(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2019-201423
(P2019-201423A)
(43)公開日　令和1年11月21日(2019.11.21)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L 12/40 | (2006.01) | H04L | 12/40 | M | 5K032 |
| H04L 12/28 | (2006.01) | H04L | 12/28 | 100A | 5K033 |
| B60R 16/02 | (2006.01) | H04L | 12/28 | 200M | |
| B60R 16/023 | (2006.01) | B60R | 16/02 | 660U | |
| | | B60R | 16/023 | P | |

審査請求 有　請求項の数 13　OL　（全 53 頁）

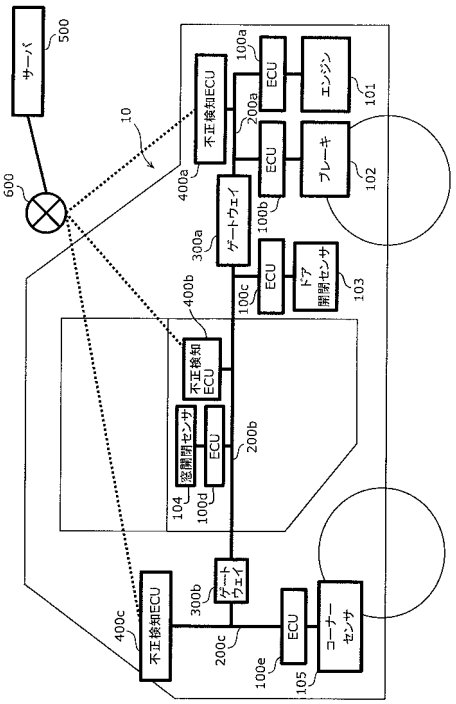
(21)出願番号　特願2019-148961 (P2019-148961)
(22)出願日　令和1年8月14日 (2019.8.14)
(62)分割の表示　特願2015-214740 (P2015-214740)の分割
原出願日　平成27年10月30日 (2015.10.30)
(31)優先権主張番号　62/105,363
(32)優先日　平成27年1月20日 (2015.1.20)
(33)優先権主張国・地域又は機関
米国 (US)

(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】不正検知ルール更新方法、不正検知電子制御ユニット及び車載ネットワークシステム

(57)【要約】
【課題】車載ネットワークシステムにおいて必要に応じて不正なフレームを検知する為の基準となるルールの更新を可能にする不正検知ルール更新方法を提供する。
【解決手段】不正検知ルール更新方法は、不正検知電子制御ユニットが接続されたバス上で送信されるメッセージについてのルールへの適合性の判定を不正検知ルールに基づいて行い、外部装置から更新用不正検知ルールと更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信し、車両が走行しているか否かを判定し、車両が走行していると判定した場合に、更にバス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、(i)バス種別情報が走行に関連する駆動系のバスを示している場合に更新処理を行わず、(ii)バス種別情報が走行に関連する駆動系のバスを示していない場合に不正検知ルールを更新する。
【選択図】図１



【特許請求の範囲】
【請求項１】
１以上のバスを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記バスに接続された不正検知電子制御ユニットを備える車載ネットワークシステムにおいて用いられる不正検知ルール更新方法であって、
前記不正検知電子制御ユニットにおいて、当該不正検知電子制御ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、
前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信し、
前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、
前記車両が走行していると判定した場合に、更に、前記バス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、
(i)前記バス種別情報が走行に関連する駆動系のバスを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、
(ii)前記バス種別情報が走行に関連する駆動系のバスを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する
不正検知ルール更新方法。
【請求項２】
前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記バスの種別を前記バス種別情報が示す場合に、前記所定更新条件が満たされたとして前記更新を行う
請求項１記載の不正検知ルール更新方法。
【請求項３】
前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、バスの種別を示すバス種別情報を含み、
前記不正検知電子制御ユニットが、前記外部装置と通信することにより前記配信データの前記受信を行い、当該不正検知電子制御ユニットが接続された前記バスの種別に該当するバス種別情報に対応する更新用不正検知ルールを前記配信データから抽出して、前記判定に係る前記不正検知ルールを、抽出した当該更新用不正検知ルールへと更新する
請求項１記載の不正検知ルール更新方法。
【請求項４】
前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、バスの種別を示すバス種別情報を含み、
１台の前記電子制御ユニットが前記配信データの前記受信を行い、当該配信データにおける各更新用不正検知ルールを、対応するバス種別情報が示すバスの種別に応じた、不正検知ルール更新用のメッセージＩＤを付したメッセージに含めて前記バスを介して送信し、
前記不正検知電子制御ユニットが、当該不正検知電子制御ユニットが接続された前記バスの種別に応じた、不正検知ルール更新用のメッセージＩＤのメッセージを当該バスから受信し、前記判定に係る前記不正検知ルールを、当該メッセージに含まれる更新用不正検知ルールへと更新する
請求項１記載の不正検知ルール更新方法。
【請求項５】
前記配信データは、付属情報を含み、
所定更新条件は、前記付属情報に関する条件であり、
前記不正検知ルールの前記更新を、受信した前記配信データにおける前記付属情報が前記所定更新条件を満たす場合には行い、前記付属情報が前記所定更新条件を満たさない場合には行わない

請求項１記載の不正検知ルール更新方法。
【請求項６】
前記所定更新条件を満たすか否かを、前記付属情報と前記電子制御ユニット又は前記不正検知電子制御ユニットが保持する情報とを比較した結果に応じて判別する
請求項５記載の不正検知ルール更新方法。
【請求項７】
前記付属情報は、前記更新用不正検知ルールのバージョンを示し、
前記不正検知電子制御ユニットは、前記判定の基礎としている前記不正検知ルールのバージョンよりも新しいバージョンを前記付属情報が示す場合に、前記所定更新条件が満たされたと判別して前記更新を行う
請求項６記載の不正検知ルール更新方法。
【請求項８】
前記付属情報は、前記更新用不正検知ルールの適用対象の車両種別を示し、
前記付属情報が、前記車載ネットワークシステムを搭載する車両に係る車両種別を示す場合に、前記所定更新条件が満たされたとして前記更新を行う
請求項５記載の不正検知ルール更新方法。
【請求項９】
前記不正検知ルール及び前記更新用不正検知ルールは、ルールへの適合性を判定するためのプログラムを含んで構成される
請求項１記載の不正検知ルール更新方法。
【請求項１０】
前記配信データには、暗号処理が施されており、
前記配信データの前記受信に際して前記暗号処理に呼応する処理を施す
請求項１記載の不正検知ルール更新方法。
【請求項１１】
前記複数の電子制御ユニットは、ＣＡＮ（Controller Area Network）プロトコルに従って前記バスを介して通信を行う
請求項１記載の不正検知ルール更新方法。
【請求項１２】
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、
不正検知ルールを保持する不正検知ルール保持部と、
自ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、前記不正検知ルールに基づいて行う不正検知処理部と、
更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信して、
前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、
前記車両が走行していると判定した場合に、更に、前記バス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、
(i)前記バス種別情報が走行に関連する駆動系のバスを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、
(ii)前記バス種別情報が走行に関連する駆動系のバスを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する
更新判定部とを備える
不正検知電子制御ユニット。
【請求項１３】
１以上のバスを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記バスに接続された不正検知電子制御ユニットを備える車載ネットワークシステムであって、
前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記バ

ス上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、
前記電子制御ユニットは、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信して、当該更新用不正検知ルールを前記バスを介して送信し、
前記不正検知電子制御ユニットは、前記バスから前記更新用不正検知ルールを受信し、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、
前記車両が走行していると判定した場合に、更に、前記バス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、
(i)前記バス種別情報が走行に関連する駆動系のバスを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、
(ii)前記バス種別情報が走行に関連する駆動系のバスを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する
車載ネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子制御ユニットが通信を行う車載ネットワークにおいて、送信された不正なフレームを検知するために用いられる不正検知ルールについてのアップデート（更新）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。
【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。
【０００５】
従来、異常なメッセージがＣＡＮのバス上に送信された場合に、バス間を接続するゲートウェイ装置が異常メッセージを検出して、他のバスに転送しないことで、バスの負荷の上昇を抑える技術が知られている（「特許文献１」参照）。また、周期的に送られてくるメッセージの周期をチェックし、不正なフレームを判定する技術が知られている（「非特

許文献１」参照）。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００７－３８９０４号公報
【非特許文献】
【０００７】
【非特許文献１】大塚 敏史、石郷岡 祐、「既存ＥＣＵを変更不要な車載ＬＡＮ向け侵入検知手法」、研究報告組込みシステム（ＥＭＢ）、情報処理学会、２０１３年３月６日、２０１３－ＥＭＢ－２８巻、６号、１－５頁
【発明の概要】
【発明が解決しようとする課題】
【０００８】
ところで、例えば車載ネットワークシステムを構成するＥＣＵの機能の変更（改良等）に伴い、メッセージ（フレーム）を不正（異常）と判定するための判定基準であるルールを更新する必要が生じ得る。また、ルールが固定であると例えば不正なＥＣＵが車載ネットワークに接続されてそのルールを回避するメッセージを送信するリスクが高まるため、ルールの変更（更新）が有用となり得る。
【０００９】
そこで、本発明は、車載ネットワークシステムにおいて必要に応じて不正なフレームを検知するための基準となるルールの更新を可能にする不正検知ルール更新方法を提供する。また、本発明は、そのルールの更新を可能にする車載ネットワークシステム、及び、その車載ネットワークシステムで不正なフレームを検知する不正検知電子制御ユニット（不正検知ＥＣＵ）を提供する。
【課題を解決するための手段】
【００１０】
上記課題を解決するために本発明の一態様に係る不正検知ルール更新方法は、１以上のバスを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記バスに接続された不正検知電子制御ユニットを備える車載ネットワークシステムにおいて用いられる不正検知ルール更新方法であって、前記不正検知電子制御ユニットにおいて、当該不正検知電子制御ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信し、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記バス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、(i)前記バス種別情報が走行に関連する駆動系のバスを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記バス種別情報が走行に関連する駆動系のバスを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する不正検知ルール更新方法である。
【００１１】
また、上記課題を解決するために本発明の一態様に係る不正検知電子制御ユニットは、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、不正検知ルールを保持する不正検知ルール保持部と、自ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、前記不正検知ルールに基づいて行う不正検知処理部と、更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信して、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記バス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、(i)前記バス種別情報が走行に関連する駆動系のバスを示してい

る場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記バス種別情報が走行に関連する駆動系のバスを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する更新判定部とを備える不正検知電子制御ユニットである。

【００１２】

また、上記課題を解決するために本発明の一態様に係る車載ネットワークシステムは、１以上のバスを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記バスに接続された不正検知電子制御ユニットを備える車載ネットワークシステムであって、前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、前記電子制御ユニットは、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報とを含む配信データを受信して、当該更新用不正検知ルールを前記バスを介して送信し、前記不正検知電子制御ユニットは、前記バスから前記更新用不正検知ルールを受信し、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記バス種別情報が走行に関連する駆動系のバスを示しているか否かを判定し、(i)前記バス種別情報が走行に関連する駆動系のバスを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記バス種別情報が走行に関連する駆動系のバスを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する車載ネットワークシステムである。

【発明の効果】

【００１３】

本発明によれば、車載ネットワークにおいて不正なフレームが送信されたと判定する基準となるルールの更新が可能となり、これにより不正なフレームを検知する機能が更新され得る。従って、車載ネットワークシステムの変更等に対応可能となり、また、車載ネットワークにおいて不正なＥＣＵがルールを回避してメッセージを送信するリスクを低減可能となる。

【図面の簡単な説明】

【００１４】

【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】実施の形態１に係るＥＣＵの構成図である。

【図４】実施の形態１に係るＥＣＵが保持する受信ＩＤリストの一例を示す図である。

【図５】実施の形態１に係るＥＣＵが保持する受信ＩＤリストの一例を示す図である。

【図６】実施の形態１に係るＥＣＵが保持する受信ＩＤリストの一例を示す図である。

【図７】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メッセージＩＤ及びデータの一例を示す図である。

【図８】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メッセージＩＤ及びデータの一例を示す図である。

【図９】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メッセージＩＤ及びデータの一例を示す図である。

【図１０】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メッセージＩＤ及びデータの一例を示す図である。

【図１１】コーナー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メッセージＩＤ及びデータの一例を示す図である。

【図１２】実施の形態１に係るゲートウェイの構成図である。

【図１３】実施の形態１に係るゲートウェイが保持する転送ルール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】実施の形態１に係る不正検知ＥＣＵが保持する不正検知ルール及びバージョン情報の一例を示す図である。

【図１６】実施の形態１に係る不正検知ＥＣＵが保持する不正検知ルール及びバージョン情報の一例を示す図である。
【図１７】実施の形態１に係る不正検知ＥＣＵが保持する不正検知ルール及びバージョン情報の一例を示す図である。
【図１８】実施の形態１に係る配信データフォーマットの一例を示す図である。
【図１９】実施の形態１に係る配信データの一例を示す図である。
【図２０】実施の形態１に係る更新結果データフォーマットの一例を示す図である。
【図２１】実施の形態１に係る更新結果データの一例を示す図である。
【図２２】実施の形態１に係るサーバの構成図である。
【図２３】実施の形態１に係る更新結果表の一例を示す図である。
【図２４】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２５】実施の形態１における不正検知ルールの更新に係る動作例を示すシーケンス図である（図２６に続く）。
【図２６】実施の形態１における不正検知ルールの更新に係る動作例を示すシーケンス図である（図２５から続く）。
【図２７】実施の形態１の変形例に係る不正検知ＥＣＵの構成図である。
【図２８】実施の形態１の変形例における不正検知ルールの更新に係る動作例を示すシーケンス図である（図２９に続く）。
【図２９】実施の形態１の変形例における不正検知ルールの更新に係る動作例を示すシーケンス図である（図２８から続く）。
【図３０】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３１】実施の形態２に係るヘッドユニットの構成図である。
【図３２】実施の形態２に係るヘッドユニットが保持する受信ＩＤリストの一例を示す図である。
【図３３】実施の形態２に係る内部配信データの一例を示す図である。
【図３４】実施の形態２に係る内部更新結果データの一例を示す図である。
【図３５】実施の形態２に係るゲートウェイが保持する転送ルールの一例を示す図である。
【図３６】実施の形態２に係る不正検知ＥＣＵの構成図である。
【図３７】実施の形態２に係る不正検知ＥＣＵが保持する不正検知ルール及びバージョン情報の一例を示す図である。
【図３８】実施の形態２に係る不正検知ＥＣＵが保持する不正検知ルール及びバージョン情報の一例を示す図である。
【図３９】実施の形態２に係る不正検知ＥＣＵが保持する不正検知ルール及びバージョン情報の一例を示す図である。
【図４０】実施の形態２に係るサーバの構成図である。
【図４１】実施の形態２に係る内部更新結果表の一例を示す図である。
【図４２】実施の形態２における不正検知ルールの更新に係る動作例を示すシーケンス図である（図４３に続く）。
【図４３】実施の形態２における不正検知ルールの更新に係る動作例を示すシーケンス図である（図４２から続く）。
【発明を実施するための形態】
【００１５】
本発明の一態様に係る不正検知ルール更新方法は、１以上のバスを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記バスに接続された不正検知電子制御ユニットを備える車載ネットワークシステムにおいて用いられる不正検知ルール更新方法であって、前記不正検知電子制御ユニットにおいて、当該不正検知電子制御ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、前記車載ネットワークシステムの外部の外部装置から更新

用不正検知ルールを含む配信データを受信して、所定更新条件が満たされた場合には前記判定に係る前記不正検知ルールを当該更新用不正検知ルールへと更新する不正検知ルール更新方法である。これにより、車載ネットワークにおいて不正なフレームが送信されたと判定する基準となるルールの更新が可能となる。従って、車載ネットワークシステムの変更等に対応可能となり、また、車載ネットワークにおいて不正なＥＣＵがルールを回避してメッセージを送信するリスクを低減可能となる。

【００１６】

また、前記配信データは、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報を含み、前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記バスの種別を前記バス種別情報が示す場合に、前記所定更新条件が満たされたとして前記更新を行うこととしても良い。これにより、バスの種別毎に必要な不正検知ルールが異なることに対応し得る。

【００１７】

また、前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、バスの種別を示すバス種別情報を含み、前記不正検知電子制御ユニットが、前記外部装置と通信することにより前記配信データの前記受信を行い、当該不正検知電子制御ユニットが接続された前記バスの種別に該当するバス種別情報に対応する更新用不正検知ルールを前記配信データから抽出して、前記判定に係る前記不正検知ルールを、抽出した当該更新用不正検知ルールへと更新することとしても良い。これにより、不正検知ルールを配信する外部装置側では一括した配信が可能となり処理負担が軽減される。

【００１８】

また、前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、バスの種別を示すバス種別情報を含み、１台の前記電子制御ユニットが前記配信データの前記受信を行い、当該配信データにおける各更新用不正検知ルールを、対応するバス種別情報が示すバスの種別に応じた、不正検知ルール更新用のメッセージＩＤを付したメッセージに含めて前記バスを介して送信し、前記不正検知電子制御ユニットが、当該不正検知電子制御ユニットが接続された前記バスの種別に応じた、不正検知ルール更新用のメッセージＩＤのメッセージを当該バスから受信し、前記判定に係る前記不正検知ルールを、当該メッセージに含まれる更新用不正検知ルールへと更新することとしても良い。これにより、１つのＥＣＵだけが外部との通信を行うため個々の不正検知ＥＣＵの処理負荷が削減され得る。また、この構成により、通信内容についてセキュリティを確保する暗号処理等の実装面では、外部との通信を行うＥＣＵでは例えば処理負荷が大きい暗号方式を用いるとしても、外部とは通信しない各不正検知ＥＣＵでは処理負荷が小さい暗号方式を選択し得るようになる。また、個々の不正検知ＥＣＵが通信する場合と比べて、サーバと車載ネットワークシステムとの間での通信回数を低減させ得る。

