(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2016-134170
(P2016-134170A)
(43)公開日　平成28年7月25日(2016.7.25)

(51)Int.Cl.		F I			テーマコード（参考）
G08G 1/16	(2006.01)	G08G	1/16	C	3D241
H04L 12/28	(2006.01)	H04L	12/28	200M	5H181
G08G 1/09	(2006.01)	H04L	12/28	100A	5K033
B60W 50/04	(2006.01)	G08G	1/09	H	
B60W 30/16	(2012.01)	B60W	50/04		

審査請求 未請求　請求項の数 15　ＯＬ　（全 37 頁）　最終頁に続く

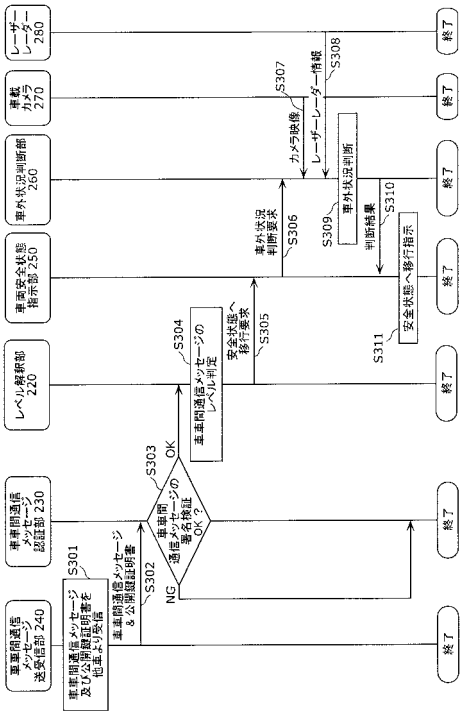
(21)出願番号　特願2015-217211 (P2015-217211)
(22)出願日　平成27年11月5日 (2015.11.5)
(31)優先権主張番号　62/105,244
(32)優先日　平成27年1月20日 (2015.1.20)
(33)優先権主張国　米国 (US)

(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】不正対処方法及び電子制御ユニット

(57)【要約】
【課題】車両が不正に制御される可能性が高い場合にその影響を抑制するために適切に対処する不正対処方法を提供する。
【解決手段】一の車両に搭載された１つ又は複数の電子制御ユニットにおいて用いられる不正対処方法では、他の車両に搭載された車載ネットワークで不正フレームが検知された際に当該他の車両に搭載された装置から送信される不正検知通知としての車車間通信メッセージを受信し、受信した内容に応じて（例えばレベル判定のステップＳ３０４）、例えば安全状態へ移行するために予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理（例えばステップＳ３０５～Ｓ３１１）を実行する。
【選択図】図１１



【特許請求の範囲】
【請求項１】
一の車両に搭載された１つ又は複数の電子制御ユニットにおいて用いられる不正対処方法であって、
他の車両に搭載された車載ネットワークで不正フレームが検知された際に当該他の車両に搭載された装置から送信される不正検知通知を受信し、
受信した前記不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する
不正対処方法。
【請求項２】
前記不正検知通知は、複数レベルのうち１つのレベルを示すレベル情報を含み、
受信した前記不正検知通知に含まれる前記レベル情報が示すレベルに応じて、不正対応処理の前記選択を行う
請求項１記載の不正対処方法。
【請求項３】
不正対応処理の前記選択は、前記複数レベルそれぞれについて不正対応処理を対応付けた対応情報を参照することにより行われ、受信した前記不正検知通知に含まれる前記レベル情報が示すレベルに前記対応情報で対応する不正対応処理の選択である
請求項２記載の不正対処方法。
【請求項４】
前記対応情報が前記複数レベルのうちいずれか１つ以上と対応付けている各不正対応処理は、前記一の車両の走行を停止させる制御、当該車両を徐行させる制御、当該車両と前方の車両との車間距離を一定範囲に保って走行させる制御、及び、当該車両の運転者への報知を行う制御のうちの少なくとも１つを含む
請求項３記載の不正対処方法。
【請求項５】
更に、受信した前記不正検知通知の内容に基づいて所定条件が満たされているか否かを判定し、当該所定条件が満たされている場合には前記一の車両の外部に当該不正検知通知を送信し、当該所定条件が満たされていない場合には当該不正検知通知を送信しない
請求項２～４のいずれか一項に記載の不正対処方法。
【請求項６】
前記不正検知通知は、転送の条件を示す条件情報を含み、
受信した前記不正検知通知に含まれる前記条件情報が示す転送の条件が満たされている場合には前記所定条件が満たされているとして前記判定を行い、当該条件情報が示す転送の条件が満たされていない場合には前記所定条件が満たされていないとして前記判定を行う
請求項５記載の不正対処方法。
【請求項７】
前記不正検知通知は、前記不正フレームを検知して当該不正検知通知を送信した前記装置を搭載する前記他の車両についての測定された位置を示す位置情報を含み、
前記所定条件は、前記一の車両についての測定した位置と、受信した前記不正検知通知に含まれる前記位置情報が示す位置との距離が一定範囲内であるという条件である
請求項５記載の不正対処方法。
【請求項８】
前記不正検知通知は回数を示す回数情報を含み、
前記所定条件は、前記不正フレームを検知して前記不正検知通知を送信した前記装置からの当該不正検知通知を受信するまでに転送がなされた回数が所定回数より少ないという条件であり、
受信した前記不正検知通知に含まれる前記回数情報に基づいて、前記所定条件が満たされているか否かに係る前記判定を行い、

受信した前記不正検知通知の前記送信に際して、当該不正検知通知に含まれる前記回数情報を更新した上で当該送信を行う
請求項５記載の不正対処方法。
【請求項９】
前記不正検知通知は、時刻を示す時刻情報を含み、
前記所定条件は、受信した前記不正検知通知に含まれる前記時刻情報が示す時刻からの経過時間が所定時間より短いという条件である
請求項５記載の不正対処方法。
【請求項１０】
受信した前記不正検知通知の前記送信に際して、当該不正検知通知に含まれる前記レベル情報を所定レベル変更規則に基づいて更新した上で当該送信を行う
請求項５記載の不正対処方法。
【請求項１１】
第１及び第２の車両間で通信を行うことで不正な事態に対処する不正対処方法であって、
前記第１の車両に搭載された車載ネットワークで不正フレームが検知された際に当該第１の車両に搭載された装置が不正検知通知を送信し、
前記第２の車両に搭載された１つ又は複数の電子制御ユニットが、前記不正検知通知を受信し、受信した当該不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する
不正対処方法。
【請求項１２】
前記第１の車両に搭載された前記装置は、前記不正フレームが検知された際に、フレームＩＤを区分して予め定められた複数レベルのうち、当該不正フレームのフレームＩＤに基づいて選定された１つのレベルを示すレベル情報を前記不正検知通知に含ませて前記送信を行い、
前記第２の車両に搭載された１つ又は複数の前記電子制御ユニットは、受信した前記不正検知通知に含まれる前記レベル情報が示すレベルに応じて、不正対応処理の前記選択を行う
請求項１１記載の不正対処方法。
【請求項１３】
一の車両に搭載された車載ネットワークに接続された電子制御ユニットにおいて用いられる不正対処方法であって、
前記一の車両に搭載された車載ネットワークで不正フレームを検知した場合に他の車両へと不正検知通知を送信する
不正対処方法。
【請求項１４】
自ユニットが搭載された車両とは別の車両に搭載された車載ネットワークで不正フレームが検知された際に当該別の車両に搭載された装置から送信される不正検知通知を受信する受信部と、
前記受信部により受信された前記不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処部とを備える
電子制御ユニット。
【請求項１５】
車載ネットワークに接続された電子制御ユニットであって、
前記車載ネットワークにおいて送信された不正フレームを検知する不正検知部と、
前記不正検知部により不正フレームが検知された場合に自ユニットを搭載する車両とは別の車両へと不正検知通知を送信する送信部とを備える
電子制御ユニット。

【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した場合に対処する技術に関する。
【背景技術】
【０００２】
近年、自動車の中のシステムには、電子制御ユニット（ＥＣＵ：Electronic Control Unit）と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐネットワークは車載ネットワークと呼ばれる。車載ネットワークには、多数の規格が存在する。その中でも最も主流な車載ネットワークの一つに、ＩＳＯ１１８９８－１で規定されているＣＡＮ（Controller Area Network）という規格が存在する。
【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】
ところで、不正なＥＣＵが、不正なメッセージをバス上に送信し、車載ネットワークを搭載する車両を不正に制御するリスクがあり、１台の車両が不正に制御されると、周囲の車両を巻き込んで衝突等の事故が発生し得る。
【０００６】
また、近年、コネクテッドカーと呼ばれるように、自動車がネットワークを介して様々な機器等と情報の交換を行うようになっている。例えば、車両同士で情報を交換する車車間通信を利用すると、未然に事故を防ぎ、より安全な交通システムを実現することが可能となる。車車間通信システムを利用した技術として、自車の近傍に位置する移動物体が危険要素であるか否かを識別し、他車に通知するシステムが知られている（特許文献１参照）。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２００７－３１０４５７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
特許文献１の技術では、車両の近傍の移動物体が危険要素であるか否かの識別をするものの、車両内部における異常について後方車両に通知しない。しかし、車両内部において車両が不正に制御されたような場合には、衝突等の事故が生じ得る。

【０００９】
そこで、本発明は、車両が不正に制御される可能性が高い場合にその影響を抑制するために適切に対処する不正対処方法を提供する。また、本発明は、車両が不正に制御される可能性が高い場合にその影響を抑制するために適切に対処する電子制御ユニット（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対処方法は、一の車両に搭載された１つ又は複数の電子制御ユニットにおいて用いられる不正対処方法であって、他の車両に搭載された車載ネットワークで不正フレームが検知された際に当該他の車両に搭載された装置から送信される不正検知通知を受信し、受信した前記不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処方法である。
【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対処方法は、第１及び第２の車両間で通信を行うことで不正な事態に対処する不正対処方法であって、前記第１の車両に搭載された車載ネットワークで不正フレームが検知された際に当該第１の車両に搭載された装置が不正検知通知を送信し、前記第２の車両に搭載された１つ又は複数の電子制御ユニットが、前記不正検知通知を受信し、受信した当該不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処方法である。
【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不正対処方法は、一の車両に搭載された車載ネットワークに接続された電子制御ユニットにおいて用いられる不正対処方法であって、前記一の車両に搭載された車載ネットワークで不正フレームを検知した場合に他の車両へと不正検知通知を送信する不正対処方法である。
【００１３】
また、上記課題を解決するために本発明の一態様に係る電子制御ユニットは、自ユニットが搭載された車両とは別の車両に搭載された車載ネットワークで不正フレームが検知された際に当該別の車両に搭載された装置から送信される不正検知通知を受信する受信部と、前記受信部により受信された前記不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処部とを備える電子制御ユニットである。
【００１４】
また、上記課題を解決するために本発明の一態様に係る電子制御ユニットは、車載ネットワークに接続された電子制御ユニットであって、前記車載ネットワークにおいて送信された不正フレームを検知する不正検知部と、前記不正検知部により不正フレームが検知された場合に自ユニットを搭載する車両とは別の車両へと不正検知通知を送信する送信部とを備える電子制御ユニットである。
【発明の効果】
【００１５】
本発明によれば、一の車両の車載ネットワークにおいて不正なフレームが検知された場合に、他の車両へとその旨を通知するため、一の車両が不正に制御された場合であっても、一の車両の周辺の他の車両への影響を抑えることが可能となる。
【図面の簡単な説明】
【００１６】
【図１】実施の形態１に係る車車間通信システムの全体構成を示す図である。
【図２】実施の形態１に係る車両の構成を示す図である。
【図３】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４】実施の形態１に係る不正検知ＥＣＵの構成図である。

【図５】実施の形態１に係る不正検知ＥＣＵが保持するホワイトリストの一例を示す図である。
【図６】実施の形態１に係る不正なフレームの検知に係る動作例を示すシーケンス図である。
【図７】実施の形態１に係るレベル情報を示す図である。
【図８】実施の形態１に係る車車間通信メッセージの構成の一例を示す図である。
【図９】実施の形態１に係る不正検知時の車両の各部の動作を示すシーケンス図である。
【図１０】実施の形態１に係る対応情報の一例を示す図である。
【図１１】実施の形態１に係る車車間通信メッセージを受信した車両の各部の動作を示すシーケンス図である。
【図１２】実施の形態２に係る複数の車両が連続的に後続車に車車間通信メッセージを通知する例を示す図である。
【図１３】実施の形態２に係る車車間通信メッセージの構成の一例を示す図である。
【図１４】実施の形態２に係る車両が車車間通信メッセージを受信して転送する場合の各部の動作を示すシーケンス図である（図１５に続く）。
【図１５】実施の形態２に係る車両が車車間通信メッセージを受信して転送する場合の各部の動作を示すシーケンス図である（図１４から続く）。
【図１６】実施の形態３に係る車車間通信メッセージの構成の一例を示す図である。
【図１７】実施の形態３に係るレベル変更条件の一例を示す図である。
【図１８】実施の形態３に係る複数の車両が連続的に後続車に車車間通信メッセージを通知する例を示す図である。
【図１９】実施の形態３に係る車両が車車間通信メッセージを受信して転送する場合の各部の動作を示すシーケンス図である（図２０に続く）。
【図２０】実施の形態３に係る車両が車車間通信メッセージを受信して転送する場合の各部の動作を示すシーケンス図である（図１９から続く）。
【図２１】実施の形態４に係る路車間通信システムの全体構成を示す図である。
【図２２】実施の形態５に係る複数の車両が連続的に後続車に車車間通信メッセージを通知する例を示す図である。
【図２３】実施の形態５に係る車車間通信メッセージの構成の一例を示す図である。
【発明を実施するための形態】
【００１７】
本発明の一態様に係る不正対処方法は、一の車両に搭載された１つ又は複数の電子制御ユニットにおいて用いられる不正対処方法であって、他の車両に搭載された車載ネットワークで不正フレームが検知された際に当該他の車両に搭載された装置から送信される不正検知通知を受信し、受信した前記不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処方法である。これにより、一の車両では、他の車両の車載ネットワークにおいて不正なフレームが検知された場合に、その旨の通知を受信でき、不正対応処理により例えば他の車両が不正に制御された場合の影響を低減し得る。
【００１８】
また、前記不正検知通知は、複数レベルのうち１つのレベルを示すレベル情報を含み、受信した前記不正検知通知に含まれる前記レベル情報が示すレベルに応じて、不正対応処理の前記選択を行うこととしても良い。これにより、不正対応処理に対応して他の車両においてレベル情報を設定することで、他の車両で不正に制御される可能性が生じた場合に適切な対処を一の車両に行わせることが可能になる。
【００１９】
また、不正対応処理の前記選択は、前記複数レベルそれぞれについて不正対応処理を対応付けた対応情報を参照することにより行われ、受信した前記不正検知通知に含まれる前記レベル情報が示すレベルに前記対応情報で対応する不正対応処理の選択であることとしても良い。これにより、対応情報としてレベルと不正対応処理の内容とを適切に設定して

