(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7280082号
(P7280082)

(45)発行日　令和5年5月23日(2023.5.23)

(24)登録日　令和5年5月15日(2023.5.15)

(51)国際特許分類
H04L 41/00 (2022.01)

FI
H04L 41/00

請求項の数　6　（全32頁）

(21)出願番号　特願2019-57269(P2019-57269)
(22)出願日　平成31年3月25日(2019.3.25)
(62)分割の表示　特願2019-516260(P2019-516260)の分割
原出願日　平成30年12月4日(2018.12.4)
(65)公開番号　特開2019-176473(P2019-176473A)
(43)公開日　令和1年10月10日(2019.10.10)
審査請求日　令和3年12月1日(2021.12.1)
(31)優先権主張番号　特願2018-64431(P2018-64431)
(32)優先日　平成30年3月29日(2018.3.29)
(33)優先権主張国・地域又は機関
日本国(JP)

(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 ９０５０４ カリフォルニア州，トーランス，スイート ４５０，ウエスト １９０ストリート ２０５０
(74)代理人　100109210
弁理士　新居 広守
(74)代理人　100137235
弁理士　寺谷 英作
(74)代理人　100131417
弁理士　道坂 伸一

最終頁に続く

(54)【発明の名称】　不正検知方法、不正検知装置及びプログラム

(57)【特許請求の範囲】

【請求項１】

車載ネットワークにおける異常なメッセージを検知する不正検知方法であって、以下を含む、

前記車載ネットワークに送出された第１メッセージを受信し、

前記第１メッセージの受信時刻が、前記第１メッセージの直前に受信した、データの種類が前記第１メッセージと同じ第２メッセージの受信時刻からの経過時間である予定時刻を含む所定範囲の時刻に収まっているか否かを判定し、

前記判定において、前記第１メッセージの受信時刻が所定範囲の時刻に収まっている場合、前記第１メッセージを正常なメッセージと判定し、

前記判定において、前記第１メッセージの受信時刻が所定範囲の時刻に収まっていない場合、前記第１メッセージの受信時に調停が発生していたか否かを検出し、

前記第１メッセージの受信時に調停が発生していなかった場合、前記第１メッセージを異常なメッセージと判定し、

前記第１メッセージの受信時に調停が発生していた場合、

１つまたは連続して続いている複数の第３メッセージと、前記１つまたは連続して続いている複数の第３メッセージに続いて前記第１メッセージが連続して受信されている場合、前記１つまたは連続して続いている複数の第３メッセージのうち、受信時刻が一番早いメッセージの受信時刻を調停の開始時刻とし、

調停の開始時刻が前記所定範囲の時刻の上限より早い場合、前記第１メッセージを正常

なメッセージと判定し、
　調停の開始時刻が前記所定範囲の時刻の上限以降の場合、前記第１メッセージを異常なメッセージと判定する、
　不正検知方法。
【請求項２】
　前記第１メッセージの直後に受信する、データの種類が前記第１メッセージと同じ第４メッセージの予定時刻を算出するための起点となる時刻である起点時刻を前記第１メッセージの受信時刻または前記第１メッセージの予定時刻に決定することを含み、
　前記第４メッセージの受信時刻が予定時刻を含む所定範囲の時刻に収まっているか否かの判定は、前記決定された時刻を前記起点時刻として用いて判定する、
　請求項１に記載の不正検知方法。
【請求項３】
　前記決定では、
　　前記判定において前記第１メッセージの受信時刻が所定範囲の時刻に収まっている場合、前記第１メッセージの受信時刻を前記起点時刻に決定し、
　　前記判定において前記第１メッセージの受信時刻が所定範囲の時刻に収まっていない場合、かつ、前記検出において前記第１メッセージの受信時に調停が発生し、調停の開始時刻が前記所定範囲の時刻の上限より早い場合、前記第１メッセージの受信時刻又は前記第１メッセージの予定時刻を前記起点時刻に決定する、
　請求項２に記載の不正検知方法。
【請求項４】
　前記第１メッセージのタイプを判定し、
　前記決定において、前記タイプに応じて前記起点となる時刻を前記メッセージの受付時刻または受け付け予定時刻に決定することを含む、
　請求項２に記載の不正検知方法。
【請求項５】
　車載ネットワークにおける異常なメッセージを検知する不正検知装置であって、
　１個以上のプロセッサと、
　記憶部と、を含み、
　前記１個以上のプロセッサは、前記記憶部を用いて、
　前記車載ネットワークに送出された第１メッセージを受信し、
　前記第１メッセージの受信時刻が、前記第１メッセージの直前に受信した、データの種類が前記第１メッセージと同じ第２メッセージの受信時刻からの経過時間である予定時刻を含む所定範囲の時刻に収まっているか否かを判定し、
　前記判定において、前記第１メッセージの受信時刻が所定範囲の時刻に収まっている場合、前記第１メッセージを正常なメッセージと判定し、
　前記判定において、前記第１メッセージの受信時刻が所定範囲の時刻に収まっていない場合、前記第１メッセージの受信時に調停が発生していたか否かを検出し、
　前記第１メッセージの受信時に調停が発生していなかった場合、前記第１メッセージを異常なメッセージと判定し、
　前記第１メッセージの受信時に調停が発生していた場合、
　　１つまたは連続して続いている複数の第３メッセージと、前記１つまたは連続して続いている複数の第３メッセージに続いて前記第１メッセージが連続して受信されている場合、前記１つまたは連続して続いている複数の第３メッセージのうち、受信時刻が一番早いメッセージの受信時刻を調停の開始時刻とし、
　　調停の開始時刻が前記所定範囲の時刻の上限より早い場合、前記第１メッセージを正常なメッセージと判定し、
　　調停の開始時刻が前記所定範囲の時刻の上限以降の場合、前記第１メッセージを異常なメッセージと判定する、
　不正検知装置。

【請求項６】
コンピュータに請求項１に記載の不正検知方法を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、車載ネットワークにおける異常なメッセージを検知する不正検知方法等に関する。
【背景技術】
【０００２】
近年、自動車の中のシステムには、電子制御ユニット（ＥＣＵ：Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐ通信ネットワークは車載ネットワークと呼ばれる。車載ネットワークには、多数の通信規格が存在する。その中でも最も主流な車載ネットワークの規格の一つに、Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅｔｗｏｒｋ（ＣＡＮ）がある。
【０００３】
ＣＡＮの規格に拠るネットワーク（ＣＡＮネットワーク）では、通信路（バス）は２本のケーブルで構成され、バスに接続されているＥＣＵはノードとも呼ばれる。バスに接続されている各ノードは、フレーム又はメッセージと呼ばれる単位でデータを送受信する。またＣＡＮでは、データの送信先又は送信元を示す識別子は用いられない。
【０００４】
フレームを送信するノード（送信ノード）は、メッセージ毎にメッセージの種類を示すメッセージＩＤと呼ばれるＩＤを付けてメッセージを送信、つまりバスに信号を送出する。メッセージを受信するノード（受信ノード）は、予め決められたメッセージＩＤを含むメッセージのみ受信、つまりバスから信号を読み取る。同一ＩＤのメッセージは、一定の周期で送信される。
【０００５】
上述の通り、自動車の中のシステムに多数配置されているＥＣＵは、それぞれがＣＡＮネットワークに接続され、様々なメッセージを互いにやりとりしながら動作している。
【０００６】
ここで、ＣＡＮネットワークの外部と通信機能を持つＥＣＵが、外部から不正にアクセスされること等により、何者かに不正に制御され、ＣＡＮネットワークに対して異常なメッセージ（攻撃メッセージ）を送信することが起こり得る。このような何者かに不正に制御されたＥＣＵ（不正ＥＣＵ）は、例えば他のＥＣＵになりすまして異常なメッセージを送信し、車両を不正に制御することが可能となる。このような、いわゆるなりすまし攻撃を検知するための方法が、例えば、特許文献１に開示されている。
【先行技術文献】
【特許文献】
【０００７】
【文献】国際公開第２０１４／１１５４５５号
【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、特許文献１に開示されている方法では、ＣＡＮネットワークバス上の送信周期の乱れにより正常なメッセージの送信周期が長くなった場合に、正しい判断ができないという課題がある。
【０００９】
本開示は、上記課題を解決するもので、バスに送出された個々のメッセージが異常なメッセージであるか否かを判定する不正検知方法、不正検知装置等を提供することを目的とする。
【課題を解決するための手段】

【００１０】
上記課題を解決するために、本開示の一態様に係る不正検知方法は、車載ネットワークにおける異常なメッセージを検知する不正検知方法であって、以下を含む、前記車載ネットワークに送出された第１メッセージを受信し、前記第１メッセージの受信時刻が、前記第１メッセージの直前に受信した、データの種類が前記第１メッセージと同じ第２メッセージの受信時刻からの経過時間である予定時刻を含む所定範囲の時刻に収まっているか否かを判定し、前記判定において、前記第１メッセージの受信時刻が所定範囲の時刻に収まっている場合、前記第１メッセージを正常なメッセージと判定し、前記判定において、前記第１メッセージの受信時刻が所定範囲の時刻に収まっていない場合、前記第１メッセージの受信時に調停が発生していたか否かを検出し、前記第１メッセージの受信時に調停が発生していなかった場合、前記第１メッセージを異常なメッセージと判定し、前記第１メッセージの受信時に調停が発生していた場合、１つまたは連続して続いている複数の第３メッセージと、前記１つまたは連続して続いている複数の第３メッセージに続いて前記第１メッセージが連続して受信されている場合、前記１つまたは連続して続いている複数の第３メッセージのうち、受信時刻が一番早いメッセージの受信時刻を調停の開始時刻とし、調停の開始時刻が前記所定範囲の時刻の上限より早い場合、前記第１メッセージを正常なメッセージと判定し、調停の開始時刻が前記所定範囲の時刻の上限以降の場合、前記第１メッセージを異常なメッセージと判定する。
【００１１】
なお、これら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又はコンピュータ読み取り可能なＣＤ－ＲＯＭなどの非一時的な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及び記録媒体の任意な組み合わせで実現されてもよい。
【発明の効果】
【００１２】
本開示の一態様に係る不正検知方法等によれば、バスに送出された個別のメッセージが異常なメッセージであるか否かを判定することができる。
【図面の簡単な説明】
【００１３】
【図１】図１は、実施の形態１における車載ネットワークシステムの全体構成を示すブロック図である。
【図２】図２は、実施の形態１におけるＣＡＮプロトコトルのメッセージ（データフレーム）のフォーマットを示す図である。
【図３】図３は、実施の形態１における車載ネットワークシステムに含まれるゲートウェイの構成を示すブロック図である。
【図４】図４は、実施の形態１における受信ＩＤリストの一例を示す図である。
【図５】図５は、実施の形態１における転送ルールの一例を示す図である。
【図６】図６は、実施の形態１における不正検知処理機能群の一例を示すブロック図である。
【図７Ａ】図７Ａは、実施の形態１における調停発生時のメッセージの受信パターンを示す図である。
【図７Ｂ】図７Ｂは、実施の形態１における調停発生時のメッセージの受信パターンを示す別の図である。
【図８】図８は、実施の形態１における不正検知処理機能群の別の一例を示すブロック図である。
【図９】図９は、実施の形態１における車載ネットワークシステムに含まれるＥＣＵの一例を示すブロック図である。
【図１０】図１０は、実施の形態１における不正検知処理の一例を示すフローチャートである。
【図１１】図１１は、実施の形態１における転送処理の一例を示すフローチャートである。