【００１９】

また、前記配信データは、付属情報を含み、前記所定更新条件は、前記付属情報に関する条件であり、前記不正検知ルールの前記更新を、受信した前記配信データにおける前記付属情報が前記所定更新条件を満たす場合には行い、前記付属情報が前記所定更新条件を満たさない場合には行わないこととしても良い。これにより、更新用不正検知ルールに関する情報に基づいて更新要否を判別できるようになる。

【００２０】

また、前記所定更新条件を満たすか否かを、前記付属情報と前記電子制御ユニット又は前記不正検知電子制御ユニットが保持する情報とを比較した結果に応じて判別することとしても良い。これにより、更新用不正検知ルールのバージョンが既存の不正検知ルールのバージョンよりも新しいか否か等といった比較判断が可能になる。

【００２１】

また、前記付属情報は、前記更新用不正検知ルールのバージョンを示し、前記不正検知

電子制御ユニットは、前記判定の基礎としている前記不正検知ルールのバージョンよりも新しいバージョンを前記付属情報が示す場合に、前記所定更新条件が満たされたと判別して前記更新を行うこととしても良い。これにより、不正検知ルールの内容変更についてバージョンによる管理が可能となる。

【００２２】

また、前記付属情報は、前記更新用不正検知ルールの適用対象の車両種別を示し、前記付属情報が、前記車載ネットワークシステムを搭載する車両に係る車両種別を示す場合に、前記所定更新条件が満たされたとして前記更新を行うこととしても良い。これにより、車種毎に独立して不正検知ルールを規定可能となる。

【００２３】

また、前記所定更新条件は、前記車載ネットワークシステムを搭載する車両の状態が所定状態であるという条件であることとしても良い。これにより、例えば比較的安全性が高い状態等を所定状態として定めておくことで、安全に不正検知ルールの更新を行うことが可能になる。

【００２４】

また、前記配信データを受信した際に前記車両の状態が前記所定状態でない場合には、前記車両の状態が前記所定状態へと変化した際に、前記判定に係る前記不正検知ルールを、既に受信している当該配信データに含まれる前記更新用不正検知ルールへと更新する、又は、前記外部装置から前記配信データを新たに受信して前記不正検知ルールを、新たに受信した当該配信データに含まれる前記更新用不正検知ルールへと更新することとしても良い。これにより、車両の状態が所定状態に変化した際に適切に不正検知ルールの更新が行える。

【００２５】

また、前記不正検知ルール及び前記更新用不正検知ルールは、ルールへの適合性を判定するためのプログラムを含んで構成されることとしても良い。これにより、不正検知のためのプログラムの更新が可能となる。

【００２６】

また、前記配信データには、暗号処理が施されており、前記配信データの前記受信に際して前記暗号処理に呼応する処理を施すこととしても良い。これにより、不正検知ルールについてセキュリティを確保し得る。

【００２７】

また、前記複数の電子制御ユニットは、ＣＡＮ（Controller Area Network）プロトコルに従って前記バスを介して通信を行うこととしても良い。これにより、ＣＡＮに従った車載ネットワークシステムにおいて不正検知ルールの更新が可能となる。

【００２８】

また、本発明の一態様に係る不正検知電子制御ユニットは、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、不正検知ルールを保持する不正検知ルール保持部と、自ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、前記不正検知ルールに基づいて行う不正検知処理部と、更新用不正検知ルールを含む配信データを受信して、所定更新条件が満たされた場合には前記不正検知ルール保持部が保持する前記不正検知ルールを当該更新用不正検知ルールへと更新する更新判定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、不正なフレームが送信されたと判定する基準となるルールの更新が可能となる。

【００２９】

また、本発明の一態様に係る車載ネットワークシステムは、１以上のバスを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記バスに接続された不正検知電子制御ユニットを備える車載ネットワークシステムであって、前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記バス上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、前記電子制御ユニットは、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルー

ルを含む配信データを受信して、当該更新用不正検知ルールを前記バスを介して送信し、前記不正検知電子制御ユニットは、前記バスから前記更新用不正検知ルールを受信し、所定更新条件が満たされた場合には前記判定に係る前記不正検知ルールを当該更新用不正検知ルールへと更新する車載ネットワークシステムである。これにより、不正検知ルールの更新が可能となるため、車載ネットワークシステムの構成の変更等に対応可能となり、また、車載ネットワークにおいて不正なＥＣＵがルールを回避してメッセージを送信するリスクを低減可能となる。

【００３０】

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良い。

【００３１】

以下、実施の形態に係る不正検知ルール更新方法を用いる車載ネットワークシステムについて、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本発明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、一例であって本発明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。

【００３２】

（実施の形態１）

以下、本発明の実施の形態として、車両に搭載されて複数のＥＣＵがバスを介して通信する車載ネットワークシステム１０において、バスに送出された不正なフレーム（メッセージ）を不正検知ＥＣＵが検知するために用いる不正検知ルールを更新する不正検知ルール更新方法について、図面を用いて説明する。不正検知ＥＣＵは、車載ネットワークシステム１０を構成するＥＣＵ間での通信に用いられるバス上で送信されるフレームについて、不正検知ルールに基づいて検査（つまりルールへの適合性の判定）を行う。不正検知ＥＣＵの検査（つまり不正検知）の結果を活用した処理により、例えばバスに不正なＥＣＵが接続されてルールに適合しない不正なフレームを送信する等により車両を不適切に制御することを防ぐことが可能になる。本実施の形態では、バス毎に接続された各不正検知ＥＣＵが車両の外部のサーバと通信することにより不正検知機能を更新（つまりフレームを不正と判定する基準、基礎等となる不正検知ルールを更新）する例を示す。

【００３３】

［１．１　車載ネットワークシステム１０の全体構成］

図１は、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２００ａ～２００ｃと、不正検知ＥＣＵ４００ａ～４００ｃ、ゲートウェイ３００ａ、３００ｂ、及び、各種機器に接続されたＥＣＵ１００ａ～１００ｅ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。また図１では、車載ネットワークシステム１０における不正検知ＥＣＵ４００ａ～４００ｃと無線通信する外部のネットワーク６００及びそのネットワーク６００と通信可能に接続されたサーバ５００とを付記している。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ＥＣＵ１００ａ～１００ｅ以外にもいくつものＥＣＵが含まれ得る。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。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。バス２００ａ～２００ｃには不正なメッセージを送信する不正なＥＣＵが接続されている可能性があり、不正検知ＥＣＵ４００ａ～４００ｃは、不正検知ルールに基づいてルールに適合しない不正なフレームがバス上に現れるとその不正なフレームを検知する。

【００３４】

不正検知ＥＣＵ４００ａ、４００ｂ、４００ｃは、それぞれバス２００ａ、バス２００ｂ、バス２００ｃに接続される一種のＥＣＵであり、自ＥＣＵが接続されたバス上に現れるフレームを監視して不正なフレームを検知した場合には、エラーフレームを送信する機能を有する。

【００３５】

ＥＣＵ１００ａ～１００ｅは、いずれかのバスと接続され、また、それぞれエンジン１０１、ブレーキ１０２、ドア開閉センサ１０３、窓開閉センサ１０４、コーナーセンサ１０５に接続されている。ＥＣＵ１００ａ～１００ｅのそれぞれは、接続されている機器（エンジン１０１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。

【００３６】

ゲートウェイ３００ａは、不正検知ＥＣＵ４００ａ、ＥＣＵ１００ａ及びＥＣＵ１００ｂがつながるバス２００ａと、不正検知ＥＣＵ４００ｂ、ＥＣＵ１００ｃ及びＥＣＵ１００ｄがつながるバス２００ｂとに接続している。ゲートウェイ３００ｂは、不正検知ＥＣＵ４００ｂ、ＥＣＵ１００ｃ及びＥＣＵ１００ｄがつながるバス２００ｂと、不正検知ＥＣＵ４００ｃ及びＥＣＵ１００ｅがつながるバス２００ｃとに接続している。ゲートウェイ３００ａ、３００ｂは、ある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３００ａ、３００ｂも一種のＥＣＵである。

【００３７】

サーバ５００は、不正検知ＥＣＵ４００ａ～４００ｃの不正検知機能をアップデート（更新）するために配信データを送信する機能を有する。サーバ５００と不正検知ＥＣＵ４００ａ～４００ｃとの間での通信方式はいかなる方式を用いても良く、例えば無線通信の他に有線通信を用いても良い。無線通信においては、ＷｉＦｉ（登録商標）、或いは携帯電話網等に用いられる３Ｇ（3rd Generation）回線、４Ｇ（ＬＴＥ：Long Term Evolution）等を用いても良い。

【００３８】

［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。

【００３９】

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。

【００４０】

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。

【００４１】

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。

【００４２】

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。

【００４３】

ＩＤＥと「ｒ」とは、両方ドミナント１ｂｉｔで構成される。

【００４４】

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。

【００４５】

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。

【００４６】

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。

【００４７】

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。

【００４８】

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を確認できる。

【００４９】

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。

【００５０】

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。

【００５１】

［１．３　ＥＣＵ１００ａの構成］

図３は、ＥＣＵ１００ａの構成図である。ＥＣＵ１００ａは、フレーム送受信部１１０と、フレーム解釈部１２０と、受信ＩＤ判断部１３０と、受信ＩＤリスト保持部１４０と、フレーム処理部１５０と、フレーム生成部１６０と、データ取得部１７０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、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。

【００５２】

フレーム送受信部１１０は、バス２００ａ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２００ａからフレームを１ｂｉｔずつ受信し、フレーム解釈部１２０に転送する。また、フレーム生成部１６０より通知を受けたフレームの内容をバス２００ａに送信する。

【００５３】

フレーム解釈部１２０は、フレーム送受信部１１０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１３０へ転送する。フレーム解釈部１２０は、受信ＩＤ判断部１３０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１５０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１２０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１６０へ通知する。また、フレーム解釈部１２０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。

【００５４】

受信ＩＤ判断部１３０は、フレーム解釈部１２０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１４０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１３０は、フレーム解釈部１２０へ通知する。

【００５５】

受信ＩＤリスト保持部１４０は、ＥＣＵ１００ａ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４に、受信ＩＤリストの一例を示す。

【００５６】

フレーム処理部１５０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１０１に接続されたＥＣＵ１００ａ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。ＥＣＵ１００ａ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、ＥＣＵ１００ａのフレーム処理部１５０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１０１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。

【００５７】

データ取得部１７０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１６０に通知する。

【００５８】

フレーム生成部１６０は、フレーム解釈部１２０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１１０へ通知して送信させる。また、フレーム生成部１６０は、データ取得部１７０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１１０へ通知する。

【００５９】

なお、ＥＣＵ１００ｂ～１００ｅも、上述したＥＣＵ１００ａと基本的に同様の構成を備える。受信ＩＤリスト保持部１４０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が、同じ内容であっても良い。また、フレーム処理部１５０の処理内容は、ＥＣＵ毎に異なる。例えば、ＥＣＵ１００ｃにおけるフレーム処理部１５０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、ＥＣＵ１００ｂ、ＥＣＵ１００ｄ及びＥＣＵ１００ｅにおけるフレーム処理部１５０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、ＥＣＵ１００ａ～１００ｅ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７～図１１を用いて説明する。

【００６０】

［１．４　受信ＩＤリスト例１］

図４は、ＥＣＵ１００ａ及びＥＣＵ１００ｂ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。
【００６１】
［１．５　受信ＩＤリスト例２］
図５は、ＥＣＵ１００ｃ及びＥＣＵ１００ｄ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。
【００６２】
［１．６　受信ＩＤリスト例３］
図６は、ＥＣＵ１００ｅ、ゲートウェイ３００ａ及びゲートウェイ３００ｂ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」、「４」及び「５」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。
【００６３】
［１．７　エンジンに係るＥＣＵ１００ａの送信フレーム例］
図７は、エンジン１０１に接続されたＥＣＵ１００ａ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。ＥＣＵ１００ａ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７の上行から下行へと、ＥＣＵ１００ａ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。
【００６４】
［１．８　ブレーキに係るＥＣＵ１００ｂの送信フレーム例］
図８は、ブレーキ１０２に接続されたＥＣＵ１００ｂ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。ＥＣＵ１００ｂ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８の上行から下行へと、ＥＣＵ１００ｂ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。
【００６５】
［１．９　ドア開閉センサに係るＥＣＵ１００ｃの送信フレーム例］
図９は、ドア開閉センサ１０３に接続されたＥＣＵ１００ｃ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。ＥＣＵ１００ｃ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９の上行から下行へと、ＥＣＵ１００ｃ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。
【００６６】
［１．１０　窓開閉センサに係るＥＣＵ１００ｄの送信フレーム例］
図１０は、窓開閉センサ１０４に接続されたＥＣＵ１００ｄ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。ＥＣＵ１００ｄ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１０の上行から下行へと、ＥＣＵ１００ｄ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。

【００６７】

［１．１１　コーナーセンサに係るＥＣＵ１００ｅの送信フレーム例］

図１１は、コーナーセンサ１０５に接続されたＥＣＵ１００ｅ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。ＥＣＵ１００ｅが送信するフレームのメッセージＩＤは「５」である。データ長は１Ｂｙｔｅである。データの値は、コーナーセンサ１０５が、車両のコーナーから一定距離範囲に障害物が存在することを検知すれば「１」、障害物を検知しなければ「０」である。図１１の上行から下行へと、ＥＣＵ１００ｅから定期的に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、車両のコーナーに障害物が検知されない状態から次第に障害物が検知される状態へと移った様子を表している。

【００６８】

［１．１２　ゲートウェイ３００ａの構成］

図１２は、ゲートウェイ３００ａの構成図である。ゲートウェイ３００ａは、フレーム送受信部３１０と、フレーム解釈部３２０と、受信ＩＤ判断部３３０と、受信ＩＤリスト保持部３４０と、転送処理部３５１と、転送ルール保持部３５２と、フレーム生成部３６０とを含んで構成される。なお、ゲートウェイ３００ｂも同様の構成を有する。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３００ａ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。

【００６９】

フレーム送受信部３１０は、バス２００ａ、２００ｂ、２００ｃ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３２０に転送する。また、フレーム生成部３６０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２００ａ、２００ｂ、２００ｃに１ｂｉｔずつ送信する。

【００７０】

フレーム解釈部３２０は、フレーム送受信部３１０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３２０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３５１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３２０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３６０へ通知する。また、フレーム解釈部３２０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。

【００７１】

受信ＩＤ判断部３３０は、フレーム解釈部３２０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３２０へ通知する。

【００７２】

受信ＩＤリスト保持部３４０は、ゲートウェイ３００ａ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６参照）を保持する。

【００７３】

転送処理部３５１は、転送ルール保持部３５２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３２０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３６０へ通知する。なお、ゲートウェイ３００ａ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。

【００７４】

転送ルール保持部３５２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１３は、転送ルールの一例を示した図である。

【００７５】

フレーム生成部３６０は、フレーム解釈部３２０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３１０へ通知して送信させる。また、フレーム生成部３６０は、転送処理部３５１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３１０へ通知する。

【００７６】

［１．１３　転送ルール例］

図１３は、ゲートウェイ３００ａ及びゲートウェイ３００ｂが保持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１３中の「＊」は、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、図１３中の「－」は転送対象のフレームがないことを示す。図１３の例は、バス２００ａ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２００ｂ及びバス２００ｃ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２００ｂから受信するフレームのうち、バス２００ｃには全てのフレームが転送されるが、バス２００ａ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２００ｃから受信されるフレームは、バス２００ｂに転送されないように設定されていることを示している。

【００７７】

［１．１４　不正検知ＥＣＵ４００ａの構成］

図１４は、不正検知ＥＣＵ４００ａの構成図である。不正検知ＥＣＵ４００ａは、フレーム送受信部４１０と、フレーム解釈部４２０と、フレーム生成部４６０と、不正検知処理部４８０と、不正検知ルール保持部４８１と、外部通信部４９０と、暗復号処理部４９１と、ＭＡＣ処理部４９２と、鍵保持部４９３と、更新判定部４９４と、車両Ｎｏ．保持部４９５と、バス種別保持部４９６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。なお、不正検知ＥＣＵ４００ｂ及び不正検知ＥＣＵ４００ｃも基本的に同様の構成を備えるが、不正検知ルール保持部４８１の保持内容（不正検知ルール及びバージョン情報）が互いに異なり得る。

【００７８】

フレーム送受信部４１０は、バス２００ａ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４１０は、バス２００ａからフレームを１ｂｉｔずつ受信し、フレーム解釈部４２０に転送する。また、フレーム生成部４６０より通知を受けたフレームの内容をバス２００ａに送信する。

