済み I D リスト保持部 1 1 4に保持している受信済み I D リストを更新する。

【 0 1 2 0 】

ステップS 1 7 1では、異常検知装置 1 1 0 aは、バス 1 3 0から受信したメッセージの I Dを読み出す。

10

【 0 1 2 1 】

ステップS 1 7 2では、異常検知装置 1 1 0 aは、受信済み I D リストにステップS 1 7 1で読み出した I Dが存在するか否かを判断する。

【 0 1 2 2 】

異常検知装置 1 1 0 aは、受信済み I D リストに読み出した I Dが存在しない場合（ステップS 1 7 2で N Oの場合）は、ステップS 1 7 3で、受信済み I D リストに読み出した I Dを追加する。異常検知装置 1 1 0 aは、受信済み I D リストに読み出した I Dが存在する場合（ステップS 1 7 2で Y E Sの場合）は、ステップS 1 7 4の処理を行う。

【 0 1 2 3 】

ステップS 1 7 4では、異常検知装置 1 1 0 aは、読み出した I Dについて、受信済み I D リスト保持部 1 1 4に記録されるメッセージ受信回数をインクリメントして更新する。

20

【 0 1 2 4 】

[1 - 1 8 . 送信済み I D リスト更新処理フロー]

図 1 8は、送信済み I D リスト更新処理のフローチャートである。図 1 8は、図 1 6のステップS 1 6 5の送信済み I D リスト更新処理の詳細な処理フローである。異常検知装置 1 1 0 aは、E C U 1 0 1 aからメッセージが送信された際に、送信済み I D リスト保持部 1 1 3に保持している送信済み I D リストを更新する。

【 0 1 2 5 】

ステップS 1 8 1では、異常検知装置 1 1 0 aは、E C U 1 0 1 aから受信したメッセージの I Dを読み出す。

30

【 0 1 2 6 】

ステップS 1 8 2では、異常検知装置 1 1 0 aは、送信済み I D リストにステップS 1 8 1で読み出した I Dが存在するか否かを判断する。

【 0 1 2 7 】

異常検知装置 1 1 0 aは、送信済み I D リストに読み出した I Dが存在しない場合（ステップS 1 8 2で N Oの場合）は、ステップS 1 8 3で、送信済み I D リストに読み出した I Dを追加する。異常検知装置 1 1 0 aは、送信済み I D リストに読み出した I Dが存在する場合（ステップS 1 8 2で Y E Sの場合）は、ステップS 1 8 4の処理を行う。

40

【 0 1 2 8 】

ステップS 1 8 4では、異常検知装置 1 1 0 aは、読み出した I Dについて、送信済み I D リスト保持部 1 1 3に記録されるメッセージ送信回数をインクリメントして更新する。

【 0 1 2 9 】

[1 - 1 9 . 受信済み I D リストによる異常検知処理フロー]

図 1 9は、受信済み I D リストによる異常検知処理のフローチャートである。図 1 9は、図 1 6のステップS 1 6 6の受信済み I D リストによる、異常検知装置 1 1 0 aに接続された E C U 1 0 1 aの異常検知処理の詳細な処理フローである。

【 0 1 3 0 】

50

ステップS 1 9 1では、異常検知装置 1 1 0 aは、ECU 1 0 1 aから受信したメッセージのIDを読み出す。

【0 1 3 1】

ステップS 1 9 2では、異常検知装置 1 1 0 aは、読み出したIDが受信済みIDリストに存在するか否かを判断する。

【0 1 3 2】

異常検知装置 1 1 0 aは、読み出したIDが受信済みIDリストに存在する場合（ステップS 1 9 2でYESの場合）、ECU 1 0 1 aから受信したメッセージが異常であると検知して、ステップS 1 9 3、S 1 9 4およびS 1 9 5の処理を行う。異常検知装置 1 1 0 aは、読み出したIDが受信済みIDリストに存在しない場合（ステップS 1 9 2でNOの場合）、ECU 1 0 1 aから受信したメッセージは正常であると検知して、ステップS 1 9 6の処理を行う。

10

【0 1 3 3】

ステップS 1 9 3では、異常検知装置 1 1 0 aは、受信したメッセージを破棄する。つまり、異常検知装置 1 1 0 aは、ECU 1 0 1 aから受信したメッセージをバス1 3 0へ送信しない。ECU 1 0 1 aからのメッセージをバス1 3 0に送信しないようにすることで、異常なメッセージがバス1 3 0に流れることを抑制できる。

【0 1 3 4】

ステップS 1 9 4では、異常検知装置 1 1 0 aは、ECU 1 0 1 aが異常であるとバス1 3 0に通知する。

20

【0 1 3 5】

ステップS 1 9 5では、異常検知装置 1 1 0 aは、ECU 1 0 1 aにECU 1 0 1 aが異常であると通知する。

【0 1 3 6】

一方で、ステップS 1 9 6では、異常検知装置 1 1 0 aは、ECU 1 0 1 aから受信したメッセージは正常なため、バス1 3 0へ当該メッセージを転送する。

【0 1 3 7】

[1 - 2 0 . 受信済みIDリストによる異常検知処理フロー（変形例）]

図20は、受信済みIDリストによる異常検知処理の変形例のフローチャートである。図20は、図16のステップS 1 6 6の受信済みIDリストによる異常検知処理の変形例の詳細な処理フローである。図19における受信済みIDリストによる異常検知処理では、受信したメッセージのIDが受信済みIDリストに存在する場合、異常検知装置 1 1 0 aは、ステップS 1 9 3にて受信したメッセージを破棄しバス1 3 0に転送しないという処理を行うようにしたが、図20の変形例では、ステップS 1 9 3の処理を実施せず、代わりにステップS 2 0 1の処理を実施する。具体的には、異常検知装置 1 1 0 aは、ECU 1 0 1 aをバス1 3 0から隔離する。より具体的には、異常検知装置 1 1 0 aは、ECU 1 0 1 aから受信するメッセージをすべて遮断する。これにより、ECU 1 0 1 aをバス1 3 0から隔離し被害が拡大することを防止して、異常メッセージのみを遮断する場合と比べて、車載ネットワーク1 0 0に不正なECUが与える影響をより軽減できる。なお、例えば、異常検知装置 1 1 0 aとECU 1 0 1 aとの間に異常検知装置 1 1 0 aとECU 1 0 1 aとの接続および非接続を切り替えるスイッチが設けられていてもよく、当該スイッチの切り替えによって異常検知装置 1 1 0 aとECU 1 0 1 aと接続されないようにすることで、ECU 1 0 1 aをバス1 3 0から隔離してもよい。

30

40

【0 1 3 8】

[1 - 2 1 . 送信済みIDリストによる異常検知処理フロー]

図21は、送信済みIDリストによる異常検知処理のフローチャートである。図21は、図16のステップS 1 6 4の送信済みIDリストによる、バス1 3 0に存在するECUの異常検知処理の詳細な処理フローである。

【0 1 3 9】

ステップS 2 1 1では、異常検知装置 1 1 0 aは、バス1 3 0から受信したメッセージ

50

のIDを読み出す。

【0140】

ステップS212では、異常検知装置110aは、読み出したIDが送信済みIDリストに存在するか否かを判断する。

【0141】

異常検知装置110aは、読み出したIDが送信済みIDリストに存在する場合（ステップS212でYESの場合）、バス130から受信したメッセージが異常であると検知して、ステップS213、S214およびS215の処理を行う。異常検知装置110aは、読み出したIDが送信済みIDリストに存在しない場合（ステップS212でNOの場合）、バス130から受信したメッセージは正常であると検知して、ステップS216の処理を行う。

10

【0142】

ステップS213では、異常検知装置110aは、受信したメッセージを破棄する。つまり、異常検知装置110aは、バス130から受信したメッセージをECU101aへ送信しない。バス130に存在するECUからのメッセージをECU101aに送信しないようにすることで、異常なメッセージがECU101aに送信されることを抑制できる。

【0143】

ステップS214では、異常検知装置110aは、バス130に異常なECUが存在することをバス130に通知する。

20

【0144】

ステップS215では、異常検知装置110aは、ECU101aにバス130に異常なECUが存在することを通知する。

【0145】

一方で、ステップS216では、異常検知装置110aは、バス130から受信したメッセージは正常なため、ECU101aへ当該メッセージを転送する。

【0146】

以上のように、車載ネットワーク100内に必ずしもIDSECU120を追加（つまり、ネットワークトラフィックおよびコストが増大）したり、各ECUが送信するメッセージのIDを予め記憶させておいたりすることなく、車載ネットワーク100における異常を容易に検知できる。

30

【0147】

[1-22. 異常検知装置がIDSECUから異常通知を受信した場合の処理フロー]

図22は、異常検知装置がIDSECU120から異常通知を受信した場合の処理のフローチャートである。なお、図22には、異常検知装置がIDSECU120から異常通知を受信する前のIDSECU120での処理（ステップS221からステップS224）についても示している。

【0148】

ステップS221では、IDSECU120がバス130からメッセージを受信する。

【0149】

ステップS222では、IDSECU120は受信したメッセージの異常判定を行う。

40

【0150】

ステップS223では、ステップS222の異常判定の結果が異常か否かを判断する。IDSECU120は、異常判定の結果が異常である場合（ステップS223でYESの場合）、ステップS224の処理を行い、異常判定の結果が異常でない場合（ステップS223でNOの場合）、処理を終了する。