おけば、他の車両で不正に制御される可能性が生じた場合に適切な対処を一の車両に行わせることが可能になる。

【００２０】

また、前記対応情報が前記複数レベルのうちいずれか１つ以上と対応付けている各不正対応処理は、前記一の車両の走行を停止させる制御、当該車両を徐行させる制御、当該車両と前方の車両との車間距離を一定範囲に保って走行させる制御、及び、当該車両の運転者への報知を行う制御のうちの少なくとも１つを含むこととしても良い。これにより、他の車両で不正に制御される可能性が生じた場合に一の車両を安全状態に移行させることが可能になり、例えば複数車両を巻き込んだ事故の発生を抑制し得る。

【００２１】

また、更に、受信した前記不正検知通知の内容に基づいて所定条件が満たされているか否かを判定し、当該所定条件が満たされている場合には前記一の車両の外部に当該不正検知通知を送信し、当該所定条件が満たされていない場合には当該不正検知通知を送信しないこととしても良い。これにより、一定条件下で不正検知通知の転送が可能となり、例えば個々の車両における車車間通信で比較的小さい送信出力を用いても、ある程度広い範囲（その範囲を走行中の車両）に不正検知通知を伝達することが可能となり得る。不正検知通知を伝達された車両は例えば安全状態に移行する等の対処を行うことができる。また、条件付きで転送がなされるため、不必要に広範囲にまで転送が行われないように条件を定めておくような利用が可能となる。

【００２２】

また、前記不正検知通知は、転送の条件を示す条件情報を含み、受信した前記不正検知通知に含まれる前記条件情報が示す転送の条件が満たされている場合には前記所定条件が満たされているとして前記判定を行い、当該条件情報が示す転送の条件が満たされていない場合には前記所定条件が満たされていないとして前記判定を行うこととしても良い。これにより、例えば不正検知通知を送信する車両が、その不正検知通知についての転送条件を定めることが可能となる。

【００２３】

また、前記不正検知通知は、前記不正フレームを検知して当該不正検知通知を送信した前記装置を搭載する前記他の車両についての測定された位置を示す位置情報を含み、前記所定条件は、前記一の車両についての測定した位置と、受信した前記不正検知通知に含まれる前記位置情報が示す位置との距離が一定範囲内であるという条件であることとしても良い。また、前記不正検知通知は回数を示す回数情報を含み、前記所定条件は、前記不正フレームを検知して前記不正検知通知を送信した前記装置からの当該不正検知通知を受信するまでに転送がなされた回数が所定回数より少ないという条件であり、受信した前記不正検知通知に含まれる前記回数情報に基づいて、前記所定条件が満たされているか否かに係る前記判定を行い、受信した前記不正検知通知の前記送信に際して、当該不正検知通知に含まれる前記回数情報を更新した上で当該送信を行うこととしても良い。また、前記不正検知通知は、時刻を示す時刻情報を含み、前記所定条件は、受信した前記不正検知通知に含まれる前記時刻情報が示す時刻からの経過時間が所定時間より短いという条件であることとしても良い。これらにより、不正が検知された車両から、ある程度の範囲内に限定して不正検知通知が伝達されるようになり、十分離れた車両が不正対応処理を行うことによる弊害（例えば不正対応処理として停止、徐行等を行うことによる交通渋滞の発生等）が防止され得る。即ち、全ての車両が安全状態にするための不正対応処理を行うのではなく、不正が検知された車両から一定の範囲にある車両のみを例えば安全状態に移行することができ、交通システムへの影響（交通渋滞の発生等）を抑えることが可能となる。

【００２４】

また、受信した前記不正検知通知の前記送信に際して、当該不正検知通知に含まれる前記レベル情報を所定レベル変更規則に基づいて更新した上で当該送信を行うこととしても良い。これにより、不正が検知された車両の周辺の複数の各車両において行われる不正対応処理を相違させ得る。このため、例えば、不正が検知された車両からの距離が離れるに

つれてレベルを低くすること等が可能となり、これに対応してレベルが低くなる程、不正対応処理の程度を、例えば停止から徐行、徐行から一定車間距離を保って走行等と、交通システムへの悪影響が小さくなるようにすることができる。

【００２５】

また、本発明の一態様に係る不正対処方法は、第１及び第２の車両間で通信を行うことで不正な事態に対処する不正対処方法であって、前記第１の車両に搭載された車載ネットワークで不正フレームが検知された際に当該第１の車両に搭載された装置が不正検知通知を送信し、前記第２の車両に搭載された１つ又は複数の電子制御ユニットが、前記不正検知通知を受信し、受信した当該不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処方法である。これにより、第１の車両で車載ネットワークにおいて不正フレームが検知された場合に、第２の車両で適切な不正対応処理により対処することが可能となり得る。

【００２６】

また、前記第１の車両に搭載された前記装置は、前記不正フレームが検知された際に、フレームＩＤを区分して予め定められた複数レベルのうち、当該不正フレームのフレームＩＤに基づいて選定された１つのレベルを示すレベル情報を前記不正検知通知に含ませて前記送信を行い、前記第２の車両に搭載された１つ又は複数の前記電子制御ユニットは、受信した前記不正検知通知に含まれる前記レベル情報が示すレベルに応じて、不正対応処理の前記選択を行うこととしても良い。これにより、レベル情報が、機能を分類した機能種別毎に設定され得る。このため、車載ネットワークにおいてフレームＩＤを機能種別毎に区分して、不正フレームにより生じる影響（区分毎に異なる影響）の程度に対応した不正対応処理が実行され得る。機能種別は、例えば、駆動系機能、シャーシ系機能、ボディ系機能、安全快適機能、ＩＴＳ（Intelligent Transport Systems）系機能、テレマティクス系機能、インフォテインメント系機能等である。

【００２７】

また、本発明の一態様に係る不正対処方法は、一の車両に搭載された車載ネットワークに接続された電子制御ユニットにおいて用いられる不正対処方法であって、前記一の車両に搭載された車載ネットワークで不正フレームを検知した場合に他の車両へと不正検知通知を送信する不正対処方法である。これにより、一の車両において不正に制御される可能性がある程度高まったこと（つまり不正フレームが検知されたこと）を、他の車両において知ることが可能となる。

【００２８】

また、本発明の一態様に係る電子制御ユニット（ＥＣＵ）は、自ユニットが搭載された車両とは別の車両に搭載された車載ネットワークで不正フレームが検知された際に当該別の車両に搭載された装置から送信される不正検知通知を受信する受信部と、前記受信部により受信された前記不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、当該選択した不正対応処理を実行する不正対処部とを備える電子制御ユニットである。このＥＣＵを搭載した車両において、別の車両で不正フレームが検知されたことに対処することが可能になる。

【００２９】

また、本発明の一態様に係る電子制御ユニット（ＥＣＵ）は、車載ネットワークに接続された電子制御ユニットであって、前記車載ネットワークにおいて送信された不正フレームを検知する不正検知部と、前記不正検知部により不正フレームが検知された場合に自ユニットを搭載する車両とは別の車両へと不正検知通知を送信する送信部とを備える電子制御ユニットである。これにより、不正フレームを検知した場合に他の車両にその旨を伝達することが可能となり、このため他の車両において対処が可能となり得る。

【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対処方法を用いる車車間通信システムについて、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、車両に搭載された複数のＥＣＵがバスを介して通信する車載ネットワークシステムでバスに送出された不正なフレーム（不正なＣＡＮメッセージ）を検知した場合にその車両から車車間通信で後方の車両に通知する車車間通信システムについて、図面を用いて説明する。その後方の車両においては、車車間通信で受信した内容に応じてその車両を安全状態にするための不正対応処理を実施する。

【００３３】

［１．１　車車間通信システムの全体構成］

図１は、車車間通信システムの全体構成を示す図である。車車間通信システムは、車両１０（車両Ａ）と車両２０（車両Ｂ）と認証局５０とを含んで構成される。

【００３４】

ここでは、車車間通信システムは、公開鍵暗号基盤（ＰＫＩ：Public Key Infrastructure）を利用するものとする。各車両は、車車間通信で使用する秘密鍵と公開鍵証明書とを保有する。公開鍵証明書は、秘密鍵と対となる公開鍵の所有者を証明するものとして、信頼できる第三者機関である認証局（ＣＡ：Certification Authority）５０によって与えられた電子署名を含む。図１では、認証局５０を１つ示したが、認証局は階層関係を持って複数存在しても良い。ＣＡ証明書１３００は、認証局５０の公開鍵を含む。

【００３５】

車両１０（車両Ａ）は、車両Ａ秘密鍵１３０１と、車両Ａ公開鍵証明書１３０２と、ＣＡ証明書１３００と、証明書失効リスト（ＣＲＬ：Certificate Revocation List）１３０３とを保持している。

【００３６】

車両２０（車両Ｂ）は、車両Ｂ秘密鍵２３０１と、車両Ｂ公開鍵証明書Ｂ２３０２と、ＣＡ証明書１３００と、ＣＲＬ１３０３とを保持している。

【００３７】

車両Ａ公開鍵証明書１３０２と車両Ｂ公開鍵証明書Ｂ２３０２とのそれぞれは、認証局５０の秘密鍵（不図示）で電子署名が付与され、認証局５０から配布される。各車両への公開鍵証明書、秘密鍵等の記録（例えば車両に備えられるＥＣＵへの書き込み）は、車両の製造段階、出荷段階、車両に搭載されるＥＣＵの製造段階等のいずれにおいて行われても良い。

【００３８】

ＣＲＬ１３０３は、認証局５０から発行され、無効にすべき公開鍵証明書の識別情報がリスト化されたものである。

【００３９】

車両Ａから車両Ｂに対して車車間通信により、送信される車車間通信メッセージ３００は、車両Ａ秘密鍵１３０１で署名されている。

【００４０】

例えば、走行している車両１０（車両Ａ）の後方を車両２０（車両Ｂ）が走行している。ここでは、説明の便宜上、車両１０は、後方に指向性を有する送信アンテナ（不図示）

を用いて無線通信を行うことを前提として説明するが、その他の通信方法で車両１０から少なくとも通常の車間距離を空けた後方の車両が受信可能なように車車間通信を行っても良い。なお、車車間通信に利用する周波数帯は、国によって異なり、一例としては、日本では７００ＭＨｚ、米国、欧州では５．９ＧＨｚ帯が利用される。しかし、本実施の形態で示す車車間通信は、技術的には必ずしもこれらの周波数帯での無線通信に限られず実施可能である。

【００４１】

車両１０（車両Ａ）が、車両２０（車両Ｂ）に対して車車間メッセージを送信する場合には、車車間通信メッセージ３００と車両Ａ公開鍵証明書１３０２とを送信する。車両２０は、ＣＡ証明書１３００の公開鍵を利用して、受信した車両Ａ公開鍵証明書１３０２を署名検証し、続いて車両Ａ公開鍵証明書に含まれる車両Ａの公開鍵を利用して、車車間通信メッセージ３００の署名検証を行う。なお、車両１０（車両Ａ）は、不正なＣＡＮメッセージを検知した場合に不正検知通知としての車車間通信メッセージ３００を送信する。不正検知通知は、不正検知がなされた旨の伝達を車両間で行うための通知であり、不正検知通知としての車車間通信メッセージ３００は、不正検知に関する情報を含む車車間通信メッセージである。

【００４２】

［１．２　車両の構成］

図２は、車両１０（車両Ａ）及び車両２０（車両Ｂ）の構成を示す図である。

【００４３】

車両１０は、ＣＡＮバス１００と、ＥＣＵ１０１、１０２、１０３と、不正検知ＥＣＵ１１０と、レベル解釈部１２０と、車車間通信メッセージ認証部１３０と、車車間通信メッセージ送受信部１４０と、車両安全状態指示部１５０と、車外状況判断部１６０と、車載カメラ１７０と、レーザーレーダー１８０と、位置情報取得部１９０とを含んで構成される。

【００４４】

ＣＡＮバス１００は、車載ネットワークにおける通信路であり、ＣＡＮプロトコルに従って複数のＥＣＵがフレーム（ＣＡＮメッセージ）の授受を行うために用いるバス（信号線）である。図２では便宜上１つのバスを示しているが、複数のバスが含まれても良く、例えばゲートウェイの機能を有するＥＣＵが複数のバス間でのＣＡＮメッセージの転送を行い得る。

【００４５】

ＥＣＵ１０１～１０３は、ＣＡＮバス１００と接続されている。また、ＥＣＵ１０１～１０３は、それぞれがセンサ、アクチュエータ等の各種機器（不図示）と接続されていても良く、例えば、接続されている機器の状態を取得してその状態を表すデータフレームをＣＡＮバス１００で送信し、或いは、個別に保持する受信ＩＤリスト（受信対象のＣＡＮメッセージＩＤを列挙したリスト）に従って特定のＣＡＮメッセージＩＤが付されたデータフレームを受信してその内容に従って接続されている機器を制御し得る。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。図２では、便宜上、ＥＣＵ１０１、１０２、１０３の３つだけを図示しているが、車両１０内にはいくつものＥＣＵが含まれ、ＣＡＮバス１００を介して相互に通信する。これらのＥＣＵは、複数に機能種別（後述）のいずれかに分類される。

【００４６】

不正検知ＥＣＵ１１０は、一種のＥＣＵであり、ＣＡＮバス１００に流れるフレーム（ＣＡＮメッセージ）に不正がないかを監視し、不正を検知した場合に、不正検知内容を示

す不正情報をレベル解釈部１２０に通知する。ＣＡＮバス１００には例えば不正なＥＣＵが接続されて不正なＣＡＮメッセージを送信する可能性があり、不正検知ＥＣＵ１１０は、所定のホワイトリスト（後述）で示されるルールに基づいて、バス上に現れたＣＡＮメッセージが、ルールに適合しない不正なＣＡＮメッセージか否かを判定する検査により、不正を検知する。

