(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6539363号
(P6539363)
(45)発行日　令和1年7月3日(2019.7.3)　(24)登録日　令和1年6月14日(2019.6.14)

(51)Int.Cl.　F I
H04L 12/28 (2006.01)　H04L 12/28 200M
H04L 12/66 (2006.01)　H04L 12/28 100A
H04L 12/66 B

請求項の数 13　(全 40 頁)

(21)出願番号　特願2018-19993(P2018-19993)
(22)出願日　平成30年2月7日(2018.2.7)
(65)公開番号　特開2018-182724(P2018-182724A)
(43)公開日　平成30年11月15日(2018.11.15)
審査請求日　平成30年12月25日(2018.12.25)
(31)優先権主張番号　特願2017-76568(P2017-76568)
(32)優先日　平成29年4月7日(2017.4.7)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(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】不正通信検知方法、不正通信検知システム及びプログラム

(57)【特許請求の範囲】
【請求項１】
記憶部を含む情報処理システムで実行される、ネットワーク及び前記ネットワークに接続される１以上の電子制御ユニットを含む車載ネットワークシステムにおける不正通信の検知方法であって、
前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知ステップと、
前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存する情報保存ステップと、
前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別する通信パターン識別ステップと、
前記メッセージが、前記通信パターン識別ステップで識別された通信パターンに適合するか否かを判定する通信パターン判定ステップとを含み、
少なくとも前記不正検知ステップ及び前記通信パターン判定ステップは、前記ネットワークに順次送出されて受信された複数のメッセージのそれぞれに対して実行され、
前記通信パターン判定ステップの実行後に受信されたメッセージに対して実行される前記不正検知ステップでは、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定ステップにおける判定結果を用い、
前記情報保存ステップでは、前記不正検知ステップにおいて攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存する

、
不正通信検知方法。
【請求項２】
前記通信パターン識別ステップでは、前記通信パターンとして、前記複数のメッセージに含まれるデータ値の変化に関するパターンが識別される、
請求項１に記載の不正通信検知方法。
【請求項３】
前記データ値の変化に関するパターンは、前記複数のメッセージに含まれる同じ種類のデータ量を表す複数のメッセージそれぞれに含まれる前記データ値の変化の有無に関するパターン、前記同じ種類のデータ量を表す複数のメッセージに含まれるデータ量の増加若しくは減少に関するパターン、又は前記同じ種類のデータ量を表すメッセージに含まれるデータ値と、他の種類のデータ量を表すメッセージに含まれるデータ値との差分若しくは比に関するパターンである、
請求項２に記載の不正通信検知方法。
【請求項４】
前記通信パターン識別ステップでは、前記通信パターンとして、前記複数のメッセージの通信タイミングに関するパターンが識別される、
請求項１に記載の不正通信検知方法。
【請求項５】
前記複数のメッセージの通信タイミングに関する通信パターンは、前記複数のメッセージに含まれる同じ種類のデータ量を表す複数のメッセージの送信時刻の間隔に関するパターン、又は前記同じ種類のデータ量を表す複数のメッセージ同士又は異なる種類のデータ量を表すメッセージ間の送信時刻の差分に関するパターンである、
請求項４に記載の不正通信検知方法。
【請求項６】
前記通信パターン識別ステップにおいて、前記攻撃メッセージに関する情報に統計学的処理を実行して得られるモデルを前記通信パターンとして取得することで前記通信パターンを識別し、
さらに、前記通信パターンを用いて、次に受信されるメッセージに含まれるデータ値の予測値を算出するデータ値予測ステップを含み、
前記通信パターン判定ステップにおいて、前記予測値と、前記受信されたメッセージが含むデータ値との比較の結果に基づいて当該受信されたメッセージが前記通信パターンに適合するか否かを判定する、
請求項１から５のいずれか一項に記載の不正通信検知方法。
【請求項７】
前記通信パターン識別ステップでは、さらに前記グレーメッセージに関する情報を前記統計学的処理の実行の対象として前記通信パターンを取得する、
請求項６に記載の不正通信検知方法。
【請求項８】
前記不正検知ステップは、所定のタイミングで前記グレーメッセージが攻撃メッセージであるか否かを判定する、
請求項１から５のいずれか一項に記載の不正通信検知方法。
【請求項９】
前記車載ネットワークシステムを搭載する車両は、運転者による当該車両の運転行動の少なくとも一部を支援又は代行するための自動運転機能を備え、
さらに、前記自動運転機能が実行中であるか否かを認識する車両状態認識ステップを含み、
前記情報保存ステップは、前記車両状態認識ステップにおいて前記自動運転機能が実行中でないと認識されているときに実行され、
前記通信パターン判定ステップは、前記車両状態認識ステップにおいて前記自動運転機

