(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7033499号
(P7033499)

(45)発行日　令和4年3月10日(2022.3.10)

(24)登録日　令和4年3月2日(2022.3.2)

(51)国際特許分類
H04L 43/08 (2022.01)

FI
H04L 43/08

請求項の数　10　（全31頁）

(21)出願番号　特願2018-97207(P2018-97207)
(22)出願日　平成30年5月21日(2018.5.21)
(65)公開番号　特開2019-29993(P2019-29993A)
(43)公開日　平成31年2月21日(2019.2.21)
審査請求日　令和3年1月19日(2021.1.19)
(31)優先権主張番号　特願2017-144490(P2017-144490)
(32)優先日　平成29年7月26日(2017.7.26)
(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】　異常検知装置および異常検知方法

(57)【特許請求の範囲】
【請求項１】
移動体に搭載され、通信プロトコルが互いに異なる第１ネットワークおよび第２ネットワークを有するネットワークシステムにおける異常を検知する異常検知装置であって、
前記第２ネットワークから取得される前記移動体の状態を示す状態情報を含む第２フレームを受信する第１通信部と、
前記第１ネットワークの通信プロトコルによる第１フレームを送受信する第２通信部と、
異常検知ルールを保持する異常検知ルール保持部と、
前記状態情報と、前記異常検知ルールとを参照して、前記第２通信部において受信された前記第１フレームに含まれる制御コマンドが異常であるか否かを検知する異常検知処理部と、を備え、
前記異常検知処理部は、前記制御コマンドが異常であることを検知した場合、当該制御コマンドの前記第２ネットワークへの転送を禁止し、
前記異常検知ルールは、前記移動体の異なる複数の状態のそれぞれにおいて許可される制御コマンドを示す第１ルールを含み、
前記異常検知処理部は、前記第２フレームに含まれる前記状態情報が示す前記移動体の状態が、前記制御コマンドが前記第１ルールにおいて対応付けられている状態に含まれない場合、前記制御コマンドが異常であることを検知し、
前記第２フレームは、前記状態情報を含む複数のフレームが格納されており、
前記異常検知ルールは、さらに、前記第２フレームに含まれる前記複数のフレームのそれ

ぞれが異常であるか否かを検知するための第２ルールを含み、
前記第２ルールは、同一種類のフレームにおいて許可されるフレームの受信周期の範囲を示し、
前記異常検知処理部は、前記第２フレームに含まれる前記複数のフレームにそれぞれ対応する受信時刻を用いて、同一種類の前記複数のフレームのうちで、第３フレームの第１受信時刻の、前記第３フレームよりも１つ前に受信された第４フレームの第２受信時刻の差分が受信周期の範囲外である場合、前記第２フレームが異常であることを検知し、
前記異常検知処理部は、さらに、前記第２ルールを用いて前記第２フレームが異常であることを検知した場合、前記制御コマンドの前記第２ネットワークへの転送を禁止する
異常検知装置。
【請求項２】
前記制御コマンドは、走行する、曲がる、および、止まるの少なくとも１つを前記移動体に実行させる制御コマンドである
請求項１に記載の異常検知装置。
【請求項３】
前記第２フレームは、前記第２ネットワークの通信プロトコルによる前記状態情報を含むフレームが格納された前記第１フレームである、
請求項１に記載の異常検知装置。
【請求項４】
前記第１ネットワークは、Ｅｔｈｅｒｎｅｔ（登録商標）によるネットワークであり、
前記第２ネットワークは、ＣＡＮによるネットワークであり、
前記第１通信部は、前記状態情報を示すＣＡＮフレームが格納されたＥｔｈｅｒｎｅｔ（登録商標）フレームである第２フレームを受信する
請求項１に記載の異常検知装置。
【請求項５】
前記第２フレームは、前記状態情報を示すＣＡＮフレームを含む複数のＣＡＮフレームが格納されており、
前記異常検知ルールは、さらに、前記複数のＣＡＮフレームのそれぞれが異常であるか否かを検知するための第２ルールを含み、
前記複数のＣＡＮフレームのそれぞれは、種類毎に異なる識別子を有し、
前記第２ルールは、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示し、
前記異常検知処理部は、前記複数のＣＡＮフレームにそれぞれ対応する受信時刻を用いて、互いに同じ識別子を有する前記複数のＣＡＮフレームのうちで、第１ＣＡＮフレームの第１受信時刻の、前記第１ＣＡＮフレームよりも１つ前に受信された第２ＣＡＮフレームの第２受信時刻からの差分が、前記第２ルールにおいて前記同じ識別子に対応付けられている受信周期の範囲外である場合、前記第１ＣＡＮフレームが異常であることを検知する
請求項４に記載の異常検知装置。
【請求項６】
前記第２ルールは、さらに、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可される変化量であって、当該ＣＡＮフレームの１つ前のＣＡＮフレームのデータ値からの変化量を示し、
前記異常検知処理部は、さらに、前記第１ＣＡＮフレームの第１データ値の、前記第２ＣＡＮフレームの第２データ値からの差分が、前記第２ルールにおいて前記同じ識別子に対応付けられている前記変化量を超える場合、前記第１ＣＡＮフレームが異常であることを検知する
請求項５に記載の異常検知装置。
【請求項７】
前記第２フレームは、前記状態情報を示すＣＡＮフレームを含む複数のＣＡＮフレームが格納されており、

前記異常検知ルールは、さらに、前記複数のＣＡＮフレームのそれぞれが異常であるか否かを検知するための第３ルールを含み、
前記複数のＣＡＮフレームのそれぞれは、種類毎に異なる識別子を有し、
前記第３ルールは、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示し、
前記異常検知処理部は、前記複数のＣＡＮフレームにそれぞれ対応する受信時刻を用いて、互いに同じ識別子を有する前記複数のＣＡＮフレームのうちで、第１ＣＡＮフレームの第１受信時刻の、前記第１ＣＡＮフレームよりも１つ前に受信された第２ＣＡＮフレームの第２受信時刻からの差分が、前記第３ルールにおいて前記同じ識別子に対応付けられている受信周期の範囲内である場合、前記第１ＣＡＮフレームが異常であることを検知する
請求項４に記載の異常検知装置。
【請求項８】
前記第３ルールは、さらに、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可される変化量であって、当該ＣＡＮフレームの１つ前のＣＡＮフレームのデータ値からの変化量を示し、
前記異常検知処理部は、さらに、前記第１ＣＡＮフレームの第１データ値の、前記第２ＣＡＮフレームの第２データ値からの差分が、前記第３ルールにおいて前記同じ識別子に対応付けられている前記変化量の範囲内である場合、前記第１ＣＡＮフレームが異常であることを検知する
請求項７に記載の異常検知装置。
【請求項９】
前記異常検知処理部は、
複数の前記識別子のそれぞれに対応付けられたルールを前記異常検知ルールとして取得し、
前記異常検知ルールを参照して、前記ＣＡＮフレームが異常であることを検知する
請求項５から８のいずれか１項に記載の異常検知装置。
【請求項１０】
移動体に搭載され、通信プロトコルが互いに異なる第１ネットワークおよび第２ネットワークを有するネットワークシステムにおける異常を検知する異常検知装置による異常検知方法であって、
前記第２ネットワークから取得される前記移動体の状態を示す状態情報を含む第２フレームを受信する第１通信ステップと、
前記第１ネットワークの通信プロトコルによる第１フレームを送受信する第２通信ステップと、
前記状態情報と、前記異常検知装置が備える保持部が保持する異常検知ルールとを参照して、前記第２通信ステップにおいて受信された前記第１フレームに含まれる制御コマンドが異常であるか否かを検知する検知ステップと、
前記検知ステップにおいて、前記制御コマンドが異常であることを検知された場合、当該制御コマンドの前記第２ネットワークへの転送を禁止する禁止ステップと、を含み、
前記異常検知ルールは、前記移動体の異なる複数の状態のそれぞれにおいて許可される制御コマンドを示す第１ルールを含み、
前記検知ステップでは、前記第２フレームに含まれる前記状態情報が示す前記移動体の状態が、前記制御コマンドが前記第１ルールにおいて対応付けられている状態に含まれない場合、前記制御コマンドが異常であることを検知し、
前記第２フレームは、前記状態情報を含む複数のフレームが格納されており、
前記異常検知ルールは、さらに、前記第２フレームに含まれる前記複数のフレームのそれぞれが異常であるか否かを検知するための第２ルールを含み、
前記第２ルールは、同一種類のフレームにおいて許可されるフレームの受信周期の範囲を示し、
前記検知ステップでは、前記第２フレームに含まれる前記複数のフレームにそれぞれ対応する受信時刻を用いて、同一種類の前記複数のフレームのうちで、第３フレームの第１

受信時刻の、前記第３フレームよりも１つ前に受信された第４フレームの第２受信時刻の差分が受信周期の範囲外である場合、前記第２フレームが異常であることを検知し、
前記検知ステップでは、さらに、前記第２ルールを用いて前記第２フレームが異常であることを検知した場合、前記制御コマンドの前記第２ネットワークへの転送を禁止する
異常検知方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、移動体に搭載されるネットワークシステムにおける異常を検知する異常検知装置および異常検知方法に関する。
【背景技術】
【０００２】
特許文献１には、車両を制御するための車内ネットワークシステムについて開示されている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１２－６４４６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
特許文献１の技術では、車両のような移動体に搭載されるネットワークシステムにおいて、効果的に異常を検知することができないおそれがある。
【０００５】
本開示は、移動体に搭載されるネットワークシステムにおいて、効果的に異常を検知することができる異常検知装置および異常検知方法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】
【０００６】
上記課題を解決するために本開示の一態様に係る異常検知装置は、移動体に搭載され、通信プロトコルが互いに異なる第１ネットワークおよび第２ネットワークを有するネットワークシステムにおける異常を検知する異常検知装置であって、前記第２ネットワークから取得される前記移動体の状態を示す状態情報を受信する第１通信部と、前記第１ネットワークの通信プロトコルによる第１フレームを送受信する第２通信部と、異常検知ルールを保持する異常検知ルール保持部と、前記状態情報と、前記異常検知ルールとを参照して、前記第２通信部において受信された前記第１フレームに含まれる制御コマンドが異常であるか否かを検知する異常検知処理部と、を備え、前記異常検知処理部は、前記制御コマンドが異常であることを検知した場合、当該制御コマンドの転送を禁止する。
【０００７】
なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。
【発明の効果】
【０００８】
本開示の異常検知装置および異常検知方法によれば、移動体に搭載されるネットワークシステムにおいて、効果的に異常を検知することができる。
【図面の簡単な説明】
【０００９】
【図１】図１は、実施の形態１における車載ネットワークの全体構成図である。
【図２】図２は、第２ネットワークで送受信されるデータフレーム（ＣＡＮフレーム）の

フォーマットを示す図である。
【図３】図３は、第１ネットワークで送受信されるＥフレームのフォーマットを示す図である。
【図４】図４は、Ｅフレームのペイロード内のデータ構成例を示す図である。
【図５】図５は、ＣＡＮゲートウェイの機能構成の一例を示すブロック図である。
【図６】図６は、実施の形態１に係るＣＡＮゲートウェイが受信した複数のＣＡＮフレームに基づいてＥフレームを送信するイメージを示す図である。
【図７】図７は、自動運転ＤＣＵの機能構成の一例を示すブロック図である。
【図８】図８は、スイッチルール保持部が保持するスイッチルールの一例を示す図である。
【図９】図９は、実施の形態１に係る自動運転ＤＣＵの異常検知ルール保持部が保持する異常検知ルールの一例を示す図である。
【図１０】図１０は、実施の形態１に係るネットワークシステムにおける異常検知方法の一例を示すシーケンス図である。
【図１１】図１１は、実施の形態１に係るネットワークシステムにおける異常検知方法の一例を示すシーケンス図である。
【図１２】図１２は、実施の形態２に係るＣＡＮゲートウェイが受信した複数のＣＡＮフレームに基づいてＥフレームを送信するイメージを示す図である。
【図１３】図１３は、実施の形態２に係る自動運転ＤＣＵの異常検知ルール保持部１０５が保持する異常検知ルールの一例を示す図である。
【図１４】図１４は、実施の形態２に係るネットワークシステムにおける異常検知方法の一例を示すシーケンス図である。
【図１５】図１５は、実施の形態２に係るネットワークシステムにおける異常検知方法の一例を示すシーケンス図である。
【図１６】図１６は、実施の形態３に係るＣＡＮゲートウェイが受信した複数のＣＡＮフレームに基づいてＥフレームを送信するイメージを示す図である。
【図１７】図１７は、実施の形態３における自動運転ＤＣＵにおけるＣＡＮの異常検知をするときの検知ルールを定義したテーブルを示す図である。