【００４７】

レベル解釈部１２０は、不正検知内容を示す不正情報を参照し、不正検知通知として車車間通信メッセージを送信する場合に車車間通信メッセージ内に含ませるためのセキュリティレベルを示すレベル情報を定めて車車間通信メッセージ認証部１３０に通知する。セキュリティレベルは、不正として検知されたＣＡＮメッセージの機能種別毎に区別して定められる（詳細は図７を用いて後述する）。また、レベル解釈部１２０は、所定の対応情報（安全状態リスト）に基づいて、他車（他車両）から受信された車車間通信メッセージに含まれるレベル情報が示すセキュリティレベルに応じた安全状態に移行するための指示（不正対応処理の実行指示）を、車両安全状態指示部１５０に通知する。不正対応処理は、車両安全状態指示部１５０が行う安全状態に移行するための制御である。不正対応処理には、車両の走行を停止させる制御のための不正対応処理、車両を徐行させる制御のための不正対応処理、車両と前方の車両との車間距離を一定範囲に保って走行させる制御のための不正対応処理、車両の運転者への報知の制御のための不正対応処理等がある。

【００４８】

車車間通信メッセージ認証部１３０は、車車間通信メッセージ３００の送信に際して、レベル解釈部１２０から取得したレベル情報、位置情報取得部１９０から取得した車両の位置情報等を含ませて、車車間通信メッセージ３００を形成して、車両の秘密鍵を利用して署名を生成して車車間通信メッセージ３００に含ませる。また、車車間通信メッセージ認証部１３０は、他車両から受信した車車間通信メッセージについての署名検証を行って、車車間通信メッセージに含まれるレベル情報をレベル解釈部１２０に通知する。

【００４９】

車車間通信メッセージ送受信部１４０は、他車両に対して車車間通信メッセージを送信し、また、他車両から車車間通信メッセージを受信する。

【００５０】

車両安全状態指示部１５０は、他車両から受信した車車間通信メッセージ内のレベル情報が示すセキュリティレベルに応じたレベル解釈部１２０による指示（不正対応処理の実行指示）を受けて、不正対応処理を実行することで、車両内の各部（各ＥＣＵ等）に、車両の走行を停止させるための指示、車両を徐行させるための指示、車両と前方の車両との車間距離を一定範囲に保って走行させる指示、及び、車両の運転者への報知を行う指示を与える。この指示は、車外状況判断部１６０から通知される情報を用いてなされ、また、例えば予め制御のために規定したＣＡＮメッセージをＣＡＮバス１００で送信すること等により行われる。

【００５１】

車外状況判断部１６０は、車載カメラ１７０、レーザーレーダー１８０等の車両に搭載された各種センサから取得した情報を解析し、自車両の近傍の状況を判断しながら、車両を適切に安全状態に移行できるようにするための情報を、車両安全状態指示部１５０に通知する。例えば、車載カメラで白線を検知し、レーザーレーダーで周囲の物体を検知することで、路肩に寄せて車両の走行を停止したり、徐行したり、前方の車両と一定の間隔を空けて走行したりすること等を適切に実現するための情報を通知する。

【００５２】

位置情報取得部１９０は、例えばＧＰＳ（Global Positioning System）受信機で実現され、車両の緯度、経度、高度等の位置情報を取得して車車間通信メッセージ認証部１３０に通知する。

【００５３】

なお、電子回路で構成された１つ又は複数の装置（ＥＣＵ）により、レベル解釈部１２

０、車車間通信メッセージ認証部１３０、車車間通信メッセージ送受信部１４０、車両安全状態指示部１５０及び車外状況判断部１６０が実現される。図２では、車両安全状態指示部１５０及び車外状況判断部１６０をＣＡＮバス１００に接続しているが、車両安全状態指示部１５０及び車外状況判断部１６０を実現する１つ又は複数の装置をＣＡＮバス１００に直接接続させずに、その装置が、ＣＡＮバス１００に接続されたＥＣＵを介して、ＣＡＮバス１００に対して指示を与え、ＣＡＮバス１００からの情報を受信するようにしてもよい。

【００５４】

車両２０も、車両１０と同様な構成を備え、ＣＡＮバス２００と、ＥＣＵ２０１、２０２、２０３と、不正検知ＥＣＵ２１０と、レベル解釈部２２０と、車車間通信メッセージ認証部２３０と、車車間通信メッセージ送受信部２４０と、車両安全状態指示部２５０と、車外状況判断部２６０と、車載カメラ２７０と、レーザーレーダー２８０と、位置情報取得部２９０とを含んで構成される。なお、図２において同様の構成要素同士には、符号が相違するが同一名称を付している。

【００５５】

［１．３　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（ＣＡＮメッセージ）の１つであるデータフレームについて説明する。

【００５６】

図３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。

【００５７】

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。

【００５８】

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（ＣＡＮ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。

【００５９】

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。

【００６０】

ＩＤＥと「ｒ」とは、両方ドミナント１ｂｉｔで構成される。

【００６１】

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。

【００６２】

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、車両の車載ネットワークシステム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。

【００６３】

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。

【００６４】
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。
【００６５】
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。
【００６６】
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。
【００６７】
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。
【００６８】
［１．４　不正検知ＥＣＵ１１０の構成］
図４は、不正検知ＥＣＵ１１０の構成図である。不正検知ＥＣＵ１１０は、フレーム送受信部１１６と、フレーム解釈部１１５と、不正フレーム検知部１１３と、ホワイトリスト保持部１１２と、フレーム生成部１１４と、不正情報通知部１１１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ＥＣＵ１１０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１１６は、ＣＡＮバス１００に対して、ＣＡＮのプロトコルに従ったフレーム（ＣＡＮメッセージ）を送受信する。即ち、フレーム送受信部１１６は、ＣＡＮバス１００からフレームを１ｂｉｔずつ受信し、フレーム解釈部１１５に転送する。また、フレーム生成部１１４より通知を受けたフレームの内容をＣＡＮバス１００に送信する。
【００７０】
フレーム解釈部１１５は、フレーム送受信部１１６よりフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。ＩＤフィールドと判断した値は、不正フレーム検知部１１３へ転送する。また、フレーム解釈部１１５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１１４へ通知する。また、フレーム解釈部１１５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】
フレーム生成部１１４は、フレーム解釈部１１５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１１６へ通知して送信させる。また、フレーム生成部１１４は、不正フレーム検知部１１３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１１６へ通知して送信させる。
【００７２】
ホワイトリスト保持部１１２は、ＣＡＮバス１００上で送信される正規のフレームに含まれるＣＡＮメッセージＩＤを規定したホワイトリスト（図５参照）を保持する。ホワイトリストには、ＣＡＮメッセージＩＤそれぞれについてＣＡＮメッセージが不正か否かの判定に用いられる条件も含まれている。
【００７３】

不正フレーム検知部１１３は、ホワイトリスト保持部１１２が保持しているホワイトリストにより特定されるルールに基づいて、ＣＡＮバス１００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。不正フレーム検知部１１３は、具体的には、フレーム解釈部１１５から通知されるＩＤフィールドの値（ＣＡＮメッセージＩＤ）を受け取り、そのＣＡＮメッセージＩＤが、ホワイトリストに載っていない場合或いはホワイトリストでそのＣＡＮメッセージＩＤに対応して定められた条件が満たされない場合には、不正と判定してエラーフレームを送信するように、フレーム生成部１１４へ通知する。なお、この場合に、ＣＡＮバス１００上において、不正と判定されたＣＡＮメッセージのビット値は、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。不正フレーム検知部１１３は、不正と判定したＣＡＮメッセージ（不正フレーム）の内容である不正検知内容を不正情報通知部１１１に通知する。

【００７４】

不正情報通知部１１１は、不正検知内容を示す不正情報をレベル解釈部１２０に通知する。

【００７５】

［１．５　ホワイトリスト］

図５は、不正検知ＥＣＵ１１０内のホワイトリスト保持部１１２が保持するホワイトリストの一例を示す図である。ホワイトリスト１１２０は、ＩＤ（ＣＡＮメッセージＩＤ）１１２１それぞれについて、データ長１１２２、データ範囲１１２３、及び、周期１１２４を対応付けたデータである。

【００７６】

ＣＡＮメッセージＩＤ１１２１は、車両の仕様として車載ネットワークにおけるＣＡＮバス１００に送出されても良いと定められている正規のＣＡＮメッセージＩＤを示す。

【００７７】

データ長１１２２は、ＤＬＣ（図３参照）であり、対応するＣＡＮメッセージＩＤのＣＡＮメッセージについて仕様上定められている正規のデータ長を示す。

【００７８】

データ範囲１１２３は、対応するＣＡＮメッセージＩＤのＣＡＮメッセージについて仕様上定められている正規のデータフィールドの内容として期待されるデータ範囲を示す。

【００７９】

周期１１２４は、対応するＣＡＮメッセージＩＤのＣＡＮメッセージが周期的に送信される周期性メッセージである場合に仕様上定められている正規の周期を示す。

【００８０】

図５の例では、速度に関するＩＤ「０ｘ１００」のＣＡＮメッセージについて、データ長が８バイトで、データの範囲が０から１８０までで、１０ｍｓ周期であるという条件を満たす場合には、正規のＣＡＮメッセージであることを示している。

【００８１】

また、エンジンの回転数に関するＩＤ「０ｘ２００」のＣＡＮメッセージについて、データ長が８バイトで、データの範囲が０から１００００までで、１０ｍｓ周期であるという条件を満たす場合には、正規のＣＡＮメッセージであることを示している。

【００８２】

また、走行距離に関するＩＤ「０ｘ３００」のＣＡＮメッセージについて、データ長が８バイトであり、データの範囲が０から９９９９９９９までで、２０ｍｓ周期であるという条件を満たす場合には、正規のＣＡＮメッセージであることを示している。

【００８３】

また、ドアの開閉状態に関するＩＤ「０ｘ４００」のＣＡＮメッセージについて、データ長が１バイトで、データの範囲が０又は１で、１０００ｍｓ周期であるという条件を満たす場合には、正規のＣＡＮメッセージであることを示している。

【００８４】

不正検知ＥＣＵ１１０は、ホワイトリスト１１２０の各ＣＡＮメッセージＩＤに対応す

る条件に適合しないＣＡＮメッセージを、不正なＣＡＮメッセージと判定する。
【００８５】
［１．６　不正検知シーケンス］
図６は、不正検知ＥＣＵ１１０により不正フレーム（つまり不正なＣＡＮメッセージ）を検知する動作例を示すシーケンス図である。各シーケンスは、各装置における各処理手順（ステップ）を示す。以下、図６に即して、ＣＡＮバス１００に不正なＥＣＵが接続されてＣＡＮメッセージＩＤが「０ｘ１００」、データが「２５５（０ｘＦＦ）」となるフレーム（ＣＡＮメッセージ）を送信する場合における、ＣＡＮバス１００に接続された不正検知ＥＣＵ１１０、ＥＣＵ１０１～１０３の動作について説明する。
【００８６】
まず、不正なＥＣＵは、メッセージＩＤが「０ｘ１００」、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Ｓ１０１）。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ＣＡＮバス１００上に送出される。
【００８７】
不正なＥＣＵがＩＤフィールド（ＣＡＮメッセージＩＤ）までをＣＡＮバス１００に送出し終えたときにおいて、不正検知ＥＣＵ１１０、ＥＣＵ１０１～１０３はそれぞれＣＡＮメッセージＩＤを受信する（ステップＳ１０２）。
【００８８】
ＥＣＵ１０１～１０３はそれぞれ、受信すべきＣＡＮメッセージＩＤであるか否かを、保持している受信ＩＤリストを用いてチェックし、不正検知ＥＣＵ１１０はホワイトリスト（図５参照）を用いて不正なＣＡＮメッセージか否かを判定すべくＣＡＮメッセージＩＤをチェックする（ステップＳ１０３）。図６の例では、ＥＣＵ１０１及びＥＣＵ１０２は、「０ｘ０１００」は、受信すべきＣＡＮメッセージＩＤでないため、受信を終了する。ＥＣＵ１０３は、「０ｘ０１００」が受信すべきＣＡＮメッセージＩＤであるので処理を継続する。また、不正検知ＥＣＵ１１０は、ホワイトリストにＣＡＮメッセージＩＤ「０ｘ１００」があるため受信を継続する。
【００８９】
不正検知ＥＣＵ１１０は、ＣＡＮバス１００に現れたＣＡＮメッセージについて、ホワイトリストが示す正規の周期でメッセージが送信されているか否かを判別する（ステップＳ１０４）。正規の周期でない場合は、ステップＳ１０８に移行してエラーフレームの送信を行う。
【００９０】
次に不正検知ＥＣＵ１１０は、ＣＡＮバス１００に現れたＣＡＮメッセージについて、ホワイトリストが示す正規のデータサイズ（ＤＬＣ）の条件を満たすか否かを判別する（ステップＳ１０５）。正規のデータサイズでない場合は、ステップＳ１０８に移行してエラーフレームの送信を行う。
【００９１】
次に不正検知ＥＣＵ１１０は、ＣＡＮバス１００に現れたＣＡＮメッセージについて、ホワイトリストが示す正規のデータ範囲の条件を満たすか否かを判別する（ステップＳ１０６）。正規のデータ範囲の条件を満たす場合は、不正検知ＥＣＵ１１０は処理を終了する。図６の例では、受信したデータが「２５５（０ｘＦＦ）」であり、ホワイトリストのデータ範囲外であるのでエラーフレームのブロードキャスト（つまりＣＡＮバス１００での送信）に向けて、フレームを生成する。
【００９２】
ＥＣＵ１０３は、不正検知ＥＣＵがホワイトリストを用いてＣＡＮメッセージが不正か否かを判定している間に、データフレームの受信を続ける（ステップＳ１０７）。
【００９３】
不正検知ＥＣＵ１１０は、ステップＳ１０３～Ｓ１０６での判別によりＣＡＮメッセージが不正であると判定した場合には、エラーフレームをブロードキャスト（送信）する（