【0151】

ステップS224では、IDSECU120は、異常と判定したメッセージに含まれる異常なIDを示す異常ID情報をバス130に接続されている異常検知装置110a、110b、110dおよび110fに通知する。ここでは、異常検知装置110aに着目し

50

て説明する。

【0152】

ステップS225では、異常検知装置110aが、IDSECU120から送信された異常なIDを示す異常ID情報をバス130から受信する。異常検知装置110aは、IDSECU120から送信された異常なIDを示す異常ID情報をバス130から受信した場合に、受信済みIDリストから異常ID情報が示すIDを消去する。具体的には以下の処理が行われる。

【0153】

ステップS226では、異常検知装置110aは、受信した異常ID情報が示す異常なIDが受信済みIDリストに存在するか否かを判断する。異常なIDが受信済みIDリストに存在する場合（ステップS226でYESの場合）は、異常検知装置110aは、ステップS227の処理を行い、異常なIDが受信済みIDリストに存在しない場合（ステップS226でNOの場合）は、異常検知装置110aは、処理を終了する。

【0154】

ステップS227では、異常検知装置110aは、受信済みIDリストから異常なIDを消去する。

【0155】

正規メッセージがバス130に流れる前に、攻撃者が不正メッセージをバス130へ送信する場合が考えられる。この場合、受信済みIDリストに不正メッセージに含まれるIDが追加されることになる。例えば、正規なECU101aが送信するメッセージに含まれるIDが不正メッセージに含まれる場合、正規なECU101aから送信される正規メッセージが不正メッセージであると判定されてしまう。つまり、以降は、正規メッセージがバス130へ送信されず、攻撃者がECU101aになりすまして不正メッセージがバス130へ送信されることになる。これに対して、上記説明のように、例えばIDSECU120が車載ネットワーク100に配置されることで、攻撃者が送信した不正メッセージを検知することが可能となる。したがって、正規メッセージがバス130に流れる前に、攻撃者が不正メッセージをバス130へ送信した場合（つまり、受信済みIDリストが汚染された場合）であっても、受信済みIDリストを修正して、受信済みIDリストに追加された不正メッセージに含まれるID（例えばECU101aが送信するメッセージに含まれるID）を受信済みIDリストから消去することで正規メッセージを不正メッセージであると異常検知装置110aが誤検知することを防止することが可能である。

【0156】

[1-23. 異常検知装置の全体処理フロー（変形例）]

図23は、異常検知装置110aの全体処理の変形例を記載したフローチャートである。図23は、図16の異常検知装置110aの全体処理のフローチャートの変形例である。具体的には、図23では、図16の全体処理に加えて、ステップS167の車両シャットダウン操作があるか否かの判断の処理、ステップS231の車両10の起動時の処理、および、ステップS232の車両10のシャットダウン時の処理が追加されている。

【0157】

ステップS231は、後ほど図27にて詳細に説明する。

【0158】

ステップS167では、異常検知装置110aは、車両シャットダウン操作があれば（ステップS167でYESの場合）、ステップS232を行い、車両シャットダウン操作がなければ（ステップS167でNOの場合）、ステップS161に戻る。ステップS232については、図24から図26にて詳細に説明する。

【0159】

[1-24. 車両シャットダウン時の処理フロー]

図24は、異常検知装置110aの車両シャットダウン時の処理のフローチャートである。図24は、図23のステップS232の異常検知装置110aの車両シャットダウン時の処理の詳細なフローチャートである。

10

20

30

40

50

【 0 1 6 0 】

ステップ S 2 4 1 では、異常検知装置 1 1 0 a は、低頻度受信済み I D 退避処理を行う。ステップ S 2 4 1 の処理は、図 2 5 にて詳細に説明する。

【 0 1 6 1 】

ステップ S 2 4 2 では、異常検知装置 1 1 0 a は、低頻度送信済み I D 退避処理を行う。ステップ S 2 4 2 の処理は、図 2 6 にて詳細に説明する。

【 0 1 6 2 】

[1 - 2 5 . 低頻度受信済み I D の退避処理フロー]

図 2 5 は、低頻度受信済み I D の退避の処理のフローチャートである。図 2 5 は、図 2 4 のステップ S 2 4 1 の低頻度受信済み I D 退避処理の詳細な処理のフローチャートである。

10

【 0 1 6 3 】

ステップ S 2 5 1 では、異常検知装置 1 1 0 a は、受信済み I D リストから、低頻度受信済み I D の退避の処理においてまだ選択していない I D を選択する。

【 0 1 6 4 】

ステップ S 2 5 2 では、異常検知装置 1 1 0 a は、選択した I D について、受信済み I D リスト保持部 1 1 4 に記録されたメッセージ受信回数に基づくメッセージ受信頻度を算出する。例えば、異常検知装置 1 1 0 a は、メッセージ受信回数を車両 1 0 の起動からシャットダウンまでの時間で割ることでメッセージ受信頻度を算出する。なお、異常検知装置 1 1 0 a は、選択した I D について、受信済み I D リスト保持部 1 1 4 に記録されたメッセージ受信回数を取得してもよい。メッセージ受信回数は、例えば、シャットダウン前最近 1 分間、3 0 分間または 1 時間等の所定の時間に E C U 1 0 1 a がバス 1 3 0 からメッセージを受信した回数であってもよい。

20

【 0 1 6 5 】

ステップ S 2 5 3 では、異常検知装置 1 1 0 a は、ステップ S 2 5 2 で算出したメッセージ受信頻度が予め設定した所定の値以下であるか否かの判断を行う。異常検知装置 1 1 0 a は、メッセージ受信頻度が所定の値以下ならば（ステップ S 2 5 3 で Y E S の場合）、メッセージ受信頻度が所定の値以下となっている I D を低頻度受信済み I D と判断し、ステップ S 2 5 4 の処理を行い、メッセージ受信頻度が所定の値よりも大きいならば（ステップ S 2 5 3 で N O の場合）、ステップ S 2 5 5 の処理を行う。なお、異常検知装置 1 1 0 a は、ステップ S 2 5 2 で、選択した I D について、受信済み I D リスト保持部 1 1 4 に記録されたメッセージ受信回数を取得する場合、ステップ S 2 5 2 で取得したメッセージ受信回数が予め設定した所定の値以下であるか否かの判断を行ってもよい。そして、異常検知装置 1 1 0 a は、メッセージ受信回数が所定の値以下ならば、メッセージ受信回数が所定の値以下となっている I D を低頻度受信済み I D と判断し、ステップ S 2 5 4 の処理を行い、メッセージ受信回数が所定の値よりも大きいならば、ステップ S 2 5 5 の処理を行う。このように、メッセージ受信回数が少なければメッセージ受信頻度も低いとみなすことで、ステップ S 2 5 2 においてメッセージ受信回数からメッセージ受信頻度を算出せず、メッセージ受信回数を取得するだけでもよい。

30

【 0 1 6 6 】

ステップ S 2 5 4 では、異常検知装置 1 1 0 a は、選択した I D を不揮発性メモリに退避させる。

40

【 0 1 6 7 】

そして、ステップ S 2 5 5 では、異常検知装置 1 1 0 a は、受信済み I D リストに未選択の I D が存在するか否かを判定し、存在する場合（ステップ S 2 5 5 で Y E S の場合）は、ステップ S 2 5 1 に戻り、存在しない場合（ステップ S 2 5 5 で N O の場合）は、処理を終了する。これにより、複数の低頻度受信済み I D を不揮発性メモリに退避することができる。

【 0 1 6 8 】

[1 - 2 6 . 低頻度送信済み I D の退避処理フロー]

50

図 2 6 は、低頻度送信済み I D の退避の処理フローチャートである。図 2 6 は、図 2 4 のステップ S 2 4 2 の低頻度送信済み I D 退避処理の詳細な処理のフローチャートである。

【 0 1 6 9 】

ステップ S 2 6 1 では、異常検知装置 1 1 0 a は、送信済み I D リストから、低頻度送信済み I D の退避の処理においてまだ選択していない I D を選択する。

【 0 1 7 0 】

ステップ S 2 6 2 では、異常検知装置 1 1 0 a は、選択した I D について、送信済み I D リスト保持部 1 1 3 に記録されたメッセージ送信回数に基づくメッセージ送信頻度を算出する。例えば、異常検知装置 1 1 0 a は、メッセージ送信回数を車両 1 0 の起動からシャットダウンまでの時間で割ることでメッセージ送信頻度を算出する。なお、異常検知装置 1 1 0 a は、選択した I D について、送信済み I D リスト保持部 1 1 3 に記録されたメッセージ送信回数を取得してもよい。メッセージ送信回数は、シャットダウン前最近 1 分間、30 分間または 1 時間等の所定の時間に E C U 1 0 1 a がバス 1 3 0 へメッセージを送信した回数であってもよい。

