(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-97206
(P2019-97206A)
(43)公開日　令和1年6月20日(2019.6.20)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/40	(2006.01)	H04L 12/40	M	5K032

審査請求 有　請求項の数 6　ＯＬ　（全 40 頁）

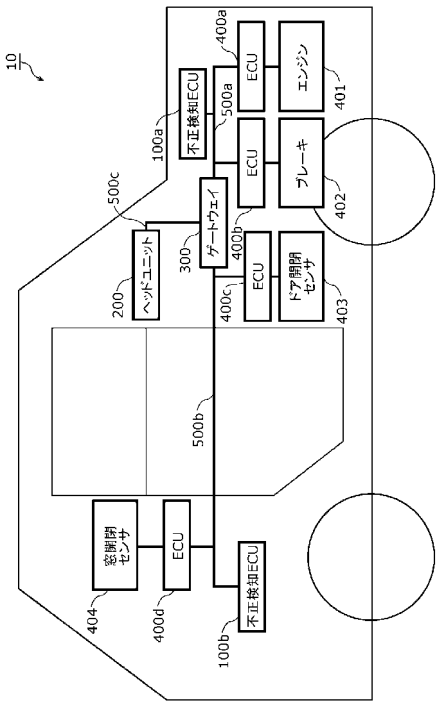
(21)出願番号　特願2019-29007(P2019-29007)
(22)出願日　平成31年2月21日(2019.2.21)
(62)分割の表示　特願2016-208163(P2016-208163)の分割
原出願日　平成27年3月12日(2015.3.12)
(31)優先権主張番号　61/974,739
(32)優先日　平成26年4月3日(2014.4.3)
(33)優先権主張国　米国(US)
(31)優先権主張番号　特願2014-245451(P2014-245451)
(32)優先日　平成26年12月4日(2014.12.4)
(33)優先権主張国　日本国(JP)

(71)出願人　514136668
パナソニック　インテレクチュアル　プロパティ　コーポレーション　オブ　アメリカ
Ｐａｎａｓｏｎｉｃ　Ｉｎｔｅｌｌｅｃｔｕａｌ　Ｐｒｏｐｅｒｔｙ　Ｃｏｒｐｏｒａｔｉｏｎ　ｏｆ　Ａｍｅｒｉｃａ
アメリカ合衆国　９０５０３　カリフォルニア州，トーランス，スイート　２００，マリナー　アベニュー　２０００
(74)代理人　100109210
弁理士　新居　広守
(74)代理人　100137235
弁理士　寺谷　英作

最終頁に続く

(54)【発明の名称】不正対処方法、不正検知電子制御ユニット、および、ネットワーク通信システム

(57)【要約】
【課題】バスに送信される不正なフレームに基づく処理が電子制御ユニット（ＥＣＵ）で実行されることを阻止するシステムを提供する。
【解決手段】ネットワーク通信システムは、ＥＣＵの通信用の複数のバス間でフレームを転送するゲートウェイ３００と、各バスに接続された不正検知ＥＣＵ１００ａ、１００ｂを備え、不正検知ＥＣＵは、フレームを受信する受信部と、受信されたフレームの所定フィールドの内容が不正を示す所定条件に該当するか否かを判定する判定部と、所定条件に該当すると判定された場合にエラーフレームを送信する送信部と、エラーフレームを送信した回数をエラーフレームの対象のフレームのＩＤ毎に記録する記録部と、ＩＤ毎の回数が所定回数を超えている場合に報知を行う報知部とを備え、判定部は、所定フィールドで表されるＩＤを、複数の不正検知ＥＣＵ毎に異なるＩＤリスト情報が示すＩＤと比較することにより所定条件に係る判定を行う。
【選択図】図１



【特許請求の範囲】
【請求項１】
ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットと当該バスに接続された不正検知電子制御ユニットとを備えるネットワーク通信システムであって、
前記不正検知電子制御ユニットは、
送信が開始されたフレームを受信する受信部と、
前記受信部により受信されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定部と、
前記判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信部と、
前記送信部においてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録部と、
前記記録部により記録されたＩＤ毎の回数が所定回数を超えている場合に、報知を行う報知部とを備え、
前記ネットワーク通信システムは、前記複数の電子制御ユニットの通信に複数のバスを用い、前記複数のバスの間でフレームを転送する機能を有するゲートウェイ装置と、異なるバスの各々に接続された複数の前記不正検知電子制御ユニットとを備え、
前記所定フィールドは、ＩＤを表すフィールドであり、
前記判定部は、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行い、
前記ＩＤリスト情報は、複数の前記不正検知電子制御ユニット毎に異なる
ネットワーク通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、電子制御ユニットが通信を行う車載ネットワーク等において送信された不正なフレームを検知して対処する技術に関する。
【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一つに、ＩＳＯ１１８９８－１で規定されているＣＡＮ（Controller Area Network）という規格が存在する（「非特許文献１」参照）。
【０００３】
ＣＡＮでは、通信路は２本のバスで構成され、バスに接続されているＥＣＵはノードと呼ばれる。バスに接続されている各ノードは、フレームと呼ばれるメッセージを送受信する。フレームを送信する送信ノードは、２本のバスに電圧をかけ、バス間で電位差を発生させることによって、レセシブと呼ばれる「１」の値と、ドミナントと呼ばれる「０」の値を送信する。複数の送信ノードが全く同一のタイミングで、レセシブとドミナントを送信した場合は、ドミナントが優先されて送信される。受信ノードは、受け取ったフレームのフォーマットに異常がある場合には、エラーフレームと呼ばれるフレームを送信する。エラーフレームとは、ドミナントを６ｂｉｔ連続して送信することで、送信ノードや他の受信ノードにフレームの異常を通知するものである。
【０００４】
またＣＡＮでは送信先や送信元を指す識別子は存在せず、送信ノードはフレーム毎にメ

ッセージＩＤと呼ばれるＩＤを付けて送信し（つまりバスに信号を送出し）、各受信ノードは予め定められたメッセージＩＤのみを受信する（つまりバスから信号を読み取る）。また、ＣＳＭＡ／ＣＡ（Carrier Sense Multiple Access/Collision Avoidance）方式を採用しており、複数ノードの同時送信時にはメッセージＩＤによる調停が行われ、メッセージＩＤの値が小さいフレームが優先的に送信される。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】ＣＡＮ Ｓｐｅｃｉｆｉｃａｔｉｏｎ ２．０ Ｐａｒｔ Ａ、［ｏｎｌｉｎｅ］、ＣＡＮ ｉｎ Ａｕｔｏｍａｔｉｏｎ（ＣｉＡ）、［平成２６年１１月１４日検索］、インターネット（ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｃａｎ－ｃｉａ．ｏｒｇ／ｆｉｌｅａｄｍｉｎ／ｃｉａ／ｓｐｅｃｉｆｉｃａｔｉｏｎｓ／ＣＡＮ２０Ａ．ｐｄｆ）

【非特許文献２】ＲＦＣ２１０４ ＨＭＡＣ： Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ ｆｏｒ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ

【発明の概要】

【発明が解決しようとする課題】

【０００６】

ところで、車載ネットワークにおいて不正なノードがバスに接続され、不正なノードが不正にフレームを送信することで、車体を不正にコントロールしてしまう可能性がある。

【０００７】

そこで、本開示は、車載ネットワーク等の、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おいて、バスに送信される不正なフレームに基づく処理がＥＣＵにより実行されることを阻止する不正検知電子制御ユニット（不正検知ＥＣＵ）を提供する。また、本開示は、不正なフレームに対応した処理が実行されるのを阻止する不正対処方法、及び、不正検知ＥＣＵを備えるネットワーク通信システムを提供する。

【課題を解決するための手段】

【０００８】

上記課題を解決するために本開示の一態様に係る不正対処方法は、ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備えるネットワーク通信システムにおいて用いられる不正対処方法であって、送信が開始されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定ステップと、前記判定ステップにおいて前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信ステップと、前記送信ステップにおいてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録ステップと、前記記録ステップにより記録されたＩＤ毎の回数が所定回数を超えている場合に、報知を行う報知ステップとを含む不正対処方法である。

【０００９】

また、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電子制御ユニットは、ＣＡＮプロトコルに従って通信する複数の電子制御ユニットが通信に用いるバスに接続される不正検知電子制御ユニットであって、送信が開始されたフレームを受信する受信部と、前記受信部により受信されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定部と、前記判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信部と、前記送信部においてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録部と、前記記録部により記録されたＩＤ毎の回数が所定回数を超えている場合に、報知を行う報知部とを備える不正検知電子制御ユニットである。

【００１０】
また、上記課題を解決するために本開示の一態様に係るネットワーク通信システムは、ＣＡＮプロトコルに従ってバスを介して通信する複数の電子制御ユニットと当該バスに接続された不正検知電子制御ユニットとを備えるネットワーク通信システムであって、前記不正検知電子制御ユニットは、送信が開始されたフレームを受信する受信部と、前記受信部により受信されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定部と、前記判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信部と、前記送信部においてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録部と、前記記録部により記録されたＩＤ毎の回数が所定回数を超えている場合に、報知を行う報知部とを備え、前記ネットワーク通信システムは、前記複数の電子制御ユニットの通信に複数のバスを用い、前記複数のバスの間でフレームを転送する機能を有するゲートウェイ装置と、異なるバスの各々に接続された複数の前記不正検知電子制御ユニットを備え、前記所定フィールドは、ＩＤを表すフィールドであり、前記判定部は、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行い、前記ＩＤリスト情報は、複数の前記不正検知電子制御ユニット毎に異なるネットワーク通信システムである。

【発明の効果】
【００１１】
本開示によれば、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おいて、バスに不正なノードが接続され不正なフレームが送信されたとしても、不正なフレームに基づく処理がＥＣＵにより実行されるのを阻止できる。

【図面の簡単な説明】
【００１２】
【図１】実施の形態１に係る車載ネットワークシステムの全体構成を示す図である。
【図２】ＣＡＮプロトコルで規定されるデータフレームのフォーマットを示す図である。
【図３】ＣＡＮプロトコルで規定されるエラーフレームのフォーマットを示す図である。
【図４】ヘッドユニットの構成図である。
【図５】受信ＩＤリストの一例を示した図である。
【図６】ゲートウェイの構成図である。
【図７】転送ルールの一例を示した図である。
【図８】実施の形態１に係るＥＣＵの構成図である。
【図９】受信ＩＤリストの一例を示した図である。
【図１０】エンジンに接続されたＥＣＵから送信されるフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図１１】ブレーキに接続されたＥＣＵから送信されるフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図１２】ドア開閉センサに接続されたＥＣＵから送信されるフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図１３】窓開閉センサに接続されたＥＣＵから送信されるフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図１４】実施の形態１に係る不正検知ＥＣＵの構成図である。
【図１５】不正検知ＥＣＵに保持される正規ＩＤリストの一例を示した図である。
【図１６】不正検知ＥＣＵに保持される正規ＩＤリストの一例を示した図である。
【図１７】メッセージＩＤ毎の不正検知カウンタの状態の一例を示す図である。
【図１８】実施の形態１における不正なフレームの検知及び実行阻止に係る動作例を示すシーケンス図である。
【図１９】実施の形態２に係る車載ネットワークシステムの全体構成を示す図である。

【図２０】実施の形態２に係る不正検知ＥＣＵの構成図である。
【図２１】不正検知ＥＣＵに保持されるデータ範囲リストの一例を示した図である。
【図２２】実施の形態２における不正なフレームの検知及び実行阻止に係る動作例を示すシーケンス図である（図２３に続く）。
【図２３】実施の形態２における不正なフレームの検知及び実行阻止に係る動作例を示すシーケンス図である（図２２から続く）。
【図２４】実施の形態３に係る車載ネットワークシステムの全体構成を示す図である。
【図２５】実施の形態３に係るＥＣＵの構成図である。
【図２６】エンジンに接続されたＥＣＵから送信されるデータフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図２７】ブレーキに接続されたＥＣＵから送信されるデータフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図２８】ドア開閉センサに接続されたＥＣＵから送信されるデータフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図２９】窓開閉センサに接続されたＥＣＵから送信されるデータフレームにおけるＩＤ及びデータフィールドの一例を示す図である。
【図３０】実施の形態３に係る不正検知ＥＣＵの構成図である。
【図３１】実施の形態３に係るカウンタ保持部に保持されているメッセージＩＤ毎のカウンタ値の一例を示す図である。
【図３２】実施の形態３における不正なフレームの検知及び実行阻止に係る動作例を示すシーケンス図である（図３３に続く）。
【図３３】実施の形態３における不正なフレームの検知及び実行阻止に係る動作例を示すシーケンス図である（図３２から続く）。
【発明を実施するための形態】
【００１３】
本開示の一態様に係る不正対処方法は、ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備えるネットワーク通信システムにおいて用いられる不正対処方法であって、送信が開始されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定ステップと、前記判定ステップにおいて前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信ステップとを含む不正対処方法である。なお、不正を示す所定条件の一例としては、例えば所定フィールドの内容が、正当値群を示すリストに含まれていないこと、不正値群を示すリストに含まれていること、一定範囲内又は一定特徴を有する値（例えば偶数等）であること、内容値に所定演算を施した結果が所定値となること等が挙げられる。これにより、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おいて、バスに不正なノードが接続され不正なフレームが送信されたとしても、不正なフレームに基づく処理が各ノード（ＥＣＵ）により実行されるのを阻止できる。
【００１４】
また、前記送信ステップでは、前記フレームにおけるＣＲＣシーケンスの最後尾が送信される前に、前記エラーフレームの前記送信を行うこととしても良い。これにより、例えば、ＣＲＣシーケンスを確認してフレームを処理するＥＣＵが、不正なフレームに基づく処理を実行できなくなる。
【００１５】
また、前記所定フィールドは、ＩＤを表すフィールドであり、前記判定ステップでは、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行うこととしても良い。これにより、例えば、データフレーム或いはリモートフレームにおけるＩＤフィールドで不正を判断可能となり、各ＥＣＵでの不正なフレームについての処理の実行を阻止できる。

【００１６】
また、前記所定フィールドは、コントロールフィールドであり、前記判定ステップでは、前記所定フィールドの内容により表されるデータ長が予め定められた範囲に含まれるか否かを判別することにより、前記内容が前記所定条件に該当するか否かの前記判定を行うこととしても良い。これにより、例えば、データフレーム或いはリモートフレームにおけるコントロールフィールドで不正を判断可能となり、各ＥＣＵでの不正なフレームについての処理の実行を阻止できる。
【００１７】
また、前記判定ステップでは、送信された前記フレームがデータフレームである場合に前記判定を行い、前記所定フィールドは、データフィールドであることとしても良い。これにより、不正なデータフレームのデータに従って各ＥＣＵがそのデータに対応した処理を実行してしまうことを阻止できる。
【００１８】
また、前記判定ステップでは、前記所定フィールドの内容であるデータ値が予め定められた範囲に含まれるか否かを判別することにより、前記内容が前記所定条件に該当するか否かの前記判定を行うこととしても良い。これにより、例えば不正な範囲のデータ値を含ませた不正なデータフレームが送信されても、各ＥＣＵがそのデータに対応した処理を実行してしまうことを阻止できる。
【００１９】
また、前記判定ステップでは、前記所定フィールドの内容におけるメッセージ認証コードを予め定められた検証処理手順により検証し、当該検証に失敗した場合には、前記内容が前記所定条件に該当すると判定することとしても良い。これにより、正規なメッセージ認証コードを付加していない不正なフレームが送信された場合に各ＥＣＵでの不正なフレームについての処理の実行を阻止できる。
【００２０】
また、正当な電子制御ユニットにより送信されるデータフレームは、データフィールド内に、データフレームが送信される度に変化する変数に応じて算定されたメッセージ認証コードを含み、前記判定ステップでは、データフレームが送信される度に変化する前記変数を、前記所定フィールドの内容における前記メッセージ認証コードが反映していない場合に、前記内容が前記所定条件に該当すると判定することとしても良い。これにより、例えばメッセージ認証コードについての不正な解読を困難化できる。
【００２１】
また、メッセージ認証コード鍵を有する正当な電子制御ユニットにより送信されるデータフレームは、データフィールド内に前記メッセージ認証コード鍵を用いて生成されたメッセージ認証コードを含み、前記判定ステップでは、前記メッセージ認証コード鍵に呼応する鍵を用いて前記所定フィールドの内容における前記メッセージ認証コードの前記検証を行うこととしても良い。これにより、例えば正規な複数のＥＣＵについて、メッセージ認証コード鍵を除くメッセージ認証コード生成のための構成を共通化できる。
【００２２】
また、前記不正対処方法は更に、前記送信ステップにおいてエラーフレームを送信した回数を記録する記録ステップと、前記記録ステップにより記録された回数が所定回数を超えた場合に報知を行う報知ステップとを含むこととしても良い。これにより、不正なフレームが繰り返して送信された場合にユーザ等に報知することができる。
【００２３】
また、本開示の一態様に係る不正検知電子制御ユニット（不正検知ＥＣＵ）は、ＣＡＮ（Controller Area Network）プロトコルに従って通信する複数の電子制御ユニットが通信に用いるバスに接続される不正検知電子制御ユニットであって、送信が開始されたフレームを受信する受信部と、前記受信部により受信されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定部と、前記判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、