ステップＳ１０８）。このエラーフレームを受信することで、ＥＣＵ１０３は、データフレームの受信を中止する（ステップＳ１０９）。

【００９４】

不正検知ＥＣＵ１１０は、不正と判定しているＣＡＮメッセージについての内容を示す不正情報をレベル解釈部１２０へ通知する（ステップＳ１１０）。

【００９５】

［１．７　レベル情報］

図７は、レベル解釈部１２０が保持するレベル情報１２００の一例を示す。

【００９６】

レベル情報１２００は、機能種別１２０１と、ＩＤ（ＣＡＮメッセージＩＤ）１２０２と、レベル１２０３とを対応付けた情報である。

【００９７】

機能種別１２０１は、ＣＡＮメッセージを送信するＥＣＵの機能を分類して定めた機能種別を示す。ＥＣＵの機能の分類例として、例えば駆動系機能、シャーシ系機能、ボディ系機能、安全快適機能、ＩＴＳ系機能、テレマティクス系機能、インフォテインメント系機能等がある。駆動系機能は、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「走る」（走行）に関連する機能である。シャーシ系機能は、ブレーキ、ステアリング等の「曲がる」、「止まる」等といった車両の挙動等の制御に関連する機能である。ボディ系機能は、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機能である。安全快適機能は、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機能である。ＩＴＳ系機能は、ＥＴＣ（Electronic Toll Collection System）等の高度道路交通システムに対応した機能である。テレマティクス系機能は、移動体通信を用いたサービスに対応する機能である。インフォテインメント系機能は、カーナビゲーション、オーディオ等に関連したエンターテインメント機能である。

【００９８】

ＣＡＮメッセージＩＤ１２０２は、対応する機能種別１２０１に属するＥＣＵが送信することと定められているＣＡＮメッセージのＩＤ（ＣＡＮメッセージＩＤ）を示す。

【００９９】

レベル１２０３は、対応する機能種別１２０１が示す機能種別に属するＥＣＵの機能の性質に応じて、そのＥＣＵが不正に制御された場合の車両の安全性等に鑑みて予め定められたレベルであるセキュリティレベルを示し、例えば、１から４までの４段階のうちいずれかの値を表す。ここでは、セキュリティレベルが高い程、安全性への影響が大きいものとしている。図７の例では、駆動系機能及びシャーシ系機能は、車両の「走る」、「曲がる」、「止まる」といった基本機能に関するため、これらの機能を担うＥＣＵが不正に制御される場合は、他の車両との事故にもつながり易いと考えられることから、セキュリティレベルを４と高く設定している。逆に、インフォテインメント系機能を担うＥＣＵが不正に制御される場合は、車両の事故への直接的な影響が小さいと考えられることから、セキュリティレベルを１と低く設定している。

【０１００】

［１．８　車車間通信メッセージフォーマット］

車両間で不正検知がなされた旨の伝達を行うための不正検知通知として車車間通信メッセージ３００が用いられる。

【０１０１】

図８は、車車間通信メッセージ３００の構成の一例を示す図である。車車間通信メッセージ３００のフォーマットは、共通アプリヘッダ部と、共通アプリデータ部と、自由アプリヘッダ部と、自由アプリデータ部とから構成される。図８では、車両において不正検知ＥＣＵ１１０により不正が検知された場合において、不正検知がなされた旨を伝達するという用途のために、自由アプリデータ部が用いられ、その他の用途で通信する場合には自由アプリデータ部をその用途毎に予め定めた別のフォーマットとすることを可能にする例

となっている。
【０１０２】
共通アプリヘッダ部は、共通アプリヘッダ情報３０１で構成され、共通アプリヘッダ情報３０１は、共通アプリデータ部のサイズ情報を含む。
【０１０３】
共通アプリデータ部は、時刻情報３０２と、位置情報３０３と、車両状態情報３０４と、車両属性情報３０５とを含む。
【０１０４】
時刻情報３０２は、年、月、日、時、分、秒といった時刻情報を示す。
【０１０５】
位置情報３０３は、ＧＰＳ受信機等により取得した緯度、経度、高度といった車両の位置を示す情報である。
【０１０６】
車両状態情報３０４は、車速、車両方位角、前後加速度、シフトポジション、ステアリング角度等の情報である。
【０１０７】
車両属性情報３０５は、大型、普通、二輪車等の車両サイズや、自家用車、緊急車両、道路維持作業用等の用途種別や、車幅と車長と車高といった車両サイズ等の情報を含む。
【０１０８】
自由アプリヘッダ部は、自由アプリヘッダ情報３０６で構成され、自由アプリヘッダ情報３０６は、自由アプリデータ部のサイズやオフセット等の情報を含む。
【０１０９】
自由アプリデータ部は、不正検知に関する情報を示し、レベル情報３０７と、不正車両位置情報３０８と、署名データ３０９とを含んで構成される。
【０１１０】
レベル情報３０７は、図７で示した、不正検知ＥＣＵ１１０が検知した不正なＣＡＮメッセージ（不正検知内容）に対応したレベル（セキュリティレベル）を示す。
【０１１１】
不正車両位置情報３０８は、不正検知ＥＣＵ１１０により不正を検知した車両（つまり不正を検知した不正検知ＥＣＵを搭載した車両）について測定された、不正検知の際の位置を示す位置情報である。
【０１１２】
署名データ３０９は、車車間通信メッセージ３００に対する電子署名である。
【０１１３】
［１．９　不正検知シーケンス］
図９は、車両１０（車両Ａ）で不正を検知した場合において車両２０（車両Ｂ）への車車間通信メッセージ３００を送信するまでの車両１０の各部の動作例を示すシーケンス図である。
【０１１４】
車両１０（車両Ａ）の不正検知ＥＣＵ１１０は、不正なＣＡＮメッセージを検知した場合に、不正検知内容である不正なＣＡＮメッセージのフレームＩＤ（ＣＡＮメッセージＩＤ）を含む不正情報をレベル解釈部１２０へ通知する（ステップＳ２０１）。
【０１１５】
不正情報の通知を受けた、車両１０のレベル解釈部１２０は、保持しているレベル情報１２００に基づいて、不正情報が示すＣＡＮメッセージＩＤに応じたレベル（セキュリティレベル）を特定してそのレベルを示すレベル情報を定める（ステップＳ２０２）。つまり、レベル情報は、ＣＡＮメッセージＩＤを区分して予め定められた複数レベルのうち、その不正フレーム（不正なＣＡＮメッセージ）のＣＡＮメッセージＩＤに基づいて選定された１つのレベルを示す。
【０１１６】

レベル解釈部１２０はその定めたレベル情報を、車両１０の車車間通信メッセージ認証部１３０に通知する（ステップＳ２０３）。

【０１１７】

レベル情報の通知を受けた、車両１０の車車間通信メッセージ認証部１３０は、位置情報取得部１９０より車両１０の現在の位置情報を取得して、その位置情報と、通知を受けたレベル情報とを設定して車車間通信メッセージ３００を形成する。

【０１１８】

続いて、車両１０の車車間通信メッセージ認証部１３０は、車両Ａ秘密鍵１３０１を用いて車車間通信メッセージ３００に電子署名を付加する（ステップＳ２０５）。その車車間通信メッセージ認証部１３０は、電子署名を付加した車車間通信メッセージ３００を、車両１０の車車間通信メッセージ送受信部１４０へ通知する（ステップＳ２０６）。

【０１１９】

車車間通信メッセージ３００の通知を受けた、車両１０の車車間通信メッセージ送受信部１４０は、車車間通信メッセージ３００と車両Ａ公開鍵証明書１３０２とを、車車間通信により車両２０（車両Ｂ）に送信する。なお、車両１０（車両Ａ）から車両２０（車両Ｂ）への車車間通信メッセージ３００の送信は、特に宛先の車両１０を特定するものではない。これにより、車車間通信メッセージ３００は、車両Ａの後方に伝搬され得る通信方法により、不特定の車両に対してブロードキャストされる。

【０１２０】

［１．１０　対応情報（安全状態リスト）］

図１０は、レベル解釈部１２０が参照する対応情報（安全状態リスト）を示す図である。対応情報（安全状態リスト）は、車車間通信メッセージ３００を受信した車両が、車車間通信メッセージ３００内のレベル情報が示すレベル（セキュリティレベル）に応じて、安全状態に移行する制御を行うための不正対応処理を実行する際に、予め定められた複数の不正対応処理のうち、どの安全状態に移行するための不正対応処理を実行すべきかを対応付けた情報である。

【０１２１】

対応情報（安全状態リスト）２４００は、複数のレベル２４０１の値（セキュリティレベル）それぞれについて、レベル２４０１と、不正対応処理２４０２とを対応付けて構成される。

【０１２２】

レベル２４０１は、図７に示したレベル情報におけるレベル１２０３と同様のセキュリティレベルを示す。

【０１２３】

不正対応処理２４０２は、セキュリティレベル毎に対応して定められた、安全状態に移行する制御を行うための不正対応処理を特定するための情報である。図１０の対応情報の例では、セキュリティレベルが「１」の場合は、車両の運転者への報知の制御のための不正対応処理が対応付けられ、セキュリティレベルが「２」の場合は、車両と前方の車両との車間距離を一定範囲に保って走行させる制御のための不正対応処理が対応付けられ、セキュリティレベルが「３」の場合は、車両を徐行させる制御のための不正対応処理が対応付けられ、セキュリティレベルが「４」の場合は、車両の走行を停止させる制御のための不正対応処理が対応付けられている。車両の運転者への報知の制御は、例えば、車両が備える、カーナビゲーション等に用いられるディスプレイ画面に、運転者の注意を喚起するようなメッセージを表示する制御、或いは、車両内のインストルメントパネル（インパネ）等のＬＥＤ（Light-Emitting Diode）を点灯させて運転者に通知する制御等である。この対応情報２４００での対応付けは、例えば、車両の事故への直接的な影響が小さいと考えられる不正が検知された場合においては交通渋滞を引き起こさないように、交通システムへ悪影響を抑制するように考慮してなされることが有用である。

【０１２４】

［１．１１　不正検知通知に対応した安全状態への移行シーケンス］

図１１は、車両１０（車両Ａ）から車車間通信メッセージを受信した車両２０（車両Ｂ）における安全状態への移行までの各部の動作を示すシーケンス図である。

【０１２５】

車両２０（車両Ｂ）の車車間通信メッセージ送受信部２４０は、車両１０（車両Ａ）から不正検知通知としての車車間通信メッセージ３００と車両Ａ公開鍵証明書１３０２とを受信する（ステップＳ３０１）。

【０１２６】

続いて車両２０の車車間通信メッセージ送受信部２４０は、車車間通信メッセージ認証部２３０へ車車間通信メッセージ３００と車両Ａ公開鍵証明書１３０２とを通知する（ステップＳ３０２）。

【０１２７】

車両２０の車車間通信メッセージ認証部２３０は、ＣＡ証明書１３００の公開鍵を用いて、受信した車両Ａ公開鍵証明書１３０２の署名検証を行い、続いて車両Ａ公開鍵証明書１３０２を用いて、受信した車車間通信メッセージ３００の署名検証を行う（ステップＳ３０３）。署名検証に失敗すると、処理を終了する。署名検証に成功するとレベル解釈部２２０に車車間通信メッセージ３００のレベル情報を通知する。

【０１２８】

車両２０のレベル解釈部２２０は、図１０で示した対応情報（安全状態リスト）を参照して、車車間通信メッセージ３００のレベル情報が示すレベル（セキュリティレベル）に応じて、どの安全状態に移行するための不正対応処理を実行すべきかを特定（判定）して（ステップＳ３０４）、その不正対応処理の実行指示（安全状態への移行要求）を車両安全状態指示部２５０に通知する（ステップＳ３０５）。このステップＳ３０５～Ｓ３１１で不正対応処理が行われることになる。

【０１２９】

車両２０の車両安全状態指示部２５０は、安全状態に移行するための不正対応処理を実行し、必要に応じて車外状況判断部２６０に対して車外状況の判断を要求する（ステップＳ３０６）。

【０１３０】

車外状況判断部２６０は、車載カメラ２７０やレーザーレーダー２８０等の各種センサから情報を取得し（ステップＳ３０７、Ｓ３０８）、取得した情報を解析して車両２０の近傍の状況を判断して（ステップＳ３０９）、その判断結果としての、車両を適切に安全状態に移行できるようにするための情報を、車両安全状態指示部２５０に通知する（ステップＳ３１０）。

【０１３１】

車両２０の車両安全状態指示部２５０は、必要に応じて車外状況判断部２６０からの情報を利用し、不正対応処理の実行を継続することで、車両２０を安全状態に移行するよう制御する（ステップＳ３１１）。これにより、車両１０（車両Ａ）が送信した不正検知通知としての車車間通信メッセージ３００が示すセキュリティレベルに応じて、車両２０（車両Ｂ）において適切な安全状態への移行が実現される。

【０１３２】

［１．１２　実施の形態１の効果］

上述したように実施の形態１に係る車車間通信システムが用いる不正対処方法は、例えば車両Ａ（第１の車両）及び車両Ｂ（第２の車両）の車両間で通信を行うことで不正な事態に対処する不正対処方法である。ここで、車両Ａ（第１の車両）に搭載された車載ネットワークで不正フレームが検知された際にその車両Ａに搭載された装置（例えばＥＣＵ等）が不正検知通知を送信し、車両Ｂ（第２の車両）に搭載された１つ又は複数のＥＣＵが、不正検知通知を受信し、受信したその不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、その選択した不正対応処理を実行する。不正フレームが検知された状況は、車両が不正に制御される可能性が高いため、他車両に通知することで、不正制御の影響を抑制することが可能となる。より具体的には、

車両Ａに搭載された装置は、不正フレームが検知された際に、フレームＩＤを区分して予め定められた複数レベルのうち、その不正フレームのフレームＩＤに基づいて選定された１つのレベルを示すレベル情報を不正検知通知に含ませて送信を行う。そして、車両Ｂに搭載された１つ又は複数のＥＣＵは、受信した不正検知通知に含まれるレベル情報が示すレベルに応じて、不正対応処理の選択を行って、選択した不正対応処理の実行により安全状態へと移行する。

【０１３３】

このような車車間通信システムが用いる不正対処方法によれば、前方の車両（車両Ａ）の内部の車載ネットワークにおいて不正なＣＡＮメッセージによりその車両Ａが不正制御されるような状況であっても、車両Ａが不正検知通知を後方の車両に通知する。そして不正検知通知を受信した後方の車両（車両Ｂ）は、不正検知通知で示されるレベル（セキュリティレベル）に応じた安全状態に移行することができ、状況に応じた適切な対処が可能となる。これにより、車両Ｂが巻き込まれるような事故の発生等が防止され得る。また、不正検知通知として示されるレベルは、例えば車載ネットワークで検知された不正なＣＡＮメッセージによる影響の程度に鑑みて予め設定しておくことができ、また、そのレベルに対応して移行する安全状態は、例えば交通システムへの悪影響を抑制するように考慮して予め設定しておくことができるため、不正検知通知を受信した車両は、状況に応じて適切な安全状態へと移行可能になり得る。