能が実行中であると認識されているときに実行される、
請求項１から８のいずれか一項に記載の不正通信検知方法。
【請求項１０】
前記攻撃メッセージは、前記車載ネットワークシステムに含まれる前記１以上の電子制御ユニットのいずれかによって前記ネットワークに送出され、
前記不正検知ステップ、前記情報保存ステップ、前記通信パターン識別ステップ、及び前記通信パターン判定ステップの少なくとも一部は、前記攻撃メッセージを送出する電子制御ユニットとは別の前記車載ネットワークシステムに含まれる電子制御ユニット、又は前記車載ネットワークシステムがさらに含むゲートウェイによって実行される
請求項１から９のいずれか一項に記載の不正通信検知方法。
【請求項１１】
前記車載ネットワークシステムに含まれる前記１以上の電子制御ユニットの少なくとも１つは、前記車載ネットワークシステムの外部から送信されたデータを取得する送信データ取得部を備え、
前記送信データ取得部を備える前記電子制御ユニットは、前記車載ネットワークシステムの外部から送信されたデータに含まれるメッセージに対して少なくとも前記不正検知ステップを実行する
請求項１から１０のいずれか一項に記載の不正通信検知方法。
【請求項１２】
ネットワーク及び前記ネットワークに接続される１以上の電子制御ユニットを含む車載ネットワークシステムにおける不正制御を検知するための不正通信検知システムであって、
１個以上のプロセッサと、
記憶部とを含み、
前記１個以上のプロセッサは、前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知を実行し、
前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存し、
前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別し、
前記メッセージが、識別された前記通信パターンに適合するか否かを判定する通信パターン判定を実行し、
少なくとも前記不正検知及び前記通信パターン判定は、前記ネットワークに順次送出された複数のメッセージのそれぞれに対して実行し、
前記通信パターン判定の実行後に送出されたメッセージに対する前記不正検知において、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定における判定結果を用い、
前記不正検知の実行において攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存する、
不正通信検知システム。
【請求項１３】
ネットワーク及び前記ネットワークに接続される１以上の電子制御ユニットを含む車載ネットワークシステムにおける不正通信を検知するためのシステムであって、１個以上のプロセッサと記憶部とを含む不正通信検知システムにおいて、前記１個以上のプロセッサに請求項１に記載の不正通信検知方法を実施させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車載ネットワークにおける不正メッセージの通信を検知する検知方法等に関する。

【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，以下、ＥＣＵとも表記する）と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐ通信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規格の一つに、Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅｔｗｏｒｋ（以降、ＣＡＮ）がある。
【０００３】
ＣＡＮの規格に拠るネットワーク（以下、ＣＡＮネットワークともいう）では、通信路（バス）は２本のケーブルで構成され、バスに接続されているＥＣＵはノードとも呼ばれる。バスに接続されている各ノードは、フレーム又はメッセージと呼ばれる単位でデータを送受信する。またＣＡＮでは、データの送信先又は送信元を示す識別子は用いられない。フレームを送信するノード（以下、送信ノードともいう）は、メッセージごとにメッセージの種類を示すメッセージＩＤと呼ばれるＩＤを付けて送信、つまりバスに信号を送出する。メッセージを受信するノード（以下、受信ノードともいう）は、あらかじめ決められたメッセージＩＤを含むメッセージのみ受信、つまりバスから信号を読み取る。同一ＩＤのメッセージは、所定の一定の周期で送信される。
【０００４】
上述の通り、自動車の中のシステムに多数配置されているＥＣＵは、それぞれがＣＡＮネットワークに接続され、様々なメッセージを互いにやりとりしながら動作している。ここで、ＣＡＮネットワークの外部と通信機能を持つＥＣＵが外部から攻撃される等して乗っ取られ、ＣＡＮネットワークに対して不正なメッセージ（以降、攻撃メッセージ）を送信するようになることが起こり得る。このような乗っ取られたＥＣＵ（以下、不正ＥＣＵともいう）は、例えば他のＥＣＵになりすまして攻撃メッセージを送信することで、自動車を不正に制御することが可能となる。このような、いわゆるなりすまし攻撃を検知するための方法として、例えば、特許文献１に記載の方法がある。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】国際公開第２０１４／１１５４５５号
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、特許文献１に記載の方法では、発生しているなりすまし攻撃を検知できるだけであり、どのメッセージが攻撃メッセージかを判断できないという課題がある。
【０００７】
本発明は、上記課題を解決するもので、バスに送出された個々のメッセージが攻撃メッセージであるか否かを判定する不正通信検知方法、不正通信検知システム等を提供することを目的とする。
【課題を解決するための手段】
【０００８】
上記課題を解決するために、本開示の一態様に係る不正通信検知方法は、記憶部を含む情報処理システムで実行される、ネットワーク及び前記ネットワークに接続される１以上の電子制御ユニットを含む車載ネットワークシステムにおける不正通信の検知方法であって、前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知ステップと、前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存する情報保存ステップと、前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別する通信パターン識別ステップと、前記メッセージが、前記通信パターン識別ステップで識別された通信パター

