

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号  
特許第7121737号  
(P7121737)

(45)発行日 令和4年8月18日(2022.8.18)

(24)登録日 令和4年8月9日(2022.8.9)

(51)国際特許分類 F I  
 H 0 4 L 12/66 (2006.01) H 0 4 L 12/66  
 H 0 4 L 12/22 (2006.01) H 0 4 L 12/22  
 H 0 4 L 12/28 (2006.01) H 0 4 L 12/28 1 0 0 A

請求項の数 10 (全37頁)

(21)出願番号	特願2019-537416(P2019-537416)	(73)特許権者	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 9 0 5 0 4 カリフォルニア州, トーランス, スイート 4 5 0 , ウェスト 1 9 0 ストリート 2 0 5 0
(86)(22)出願日	平成31年4月22日(2019.4.22)	(74)代理人	100109210 弁理士 新居 広守
(86)国際出願番号	PCT/JP2019/017014	(74)代理人	100137235 弁理士 寺谷 英作
(87)国際公開番号	WO2019/225257	(74)代理人	100131417 弁理士 道坂 伸一
(87)国際公開日	令和1年11月28日(2019.11.28)		
審査請求日	令和3年11月9日(2021.11.9)		
(31)優先権主張番号	特願2018-98855(P2018-98855)		
(32)優先日	平成30年5月23日(2018.5.23)		
(33)優先権主張国・地域又は機関	日本国(JP)		

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)【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、

10

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、

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。

**【請求項 6】**

30

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、

40

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

50

いる I D 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 I D を前記送信済み I D 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 I D を消去し、当該 I D を前記送信済み I D 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 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 I D が前記受信済み I D リストに存在しない場合に、当該 I D を前記受信済み I D 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 I D が前記受信済み 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。

【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。

【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

10

20

30

40

50

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。

【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。

10

【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、IDSECU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。

20

【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】

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

30

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】

40

【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コントローラーを改造する（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

50

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。

10

【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。

20

【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。

30

【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、IDSECUの構成図である。

【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。

40

【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。

【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

50

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、I D S E C U 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 I D 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 I D リスト更新処理のフローチャートである。

【図 19】図 19 は、実施の形態 1 における、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。

10

【図 20】図 20 は、実施の形態 1 における、受信済み I D 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 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 22】図 22 は、実施の形態 1 における、異常検知装置が I D S E C U 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。

【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。

20

【図 25】図 25 は、実施の形態 1 における、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 26】図 26 は、実施の形態 1 における、低頻度送信済み I D 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】

【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 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 リスト保持部と、前記通信部および前記受信済み I D 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 I D が前記受信済み I D リストに存在しない場合に、当該 I D を前記受信済み I D 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 I D が前記受信済み I D リストに存在する場合に、当該メッセージを前記ネットワークへ送信しないことを特徴とする。

30

40

【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 I D を受信済み I D リストに追加していく。つまり、異常検知装置は、複数の E C U のうち、自身を介してネットワークと接続された第 1 E C U 以外の E C U がネットワーク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。一般的に、車載ネットワークにおける複数の 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になっていることが多い。この仕様のもとでは、受信済み I D リストは、第 1 E C U が送信しないメッセージの I D のリストとなる。これに対して、異常検知装置が第 1 E C U から受信したメッセージ(

50

つまり、第1 ECUが送信したメッセージ)のIDが受信済みIDリストに存在する場合、本来第1 ECUが送信するはずのないメッセージを第1 ECUが送信していることになる。つまり、第1 ECU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IDSEC 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遮断可能である。

10

【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。

【0020】

この場合、第1 ECU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1 ECU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。

【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。

20

【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は考えられる。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1 ECU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1 ECU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1 ECU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2 ECUとして例えばIDSEC U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1 ECU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。

30

【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。

40

【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

50

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。

10

## 【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。

20

## 【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。

30

## 【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1ECU以外のECUが送信したメッセージ)のIDを送信済み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検知可能である。

40

## 【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

50

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。

#### 【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。

#### 【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。

#### 【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。

#### 【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。

10

20

30

40

50

## 【 0 0 3 6 】

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。

## 【 0 0 3 7 】

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。

## 【 0 0 3 8 】

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。

10

## 【 0 0 3 9 】

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。

## 【 0 0 4 0 】

（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。

20

## 【 0 0 4 1 】

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、ECU101a、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。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。

30

40

## 【 0 0 4 2 】

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。

## 【 0 0 4 3 】

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。

## 【 0 0 4 4 】

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

50

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。

【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。

10

【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

20

【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。

30

【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。

40

【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

50

る。

#### 【 0 0 5 2 】

本実施の形態の車載ネットワーク 1 0 0 では、図 5 に示すように、同じ I D のメッセージを複数の E C U が送信しないものとする。例えば、エンジン E C U が送信する「 0 x 1 3 」という I D を含むメッセージを、ブレーキ E C U またはドア制御 E C U は送信しない。同じ I D のメッセージを複数の E C U が送信しない、という仕様は C A N 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 1 0 0 における異常を容易に検知することを可能としている。

#### 【 0 0 5 3 】

##### [ 1 - 6 . I D S E C U の構成 ]

図 6 は、I D S E C U 1 2 0 の構成図である。I D S E C U 1 2 0 は、C A N メッセージの送受信を行う通信部 1 2 1 と、受信したメッセージの異常検知を行う異常検知部 1 2 2 を持つ E C U であって、複数の E C U のうちの第 1 E C U (例えば、E C U 1 0 1 a、E C U 1 0 1 b、E C U 1 0 1 d および E C U 1 0 1 f ) とは異なる第 2 E C U である。

#### 【 0 0 5 4 】

通信部 1 2 1 は、バス 1 3 0 に流れるメッセージを受信し、また、バス 1 3 0 に流れるメッセージに含まれる異常な I D を示す異常 I D 情報をバス 1 3 0 へ送信する。

#### 【 0 0 5 5 】

異常検知部 1 2 2 は、通信部 1 2 1 が受信したバス 1 3 0 に流れるメッセージの異常検知を行う。例えば、I D S E C U 1 2 0 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 1 2 2 は、バス 1 3 0 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 1 2 2 は、判定ルールに基づいて、バス 1 3 0 を流れるメッセージの送信周期に異常があったり、バス 1 3 0 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。

#### 【 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。

#### 【 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。

#### 【 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

10

20

30

40

50

0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ECU101aへ送信する通信回路である。通信部111は、バス130からECU101aへ送信されるメッセージおよび、ECU101aからバス130へ送信されるメッセージを中継する機能を持つ。