【０１３４】

（実施の形態２）

以下、上述した車車間通信システムを一部変形した形態について示す。

【０１３５】

実施の形態１で示した車車間通信システムの不正対処方法では、車両１０（車両Ａ）で不正が検知されたことに係る不正検知通知を、車両１０の後方の１台の車両２０（車両Ｂ）に伝達する例を示した。これに対して、本実施の形態に係る車車間通信システムは、不正対処方法として不正検知通知の転送を行い得る。即ち、本実施の形態に係る車車間通信システムでは、車両１０（車両Ａ）が検知した不正に係る不正検知通知を送信し、この不正検知通知を受信した車両がその不正検知通知を一定条件下で転送することで、車両１０（車両Ａ）に後続する複数の車両が受信可能となるように不正検知通知の伝達を行う。実施の形態２に係る車車間通信システムの構成（例えば各車両の構成要素等）は、実施の形態１で示したものと同様であるため説明を省略し、ここでは、実施の形態１と異なる部分を説明する。

【０１３６】

［２．１　車車間通信メッセージの伝達］

図１２は、複数の車両が連続的に後続車に不正検知通知としての車車間通信メッセージを通知する例を示す図である。不正検知通知としての車車間通信メッセージを受信した車両は、所定条件（転送条件）が満たされるか否かを判定して、満たされると判定した場合に車両の外部へと不正検知通知の送信（転送）を行う。転送条件は、転送するか否かに係る条件であり、図１２の例では、不正を検知した車両からの距離が５００ｍ未満という条件である。

【０１３７】

この例では、車両１０（車両Ａ）で不正を検知し、車両Ａから他の車両へ不正検知通知としての車車間通信メッセージ３００ａを送信する。車両Ａに後続する車両２０（車両Ｂ）は、車両Ａからの車車間通信メッセージ３００ａを受信して、車車間通信メッセージ３００ａに含まれる不正検知に関する情報（図１２の例ではレベル４を示すレベル情報等）を他の車両に転送するために、その不正検知に関する情報を含む車車間通信メッセージ３００ｂを送信する。車両Ｂに後続する車両３０（車両Ｃ）は、車両Ｂからの車車間通信メッセージ３００ｂを受信して、車車間通信メッセージ３００ｂに含まれる不正検知に関する情報を他の車両に転送するために、その不正検知に関する情報を含む車車間通信メッセージ３００ｃを送信する。車両Ｃに後続する車両４０（車両Ｄ）は、車両Ｃからの車車間

通信メッセージ３００ｃを受信する。車両Ｄは、車両Ａから５００ｍ離れており、不正を検知した車両からの距離が５００ｍ未満であるという転送条件を満たさないため、転送を行わない。なお、車両Ｃ及び車両Ｄも、車両Ｂと基本的に同様の構成を備える。

【０１３８】

［２．２　車車間通信メッセージフォーマット］

図１３は、本実施の形態に係る車車間通信メッセージの構成の一例を示す図である。

【０１３９】

本実施の形態における車車間通信メッセージ３００ａ（車車間通信メッセージ３００ｂ、３００ｃも同様）は、実施の形態１で示した車車間通信メッセージ３００の構成（図８参照）に、転送条件を示す条件情報３１０を追加した構成を有する。これにより、再送信（転送）がなされる範囲を限定することができる。

【０１４０】

条件情報３１０が示す転送条件は、不正検知がなされた車両からの距離についての条件であり、例えば、一の車両についての測定した位置と、受信した不正検知通知に含まれる位置情報（不正車両位置情報３０８）が示す位置との距離が一定範囲内であるという条件である。条件情報３１０は、具体例としては不正検知がなされた車両から５００ｍ未満の距離であること等を示す。この場合に、車車間通信メッセージ３００ａ等を受信した車両が、不正検知がなされた車両から５００ｍ未満であれば転送を行うことになる。なお、不正検知がなされた車両の位置は、車車間通信メッセージ３００ａ内の不正車両位置情報３０８により示されている。従って、車車間通信メッセージ３００ａを受信した車両（例えば車両２０）では、不正車両位置情報３０８が示す不正検知がなされた車両Ａの位置と、例えば位置情報取得部２９０（図２参照）により検知される自車両の位置との距離を算出して、条件情報３１０が示す転送条件に基づいて、車車間通信メッセージ３００ａの再送信（転送）を行うか否かを決定する。ここで、車車間通信メッセージ３００ａの転送とは、車車間通信メッセージ３００ａの内容を一部変更した転送（つまり車車間通信メッセージ３００ｂの送信）を含む。車車間通信メッセージ３００ａ～３００ｂのそれぞれにおける署名データ３０９、共通アプリデータ部等の具体的な値は車両毎に異なり得る。しかし、車車間通信メッセージ３００ａ～３００ｂのそれぞれにおけるレベル情報３０７、不正車両位置情報３０８及び条件情報３１０の具体的な値は同一である。

【０１４１】

［２．３　不正検知通知の転送のシーケンス］

図１４及び図１５は、車両が車車間通信メッセージを受信して転送する場合の各部の動作を示すシーケンス図である。ここでは、車両１０（車両Ａ）から不正検知通知としての車車間通信メッセージを車両２０（車両Ｂ）が受信する場合を例にして説明する。

【０１４２】

ステップＳ４０１からステップＳ４１１は、実施の形態１で示したステップＳ３０１からステップＳ３１１（図１１参照）と同様であるので、説明を省略する。

【０１４３】

ステップＳ４１２において車両Ｂのレベル解釈部２２０は、ステップＳ４０４で参照したレベル情報３０７を含む車車間通信メッセージ３００ａの条件情報３１０が示す転送条件を参照し、転送条件が満たされるか否かを判別する。即ち、レベル解釈部２２０は、位置情報取得部２９０から自車両の位置を取得して、車車間通信メッセージ３００ａの不正車両位置情報３０８を参照し、不正が検知された車両Ａから自車両が離れている距離を算出する。算出した距離が、転送条件を満たすならば、レベル解釈部２２０は、車車間通信メッセージ３００ａに含まれていたレベル情報３０７、不正車両位置情報３０８及び条件情報３１０と同一の情報を、車車間通信メッセージ３００ｂのレベル情報３０７、不正車両位置情報３０８及び条件情報３１０に設定できるように車車間通信メッセージ認証部２３０に渡して、署名を要求する（ステップＳ４１３）。また、転送条件が満たされない場合には、車両Ｂでは、転送を行わずに処理を終了する。

【０１４４】

ステップＳ４１３で署名を要求された車車間通信メッセージ認証部２３０は、レベル解釈部２２０に渡された情報を設定して車車間通信メッセージ３００ｂを形成して、車両Ｂの秘密鍵２３０１を利用して電子署名を生成して署名データ３０９として車車間通信メッセージ３００ｂに含ませる（ステップＳ４１４）。

【０１４５】

そして車車間通信メッセージ認証部２３０は、電子署名を付加した車車間通信メッセージ３００ｂを、車両Ｂの車車間通信メッセージ送受信部２４０へ通知して送信を要求する（ステップＳ４１５）。

【０１４６】

続いて車車間通信メッセージ送受信部２４０は、車車間通信メッセージ３００ｂと車両Ｂ公開鍵証明書２３０２とを、車車間通信により後方の車両３０（車両Ｃ）に送信する。なお、車両Ａから車両Ｂへの不正検知通知としての車車間通信メッセージ３００ａと同様に、その不正検知通知の転送となる車両Ｂから車両Ｃへの車車間通信メッセージ３００ｂの送信も、特に送信の宛先として車両Ｃを特定するものではない。これにより、車車間通信メッセージ３００ｂは、車両Ｂの後方に伝搬され得る通信方法により、不特定の車両に対してブロードキャストされる。

【０１４７】

上述した車両Ｂと同様に、他の車両（例えば車両Ｂの後方を走行している車両Ｃ）においても、受信した車車間通信メッセージが示す転送条件が満たされる場合に不正検知通知の転送が行われ、転送条件が満たされない場合に転送が行われない。

【０１４８】

［２．４　実施の形態２の効果］

実施の形態２に係る車車間通信システムが用いる不正対処方法によれば、実施の形態１に係る車車間通信システムにより生じる効果に加えて、不正が検知された車両に後続する複数の車両を安全な状態に移行することが可能になる。このため、例えば３台以上の車両を巻き込んだ大きな事故の発生が防止され得る。

【０１４９】

（実施の形態３）

以下、実施の形態２で示した車車間通信システムを一部変形した形態について示す。

【０１５０】

本実施の形態に係る車車間通信システムが用いる不正対処方法では、不正検知通知（車車間通信メッセージ）における不正検知に関する情報の一部であるレベル情報の内容を変更して転送する。実施の形態３に係る車車間通信システムについて、上述の実施の形態１又は実施の形態２で示したものと同様の点については説明を省略し、ここでは、相違する点について説明する。

【０１５１】

［３．１　車車間通信メッセージフォーマット］

図１６は、本実施の形態２に係る車車間通信メッセージの構成の一例を示す図である。

【０１５２】

本実施の形態における車車間通信メッセージ３００Ａは、実施の形態２で示した車車間通信メッセージ３００ａの構成（図１３参照）に、再設定レベル情報３１１と、再設定レベル情報を更新するための規則である所定レベル変更規則を示すレベル変更条件３１２とを追加した構成を有する。これにより、車車間通信メッセージの再送信（転送）に際してセキュリティレベルを変更して伝達することが可能になる。

【０１５３】

再設定レベル情報３１１には、車車間通信メッセージを受信した車両が、他車両に車車間通信メッセージを再送信（転送）する際に、レベル変更条件３１２に応じて、不正検知がなされた車両において設定されたレベル情報３０７が示すセキュリティレベルを変更した値（レベル）が設定される。なお、不正を検知した車両Ａにおいては、車車間通信メッセージ３００Ａの再設定レベル情報３１１に、レベル情報３０７と同値を設定する。

【０１５４】
［３．２　レベル変更条件３１２］
図１７は、レベル変更条件３１２の一例を示す図である。図１７の例では、所定レベル変更規則を示すレベル変更条件３１２は、具体的にはレベルを変更するための各条件（不正車両との距離）に応じたその変更の内容（レベル変更内容）を示している。
【０１５５】
車車間通信メッセージ３００Ａを受信した車両は、自車両の位置と不正車両（つまり不正が検知された車両Ａ）の位置とから、不正車両と自車両との距離を算出し、算出した距離と、レベル変更条件３１２が示すレベルを変更するための条件とを比較することで、その距離に応じて、再設定レベル情報３１１に設定すべき値を特定できる。
【０１５６】
図１７の例では、不正車両との距離が１００ｍ未満であれば、不正車両で設定された再設定レベル情報３１１について、転送の際に変更しないで維持する。例えば、不正車両との距離が１００ｍ未満の位置にいる車両が送信（転送）した車車間通信メッセージでは、レベル情報３０７に「レベル４」が設定され、再設定レベル情報３１１にも同値の「レベル４」が設定される。
【０１５７】
また、図１７の例では、不正車両との距離が１００ｍ以上かつ３００ｍ未満という条件に該当した場合のレベル変更内容が、再設定レベル情報３１１を不正車両で設定されたレベル情報３０７から１つ下げる（１減ずる）ことを示している。例えば、不正車両との距離が１００ｍ以上かつ３００ｍ未満の位置にいる車両が送信（転送）した車車間通信メッセージでは、レベル情報３０７に「レベル４」が設定され、再設定レベル情報３１１には１減じた「レベル３」が設定される。
【０１５８】
また、図１７の例では、不正車両との距離が３００ｍ以上かつ５００ｍ未満という条件に該当した場合のレベル変更内容が、再設定レベル情報３１１を不正車両で設定されたレベル情報３０７から２つ下げる（２減ずる）ことを示している。例えば、不正車両との距離が３００ｍ以上かつ５００ｍ未満の位置にいる車両が送信（転送）した車車間通信メッセージでは、レベル情報３０７に「レベル４」が設定され、再設定レベル情報３１１には１減じた「レベル２」が設定される。
【０１５９】
なお、実施の形態２では車車間通信メッセージを受信した各車両が、レベル情報３０７が示すレベル（セキュリティレベル）に応じて、安全状態に移行する不正対応処理を実行したが、本実施の形態では、車車間通信メッセージを受信した各車両は、再設定レベル情報３１１に設定されたレベル（セキュリティレベル）に応じて、安全状態に移行する不正対応処理を実行する。
【０１６０】
［３．３　車車間通信メッセージの伝達］
図１８は、複数の車両が連続的に後続車に不正検知通知としての車車間通信メッセージを通知する例を示す図である。不正検知通知としての車車間通信メッセージを受信した車両は、転送条件が満たされる場合において不正検知通知でのレベル変更条件３１２に応じて再設定レベル情報３１１を変更して、不正検知通知の転送を行う。図１８の例は、図１７に例示したレベル変更条件３１２を用いて、不正検知通知の再送信（転送）を行った例である。車両１０（車両Ａ）と車両２０（車両Ｂ）との間には１台以上の他の車両が含まれていて車車間通信メッセージの転送を行うこともあり得る。また車両Ｂと車両３０（車両Ｃ）との間に１台以上の他の車両が含まれていて車車間通信メッセージの転送を行うこともあり得る。
【０１６１】
図１８の例では、車両Ａが車載ネットワーク上で不正を検知し、不正内容に応じてレベル情報３０７及び再設定レベル情報３１１を「レベル３」と定めて車車間通信メッセージ

３００Ａを送信している。車車間通信メッセージ３００Ｂ～３００Ｅも、車車間通信メッセージ３００Ａと同一のフォーマット（図１６参照）で構成される。例えば車車間通信メッセージ３００Ａが他の車両により転送されて車車間通信メッセージ３００Ｂとして車両Ｂにおいて受信される。

【０１６２】

車両Ａの位置から１００ｍ離れた車両Ｂにおいては、車車間通信メッセージ３００Ｂのレベル変更条件３１２に基づいて、不正車両との距離が１００ｍ以上かつ３００ｍ未満という条件に該当するため、再設定レベル情報３１１を不正車両で設定されたレベル情報３０７から１減じて、再設定レベル情報３１１を「レベル２」とした車車間通信メッセージ３００Ｃを送信する。例えば車車間通信メッセージ３００Ｃが他の車両により転送されて車車間通信メッセージ３００Ｄとして車両Ｃにおいて受信される。