ンに適合するか否かを判定する通信パターン判定ステップとを含み、少なくとも前記不正検知ステップ及び前記通信パターン判定ステップは、前記ネットワークに順次送出されて受信された複数のメッセージのそれぞれに対して実行され、前記通信パターン判定ステップの実行後に受信されたメッセージに対して実行される前記不正検知ステップでは、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定ステップにおける判定結果を用い、前記情報保存ステップでは、前記不正検知ステップにおいて攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存する。

【０００９】

なお、これらの包括的又は具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラム又はコンピュータ読み取り可能なＣＤ－ＲＯＭなどの非一時的な記録媒体で実現されてもよく、システム、装置、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

【発明の効果】

【００１０】

本開示の一態様に係る不正通信検知方法等によれば、バスに送出された個別のメッセージが攻撃メッセージであるか否かを判定することができる。

【図面の簡単な説明】

【００１１】

【図１】図１は、実施の形態１における車載ネットワークシステムの全体構成を示すブロック図である。

【図２】図２は、ＣＡＮプロトコトルのデータフレームフォーマットを示す図である。

【図３】図３は、本開示における車載ネットワークシステムに含まれるゲートウェイの機能構成の一例を示すブロック図である。

【図４】図４は、実施の形態１における受信ＩＤリストのデータ構成の一例を示す図である。

【図５】図５は、実施の形態１におけるゲートウェイで保持される転送ルールのデータ構成の一例を示す図である。

【図６】図６は、実施の形態１における不正検知処理機能群の機能構成の一例を示すブロック図である。

【図７】図７は、実施の形態１における不正検知部の機能構成を示すブロック図である。

【図８】図８は、実施の形態１における不正検知処理機能群の機能構成の他の例を示すブロック図である。

【図９】図９は、実施の形態１における上記の車載ネットワークシステムに含まれるＥＣＵの機能構成の一例を示すブロック図である。

【図１０】図１０は、実施の形態１における不正検知処理の一例を示すフロー図である。

【図１１】図１１は、実施の形態１における転送処理の一例を示すフロー図である。

【図１２】図１２は、実施の形態２における不正検知処理機能群の機能構成の一例を示すブロック図である。

【図１３】図１３は、実施の形態２における不正検知処理機能群の機能構成の他の例を示すブロック図である。

【図１４】図１４は、実施の形態２における不正検知処理の一例を示すフロー図である。

【図１５】図１５は、実施の形態３における車載ネットワークシステムの全体構成を示すブロック図である。

【図１６】図１６は、本開示における車載ネットワークシステムに含まれるゲートウェイの機能構成の他の例を示すブロック図である。

【図１７】図１７は、実施の形態３における不正検知処理機能群の機能構成の一例を示すブロック図である。

【図１８】図１８は、実施の形態３における不正検知処理機能群の機能構成の他の例を示すブロック図である。

【図１９】図１９は、実施の形態３におけるサーバの構成の一例を示すブロック図である。
【図２０】図２０は、変形例における不正検知処理機能群の機能構成の一例を示す図である。
【図２１】図２１は、変形例における不正検知処理機能群の機能構成の他の例を示すブロック図である。
【図２２】図２２は、変形例における不正検知処理機能群の機能構成の他の例を示すブロック図である。
【図２３】図２３は、変形例における不正検知処理機能群の機能構成の他の例を示すブロック図である。
【図２４】図２４は、変形例におけるＥＣＵの機能構成の一例を示すブロック図である。
【図２５】図２５は、変形例におけるＥＣＵの機能構成の一例を示すブロック図である。
【図２６】図２６は、変形例におけるＥＣＵの機能構成の一例を示すブロック図である。
【発明を実施するための形態】
【００１２】
（本開示の基礎になった知見）