【0061】

送信済みIDリスト保持部113は、通信部111がECU101aから受信しバス130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リストについては後述する。

【0062】

受信済みIDリスト保持部114は、通信部111がバス130から受信しECU101a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リストについては後述する。

10

【0063】

制御部112は、通信部111、送信済みIDリスト保持部113および受信済みIDリスト保持部114を制御する。制御部112は、以下の処理を行う（それぞれ詳細は後述する）。

【0064】

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リストに追加する。また、制御部112は、通信部111がECU101a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。例えば、制御部112は、通信部111がECU101a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、ECU101aをバス130から隔離する。

20

【0065】

また、制御部112は、通信部111が複数のECUのうち他のECU（具体的には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。

【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ECU101a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。

30

【0067】

また、制御部112は、ECU101a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ECU101aへ送信しない。

40

【0068】

また、制御部112は、通信部111がECU101a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

50

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ECU101a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。

#### 【0069】

なお、異常検知装置110b、110c、110d、110eおよび110fは、異常検知装置110aと同様の構成であり、異常検知装置110a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110b、110c、110d、110eおよび110fに接続されるECUはそれぞれECU101b、101c、101d、101eおよび101fである点異なる。

10

#### 【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ECU101gの構成図である。図8において、ECU101gは、図7に示した異常検知装置110a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110aが有する機能を異常検知部110gとして示し、ECU101a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110g(異常検知装置110aに対応)は、バス130とECU処理部115(ECU101a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。

#### 【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110aに接続されたECU101a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。

20

30

#### 【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。

40

#### 【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

50

装置 110 a に接続された ECU 101 a 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 110 a に接続された ECU 101 a 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、ECU 101 a が送信したメッセージとは、異常検知装置 110 a が ECU 101 a から受信して、異常検知装置 110 a 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 ECU 101 a 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 ECU 101 a 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。

10

**【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。

20

**【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 11 は、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 11 では異常検知装置 110 a が、受信済み ID リストに存在しない ID のメッセージをバス 130 から受信した場合の受信済み 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。

**【0078】**

ステップ S 111 では、バス 130 から異常検知装置 110 a にメッセージが送信される。

30

**【0079】**

ステップ S 112 では、異常検知装置 110 a がバス 130 から受信したメッセージの ID を読み出す。

**【0080】**

ステップ S 113 では、異常検知装置 110 a は、ステップ S 112 で読み出した ID が受信済み ID リストに存在するか否かを確認し、読み出した ID が受信済み ID リストに存在していないと判断する場合、受信済み ID リストに、読み出した ID を追加する。

**【0081】**

ステップ S 114 では、異常検知装置 110 a がバス 130 から受信したメッセージを ECU 101 a に転送する。

40

**【0082】**

このようにして、異常検知装置 110 a は、バス 130 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 110 a は、複数の ECU のうち、自身を介してバス 130 と接続された ECU 101 a 以外の ECU がバス 130 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。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、受信済み ID リストは、ECU 101 a が送信しないメッセージの ID のリストとなる。

50

## 【 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バス 1 3 0 に送信し、バス 1 3 0 に接続された E C U 1 0 1 a 以外の各ノードに E C U 1 0 1 a が異常であることを通知する。例えば、E C U 1 0 1 a に異常があることを E C U 1 0 1 a 以外の各ノードが認識することで、各ノードは、E C U 1 0 1 a の機能に応じて適切な処理ができる。例えば、E C U 1 0 1 a が車両 1 0 の走行に関する E C U である場合、各ノードは、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 0 8 9 】

ステップ S 1 2 6 では、異常検知装置 1 1 0 a は、E C U 1 0 1 a が異常であるという通知を E C U 1 0 1 a 自身に送信する。E C U 1 0 1 a が自身に異常があることを認識することで、E C U 1 0 1 a は、E C U 1 0 1 a 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。

## 【 0 0 9 0 】

## [ 1 - 1 3 . 送信済み I D リストのアップデート処理シーケンス ]

図 1 3 は、送信済み 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 3 では、送信済み I D リストに存在しない I D を異常検知装置 1 1 0 a が自身に接続された E C U 1 0 1 a から受信した場合の送信済み 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 9 1 】

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

## 【 0 0 9 2 】

ステップ S 1 3 2 では、E C U 1 0 1 a が送信したメッセージを異常検知装置 1 1 0 a が受信し、I D を読み出す。

## 【 0 0 9 3 】

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

10

20

30

40

50

## 【 0 0 9 4 】

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

## 【 0 0 9 5 】

このようにして、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 を送信済み 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 がバス 1 3 0 へ送信したメッセージの I D を送信済み 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、送信済み I D リストは、E C U 1 0 1 a 以外の E C U 等が送信しないメッセージの I D のリストとなる。

10

## 【 0 0 9 6 】

[ 1 - 1 4 . 送信済み I D リストによる異常検知処理シーケンス ]

図 1 4 は、送信済み 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 4 では、送信済み I D リストに存在する I D のメッセージ（つまり、E C U 1 0 1 a 以外の E C U 等が送信しないメッセージ）がバス 1 3 0 に送信された場合のシーケンスである。

## 【 0 0 9 7 】

ステップ S 1 4 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。これにより、異常検知装置 1 1 0 a は、バス 1 3 0 からのメッセージを受信する。

20

## 【 0 0 9 8 】

ステップ S 1 4 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 9 9 】

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 I D が送信済み I D リストに存在するか否かを確認し、読み出した I D が送信済み 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 以外の E C U 等が送信するはずのないメッセージを E C U 1 0 1 a 以外の E C U 等が送信していることになる。つまり、E C U 1 0 1 a 以外の E C U 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 E C U 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、E C U 1 0 1 a 以外の E C U 等からのメッセージを E C U 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 E C U 1 0 1 a に送信されることを抑制できる。

30

## 【 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 E C U 等が存在することを E C U 1 0 1 a に通知している。例えば、異常な E C U 等は、E C U 1 0 1 a が送信するメッセージに含まれる I D を使って不正メッセージを送信しているため、E C U 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、E C U 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、E C U 1 0 1 a が車両 1 0 の走行に関する E C U である場合、E C U 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。

40

## 【 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 E C U 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 E C U 1 0 1 a 以外の E C U 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 E C U は、E C U 1 0 1 a が有する機能に応じて適切な処理ができる。

## 【 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 I D リストに含まれる I D および受信済み I D リスト

50

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10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。