【００７９】

フレーム解釈部４２０は、フレーム送受信部４１０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、不正検知処理部４８０へ転送する。また、フレーム解釈部４２０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４６０へ通知する。また、フレーム解釈部４２０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。
【００８０】
フレーム生成部４６０は、フレーム解釈部４２０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４１０へ通知して送信させる。また、フレーム生成部４６０は、不正検知処理部４８０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４１０へ通知して送信させる。
【００８１】
不正検知処理部４８０は、不正検知ルール保持部４８１が保持している不正検知ルールに基づいて、バス２００ａから取得されたフレームが不正か否かについて判定する機能を有する。本実施の形態において不正検知ルールとして、不正でないメッセージＩＤを列挙した所謂ホワイトリストを用いる。不正検知処理部４８０は、具体的には、フレーム解釈部４２０から通知されるＩＤフィールドの値（ＩＤ）を受け取り、そのＩＤが、不正検知ルールとしてのメッセージＩＤのリスト（ホワイトリスト）に載っていない場合には、エラーフレームを送信するように、フレーム生成部４６０へ通知する。この場合に、バス２００ａにおいて、不正検知ルールとしてのメッセージＩＤのリストに載っていないＩＤを含むフレーム（不正なフレーム）のビット値は、レセシブに優先するドミナントが複数連続して構成されるエラーフレームにより、上書きされることになる。
【００８２】
不正検知ルール保持部４８１は、不正検知ルールとして、バス２００ａを送信されるフレームに含まれるメッセージＩＤを規定したリストを保持し、その不正検知ルールについてのバージョンを示すバージョン情報を保持する（図１５参照）。また、不正検知ルール保持部４８１は、更新判定部４９４からの新たな不正検知ルール（更新用不正検知ルールとも称する。）の通知に応じて、更新用不正検知ルールで先に保持していた不正検知ルールを更新し、更新した結果を更新判定部４９４へ通知する。
【００８３】
外部通信部４９０は、サーバ５００とネットワーク６００を介して通信することで、不正検知ルールを更新するための更新用不正検知ルール（新たな不正検知ルール）等を含む配信データを取得する。また、外部通信部４９０は、ネットワーク６００を介して更新結果データをサーバ５００へ通知する。外部通信部４９０は、取得した配信データを暗復号処理部４９１へ送信し、復号した結果を取得する。また、復号した配信データにおける検証用データとしてのメッセージ認証コード（ＭＡＣ：Message Authentication Code）をＭＡＣ処理部４９２へ通知し、ＭＡＣの検証結果を受け取る。外部通信部４９０は、復号した配信データから更新用不正検知ルールと付属情報（対象車種、バス種別、バージョン情報等）と抽出し、更新判定部４９４へ通知する。また、更新判定部４９４から受け取った不正検知ルールの更新結果等に基づき、更新結果データを生成し、ＭＡＣ処理部４９２へ通知し、生成したＭＡＣを含んだ更新結果データを受け取る。図１８に配信データフォーマットの一例を、図１９に配信データの一例を示す。また、図２０に更新結果データフォーマットの一例を、図２１に更新結果データの一例を示す。サーバ５００から配信される配信データには暗号処理が施されている。ここで、サーバ５００が施す暗号処理は、例えば、暗号化、検証用データの付加等である。これに対して、暗復号処理部４９１及びＭＡＣ処理部４９２は、配信データについてサーバ５００等で実行された暗号処理に呼応する暗号処理（例えば暗号化に呼応する復号、検証用データの付加に呼応する検証）を実行する。
【００８４】
暗復号処理部４９１は、外部通信部４９０から通知される暗号化された配信データを、鍵保持部４９３から取得する鍵を用いて復号し、復号した配信データを外部通信部４９０へ通知する。
【００８５】
ＭＡＣ処理部４９２は、外部通信部４９０から通知される配信データにおけるＭＡＣを

、鍵保持部４９３から取得する鍵を用いて検証し、検証結果を外部通信部４９０へ通知する。またＭＡＣ処理部４９２は、外部通信部４９０から通知される更新結果データに基づいて、鍵保持部４９３から取得する鍵を用いてＭＡＣを生成してその更新結果データにＭＡＣを含ませて外部通信部４９０へ通知する。

【００８６】

鍵保持部４９３は、暗復号処理部４９１とＭＡＣ処理部４９２とが暗号処理において利用する鍵を管理する。

【００８７】

更新判定部４９４は、外部通信部４９０から更新用不正検知ルールと付属情報とを受け取り、バス種別保持部４９６から取得したバス種別と、車両Ｎｏ．保持部４９５が保持する車種と、不正検知ルール保持部４８１が保持する不正検知ルールに対応するバージョン情報とに基づいて、不正検知ルール保持部４８１が保持する不正検知ルールを更新する必要があるか否かを判別する。更新判定部４９４は、更新する必要があると判別した場合には、不正検知ルール保持部４８１へ通知し、不正検知ルールの更新を行う。また、更新結果と車両Ｎｏ．保持部４９５から取得した車両Ｎｏ．とを外部通信部４９０へ通知する。

【００８８】

車両Ｎｏ．保持部４９５は、不正検知ＥＣＵ４００ａを搭載している車両の識別子を示す車両Ｎｏ．（車両Ｎｕｍｂｅｒ）とその車両の車種（車両種別）とを保持する。

【００８９】

バス種別保持部４９６は、不正検知ＥＣＵ４００ａが接続されるバスの種別を保持する。バスの種別には、例えば「駆動系」、「ボディ系」、「安全系」等がある。「駆動系」は、例えばエンジン、モータ、燃料、電池、トランスミッション等の制御といった車両の走行に関連する駆動系機能を有するＥＣＵが接続されるバスの種別である。「ボディ系」は、例えばドアロック、エアコン、ライト、ウィンカー等といった車両の装備の制御に関連するボディ系機能を有するＥＣＵが接続されるバスの種別である。「安全系」は、例えば、自動ブレーキ、車線維持機能、車間距離維持機能、衝突防止機能、エアバッグ等といった自動的に安全で快適な運転を実現するための安全機能を有するＥＣＵが接続されるバスの種別である。例えば車両の走行に関連する、エンジンに係るＥＣＵ１００ａ及びブレーキに係るＥＣＵ１００ｂが接続されるバス２００ａは、「駆動系」のバスである。また、車両の装備の制御に関連する、ドア開閉センサに係るＥＣＵ１００ｃ及び窓開閉センサに係るＥＣＵ１００ｄが接続されるバス２００ｂは、「ボディ系」のバスである。また、衝突防止機能に関連するコーナーセンサに係るＥＣＵ１００ｅが接続されるバス２００ｃは、「安全系」のバスである。

【００９０】

［１．１５　不正検知ＥＣＵ４００ａにおける不正検知ルール例］

図１５は、不正検知ＥＣＵ４００ａが保持する不正検知ルール及びバージョン情報の一例を示す。同図に示す不正検知ルール（正規のメッセージＩＤを列挙したリスト）では、不正検知ＥＣＵ４００ａが接続するバス２００ａで送信されるフレーム（メッセージ）は、メッセージＩＤが「１」、「２」及び「３」のいずれにも該当しないと不正なフレームであることを示す。また、バージョン情報は、この不正検知ルールのバージョン（Ｖｅｒ．）が１．０であることを示す。

【００９１】

［１．１６　不正検知ＥＣＵ４００ｂにおける不正検知ルール例］

図１６は、不正検知ＥＣＵ４００ｂが保持する不正検知ルール及びバージョン情報の一例を示す。同図に示す不正検知ルールでは、不正検知ＥＣＵ４００ｂが接続するバス２００ｂで送信されるフレームは、メッセージＩＤが「１」、「２」、「３」及び「４」のいずれにも該当しないと不正なフレームであることを示す。また、バージョン情報は、この不正検知ルールのバージョン（Ｖｅｒ．）が１．０であることを示す。

【００９２】

［１．１７　不正検知ＥＣＵ４００ｃにおける不正検知ルール例］

図１７は、不正検知ＥＣＵ４００ｃが保持する不正検知ルール及びバージョン情報の一例を示す。同図に示す不正検知ルールでは、不正検知ＥＣＵ４００ｃが接続するバス２００ｃで送信されるフレームは、メッセージＩＤが「１」、「２」、「３」、「４」及び「５」のいずれにも該当しないと不正なフレームであることを示す。また、バージョン情報は、この不正検知ルールのバージョン（Ｖｅｒ．）が１．０であることを示す。

【００９３】

［１．１８　配信データフォーマット例］

図１８は、サーバ５００から不正検知ＥＣＵ４００ａ～４００ｃに対して送信される配信データについてのフォーマット（配信データフォーマット）の一例を示す。同図の配信データフォーマットは、配信データが対象車種、不正検知ルールリスト、ＭＡＣを含んで構成されることを示す。対象車種は、配信データの不正検知ルールリストに含まれる更新用不正検知ルール（新しい不正検知ルール）を更新すべき不正検知ＥＣＵを搭載する車両の車種（車両種別）を示す。不正検知ルールリストは、対象車種の車両における車載ネットワークに含まれるバスの種別毎に対する各不正検知ルール（更新用不正検知ルール）を含む。

【００９４】

［１．１９　配信データ例］

図１９は、配信データの内容についての一例を示す。同図の例では、配信データが、車種Ａに対するものであり、対象バス種別（バス種別情報）が示す「駆動系」、「ボディ系」及び「安全系」のそれぞれのバスでの不正なフレームの検知に用いられる不正検知ルール（更新用不正検知ルール）とそのバージョン情報（不正検知ルールＶｅｒ．）とを表している。このように配信データは、１以上（図１９の例では複数）の更新用不正検知ルールと、付属情報（対象車種、バス種別、バージョン情報等）とを含んで構成される。

【００９５】

［１．２０　更新結果データフォーマット例］

図２０は、不正検知ＥＣＵ４００ａ～４００ｃからサーバ５００へと送信される更新結果データについてのフォーマット（更新結果データフォーマット）の一例を示す。同図の更新結果データフォーマットは、更新結果データが、対象車種、車両Ｎｏ．、バス種別、更新後不正検知ルールＶｅｒ．（バージョン）、ＭＡＣを含んで構成されることを示す。更新結果データの対象車種及び車両Ｎｏ．は、更新結果データの送信元の不正検知ＥＣＵを搭載している車両の車種とその車両の車両Ｎｏ．とを示す。また、更新結果データのバス種別は、更新結果データの送信元の不正検知ＥＣＵが接続されているバスのバス種別（つまりバス種別保持部４９６が保持しているバス種別）を示す。更新結果データの更新後不正検知ルールＶｅｒ．は、更新結果データの送信元の不正検知ＥＣＵにおいて更新した不正検知ルールに対応するバージョン情報が示すバージョンである。

【００９６】

［１．２１　更新結果データ例］

図２１は、更新結果データの内容についての一例を示す。同図の例は、「車種Ａの車両Ｎｏ．００００００００１における駆動系のバスに接続された不正検知ＥＣＵが配信データを受け取った結果として、不正検知ルールをバージョン２．０へと更新した」という旨を示す。もし、不正検知ＥＣＵが配信データを受け取った結果として、更新を行わなかった場合には、例えば、更新結果データにおける不正検知ルールＶｅｒ．を「－」（なし）を示すようにして更新しない旨を表すことができる。

【００９７】

［１．２２　サーバ５００の構成］

図２２は、サーバ５００の構成図である。サーバ５００は、車載ネットワークシステム１０が搭載される車両の外部に所在するコンピュータである。サーバ５００は、複数の車両それぞれに車載ネットワークシステム１０が搭載されていることを前提として、各車両（つまり車載ネットワークシステム）に対して不正検知ルール（更新用不正検知ルール）を含む配信データを送信し、各車両における不正検知ルールの更新の状況を管理する。

【００９８】
サーバ５００は、図２２に示すように、通信部５１０と、配信データ管理部５２０と、不正検知ルール保持部５３０と、暗復号処理部５９１と、ＭＡＣ処理部５９２と、鍵保持部５９３と、更新結果管理部５４０と、更新結果表保持部５５０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、サーバ５００におけるハードディスク、メモリ等の記憶媒体、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、通信回路等により実現される。
【００９９】
通信部５１０は、配信データ管理部５２０から通知された配信データを、ネットワーク６００を介して不正検知ＥＣＵ４００ａ～４００ｃへ送信する。また、不正検知ＥＣＵ４００ａ～４００ｃからの更新結果データを受信し、更新結果管理部５４０へ通知する。
【０１００】
配信データ管理部５２０は、不正検知ルール保持部５３０から、最新バージョンの不正検知ルールとその不正検知ルールに対応する付属情報（対象車種、バス種別、バージョン情報等）とを取得する。配信データ管理部５２０は、取得した不正検知ルール及び付属情報をＭＡＣ処理部５９２へ通知してＭＡＣを取得し、取得した不正検知ルール、付属情報及びＭＡＣを暗復号処理部５９１へ通知して、暗号化した配信データ（図１８、図１９参照）を取得する。これにより、配信データは、検証用のＭＡＣの付加、及び、暗号化という暗号処理が施されたものとなる。
【０１０１】
不正検知ルール保持部５３０は、最新バージョンの不正検知ルール（つまり各車載ネットワークシステム１０において更新のために用いられる更新用不正検知ルール）とその不正検知ルールに対応する付属情報を記録媒体等に保持する。なお、不正検知ルール及び付属情報は、サーバ５００の管理者、運用者等の操作により、或いは他のコンピュータから受信することにより、不正検知ルール保持部５３０の記録媒体等に格納される。なお、不正検知ルールを定める者は、車種別の通信仕様の変更に伴って随時不正検知ルールの更新を行い得る。また、特定の車両やバス種別毎に異なる不正検知ルールを生成し得る。
【０１０２】
暗復号処理部５９１は、鍵保持部５９３から取得した鍵を用いて配信データ管理部５２０から通知されるデータを暗号化し、配信データ管理部５２０へ暗号化された配信データを通知する。
【０１０３】
ＭＡＣ処理部５９２は、鍵保持部５９３から取得した鍵を用いて配信データ管理部５２０から通知されるデータを用いてＭＡＣを生成し、生成したＭＡＣを配信データ管理部５２０へ通知する。また、更新結果管理部５４０から通知された更新結果データに含まれるＭＡＣを鍵保持部５９３から取得する鍵を用いて検証して、その検証結果を更新結果管理部５４０へ通知する。
【０１０４】
鍵保持部５９３は、暗復号処理部５９１とＭＡＣ処理部５９２とが暗号処理において利用する鍵を管理する。
【０１０５】
更新結果管理部５４０は、通信部５１０から通知された更新結果データ（図２０、図２１参照）及び通知を受けた日時に基づいて、更新結果表保持部５５０で保持する更新結果表を更新する。
【０１０６】
更新結果表保持部５５０は、不正検知ＥＣＵ４００ａ～４００ｃの更新結果表を保持する。図２３に、更新結果表の一例を示す。
【０１０７】
［１．２３　更新結果表］
図２３は、サーバ５００が保持する更新結果表の一例を示す。同図に例示する更新結果

表では、車種Ａの車両Ｎｏ．００００００００１の車両における各種のバスに接続された不正検知ＥＣＵ毎の不正検知ルールの更新後のバージョンと最終更新日時とを記載して管理している。最終更新日時としては例えば、更新結果管理部５４０が更新結果データの通知を受けた日時を設定し得る。なお、同図に例示する更新結果表では、車種Ａの車両Ｎｏ．００００００００１の車両についての更新結果に係るデータを示したが、サーバ５００が複数の車両の不正検知ＥＣＵに配信データを送信することにより、更新結果表は、車種或いは車両Ｎｏ．が相異なる複数の車両についての不正検知ルールの更新結果に係るデータを含み得る。

【０１０８】

［１．２４　不正フレームの検知に係るシーケンス］

以下、車載ネットワークシステム１０のバス２００ａに不正なＥＣＵが接続された場合における、バス２００ａに接続された不正検知ＥＣＵ４００ａ、ＥＣＵ１００ａ、ＥＣＵ１００ｂ、ゲートウェイ３００ａ等の動作について説明する。

【０１０９】

図２４は、不正検知ＥＣＵ４００ａ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２００ａ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。各シーケンスは、各種装置における各処理手順（ステップ）を示す。

【０１１０】

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（ステップ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２００ａ上に送出される。

【０１１１】

不正なＥＣＵがＩＤフィールド（メッセージＩＤ）までをバス２００ａに送出し終えたときにおいて、不正検知ＥＣＵ４００ａ、ＥＣＵ１００ａ、ＥＣＵ１００ｂ及びゲートウェイ３００ａはそれぞれメッセージＩＤを受信する（ステップＳ１００２）。

【０１１２】

ＥＣＵ１００ａ、ＥＣＵ１００ｂ及びゲートウェイ３００ａ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（ステップＳ１００３）。このとき、不正検知ＥＣＵ４００ａは、保持している不正検知ルールとしてのメッセージＩＤのリスト（ホワイトリスト）を用いてメッセージＩＤをチェックする（ステップＳ１００４）。即ち、不正検知ＥＣＵ４００ａは、不正検知ルールを基準として、送信されたフレームにおけるＩＤフィールドの内容が、ルールに適合しているか否かの判定を行う。この判定では、不正検知ルールとしてのメッセージＩＤのリストに掲載されていない場合にはルールに適合しない（つまり不正なメッセージＩＤであり、送信されたフレームが不正なフレームである）と判定する。

【０１１３】

ステップＳ１００３において、ＥＣＵ１００ａ及びＥＣＵ１００ｂ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４参照）、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、ステップＳ１００３においてゲートウェイ３００ａ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６参照）、受信を継続する。また、ステップＳ１００４において不正検知ＥＣＵ４００ａは、保持している不正検知ルールとしてのメッセージＩＤのリスト（図１５参照）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（ステップＳ１００５）。

【０１１４】

ステップＳ１００３に続いて、ゲートウェイ３００ａはフレームの受信を継続する。例えば、不正検知ＥＣＵ４００ａ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２００ａ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３００ａ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（ステップＳ１００６）。

【０１１５】

次にエラーフレームの発行準備が終わって、不正検知ＥＣＵ４００ａがエラーフレームを送信する（ステップ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２００ａ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。

【０１１６】

ステップ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３００ａ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（ステップＳ１００８）。つまり、ゲートウェイ３００ａ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。

【０１１７】

［１．２５　不正検知ルールの更新に係るシーケンス］

図２５及び図２６は、不正検知ルールの更新（アップデート）に係る動作例を示すシーケンス図である。サーバ５００は各車両の各車載ネットワークシステム１０における各不正検知ＥＣＵに対して更新用不正検知ルールを含む配信データを送信し得るが、ここでは、不正検知ＥＣＵ４００ａが保持する不正検知ルールの更新に注目して説明する。

【０１１８】

まず、サーバ５００において、最新の不正検知ルール（つまり車載ネットワークシステム１０の不正検知ＥＣＵでの更新用となる不正検知ルール）及び付属情報を取得する（ステップＳ１１０１）。

