(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6849528号
(P6849528)
(45)発行日　令和3年3月24日(2021.3.24)　(24)登録日　令和3年3月8日(2021.3.8)

(51)Int.Cl.　　F I
H04L 12/40 (2006.01)　　H04L 12/40　M
H04L 12/28 (2006.01)　　H04L 12/28　200M

請求項の数 21　(全 47 頁)

(21)出願番号　特願2017-96138(P2017-96138)
(22)出願日　平成29年5月15日(2017.5.15)
(65)公開番号　特開2018-26791(P2018-26791A)
(43)公開日　平成30年2月15日(2018.2.15)
審査請求日　令和1年11月25日(2019.11.25)
(31)優先権主張番号　特願2016-148990(P2016-148990)
(32)優先日　平成28年7月28日(2016.7.28)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　514136668
パナソニック　インテレクチュアル　プロパティ　コーポレーション　オブ　アメリカ
Panasonic Intellectual Property Corporation of America
アメリカ合衆国　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　20000
(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】フレーム伝送阻止装置、フレーム伝送阻止方法及び車載ネットワークシステム

(57)【特許請求の範囲】
【請求項１】
車両に搭載された複数の電子制御ユニットがバスを介して通信する車載ネットワークシステムにおける当該バスに接続される前記車両に搭載されたフレーム伝送阻止装置であって、
前記バスからフレームを受信する受信部と、
フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、
前記管理情報を記憶している記憶部と、
前記記憶部に記憶された前記管理情報を更新する更新部とを備え、
前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、
前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、
当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、
当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、
前記更新部は、

前記車両の外に所在する外部装置が送信した指示情報が、所定ＩＤを有するフレームの伝送の阻止を許容しない指示を示す場合には、前記外部装置が所定権限を有することの認証が成功していることを条件として、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容しないことを示すように更新し、

前記指示情報が、前記所定ＩＤを有するフレームの伝送の阻止を許容する指示を示す場合には、前記外部装置が前記所定権限を有するか否かに拘わらず、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容することを示すように更新する

フレーム伝送阻止装置。

【請求項２】

車両に搭載された複数の電子制御ユニットがバスを介して通信する車載ネットワークシステムにおける当該バスに接続される前記車両に搭載されたフレーム伝送阻止装置であって、

前記バスからフレームを受信する受信部と、

フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、

前記管理情報を記憶している記憶部と、

前記記憶部に記憶された前記管理情報を更新する更新部と、

前記受信部により受信されたフレームが前記所定条件を満たす場合に、当該フレームに関する情報を含む分析用情報を前記車両の外に所在する外部装置に送信する通信部とを備え、

前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、

前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、

前記更新部は、前記外部装置が送信した指示情報に応じて前記管理情報を更新する

フレーム伝送阻止装置。

【請求項３】

複数の電子制御ユニットがバスを介して通信するネットワークシステムにおける当該バスに接続されるフレーム伝送阻止装置であって、

前記バスからフレームを受信する受信部と、

フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、

前記管理情報を記憶している記憶部と、

前記記憶部に記憶された前記管理情報を更新する更新部とを備え、

前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、

前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、

前記更新部は、前記受信部により受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しない

ことを示す場合において、当該フレームのＩＤとは異なる特定ＩＤを有する、前記受信部で受信されたフレームに基づいて異常の発生を検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新する
フレーム伝送阻止装置。
【請求項４】
複数の電子制御ユニットがバスを介して通信するネットワークシステムにおける当該バスに接続されるフレーム伝送阻止装置であって、
前記バスからフレームを受信する受信部と、
フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、
前記管理情報を記憶している記憶部と、
前記記憶部に記憶された前記管理情報を更新する更新部とを備え、
前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、
前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、
前記更新部は、前記受信部により受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、前記複数の電子制御ユニットのうち予め定められた特定の電子制御ユニットが異常であることを検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新する
フレーム伝送阻止装置。
【請求項５】
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し、
前記所定条件を満たすフレームの伝送を阻止する前記所定処理は、前記受信部により当該フレームの最後尾のビットが受信される前にエラーフレームを前記バスへ送信する処理を含む
請求項１～４のいずれか一項に記載のフレーム伝送阻止装置。
【請求項６】
前記管理情報における前記複数のＩＤそれぞれに対応するフラグ情報は、前記更新部による更新が一度もなされていない状態では、フレームの伝送の阻止を許容しないことを示す
請求項１～４のいずれか一項に記載のフレーム伝送阻止装置。
【請求項７】
前記フラグ情報は、１ビットの情報である
請求項１～６のいずれか一項に記載のフレーム伝送阻止装置。
【請求項８】
前記フレーム伝送阻止装置は更に、前記処理部が一のＩＤを有するフレームの伝送を阻止する前記所定処理を実行する場合に、当該一のＩＤを有するフレームの伝送の阻止を許容する指示を示す、他の車両向けの指示情報を送信する通信部を備える
請求項１記載のフレーム伝送阻止装置。
【請求項９】
前記所定条件は、フレームのＩＤについての条件であり、
前記処理部は、前記受信部により受信されたフレームのＩＤが前記所定条件を満たす場合において前記管理情報に基づいて前記所定処理を実行するか否かを切り替える

請求項１～８のいずれか一項に記載のフレーム伝送阻止装置。
【請求項１０】
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し、
前記所定条件は、フレームとしてのデータフレームのＤＬＣ（Data Length Code）についての条件であり、
前記処理部は、前記受信部により受信されたフレームのＤＬＣが前記所定条件を満たす場合において前記管理情報に基づいて前記所定処理を実行するか否かを切り替える
請求項１～８のいずれか一項に記載のフレーム伝送阻止装置。
【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し、
前記所定条件は、フレームとしてのデータフレームのデータフィールド内のデータについての条件であり、
前記処理部は、前記受信部により受信されたフレームのデータフィールド内のデータが前記所定条件を満たす場合において前記管理情報に基づいて前記所定処理を実行するか否かを切り替える
請求項１～８のいずれか一項に記載のフレーム伝送阻止装置。
【請求項１２】
前記所定条件は、フレームに適正なメッセージ認証コードが含まれない場合に満たされる条件である
請求項１～８のいずれか一項に記載のフレーム伝送阻止装置。
【請求項１３】
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し、
前記所定条件を満たすフレームの伝送を阻止する前記所定処理は、当該フレームが伝送されている際にドミナント信号を前記バスへ送信する処理を含む
請求項１～４のいずれか一項に記載のフレーム伝送阻止装置。
【請求項１４】
車両に搭載された複数の電子制御ユニットがバスを介して通信する車載ネットワークシステムで用いられるフレーム伝送阻止方法であって、
前記車載ネットワークシステムは、フレームの伝送の阻止を許容するか否かを示す管理情報を記憶する記憶部を備え、
前記フレーム伝送阻止方法は、
前記バスからフレームを受信する受信ステップと、
前記管理情報に基づいて、前記受信ステップで受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理ステップと、
前記記憶部に記憶された前記管理情報を更新する更新ステップとを含み、
前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、
前記処理ステップは、前記受信ステップにより受信されたフレームが前記所定条件を満たす場合において、
　当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、
　当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、
前記更新ステップは、
　前記車両の外に所在する外部装置が送信した指示情報が、所定ＩＤを有するフレームの伝送の阻止を許容しない指示を示す場合には、前記外部装置が所定権限を有することの

認証が成功していることを条件として、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容しないことを示すように更新し、

前記指示情報が、前記所定ＩＤを有するフレームの伝送の阻止を許容する指示を示す場合には、前記外部装置が前記所定権限を有するか否かに拘わらず、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容することを示すように更新する

フレーム伝送阻止方法。

【請求項１５】

車両に搭載された複数の電子制御ユニットがバスを介して通信する車載ネットワークシステムで用いられるフレーム伝送阻止方法であって、

前記車載ネットワークシステムは、フレームの伝送の阻止を許容するか否かを示す管理情報を記憶する記憶部を備え、

前記フレーム伝送阻止方法は、

前記バスからフレームを受信する受信ステップと、

前記管理情報に基づいて、前記受信ステップで受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理ステップと、

前記記憶部に記憶された前記管理情報を更新する更新ステップと、

前記受信ステップにより受信されたフレームが前記所定条件を満たす場合に、当該フレームに関する情報を含む分析用情報を前記車両の外に所在する外部装置に送信する通信ステップとを含み、

前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、

前記処理ステップは、前記受信ステップにより受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、

前記更新ステップは、前記外部装置が送信した指示情報に応じて前記管理情報を更新する

フレーム伝送阻止方法。

【請求項１６】

複数の電子制御ユニットがバスを介して通信するネットワークシステムで用いられるフレーム伝送阻止方法であって、

前記ネットワークシステムは、フレームの伝送の阻止を許容するか否かを示す管理情報を記憶する記憶部を備え、

前記フレーム伝送阻止方法は、

前記バスからフレームを受信する受信ステップと、

前記管理情報に基づいて、前記受信ステップで受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理ステップと、

前記記憶部に記憶された前記管理情報を更新する更新ステップとを含み、

前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、

前記処理ステップは、前記受信ステップにより受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、

前記更新ステップは、前記受信ステップにより受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、当該フレームのＩＤとは異なる特定ＩＤを有する、前記受信ステップで受信されたフレームに基づいて異常の発生を検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新する
フレーム伝送阻止方法。
【請求項１７】
複数の電子制御ユニットがバスを介して通信するネットワークシステムで用いられるフレーム伝送阻止方法であって、
前記ネットワークシステムは、フレームの伝送の阻止を許容するか否かを示す管理情報を記憶する記憶部を備え、
前記フレーム伝送阻止方法は、
前記バスからフレームを受信する受信ステップと、
前記管理情報に基づいて、前記受信ステップで受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理ステップと、
前記記憶部に記憶された前記管理情報を更新する更新ステップとを含み、
前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、
前記処理ステップは、前記受信ステップにより受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、
前記更新ステップは、前記受信ステップにより受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、前記複数の電子制御ユニットのうち予め定められた特定の電子制御ユニットが異常であることを検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新する
フレーム伝送阻止方法。
【請求項１８】
バスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、
前記バスからフレームを受信する受信部と、
フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、
前記管理情報を記憶している記憶部と、
前記記憶部に記憶された前記管理情報を更新する更新部とを備え、
前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、
前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、
　当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、
　当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、
前記更新部は、
　車両の外に所在する外部装置が送信した指示情報が、所定ＩＤを有するフレームの伝送の阻止を許容しない指示を示す場合には、前記外部装置が所定権限を有することの認証

が成功していることを条件として、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容しないことを示すように更新し、

前記指示情報が、前記所定ＩＤを有するフレームの伝送の阻止を許容する指示を示す場合には、前記外部装置が前記所定権限を有するか否かに拘わらず、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容することを示すように更新する

車載ネットワークシステム。

【請求項１９】

バスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、

前記バスからフレームを受信する受信部と、

フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、

前記管理情報を記憶している記憶部と、

前記記憶部に記憶された前記管理情報を更新する更新部と、

前記受信部により受信されたフレームが前記所定条件を満たす場合に、当該フレームに関する情報を含む分析用情報を車両の外に所在する外部装置に送信する通信部とを備え、

前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、

前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、

前記更新部は、前記外部装置が送信した指示情報に応じて前記管理情報を更新する

車載ネットワークシステム。

【請求項２０】

バスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、

前記バスからフレームを受信する受信部と、

フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、

前記管理情報を記憶している記憶部と、

前記記憶部に記憶された前記管理情報を更新する更新部とを備え、

前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、

前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、

前記更新部は、前記受信部により受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、当該フレームのＩＤとは異なる特定ＩＤを有する、前記受信部で受信されたフレームに基づいて異常の発生を検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新する

車載ネットワークシステム。

【請求項２１】
バスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、
前記バスからフレームを受信する受信部と、
フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部と、
前記管理情報を記憶している記憶部と、
前記記憶部に記憶された前記管理情報を更新する更新部とを備え、
前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、
前記処理部は、前記受信部により受信されたフレームが前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行せず、
前記更新部は、前記受信部により受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、前記複数の電子制御ユニットのうち予め定められた特定の電子制御ユニットが異常であることを検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新する
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、車載ネットワークシステム等のネットワークへの不正なフレームの伝送を阻止するセキュリティ対策技術に関する。
【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を繋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、多数の通信規格が存在する。その中でも最も主流な車載ネットワークの一つに、ＩＳＯ１１８９８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本のワイヤで構成されたバスであり、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、データフレームと呼ばれるフレームを送受信する。データフレームを送信する送信ノードは、２本のワイヤに電圧をかけ、ワイヤ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、受け取ったデータ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、送信ノード及び他の受信ノードにデータ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、送信ノードはデータフレーム毎にＩＤ（identifier）を付けて送信し、各受信ノードは予め定められたＩＤのデータフレームのみを受信する。また、ＣＳＭＡ／ＣＡ（Carrier Sense Multiple Access/Collis

ion Avoidance）方式を採用しており、複数ノードの同時送信時にはＩＤによる調停が行われ、ＩＤの値が小さいデータフレームが優先的に送信される。

【０００５】

車載ネットワークシステムについては、攻撃者がバスにアクセスして不正なデータフレーム等の攻撃フレームを送信することでＥＣＵを不正に制御するといった脅威が存在し、セキュリティ対策が検討されている。

【０００６】

例えば特許文献１には、規定された通信間隔内に同一の識別子を有するフレームを２つ受信した場合にその各フレームを破棄して転送しないことで、不正フレームの伝送を阻止する方法が記載されている。また非特許文献１には、複数のノードは同一のＩＤをもつデータフレームを送信しないという前提条件下で、自ノードが送信するＩＤと同一ＩＤのデータフレームの送信を検出した際にエラーフレームを利用して不正なデータフレームの伝送を阻止する方法が記載されている。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開２０１４－１４６８６８号公報

【非特許文献】

【０００８】

【非特許文献１】Ｍａｔｓｕｍｏｔｏ、外４名、「Ａ Ｍｅｔｈｏｄ ｏｆ Ｐｒｅｖｅｎｔｉｎｇ Ｕｎａｕｔｈｏｒｉｚｅｄ Ｄａｔａ Ｔｒａｎｓｍｉｓｓｉｏｎ ｉｎ Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅｔｗｏｒｋ」、Ｖｅｈｉｃｕｌａｒ Ｔｅｃｈｎｏｌｏｇｙ Ｃｏｎｆｅｒｅｎｃｅ（ＶＴＣ Ｓｐｒｉｎｇ）、ＩＥＥＥ、２０１２年

【発明の概要】

【発明が解決しようとする課題】

【０００９】

従来の方法では、例えば車両製造段階等に予め規定されたＩＤ、通信間隔等のルールに基づく条件判定の結果によってフレームの伝送を阻止する。このような方法では、車両製造後等における車載ネットワークシステムを構成するＥＣＵ群の編成の変更、例えばＥＣＵの追加、交換等に適切に対応できず、例えば、追加されたＥＣＵが送信した特段の問題を引き起こさないフレームの伝送を誤って阻止する可能性がある。

【００１０】

そこで、本発明は、ネットワークシステムにおいて、攻撃者により送信された攻撃フレームの伝送の阻止が可能であり、特段の問題を引き起こさないフレームの伝送の阻止を抑制し得るフレーム伝送阻止装置を提供する。また、本発明は、フレームの伝送の阻止を適切に行うためのフレーム伝送阻止方法及び車載ネットワークシステムを提供する。

【課題を解決するための手段】

【００１１】

上記課題を解決するために本発明の一態様に係るフレーム伝送阻止装置は、複数の電子制御ユニットがバスを介して通信するネットワークシステムにおける当該バスに接続されるフレーム伝送阻止装置であって、前記バスからフレームを受信する受信部と、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部とを備えるフレーム伝送阻止装置である。

【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フレーム伝送阻止方法は、複数の電子制御ユニットがバスを介して通信するネットワークシステムで用いられるフレーム伝送阻止方法であって、前記バスからフレームを受信する受信ステップと、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信ステップで受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否