【発明を実施するための形態】
【００１０】
（本発明の基礎となった知見）
本発明者は、「背景技術」の欄において記載した、車内ネットワークシステムに関し、以下の問題が生じることを見出した。
【００１１】
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。また、より多くの情報を伝送するための規格として、ＩＥＥＥ ８０２．３で規定されているＥｔｈｅｒｎｅｔ（登録商標）という規格が存在する。
【００１２】
先進運転支援システムや自動運転においては、カメラもしくはＬＩＤＡＲ（Ｌｉｇｈｔ Ｄｅｔｅｃｔｉｏｎ ａｎｄ Ｒａｎｇｉｎｇ）などのセンサにより得られたデータ、または、ダイナミックマップに用いるデータのような膨大な情報を処理する必要があるため、データ伝送速度が高いＥｔｈｅｒｎｅｔ（登録商標）の導入が進んでいる。一方で、従来から存在するＣＡＮも車両制御系としては利用されている。そのため、ＣＡＮとＥｔｈｅｒｎｅｔ（登録商標）とが混在する車載ネットアーキテクチャが増えている。
【００１３】
自動車は、外部ネットワークと接続され、電子制御化が進んでいる。これにより、自動車は、自動車の制御系コマンドがなりすまされることで、不正に操作される脅威がある。そ

のような脅威から守るために、特許文献１の技術では、後付け電子制御装置から、車内ネットワークシステムの車両制御系ネットワークにデータを送信する場合に、車内ネットワークの情報系ネットワークに送信されたデータを車両制御系ネットワークへ転送することの可否の判断をしていている。しかし、特許文献１の技術では、複数の異なる通信プロトコル上に流れる情報を元に転送可否の判断をしていない。したがって、従来技術には、例えば、ＣＡＮおよびＥｔｈｅｒｎｅｔ（登録商標）のような互いに異なる通信プロトコルによる複数のネットワークの間でデータの転送を行う場合に、適切に転送可否の判断をできないという課題があった。

【００１４】

本発明者らは、鋭意検討の上、複数の異なる通信プロトコル上に流れる情報を参照し、車両制御系のメッセージが不正であるかどうかを判断することで、安全な自動運転または先進運転支援システムを実現するための異常検知装置および異常検知方法を見出すに至った。

【００１５】

本開示の一態様に係る異常検知装置は、移動体に搭載され、通信プロトコルが互いに異なる第１ネットワークおよび第２ネットワークを有するネットワークシステムにおける異常を検知する異常検知装置であって、前記第２ネットワークから取得される前記移動体の状態を示す状態情報を受信する第１通信部と、前記第１ネットワークの通信プロトコルによる第１フレームを送受信する第２通信部と、異常検知ルールを保持する異常検知ルール保持部と、前記状態情報と、前記異常検知ルールとを参照して、前記第２通信部において受信された前記第１フレームに含まれる制御コマンドが異常であるか否かを検知する異常検知処理部と、を備え、前記異常検知処理部は、前記制御コマンドが異常であることを検知した場合、当該制御コマンドの転送を禁止する。

【００１６】

これにより、異常検知装置は、第２ネットワークから得られる移動体の状態情報と、異常検知ルールとに基づき、生成された自動運転の制御コマンドが異常であるかを検知する。このため、移動体に搭載されるネットワークシステムにおいて、効果的に異常を検知することができる。

【００１７】

また、異常検知装置は、異常があることを検知された制御コマンドの転送を禁止する。このため、例えば第１ネットワークに接続される機器に脆弱性があって、第１ネットワーク経由で攻撃された場合であっても、異常検知装置は、不正な自動運転の制御を防止することができる。し、異常検知時に、自動運転や先進運転システムといった車両制御コマンドの実行を防止することが可能となる。

【００１８】

また、前記異常検知ルールは、前記移動体の異なる複数の状態のそれぞれにおいて許可される制御コマンドを示す第１ルールを含み、前記異常検知処理部は、前記状態情報が示す前記移動体の状態が、前記制御コマンドが前記第１ルールにおいて対応付けられている状態に含まれない場合、前記制御コマンドが異常であることを検知してもよい。

【００１９】

これにより、異常検知装置は、例えば、現時点の車速、ステアリングの操舵角度状態、シフトポジションなどの車両状態に基づいて車両制御コマンドの異常を検知することが可能となる。

【００２０】

また、前記制御コマンドは、進む、曲がる、および、止まるの少なくとも１つを前記移動体に実行させる制御コマンドであってもよい。

【００２１】

これにより、異常検知装置は、例えば、走行中の急ハンドル、急ブレーキや急加速、停車中の急発信など、自動運転または先進運転支援システムの制御コマンドの異常を検知し、安全な運転環境を提供することが可能となる。

【００２２】

また、前記第１ネットワークは、Ｅｔｈｅｒｎｅｔ（登録商標）によるネットワークであり、前記第２ネットワークは、ＣＡＮによるネットワークであり、前記第１通信部は、前記状態情報を含むＣＡＮフレームを受信することで前記状態情報を受信し、前記異常検知ルールは、さらに、前記ＣＡＮフレームが異常であるか否かを検知するための第２ルールを含み、前記異常検知処理部は、さらに、前記ＣＡＮフレームが異常であることを検知した場合、前記制御コマンドの転送を禁止してもよい。

【００２３】

これにより、ＣＡＮフレームの異常を検知した上で、車両制御コマンドの実行が可能となる。

【００２４】

また、前記第１ネットワークは、Ｅｔｈｅｒｎｅｔ（登録商標）によるネットワークであり、前記第２ネットワークは、ＣＡＮによるネットワークであり、前記第１通信部は、前記状態情報を示すＣＡＮフレームが格納されたＥｔｈｅｒｎｅｔ（登録商標）フレームである第２フレームを受信してもよい。

【００２５】

これにより、状態情報を示すＣＡＮフレームがＥｔｈｅｒｎｅｔ（登録商標）フレームに格納され、Ｅｔｈｅｒｎｅｔ（登録商標）上の機器でＣＡＮフレームの異常検知が可能となる。

【００２６】

また、前記第２フレームは、前記状態情報を示すＣＡＮフレームを含む複数のＣＡＮフレームが格納されており、前記異常検知ルールは、さらに、前記複数のＣＡＮフレームのそれぞれが異常であるか否かを検知するための第２ルールを含み、前記複数のＣＡＮフレームのそれぞれは、種類毎に異なる識別子を有し、前記第２ルールは、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示し、前記異常検知処理部は、前記複数のＣＡＮフレームにそれぞれ対応する受信時刻を用いて、互いに同じ識別子を有する前記複数のＣＡＮフレームのうちで、第１ＣＡＮフレームの第１受信時刻の、前記第１ＣＡＮフレームよりも１つ前に受信された第２ＣＡＮフレームの第２受信時刻からの差分が、前記第２ルールにおいて前記同じ識別子に対応付けられている受信周期の範囲外である場合、前記第１ＣＡＮフレームが異常であることを検知してもよい。

【００２７】

これにより、第２ネットワーク上において異常が発生している場合であっても、第１ネットワークにおける機器において周期性を持つＣＡＮフレームの異常を検知できるため、自動運転や先進運転支援システムを安全に停止することが可能となる。

【００２８】

また、前記第２ルールは、さらに、複数の前記識別子のそれぞれに対応する状態情報おいて許可される変化量であって、当該状態情報の１つ前の状態情報のデータ値からの変化量を示し、前記異常検知処理部は、さらに、前記第１状態情報の第１データ値の、前記第２状態情報の第２データからの差分が、前記第２ルールにおいて前記同じ識別子に対応付けられている前記変化量を超える場合、前記第１状態情報が異常であることを検知してもよい。

【００２９】

これにより、異常検知装置は、第２ネットワーク上において異常が発生している場合であっても、第１ネットワークにおける機器においてＣＡＮフレームのデータ値の異常を検知できるため、自動運転を停止することが可能となる。

【００３０】

また、前記第２フレームは、前記状態情報を示すＣＡＮフレームを含む複数のＣＡＮフレームが格納されており、前記異常検知ルールは、さらに、前記複数のＣＡＮフレームのそれぞれが異常であるか否かを検知するための第３ルールを含み、前記複数のＣＡＮフレームのそれぞれは、種類毎に異なる識別子を有し、前記第３ルールは、複数の前記識別子の

それぞれに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示し、前記異常検知処理部は、前記複数のＣＡＮフレームにそれぞれ対応する受信時刻を用いて、互いに同じ識別子を有する前記複数のＣＡＮフレームのうちで、第１ＣＡＮフレームの第１受信時刻の、前記第１ＣＡＮフレームよりも１つ前に受信された第２ＣＡＮフレームの第２受信時刻からの差分が、前記第３ルールにおいて前記同じ識別子に対応付けられている受信周期の範囲内である場合、前記第１ＣＡＮフレームが異常であることを検知してもよい。

【００３１】

これにより、第２ネットワーク上において異常が発生している場合であっても、第１ネットワークにおける機器において周期性を持つＣＡＮフレームの異常を検知できるため、自動運転や先進運転支援システムを安全に停止することが可能となる。

【００３２】

また、前記第３ルールは、さらに、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可される変化量であって、当該ＣＡＮフレームの１つ前のＣＡＮフレームのデータ値からの変化量を示し、前記異常検知処理部は、さらに、前記第１ＣＡＮフレームの第１データ値の、前記第２ＣＡＮフレームの第２データ値からの差分が、前記第３ルールにおいて前記同じ識別子に対応付けられている前記変化量の範囲内である場合、前記第１ＣＡＮフレームが異常であることを検知してもよい。

【００３３】

これにより、異常検知装置は、第２ネットワーク上において異常が発生している場合であっても、第１ネットワークにおける機器においてＣＡＮフレームのデータ値の異常を検知できるため、自動運転を停止することが可能となる。

【００３４】

また、前記異常検知処理部は、複数の前記識別子のそれぞれに対応付けられたルールを前記異常検知ルールとして取得し、前記異常検知ルールを参照して、前記状態情報が異常であることを検知してもよい。

【００３５】

これにより、例えば、第２ネットワーク側の処理が逼迫している際に、第２ネットワーク上における異常検知を第１ネットワーク上における機器で実施することが可能となり、負荷分散につながる。

【００３６】

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で読み取り可能な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よい。

【００３７】

以下、実施の形態に係る異常検知装置および異常検知方法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、処理の要素としてのステップ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。

【００３８】

（実施の形態１）

図１は、実施の形態１における車載ネットワークの全体構成図である。

【００３９】

車両１のネットワークシステム３は、制御装置、センサ、アクチュエータ、ユーザインタフェース装置等の各種機器が搭載された車両１におけるネットワーク通信システムである。ネットワークシステム３は、第１ネットワーク１０と第２ネットワーク２０とを有する

。車両１は、移動体の一例である。第１ネットワーク１０は、Ｅｔｈｅｒｎｅｔ（登録商標）プロトコルに従ってＥｔｈｅｒｎｅｔ（登録商標）フレーム（以下、「Ｅフレーム」という）の伝送が行われるＥｔｈｅｒｎｅｔ（登録商標）のネットワークである。第２ネットワーク２０は、ＣＡＮプロトコルに従ってバスでデータフレーム（ＣＡＮフレーム）等の伝送が行われるＣＡＮのネットワークである。

【００４０】

図１に示すように、ネットワークシステム３は、セントラルゲートウェイ４００と、テレマティクスコントロールユニット４１０と、診断ポート４２０と、自動運転ＤＣＵ（Ｄｏｍａｉｎ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）１００と、自動運転ＥＣＵ１１０と、カメラ１２０と、ＬＩＤＡＲ１３０と、ダイナミックマップＥＣＵ１４０と、インフォテインメントＤＣＵ３００と、ＩＶＩ（Ｉｎ－Ｖｅｈｉｃｌｅ Ｉｎｆｏｔａｉｎｍｅｎｔ）３１０と、ＣＡＮゲートウェイ２００と、エンジンＥＣＵ２１０と、ステアリングＥＣＵ２２０と、ブレーキＥＣＵ２３０と、ウィンドウＥＣＵ２４０と、第１伝送路１１と、第２伝送路２１とを含んで構成される。第１伝送路１１は、第１ネットワーク１０の伝送路であり、例えばＥｔｈｅｒｎｅｔ（登録商標）ケーブルである。第２伝送路２１は、第２ネットワーク２０の伝送路であり、例えばＣＡＮバスである。

【００４１】

なお、ネットワークシステム３には、上記の各ＥＣＵ１１０、１４０、２１０、２２０、２３０、２４０または各ＤＣＵ１００、３００の他にもいくつものＥＣＵまたはＤＣＵが含まれてもよい。例えば、第２伝送路２１には、各ＥＣＵ２１０、２２０、２３０、２４０以外にも、図示しないＥＣＵが接続されてもよい。

【００４２】

各ＥＣＵ１１０、１４０、２１０、２２０、２３０、２４０または各ＤＣＵ１００、３００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プログラム（ソフトウェアとしてのコンピュータプログラム）を記憶することができる。メモリとして、不揮発性メモリを含んでもよい。例えばプロセッサが、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。