【０１１９】

サーバ５００は、取得した不正検知ルール及び付属情報について付加するためのＭＡＣを生成する（ステップＳ１１０２）。

【０１２０】

サーバ５００は、不正検知ルール、付属情報及びＭＡＣにより所定の配信データフォーマットに従って配信データを構成し、配信データを暗号化する（ステップＳ１１０３）。

【０１２１】

続いてサーバ５００は、暗号化した配信データを不正検知ＥＣＵ４００ａに送信する（ステップＳ１１０４ａ）。これに呼応して、不正検知ＥＣＵ４００ａは、外部通信部４９０により配信データ（詳しくは暗号化された配信データ）を受信する（ステップＳ１１０４ｂ）。

【０１２２】

不正検知ＥＣＵ４００ａの外部通信部４９０は、暗号化された配信データを暗復号処理部４９１に復号させる（ステップＳ１１０５）。

【０１２３】

次に不正検知ＥＣＵ４００ａの外部通信部４９０は、配信データに含まれるＭＡＣをＭＡＣ処理部４９２に検証させる（ステップＳ１１０６）。このＭＡＣの検証に成功した場合には、不正検知ＥＣＵ４００ａの外部通信部４９０は、受信した配信データの内容である不正検知ルール（更新用不正検知ルール）と付属情報（対象車種、バス種別、バージョ

ン情報等）とを更新判定部４９４に伝える。
【０１２４】
ステップＳ１１０６でのＭＡＣの検証が成功した場合に、不正検知ＥＣＵ４００ａの更新判定部４９４は、不正検知ＥＣＵ４００ａが接続されているバス２００ａに係るバス種別をバス種別保持部４９６から取得する（ステップＳ１１０７）。また、更新判定部４９４は、車両Ｎｏ．保持部４９５から車種を取得する。
【０１２５】
次に不正検知ＥＣＵ４００ａの更新判定部４９４は、不正検知ルール保持部４８１が保持する不正検知ルールに対応するバージョン情報を取得する（ステップＳ１１０８）。
【０１２６】
続いて不正検知ＥＣＵ４００ａの更新判定部４９４は、配信データに応じて不正検知ルールを更新する必要があるか否かについて判別する（ステップＳ１１０９）。具体的には、更新判定部４９４は、この判別を、バス種別保持部４９６から取得したバス種別、車両Ｎｏ．保持部４９５から取得した車種、及び、不正検知ルール保持部４８１から取得したバージョン情報が示すバージョンのそれぞれと、配信データに含まれた付属情報が示すバス種別、車種及びバージョン（つまり図１９の対象車種、バス種別、不正検知ルールＶｅｒ．）のそれぞれを比較することにより行う。更新判定部４９４は、車種及びバス種別が一致し、かつ、配信データの内容である更新用不正検知ルールのバージョンが、不正検知ＥＣＵ４００ａが既に用いている不正検知ルールのバージョンより新しいバージョンである場合に限って、更新する必要があると判別する。
【０１２７】
ステップＳ１１０９で更新する必要があると判別した場合には、不正検知ＥＣＵ４００ａの更新判定部４９４は、不正検知ルール保持部４８１に保持されている不正検知ルールを、配信データに含まれる不正検知ルール（更新用不正検知ルール）へと更新する（ステップＳ１１１０）。即ち、不正検知ＥＣＵ４００ａは、サーバ５００から受信した配信データから、接続されているバスの種別に該当するバス種別情報（対象バス種別）に対応する更新用不正検知ルールを抽出して、不正検知ルール保持部４８１が保持していた不正検知ルールを、抽出した更新用不正検知ルールへと更新する。
【０１２８】
ステップＳ１１１０で更新した場合、ステップＳ１１０６でＭＡＣの検証に失敗した場合、或いは、ステップＳ１１０９で更新する必要がないと判別した場合において、更新判定部４９４は、車両Ｎｏ．保持部４９５から車両Ｎｏ．を取得し（ステップＳ１１１１）、取得した車両Ｎｏ．と、更新結果を示す更新結果データとを外部通信部４９０に伝える。更新結果データ（図２１参照）は、例えば、不正検知ルールＶｅｒ．により、更新をした場合には更新後の不正検知ルールのバージョンを示し、更新しなかった場合には、更新なしの旨を示す。
【０１２９】
次に外部通信部４９０では、更新結果に基づいて更新結果データを生成して、その更新結果データに基づきＭＡＣ処理部４９２にＭＡＣを生成させて、更新結果データにＭＡＣを含める（ステップＳ１１１２）。そして外部通信部４９０は、更新結果データをサーバ５００へと送信する（ステップＳ１１１３ａ）。
【０１３０】
サーバ５００では、更新結果データを受信し（ステップＳ１１１３ｂ）、更新結果データにおけるＭＡＣの検証を行う（ステップＳ１１１４）。
【０１３１】
サーバ５００は、ＭＡＣの検証に成功した場合に、更新結果データに基づいて更新結果表（図２３参照）を更新する（ステップＳ１１１５）。ステップＳ１１１４でＭＡＣの検証に失敗した場合にはサーバ５００は、更新結果表の更新を行わない。
【０１３２】
［１．２６　実施の形態１の効果］

実施の形態１に係る車載ネットワークシステム１０では、バスで送信されるフレームが不正か否かを不正検知ＥＣＵにおいて判定する基準となる不正検知ルールを、更新するか否かを判別するため、必要に応じて不正検知ルールを更新することが可能になる。また、更新するか否かを不正検知ＥＣＵが接続されているバスの種別に応じて判別するため、バスの種別毎に独立して不正検知ルールの更新が実現できる。また、更新用となる不正検知ルールを配信するサーバは、一律に各バス種別に対応する最新のバージョンの不正検知ルールを配信できるため、個別に更新内容を選定して送信するよりも、処理負荷が低減され得る。また、更新結果データをサーバに通知するので、サーバにおいて、更新結果を管理して必要に応じて配信データを再送する等の制御が可能になる。

【０１３３】

［１．２７　実施の形態１の変形例］

以下、上述した車載ネットワークシステム１０において、不正検知ＥＣＵ４００ａ～ｃを、その不正検知ＥＣＵ４００ａ～ｃを一部変形してなる不正検知ＥＣＵ１４００ａ～ｃに、置き換えた例について説明する。

【０１３４】

不正検知ＥＣＵ４００ａを一部変形してなる不正検知ＥＣＵ１４００ａでは、不正検知ルールを更新するか否かの判別において、更に、不正検知ＥＣＵ１４００ａを搭載している車両についての車両状態（例えば走行中、停車中等といった走行状態等）を参照する。これにより、不正検知ＥＣＵ１４００ａは、車両状態が例えば安全性の高い所定状態（例えば停車中或いは駐車中等）でなければ不正検知ルールの更新を行わない。

【０１３５】

［１．２８　不正検知ＥＣＵ１４００ａの構成］

図２７は、不正検知ＥＣＵ１４００ａの構成図である。不正検知ＥＣＵ１４００ａは、フレーム送受信部４１０と、フレーム解釈部４２０と、フレーム生成部４６０と、不正検知処理部４８０と、不正検知ルール保持部４８１と、外部通信部４９０と、暗復号処理部４９１と、ＭＡＣ処理部４９２と、鍵保持部４９３と、更新判定部１４９４と、車両Ｎｏ．保持部４９５と、バス種別保持部４９６と、車両状態保持部１４９７と、車両状態判定部１４９８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ＥＣＵ１４００ａ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ＥＣＵ４００ｂを置き換える不正検知ＥＣＵ１４００ｂ、及び、不正検知ＥＣＵ４００ｃを置き換える不正検知ＥＣＵ１４００ｃも基本的に同様の構成を備えるが、不正検知ルール保持部４８１の保持内容（不正検知ルール及びバージョン情報）が互いに異なり得る。実施の形態１（図１４）と同一の構成要素については、同一の符号を付して、説明を省略する。

【０１３６】

更新判定部１４９４は、外部通信部４９０から更新用不正検知ルールと付属情報とを受け取り、バス種別保持部４９６から取得したバス種別と、車両Ｎｏ．保持部４９５が保持する車種と、不正検知ルール保持部４８１が保持する不正検知ルールに対応するバージョン情報と、車両状態保持部１４９７が保持する車両状態とに基づいて、不正検知ルール保持部４８１が保持する不正検知ルールを更新する必要があるか否かを判別する。更新判定部１４９４は、更新する必要があると判別した場合には、不正検知ルール保持部４８１へ通知し、不正検知ルールの更新を行う。また、更新結果と車両Ｎｏ．保持部４９５から取得した車両Ｎｏ．とを外部通信部４９０へ通知する。

【０１３７】

車両状態保持部１４９７は、車両状態判定部１４９８から車両状態を受け取って保持する。車両状態としては、車両の走行に関連する状態の他、車両において測定等により特定可能な各種状態を用いることができる。ここでは、車両状態は、「走行中」及び「停車中」のいずれかであるものとして説明する。

【０１３８】

車両状態判定部１４９８は、車速センサ等のセンサ（不図示）により測定された測定値等を取得することで現在の車両状態を判定して、判定結果としての車両状態を車両状態保持部１４９７に伝える。なお、車両状態判定部１４９８は、車速センサ等のセンサを含んで構成されても良いし、外部の車速センサ等のセンサと専用の通信路で通信しても良いし、その外部のセンサに接続されたＥＣＵからバス２００ａ経由で測定値等を受信しても良い。

【０１３９】

［１．２９　不正検知ルールの更新に係るシーケンス］

図２８及び図２９は、不正検知ルールの更新（アップデート）に係る動作例を示すシーケンス図である。サーバ５００は各車両の各車載ネットワークシステム１０における各不正検知ＥＣＵに対して更新用不正検知ルールを含む配信データを送信し得るが、ここでは、不正検知ＥＣＵ１４００ａが保持する不正検知ルールの更新に注目して説明する。また、実施の形態１で示したステップ（図２５、図２６参照）と同じステップについては、同一の符号を付して、ここでの説明を適宜省略する。

【０１４０】

サーバ５００が、配信データを不正検知ＥＣＵ１４００ａに送信し（ステップＳ１１０１～Ｓ１１０４ａ）、不正検知ＥＣＵ１４００ａは、外部通信部４９０から、ＭＡＣの検証に成功した配信データの内容である不正検知ルール（更新用不正検知ルール）と付属情報（対象車種、バス種別、バージョン情報等）とを更新判定部１４９４に伝える（ステップＳ１１０４ｂ～Ｓ１１０６）。

【０１４１】

次に不正検知ＥＣＵ１４００ａの更新判定部１４９４は、不正検知ＥＣＵ１４００ａが接続されているバス２００ａに係るバス種別をバス種別保持部４９６から取得し、車両Ｎｏ．保持部４９５から車種を取得し、不正検知ルール保持部４８１から不正検知ルールに対応するバージョン情報を取得する（ステップＳ１１０７、Ｓ１１０８）。そして、更新判定部１４９４は、車両状態保持部１４９７から車両状態を取得する（ステップＳ１２０８）。

【０１４２】

続いて不正検知ＥＣＵ１４００ａの更新判定部１４９４は、配信データに応じて不正検知ルールを更新する必要があるか否かについて判別する（ステップＳ１２０９）。具体的には、更新判定部１４９４は、この判別を、バス種別保持部４９６から取得したバス種別、車両Ｎｏ．保持部４９５から取得した車種、及び、不正検知ルール保持部４８１から取得したバージョン情報が示すバージョンのそれぞれと、配信データに含まれた付属情報が示すバス種別、車種及びバージョンのそれぞれを比較し、更に、車両状態保持部１４９７から取得した車両状態が所定状態（ここでは停車中とする。）であるかどうかを確認することにより行う。更新判定部１４９４は、車種及びバス種別が一致し、配信データの内容である更新用不正検知ルールのバージョンが、不正検知ＥＣＵ１４００ａが既に用いている不正検知ルールのバージョンより新しいバージョンであり、かつ、車両状態が停車中である場合に限って、更新する必要があると判別する。なお、走行に関連する駆動系のバスに接続された不正検知ＥＣＵでは、停車中でないと不正検知ルールの更新を行わないが、駆動系以外のバスに接続された不正検知ＥＣＵでは走行中に不正検知ルールの更新を行い得るといったように、バス種別に応じて車両状態についての更新の要件となる所定状態を異ならせても良い。

【０１４３】

ステップＳ１２０９で更新する必要があると判別した場合には、不正検知ＥＣＵ１４００ａの更新判定部１４９４は、不正検知ルール保持部４８１に保持されている不正検知ルールを、配信データに含まれる不正検知ルール（更新用不正検知ルール）へと更新する（ステップＳ１１１０）。

【０１４４】

［１．３０　実施の形態１の変形例の効果］

実施の形態１の変形例１に係る車載ネットワークシステム１０では、バスで送信されるフレームが不正か否かを不正検知ＥＣＵにおいて判定する基準となる不正検知ルールを更新するか否かを、不正検知ＥＣＵが接続されているバスの種別、不正検知ＥＣＵを搭載する車両の車両状態等に応じて判別する。このため、車両状態が例えば安全性が高い所定状態である場合に限って不正検知ルールの更新を行うこと等が可能となる。

【０１４５】

（実施の形態２）

以下、実施の形態１で示した車載ネットワークシステム１０を一部変形してなる車載ネットワークシステム２０について説明する。

【０１４６】

実施の形態１に係る車載ネットワークシステム１０においては、不正検知ＥＣＵ４００ａ～４００ｃのそれぞれが、サーバ５００と通信することにより更新用不正検知ルール等を取得して、バス上での不正なフレームの検査に用いる不正検知ルールを更新する機能を有する。これに対して、本実施の形態に係る車載ネットワークシステム２０では、ヘッドユニットという一種のＥＣＵが外部のサーバ５００との通信機能を担い、各不正検知ＥＣＵは、ヘッドユニットを経由して更新用不正検知ルール等を取得することにより、不正検知機能を更新する。

【０１４７】

［２．１　車載ネットワークシステム２０の全体構成］

図３０は、車載ネットワークシステム２０の全体構成を示す図である。車載ネットワークシステム２０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２０は、バス２００ａ～２００ｄと、不正検知ＥＣＵ２４００ａ～２４００ｃ、ゲートウェイ２３００ａ、２３００ｂ、ヘッドユニット８００、及び、各種機器に接続されたＥＣＵ１００ａ～１００ｅ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。また図３０では、車載ネットワークシステム２０におけるヘッドユニット８００と無線通信する外部のネットワーク６００及びそのネットワーク６００と通信可能に接続されたサーバ２５００とを付記している。実施の形態１に係る車載ネットワークシステム１０（図１参照）と同一の構成要素については、同一の符号を付して、ここでの説明を省略する。また、車載ネットワークシステム２０は、ここで特に説明しない点については車載ネットワークシステム１０と同様である。

【０１４８】

ゲートウェイ２３００ａは、不正検知ＥＣＵ２４００ａ、ＥＣＵ１００ａ及びＥＣＵ１００ｂがつながるバス２００ａと、不正検知ＥＣＵ２４００ｂ、ＥＣＵ１００ｃ及びＥＣＵ１００ｄがつながるバス２００ｂと、ヘッドユニット８００がつながるバス２００ｄとに接続している。ゲートウェイ２３００ｂは、不正検知ＥＣＵ２４００ｂ、ＥＣＵ１００ｃ及びＥＣＵ１００ｄがつながるバス２００ｂと、不正検知ＥＣＵ２４００ｃ及びＥＣＵ１００ｅがつながるバス２００ｃとに接続している。ゲートウェイ２３００ａ、２３００ｂは、ある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２３００ａ、２３００ｂも一種のＥＣＵである。

【０１４９】

不正検知ＥＣＵ２４００ａ～２４００ｃは、実施の形態１で示した不正検知ＥＣＵ４００ａ～４００ｃを一部変形したものであり、自ＥＣＵが接続されたバス上に現れるフレームを監視して不正なフレームを検知した場合には、エラーフレームを送信する機能を有する（図２４参照）。従って、不正検知ＥＣＵ２４００ａ～２４００ｃは、不正検知ＥＣＵ４００ａ～４００ｃと同様に、バス上で不正なフレームが送信された場合に、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。

【０１５０】

ヘッドユニット８００は、車両用通信装置であり、例えば、自動車のインストルメント

パネル（インパネ）等に設けられ、運転者（ユーザ）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。

【０１５１】

サーバ２５００は、車載ネットワークシステム２０における不正検知ＥＣＵ２４００ａ～２４００ｃの不正検知機能の基礎となる不正検知ルールを更新するために配信データを、ネットワーク６００を介してヘッドユニット８００へと送信する機能を有する。サーバ２５００とヘッドユニット８００との間での通信方式はいかなる方式を用いても良い。

【０１５２】

［２．２　ヘッドユニット８００の構成］

図３１は、ヘッドユニット８００の構成図である。ヘッドユニット８００は、フレーム送受信部８１０と、フレーム解釈部８２０と、受信ＩＤ判断部８３０と、受信ＩＤリスト保持部８４０と、フレーム処理部８５０と、フレーム生成部８６０と、表示制御部８５３と、更新管理部８５４と、更新結果表保持部８５５、外部通信部８９０と、暗復号処理部８９１と、ＭＡＣ処理部８９２と、鍵保持部８９３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８００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。

【０１５３】

フレーム送受信部８１０は、バス２００ｄに対して、ＣＡＮの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８１０は、バス２００ｄからフレームを１ｂｉｔずつ受信し、フレーム解釈部８２０に転送する。また、フレーム生成部８６０より通知を受けたフレームの内容をバス２００ｄに送信する。

【０１５４】

フレーム解釈部８２０は、フレーム送受信部８１０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８３０へ転送する。また、フレーム解釈部８２０は、受信ＩＤ判断部８３０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８５０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８２０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８６０へ通知する。また、フレーム解釈部８２０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。