かを切り替える処理ステップとを含むフレーム伝送阻止方法である。
【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車載ネットワークシステムは、バスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、前記バスからフレームを受信する受信部と、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部とを備える車載ネットワークシステムである。
【発明の効果】
【００１４】
本発明によれば、攻撃者により送信された攻撃フレームの伝送が適切に阻止され、特段の問題を引き起こさないフレームの伝送の阻止が抑制され得る。
【図面の簡単な説明】
【００１５】
【図１】実施の形態１に係る車載ネットワークシステムの構成を示す図である。
【図２】ＣＡＮプロトコルで規定されるデータフレームのフォーマットを示す図である。
【図３】ＣＡＮプロトコルで規定されるエラーフレームのフォーマットを示す図である。
【図４】実施の形態１に係るＥＣＵの構成図である。
【図５】実施の形態１に係るＥＣＵにおける受信ＩＤリストの一例を示した図である。
【図６】実施の形態１に係るエンジンＥＣＵが送信するデータフレームのＩＤ及びデータの一例を示す図である。
【図７】実施の形態１に係るブレーキＥＣＵが送信するデータフレームのＩＤ及びデータの一例を示す図である。
【図８】実施の形態１に係るドア開閉センサＥＣＵが送信するデータフレームのＩＤ及びデータの一例を示す図である。
【図９】実施の形態１に係るウィンドウ開閉センサＥＣＵが送信するデータフレームのＩＤ及びデータの一例を示す図である。
【図１０】実施の形態１に係る不正検知ＥＣＵの構成図である。
【図１１】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の一例を示す図である。
【図１２】実施の形態１に係る不正検知ＥＣＵが保持する管理情報の一例を示す図である。
【図１３】実施の形態１に係るサーバの構成図である。
【図１４】実施の形態１に係る不正検知ＥＣＵによる不正フレームの検知及び伝送阻止のシーケンスの一例を示す図である。
【図１５】実施の形態１に係る不正検知ＥＣＵにおける動作不良検知処理の一例を示すフローチャートである。
【図１６】実施の形態１に係る不正検知ＥＣＵが送信する不正検知メッセージのフォーマット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における伝送阻止機能のアクティベートに係る更新処理の一例を示すフローチャートである。
【図１８】実施の形態１に係るサーバが送信するファームウェア（ＦＷ：firmware）を含む配信メッセージのフォーマットの一例を示す図である。
【図１９】実施の形態２に係る車載ネットワークシステムの構成を示す図である。
【図２０】実施の形態２に係る不正検知ＥＣＵの構成図である。
【図２１】実施の形態２に係るサーバの構成図である。
【図２２】実施の形態２に係る不正検知ＥＣＵによる不正フレームの検知及び伝送阻止のシーケンスの一例を示す図である。
【図２３】実施の形態２に係る不正検知ＥＣＵにおける動作不良検知処理の一例を示すフローチャートである。

【図２４】実施の形態２に係る不正検知ＥＣＵが車車間通信で送信する異常通知メッセージのフォーマットの一例を示す図である。
【図２５】実施の形態２に係る不正検知ＥＣＵがサーバに送信する不正検知メッセージのフォーマットの一例を示す図である。
【図２６】実施の形態２に係る不正検知ＥＣＵにおける伝送阻止機能アクティベーション処理の一例を示すフローチャートである。
【図２７】実施の形態２に係るサーバにおけるディアクティベーションメッセージの送信に係る処理の一例を示すフローチャートである。
【図２８】実施の形態２に係るサーバが送信するディアクティベーションメッセージのフォーマットの一例を示す図である。
【図２９】実施の形態２に係る不正検知ＥＣＵにおける伝送阻止機能ディアクティベーション処理の一例を示すフローチャートである。
【図３０】変形例に係るフレーム伝送阻止装置の構成図である。
【発明を実施するための形態】
【００１６】
本発明の一態様に係るフレーム伝送阻止装置は、複数の電子制御ユニットがバスを介して通信するネットワークシステムにおける当該バスに接続されるフレーム伝送阻止装置であって、前記バスからフレームを受信する受信部と、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部とを備えるフレーム伝送阻止装置である。このフレーム伝送阻止装置は、攻撃フレーム以外の特段の問題（例えばネットワークシステムの動作不良等）を引き起こさないフレームの伝送の阻止の抑制を実現するために有用な構成を備えている。このフレーム伝送阻止装置によれば、攻撃者により送信された攻撃フレームの伝送の阻止が可能となり、攻撃フレーム以外の特段の問題を引き起こさないフレームの伝送の阻止の抑制を実現し得る。例えば、製造段階でのネットワークシステムについて規定したルールから外れる不正なフレームが該当するように所定条件を定めてフレーム伝送阻止装置を製造して利用することが想定される。この場合において、フレーム伝送阻止装置は、その所定条件を満たすフレームの伝送を単純に阻止するのではなく、管理情報によって阻止するか否かが変更され得る。このため、フレーム伝送阻止装置の製造後においても、ネットワークシステムにおけるＥＣＵの追加等に対応して管理情報を変更すれば、追加されたＥＣＵが送信する特段の問題を引き起こさないフレームを、不正な攻撃フレームと誤検知して伝送阻止するような事態を防止できる。なお、フレーム伝送阻止装置が参照する管理情報は、例えば、フレーム伝送阻止装置外から受信されても良いし、例えば、フレーム伝送阻止装置内の記憶媒体等から読み出されても良い。
【００１７】
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し、前記所定条件を満たすフレームの伝送を阻止する前記所定処理は、前記受信部により当該フレームの最後尾のビットが受信される前にエラーフレームを前記バスへ送信する処理を含むこととしても良い。これにより、伝送阻止の対象となる所定条件を満たすフレームを管理情報に基づいて阻止することとした場合に、バス上でのそのフレームの伝送をエラーフレームの送信によって効率的に阻止することが可能となる。また、管理情報によって、特段の問題を引き起こさないフレームの伝送がエラーフレームによって阻止されることを抑制できるので、そのフレームの再送によるトラフィックの増大等といったその阻止の悪影響が抑制される。
【００１８】
また、前記フレーム伝送阻止装置は、前記管理情報を記憶している記憶部と、前記記憶部に記憶された前記管理情報を更新する更新部とを備え、前記管理情報は、複数のＩＤそれぞれに対応して、当該ＩＤを有し前記所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含み、前記処理部は、前記受信部により受信されたフレーム

が前記所定条件を満たす場合において、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容することを示すときには前記所定処理を実行し、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示すときには前記所定処理を実行しないこととしても良い。これにより、例えばフレームの内容であるデータの種別等を識別する、フレームが有するＩＤ（identifier）毎に、フレームの伝送阻止を許容するか否かを変更することが可能となる。

【００１９】

また、前記管理情報における前記複数のＩＤそれぞれに対応するフラグ情報は、前記更新部による更新が一度もなされていない状態では、フレームの伝送の阻止を許容しないことを示すこととしても良い。これにより、フレームの伝送の阻止による弊害が抑制され得る。例えば、更新部に、ネットワークシステムに追加されたＥＣＵが送信するフレームと同じＩＤのフレームによりネットワークシステム等に動作不良等の異常が生じた場合にそのＩＤに対応するフラグ情報を、伝送阻止を許容することを示すように更新させるような運用が想定される。この例では、動作不良等の異常が生じない限りそのフレームの伝送が阻止されないので、阻止による弊害が生じない。

【００２０】

また、前記フラグ情報は、１ビットの情報であることとしても良い。これにより、ＩＤ毎のフラグ情報を含む管理情報の記憶に必要な記憶媒体の容量を小さく抑えることが可能となる。

【００２１】

また、前記更新部は、前記フレーム伝送阻止装置が外部から受信した指示情報に応じて前記管理情報を更新することとしても良い。これにより、フレーム伝送阻止装置に対して、ネットワークシステム内の電子制御ユニット等の装置或いはネットワークシステム外の装置等から必要に応じて指示情報を与えてフレームの伝送阻止機能の実行を制御することが可能となる。この場合には、フレーム伝送阻止装置は、例えば管理情報を更新すべきか否かを適切に判定するための構成を有さなくても良い。

【００２２】

また、前記ネットワークシステムは、車載ネットワークシステムであり、前記複数の電子制御ユニットと前記バスと前記フレーム伝送阻止装置とは車両に搭載され、前記更新部は、前記車両の外に所在する外部装置が送信した前記指示情報に応じて前記管理情報を更新することとしても良い。これにより、車両の外部のサーバ装置、他の車両等によって、必要に応じて指示情報を与えてフレームの伝送阻止機能の実行を制御することが可能となる。例えば、フレーム伝送阻止装置によるフレームの伝送阻止機能の実行を、複数の車両から情報を収集して分析することで適切に指示情報を決定するサーバ装置等により制御するような運用が可能となる。指示情報として、例えば、フレーム伝送阻止装置におけるフレームの伝送阻止機能をアクティベートする指示つまり伝送阻止を許容するようにする指示、或いは、伝送阻止機能をディアクティベートする指示つまり伝送阻止を許容しないようにする指示等が想定される。

【００２３】

また、前記更新部は、前記外部装置が送信した前記指示情報が、所定ＩＤを有するフレームの伝送の阻止を許容しない指示を示す場合には、前記外部装置が所定権限を有することの認証が成功していることを条件として、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容しないことを示すように更新し、前記指示情報が、前記所定ＩＤを有するフレームの伝送の阻止を許容する指示を示す場合には、前記外部装置が前記所定権限を有するか否かに拘わらず、前記管理情報における前記所定ＩＤに対応するフラグ情報を、前記所定ＩＤを有するフレームの伝送の阻止を許容することを示すように更新することとしても良い。これにより、攻撃者による攻撃の可能性に鑑みて防御のためにフレームの伝送阻止を一旦許容したような場合において、その許容を止めるためには所定権限を必要とするので、ネットワークシステムのセキュリティが高まる。

【００２４】
また、前記フレーム伝送阻止装置は更に、前記処理部が一のＩＤを有するフレームの伝送を阻止する前記所定処理を実行する場合に、当該一のＩＤを有するフレームの伝送の阻止を許容する指示を示す、他の車両向けの指示情報を送信する通信部を備えることとしても良い。このフレーム伝送阻止装置は、例えば、自装置が搭載された車両の車載ネットワークシステムに対して、攻撃者による攻撃フレームの送信がなされた場合に、指示情報の送信により、同様のフレーム伝送阻止装置を搭載した他の車両を同様の攻撃から保護し得る。
【００２５】
また、前記フレーム伝送阻止装置は更に、前記受信部により受信されたフレームが前記所定条件を満たす場合に、当該フレームに関する情報を含む分析用情報を前記外部装置に送信する通信部を備えることとしても良い。これにより、例えば、所定条件を満たすフレームの伝送が特段の問題を引き起こすことになるか否かの判別のための分析に必要な分析用情報を外部装置に送信できる。例えば、外部装置であるサーバ装置等によって複数の車両から分析用情報を収集して分析することで適切に指示情報を決定するような運用が可能となる。分析用情報を活用した結果として外部装置が指示情報を送信すれば、フレーム伝送阻止装置は、その指示情報を受信して管理情報を更新し得る。
【００２６】
また、前記更新部は、前記受信部により受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、当該フレームのＩＤとは異なる特定ＩＤを有する、前記受信部で受信されたフレームに基づいて異常の発生を検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新することとしても良い。これにより、所定条件を満たすフレームの伝送がバスを流れる他の種類のフレームに異常をもたらしているような、特段の問題を引き起こすフレームの伝送を、フレーム伝送阻止装置が適切に阻止し得る。例えば、製造段階等でネットワークシステムにおいて用いられるフレームのＩＤを特定ＩＤとして用いるようにフレーム伝送阻止装置を製造することが想定される。また、例えば、製造段階等でネットワークシステムにおいて重要なデータに係るフレームのＩＤが規定されている場合にそのＩＤを特定ＩＤとして用いることが想定される。
【００２７】
また、前記更新部は、前記受信部により受信されたフレームが前記所定条件を満たし、かつ、当該フレームのＩＤに対応する前記フラグ情報が当該フレームの伝送の阻止を許容しないことを示す場合において、前記複数の電子制御ユニットのうち予め定められた特定の電子制御ユニットが異常であることを検出したときには、当該フラグ情報を、前記阻止を許容することを示すように更新することとしても良い。これにより、所定条件を満たすフレームの伝送が特定のＥＣＵに異常をもたらしているような、特段の問題を引き起こすフレームの伝送を、フレーム伝送阻止装置が適切に阻止し得る。例えば、製造段階等でネットワークシステムが備えるＥＣＵを特定のＥＣＵとして用いるようにフレーム伝送阻止装置を製造することが想定される。また、例えば、ネットワークシステムにおいて重要なＥＣＵ、例えば車載ネットワークシステムであれば車両の走行制御に関わるＥＣＵを、特定のＥＣＵとして用いることが想定される。
【００２８】
また、前記所定条件は、フレームのＩＤについての条件であり、前記処理部は、前記受信部により受信されたフレームのＩＤが前記所定条件を満たす場合において前記管理情報に基づいて前記所定処理を実行するか否かを切り替えることとしても良い。これにより、例えば、構築されたネットワークシステムで利用されないフレームのＩＤつまり不正と推定されるＩＤ群等を示すように所定条件を定めておくと、管理情報に基づいて、攻撃者によってバスに送信された攻撃フレームの伝送阻止が実現され得る。この攻撃フレームの伝送阻止により、ネットワークシステムのセキュリティが確保される。
【００２９】

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し、前記所定条件は、フレームとしてのデータフレームのＤＬＣ（Data Length Code）についての条件であり、前記処理部は、前記受信部により受信されたフレームのＤＬＣが前記所定条件を満たす場合において前記管理情報に基づいて前記所定処理を実行するか否かを切り替えることとしても良い。これにより、例えば、構築されたネットワークシステムで利用されないＤＬＣつまり不正と推定されるＤＬＣを示すように所定条件を定めておくと、管理情報に基づいて、攻撃者によってバスに送信された、そのＤＬＣを含む攻撃フレームの伝送阻止が実現され得る。

【００３０】

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し、前記所定条件は、フレームとしてのデータフレームのデータフィールド内のデータについての条件であり、前記処理部は、前記受信部により受信されたフレームのデータフィールド内のデータが前記所定条件を満たす場合において前記管理情報に基づいて前記所定処理を実行するか否かを切り替えることとしても良い。これにより、例えば、不正と推定されるデータを示すように所定条件を定めておくと、管理情報に基づいて、攻撃者によってバスに送信された、そのデータを含む攻撃フレームの伝送阻止が実現され得る。

【００３１】

また、前記所定条件は、フレームに適正なメッセージ認証コードが含まれない場合に満たされる条件であることとしても良い。これにより、管理情報に基づいて、攻撃者によってバスに送信された、適正なメッセージ認証コードを含まない攻撃フレームの伝送阻止が実現され得る。

【００３２】

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し、前記所定条件を満たすフレームの伝送を阻止する前記所定処理は、当該フレームが伝送されている際にドミナント信号を前記バスへ送信する処理を含むこととしても良い。これにより、伝送阻止の対象となる所定条件を満たすフレームを管理情報に基づいて阻止することとした場合に、バス上でのそのフレームの完全な状態での伝送を、ドミナント信号の送信でそのフレームの内容を上書きして改変することによって阻止し得る。バス上のフレームの内容の改変は、例えば受信エラー等を引き起こし、受信ノードのＥＣＵにおいてそのフレームを正常なフレームと同様に処理することが防止され得る。

【００３３】

また、本発明の一態様に係るフレーム伝送阻止方法は、複数の電子制御ユニットがバスを介して通信するネットワークシステムで用いられるフレーム伝送阻止方法であって、前記バスからフレームを受信する受信ステップと、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信ステップで受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理ステップとを含むフレーム伝送阻止方法である。これにより、管理情報に基づいてフレームの伝送阻止に係る所定処理の実行が制御されるので、攻撃者により送信された攻撃フレームの伝送阻止の実現が可能となり、攻撃フレーム以外の特段の問題を引き起こさないフレームの伝送阻止の抑制の実現が可能となり得る。

【００３４】

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、バスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、前記バスからフレームを受信する受信部と、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、前記受信部により受信されたフレームが所定条件を満たす場合に当該フレームの伝送を阻止する所定処理を実行するか否かを切り替える処理部とを備える車載ネットワークシステムである。これにより、車載ネットワークに対して攻撃者により送信された攻撃フレームの伝送阻止の実現が可能となり、攻撃フレーム以外の特段の問題を引き起こさないフレ

ームの伝送阻止の抑制の実現が可能となり得る。

【００３５】

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。

【００３６】

以下、実施の形態に係るフレーム伝送阻止方法を用いるフレーム伝送阻止装置を含む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、処理の要素としてのステップ及びステップの順序等は、一例であって本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。

【００３７】

（実施の形態１）

以下、本発明の実施の形態１として、ＣＡＮプロトコルに従って通信を行う複数のＥＣＵと、不正と検知したデータフレームの伝送を阻止する機能を有するフレーム伝送阻止装置としての不正検知ＥＣＵとを含む車載ネットワークシステム１０について、図面を用いて説明する。