【0104】

しかし、車両10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。

【0105】

以下では、正規のIDが追加される前に、異常なID（例えばECU101a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110a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。

10

【0106】

図15は、IDSECU120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15では、図3に示すように、車載ネットワーク100にIDSECU120が存在する場合に、IDSECU120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。IDSECU120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110aが保持する受信済みIDリストから消去する。

【0107】

ステップS151では、バス130からIDSECU120へメッセージが送信される。

【0108】

ステップS152では、IDSECU120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。

20

【0109】

ステップS153では、IDSECU120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、IDSECU120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、IDSECU120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。

30

【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、IDSECU120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。

40

【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

50

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。

10

【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。

20

【0118】

ステップS163は、図17を用いて後述し、ステップS164は、図21を用いて後述し、ステップS165は、図18を用いて後述し、ステップS166は、図19および図20を用いて後述する。

【0119】

[1-17. 受信済みIDリスト更新処理フロー]

図17は、受信済みIDリスト更新処理のフローチャートである。図17は、図16のステップS163の受信済みID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110aは、バス130からメッセージが送信された際に、受信済みIDリスト保持部114に保持している受信済みIDリストを更新する。

30

【0120】

ステップS171では、異常検知装置110aは、バス130から受信したメッセージのIDを読み出す。

【0121】

ステップS172では、異常検知装置110aは、受信済みIDリストにステップS171で読み出したIDが存在するか否かを判断する。

【0122】

異常検知装置110aは、受信済みIDリストに読み出したIDが存在しない場合(ステップS172でNOの場合)は、ステップS173で、受信済みIDリストに読み出したIDを追加する。異常検知装置110aは、受信済みIDリストに読み出したIDが存在する場合(ステップS172でYESの場合)は、ステップS174の処理を行う。

40

【0123】

ステップS174では、異常検知装置110aは、読み出したIDについて、受信済みIDリスト保持部114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。

【0124】

[1-18. 送信済みIDリスト更新処理フロー]

図18は、送信済みIDリスト更新処理のフローチャートである。図18は、図16のステップS165の送信済みID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110aは、ECU101aからメッセージが送信された際に、送信済みIDリスト保持部113に保持している送信済みIDリストを更新する。

50

## 【 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。

## 【 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。

10

## 【 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 】

ステップ S 1 9 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。

20

## 【 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 I D が受信済み I D 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 I D が受信済み I D リストに存在する場合（ステップ S 1 9 2 で Y E S の場合）、E C U 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 I D が受信済み I D リストに存在しない場合（ステップ S 1 9 2 で N O の場合）、E C U 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。

30

## 【 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、E C U 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。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 1 3 4 】

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

40

## 【 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、E C U 1 0 1 a に E C U 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、E C U 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 I D リストによる異常検知処理フロー（変形例） ]

図 2 0 は、受信済み I D 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 2 0 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処理の変形例

50

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 110a は、ステップ S193 にて受信したメッセージを破棄しバス 130 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 S193 の処理を実施せず、代わりにステップ S201 の処理を実施する。具体的には、異常検知装置 110a は、ECU101a をバス 130 から隔離する。より具体的には、異常検知装置 110a は、ECU101a から受信するメッセージをすべて遮断する。これにより、ECU101a をバス 130 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 100 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 110a と ECU101a との間に異常検知装置 110a と ECU101a 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 110a と ECU101a と接続されないようにすることで、ECU101a をバス 130 から隔離してもよい。

10

#### 【0138】

[ 1 - 21 . 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 S164 の送信済み ID リストによる、バス 130 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。

#### 【0139】

ステップ S211 では、異常検知装置 110a は、バス 130 から受信したメッセージの ID を読み出す。

20

#### 【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。

30

#### 【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。

#### 【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。

40

#### 【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。

50

## 【 0 1 4 7 】

[ 1 - 2 2 . 異常検知装置が I D S E C U から異常通知を受信した場合の処理フロー ]

図 2 2 は、異常検知装置が I D S E C U 1 2 0 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 2 2 には、異常検知装置が I D S E C U 1 2 0 から異常通知を受信する前の I D S E C U 1 2 0 での処理 ( ステップ S 2 2 1 からステップ S 2 2 4 ) についても示している。

## 【 0 1 4 8 】

ステップ S 2 2 1 では、 I D S E C U 1 2 0 がバス 1 3 0 からメッセージを受信する。

## 【 0 1 4 9 】

ステップ S 2 2 2 では、 I D S E C U 1 2 0 は受信したメッセージの異常判定を行う。

10

## 【 0 1 5 0 】

ステップ S 2 2 3 では、ステップ S 2 2 2 の異常判定の結果が異常か否かを判断する。 I D S E C U 1 2 0 は、異常判定の結果が異常である場合 ( ステップ S 2 2 3 で Y E S の場合 ) 、ステップ S 2 2 4 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 S 2 2 3 で N O の場合 ) 、処理を終了する。

## 【 0 1 5 1 】

ステップ S 2 2 4 では、 I D S E C U 1 2 0 は、異常と判定したメッセージに含まれる異常な I D を示す異常 I D 情報をバス 1 3 0 に接続されている異常検知装置 1 1 0 a 、 1 1 0 b 、 1 1 0 d および 1 1 0 f に通知する。ここでは、異常検知装置 1 1 0 a に着目して説明する。

20

## 【 0 1 5 2 】

ステップ S 2 2 5 では、異常検知装置 1 1 0 a が、 I D S E C U 1 2 0 から送信された異常な I D を示す異常 I D 情報をバス 1 3 0 から受信する。異常検知装置 1 1 0 a は、 I D S E C U 1 2 0 から送信された異常な I D を示す異常 I D 情報をバス 1 3 0 から受信した場合に、受信済み I D リストから異常 I D 情報が示す I D を消去する。具体的には以下の処理が行われる。

## 【 0 1 5 3 】

ステップ S 2 2 6 では、異常検知装置 1 1 0 a は、受信した異常 I D 情報が示す異常な I D が受信済み I D リストに存在するか否かを判断する。異常な I D が受信済み I D リストに存在する場合 ( ステップ S 2 2 6 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 2 7 の処理を行い、異常な I D が受信済み I D リストに存在しない場合 ( ステップ S 2 2 6 で N O の場合 ) は、異常検知装置 1 1 0 a は、処理を終了する。