【０１５５】

受信ＩＤ判断部８３０は、フレーム解釈部８２０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８４０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８３０は、フレーム解釈部８２０へ通知する。

【０１５６】

受信ＩＤリスト保持部８４０は、ヘッドユニット８００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３２に、ヘッドユニット８００における受信ＩＤリストの一例を示す。

【０１５７】

フレーム処理部８５０は、各ＥＣＵから送信され、受信したフレームのデータ（例えばエンジンに係るＥＣＵ１００ａから得られた時速等）を表示できる形式に変換し、表示制御部８５３に通知する。また、フレーム処理部８５０は、不正検知ＥＣＵ２４００ａ～２４００ｃから送信されたフレームに含まれる内部更新結果データ（後述）を更新管理部８

５４へ通知する。
【０１５８】
表示制御部８５３は、フレーム処理部８５０から通知されたデータを表示する。
【０１５９】
フレーム生成部８６０は、フレーム解釈部８２０から通知されたエラーフレーム送信の要求に従い、エラーフレームを構成し、フレーム送受信部８１０へ通知する。また、更新管理部８５４からの指示に従ってデータフレームを構成し、フレーム送受信部８１０へ通知する。
【０１６０】
更新管理部８５４は、外部通信部８９０から受信した配信データに含まれる不正検知ルール（更新用不正検知ルール）及び付属情報（バス種別情報、バージョン情報等）をＣＡＮプロトコルに従った形式に変換して、フレーム生成部８６０に渡すことによりデータフレームを生成させる。なお、配信データに含まれる付属情報のうち、対象車種の情報については、例えば更新管理部８５４が、ヘッドユニット８００を搭載している車両の車種と比較し、一致しない場合には配信データを破棄し得る。ここで、ヘッドユニット８００が車載ネットワークシステム２０におけるバスを介して不正検知ＥＣＵ２４００ａ～２４００ｃへと配信するデータフレームを内部配信データと称する。内部配信データは、更新用不正検知ルール、バス種別及びバージョン情報を含む（図３３参照）。ここでは、内部配信データとして、「駆動系」のバス種別のバス２００ａに接続された不正検知ＥＣＵ２４００ａが受信可能なように配信するデータフレームには、「０ｘ０Ｅ０」という不正検知ルール更新用のメッセージＩＤを付し、「ボディ系」のバス種別のバス２００ｂに接続された不正検知ＥＣＵ２４００ｂが受信可能なように配信するデータフレームには、「０ｘ０Ｅ１」という不正検知ルール更新用のメッセージＩＤを付し、「安全系」のバス種別のバス２００ｃに接続された不正検知ＥＣＵ２４００ｃが受信可能なように配信するデータフレームには、「０ｘ０Ｅ２」という不正検知ルール更新用のメッセージＩＤを付すものとする。なお、不正検知ＥＣＵ２４００ａ～２４００ｃは、それぞれが対応する不正検知ルール更新用のメッセージＩＤのデータフレームを受信して、内部配信データを取得することで、不正検知ルールを更新するか否かを判別して必要に応じて更新する。また、更新管理部８５４は、フレーム処理部８５０から受信した内部更新結果データに基づいて、更新結果表保持部８５５で保持する内部更新結果表を更新する。
【０１６１】
更新結果表保持部８５５は、不正検知ＥＣＵ２４００ａ～２４００ｃからの内部更新結果データ（図３４参照）により構成される内部更新結果表を記憶媒体等に保持する。なお、内部更新結果表に基づいて、更新管理部８５４が、配信データに含まれる各種バス用の各不正検知ルールのうち、バージョン情報の点で更新が必要な不正検知ルールを選択することで、ヘッドユニット８００から特定の不正検知ルールに係る内部配信データの送信を行っても良く、また、同様に更新失敗に際しての内部配信データの再送信を行っても良い。
【０１６２】
外部通信部８９０は、サーバ２５００とネットワーク６００を介して通信することで、不正検知ＥＣＵ２４００ａ～２４００ｃにおける不正検知ルールを更新するための更新用不正検知ルール（新たな不正検知ルール）等を含む配信データを取得する。外部通信部８９０は、取得した配信データを暗復号処理部８９１へ送信し、復号した結果を取得する。また、復号した配信データにおける検証用データとしてのＭＡＣをＭＡＣ処理部８９２へ通知し、ＭＡＣの検証結果を受け取る。外部通信部８９０は、復号した配信データから更新用不正検知ルールと付属情報（対象車種、バス種別情報、バージョン情報等）と抽出し、更新管理部８５４へ通知する。サーバ２５００から配信される配信データには暗号処理が施されている。ここで、サーバ２５００が施す暗号処理は、例えば、暗号化、検証用データの付加等である。これに対して、暗復号処理部８９１及びＭＡＣ処理部８９２は、配信データについてサーバ２５００等で実行された暗号処理に呼応する暗号処理（例えば暗

号化に呼応する復号、検証用データの付加に呼応する検証）を実行する。
【０１６３】
暗復号処理部８９１は、外部通信部８９０から通知される暗号化された配信データを、鍵保持部８９３から取得する鍵を用いて復号し、復号した配信データを外部通信部８９０へ通知する。
【０１６４】
ＭＡＣ処理部８９２は、外部通信部８９０から通知される配信データにおけるＭＡＣを、鍵保持部８９３から取得する鍵を用いて検証し、検証結果を外部通信部８９０へ通知する。
【０１６５】
鍵保持部８９３は、暗復号処理部８９１とＭＡＣ処理部８９２とが暗号処理において利用する鍵を管理する。
【０１６６】
［２．３　ヘッドユニット８００における受信ＩＤリスト例］
図３２は、ヘッドユニット８００の受信ＩＤリスト保持部８４０が保持する受信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」、「４」及び「５」の他に、「０ｘ０Ｆ０」、「０ｘ０Ｆ１」及び「０ｘ０Ｆ２」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。ここでは、別々のバスに接続された不正検知ＥＣＵ２４００ａ～２４００ｃとの通信のため、ＩＤを区別している。例えば「０ｘ０Ｆ０」というメッセージＩＤは、「駆動系」のバス種別のバス２００ａに接続された不正検知ＥＣＵ２４００ａからの内部更新結果データを含むデータフレームを受信するために用いられる。また「０ｘ０Ｆ１」というメッセージＩＤは、「ボディ系」のバス種別のバス２００ｂに接続された不正検知ＥＣＵ２４００ｂからの内部更新結果データを含むデータフレームを受信するために用いられる。また「０ｘ０Ｆ２」というメッセージＩＤは、「安全系」のバス種別のバス２００ｃに接続された不正検知ＥＣＵ２４００ｃからの内部更新結果データを含むデータフレームを受信するために用いられる。
【０１６７】
［２．４　ヘッドユニット８００が送信する内部配信データ］
図３３は、ヘッドユニット８００から不正検知ＥＣＵ２４００ａが受信可能なように送信する内部配信データの一例を示す。同図は、データフレームのＩＤ（メッセージＩＤ）を「０ｘ０Ｅ０」にしており、データフィールド内に不正検知ルール（更新用不正検知ルール）とバージョン情報とを含んでいる例を示している。この例では、バージョン情報が示すバージョンは「２．０」を意味し、不正検知ルールは、メッセージＩＤとして「１」、「２」、「３」及び「４」の４つを掲載したホワイトリストを示し、これらの４つのＩＤ以外を含むフレームが不正なフレームと判定されることを表している。
【０１６８】
［２．５　ヘッドユニット８００が受信する内部更新結果データ］
図３４は、不正検知ＥＣＵ２４００ａからヘッドユニット８００に通知する内部更新結果データの一例を示す。同図に例示する内部更新結果データは、駆動系のバスに接続された不正検知ＥＣＵが内部配信データを受け取った結果として、不正検知ルールをバージョン２．０へと更新した旨を表している。
【０１６９】
［２．６　ゲートウェイ２３００ａ、２３００ｂの構成］
ゲートウェイ２３００ａは、実施の形態１で示したゲートウェイ３００ａ（図１２参照）と基本的に同様の機能を有する他、バス２００ｄが接続され、転送ルール保持部３５２が保持する転送ルールの内容が異なる。ゲートウェイ２３００ｂは、実施の形態１で示したゲートウェイ３００ｂと基本的に同様の機能を有するが、転送ルール保持部３５２が保持する転送ルールの内容が異なる。ゲートウェイ２３００ａ、２３００ｂにおける転送ルールは、ヘッドユニット８００から送信された内部配信データが、受信されるべき不正検

知ＥＣＵに伝達されるように定められており、また、各不正検知ＥＣＵからの内部更新結果データがヘッドユニット８００に伝達されるように定められている。

【０１７０】

［２．７　転送ルール例］

図３５は、ゲートウェイ２３００ａが保持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３５中の「＊」は、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。図３５の例は、バス２００ａ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２００ｂ及びバス２００ｄ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２００ｂから受信するフレームのうち、バス２００ｄには全てのフレームが転送されるが、バス２００ａ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２００ｄから受信されるフレームは、「駆動系」のバス２００ａにはメッセージＩＤが「０ｘＥ０」であるフレーム（内部配信データ）が転送され、ゲートウェイ２３００ｂを経由して「安全系」のバス２００ｃへの伝達経路ともなる「ボディ系」のバス２００ｂにはメッセージＩＤが「０ｘＥ１」及び「０ｘＥ２」であるフレーム（内部配信データ）が転送されるように設定されていることを示している。

【０１７１】

［２．８　不正検知ＥＣＵ２４００ａの構成］

図３６は、不正検知ＥＣＵ２４００ａの構成図である。不正検知ＥＣＵ２４００ａは、フレーム送受信部４１０と、フレーム解釈部２４２０と、フレーム処理部２４５０と、フレーム生成部２４６０と、不正検知処理部４８０と、不正検知ルール保持部４８１と、更新判定部２４９４と、バス種別保持部４９６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ＥＣＵ２４００ａ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ＥＣＵ２４００ｂ及び不正検知ＥＣＵ２４００ｃも基本的に同様の構成を備えるが、不正検知ルール保持部４８１の保持内容（不正検知ルール及びバージョン情報）と、フレーム生成部２４６０が生成する内部更新結果データとしてのデータフレームに含ませるメッセージＩＤと、フレーム解釈部２４２０がフレーム処理部２４５０に通知する内部配信データを他のデータフレームと区別するためのメッセージＩＤとが互いに異なり得る。不正検知ＥＣＵ２４００ａの構成要素のうち、実施の形態１で示した不正検知ＥＣＵ４００ａと同一の構成要素については、同一の符号を付して、説明を省略する。

【０１７２】

フレーム解釈部２４２０は、フレーム送受信部４１０よりフレームの値を受け取り、ＣＡＮプロトコルにおける各フィールドにマッピングするよう解釈を行う。ＩＤフィールドと判断した値は不正検知処理部４８０へ転送する。また、内部配信データについての不正検知ルール更新用のメッセージＩＤ「０ｘ０Ｅ０」を含むフレームのデータの内容についてはフレーム処理部２４５０へ通知する。また、フレーム解釈部２４２０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２４６０へ通知する。また、フレーム解釈部２４２０は、エラーフレームを受信した場合、受信中のフレームに対し、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。

【０１７３】

フレーム生成部２４６０は、フレーム解釈部２４２０又は不正検知処理部４８０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４１０へ通知して送信させる。また、フレーム生成部２４６０は、更新判定部２４９４から不正検知ルールの更新結果が通知された場合は、その更新結果に応じて内部更新結果データとしてのメッセージＩＤが「０ｘＦ０」であるデータフレームを構成し、フレーム送受信部４１０へ通知して送信させる。

【０１７４】
フレーム処理部２４５０は、受信した内部配信データから不正検知ルール（更新用不正検知ルール）と付属情報（バス種別を示すバス種別情報、及び、バージョン情報）とを抽出し、更新判定部２４９４へ通知する。
【０１７５】
不正検知ルール保持部４８１は、不正検知ルールとして、バス２００ａを送信されるフレームに含まれるメッセージＩＤを規定したリストを保持し、その不正検知ルールについてのバージョンを示すバージョン情報を保持する（図３７参照）。また、不正検知ルール保持部４８１は、更新判定部２４９４からの新たな不正検知ルール（更新用不正検知ルール）の通知に応じて、更新用不正検知ルールで先に保持していた不正検知ルールを更新し、更新した結果を更新判定部２４９４へ通知する。
【０１７６】
更新判定部２４９４は、フレーム処理部２４５０から更新用不正検知ルール、バス種別を示すバス種別情報及びバージョン情報を受け取り、バス種別保持部４９６から取得したバス種別と、不正検知ルール保持部４８１が保持する不正検知ルールに対応するバージョン情報とに基づいて、不正検知ルール保持部４８１が保持する不正検知ルールを更新する必要があるか否かを判別する。更新判定部２４９４は、更新する必要があると判別した場合には、不正検知ルール保持部４８１へ通知し、不正検知ルールの更新を行う。また、更新結果をフレーム生成部２４６０へ通知する。
【０１７７】
［２．９　不正検知ＥＣＵ２４００ａにおける不正検知ルール例］
図３７は、不正検知ＥＣＵ２４００ａが保持する不正検知ルール及びバージョン情報の一例を示す。同図に示す不正検知ルール（正規のメッセージＩＤを列挙したリスト）では、不正検知ＥＣＵ２４００ａが接続するバス２００ａで送信されるフレーム（メッセージ）は、メッセージＩＤが「１」、「２」、「３」、「０ｘ０Ｅ０」及び「０ｘ０Ｆ０」のいずれにも該当しないと不正なフレームであることを示す。また、図３７に示すバージョン情報は、この不正検知ルールのバージョン（Ｖｅｒ．）が１．０であることを示す。
【０１７８】
［２．１０　不正検知ＥＣＵ２４００ｂにおける不正検知ルール例］
図３８は、不正検知ＥＣＵ２４００ｂが保持する不正検知ルール及びバージョン情報の一例を示す。同図に示す不正検知ルールでは、不正検知ＥＣＵ２４００ｂが接続するバス２００ｂで送信されるフレームは、メッセージＩＤが「１」、「２」、「３」、「４」、「０ｘ０Ｅ１」、「０ｘ０Ｅ２」、「０ｘ０Ｆ１」及び「０ｘ０Ｆ２」のいずれにも該当しないと不正なフレームであることを示す。また、バージョン情報は、この不正検知ルールのバージョン（Ｖｅｒ．）が１．０であることを示す。
【０１７９】
［２．１１　不正検知ＥＣＵ２４００ｃにおける不正検知ルール例］
図３９は、不正検知ＥＣＵ２４００ｃが保持する不正検知ルール及びバージョン情報の一例を示す。同図に示す不正検知ルールでは、不正検知ＥＣＵ２４００ｃが接続するバス２００ｃで送信されるフレームは、メッセージＩＤが「１」、「２」、「３」、「４」、「５」、「０ｘ０Ｅ２」及び「０ｘ０Ｆ２」のいずれにも該当しないと不正なフレームであることを示す。また、バージョン情報は、この不正検知ルールのバージョン（Ｖｅｒ．）が１．０であることを示す。
【０１８０】
［２．１２　サーバ２５００の構成］
図４０は、サーバ２５００の構成図を示す。サーバ２５００は、実施の形態１で示したサーバ５００（図２２参照）を一部変形したものであり、車載ネットワークシステム２０が搭載される車両の外部に所在するコンピュータである。サーバ２５００は、通信部２５１０と、配信データ管理部５２０と、不正検知ルール保持部５３０と、暗復号処理部５９１と、ＭＡＣ処理部５９２と、鍵保持部５９３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、サーバ２５００におけるハードディスク、メモリ等の記憶媒体、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、通信回路等により実現される。なお、サーバ２５００の構成要素のうち実施の形態１で示したサーバ５００と同等の構成要素については、同じ符号を付して、説明を省略する。

【０１８１】

通信部２５１０は、配信データ管理部５２０から通知された配信データ（図１８、図１９参照）を、ネットワーク６００を介してヘッドユニット８００へ通知する。なお、サーバ２５００は１台以上の各車両の各車載ネットワークシステム２０におけるヘッドユニット８００に対して更新用不正検知ルールを含む配信データを送信し得る。

【０１８２】

［２．１３　内部更新結果表］

図４１は、ヘッドユニット８００が保持する内部更新結果表の一例を示す。同図に例示する内部更新結果表では、バス種別毎に、最終的な更新後の不正検知ルールについてのバージョンを記載して管理している。

【０１８３】

［２．１４　不正検知ルールの更新に係るシーケンス］

図４２及び図４３は、不正検知ルールの更新（アップデート）に係る動作例を示すシーケンス図である。実施の形態１における不正検知ルールの更新に係るシーケンス（図２５、図２６参照）と同様のステップについては、同一の符号を付して適宜説明を省略する。なお、実施の形態１に係るサーバ５００による配信データの送信の宛先は不正検知ＥＣＵ４００ａ～４００ｃであったが、サーバ２５００による配信データの送信の宛先はヘッドユニット８００であり、車載ネットワークシステム２０においてヘッドユニット８００が配信データに基づく内部配信データを不正検知ＥＣＵ２４００ａ～２４００ｃへとバスを介して送信する。ここでは、ヘッドユニット８００及び不正検知ＥＣＵ２４００ａに注目して説明する。

【０１８４】

まず、サーバ２５００が、配信データを構成して暗号化し（ステップＳ１１０１～Ｓ１１０３）、ヘッドユニット８００に送信する（ステップＳ２１０４ａ）。これに呼応して、ヘッドユニット８００は、外部通信部８９０により配信データ（詳しくは暗号化された配信データ）を受信する（ステップＳ２１０４ｂ）。