不正ＥＣＵから攻撃メッセージが送信され始めると、ＣＡＮネットワークでは同じＩＤのメッセージに正常メッセージと攻撃メッセージとが混在するようになる。このような状況では、正常なメッセージの送信のタイミングと攻撃メッセージの送信のタイミングとがごく近くなる、又は攻撃者によって意図的に近づけられた結果、攻撃メッセージの送信のタイミングも許容差内に収まる場合がある。このような場合には、正常メッセージと攻撃メッセージとの区別が難しくなり、誤検知の発生の可能性が高まる。同様のことは、メッセージの送信のタイミングのみならず、メッセージが含むデータ値についても起こる。
【００１３】
そこで、本開示の一態様に係る不正通信検知方法は、記憶部を含む情報処理システムで実行される、ネットワーク及び前記ネットワークに接続される１以上の電子制御ユニットを含む車載ネットワークシステムにおける不正通信の検知方法であって、前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知ステップと、前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存する情報保存ステップと、前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別する通信パターン識別ステップと、前記メッセージが、前記通信パターン識別ステップで識別された通信パターンに適合するか否かを判定する通信パターン判定ステップとを含み、少なくとも前記不正検知ステップ及び前記通信パターン判定ステップは、前記ネットワークに順次送出されて受信された複数のメッセージのそれぞれに対して実行され、前記通信パターン判定ステップの実行後に受信されたメッセージに対して実行される前記不正検知ステップでは、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定ステップにおける判定結果を用い、前記情報保存ステップでは、前記不正検知ステップにおいて攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存する。
【００１４】
これにより、車載ネットワークシステムに送出されたメッセージが攻撃メッセージであるか否かが、攻撃メッセージの特徴を反映するパターンに照らして判定される。その結果、個々のメッセージが攻撃メッセージであるか否かの判定は、より高い精度で実行される。
【００１５】
また例えば、前記通信パターン識別ステップでは、前記通信パターンとして、前記複数のメッセージに含まれるデータ値の変化に関するパターンが識別されてもよい。より具体的には、前記データ値の変化に関するパターンは、前記複数のメッセージに含まれる同じ種類のデータ量を表す複数のメッセージそれぞれに含まれる前記データ値の変化の有無に

関するパターン、前記同じ種類のデータ量を表す複数のメッセージに含まれるデータ量の増加若しくは減少に関するパターン、又は前記同じ種類のデータ量を表すメッセージに含まれるデータ値と、他の種類のデータ量を表すメッセージに含まれるデータ値との差分若しくは比に関するパターンであってもよい。

【００１６】

これにより、個々のメッセージが攻撃メッセージであるか否かの判定は、メッセージ間のデータ値の変化又はその変化の有無に関するパターンに照らして行われるため、より高い精度での実行が可能である。

【００１７】

また例えば、前記通信パターン識別ステップでは、前記通信パターンとして、前記複数のメッセージの通信タイミングに関するパターンが識別されてもよい。より具体的には、前記複数のメッセージの通信タイミングに関する通信パターンは、前記複数のメッセージに含まれる同じ種類のデータ量を表す複数のメッセージの送信時刻の間隔に関するパターン、又は前記同じ種類のデータ量を表す複数のメッセージ同士又は異なる種類のデータ量を表すメッセージ間の送信時刻の差分に関するパターンであってもよい。

【００１８】

これにより、個々のメッセージが攻撃メッセージであるか否かの判定は、メッセージ間の受信間隔に関するパターンに照らして行われるため、より高い精度での実行が可能である。

また、前記不正検知ステップは、所定のタイミングで前記グレーメッセージが攻撃メッセージであるか否かを判定してもよい。

これにより、一時的には攻撃メッセージであるか否かの判定が困難なために判定が保留されたメッセージに対して、再度の判定が実行される。このように再度の判定で攻撃メッセージであるか否か判定の結果が得られれば、その結果はその後の判定に用いられる通信パターンの増強に役立てられ、より高い精度での判定の実行を可能にする。