【００４３】

各ＥＣＵ２１０、２２０、２３０、２４０は、ＣＡＮプロトコルに従ってフレームの授受を行う。各ＥＣＵ２１０、２２０、２３０、２４０は、それぞれエンジン、ステアリング、ブレーキ、ウィンドウ開閉センサといった機器に接続されており、その機器の状態を取得し、例えば周期的に、状態を表すデータフレームを、第２伝送路２１等で構成される第２ネットワーク２０に送信している。また、各ＥＣＵ２１０、２２０、２３０、２４０は、第２ネットワーク２０を構成する第２伝送路２１からデータフレームを受信して、データフレームを解釈し、受信すべきＣＡＮ－ＩＤを有するデータフレームか否かの判別を行う。そして、各ＥＣＵ２１０、２２０、２３０、２４０は、判別の結果、必要に応じてデータフレーム内のデータ（データフィールドの内容）に従って、当該ＥＣＵに接続されている機器の制御を行ってもよいし、必要に応じてデータフレームを生成して送信してもよい。

【００４４】

各ＥＣＵ１１０、１４０または各ＤＣＵ１００、３００は、Ｅｔｈｅｒｎｅｔ（登録商標）プロトコルに従ってＥフレームの送信又は受信を行う。各ＤＣＵ１００、３００は、それぞれＩＶＩ３１０、自動運転ＥＣＵ１１０、カメラ１２０、ＬＩＤＡＲ１３０、ダイナミックマップＥＣＵ１４０といった機器に接続されており、その機器から取得した情報に基づく処理を行う。また、各ＤＣＵ１００、３００は、必要に応じて接続されている機器を制御してもよいし、必要に応じて他のＥＣＵへの情報の送信を行ってもよい。

【００４５】

セントラルゲートウェイ４００には、テレマティクスコントロールユニット４１０と診断ポート４２０と、自動運転ＤＣＵ１００と、ＣＡＮゲートウェイ２００と、インフォテインメントＤＣＵ３００が、第１伝送路１１で接続される。セントラルゲートウェイ４００は、例えば、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。

【００４６】

テレマティクスコントロールユニット４１０は、車両１が外部ネットワーク３０上にあるサーバ２と通信するユニットである。テレマティクスコントロールユニット４１０は、例えば、第３世代移動通信システム（３Ｇ）、第４世代移動通信システム（４Ｇ）、または、ＬＴＥ（登録商標）などのような移動通信システムで利用される通信規格に適合した無線通信インタフェースを有していてもよいし、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ規格に適合した無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）インタフェースを有していてもよい。つまり、外部ネットワーク３０は、携帯電話通信網、Ｗｉ－Ｆｉなどである。サーバ２は、例えば車両１のＥＣＵに対して情報を提供する機能等を有するコンピュータである。

【００４７】

診断ポート４２０は、ディーラが車両１の故障診断に使うためのポートであり、診断用のコマンドの送受信に利用されるポートである。

【００４８】

自動運転ＤＣＵ１００は、自動運転ＥＣＵ１１０と、カメラ１２０と、ＬＩＤＡＲ１３０と、ダイナミックマップＥＣＵ１４０と、第１伝送路１１で接続されている。

【００４９】

自動運転ＥＣＵ１１０は、車両１の運転を制御する制御コマンドを生成する。具体的には、自動運転ＥＣＵ１１０は、車輪の操舵を行うステアリング、車輪を回転駆動させるエンジン、モータなどの動力源、車輪の制動するブレーキなどを制御する制御コマンドを生成する。つまり、制御コマンドは、進む（つまり、走行する）、曲がる、止まるの少なくとも１つを車両１に実行させる制御コマンドである。自動運転ＥＣＵ１１０は、生成した制御コマンドを第２ネットワーク２０に送信する。

【００５０】

カメラ１２０は、車外の状況、つまり、車両１の周囲を撮影するカメラである。カメラ１２０は、例えば、車両１の車体の外側に配置されていてもよい。

【００５１】

ＬＩＤＡＲ１３０は、車外の障害物を感知するためのセンサである。ＬＩＤＡＲ１３０は、例えば、車両１の水平方向において３６０度全方位、および、垂直方向において所定の角度（例えば３０度）の角度範囲の検出範囲にある物体との距離を検出するレーザセンサである。ＬＩＤＡＲ１３０は、車両１の周囲にレーザを発し、周囲の物体に反射されたレーザを検知することで、ＬＩＤＡＲ１３０から物体までの距離を計測する。

【００５２】

ダイナミックマップＥＣＵ１４０は、ダイナミックマップに用いるデータを受信し、受信したデータを用いてダイナミックマップを復号するための電子制御ユニットである。復号されたダイナミックマップは、例えば、自動運転ＥＣＵ１１０による自動運転の制御に用いられる。

【００５３】

ＣＡＮゲートウェイ２００は、第２ネットワーク２０および第１ネットワーク１０に接続されているゲートウェイである。第２ネットワーク２０は、本実施の形態では、エンジンＥＣＵ２１０、ステアリングＥＣＵ２２０、ブレーキＥＣＵ２３０の制御系バスと、ウィンドウ開閉を制御するウィンドウＥＣＵ２４０が接続されるボディ系バスとの２本のＣＡＮバスを備えている。ＣＡＮゲートウェイ２００は、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。ＣＡＮゲートウェイ２００は、２つの伝送路１１、２１のうち、一の伝送路から受信したフレームを他の伝送路に転送（または中継）する機能を有する。ＣＡＮゲートウェイ２００によるフレームの転送は、フレームに係るデー

タの中継である。ＣＡＮゲートウェイ２００は、フレームの転送において、転送先の伝送路で用いられる通信プロトコルに対応した、通信方式、フレームフォーマット等の変換が行われてもよい。また、ＣＡＮゲートウェイ２００は、伝送路間でのフレームの転送として、１以上の伝送路から受信した１以上のフレームに対応して、１以上のフレームの、１以上複数の伝送路への送信を行ってもよい。

【００５４】

インフォテインメントＤＣＵ３００は、ＩＶＩ３１０と、第１伝送路１１で接続されており、情報系ネットワークのドメイン管理を行う。ＩＶＩ３１０は、ディスプレイを備え、映像、音声等の再生といったマルチメディア機能を有する装置である。

【００５５】

図２は、第２ネットワークで送受信されるデータフレーム（ＣＡＮフレーム）のフォーマットを示す図である。

【００５６】

第２ネットワーク２０では、各ＥＣＵ２１０、２２０、２３０、２４０等がＣＡＮプロトコルに従って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が、ここでは、主にデータフレームに注目して説明する。

【００５７】

図２の（ａ）は標準フォーマットである。標準フォーマットにおいては、データフレームは、ＳＯＦ（Start Of Frame）、ＩＤ（ＣＡＮ－ＩＤ）、ＲＴＲ（Remote Transmission Request）、ＩＤＥ（Identifier Extension）、予約ビット「ｒ」、サイズ、データ、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）で構成される。ここで、ＩＤフィールドの内容としてのＩＤ（ＣＡＮ－ＩＤ）は、データの種類を示す識別子であり、メッセージＩＤとも称される。つまり、ＣＡＮフレームは、種類毎に異なる識別子を有する。なお、ＣＡＮでは、複数のノードが同時に送信を開始した場合、このＣＡＮ－ＩＤが小さい値を持つフレームを優先する通信調停がなされる。サイズは、後続するデータフィールド（データ）の長さを示すＤＬＣ（Data Length Code）である。データ（データフィールドの内容）の仕様については、ＣＡＮプロトコルで規定されておらず、ネットワークシステム３において定められる。従って、車両の車種、製造者（製造メーカ）等に依存した仕様となり得る。

【００５８】

図２の（ｂ）は拡張フォーマットである。本実施の形態では第２ネットワーク２０で標準フォーマットが用いられることとして説明するが、第１ネットワーク１０において拡張フォーマットが用いられる場合には、１１ビットのＩＤフィールドのベースＩＤ（ＣＡＮ－ＩＤの一部）と、１８ビットの拡張ＩＤ（ＣＡＮ－ＩＤの残部）とを合わせた２９ビットをＣＡＮ－ＩＤと扱えばよい。

【００５９】

図３は、第１ネットワークで送受信されるＥフレームのフォーマットを示す図である。

【００６０】

同図に示すように、Ｅフレームは、主たる伝送内容であるデータを格納するＥｔｈｅｒｎｅｔ（登録商標）ペイロード（「Ｅペイロード」とも言う。）と、Ｅｔｈｅｒｎｅｔ（登録商標）ヘッダ（「Ｅヘッダ」とも言う。）とにより構成される。Ｅヘッダには、宛先ＭＡＣアドレスおよび送信元ＭＡＣアドレスが含まれる。また、Ｅペイロードには、ＩＰヘッダ、ＴＣＰ／ＵＤＰヘッダおよびデータが含まれる。ＩＰヘッダには、送信元ＩＰアドレスおよび送信先アドレスが含まれる。なお、図３では、ＩＰヘッダは、「ＩＰ　ｖ４ヘッダ」と表記している。ＴＣＰ／ＵＤＰヘッダは、ＴＣＰヘッダまたはＵＤＰヘッダを示し、ＴＣＰ／ＵＤＰヘッダには、送信元ポート番号および送信先ポート番号が含まれる。

【００６１】

ネットワークシステム３におけるＣＡＮゲートウェイ２００は、ＣＡＮバスから受信した

ＣＡＮフレームを第１ネットワーク１０へと転送する際に、複数のＣＡＮフレーム情報を含むＥフレームを送信する。ＣＡＮフレーム情報は、ＣＡＮバスで伝送されたＣＡＮフレームから抽出した情報であり、少なくともデータフィールドの内容（データ）を含む。ＣＡＮフレーム情報は、例えばＣＡＮ－ＩＤ及びサイズを含んでもよい。

【００６２】

図３に示すＥフレームのペイロード内のデータ構成例を図４に示す。図４の例では、ＣＡＮフレーム情報は、ＣＡＮ－ＩＤ、サイズ及びデータで構成される。図４のメッセージ数（ＭＳＧ数）は、ＣＡＮフレーム情報の個数を示す。なお、メッセージ数の代わりに、ＣＡＮフレーム情報の全体のデータ量等を示す情報を用いてもよい。また、ＣＡＮフラグは、Ｅフレームが第２ネットワーク２０から伝送される情報（つまりＣＡＮフレーム情報）を含むか否かを識別するための識別フラグであり、ＥフレームのＥペイロードにＣＡＮフレーム情報を含む場合においてＯＮにされ、それ以外の場合にＯＦＦ（つまりＯＮと相反する情報を示す値）にされるフラグである。図４の例では、ＥフレームのＥペイロードの先頭にＣＡＮフラグを配置する例を示しているがこれは一例に過ぎない。図４の例のような複数のＣＡＮフレーム情報をＥフレームのＥペイロードに含ませることで、例えば、伝送効率が高まり得る。

【００６３】

図５は、ＣＡＮゲートウェイの機能構成の一例を示すブロック図である。

【００６４】

同図に示すように、ＣＡＮゲートウェイ２００は、Ｅｔｈｅｒｎｅｔ（登録商標）送受信部２０１（以下、「Ｅ送受信部２０１」と言う。）と、ＣＡＮ送受信部２０２ａ、２０２ｂと、転送制御部２０３と、転送ルール保持部２０４とを備える。これらの各構成要素は、ＣＡＮゲートウェイ２００における通信回路、メモリ、デジタル回路、メモリに格納されたプログラムを実行するプロセッサ等により実現される。

【００６５】

Ｅ送受信部２０１は、第１ネットワーク１０を構成する第１伝送路１１に接続される通信回路等である。Ｅ送受信部２０１は、第１伝送路１１からＥフレームを受信する。また、Ｅ送受信部２０１は、第１伝送路１１にＥフレームを送信する。

【００６６】

ＣＡＮ送受信部２０２ａは、第２ネットワーク２０を構成するＣＡＮバス２１ａに接続される通信回路等である。ＣＡＮ送受信部２０２ａは、ＣＡＮバス２１ａからＣＡＮフレームを逐次受信する。また、ＣＡＮ送受信部２０２ａは、ＣＡＮバス２１ａにＣＡＮフレームを送信する。

【００６７】

ＣＡＮ送受信部２０２ｂは、第２ネットワーク２０を構成するＣＡＮバス２１ｂに接続される通信回路等である。ＣＡＮ送受信部２０２ｂは、ＣＡＮバス２１ｂからＣＡＮフレームを逐次受信する。ＣＡＮ送受信部２０２ｂは、ＣＡＮバス２１ｂにＣＡＮフレームを送信する。

【００６８】

転送ルール保持部２０４は、メモリ等の記憶媒体で実現され、フレームの転送の条件等を定める基準情報を保持する。基準情報は、例えば、転送対象のＣＡＮ－ＩＤ及び転送元のバスと宛先（ＭＡＣアドレス等）とを対応付けた転送ルール情報、優先転送対象のＣＡＮ－ＩＤ及び転送元のバスと宛先とを対応付けた優先転送リスト等である。

【００６９】

転送制御部２０３は、例えばプログラムを実行するプロセッサ等で実現され、受信したフレームを転送すべきか否か判定し判定結果に応じて転送に係る制御を行う。この転送に係る制御は、例えば、逐次受信した複数のＣＡＮフレームに基づいて、複数のＣＡＮフレーム情報をペイロードとして含ませたＥフレームを、Ｅ送受信部２０１に第１伝送路１１へと送信させる制御である。