当該フレームの最後尾が送信される前にエラーフレームを送信する送信部とを備える不正検知電子制御ユニットである。これにより、ＣＡＮプロトコルに従って通信する複数のＥＣＵを接続するバスに不正なノードが接続され不正なフレームが送信されたとしても、不正なフレームに基づく処理が各ＥＣＵにより実行されるのを阻止できる。

【００２４】

また、本開示の一態様に係るネットワーク通信システムは、ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットと当該バスに接続された不正検知電子制御ユニットとを備えるネットワーク通信システムであって、前記不正検知電子制御ユニットは、送信が開始されたフレームを受信する受信部と、前記受信部により受信されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定部と、前記判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信部とを備えるネットワーク通信システムである。これにより、バスに不正なノードが接続され不正なフレームが送信されたとしても、不正なフレームに基づく処理がＥＣＵにより実行されるのを阻止できる。

【００２５】

なお、これらの全般的又は具体的な態様は、システム、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等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されても良い。

【００２６】

以下、実施の形態に係る不正検知ＥＣＵ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。従って、以下の実施の形態で示される数値、構成要素、構成要素の配置及び接続形態、並びに、ステップ（工程）及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。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。また、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。

【００２７】

（実施の形態１）

以下、本開示の実施の形態として、メッセージＩＤを用いて他のノード（ＥＣＵ）において不正なフレームに基づく処理が実行されることを阻止するための不正対処方法を実現する不正検知ＥＣＵを含む車載ネットワークシステム１０について図面を用いて説明する。

【００２８】

［１．１　車載ネットワークシステム１０の全体構成］

図１は、実施の形態１に係る車載ネットワークシステム１０の全体構成を示す図である。車載ネットワークシステム１０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一例であり、制御装置、センサ等の各種機器が搭載された自動車におけるネットワーク通信システムである。車載ネットワークシステム１０は、バス５００ａ、５００ｂと、不正検知ＥＣＵ１００ａ、１００ｂ、ヘッドユニット２００、ゲートウェイ３００、及び、各種機器に接続されたＥＣＵ４００ａ～４００ｄ等のＥＣＵといったバスに接続された各ノードとを含んで構成される。なお、図１では省略しているものの、車載ネットワークシステム１０にはＥＣＵ４００ａ～４００ｄ以外にもいくつものＥＣＵが含まれ得るが、ここでは、便宜上ＥＣＵ４００ａ～４００ｄに注目して説明を行う。ＥＣＵは、例えば、プロセッサ（マイクロプロセッサ）、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制御プログラム（コンピュータプログラム）を記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）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。なお、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、プロセッサ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。ここでは、バス５００ａ、５００ｂには不正なフレームを送信する不正ＥＣＵが接続されている可能性があることを前提として説明する。

【００２９】

不正検知ＥＣＵ１００ａ、１００ｂは、それぞれバス５００ａ、バス５００ｂに接続され、ＥＣＵ４００ａ～４００ｄ等により送信されたフレームが不正であるかどうかを判定し、不正であればエラーフレームを送信する機能を有するＥＣＵである。

【００３０】

ＥＣＵ４００ａ～４００ｄは、いずれかのバスと接続され、また、それぞれエンジン４０１、ブレーキ４０２、ドア開閉センサ４０３、窓開閉センサ４０４に接続されている。ＥＣＵ４００ａ～４００ｄのそれぞれは、接続されている機器（エンジン４０１等）の状態を取得し、定期的に状態を表すフレーム（後述するデータフレーム）等をネットワーク（つまりバス）に送信している。

【００３１】

ゲートウェイ３００は、不正検知ＥＣＵ１００ａ、ＥＣＵ４００ａ及びＥＣＵ４００ｂがつながるバス５００ａと、不正検知ＥＣＵ１００ｂ、ＥＣＵ４００ｃ及びＥＣＵ４００ｄがつながるバス５００ｂと、ヘッドユニット２００がつながるバス５００ｃとに接続しており、それぞれのバスから受信したフレームを他のバスに転送する機能を有する。また受信したフレームを転送するかしないかを接続されたバス間毎に切り替えることも可能である。ゲートウェイ３００も一種のＥＣＵである。

【００３２】

ヘッドユニット２００は、フレームを受信する機能を持ち、ＥＣＵ４００ａ～４００ｄから送信されるフレームを受信し、各種状態をディスプレイ（図示しない）に表示して、ユーザに提示する機能を持つ。ヘッドユニット２００も一種のＥＣＵである。

【００３３】

この車載ネットワークシステム１０においてはＣＡＮプロトコルに従って各ＥＣＵがフレームの授受を行う。ＣＡＮプロトコルにおけるフレームには、データフレーム、リモートフレーム、オーバーロードフレーム及びエラーフレームがある。説明の便宜上、まずはデータフレーム及びエラーフレームを中心に説明する。

【００３４】

［１．２　データフレームフォーマット］

以下、ＣＡＮプロトコルに従ったネットワークで用いられるフレームの１つであるデータフレームについて説明する。

【００３５】

図２は、ＣＡＮプロトコルで規定されるデータフレームのフォーマットを示す図である。同図には、ＣＡＮプロトコルで規定される標準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、ＳＯＦ（Start Of Frame）、ＩＤフィールド、ＲＴＲ（Remote Transmission Request）、ＩＤＥ（Identifier Extension）、予約ビット「ｒ」、ＤＬＣ（Data Length Code）、データフィールド、ＣＲＣ（Cyclic Redundancy Check）シーケンス、ＣＲＣデリミタ「ＤＥＬ」、ＡＣＫ（Acknowledgement）スロット、ＡＣＫデリミタ「ＤＥＬ」、及び、ＥＯＦ（End Of Frame）の各フィールドで構成される。

【００３６】

ＳＯＦは、１ｂｉｔのドミナントで構成される。バスがアイドルの状態はレセシブになっており、ＳＯＦによりドミナントへ変更することでフレームの送信開始を通知する。

【００３７】

ＩＤフィールドは、１１ｂｉｔで構成される、データの種類を示す値であるＩＤ（メッセージＩＤ）を格納するフィールドである。複数のノードが同時に送信を開始した場合、このＩＤフィールドで通信調停を行うために、ＩＤが小さい値を持つフレームが高い優先度となるよう設計されている。

【００３８】

ＲＴＲは、データフレームとリモートフレームとを識別するための値であり、データフレームにおいてはドミナント１ｂｉｔで構成される。

【００３９】

ＩＤＥと「ｒ」とは、両方ドミナント１ｂｉｔで構成される。

【００４０】

ＤＬＣは、４ｂｉｔで構成され、データフィールドの長さを示す値である。なお、ＩＤＥ、「ｒ」及びＤＬＣを合わせてコントロールフィールドと称する。

【００４１】

データフィールドは、最大６４ｂｉｔで構成される送信するデータの内容を示す値である。８ｂｉｔ毎に長さを調整できる。送られるデータの仕様については、ＣＡＮプロトコルで規定されておらず、車載ネットワークシステム１０において定められる。従って、車種、製造者（製造メーカ）等に依存した仕様となる。

【００４２】

ＣＲＣシーケンスは、１５ｂｉｔで構成される。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送信値より算出される。

【００４３】

ＣＲＣデリミタは、１ｂｉｔのレセシブで構成されるＣＲＣシーケンスの終了を表す区切り記号である。なお、ＣＲＣシーケンス及びＣＲＣデリミタを合わせてＣＲＣフィールドと称する。

【００４４】

ＡＣＫスロットは、１ｂｉｔで構成される。送信ノードはＡＣＫスロットをレセシブにして送信を行う。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ＡＣＫスロットをドミナントとして送信する。レセシブよりドミナントが優先されるため、送信後にＡＣＫスロットがドミナントであれば、送信ノードは、いずれかの受信ノードが受信に成功していること確認できる。

【００４５】

ＡＣＫデリミタは、１ｂｉｔのレセシブで構成されるＡＣＫの終了を表す区切り記号である。

【００４６】

ＥＯＦは、７ｂｉｔのレセシブで構成されており、データフレームの終了を示す。

【００４７】

［１．３　エラーフレームフォーマット］

図３は、ＣＡＮプロトコルで規定されるエラーフレームのフォーマットを示す図である。エラーフレームは、エラーフラグ（プライマリ）と、エラーフラグ（セカンダリ）と、エラーデリミタとから構成される。

【００４８】

エラーフラグ（プライマリ）は、エラーの発生を他のノードに知らせるために使用される。エラーを検知したノードはエラーの発生を他のノードに知らせるために６ｂｉｔのドミナントを連続で送信する。この送信は、ＣＡＮプロトコルにおけるビットスタッフィングルール（連続して同じ値を６ｂｉｔ以上送信しない）に違反し、他のノードからのエラーフレーム（セカンダリ）の送信を引き起こす。

【００４９】

エラーフラグ（セカンダリ）は、エラーの発生を他のノードに知らせるために使用される連続した６ビットのドミナントで構成される。エラーフラグ（プライマリ）を受信してビットスタッフィングルール違反を検知した全てのノードがエラーフラグ（セカンダリ）を送信することになる。

【００５０】

エラーデリミタ「ＤＥＬ」は、８ｂｉｔの連続したレセシブであり、エラーフレームの終了を示す。

【００５１】

［１．４　ヘッドユニット２００の構成］
ヘッドユニット２００は、例えば、自動車のインパネ等に設けられ、運転者に視認されるための情報を表示する液晶ディスプレイ（ＬＣＤ：liquid crystal display）等の表示装置、運転者の操作を受け付ける入力手段等を備える一種のＥＣＵである。
【００５２】
図４は、ヘッドユニット２００の構成図である。ヘッドユニット２００は、フレーム送受信部２７０と、フレーム解釈部２６０と、受信ＩＤ判断部２４０と、受信ＩＤリスト保持部２５０と、フレーム処理部２２０と、表示制御部２１０と、フレーム生成部２３０とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、ヘッドユニット２００における通信回路、ＬＣＤ、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。
【００５３】
フレーム送受信部２７０は、バス５００ｃに対して、ＣＡＮプロトコルに従ったフレームを送受信する。バス５００ｃからフレームを１ｂｉｔずつ受信し、フレーム解釈部２６０に転送する。また、フレーム生成部２３０より通知を受けたフレームの内容をバス５００ｃに１ｂｉｔずつ送信する。
【００５４】
フレーム解釈部２６０は、フレーム送受信部２７０よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。フレーム解釈部２６０は、ＩＤフィールドと判断した値は受信ＩＤ判断部２４０へ転送する。フレーム解釈部２６０は、受信ＩＤ判断部２４０から通知される判定結果に応じて、ＩＤフィールドの値と、ＩＤフィールド以降に現れるデータフィールドとを、フレーム処理部２２０へ転送するか、その判定結果を受けた以降においてフレームの受信を中止する（つまりそのフレームとしての解釈を中止する）かを決定する。また、フレーム解釈部２６０は、例えば、ＣＲＣの値が合わなかったり、ドミナント固定とされている項目がレセシブだったりする等、ＣＡＮプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部２３０へ通知する。また、フレーム解釈部２６０は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。例えばデータフレームの途中からエラーフレームと解釈された場合においては、そのデータフレームの解釈は中止され、そのデータフレームに応じて特段の処理を行うことがなくなる。
【００５５】
受信ＩＤ判断部２４０は、フレーム解釈部２６０から通知されるＩＤフィールドの値を受け取り、受信ＩＤリスト保持部２５０が保持しているメッセージＩＤのリストに従い、そのＩＤフィールド以降のフレームの各フィールドを受信するかどうかの判定を行う。この判定結果を、受信ＩＤ判断部２４０は、フレーム解釈部２６０へ通知する。
【００５６】
受信ＩＤリスト保持部２５０は、ヘッドユニット２００が受信するＩＤ（メッセージＩＤ）のリストである受信ＩＤリストを保持する。図５は、受信ＩＤリストの一例を示した図である。ヘッドユニット２００は、エンジン４０１に接続されたＥＣＵ４００ａからメッセージＩＤが「１」であるフレーム（メッセージ）を受信し、ブレーキ４０２に接続されたＥＣＵ４００ｂからメッセージＩＤが「２」であるフレームを受信し、ドア開閉センサ４０３に接続されたＥＣＵ４００ｃからメッセージＩＤが「３」であるフレームを受信し、窓開閉センサ４０４に接続されたＥＣＵ４００ｄからメッセージＩＤが「４」であるフレームを受信する。
【００５７】
フレーム処理部２２０は、受信したフレームの内容（例えばメッセージＩＤ及びデータフィールドの内容）に基づいて、例えばＬＣＤに表示されるべき画像を形成して、表示制御部２１０に通知する。なお、フレーム処理部２２０は、受信したデータフィールドの内

容を保持し、入力手段を通じて受け付けた運転者による操作に応じて、ＬＣＤに表示されるべき画像（例えば車速表示用の画像、窓開閉状態表示用の画像等）を選択して通知しても良い。

【００５８】

表示制御部２１０は、フレーム処理部２２０より通知を受けた内容をＬＣＤ等に表示する。

【００５９】

フレーム生成部２３０は、フレーム解釈部２６０からのエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部２７０へ通知して送信させる。

【００６０】

［１．５　受信ＩＤリスト例１］

上述した図５は、ヘッドユニット２００、ゲートウェイ３００、ＥＣＵ４００ｃ及びＥＣＵ４００ｄのそれぞれにおいて保持される受信ＩＤリストの一例を示す図である。同図に例示する受信ＩＤリストは、ＩＤ（メッセージＩＤ）の値が「１」、「２」、「３」及び「４」のいずれかであるメッセージＩＤを含むフレームを選択的に受信して処理するために用いられる。例えば、ヘッドユニット２００の受信ＩＤリスト保持部２５０に図５の受信ＩＤリストが保持されていると、メッセージＩＤが「１」、「２」、「３」及び「４」のいずれでもないフレームについては、フレーム解釈部２６０でのＩＤフィールド以後のフレームの解釈が中止される。

【００６１】

［１．６　ゲートウェイ３００の構成］

図６は、ゲートウェイ３００の構成図である。ゲートウェイ３００は、フレーム送受信部３６０と、フレーム解釈部３５０と、受信ＩＤ判断部３３０と、受信ＩＤリスト保持部３４０と、フレーム生成部３２０と、転送処理部３１０と、転送ルール保持部３７０とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、ゲートウェイ３００における通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。

【００６２】

フレーム送受信部３６０は、バス５００ａ、５００ｂ、５００ｃそれぞれに対して、ＣＡＮプロトコルに従ったフレームを送受信する。バスからフレームを１ｂｉｔずつ受信し、フレーム解釈部３５０に転送する。また、フレーム生成部３２０より通知を受けた転送先のバスを示すバス情報及びフレームに基づいて、そのフレームの内容をバス５００ａ、５００ｂ、５００ｃに１ｂｉｔずつ送信する。