【００３８】

［１．１　車載ネットワークシステム１０の構成］

図１は、車両に搭載された車載ネットワークシステム１０の構成を示す図である。なお、同図には、他の車両及び車外のサーバ５００を付記している。

【００３９】

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システムの一例であり、制御装置、センサ、アクチュエータ、ユーザインタフェース装置等の各種機器が搭載された車両（例えば自動車）におけるネットワークシステムである。車載ネットワークシステム１０は、バス（ネットワークバス）を介してフレームに係る通信を行う複数のＥＣＵを備え、一定条件下でフレームの伝送を阻止するフレーム伝送阻止方法を用いる。具体的には図１に示すように車載ネットワークシステム１０は、バス２００と、バス２００に接続されたＥＣＵ１００ａ～１００ｄ及び不正検知ＥＣＵ４００と、通信モジュール６００とを含んで構成される。なお、車載ネットワークシステム１０には、不正検知ＥＣＵ４００及びＥＣＵ１００ａ～１００ｄ以外にもいくつものＥＣＵが含まれ得るが、ここでは、便宜上、不正検知ＥＣＵ４００及びＥＣＵ１００ａ～１００ｄに注目して説明を行う。ＥＣＵ１００ａをエンジンＥＣＵ１００ａとも称し、ＥＣＵ１００ｂをブレーキＥＣＵ１００ｂとも称し、ＥＣＵ１００ｃをドア開閉センサＥＣＵ１００ｃとも称し、ＥＣＵ１００ｄをウィンドウ開閉センサＥＣＵ１００ｄとも称する。

【００４０】

各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、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。各ＥＣＵは、ＣＡＮプロトコルに従って、バス２００を介してフレームの授受を行い得る。ＥＣＵ間で授受されるフレームにはデータフレームがある。データフレームは、例えば、車両の状態に関するデータ、車両に対して制御を指示するデータ等といった、車両の制御のために用いられるデータ等を含み得る。各ＥＣＵは、各種機器に接続され得る。エン

ジンＥＣＵ１００ａは、エンジン３１０と接続されており、エンジン３１０の状態を示すデータフレームを周期的にバス２００に送信する。ブレーキＥＣＵ１００ｂは、ブレーキ３２０と接続されており、ブレーキ３２０の状態を示すデータフレームを周期的にバス２００に送信する。ドア開閉センサＥＣＵ１００ｃは、ドア開閉センサ３３０と接続されており、ドア開閉センサ３３０により検知されたドアの開閉状態を示すデータフレームを周期的にバス２００に送信する。また、ウィンドウ開閉センサＥＣＵ１００ｄは、ウィンドウ開閉センサ３４０と接続されており、ウィンドウ開閉センサ３４０により検知されたウィンドウの開閉状態を示すデータフレームを周期的にバス２００に送信する。

【００４１】

不正検知ＥＣＵ４００は、フレーム伝送阻止装置として機能する一種のＥＣＵであり、バス２００に接続される。不正検知ＥＣＵ４００は、バス２００に流れるデータフレームを監視し、予め定められた不正なフレームに関する所定条件を満たすデータフレームを検知した場合に、所定の管理情報に基づいてそのフレームの伝送を阻止する所定処理を実行する機能（伝送阻止機能と称する）を有する。

【００４２】

通信モジュール６００は、サーバ５００と通信するための通信回路を含むモジュールであり、不正検知ＥＣＵ４００にＵＳＢ（Universal Serial Bus）等のインタフェースにより直接接続している。

【００４３】

車載ネットワークシステム１０は、複数の車両それぞれに搭載され得る。

【００４４】

サーバ５００は、複数の車両と通信し得る、車両外部に所在するサーバ装置としてのコンピュータである。例えば、サーバ５００と複数の車両とで車両管理システムを形成している。サーバ５００は、有線又は無線の通信網を介して、複数の車両それぞれにおける不正検知ＥＣＵ４００に接続された通信モジュール６００と通信する。サーバ５００は、不正検知ＥＣＵ４００のファームウェア（ＦＷ）を更新するために、不正検知ＥＣＵ４００に対して、更新用のＦＷを含む配信メッセージを送信する機能を有する。

【００４５】

［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データフレームについて説明する。

【００４６】

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）で構成される。

【００４７】

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が、フレームの送信開始の通知となる。

【００４８】

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。

【００４９】

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。
【００５０】
ＩＤＥと「ｒ」とは、両方ドミナント１ｂｉｔで構成される。
【００５１】
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。
【００５２】
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。データフィールドは、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において定められる。従って、車種、製造者等に依存した仕様となる。
【００５３】
ＣＲＣシーケンスは、１５ｂｉｔで構成される。ＣＲＣシーケンスは、ＳＯＦ、ＩＤフィールド、コントロールフィールド及びデータフィールドの送信値より算出される。
【００５４】
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。
【００５５】
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。
【００５６】
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。
【００５７】
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。
【００５８】
［１．３　エラーフレームフォーマット］
図３は、ＣＡＮプロトコルで規定されるエラーフレームのフォーマットを示す図である。エラーフレームは、エラーフラグ（プライマリ）と、エラーフラグ（セカンダリ）と、エラーデリミタ「ＤＥＬ」とから構成される。
【００５９】
エラーフラグ（プライマリ）は、エラーの発生を他のノードに知らせるために使用される。エラーを検知したノードはエラーの発生を他のノードに知らせるために６ｂｉｔのドミナントを連続で送信する。この送信は、ＣＡＮプロトコルにおけるビットスタッフィングルール（つまり連続して同じ値を６ｂｉｔ以上送信しないルール）に違反し、他のノードからのエラーフレーム（セカンダリ）の送信を引き起こす。
【００６０】
エラーフラグ（セカンダリ）は、エラーの発生を他のノードに知らせるために使用される連続した６ビットのドミナントで構成される。エラーフラグ（プライマリ）を受信してビットスタッフィングルール違反を検知した全てのノードがエラーフラグ（セカンダリ）を送信することになる。
【００６１】
エラーデリミタ「ＤＥＬ」は、８ｂｉｔの連続したレセシブであり、エラーフレームの終了を示す。
【００６２】
［１．４　ＥＣＵ１００ａの構成］
図４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、例えばＥＣＵ１００ａにおける通信回路、メモリに格納されたプログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、ＥＣＵ１００ｂ～１００ｄも、ＥＣＵ１００ａと同様の構成を備える。

【００６３】

フレーム送受信部１１０は、バス２００に対して、ＣＡＮのプロトコルに従ったフレームを送受信する。バス２００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２００に送信する。通信調停といったＣＡＮのプロトコルに則った処理も、フレーム送受信部１１０において実現される。

【００６４】

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、或いは、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。

【００６５】

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。

【００６６】

受信ＩＤリスト保持部１４０は、ＥＣＵ１００ａが受信するＩＤのリストである受信ＩＤリストを保持する。図５に、受信ＩＤリストの一例を示す。

【００６７】

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。エンジン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、エンジンＥＣＵ１００ａのフレーム処理部１５０は、例えば、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３１０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。ＥＣＵ１００ａと同様の構成を備えるＥＣＵ１００ｃのフレーム処理部１５０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処理等を行う。なお、フレーム処理部１５０は、ここで例示した以外のフレームのデータに係る処理を行っても良い。

【００６８】

データ取得部１７０は、ＥＣＵに繋がっている機器、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。

【００６９】

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ＩＤをつけてデータフレームを構成し、フレーム送受信部１１０へ通知する。なお、ＥＣＵ１００ａ～１００ｄ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６～図９を用いて説明する。

【００７０】

［１．５　受信ＩＤリスト例］

図５は、ＥＣＵ１００ａ～１００ｄ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の値が、全て（ＡＬＬ）であることを示すＩＤリストとなっている。この例は、ＥＣＵが、いかなるＩＤを含むデータフレームも、バス２００から受信する例を示している。

【００７１】

［１．６　エンジンＥＣＵ１００ａの送信フレーム例］

図６は、エンジン３１０に接続されたエンジンＥＣＵ１００ａから送信されるデータフレームにおけるＩＤ及びデータフィールドのデータの一例を示す図である。エンジンＥＣＵ１００ａが送信するデータフレームの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６の上行から下行へと、エンジンＥＣＵ１００ａから逐次送信される各データフレームに対応する各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。

【００７２】

［１．７　ブレーキＥＣＵ１００ｂの送信フレーム例］

図７は、ブレーキ３２０に接続されたブレーキＥＣＵ１００ｂから送信されるデータフレームにおけるＩＤ及びデータフィールドのデータの一例を示す図である。ブレーキＥＣＵ１００ｂが送信するデータフレームの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７の上行から下行へと、ブレーキＥＣＵ１００ｂから逐次送信される各データフレームに対応する各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。

【００７３】

［１．８　ドア開閉センサＥＣＵ１００ｃの送信フレーム例］

図８は、ドア開閉センサ３３０に接続されたドア開閉センサＥＣＵ１００ｃから送信されるデータフレームにおけるＩＤ及びデータフィールド（データ）の一例を示す図である。ドア開閉センサＥＣＵ１００ｃが送信するデータフレームの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８の上行から下行へと、ドア開閉センサＥＣＵ１００ｃから逐次送信される各データフレームに対応する各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。

【００７４】

［１．９　ウィンドウ開閉センサＥＣＵ１００ｄの送信フレーム例］

図９は、ウィンドウ開閉センサ３４０に接続されたウィンドウ開閉センサＥＣＵ１００ｄから送信されるデータフレームにおけるＩＤ及びデータフィールド（データ）の一例を示す図である。ウィンドウ開閉センサＥＣＵ１００ｄが送信するデータフレームのＩＤは「４」である。データは、窓（ウィンドウ）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９の上行から下行へと、ウィンドウ開閉センサＥＣＵ１００ｄから逐次送信される各データフレームに対応する各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。

【００７５】

［１．１０　不正検知ＥＣＵ４００の構成］

図１０は、不正検知ＥＣＵ４００の構成図である。不正検知ＥＣＵ４００は、フレーム送受信部４１０と、フレーム解釈部４２０と、不正検知処理部４３０、不正検知ルール保持部４３１、状態確認部４４０と、状態保持部４４１と、フレーム生成部４５０と、更新処理部４６０と、外部通信部４７０と、署名処理部４８０と、鍵保持部４８１と、車種情報保持部４９１と、車台番号情報保持部４９２とを含んで構成される。これらの各構成要素の各機能は、例えば不正検知ＥＣＵ４００における通信回路、メモリに格納されたプログラムを実行するプロセッサ或いはデジタル回路等により実現される。

【００７６】

フレーム送受信部４１０は、バス２００に対して、ＣＡＮプロトコルに従ったフレームを送受信する。フレーム送受信部４１０は、バスからフレームを１ｂｉｔずつ受信する受信部として機能し、受信したフレームをフレーム解釈部４２０に転送する。また、フレーム生成部４５０より通知を受けたフレームに基づいて、そのフレームの内容をバス２００に１ｂｉｔずつ送信する。

【００７７】

フレーム解釈部４２０は、フレーム送受信部４１０より受信されたフレームの値を受け取り、ＣＡＮプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。フレーム解釈部４２０は、受信されたデータフレームにおけるＩＤフィールドと判断した値つまりＩＤを、不正検知処理部４３０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４５０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。

【００７８】

不正検知処理部４３０は、フレーム解釈部４２０から通知されるＩＤフィールドの値を受け取り、つまり不正検知ＥＣＵ４００が受信したデータフレームのＩＤを受け取る。不正検知処理部４３０は、受け取ったＩＤについて不正か否かの判定を、不正検知ルール保持部４３１に保持している不正検知ルールを表す正規ＩＤリストに従って行う。不正検知処理部４３０は、不正と判定した場合つまり不正を検知した場合に、状態確認部４４０へ通知する。不正検知ＥＣＵ４００では、不正検知処理部４３０で不正と検知されたＩＤを有する受信中のデータフレームが、不正なデータフレームと検知されることになる。なお、検知された不正なデータフレームは、予め定められて不正検知ルール保持部４３１に保持された不正検知ルールに基づいて、不正と判定されたものに過ぎない。不正検知ルールは、例えば、不正である可能性が高いデータフレームをその他のデータフレームと区別して不正を検知するために規定され得る。不正検知ルールは、例えば、完全に誤検知が生じないように規定されなくても、攻撃の防御を安全に行う見地から規定されても良い。また、車載ネットワークシステム１０へのＥＣＵの追加その他の状況の変化によって、不正か否かを的確に区別することが困難となり得る。このため、不正検知ルールに基づいて不正と判定されたデータフレームは、例えば不正と推定されるものの、必ずしも車載ネットワークシステム１０に悪影響を及ぼすものとは限らず、必ずしもそのデータフレームのデータが不正であるとは限らない。

【００７９】

不正検知ルール保持部４３１は、不正検知ＥＣＵ４００が受信するデータフレームに含まれるＩＤが不正か否かを示す不正検知ルールに係る情報を保持する。図１１に、不正検知ルールの一例を示す。

【００８０】

状態確認部４４０は、不正検知処理部４３０によって不正なデータフレームが検知された場合に、状態保持部４４１が保持する管理情報が示す伝送阻止機能のアクティベートに係る状態を確認する。伝送阻止機能がアクティベートされた状態は、伝送阻止機能の実行が許容された状態、つまり不正検知処理部４３０によって不正と検知されたデータフレー

ムの、車載ネットワークでの伝送の阻止が許容された状態である。伝送阻止機能がアクティベートされていない状態は、伝送阻止機能の実行が許容されていない状態、つまり不正検知処理部４３０によって不正と検知されたデータフレームの、車載ネットワークでの伝送の阻止が許容されていない状態である。状態確認部４４０は、不正なデータフレームが検知された場合に、伝送阻止機能がアクティベートされた状態であれば、フレーム生成部４５０へエラーフレームを送信するよう通知する。状態確認部４４０は、不正なデータフレームが検知された場合において、不正伝送阻止機能がアクティベートされていない状態であれば、車両の状態を確認し、動作不良等といった異常が検知されたときには、外部通信部４７０に、不正と検知されたデータフレームに関するログ情報を通知する。

【００８１】

状態保持部４４１は、例えば不揮発性メモリ等の記憶媒体の一領域で実現され、伝送阻止機能のアクティベートに係る状態を示す管理情報を保持する。図１２に、管理情報の一例を示す。

【００８２】

フレーム生成部４５０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４５０は、状態確認部４４０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。

【００８３】

更新処理部４６０は、更新処理を行う。更新処理は、外部通信部４７０からＦＷを取得して、ＦＷによって状態保持部４４１が保持する管理情報の更新を行う処理である。なお、更新処理部４６０は、外部通信部４７０から取得したＦＷによって、管理情報に加えて或いは管理情報の代わりに、不正検知ルールの更新を行うこととしても良い。更新処理部４６０でのＦＷによる管理情報の更新は、例えば、プロセッサに、管理情報を更新するためのＦＷを実行させることで実現され、或いは、新たな管理情報の内容を示すデータを含むＦＷのそのデータを、状態保持部４４１に管理情報として保持させることで実現される。

【００８４】

外部通信部４７０は、通信モジュール６００を介してサーバ５００と通信し、配信メッセージを取得する。外部通信部４７０は、取得した配信メッセージを署名処理部４８０へ通知して配信メッセージの署名の検証結果を取得し、検証が成功していれば配信メッセージにおけるＦＷを更新処理部４６０へ通知する。また、外部通信部４７０は、状態確認部４４０から通知されたデータフレームに関するログ情報に、車種情報保持部４９１より取得した車種情報と、車台番号情報保持部４９２より取得した車台番号情報とを付加して、署名なし不正検知メッセージを生成する。不正検知メッセージは、不正と検知されたデータフレームに関するログ情報を含み、例えば車載ネットワークシステム１０に異常が生じているか否か等について、サーバ５００で分析されるべき分析用情報である。外部通信部４７０は、署名なし不正検知メッセージを、署名処理部４８０に通知して署名データを取得することで署名付きの不正検知メッセージに変換し、その署名付きの不正検知メッセージを、通信モジュール６００を介してサーバ５００へと送信する。

【００８５】

署名処理部４８０は、外部通信部４７０から通知された署名付きの配信メッセージを、鍵保持部４８１から取得する鍵を用いて検証し、検証結果を外部通信部４７０へ通知する。また、署名処理部４８０は、外部通信部４７０から通知された署名なし不正検知メッセージに対して、鍵保持部４８１から取得する鍵を用いて署名データを生成し、生成した署名データを外部通信部４７０へ通知する。

【００８６】

鍵保持部４８１は、署名処理部４８０が利用する鍵を保持する。

【００８７】

車種情報保持部４９１は、不正検知ＥＣＵ４００を搭載している車両の車種を示す車種情報を保持する。

【００８８】

車台番号情報保持部４９２は、不正検知ＥＣＵ４００を搭載している車両の識別用の情報としての車台番号情報を保持する。車台番号情報は、例えば、車両形式と製造番号とを示す。

【００８９】

［１．１１　不正検知ルール］

図１１は、不正検知ＥＣＵ４００の不正検知ルール保持部４３１が保持する不正検知ルールの一例を示す。

【００９０】

同図の例の不正検知ルールに係る正規ＩＤリストは、所謂ホワイトリストである。この例の正規ＩＤリストは、バス２００に、「１」、「２」、「３」、「４」のいずれかであるＩＤを有するデータフレームが送信されても不正と判定されず、その他のＩＤを有するデータフレームが送信されると不正と判定（つまり不正と検知）されるという不正検知ルールを表す。