【００７０】

図６は、実施の形態１に係るＣＡＮゲートウェイ２００が受信した複数のＣＡＮフレーム（ＣＡＮフレーム１～Ｎ）に基づいてＥフレームを送信するイメージを示す図である。

【００７１】

同図に示すように、ＣＡＮゲートウェイ２００はフレームを転送する際に、フレームの構成を変更する。送信されるＥフレームのペイロードには、例えば予め定められた数であるＮ個のＣＡＮフレーム情報が含まれる。そのＮ個のＣＡＮフレーム情報のデータは、受信されたＮ個のＣＡＮフレームのデータフィールドの内容（データ）等である。受信され転送待ちになっているＣＡＮフレームの内容は、例えば、ＣＡＮゲートウェイ２００が備えるメモリ等の記憶媒体（バッファ）に格納される。図６のＮ個のＣＡＮフレーム情報を含むＥフレームは、例えばセントラルゲートウェイ４００を経由して、宛先のＥＣＵまたはＤＣＵ（例えばインフォテインメントＤＣＵ３００）に受信されることになる。Ｅフレームのヘッダの送信元ＭＡＣアドレスとして、ＣＡＮゲートウェイ２００のＭＡＣアドレスが設定され、ＥフレームのＥペイロードには、ＣＡＮフレーム情報が含まれることを示す、ＯＮにしたＣＡＮフラグが設定される。Ｅフレームの宛先ＭＡＣアドレスとしては、転送ルール保持部２０４が保持する転送ルール情報等に従って、宛先となるＥＣＵまたはＤＣＵのＭＡＣアドレスが設定される。

【００７２】

なお、本実施の形態では、ＣＡＮゲートウェイ２００は、自動運転の制御コマンドの異常を検知するために、第２ネットワーク２０に流れる車両状態を示す状態情報を含むＮ個のＣＡＮフレームを結合して１つのＥフレームに変換する。本実施の形態では、ＣＡＮフレームに含まれる車両状態は、現在の車速、ステアリングの角度、シフトポジションなどである。車両状態は、移動体の状態の一例である。

【００７３】

転送制御部２０３は、判定等の結果に応じて一定条件下でＥ送受信部２０１、ＣＡＮ送受信部２０２ａ、２０２ｂを制御して、フレームの送信を行わせる。転送制御部２０３は、ＣＡＮ送受信部２０２ａ、２０２ｂにより受信されたＣＡＮフレームについて、ＣＡＮ－ＩＤに基づいてそのＣＡＮフレームのデータが第１ネットワーク１０に送信されるべきか否かを判定する。この判定は、例えば、予め定められた、ＣＡＮ－ＩＤに関する基準情報に従って行われる。また、転送制御部２０３は、ＣＡＮフレームのデータの宛先を、基準情報に従って選定する。ＣＡＮフレームが第１ネットワーク１０に送信されるべきか否かの判定及びＣＡＮフレームのデータを含むフレーム（Ｅフレーム或いはＣＡＮフレーム）の宛先の選定は、例えば、データが第１ネットワーク１０に送信されるべき１つ以上のＣＡＮフレームのＣＡＮ－ＩＤ等を示す転送ルール情報を用いて行われる。

【００７４】

図７は、自動運転ＤＣＵ１００の機能構成の一例を示すブロック図である。

【００７５】

同図に示すように、自動運転ＤＣＵ１００は、第１通信部１０１ａと、第２通信部１０１ｂと、スイッチ処理部１０２と、スイッチルール保持部１０３と、異常検知処理部１０４と、異常検知ルール保持部１０５とを有する。自動運転ＤＣＵ１００は、異常検知装置の一例である。

【００７６】

第１通信部１０１ａは、本実施の形態では１つのＥｔｈｅｒｎｅｔ（登録商標）ポート（ポートＰ１）を備える。ポートＰ１は、セントラルゲートウェイ４００と第１伝送路１１で接続されている。つまり、第１通信部１０１ａは、セントラルゲートウェイ４００との間でデータの送受信を行う。つまり、第１通信部１０１ａは、ＣＡＮフレームがデータとして格納されたＥフレームを受信する。これにより、第１通信部１０１ａは、ＣＡＮフレームを受信することで、ＣＡＮフレームに含まれる状態情報を受信する。

【００７７】

第２通信部１０１ｂは、本実施の形態では４つのＥｔｈｅｒｎｅｔ（登録商標）ポート（ポートＰ２～Ｐ５）を備える。ポートＰ２～Ｐ５は、それぞれ、カメラ１２０、ＬＩＤＡ

Ｒ１３０、ダイナミックマップＥＣＵ１４０および自動運転ＥＣＵ１１０と第１伝送路１１で接続されている。つまり、第２通信部１０１ｂは、第１ネットワーク１０の通信プロトコル（つまりＥｔｈｅｒｎｅｔ（登録商標）プロトコル）による第１フレーム（つまりＥフレーム）を送受信する。また、第２通信部１０１ｂは、ポートＰ１でのＥフレームの送受信を行う第１通信部１０１ａを含む。

【００７８】

スイッチ処理部１０２は、第２通信部１０１ｂにより受信されたＥフレームを、スイッチルール保持部１０３が保持するルールに基づき、適切な転送先に転送する処理を行う。

【００７９】

図８は、スイッチルール保持部１０３が保持するスイッチルールの一例を示す図である。

【００８０】

同図に示すように、スイッチルールは、入力ポート、送信元ＩＰアドレス、送信元ＭＡＣアドレス、出力ポート、送信先ＩＰアドレス、送信先ＭＡＣアドレスから構成される。本実施の形態のおけるスイッチルールは、正常なＥフレームの正しい転送先を示すホワイトリストである。スイッチルールでは、例えば、ポートＰ１において、ＣＡＮゲートウェイ２００からのＥフレームがセントラルゲートウェイ４００を介して受信され、ポートＰ５に接続される自動運転ＥＣＵ１１０へ転送する経路が許可されていることを示している。この場合、入力ポートとなるポートＰ１で受信するＥフレームの送信元ＭＡＣアドレスはセントラルゲートウェイ４００のＭＡＣアドレスが設定されており、送信元ＩＰアドレスはＣＡＮゲートウェイ２００のＩＰアドレスが設定されている。一方、出力ポートとなるポート５に接続されている送信先ＩＰアドレスおよび送信先ＭＡＣアドレスには、自動運転ＥＣＵのＩＰアドレスおよびＭＡＣアドレスが設定されている。

【００８１】

また、図８のスイッチルールでは、ポート２に接続されているカメラ１２０、ポート３に接続されているＬＩＤＡＲ１３０、および、ポート４に接続されているダイナミックマップＥＣＵ１４０は、ポート５に接続される自動運転ＥＣＵ１１０への転送が許可されていることを示している。また、ポート５に接続される自動運転ＥＣＵ１１０からのＥフレームは、ＣＡＮゲートウェイ２００に送信する必要があるので、送信先ＩＰにはＣＡＮゲートウェイ２００のＩＰアドレスが設定され、送信先ＭＡＣアドレスにはセントラルゲートウェイのＭＡＣアドレスが設定されている。

【００８２】

なお、スイッチルールでは、入力または出力における送信元および送信先には、ＩＰアドレスおよびＭＡＣアドレスで定義されているが、これに限定されない。例えば、ＩＰアドレスだけが定義されていてもよいし、ＭＡＣアドレスだけが定義されていてもよい。また、スイッチルールには、ＩＰアドレスまたはＭＡＣアドレス以外の送信元または送信先が識別できる情報が定義されていてもよいし、サービスポート番号が定義されてもよい。これにより、入力または出力における送信元および送信先を、スイッチルールで許可されている経路に制限することができる。

【００８３】

図８のスイッチルールは、ホワイトリストにより定義されたが、ブラックリストにより定義されてもよい。また、図８で示したスイッチルールは、一部であり、これが全てではない。つまり、スイッチルールは、必要な経路が網羅されるように設定されるものとする。

【００８４】

異常検知処理部１０４は、ＣＡＮゲートウェイ２００経由で第２ネットワーク２０から第１通信部１０１ａにより受信された車両１の状態情報と、異常検知ルール保持部１０５に保持されている異常検知ルールとを参照して、第２通信部１０１ｂにおいて受信されたＥフレームに含まれる制御コマンドが異常であるか否かを検知する。制御コマンドは、例えば、自動運転ＥＣＵ１１０が生成する自動運転制御コマンドである。異常検知処理部１０４は、制御コマンドが正常であると判断した場合、セントラルゲートウェイ４００からＣＡＮゲートウェイ２００を介して当該制御コマンドを第２通信部１０１ｂに第２ネットワ

ーク２０へ送信させる。異常検知処理部１０４は、制御コマンドが異常であると判断した場合、第２通信部１０１ｂによる制御コマンドの第２ネットワーク２０への転送を禁止する。

【００８５】

図９は、実施の形態１に係る自動運転ＤＣＵ１００の異常検知ルール保持部１０５が保持する異常検知ルールの一例を示す図である。異常検知ルールは、第２ネットワーク２０から取得される車両状態をベースにしたＥｔｈｅｒｎｅｔ（登録商標）における自動運転制御が許可されるルールである。つまり、異常検知ルールは、車両の複数の状態のそれぞれにおいて許可される制御コマンドを示す第１ルールを含む。

【００８６】

同図に示すように、異常検知ルールの第１ルールは、車両１の車速状態およびシフト状態に応じて許可される、車速指示および操舵指示の組み合わせを示す。なお、車速状態とは、車両１の走行中の速度を示し、例えば、０ｋｍ／ｈ以上３０ｋｍ／ｈ未満の速度範囲を低速、３０ｋｍ／ｈ以上６０ｋｍ／ｈ未満の速度を中速、６０ｋｍ／以上１００ｋｍ／ｈ以下を高速とそれぞれ定義したものである。また、シフト状態とは、シフトポジションを示し、例えばパーキング（Ｐ）、リバース（Ｒ）、ニュートラル（Ｎ）、ドライブ（Ｄ）などである。車速指示は、現在の車速から許可される増減の速度値を示す。また、操舵指示は、現在のステアリングの旋回角度から許可される増減の角度を示す。

【００８７】

第１ルールでは、例えば、車速状態が低速であり、かつ、シフト状態がドライブ（Ｄ）のときに、自動運転制御における車速指示が、状態情報が示す現時点の車速から１０ｋｍ／ｈの範囲であれば、車速を増減することが許可されている。また、第１ルールでは、例えば、車速状態が中速であり、かつ、シフト状態がドライブ（Ｄ）のときに、自動運転制御における車速指示が、状態情報が示す現時点の車速から２０ｋｍ／ｈの範囲であれば、車速を増減することが許可されている。また、第１ルールでは、例えば、車速状態が高速であり、かつ、シフト状態がドライブ（Ｄ）のときに、自動運転制御における車速指示が、状態情報が示す現時点の車速から３０ｋｍ／ｈの範囲であれば、車速を増減することが許可されている。

【００８８】

第１ルールでは、操舵指示のステアリングの旋回指示角度においても車速と同様に定義されている。つまり、第１ルールでは、例えば、車速状態が低速であり、かつ、シフト状態がドライブ（Ｄ）のときに、自動運転制御における操舵指示が、状態情報が示す現時点のステアリングの角度から左右３６０度以内であれば、ステアリングの角度を変更することが許可されている。また、第１ルールでは、例えば、車速状態が中速であり、かつ、シフト状態がドライブ（Ｄ）のときに、自動運転制御における操舵指示が、状態情報が示す現時点のステアリングの角度から左右１８０度以内であれば、ステアリングの角度を変更することが許可されている。また、第１ルールでは、例えば、車速状態が高速であり、かつ、シフト状態がドライブ（Ｄ）のときに、自動運転制御における操舵指示が、状態情報が示す現時点のステアリングの角度から左右９０度以内であれば、ステアリングの角度を変更することが許可されている。

【００８９】

異常検知処理部１０４は、状態情報が示す車両１の状態が、制御コマンドが第１ルールにおいて対応付けられている状態に含まれない場合、制御コマンドが異常であることを検知する。つまり、異常検知処理部１０４は、例えば、車両状態に第１ルールにおいて対応付けられている、許可される範囲の車速の増減を超える車速指示、または、許可される範囲のステアリングの角度を超える操舵指示を含む制御コマンドが第２通信部１０１ｂにより受信された場合、当該制御コマンドが異常であることを検知し、第１通信部１０１ａによる第２ネットワーク２０への当該制御コマンドの転送を禁止する。