【００６３】

フレーム解釈部３５０は、フレーム送受信部３６０よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。ＩＤフィールドと判断した値は受信ＩＤ判断部３３０へ転送する。フレーム解釈部３５０は、受信ＩＤ判断部３３０から通知される判定結果に応じて、ＩＤフィールドの値と、ＩＤフィールド以降に現れるデータフィールド（データ）とを、転送処理部３１０へ転送するか、その判定結果を受けた以降においてフレームの受信を中止する（つまりそのフレームとしての解釈を中止する）かを決定する。また、フレーム解釈部３５０は、ＣＡＮプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部３２０へ通知する。また、フレーム解釈部３５０は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

【００６４】

受信ＩＤ判断部３３０は、フレーム解釈部３５０から通知される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、

そのＩＤフィールド以降のフレームの各フィールドを受信するかどうかの判定を行う。この判定結果を、受信ＩＤ判断部３３０は、フレーム解釈部３５０へ通知する。

【００６５】

受信ＩＤリスト保持部３４０は、ゲートウェイ３００が受信するＩＤ（メッセージＩＤ）のリストである受信ＩＤリスト（図５参照）を保持する。

【００６６】

転送処理部３１０は、転送ルール保持部３７０が保持する転送ルールに従って、受信したフレームのメッセージＩＤに応じて、転送するバスを決定し、転送するバスを示すバス情報とフレーム解釈部３５０より通知されたメッセージＩＤとデータとをフレーム生成部３２０へ通知する。なお、ゲートウェイ３００は、あるバスから受信されたエラーフレームについては他のバスに転送しない。

【００６７】

転送ルール保持部３７０は、バス毎のフレームの転送についてのルールを表す情報である転送ルールを保持する。図７は、転送ルールの一例を示した図である。

【００６８】

フレーム生成部３２０は、フレーム解釈部３５０から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部３６０へ通知して送信させる。また、フレーム生成部３２０は、転送処理部３１０より通知されたメッセージＩＤとデータとを使ってフレームを構成し、フレーム及びバス情報をフレーム送受信部３６０へ通知する。

【００６９】

［１．７　転送ルール例］

図７は、上述したようにゲートウェイ３００が保有する転送ルールの一例を示す。この転送ルールは、転送元のバスと転送先のバスと転送対象のＩＤ（メッセージＩＤ）とを対応付けている。図７中のメッセージＩＤにかかわらずフレームの転送がなされることを表している。また、同図中の「－」は転送対象のフレームがないことを示す。同図の例は、バス５００ａから受信するフレームはメッセージＩＤにかかわらず、バス５００ｂ及びバス５００ｃに転送するように設定されていることを示している。また、バス５００ｂから受信するフレームのうち、バス５００ｃには全てのフレームが転送されるが、バス５００ａにはメッセージＩＤが「３」であるフレームのみが転送されるように設定されていることを示している。また、バス５００ｃから受信されるフレームは、バス５００ａにもバス５００ｂにも転送されないように設定されていることを示している。

【００７０】

［１．８　ＥＣＵ４００ａの構成］

図８は、ＥＣＵ４００ａの構成図である。ＥＣＵ４００ａは、フレーム送受信部４６０と、フレーム解釈部４５０と、受信ＩＤ判断部４３０と、受信ＩＤリスト保持部４４０と、フレーム処理部４１０と、フレーム生成部４２０と、データ取得部４７０とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、ＥＣＵ４００ａにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。

【００７１】

フレーム送受信部４６０は、バス５００ａに対して、ＣＡＮプロトコルに従ったフレームを送受信する。バス５００ａからフレームを１ｂｉｔずつ受信し、フレーム解釈部４５０に転送する。また、フレーム生成部４２０より通知を受けたフレームの内容をバス５００ａに送信する。

【００７２】

フレーム解釈部４５０は、フレーム送受信部４６０よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。ＩＤフィールドと判断した値は受信ＩＤ判断部４３０へ転送する。フレーム解釈部４５０は、受信ＩＤ判断部４３０から通知される判定結果に応じて、ＩＤ

フィールドの値と、ＩＤフィールド以降に現れるデータフィールドとを、フレーム処理部４１０へ転送するか、その判定結果を受けた以降においてフレームの受信を中止する（つまりそのフレームとしての解釈を中止する）かを決定する。また、フレーム解釈部４５０は、ＣＡＮプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部４２０へ通知する。また、フレーム解釈部４５０は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

【００７３】

受信ＩＤ判断部４３０は、フレーム解釈部４５０から通知されるＩＤフィールドの値を受け取り、受信ＩＤリスト保持部４４０が保持しているメッセージＩＤのリストに従い、そのＩＤフィールド以降のフレームの各フィールドを受信するかどうかの判定を行う。この判定結果を、受信ＩＤ判断部４３０は、フレーム解釈部４５０へ通知する。

【００７４】

受信ＩＤリスト保持部４４０は、ＥＣＵ４００ａが受信するＩＤ（メッセージＩＤ）のリストである受信ＩＤリストを保持する。図９は、受信ＩＤリストの一例を示した図である。

【００７５】

フレーム処理部４１０は、受信したフレームのデータに応じてＥＣＵ毎に異なる機能に係る処理を行う。例えば、エンジン４０１に接続されたＥＣＵ４００ａは、時速が３０ｋｍを超えた状態でドアが開いている状態だと、アラーム音を鳴らす機能を備える。ＥＣＵ４００ａは、例えばアラーム音を鳴らすためのスピーカ等を有している。そして、ＥＣＵ４００ａのフレーム処理部４１０は、他のＥＣＵから受信したデータ（例えばドアの状態を示す情報）を管理し、エンジン４０１から取得された時速に基づいて一定条件下でアラーム音を鳴らす処理等を行う。

【００７６】

データ取得部４７０は、ＥＣＵにつながっている機器、センサ等の状態を示すデータを取得し、フレーム生成部４２０に通知する。

【００７７】

フレーム生成部４２０は、フレーム解釈部４５０から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部４６０へ通知して送信させる。また、フレーム生成部４２０は、データ取得部４７０より通知されたデータの値に対して、予め定められたメッセージＩＤをつけてフレームを構成し、フレーム送受信部４６０へ通知する。

【００７８】

なお、ＥＣＵ４００ｂ～４００ｄも、上述したＥＣＵ４００ａと基本的に同様の構成を備える。但し、受信ＩＤリスト保持部４４０に保持される受信ＩＤリストはＥＣＵ毎に異なる内容となり得る。ＥＣＵ４００ｂは図９に例示する受信ＩＤリストを保持し、ＥＣＵ４００ｃ及びＥＣＵ４００ｄは図５に例示する受信ＩＤリストを保持する。また、フレーム処理部４１０の処理内容は、ＥＣＵ毎に異なる。例えば、ＥＣＵ４００ｃにおけるフレーム処理部４１０の処理内容は、ブレーキがかかっていない状況でドアが開くとアラーム音を鳴らす機能に係る処理を含む。例えば、ＥＣＵ４００ｂ及びＥＣＵ４００ｄにおけるフレーム処理部４１０では特段の処理を行わない。なお、各ＥＣＵは、ここで例示した以外の機能を備えていても良い。なお、ＥＣＵ４００ａ～４００ｄのそれぞれが送信するフレームの内容については後に図１０～図１３を用いて説明する。

【００７９】

［１．９　受信ＩＤリスト例２］

上述した図９は、ＥＣＵ４００ａ及びＥＣＵ４００ｂのそれぞれにおいて保持される受信ＩＤリストの一例を示す図である。同図に例示する受信ＩＤリストは、ＩＤ（メッセージＩＤ）の値が「１」、「２」及び「３」のいずれかであるメッセージＩＤを含むフレー

ムを選択的に受信して処理するために用いられる。例えば、ＥＣＵ４００ａの受信ＩＤリスト保持部４４０に図９の受信ＩＤリストが保持されていると、メッセージＩＤが「１」、「２」及び「３」のいずれでもないフレームについては、フレーム解釈部４５０でのＩＤフィールド以後のフレームの解釈が中止される。

【００８０】

［１．１０　エンジンに係るＥＣＵ４００ａの送信フレーム例］

図１０は、エンジン４０１に接続されたＥＣＵ４００ａから送信されるフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ４００ａが送信するフレームのメッセージＩＤは「１」である。データは、時速（ｋｍ／時）を表し、最低０（ｋｍ／時）～最高１８０（ｋｍ／時）までの範囲の値を取り、データ長は１Ｂｙｔｅである。図１０の上行から下行へと、ＥＣＵ４００ａから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、０ｋｍ／時から１ｋｍ／時ずつ加速されている様子を表している。

【００８１】

［１．１１　ブレーキに係るＥＣＵ４００ｂの送信フレーム例］

図１１は、ブレーキ４０２に接続されたＥＣＵ４００ｂから送信されるフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ４００ｂが送信するフレームのメッセージＩＤは「２」である。データは、ブレーキのかかり具合を割合（％）で表し、データ長は１Ｂｙｔｅである。この割合は、ブレーキを全くかけていない状態を０（％）、ブレーキを最大限かけている状態を１００（％）としたものである。図１１の上行から下行へと、ＥＣＵ４００ｂから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、１００％から徐々にブレーキを弱めている様子を表している。

【００８２】

［１．１２　ドア開閉センサに係るＥＣＵ４００ｃの送信フレーム例］

図１２は、ドア開閉センサ４０３に接続されたＥＣＵ４００ｃから送信されるフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ４００ｃが送信するフレームのメッセージＩＤは「３」である。データは、ドアの開閉状態を表し、データ長は１Ｂｙｔｅである。データの値は、ドアが開いている状態が「１」、ドアが閉まっている状態が「０」である。図１２の上行から下行へと、ＥＣＵ４００ｃから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、ドアが開いている状態から次第に閉められた状態へと移った様子を表している。

【００８３】

［１．１３　窓開閉センサに係るＥＣＵ４００ｄの送信フレーム例］

図１３は、窓開閉センサ４０４に接続されたＥＣＵ４００ｄから送信されるフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ４００ｄが送信するフレームのメッセージＩＤは「４」である。データは、窓の開閉状態を割合（％）で表し、データ長は１Ｂｙｔｅである。この割合は、窓が完全に閉まっている状態を０（％）、窓が全開の状態を１００（％）としたものである。図１３の上行から下行へと、ＥＣＵ４００ｄから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、窓が閉まっている状態から徐々に開いていく様子を表している。

【００８４】

［１．１４　不正検知ＥＣＵ１００ａの構成］

図１４は、不正検知ＥＣＵ１００ａの構成図である。不正検知ＥＣＵ１００ａは、フレーム送受信部１６０と、フレーム解釈部１５０と、不正フレーム検知部１３０と、正規ＩＤリスト保持部１２０と、不正検知カウンタ保持部１１０と、フレーム生成部１４０とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、不正検知ＥＣＵ１００ａにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、不正検知ＥＣＵ１００ｂも基

本的に同様の構成を備えるが、正規ＩＤリスト保持部１２０が保持するリスト情報（正規ＩＤリスト）の内容が不正検知ＥＣＵ１００ａと不正検知ＥＣＵ１００ｂとでは異なる。

【００８５】

フレーム送受信部１６０は、バス５００ａに対して、ＣＡＮプロトコルに従ったフレームを送受信する。即ち、フレーム送受信部１６０は、バス上でのフレームの送信が開始された場合においてフレームを受信する言わば受信部として働き、また、バスにエラーフレーム等を送信する言わば送信部として働く。即ち、フレーム送受信部１６０は、バス５００ａからフレームを１ｂｉｔずつ受信し、フレーム解釈部１５０に転送する。また、フレーム生成部１４０より通知を受けたフレームの内容をバス５００ａに送信する。

【００８６】

フレーム解釈部１５０は、フレーム送受信部１６０よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。ＩＤフィールドと判断した値は、不正フレーム検知部１３０へ転送する。また、フレーム解釈部１５０は、ＣＡＮプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部１４０へ通知する。また、フレーム解釈部１５０は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

【００８７】

不正フレーム検知部１３０は、フレーム解釈部１５０から通知されるＩＤフィールドの値を受け取り、ＩＤフィールドの値が不正を示す所定条件に該当するか否かを判定する。即ち不正フレーム検知部１３０は、受信されたフレームにおける所定フィールドの内容が不正を示す所定条件に該当するか否かを判定する言わば判定部として機能する。この不正を示す所定条件は、ＩＤフィールドの値が、正規ＩＤリスト保持部１２０が保持しているメッセージＩＤのリストに載っていないという条件である。即ち、正規ＩＤリスト保持部１２０が保持しているメッセージＩＤのリストに従い、通知されたＩＤフィールドの値（メッセージＩＤ）が不正かどうかの判定を行う。このリスト（つまり後述する正規ＩＤリスト）に載っていないメッセージＩＤを受信した場合は、不正の検知回数をインクリメントするために、受信したメッセージＩＤを不正検知カウンタ保持部１１０へ通知する。また、正規ＩＤリストに載っていないメッセージＩＤを受信した場合は、エラーフレームを送信するように、フレーム生成部１４０へ通知する。また、不正の検知回数が一定回数以上に達した場合に、不正検知カウンタ保持部１１０より通知を受け、該当するメッセージＩＤを発行する不正なＥＣＵが存在することを示すエラー表示メッセージ（フレーム）を送信するようフレーム生成部１４０へ通知する。エラー表示メッセージのメッセージＩＤは予め定められており、このメッセージＩＤのメッセージ（フレーム）をヘッドユニット２００が受信してエラー表示を行うようになっている。このエラー表示メッセージについては便宜上説明を省略していたが、エラー表示メッセージのメッセージＩＤは、ゲートウェイ３００及びヘッドユニット２００が保持する受信ＩＤリスト、及び、後述する正規ＩＤリストに掲載される。但し、図１５、図１６ではエラー表示メッセージについてのメッセージＩＤを省略している。

【００８８】

正規ＩＤリスト保持部１２０は、車載ネットワークシステム１０においてバス５００ａ上を送信されることとなるフレームに含まれるメッセージＩＤを予め規定したリストである正規ＩＤリストを保持する（図１５、図１６参照）。

【００８９】

不正検知カウンタ保持部１１０は、メッセージＩＤ毎に検知回数をカウントするための不正検知カウンタを保持しており、不正フレーム検知部１３０からメッセージＩＤが通知されると、該当する不正検知カウンタをインクリメント（増加）する。不正検知カウンタが一定数（所定回数）以上に達した場合、不正フレーム検知部１３０に一定数を超えたことを通知する。ここでいう一定数（所定回数）の一例は、ＣＡＮプロトコルにおける送信

エラーカウンタの取り扱い規則に対応して定められた値である。ＣＡＮプロトコルでは、ＥＣＵがエラーフレームによって送信を阻止する度に送信エラーカウンタが８カウントアップする。そして、この結果として送信ノードにおける送信エラーカウンタが１２８迄カウントアップすれば送信ノードはパッシブ状態に遷移してフレーム送信をしなくなるように規定されている。従って、１２８／８（＝１６）より大きな１７をこの一定数として定めておけば、ＣＡＮプロトコルにおける送信エラーカウンタに係る規則を無視した送信ノード（不正なＥＣＵ）の存在が推定される場合に不正検知ＥＣＵ１００ａからエラー表示メッセージが送信されるようになる。なお、不正なフレームを送信する、不正なＥＣＵが、ＣＡＮプロトコルにおける送信エラーカウンタに係る規則に従うものであった場合には、不正検知ＥＣＵ１００ａによるエラーフレームの送信によって、不正なＥＣＵの送信エラーカウンタは８インクリメントされる。この場合、不正なフレームの送信を繰り返すことで不正なＥＣＵの送信エラーカウンタが１２８まで上昇すると、不正なＥＣＵがパッシブ状態に遷移し、不正なＥＣＵによる不正なフレームの送信が停止することになる。