30

## 【 0 1 5 4 】

ステップ S 2 2 7 では、異常検知装置 1 1 0 a は、受信済み I D リストから異常な I D を消去する。

## 【 0 1 5 5 】

正規メッセージがバス 1 3 0 に流れる前に、攻撃者が不正メッセージをバス 1 3 0 へ送信する場合が考えられる。この場合、受信済み I D リストに不正メッセージに含まれる I D が追加されることになる。例えば、正規な E C U 1 0 1 a が送信するメッセージに含まれる I D が不正メッセージに含まれる場合、正規な E C U 1 0 1 a 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 1 3 0 へ送信されず、攻撃者が E C U 1 0 1 a になりすまして不正メッセージがバス 1 3 0 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 I D S E C U 1 2 0 が車載ネットワーク 1 0 0 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 1 3 0 に流れる前に、攻撃者が不正メッセージをバス 1 3 0 へ送信した場合 ( つまり、受信済み I D リストが汚染された場合 ) であっても、受信済み I D リストを修正して、受信済み I D リストに追加された不正メッセージに含まれる I D ( 例えば E C U 1 0 1 a が送信するメッセージに含まれる I D ) を受信済み I D 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 1 1 0 a が誤検知することを防止することが可能である。

40

50

## 【 0 1 5 6 】

[ 1 - 2 3 . 異常検知装置の全体処理フロー（変形例） ]

図 2 3 は、異常検知装置 1 1 0 a 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 2 3 は、図 1 6 の異常検知装置 1 1 0 a 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 2 3 では、図 1 6 の全体処理に加えて、ステップ S 1 6 7 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 S 2 3 1 の車両 1 0 の起動時の処理、および、ステップ S 2 3 2 の車両 1 0 のシャットダウン時の処理が追加されている。

## 【 0 1 5 7 】

ステップ S 2 3 1 は、後ほど図 2 7 にて詳細に説明する。

## 【 0 1 5 8 】

ステップ S 1 6 7 では、異常検知装置 1 1 0 a は、車両シャットダウン操作があれば（ステップ S 1 6 7 で Y E S の場合）、ステップ S 2 3 2 を行い、車両シャットダウン操作がなければ（ステップ S 1 6 7 で N O の場合）、ステップ S 1 6 1 に戻る。ステップ S 2 3 2 については、図 2 4 から図 2 6 にて詳細に説明する。

## 【 0 1 5 9 】

[ 1 - 2 4 . 車両シャットダウン時の処理フロー ]

図 2 4 は、異常検知装置 1 1 0 a 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 2 4 は、図 2 3 のステップ S 2 3 2 の異常検知装置 1 1 0 a 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。

## 【 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。

## 【 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引してもよい。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。

## 【 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

10

20

30

40

50

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S252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110a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IDを低頻度受信済みIDと判断し、ステップS254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S255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S252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。

【0166】

ステップS254では、異常検知装置110aは、選択したIDを不揮発性メモリに退避させる。

10

【0167】

そして、ステップS255では、異常検知装置110aは、受信済みIDリストに未選択のIDが存在するか否かを判定し、存在する場合(ステップS255でYESの場合)は、ステップS251に戻り、存在しない場合(ステップS255でNO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IDを不揮発性メモリに退避することができる。

【0168】

[1-26. 低頻度送信済みIDの退避処理フロー]

図26は、低頻度送信済みIDの退避の処理フローチャートである。図26は、図24のステップS242の低頻度送信済みID退避処理の詳細な処理のフローチャートである。

20

【0169】

ステップS261では、異常検知装置110aは、送信済みIDリストから、低頻度送信済みIDの退避の処理においてまだ選択していないIDを選択する。

【0170】

ステップS262では、異常検知装置110aは、選択したIDについて、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110aは、メッセージ送信回数を車両10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110aは、選択したIDについて、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を取ってもよい。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ECU101aがバス130へメッセージを送信した回数であってもよい。

30

【0171】

ステップS263では、異常検知装置110aは、ステップS262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110aは、メッセージ送信頻度が所定の値以下ならば(ステップS263でYES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IDを低頻度送信済みIDと判断し、ステップS264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S263でNOの場合)、ステップS265の処理を行う。なお、異常検知装置110aは、ステップS262で、選択したIDについて、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を取ってもよい。そして、異常検知装置110a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IDを低頻度送信済みIDと判断し、ステップS264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S265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110aは、ステップS262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ってもよい。

40

【0172】

50

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。

【 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を次の車両 1 0 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 1 0 の起動時から E C U 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 1 0 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 1 0 の前回の起動時の E C U 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 1 0 が起動するごとに、図 2 7 に示す処理が行われる。

【 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 】

E C U のファームウェアアップデートに伴い E C U のファームウェア情報が変更された場合、E C U から送信されるメッセージに含まれる I D 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 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、仕様が変更された 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。

【 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 1 0 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

10

20

30

40

50

む正規メッセージがバス130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バス130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。

【0183】

さらに、ステップS277では、異常検知装置110aは、図26のステップS264にて不揮発性メモリに退避していた低頻度送信済みIDを異常検知装置110aの送信済みIDリストに読み込む。

【0184】

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ECU101aから送信されるメッセージに含まれるID）は、車両10が起動した後、当該IDを含むメッセージを異常検知装置110aがECU101a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110aが受信するまでに、攻撃者がECU101aを攻撃して不正なECU101aから不正メッセージを異常検知装置110a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110a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110a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S271からステップS275の処理が行われず、ステップS276およびステップS277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、持っていないてもよい。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

10

20

30

40

50

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、持っていないてもよい。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。