【００９１】

［１．１２　管理情報］

図１２は、不正検知ＥＣＵ４００の状態保持部４４１が保持する管理情報の一例を示す。管理情報は、伝送阻止機能の実行が許容されているか否かを示す情報である。

【００９２】

図１２の例では、管理情報は、データフレームのＩＤ毎に、そのＩＤを有するデータフレームが不正検知ルールによって不正と検知された場合にそのデータフレームの伝送を阻止する伝送阻止機能を実行が許容されるか否かを示すフラグ情報を対応付けている。

【００９３】

フラグ情報は、例えば１ビットで構成され、例えば、ビット値が１であれば伝送阻止機能の実行が許容されることを示し、ビット値が０であれば伝送阻止機能の実行が許容されないことを示す。一例としては、更新処理部４６０による管理情報の更新が一度もなされていない状態では、フラグ情報が、データフレームの伝送の阻止を許容しないことを示すようにしても良い。

【００９４】

図１２の例では、ＩＤ「１」用フラグ情報は、ビット値が０であって、伝送阻止機能の実行が許容されていない状態を示している。これは、ＩＤ「１」のデータフレームについては不正検知ＥＣＵ４００の伝送阻止機能がアクティベートされていない状態を表す。また、図１２の例では、ＩＤ「５」用フラグ情報は、ビット値が１であって、伝送阻止機能の実行が許容されている状態を示している。これは、ＩＤ「５」のデータフレームについては不正検知ＥＣＵ４００の伝送阻止機能がアクティベートされた状態を表す。また、例えば図１２の例でＩＤ「６」用フラグ情報のビット値が０であることは、バス２００に流れるＩＤ「６」のデータフレームが不正と検知された場合においてそのデータフレームの伝送の阻止が許容されないことを意味する。例えば、ＩＤ「６」用フラグ情報のビット値を１に変化させると、バス２００に流れるＩＤ「６」のデータフレームが不正と検知された場合においてそのデータフレームの伝送の阻止が許容されることになる。

【００９５】

なお、フラグ情報のビット値の０と１との意味を逆にしても良いし、フラグ情報を複数ビット列で構成しても良い。また、管理情報は、不正検知ルールによって不正と検知されたデータフレームが、いかなるＩＤを有する場合であっても一括して、伝送阻止機能を実行するか否かを切り替えるための１つのフラグ情報だけで構成されても良い。

【００９６】

［１．１３　サーバ５００の構成］

サーバ５００は、メモリ、ハードディスク等の記憶媒体、プロセッサ、通信回路等を含

む。

【００９７】

図１３は、サーバ５００の構成図である。サーバ５００は、機能面の構成要素として、通信部５１０と、分析部５２０と、ＦＷ保持部５３０と、配信メッセージ生成部５４０と、署名処理部５５０と、鍵保持部５６０とを含んで構成される。これらの各構成要素は、サーバ５００における通信回路、メモリに格納されたプログラムを実行するプロセッサ等により実現される。

【００９８】

通信部５１０は、配信メッセージ生成部５４０から伝えられた配信メッセージを、車両に対して送信する。この配信メッセージは、車両の通信モジュール６００で受信され、不正検知ＥＣＵ４００に伝えられる。また、通信部５１０は、車両の不正検知ＥＣＵ４００から通信モジュール６００を介して送信された不正検知メッセージを受信し、分析部５２０へ通知する。

【００９９】

分析部５２０は、通知された不正検知メッセージを署名処理部５５０へ通知して不正検知メッセージの署名の検証結果を取得する。また、分析部５２０は、署名検証に成功した不正検知メッセージである分析用情報に含まれる、不正と検知されたデータフレームに関するログ情報を分析することで、車両の動作不良等といった車載ネットワークシステム１０に係る異常を引き起こす不正なデータフレームであるか否かを判断する。分析部５２０は、不正と検知されたデータフレームが異常を引き起こす不正なデータフレームであると判断した場合には、同様のデータフレームが不正検知ＥＣＵ４００で不正と検知された際にそのデータフレームの伝送を阻止する伝送阻止機能をアクティベートするＦＷを生成する。分析部５２０は、その生成したＦＷをＦＷ保持部５３０へ保持させる。なお、不正検知ＥＣＵ４００が、分析用情報に含ませる、不正と検知されたデータフレームに関するログ情報は、例えば、そのデータフレームの内容、そのデータフレームと同一ＩＤのデータフレームの受信周期或いは受信頻度、そのデータフレームの受信の後の一定時間の間に車両の監視により得られた、車両の状態に係るログデータを含み得る。車両の監視により得られたログデータの一例は、例えば、バス２００から受信された各種のデータフレームの内容と受信時刻等といった情報等である。なお、分析部５２０は、不正と検知されたデータフレームに関するログ情報を分析することで、車両の動作不良等といった車載ネットワークシステム１０に係る異常を引き起こす不正なデータフレームを１つ又は複数特定することとしても良い。この場合には、分析部５２０は、異常を引き起こす不正なデータフレームとして特定したデータフレームと同様のデータフレームが不正検知ＥＣＵ４００で不正と検知された際にそのデータフレームの伝送を阻止する伝送阻止機能をアクティベートするＦＷを生成する。

【０１００】

ＦＷ保持部５３０は、不正検知ＥＣＵ４００に配信するＦＷを保持する。

【０１０１】

配信メッセージ生成部５４０は、不正検知ＥＣＵ４００へ配信するＦＷを含ませた配信メッセージを生成し、署名処理部５５０に通知して署名データを生成させることで、署名付き配信メッセージを得て、署名付き配信メッセージを、通信部５１０へ伝える。

【０１０２】

署名処理部５５０は、分析部５２０から通知された署名付きの不正検知メッセージの署名を、鍵保持部５６０から取得する鍵を用いて検証し、検証結果を分析部５２０へと通知する。また、署名処理部５５０は、配信メッセージ生成部５４０より通知された配信メッセージに対して、鍵保持部５６０から取得する鍵を用いて署名データを生成し、生成した署名データを配信メッセージ生成部５４０へ通知する。

【０１０３】

鍵保持部５６０は、署名処理部５５０が利用する鍵を保持する。

【０１０４】

［１．１４　不正フレームの検知及び伝送阻止のシーケンス］

図１４は、不正検知ＥＣＵ４００による不正フレームの検知及び伝送阻止のシーケンスの一例を示す。この例は、車載ネットワークシステム１０のバス２００に、攻撃者に支配された不正ＥＣＵが接続されていることを想定した例となっている。図１４では、不正検知ＥＣＵ４００及びＥＣＵ１００ａの動作を示すが、例えばＥＣＵ１００ｂ～１００ｄもＥＣＵ１００ａと同様の動作を行い得る。以下、図１４に即して、不正フレームの検知及び伝送阻止のシーケンスについて説明する。なお、ここでは、不正検知ＥＣＵ４００は、図１１で例示した正規ＩＤリストを保持しているものとして説明する。

【０１０５】

不正ＥＣＵは、ＩＤ「５」を有しデータフィールドのデータが「０ｘＦＦ」であるデータフレームのバス２００への送信を開始する（ステップＳ１００１）。なお、バス２００へのデータフレームの送信は、バス２００に接続された各ＥＣＵがそのデータフレームを受信可能となるブロードキャストとなる。

【０１０６】

不正検知ＥＣＵ４００及びＥＣＵ１００ａは、データフレームのＩＤを受信する（ステップＳ１００２）。

【０１０７】

ＥＣＵ１００ａは、受信ＩＤリスト（図５参照）を使って、バス２００から受信したＩＤがデータフィールドの内容を受信すべきデータフレームのＩＤであるか否かを判定する（ステップＳ１００３）。ＥＣＵ１００ａは、受信ＩＤリストに従って、ＩＤ「５」のデータフレームのデータフィールドの受信をするデータフィールド受信処理を継続する（ステップＳ１００４）。

【０１０８】

不正検知ＥＣＵ４００は、不正検知ルールに係る正規ＩＤリストに従って、バス２００から受信したＩＤが不正なデータフレームのＩＤであるか否かを判定する（ステップＳ１００５）。不正検知ＥＣＵ４００は、正規ＩＤリストにＩＤ「５」が含まれていないことから、受信したＩＤ「５」を有する受信中のデータフレームが不正と判定して、ステップＳ１００６に進む。もし、正規ＩＤリストにＩＤ「５」が含まれていれば、不正検知ＥＣＵ４００は、受信中のデータフレームを不正でないと判定して処理を終了する。

【０１０９】

ステップＳ１００６で、不正検知ＥＣＵ４００は、管理情報を参照して、伝送阻止機能がアクティベートされているか否かを判定する。

【０１１０】

ステップＳ１００６で伝送阻止機能がアクティベートされていないと判定した場合には、不正検知ＥＣＵ４００は、動作不良検知処理を行う（ステップＳ１００７）。動作不良検知処理については、後に図１５を用いて説明する。

【０１１１】

不正検知ＥＣＵ４００は、例えば図１２で例示した内容の管理情報を保持している場合においては、ＩＤ「５」を有するデータフレームについての伝送の阻止が許容され、つまりそのデータフレームについての伝送阻止機能がアクティベートされていると判定する。

【０１１２】

ステップＳ１００６で伝送阻止機能がアクティベートされていると判定した場合には、不正検知ＥＣＵ４００は、エラーフレームを生成し（ステップＳ１００８）、エラーフレームをバス２００に送信する（ステップＳ１００９）。これにより、ＩＤ「５」を有するデータフレームの受信中においてエラーフレームがバス２００にブロードキャストされるので、そのデータフレームの伝送が阻止されることになる。なお、ステップＳ１００９では、ステップＳ１００５で不正と判定されたデータフレームの伝送を阻止するためのエラーフレームのバス２００への送信は、そのデータフレームの最後尾のビットが受信される前に行なわれる。

【０１１３】

エラーフレームを受信したＥＣＵ１００ａは、受信中のデータフレームのデータフィールドの受信を中止する（ステップＳ１０１０）。不正検知ＥＣＵ４００が送信したエラーフレームにより、バス２００に接続された各ＥＣＵでは、不正ＥＣＵが送信したデータフレームの受信が中断されることになる。このため、例えば、ＥＣＵ１００ａがその不正なデータフレームの内容に従ってエンジン３１０を制御すること等が、防止される。

【０１１４】

［１．１５　不正検知ＥＣＵ４００における動作不良検知処理］

図１５は、不正検知ＥＣＵ４００における動作不良検知処理の一例を示す。以下、同図に即して動作不良検知処理を説明する。

【０１１５】

不正検知ＥＣＵ４００は、不正なデータフレームを検知した後に、一定時間、車両の動作不良（つまり異常）の検知のための監視を行う（ステップＳ１１０１）。この一定時間の車両の監視により車両の状態に係るログデータが得られる。

【０１１６】

車両の動作不良の一例は、特定ＩＤを有するデータフレームが、通常は略一定周期でバス２００に流れるのに、その周期で送信されていないことである。この他、車両の動作不良の一例として、バス２００を流れる特定ＩＤを有するデータフレームのデータの値、受信頻度等が、仕様或いは通常とは異なることが挙げられる。この特定ＩＤは、例えば、不正と検知されたデータフレームのＩＤとは異なるＩＤである。例えば、特定ＩＤとして、車載ネットワークシステム１０において用いられるデータフレームのうち、車両の走行制御に関連するデータ等といった重要なデータに係るデータフレームのＩＤを用いることは、有用である。また、車両の動作不良の一例として、車載ネットワークシステム１０を構成する特定のＥＣＵの動作が仕様或いは通常と異なることが、そのＥＣＵがバス２００に送信したフレーム或いは車載センサのセンシング結果等に基づき判明したことが挙げられる。

【０１１７】

不正検知ＥＣＵ４００は、ステップＳ１１０１で、動作不良が検知された場合に、通信モジュール６００を介して、サーバ５００へ、不正と検知されたデータフレームに関するログ情報（例えばログデータ等）を含む不正検知メッセージを送信する（ステップＳ１１０２）。

【０１１８】

［１．１６　不正検知メッセージのフォーマット］

図１６に、不正検知ＥＣＵ４００がサーバ５００に送信する不正検知メッセージのフォーマットの一例を示す。不正検知メッセージは、不正検知ＥＣＵ４００から通信モジュール６００を介してサーバ５００に送信される。

【０１１９】

図１６の例では、不正検知メッセージは、車種情報、車台番号情報、発生現象情報、ログ情報、及び、署名データで構成される。発生現象情報は、例えば、検知された動作不良の種類を示す情報である。ログ情報は、不正と検知されたデータフレームの内容、そのデータフレームの受信後の一定時間にバス２００に流れたデータフレームについてのログデータ等を含む。

【０１２０】

［１．１７　不正検知ＥＣＵ４００における更新処理］

図１７は、不正検知ＥＣＵ４００における伝送阻止機能のアクティベートに係る更新処理の一例を示す。以下、同図に即して更新処理を説明する。

【０１２１】

不正検知ＥＣＵ４００は、サーバ５００が送信した、更新用のＦＷを含む配信メッセージを受信する通信モジュール６００を介して、その配信メッセージを取得する（ステップＳ１２０１）。

【０１２２】

続いて、不正検知ＥＣＵ４００は、配信メッセージに付されている署名データを検証する（ステップＳ１２０２）。

【０１２３】

不正検知ＥＣＵ４００は、配信メッセージの送信元が、正しいサーバ５００であるか否かを、ステップＳ１２０２での検証結果が検証の成功を示すか否かに基づいて判定し（ステップＳ１２０３）、送信元が正しいサーバ５００でない場合にはＦＷの更新をスキップして更新処理を終了する。

【０１２４】

ステップＳ１２０３で検証結果が成功を示す場合つまり送信元が正しいサーバ５００である場合には、不正検知ＥＣＵ４００は、配信メッセージに含まれるＦＷによってＦＷの更新を行う（ステップＳ１２０４）。このＦＷの更新によって、例えば、管理情報が更新される。この管理情報の更新により、例えば、伝送阻止機能がアクティベートされ得る。なお、ステップＳ１２０４で、不正検知ＥＣＵ４００は、配信メッセージに含まれる車種情報が、自装置を搭載している車両の車種と同一であるか否かを確認して同一である場合に限ってＦＷの更新を行うこととしても良い。

【０１２５】

［１．１８　配信メッセージのフォーマット］

図１８に、サーバ５００が車両へと配信する配信メッセージのフォーマットの一例を示す。

【０１２６】

図１８の例では、配信メッセージは、配信の対象となる車両の車種を示す車種情報、更新用のＦＷ、及び、署名データで構成される。更新用のＦＷは、一例としては、管理情報（図１２参照）における１つ以上のＩＤに対応するフラグ情報を更新するためのデータ或いはプログラムを含む。

【０１２７】

［１．１９　実施の形態１の効果］

実施の形態１に係る車両の車載ネットワークシステム１０では、不正検知ＥＣＵ４００が、バス２００を流れるデータフレームを不正と判定した場合に、管理情報により伝送阻止機能がアクティベートされた状態が示される場合にはそのデータフレームの伝送を阻止する。また、不正検知ＥＣＵ４００は、伝送阻止機能がアクティベートされていない状態においては、そのデータフレームの伝送を阻止しない。データフレームが不正と検知されて、動作不良が検知された車両から得た、ログ情報を分析してサーバ５００が生成したＦＷがサーバ５００から配信されることで、不正検知ＥＣＵ４００では、伝送阻止機能がアクティベートされ得る。サーバ５００は、異常を引き起こす不正なデータフレームと判断したそのデータフレームの伝送の阻止を許容するように管理情報を更新するＦＷを生成する。これにより、例えば、攻撃者により車両に異常を引き起こす攻撃フレームがバス２００に送信された場合に、不正検知ＥＣＵ４００がその攻撃フレームの伝送を阻止するようになる。また、不正検知ＥＣＵ４００における管理情報によって、車両に異常を引き起こさないデータフレームについては、そのデータフレームの伝送の阻止が許容されず、誤ってその伝送の阻止を行うことの悪影響が防止される。

【０１２８】

（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を部分的に変形した車載ネットワークシステム１１について説明する。車載ネットワークシステム１１は、不正と判定したデータフレームの伝送を阻止する伝送阻止機能を、車車間通信によってアクティベートでき、サーバ１５００からの指示によってディアクティベートできるフレーム伝送阻止装置としての不正検知ＥＣＵを備える。

【０１２９】

［２．１　車載ネットワークシステム１１の構成］

図１９は、車両に搭載された車載ネットワークシステム１１の構成を示す図である。な

お、同図には、他の車両及び車外のサーバ１５００を付記している。車載ネットワークシステム１１は、複数の車両それぞれに搭載される。サーバ１５００と複数の車両とで車両管理システムを形成している。