【図１２】図１２は、実施の形態２における不正検知処理機能群の一例を示すブロック図である。
【図１３】図１３は、実施の形態２における不正検知処理の一例を示すフローチャートである。
【図１４】図１４は、変形例における不正検知処理機能群の一例を示す図である。
【図１５】図１５は、変形例における不正検知処理機能群の一例を示す図である。
【図１６】図１６は、変形例におけるＥＣＵの一例を示すブロック図である。
【図１７】図１７は、変形例におけるＥＣＵの一例を示すブロック図である。
【図１８】図１８は、変形例におけるＥＣＵの一例を示すブロック図である。
【発明を実施するための形態】
【００１４】
（本開示の基礎になった知見）
ＣＡＮネットワーク上に、多くのＥＣＵが接続されている場合、それぞれのＥＣＵが独立してメッセージを送信しようとすると、メッセージの送信タイミングが同じになる可能性が高くなる。
【００１５】
その場合は、ＣＡＮネットワークには、「調停」と呼ばれる機能があり、ＩＤの小さいメッセージが優先的に送信され、ＩＤの大きなメッセージは、送信を待つことになる。そうすると、メッセージを送信する送信タイミングにずれが生じるため、メッセージの送信間隔に応じて正常なメッセージか異常なメッセージかを判定する機能が誤作動し、正常なメッセージを異常なメッセージであると判定する可能性が生じる。
【００１６】
そこで、本開示の一態様に係る不正検知方法は、記憶部を含む情報処理システムで実行される、車載ネットワークシステムにおける異常なメッセージを検知する不正検知方法であって、前記車載ネットワークシステムに、繰り返し送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップと、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していたか否かを検出する調停検出ステップと、前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していなかった場合、前記メッセージを異常なメッセージと判定するメッセージ判定ステップとを含む。
【００１７】
これにより、車載ネットワークシステムに送出されたメッセージに調停などによって送信遅れが生じた場合に、受信したメッセージが、正常なメッセージか否かを適切に判定できる。その結果、個々のメッセージが異常なメッセージであるか否かの判定は、より高い精度で実行される。
【００１８】
また例えば、前記周期異常判定ステップで周期を判定する際に周期の起点となる時刻を前記メッセージの受け付け時刻または、受け付け予定時刻に決定する周期起点決定ステップとを含み、前記周期異常検知ステップでは、前記周期起点決定ステップで決定された起点を用いて周期を判定してもよい。
【００１９】
これにより、調停が発生した際のメッセージ送信方法が複数ある場合においても、メッセージの受信時刻に現れる特徴に基づいて正常なメッセージであるか否かを判断することで、より高い精度で異常なメッセージを判定できる。
【００２０】
また、例えば、前記メッセージの送信タイプを判定する送信タイプ判定ステップを含み、前記周期起点決定ステップでは、送信タイプに応じて前記メッセージの受け付け時刻または受け付け予定時刻に決定してもよい。
【００２１】
これにより、車載ネットワークに送出されたメッセージの送信タイプに応じた、調停検

出を行うことができる。
【００２２】
　また、例えば、前記調停検出ステップでは、前記メッセージが、前記メッセージを受信する周期の正常範囲内の時刻に受信された他のメッセージから連続して受信された１つ以上のメッセージに含まれる場合、調停が発生したと判定してもよい。
【００２３】
　これにより、調停などによってメッセージの送信遅れが生じた場合でも、受信したメッセージが正常なメッセージか否かを適切に判定できる。
【００２４】
　また、本開示の一態様に係る不正検知装置は、車載ネットワークシステムにおける異常なメッセージを検知する不正検知装置であって、１個以上のプロセッサと、記憶部と、を含み、前記記憶部を用いて、前記１個以上のプロセッサは、前記車載ネットワークシステムに送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップと、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していたかどうかを検出する調停検出ステップと、前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していた場合、前記メッセージを正常なメッセージと判定する周期判定ステップとを行う。
【００２５】
　これにより、車載ネットワークシステムに送出されたメッセージが調停などにより送信遅れが生じても、正常なメッセージか否かを適切に判定できる。その結果、個々のメッセージが異常なメッセージであるか否かの判定も、より高い精度で実行される。
【００２６】
　また、本開示の一態様に係るプログラムは、上記の不正検知装置において、前記１個以上のプロセッサに上記の不正検知方法のいずれかを実施させるためのプログラムである。
【００２７】
　これにより、車載ネットワークシステムに送出されたメッセージに調停などによって送信遅れが生じても、正常なメッセージか否かを適切に判定できる。その結果、個々のメッセージが異常なメッセージであるか否かの判定も、より高い精度で実行される。
【００２８】
　以下、実施の形態について図面を参照しながら具体的に説明する。
【００２９】
　なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置および接続形態、ステップ、ステップの順序などは一例であり、本開示を限定する趣旨ではない。以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素は、任意で含まれる構成要素として説明されるものである。
【００３０】
　（実施の形態１）
　［１．概要］
　本実施の形態では、車載ネットワークシステムにおいて、送信されているメッセージが異常なメッセージであるか否かの判定がなされる場合について図面を参照しながら説明する。なお、ここで、異常なメッセージは、基本的に、不正なメッセージである。
【００３１】
　［１．１　車載ネットワークシステムの全体構成］
　図１は、本実施の形態における車載ネットワークシステム１０の全体構成を示すブロック図である。
【００３２】
　図１において、車載ネットワークシステム１０は、ＣＡＮネットワークで構成され、ＥＣＵ１００ａ、ＥＣＵ１００ｂ、ＥＣＵ１００ｃ、及びＥＣＵ１００ｄと、バス２００ａ及びバス２００ｂと、ゲートウェイ３００とを含む。

【００３３】
以下では、ＥＣＵ１００ａ、ＥＣＵ１００ｂ、ＥＣＵ１００ｃ、ＥＣＵ１００ｄを、集合的にＥＣＵ１００とする場合がある。又、ＥＣＵ１００ａ、ＥＣＵ１００ｂ、ＥＣＵ１００ｃ、ＥＣＵ１００ｄのいずれかを指して、ＥＣＵ１００として説明する場合がある。
【００３４】
また、以下では、バス２００ａ、バス２００ｂ集合的にバス２００とする場合がある。又、バス２００ａ及びバス２００ｂのいずれか一方を指して、バス２００とする場合がある。
【００３５】
ＥＣＵ１００ａはエンジン１０１に接続され、ＥＣＵ１００ｂはブレーキ１０２に接続される。また、ＥＣＵ１００ｃはドア開閉センサ１０３に接続され、ＥＣＵ１００ｄはウィンドウ開閉センサ１０４に接続されている。
【００３６】
ＥＣＵ１００は、接続されている機器の状態を取得し、取得した状態を表すメッセージを周期的にバス２００に送出する。例えばＥＣＵ１００ａは、エンジン１０１の回転数を取得し、この回転数を表すデータ値を含むメッセージに所定のＩＤを付けてバス２００に送出する。
【００３７】
また、各ＥＣＵ１００は、他のＥＣＵ１００が送信したメッセージをバス２００から読み出し、メッセージに付されたＩＤに応じて選択的に受信する。この選択的な受信については後述する。
【００３８】
ゲートウェイ３００は、ＥＣＵ１００ａ及びＥＣＵ１００ｂが接続されているバス２００ａと、ＥＣＵ１００ｃ及びＥＣＵ１００ｄが接続されているバス２００ｂとを接続している。ゲートウェイ３００は一方のバスから受信したメッセージを、もう一方のバスに転送する機能を持つ。ゲートウェイ３００もまた、ＣＡＮネットワーク上ではひとつのノードである。
【００３９】
なお、車載ネットワークシステム１０は、メッセージが異常なメッセージであるか否かの判定をする不正通信検知システム等が適用可能な対象を説明するための例であり、その適用対象は車載ネットワークシステム１０に限定されない。ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）等を用いた各種ネットワークシステム又は分散データベース等に適用されてもよい。
【００４０】
［１．２ メッセージのデータフォーマット］
図２は、ＣＡＮプロトコルのメッセージ（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メッセージを示している。
【００４１】
メッセージは、Ｓｔａｒｔ Ｏｆ Ｆｒａｍｅ（ＳＯＦ）と、ＩＤフィールド、Ｒｅｍｏｔｅ Ｔｒａｎｓｉｍｉｓｓｉｏｎ Ｒｅｑｕｅｓｔ（ＲＴＲ）、ＩＤＥ（ＩＤｅｎｔｉｆｉｅｒ Ｅｘｔｅｎｓｉｏｎ）、予約ｂｉｔ（ｒ）、データレングスコード（ＤＬＣ）、データフィールド、ＣＲＣ（Ｃｙｃｒｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）シーケンス、ＣＲＣデリミタ（図中、左のＤＥＬ）と、ＡＣＫ（Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ）スロットと、ＡＣＫデリミタ（図中、右のＤＥＬ）と、ＥＯＦ（Ｅｎｄ Ｏｆ Ｆｒａｍｅ）から構成される。
【００４２】
ＳＯＦは、１ｂｉｔのドミナントである。ドミナントは、優性の意である。ドミナントは、データの伝達にデジタル方式が用いられるＣＡＮネットワークにおいて、“０”の値を送信するようにバスを構成する２本のケーブルに電圧がかけられた状態、または送信され

るこの“０”の値のことである。これに対し、“バスを構成する２本のケーブルに１”の値を送信するように電圧がかけられた状態、または送信されるこの“１”の値のことはレセシブと呼ばれる。レセシブは、劣勢の意である。２つのノードからバスに同時に“０”の値と“１”の値とが送信された場合には、“０”の値が優先される。アイドル時のバスはレセシブの状態である。各ＥＣＵ１００は、バス２００の状態をレセシブからドミナントへ変化させることでメッセージの送信を開始し、他のＥＣＵ１００はこの変化を読み取って同期する。図２において、メッセージを構成するドミナント又はレセシブを示す線が実線である部分は、ドミナント又はレセシブの各値を取り得ることを示す。ＳＯＦはドミナントの状態で固定されているため、ドミナントの線は実線であり、レセシブの線は破線である。

【００４３】

ＩＤとは、メッセージが含むデータの種類を示す１１ｂｉｔの値である。またＣＡＮでは、複数のノードが同時に送信を開始したメッセージ間での通信調停において、ＩＤの値がより小さいメッセージがより高い優先度となるよう設計されている。

【００４４】

ＲＴＲとは、フレームがメッセージ（データフレーム）であることを示す１ｂｉｔのドミナントである。

【００４５】

ＩＤＥとは、それぞれ１ｂｉｔのドミナントである。

【００４６】

ＤＬＣは、続くデータフィールドの長さを示す４ｂｉｔの値である。

【００４７】

データフィールドは、送信されるデータの内容を示す値であり、最大６４ｂｉｔ長で、８ｂｉｔ単位で長さを調整できる。送られるデータのこの部分への割り当てに関する仕様は、車種又は製造者に依存する。

【００４８】

ＣＲＣシーケンスは、ＳＯＦ、ＩＤフィールド、コントロールフィールド、データフィールドの送信値より算出される１５ｂｉｔの値である。

【００４９】

ＣＲＣデリミタは１ｂｉｔのレセシブ固定の、ＣＲＣシーケンスの終了を表す区切り記号である。受信ノードは、受信したメッセージのＳＯＦ、ＩＤフィールド、コントロールフィールド、及びデータフィールドの値から算出した結果をＣＲＣシーケンスの値と比較することで異常の有無を判断する。

【００５０】

ＡＣＫスロットは１ｂｉｔ長で、送信ノードはこの部分でレセシブを送信する。受信ノードはＣＲＣシーケンスまで正常に受信ができていれば確認応答としてドミナントを送信する。ドミナントが優先されるため、１メッセージの通信がＣＲＣシーケンスまで正常に行われていれば、ＡＣＫスロットの送信中のバス２００はドミナントである。

【００５１】

ＡＣＫデリミタは１ｂｉｔのレセシブに固定されており、ＡＣＫスロットの終了を表す区切り記号である。

【００５２】

ＥＯＦは７ｂｉｔのレセシブに固定されており、メッセージの終了を示す。

【００５３】

［１．３　ゲートウェイの構成］

図３は、本実施の形態における車載ネットワークシステム１０に含まれるゲートウェイ３００の構成を示すブロック図である。図３において、ゲートウェイ３００は、フレーム送受信部３１０と、フレーム解釈部３２０と、受信ＩＤ判定部３３０と、受信ＩＤリスト保持部３４０と、フレーム処理部３５０と、転送ルール保持部３６０と、不正検知処理機能群３７０と、フレーム生成部３８０とを備える。

【００５４】

なお、これらの構成は機能を示す構成であり、ゲートウェイ３００は、例えばプロセッサで実現される処理部、半導体メモリ等で実現される記憶部、入出力ポートで実現される入出力部等を備える情報処理装置として提供される。

【００５５】

上記の機能を示す構成は、記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを記録することで実現される。若しくは、記憶部へ所定のデータを記録することの代わりに、入出力部を介してデータの送受信を実行することでこれらの構成が実現されてもよい。又は、上記の機能を示す構成は、これらの組み合わせで実現されてもよい。