10

【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。

20

【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。

【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。

30

【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。

【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良い。

40

【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。

【0198】

50

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。

【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。

10

【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。

20

【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。

【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。

30

【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。

【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。

40

【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

50

内に含まれてもよい。

【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。

【符号の説明】

【0209】

10 車両

100 車載ネットワーク

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

110 a、110 b、110 c、110 d、110 e、110 f 異常検知装置

110 g 異常検知部

111 通信部

112 制御部

113 送信済みIDリスト保持部

114 受信済みIDリスト保持部

115 ECU処理部

120 IDSECU

121 通信部

122 異常検知部

130 バス

10

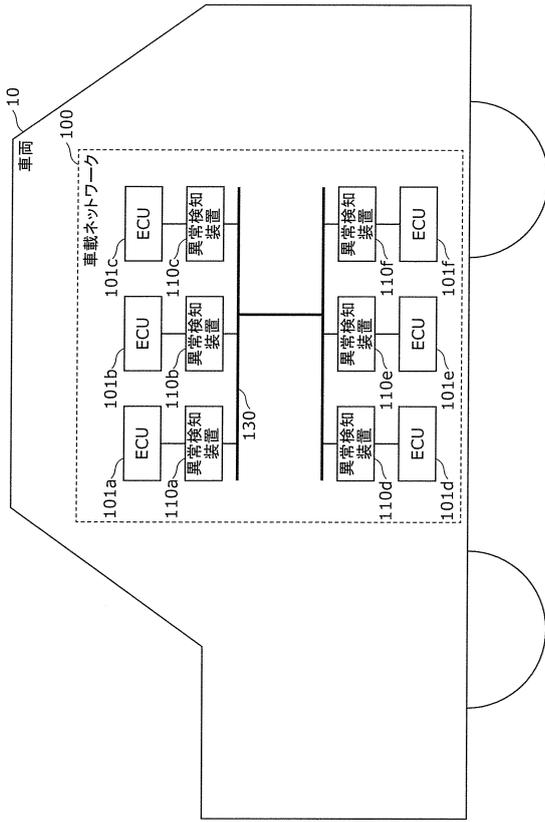
20

30

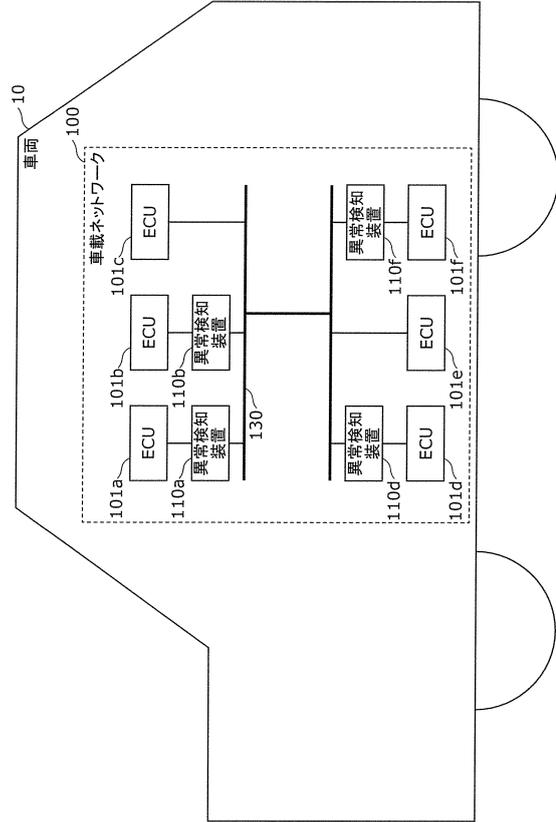
40

50

【図面】  
【図 1】



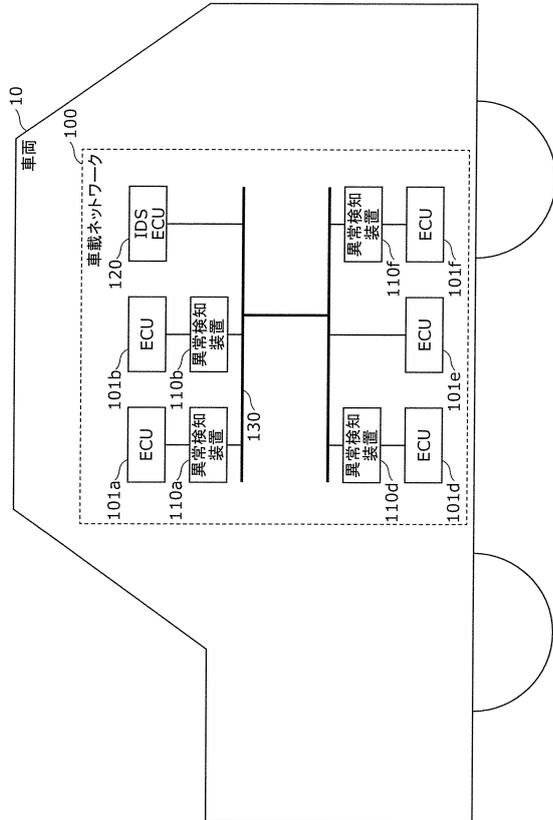
【図 2】



10

20

【図 3】



【図 4】



30

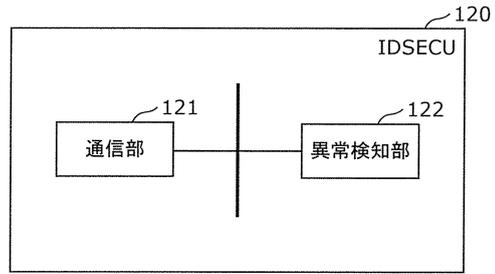
40

50

【図 5】

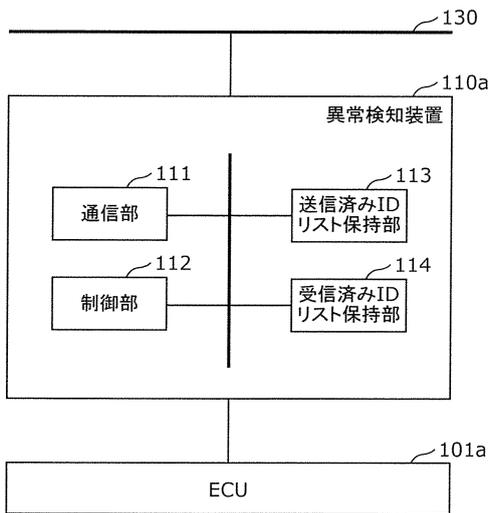
ECU 名	送信を担当するメッセージの ID
エンジン ECU	0x13, 0x15, 0x10
ブレーキ ECU	0x160, 0x330, 0x378
ドア制御 ECU	0x430
...	...