10

【 0 1 7 1 】

ステップ S 2 6 3 では、異常検知装置 1 1 0 a は、ステップ S 2 6 2 で算出したメッセージ送信頻度が予め設定した所定の値以下であるか否かの判定を行う。異常検知装置 1 1 0 a は、メッセージ送信頻度が所定の値以下ならば（ステップ S 2 6 3 で Y E S の場合）、メッセージ送信頻度が所定の値以下となっている I D を低頻度送信済み I D と判断し、ステップ S 2 6 4 の処理を行い、メッセージ送信頻度が所定の値よりも大きいならば（ステップ S 2 6 3 で N O の場合）、ステップ S 2 6 5 の処理を行う。なお、異常検知装置 1 1 0 a は、ステップ S 2 6 2 で、選択した I D について、送信済み I D リスト保持部 1 1 3 に記録されたメッセージ送信回数を取得する場合、ステップ S 2 6 2 で取得したメッセージ送信回数が予め設定した所定の値以下であるか否かの判断を行ってもよい。そして、異常検知装置 1 1 0 a は、メッセージ送信回数が所定の値以下ならば、メッセージ送信回数が所定の値以下となっている I D を低頻度送信済み I D と判断し、ステップ S 2 6 4 の処理を行い、メッセージ送信回数が所定の値よりも大きいならば、ステップ S 2 6 5 の処理を行う。このように、メッセージ送信回数が少なければメッセージ送信頻度も低いとみなすことで、異常検知装置 1 1 0 a は、ステップ S 2 6 2 においてメッセージ送信回数からメッセージ送信頻度を算出せず、メッセージ送信回数を取得するだけでもよい。

20

30

【 0 1 7 2 】

ステップ S 2 6 4 では、異常検知装置 1 1 0 a は、選択した I D を不揮発性メモリに退避させる。

【 0 1 7 3 】

そして、ステップ S 2 6 5 では、異常検知装置 1 1 0 a は、送信済み I D リストに未選択の I D が存在するか否かを判定し、存在する場合（ステップ S 2 5 5 で Y E S の場合）は、ステップ S 2 6 1 に戻り、存在しない場合（ステップ S 2 5 5 で N O の場合）は、処理を終了する。これにより、複数の低頻度送信済み I D を不揮発性メモリに退避することができる。

40

【 0 1 7 4 】

[1 - 2 7 . 車両起動時の処理フロー]

図 2 7 は、異常検知装置 1 1 0 a の車両起動時の処理のフローチャートである。図 2 7 は、図 2 3 のステップ S 2 3 1 の異常検知装置 1 1 0 a の車両起動時の詳細な処理のフローチャートである。

【 0 1 7 5 】

ステップ S 2 7 1 では、異常検知装置 1 1 0 a は、車両 1 0 の起動時に、異常検知装置 1 1 0 a に接続された E C U 1 0 1 a のファームウェア情報を確認する。

【 0 1 7 6 】

そして、ステップ S 2 7 2 では、異常検知装置 1 1 0 a は、現在のファームウェア情報

50

を次回の車両 10 の起動時に行うステップ S 2 7 1 の処理で使用するために退避する。

【 0 1 7 7 】

次に、ステップ S 2 7 3 では、異常検知装置 1 1 0 a は、前回の車両 10 の起動時から ECU 1 0 1 a のファームウェア情報が変更（更新）されているか否かを判断する。ファームウェア情報が変更されている場合（ステップ S 2 7 3 で Y E S の場合）は、異常検知装置 1 1 0 a は、ステップ S 2 7 4 の処理を行う。ファームウェア情報が変更されていない場合（ステップ S 2 7 3 で N O の場合）は、異常検知装置 1 1 0 a は、ステップ S 2 7 6 の処理を行う。なお、車両 10 の初回起動時は、前回のファームウェア情報は存在しないので、ファームウェア情報が変更されていないものとして扱う。また、車両 10 の前回の起動時の ECU 1 0 1 a のファームウェア情報は、前回の起動時のステップ S 2 7 2 の処理で退避されている。つまり、車両 10 が起動するごとに、図 2 7 に示す処理が行われる。

10

【 0 1 7 8 】

ステップ S 2 7 4 では、異常検知装置 1 1 0 a は、図 2 5 のステップ S 2 5 4 にて不揮発性メモリに退避していた低頻度受信済み I D をリセットする。

【 0 1 7 9 】

さらに、ステップ S 2 7 5 では、異常検知装置 1 1 0 a は、図 2 6 のステップ S 2 6 4 にて不揮発性メモリに退避していた低頻度送信済み I D をリセットする。

【 0 1 8 0 】

ECU のファームウェアアップデートに伴い ECU のファームウェア情報が変更された場合、ECU から送信されるメッセージに含まれる I D の仕様変更されることがある。したがって、この場合に、不揮発性メモリに退避させた I D を消去し、当該 I D を受信済み I D リストまたは送信済み I D リストに追加しないようにすることで、仕様変更された I D が原因で発生する正常メッセージの誤遮断を防止することが可能である。

20

【 0 1 8 1 】

ステップ S 2 7 6 では、異常検知装置 1 1 0 a は、図 2 5 のステップ S 2 5 4 にて不揮発性メモリに退避していた低頻度受信済み I D を異常検知装置 1 1 0 a の受信済み I D リストに読み込む。

【 0 1 8 2 】

メッセージ受信回数またはメッセージ受信頻度が所定の値以下となっている I D （低頻度で受信されるメッセージに含まれる I D ）は、車両 10 が起動した後、当該 I D を含むメッセージがバス 1 3 0 を流れるまでに時間を要する場合がある。つまり、当該 I D を含む正規メッセージがバス 1 3 0 を流れるまでに、攻撃者が当該 I D を含む不正メッセージをバス 1 3 0 へ送信して、受信済み I D リストに不正メッセージに含まれる I D が追加されてしまう（言い換えると、受信済み I D リストが不正な I D で汚染されてしまう）場合がある。これに対して、車両 10 の起動時に、不揮発性メモリに退避させた低頻度で受信されるメッセージに含まれる I D を受信済み I D リストに追加することで、低頻度で受信されるメッセージが最初にネットワークバスに流れる前に攻撃者が不正メッセージを送信することによる受信済み I D リストの汚染を防ぐことが可能である。また、高頻度に受信されるメッセージの含まれる I D を不揮発性メモリに退避させないことで、その分メモリ容量を削減することが可能である。

30

40

【 0 1 8 3 】

さらに、ステップ S 2 7 7 では、異常検知装置 1 1 0 a は、図 2 6 のステップ S 2 6 4 にて不揮発性メモリに退避していた低頻度送信済み I D を異常検知装置 1 1 0 a の送信済み I D リストに読み込む。

【 0 1 8 4 】

メッセージ送信回数またはメッセージ送信頻度が所定の値以下となっている I D （低頻度で ECU 1 0 1 a から送信されるメッセージに含まれる I D ）は、車両 10 が起動した後、当該 I D を含むメッセージを異常検知装置 1 1 0 a が ECU 1 0 1 a から受信するまでに時間を要する場合がある。つまり、当該 I D を含む正規メッセージを異常検知装置 1

50

10 a が受信するまでに、攻撃者が ECU 101 a を攻撃して不正な ECU 101 a から不正メッセージを異常検知装置 110 a へ送信して、送信済み ID リストに不正メッセージに含まれる ID が追加されてしまう（言い換えると、送信済み ID リストが不正な ID で汚染されてしまう）場合がある。これに対して、車両 10 の起動時に、不揮発性メモリに退避させた低頻度で送信されるメッセージに含まれる ID を送信済み ID リストに追加することで、低頻度で送信されるメッセージを異常検知装置 110 a が受信する前に攻撃者が不正メッセージを送信することによる送信済み ID リストの汚染を防ぐことが可能である。また、高頻度で送信されるメッセージに含まれる ID を不揮発性メモリに退避させないことで、その分メモリ容量を削減することが可能である。

【0185】

なお、異常検知装置 110 a は、車両 10 の起動時に、ファームウェア情報の確認を行わず、不揮発性メモリに退避させた ID を受信済み ID リストまたは送信済み ID リストに追加してもよい。つまり、車両 10 の起動時にステップ S 271 からステップ S 275 の処理が行われず、ステップ S 276 およびステップ S 277 の処理が行われてもよい。

【0186】

（他の実施の形態）

例えば、上記実施の形態では、異常検知装置は、送信済み ID リスト保持部 113 を備えていたが、備えていなくてもよい。この場合、制御部 112 は、送信済み ID リスト保持部 113 に関連する制御を行わなくてもよい。

【0187】

また、例えば、上記実施の形態では、異常検知装置は、受信済み ID リスト保持部 114 を備えていたが、備えていなくてもよい。この場合、制御部 112 は、受信済み ID リスト保持部 114 に関連する制御を行わなくてもよい。

【0188】

また、例えば、上記実施の形態では、制御部 112 は、通信部 111 が ECU から受信したメッセージの ID が受信済み ID リストに存在する場合に、当該 ECU をバス 130 から隔離するとしたが、隔離しなくてもよく、当該メッセージをバス 130 へ送信しないようにするのみでもよい。

【0189】

また、例えば、上記実施の形態では、受信済み ID リスト保持部 114 は、受信済み ID リストに含まれる ID 毎のメッセージ受信回数を記録する領域を持っているとしたが、持っていないともよい。この場合、制御部 112 は、メッセージ受信回数に関連する制御を行わなくてもよい。

【0190】

また、例えば、上記実施の形態では、送信済み ID リスト保持部 113 は、送信済み ID リストに含まれる ID 毎のメッセージ送信回数を記録する領域を持っているとしたが、持っていないともよい。この場合、制御部 112 は、メッセージ送信回数に関連する制御を行わなくてもよい。