【０１８５】

ヘッドユニット８００の外部通信部８９０は、暗号化された配信データを暗復号処理部８９１に復号させる（ステップＳ２１０５）。

【０１８６】

次にヘッドユニット８００の外部通信部８９０は、配信データに含まれるＭＡＣをＭＡＣ処理部８９２に検証させる（ステップＳ２１０６）。このＭＡＣの検証に失敗した場合には処理を終え、このＭＡＣの検証に成功した場合には、ヘッドユニット８００の外部通信部８９０は、受信した配信データの内容である不正検知ルール（更新用不正検知ルール）と付属情報（対象車種、バス種別、バージョン情報等）とを更新管理部８５４に伝える。

【０１８７】

ヘッドユニット８００の更新管理部８５４は、配信データに含まれる不正検知ルール（更新用不正検知ルール）及び付属情報（バス種別、バージョン情報等）をＣＡＮプロトコルに従った形式の内部配信データに変換し、これによりヘッドユニット８００は、内部配信データを、バス２００ｄを介して送信（ブロードキャスト）する（ステップＳ２１０７ａ）。更新用不正検知ルール、バス種別及びバージョン情報を含む内部配信データはゲートウェイ２３００ａを経由してバス２００ａに接続された不正検知ＥＣＵ２４００ａに受信される（ステップＳ２１０７ｂ）。

【０１８８】

次に不正検知ＥＣＵ２４００ａの更新判定部２４９４は、不正検知ＥＣＵ２４００ａが

接続されているバス２００ａに係るバス種別をバス種別保持部４９６から取得し、不正検知ルール保持部４８１から不正検知ルールに対応するバージョン情報を取得する（ステップＳ１１０７、Ｓ１１０８）。

【０１８９】

続いて不正検知ＥＣＵ２４００ａの更新判定部２４９４は、内部配信データに応じて不正検知ルールを更新する必要があるか否かについて判別する（ステップＳ１１０９）。具体的には、更新判定部２４９４は、この判別を、バス種別保持部４９６から取得したバス種別、及び、不正検知ルール保持部４８１から取得したバージョン情報のそれぞれと、内部配信データに含まれたバス種別及びバージョン情報のそれぞれを比較することにより行う。更新判定部１４９４は、バス種別が一致し、内部配信データの内容である更新用不正検知ルールのバージョンが、不正検知ＥＣＵ２４００ａが既に用いている不正検知ルールのバージョンより新しいバージョンである場合に限って、更新する必要があると判別する。

【０１９０】

ステップＳ１１０９で更新する必要があると判別した場合には、不正検知ＥＣＵ２４００ａの更新判定部２４９４は、不正検知ルール保持部４８１に保持されている不正検知ルールを、内部配信データに含まれる不正検知ルール（更新用不正検知ルール）へと更新する（ステップＳ１１１０）。

【０１９１】

ステップＳ１１１０で更新した場合、或いは、ステップＳ１１０９で更新する必要がないと判別した場合において、更新判定部２４９４が更新結果をフレーム生成部２４６０に通知することで、不正検知ＥＣＵ２４００ａは、更新結果に応じて内部更新結果データとしてのメッセージＩＤが「０ｘＦ０」であるデータフレームを、バス２００ａを介して送信（ブロードキャスト）する（ステップＳ２１１０ａ）。内部更新結果データはゲートウェイ２３００ａを経由してバス２００ｄに接続されたヘッドユニット８００に受信される（ステップＳ２１１０ｂ）。

【０１９２】

続いてヘッドユニット８００は、受信した内部更新結果データに基づいて内部更新結果表を更新する（ステップＳ２１１５）。

【０１９３】

［２．１５　実施の形態２の効果］

実施の形態２に係る車載ネットワークシステム２０では、不正検知ＥＣＵにおける不正検知ルールをヘッドユニット経由で取得し、不正検知ＥＣＵがつながるバスの種別に応じて不正検知ルールの更新を行うかどうかを切り替えているので、更新に失敗した際の不正検知ルールの再送制御等が比較的容易になる。また、実施の形態１の場合に比べて、不正検知ルールの更新状態についてサーバで管理すべきデータが削減される。また、車載ネットワークシステム２０において、１つのヘッドユニット８００だけが外部との通信及び暗号処理を行うため個々の不正検知ＥＣＵの処理負荷が削減されるので、不正検知ＥＣＵを比較的少ないリソースで構成することが可能となる。

【０１９４】

（他の実施の形態）

以上のように、本発明に係る技術の例示として実施の形態１、２を説明した。しかしながら、本発明に係る技術は、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発明の一実施態様に含まれる。

【０１９５】

（１）上記実施の形態では、不正検知機能をアップデート（更新）するための配信データを送信する外部装置としてのサーバを示したが、この配信データに相当する情報を、車載ネットワークにおける、ＯＢＤ２（On-Board Diagnostics２）と呼ばれる診断ポート（外部ツール接続用のインタフェース）から接続される外部装置である外部ツール（所謂診

断ツール等）から送信しても良い。また、外部ツールを個々の不正検知ＥＣＵに接続して外部ツールから配信データに相当する情報を入力しても良い。また、実施の形態２で示したヘッドユニット８００における内部更新結果表の内容を、診断ポートに接続した外部ツールが取得できるようにしても良い。なお、ヘッドユニット８００は、ユーザ操作に応じて内部更新結果表の内容を表示しても良い。

【０１９６】

（２）上記実施の形態では、不正検知ルールとして正規のＩＤを列挙したホワイトリストを用いてフレームが不正か否かの判定を行う例を示したが、フレームの検査（不正か否かの判定）には他の判定基準を定めた不正検知ルールを用いても良い。例えば、正規でないＩＤで構成されたブラックリストを用いて判定を行っても良いし、ＤＬＣを用いた判定、送信メッセージの周期時間を用いた判定、一定時間内における送信頻度を用いた判定、或いは、適正なデータを示すデータフィールドを用いた判定を行っても良い。いかなる検査（フレームが不正か否かの判定）の方法を用いても、その判定の基準となるルールを表すものが不正検知ルールである。不正検知ルールは、バス上に現れるフレームが不正か否か（つまりルールに適合するか否か）の判定の基準となるルールとしての情報、そのルールへの適合性を判定するためのプログラム（判定アルゴリズムを実現するプログラム等）、或いは、情報及びプログラムを包含するファームウェア等であり得る。ファームウェアは、例えば、ＥＣＵ内のプログラム等のソフトウェア、プログラムで用いられるデータを含み、例えば、ＥＣＵ内のプロセッサにおけるマイクロコード、或いはＥＣＵがＰＬＣ（Programmable Logic Device）又はＦＰＧＡ（Field Programmable Gate Array）を含む場合にこれらにおける回路構成用のデータ等を含み得る。なお、例えば不正検知ルールが、判定の基準となるルールとしての情報と、判定を行うためのアルゴリズムを実現するプログラムとに区別できる場合に、配信ルールの送信に際してそれぞれ別個の鍵を用いた暗号処理（暗号化、ＭＡＣの付加等）を施しても良い。また暗号処理に呼応した処理（復号、ＭＡＣの検証等）に用いる鍵を、バス種別、不正検知ＥＣＵ毎に別個になるようにしても良い。

【０１９７】

（３）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、データフレームのＩＤ（メッセージＩＤ）を表す。なお、車載ネットワークシステムは、必ずしもＣＡＮプロトコルに完全に準拠したものでなくても良い。

【０１９８】

（４）上記実施の形態では、配信データを、外部装置であるサーバからプッシュしているが、ヘッドユニット或いは不正検知ＥＣＵから不正検知ルールの更新のための配信データがあるかどうかを問い合わせるとしても良い。問い合わせるタイミングとしては、定期的の他に、車両状態の変化のタイミング（例えばエンジン始動時、イグニッションキーがイグニッションキーシリンダに差し込まれた時）等としても良い。

【０１９９】

（５）上記実施の形態では、配信データの中に、不正検知ルールとバージョン情報とをセットでサーバからプッシュしているが、バージョン情報だけを送信してから必要に応じて配信データを送るとしても良い。また、配信データを送信するタイミングもサーバで車両状態を考慮して送信しても良い。この場合には、サーバは車両状態を不正検知ＥＣＵ或いはヘッドユニットから取得して判定する。

【０２００】

（６）上記実施の形態２ではヘッドユニットから不正検知ＥＣＵへの内部配信データの配信を、バス経由でＣＡＮプロトコルに従って行うこととしたが、それ以外の方法で配信しても良い。例えば、ヘッドユニットと不正検知ＥＣＵとを結ぶ専用通信路を用いても良い。

【０２０１】

（７）上記実施の形態１の変形例で示した不正検知ＥＣＵは、ステップＳ１２０９において車両状態が所定状態でないことにより不正検知ルールの更新を行うべきでないと判別した場合には、取得した配信データに含まれる更新用不正検知ルールを一時的に保持して、車両状態が所定状態に変更されるのを待って不正検知ルール保持部４８１に保持されている不正検知ルールの更新（更新用不正検知ルールへの更新）を行っても良い。また、車両状態が所定状態に変更されるのを待ってからサーバ（外部装置）に配信データの再送を要求して、配信データを新たに受信して不正検知ルールを、新たに受信したその配信データに含まれる更新用不正検知ルールへと更新しても良い。

【０２０２】

（８）上記実施の形態で示した配信データに付加するＭＡＣについては、共通鍵としても良いし、公開鍵で検証可能な署名としても良い。また実施の形態２では、サーバとヘッドユニットのみで暗号処理（暗号化、ＭＡＣ生成、ＭＡＣ検証）を行っているが、ヘッドユニットと不正検知ＥＣＵとの間の通信においても事前に鍵共有を行い、通信内容に対して暗号処理を行っても良い。なお、暗号化及び復号に使用する鍵と、ＭＡＣの生成及び検証に使用する鍵は、同一の鍵であっても別々の鍵であっても良い。

【０２０３】

（９）上記実施の形態２では、不正検知ＥＣＵが、外部と接続するヘッドユニット経由で、不正検知ルール等を受信しているが、ヘッドユニットは一例にすぎず、外部と接続する別のＥＣＵを介して受信しても良い。外部と接続するＥＣＵは、例えば、複数のプロトコルによる通信バスと接続するセントラルゲートウェイ、診断ポートを制御するゲートウェイ等であっても良い。

【０２０４】

（１０）上記実施の形態では、不正検知ＥＣＵが接続するバスの種類として「駆動系」、「ボディ系」、「安全系」を例示したが、いかなる体系でバスの種別を区分しても良いし、その区分の数がいくつであっても良い。

【０２０５】

（１１）上記実施の形態では、不正検知ルールを更新する必要があるか否かの判別を、車種、バス種別、バージョン情報、車両状態等に応じて行う例を示したが、この判別の条件となる所定更新条件として、その例示した条件（車種、バス種別、バージョン情報、車両状態等）の一部だけを用いても良いし、また例示した以外の条件を加えても良い。所定更新条件は、不正検知ルールに対応して定められた付属情報（車種、バス種別、バージョン情報等）に関する条件だけであっても良いし、付属情報とは独立した車両状態等に関する条件を含んでいても良い。また、このような所定更新条件が満たされるか否かの判別は、不正検知ＥＣＵ及びその他のＥＣＵ（ヘッドユニット等）のいずれが行っても、分担して行っても良い。所定更新条件が満たされると、不正検知ＥＣＵが不正フレームの判定に用いる不正検知ルールが、新たな不正検知ルール（更新用不正検知ルール）へ更新されるように構成してれば良い。例えば、所定更新条件が付属情報に関する条件だけである場合においては、不正検知ＥＣＵは、不正検知ルールの更新を、不正検知ＥＣＵが受信した配信データ或いは内部配信データにおける付属情報が所定更新条件を満たす場合には行い、付属情報が所定更新条件を満たさない場合には行わない。また、付属情報としての車種を含ませる場合には、その付属情報の車種が、車載ネットワークシステムを搭載する車両の車種を示す場合に、その車載ネットワークシステムでは所定更新条件が満たされたとして不正検知ルールの更新を行い得る。

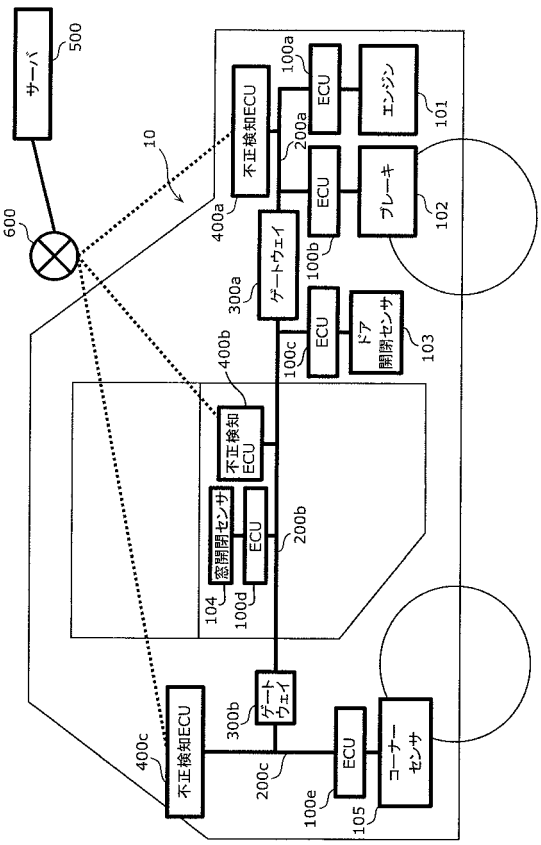
【０２０６】

（１２）上記実施の形態における不正検知ＥＣＵ及び他のＥＣＵは、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置であることとしたが、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。

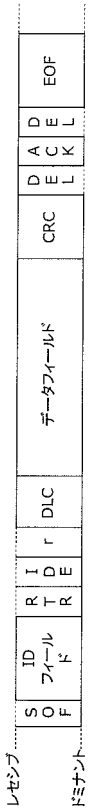
【０２０７】
（１３）上記実施の形態における各装置を構成する構成要素の一部又は全部は、１個のシステムＬＳＩ（Large Scale Integration：大規模集積回路）から構成されているとしても良い。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ等を含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムＬＳＩは、その機能を達成する。また、上記各装置を構成する構成要素の各部は、個別に１チップ化されていても良いし、一部又は全部を含むように１チップ化されても良い。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良い。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ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。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。
【０２０８】
（１４）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良い。前記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。前記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カード又は前記モジュールは、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良い。
【０２０９】
（１５）本発明の一態様としては、例えば図２５、図２６、図２８、図２９、図４２、図４３等に示す不正検知ルール更新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。また、本発明の一態様としては、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。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号を、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良い。また、本発明の一態様としては、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。また、前記プログラム若しく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、又は、前記プログラム若しく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。
【０２１０】
（１６）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発明の範囲に含まれる。
【産業上の利用可能性】
【０２１１】
本発明は、車載ネットワークにおいて、バス上への不正なフレームの送信の検知を行う基準となるルールを更新するために利用可能である。

【符号の説明】
【０２１２】
１０、２０　車載ネットワークシステム
１００ａ～１００ｅ　電子制御ユニット（ＥＣＵ）
１０１　エンジン
１０２　ブレーキ
１０３　ドア開閉センサ
１０４　窓開閉センサ
１０５　コーナーセンサ
１１０、３１０、４１０、８１０　フレーム送受信部
１２０、３２０、４２０、８２０、２４２０　フレーム解釈部
１３０、３３０、８３０　受信ＩＤ判断部
１４０、３４０、８４０　受信ＩＤリスト保持部
１５０、８５０、２４５０　フレーム処理部
１６０、３６０、４６０、８６０、２４６０　フレーム生成部
１７０　データ取得部
２００ａ～２００ｄ　バス
３００ａ、３００ｂ、２３００ａ、２３００ｂ　ゲートウェイ
３５１　転送処理部
３５２　転送ルール保持部
４００ａ～４００ｃ、１４００ａ、２４００ａ～２４００ｃ　不正検知電子制御ユニット（不正検知ＥＣＵ）
４８０　不正検知処理部
４８１、５３０　不正検知ルール保持部
４９０、８９０　外部通信部
４９１、５９１、８９１　暗復号処理部
４９２、５９２、８９２　ＭＡＣ処理部
４９３、５９３、８９３　鍵保持部
４９４、１４９４、２４９４　更新判定部
４９５　車両Ｎｏ．保持部
４９６　バス種別保持部
５００、２５００　サーバ
５１０、２５１０　通信部
５２０　配信データ管理部
５４０　更新結果管理部
５５０、８５５　更新結果表保持部
６００　ネットワーク
８００　ヘッドユニット
８５３　表示制御部
８５４　更新管理部
１４９７　車両状態保持部
１４９８　車両状態判定部

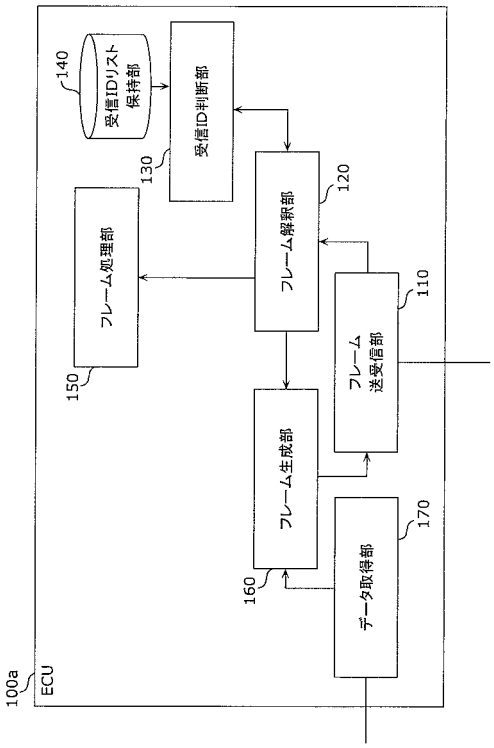
【図１】




【図２】




【図３】




【図４】

| 受信IDリスト |
|---|
| 1 |
| 2 |
| 3 |

【図５】

| 受信IDリスト |
|---|
| 1 |
| 2 |
| 3 |
| 4 |

【図６】

| 受信IDリスト |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |

【図７】

| ID | データ |
|---|---|
| 1 | 0 |
| 1 | 1 |
| 1 | 2 |
| 1 | 3 |
| 1 | 4 |
| … | … |