【図 6】

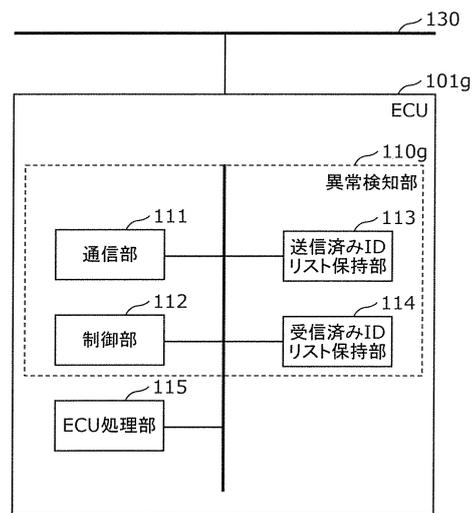


10

【図 7】



【図 8】



20

【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】

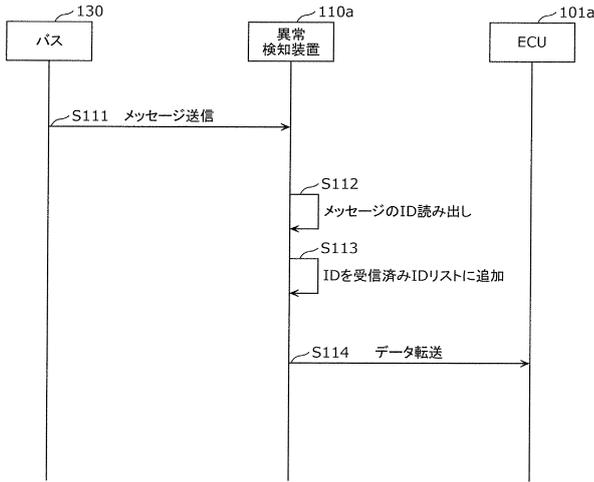
送信したメッセージの ID	送信回数	最近 1 分間の送信回数
0x253	6780	293
0x272	243	16
0x349	60	1
...	...	...