【００１９】

また例えば、前記通信パターン識別ステップにおいて、前記攻撃メッセージに関する情報に統計学的処理を実行して得られるモデルを前記通信パターンとして取得することで前記通信パターンを識別し、さらに、前記通信パターンを用いて、次に受信されるメッセージに含まれるデータ値の予測値を算出するデータ値予測ステップを含み、前記通信パターン判定ステップにおいて、前記予測値と、前記受信されたメッセージが含むデータ値との比較の結果に基づいて当該受信されたメッセージが前記通信パターンに適合するか否かを判定してもよい。より具体的には、前記通信パターン識別ステップにおいて、前記モデルとして、ＡＲ（ＡｕｔｏＲｅｇｒｅｓｓｉｖｅ）モデル、ＡＲＭＡ（ＡｕｔｏＲｅｇｒｅｓｓｉｖｅ　Ｍｏｖｉｎｇ　Ａｖｅｒａｇｅ）モデル、ＨＭＭ（Ｈｉｄｄｅｎ　Ｍａｒｋｏｖ　Ｍｏｄｅｌ）、又はベイジアン（Ｂａｙｅｓｉａｎ）モデルを取得してもよい。

【００２０】

これにより、個々のメッセージが攻撃メッセージであるか否かの判定には、攻撃メッセージが持ち得る値として予測されるデータ値が用いられるため、実際にあった攻撃パターンどおりでない攻撃であっても検知できる可能性が高まる。したがって、車載ネットワークシステムの安全をより確実に守ることができる。

【００２１】

また例えば、前記通信パターン識別ステップでは、さらに前記グレーメッセージに関する情報を前記統計学的処理の実行の対象として前記通信パターンを取得してもよい。

【００２２】

これにより、一時的には攻撃メッセージであるか否かの判定が困難なメッセージの当該判定を保留し、事後的に判定をすることができる。このように事後的な判定の結果は、その後の判定に用いられる通信パターンの増強に役立てられ、より高い精度での判定の実行を可能にする。

【００２３】

また例えば、前記車載ネットワークシステムを搭載する車両は、運転者による当該車両の運転行動の少なくとも一部を支援又は代行するための自動運転機能を備え、さらに、前記自動運転機能が実行中であるか否かを認識する車両状態認識ステップを含み、前記情報保存ステップは、前記車両状態認識ステップにおいて前記自動運転機能が実行中でないと認識されているときに実行され、前記通信パターン判定ステップは、前記車両状態認識ステップにおいて前記自動運転機能が実行中であると認識されているときに実行されてもよい。

【００２４】

これにより、車両が攻撃メッセージであるか否かの判定が比較的容易な状態にあるときに当該判定を行うことで効率よく通信パターンの増強を行うことができ、判定の精度の向上が促進される。

【００２５】

また例えば、前記攻撃メッセージは、前記車載ネットワークシステムに含まれる前記１以上の電子制御ユニットのいずれかによって前記ネットワークに送出され、前記不正検知ステップ、前記情報保存ステップ、前記通信パターン識別ステップ、及び前記通信パターン判定ステップの少なくとも一部は、前記攻撃メッセージを送出する電子制御ユニットとは別の前記車載ネットワークシステムに含まれる電子制御ユニット、又は前記車載ネットワークシステムがさらに含むゲートウェイによって実行されてもよい。

【００２６】

これにより、例えば車載ネットワークシステムの内部にあるＥＣＵが攻撃者によって乗っ取られて攻撃メッセージを送出すると、不正通信が検知される。

【００２７】

また例えば、前記車載ネットワークシステムに含まれる前記１以上の電子制御ユニットの少なくとも１つは、前記車載ネットワークシステムの外部から送信されたデータを取得する送信データ取得部を備え、前記送信データ取得部を備える前記電子制御ユニットは、前記車載ネットワークシステムの外部から送信されたデータに含まれるメッセージに対して少なくとも前記不正検知ステップを実行してもよい。

【００２８】

これにより外部から送り込みが試みられる攻撃メッセージの車載ネットワークシステムへの侵入を抑制することができる。

【００２９】

また、本開示の一態様に係る不正通信検知システムは、ネットワーク及び前記ネットワークに接続される１以上の電子制御ユニットを含む車載ネットワークシステムにおける不正制御を検知するための不正制御検知システムであって、１個以上のプロセッサと、記憶部とを含み、前記１個以上のプロセッサは、前記ネットワークに送出されたメッセージが攻撃メッセージであるか否かを判定する不正検知を実行し、前記メッセージが攻撃メッセージである場合、前記攻撃メッセージに関する情報を前記記憶部に保存し、前記攻撃メッセージに関する情報から、前記ネットワークにおいて発生する通信パターンを識別し、前記メッセージが、識別された前記通信パターンに適合するか否かを判定する通信パターン判定を実行し、少なくとも前記不正検知及び前記通信パターン判定は、前記ネットワークに順次送出された複数のメッセージのそれぞれに対して実行し、前記通信パターン判定の実行後に送出されたメッセージに対する前記不正検知において、当該メッセージが攻撃メッセージであるか否かの判定に、実行済みの当該通信パターン判定における判定結果を用い、前記不正検知の実行において攻撃メッセージであるか否かの判定が不可能であったグレーメッセージに関する情報をさらに前記記憶部に保存する。