【図８】

| ID | データ |
|---|---|
| 2 | 100 |
| 2 | 90 |
| 2 | 80 |
| 2 | 70 |
| 2 | 60 |
| … | … |

【図９】

| ID | データ |
|---|---|
| 3 | 1 |
| 3 | 1 |
| 3 | 0 |
| 3 | 0 |
| 3 | 0 |
| … | … |

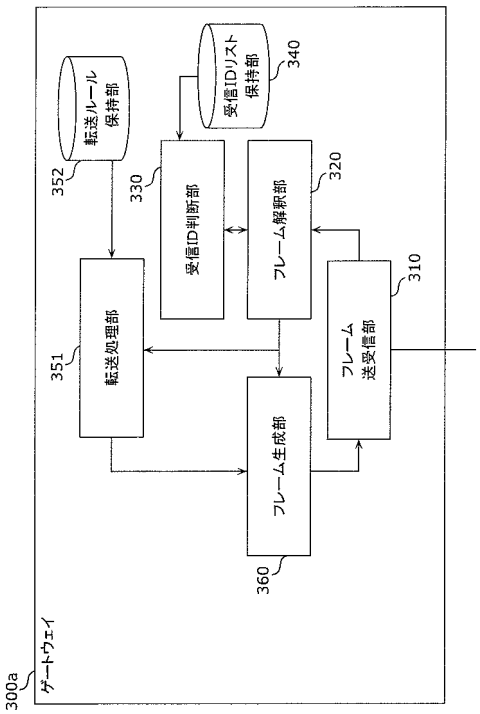
【図１０】

| ID | データ |
|---|---|
| 4 | 0 |
| 4 | 10 |
| 4 | 20 |
| 4 | 30 |
| 4 | 40 |
| … | … |

【図１１】

| ID | データ |
|---|---|
| 5 | 0 |
| 5 | 0 |
| 5 | 1 |
| 5 | 1 |
| 5 | 1 |
| … | … |

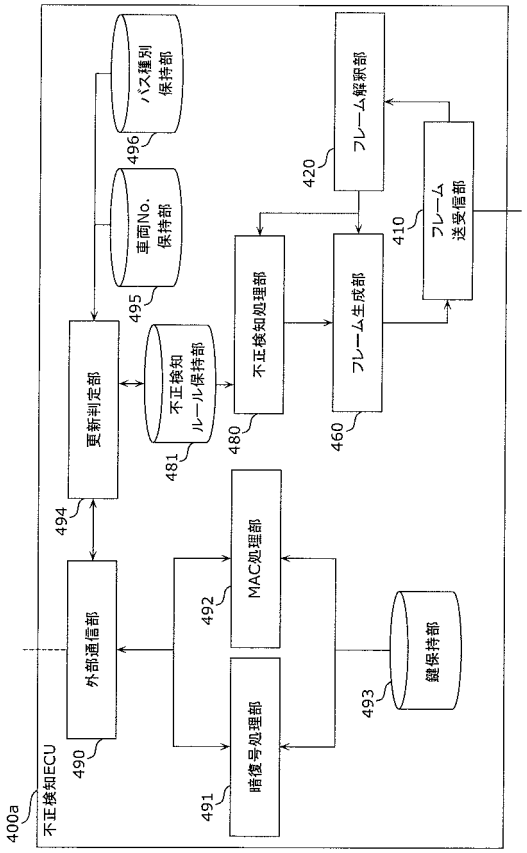
【図１２】



【図１３】

| 転送元 | 転送先 | ID |
|---|---|---|
| 200a | 200b | * |
| 200b | 200a | 3 |
| 200b | 200c | * |
| 200c | 200b | – |

【図１４】




【図１５】

| Ver. | ID |
|---|---|
| 1.0 | 1 |
| | 2 |
| | 3 |

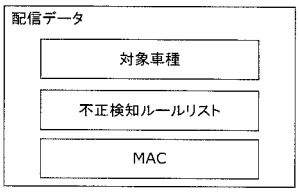
【図１６】

| Ver. | ID |
|---|---|
| 1.0 | 1 |
| | 2 |
| | 3 |
| | 4 |

【図１７】

| Ver. | ID |
|---|---|
| 1.0 | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 5 |

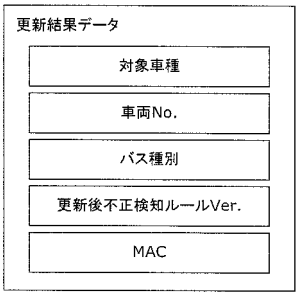
【図１８】




【図１９】

| 対象車種 | 不正検知ルールリスト | | |
|---|---|---|---|
| | バス種別 | 不正検知ルールVer. | 不正検知ルール |
| 車種A | 駆動系 | 2.0 | 1, 2, 3, 4 |
| | ボディ系 | 1.0 | 1, 2, 3, 4 |
| | 安全系 | 1.0 | 1, 2, 3, 4, 5 |

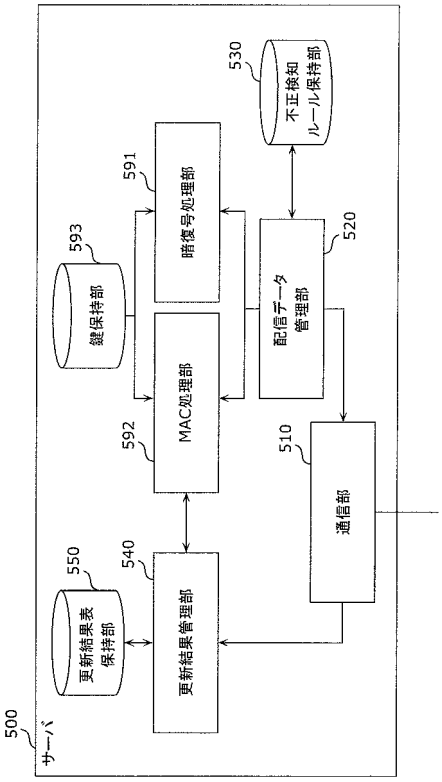
【図２０】



【図２１】

| 対象車種 | 車両No. | バス種別 | 更新後不正検知ルールVer. |
|---|---|---|---|
| 車種A | 00000001 | 駆動系 | 2.0 |

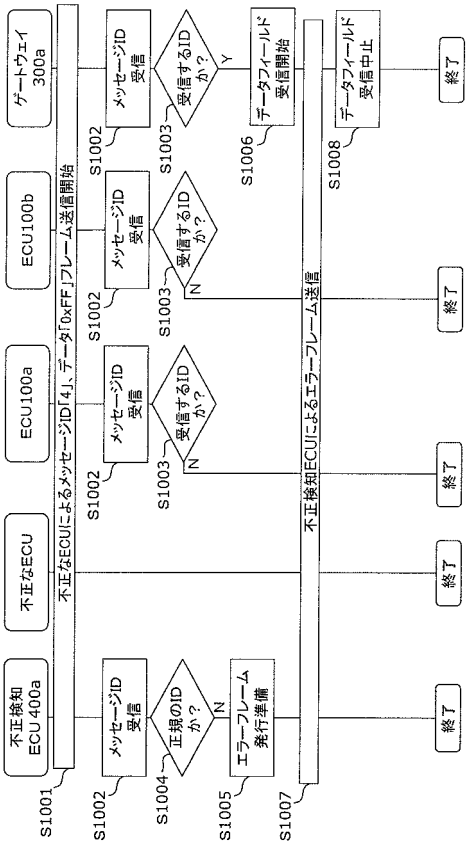
【図２２】



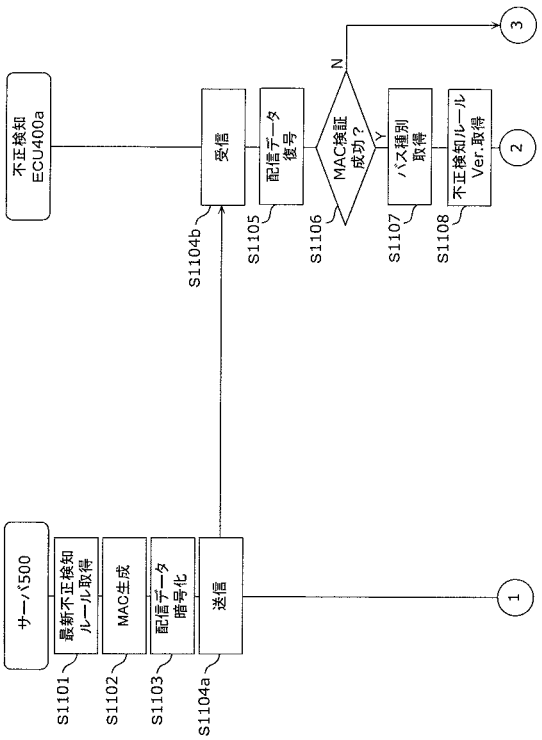

【図２３】

| 対象車種 | 車両No. | バス種別 | 最終更新不正検知ルールVer. | 最終更新日時 |
|---|---|---|---|---|
| A | 00000001 | 駆動系 | 2.0 | 20X1年7月1日13:00 |
| A | 00000001 | ボディ系 | 1.0 | 20X1年7月1日13:00 |
| A | 00000001 | 安全系 | 1.0 | 20X1年7月1日13:00 |

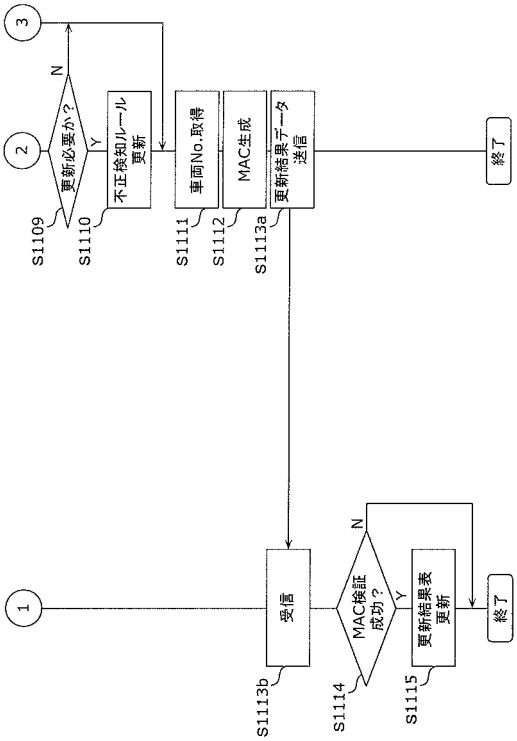
【図２４】



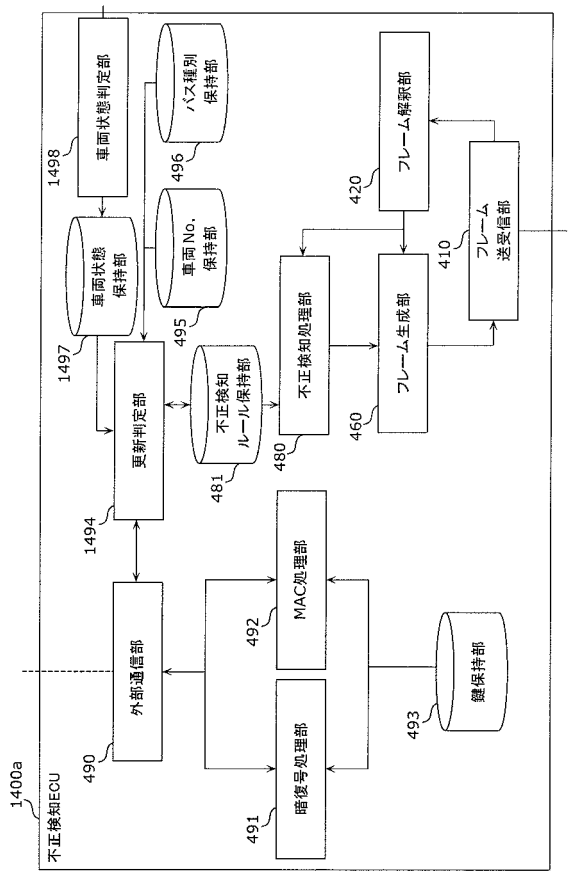
【図２５】



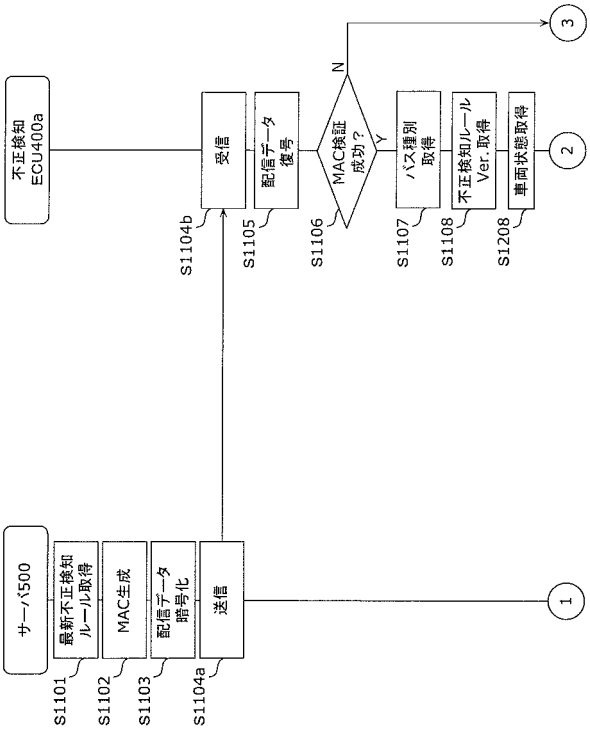

【図２６】



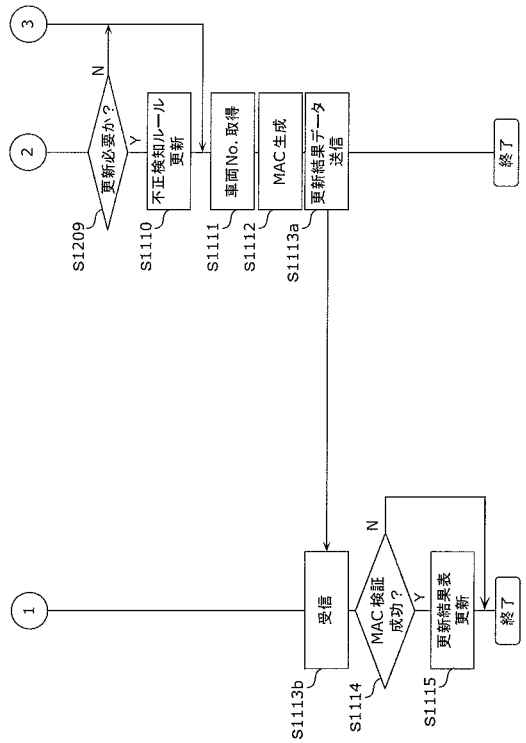

【図２７】



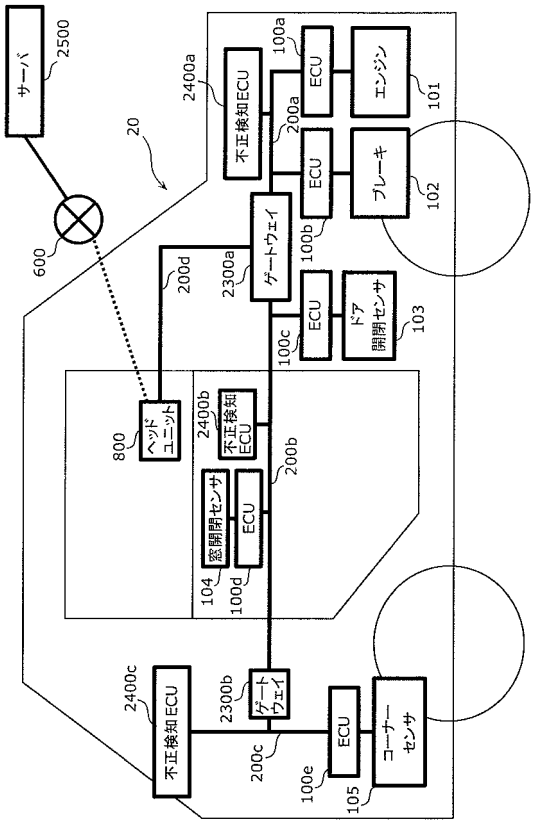

【図２８】



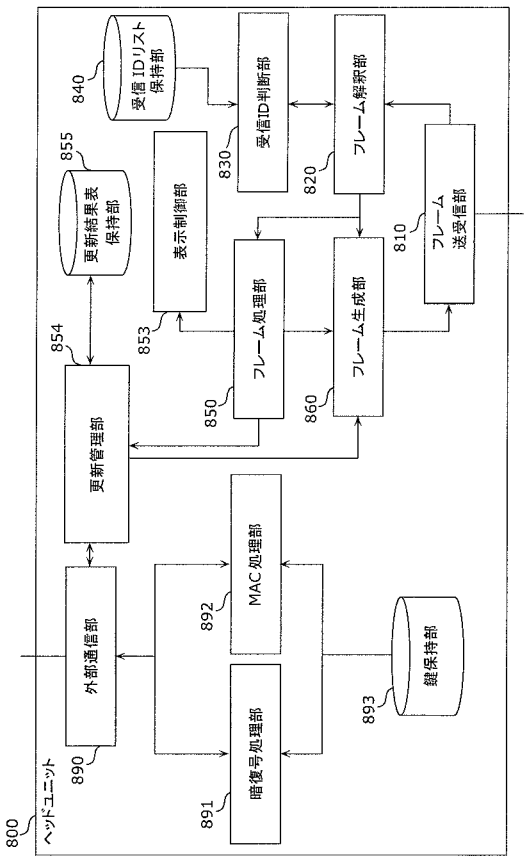
【図２９】




【図３０】




【図３１】




【図３２】

| 発信IDリスト |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 0x0F0 |
| 0x0F1 |
| 0x0F2 |