【０１６３】

車両Ａの位置から３００ｍ離れた車両Ｃにおいては、車車間通信メッセージ３００Ｄのレベル変更条件３１２に基づいて、不正車両との距離が３００ｍ以上かつ５００ｍ未満という条件に該当するため、再設定レベル情報３１１を不正車両で設定されたレベル情報３０７から２減じて、再設定レベル情報３１１を「レベル１」とした車車間通信メッセージ３００Ｅを送信する。

【０１６４】

車両４０（車両Ｄ）では、不正車両との距離が５００ｍの位置にいるため、車車間通信メッセージ３００Ｅの条件情報３１０が示す「５００ｍ未満」という条件が満たされず、車車間通信メッセージの再送信（転送）が行われない。

【０１６５】

［３．４　不正検知通知の転送のシーケンス］

図１９及び図２０は、車両が車車間通信メッセージを受信して一定条件下でレベル情報を変更して転送する場合の各部の動作を示すシーケンス図である。ここでは、車両１０（車両Ａ）から送信され他の車両で転送された不正検知通知としての車車間通信メッセージＢを車両２０（車両Ｂ）が受信する場合を例にして説明する。

【０１６６】

ステップＳ５０１からステップＳ５１１は、実施の形態１で示したステップＳ３０１からステップＳ３１１（図１１参照）と同様であるので、説明を省略する。但し、ステップＳ５０４では、車両Ｂのレベル解釈部２２０は、図１０で示した対応情報（安全状態リスト）を参照して、車車間通信メッセージ３００Ｂの再設定レベル情報３１１が示すレベル（セキュリティレベル）に応じて、どの安全状態に移行するための不正対応処理を実行すべきかを特定して、その不正対応処理の実行指示（安全状態への移行要求）を車両安全状態指示部２５０に通知する（ステップＳ５０５）。

【０１６７】

ステップＳ５１２において車両Ｂのレベル解釈部２２０は、ステップＳ５０４で再設定レベル情報３１１を参照した車車間通信メッセージ３００Ｂの条件情報３１０が示す転送条件を参照し、転送条件が満たされるか否かを判別する。転送条件が満たされるならば、レベル解釈部２２０は、車車間通信メッセージ３００Ｂのレベル変更条件３１２に基づいて、レベル変更条件３１２が示す各条件のうち自車両が該当する条件に対応するレベル変更内容を参照して、レベルの変更が必要か否かを判断し（ステップＳ５１３）、レベルの変更が必要と判断した場合に限り、レベル変更内容に従って再設定レベル情報３１１を下げる（ステップＳ５１４）。そして、レベル解釈部２２０は、車車間通信メッセージ３００Ｂに含まれていたレベル情報３０７、不正車両位置情報３０８、条件情報３１０及びレベル変更条件３１２と同一の情報を、車車間通信メッセージ３００Ｃのレベル情報３０７、不正車両位置情報３０８、条件情報３１０及びレベル変更条件３１２に設定できるように、また、ステップＳ５１３での判断に応じて、レベル値を維持した又は減じた再設定レベル情報３１１を車車間通信メッセージ３００Ｃの再設定レベル情報３１１に設定できるように、車車間通信メッセージ認証部２３０に渡して、署名を要求する（ステップＳ５１

５）。また、転送条件が満たされない場合には、車両Ｂでは、転送を行わずに処理を終了する。

【０１６８】

ステップＳ５１５で署名を要求された車車間通信メッセージ認証部２３０は、レベル解釈部２２０に渡された情報を設定して車車間通信メッセージ３００Ｃを形成して、車両Ｂの秘密鍵２３０１を利用して電子署名を生成して署名データ３０９として車車間通信メッセージ３００Ｃに含ませる（ステップＳ５１６）。

【０１６９】

そして車車間通信メッセージ認証部２３０は、電子署名を付加した車車間通信メッセージ３００Ｃを、車両Ｂの車車間通信メッセージ送受信部２４０へ通知して送信を要求する（ステップＳ５１７）。

【０１７０】

続いて車車間通信メッセージ送受信部２４０は、車車間通信メッセージ３００Ｃと車両Ｂ公開鍵証明書２３０２とを、車車間通信により他車両に伝搬すべく送信する（ステップＳ５１８）。

【０１７１】

［３．５　実施の形態３の効果］

実施の形態３に係る車車間通信システムが用いる不正対処方法によれば、不正車両の後続車両では不正車両から離れている程、不正検知通知に係るレベル（再設定レベル情報が示すセキュリティレベル）を下げている。これにより、不正検知通知を受けた車両において不正対応処理による安全状態への移行によって、交通システムに与える悪影響（例えば交通渋滞の発生等）を抑制することが可能となる。

【０１７２】

（実施の形態４）

上述した実施の形態１から３では、車車間通信の例を示したが、車両と道路に設置された路側機との間で路車間通信を行うこととしても良い。本実施の形態では、路車間通信をするための路車間通信システムの構成を示す。

【０１７３】

［４．１　路車間通信システムの構成］

図２１は、路車間通信システムの全体構成を示す図である。車両１０（車両Ａ）が、自車両の車載ネットワークにおける不正を検知し、その不正検知に関する情報を示す不正検知通知を送信し、路側機７０が受信する路車間通信のための構成を示している。車両Ａの構成は、上述した実施の形態１～３のいずれかにおける車両Ａと同様であるので、説明を省略する。本実施の形態の路車間通信システムは、実施の形態１で示した車車間通信システムとは、車両Ａから送信される車車間通信メッセージ３００を受信する物が、移動する車両でなく道路に設置された路側機７０となった点で異なる。

【０１７４】

路側機７０は、位置情報取得部７９０と、路車間通信メッセージ送受信部７４０と、路車間通信メッセージ認証部７３０と、レベル解釈部７２０と、車両安全状態指示部７５０と外部サーバ通信部７７０とを含んで構成される。

【０１７５】

レベル解釈部７２０は、実施の形態１～３のいずれかで示した車両２０（車両Ｂ）のレベル解釈部２２０と同じ機能を有する。但し、レベル解釈部７２０は、所定の対応情報（安全状態リスト）に基づいて、車両Ａから受信した車車間通信メッセージに含まれるレベル情報が示すセキュリティレベルに応じた安全状態に別の車両を移行させるための指示（不正対応処理の実行指示）を、車両安全状態指示部７５０に通知する。本実施の形態における不正対応処理は、車両安全状態指示部７５０が行う、路側機７０の周辺を走行中の車両を安全状態に移行するための制御である。例えば、不正対応処理には、路側機７０の周辺を走行中の車両の走行を停止させる制御のための不正対応処理、その車両を徐行させる制御のための不正対応処理、その車両と前方の車両との車間距離を一定範囲に保って走行

させる制御のための不正対応処理、その車両の運転者への報知の制御のための不正対応処理等がある。

【０１７６】

路車間通信メッセージ認証部７３０は、署名生成及び署名検証に必要となる秘密鍵及び公開鍵証明書を保持し、車車間通信メッセージに対して署名生成或いは署名検証を行う。路車間通信メッセージ認証部７３０は、車車間通信メッセージの送信（転送）に際して、レベル解釈部７２０から取得した情報に、位置情報取得部７９０から取得した路側機７０の位置情報等を含ませて、車車間通信メッセージを形成して、車両の秘密鍵を利用して署名を生成して車車間通信メッセージに含ませる。なお位置情報取得部７９０は、路側機７０の設置された位置を示す位置情報を記録しておきその位置情報を路車間通信メッセージ認証部７３０に通知しても良い。また、路車間通信メッセージ認証部７３０は、車両から受信した車車間通信メッセージについての署名検証を行って、車車間通信メッセージに含まれるレベル情報をレベル解釈部７２０に通知する。

【０１７７】

車両安全状態指示部７５０は、不正対応処理を実行して、路車間通信メッセージ送受信部７４０を介して、路側機７０の周辺に所在する車両に対して、安全状態に移行することを指示する路車間通信メッセージを送信する。このときの路車間通信メッセージのフォーマットは、実施の形態１から実施の形態３で説明した車車間通信メッセージと同様である。なお、路側機７０が電光掲示板を備え、車両安全状態指示部７５０が電光掲示板に、周辺の車両を安全状態に導くための指示情報等を表示させることとしても良い。

【０１７８】

外部サーバ通信部７７０は、車両Ａから受信した車車間通信メッセージを外部サーバ（不図示）に送信する。外部サーバは、路側機７０から受信した車車間通信メッセージを蓄積しておき、蓄積したデータを解析することで指示内容を決定して、路側機７０に対して車両を安全な状態に移行するように指示しても良い。外部サーバから指示を受けた路側機７０は、路車間通信を用いて、路側機７０の周辺に位置している車両に対して安全状態に移行するように指示しても良い。

【０１７９】

［４．２　実施の形態４の効果］

本実施の形態４で示した路車間通信システムを、実施の形態１～３のいずれかで示した車車間通信システムと併用することにより、路車間通信で路側機の周辺にいる車両に対して安全状態に移行するよう指示を通知すること等が可能となり、より安全な交通システムが実現可能となる。

【０１８０】

（実施の形態５）

以下、実施の形態２で示した車車間通信システムを一部変形した形態について示す。

【０１８１】

本実施の形態に係る車車間通信システムが用いる不正対処方法では、不正検知通知（車車間通信メッセージ）の転送を行うか否かを判定する際に用いる所定条件（転送条件）の内容が、実施の形態２で示したものと異なる。本実施の形態における転送条件は、不正フレームを検知して不正検知通知を送信した車両（車両における装置）からのその不正検知通知を受信するまでに転送がなされた回数が所定回数より少ないという条件である。不正検知通知としての車車間通信メッセージに回数情報を含ませておき、不正検知通知を受信した車両（その車両の装置）では、受信した不正検知通知に含まれる回数情報に基づいて、転送条件が満たされているか否かに係る判定を行う。そして、不正検知通知を受信した車両で転送条件が満たされていると判定した場合には、受信した不正検知通知の送信（転送）に際して、不正検知通知に含まれる回数情報を更新した上でその転送を行う。

【０１８２】

実施の形態５に係る車車間通信システムについて、上述の実施の形態１又は実施の形態２で示したものと同様の点については説明を省略し、ここでは、相違する点について説明

する。

【０１８３】

［５．１　車車間通信メッセージの伝達］

図２２は、複数の車両が連続的に後続車に不正検知通知としての車車間通信メッセージを通知する例を示す図である。不正検知通知としての車車間通信メッセージを受信した車両は、転送条件が満たされる場合に不正検知通知の転送を行う。図２２の例では転送条件は、不正車両からの不正検知通知を受信するまでに転送がなされた回数が所定回数（ここでは２回）未満という条件である。

【０１８４】

この例では、車両１０（車両Ａ）で不正を検知し、車両Ａから他の車両へ不正検知通知としての車車間通信メッセージ３９０ａを送信する。車車間通信メッセージ３９０ａは、転送回数として０回を示す回数情報を含み、転送条件として２回未満を示す条件情報を含む。車両Ａに後続する車両２０（車両Ｂ）は、車両Ａからの車車間通信メッセージ３９０ａを受信して、回数情報が示す回数（０回）が転送条件である２回未満を満たすので、車車間通信メッセージ３９０ａに含まれる不正検知に関する情報を他の車両に転送するために、その不正検知に関する情報を含む車車間通信メッセージ３９０ｂを送信する。車両Ｂは、車車間通信メッセージ３９０ｂに、転送回数として１回を示す回数情報を含ませる。車両Ｂに後続する車両３０（車両Ｃ）は、車両Ｂからの車車間通信メッセージ３９０ｂを受信して、回数情報が示す回数（１回）が転送条件である２回未満を満たすので、車車間通信メッセージ３９０ｂに含まれる不正検知に関する情報を他の車両に転送するために、その不正検知に関する情報を含む車車間通信メッセージ３９０ｃを送信する。車両Ｃは、車車間通信メッセージ３９０ｃに、転送回数として２回を示す回数情報を含ませる。車両Ｃに後続する車両４０（車両Ｄ）は、車両Ｃからの車車間通信メッセージ３９０ｃを受信する。車両Ｄでは、受信した車車間通信メッセージ３９０ｃの回数情報が示す回数（２回）が転送条件である２回未満を満たさないので、転送を行わない。

【０１８５】

［５．２　車車間通信メッセージフォーマット］

図２３は、本実施の形態に係る車車間通信メッセージの構成の一例を示す図である。

【０１８６】

本実施の形態における車車間通信メッセージ３９０ａ（車車間通信メッセージ３９０ｂ、３９０ｃも同様）は、実施の形態１で示した車車間通信メッセージ３００の構成（図８参照）に、転送回数を格納するための回数情報３９１と、転送条件を示す条件情報３９２とを追加した構成を有する。これにより、再送信（転送）がなされる範囲を限定することができる。

【０１８７】

条件情報３９２が示す転送条件は、不正フレームを検知して不正検知通知を送信した車両（その車両の装置）からのその不正検知通知を受信するまでに転送がなされた回数が所定回数より少ないという条件である。条件情報３９２は、具体例としては２回未満を示す。

【０１８８】

回数情報３９１は、転送回数を示す。車車間通信メッセージを転送する車両において、その転送の際に１増加するように更新される。

【０１８９】

［５．３　実施の形態５の効果］

実施の形態５に係る車車間通信システムが用いる不正対処方法によれば、実施の形態２で示した不正対処方法と同様に、不正が検知された車両に後続する複数の車両を安全な状態に移行することが可能になる。このため、例えば３台以上の車両を巻き込んだ大きな事故の発生が防止され得る。また、不正が検知された車両から、不正検知通知の転送回数が所定回数以上必要となる位置まで離れた車両については、安全状態に移行する制御がなされないため、交通渋滞等が防止され得る。