【００９０】

フレーム生成部１４０は、フレーム解釈部１５０から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部１６０へ通知して送信させる。また、フレーム生成部１４０は、不正フレーム検知部１３０から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部１６０へ通知して送信させる。更にフレーム生成部１４０は、不正フレーム検知部１３０から通知されたエラー表示メッセージの送信を指示する通知に従い、エラー表示メッセージをフレーム送受信部１６０へ通知して送信させる。

【００９１】

［１．１５　不正検知ＥＣＵ１００ａの正規ＩＤリスト例］

図１５は、不正検知ＥＣＵ１００ａの正規ＩＤリスト保持部１２０に保持される正規ＩＤリストの一例を示した図である。同図に例示する正規ＩＤリストは、ＩＤ（メッセージＩＤ）の値が「１」、「２」及び「３」のいずれかであるメッセージＩＤを含むフレームがバス５００ａに流れ得ることを示している。

【００９２】

［１．１６　不正検知ＥＣＵ１００ｂの正規ＩＤリスト例］

図１６は、不正検知ＥＣＵ１００ｂの正規ＩＤリスト保持部１２０に保持される正規ＩＤリストの一例を示した図である。同図に例示する正規ＩＤリストは、ＩＤ（メッセージＩＤ）の値が「１」、「２」、「３」及び「４」のいずれかであるメッセージＩＤを含むフレームがバス５００ｂに流れ得ることを示している。

【００９３】

［１．１７　不正検知カウンタ保存リスト例］

図１７は、メッセージＩＤ毎の不正検知カウンタの状態の一例を示す図である。同図の例は、メッセージＩＤが「４」の不正検知カウンタだけが、不正を一度検知しており、その他のメッセージＩＤでは一度も検知していないことを示す。即ち、この例はバス５００ａに本来流れるはずがないメッセージＩＤ「４」のメッセージ（フレーム）が一度送信されたことを不正検知ＥＣＵ１００ａが検知し、該当するメッセージＩＤ「４」に対応する不正検知カウンタを１インクリメントした場合を示している。

【００９４】

［１．１８　不正フレームの検知に係るシーケンス］

以下、上述の構成を備える車載ネットワークシステム１０のバス５００ａに不正なＥＣＵが接続された場合について、バス５００ａに接続された不正検知ＥＣＵ１００ａ、ＥＣＵ４００ａ、ＥＣＵ４００ｂ、ゲートウェイ３００等の動作について説明する。

【００９５】

図１８は、不正検知ＥＣＵ１００ａが不正なフレーム（メッセージ）を検知して、他のＥＣＵによりその不正なフレームに対応した処理がなされることを阻止する動作例を示すシーケンス図である。同図では、不正なＥＣＵが、バス５００ａにメッセージＩＤが「４

」でデータフィールド（データ）が「２５５（０ｘＦＦ）」となるデータフレームを送信する場合の例を示している。ここでの各シーケンスは、各種装置における各処理手順（ステップ）を意味する。

【００９６】

まず、不正なＥＣＵは、メッセージＩＤが「４」、データが「２５５（０ｘＦＦ）」となるデータフレームの送信を開始する（シーケンスＳ１００１）。フレームを構成する各ビットの値は、上述したデータフレームフォーマットに従ってＳＯＦ、ＩＤフィールド（メッセージＩＤ）といった順に逐次バス５００ａ上に送出される。

【００９７】

不正なＥＣＵがＩＤフィールド（メッセージＩＤ）までをバス５００ａに送出し終えたときにおいて、不正検知ＥＣＵ１００ａ、ＥＣＵ４００ａ、ＥＣＵ４００ｂ及びゲートウェイ３００はそれぞれメッセージＩＤを受信する（シーケンスＳ１００２）。

【００９８】

ＥＣＵ４００ａ、ＥＣＵ４００ｂ及びゲートウェイ３００はそれぞれ、保持している受信ＩＤリストを用いてメッセージＩＤをチェックする（シーケンスＳ１００３）。このとき、不正検知ＥＣＵ１００ａは、保持している正規ＩＤリストを用いてメッセージＩＤをチェックする（シーケンスＳ１００４）。即ち、不正検知ＥＣＵ１００ａは、送信されたフレームにおけるＩＤフィールドの内容が、不正を示す所定条件（正規ＩＤリストに掲載されていないこと）に該当するか否かを判定する。

【００９９】

シーケンスＳ１００３において、ＥＣＵ４００ａ及びＥＣＵ４００ｂは、それぞれが保持している受信ＩＤリストに「４」が含まれていないため（図９参照）、受信を終了する。つまりこれ以上不正なＥＣＵが送信を継続するフレームの解釈をせずフレームに対応した処理を行わない。また、シーケンスＳ１００３においてゲートウェイ３００は、保持している受信ＩＤリストに「４」が含まれているため（図５参照）、受信を継続する。また、シーケンスＳ１００４において不正検知ＥＣＵ１００ａは、保持している正規ＩＤリストに「４」が含まれていないため、不正なメッセージＩＤであると判断して、続いてエラーフレームの発行準備を開始する（シーケンスＳ１００５）。

【０１００】

シーケンスＳ１００３に続いて、ゲートウェイ３００はフレームの受信を継続する。例えば、不正検知ＥＣＵ１００ａがエラーフレームの発行準備をしている間に、不正なＥＣＵからはバス５００ａ上にＩＤフィールドより後の部分であるＲＴＲ、コントロールフィールド（ＩＤＥ、ｒ、ＤＬＣ）が逐次送出され、続いてデータフィールドが１ビットずつ逐次送出される。ゲートウェイ３００はこのＲＴＲ、コントロールフィールド（ＩＤＥ、ｒ、ＤＬＣ）を受信し、続いてデータフィールドの受信を開始する（シーケンスＳ１００６）。

【０１０１】

次にエラーフレームの発行準備が終わって、不正検知ＥＣＵ１００ａがエラーフレームを送信する（シーケンスＳ１００７）。このエラーフレームの送信は、不正なフレームの最後尾が送信される前（例えばＣＲＣシーケンスの最後尾が送信される前等）に行われる。この動作例においては、データフィールドの途中で行われる。このエラーフレームの送信が開始されることによりバス５００ａでは、不正なＥＣＵから送信中のフレームのデータフィールドの途中部分がエラーフレーム（優先されるドミナントのビット列）により上書きされることになる。

【０１０２】

シーケンスＳ１００７において送信されたエラーフレームを受信したゲートウェイ３００は、データフィールドの受信途中で不正なＥＣＵが送信していたフレームの受信を中止する（シーケンスＳ１００８）。つまり、ゲートウェイ３００は、不正なＥＣＵからのデータフィールドがエラーフレームで上書きされており、エラーフレームを検出するので、不正なＥＣＵが送信していたフレームの受信を継続しない。

【０１０３】
不正検知ＥＣＵ１００ａは、エラーフレームを送信する対象となったデータフレームのメッセージＩＤ「４」に対応する不正検知カウンタをインクリメントする（シーケンスＳ１００９）。
【０１０４】
インクリメントした結果としてメッセージＩＤ「４」に対応する不正検知カウンタが１７以上となった場合、不正検知ＥＣＵ１００ａは、ヘッドユニット２００に受信されるようにエラー表示を通知するフレーム（エラー表示メッセージ）を送信する（シーケンスＳ１０１０）。この結果としてヘッドユニット２００のフレーム処理部２２０によってエラー表示のための処理がなされＬＣＤ等を介してエラーが報知される。なお、エラーの報知は、ＬＣＤ等への表示の他、音声出力、発光等によるものでも良い。
【０１０５】
［１．１９　実施の形態１の効果］
実施の形態１で示した不正検知ＥＣＵは、送信されたフレーム（データフレーム）が不正なフレームか否かを、フレームのＩＤフィールドについて正規ＩＤリストを用いて判定する。これにより、データフレームにおけるＩＤフィールドによって不正を判定できるため、既存のノード（つまり不正検知ＥＣＵ及び不正なＥＣＵ以外のＥＣＵ）において不正なフレームが解釈されてそのフレームに対応する処理が実行されることを阻止できる。また、データフレームの先頭のＳＯＦに続くＩＤフィールドまで受信するだけで判定ができるため、データフレームの後部等を受信して判定を行う場合よりも、バスのトラフィックを抑えることが可能となる。
【０１０６】
また、不正検知ＥＣＵが、不正検知カウンタを用いてエラーフレームを送信した回数をカウントすることで、エラーフレームの受信により不正なメッセージＩＤを送信するノードにおける送信エラーカウンタがＣＡＮプロトコルに従えばパッシブ状態に遷移すべき上限値まで到達していることを検出することができる。これにより、不正なメッセージＩＤを送信するノードが、ＣＡＮプロトコルのエラーカウンタの仕様に準拠しているか否かを判定することが可能となる。
【０１０７】
また、不正なフレームの判定を行うノードを不正検知ＥＣＵのみとすることで、既存のネットワーク構成への影響を最小限に抑えることができ、システム全体として処理量、消費電力量を抑えることができる。
【０１０８】
（実施の形態２）
以下、本開示の実施の形態として、メッセージＩＤ毎に許容されるデータ範囲に基づいて、他のノード（ＥＣＵ）において不正なフレームに基づく処理が実行されることを阻止するための不正対処方法を実現する不正検知ＥＣＵを含む車載ネットワークシステム１１について説明する。
【０１０９】
［２．１　車載ネットワークシステム１１の全体構成］
図１９は、実施の形態２に係る車載ネットワークシステム１１の全体構成を示す図である。車載ネットワークシステム１１は、実施の形態１で示した車載ネットワークシステム１０の一部を変形したものである。車載ネットワークシステム１１は、バス５００ａ、５００ｂと、不正検知ＥＣＵ２１００ａ、２１００ｂ、ヘッドユニット２００、ゲートウェイ３００、及び、各種機器に接続されたＥＣＵ４００ａ～４００ｄ等のＥＣＵといったバスに接続された各ノードとを含んで構成される。車載ネットワークシステム１１の構成要素のうち、実施の形態１と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。
【０１１０】
不正検知ＥＣＵ２１００ａ、２１００ｂは、それぞれバス５００ａ、バス５００ｂに接

続され、ＥＣＵ４００ａ～４００ｄ等により送信されたフレームが不正であるかどうかを判定し、不正であればエラーフレームを送信する機能を有するＥＣＵである。

【０１１１】

［２．２　不正検知ＥＣＵ２１００ａの構成］

図２０は、不正検知ＥＣＵ２１００ａの構成図である。不正検知ＥＣＵ２１００ａは、フレーム送受信部１６０と、フレーム解釈部２１５０と、不正フレーム検知部２１３０と、データ範囲リスト保持部２１２０と、不正検知カウンタ保持部１１０と、フレーム生成部１４０とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、不正検知ＥＣＵ２１００ａにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。不正検知ＥＣＵ２１００ａは、実施の形態１で示した不正検知ＥＣＵ１００ａの一部を変形したものであり、実施の形態１と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。なお、不正検知ＥＣＵ２１００ｂも不正検知ＥＣＵ２１００ａと同様の構成を備える。

【０１１２】

フレーム解釈部２１５０は、実施の形態１で示したフレーム解釈部１５０を変形したものであり、フレーム送受信部１６０よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。フレームがデータフレームであると判断した場合においてデータフィールドと判断した値（データ）は、ＩＤフィールドのＩＤ（メッセージＩＤ）と共に、不正フレーム検知部２１３０へ転送する。また、フレーム解釈部２１５０は、ＣＡＮプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部１４０へ通知する。また、フレーム解釈部２１５０は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

【０１１３】

不正フレーム検知部２１３０は、実施の形態１で示した不正フレーム検知部１３０を変形したものであり、フレーム解釈部２１５０から通知されるメッセージＩＤと、データフィールドの値（データ）を受け取り、これらの値が不正を示す所定条件に該当するか否かを判定する。即ち不正フレーム検知部２１３０は、受信されたフレームにおける所定フィールドの内容が不正を示す所定条件に該当するか否かを判定する言わば判定部として機能する。この不正を示す所定条件は、データが、データ範囲リスト保持部２１２０が保持しているデータ範囲リストにメッセージＩＤと対応付けて載っているデータ範囲に入らないという条件である。不正フレーム検知部２１３０は、データ範囲リスト保持部２１２０に保持しているメッセージＩＤ毎のデータ範囲を定めたリストであるデータ範囲リストに従い、不正かどうかの判定を行う。不正フレーム検知部２１３０は、データ範囲リストで示される範囲以外のデータを受信した場合は、不正の検知回数をインクリメントするために、受信したメッセージＩＤを不正検知カウンタ保持部１１０へ通知する。この不正の検知回数が一定回数以上に達した場合において、ヘッドユニット２００で受信されるようにエラー表示メッセージを送信するための制御については実施の形態１で説明した通りであるため、ここでの説明を省略する。また、データ範囲リストで示される範囲以外のデータを受信した場合は、エラーフレームを送信するように、フレーム生成部１４０へ通知する。

【０１１４】

データ範囲リスト保持部２１２０は、車載ネットワークシステム１１においてバス上を送信されるデータフレームに含まれるデータ（データフィールドの値）について許容される範囲を予め規定したリストであるデータ範囲リストを保持する（図２１参照）。

【０１１５】

［２．３　データ範囲リスト例］

図２１は、不正検知ＥＣＵ２１００ａのデータ範囲リスト保持部２１２０に保持されるデータ範囲リストの一例を示した図である。このデータ範囲リストは、各ＩＤ（メッセージＩＤ）と、そのメッセージＩＤのデータフレームにおけるデータフィールドの値（デー

タ）として許容されるデータ範囲とを対応付けたものである。図２１の例では、メッセージＩＤが「１」のデータフレームについては、データ範囲「０～１８０」、メッセージＩＤが「２」又は「４」のデータフレームについては、データ範囲「０～１００」、メッセージＩＤが「３」のデータフレームについて、データ範囲「０、１」をそれぞれ正常としている。

【０１１６】

［２．４　不正フレームの検知に係るシーケンス］

以下、上述の構成を備える車載ネットワークシステム１１のバス５００ａに不正なＥＣＵが接続された場合について、バス５００ａに接続された不正検知ＥＣＵ２１００ａ、ＥＣＵ４００ａ、ＥＣＵ４００ｂ、ゲートウェイ３００等の動作について説明する。

【０１１７】

図２２及び図２３は、不正検知ＥＣＵ２１００ａが不正なフレーム（メッセージ）を検知して、他のＥＣＵによりその不正なフレームに対応した処理がなされることを阻止する動作例を示すシーケンス図である。図２２及び図２３では、実施の形態１で示した図１８の場合と同様に、不正なＥＣＵが、バス５００ａにメッセージＩＤが「４」でデータフィールド（データ）が「２５５（０ｘＦＦ）」となるデータフレームを送信する場合の例を示している。実施の形態１で示したシーケンスと同じシーケンスには同じ符号を付しており、ここでは説明を簡略化する。

【０１１８】

まず、不正なＥＣＵは、不正なデータフレームの送信を開始する（シーケンスＳ１００１）。不正検知ＥＣＵ２１００ａ、ＥＣＵ４００ａ、ＥＣＵ４００ｂ及びゲートウェイ３００はそれぞれメッセージＩＤを受信する（シーケンスＳ１００２）。ＥＣＵ４００ａ、ＥＣＵ４００ｂ及びゲートウェイ３００はそれぞれ、保持している受信ＩＤリストを用いてメッセージＩＤをチェックする（シーケンスＳ１００３）。ＥＣＵ４００ａ及びＥＣＵ４００ｂは、それぞれが保持している受信ＩＤリストに「４」が含まれていないため（図９参照）、受信を終了する。ゲートウェイ３００は、保持している受信ＩＤリストに「４」が含まれているため（図５参照）、受信を継続しデータフィールドの受信を行う（シーケンスＳ１００６ａ）。同様に不正検知ＥＣＵ２１００ａもデータフィールドの受信を行う（シーケンスＳ１００６ａ）。