【００９０】

次に、実施の形態１に係る車両１に搭載されるネットワークシステム３の動作について説

明する。
【００９１】
図１０および図１１は、実施の形態１に係るネットワークシステム３における異常検知方法の一例を示すシーケンス図である。
【００９２】
まず、自動運転ＤＣＵ１００は、自動運転ＥＣＵ１１０に対して、自動運転モードを有効な状態にする（Ｓ１００）。例えば、ユーザからの自動運転モードをＯＮにする入力を受け付けた場合、自動運転ＤＣＵ１００は、自動運転モードを有効な状態にする。
【００９３】
ＣＡＮゲートウェイ２００は、ＣＡＮゲートウェイ２００に接続されている各ＥＣＵ２１０、２２０、２３０、２４０から車両１の状態情報を含むＣＡＮフレームを受信し、図６に示したように、車両１の状態情報のＣＡＮフレームを含んだＥフレームを生成する（Ｓ１０１）。
【００９４】
ＣＡＮゲートウェイ２００は、車両１の状態情報のＣＡＮフレームを含むＥフレームをセントラルゲートウェイ４００に送信する（Ｓ１０２）。
【００９５】
セントラルゲートウェイ４００は、ステップＳ１０２において受信したＥフレームを自動運転ＤＣＵ１００に送信する（Ｓ１０３）。
【００９６】
自動運転ＤＣＵ１００では、第２通信部１０１ｂがカメラ１２０により撮影された映像を示す映像情報、ＬＩＤＡＲ１３０により検出された物体までの距離を示す情報に基づく障害物情報、ダイナミックマップＥＣＵ１４０により得られる地図情報を、それぞれカメラ１２０、ＬＩＤＡＲ１３０およびダイナミックマップＥＣＵ１４０から受信する（Ｓ１０４）。
【００９７】
自動運転ＤＣＵ１００では、スイッチ処理部１０２が、スイッチルール保持部１０３のスイッチルールを参照して、正しい経路で情報を受信したか否かを判定する（Ｓ１０５）。
【００９８】
これにより、自動運転ＤＣＵ１００では、ステップＳ１０４において第２通信部１０１ｂは、カメラ１２０、ＬＩＤＡＲ１３０、ダイナミックマップＥＣＵ１４０から受信した映像情報、障害物情報および地図情報などの情報のうち、正しい経路で受信したとスイッチ処理部１０２により判定された情報を、自動運転ＥＣＵ１１０に転送する（Ｓ１０６）。
【００９９】
自動運転ＥＣＵ１１０は、ステップＳ１０６で受信した映像情報、障害物情報および地図情報などの情報に基づいて、自動運転のための制御コマンドを生成する（Ｓ１０７）。ここでは、自動運転ＥＣＵ１１０は、まず制御系ＣＡＮバスに伝えるためのＣＡＮフレームを生成し、それらＣＡＮフレームをＥフレームのデータ領域に格納したＥフレームを生成する。生成されたＥフレームは、自動運転のための制御コマンドである。
【０１００】
自動運転ＥＣＵ１１０は、自動運転のための制御コマンドを自動運転ＤＣＵ１００に送信する（Ｓ１０８）。
【０１０１】
自動運転ＤＣＵ１００では、異常検知処理部１０４は、異常検知ルール保持部１０５が保持する異常検知ルールを参照する（Ｓ１０９）。ここで参照するルールは、図９で示した第１ルールである。
【０１０２】
自動運転ＤＣＵ１００では、異常検知処理部１０４は、異常検知ルールに加えて、さらにＳ１０３で受信した車両１の状態情報のＣＡＮフレームを含んだＥフレームを参照し、ステップＳ１０８によって第２通信部１０１ｂが受信した制御コマンドが異常であるか否か

を判定する（Ｓ１１０）。異常検知処理部１０４は、制御コマンドが異常であると判定した場合（ステップＳ１１０で異常）、ステップＳ１１１へ処理を移す。一方で、異常検知処理部１０４は、制御コマンドが正常であると判定した場合（ステップＳ１１０で正常）、ステップＳ１２０へ処理を移す。

【０１０３】

自動運転ＤＣＵ１００では、異常検知処理部１０４は、制御コマンドが異常であると判定したため、サーバ２またはＩＶＩ３１０に異常があったことを含む情報を、第２通信部１０１ｂを用いて通知する（Ｓ１１１）。これにより、ドライバ、または、リモートで監視しているセキュリティ監視サービスの事業者は、車両１に自動運転において異常が発生したことを把握することが可能になる。なお、この場合、異常検知処理部１０４は、制御コマンドをセントラルゲートウェイ４００に送信しない。つまり、異常検知処理部１０４は、この場合、異常であると判定した制御コマンドを、セントラルゲートウェイ４００およびＣＡＮゲートウェイ２００を介して第２ネットワーク２０に転送することを禁止する。

【０１０４】

自動運転ＤＣＵ１００では、異常検知処理部１０４は、自動運転ＥＣＵ１１０に、自動運転を終了させる終了指示を、第２通信部１０１ｂを用いて送信する（Ｓ１１２）。

【０１０５】

自動運転ＥＣＵ１１０は、ステップＳ１１２において送信された終了指示を受信した場合、自動運転モードを終了する（Ｓ１１３）。なお、自動運転ＥＣＵ１１０は、自動運転モードを終了した後に、手動運転モードに切り替えてもよい。

【０１０６】

ステップＳ１１０において、制御コマンドが正常であると判定された場合（Ｓ１１０で正常）、異常検知処理部１０４は、第２通信部１０１ｂを用いて、自動運転のための制御コマンドをセントラルゲートウェイ４００に送信する（Ｓ１２０）。

【０１０７】

セントラルゲートウェイ４００は、ステップＳ１２０において送信された自動運転制御コマンドをＣＡＮゲートウェイ２００に転送する（Ｓ１２１）。

【０１０８】

ＣＡＮゲートウェイ２００は、ステップＳ１２１で受信したＥフレームの自動運転の制御コマンドをＣＡＮフレームに変換する（Ｓ１２２）。

【０１０９】

ＣＡＮゲートウェイ２００は、ステップＳ１２２で変換したＣＡＮフレームを第２ネットワーク２０に送信する（Ｓ１２３）。これにより、制御系ＣＡＮバスに接続されるエンジンＥＣＵ２１０、ステアリングＥＣＵ２２０またはブレーキＥＣＵ２３０は、ＣＡＮフレームの自動運転の制御コマンドを受信し、受信した制御コマンドに応じた制御を実行することで自動運転制御を行う。

【０１１０】

本実施の形態に係る異常検知装置は、車両１に搭載され、通信プロトコルが互いに異なる第１ネットワーク１０および第２ネットワーク２０を有するネットワークシステム３における異常を検知する異常検知装置である。自動運転ＤＣＵ１００は、第１通信部１０１ａと、第２通信部１０１ｂと、異常検知ルール保持部１０５と、異常検知処理部１０４とを備える。第１通信部１０１ａは、第２ネットワーク２０から取得される車両１の状態を示す状態情報を受信する。第２通信部１０１ｂは、第１ネットワーク１０の通信プロトコルによるＥフレームを送受信する。異常検知ルール保持部１０５は、異常検知ルールを保持する。異常検知処理部１０４は、状態情報と、異常検知ルールとを参照して、第２通信部１０１ｂにおいて受信されたＥフレームに含まれる制御コマンドが異常であるか否かを検知する。異常検知処理部１０４は、制御コマンドが異常であることを検知した場合、当該制御コマンドの転送を禁止する。

【０１１１】

これによれば、異常検知装置は、第２ネットワーク２０から得られる車両１の状態情報と

、異常検知ルールとに基づき、生成された自動運転の制御コマンドが異常であるか否かを検知する。そして、異常検知装置は、異常があることを検知された制御コマンドの転送を禁止する。このため、例えば第１ネットワーク１０に接続される機器に脆弱性があって、第１ネットワーク１０経由で攻撃をされた場合であっても、異常検知装置は、不正な自動運転の制御を防止することが可能となる。

【０１１２】

また、本実施の形態に係る異常検知装置において、異常検知ルールは、車両１の異なる複数の状態のそれぞれにおいて許可される制御コマンドを示す第１ルールを含む。異常検知処理部１０４は、状態情報が示す車両１の状態が、制御コマンドが第１ルールにおいて対応付けられている状態に含まれない場合、制御コマンドが異常であることを検知する。このため、例えば、現時点の車速、ステアリングの操舵角度、シフトポジションなどの車両状態に基づいて制御コマンドの異常を検知することが可能となる。

【０１１３】

また、本実施の形態に係る異常検知装置において、制御コマンドは、進む、曲がる、および、止まるの少なくとも１つを車両１に実行させる制御コマンドである。このため、異常検知装置は、例えば、走行中の急ハンドル、急ブレーキまたは急加速、停車中の急発信など、自動運転における制御コマンドの異常を検知し、安全な運転環境を提供することが可能となる。

【０１１４】

また、本実施の形態に係る異常検知装置において、第１通信部１０１ａは、ＣＡＮフレームがデータとして格納されたＥフレームである第１フレームを受信する。また、第２通信部１０１ｂは、第１通信部１０１ａを含む。これによれば、異常検知装置は、Ｅフレームに変換されたＣＡＮフレームを受信するため、Ｅｔｈｅｒｎｅｔ（登録商標）上の機器でＣＡＮフレームの異常検知が可能となる。

【０１１５】

（実施の形態２）

次に実施の形態２について説明する。実施の形態２に係る異常検知装置としての自動運転ＤＣＵ１００は、実施の形態１に係る自動運転ＤＣＵ１００とほぼ同等であるので、異なる部分のみを説明する。実施の形態２では、自動運転ＤＣＵ１００にて、ＣＡＮフレームの異常検知も行う点が実施の形態１に係る自動運転ＤＣＵ１００と異なる。

【０１１６】

図１２は、実施の形態２に係るＣＡＮゲートウェイ２００が受信した複数のＣＡＮフレームに基づいてＥフレームを送信するイメージを示す図である。

【０１１７】

本実施の形態では、自動運転ＤＣＵ１００は、ＣＡＮフレームの周期を確認してＣＡＮの異常検知を行う。図１２に示すように、ＣＡＮゲートウェイ２００は、複数のＣＡＮフレームを受信し、受信した複数のＣＡＮフレームのそれぞれについて、当該ＣＡＮフレームを受信した受信時刻を当該ＣＡＮフレームに付与する。つまり、ＣＡＮゲートウェイ２００は、Ｎ個の受信時刻が付与されたＣＡＮフレームをＥフレームのデータ領域に格納することでＥフレームを生成する。実施の形態１と同様に、ＣＡＮゲートウェイ２００が、Ｅフレーム化するＣＡＮフレームに含まれる車両１の状態情報は、車速、ステアリングの角度またはシフトポジションなどである。

【０１１８】

自動運転ＤＣＵ１００の第２通信部１０１ｂは、図１２の構成のＥフレームを受信するため、複数のＣＡＮフレームと、複数のＣＡＮフレームのそれぞれが例えばＣＡＮゲートウェイ２００などの機器により受信された時刻である受信時刻とがデータとして格納されたＥフレームを受信することとなる。

【０１１９】

図１３は、実施の形態２に係る自動運転ＤＣＵ１００の異常検知ルール保持部１０５が保持する異常検知ルールの一例を示す図である。図１３に示す異常検知ルールは、ＣＡＮフ

レームが異常であるか否かを検知するための第２ルールの一例である。
【０１２０】
同図に示すように、第２ルールは、ＣＡＮフレームのデータの種類を示す識別子であるＣＡＮ－ＩＤに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示す。また、第２ルールは、さらに、複数のＣＡＮ－ＩＤのそれぞれに対応するＣＡＮフレームおいて許可される変化量であって、当該ＣＡＮフレームの１つ前のＣＡＮフレームのデータ値からの変化量を示してもよい。当該ＣＡＮフレームの１つ前のＣＡＮフレームとは、同一のＣＡＮ－ＩＤにおいて、当該ＣＡＮフレームよりも１タイミング前に受信されたＣＡＮフレームである。
【０１２１】
第２ルールは、具体的には、図１２で説明したＥフレームに付与されたＣＡＮフレームの受信時刻を参照して算出された周期が、ＣＡＮ－ＩＤが「０ｘＡ１」であるＣＡＮフレームにおいて、基本周期１０ｍｓ±３ｍｓの範囲である、つまり、１つ前に受信されたＣＡＮフレームからの受信時刻の差分が基本周期１０ｍｓ±３ｍｓの範囲内であれば正しい周期であることを示すルールである。また、第２ルールは、ＣＡＮ－ＩＤが「０ｘＡ１」であるＣＡＮフレームにおいて、１つ前に受信されたＣＡＮフレームからのデータの変化量が±５０であれば正しい変化量であることを示すルールであってもよい。他のＩＤに対しても同様に、許可される周期の範囲およびデータの変化量が定義されている。
【０１２２】
なお、第２ルールで定義されているデータ値の変化量は、車両１の状態情報と対応する数値であり、例えば、車速の変化量、ステアリングの角度の変化量などである。
【０１２３】
第２ルールを用いる場合、自動運転ＤＣＵ１００の異常検知処理部１０４は、第２通信部１０１ｂにより受信されたＥフレームから得られる複数のＣＡＮフレームにそれぞれ対応する複数の受信時刻を用いて、当該Ｅフレームに含まれる複数のＣＡＮフレームが異常であるか否かを検知する。具体的には、異常検知処理部１０４は、互いに同じ識別子を有する複数のＣＡＮフレームのうちの、第１ＣＡＮフレームの第１受信時刻と、第２ＣＡＮフレームの第２受信時刻とを比較することで第１ＣＡＮフレームに異常があるか否かを検知する。異常検知処理部１０４は、第１受信時刻の第２受信時刻からの差分が、第２ルールにおいて上記同じ識別子に対応付けられている受信周期の範囲外である場合、第１ＣＡＮフレームが異常であることを検知する。
【０１２４】
また、異常検知処理部１０４は、第１ＣＡＮフレームの第１データ値の、第２ＣＡＮフレームの第２データ値からの差分が、第２ルールにおいて前記同じ識別子に対応付けられている変化量を超える場合、第１ＣＡＮフレームが異常であることを検知してもよい。
【０１２５】
そして、異常検知処理部１０４は、ＣＡＮフレームが異常であることを検知した場合、制御コマンドの転送を禁止する。つまり、異常検知処理部１０４は、この場合、この時点で自動運転ＥＣＵ１１０から受信した制御コマンドの転送を禁止してもよいし、この時点以降で自動運転ＥＣＵ１１０から受信した制御コマンドの転送を禁止してもよい。
【０１２６】
次に、実施の形態２に係る車両１に搭載されるネットワークシステム３の動作について説明する。
【０１２７】
図１４および図１５は、実施の形態２に係るネットワークシステム３における異常検知方法の一例を示すシーケンス図である。実施の形態２に係る異常検知方法では、ステップＳ２００～Ｓ２０８までは、ステップＳ２０１のみにおいて図１２で示すＣＡＮフレームの受信時刻をＥフレームに含める点が実施の形態１に係る異常検知方法のステップＳ１０１と異なるが、他のステップＳ２００、Ｓ２０２～Ｓ２０８は、実施の形態１に係る異常検知方法におけるＳ１００、Ｓ１０２～Ｓ１０８と同様であるので説明を省略する。