【００５６】

フレーム送受信部３１０は、バス２００ａ、２００ｂのそれぞれに対して、ＣＡＮのプロトコルに従ったメッセージを送受信する。

【００５７】

より具体的には、フレーム送受信部３１０は、バス２００に送出されたメッセージを１ｂｉｔずつ読み出し、読み出したメッセージをフレーム解釈部３２０に転送する。

【００５８】

また、フレーム送受信部３１０は、フレーム生成部３８０より送信されたバス情報に応じて、メッセージをバス２００ａ及び２００ｂに１ｂｉｔずつ送出する。

【００５９】

フレーム送受信部３１０は、バス２００ａから受信したメッセージをバス２００ｂに送信し、バス２００ｂから受信したメッセージをバス２００ａに送信することでバス２００間でのメッセージの転送を実行する。

【００６０】

フレーム解釈部３２０は、フレーム送受信部３１０よりメッセージの値を受け取り、ＣＡＮプロトコルにおける各フィールドにマッピングして、受信したメッセージの解釈を行う。フレーム解釈部３２０は、ＩＤフィールドの値と解釈した一連の値を、受信ＩＤ判定部３３０へ転送する。

【００６１】

フレーム解釈部３２０はさらに、受信ＩＤ判定部３３０から通知される判定結果に応じて、メッセージのＩＤフィールドの値及びＩＤフィールド以降に現れるデータフィールドをフレーム処理部３５０へ転送するか、メッセージの受信を中止するかを決定する。

【００６２】

また、フレーム解釈部３２０は、受信したメッセージがＣＡＮプロトコルに則っていないメッセージと判断した場合は、エラーフレームを送信するようにフレーム生成部３８０へ要求する。

【００６３】

エラーフレームは、ＣＡＮネットワーク上でエラーが発生した場合に、ノードから送信される、上述のメッセージとは異なる、ＣＡＮプロトコルで規定される所定のフォーマットのフレームである。エラーフレームがバスに送出されると、そのネットワークでのメッセージの送信は中断される。

【００６４】

また、フレーム解釈部３２０は、他のノードが送信したエラーフレームを受信したと解釈した場合、読み取り中のメッセージを破棄する。

【００６５】

受信ＩＤ判定部３３０は、フレーム解釈部３２０からＩＤフィールドの値を受け取り、受信ＩＤリスト保持部３４０が保持しているメッセージＩＤのリストに従い、読み出したメッセージを受信するか否かの判定を行う。受信ＩＤ判定部３３０は、この判定の結果をフレーム解釈部３２０へ通知する。

【００６６】

受信ＩＤリスト保持部３４０は、ゲートウェイ３００が受信するメッセージＩＤのリス

ト（受信ＩＤリスト）を保持する。図４は、本実施の形態における受信ＩＤリストの一例を示す図である。図４における受信ＩＤリストの詳細は、後述する。

【００６７】

フレーム処理部３５０は、転送ルール保持部３６０が保持するデータ転送に関するルールに従って、受信したメッセージのＩＤに応じて転送先となるバス２００を決定し、転送先となるバス２００と、フレーム解釈部３２０より通知されたメッセージＩＤと、転送するデータとをフレーム生成部３８０へ通知する。

【００６８】

またフレーム処理部３５０は、フレーム解釈部３２０より受け取ったメッセージを不正検知処理機能群３７０へ送り、不正検知処理機能群３７０に対して、そのメッセージが、異常なメッセージであるか否かの判定を行うように要求する。不正検知処理機能群３７０において異常なメッセージであると判定されたメッセージを、フレーム処理部３５０は転送しない。

【００６９】

転送ルール保持部３６０は、各バス２００のデータ転送に関するルール（以下、転送ルールともいう）を保持する。図５は、本実施の形態における転送ルールの一例を示す図である。図５における転送ルールの詳細は、後述する。

【００７０】

不正検知処理機能群３７０は、受信中のメッセージが異常なメッセージであるか否かを判定する機能群である。不正検知処理機能群３７０に含まれる機能構成の詳細は後述する。

【００７１】

フレーム生成部３８０は、フレーム解釈部３２０からのエラーフレーム送信の要求に従い、エラーフレームを生成し、フレーム送受信部３１０にエラーフレームを送出させる。

【００７２】

またフレーム生成部３８０は、フレーム処理部３５０より受け取ったメッセージＩＤ及びデータを使ってメッセージフレームを生成し、バス情報とともに、フレーム送受信部３１０にメッセージフレームを送出する。

【００７３】

［１．４　受信ＩＤリスト］

図４は、本実施の形態における受信ＩＤリストの一例を示す図である。受信ＩＤリストは、ゲートウェイ３００が受信して処理するメッセージのメッセージＩＤのリストである。

【００７４】

図４において、受信ＩＤリストは、各行にメッセージのＩＤが格納されている。図４の受信ＩＤリストは、メッセージＩＤが、「１」、「２」、「３」及び「４」であり、ゲートウェイ３００は、これらのメッセージＩＤのメッセージを受信する。ゲートウェイ３００は、受信ＩＤリストに含まれないメッセージＩＤのメッセージの受信を中止する。

【００７５】

なお、ＩＤの値及び受信ＩＤリストに含まれるＩＤの個数は説明のための一例であり、ゲートウェイ３００で用いられる受信ＩＤリストの構成をこれに限定するものではない。

【００７６】

［１．５　転送ルール］

図５は、本実施の形態における転送ルールの一例を示す図である。図５において、転送ルールは、各行にメッセージの転送元のバスと転送先のバス、及び転送対象のメッセージＩＤの組み合わせが格納されている。

【００７７】

具体的には、転送ルールの１行目は、転送元「バス２００ａ」、転送先「バス２００ｂ」、ＩＤ「＊」であり、ゲートウェイ３００は、バス２００ａから受信するメッセージを、ＩＤが何であってもバス２００ｂに転送する、というルールである。転送ルールの２行目は、転送元「バス２００ｂ」、転送先「バス２００ａ」、ＩＤ「３」であり、ゲートウェイ３００は、バス２００ｂから受信するメッセージは、ＩＤが「３」のメッセージであ

ればバス２００ａに転送する、というルールである。
【００７８】
［１．６　不正検知処理機能群の構成］
図６は、本実施の形態におけるゲートウェイ３００が備える不正検知処理機能群３７０の一例を示すブロック図である。図６において、不正検知処理機能群３７０は、周期判定部３７１と、ルール判定情報保持部３７２と、調停検出部３７３と、受信メッセージ情報保持部３７４とを含む。
【００７９】
なお、これらの構成は機能を示す構成であり、ゲートウェイ３００において記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを保持する。若しくは、記憶部へ所定のデータを記録することの代わりに、入出力部を介してデータの送受信を実行することでこれらの構成が実現されてもよい。又は、これらの構成は、上記の組み合わせで実現されてもよい。
【００８０】
周期判定部３７１は、同じＩＤを持つメッセージごとに、メッセージを受信した周期（経過時間）が正常と判定できる範囲内に収まっているかどうかを判定する。
【００８１】
周期判定部３７１は、フレーム処理部３５０から受信したメッセージからメッセージのＩＤを取得し、そのＩＤに関連した周期を判定するために必要な情報を取得する。具体的には、ルール、前回受信時刻、をルール判定情報保持部３７２から取得する。
【００８２】
周期判定部３７１は、現在のメッセージを受信した時刻と、ルール判定情報保持部３７２から取得した前回受信時刻との差を求め、その差の値（経過時間）が、ルール判定情報保持部３７２から取得したルールで示される範囲内に含まれるかどうかを判定する。
【００８３】
周期判定部３７１は、上記経過時間がルールで示される範囲内に含まれる場合はＯＫと判定し、上記経過時間がルールで示される範囲から外れる場合はＮＧと判定する。
【００８４】
ここで、ルールは、同じＩＤのメッセージを前回受信してからの経過時間の上限と下限の情報であってもよい。また、ルールは、基準となる経過時間の値と、基準となる時間からのＯＫと判定される範囲の幅の情報であってもよい。
【００８５】
また、周期判定部３７１における判定は、メッセージを受信した時刻と、前回受信時刻との差が、ルールで示される範囲内に含まれるか否かの判定をするとしたが、これに限定されない。例えば、周期判定部３７１は、前回受信時刻にルールで示される経過時間の範囲を足すことで、期待する受信時刻の範囲を求め、今回受信したメッセージの受信時刻が、その期待する受信時刻の範囲内に含まれるか否かを判定してもよい。
【００８６】
また、周期判定部３７１は、調停検出部３７３に、メッセージを受信した際に調停が発生していたかどうかを問い合わせる。周期判定部３７１は、調停検出部３７３から調停が発生していたか否かを示す情報と、調停が発生していた場合は、その発生している調停の開始時刻を取得する。
【００８７】
周期判定部３７１は、ＮＧと判定した場合において、調停が発生していた場合、調停の開始時刻が上記ルールで示される範囲の上限より早い場合、すなわち、値が小さい場合には、判定をＯＫに変更する。また、調停が発生していなかった場合には、判定をＮＧのままで変更しない。
【００８８】
なお、周期判定部３７１は、メッセージを受信するたびに調停検出部３７３へ調停が発生していたか否かを問い合わせてもよい。また、ルール判定情報保持部３７２から取得し

たルールに対する判定がＮＧの場合にのみ、調停検出部３７３へ調停が発生していたか否かを問い合わせてもよい。

【００８９】

周期判定部３７１が、ルール判定情報保持部３７２から取得したルールに対する判定がＮＧの時のみ調停検出部３７３へ調停が発生していたか否かを問い合わせる場合は、周期判定部３７１は、メッセージを受信するたびに、メッセージの受信時刻を調停検出部３７３へ通知するか、受信メッセージ情報保持部３７４へ受信時刻を保存する。

【００９０】

また、周期判定部３７１は、調停検出部３７３において調停が発生していた場合、メッセージの受信時刻が基準となる経過時間の値より小さい場合に、判定をＯＫに変更してもよい。

【００９１】

また、周期判定部３７１は、判定がＯＫの場合に、その時に受信したメッセージの受信時刻を、ルール判定情報保持部３７２へ通知する。

【００９２】

ルール判定情報保持部３７２は、周期判定部３７１が使用するルールとメッセージに含まれるＩＤごとのメッセージの受信時刻を保持する。ルールは、同じＩＤのメッセージを前回受信してからの経過時間の上限と下限の情報であってもよい。また、基準となる経過時間の値と、基準となる経過時間の値からのＯＫと判定される範囲の幅を示す情報であってもよい。

【００９３】

調停検出部３７３は、周期判定部３７１からの問合せに応じて、そのメッセージを受信したときに、調停が発生していたか否かを検出する。図７Ａ、図７Ｂは、本実施の形態における調停発生時のメッセージの受信パターンを示す図である。図７Ａ、図７Ｂにおいて、三角の記号は、１つのメッセージを示し、横軸は時間を示しており、Ｔ１、Ｔ２はメッセージを受信する予定の時刻を示している。αは、ルール判定情報保持部３７２から取得したルールに対する判定がＯＫとなる範囲の幅を示している。

【００９４】

図７Ａ、図７Ｂにおいて、例えば、時刻（Ｔ１－α）は、周期判定部３７１が時刻Ｔ１においてＯＫと判定する下限値であり、時刻（Ｔ１＋α）は、周期判定部３７１が時刻Ｔ１においてＯＫと判定する上限値である。

【００９５】

また、メッセージＭ１、メッセージＭ３は、周期判定部３７１が時刻Ｔ１に受信すると予想していたメッセージであり、メッセージＭ２、メッセージＭ４は、調停が開始されたメッセージである。調停検出部３７３は、メッセージＭ２又はメッセージＭ４の受信時刻を、調停の開始時刻として、周期判定部３７１へ通知する。

【００９６】

調停検出部３７３は、予め決められた時間間隔以下でメッセージを受信した際に、調停が発生していたと判定する。例えば、図７Ａでは、メッセージＭ２からメッセージＭ１までメッセージが連続して送信されているため、メッセージＭ２からメッセージＭ１まで調停が発生していたと判定する。図７Ｂでは、メッセージＭ４と、メッセージＭ４の前の時刻Ｔ１に受信したメッセージＭ５の時間間隔が広いため、メッセージＭ４から調停が発生したと判定する。