【０１９０】
（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１～５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。
【０１９１】
（１）上記実施の形態では、車車間通信として、前方の車両から後方の車両に不正検知通知としての車車間通信メッセージを送信する例を示したが、送信先は後方の車両に限られず、自車両の周辺（例えば前方、側方等）に位置する他の車両に対して不正検知通知が伝達されれば良い。例えば、不正を検知した車両が車車間通信で自車両の後方に指向性を有する送信アンテナを用いずに全方向に一様に不正検知通知を送信しても良い。この場合において、不正検知通知としての車車間通信メッセージを受信した走行中の車両が、自車両の位置及び進行方向（車両方位角）を測定して不正検知通知としての車車間通信メッセージ中の不正車両位置情報を参照することで、概ね自車両の進行方向上に不正車両が位置する場合に限って不正対応処理の実行、不正検知通知の転送等を行うこととしても良い。また、各車両は、自車両が一度受信した不正検知通知としての車車間通信メッセージを転送した後に、その不正検知通知に基づいて他車両によって転送された不正検知通知（つまり同一の不正検知に関する情報を含む不正検知通知）を再度受信したときには転送しないようにしても良い。
【０１９２】
（２）上記実施の形態では、所定レベル変更規則を示すレベル変更条件を、車車間通信メッセージに含めていたが、車車間通信メッセージに含めず、車両内部の装置（例えばレベル解釈部等）にて保持し、必要に応じて参照することとしても良い。また、転送条件を示す条件情報についても、同様に、車車間通信メッセージに含めず、車両内部の装置（例えばレベル解釈部等）にて保持し、必要に応じて参照することとしても良い。
【０１９３】
（３）上記実施の形態では、レベル情報の値として４段階のレベル（セキュリティレベル）を示したが、レベルの区分数は４より多くても少なくても良い。
【０１９４】
（４）上記実施の形態では、レベル情報のレベルを、図７示すように不正フレームのフレームＩＤにより定まる機能種別毎に設定しているが、不正フレームの内容等に応じて、機能種別が同じであっても相違するレベルを設定しても良く、例えばフレームＩＤ毎、或いは、不正フレームのフレームＩＤを送信することとなっている個々のＥＣＵ毎に、レベルを設定しても良い。なお、実施の形態３で示した再設定レベル情報３１１の代わりに、レベル情報３０７を用いても良く、各車両において受信した不正検知通知（車車間通信メッセージ）の送信（転送）に際して、その受信した不正検知通知に含まれるレベル情報３０７を、所定レベル変更規則を示すレベル変更条件（例えば受信したレベル情報３０７が２以上であれば１減じる等といった条件）に基づいて変更して、変更後のレベル情報３０７を含む不正検知通知を送信（転送）することとしても良い。
【０１９５】
（５）上記実施の形態では、車両が、ＣＡＮバスとこれに接続されたＥＣＵで構成される車載ネットワークを搭載している例を示したが、車載ネットワークは、車両内においてＥＣＵ等の車載装置間で通信する通信ネットワークであれば、ＣＡＮバスを用いない、いかなる通信ネットワークでも良い。
【０１９６】
（６）上記実施の形態では、車両において不正検知通知を転送するか否かの判定に係る所定条件（転送条件）として、車両間の距離、或いは、転送回数についての条件を示した。しかし、転送条件は、不正検知がなされた時刻からの経過時間についての条件であっても良い。例えば、転送条件は、受信した不正検知通知に含まれる時刻情報が示す時刻から

の経過時間が所定時間（一定の上限閾値）より短いという条件であっても良い。このためには、不正を検知した車両が送信する不正検知通知において不正が検知された時刻を示す時刻情報を含ませると良い。

【０１９７】

（７）上記実施の形態で示した不正検知通知は、図８等に示すフォーマットの車車間通信メッセージで送信されることに限定されず、不正検知通知を受信した車両において実行すべき不正対応処理の選択を可能とする内容（例えば、不正なメッセージＩＤ、或いは、セキュリティレベル等）を含めば、いかなる車車間通信用フォーマットで送信されても良い。

【０１９８】

（８）上記実施の形態で示した車両が備える各構成要素の機能分担は、一例に過ぎず、その分担を変更し得る。例えば、車車間通信システムにおいて不正検知通知を受信する車両が備える１つ又は複数のＥＣＵ（電子制御ユニット）は、自ユニットが搭載された車両とは別の車両に搭載された車載ネットワークで不正フレームが検知された際にその別の車両に搭載された装置から送信される不正検知通知を受信する受信部としての機能と、受信部により受信された不正検知通知の内容に応じて、予め定められた複数の不正対応処理から実行する不正対応処理を選択し、その選択した不正対応処理を実行する不正対処部としての機能とを有し得る。また、不正検知通知を送信する車両が備える、車載ネットワークに接続された１つ又は複数の装置（例えばＥＣＵ）は、車載ネットワークにおいて送信された不正フレームを検知する不正検知部（不正フレーム検知部）としての機能と、不正検知部により不正フレームが検知された場合に自ユニットを搭載する車両とは別の車両へと不正検知通知を送信する送信部としての機能とを有し得る。

【０１９９】

（９）上記実施の形態における各装置（例えばＥＣＵ、不正検知ＥＣＵ等）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。

【０２００】

（１０）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（Field Programmable Gate Array）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。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。

【０２０１】

（１１）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。

【０２０２】

（１２）本発明の一態様としては、例えば図９、図１１、図１４、図１５、図１９、図２０等に示す不正対処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。

【０２０３】

（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】

【０２０４】

本発明は、一の車両が不正に制御される可能性が高い場合にその影響を抑制すべく他の車両を制御するために利用可能である。

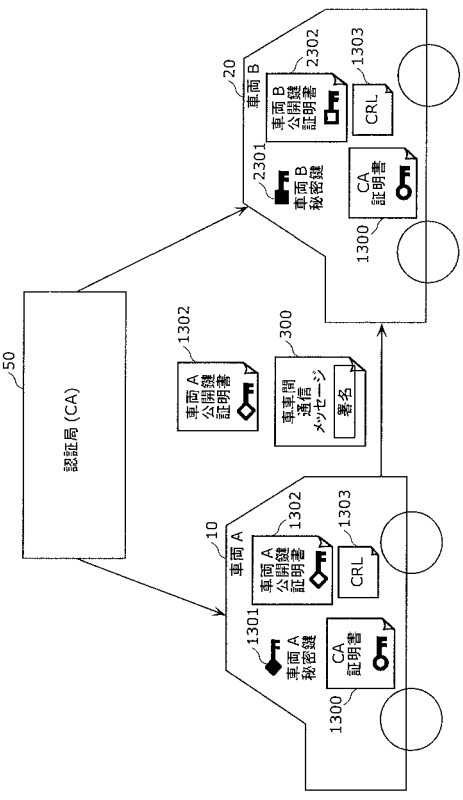
【符号の説明】

【０２０５】

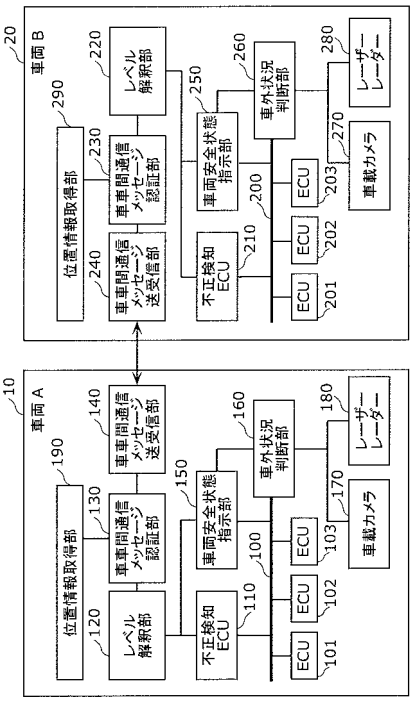
１０、２０、３０、４０　車両
５０　認証局（ＣＡ）
７０　路側機
１００　ＣＡＮバス
１０１～１０３、２０１～２０３　電子制御ユニット（ＥＣＵ）
１１０、２１０　不正検知電子制御ユニット（不正検知ＥＣＵ）
１１１　不正情報通知部
１１２　ホワイトリスト保持部
１１３　不正フレーム検知部
１１４　フレーム生成部
１１５　フレーム解釈部
１１６　フレーム送受信部
１２０、２２０、７２０　レベル解釈部
１３０、２３０　車車間通信メッセージ認証部
１４０、２４０　車車間通信メッセージ送受信部
１５０、２５０、７５０　車両安全状態指示部
１６０、２６０　車外状況判断部
１７０、２７０　車載カメラ
１８０、２８０　レーザーレーダー

１９０、２９０、７９０　位置情報取得部
１３００　ＣＡ証明書
１３０１　車両Ａ秘密鍵
１３０２　車両Ａ公開鍵証明書
１３０３　証明書失効リスト（ＣＲＬ）
２３０１　車両Ｂ秘密鍵
２３０２　車両Ｂ公開鍵証明書
３００、３００ａ～３００ｃ、３００Ａ～３００Ｅ、３９０ａ～３９０ｃ　車車間通信メッセージ
７３０　路車間通信メッセージ認証部
７４０　路車間通信メッセージ送受信部
７７０　外部サーバ通信部

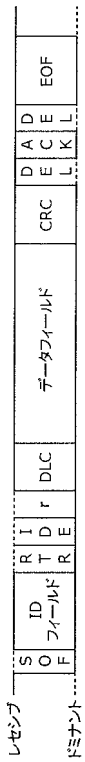
【図１】



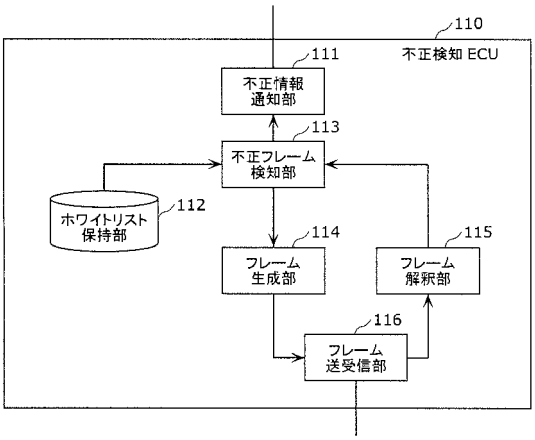
【図２】



【図３】



【図４】

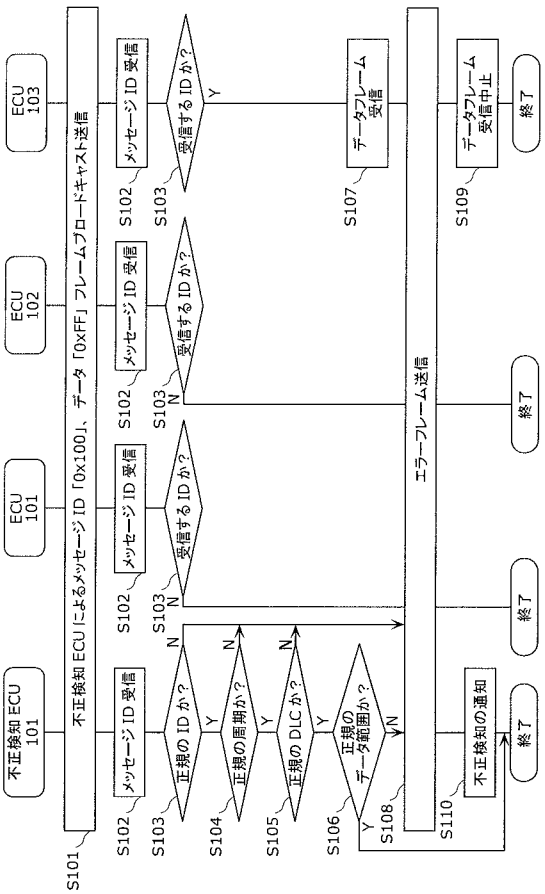


【図５】

1120 ホワイトリスト

ID	1121 データ長 [バイト]	1122 データ範囲	1123 周期 [ms]
0x100	8	0 ～ 180	10
0x200	8	0 ～ 10000	10
0x300	8	0 ～ 9999999	20
0x400	1	0, 1	1000
…	…	…	…

【図６】



【図７】

1200 レベル情報

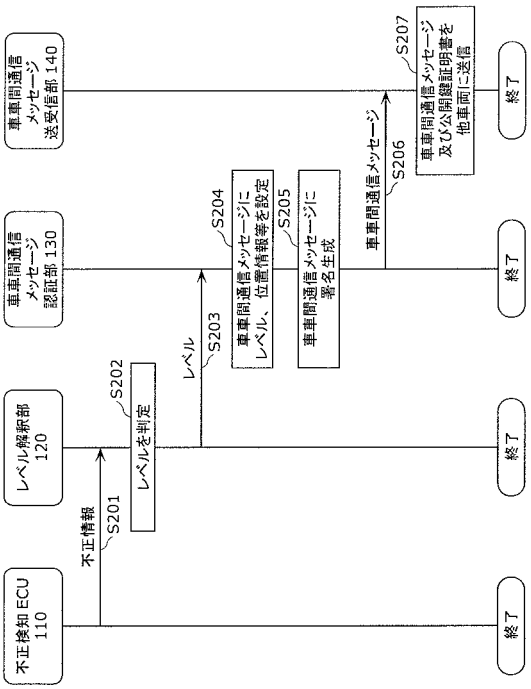
機能種別	1201 ID	1202 レベル
駆動系機能	0x100, 0x200, 0x300	4
シャーシ系機能	0x500	4
安全快適機能	0x10	3
ボディ系機能	0x400	2
ITS 機能	0x600	1
テレマティクス機能	0x700	1
インフォテインメント機能	0x800	1

【図８】

300 車車間通信メッセージ

共通アプリヘッダ部	共通アプリヘッダ情報	301
共通アプリデータ部	時刻情報	302
	位置情報	303
	車両状態情報	304
	車両属性情報	305
自由アプリヘッダ部	自由アプリヘッダ情報	306
自由アプリデータ部	レベル情報	307
	不正車両位置情報	308
	署名データ	309