【０１３０】

車載ネットワークシステム１１は、図１９に示すように、バス２００と、バス２００に接続されたＥＣＵ１００ａ～１００ｄ及び不正検知ＥＣＵ１４００と、通信モジュール１６００とを含んで構成される。なお、実施の形態１（図１参照）と同様の構成については、図１９において図１と同一の符号を付しており、説明を省略する。ここで特に説明しない点は、車載ネットワークシステム１１は実施の形態１で示した車載ネットワークシステム１０と同様である。

【０１３１】

不正検知ＥＣＵ１４００は、バス２００に接続される一種のＥＣＵである。不正検知ＥＣＵ１４００は、バス２００に流れるデータフレームを監視し、予め定められた不正なフレームに関する所定条件を満たすデータフレームを検知した場合に、所定の管理情報に基づいてそのフレームの伝送を阻止する伝送阻止機能を有する。不正検知ＥＣＵ１４００は、ここで特に説明しない点は、実施の形態１で示した不正検知ＥＣＵ４００と同様である。

【０１３２】

車両に搭載された通信モジュール１６００は、サーバ１５００及び他の車両と通信するための通信回路を含むモジュールであり、不正検知ＥＣＵ１４００にＵＳＢ等のインタフェースにより直接接続している。各車両の通信モジュール１６００間で行われる車車間通信により、各車両の不正検知ＥＣＵ１４００が互いにメッセージを授受し得る。車両の通信モジュール１６００が実行する車車間通信は、例えば一定出力の無線送信により、その車両の周囲（例えば数十ｍ、数百ｍ等の距離の範囲内）に所在する他の車両にメッセージを伝達することができる。

【０１３３】

サーバ１５００は、複数の車両と通信し得る、車両外部に所在するサーバ装置としてのコンピュータである。サーバ１５００は、有線又は無線の通信網を介して、複数の車両それぞれにおける不正検知ＥＣＵ１４００に接続された通信モジュール１６００と通信する。サーバ１５００は、実施の形態１で示したサーバ５００と同様に、不正検知ＥＣＵ１４００に対して、更新用のＦＷを含む配信メッセージを送信する機能を有する。サーバ１５００は、更に、車両の不正検知ＥＣＵ１４００の伝送阻止機能をディアクティベートするためのディアクティベーションメッセージを送信する機能を有する。また、サーバ１５００は、更に、ある車両から不正検知メッセージを受信した場合において、必要に応じて、その不正検知メッセージに含まれる車種情報及びアクティベート指示情報を含ませた異常通知メッセージを他の車両へと送信する機能を有する。なお、この機能は、車両による直接的な車車間通信による異常通知メッセージの伝送を補完する、アクティベート指示情報の中継機能である。

【０１３４】

［２．２　不正検知ＥＣＵ１４００の構成］

図２０は、不正検知ＥＣＵ１４００の構成図である。不正検知ＥＣＵ１４００は、フレーム送受信部４１０と、フレーム解釈部４２０と、不正検知処理部４３０、不正検知ルール保持部４３１、状態確認部１４４０と、状態保持部４４１と、フレーム生成部４５０と、更新処理部１４６０と、外部通信部１４７０と、署名処理部４８０と、鍵保持部４８１と、車種情報保持部４９１と、車台番号情報保持部４９２とを含んで構成される。これらの各構成要素の各機能は、例えば不正検知ＥＣＵ１４００における通信回路、メモリに格納されたプログラムを実行するプロセッサ或いはデジタル回路等により実現される。実施の形態１で示した不正検知ＥＣＵ４００（図１０参照）と同様の機能を有する構成要素については、図２０において同じ符号を付しており、説明を省略する。

【０１３５】

状態確認部１４４０は、実施の形態１で示した状態確認部４４０を変形したものである。状態確認部１４４０は、不正なデータフレームが検知された場合に、伝送阻止機能がアクティベートされた状態であれば、フレーム生成部４５０へエラーフレームを送信するよう通知する。状態確認部１４４０は、不正なデータフレームが検知された場合において、不正伝送阻止機能がアクティベートされていない状態であれば、車両の状態を確認する。状態確認部１４４０は、この確認において動作不良等といった異常が検知されたときには、サーバ１５００への送信のための不正と検知されたデータフレームに関するログ情報と、他の車両におけるフレーム伝送阻止装置の伝送阻止機能のアクティベートのためのアクティベート指示情報とを、外部通信部４７０に通知する。このアクティベート指示情報には、伝送阻止機能のアクティベートのための指示であることを示すアクティベーション命令と、不正と検知されたデータフレームのＩＤ、つまり、その伝送阻止機能のアクティベートの対象となるＩＤを特定するための対象フレーム情報とが含まれる。

【０１３６】

更新処理部１４６０は、実施の形態１で示した更新処理部４６０と同様の機能に加えて、外部通信部１４７０から、伝送阻止機能のアクティベート状態に係るアクティベート指示情報或いはディアクティベート指示情報を通知された場合にこれらの指示情報に対応して管理情報の更新を行う機能を有する。なお、ディアクティベート指示情報には、伝送の阻止を行わないディアクティベートのための指示であることを示すディアクティベーション命令と、その伝送の阻止を行わない対象となるデータフレームのＩＤを特定するための対象フレーム情報とが含まれる。更新処理部１４６０による、アクティベート指示情報に対応した管理情報の更新に係る伝送阻止機能アクティベーション処理は、対象フレーム情報で示されるＩＤに対応するフラグ情報を、伝送阻止機能がアクティベートされた状態つまり伝送の阻止を許容する状態を示す値に変更することで実現される。更新処理部１４６０による、ディアクティベート指示情報に対応した管理情報の更新に係る伝送阻止機能ディアクティベーション処理は、対象フレーム情報で示されるＩＤに対応するフラグ情報を、伝送阻止機能がアクティベートされていない状態つまり伝送の阻止を許容しない状態を示す値に変更することで実現される。

【０１３７】

外部通信部１４７０は、実施の形態１で示した外部通信部４７０を変形したものである。外部通信部１４７０は、通信モジュール１６００を介してサーバ１５００と通信し、配信メッセージ、異常通知メッセージ或いはディアクティベーションメッセージを取得する。外部通信部１４７０は、取得した配信メッセージを署名処理部４８０へ通知して配信メッセージの署名の検証結果を取得し、検証が成功していれば配信メッセージにおけるＦＷを更新処理部１４６０へ通知する。外部通信部１４７０は、取得した異常通知メッセージを署名処理部４８０へ通知して異常通知メッセージの署名の検証結果を取得し、検証が成功して車種情報が自装置の搭載されている車両と同一車種であれば、異常通知メッセージにおけるアクティベート指示情報を更新処理部１４６０へ通知する。外部通信部１４７０は、取得したディアクティベーションメッセージを署名処理部４８０へ通知してディアクティベーションメッセージの署名の検証結果を取得し、検証が成功していればディアクティベーションメッセージにおけるディアクティベート指示情報を更新処理部１４６０へ通知する。なお、車両管理システムにおいて、伝送阻止機能をディアクティベートするディアクティベーションメッセージを送信する所定権限は例えばサーバ１５００に与えられているが、車両には与えられていない。このため、ディアクティベーションメッセージの署名の検証においては、ディアクティベーションメッセージに、所定権限を有するサーバ１５００に係る署名データが付されていることを検証することが有用となる。

【０１３８】

また、外部通信部１４７０は、状態確認部１４４０から通知されたデータフレームに関するログ情報及びアクティベート指示情報に、車種情報保持部４９１より取得した車種情報と、車台番号情報保持部４９２より取得した車台番号情報とを付加して、署名なし不正検知メッセージを生成する。この不正検知メッセージは、実施の形態１で示した不正検知

メッセージにアクティベート指示情報を追加したものである。外部通信部１４７０は、署名なし不正検知メッセージを、署名処理部４８０に通知して署名データを取得することで署名付きの不正検知メッセージに変換し、その署名付きの不正検知メッセージを、通信モジュール１６００を介してサーバ１５００へと送信する。また、外部通信部１４７０は、状態確認部１４４０から通知されたアクティベート指示情報に、車種情報保持部４９１より取得した車種情報と、車台番号情報保持部４９２より取得した車台番号情報とを付加して、署名なし異常通知メッセージを生成する。外部通信部１４７０は、署名なし異常通知メッセージを、署名処理部４８０に通知して署名データを取得することで署名付きの異常通知メッセージに変換し、その署名付きの異常通知メッセージを、通信モジュール１６００を介して他の車両へと送信する。

【０１３９】

［２．３　サーバ１５００の構成］

サーバ１５００は、メモリ、ハードディスク等の記憶媒体、プロセッサ、通信回路等を含む。

【０１４０】

図２１は、サーバ１５００の構成図である。サーバ１５００は、機能面の構成要素として、通信部５１０と、分析部１５２０と、ＦＷ保持部５３０と、メッセージ生成部１５４０と、署名処理部５５０と、鍵保持部５６０とを含んで構成される。これらの各構成要素は、サーバ１５００における通信回路、メモリに格納されたプログラムを実行するプロセッサ等により実現される。実施の形態１で示したサーバ５００（図１３参照）と同様の機能を有する構成要素については、図２１において同じ符号を付しており、説明を適宜省略する。

【０１４１】

通信部５１０は、メッセージ生成部１５４０から伝えられた配信メッセージ、ディアクティベーションメッセージ或いは異常通知メッセージを、車両に対して送信する。これらのメッセージは、車両の通信モジュール１６００で受信され、不正検知ＥＣＵ１４００に伝えられる。また、通信部５１０は、車両の不正検知ＥＣＵ１４００から通信モジュール１６００を介して送信された不正検知メッセージを受信し、分析部１５２０へ通知する。

【０１４２】

分析部１５２０は、通知された不正検知メッセージを署名処理部５５０へ通知して不正検知メッセージの署名の検証結果を取得する。また、分析部１５２０は、署名検証に成功した不正検知メッセージである分析用情報に含まれる、不正と検知されたデータフレームに関するログ情報を分析することで、車両の動作不良等といった車載ネットワークシステム１１に係る異常を引き起こす不正なデータフレームであるか否かを判断する。分析部１５２０は、不正と検知されたデータフレームが異常を引き起こす不正なデータフレームであると判断した場合には、同様のデータフレームが不正検知ＥＣＵ１４００で不正と検知された際にそのデータフレームの伝送を阻止する伝送阻止機能をアクティベートするＦＷを生成する。分析部１５２０は、その生成したＦＷをＦＷ保持部５３０へ保持させる。また、分析部１５２０は、不正と検知されたデータフレームが異常を引き起こす不正なデータフレームであると判断した場合には、不正検知メッセージに含まれるアクティベート指示情報及び車種情報をメッセージ生成部１５４０に通知する。また、分析部１５２０は、不正と検知されたデータフレームが異常を引き起こす不正なデータフレームでないと判断した場合には、同様のデータフレームが不正検知ＥＣＵ１４００で不正と検知された際にそのデータフレームの伝送を阻止する伝送阻止機能をディアクティベートするためにディアクティベート指示情報をメッセージ生成部１５４０に通知する。分析部１５２０での判断は、不正と検知されたデータフレームの影響を踏まえ、例えば複数の車両から収集された情報等に基づいて行なわれても良い。なお、分析部１５２０は、メッセージ生成部１５４０に通知するディアクティベート指示情報に、伝送阻止機能をディアクティベートする対象となるデータフレームのＩＤを示す対象フレーム情報を含める。

【０１４３】

ＦＷ保持部５３０は、不正検知ＥＣＵ１４００に配信するＦＷを保持する。
【０１４４】
メッセージ生成部１５４０は、不正検知ＥＣＵ１４００へ配信するＦＷを含ませた配信メッセージを生成し、署名処理部５５０に通知して署名データを生成させることで、署名付き配信メッセージを得て、署名付き配信メッセージを、通信部５１０へ伝える。また、メッセージ生成部１５４０は、分析部１５２０からアクティベート指示情報及び車種情報の通知を受けた場合にはそのアクティベート指示情報及び車種情報を含ませた異常通知メッセージを生成し、署名処理部５５０に通知して署名データを生成させることで、署名付き異常通知メッセージを得て、署名付き異常通知メッセージを、通信部５１０へ伝える。また、メッセージ生成部１５４０は、分析部１５２０からディアクティベート指示情報の通知を受けた場合にはそのディアクティベート指示情報を含ませたディアクティベーションメッセージを生成し、署名処理部５５０に通知して署名データを生成させることで、署名付きディアクティベーションメッセージを得て、署名付きディアクティベーションメッセージを、通信部５１０へ伝える。
【０１４５】
署名処理部５５０は、分析部１５２０から通知された署名付きの不正検知メッセージの署名を、鍵保持部５６０から取得する鍵を用いて検証し、検証結果を分析部１５２０へと通知する。また、署名処理部５５０は、メッセージ生成部１５４０より通知された配信メッセージ、異常通知メッセージ或いはディアクティベーションメッセージに対して、鍵保持部５６０から取得する鍵を用いて署名データを生成し、生成した署名データをメッセージ生成部１５４０へ通知する。
【０１４６】
［２．４　不正フレームの検知及び伝送阻止のシーケンス］
図２２は、不正検知ＥＣＵ１４００による不正フレームの検知及び伝送阻止のシーケンスの一例を示す。この例は、車載ネットワークシステム１１のバス２００に、攻撃者に支配された不正ＥＣＵが接続されていることを想定した例となっている。図２２では、不正検知ＥＣＵ１４００及びＥＣＵ１００ａの動作を示すが、例えばＥＣＵ１００ｂ～１００ｄもＥＣＵ１００ａと同様の動作を行い得る。なお、実施の形態１で図１４に示した処理のステップと同様のステップについては、図２２においても同じ符号を付しており、説明を適宜省略する。
【０１４７】
不正ＥＣＵが、ＩＤ「５」を有しデータが「０ｘＦＦ」であるデータフレームの送信を開始し（ステップＳ１００１）、不正検知ＥＣＵ１４００は、データフレームのＩＤを受信する（ステップＳ１００２）。
【０１４８】
不正検知ＥＣＵ１４００は、不正検知ルールに係る正規ＩＤリスト（図１１参照）に従って、バス２００から受信したＩＤが不正なデータフレームのＩＤであるか否かを判定し（ステップＳ１００５）、正規ＩＤリストにＩＤ「５」が含まれていないことから、受信したＩＤ「５」を有する受信中のデータフレームが不正と判定する。続いて、不正検知ＥＣＵ１４００は、管理情報を参照して、伝送阻止機能がアクティベートされているか否かを判定する（ステップＳ１００６）。
【０１４９】
ステップＳ１００６で伝送阻止機能がアクティベートされていないと判定した場合には、不正検知ＥＣＵ１４００は、動作不良検知処理を行う（ステップＳ２００７）。この動作不良検知処理については、後に図２３を用いて説明する。
【０１５０】
ステップＳ１００６で伝送阻止機能がアクティベートされていると判定した場合には、不正検知ＥＣＵ１４００は、エラーフレームを、生成して送信する（ステップＳ１００８、Ｓ１００９）。
【０１５１】

［２．５　不正検知ＥＣＵ１４００における動作不良検知処理］
図２３は、不正検知ＥＣＵ１４００における動作不良検知処理の一例を示す。なお、実施の形態１で図１５に示した処理のステップと同様のステップについては、図２３においても同じ符号を付しており、説明を適宜省略する。以下、図２３に即して動作不良検知処理を説明する。
【０１５２】
不正検知ＥＣＵ１４００は、不正なデータフレームを検知した後に、一定時間、車両の動作不良（つまり異常）の検知のための監視を行う（ステップＳ１１０１）。この一定時間の車両の監視により車両の状態に係るログデータが得られる。
【０１５３】
不正検知ＥＣＵ１４００は、ステップＳ１１０１で、動作不良が検知された場合に、通信モジュール１６００を介して、周囲の車両に車車間通信で、不正と検知されたデータフレームのＩＤ示す対象フレーム情報等のアクティベート指示情報を含む異常通知メッセージ（図２４参照）を送信する（ステップＳ２１０２）。
【０１５４】
ステップＳ２１０２に続いて不正検知ＥＣＵ１４００は、通信モジュール１６００を介して、サーバ１５００へ、不正と検知されたデータフレームに関するログ情報（例えばログデータ等）とアクティベート指示情報とを含む不正検知メッセージ（図２５参照）を送信する（ステップＳ２１０３）。
【０１５５】
［２．６　異常通知メッセージのフォーマット］
図２４に、車両の不正検知ＥＣＵ１４００が通信モジュール１６００によって周囲の車両に送信する異常通知メッセージのフォーマットの一例を示す。異常通知メッセージは、一定条件下でサーバ１５００からも送信され得る。
【０１５６】
図２４の例では、異常通知メッセージは、車種情報、車台番号情報、アクティベート指示情報（つまりアクティベーション命令及び対象フレーム情報）、及び、署名データで構成される。異常通知メッセージにおける対象フレーム情報で例えば所定ＩＤを示し、この場合にアクティベート指示情報は、所定ＩＤを有するフレームの伝送の阻止を許容する指示を表す。
【０１５７】
［２．７　不正検知メッセージのフォーマット］
図２５に、不正検知ＥＣＵ１４００がサーバ１５００に送信する不正検知メッセージのフォーマットの一例を示す。不正検知メッセージは、不正検知ＥＣＵ１４００から通信モジュール１６００を介してサーバ１５００に送信される。
【０１５８】
図２５の例では、不正検知メッセージは、車種情報、車台番号情報、アクティベート指示情報（つまりアクティベーション命令及び対象フレーム情報）、発生現象情報、ログ情報、及び、署名データで構成される。この不正検知メッセージは、実施の形態１で示した不正検知メッセージ（図１６参照）にアクティベート指示情報を加えたものである。
【０１５９】
［２．８　不正検知ＥＣＵ１４００の伝送阻止機能アクティベーション処理］
図２６は、不正検知ＥＣＵ１４００における伝送阻止機能アクティベーション処理の一例を示す。以下、同図に即して伝送阻止機能アクティベーション処理を説明する。
【０１６０】
不正検知ＥＣＵ１４００は、他の車両或いはサーバ１５００が送信した異常通知メッセージを、受信する通信モジュール１６００を介して、その異常通知メッセージを取得する（ステップＳ２２０１）。
【０１６１】
続いて、不正検知ＥＣＵ１４００は、異常通知メッセージに付されている署名データを