【００３０】

これにより、車載ネットワークシステムに送出されたメッセージが攻撃メッセージであるか否かが、攻撃メッセージの特徴を反映するパターンに照らして判定される。その結果、個々のメッセージが攻撃メッセージであるか否かの判定は、より高い精度で実行される。

【００３１】
また、本開示の一態様に係るプログラムは、上記の不正検知システムにおいて、前記１個以上のプロセッサに上記の不正通信検知方法のいずれかを実施させるためのプログラムである。
【００３２】
これにより、車載ネットワークシステムに送出されたメッセージが攻撃メッセージであるか否かが、攻撃メッセージの特徴を反映するパターンに照らして判定される。その結果、個々のメッセージが攻撃メッセージであるか否かの判定は、より高い精度で実行される。
【００３３】
以下、実施の形態について図面を参照しながら具体的に説明する。
【００３４】
なお、以下で説明する実施の形態は、いずれも包括的又は具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置及び接続形態、ステップ、ステップの順序などは一例であり、本発明を限定する趣旨ではない。以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素は、任意で含まれる構成要素として説明されるものである。
【００３５】
（実施の形態１）
［１．概要］
ここでは、送信されているメッセージが攻撃メッセージであるか否かの判定がなされる車載ネットワークシステムを例に用いて実施の形態１について図面を参照しながら説明する。
【００３６】
［１．１　車載ネットワークシステムの全体構成］
図１は、一実施形態における車載ネットワークシステム１０の全体構成を示すブロック図である。
【００３７】
車載ネットワークシステム１０は、ＣＡＮネットワークで構成され、ＥＣＵ１００（図中のＥＣＵ１００ａ、ＥＣＵ１００ｂ、ＥＣＵ１００ｃ、及びＥＣＵ１００ｄであり、以下ではこれらを集合的に、又は特定しない一部を指して、以下ではＥＣＵ１００ともいう）と、バス２００（図中のバス２００ａ及びバス２００ｂであり、以下ではこれらを集合的に、又は特定しない一方を指して、以下ではバス２００ともいう）と、ゲートウェイ３００とを含む。
【００３８】
ＥＣＵ１００ａはエンジン１０１に、ＥＣＵ１００ｂはブレーキ１０２に、ＥＣＵ１００ｃはドア開閉センサ１０３に、ＥＣＵ１００ｄはウィンドウ開閉センサ１０４にそれぞれ接続されている。ＥＣＵ１００は、それぞれが接続されている機器の状態を取得し、取得した状態を表すメッセージを周期的にバス２００に送出している。例えばＥＣＵ１００ａは、エンジン１０１の一状態である回転数を取得し、この回転数を表すデータ値を含むメッセージに所定のＩＤを付けてバス２００に送出する。また、各ＥＣＵ１００は、他のＥＵＣ１００が送信したメッセージをバス２００から読み出し、メッセージに付されたＩＤに応じて選択的に受信する。この選択的な受信については後述する。
【００３９】
ゲートウェイ３００は、ＥＣＵ１００ａ及びＥＣＵ１００ｂが接続されているバス２００ａと、ＥＣＵ１００ｃ及びＥＣＵ１００ｄが接続されているバス２００ｂとを接続している。ゲートウェイ３００は一方のバスから受信したメッセージを、もう一方のバスに転送する機能を持つ。ゲートウェイ３００もまた、ＣＡＮネットワーク上ではひとつのノードである。
【００４０】

なお、車載ネットワークシステム１０は、メッセージが攻撃メッセージであるか否かの判定をする不正通信検知システム等が適用可能な対象を説明するための例であり、その適用対象は車載ネットワークシステム１０に限定されない。