【００９７】

図６において、調停検出部３７３は、周期判定部３７１からメッセージの受信時刻を受け取り、受信メッセージ情報保持部３７４に格納されている、前回メッセージの受信時刻を取得し、調停が発生したか否かを判定する。調停検出部３７３は、調停が発生していると判定した場合、受信メッセージ情報保持部３７４から調停が発生しているか否かを示す情報である調停発生状態情報を取得する。取得した調停発生状態情報が、調停が発生していないことを示す場合、調停検出部３７３は、調停発生開始時刻としてメッセージの受信

時刻を受信メッセージ情報保持部３７４で保持する。また、調停検出部３７３は、前回のメッセージの受信時刻として、今回のメッセージの受信時刻を受信メッセージ情報保持部３７４で保持し、調停発生状態情報を受信メッセージ情報保持部３７４で保持する。

【００９８】

また、調停検出部３７３は、周期判定部３７１から調停が発生しているかどうかの問い合わせがあった場合に、メッセージの受信時刻から、調停が発生しているかどうかを判定する。そして、調停が発生していた場合には、受信メッセージ情報保持部３７４から調停発生開始時刻を取得し、調停が発生している判定結果と一緒に、周期判定部３７１へ通知する。一方、調停検出部３７３は、調停が発生していなかった場合には、調停が発生していない旨を示す判定結果のみを通知する。

【００９９】

なお、調停検出部３７３は、調停が発生していなかった場合には、調停が発生していない旨を示す判定結果のみを通知するとしたが、これに限定するものではない。例えば、調停検出部３７３は、判定結果と一緒に調停発生開始時刻を示す値を通知してもよいし、前回の調停発生時の調停発生開始時刻を通知してもよい。

【０１００】

受信メッセージ情報保持部３７４は、調停検出部３７３が使用する前回のメッセージの受信時刻と、調停発生状態情報、調停発生開始時刻を保持する。

【０１０１】

なお、不正検知処理機能群３７０は、周期判定を行う機能群として説明したが、これに限定されない。図８は、本実施の形態における不正検知処理機能群３７０の別の一例を示す図であり、不正検知処理機能群３７０の変形例を示している。図８において、不正検知処理機能群３７０ａは、６種類の判定機能を含んでいる。具体的には、判定機能として、メッセージのＩＤフィールドをチェックする機能であるＩＤ判定機能、メッセージのデータ長をチェックする機能であるデータ長判定機能、メッセージが送信される周期（時間間隔）をチェックする機能である送信周期判定機能、メッセージが送信される頻度をチェックする機能である送信頻度判定機能、メッセージのデータフィールドの値（データ値）をチェックする機能であるデータ値判定機能を含み、さらに、これらの判定機能の判定結果、送信周期、頻度、データ値、又はデータ値の変化量などに基づいて車両の状態を認識し、車両状態をチェックする機能である車両状態判定機能を含む。さらに不正検知処理機能群３７０ａは、受信したメッセージが異常なメッセージであるか否かを、これらの判定機能による判定結果から総合的に判定する総合判定機能を含む。総合判定機能の結果が、不正検知処理機能群３７０ａによる不正の検知の結果となる。

【０１０２】

なお、図６における不正検知処理機能群３７０の周期判定部３７１と、ルール判定情報保持部３７２と、調停検出部３７３と、受信メッセージ情報保持部３７４とは、図８における不正検知処理機能群３７０ａの、送信周期判定機能に組み込まれていてもよい。

【０１０３】

なお、これらの構成は機能を示す構成であり、ゲートウェイ３００において記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを格納、若しくは入出力部を介してデータの送受信を実行することによって実現される。又は、これらの構成は、上記の組み合わせで実現されてもよい。

【０１０４】

［１．７　ＥＣＵの構成］

図９は、本実施の形態における車載ネットワークシステム１０に含まれるＥＣＵ１００の一例を示すブロック図である。図９において、ＥＣＵ１００は、フレーム送受信部１１０と、フレーム解釈部１２０と、受信ＩＤ判定部１３０と、受信ＩＤリスト保持部１４０と、フレーム処理部１５０と、データ取得部１７０と、フレーム生成部１８０とを備える。

【０１０５】

なお、これらの構成は機能を示す構成であり、ＥＣＵ１００は、例えばプロセッサで実

現される処理部、半導体メモリ等で実現される記憶部、入出力ポートで実現される入出力部等を備える情報処理装置として提供される。

【０１０６】

上記の機能を示す構成は、記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを保持し、若しくは入出力部を介してデータの送受信を実行することで実現される。又は、これらの構成は、上記の組み合わせで実現されてもよい。

【０１０７】

フレーム送受信部１１０は、バス２００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。

【０１０８】

より具体的には、フレーム送受信部１１０は、バス２００に送出されたメッセージを１ｂｉｔずつ読み出し、読み出したメッセージをフレーム解釈部１２０に転送する。

【０１０９】

また、フレーム送受信部１１０は、フレーム生成部１８０より通知を受けたメッセージをバス２００に送出する。

【０１１０】

フレーム解釈部１２０は、フレーム送受信部１１０よりメッセージの値を受け取り、ＣＡＮプロトコルにおける各フィールドにマッピングするようにしてメッセージの解釈を行う。フレーム解釈部１２０は、ＩＤフィールドと解釈した一連の値を、受信ＩＤ判定部１３０へ転送する。

【０１１１】

フレーム解釈部１２０はさらに、受信ＩＤ判定部１３０から通知される判定結果に応じて、メッセージのＩＤフィールドの値及びＩＤフィールド以降に現れるデータフィールドをフレーム処理部１５０へ転送するか、メッセージの受信を中止するかを決定する。

【０１１２】

また、フレーム解釈部１２０は、受信したメッセージが、ＣＡＮプロトコルに則っていないメッセージであると判断した場合は、エラーフレームを送信するようにフレーム生成部１８０へ要求する。

【０１１３】

また、フレーム解釈部１２０は、他のノードが送信したエラーフレームを受信したと判断した場合、読取中のメッセージを破棄する。

【０１１４】

受信ＩＤ判定部１３０は、フレーム解釈部１２０からＩＤフィールドの値を受け取る。そして、受信ＩＤリスト保持部１４０が保持しているメッセージＩＤのリストに従い、読み出したメッセージを受信するか否かの判定を行う。受信ＩＤ判定部１３０は、この判定の結果をフレーム解釈部１２０へ通知する。

【０１１５】

受信ＩＤリスト保持部１４０は、ＥＣＵ１００が受信する受信ＩＤリストを保持する。受信ＩＤリストは、図４と同様の形式であるため、ここではその説明を省略する。

【０１１６】

フレーム処理部１５０は、受信したメッセージのデータに応じた処理を行う。処理の内容は、ＥＣＵ１００ごとに異なる。

【０１１７】

例えば、ＥＣＵ１００ａでは、自動車の時速が３０ｋｍを超えているときに、ドアが開いていることを示すメッセージを受信すると、アラーム音を鳴らすための処理を実行する。ＥＣＵ１００ｃは、ブレーキがかかっていないことを示すメッセージを受信しているときにドアが開くと、アラーム音を鳴らすための処理を実行する。

【０１１８】

これらの処理は、説明のために一例として挙げているだけであり、ＥＣＵ１００は上記以外の処理を実行してもよい。このような処理を実行するために送出するフレームを、フ

レーム処理部１５０はフレーム生成部１８０に生成させる。
【０１１９】
データ取得部１７０は、ＥＣＵ１００に接続されている機器の状態を示すデータ又はセンサによる計測値等を示す出力データを取得し、フレーム生成部１８０に転送する。
【０１２０】
フレーム生成部１８０は、フレーム解釈部１２０からのエラーフレーム送信の要求に従い、エラーフレームを構成してフレーム送受信部１１０へ送る。
【０１２１】
またフレーム生成部１８０は、データ取得部１７０より受け取ったデータの値に対して予め定められたメッセージＩＤを付けてメッセージフレームを構成し、フレーム送受信部１１０へ送る。
【０１２２】
［１．８　不正検知処理］
図１０は、本実施の形態における不正検知処理の一例を示すフローチャートである。
【０１２３】
まず、不正検知処理機能群３７０の周期判定部３７１は、フレーム処理部３５０からメッセージを受け取る（ステップＳ１００１）。
【０１２４】
周期判定部３７１では、受け取ったメッセージが、同じＩＤを持つメッセージに対して、メッセージを受信した周期（経過時間）が正常と判定できる範囲内に収まっているかどうかを判定する（ステップＳ１００２）。
【０１２５】
周期判定部３７１は、受信したメッセージが正常と判定できる範囲内に収まっていない場合（ステップＳ１００３でＹｅｓの場合）、ステップＳ１００４へ進む。周期判定部３７１は、受信したメッセージが正常と判定できる範囲内に収まっている場合（ステップＳ１００３でＮｏの場合）、ステップＳ１００７へ進む。
【０１２６】
ステップＳ１００３で周期判定部３７１が受信したメッセージが正常と判定できる範囲に収まっていないと判定した場合（ステップＳ１００３でＹｅｓの場合）、調停検出部３７３は、メッセージ受信時に調停が発生していたか否かの検出を行う（ステップＳ１００４）。
【０１２７】
調停検出部３７３は、メッセージ受信時に調停が発生していた場合（ステップＳ１００５でＹｅｓの場合）、ステップＳ１００７へ進む。調停検出部３７３は、メッセージ受信時に調停が発生していなかった場合（ステップＳ１００５でＮｏの場合）、ステップＳ１００６へ進む。
【０１２８】
ステップＳ１００５で、調停検出部３７３において調停が発生していると検出した場合（ステップＳ１００５でＮｏの場合）、周期判定部３７１は、受信したメッセージが正常なメッセージではない、すなわち、異常なメッセージであると判定する（ステップＳ１００６）。その後、不正検知処理機能群３７０での不正検知処理を終了する。
【０１２９】
ステップＳ１００３で、周期判定部３７１が受信したメッセージが正常と判定できる範囲内に収まっていると判定した場合（ステップＳ１００３でＮｏの場合）又は、ステップＳ１００５で、調停検出部３７３がメッセージ受信時に調停が発生したと検出した場合（ステップＳ１００５でＹｅｓの場合）、周期判定部３７１は、受信したメッセージが正常なメッセージであると判定する（ステップＳ１００７）。その後、不正検知処理機能群３７０での不正検知処理を終了する。
【０１３０】
［１．９　転送処理］

図１１は、本実施の形態における転送処理の一例を示すフローチャートである。ゲートウェイ３００が行う転送処理は、転送の方向によらず実質的に共通であるため、ゲートウェイ３００がバス２００ａから受信したメッセージをバス２００ｂへ転送する場合を例に説明する。

【０１３１】

まず、フレーム送受信部３１０は、バス２００ａからメッセージを読み出す（ステップＳ１１０１）。フレーム送受信部３１０は、読み出したメッセージの各フィールドのデータをフレーム解釈部３２０へ通知する。

【０１３２】

次に、フレーム解釈部３２０は、受信ＩＤ判定部３３０と連携して、読み出したメッセージのＩＤフィールドの値（メッセージＩＤ）から、受信して処理する対象のメッセージであるか否かを判定する（ステップＳ１１０２）。フレーム解釈部３２０が処理する対象のメッセージではないと判定した場合（ステップＳ１１０２でＮｏの場合）、当該メッセージの転送は行われない。

【０１３３】

フレーム解釈部３２０は、ステップＳ１１０２で、受信して処理する対象のメッセージであると判断した場合には（ステップＳ１１０２でＹｅｓの場合）、フレーム処理部３５０へメッセージ内の各フィールドの値を転送する。その後、フレーム処理部３５０は、転送ルール保持部３６０に保持される転送ルールに従って、転送先のバスを決定する（ステップＳ１１０３）。

【０１３４】

フレーム処理部３５０は、フレーム解釈部３２０から受け取ったメッセージ内の各フィールドの値を不正検知処理機能群３７０へ通知し、異常なメッセージであるか否かの判定を要求する。不正検知処理機能群３７０は、通知されたメッセージの各フィールドの値から、通知されたメッセージが異常なメッセージであるか否かを判定し、その判定の結果をフレーム処理部３５０へ通知する（ステップＳ１１０４）。