【０１２８】
自動運転ＤＣＵ１００では、異常検知処理部１０４は、異常検知ルール保持部１０５が保持する異常検知ルールを参照する。ここで参照するルールは、図１３に示した第２ルールである。
【０１２９】
自動運転ＤＣＵ１００では、異常検知処理部１０４は、ＣＡＮフレームが異常であるか否かを判定する（Ｓ２１０）。異常検知処理部１０４は、ＣＡＮフレームが異常であると判定した場合（ステップＳ２１０で異常）、ステップＳ２１３へ処理を移す。異常検知処理部１０４は、ＣＡＮフレームが正常であると判定した場合（ステップＳ２１０で正常）、ステップＳ２１１へ処理を移す。
【０１３０】
自動運転ＤＣＵ１００では、異常検知処理部１０４は、ＣＡＮフレームの異常を検知したため、自動制御を継続するのはリスクが高いと判断し、サーバ２またはＩＶＩ３１０に対して異常があったことを含む情報を、第２通信部１０１ｂを用いて通知する（Ｓ２１３）。なお、この場合、異常検知処理部１０４は、制御コマンドをセントラルゲートウェイ４００に送信しない。つまり、異常検知処理部１０４は、この場合、異常であると判定した制御コマンドを、セントラルゲートウェイ４００およびＣＡＮゲートウェイ２００を介して第２ネットワーク２０に転送することを禁止する。
【０１３１】
ステップＳ２１１、Ｓ２１２、Ｓ２１４およびＳ２１５は、それぞれ、実施の形態１に係る異常検知方法におけるステップＳ１０９、Ｓ１１０、Ｓ１１２およびＳ１１３と同様であるので説明を省略する。また、ステップＳ２２１～Ｓ２２４は、実施の形態１に係る異常検知方法におけるＳ１２０～Ｓ１２３と同様であるので説明を省略する。
【０１３２】
なお、ステップＳ２１０の後にステップＳ２１２が行われるフローとなっているが、ステップＳ２１２の後にステップＳ２１０が行われても良い。
【０１３３】
本実施の形態に係る異常検知装置において、異常検知ルールは、さらに、ＣＡＮフレームが異常であるか否かを検知するための第２ルールを含む。異常検知処理部１０４は、さらに、ＣＡＮフレームが異常であることを検知した場合、制御コマンドの転送を禁止する。これにより、異常検知装置は、ＣＡＮフレームの異常を検知した上で、制御コマンドの実行が可能となる。つまり、第２ネットワーク２０側が正常であることを第１ネットワーク１０側の機器である異常検知装置でも確認した上で、自動運転制御コマンドの送信を判断することが可能になる。このため、異常検知装置は、第２ネットワーク２０の脆弱性をついた攻撃中であっても、不正な自動運転の制御を防止することが可能となる。
【０１３４】
また、本実施の形態に係る異常検知装置において、第２ルールは、複数の識別子のそれぞれに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示す。第２通信部１０１ｂは、複数のＣＡＮフレームと、複数のＣＡＮフレームのそれぞれが第１ネットワーク１０上の機器により受信された時刻である受信時刻とがデータとして格納されたＥフレームを受信する。異常検知処理部１０４は、複数のＣＡＮフレームにそれぞれ対応する複数の受信時刻を用いて、互いに同じ識別子を有する複数のＣＡＮフレームのうちで、第１ＣＡＮフレームの第１受信時刻の、第１ＣＡＮフレームよりも１つ前に受信された第２ＣＡＮフレームの第２受信時刻からの差分が、第２ルールにおいて上記同じ識別子に対応付けられている受信周期の範囲外である場合、第１ＣＡＮフレームが異常であることを検知する。これにより、異常検知装置は、第２ネットワーク２０上において異常が発生している場合であっても、第１ネットワーク１０における機器において周期性を持つＣＡＮフレームの異常を検知できるため、自動運転を停止することが可能となる。
【０１３５】
また、本実施の形態に係る異常検知装置において、第２ルールは、さらに、複数の前記識

別子のそれぞれに対応するＣＡＮフレームおいて許可される１つ前のＣＡＮフレームのデータ値からの変化量を示す。異常検知処理部１０４は、さらに、第１ＣＡＮフレームの第１データ値の、第２ＣＡＮフレームの第２データからの差分が、第２ルールにおいて上記同じ識別子に対応付けられている変化量を超える場合、第１ＣＡＮフレームが異常であることを検知する。これにより、異常検知装置は、第２ネットワーク２０上において異常が発生している場合であっても、第１ネットワーク１０における機器においてＣＡＮフレームのデータ値の異常を検知できるため、自動運転を停止することが可能となる。

【０１３６】

（実施の形態３）

次に実施の形態３について説明する。実施の形態３に係る異常検知装置としての自動運転ＤＣＵ１００は、ＣＡＮフレームの異常検知を行う点は実施の形態２に係る自動運転ＤＣＵとほぼ同じであるが、異常検知のルールを、Ｅフレーム内で指定できるようにしている点が異なる。

【０１３７】

図１６は、実施の形態３に係るＣＡＮゲートウェイ２００が受信した複数のＣＡＮフレームに基づいてＥフレームを送信するイメージを示す図である。

【０１３８】

図１７は、実施の形態３に係る自動運転ＤＣＵ１００にて、ＣＡＮの異常検知をするときの異常検知ルールを定義したテーブルを示すである。

【０１３９】

図１６のＥフレームの中において、異常検知ルールとしてルール１が定義されているＣＡＮフレームであれば、自動運転ＤＣＵ１００の異常検知処理部１０４は、当該ＣＡＮフレームと同じＣＡＮ－ＩＤを有するＣＡＮフレームの周期をチェックして、異常検知を行う。異常検知処理部１０４は、ルール１を用いる場合、実施の形態２で説明したＣＡＮフレームの受信時刻を参照して算出された周期と、第２ルールとを用いて異常検知を行う。

【０１４０】

また、検知ルールとしてルール２が定義されているＣＡＮフレームであれば、自動運転ＤＣＵ１００の異常検知処理部１０４は、当該ＣＡＮフレームのデータ値の変化量をチェックして、異常検知を行う。異常検知処理部１０４は、ルール２を用いる場合、実施の形態２で説明したＣＡＮフレームのデータ値と、第２ルールとを用いて異常検知を行う。

【０１４１】

また、検知ルールとしてルール３が定義されているＣＡＮフレームであれば、自動運転ＤＣＵ１００の異常検知処理部１０４は、当該ＣＡＮフレームのメッセージ認証コード（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｃｔｉｃａｔｉｏｎ Ｃｏｄｅ）をチェックして、異常検知を行う。ルール３の場合、自動運転ＤＣＵ１００は、認証するためのＭＡＣ鍵を事前に共有されていることが前提となる。つまり、この場合、異常検知処理部１０４は、メッセージ認証コードと、ＭＡＣ鍵と、が一致すれば正常と判断し、一致しなければ異常と判断する。

【０１４２】

このように、異常検知処理部１０４は、複数の識別子のそれぞれに対応付けられたルールを異常検知ルールとして取得する。そして、異常検知処理部１０４は、異常検知ルールを参照して、ＣＡＮフレームが異常であることを検知する。

【０１４３】

これにより、異常検知装置は、ＣＡＮフレーム毎に検知ルールを設定することが可能になる。例えば第２ネットワーク２０側の負荷が高く、第２ネットワーク２０側で検知処理が難しい場合は、第１ネットワーク１０上の機器で第２ネットワーク２０における異常を検知することができる。

【０１４４】

なお、ＣＡＮゲートウェイ２００は、複数のＣＡＮフレームを受信し、受信した複数のＣＡＮフレームのそれぞれについて、当該ＣＡＮフレームのＣＡＮ－ＩＤに対応付けられた異常検知のルールを付与してもよい。ここで、ＣＡＮゲートウェイ２００が付与する異常

検知のルールは、例えば、実施の形態２における図１３で説明した第２ルールであってもよい。ＣＡＮゲートウェイ２００は、第２ルールのうちのＣＡＮ－ＩＤに対応するルールを付与してもよいし、第２ルールの全てを付与してもよい。

【０１４５】

また、図１７で説明した異常検知ルールは、自動運転ＤＣＵ１００の異常検知ルール保持部１０５が保持していてもよく、この場合、当該異常検知ルールは、ＣＡＮ－ＩＤ毎に対応付けられている。

【０１４６】

（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。

【０１４７】

（１）上記の実施の形態では、車載ネットワークでＣＡＮプロトコルに従って、データフレームの伝送が行われるものとしたが、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を包含する広義の意味のものと扱われることとしてもよい。また、車載ネットワークは、ＣＡＮプロトコル以外のプロトコルを用いるものであってもよい。車両の制御のためのフレーム等の伝送がなされる車載ネットワークのプロトコルとして、例えばＬＩＮ（Ｌｏｃａｌ Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｎｅｔｗｏｒｋ）、ＭＯＳＴ（登録商標）（Ｍｅｄｉａ Ｏｒｉｅｎｔｅｄ Ｓｙｓｔｅｍｓ Ｔｒａｎｓｐｏｒｔ）、ＦｌｅｘＲａｙ（登録商標）、Ｅｔｈｅｒｎｅｔ（登録商標）等を用いてもよい。また、これらのプロトコルを用いたネットワークをサブネットワークとして、複数種類のプロトコルに係るサブネットワークを組み合わせて、車載ネットワークを構成してもよい。また、Ｅｔｈｅｒｎｅｔ（登録商標）プロトコルは、ＩＥＥＥ８０２．１に係るＥｔｈｅｒｎｅｔ（登録商標）ＡＶＢ（Ａｕｄｉｏ Ｖｉｄｅｏ Ｂｒｉｄｇｉｎｇ）、或いは、ＩＥＥＥ８０２．１に係るＥｔｈｅｒｎｅｔ（登録商標）ＴＳＮ（Ｔｉｍｅ Ｓｅｎｓｉｔｉｖｅ Ｎｅｔｗｏｒｋｉｎｇ）、Ｅｔｈｅｒｎｅｔ（登録商標）／ＩＰ（Ｉｎｄｕｓｔｒｉａｌ Ｐｒｏｔｏｃｏｌ）、ＥｔｈｅｒＣＡＴ（登録商標）（Ｅｔｈｅｒｎｅｔ（登録商標） ｆｏｒ Ｃｏｎｔｒｏｌ Ａｕｔｏｍａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ）等の派生的なプロトコルを包含する広義の意味のものと扱われることとしてもよい。なお、車載ネットワークのネットワークバスは、例えば、ワイヤ、光ファイバ等で構成される有線通信路であり得る。例えば、フレーム伝送阻止装置２４００は、上述のいずれかのプロトコルを用いてＥＣＵが通信するネットワークシステムでネットワークバスに接続され、フレームを受信し、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、受信されたフレームが所定条件を満たす場合にそのフレームの伝送を阻止する所定処理を実行するか否かを切り替えるようにしてもよい。

【０１４８】

（２）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フォーマットであっても良く、データフレームのＩＤは、拡張ＩＤフォーマットでの拡張ＩＤ等であってもよい。また、上述したデータフレームは、ＣＡＮ以外のプロトコルが用いられるネットワークにおける一種のフレームであっても良く、この場合に、そのフレームの種類等を識別するＩＤが、データフレームのＩＤに相当する。

【０１４９】

（３）上記の実施の形態では、自動運転制御コマンドの不正を防止していたが、駐車支援システムやレーンキープ機能や衝突防止機能などの先進運転支援システムの制御の異常を検知するようにしてもよい。