30

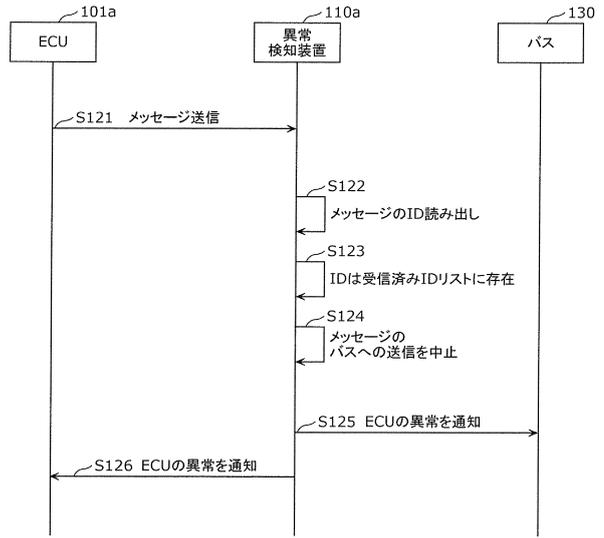
40

50

【図11】

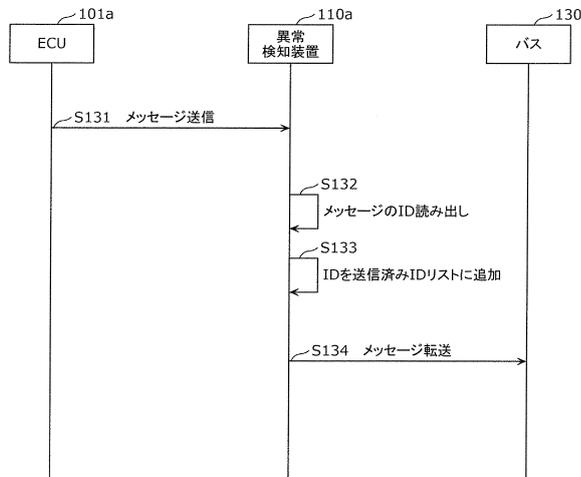


【図12】

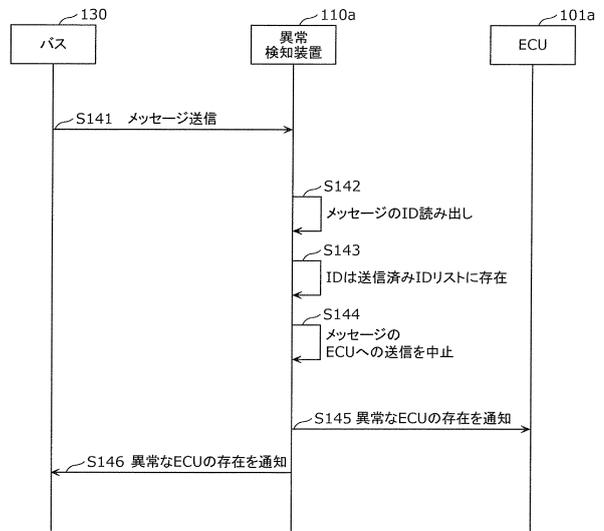


10

【図13】



【図14】



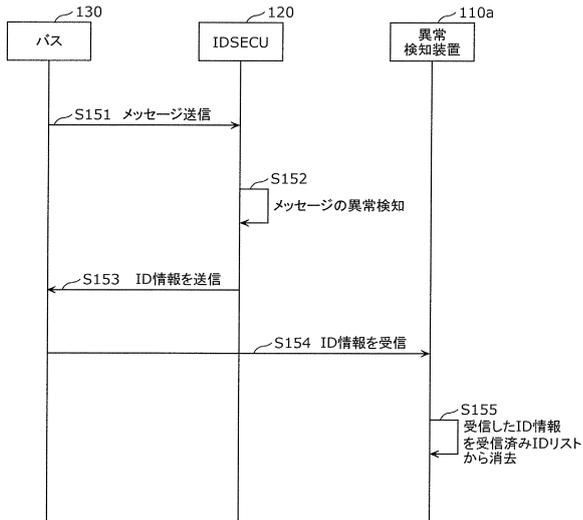
20

30

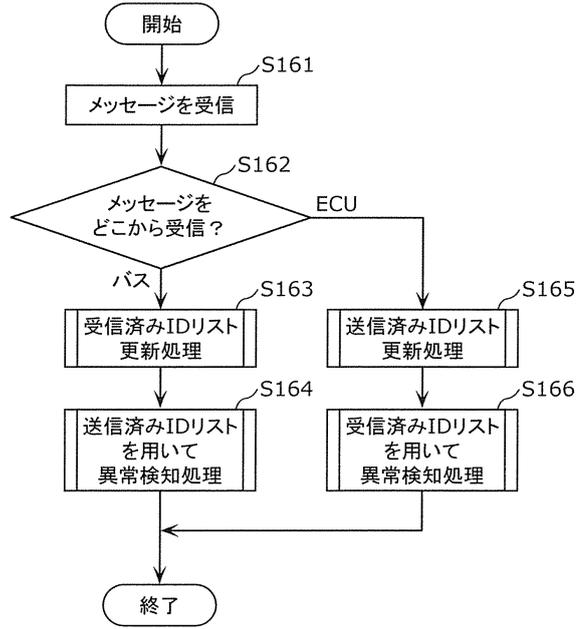
40

50

【図15】



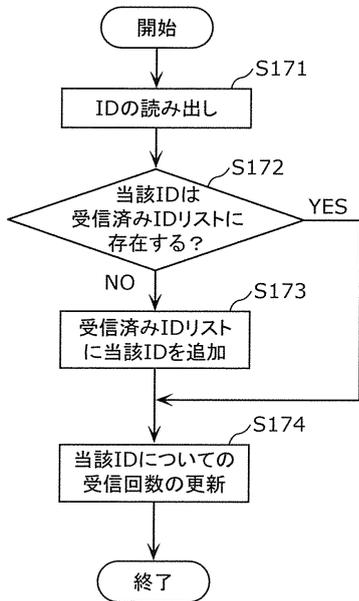
【図16】



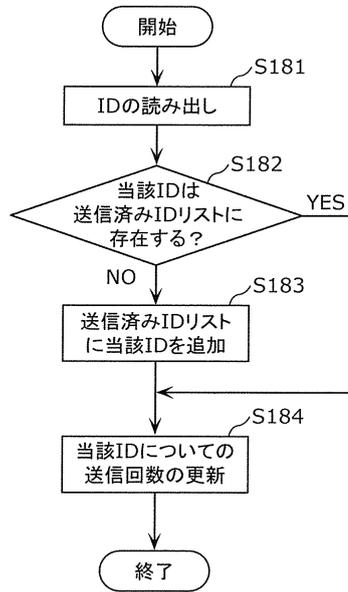
10

20

【図17】



【図18】

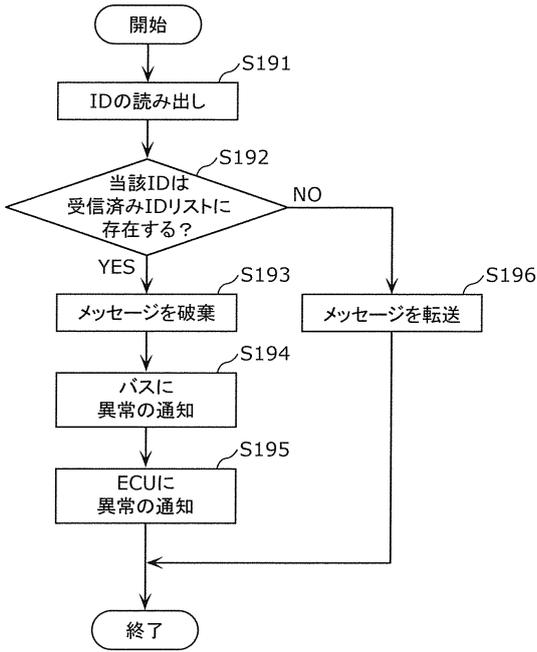


30

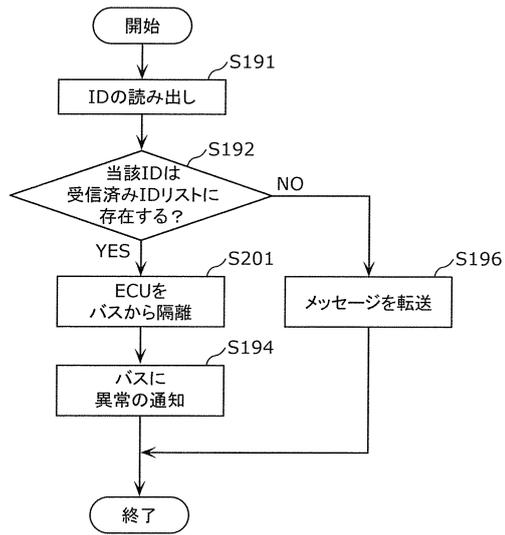
40

50

【図19】



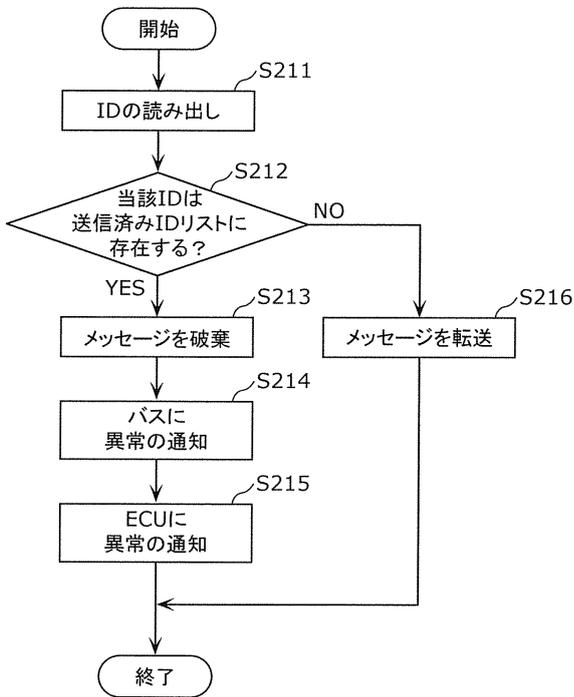
【図20】



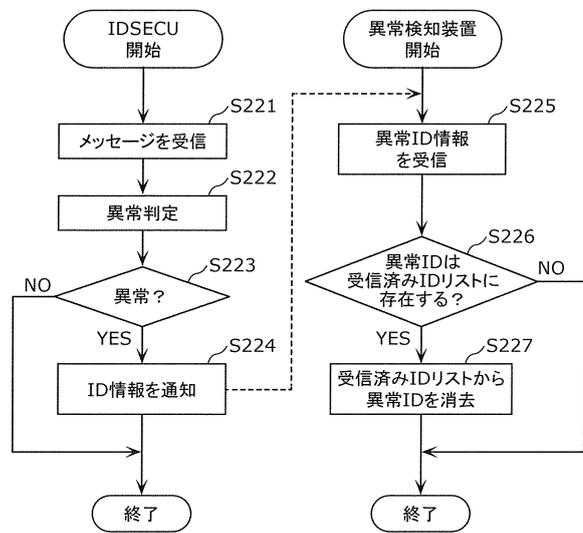
10

20

【図21】



【図22】

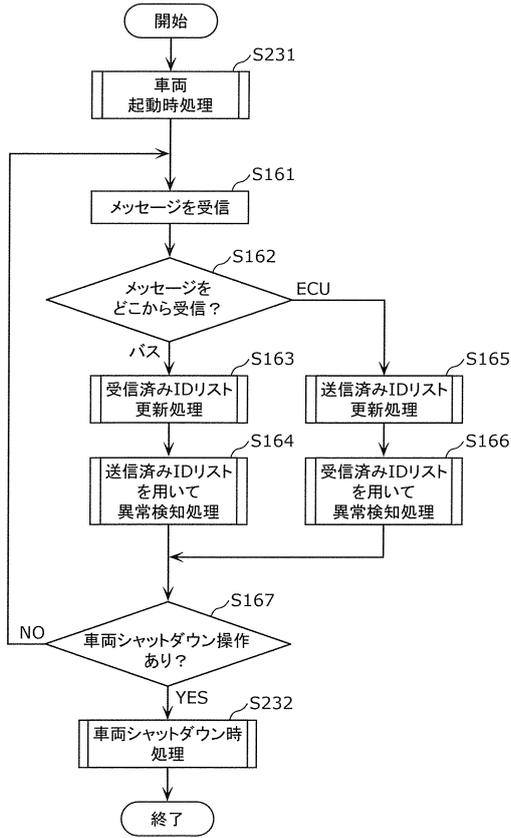


30

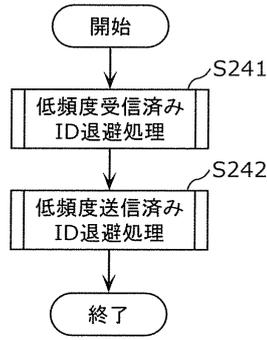
40

50

【図 2 3】



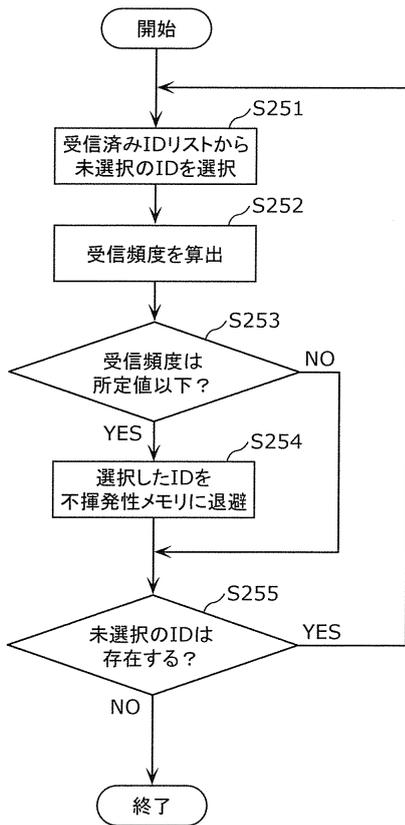
【図 2 4】



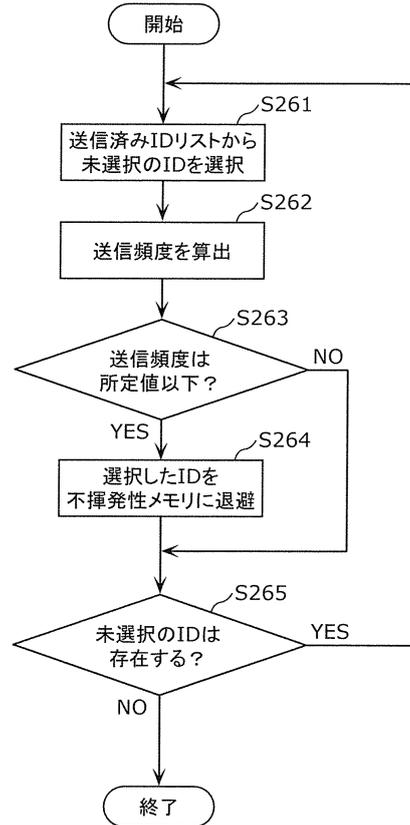