検証する（ステップＳ２２０２）。
【０１６２】
不正検知ＥＣＵ１４００は、異常通知メッセージの送信元が、正しいサーバ１５００或いは正しい車両であるか否かを、ステップＳ２２０２での検証結果が検証の成功を示すか否かに基づいて判定し（ステップＳ２２０３）、検証に失敗した場合には、伝送阻止機能のアクティベートをスキップして伝送阻止機能アクティベーション処理を終了する。
【０１６３】
ステップＳ２２０３で検証結果が成功を示す場合つまり送信元が正しいサーバ１５００或いは正しい車両である場合には、不正検知ＥＣＵ１４００は、異常通知メッセージにおける車種情報に基づいて、自装置が搭載されている車両と同じ車種であるか否かを判定する（ステップＳ２２０４）。同じ車種でない場合には、不正検知ＥＣＵ１４００は、伝送阻止機能アクティベーション処理を終了する。
【０１６４】
ステップＳ２２０４で、同じ車種であると判定した場合には、不正検知ＥＣＵ１４００は、異常通知メッセージにおけるアクティベート指示情報に従って、伝送阻止機能をアクティベートする（ステップＳ２２０５）。不正検知ＥＣＵ１４００は、このアクティベートを、管理情報における、アクティベート指示情報の対象フレーム情報が示すＩＤに対応するフラグ情報を、フレームの伝送の阻止を許容することを示す値にすることで実現する。
【０１６５】
［２．９　サーバ１５００によるディアクティベーションメッセージの送信］
図２７は、サーバ１５００におけるディアクティベーションメッセージの送信に係る処理の一例を示す。ディアクティベーションメッセージは、不正検知ＥＣＵ１４００の伝送阻止機能をディアクティベートするためのメッセージである。
【０１６６】
サーバ１５００は、車両の不正検知ＥＣＵ１４００からの不正検知メッセージを受信する（ステップＳ２３０１）。
【０１６７】
続いて、サーバ１５００は、不正検知メッセージに付されている署名データを検証する（ステップＳ２３０２）。
【０１６８】
サーバ１５００は、不正検知メッセージの送信元が、正しい車両であるか否かを、ステップＳ２３０２での検証結果が検証の成功を示すか否かに基づいて判定し（ステップＳ２３０３）、送信元が正しい車両でない場合には、ディアクティベーションメッセージの送信等を行わずに処理を終了する。
【０１６９】
ステップＳ２３０３で検証結果が成功を示す場合つまり送信元が正しい車両である場合には、サーバ１５００は、不正検知メッセージにおけるログ情報等に基づいて、不正と検知されたデータフレームが異常を引き起こす不正なデータフレームであるか否かを判断する（ステップＳ２３０４）。この判断は、異常が引き起こされる状態であるか否かの確認である。ステップＳ２３０４で、異常が引き起こされる状態でないと判断した場合には、サーバ１５００は、そのデータフレームが不正検知ＥＣＵ１４００で不正と検知された際にそのデータフレームの伝送を阻止する伝送阻止機能をディアクティベートするためにディアクティベート指示情報を含むディアクティベーションメッセージ（図２８参照）を送信する（ステップＳ２３０５）。サーバ１５００は、異常が引き起こされるか否かの判断の方法としていかなる方法を用いても良い。サーバ１５００は、ログ情報に基づいて不正と検知されたデータフレームから、一定時間が経過するまでに、車載ネットワークシステム１１において予め定められた１つ又は複数の重要なデータフレームの内容或いは送信周期等に異常がない場合に、異常が引き起こされる状態でないと判断する方法を用い得る。また、サーバ１５００は、ログ情報に基づいて不正と検知されたデータフレームから、一

定時間が経過するまでに、車載ネットワークシステム１１を構成し車両の走行の制御に関わる１つ又は複数の特定のＥＣＵが正常に動作している場合に、異常が引き起こされる状態でないと判断する方法を用い得る。また、サーバ１５００は、一例としては、ログ情報に基づいて不正と検知されたデータフレームから、ある程度十分な長さの一定時間が経過するまでに同種のメッセージが二度と受信されていない場合に、異常が引き起こされる状態でないと判断するような方法を用い得る。

【０１７０】

ステップＳ２３０４で、異常が引き起こされる状態であると判断した場合には、サーバ１５００は、ディアクティベーションメッセージの送信を行わない。なお、ステップＳ２３０４で、異常が引き起こされる状態であると判断した場合に、サーバ１５００は、例えば、伝送阻止機能をアクティベートするためのＦＷを含む配信メッセージを送信し得る。

【０１７１】

［２．１０　ディアクティベーションメッセージのフォーマット］

図２８に、サーバ１５００が車両に対して送信するディアクティベーションメッセージのフォーマットの一例を示す。ディアクティベーションメッセージは、車両の通信モジュール１６００を介して不正検知ＥＣＵ１４００に受信される。

【０１７２】

図２８の例では、ディアクティベーションメッセージは、車種情報、ディアクティベート指示情報（つまりディアクティベーション命令及び対象フレーム情報）、及び、署名データで構成される。ディアクティベーションメッセージにおける対象フレーム情報で例えば所定ＩＤを示し、この場合にディアクティベート指示情報は、所定ＩＤを有するフレームの伝送の阻止を許容しない指示を表す。

【０１７３】

［２．１１　不正検知ＥＣＵ１４００における伝送阻止機能ディアクティベーション処理］

図２９は、不正検知ＥＣＵ１４００における伝送阻止機能ディアクティベーション処理の一例を示す。以下、同図に即して伝送阻止機能ディアクティベーション処理を説明する。

【０１７４】

不正検知ＥＣＵ１４００は、通信モジュール１６００を介して、ディアクティベーションメッセージを受信する（ステップＳ２４０１）。

【０１７５】

続いて、不正検知ＥＣＵ１４００は、ディアクティベーションメッセージに付されている署名データを検証する（ステップＳ２４０２）。

【０１７６】

不正検知ＥＣＵ１４００は、ディアクティベーションメッセージの送信元が、正しいサーバ１５００であるか否かを、ステップＳ２４０２での検証結果が検証の成功を示すか否かに基づいて判定し（ステップＳ２４０３）、検証に失敗した場合には、伝送阻止機能のディアクティベートをスキップして伝送阻止機能ディアクティベーション処理を終了する。

【０１７７】

ステップＳ２４０３で検証結果が成功を示す場合、つまり送信元がディアクティベーションメッセージを送信する所定権限を有するサーバ１５００であるとの認証に成功した場合には、不正検知ＥＣＵ１４００は、ディアクティベーションメッセージにおけるディアクティベート指示情報の対象フレーム情報と、管理情報中のフラグ情報とに基づいて、対象フレームについての伝送阻止機能がアクティベートされた状態であるか否かを判定する（ステップＳ２４０４）。アクティベートされた状態でない場合には、不正検知ＥＣＵ１４００は、伝送阻止機能ディアクティベーション処理を終了する。

【０１７８】

ステップＳ２４０４で、アクティベートされた状態であると判定した場合には、不正検

知ＥＣＵ１４００は、その伝送阻止機能をディアクティベートする（ステップＳ２４０５）。不正検知ＥＣＵ１４００は、このディアクティベートを、管理情報における、ディアクティベート指示情報の対象フレーム情報が示すＩＤに対応するフラグ情報を、フレームの伝送の阻止を許容しないことを示す値にすることで実現する。

【０１７９】

［２．１２　実施の形態２の効果］

実施の形態２に係る車両の車載ネットワークシステム１１では、不正検知ＥＣＵ１４００が、バス２００を流れるデータフレームを不正と判定した場合に、管理情報により伝送阻止機能がアクティベートされた状態が示される場合にはそのデータフレームの伝送を阻止する。また、不正検知ＥＣＵ１４００は、伝送阻止機能がアクティベートされていない状態においては、そのデータフレームの伝送を阻止しない。データフレームが不正と検知されて、動作不良が検知された車両の不正検知ＥＣＵ１４００は、他の車両に対して、異常通知メッセージを送信する。これにより、他の車両では、不正と検知されたデータフレームについての伝送阻止機能がアクティベートされ、迅速に攻撃者による攻撃に対する防御を実現し得る。これは、攻撃者による局所的な車両群への一斉攻撃への迅速な防御を可能にしている。また、サーバ１５００は、異常を引き起こすものではないと総合的に判断したデータフレームを対象として、車両の不正検知ＥＣＵ１４００による伝送阻止機能をディアクティベートするディアクティベーションメッセージを送信する。ディアクティベーションメッセージを送信する所定権限はサーバ１５００が有する。車両において一旦アクティベートされた伝送阻止機能を、所定権限を有するサーバ１５００からのみディアクティベートできるようにしておくことで、セキュリティを高めている。

【０１８０】

（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。

【０１８１】

（１）上記実施の形態では、通信モジュール６００、１６００が不正検知ＥＣＵと直接接続する例を示したが、通信モジュール６００、１６００は、ＣＡＮのバス２００に繋がる通信モジュールＥＣＵであっても良い。この場合には、不正検知ＥＣＵは、バス２００経由で通信モジュールＥＣＵとメッセージの授受を行うことで、通信モジュールＥＣＵを介してサーバ５００、１５００或いは他の車両とメッセージの送受信を行うこととしても良い。また、通信モジュール６００、１６００は、不正検知ＥＣＵ４００、１４００内に通信部として備えられていても良い。

【０１８２】

（２）上記実施の形態では、フレーム伝送阻止装置としての不正検知ＥＣＵ４００、１４００が通信モジュール６００、１６００を介して車両外部のサーバ５００、１５００或いは他の車両とメッセージの送受信する例を示したが、フレーム伝送阻止装置内に車両外部との通信回路を有して、サーバ５００等と通信できるようにしても良い。フレーム伝送阻止装置の一例を図３０に示す。図３０に示したフレーム伝送阻止装置２４００は、例えば車両に搭載され、車載ネットワークシステム１０、１１等のバス２００（図１、図１９参照）に接続され、例えばプロセッサ、メモリ等の集積回路、通信回路等を含む装置である。フレーム伝送阻止装置２４００は、機能面では、例えば、受信部２４１０、処理部２４２０、記憶部２４３０、通信部２４４０及び更新部２４５０を含んで構成される。受信部２４１０は、通信回路等で構成され、バス２００からフレームを受信する。受信部２４１０は、上述のフレーム送受信部１１０において受信機能を担う部分に相当する。処理部２４２０は、例えばメモリに格納されたプログラムを実行するプロセッサ、通信回路等で実現され、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、受信部２４１０により受信されたフレームが所定条件を満たす場合にそのフレームの伝送を阻止す

る所定処理を実行するか否かを切り替える。処理部２４２０は、例えば、上述の不正検知処理部４３０、状態確認部４４０、１４４０等で構成されても良い。所定条件は例えば不正なフレームを検知するための条件である。所定条件は、例えばフレームのＩＤについての条件であり、例えば図１１で示した正規ＩＤリスト等のＩＤではない場合に満たされる条件であり得る。処理部２４２０は、送信部２４２１を含み、例えば上述の所定処理として、受信部２４１０により所定条件を満たすフレームの最後尾のビットが受信される前にエラーフレームをバス２００へ送信する処理を行い得る。処理部２４２０は、フレームの伝送の阻止のための所定処理としてそのフレームが伝送されている際に、エラーフレームを構成するに満たない数のドミナント信号をバス２００へ送信する処理を行うこととしても良い。このドミナント信号でバス２００上のフレームの内容が改変され、例えばＣＲＣの不整合等といった受信エラー等を引き起こすと、受信ノードのＥＣＵでそのフレームを正常なフレームと同様に処理することが防止され得る。フレーム伝送阻止装置２４００が、複数のバス間を接続して一方のバスから受信したデータフレームを他方のバスに転送する転送機能を有するゲートウェイ装置であっても良く、この場合には処理部２４２０は、フレームの伝送の阻止する所定処理として、フレームの転送を抑止する処理を行い得る。記憶部２４３０は、メモリ等の記憶媒体の一領域に管理情報を記憶しており、例えば上述の状態保持部４４１等に相当する。通信部２４４０は、例えば無線通信回路等で構成され、車両外部のサーバ装置、他の車両内の装置等といった外部装置と通信する。例えば通信部２４４０は、他の車両向けの異常通知メッセージ（図２４参照）等を送信し得る。更新部２４５０は、例えばプログラムを実行するプロセッサ等で構成され、記憶部２４３０に記憶された管理情報を更新する。更新部２４５０は、例えば上述の更新処理部４６０、１４６０等で構成されても良い。記憶部２４３０における管理情報は、複数のＩＤそれぞれに対応して、そのＩＤを有し所定条件を満たすフレームの伝送の阻止を許容するか否かを示すフラグ情報を含むこととしても良い。これに対応して処理部２４２０は、受信部２４１０により受信されたフレームが所定条件を満たす場合において、そのフレームのＩＤに対応するフラグ情報がそのフレームの伝送の阻止を許容することを示すときには所定処理を実行し、そのフレームのＩＤに対応するフラグ情報がそのフレームの伝送の阻止を許容しないことを示すときには所定処理を実行しないこととしても良い。また、更新部２４５０は、フレーム伝送阻止装置２４００が、バス２００に接続された異常監視用のＥＣＵ等から、或いは、車両外部の外部装置等から、受信した指示情報に応じて管理情報を更新しても良い。この指示情報は、例えば、上記実施の形態で示したアクティベート指示情報、ディアクティベート指示情報等であり得る。

【０１８３】

（３）上記実施の形態では、不正検知ＥＣＵ４００、１４００が、不正なデータフレームを検知した場合において、車両の動作不良を検知したときに、車両外部へ不正検知メッセージを送信する例を示した。しかし、不正検知ＥＣＵ４００、１４００は、不正なデータフレームが検知された場合において、伝送阻止機能がアクティベートされていない状態であれば、動作不良等といった異常が検知されるか否かに拘わらず、車両外部のサーバ等の外部装置に対して、不正と検知されたデータフレームに関するログ情報等を含む情報を送信することとしても良い。上述のフレーム伝送阻止装置２４００では、受信部２４１０により受信されたフレームが所定条件を満たす場合に、通信部２４４０が、そのフレームに関する情報を含む分析用情報を車両外部の外部装置に送信することとしても良い。また、不正検知ＥＣＵ４００、１４００は、自ら異常か否かの判断ができない場合等においてサーバ５００、１５００等の外部装置に異常を引き起こすか否かの判断を委ねることとしても良い。サーバ５００等の外部装置では、複数の車両から収集される情報に基づいて判断の精度を上げることが可能である。そして、外部装置は異常を引き起こすと判断した場合に必要に応じて不正検知ＥＣＵ４００、１４００の伝送阻止機能をアクティベートするためのアクティベート指示情報を含むメッセージを不正検知ＥＣＵ４００、１４００に対して送信し得る。また、上記実施の形態では、サーバ５００では分析部５２０及び配信メッセージ生成部５４０等によって車両の不正検知ＥＣＵ４００の伝送阻止機能のアクティ

ベート状態を変更するＦＷを含む配信メッセージを生成し、サーバ１５００では分析部１５２０及びメッセージ生成部１５４０等によって車両の不正検知ＥＣＵ１４００の伝送阻止機能のアクティベート状態を変更する配信メッセージ或いはディアクティベーションメッセージを生成する例を示した。サーバ５００、１５００が送信するこれらのメッセージの生成は、サーバ５００、１５００に対する操作者の指示等に基づいて行われることとしても良い。