【００４１】

［１．２　メッセージのデータフォーマット］

図２は、ＣＡＮプロトコルのメッセージのフォーマットを示す図である。ここではＣＡＮプロトコルにおける標準ＩＤフォーマットにおけるメッセージを示している。

【００４２】

メッセージは、Ｓｔａｒｔ　Ｏｆ　Ｆｒａｍｅ（図中及び以下、ＳＯＦともいう）と、ＩＤフィールド、Ｒｅｍｏｔｅ　Ｔｒａｎｓｉｍｉｓｓｉｏｎ　Ｒｅｑｕｅｓｔ（図中及び以下、ＲＴＲともいう）、ＩＤｅｎｔｉｆｉｅｒ　Ｅｘｔｅｎｓｉｏｎ（図中及び以下、ＩＤＥともいう）、予約ｂｉｔ（図中及び以下、ｒともいう）、データレングスコード（図中及び以下、ＤＬＣともいう）、データフィールド、Ｃｙｃｒｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ（図中及び以下、ＣＲＣともいう）シーケンス、ＣＲＣデリミタ（図中、左のＤＥＬ）と、Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ（図中及び以下、ＡＣＫともいう）スロットと、ＡＣＫデリミタ（図中、右のＤＥＬ）と、エンドオブフレーム（図中及び以下、ＥＯＦともいう）から構成される。

【００４３】

ＳＯＦは、１ｂｉｔのドミナントである。ドミナント（優性の意）とは、データの伝達にデジタル方式が用いられるＣＡＮネットワークにおいて、“０”の値を送信するようにバスを構成する２本のケーブルに電圧がかけられた状態、又は送信されるこの“０”の値のことである。これに対し、“バスを構成する２本のケーブルに１”の値を送信するように電圧がかけられた状態、又は送信されるこの“１”の値のことはレセシブ（劣性の意）と呼ばれる。２つのノードからバスに同時に“０”の値と“１”の値とが送信された場合には、“０”の値が優先される。アイドル時のバスはレセシブである。各ＥＣＵ１００は、バス２００の状態をレセシブからドミナントへ変化させることでメッセージの送信を開始し、他のＥＣＵ１００はこの変化を読み取って同期する。図２中のメッセージを構成するドミナント又はレセシブを示す線が実線である部分は、ドミナント又はレセシブの各値を取り得ることを示す。ＳＯＦはドミナント固定であるため、ドミナントの線は実線であり、レセシブの線は破線である。

【００４４】

ＩＤとは、メッセージが含むデータの種類を示す１１ｂｉｔの値である。またＣＡＮでは、複数のノードが同時に送信を開始したメッセージ間での通信調停において、ＩＤの値がより小さいメッセージがより高い優先度となるよう設計されている。

【００４５】

ＲＴＲとは、フレームがメッセージ（データフレーム）であることを示す１ｂｉｔのドミナントである。

【００４６】

ＩＤＥとｒは、それぞれ１ｂｉｔのドミナントである。

【００４７】

ＤＬＣは、続くデータフィールドの長さを示す４ｂｉｔの値である。

【００４８】

データフィールドは、送信されるデータの内容を示す値であり、最大６４ｂｉｔ長で、８ｂｉｔ単位で長さを調整できる。送られるデータのこの部分への割り当てに関する仕様は、車種や製造者に依存する。

【００４９】

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、データフィールドの送信値より算出される１５ｂｉｔの値である。

【００５０】

ＣＲＣデリミタは１ｂｉｔのレセシブ固定の、ＣＲＣシーケンスの終了を表す区切り記

号である。受信ノードは、受信したメッセージの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値から算出した結果をＣＲＣシーケンスの値と比較することで異常の有無を判断する。

【００５１】

ＡＣＫスロットは１ｂｉｔ長で、送信ノードはこの部分でレセシブを送信する。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確認応答としてドミナントを送信する。ドミナントが優先されるため、１メッセージの通信がＣＲＣシーケンスまで正常に行われていれば、ＡＣＫスロットの送信中のバス２００はドミナントである。

【００５２】

ＡＣＫデリミタは１ｂｉｔのレセシブ固定の、ＡＣＫスロットの終了を表す区切り記号である。

【００５３】

ＥＯＦは７ｂｉｔのレセシブ固定で、メッセージの終了を示す。

【００５４】

［１．３　ゲートウェイの構成］

図３は、車載ネットワークシステム１０に含まれるゲートウェイ３００の構成を示す図である。ゲートウェイ３００は、フレーム送受信部３１０と、フレーム解釈部３２０と、受信ＩＤ判定部３３０と、受信ＩＤリスト保持部３４０と、フレーム処理部３５０と、転送ルール保持部３６０と、不正検知処理機能群３７０と、フレーム生成部３８０とを備える。