【図３３】

| ID | 不正検知ルールリスト | | |
|---|---|---|---|
| | 不正検知ルールVer. | ルール数 | 不正検知ルール |
| 0x0E0 | 20 | 04 | 01 02 03 04 |

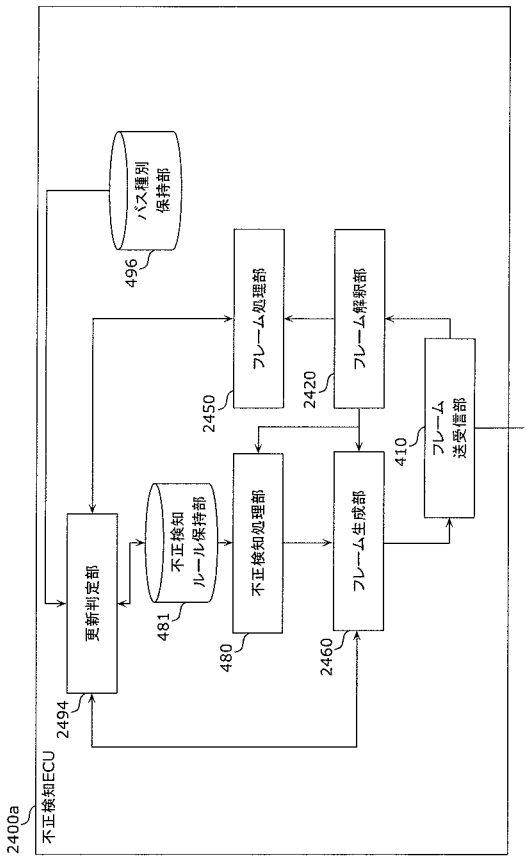
【図３４】

| ID | 更新後不正検知ルールVer. |
|---|---|
| 0x0F0 | 20 |

【図３５】

| 転送元 | 転送先 | ID |
|---|---|---|
| 200a | 200b | * |
| 200a | 200d | * |
| 200b | 200a | 3 |
| 200b | 200d | * |
| 200d | 200a | 0x0E0 |
| 200d | 200b | 0x0E1、0x0E2 |

【図３６】




【図３７】

| Ver. | ID |
|---|---|
| 1.0 | 1 |
| | 2 |
| | 3 |
| | 0x0E0 |

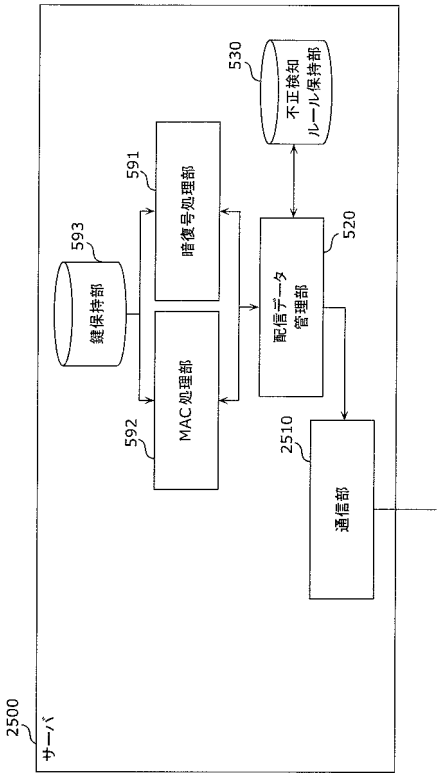
【図３８】

| Ver. | ID |
|---|---|
| 1.0 | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 0x0E1 |
| | 0x0E2 |
| | 0x0F1 |
| | 0x0F2 |

【図３９】

| Ver. | ID |
|---|---|
| 1.0 | 1 |
| | 2 |
| | 3 |
| | 4 |
| | 5 |
| | 0x0E2 |
| | 0x0F2 |

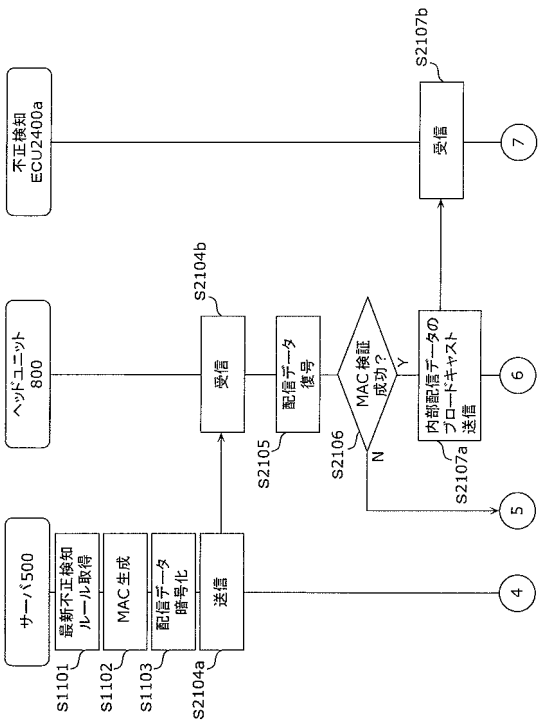
【図４０】



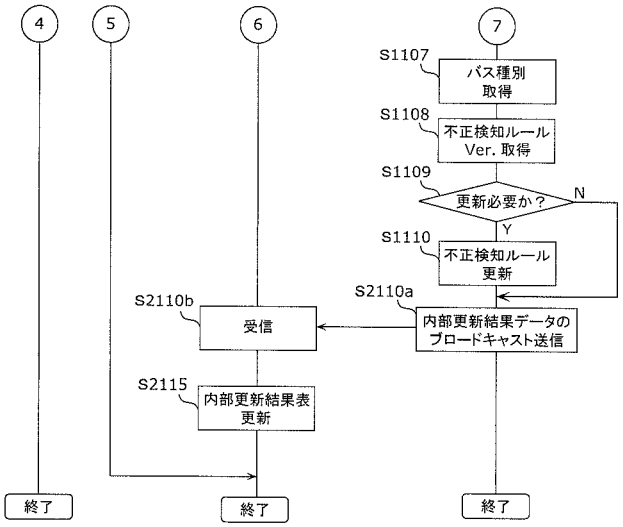

【図４１】

| バス種別 | 最終更新不正検知ルール Ver. |
|---|---|
| 駆動系 | 2.0 |
| ボディ系 | 1.0 |
| 安全系 | 1.0 |

【図４２】



【図４３】




【手続補正書】
【提出日】令和1年8月29日(2019.8.29)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
複数の電子制御ユニットがメッセージの授受を行う通信に用いるネットワークに接続される不正検知電子制御ユニットにおいて用いられる不正検知ルール更新方法であって、
自ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、
更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信し、
前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、
前記車両が走行していると判定した場合に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、
(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、
(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する
不正検知ルール更新方法。
【請求項２】
前記不正検知電子制御ユニットが接続された前記ネットワークの種別を前記種別情報が

示す場合に、前記所定更新条件が満たされたとして前記更新を行う
請求項１記載の不正検知ルール更新方法。
【請求項３】
前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、ネットワークの種別を示す種別情報を含み、
前記外部装置と通信することにより前記配信データの前記受信を行い、当該不正検知電子制御ユニットが接続された前記ネットワークの種別に該当する種別情報に対応する更新用不正検知ルールを前記配信データから抽出して、前記判定に係る前記不正検知ルールを、抽出した当該更新用不正検知ルールへと更新する
請求項１記載の不正検知ルール更新方法。
【請求項４】
前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、ネットワークの種別を示す種別情報を含み、
前記不正検知電子制御ユニットが接続された前記ネットワークの種別に応じた、不正検知ルール更新用のメッセージＩＤのメッセージを当該ネットワークから受信し、前記判定に係る前記不正検知ルールを、当該メッセージに含まれる更新用不正検知ルールへと更新する
請求項１記載の不正検知ルール更新方法。
【請求項５】
前記配信データは、付属情報を含み、
所定更新条件は、前記付属情報に関する条件であり、
前記不正検知ルールの前記更新を、受信した前記配信データにおける前記付属情報が前記所定更新条件を満たす場合には行い、前記付属情報が前記所定更新条件を満たさない場合には行わない
請求項１記載の不正検知ルール更新方法。
【請求項６】
前記所定更新条件を満たすか否かを、前記付属情報と前記不正検知電子制御ユニットが保持する情報とを比較した結果に応じて判別する
請求項５記載の不正検知ルール更新方法。
【請求項７】
前記付属情報は、前記更新用不正検知ルールのバージョンを示し、
前記判定の基礎としている前記不正検知ルールのバージョンよりも新しいバージョンを前記付属情報が示す場合に、前記所定更新条件が満たされたと判別して前記更新を行う
請求項６記載の不正検知ルール更新方法。
【請求項８】
前記付属情報は、前記更新用不正検知ルールの適用対象の車両種別を示し、
前記付属情報が、前記車載ネットワークシステムを搭載する車両に係る車両種別を示す場合に、前記所定更新条件が満たされたとして前記更新を行う
請求項５記載の不正検知ルール更新方法。
【請求項９】
前記不正検知ルール及び前記更新用不正検知ルールは、ルールへの適合性を判定するためのプログラムを含んで構成される
請求項１記載の不正検知ルール更新方法。
【請求項１０】
前記配信データには、暗号処理が施されており、
前記配信データの前記受信に際して前記暗号処理に呼応する処理を施す
請求項１記載の不正検知ルール更新方法。
【請求項１１】
前記複数の電子制御ユニットは、ＣＡＮ（Controller Area Network）プロトコルに従って前記ネットワークを介して通信を行う

請求項１記載の不正検知ルール更新方法。
【請求項１２】
複数の電子制御ユニットが通信に用いるネットワークに接続される不正検知電子制御ユニットであって、
不正検知ルールを保持する不正検知ルール保持部と、
自ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、前記不正検知ルールに基づいて行う不正検知処理部と、
更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信して、
前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、
前記車両が走行していると判定した場合に、更に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、
(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、
(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する更新判定部とを備える
不正検知電子制御ユニット。
【請求項１３】
１以上のネットワークを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記ネットワークに接続された不正検知電子制御ユニットを備える車載ネットワークシステムであって、
前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、
前記電子制御ユニットは、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信して、当該更新用不正検知ルールを前記ネットワークを介して送信し、
前記不正検知電子制御ユニットは、前記ネットワークから前記更新用不正検知ルールを受信し、
前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、
前記車両が走行していると判定した場合に、更に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、
(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、
(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する
車載ネットワークシステム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正の内容】
【００１０】
上記課題を解決するために本発明の一態様に係る不正検知ルール更新方法は、複数の電子制御ユニットがメッセージの授受を行う通信に用いるネットワークに接続される不正検知電子制御ユニットにおいて用いられる不正検知ルール更新方法であって、自ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信し、前記

車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する不正検知ルール更新方法である。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
また、上記課題を解決するために本発明の一態様に係る不正検知電子制御ユニットは、複数の電子制御ユニットが通信に用いるネットワークに接続される不正検知電子制御ユニットであって、不正検知ルールを保持する不正検知ルール保持部と、自ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、前記不正検知ルールに基づいて行う不正検知処理部と、更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信して、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する更新判定部とを備える不正検知電子制御ユニットである。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
また、上記課題を解決するために本発明の一態様に係る車載ネットワークシステムは、１以上のネットワークを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記ネットワークに接続された不正検知電子制御ユニットを備える車載ネットワークシステムであって、前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、前記電子制御ユニットは、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信して、当該更新用不正検知ルールを前記ネットワークを介して送信し、前記不正検知電子制御ユニットは、前記ネットワークから前記更新用不正検知ルールを受信し、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する
車載ネットワークシステムである。

【手続補正５】
【補正対象書類名】明細書

【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
本発明の一態様に係る不正検知ルール更新方法は、複数の電子制御ユニットがメッセージの授受を行う通信に用いるネットワークに接続される不正検知電子制御ユニットにおいて用いられる不正検知ルール更新方法であって、自ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信し、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する不正検知ルール更新方法である。これにより、不正なフレームが送信されたと判定する基準となるルールの更新が可能となる。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
また、前記配信データは、前記更新用不正検知ルールの適用対象のバスの種別を示すバス種別情報を含み、前記不正検知電子制御ユニットは、前記不正検知電子制御ユニットが接続された前記ネットワークの種別を前記種別情報が示す場合に、前記所定更新条件が満たされたとして前記更新を行うこととしても良い。これにより、バスの種別毎に必要な不正検知ルールが異なることに対応し得る。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
また、前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、ネットワークの種別を示す種別情報を含み、前記外部装置と通信することにより前記配信データの前記受信を行い、当該不正検知電子制御ユニットが接続された前記ネットワークの種別に該当する種別情報に対応する更新用不正検知ルールを前記配信データから抽出して、前記判定に係る前記不正検知ルールを、抽出した当該更新用不正検知ルールへと更新することとしても良い。これにより、不正検知ルールを配信する外部装置側では一括した配信が可能となり処理負担が軽減される。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
また、前記配信データは、複数の更新用不正検知ルールを含み、当該複数の更新用不正検知ルールそれぞれに対応した、ネットワークの種別を示す種別情報を含み、前記不正検知電子制御ユニットが接続された前記ネットワークの種別に応じた、不正検知ルール更新

用のメッセージＩＤのメッセージを当該ネットワークから受信し、前記判定に係る前記不正検知ルールを、当該メッセージに含まれる更新用不正検知ルールへと更新することとしても良い。これにより、１つのＥＣＵだけが外部との通信を行うため個々の不正検知ＥＣＵの処理負荷が削減され得る。また、この構成により、通信内容についてセキュリティを確保する暗号処理等の実装面では、外部との通信を行うＥＣＵでは例えば処理負荷が大きい暗号方式を用いるとしても、外部とは通信しない各不正検知ＥＣＵでは処理負荷が小さい暗号方式を選択し得るようになる。また、個々の不正検知ＥＣＵが通信する場合と比べて、サーバと車載ネットワークシステムとの間での通信回数を低減させ得る。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
また、前記所定更新条件を満たすか否かを、前記付属情報と前記不正検知電子制御ユニットが保持する情報とを比較した結果に応じて判別することとしても良い。これにより、更新用不正検知ルールのバージョンが既存の不正検知ルールのバージョンよりも新しいか否か等といった比較判断が可能になる。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】
また、前記付属情報は、前記更新用不正検知ルールのバージョンを示し、前記判定の基礎としている前記不正検知ルールのバージョンよりも新しいバージョンを前記付属情報が示す場合に、前記所定更新条件が満たされたと判別して前記更新を行うとしても良い。これにより、不正検知ルールの内容変更についてバージョンによる管理が可能となる。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正の内容】
【００２２】
また、前記付属情報は、前記更新用不正検知ルールのバージョンを示し、前記判定の基礎としている前記不正検知ルールのバージョンよりも新しいバージョンを前記付属情報が示す場合に、前記所定更新条件が満たされたと判別して前記更新を行うこととしても良い。これにより、車種毎に独立して不正検知ルールを規定可能となる。

【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正の内容】
【００２７】
また、前記複数の電子制御ユニットは、ＣＡＮ（Controller Area Network）プロトコルに従って前記ネットワークを介して通信を行うこととしても良い。これにより、ＣＡＮに従った車載ネットワークシステムにおいて不正検知ルールの更新が可能となる。

【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２８

【補正方法】変更
【補正の内容】
【００２８】
また、本発明の一態様に係る不正検知電子制御ユニットは、複数の電子制御ユニットが通信に用いるネットワークに接続される不正検知電子制御ユニットであって、不正検知ルールを保持する不正検知ルール保持部と、自ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、前記不正検知ルールに基づいて行う不正検知処理部と、更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信して、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する更新判定部とを備える。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】変更
【補正の内容】
【００２９】
また、本発明の一態様に係る車載ネットワークシステムは、１以上のネットワークを介した通信によりメッセージの授受を行う複数の電子制御ユニット及び前記ネットワークに接続された不正検知電子制御ユニットを備える車載ネットワークシステムであって、前記不正検知電子制御ユニットは、当該不正検知電子制御ユニットが接続された前記ネットワーク上で送信されるメッセージについてのルールへの適合性の判定を、不正検知ルールに基づいて行い、前記電子制御ユニットは、前記車載ネットワークシステムの外部の外部装置から更新用不正検知ルールと、前記更新用不正検知ルールの適用対象のネットワークの種別を示す種別情報とを含む配信データを受信して、当該更新用不正検知ルールを前記ネットワークを介して送信し、前記不正検知電子制御ユニットは、前記ネットワークから前記更新用不正検知ルールを受信し、前記車載ネットワークシステムを搭載する車両が走行しているか否かを判定し、前記車両が走行していると判定した場合に、更に、前記種別情報が走行に関連する駆動系のネットワークを示しているか否かを判定し、(i)前記種別情報が走行に関連する駆動系のネットワークを示している場合には、前記更新用不正検知ルールによる更新処理を行わず、(ii)前記種別情報が走行に関連する駆動系のネットワークを示していない場合には、前記不正検知ルールを前記更新用不正検知ルールへと更新する車載ネットワークシステムである。これにより、不正検知ルールの更新が可能となるため、車載ネットワークシステムの構成の変更等に対応可能となり、また、車載ネットワークにおいて不正なＥＣＵがルールを回避してメッセージを送信するリスクを低減可能となる。

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　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　CA07　DA01　EA06
5K033 AA05　BA06　CA07　DA01　DA13　DB20　EA06