【０１１９】

シーケンスＳ１００６ａに続いて、不正検知ＥＣＵ２１００ａは、データ範囲リスト（図２１参照）を用いて、データフィールドのデータをチェックする（シーケンスＳ２００１）。即ち、不正検知ＥＣＵ２１００ａは、送信されたフレームにおけるＩＤフィールドの内容が、不正を示す所定条件（データ範囲リストに記載されているデータの範囲に入らないこと）に該当するか否かを判定する。不正検知ＥＣＵ２１００ａは、データ範囲リストにおいてＩＤ「４」に対応する「２５５（０ｘＦＦ）」の値が記載されていないため、不正なデータフレームであると判断し、続いてエラーフレームの発行準備を開始する（シーケンスＳ１００５）。

【０１２０】

不正検知ＥＣＵ２１００ａがエラーフレームの発行準備をしている間に、不正なＥＣＵからはバス５００ａ上にデータフィールドより後の部分であるＣＲＣフィールド（ＣＲＣシーケンス及びＣＲＣデリミタ）が１ビットずつ逐次送出される。ゲートウェイ３００はこのＣＲＣフィールドの受信を開始する（シーケンスＳ２００２）。

【０１２１】

次にエラーフレームの発行準備が終わって、不正検知ＥＣＵ２１００ａがエラーフレームを送信する（シーケンスＳ１００７）。このエラーフレームの送信が開始されることによりバス５００ａでは、不正なＥＣＵから送信中のフレームのＣＲＣシーケンスの途中部分がエラーフレーム（優先されるドミナントのビット列）により上書きされることになる。

【０１２２】

シーケンスＳ１００７において送信されたエラーフレームを受信したゲートウェイ３００は、ＣＲＣシーケンスを含むＣＲＣフィールドの受信途中で、不正なＥＣＵが送信していたデータフレームの受信を中止する（シーケンスＳ２００３）。つまり、ゲートウェイ３００は、不正なＥＣＵからのＣＲＣシーケンスがエラーフレームで上書きされており、エラーフレームを検出するので、不正なＥＣＵが送信していたデータフレームの受信を継続しない。

【０１２３】

不正検知ＥＣＵ２１００ａは、エラーフレームを送信する対象となったデータフレームのＩＤ「４」に対応する不正検知カウンタをインクリメントする（シーケンスＳ１００９）。インクリメントした結果としてＩＤ「４」に対応する不正検知カウンタが１７以上となった場合、不正検知ＥＣＵ２１００ａは、エラー表示メッセージを送信する（シーケンスＳ１０１０）。

【０１２４】

［２．５　実施の形態２の効果］

実施の形態２で示した不正検知ＥＣＵは、送信されたフレームが不正なフレームか否かを、フレーム（データフレーム）のＩＤフィールド及びデータフィールドについてデータ範囲リストを用いて判定する。これにより、データフレームにおけるＩＤフィールドとデータフィールドとの組み合わせによって不正を判定できるため、既存のＥＣＵ（つまり不正検知ＥＣＵ及び不正なＥＣＵ以外のＥＣＵ）において不正なフレームが解釈されてそのフレームに対応する処理が実行されることを阻止することができる。また、データフレームのデータフィールドまで受信するだけで判定ができるため、データフレームの後部を受信して判定を行う場合よりも、バスのトラフィックを抑えることが可能となる。

【０１２５】

また、不正検知ＥＣＵが、不正検知カウンタを用いてエラーフレームを送信した回数をカウントすることで、エラーフレームの受信により不正なメッセージＩＤを送信するノードにおける送信エラーカウンタがＣＡＮプロトコルに従えばパッシブ状態に遷移すべき上限値まで到達していることを検出することができる。これにより、不正なメッセージＩＤを送信するノードが、ＣＡＮプロトコルのエラーカウンタの仕様に準拠しているか否かを判定することが可能となる。

【０１２６】

また、不正なフレームの判定を行うノードを不正検知ＥＣＵのみとすることで、既存のネットワーク構成への影響を最小限に抑えることができ、システム全体として処理量、消費電力量を抑えることができる。

【０１２７】

（実施の形態３）

以下、本開示の実施の形態として、メッセージＩＤ、データ及びカウンタ値から算出されるメッセージ認証コード（ＭＡＣ：Message Authentication Code）を用いて、他のノード（ＥＣＵ）において不正なフレームに基づく処理が実行されることを阻止するための不正対処方法を実現する不正検知ＥＣＵを含む車載ネットワークシステム１２について説明する。

【０１２８】

［３．１　車載ネットワークシステム１２の全体構成］

図２４は、実施の形態３に係る車載ネットワークシステム１２の全体構成を示す図である。車載ネットワークシステム１２は、実施の形態１で示した車載ネットワークシステム１０の一部を変形したものである。車載ネットワークシステム１２は、バス５００ａ、５００ｂと、不正検知ＥＣＵ３１００ａ、３１００ｂ、ヘッドユニット２００、ゲートウェイ３００、及び、各種機器に接続されたＥＣＵ３４００ａ～３４００ｄ等のＥＣＵといったバスに接続された各ノードとを含んで構成される。車載ネットワークシステム１２の構成要素のうち、実施の形態１と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。

【０１２９】
不正検知ＥＣＵ３１００ａ、３１００ｂは、それぞれバス５００ａ、バス５００ｂに接続され、ＥＣＵ３４００ａ～３４００ｄ等により送信されたフレームが不正であるかどうかを判定し、不正であればエラーフレームを送信する機能を有するＥＣＵである。
【０１３０】
ＥＣＵ３４００ａ～３４００ｄは、いずれかのバスと接続され、また、それぞれエンジン４０１、ブレーキ４０２、ドア開閉センサ４０３、窓開閉センサ４０４に接続されている。ＥＣＵ３４００ａ～３４００ｄのそれぞれは、接続されている機器（エンジン４０１等）の状態を取得し、定期的に状態を表すデータフレームをネットワーク（つまりバス）に送信している。送信されるデータフレームのデータフィールドには、メッセージＩＤとデータ値と送信毎にインクリメントされるカウンタ値とから計算により導出されるメッセージ認証コード（ＭＡＣ）が付与される。
【０１３１】
［３．２　ＥＣＵ３４００ａの構成］
図２５は、ＥＣＵ３４００ａの構成図である。ＥＣＵ３４００ａは、フレーム送受信部４６０と、フレーム解釈部４５０と、受信ＩＤ判断部４３０と、受信ＩＤリスト保持部４４０と、フレーム処理部４１０と、フレーム生成部３４２０と、データ取得部４７０と、ＭＡＣ生成部３４１０と、ＭＡＣ鍵保持部３４３０と、カウンタ保持部３４４０とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、ＥＣＵ３４００ａにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。ＥＣＵ３４００ａは、実施の形態１で示したＥＣＵ４００ａの一部を変形したものであり、実施の形態１と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。
【０１３２】
フレーム生成部３４２０は、実施の形態１で示したフレーム生成部４２０の一部を変形したものである。フレーム生成部３４２０は、フレーム解釈部４５０から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部４６０へ通知して送信させる。また、フレーム生成部３４２０は、データ取得部４７０より通知されたデータの値と予め定められたメッセージＩＤとをＭＡＣ生成部３４１０へ通知して、算出されたＭＡＣを受け取る。フレーム生成部３４２０は、予め定められたメッセージＩＤとデータ取得部４７０より通知されたデータの値とＭＡＣ生成部３４１０から受け取ったＭＡＣとを含むようにフレームを構成し（図２６参照）、フレーム送受信部４６０へ通知する。
【０１３３】
ＭＡＣ生成部３４１０は、フレーム生成部３４２０より通知されるメッセージＩＤとデータの値と、カウンタ保持部３４４０で保持するカウンタ値とを結合した値（結合値）に対し、ＭＡＣ鍵保持部３４３０で保持するＭＡＣ鍵を用いて、ＭＡＣを算出（計算により導出）して、この算出した結果であるＭＡＣをフレーム生成部３４２０へと通知する。ここではＭＡＣの計算方法として、ＨＭＡＣ（Hash-based Message Authentication Code）（非特許文献２参照）を採用し、上述した結合値に対し、所定のブロック分（例えば４Ｂｙｔｅｓ）までパディングした値でＭＡＣ鍵を使って計算し、出てきた計算結果の先頭４ｂｙｔｅｓをＭＡＣとする。なお、ここでは、ＭＡＣを算出するために用いる結合値は、メッセージＩＤとデータの値とカウンタ保持部３４４０で保持するカウンタ値とを使用しているが、これらの３つのうち、いずれか１つ又は２つの組み合わせを用いてＭＡＣを算出しても良い。
【０１３４】
ＭＡＣ鍵保持部３４３０は、ＭＡＣを計算するため必要となるＭＡＣ鍵を保持する。
【０１３５】
カウンタ保持部３４４０は、ＭＡＣを計算するために必要となるカウンタ値を保持する。なお、このカウンタ値は、フレーム送受信部４６０においてデータフレームが正常に送

信された度にインクリメントされる。
【０１３６】
なお、ＥＣＵ３４００ｂ～３４００ｄは、それぞれ実施の形態１で示したＥＣＵ４００ｂ～４００ｄの一部を変形したものであり、上述したＥＣＵ３４００と基本的に同様の構成を備える。但し、受信ＩＤリスト保持部４４０に保持される受信ＩＤリストはＥＣＵ毎に異なる内容となり得る。例えばＥＣＵ３４００ａ及びＥＣＵ３４００ｂは図９に例示する受信ＩＤリストを保持し、ＥＣＵ３４００ｃ及びＥＣＵ３４００ｄは図５に例示する受信ＩＤリストを保持する。また、フレーム処理部４１０の処理内容は、実施の形態１で示したようにＥＣＵ毎に異なる。以下、ＥＣＵ３４００ａ～３４００ｄのそれぞれが送信するフレームの内容について図２６～図２９を用いて説明する。
【０１３７】
［３．３　エンジンに係るＥＣＵ３４００ａの送信フレーム例］
図２６は、エンジン４０１に接続されたＥＣＵ３４００ａから送信されるデータフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ３４００ａが送信するフレームのメッセージＩＤは「１」である。データは、同図において１バイト毎に空白で区分して表しており、先頭の１ｂｙｔｅが時速（ｋｍ／時）を表し、次の１ｂｙｔｅはカウンタ値を表し、次の４ｂｙｔｅｓがＭＡＣを表す。なお、図２６の例においてＭＡＣは１６進数で表記している。先頭１ｂｙｔｅの時速（ｋｍ／時）は、最低０（ｋｍ／時）～最高１８０（ｋｍ／時）までの範囲の値を取る。図２６の上行から下行へと、ＥＣＵ３４００ａから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、カウンタ値が次第に増加し、時速が０ｋｍ／時から１ｋｍ／時ずつ加速されている様子を表している。
【０１３８】
［３．４　ブレーキに係るＥＣＵ３４００ｂの送信フレーム例］
図２７は、ブレーキ４０２に接続されたＥＣＵ３４００ｂから送信されるデータフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ３４００ｂが送信するフレームのメッセージＩＤは「２」である。データは、同図において１バイト毎に空白で区分して表しており、先頭の１ｂｙｔｅがブレーキのかかり具合を割合（％）で表し、次の１ｂｙｔｅはカウンタ値を表し、次の４ｂｙｔｅｓがＭＡＣを表す。なお、図２７の例においてＭＡＣは１６進数で表記している。先頭１ｂｙｔｅのブレーキのかかり具合は、ブレーキを全くかけていない状態を０（％）、ブレーキを最大限かけている状態を１００（％）としたものである。図２７の上行から下行へと、ＥＣＵ３４００ｂから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、カウンタ値が次第に増加し、ブレーキについては１００％から徐々にブレーキを弱めている様子を表している。
【０１３９】
［３．５　ドア開閉センサに係るＥＣＵ３４００ｃの送信フレーム例］
図２８は、ドア開閉センサ４０３に接続されたＥＣＵ３４００ｃから送信されるデータフレームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ３４００ｃが送信するフレームのメッセージＩＤは「３」である。データは、同図において１バイト毎に空白で区分して表しており、先頭の１Ｂｙｔｅがドアの開閉状態を表し、次の１ｂｙｔｅはカウンタ値を表し、次の４ｂｙｔｅｓがＭＡＣを表す。なお、図２８の例においてＭＡＣは１６進数で表記している。先頭１ｂｙｔｅのドアの開閉状態は、ドアが開いている状態を「１」、ドアが閉まっている状態を「０」としたものである。図２８の上行から下行へと、ＥＣＵ３４００ｃから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、カウンタ値が次第に増加し、ドアが開いている状態から次第に閉められた状態へと移った様子を表している。
【０１４０】
［３．６　窓開閉センサに係るＥＣＵ３４００ｄの送信フレーム例］
図２９は、窓開閉センサ４０４に接続されたＥＣＵ３４００ｄから送信されるデータフ

レームにおけるＩＤ（メッセージＩＤ）及びデータフィールド（データ）の一例を示す図である。ＥＣＵ３４００ｄが送信するフレームのメッセージＩＤは「４」である。データは、同図において１バイト毎に空白で区分して表しており、先頭の１Ｂｙｔｅが窓の開閉状態を割合（％）で表し、次の１ｂｙｔｅはカウンタ値を表し、次の４ｂｙｔｅｓがＭＡＣを表す。なお、図２９の例においてＭＡＣは１６進数で表記している。先頭１ｂｙｔｅの窓の開閉状態は、窓が完全に閉まっている状態を０（％）、窓が全開の状態を１００（％）としたものである。図２９の上行から下行へと、ＥＣＵ３４００ｄから逐次送信される各フレームに対応する各メッセージＩＤ及びデータを例示しており、カウンタ値が次第に増加し、窓が閉まっている状態から徐々に開いていく様子を表している。

【０１４１】

［３．７　不正検知ＥＣＵ３１００ａの構成］

図３０は、不正検知ＥＣＵ３１００ａの構成図である。不正検知ＥＣＵ３１００ａは、フレーム送受信部１６０と、フレーム解釈部３１５０と、不正ＭＡＣ検知部３１３０と、ＭＡＣ鍵保持部３１８０と、カウンタ保持部３１９０と、フレーム生成部１４０と、ＭＡＣ生成部３１７０と、不正検知カウンタ保持部１１０から構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、不正検知ＥＣＵ３１００ａにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。不正検知ＥＣＵ３１００ａは、実施の形態１で示した不正検知ＥＣＵ１００ａの一部を変形したものであり、実施の形態１と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。なお、不正検知ＥＣＵ３１００ｂも同様の構成である。

【０１４２】

フレーム解釈部３１５０は、実施の形態１で示したフレーム解釈部１５０を変形したものであり、フレーム送受信部１６０よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。フレームがデータフレームであると判断した場合においてデータフィールドと判断した値（データ）は、ＩＤフィールドのＩＤ（メッセージＩＤ）と共に、不正ＭＡＣ検知部３１３０へ転送する。また、フレーム解釈部３１５０は、ＣＡＮプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部１４０へ通知する。また、フレーム解釈部３１５０は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