【０１３５】

ステップＳ１１０４で不正検知処理機能群３７０が、メッセージは異常なメッセージであると判定した場合（ステップＳ１１０５でＹｅｓの場合）、そのメッセージの転送は行われない。

【０１３６】

ステップＳ１１０４で不正検知処理機能群３７０が、メッセージは異常なメッセージではなく正常なメッセージであると判定した場合（ステップＳ１１０５でＮｏの場合）、フレーム処理部３５０は、そのメッセージをステップＳ１１０３で決定した転送先のバスに、転送するようフレーム生成部３８０へ要求する。

【０１３７】

フレーム生成部３８０は、フレーム処理部３５０からの要求を受けて、指定された転送先が受信するようメッセージを生成し、このメッセージをフレーム送受信部３１０に送出させる（ステップＳ１１０６）。

【０１３８】

なお、上記の例では、受信したメッセージの転送先の決定（ステップＳ１１０３）の後にこのメッセージが異常なメッセージであるかの判定（ステップＳ１１０４）がなされているが、これに限定されない。受信したメッセージが異常なメッセージであるかの判定の後にこのメッセージの転送先の決定がなされてもよい。また、受信したメッセージの転送先の決定と異常なメッセージであるかの判定が並行して行われてもよい。

【０１３９】

［１．１０　効果］

本実施の形態では、不正検知処理機能群３７０は、車載ネットワークシステムのネットワークを流れるメッセージを監視し、メッセージが所定の周期より遅れて受信された場合、調停によって遅れたのかどうかを判定することで、異常なメッセージであるか否かを判

定する。これにより従来の不正検知の技術で用いられていたような、例えば所定の周期より短い時間間隔でメッセージを受信したときに、不正が発生したと判断する技術では、正常なメッセージであるか異常なメッセージであるかの判定が困難であったメッセージに関しても、より高い精度で異常なメッセージであるか否かを判定することが可能になる。その結果、車載ネットワークシステムの安全性が高められる。

【０１４０】

（実施の形態２）

［２．概要］

実施の形態２では、実施の形態１の不正検知処理機能群３７０の代わりに、不正検知処理機能群３７０ｂが用いられる。不正検知処理機能群３７０ｂにおいて周期判定部が、ルール判定情報保持部へ通知するメッセージの受信時刻の決定に、調停検出部３７３の検出結果を利用する。このような不正検知処理機能群３７０ｂは、実施の形態１で説明した図３における不正検知処理機能群３７０に代えてゲートウェイ３００に含まれ得る。

【０１４１】

なお、この不正検知処理機能群３７０ｂを含むゲートウェイ、及びこのゲートウェイを備える車載ネットワークシステムは実施の形態１と基本的に共通のため、その構成についての説明を省略する。

【０１４２】

［２．１　不正検知処理機能群の構成］

図１２は、本実施の形態における不正検知処理機能群３７０ｂを示すブロック図である。図１２において、図６と同じ構成要素については同じ符号を用い、説明を省略する。また、同じ構成の一部については、図示を省略する。以下、不正検知処理機能群３７０ｂについて、不正検知処理機能群３７０との差異点を中心に説明する。

【０１４３】

不正検知処理機能群３７０ｂは、実施の形態１における不正検知処理機能群３７０の構成に加え、周期起点決定部３７５と、送信タイプ判定部３７６を含む。また、不正検知処理機能群３７０ｂは、周期判定部３７１に代えて周期判定部３７１ｂを含む。

【０１４４】

これらの構成は機能を示す構成であり、ゲートウェイ３００において記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを保持する。若しくは、記憶部へ所定のデータを記録することの代わりに、入出力部を介してデータの送受信を実行することで実現される。又は、これらの構成は上記の組み合わせで実現される。

【０１４５】

周期起点決定部３７５は、周期判定部３７１ｂがメッセージを受信した周期（経過時間）が正常と判断できる範囲内に収まっているかどうかを判定するときに、経過時間を算出するための起点として利用する「前回受信時刻」の値を決定する。周期起点決定部３７５は、周期判定部３７１ｂからの問合せを受け、経過時間を算出するための起点として利用する「前回受信時刻」の値を決定し、周期判定部３７１ｂへ通知する。

【０１４６】

周期起点決定部３７５は、受信したメッセージのＩＤを送信タイプ判定部３７６へ通知し、送信タイプの判定を依頼する。周期起点決定部３７５は、送信タイプ判定部３７６が判定した結果に応じて、「前回受信時刻」の値を決定する。

【０１４７】

例えば、メッセージの受信時刻（今回受信時刻）を「前回受信時刻」の値とする送信タイプ（Ａタイプ）と、メッセージを受信する予定だった時刻（受信予定時刻）、つまり、前回受信時刻に、ルールとして保持している基準となる経過時間を足した値を「前回受信時刻」の値とする送信タイプ（Ｂタイプ）とがあるとする。

【０１４８】

この時、周期起点決定部３７５は、送信タイプ判定部３７６が送信タイプをＡタイプと判定したときは、今回受信時刻を「前回受信時刻」として周期判定部３７１ｂへ通知する

。また、周期起点決定部３７５は、送信タイプ判定部３７６が送信タイプをＢタイプと判定したときには、受信予定時刻を「前回受信時刻」として周期判定部３７１ｂへ通知する。
【０１４９】
　また、周期起点決定部３７５は、周期判定部３７１ｂから受信したメッセージと共に、そのメッセージを受信した際に調停が発生していたかどうかの情報も取得し、調停が発生していたかどうかで、起点となる時刻を決定してもよい。
【０１５０】
　例えば、そのメッセージを受信した際に調停が発生していなかった場合には、周期起点決定部３７５は常に今回受信時刻を「前回受信時刻」として周期判定部３７１ｂへ通知する。そして、そのメッセージを受信した際に調停が発生していた場合にのみ、周期起点決定部３７５は送信タイプ判定部３７６へ送信タイプの判定を依頼し、得られた送信タイプによって起点となる時刻を上述した方法等で決定してもよい。
【０１５１】
　送信タイプ判定部３７６は、周期起点決定部３７５からの問合せに応じて、受信したメッセージのＩＤから、送信タイプを判定し、周期起点決定部３７５へ通知する。
【０１５２】
　送信タイプの判定は、例えば、送信タイプ判定部３７６が、ＩＤとそのＩＤの送信タイプの組が記載されたテーブルを事前に保持しておき、周期起点決定部３７５からの問合せに応じて、事前に保持しておいたテーブルから、受信したメッセージのＩＤに対応した送信タイプを判定する。
【０１５３】
　周期判定部３７１ｂは、実施の形態１における周期判定部３７１と同様の処理を行い、受信したメッセージが最終的に正常なメッセージであると判定した際に、ルール判定情報保持部３７２に保持を依頼する前回受信時刻の決定を、周期起点決定部３７５へ依頼する。つまり、周期判定部３７１ｂは、周期起点決定部３７５が通知してきた前回受信時刻を、ルール判定情報保持部３７２へ通知し、保持を依頼する。
【０１５４】
　なお、周期起点決定部３７５は、メッセージを受信した際に調停が発生していたかどうかの情報を、周期判定部３７１ｂから取得するとしたが、これに限定されない。例えば、周期起点決定部３７５が直接、調停検出部３７３からメッセージを受信した際に調停が発生していたかどうかの情報を取得してもよい。
【０１５５】
［２．２　不正検知処理］
　図１３は、本実施の形態における不正検知処理の一例を示すフローチャートである。図１０と共通のステップについては、図１３において同じ参照符号を用いて示し、一部説明を省略する。
【０１５６】
　まず、不正検知処理機能群３７０ｂの周期判定部３７１ｂは、フレーム処理部３５０からメッセージを受け取る（ステップＳ１００１）。
【０１５７】
　ステップＳ１００２からステップＳ１００７までの処理は、図１０と共通であるため、説明を省略する。
【０１５８】
　周期判定部３７１は、ステップＳ１００７で受信したメッセージが正常なメッセージであると判定すると、周期起点決定部３７５へ、前回受信時刻の決定を依頼する。周期判定部３７１ｂは、周期起点決定部３７５が通知してきた前回受信時刻を、ルール判定情報保持部３７２へ通知し、ルール判定情報保持部３７２が保持する前回受信時刻を更新する（Ｓ１００８）。その後、不正検知処理機能群３７０ｂでの不正検知処理は終了する。
【０１５９】
［２．３　効果］

本実施の形態では、不正検知処理機能群３７０ｂでの不正検知処理において、周期判定部３７１がメッセージを受信した周期（経過時間）が正常と判断できる範囲内に収まっているかどうかを判定する際に利用する「前回受信時刻」の値を、送信タイプ又は、調停が発生していたかどうかにより柔軟に決定する。これにより、従来起こりえた、ＩＤごとに送信方法が異なる場合又は、調停が発生した際の送信タイミングのズレにより周期検知が正しくできない場合でも、より高い精度で異常なメッセージであるか否かの判定をすることができる。その結果、車載ネットワークシステムの安全性が高められる。

【０１６０】

［３．その他の変形例］

本開示は、上記で説明した各実施の形態に限定されない。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実施の形態に施したもの、及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、本開示の範囲内に含まれる。例えば以下のような変形例も本開示に含まれる。

【０１６１】

（１）上記の実施の形態２では、不正検知処理機能群３７０ｂは、周期判定部３７１ｂと、ルール判定情報保持部３７２と、調停検出部３７３と、受信メッセージ情報保持部３７４と、周期起点決定部３７５と、送信タイプ判定部３７６とを備えると説明したが、これに限定されない。

【０１６２】

図１４は、変形例における不正検知処理機能群の一例を示す図である。図１４に示すように、不正検知処理機能群３７０ｃは、周期判定部３７１ｃと、ルール判定情報保持部３７２と、調停検出部３７３と、受信メッセージ情報保持部３７４と、周期起点決定部３７５ｃと、送信タイプ判定部３７６ｃと、周期タイプ学習部３７７と、周期タイプ保持部３７８とを備える。

【０１６３】

周期タイプ学習部３７７は、周期判定部３７１ｃから受信した情報を元に、ＩＤごとの周期タイプを判定する。判定方法としては、例えば、周期タイプ学習部３７７は、ＩＤごとに受信したメッセージの受信時刻を記録（蓄積）していき、一定数の受信時刻が蓄積できたタイミングで、ＩＤごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求める。

【０１６４】

周期タイプ学習部３７７は、その受信時刻の差が、ＩＤごとに決められている経過時間の基準値と比較したときに、（１）基準値と同程度か、（２）基準値より短いか、（３）基準値より長いかを判定する。

【０１６５】

ここで、基準値と同程度か否かの判定には、予め決められたしきい値（上限用と下限用）を用いる。周期タイプ学習部３７７は、基準値から下限用のしきい値を引いた値から、基準値に上限用のしきい値を足した値の間に、経過時間が含まれる場合に、「基準値と同程度」と判定し、経過時間が、基準値から下限用のしきい値を引いた値より小さい場合に、「基準値より短い」と判定し、経過時間が、基準値に上限用のしきい値を足した値より大きい場合に、「基準値より長い」と判定する。

【０１６６】

周期タイプ学習部３７７は、判定した結果（１．基準値と同程度か、２．基準値より短いか、３．基準値より長いか）の数をＩＤと一緒に周期タイプ保持部３７８へ通知する。

【０１６７】

周期タイプ保持部３７８は、周期タイプ学習部３７７から通知された周期タイプの判定結果を保持し、送信タイプ判定部３７６からの問合せに応じて、周期タイプを通知する。周期タイプ保持部３７８は、周期タイプ学習部３７７からの通知を受けた際に、既に通知されたＩＤと同じＩＤの判定結果を保持していた場合、新たに通知された判定結果で上書きしてもよいし、既に保持していた値に足した値で更新してもよい。