【0191】

本開示の車載ネットワーク 100 は、典型的には上述のとおり車載の CAN ネットワークであるが、これに限定されない。例えば、CAN-FD (CAN with Flexible Data rate)、FlexRay (登録商標)、Ethernet (登録商標)、LIN (Local Interconnect Network)、MOST (Media Oriented Systems Transport) などのネットワークであってもよい。あるいはこれらのネットワークをサブネットワークとして、CAN ネットワークと組み合わせた車載ネットワークであってもよい。

【0192】

また、上記実施の形態では、自動車に搭載される車載ネットワーク 100 におけるセキュリティ対策として説明したが、本開示の適用範囲はこれに限られない。本開示は、自動車に限らず、建機、農機、船舶、鉄道、飛行機などのモビリティにも適用してもよい。す

10

20

30

40

50

なわち、本開示は、モビリティネットワークおよびモビリティネットワークシステムにおけるサイバーセキュリティ対策として適用可能である。

【0193】

上記の実施の形態における各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。RAMまたはハードディスクユニットには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

10

【0194】

上記の実施の形態における各装置は、構成する構成要素の一部または全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。RAMには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

【0195】

また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部またはすべてを含むように1チップ化されてもよい。

20

【0196】

また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路または汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用してもよい。

【0197】

さらには、半導体技術の進歩または派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

30

【0198】

上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なICカードまたは単体のモジュールから構成されているとしてもよい。ICカードまたはモジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。ICカードまたはモジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、ICカードまたはモジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

40

【0199】

本開示は、異常検知装置として実現できるだけでなく、異常検知装置を構成する各構成要素が行うステップ(処理)を含む異常検知方法として実現できる。

【0200】

異常検知方法は、複数のECUと、バス130と、異常検知装置から構成される車載ネットワーク100に配置される異常検知装置により実行される異常検知方法であって、異常検知装置は、バス130と複数のECUのうちのいずれかの第1ECUの間に配置され、前記第1ECUからメッセージを受信して当該メッセージをバス130へ送信し、バス130からメッセージを受信して当該メッセージを前記第1ECUへ送信する通信部111と、通信部111がバス130から受信し前記第1ECUへ送信したメッセージのID

50

のリストである受信済みIDリストを保持する受信済みIDリスト保持部114と、を備え、異常検知方法では、通信部111がバス130から受信したメッセージのIDが受信済みIDリストに存在しない場合(図17のステップS172でNoの場合)に、当該IDを受信済みIDリストに追加し(図17のステップS173)、通信部111が前記第1ECUから受信したメッセージのIDが受信済みIDリストに存在する場合(図19のステップS192でYes)に、当該メッセージをバス130へ送信しない(図19のステップS193)ことを特徴とする。

【0201】

また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、コンピュータプログラムからなるデジタル信号であるとしてもよい。

10

【0202】

また、本開示は、コンピュータプログラムまたはデジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(登録商標)Disc)、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されているデジタル信号であるとしてもよい。

【0203】

また、本開示は、コンピュータプログラムまたはデジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

20

【0204】

また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムにしたがって動作するとしてもよい。

【0205】

また、プログラムまたはデジタル信号を記録媒体に記録して移送することにより、またはプログラムまたはデジタル信号を、ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0206】

以上、一つまたは複数の態様に係る異常検知装置などについて、実施の形態に基づいて説明したが、本開示は、この実施の形態に限定されるものではない。本開示の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したもの、および異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

30

【0207】

例えば、上記実施の形態において、特定の構成要素が実行する処理を特定の構成要素の代わりに別の構成要素が実行してもよい。また、複数の処理の順序が変更されてもよいし、複数の処理が並行して実行されてもよい。

【産業上の利用可能性】

【0208】

本開示は、車載ネットワークを搭載した車両等に利用可能である。

40

【符号の説明】

【0209】

10 車両

100 車載ネットワーク

101a、101b、101c、101d、101e、101f、101g ECU

110a、110b、110c、110d、110e、110f 異常検知装置

110g 異常検知部

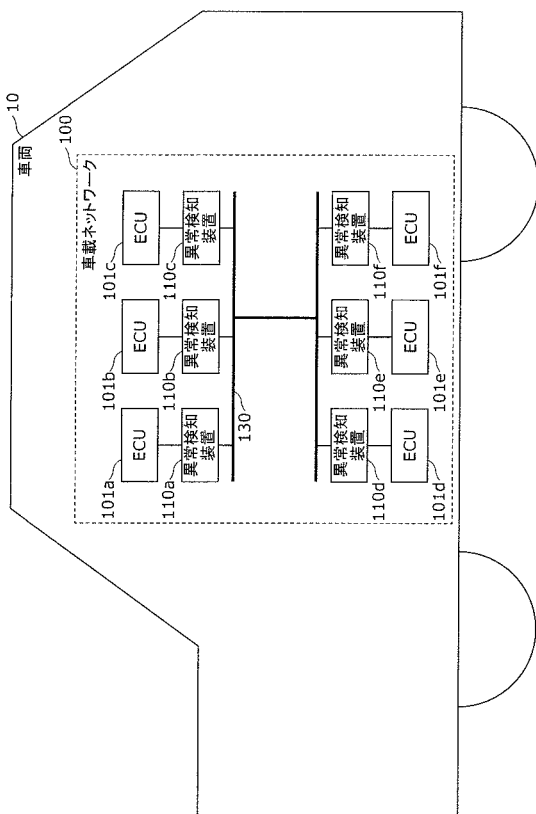
111 通信部

112 制御部

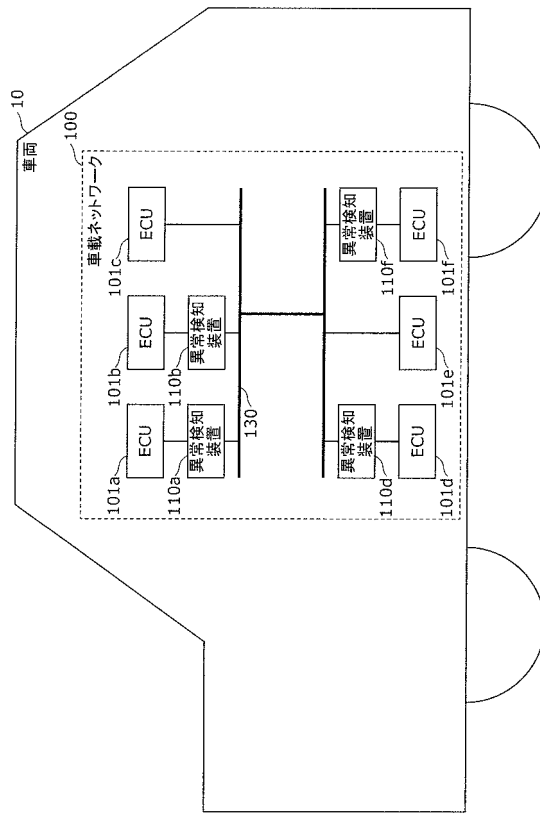
50

- 1 1 3 送信済みIDリスト保持部
- 1 1 4 受信済みIDリスト保持部
- 1 1 5 ECU処理部
- 1 2 0 IDSECU
- 1 2 1 通信部
- 1 2 2 異常検知部
- 1 3 0 バス

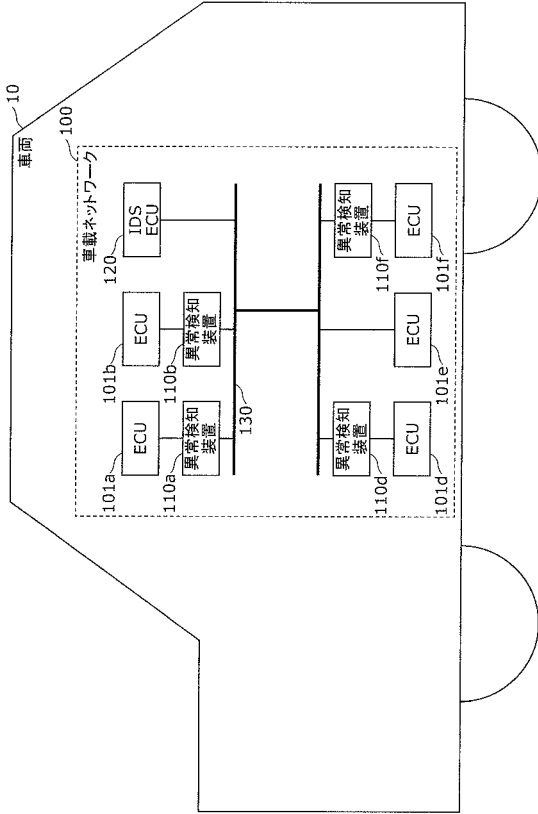
【 図 1 】



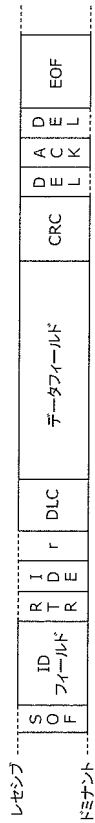
【 図 2 】



【 図 3 】



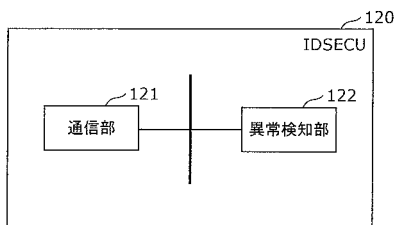
【 図 4 】



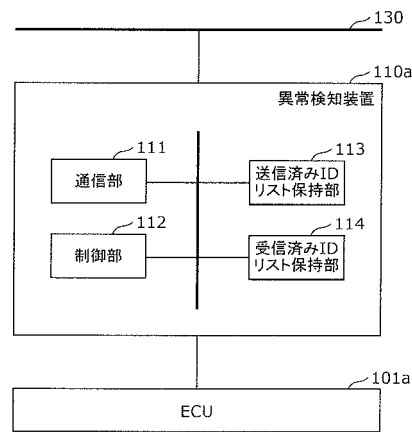
【 図 5 】

ECU 名	送信を担当するメッセージの ID
エンジン ECU	0x13, 0x15, 0x10
ブレーキ ECU	0x160, 0x330, 0x378
ドア制御 ECU	0x430
...	...