【０１４３】

不正ＭＡＣ検知部３１３０は、フレーム解釈部３１５０から通知されるメッセージＩＤと、データフィールドの値（データ）を受け取ってデータフィールド中のＭＡＣを検証する機能を有する。不正ＭＡＣ検知部３１３０は、通知されたメッセージＩＤ及びデータフィールドの値を、ＭＡＣ生成部３１７０へと通知し、ＭＡＣ生成部３１７０により生成されたＭＡＣを取得する。不正ＭＡＣ検知部３１３０は、データフィールドのデータが不正を示す所定条件に該当するか否かを判定する。即ち不正ＭＡＣ検知部３１３０は、受信されたフレームにおける所定フィールドの内容が不正を示す所定条件に該当するか否かを判定する言わば判定部として機能する。この不正を示す所定条件は、定められた検証処理手順（ＭＡＣの生成、ＭＡＣの比較等を含む手順）での検証に失敗することであり、つまり、データに含まれるＭＡＣが、ＭＡＣ生成部３１７０により生成されたＭＡＣと相違するという条件である。不正ＭＡＣ検知部３１３０は、ＭＡＣ生成部３１７０から取得したＭＡＣと、データフィールド中のＭＡＣとを比較することで、不正かどうかの判定（即ちＭＡＣの検証）を行う。両ＭＡＣの値の比較の結果、不一致の場合は、不正の検知回数をインクリメントするために、受信したメッセージＩＤを不正検知カウンタ保持部１１０へ通知する。この不正の検知回数が一定回数以上に達した場合において、ヘッドユニット２００で受信されるようにエラー表示メッセージを送信するための制御については実施の形態１で説明した通りであるため、ここでの説明を省略する。また、両ＭＡＣの値の比較の結果、不一致の場合は、エラーフレームを送信するように、フレーム生成部１４０へ通知す

る。ＭＡＣ値の比較の結果、一致する場合は、カウンタ保持部３１９０が保持する、メッセージＩＤに対応するカウンタ値をインクリメントするようにＭＡＣ生成部３１７０へ通知する。

【０１４４】

ＭＡＣ生成部３１７０は、不正ＭＡＣ検知部３１３０より通知されたメッセージＩＤを使って、ＭＡＣ鍵保持部３１８０より、対応するＭＡＣ鍵を取得し、カウンタ保持部３１９０より対応するカウンタをそれぞれ取得する。ＭＡＣ生成部３１７０は、不正ＭＡＣ検知部３１３０より通知されたデータフィールドの値（先頭１Ｂｙｔｅの値）と、カウンタ保持部３１９０より取得したカウンタ値に対して、ＭＡＣ鍵保持部３１８０より取得したＭＡＣ鍵を使ってＭＡＣを算出（計算により導出）し、算出したＭＡＣを不正ＭＡＣ検知部３１３０へ通知する。なお、不正検知ＥＣＵ３１００ａ、３１００ｂ及びＥＣＵ３４００ａ～３４００ｄのいずれにおいても、ＭＡＣ鍵を用いてＭＡＣを算出するアルゴリズムは同一のものを用いる。

【０１４５】

ＭＡＣ鍵保持部３１８０は、ＭＡＣを計算するため必要となるＭＡＣ鍵をメッセージＩＤ毎に対応付けて保持する。このＭＡＣ鍵保持部３１８０が保持するＭＡＣ鍵は、対応付けられたメッセージＩＤ毎に異なる値である。なお、ＥＣＵ及び不正検知ＥＣＵにおいて用いられるＭＡＣ鍵は、１つの送信ノードが複数のメッセージＩＤそれぞれのフレームを送信する場合を想定すると、送信ノード毎に異なる鍵であることとしても良い。また、ＭＡＣ鍵は、例えば同一のバス上で送信されるフレームに同一の値が用いられるようにしても良いし、異なるバス上であっても同一の鍵（値）としても良いし、車一台あたり同一の鍵としても良く、同一車種で同一の鍵としても良く、同一製造メーカ毎に同一の鍵としても良く、異なる製造メーカであっても同一の鍵としても良い。

【０１４６】

カウンタ保持部３１９０は、ＭＡＣ値を計算するために必要となるカウンタ値をメッセージＩＤ毎に保持する。このカウンタ値は、フレームを正常に受信した場合（つまり不正ＭＡＣ検知部３１３０において比較した両ＭＡＣが一致する場合）には、インクリメントされる。

【０１４７】

［３．８　カウンタ値の例］

図３１は、カウンタ保持部３１９０に保持されているメッセージＩＤ毎のカウンタ値の一例を示す図である。同図では、メッセージＩＤが「１」のカウンタが１回、メッセージＩＤが「２」のカウンタが１０回、メッセージＩＤが「３」のカウンタが１５回、メッセージＩＤが「４」のカウンタが１００回をそれぞれ示している。この各メッセージＩＤに対応するカウンタ値は、そのメッセージＩＤを含むフレームが正常に受信されている回数を表している。

【０１４８】

［３．９　不正フレームの検知に係るシーケンス］

以下、上述の構成を備える車載ネットワークシステム１２のバス５００ａに不正なＥＣＵが接続された場合について、バス５００ａに接続された不正検知ＥＣＵ３１００ａ、ＥＣＵ３４００ａ、ＥＣＵ３４００ｂ、ゲートウェイ３００等の動作について説明する。

【０１４９】

図３２及び図３３は、不正検知ＥＣＵ３１００ａが不正なフレーム（メッセージ）を検知して、他のＥＣＵによりその不正なフレームに対応した処理がなされることを阻止する動作例を示すシーケンス図である。図３２及び図３３では、実施の形態１で示した図１８並びに実施の形態２で示した図２２及び図２３の場合と同様に、不正なＥＣＵが、バス５００ａに接続された例を示している。この不正なＥＣＵは、メッセージＩＤが「４」でデータフィールド（データ）が「０ｘＦＦ　ＦＦ　ＦＦＦＦＦＦＦＦ」（６Ｂｙｔｅ）となるデータフレームを送信する。実施の形態１又は２で示したシーケンスと同じシーケンスには同じ符号を付しており、ここでは説明を簡略化する。

【０１５０】
まず、不正なＥＣＵは、上述した不正なデータフレームの送信を開始する（シーケンスＳ１００１ａ）。不正検知ＥＣＵ３１００ａ、ＥＣＵ３４００ａ、ＥＣＵ３４００ｂ及びゲートウェイ３００はそれぞれメッセージＩＤを受信する（シーケンスＳ１００２）。ＥＣＵ３４００ａ、ＥＣＵ３４００ｂ及びゲートウェイ３００はそれぞれ、保持している受信ＩＤリストを用いてメッセージＩＤをチェックする（シーケンスＳ１００３）。ＥＣＵ３４００ａ及びＥＣＵ３４００ｂは、それぞれが保持している受信ＩＤリストに「４」が含まれていないため（図９参照）、受信を終了する。ゲートウェイ３００は、保持している受信ＩＤリストに「４」が含まれているため（図５参照）、受信を継続しデータフィールドの受信を行う（シーケンスＳ１００６ａ）。同様に不正検知ＥＣＵ３１００ａもデータフィールドの受信を行う（シーケンスＳ１００６ａ）。

【０１５１】
シーケンスＳ１００６ａに続いて、不正検知ＥＣＵ３１００ａは、データフィールドにおけるデータに含まれるＭＡＣを検証（チェック）する（シーケンスＳ３００１）。即ち、不正検知ＥＣＵ３１００ａは、送信されたフレームにおけるＩＤフィールドの内容が、不正を示す所定条件（ＭＡＣの検証に失敗すること）に該当するか否かを判定する。不正検知ＥＣＵ３１００ａは、不正なＥＣＵにより送信されたデータフレームにおけるデータフィールドの６Ｂｙｔｅのデータ「０ｘＦＦＦＦＦＦＦＦ」について、後半４ＢｙｔｅのＭＡＣと、メッセージＩＤ「４」に対応するＭＡＣ鍵とカウンタを用いて算定したＭＡＣとを比較することでＭＡＣの検証を行う。この比較の結果は不一致になり検証が失敗するので、不正検知ＥＣＵ３１００ａでは、不正なデータフレームであると判断し、続いてエラーフレームの発行準備を開始する（シーケンスＳ１００５）。

【０１５２】
不正検知ＥＣＵ３１００ａがエラーフレームの発行準備をしている間に、ゲートウェイ３００はＣＲＣフィールドの受信を開始する（シーケンスＳ２００２）。

【０１５３】
次にエラーフレームの発行準備が終わって、不正検知ＥＣＵ３１００ａがエラーフレームを送信する（シーケンスＳ１００７）。このエラーフレームの送信が開始されることによりバス５００ａでは、不正なＥＣＵから送信中のフレームのＣＲＣシーケンスの途中部分がエラーフレームにより上書きされることになる。

【０１５４】
シーケンスＳ１００７において送信されたエラーフレームを受信したゲートウェイ３００は、ＣＲＣシーケンスを含むＣＲＣフィールドの受信途中で、不正なＥＣＵが送信していたデータフレームの受信を中止する（シーケンスＳ２００３）。

【０１５５】
不正検知ＥＣＵ３１００ａは、エラーフレームを送信する対象となったデータフレームのＩＤ「４」に対応する不正検知カウンタをインクリメントする（シーケンスＳ１００９）。インクリメントした結果としてＩＤ「４」に対応する不正検知カウンタが１７以上となった場合、不正検知ＥＣＵ３１００ａは、エラー表示メッセージを送信する（シーケンスＳ１０１０）。

【０１５６】
［３．１０　実施の形態３の効果］
実施の形態３で示した不正検知ＥＣＵは、送信されたフレームが不正なフレームか否かを、フレーム（データフレーム）のデータフィールドに含ませたＭＡＣを検証することによって判定する。これにより、既存のＥＣＵ（つまり不正検知ＥＣＵ及び不正なＥＣＵ以外のＥＣＵ）において不正なフレームが解釈されてそのフレームに対応する処理が実行されることを阻止することができる。また、データフレームのデータフィールドまで受信するだけで判定ができるため、データフレームの後部を受信して判定を行う場合よりも、バスのトラフィックを抑えることが可能となる。

【０１５７】

また、不正検知ＥＣＵが、不正検知カウンタを用いてエラーフレームを送信した回数をカウントすることで、エラーフレームの受信により不正なメッセージＩＤを送信するノードにおける送信エラーカウンタがＣＡＮプロトコルに従えばパッシブ状態に遷移すべき上限値まで到達していることを検出することができる。これにより、不正なメッセージＩＤを送信するノードが、ＣＡＮプロトコルのエラーカウンタの仕様に準拠しているか否かを判定することが可能となる。

【０１５８】

また、ＭＡＣの検証を行うノードを不正検知ＥＣＵのみとすることで、不正検知ＥＣＵ以外のＥＣＵで検証する必要がなく、システム全体として処理量、消費電力量を抑えることができる。

【０１５９】

（他の実施の形態）

以上のように、本開示に係る技術の例示として実施の形態１～３を説明した。しかしながら、本開示に係る技術は、これに限定されず、適宜、変更、置き換え、付加、省略等を行った実施の形態にも適用可能である。例えば、以下のような変形例も本開示の一実施態様に含まれる。

【０１６０】

（１）上記実施の形態では、ＥＣＵ４００ａ～４００ｄ或いはＥＣＵ３４００ａ～３４００ｄによりフレームが定期的に送信される例を示したが、フレームは、状態変化を通知するイベントとして送信されることとしても良い。例えば、ＥＣＵは、ドアの開閉状態を定期的に送信するのではなく、ドアの開閉状態が変化した場合にのみ、フレームを送信するとしても良い。また、ＥＣＵがフレームを、定期的に送信、かつ、状態変化が発生した時に送信することとしても良い。

【０１６１】

（２）実施の形態３では、データ値とカウンタ値からＭＡＣを算出する例を示したが、データ値のみからＭＡＣを算出することとしても良い。またカウンタ値のみからＭＡＣを算出することとしても良い。また、フレームに含まれるＭＡＣのサイズは４ｂｙｔｅｓに制限されるものではなく、送信毎に異なるサイズであっても良い。同様に時速等のデータ値のサイズ及びカウンタ値のサイズも１ｂｙｔｅに制限されるものではない。また、必ずしもフレームにカウンタ値が含まれていなくても良い。

【０１６２】

（３）実施の形態３では、カウンタ値を送信毎にインクリメントする例を示したが、カウンタ値が時刻に応じて自動的にインクリメントされる値であっても良い。また、時刻そのものの値をカウンタの代わりに使用しても良い。即ち、データフレームが送信される度に変化する変数（カウンタ、時刻等）に基づいてＭＡＣが生成されるようにすると、ＭＡＣの不正な解読を困難化することが可能となる。また、実施の形態３では、不正検知ＥＣＵにおけるＭＡＣ生成部３１７０が、メッセージＩＤとデータフィールドの先頭１Ｂｙｔｅと、カウンタ保持部３１９０のカウンタ値とからＭＡＣ値を算出することとした。この代わりに、メッセージＩＤとデータフィールドの先頭１Ｂｙｔｅと、データフィールドの次の１Ｂｙｔｅであるカウンタ値とからＭＡＣ値を算出することとしても良い。また、不正ではないと判定されたデータフィールドにおけるカウンタ値に合わせるように、カウンタ保持部３１９０のカウンタ値を更新することとしても良い。

【０１６３】

（４）上記実施の形態では、ＣＡＮプロトコルにおけるデータフレームを標準ＩＤフォーマットで記述しているが、拡張ＩＤフォーマットで合っても良い。拡張ＩＤフォーマットの場合には、標準ＩＤフォーマットにおけるＩＤ位置のベースＩＤと、拡張ＩＤとを合わせて２９ビットでＩＤ（メッセージＩＤ）を表すので、この２９ビットのＩＤを上述の実施の形態におけるＩＤ（メッセージＩＤ）と扱えば良い。

【０１６４】

（５）上記実施の形態では、ＭＡＣ算出のアルゴリズムをＨＭＡＣとしているが、これ

ＣＢＣ－ＭＡＣ（Cipher Block Chaining Message Authentication Code）、ＣＭＡＣ（(Cipher-based MAC）であっても良い。また、ＭＡＣ計算に用いられるパディングについては、ゼロパディング、ＩＳＯ１０１２６、ＰＫＣＳ＃１、ＰＫＣＳ＃５、ＰＫＣＳ＃７、その他、ブロックのデータサイズが計算に必要となるパディングの方式であれば何でも良い。また４ｂｙｔｅｓ等のブロックへのサイズの変更方法についても、先頭、最後尾、中間のいずれの部分にパディングを行っても良い。また、ＭＡＣ算出に用いるデータは、連続しているデータ（例えば４ｂｙｔｅｓ分の連続データ）でなくても、特定のルールに従って１ｂｉｔずつ収集して結合したものでも良い。

【０１６５】

（６）上記実施の形態では、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も適用可能である。また、ＣＡＮプロトコルは、オートメーションシステム内の組み込みシステム等に用いられるＣＡＮＯｐｅｎ、或いは、ＴＴＣＡＮ（Time-Triggered CAN)、ＣＡＮＦＤ（CAN with Flexible Data Rate）等の派生的なプロトコルも包含する広義の意味のものと扱われるべきである。

【０１６６】

（７）上記実施の形態では、不正なＥＣＵがバスに接続される例を示したが、ＥＣＵ４００ａ～４００ｄ或いはＥＣＵ３４００ａ～３４００ｄのような既存のＥＣＵが何らかの要因によって不正なＥＣＵとして働く可能性もある。その場合であっても、上記実施の形態で示したように不正検知ＥＣＵが適切に不正なフレームを検知してエラーフレームを送信することで、他のＥＣＵが不正なフレームを処理してしまうことを阻止できる。

【０１６７】

（８）実施の形態２では、メッセージＩＤと許容されているデータ範囲とが対応付けられたデータ範囲リストを用いて、受信されたデータフレームのデータが、メッセージＩＤ毎に許容されているデータ範囲に含まれているか否かによって、不正か否かの判定を行うこととしたが、データ範囲リストにメッセージＩＤを含ませず、全てのメッセージＩＤに共通して許容されているデータ範囲（例えば「０～１８０」）を定めておき、メッセージＩＤにかかわらず不正か否かの判定を行うこととしても良い。また、不正検知ＥＣＵが保持するデータ範囲リストは、その不正検知ＥＣＵが接続されたバスにおいて送信され得るメッセージＩＤとデータ範囲とを対応付けたものとしても良い。これにより、データ範囲リストが、実施の形態１で示した正規ＩＤリストとしても用いることができるようになる。これを利用して実施の形態２に示した不正検知ＥＣＵにおいても実施の形態１で示したメッセージＩＤのチェック（シーケンスＳ１００４）を行うようにしても良い。