【０１８４】

（４）上記実施の形態では、不正検知ＥＣＵ４００、１４００が、サーバ５００、１５００、他の車両等から送信されるメッセージに基づいて、伝送阻止機能のアクティベート状態を示す管理情報を更新する例を示した。しかし、不正検知ＥＣＵ４００、１４００は、不正なデータフレームを検知した場合に、車両に異常が引き起こされたか否かを自ら検査して検査結果として異常の発生を検出したときに（例えばステップＳ１１０１で動作不良を検知したときに）、自ら管理情報を更新して伝送阻止機能をアクティベートされた状態にすることとしても良い。具体例として、不正検知ＥＣＵ４００の更新処理部４６０は、フレーム送受信部１１０により受信されたデータフレームが、正規ＩＤリストに含まれないＩＤを有するという不正検知ルールに係る所定条件を満たし、かつ、管理情報におけるそのデータフレームのＩＤに対応するフラグ情報がそのデータフレームの伝送の阻止を許容しないことを示す場合において、そのデータフレームのＩＤとは異なる特定ＩＤを有する、フレーム送受信部１１０で受信されたデータフレームに基づいて異常の発生を検出したときには、そのフラグ情報を伝送の阻止を許容することを示すように更新することとしても良い。例えば、特定ＩＤを有するデータフレームの受信周期、受信頻度、データフレームの内容等が正常状態と異なるか否かを判別することで異常は検出され得る。例えば、特定ＩＤを有するデータフレームが一定時間経過しても受信されない場合に異常と検出しても良い。例えば重要なデータフレームのＩＤを特定ＩＤとして定めておくことが有用である。これにより、不正なデータフレームが検知され、重要なデータフレームに異常が発生したような場合に、その後の不正なデータフレームの伝送が阻止されるようになる。また別の具体例として、更新処理部４６０は、フレーム送受信部１１０により受信されたデータフレームが所定条件を満たし、かつ、フラグ情報がそのデータフレームの伝送の阻止を許容しないことを示す場合において、特定のＥＣＵが異常であることを検出したときには、そのフラグ情報を伝送の阻止を許容することを示すように更新することとしても良い。例えばエンジンＥＣＵ１００ａ、ブレーキＥＣＵ１００ｂ等といった車両の走る、曲がる、或いは止まることの制御に関わるＥＣＵを、上述の特定のＥＣＵとして定めておくことが有用である。また、ゲートウェイ機能を有するゲートウェイＥＣＵ、車両の運転者へのユーザインタフェースを提供するヘッドユニットＥＣＵ等を上述の特定のＥＣＵとして定めておくことも有用である。特定のＥＣＵの異常は、特定のＥＣＵが送信するフレームの内容、特定のＥＣＵを監視する監視ＥＣＵ等からの通知、特定のＥＣＵの制御対象のアクチュエータ等に関連するセンサでの測定結果、特定のＥＣＵとの個別通信による検査結果等に基づいて検出し得る。例えば、エンジン回転数のセンサによる測定値がある単位時間に通常範囲を超えて急上昇した場合に、エンジンＥＣＵの異常を検出できる。例えば、車両の加速度の急激な変化をエンジンＥＣＵ或いはブレーキＥＣＵの異常と検出しても良い。これにより、不正なデータフレームが検知され、車両の走行に影響するＥＣＵに異常が発生したような場合に、その後の不正なデータフレームの伝送が阻止されるようになる。また、車載ネットワークシステムへの不正でない新たなＥＣＵの追加等により、そのＥＣＵが送信したデータフレームが不正と検知された場合においても、車両の走行に影響するＥＣＵに異常が発生していないようなときには、そのデータフレームの伝送は阻止されず、阻止による悪影響が防止される。また、不正検知ＥＣＵ１４００は、アクティベート指示情報を含む異常通知メッセージを他の車両に送信する場合（ステップＳ２１０２）において、自車両の管理情報についても同様に伝送阻止機能がアクティベートされた状態となるように更新しても良い。具体例としては、不正検知ＥＣＵ１４００は、不正と検知したデータフレームが車両に異常を引き起こすと判定した場合においてそのデータフレー

ムのＩＤに対応するフラグ情報を伝送阻止機能がアクティベートされた状態を示すようにし、そのＩＤを有するデータフレームに対してエラーフレームの送信で伝送阻止を行う。そして、そのＩＤを有するデータフレームの伝送の阻止を許容するアクティベート指示情報を含むメッセージを他の車両に送信する。

【０１８５】

（５）上記実施の形態では、不正検知ＥＣＵ４００、１４００が、不正なデータフレームを検知するために、ＩＤフィールドに係る正規ＩＤリストを用いたが、ＩＤフィールド以外のフィールドの値を用いてもよい。つまり、フレーム伝送阻止装置において、管理情報次第で伝送阻止の対象となるフレームの所定条件として、ＩＤを用いる例を示したが、そのフレームのＩＤ以外についての条件を定めても良い。例えば、所定条件は、フレームとしてのデータフレームのＤＬＣについての条件であっても良いし、データフレームのデータフィールド内のデータについての条件であっても良い。また、車載ネットワークシステムにおいてＥＣＵ間で授受されるフレームにメッセージ認証コード（ＭＡＣ：Message Authentication Code）を含ませるように定めておく場合において、所定条件は、フレームに適正なＭＡＣが含まれない場合に満たされる条件であっても良い。フレームに適正なＭＡＣが含まれるか否かは、例えば、フレーム中の予め特定可能に規定された位置に所在するデータ値としてのＭＡＣを、予め定められた検証方法によって検証して、検証に成功するか否かで判別可能である。また、所定条件は、フレームが送信される周期、頻度等に係る条件であっても良い。

【０１８６】

（６）上記実施の形態では、フレーム伝送阻止装置としての不正検知ＥＣＵ４００、１４００において不正検知ルールによってフレームの不正を検知し、不正と検知されたフレームの伝送阻止機能のアクティベート状態の変更を、ＦＷの更新等によって行う例を示した。しかし、ＦＷの更新により、伝送阻止機能のアクティベート状態の変更の代わりに不正検知ルールを更新しても良い。具体的には、製品出荷時において不正検知ＥＣＵ４００は、全てのＩＤを不正ではないと扱うよう定めた不正検知ルールを保持するようにしておき、伝送阻止機能は既にアクティベートされている状態としておき、ＦＷの更新により、不正なフレームの伝送を阻止するように、不正検知ルールの方を変更するようにしても良い。

【０１８７】

（７）上記実施の形態では、不正検知ＥＣＵ４００が、サーバ５００に送信する不正検知メッセージに含ませる、不正と検知されたデータフレームに関するログ情報は、そのデータフレームの検知後の一定時間にバス２００に流れたデータフレームについてのログデータ等を含むこととした。そして、サーバ５００が、ログ情報を分析することで、車両の動作不良等といった車載ネットワークシステム１０に係る異常を引き起こす不正なデータフレームであるか否かを判断する例を示した。しかし、不正検知ＥＣＵ４００は、不正なデータフレームを検知した後の一定時間ではなく、検知前の一定時間、或いはその検知の前後に亘る一定時間の間にバス２００から受信された各種のデータフレームの内容と受信時刻等といった情報を、ログ情報に含ませることとしても良い。また、不正検知ＥＣＵ４００は、不正なデータフレームを検知した前の一定時間、又はその検知の前後に亘る一定時間の間にバス２００から受信されたデータフレームに基づいて、不正と検知したデータフレームによって異常が引き起こされているか否かを判定しその異常が引き起こされていれば不正と検知したデータフレームについての伝送阻止機能をアクティベートすることとしても良い。

【０１８８】

（８）上記実施の形態２では、不正検知ＥＣＵ１４００は、車種情報が、自装置が搭載されている車両と同じ車種を示すか否かを判定することとしたが、これは、動作不良等の異常の起きた車両と、自装置が搭載されている車両との共通性を判定して、伝送阻止機能をアクティベートするか否かを決める一例であり、車種情報以外にも、車両の年式、型式、モデル、製造メーカ等の情報を用いて、共通性を判定しても良い。

【０１８９】
（９）上記実施の形態２では、ＩＤで対象フレームを特定して、伝送阻止機能のアクティベート又はディアクティベートの指示が行われる例を示したが、全てのフレームを対象に一括でアクティベート又はディアクティベートの指示が行われることとしても良い。また、対象フレームの特定の方法は、ＩＤに限られず、例えば、フレーム中の特定位置のビット列等で特定しても良い。また、アクティベート指示情報又はディアクティベート指示情報が、ＦＷで表され、不正検知ＥＣＵのＦＷの更新によって伝送阻止機能のアクティベート状態が変更されることとしても良い。また、管理情報は、必ずしもＩＤ毎のフラグ情報で構成されている必要はなく、不正と検知された全てのデータフレームの伝送の阻止を許容するか否かを示す１つのフラグだけで構成されても良い。

【０１９０】
（１０）上記実施の形態で或いは上述の変形例で示したフレーム伝送阻止装置の構成要素は、バス２００に接続された複数のＥＣＵ等といった複数の装置に分散して備えられても良い。また、フレーム伝送阻止装置は、自装置内に保持される管理情報を参照する代わりに、自装置の外部から得られた管理情報を参照することで、不正と検知されたフレームについての伝送の阻止のための所定処理（例えばエラーフレームの送信等）を行うか否かを切り替えても良い。この場合に、不正と検知されたフレームの伝送の阻止を許容するか否かを示す管理情報は、ハードディスクその他の記憶媒体に記憶された情報を読み出して参照されても良いし、スイッチその他のハードウェアにより形成された状態を読み取ることで参照されても良いし、外部から情報を受信することで参照されても良い。

【０１９１】
（１１）上記の実施の形態では、車載ネットワークでＣＡＮプロトコルに従って、データフレームの伝送が行われるものとしたが、ＣＡＮプロトコルは、オートメーションシステム内の組み込みシステム等に用いられるＣＡＮＯｐｅｎ、或いは、ＴＴＣＡＮ（Time-Triggered CAN）、ＣＡＮＦＤ（CAN with Flexible Data Rate）等の派生的なプロトコルを包含する広義の意味のものと扱われることとしても良い。また、車載ネットワークは、ＣＡＮプロトコル以外のプロトコルを用いるものであっても良い。車両の制御のためのフレーム等の伝送がなされる車載ネットワークのプロトコルとして、例えばＬＩＮ（Local Interconnect Network）、ＭＯＳＴ（登録商標）（Media Oriented Systems Transport）、ＦｌｅｘＲａｙ（登録商標）、Ｅｔｈｅｒｎｅｔ（登録商標）等を用いても良い。また、これらのプロトコルを用いたネットワークをサブネットワークとして、複数種類のプロトコルに係るサブネットワークを組み合わせて、車載ネットワークを構成しても良い。また、Ｅｔｈｅｒｎｅｔ（登録商標）プロトコルは、ＩＥＥＥ８０２．１に係るＥｔｈｅｒｎｅｔ（登録商標）ＡＶＢ（Audio Video Bridging）、或いは、ＩＥＥＥ８０２．１に係るＥｔｈｅｒｎｅｔ（登録商標）ＴＳＮ（Time Sensitive Networking）、Ｅｔｈｅｒｎｅｔ（登録商標）／ＩＰ（Industrial Protocol）、ＥｔｈｅｒＣＡＴ（登録商標）（Ethernet（登録商標） for Control Automation Technology）等の派生的なプロトコルを包含する広義の意味のものと扱われることとしても良い。なお、車載ネットワークのネットワークバスは、例えば、ワイヤ、光ファイバ等で構成される有線通信路であり得る。例えば、フレーム伝送阻止装置２４００は、上述のいずれかのプロトコルを用いてＥＣＵが通信するネットワークシステムでネットワークバスに接続され、フレームを受信し、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、受信されたフレームが所定条件を満たす場合にそのフレームの伝送を阻止する所定処理を実行するか否かを切り替えるようにしても良い。

【０１９２】
（１２）上記実施の形態では、ＣＡＮプロトコルにおけるデータフレームを標準ＩＤフォーマットで記述しているが、拡張ＩＤフォーマットであっても良く、データフレームのＩＤは、拡張ＩＤフォーマットでの拡張ＩＤ等であっても良い。また、上述したデータフレームは、ＣＡＮ以外のプロトコルが用いられるネットワークにおける一種のフレームであっても良く、この場合に、そのフレームの種類等を識別するＩＤが、データフレームの

ＩＤに相当する。

【０１９３】

（１３）上記実施の形態では、フレーム伝送阻止装置が、車両に搭載され、車両の制御のための通信を行う車載ネットワークシステムに含まれる例を示したが、車両以外の制御対象の制御のためのネットワークシステムに含まれるものであっても良い。車両以外の制御対象は、例えば、ロボット、航空機、船舶、機械等である。

【０１９４】

（１４）上記実施の形態で示したＥＣＵ等の各装置は、メモリ、プロセッサ等の他に、ハードディスクユニット、ディスプレイユニット、キーボード、マウス等を備えるものであっても良い。また、上記実施の形態で示したＥＣＵ等の各装置は、メモリに記憶されたプログラムがプロセッサにより実行されてソフトウェア的にその各装置の機能を実現するものであっても良いし、専用のハードウェア（デジタル回路等）によりプログラムを用いずにその機能を実現するものであっても良い。また、その各装置内の各構成要素の機能分担は変更可能である。

【０１９５】

（１５）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。更には、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行っても良い。バイオ技術の適用等が可能性としてあり得る。

【０１９６】

（１６）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。

【０１９７】

（１７）本発明の一態様としては、例えば図１４、図１５、図１７、図２２、図２３、図２６、図２７、図２９等に示す処理手順の全部又は一部を含むフレーム伝送阻止方法であるとしても良い。例えば、フレーム伝送阻止方法は、複数のＥＣＵがバスを介して通信するネットワークシステムで用いられ、バスからフレームを受信する受信ステップ（例えばステップＳ１００２）と、フレームの伝送の阻止を許容するか否かを示す管理情報に基づいて、受信ステップで受信されたフレームが所定条件を満たす場合にそのフレームの伝送を阻止する所定処理を実行するか否かを切り替える処理ステップ（例えばステップＳ１００６～Ｓ１００８）とを含む方法である。また、本発明の一態様としては、この方法をコンピュータにより実現するプログラム（コンピュータプログラム）であるとしても良いし、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。

【０１９８】

（１８）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】

【０１９９】

本発明は、車載ネットワーク等のネットワークへの不正なフレームの伝送を阻止するために利用可能である。

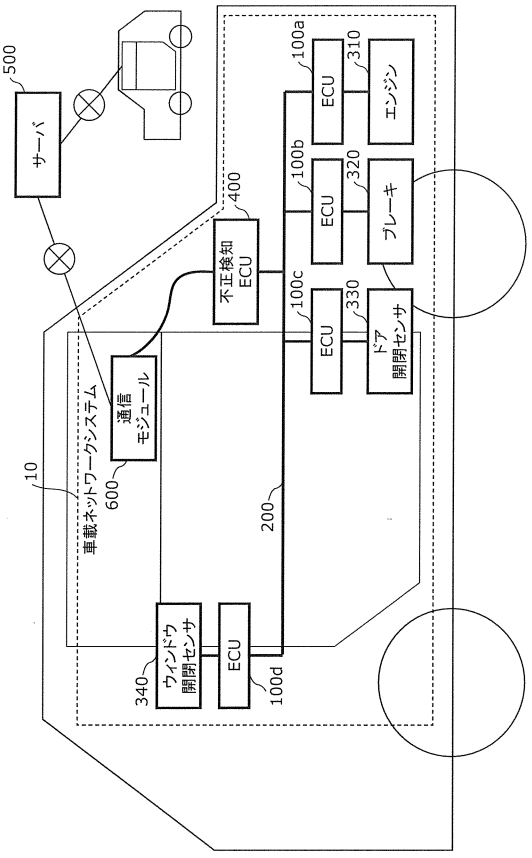
【符号の説明】

【０２００】

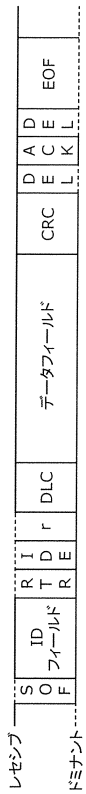
１０、１１　車載ネットワークシステム
１００ａ　電子制御ユニット（エンジンＥＣＵ）
１００ｂ　電子制御ユニット（ブレーキＥＣＵ）
１００ｃ　電子制御ユニット（ドア開閉センサＥＣＵ）
１００ｄ　電子制御ユニット（ウィンドウ開閉センサＥＣＵ）
１１０、４１０　フレーム送受信部
１２０、４２０　フレーム解釈部
１３０　受信ＩＤ判断部
１４０　受信ＩＤリスト保持部
１５０　フレーム処理部
１６０　フレーム生成部
１７０　データ取得部
２００　バス
３１０　エンジン
３２０　ブレーキ
３３０　ドア開閉センサ
３４０　ウィンドウ開閉センサ
４００、１４００　不正検知ＥＣＵ（フレーム伝送阻止装置）
４３０　不正検知処理部
４３１　不正検知ルール保持部
４４０、１４４０　状態確認部
４４１　状態保持部
４５０　フレーム生成部
４６０、１４６０　更新処理部
４７０、１４７０　外部通信部
４８０、５５０　署名処理部
４８１、５６０　鍵保持部