【０１５０】
（４）上記実施の形態では、異常検知時にサーバ２やＩＶＩ（Ｉｎ－Ｖｅｈｉｃｌｅ Ｉｎｆｏｔａｉｎｍｅｎｔ）３１０に異常通知していたが、Ｖ２ＸやＶ２Ｉによる通信が可能であれば、車車間通信や路車間通信に対応してれば、他の車両に異常通知や、インフラ装置に異常通知してもよい。これにより自車周辺の車両や通行人の保有デバイスに異常を通知することができ、事故防止につなげることが可能となる。
【０１５１】
（５）上記実施の形態では、異常検知時にサーバ２やＩＶＩ（Ｉｎ－Ｖｅｈｉｃｌｅ Ｉｎｆｏｔａｉｎｍｅｎｔ）３１０に異常通知していたが、車載ネットワーク上のデバイスにログとして残すようにしてもよい。ログに残した場合は、診断ポートからログを読み出すことで、ディーラが異常内容を把握することが可能になる。また、ログを定期的にサーバ２に送信するようにしてもよい。これにより、リモートで車両の異常検知が可能となる。
【０１５２】
（６）上記実施の形態では、ＣＡＮゲートウェイが車両の状態情報のＣＡＮフレームをＥフレームのデータに格納しているが、車両の状態情報が識別できる形であれば、ＣＡＮフレームのフォーマットでなくてもよい。
【０１５３】
（７）上記実施の形態では、自動運転ＤＣＵ１００が第２伝送路２１と接続されていないが、自動運転ＤＣＵが第２伝送路と接続されてもよい。この場合、第２伝送路上に流れるＣＡＮフレームを読み込み、車両の状態情報を受信してもよい。さらにこの場合、自動運転制御コマンドも直接第２伝送路に対して送信するようにしてもよい。
【０１５４】
（８）上記実施の形態では、図９の自動運転の制御コマンドの異常検知ルール、または、図１３の異常検知ルールは、ホワイトリストとして正常な条件を定義しているが、ブラックリストとして定義された第３ルールであってもよい。
【０１５５】
例えば、実施の形態２においては、ホワイトリストが定義された第２ルールの代わりにブラックリストが定義された第３ルールが異常検知ルールとして用いられてもよい。
【０１５６】
第３ルールは、ＣＡＮフレームのデータの種類を示す識別子であるＣＡＮ－ＩＤに対応するＣＡＮフレームおいて許可されるＣＡＮフレームの受信周期の範囲を示す。また、第３ルールは、さらに、複数の前記識別子のそれぞれに対応するＣＡＮフレームおいて許可される変化量であって、当該ＣＡＮフレームの１つ前のＣＡＮフレームのデータ値からの変化量を示す。
【０１５７】
第３ルールを用いる場合、自動運転ＤＣＵ１００の異常検知処理部１０４は、第２通信部１０１ｂにより受信されたＥフレームから得られる複数のＣＡＮフレームにそれぞれ対応する複数の受信時刻を用いて、当該Ｅフレームに含まれる複数のＣＡＮフレームが異常であるか否かを検知する。具体的には、異常検知処理部１０４は、互いに同じ識別子を有する複数のＣＡＮフレームのうちの、第１ＣＡＮフレームの第１受信時刻と、第２ＣＡＮフレームの第２受信時刻とを比較することで第１ＣＡＮフレームに異常があるか否かを検知する。異常検知処理部１０４は、第１受信時刻の第２受信時刻からの差分が、第２ルールにおいて上記同じ識別子に対応付けられている受信周期の範囲内である場合、第１ＣＡＮフレームが異常であることを検知する。
【０１５８】
これにより、異常検知装置は、第２ネットワーク２０上において異常が発生している場合であっても、第１ネットワーク１０における機器において周期性を持つＣＡＮフレームの異常を検知できるため、自動運転を停止することが可能となる。
【０１５９】
また、異常検知処理部１０４は、前記第１ＣＡＮフレームの第１データ値の、第２ＣＡＮ

フレームの第２データ値からの差分が、第３ルールにおいて前記同じ識別子に対応付けられている変化量の範囲内である場合、第１ＣＡＮフレームが異常であることを検知してもよい。

【０１６０】

これにより、異常検知装置は、第２ネットワーク２０上において異常が発生している場合であっても、第１ネットワーク１０における機器においてＣＡＮフレームのデータ値の異常を検知できるため、自動運転を停止することが可能となる。

【０１６１】

また、異常検知ルールは、ホワイトリストとブラックリストを合わせて異常検知をしてもよい。

【０１６２】

（９）上記実施の形態では、図８のスイッチルールは、正常な送信元、送信先のＩＰとＭＡＣアドレスとポート番号をホワイトリスト形式で定義しているが、ブラックリリストとして定義されていてもよい。また、スイッチルールに定義されるルールとして、流量、通信頻度、ペイロードの値の条件が定義されていてもよい。

【０１６３】

（１０）上記実施の形態では、フレーム異常検知装置が、車両に搭載され、車両の制御のための通信を行う車載ネットワークシステムに含まれる例を示したが、車両以外の移動体の制御対象の制御のためのネットワークシステムに含まれるものであってもよい。つまり、移動体は、例えば、ロボット、航空機、船舶、機械、建設機械、農作業機器、ドローン等である。

【０１６４】

（１１）上記実施の形態で示したＥＣＵ等の各装置は、メモリ、プロセッサ等の他に、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、マウス等を備えるものであってもよい。また、上記実施の形態で示したＥＣＵ等の各装置は、メモリに記憶された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その各装置の機能を実現するものであってもよいし、専用のハードウェア（デジタル回路等）によりプログラムを用いずにその機能を実現するものであってもよい。また、その各装置内の各構成要素の機能分担は変更可能である。

【０１６５】

（１２）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又は全部は、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等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。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よいし、一部又は全部を含むように１チップ化されてもよい。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よい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。更には、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得る。

【０１６６】

（１３）上記各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又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カード又は前記モジュー

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。ＩＣカード又は前記モジュールは、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従って動作することにより、ＩＣカード又はモジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

【０１６７】

（１４）本開示の一態様としては、異常検知の方法をコンピュータにより実現するプログラム（コンピュータプログラム）であるとしてもよいし、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よい。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又は前記デジタル信号をコンピュータで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。また、本開示の一態様としては、コンピュータプログラム又はデジタル信号を、電気通信回線、無線又は有線通信回線、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。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、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従って動作するとしてもよい。また、プログラム若しく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、又は、プログラム若しくはデジタル信号を、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。

【０１６８】

（１５）上記実施の形態及び上記変形例で示した各構成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】

【０１６９】

本開示にかかる異常検知装置は、効果的に異常を検知することができる異常検知装置および異常検知方法等として有用である。

【符号の説明】

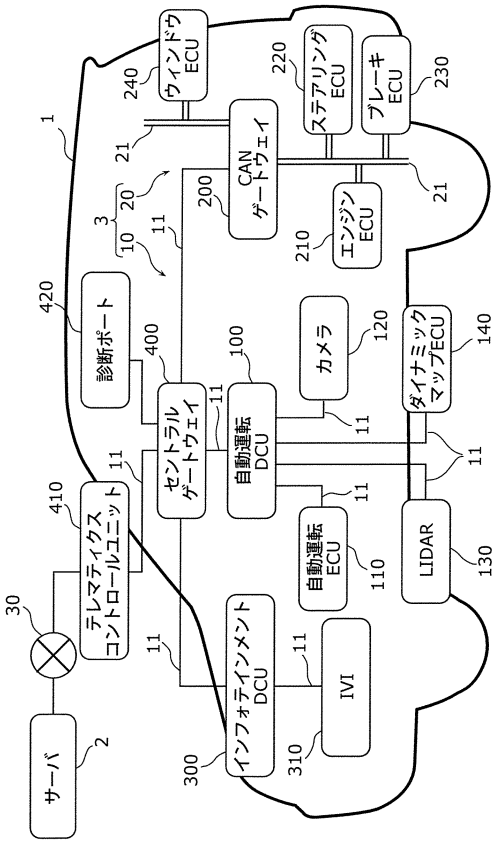
【０１７０】

１　車両
２　サーバ
３　ネットワークシステム
１０　第１ネットワーク
１１　第１伝送路
２０　第２ネットワーク
２１　第２伝送路
２１ａ、２１ｂ　ＣＡＮバス
３０　外部ネットワーク
１００　自動運転ＤＣＵ
１０１ａ　第１通信部
１０１ｂ　第２通信部
１０２　スイッチ処理部
１０３　スイッチルール保持部
１０４　異常検知処理部
１０５　異常検知ルール保持部
１１０　自動運転ＥＣＵ
１２０　カメラ
１３０　ＬＩＤＡＲ

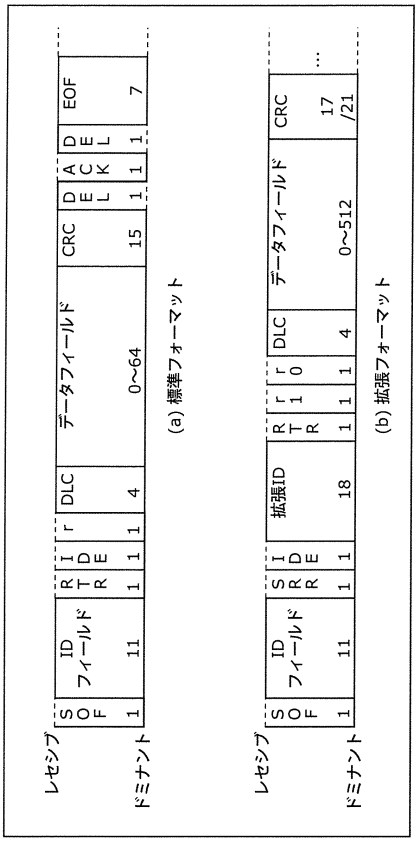
１４０　ダイナミックマップＥＣＵ
２００　ＣＡＮゲートウェイ
２０１　Ｅ送受信部
２０２ａ、２０２ｂ　ＣＡＮ送受信部
２０３　転送制御部
２０４　転送ルール保持部
２１０　エンジンＥＣＵ
２２０　ステアリングＥＣＵ
２３０　ブレーキＥＣＵ
２４０　ウィンドウＥＣＵ
３００　インフォテインメントＤＣＵ
３１０　ＩＶＩ
４００　セントラルゲートウェイ
４１０　テレマティクスコントロールユニット
４２０　診断ポート
Ｐ１～Ｐ５　ポート

【図面】

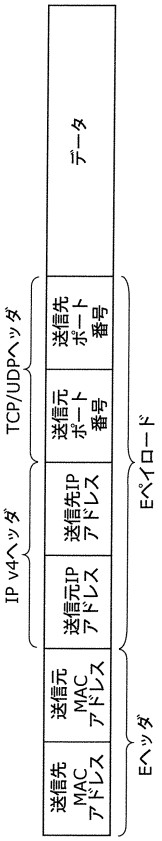
【図１】



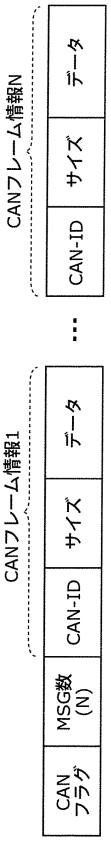
【図２】



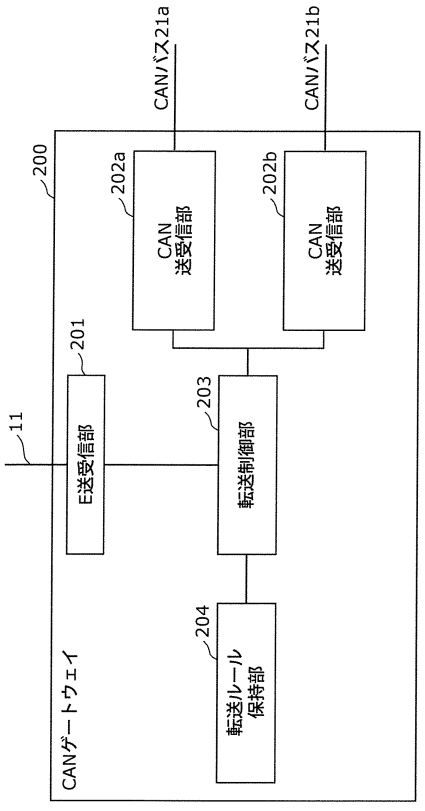
【図３】


送信先MACアドレス
送信元MACアドレス
送信元IPアドレス
送信先IPアドレス
送信元ポート番号
送信先ポート番号
データ
Eヘッダ
IP v4ヘッダ
TCP/UDPヘッダ
Eペイロード