【０１６８】

（９）実施の形態２で示したメッセージＩＤと許容されているデータ範囲とが対応付けられたデータ範囲リストの代わりに、不正検知ＥＣＵが、メッセージＩＤと、許容されているデータ長とを対応付けたデータ長リストを用いることとしても良い。この場合には、不正検知ＥＣＵは、受信されたデータフレームのコントロールフィールドの値が不正を示す所定条件に該当するか否かを判定する。この不正を示す所定条件は、コントロールフィールドにおけるデータ長（ＤＬＣ）が、データ長リストにおいてメッセージＩＤに対応付けられているデータ長ではないという条件である。不正検知ＥＣＵは、受信されたＤＣＬが、データ長リストにおいてメッセージＩＤ毎に許容されているデータ長であるか否かによって、不正か否かの判定を行う。

【０１６９】

（１０）上記実施の形態では、特にデータフレームに注目して説明したが、リモートフレームについても不正検知ＥＣＵが一定の不正を検知することが可能である。例えば、不正検知ＥＣＵが、実施の形態１で示した正規ＩＤリストを用いて受信したリモートフレームにおけるメッセージＩＤが不正か否かを判定しても良い。また、不正検知ＥＣＵが、上

述したデータ長リストを用いて受信したリモートフレームにおけるコントロールフィールドにおけるデータ長（ＤＬＣ）が、メッセージＩＤ毎に許容されているデータ長であるか否かにより不正か否かを判定しても良い。また、上記実施の形態で示した不正検知ＥＣＵが不正なフレームを受信することで不正の検知を行った場合に送信するエラーフレームは、不正の検知後に迅速に送信されると良い。なお、不正検知ＥＣＵは、不正の検知後、その不正なフレームのＣＲＣシーケンスの最後尾が送信される前までにエラーフレームを送信することは有用である。これにより他のＥＣＵは、エラーフレームの検出或いはＣＲＣのチェックでのエラー検出により、その不正なフレームの処理を中止することになる。なお、リモートフレームもデータフレームと同様にメッセージＩＤ、コントロールフィールド及びＣＲＣシーケンスを含む。

【０１７０】

（１１）上記実施の形態では、不正検知ＥＣＵが一定条件下でエラー表示メッセージを送信することを示したが、エラー表示メッセージを送信しないこととしても良い。この場合には、ゲートウェイ及びヘッドユニット等のＥＣＵは特に不正検知ＥＣＵに対応した構成（エラー表示メッセージを受信するための受信ＩＤリスト等）を保持する必要がなくなる。なお、不正検知ＥＣＵは、エラー表示メッセージの送信の代わりに自らスピーカ或いはディスプレイ等を備える場合においてエラーを自ら報知しても良いし、エラーのログを記憶媒体等に記録しても良い。

【０１７１】

（１２）上記実施の形態で示した不正フレーム検知部及び不正ＭＡＣ検知部はＣＡＮコントローラと呼ばれるハードウェア、または、ＣＡＮコントローラと接続して動作するプロセッサ上で動作するファームウェアに実装しても良い。また、ＭＡＣ鍵保持部、カウンタ保持部、正規ＩＤリスト保持部、データ範囲リスト保持部は、ＣＡＮコントローラと呼ばれるハードウェアのレジスタ、または、ＣＡＮコントローラと接続して動作するプロセッサ上で動作するファームウェアに格納されていても良い。

【０１７２】

（１３）上記実施の形態における各ＥＣＵ（ゲートウェイ及びヘッドユニットを含む）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こととしたが、ハードディスク装置、ディスプレイ、キーボード、マウス等の他のハードウェア構成要素を含んでいても良い。また、メモリに記憶された制御プログラムがプロセッサにより実行されてソフトウェア的に機能を実現する代わりに、専用のハードウェア（デジタル回路等）によりその機能を実現することとしても良い。

【０１７３】

（１４）上記実施の形態における各装置を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良い。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等を含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従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。

【０１７４】

また、上記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チップ化されても良い。

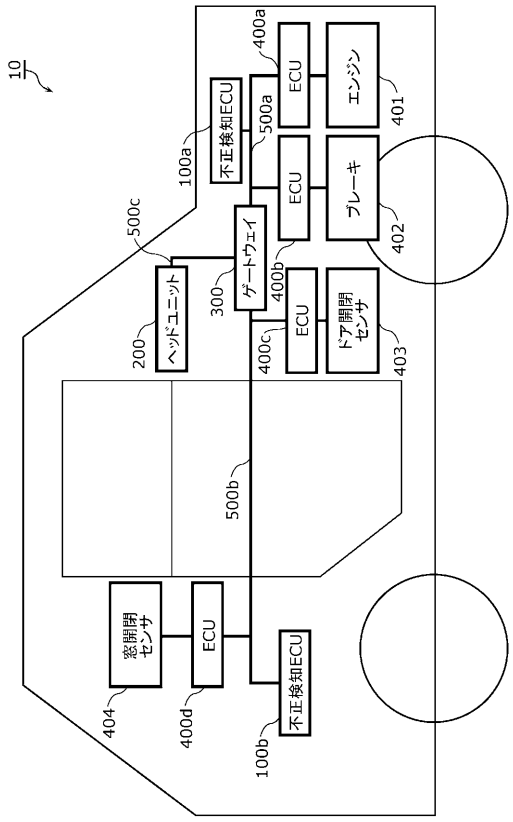
【０１７５】

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、専用回路又は汎用プロセッサで実現しても良い。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リコンフィギュラブル・プロセッサを利用しても良い。

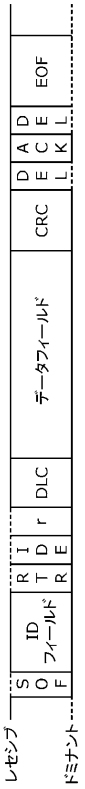
【０１７６】
さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行っても良い。バイオ技術の適用等が可能性としてあり得る。
【０１７７】
（１５）上記各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしても良い。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭ等から構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記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良い。
【０１７８】
（１６）本開示の一態様としては、上記に示す不正対処方法等の方法であるとしても良い。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良いし、前記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良い。
【０１７９】
また、本開示の一態様としては、前記コンピュータプログラムまたは前記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）、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。
【０１８０】
また、本開示の一態様としては、前記コンピュータプログラムまたは前記デジタル信号を、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良い。
【０１８１】
また、本開示の一態様としては、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、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしても良い。
【０１８２】
また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を、前記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良い。
【０１８３】
（１７）上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることで実現される形態も本開示の範囲に含まれる。
【産業上の利用可能性】
【０１８４】
本開示は、車載ネットワークシステム等において不正なＥＣＵによる影響を抑制するために利用可能である。
【符号の説明】
【０１８５】
１０，１１，１２　車載ネットワークシステム
１００ａ，１００ｂ，２１００ａ，２１００ｂ，３１００ａ，３１００ｂ　不正検知電子制御ユニット（不正検知ＥＣＵ）
１１０　不正検知カウンタ保持部
１２０　正規ＩＤリスト保持部
１３０，２１３０　不正フレーム検知部

１４０，２３０，３２０，４２０，３４２０　フレーム生成部
１５０，２６０，３５０，４５０，２１５０，３１５０　フレーム解釈部
１６０，２７０，３６０，４６０　フレーム送受信部
２００　ヘッドユニット
２１０　表示制御部
２２０，４１０　フレーム処理部
２４０，３３０，４３０　受信ＩＤ判断部
２５０，３４０，４４０　受信ＩＤリスト保持部
３００　ゲートウェイ
３１０　転送処理部
３７０　転送ルール保持部
４００ａ，４００ｂ，４００ｃ，４００ｄ，３４００ａ，３４００ｂ，３４００ｃ，３４００ｄ　電子制御ユニット（ＥＣＵ）
４０１　エンジン
４０２　ブレーキ
４０３　ドア開閉センサ
４０４　窓開閉センサ
４７０　データ取得部
５００ａ，５００ｂ，５００ｃ　バス
２１２０　データ範囲リスト保持部
３１３０　不正ＭＡＣ検知部
３４１０，３１７０　ＭＡＣ生成部
３４３０，３１８０　ＭＡＣ鍵保持部
３４４０，３１９０　カウンタ保持部

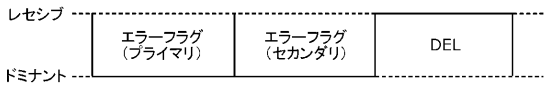
【図１】



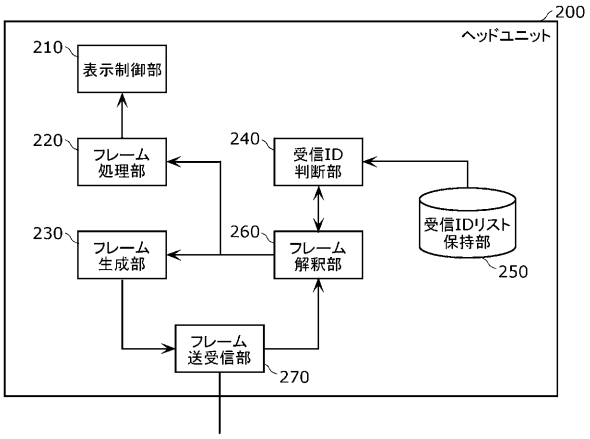
【図２】



【図３】



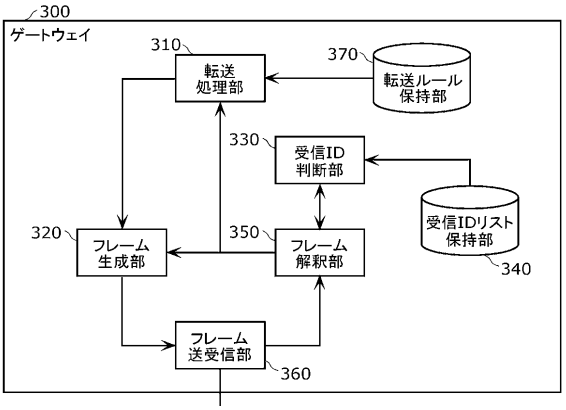
【図４】



【図５】

受信IDリスト
1
2
3
4

【図６】

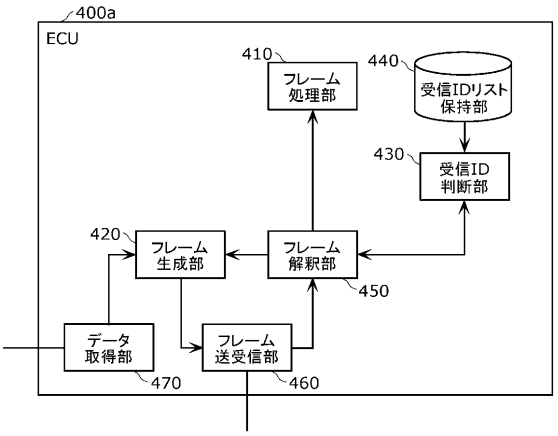


【図７】

転送ルール

転送元	転送先	ID
500a	500b	*
500a	500c	*
500b	500a	3
500b	500c	*
500c	500a	-
500c	500b	-