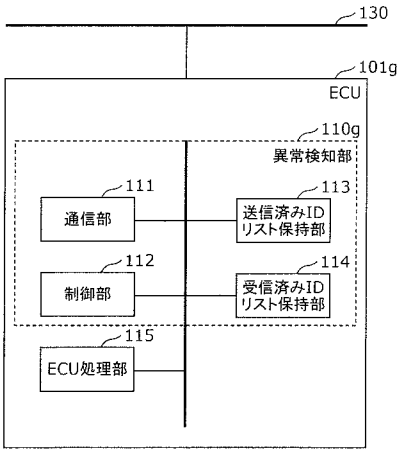
【 図 6 】



【 図 7 】



【図 8】



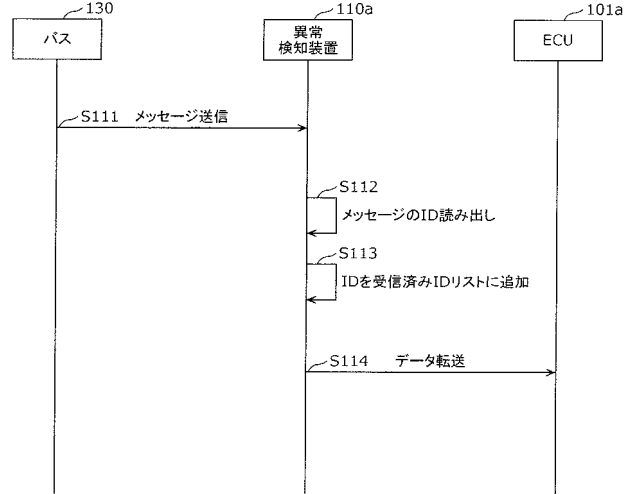
【図 9】

受信したメッセージの ID	受信回数	最近 1 分間の受信回数
0x25	56330	89
0x27	4424	16
0x89	566	2
...

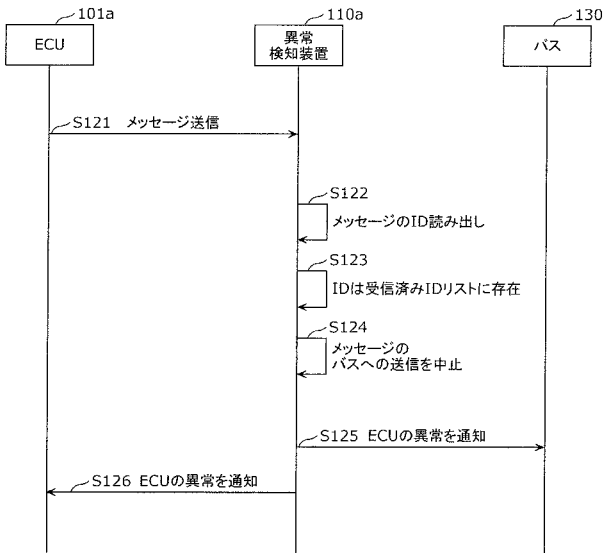
【図 10】

送信したメッセージの ID	送信回数	最近 1 分間の送信回数
0x253	6780	293
0x272	243	16
0x349	60	1
...