【０１６８】
周期判定部３７１ｃは、受信したメッセージのうち、最終的にＯＫと判定したメッセージ関する情報を、周期タイプ学習部３７７へ通知する。
【０１６９】
送信タイプ判定部３７６ｃは、周期起点決定部３７５ｃから送信タイプの判定を依頼された際に、依頼されたＩＤに関連する受信タイミングごとの経過時間と経過時間の基準値とを比較した結果を周期タイプ保持部３７８より取得する。送信タイプ判定部３７６は、（２）基準値より短いと判定した数が、（３）基準値より長いと判定した数より少なかった場合、送信タイプがＡタイプであると判定し、（２）基準値より短いと判定した数と、（３）基準値より長いと判定した数とが、ほぼ同じ数であった場合に、送信タイプがＢタイプであると判定し、それ以外の場合は、送信タイプが判定できないと判定する。（２）基準値より短いと判定した数が（３）基準値より長いと判定した数より少ないとの判定は、判定した数そのものが予め決められた数以上の差があるかどうかで判定してもよいし、判定した数の比が予め決められた値より小さいかどうかで判定してもよい。（１）基準値と同じぐらいか、（２）基準値より短いか、（３）基準値より長いかのそれぞれの割合を求め、その割合が予め決められた値以上の差があるかどうかで判定してもよい。（２）基準値より短いと判定した数と、（３）基準値より長いと判定した数とが、ほぼ同じ数との判定は、判定した数そのものが予め決められた数以内の差に収まっているかどうか判定してもよいし、判定した数の比が予め決められた値より大きい、または予め決められた範囲に収まっているかどうかで判定してもよい。（１）基準値と同じぐらいか、（２）基準値より短いか、（３）基準値より長いかのそれぞれの割合を求め、その割合が予め決められた値以内の差に収まっているかどうかで判定してもよい。
【０１７０】
送信タイプ判定部３７６ｃは、周期起点決定部３７５ｃからの要求に応じて、判定した結果を通知する。送信タイプ判定部３７６ｃは、送信タイプが判定できなかった場合には、予め決められたタイプを周期起点決定部３７５ｃへ通知する。
【０１７１】
なお、周期タイプ学習部３７７は、ＩＤごとに受信したメッセージの受信時刻を記録していき、一定数の受信時刻が蓄積できたタイミングで、ＩＤごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求めるとしたが、これに限定されるものではない。
【０１７２】
例えば、周期タイプ学習部３７７は、車両が工場から出荷される前に、周期タイプを学習する時間を設け、その間に受信したメッセージの受信時刻を蓄積し、ＩＤごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求めてもよい。
【０１７３】
さらに、周期タイプ学習部３７７は、工場出荷後から受信時刻を蓄積し、一定数、または、一定時間、受信時刻を蓄積したタイミングで、ＩＤごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求めてもよい。
【０１７４】
また、周期タイプ学習部３７７は、車両外部の機器からメッセージの受信時刻を蓄積するように指示を受け、受信時刻を蓄積し、外部の機器から蓄積停止の指示を受けるまで一定数、または、一定時間、受信時刻を蓄積したタイミングで、ＩＤごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求めてもよい。
【０１７５】
また、周期タイプ学習部３７７は、メッセージを受信するたびに受信時刻を記録し、一定数、または、一定時間の受信時刻が蓄積できた後は、メッセージを受信するごとに、受信時刻の一つ前の受信時刻との差（経過時間）を求めてもよい。
【０１７６】
なお、周期タイプ学習部３７７は、受信時刻を記録し、あるタイミングでＩＤごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求めるとしたが、これに限定

されるものではない。例えば、周期タイプ学習部３７７は、メッセージを受信するごとに、前のメッセージの受信時刻との差（経過時間）を求め、経過時間を記録（蓄積）し、最新の受信時刻を記録してもよい。

【０１７７】

なお、基準値と同じぐらいかどうかの判定には、予め決められたしきい値（上限用と下限用）を用いるとしたが、これに限定されるものではない。例えば、１つのしきい値を用いて、下限も上限も同じ値を用いてもよいし、基準値としきい値という組み合わせではなく、下限値と上限値の２つの値を用いてもよい。

【０１７８】

なお、周期タイプ学習部３７７は、判定した結果（（１）基準値と同じぐらいか、（２）基準値より短いか、（３）基準値より長いか）の数を周期タイプ保持部３７８へ通知するとしたが、これに限定されるものではない。例えば、割合を通知してもよいし、周期タイプ保持部３７８へ既に保持されている値があれば、その値に、今回の値を足した数を通知してもよい。

【０１７９】

これにより、送信タイプを事前に設定することなく、自動的に送信タイプを判定することが可能となる。更に、修理などでＥＣＵが交換された場合にも、自動的に送信タイプを判定することが可能となる。その結果、更なる不正検知精度の向上又は、処理コスト、製造コストを低減することが可能となる。

【０１８０】

（２）上記の実施の形態２では、不正検知処理機能群３７０ｂは、周期判定部３７１ｂと、ルール判定情報保持部３７２と、調停検出部３７３と、受信メッセージ情報保持部３７４と、周期起点決定部３７５と、送信タイプ判定部３７６とを備えると説明したが、これに限定されない。

【０１８１】

図１５は、変形例における不正検知処理機能群の一例を示す図である。図１５に示すように、不正検知処理機能群３７０ｄは、周期判定部３７１ｂと、ルール判定情報保持部３７２と、調停検出部３７３と、受信メッセージ情報保持部３７４と、周期起点決定部３７５ｄとを備える。

【０１８２】

周期起点決定部３７５ｄは、メッセージの受信時に調停が発生していたかどうかで、周期の起点を決定する。例えば、調停が発生していなかった場合には、周期起点決定部３７５ｄは今回受信時刻を「前回受信時刻」として周期判定部３７１ｂへ通知し、調停が発生していた場合には、周期起点決定部３７５ｄは受信予定時刻を「前回受信時刻」として周期判定部３７１ｂへ通知する。

【０１８３】

なお、周期起点決定部３７５ｄは、今回受信時刻を「前回受信時刻」とするか、受信予定時刻を「前回受信時刻」とするかを周期判定部３７１ｂへ通知するとしたが、これに限定されるものではない。

【０１８４】

例えば、周期起点決定部３７５ｄは、調停が発生した１回目は今回受信時刻を「前回受信時刻」として、その後、調停が連続して発生する度に、予め決められた時間又は予め決められた割合で、受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部３７１ｂへ通知してもよい。また、調停が発生した１回目から受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部３７１ｂへ通知してもよい。

【０１８５】

また、周期起点決定部３７５ｄは、それぞれのＩＤごとに事前に、どれだけ今回受信時刻から受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部３７１ｂへ通知するかを、例えば、歪度（Ｓｋｅｗｎｅｓｓ）又は尖度（Ｋｕｒｔｏｓｉｓ）などの統計的な数値を用いて算出しておき、その事前に算出しておいた値分、今回受信時刻から受信

予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部３７１ｂへ通知してもよい。
【０１８６】
　また、歪度又は尖度だけでなく、中央値又は平均値、最頻値などから求まる値又は、標準偏差などの値を使用して、どれだけ今回受信時刻から受信予定時刻へ近づけた時刻を「前回受信時刻」とするかを決定してもよい。この時、それぞれの値を個別に利用してもよいし、いくつかの値から計算した値を用いてもよい。また、周期タイプ学習部３７７により、これらを学習してもよい。
【０１８７】
　これにより、前回時刻を二者択一で決定するよりも、柔軟に決定することが出来るため、より検知精度を向上させることが出来る。
【０１８８】
　（３）上記各実施の形態では、ＥＣＵ１００は、フレーム送受信部１１０と、フレーム解釈部１２０と、受信ＩＤ判定部１３０と、受信ＩＤリスト保持部１４０と、フレーム処理部１５０と、データ取得部１７０と、フレーム生成部１８０とを備えると説明したが、本開示における車載ネットワークシステムが備えるＥＣＵ１００の構成はこれに限定されるものではない。
【０１８９】
　図１６は、変形例におけるＥＣＵの一例を示すブロック図である。図１６に示すＥＣＵ１００ｅは、さらに不正検知処理機能群３７０を備える。この場合、異常なメッセージであるか否かの判定を、フレーム処理部１５０が不正検知処理機能群３７０へ要求してもよいし、フレーム解釈部１２０が要求してもよい。
【０１９０】
　図１７は、変形例におけるＥＣＵの一例を示すブロック図である。図１７に示すＥＣＵ１００ｆは、フレーム送受信部１１０と、フレーム解釈部１２０と、フレーム生成部１８０とで構成される。この場合、フレーム解釈部１２０は、例えばＩＤによらず全てのメッセージを受信し、全てのメッセージについて不正検知処理機能群３７０へ異常なメッセージであるかどうかの判定を依頼してもよい。
【０１９１】
　また、ＥＣＵ１００ｆは、図１７の構成に加えて、受信ＩＤ判定部１３０と、受信ＩＤリスト保持部１４０とを備え、受信ＩＤリスト保持部が保持する受信ＩＤリストに記載されたメッセージＩＤを持つメッセージのみを受信し、そのメッセージに関して、不正検知処理機能群３７０へ異常なメッセージであるか否かの判定を依頼してもよい。なお、不正検知処理機能群３７０は、上述の３７０ａ～３７０ｄのいずれに代えられてもよい。
【０１９２】
　これにより、ゲートウェイだけでなく、ＥＣＵ１００でも、バスに送信されているメッセージが異常なメッセージであるか否かを判定できる。その結果、例えば車載ネットワークシステムにおける不正検知のための仕組の冗長性が向上し、より高度に安全が確保される。
【０１９３】
　図１８は、変形例におけるＥＣＵの一例を示すブロック図である。図１８に示すＥＣＵ１００ｇは、バス２００へ送信するデータを他の接続機器又は外部等から取得する送信データ取得部１７１を備えてもよい。ＥＣＵ１００ｇが備える不正検知処理機能群３７０ｅは、送信データ取得部１７１から受信したデータが異常なメッセージであるか否かについても判定し、異常なメッセージではないと判定した場合のみ、フレーム生成部１８０へメッセージの送信を依頼してもよい。なお、不正検知処理機能群３７０ｅの構成は、不正検知処理機能群３７０、３７０ａ、３７０ｂ、３７０ｃ、３７０ｄのいずれかの構成と共通であってもよい。
【０１９４】
　これにより、例えば、カーナビゲーションと一緒に利用されるＥＣＵ１００ｆが、乗っ取られたカーナビゲーションから異常なメッセージが送信されるような場合において、そ

のメッセージのネットワークへの拡散を抑制することができる。または、車外から送り込みが試みられる異常なメッセージの車載ネットワークシステム内部への侵入を抑制することができる。

【０１９５】

（４）上記各実施の形態では、不正の検知に応じたアクションとして、受信したメッセージを転送しない例を示したが、これに限定されない。例えば、上述の不正検知処理機能群を備えるゲートウェイ又はＥＣＵ１００は、メッセージの受信中に不正検知処理を行い、異常なメッセージであると判定した時点で、エラーフレームを送信することで、ネットワークから受信中のメッセージを無効化してもよい。

【０１９６】

これにより、異常なメッセージが見つかったバスに接続された他のＥＣＵ１００が異常なメッセージを受信することを防止することができる。同様のアクションは、転送しないメッセージに対しても適用できる。

【０１９７】

また、上述の不正検知処理機能群を備えるゲートウェイ３００又はＥＣＵ１００はさらに、不正の発生のユーザ若しくは外部のサーバ等への通知、不正の発生のログへの記録、又は車両のフェールセーフモードへの移行を実行してもよい。

【０１９８】

これにより、不正検知後の柔軟な対応が可能となる。また異常なメッセージと判定した複数のメッセージをデータの１以上の系列として扱い、各系列について、データの値又は受信間隔の集合を不正なラベルとして学習してもよい。

【０１９９】

（５）上記各実施の形態では、標準フォーマットのＩＤにおける例を示したが、拡張フォーマットのＩＤであってもよい。

【０２００】

（６）上記各実施の形態では、メッセージは平文で送信される例を示したが、暗号化されていてもよい。またメッセージにメッセージ認証コードを含んでいてもよい。

【０２０１】

（７）上記実施の形態では、正常モデルと、受信ログとを平文で保持している例を示したが、これらを暗号化して保持していてもよい。

【０２０２】

（８）上記の実施の形態では、ＣＡＮプロトコルに従って通信するネットワーク通信システムの例として車載ネットワークを示した。本開示に係る技術は、車載ネットワークでの利用に限定されるものではなく、ロボット、産業機器等のネットワークその他、車載ネットワーク以外のＣＡＮプロトコルに従って通信するネットワーク通信システムに利用してもよい。