10

20

【図 2 5】



【図 2 6】

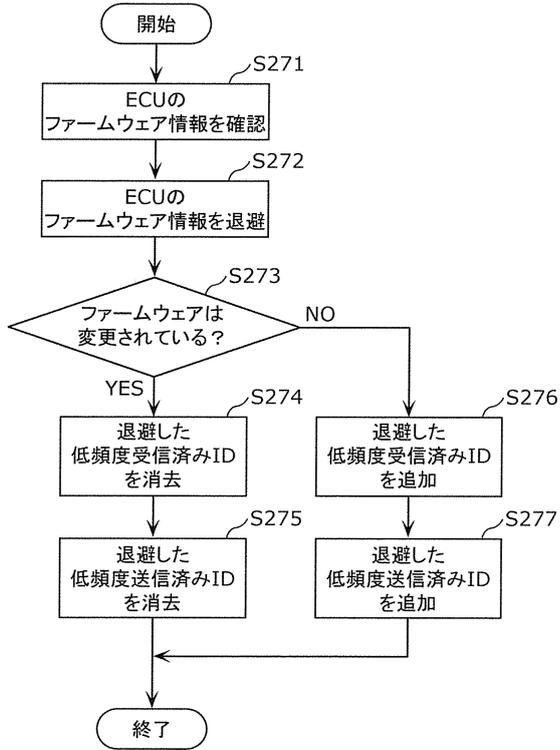


30

40

50

【図 27】



10

20

30

40

50

## フロントページの続き

(72)発明者 高橋 良太

日本国大阪府門真市大字門真 1 0 0 6 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 1 0 0 6 番地 パナソニック株式会社内

審査官 佐々木 洋

(56)参考文献 特開 2 0 1 7 - 0 9 1 2 8 0 ( J P , A )

特開 2 0 1 7 - 0 2 8 5 6 7 ( J P , A )

特開 2 0 1 7 - 1 9 5 5 2 4 ( J P , A )

特開 2 0 1 8 - 0 2 6 7 9 1 ( J P , A )

国際公開第 2 0 1 9 / 2 2 5 2 5 9 ( W O , A 1 )

特開 2 0 1 7 - 0 5 0 7 9 5 ( J P , A )

特開 2 0 1 5 - 0 9 8 3 1 2 ( J P , A )

特開 2 0 1 4 - 0 1 1 6 2 1 ( J P , 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年01月19日, pp.1-6

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年01月21日, pp.1-8

(58)調査した分野 (Int.Cl., D B 名)

H 0 4 L 1 2 / 6 6

H 0 4 L 1 2 / 2 2

H 0 4 L 1 2 / 2 8