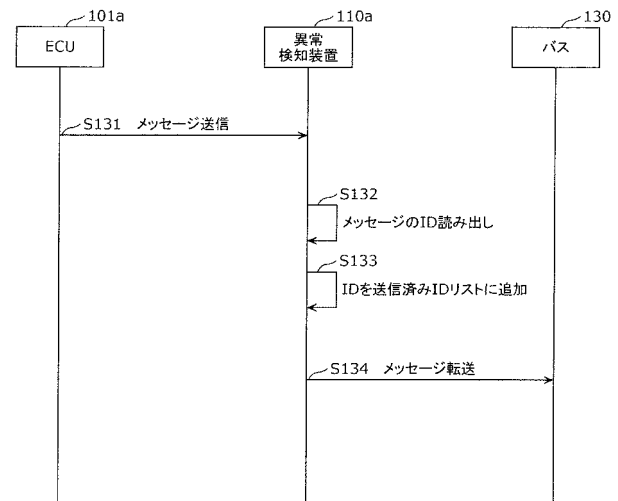
【図 11】



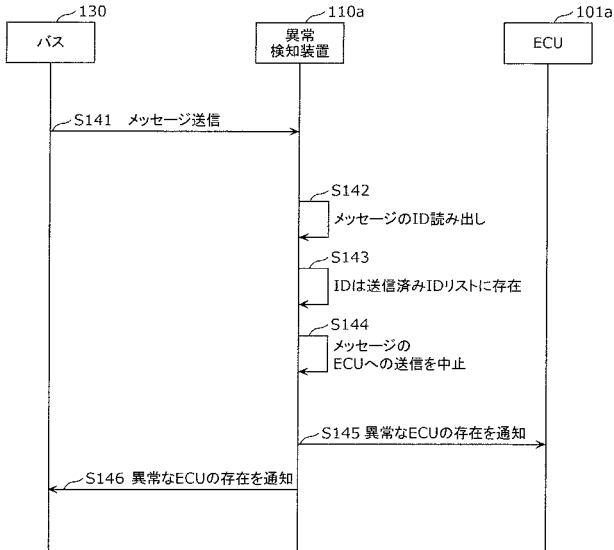
【図 12】



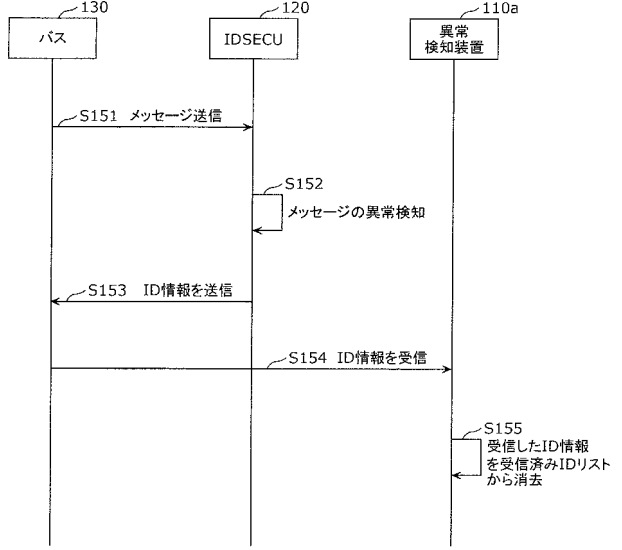
【図 13】



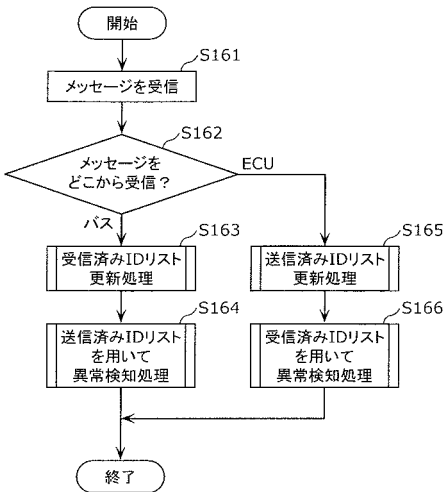
【図14】



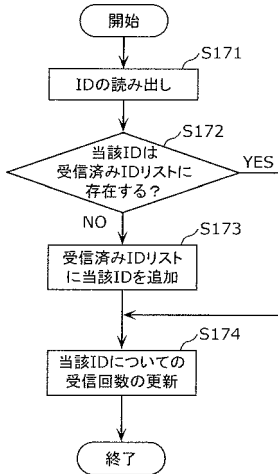
【図15】



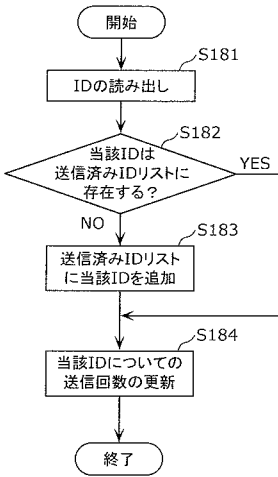
【図16】



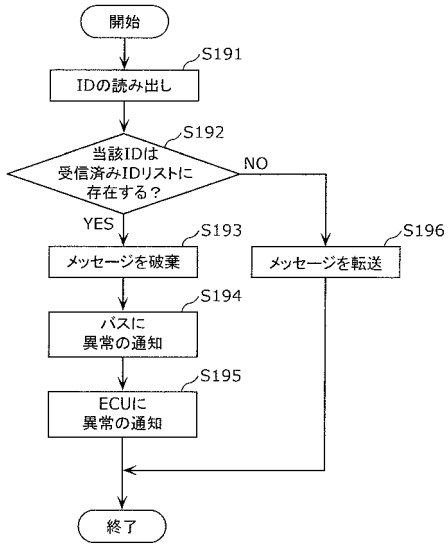
【図17】



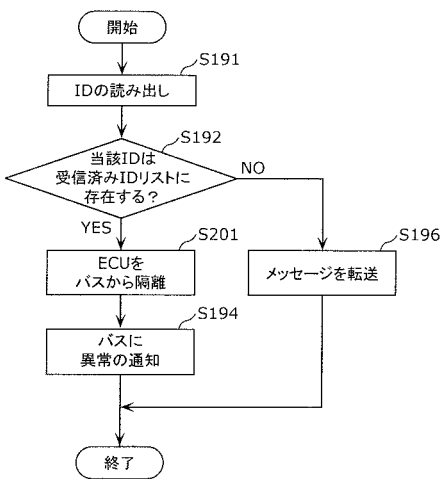
【図18】



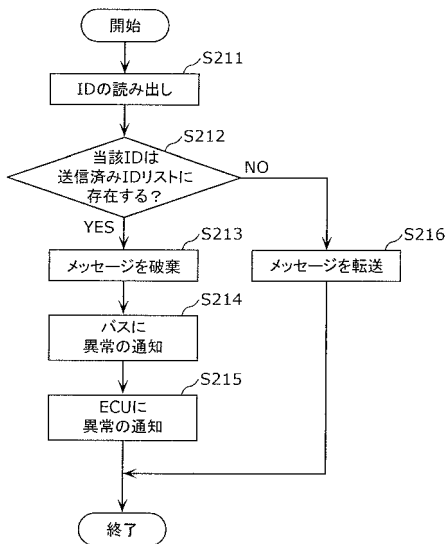
【図19】



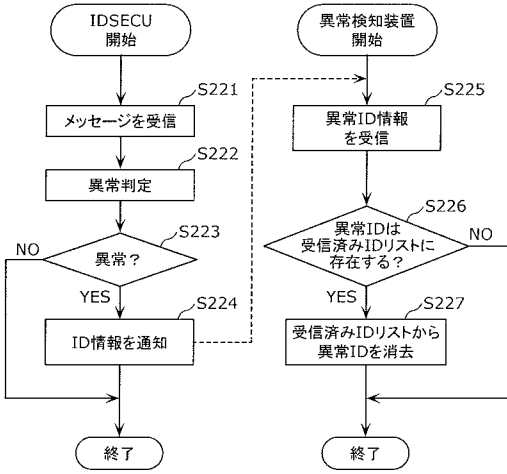
【図20】



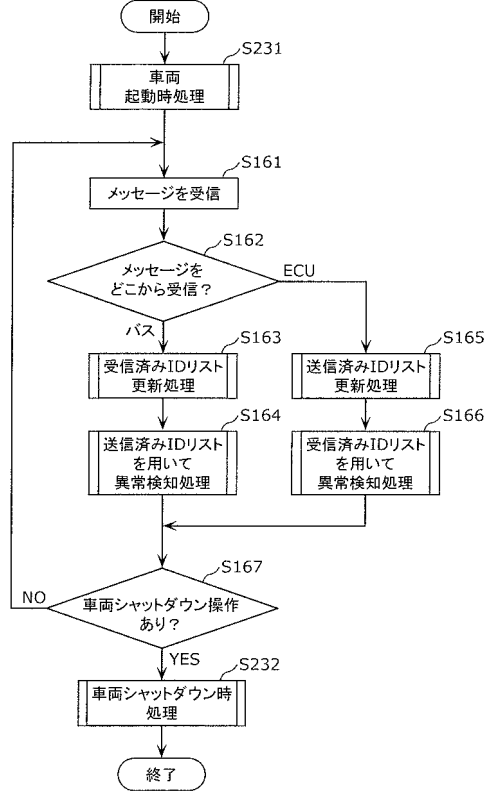
【図21】



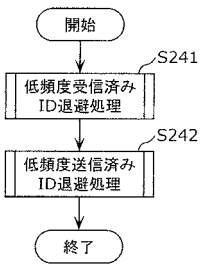
【図 2 2】



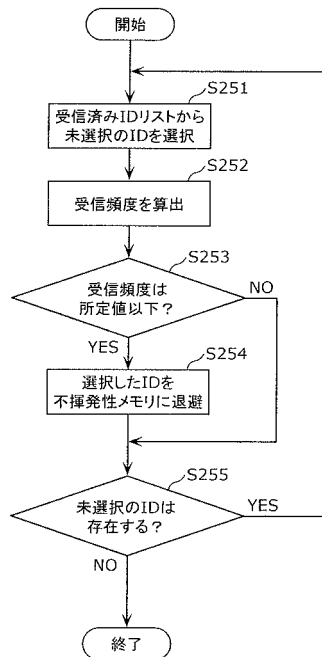
【図 2 3】



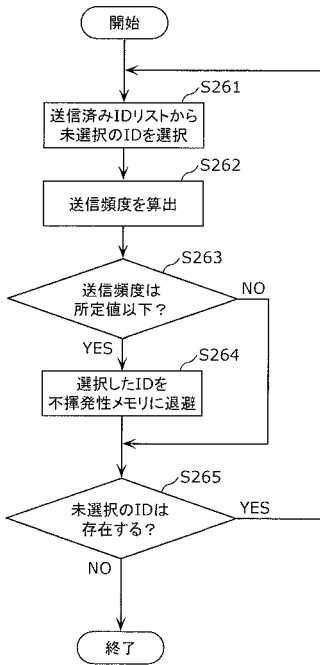
【図 2 4】



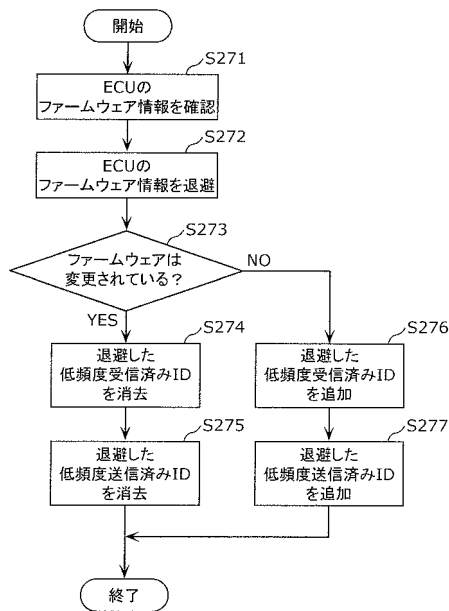
【図 2 5】



【図 26】



【図 27】



【手続補正書】

【提出日】令和1年7月10日(2019.7.10)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

複数の電子制御ユニットと、ネットワークと、異常検知装置から構成される車載ネットワークに配置される異常検知装置であって、

前記異常検知装置は、

前記ネットワークと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、

前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークへ送信し、前記ネットワークからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、

前記通信部が前記ネットワークから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、

前記通信部および前記受信済みIDリスト保持部を制御する制御部と、を備え、

前記制御部は、

前記通信部が前記ネットワークから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、

前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、当該メッセージを前記ネットワークへ送信しないことを特

徴とする、

異常検知装置。

【請求項 2】

前記制御部は、前記通信部が前記第 1 電子制御ユニットから受信したメッセージの ID が前記受信済み ID リストに存在する場合に、前記第 1 電子制御ユニットを前記ネットワークから隔離することを特徴とする、

請求項 1 記載の異常検知装置。

【請求項 3】

前記制御部は、前記通信部が前記複数の電子制御ユニットのうちの前記第 1 電子制御ユニットとは異なる第 2 電子制御ユニットから送信された異常な ID を示す異常 ID 情報を前記ネットワークから受信した場合に、前記受信済み ID リストから前記異常 ID 情報が示す ID を消去することを特徴とする、

請求項 1 または 2 に記載の異常検知装置。

【請求項 4】

前記受信済み ID リスト保持部は、前記受信済み ID リストに含まれる ID 毎のメッセージ受信回数を記録する領域を持ち、

前記制御部は、

前記通信部が前記ネットワークからメッセージを受信したとき、当該メッセージの ID について記録されるメッセージ受信回数を更新し、

前記車載ネットワークを搭載した車両のシャットダウン時に、前記受信済み ID リストに含まれる ID のうち、前記受信済み ID リスト保持部に記録されたメッセージ受信回数、または、当該メッセージ受信回数に基づくメッセージ受信頻度が所定の値以下となっている ID を不揮発性メモリに退避させ、

前記車両の起動時に、前記不揮発性メモリに退避させた前記 ID を前記受信済み ID リストに追加することを特徴とする、

請求項 1 ~ 3 のいずれか 1 項に記載の異常検知装置。

【請求項 5】

前記制御部は、前記車両の起動時に、前回の起動時から前記第 1 電子制御ユニットのファームウェア情報に変更されている場合に、前記不揮発性メモリに退避させた前記 ID を消去し、当該 ID を前記受信済み ID リストに追加しないことを特徴とする、

請求項 4 記載の異常検知装置。

【請求項 6】

前記異常検知装置は、さらに、前記通信部が前記第 1 電子制御ユニットから受信し前記ネットワークへ送信したメッセージの ID のリストである送信済み ID リストを保持する送信済み ID リスト保持部を備え、