【０２０３】

また、車載ネットワークシステム１０としてＣＡＮプロトコルを用いていたが、これに限るものではない。例えば、ＣＡＮ－ＦＤ（ＣＡＮ ｗｉｔｈ Ｆｌｅｘｉｂｌｅ Ｄａｔａ Ｒａｔｅ）、ＦｌｅｘＲａｙ、Ｅｔｈｅｒｎｅｔ、ＬＩＮ（Ｌｏｃａｌ Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｎｅｔｗｏｒｋ）、ＭＯＳＴ（Ｍｅｄｉａ Ｏｒｉｅｎｔｅｄ Ｓｙｓｔｅｍｓ Ｔｒａｎｓｐｏｒｔ）などを用いてもよい。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、組み合わせたネットワークであってもよい。

【０２０４】

（９）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（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ハードディスクユニット、ディスプレイユニット、キーボード、マウス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されて構成されたものである。

【０２０５】

（１０）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。

【０２０６】

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、一部又はすべてを含むように１チップ化されてもよい。

【０２０７】

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（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、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、専用回路又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）又は、ＬＳＩ内部の回路セルの接続又は設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

【０２０８】

さらには、半導体技術の進歩又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。

【０２０９】

（１１）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カードまたは前記モジュールは、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。

【０２１０】

（１２）本開示は、上記に示す方法であるとしてもよい。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。

【０２１１】

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。

【０２１２】

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。

【０２１３】

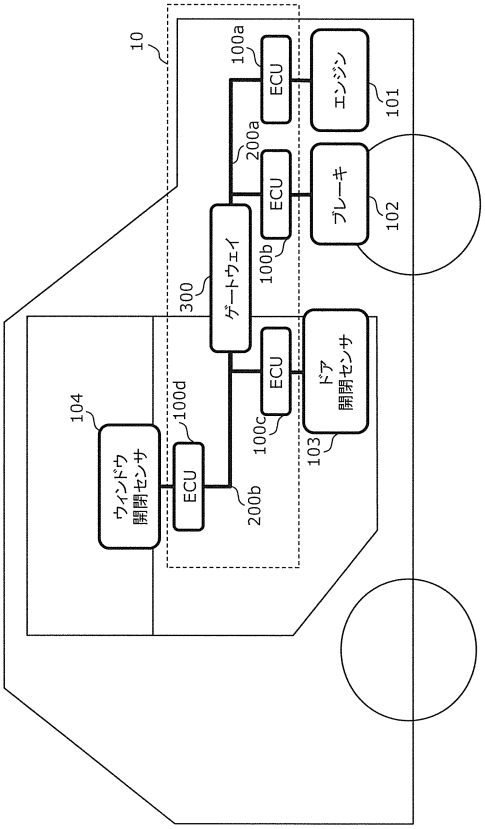
また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、上記コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムにしたがって動作するとしてもよい。

【０２１４】
　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。
【０２１５】
　（１３）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。
【０２１６】
　以上、一つ又は複数の態様に係る車載ネットワークにおける、異常なメッセージによる不正制御を目的とする不正通信検知の基準として用いられるメッセージの決定のための技術について実施の形態及びその変形例に基づいて説明した。これらの各実施の形態及びその変形例では、車載ネットワークシステムに接続されて通信するゲートウェイ若しくはＥＣＵ、又はこれらとサーバコンピュータとの組み合わせによって不正通信検知の基準として用いられるメッセージが決定される。このような不正通信検知を実行する、１個以上のプロセッサ及び記憶部を含むシステムを、本開示では不正通信検知基準決定システムと呼ぶ。したがって、不正通信検知基準決定システムは車載ネットワークシステムに接続される１台のゲートウェイのように１個の装置によって実現されるものも、このようなゲートウェイとＥＣＵとの組み合わせ、又はゲートウェイ若しくはＥＣＵと遠隔にあるサーバコンピュータとの組み合わせのように複数個の装置によって実現されるものも含む。
【０２１７】
　また、この技術は、上記各実施の形態又はその変形例において、各構成要素が実行する処理のステップの一部又は全部を含む方法として、又は不正通信検知基準決定システムのプロセッサに実行されて、不正通信検知基準決定システムがこの方法を実施させるためのプログラムとしても実現可能である。
【０２１８】
　また、上記実施の形態又はその変形例において、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】
【０２１９】
　本開示にかかる車載ネットワークシステム等に適用可能である。
【符号の説明】
【０２２０】
　１０　車載ネットワークシステム
　１００、１００ａ、１００ｂ、１００ｃ、１００ｄ、１００ｅ、１００ｆ、１００ｇ　ＥＣＵ
　１０１　エンジン
　１０２　ブレーキ
　１０３　ドア開閉センサ
　１０４　ウィンドウ開閉センサ
　１１０　フレーム送受信部
　１２０　フレーム解釈部
　１３０　受信ＩＤ判定部
　１４０　受信ＩＤリスト保持部
　１５０　フレーム処理部
　１７０　データ取得部
　１７１　送信データ取得部
　１８０、３８０　フレーム生成部
　２００、２００ａ、２００ｂ　バス
　３００　ゲートウェイ
　３１０　フレーム送受信部

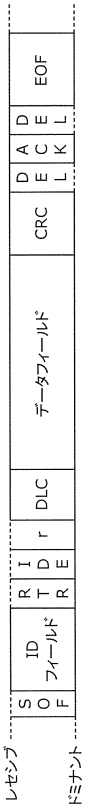
３２０　フレーム解釈部
３３０　受信ＩＤ判定部
３４０　受信ＩＤリスト保持部
３５０　フレーム処理部
３６０　転送ルール保持部
３７０、３７０ａ、３７０ｂ、３７０ｃ、３７０ｄ、３７０ｅ　不正検知処理機能群
３７１、３７１ｂ、３７１ｃ　周期判定部
３７２　ルール判定情報保持部
３７３　調停検出部
３７４　受信メッセージ情報保持部
３７５、３７５ｃ、３７５ｄ　周期起点決定部
３７６、３７６ｃ　送信タイプ判定部
３７７　周期タイプ学習部
３７８　周期タイプ保持部