【図９】

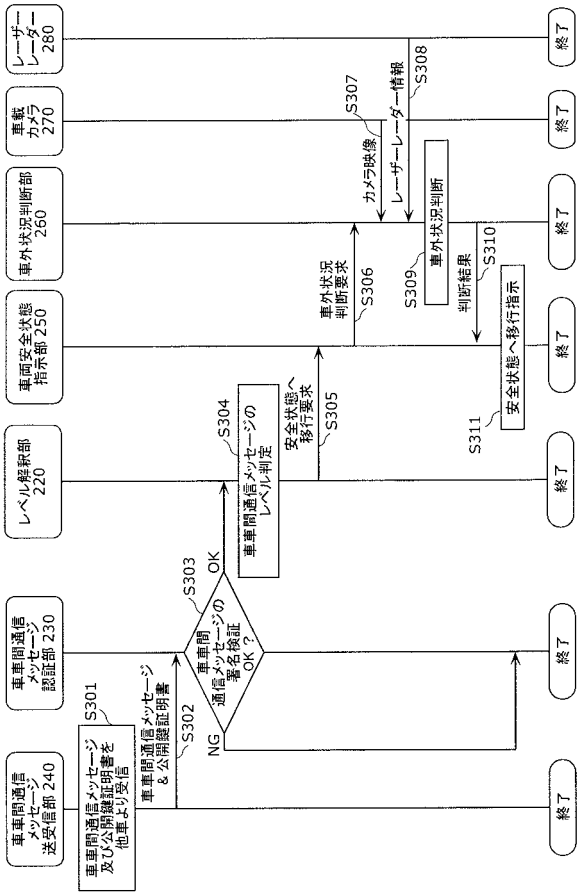


【図１０】

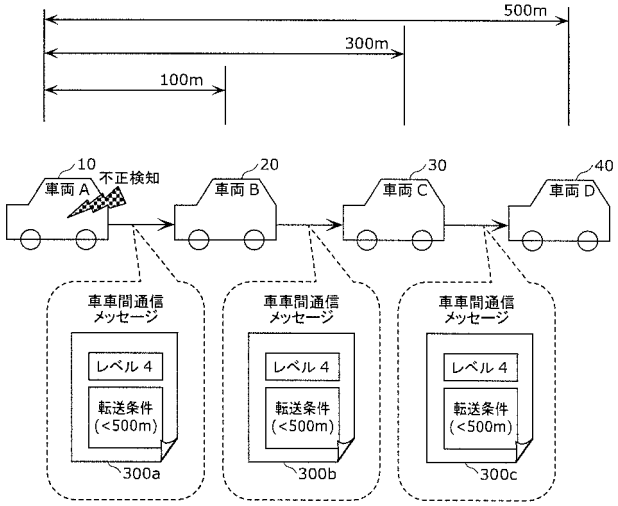
2400

対応情報 2401	2402
レベル	不正対応処理
4	路肩に寄せて停止
3	徐行
2	一定の車間距離をあけて走行
1	運転者に報知

【図１１】



【図１２】

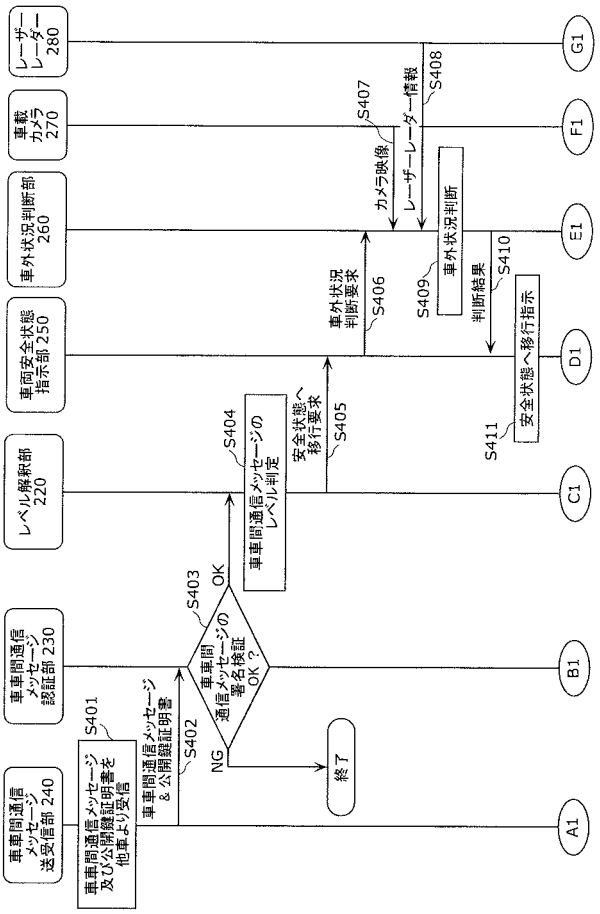


【図１３】

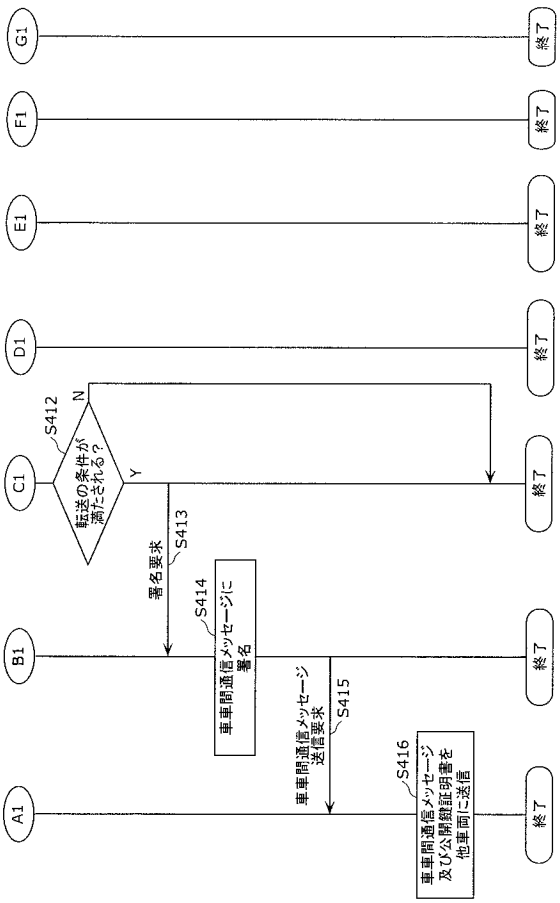
300a
車車間通信メッセージ

共通アプリヘッダ部	共通アプリヘッダ情報	301
共通アプリデータ部	時刻情報	302
	位置情報	303
	車両状態情報	304
	車両属性情報	305
自由アプリヘッダ部	自由アプリヘッダ情報	306
自由アプリデータ部	レベル情報	307
	不正車両位置情報	308
	条件情報（転送条件：500m 未満）	310
	署名データ	309

【図１４】



【図１５】



【図１６】

300A
車車間通信メッセージ

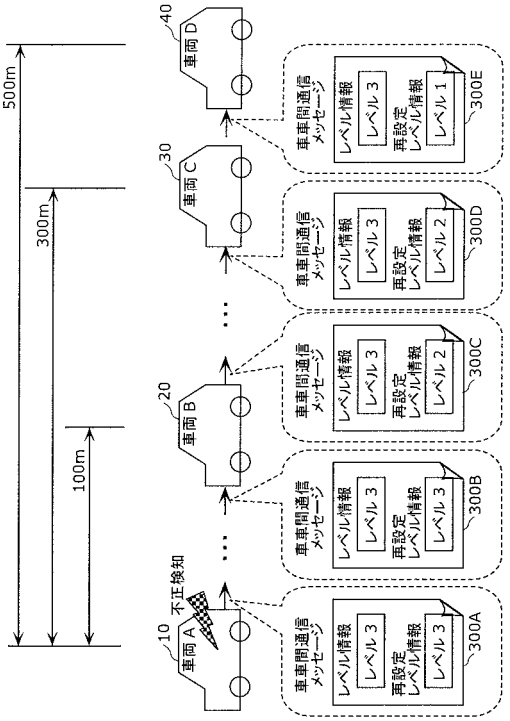
共通アプリヘッダ部	共通アプリヘッダ情報	301
共通アプリデータ部	時刻情報	302
	位置情報	303
	車両状態情報	304
	車両属性情報	305
自由アプリヘッダ部	自由アプリヘッダ情報	306
自由アプリデータ部	レベル情報	307
	再設定レベル情報	311
	レベル変更条件	312
	不正車両位置情報	308
	条件情報（転送条件：500m 未満）	310
	署名データ	309

【図１７】

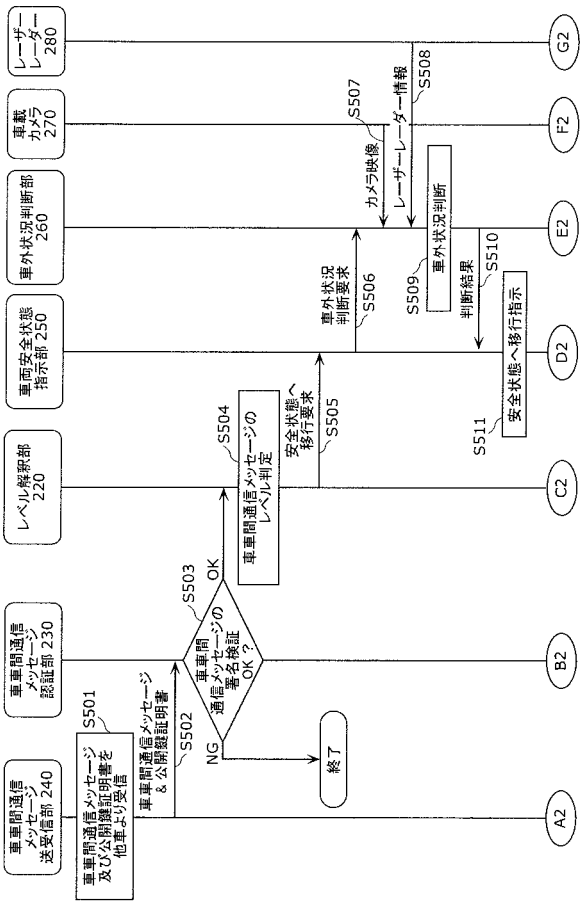
312
レベル変更条件

不正車両との距離	レベル変更内容
不正車両距離 ＜ 100m	不正検知時設定レベル維持（レベル情報のレベル）
100m ≦ 不正車両距離 ＜ 300m	不正検知時設定レベルから１つ下げる（レベル情報のレベル-1）
300m ≦ 不正車両距離 ＜ 500m	不正検知時設定レベルから２つ下げる（レベル情報のレベル-2）

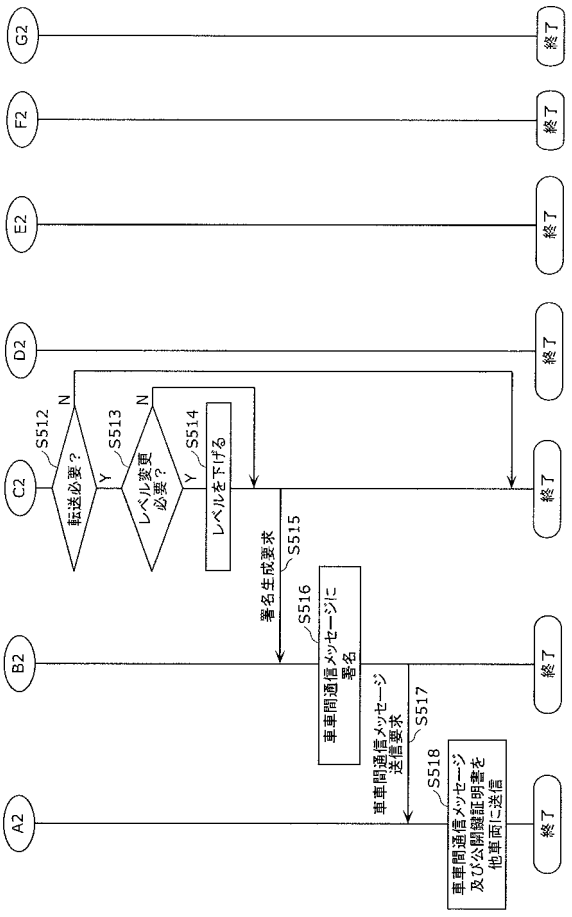
【図１８】



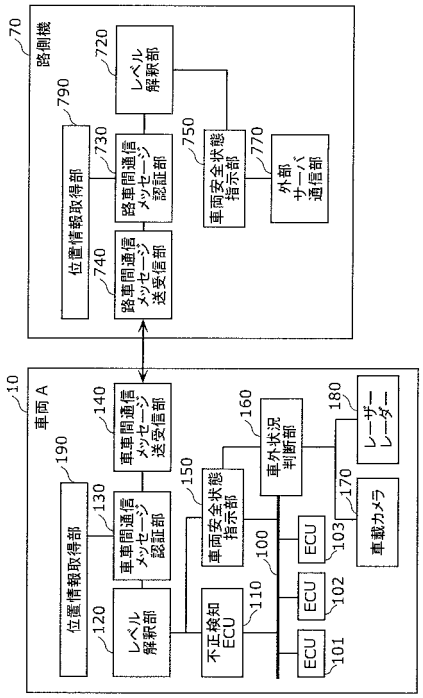
【図１９】



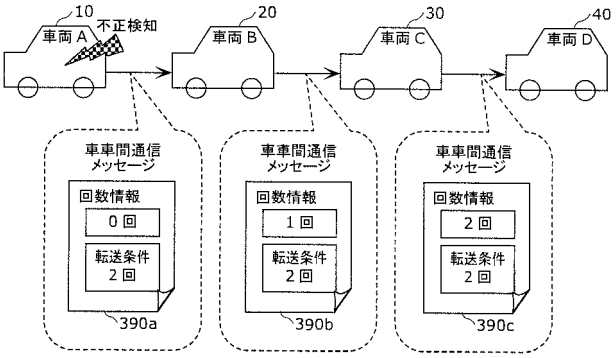
【図２０】



【図２１】



【図２２】



【図２３】

390a
車車間通信メッセージ

共通アプリヘッダ部	共通アプリヘッダ情報	301
共通アプリデータ部	時刻情報	302
	位置情報	303
	車両状態情報	304
	車両属性情報	305
自由アプリヘッダ部	自由アプリヘッダ情報	306
自由アプリデータ部	レベル情報	307
	回数情報	391
	条件情報（転送条件：２回未満）	392
	署名データ	309

フロントページの続き

(51)Int.Cl.			F I			テーマコード（参考）
Ｂ６０Ｒ	***16/023***	***(2006.01)***	Ｂ６０Ｗ	30/16		
Ｂ６０Ｒ	***21/00***	***(2006.01)***	Ｂ６０Ｒ	16/023	Ｐ	
			Ｂ６０Ｒ	21/00	６２８Ｂ	

(74)代理人 100131417
弁理士 道坂 伸一
(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 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 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 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) 3D241 BA02 BA31 BA60 BA64 BA65 BB72 BC01 CD05 CD07 CD12
CD21 CD26 CD28 CD29 CE02 CE03 CE04 CE05 DB01B DB01Z
DC02B DC02Z DC33Z DC35Z DC60Z
5H181 AA01 BB04 BB17 BB18 CC03 CC04 CC14 CC24 FF05 FF13
LL01 LL04 LL06 LL09
5K033 AA08 BA06 BA08 DA01 EA03 EA07