前記制御部は、さらに、

前記送信済み ID リスト保持部を制御し、

前記通信部が前記第 1 電子制御ユニットから受信したメッセージの ID が前記送信済み ID リストに存在しない場合に、当該 ID を前記送信済み ID リストに追加し、

前記通信部が前記ネットワークから受信したメッセージの ID が前記送信済み ID リストに存在する場合、当該メッセージを前記第 1 電子制御ユニットへ送信しないことを特徴とする、

請求項 1 ~ 5 のいずれか 1 項に記載の異常検知装置。

【請求項 7】

前記送信済み ID リスト保持部は、前記送信済み ID リストに含まれる ID 毎のメッセージ送信回数を記録する領域を持ち、

前記制御部は、

前記通信部が前記第 1 電子制御ユニットからメッセージを受信したときに、当該メッセージの ID について記録されるメッセージ送信回数を更新し、

前記車載ネットワークを搭載した車両のシャットダウン時に、前記送信済み ID リスト

に含まれるIDのうち、前記送信済みIDリスト保持部に記録されたメッセージ送信回数、または、当該メッセージ送信回数に基づくメッセージ送信頻度が所定の値以下となっているIDを不揮発性メモリに退避させ、

前記車両の起動時に、前記不揮発性メモリに退避させた前記IDを前記送信済みIDリストに追加することを特徴とする、

請求項6記載の異常検知装置。

【請求項8】

前記制御部は、前記車両の起動時に、前回の起動時から前記第1電子制御ユニットのファームウェア情報に変更されている場合に、前記不揮発性メモリに退避させた前記IDを消去し、当該IDを前記送信済みIDリストに追加しないことを特徴とする、

請求項7記載の異常検知装置。

【請求項9】

複数の電子制御ユニットと、ネットワークと、異常検知装置から構成される車載ネットワークに配置される異常検知装置により実行される異常検知方法であって、

前記異常検知装置は、

前記ネットワークと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、

前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークへ送信し、前記ネットワークからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、

前記通信部が前記ネットワークから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、を備え、

前記異常検知方法では、

前記通信部が前記ネットワークから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、

前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、当該メッセージを前記ネットワークへ送信しないことを特徴とする、

異常検知方法。

【請求項10】

請求項9に記載の異常検知方法をコンピュータに実行させるプログラム。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

上記課題を解決するために、本開示の一態様に係る異常検知装置は、複数の電子制御ユニットと、ネットワークと、異常検知装置から構成される車載ネットワークに配置される異常検知装置であって、前記異常検知装置は、前記ネットワークと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークへ送信し、前記ネットワークからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、前記通信部が前記ネットワークから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、前記通信部および前記受信済みIDリスト保持部を制御する制御部と、を備え、前記制御部は、前記通信部が前記ネットワークから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリ

ストに存在する場合に、当該メッセージを前記ネットワークへ送信しないことを特徴とする。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正の内容】

【0017】

本開示の異常検知装置は、複数の電子制御ユニットと、ネットワークと、異常検知装置から構成される車載ネットワークに配置される異常検知装置であって、前記異常検知装置は、前記ネットワークと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークへ送信し、前記ネットワークからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、前記通信部が前記ネットワークから受信し前記第1電子制御ユニットへ送信したメッセージのIDのリストである受信済みIDリストを保持する受信済みIDリスト保持部と、前記通信部および前記受信済みIDリスト保持部を制御する制御部と、を備え、前記制御部は、前記通信部が前記ネットワークから受信したメッセージのIDが前記受信済みIDリストに存在しない場合に、当該IDを前記受信済みIDリストに追加し、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、当該メッセージを前記ネットワークへ送信しないことを特徴とする。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正の内容】

【0018】

異常検知装置は、ネットワークから受信したメッセージのIDを受信済みIDリストに追加していく。つまり、異常検知装置は、複数のECUのうち、自身を介してネットワークと接続された第1ECU以外のECUがネットワークへ送信したメッセージのIDを受信済みIDリストに追加していく。一般的に、車載ネットワークにおける複数のECUのそれぞれは、同じIDを含むメッセージを送信しないという仕様になっていることが多い。この仕様のもとでは、受信済みIDリストは、第1ECUが送信しないメッセージのIDのリストとなる。これに対して、異常検知装置が第1ECUから受信したメッセージ（つまり、第1ECUが送信したメッセージ）のIDを受信済みIDリストに存在する場合、本来第1ECUが送信するはずのないメッセージを第1ECUが送信していることになる。つまり、第1ECUが異常なメッセージを送信していることがわかる。したがって、このような場合に、第1ECUからのメッセージをネットワークに送信しないようにすることで、異常なメッセージがネットワークに流れることを抑制できる。このように、車載ネットワーク内にIDS ECUを追加（つまり、ネットワークトラフィックおよびコストが増大）したり、各ECUが送信するメッセージのIDを予め記憶させておいたりすることなく、車載ネットワークにおける異常を容易に検知できる。また、正規メッセージがネットワークに流れる前に、攻撃者が不正メッセージをネットワークへ送信しない限り、誤検知をすることなく異常メッセージを遮断可能である。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】変更

【補正の内容】

【0019】

また例えば、前記制御部は、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記受信済みIDリストに存在する場合に、前記第1電子制御ユニットを前記ネットワークから隔離してもよい。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】変更

【補正の内容】

【0020】

この場合、第1ECUが不正なECUであるため、不正なECUをネットワークから隔離する（例えば、第1ECUから送信される全てのメッセージを異常検知装置において遮断してネットワークへ送信しないようにする）ことが可能となり、異常メッセージのみを遮断する場合と比べて、車載ネットワークに不正なECUが与える影響をより軽減できる。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】変更

【補正の内容】

【0021】

また例えば、前記制御部は、前記通信部が前記複数の電子制御ユニットのうちの前記第1電子制御ユニットとは異なる第2電子制御ユニットから送信された異常なIDを示す異常ID情報を前記ネットワークから受信した場合に、前記受信済みIDリストから前記異常ID情報が示すIDを消去してもよい。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0022

【補正方法】変更

【補正の内容】

【0022】

正規メッセージがネットワークに流れる前に、攻撃者が不正メッセージをネットワークへ送信する場合が考えられる。この場合、受信済みIDリストに不正メッセージに含まれるIDが追加されることになる。例えば、正規な第1ECUが送信するメッセージに含まれるIDが不正メッセージに含まれる場合、正規な第1ECUから送信される正規メッセージが不正メッセージであると判定されてしまう。つまり、以降は、正規メッセージがネットワークへ送信されず、攻撃者が第1ECUになりすまして不正メッセージがネットワークへ送信されることになる。これに対して、第2ECUとして例えばIDSECU等が車載ネットワークに配置されることで、攻撃者が送信した不正メッセージを検知することが可能となる。したがって、正規メッセージがネットワークに流れる前に、攻撃者が不正メッセージをネットワークへ送信した場合（つまり、受信済みIDリストが汚染された場合）であっても、受信済みIDリストを修正して、受信済みIDリストに追加された不正メッセージに含まれるID（つまり第1ECUが送信するメッセージに含まれるID）を受信済みIDリストから消去することで、異常検知装置が正規メッセージを不正メッセージであると誤検知することを防止することが可能である。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0023

【補正方法】変更

【補正の内容】

【0023】

また例えば、前記受信済みIDリスト保持部は、前記受信済みIDリストに含まれるID毎のメッセージ受信回数を記録する領域を持ち、前記制御部は、前記通信部が前記ネットワークからメッセージを受信したとき、当該メッセージのIDについて記録されるメッセージ受信回数を更新し、前記車載ネットワークを搭載した車両のシャットダウン時に、前記受信済みIDリストに含まれるIDのうち、前記受信済みIDリスト保持部に記録されたメッセージ受信回数、または、当該メッセージ受信回数に基づくメッセージ受信頻度が所定の値以下となっているIDを不揮発性メモリに退避させ、前記車両の起動時に、前記不揮発性メモリに退避させた前記IDを前記受信済みIDリストに追加してもよい。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正の内容】

【0024】

メッセージ受信回数またはメッセージ受信頻度が所定の値以下となっているID（低頻度で受信されるメッセージに含まれるID）は、車両が起動した後、当該IDを含むメッセージがネットワークを流れるまでに時間を要する場合がある。つまり、当該IDを含む正規メッセージがネットワークを流れるまでに、攻撃者が当該IDを含む不正メッセージをネットワークへ送信して、受信済みIDリストに不正メッセージに含まれるIDが追加されてしまう（言い換えると、受信済みIDリストが不正なIDで汚染されてしまう）場合がある。これに対して、車両の起動時に、不揮発性メモリに退避させた低頻度で受信されるメッセージに含まれるIDを受信済みIDリストに追加することで、低頻度で受信されるメッセージが最初にネットワークに流れる前に攻撃者が不正メッセージを送信することによる受信済みIDリストの汚染を防ぐことが可能である。また、高頻度で受信されるメッセージの含まれるIDを不揮発性メモリに退避させないことで、その分メモリ容量を削減することが可能である。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0027

【補正方法】変更

【補正の内容】

【0027】

また例えば、前記異常検知装置は、さらに、前記通信部が前記第1電子制御ユニットから受信し前記ネットワークへ送信したメッセージのIDのリストである送信済みIDリストを保持する送信済みIDリスト保持部を備え、前記制御部は、さらに、前記送信済みIDリスト保持部を制御し、前記通信部が前記第1電子制御ユニットから受信したメッセージのIDが前記送信済みIDリストに存在しない場合に、当該IDを前記送信済みIDリストに追加し、前記通信部が前記ネットワークから受信したメッセージのIDが前記送信済みIDリストに存在する場合、当該メッセージを前記第1電子制御ユニットへ送信しなくてもよい。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0028