【図面】

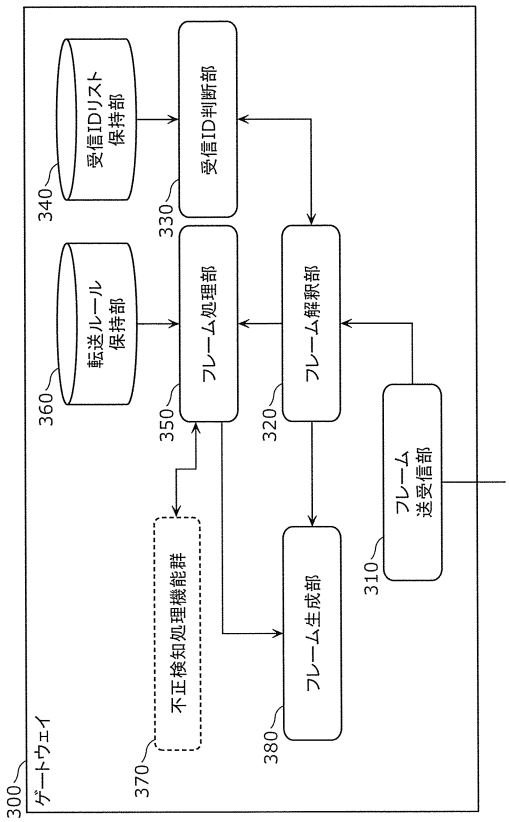
【図１】



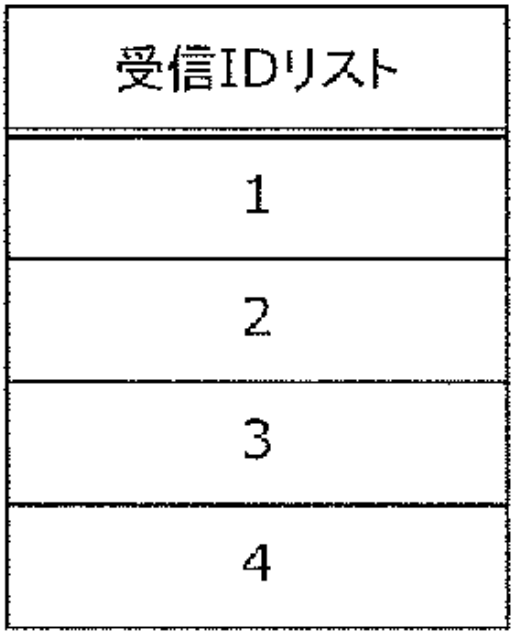
【図２】



【図３】



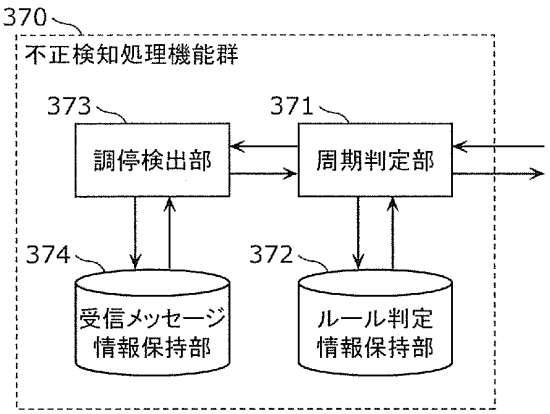
【図４】



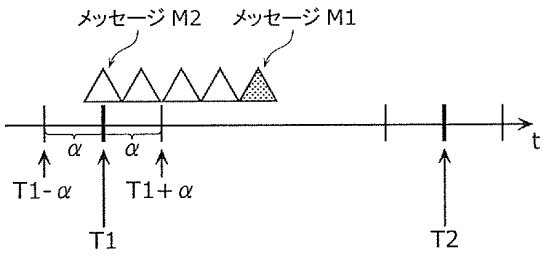
【図５】

転送元	転送先	ID
バス200a	バス200b	*
バス200b	バス200a	3

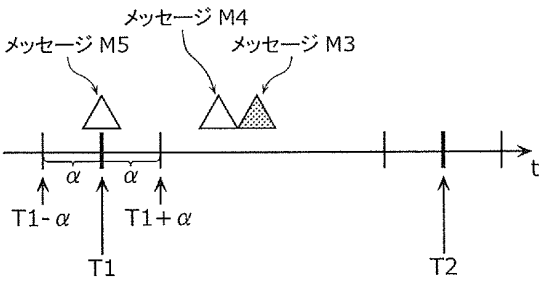
【図６】



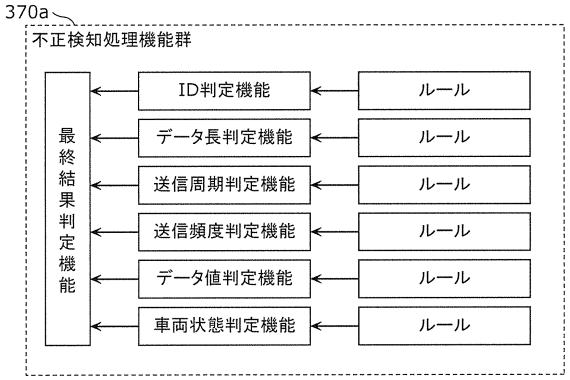
【図７Ａ】


メッセージ M2
メッセージ M1
α
α
T1-α
T1+α
T1
T2
t

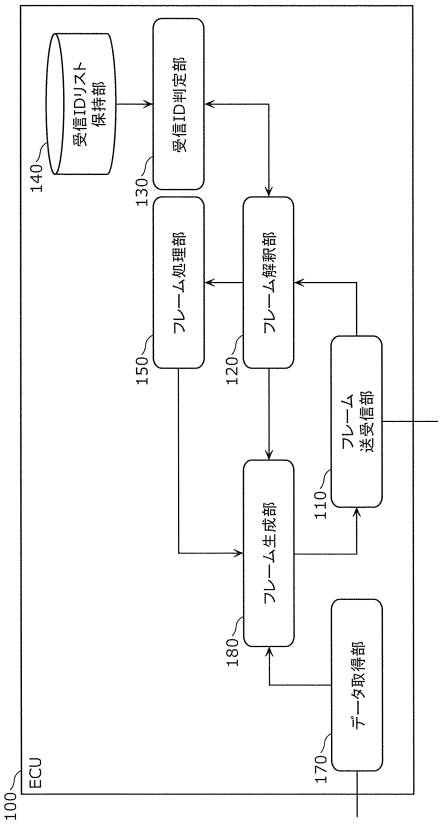
【図７Ｂ】


メッセージ M4
メッセージ M5
メッセージ M3
α
α
T1-α
T1+α
T1
T2
t

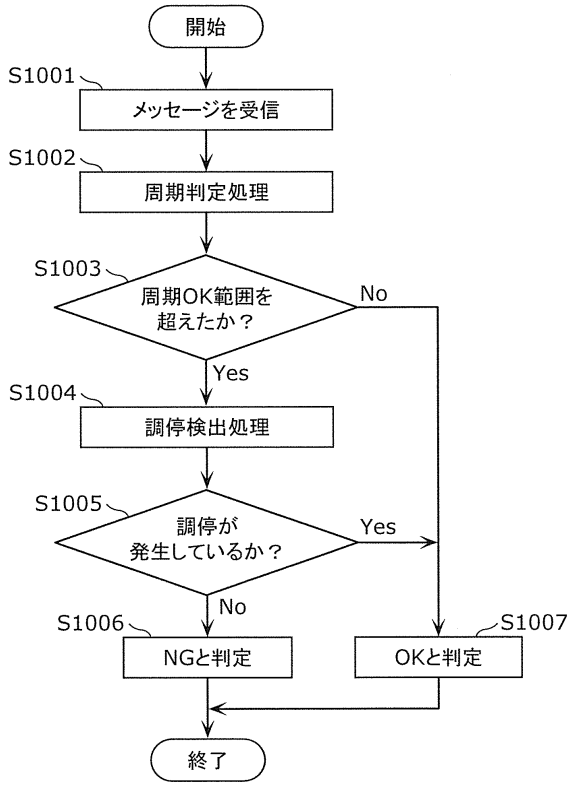
【図８】


370a
不正検知処理機能群
最終結果判定機能
ID判定機能
データ長判定機能
送信周期判定機能
送信頻度判定機能
データ値判定機能
車両状態判定機能
ルール
ルール
ルール
ルール
ルール
ルール

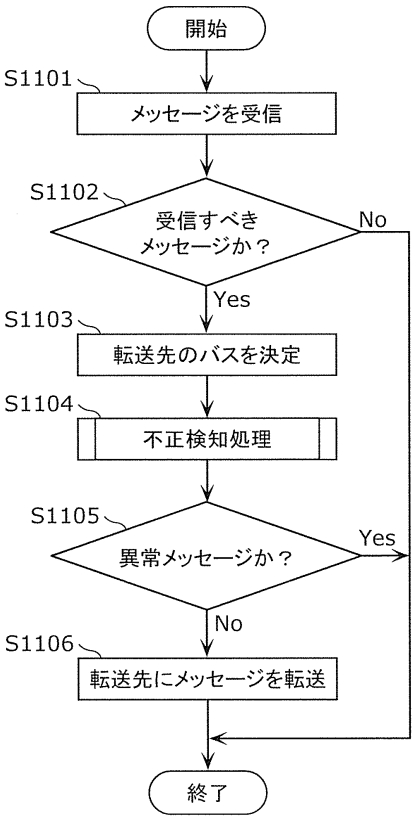
【図９】


ECU
100
受信IDリスト保持部
140
受信ID判定部
130
フレーム処理部
150
フレーム解釈部
120
フレーム送受信部
110
フレーム生成部
180
データ取得部
170

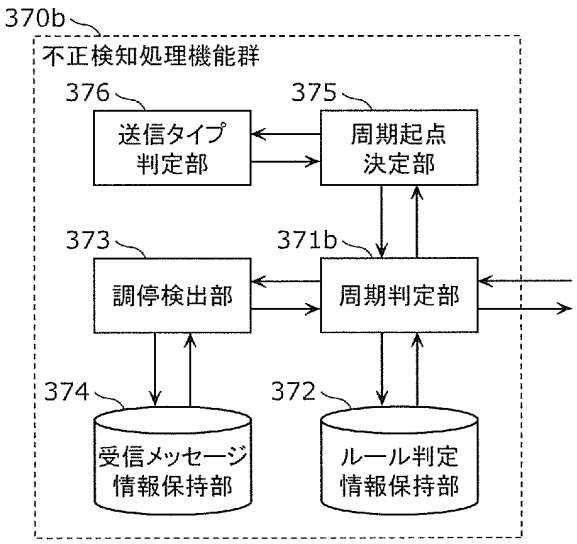
【図１０】



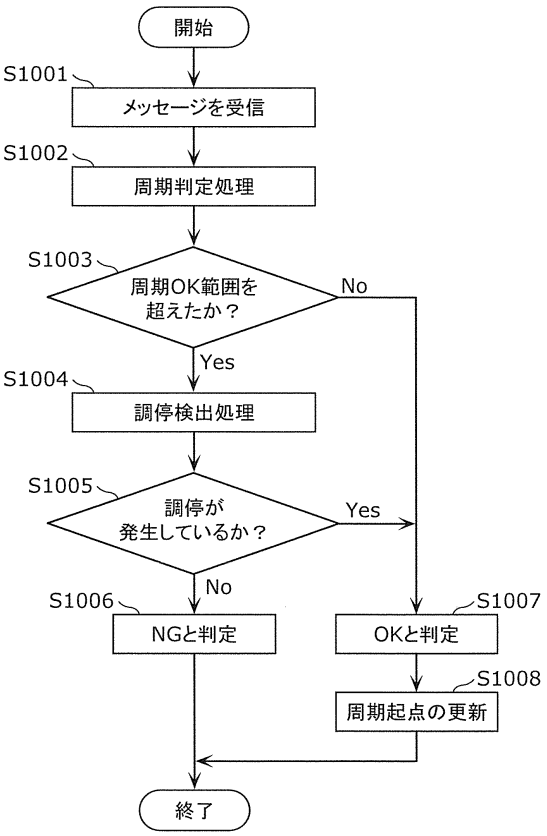
【図１１】



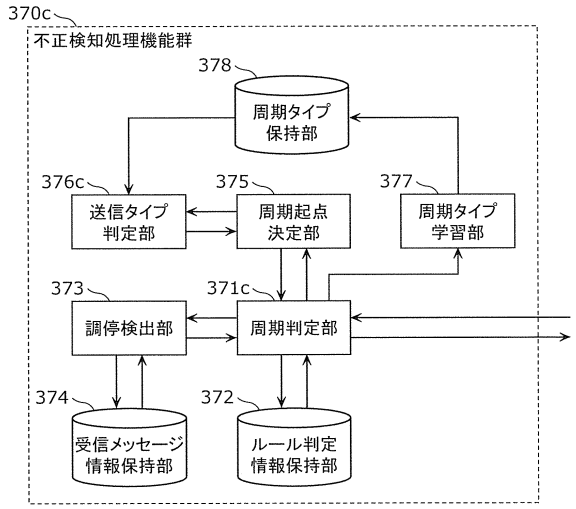
【図１２】



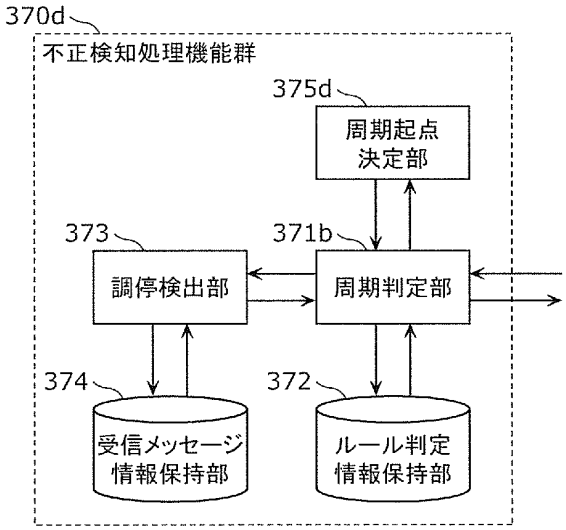
【図１３】



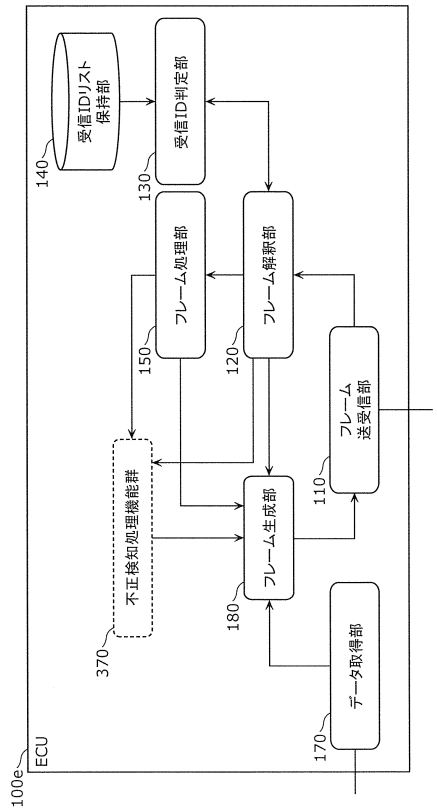
【図１４】



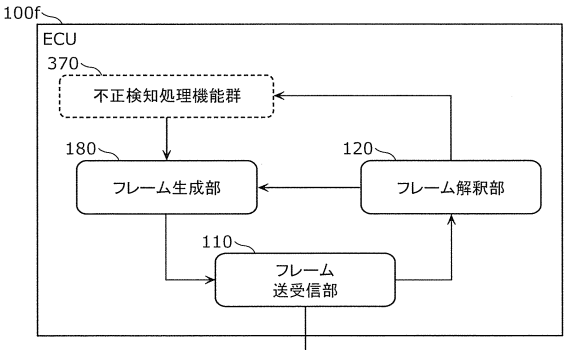
【図１５】



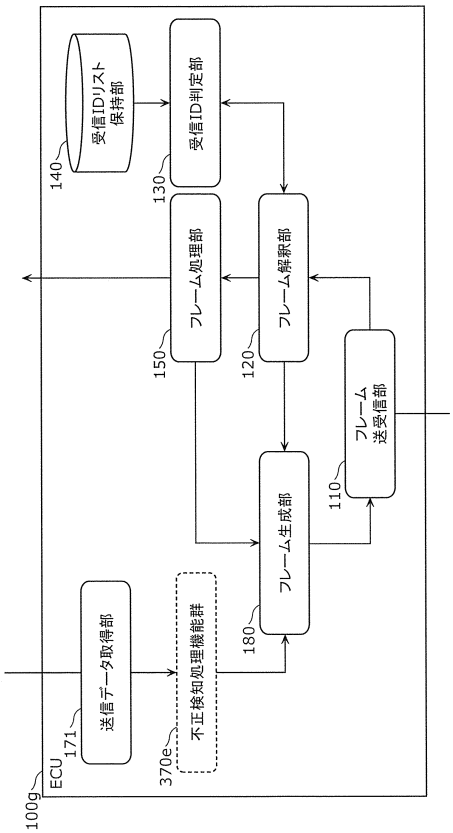
【図１６】



【図１７】



【図１８】


受信IDリスト保持部
140
受信ID判定部
130
フレーム処理部
150
フレーム解釈部
120
フレーム送受信部
110
フレーム生成部
180
送信データ取得部
171
不正検知処理機能群
370e
ECU
100g

フロントページの続き

(72)発明者　前田 学
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　岸川 剛
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　国宗 大介
京都府長岡京市神足焼町１番地 パナソニックデバイスシステムテクノ株式会社内
審査官　大石 博見
(56)参考文献　国際公開第２０１６／０８０４２２（WO，Ａ１）
国際公開第２０１３／０９４０７２（WO，Ａ１）
矢嶋 純 Jun Yajima，ＣＡＮの周期送信メッセージに対する攻撃検知手法の詳細評価とその評価手法，２０１７年 暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１７）予稿集 ［ＵＳＢ］ ２０１７年 暗号と情報セキュリティシンポジウム概要集 Abstracts of 2017 Symposium on Cryptography and Information Security，日本，電子情報通信学会，2017年01月27日，ｐｐ１－８
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　４１／００