４９１　車種情報保持部
４９２　車台番号情報保持部
５００、１５００　サーバ
５１０、２４４０　通信部
５２０、１５２０　分析部
５３０　ＦＷ保持部
５４０　配信メッセージ生成部
６００、１６００　通信モジュール
１５４０　メッセージ生成部
２４００　フレーム伝送阻止装置
２４１０　受信部
２４２０　処理部
２４２１　送信部
２４３０　記憶部
２４５０　更新部

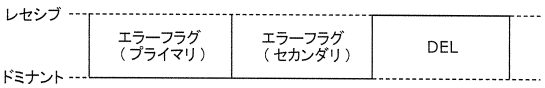
【図１】



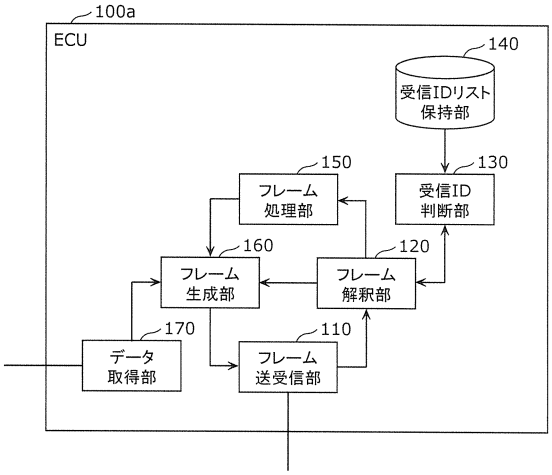
【図２】



【図３】



【図４】



【図５】

IDリスト
(ALL)

【図６】

ID	データ
1	0
1	1
1	2
1	3
1	4
…	…

【図７】

ID	データ
2	100
2	90
2	80
2	70
2	60
…	…

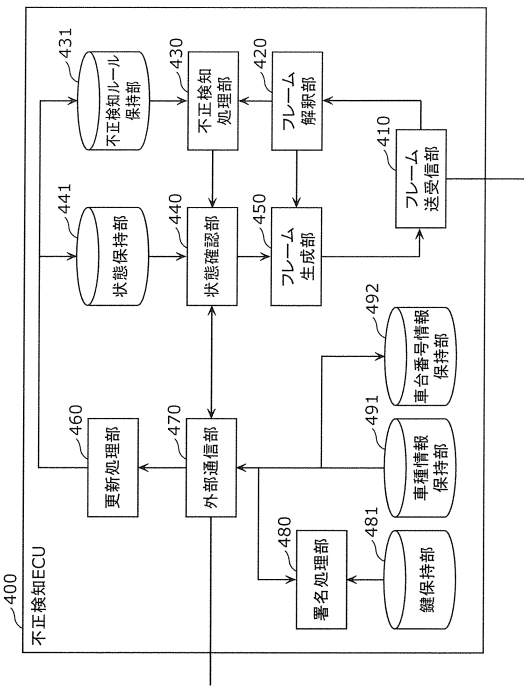
【図８】

ID	データ
3	1
3	1
3	0
3	0
3	0
…	…

【図９】

ID	データ
4	0
4	10
4	20
4	30
4	40
…	…

【図１０】



【図１１】

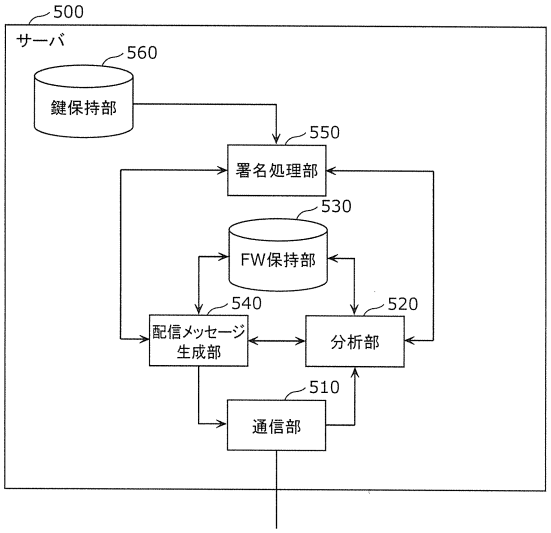
ID
1
2
3
4

【図１２】

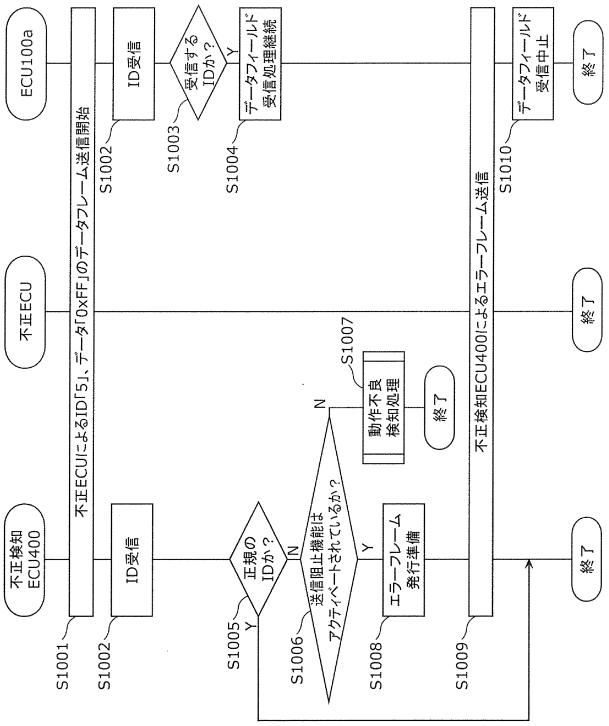
管理情報

0 (ID「1」用フラグ情報)
0 (ID「2」用フラグ情報)
0 (ID「3」用フラグ情報)
0 (ID「4」用フラグ情報)
1 (ID「5」用フラグ情報)
0 (ID「6」用フラグ情報)
⋮

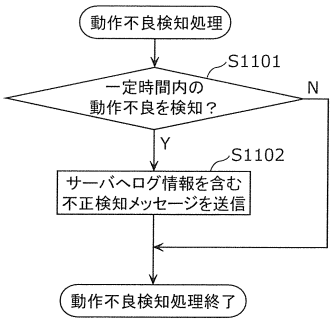
【図１３】



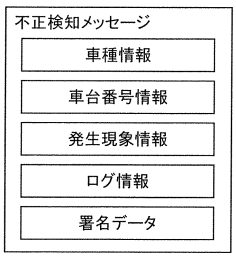
【図１４】



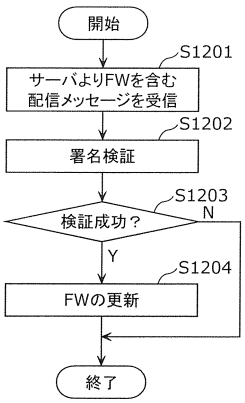
【図１５】



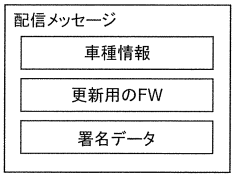
【図１６】



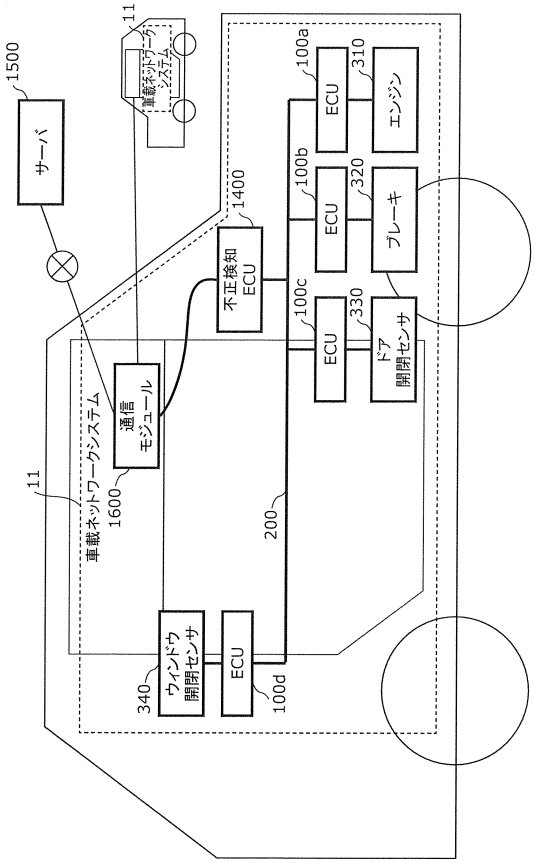
【図１７】



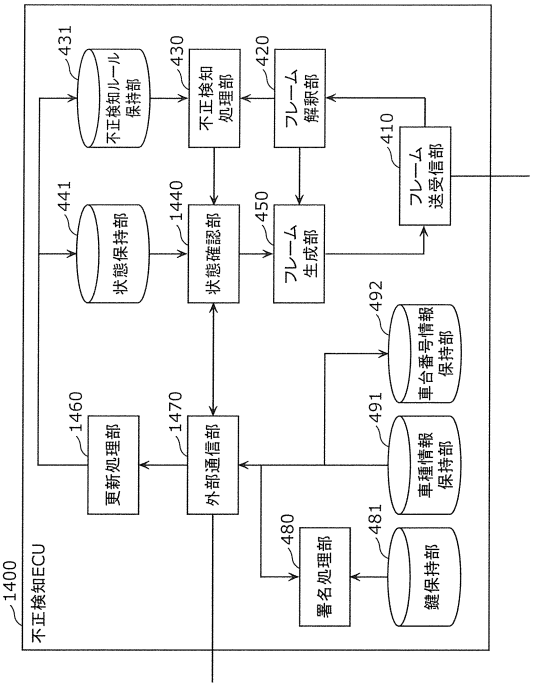
【図１８】



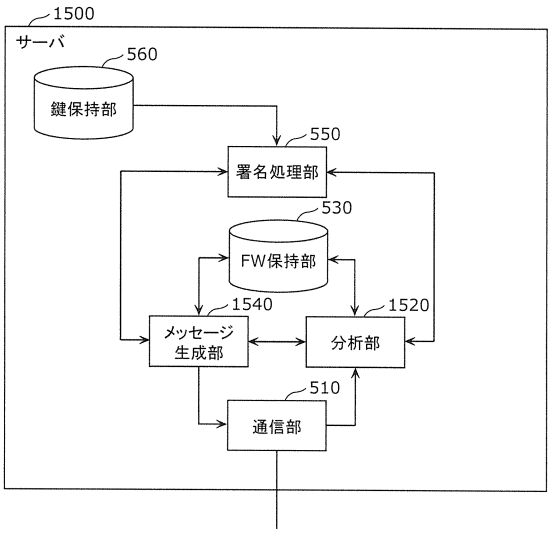
【図１９】



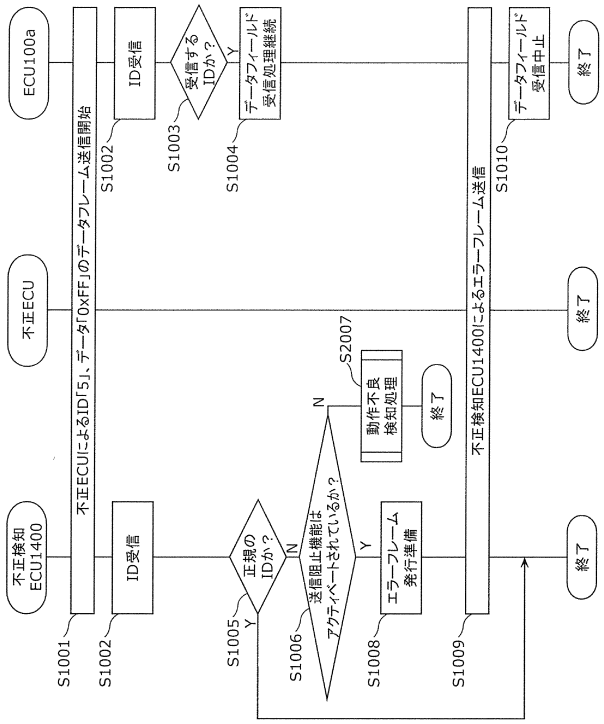
【図２０】



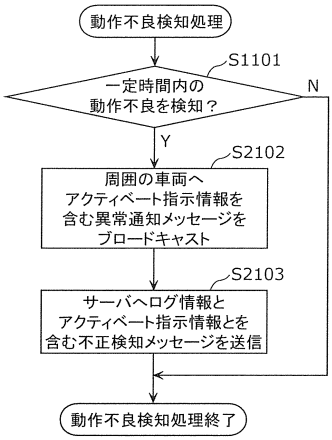
【図２１】



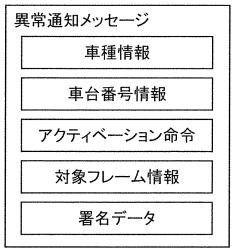
【図２２】



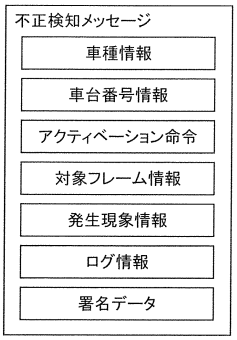
【図２３】



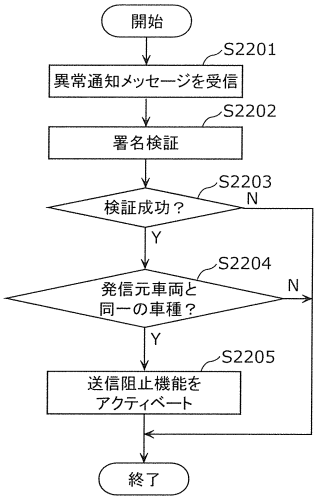
【図２４】



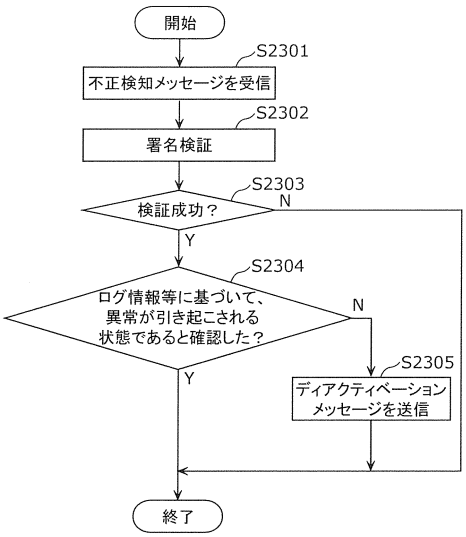
【図２５】



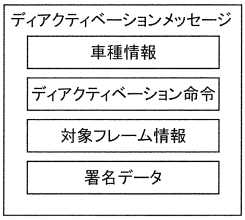
【図２６】



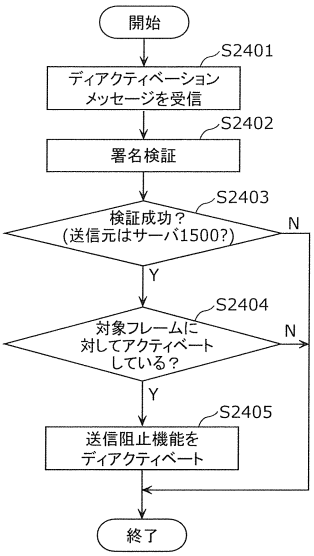
【図２７】



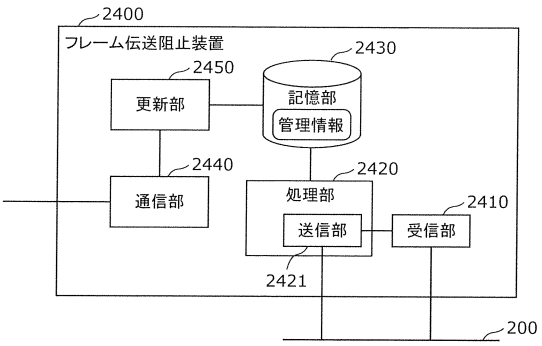
【図２８】



【図２９】



【図３０】


2400
フレーム伝送阻止装置
2430
2450
更新部
記憶部
管理情報
2440
通信部
2420
処理部
2410
送信部
受信部
2421
200

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 安齋 潤
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

審査官 宮島 郁美

(56)参考文献 特開２０１４－２３６２４８（ＪＰ，Ａ）
特開２０１６－１３４９１３（ＪＰ，Ａ）
特開２０１６－１３４９１４（ＪＰ，Ａ）
国際公開第２０１５／１５９５２０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／２８，１２／４４－１２／４６