【図８】



【図９】

受信IDリスト
1
2
3

【図１０】

ID	データ
1	0
1	1
1	2
1	3
1	4
…	…

【図１１】

ID	データ
2	100
2	90
2	80
2	70
2	60
…	…

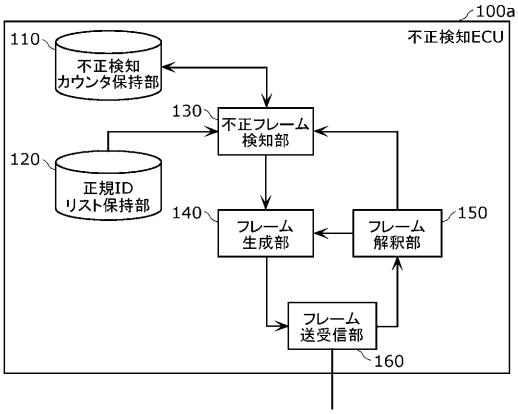
【図１２】

ID	データ
3	1
3	1
3	0
3	0
3	0
…	…

【図１３】

ID	データ
4	0
4	10
4	20
4	30
4	40
…	…

【図１４】



【図１５】

正規IDリスト
1
2
3

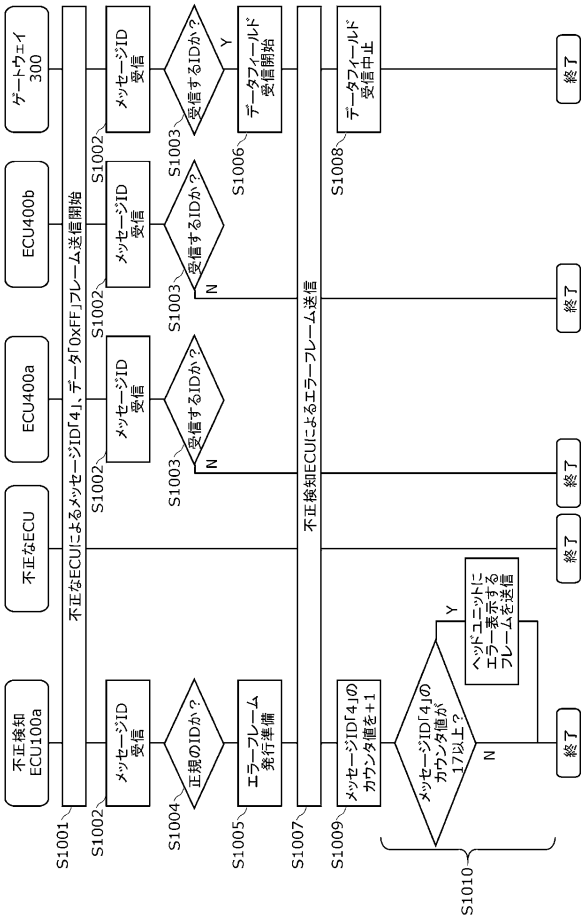
【図１６】

正規IDリスト
1
2
3
4

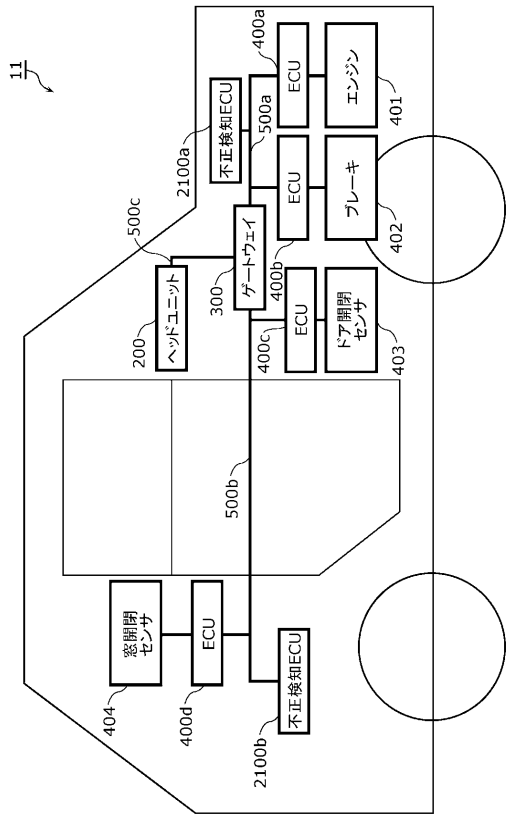
【図１７】

ID	不正検知カウンタ
1	0
2	0
3	0
4	1
5	0
…	…

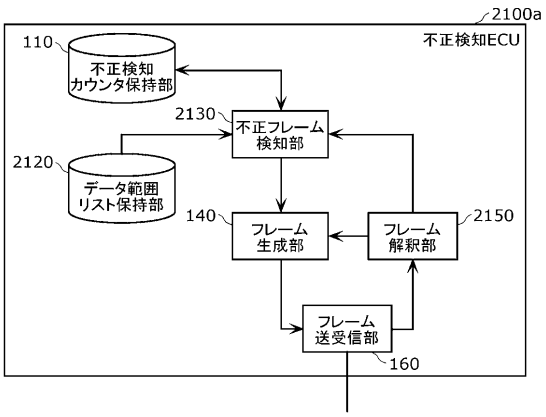
【図１８】



【図１９】



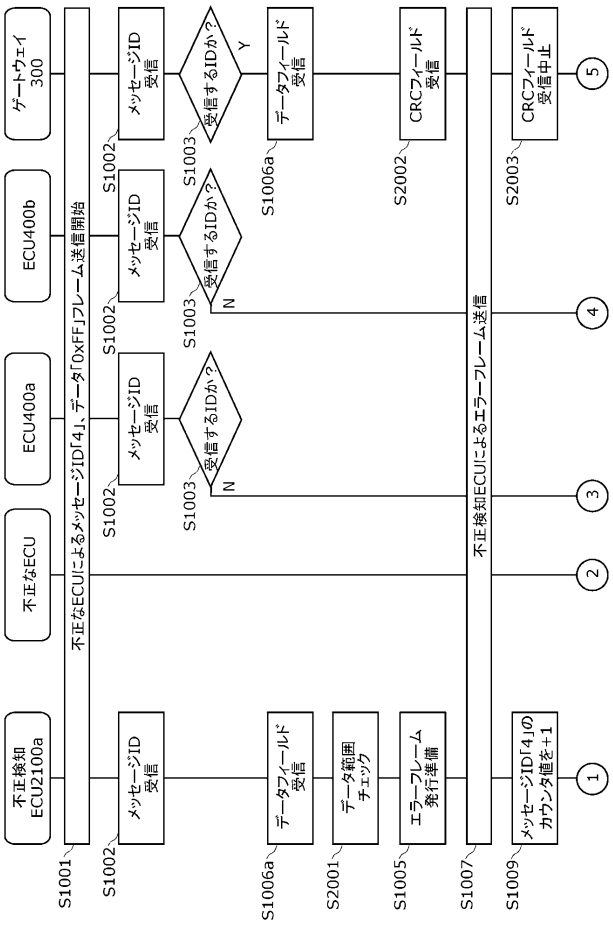
【図２０】



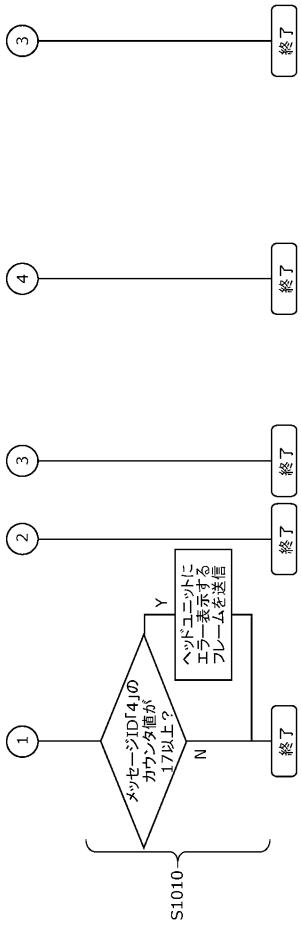
【図２１】

ID	データ範囲
1	0～180
2	0～100
3	0, 1
4	0～100
…	…

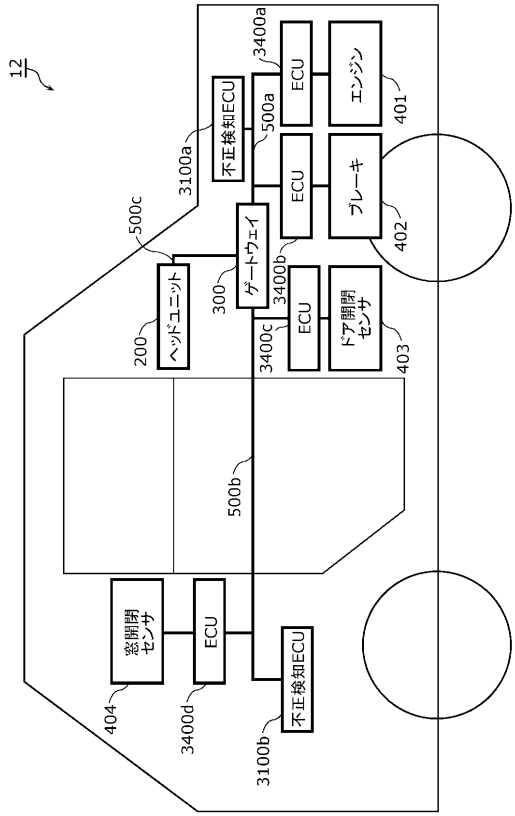
【図２２】



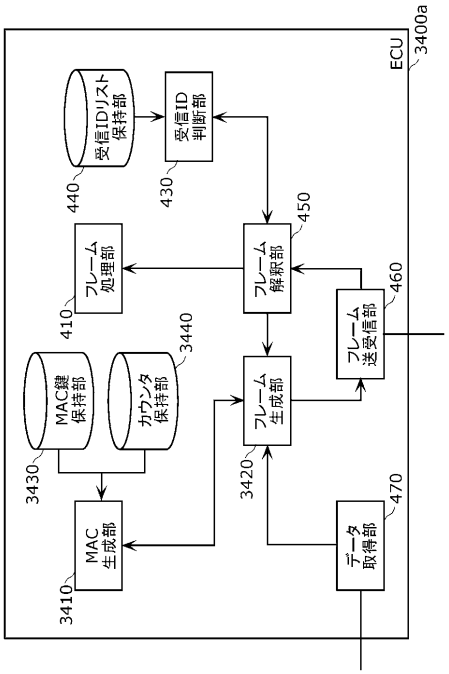
【図２３】



【図２４】



【図２５】



【図２６】

ID	データ
1	0 1 0x1a c4 f7 d3
1	1 2 0xf9 3b 65 9e
1	2 3 0x34 5c ef 79
1	3 4 0x90 2a e3 dd
1	4 5 0x31 2c d5 ee
…	…

【図２７】

ID	データ
2	100 1 0x34 5d ef 78
2	90 2 0x34 2d d5 ea
2	80 3 0x90 8a e8 6b
2	70 4 0x4a d4 f7 d8
2	60 5 0xf1 32 7e 6a
…	…

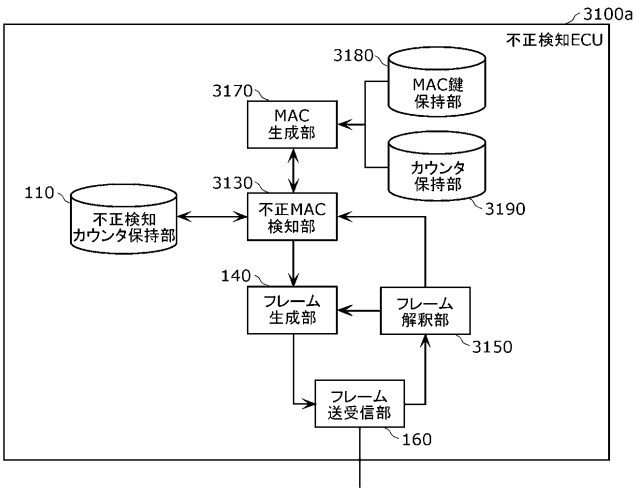
【図２８】

ID	データ
3	1 1 0x92 d5 e8 3b
3	1 2 0x81 a2 c5 ca
3	0 3 0xf8 4d 66 9a
3	0 4 0x95 a2 3e ac
3	0 5 0x1b c5 f6 d1
…	…

【図２９】

ID	データ
4	0 1 0x9d 20 03 d3
4	10 2 0x3a 2d 5b ef
4	20 3 0x4c c8 3b b5
4	30 4 0x5f f1 d2 da
4	40 5 0xb1 0b 70 a4
…	…

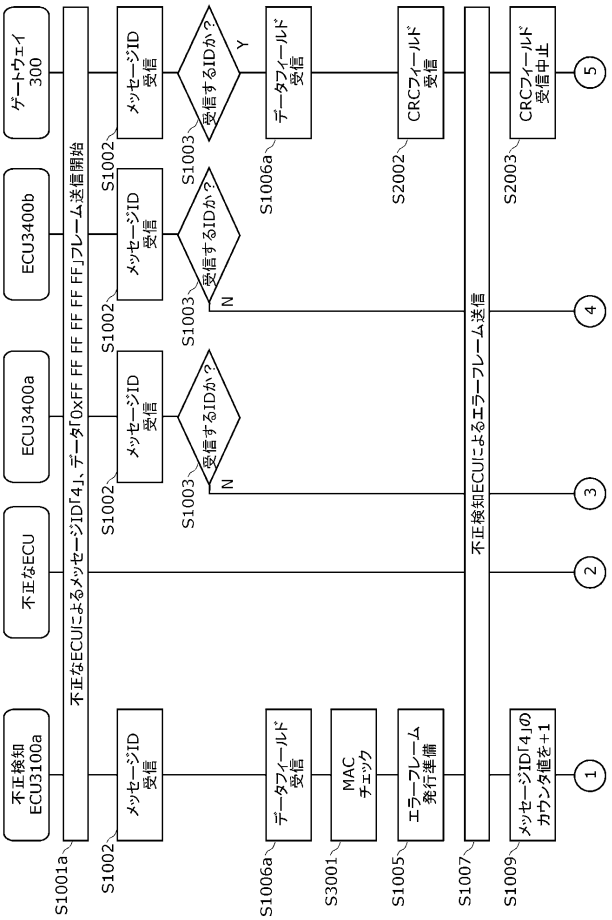
【図３０】



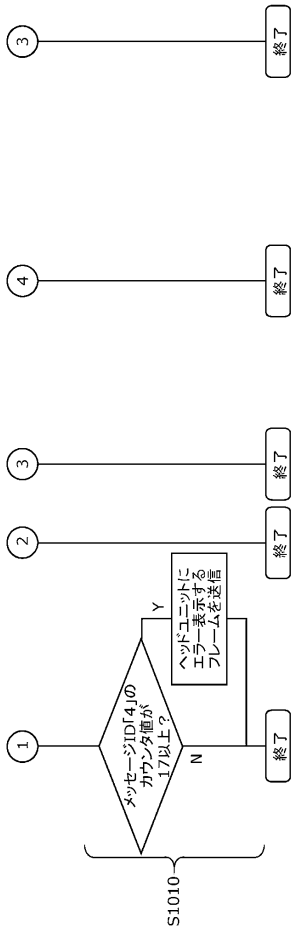
【図３１】

ID	カウンタ
1	1
2	10
3	15
4	100
5	0
…	…

【図３２】



【図３３】



【手続補正書】
【提出日】平成31年3月6日(2019.3.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備えるネットワーク通信システムにおいて用いられる不正対処方法であって、
送信が開始されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する第１の判定ステップと、
前記第１の判定ステップにおいて前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信ステップと、
前記送信ステップにおいてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録ステップと、
前記記録ステップにより記録されたＩＤ毎の回数が所定回数を超えている場合に、不正であると判定する第２の判定ステップとを含み、
前記所定フィールドは、ＩＤを表すフィールドであり、
前記第１の判定ステップでは、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行い、
前記第１の判定ステップでは、前記所定フィールドの内容により表されるＩＤを、前記ＩＤリスト情報が示す１以上の全てのＩＤ全と比較し、一致しない場合、前記所定条件に該当すると判定する、
不正対処方法。
【請求項２】
前記送信ステップでは、前記フレームにおけるＣＲＣシーケンスの最後尾が送信される前に、前記エラーフレームの前記送信を行う
請求項１記載の不正対処方法。
【請求項３】
前記所定回数は、ＣＡＮプロトコルにおける送信エラーカウンタの取り扱い規則に対応して定められたパッシブ状態に遷移すべき値を示し、
前記第２の判定ステップにおいて、前記記録ステップにより記録されたＩＤ毎の回数が前記所定回数を超えている場合に、前記所定回数を超えた前記ＩＤのフレームを送信した電子制御ユニットが、パッシブ状態に遷移しない不正な電子制御ユニットであると判定する
請求項１記載の不正対処方法。
【請求項４】
ＣＡＮ（Controller Area Network）プロトコルに従って通信する複数の電子制御ユニットが通信に用いるバスに接続される不正検知電子制御ユニットであって、
送信が開始されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する第１の判定部と、
前記第１の判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信部と、

前記送信部においてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録部と、
前記記録部により記録されたＩＤ毎の回数が所定回数を超えている場合に、不正であると判定する第２の判定部とを備え、
前記所定フィールドは、ＩＤを表すフィールドであり、
前記第１の判定部は、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行い、
前記第１の判定部は、前記所定フィールドの内容により表されるＩＤを、前記ＩＤリスト情報が示す１以上の全てのＩＤと比較し、一致しない場合、前記所定条件に該当すると判定する、
不正検知電子制御ユニット。
【請求項５】
前記所定回数は、ＣＡＮプロトコルにおける送信エラーカウンタの取り扱い規則に対応して定められたパッシブ状態に遷移すべき値を示し、
前記第２の判定部において、前記記録部により記録されたＩＤ毎の回数が前記所定回数を超えている場合に、前記所定回数を超えた前記ＩＤのフレームを送信した電子制御ユニットが、パッシブ状態に遷移しない不正な電子制御ユニットであると判定する
請求項４記載の不正検知電子制御ユニット。
【請求項６】
ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備えるネットワーク通信システムであって、
送信が開始されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する第１の判定部と、
前記第１の判定部において前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信部と、
前記送信部においてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録部と、
前記記録部により記録されたＩＤ毎の回数が所定回数を超えている場合に、不正であると判定する第２の判定部とを備え、
前記所定フィールドは、ＩＤを表すフィールドであり、
前記第１の判定部は、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行い、
前記第１の判定部は、前記所定フィールドの内容により表されるＩＤを、前記ＩＤリスト情報が示す１以上の全てのＩＤと比較し、一致しない場合、前記所定条件に該当すると判定する、
ネットワーク通信システム。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】
上記課題を解決するために本開示の一態様に係る不正対処方法は、ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備えるネットワーク通信システムにおいて用いられる不正対処方法であって、送信が開始さ

れたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する第１の判定ステップと、前記第１の判定ステップにおいて前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信ステップと、前記送信ステップにおいてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録ステップと、前記記録ステップにより記録されたＩＤ毎の回数が所定回数を超えている場合に、不正であると判定する第２の判定ステップとを含み、前記所定フィールドは、ＩＤを表すフィールドであり、前記第１の判定ステップでは、前記所定フィールドの内容により表されるＩＤを、予め定められたＩＤリスト情報が示す１以上のＩＤと比較することにより、前記所定条件に該当するか否かの前記判定を行い、前記判定ステップでは、前記所定フィールドの内容により表されるＩＤを、前記ＩＤリスト情報が示す１以上の全てのＩＤ全と比較し、一致しない場合、前記所定条件に該当すると判定する。

上記課題を解決するために本開示の一態様に係る不正対処方法は、ＣＡＮ（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備えるネットワーク通信システムにおいて用いられる不正対処方法であって、送信が開始されたフレームにおける所定フィールドの内容が、不正を示す所定条件に該当するか否かを判定する判定ステップと、前記判定ステップにおいて前記フレームの所定フィールドの内容が前記所定条件に該当すると判定された場合に、当該フレームの最後尾が送信される前にエラーフレームを送信する送信ステップと、前記送信ステップにおいてエラーフレームを送信した回数を、前記エラーフレームを送信する対象となった前記フレームに含まれるＩＤフィールドの内容により表されるＩＤ毎に、記録する記録ステップと、前記記録ステップにより記録されたＩＤ毎の回数が所定回数を超えている場合に、報知を行う報知ステップとを含む不正対処方法である。

フロントページの続き

(74)代理人　100131417
弁理士　道坂　伸一
(72)発明者　氏家　良浩
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　松島　秀樹
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　芳賀　智之
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　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　海上　勇二
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
Ｆターム(参考) 5K032 AA05　BA06　CD01　DA02　EA01　EA04