【補正方法】変更

【補正の内容】

【0028】

異常検知装置は、第1ECUから受信したメッセージのIDを送信済みIDリストに追加していく。車載ネットワークにおける複数のECUのそれぞれは、同じIDを含むメッセージを送信しないという仕様のもとでは、送信済みIDリストは、複数のECUのうちの第1ECU以外のECU等が送信しないメッセージのIDのリストとなる。これに対し

て、異常検知装置がネットワークから受信したメッセージ（つまり、第1 ECU以外の ECU が送信したメッセージ）の ID が送信済み ID リストに存在する場合、本来第1 ECU 以外の ECU 等が送信するはずのないメッセージを第1 ECU 以外の ECU 等が送信していることになる。つまり、第1 ECU 以外の ECU 等が異常なメッセージを送信していることがわかる。したがって、このような場合に、第1 ECU 以外の ECU 等からのメッセージを第1 ECU に送信しないようにすることで、異常なメッセージが第1 ECU に送信されることを抑制できる。このように車載ネットワーク内に ID SEC U を追加（つまり、ネットワークトラフィックおよびコストが増大）したり、各 ECU が送信するメッセージの ID を予め記憶させておいたりすることなく、車載ネットワークにおける異常を容易に検知できる。また、正規メッセージがネットワークに流れる前に、攻撃者が不正メッセージをネットワークへ送信しない限り、誤検知をすることなく異常メッセージを検知可能である。

【**手続補正 13**】

【**補正対象書類名**】明細書

【**補正対象項目名**】0033

【**補正方法**】変更

【**補正の内容**】

【**0033**】

本開示の異常検知方法は、複数の電子制御ユニットと、ネットワークと、異常検知装置から構成される車載ネットワークに配置される異常検知装置により実行される異常検知方法であって、前記異常検知装置は、前記ネットワークと前記複数の電子制御ユニットのうちのいずれかの第1電子制御ユニットの間に配置され、前記第1電子制御ユニットからメッセージを受信して当該メッセージを前記ネットワークへ送信し、前記ネットワークからメッセージを受信して当該メッセージを前記第1電子制御ユニットへ送信する通信部と、前記通信部が前記ネットワークから受信し前記第1電子制御ユニットへ送信したメッセージの ID のリストである受信済み ID リストを保持する受信済み ID リスト保持部と、を備え、前記異常検知方法では、前記通信部が前記ネットワークから受信したメッセージの ID が前記受信済み ID リストに存在しない場合に、当該 ID を前記受信済み ID リストに追加し、前記通信部が前記第1電子制御ユニットから受信したメッセージの ID が前記受信済み ID リストに存在する場合に、当該メッセージを前記ネットワークへ送信しないことを特徴とする。

【**手続補正 14**】

【**補正対象書類名**】明細書

【**補正対象項目名**】0041

【**補正方法**】変更

【**補正の内容**】

【**0041**】

車載ネットワーク100は、複数の ECU と、ネットワークと、異常検知装置から構成される。例えば、図1に示す例では、車載ネットワーク100は、複数の ECU のそれぞれに対応するように設けられた複数の異常検知装置を備える。例えば、車載ネットワーク100は、複数の ECU として、ECU 101a、101b、101c、101d、101e および 101f とバス130（ネットワーク）と異常検知装置110a、110b、110c、110d、110e および 110f とから構成される。ECU 101a とバス130は、異常検知装置110aを間に介して接続され、通信を行う。ECU 101b とバス130は、異常検知装置110bを間に介して接続され、通信を行う。ECU 101c とバス130は、異常検知装置110cを間に介して接続され、通信を行う。ECU 101d とバス130は、異常検知装置110dを間に介して接続され、通信を行う。ECU 101e とバス130は、異常検知装置110eを間に介して接続され、通信を行う。ECU 101f とバス130は、異常検知装置110fを間に介して接続され、通信を行う。例えば、異常検知装置110aに着目すると、異常検知装置110aは、バス130

と複数の ECU のうちのいずれかの第 1 ECU (ここでは ECU 101a) の間に配置される。 ECU 101a がバス 130 へ向けてメッセージを送信する際、および、 ECU 101a がバス 130 からメッセージが受信する際に、異常検知装置 110a を介してメッセージの送受信が行われる。

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2019/017014
A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. H04L12/40(2006.01) i, B60R16/02(2006.01) i, B60R16/023(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) Int. Cl. H04L12/40, B60R16/02, B60R16/023 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 1971-2019 Registered utility model specifications of Japan 1996-2019 Published registered utility model applications of Japan 1994-2019 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 2017-91280 A (FUJITSU LTD.) 25 May 2017, paragraphs [0002], [0014]-[0037], fig. 1 (Family: none)	1-10
A	JP 2017-28567 A (FUJITSU LTD.) 02 February 2017, paragraphs [0015]-[0076], fig. 1-5 & US 2017/0026373 A1, paragraphs [0028]-[0089], fig. 1-5 & DE 102016212752 A1	1-10
A	JP 2017-195524 A (MITSUBISHI ELECTRIC CORP.) 26 October 2017, paragraphs [0017]-[0063], fig. 1-7 (Family: none)	1-10
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> 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 17.05.2019		Date of mailing of the international search report 28.05.2019
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/JP2019/017014

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 2018-26791 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 15 February 2018, paragraphs [0037]-[0044], [0104]-[0113], fig. 1, 5, 14 & WO 2018/20833 A1 & CN 109076001 A	1-10
A	矢嶋純他, 非周期送信メッセージによる攻撃を検知可能にするセキュリティ CAN アダプタ, 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 19 January 2016, pp. 1-6, non-official translation (YAJIMA, Jun, HASEBE, Takayuki. Security CAN Adapter Enabling Attack Detection Using Non-Periodically Transmitted Messages. 2016 Symposium on Cryptography and Information Security (SCIS2016).)	1-10
A	関口大樹他, 不正 CAN データ送信を抑制するホワイトリスト・ハブ, 2014 年暗号と情報セキュリティシンポジウム (SCIS2014), 21 January 2014, pp. 1-8, non-official translation (SEKIGUCHI, Daiki et al. Whitelist/Hub for Controlling Unauthorized CAN Data Transmission. 2014 Symposium on Cryptography and Information Security (SCIS2014).)	1-10

国際調査報告		国際出願番号 PCT/J P 2 0 1 9 / 0 1 7 0 1 4									
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. H04L12/40(2006.01)i, B60R16/02(2006.01)i, B60R16/023(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. H04L12/40, B60R16/02, B60R16/023											
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>1971-2019年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2019年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2019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	1971-2019年	日本国実用新案登録公報	1996-2019年	日本国登録実用新案公報	1994-2019年
日本国実用新案公報	1922-1996年										
日本国公開実用新案公報	1971-2019年										
日本国実用新案登録公報	1996-2019年										
日本国登録実用新案公報	1994-2019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 2017-91280 A (富士通株式会社) 2017.05.25, [0002], [0014]-[0037], Fig.1 (ファミリーなし)	1-10									
A	JP 2017-28567 A (富士通株式会社) 2017.02.02, [0015]-[0076], Fig.1-5 &US 2017/0026373 A1 [0028]-[0089], Fig.1-5 &DE 102016212752 A1	1-10									
A	JP 2017-195524 A (三菱電機株式会社) 2017.10.26, [0017]-[0063], Fig.1-7 (ファミリーなし)	1-10									
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> 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		の日の後に公表された文献									
「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		「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									
「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		「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									
「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)		「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									
「O」口頭による開示、使用、展示等に言及する文献		「&」同一パテントファミリー文献									
「P」国際出願日前で、かつ優先権の主張の基礎となる出願											
国際調査を完了した日 17.05.2019		国際調査報告の発送日 28.05.2019									
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) 玉木 宏治	5X 3047								
		電話番号 03-3581-1101 内線 3596									

国際調査報告		国際出願番号 PCT/J P 2 0 1 9 / 0 1 7 0 1 4
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 2018-26791 A (パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ) 2018.02.15, [0037]-[0044], [0104]-[0113], Fig. 1, 5, 14 & WO 2018/20833 A1 & CN 109076001 A	1-10
A	矢嶋 純 他, 非周期送信メッセージによる攻撃を検知可能にする セキュリティ CAN アダプタ, 2016年 暗号と情報セキュリティシンポ ジウム (SCIS2016), 2016.01.19, pp. 1-6	1-10
A	関口 大樹 他, 不正 CAN データ送信を抑制するホワイトリスト・ ハブ, 2014年 暗号と情報セキュリティシンポジウム (SCIS2014), 2014.01.21, pp. 1-8	1-10

フロントページの続き

(81)指定国・地域 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(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), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), 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, 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

(74)代理人 100131417

弁理士 道坂 伸一

(72)発明者 高橋 良太

日本国大阪府門真市大字門真1006番地 パナソニック株式会社内

(72)発明者 佐々木 崇光

日本国大阪府門真市大字門真1006番地 パナソニック株式会社内

Fターム(参考) 5K032 AA05 BA06 CC05 DA01 DB28 EA02 EA06

5K033 AA05 BA06 CB06 DA01 DB20 EA02 EA06

(注)この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。