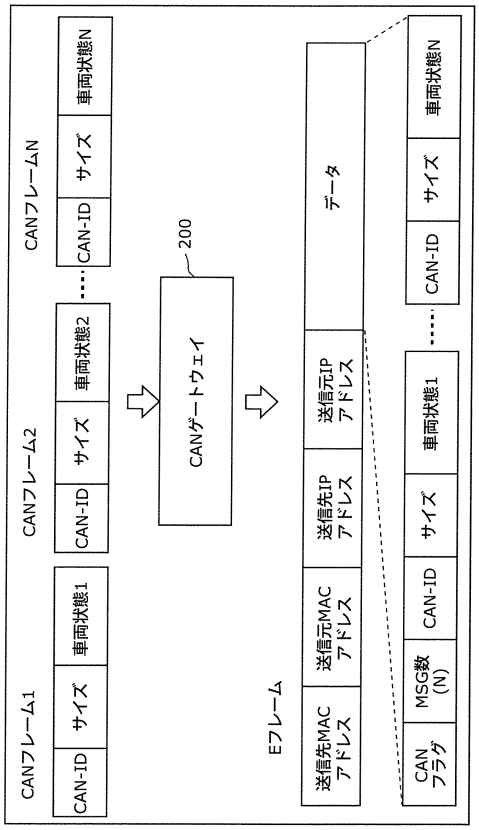
【図４】


CANフレーム情報1
CANフラグ
MSG数(N)
CAN-ID
サイズ
データ
CANフレーム情報N
CAN-ID
サイズ
データ

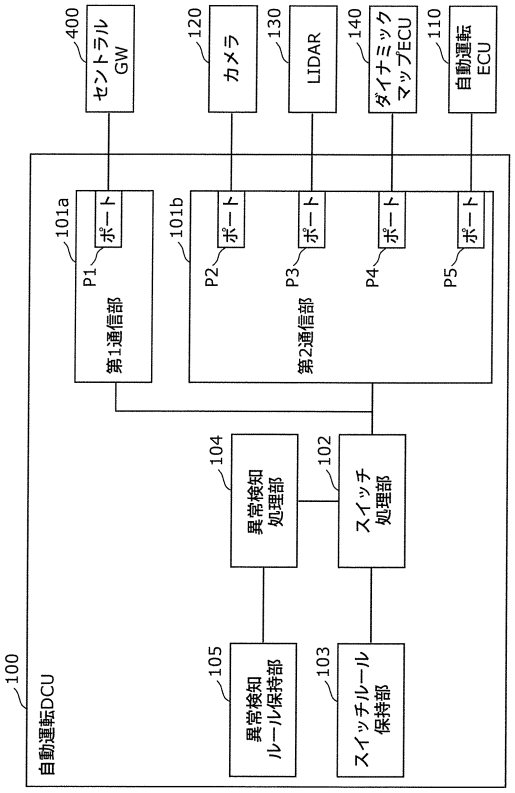
【図５】


CANゲートウェイ
200
11
E送受信部
201
転送制御部
203
転送ルール保持部
204
CAN送受信部
202a
CAN送受信部
202b
CANバス21a
CANバス21b

【図６】


CANフレーム1
CAN-ID
サイズ
車両状態1
CANフレーム2
CAN-ID
サイズ
車両状態2
CANフレームN
CAN-ID
サイズ
車両状態N
CANゲートウェイ
200
Eフレーム
CANフラグ
MSG数(N)
送信先MACアドレス
送信元MACアドレス
CAN-ID
サイズ
送信先IPアドレス
車両状態1
送信元IPアドレス
データ
CAN-ID
サイズ
車両状態N

【図７】



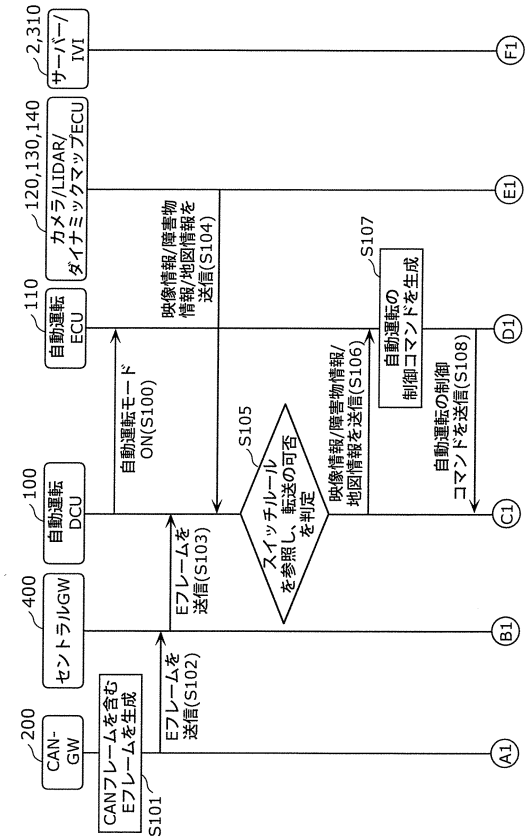
【図８】

入力ポート	送信元IPアドレス	送信元MACアドレス	出力ポート	送信先IPアドレス	送信先MACアドレス
P1	CANゲートウェイ	セントラル ゲートウェイ	P5	自動運転 ECU	自動運転 ECU
P2	カメラ	カメラ	P5	自動運転 ECU	自動運転 ECU
P3	LIDAR	LIDAR	P5	自動運転 ECU	自動運転 ECU
P4	ダイナミックマップ ECU	ダイナミックマップ ECU	P5	自動運転 ECU	自動運転 ECU
P5	自動運転 ECU	自動運転 ECU	P1	CANゲートウェイ	セントラル ゲートウェイ
P2	カメラ	カメラ	P1	IVI	インフォテインメント DCU
P4	ダイナミック マップ	ダイナミック マップ	P1	地図サーバ	セントラル ゲートウェイ
P3	カメラ	カメラ	P1	地図サーバ	セントラル ゲートウェイ
-	自動運転 DCU	自動運転 DCU	P1	監視サーバ	セントラル ゲートウェイ

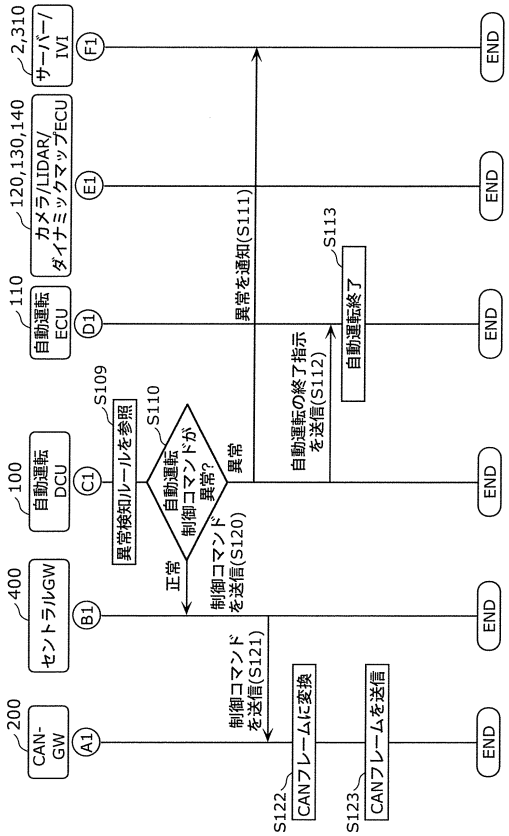
【図９】

車速状態	シフト状態	車速指示	操舵指示
低速	D	⊿10km	⊿360度
中速	D	⊿20km	⊿180度
高速	D	⊿30km	⊿90度

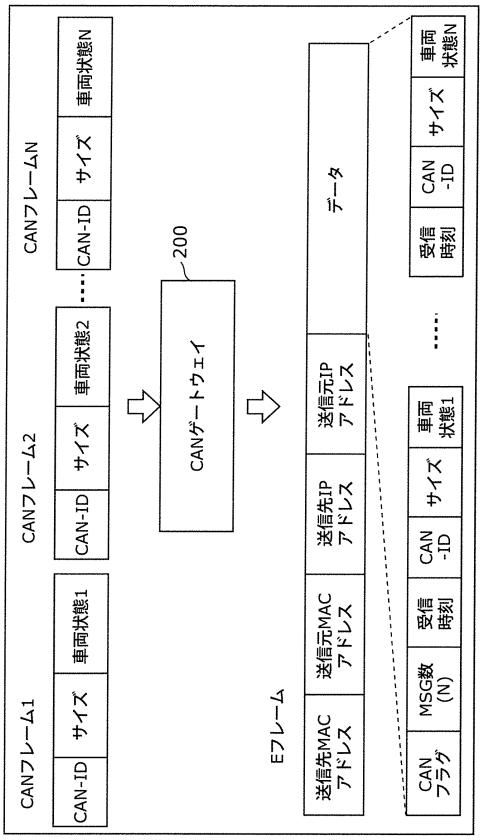
【図１０】



【図１１】



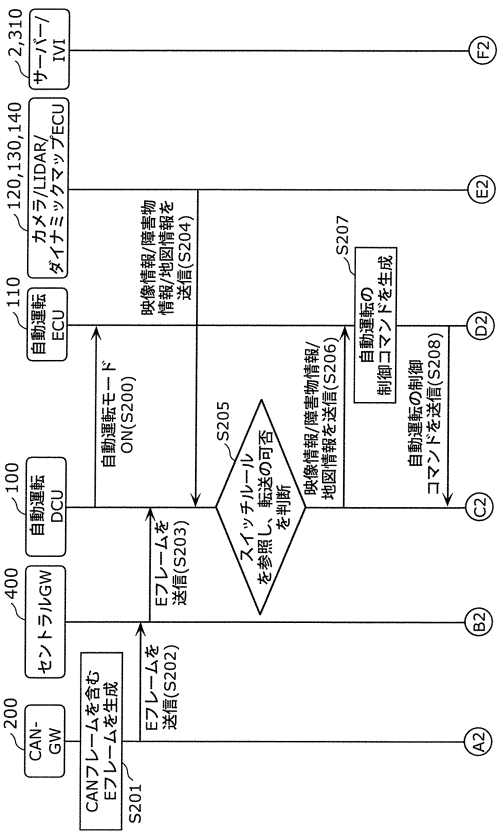
【図１２】



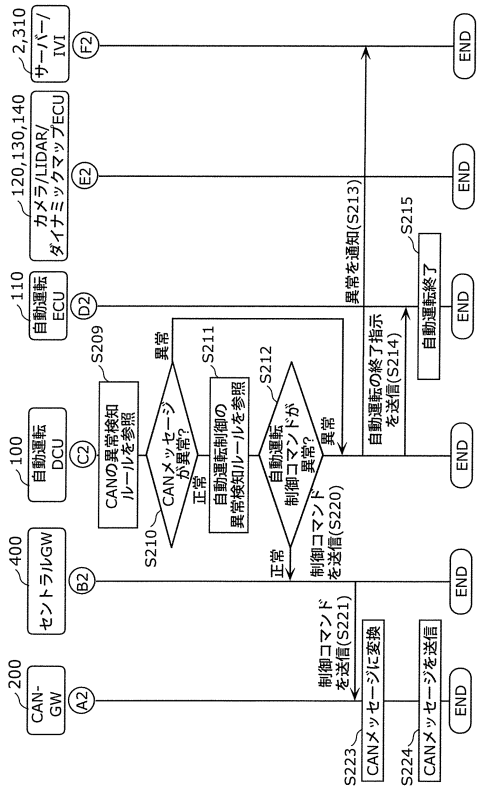
【図１３】

CAN-ID	周期	周期マージン	データ値の変化量
0xA1	10ms	±3ms	±50
0xA2	20ms	±5ms	±100
0xA3	30ms	±10ms	±200

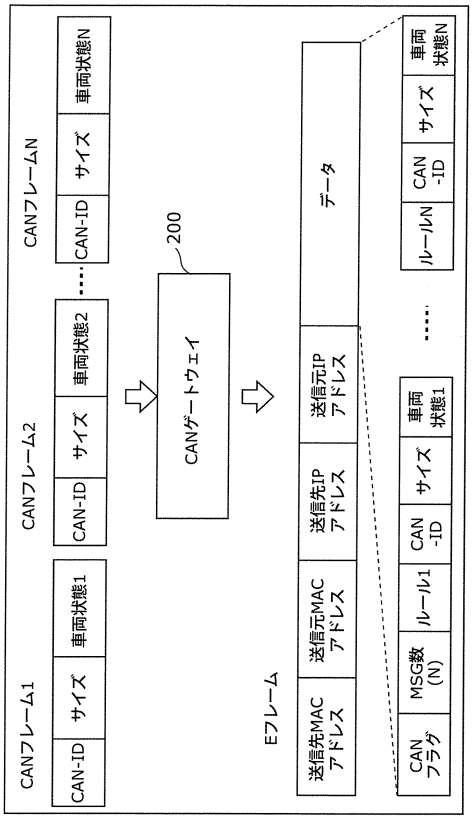
【図１４】



【図１５】



【図１６】



【図１７】

ルール1	周期チェック
ルール2	データ変化量チェック
ルール3	MACチェック

フロントページの続き

(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　田邉 正人
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　鳥崎 唯之
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　寺澤 弘泰
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　加藤 遼
大阪府門真市大字門真１００６番地 パナソニック株式会社内
審査官　安藤 一道
(56)参考文献　特開２０１６－０７４３１７（ＪＰ，Ａ）
特開２０１５－０６７１８７（ＪＰ，Ａ）
国際公開第２０１７／１１９０２７（WO，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　４３／０８