【００５５】

なお、これらの構成要素は機能構成要素であり、ゲートウェイ３００は、例えばプロセッサで実現される処理部、半導体メモリ等で実現される記憶部、入出力ポートで実現される入出力部等を備える情報処理装置として提供される。上記に挙げた各機能構成要素は、記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。

【００５６】

フレーム送受信部３１０は、バス２００ａ、２００ｂのそれぞれに対して、ＣＡＮのプロトコルに従ったメッセージを送受信する。より具体的には、フレーム送受信部３１０は、バス２００に送出されたメッセージを１ｂｉｔずつ読み出し、読み出したメッセージをフレーム解釈部３２０に転送する。また、フレーム送受信部３１０は、フレーム生成部３８０より通知を受けたバス情報に応じて、メッセージをバス２００ａ及び２００ｂに１ｂｉｔずつ送出する。バス２００ａから受信したメッセージをバス２００ｂに送信し、バス２００ｂから受信したメッセージをバス２００ａに送信することでバス２００間でのメッセージの転送を実行する。

【００５７】

フレーム解釈部３２０は、フレーム送受信部３１０よりメッセージの値を受け取り、ＣＡＮプロトコルにおける各フィールドにマッピングするようにしてフレーム（メッセージ）の解釈を行う。この解釈においてＩＤフィールドの値と判断した一連の値を、フレーム解釈部３２０は受信ＩＤ判定部３３０へ転送する。

【００５８】

フレーム解釈部３２０はさらに、受信ＩＤ判定部３３０から通知される判定結果に応じて、メッセージのＩＤフィールドの値及びＩＤフィールド以降に現れるデータフィールドをフレーム処理部３５０へ転送するか、メッセージの受信を中止するかを決定する。

【００５９】

またフレーム解釈部３２０は、ＣＡＮプロトコルに則っていないメッセージと判断した場合は、エラーフレームを送信するようにフレーム生成部３８０へ要求する。エラーフレームとは、ＣＡＮネットワーク上でエラーが発生した場合にノードから送信される、上述のメッセージとは異なる、ＣＡＮプロトコルで規定される所定のフォーマットのフレーム

である。エラーフラグがバスに送出されると、そのネットワークでの直近のメッセージの送信は中断される。

【００６０】

また、フレーム解釈部３２０は、他のノードが送信したエラーフレームを受信したと判断した場合、読取中のメッセージを破棄する。

【００６１】

受信ＩＤ判定部３３０は、フレーム解釈部３２０からＩＤフィールドの値を受け取り、受信ＩＤリスト保持部３４０が保持しているメッセージＩＤのリストに従い、読み出したメッセージを受信するか否かの判定を行う。受信ＩＤ判定部３３０は、この判定の結果をフレーム解釈部３２０へ通知する。

【００６２】

受信ＩＤリスト保持部３４０は、ゲートウェイ３００が受信するメッセージＩＤのリスト（以下、受信ＩＤリストともいう）を保持する。図４は、受信ＩＤリストのデータ構成の一例を示す図である。受信ＩＤリストの詳細は、この例を用いて後述する。

【００６３】

フレーム処理部３５０は、転送ルール保持部３６０が保持する転送ルールに従って、受信したメッセージのＩＤに応じて転送先のバスを決定し、転送先のバスと、フレーム解釈部３２０より通知されたメッセージＩＤと、転送するデータとをフレーム生成部３８０へ渡す。

【００６４】

またフレーム処理部３５０は、フレーム解釈部３２０より受け取ったメッセージを不正検知処理機能群３７０へ送り、そのメッセージが、攻撃メッセージであるか否かの判定を要求する。フレーム処理部３５０は、不正検知処理機能群３７０で攻撃メッセージであると判定されたメッセージを、転送しない。

【００６５】

転送ルール保持部３６０は、バスごとのデータ転送に関するルール（以下、転送ルールともいう）を保持する。図５は、転送ルールのデータ構成の一例を示した図である。転送ルールの詳細は、この例を用いて後述する。

【００６６】

不正検知処理機能群３７０は、受信中のメッセージが攻撃メッセージであるかどうかを判定する機能群である。不正検知処理機能群３７０に含まれる機能構成の詳細は後述する。

【００６７】

フレーム生成部３８０は、フレーム解釈部３２０からのエラーフレーム送信の要求に従い、エラーフレームを構成してフレーム送受信部３１０に送出させる。

【００６８】

またフレーム生成部３８０は、フレーム処理部３５０より受け取ったメッセージＩＤ及びデータとを使ってメッセージフレームを構成し、バス情報とともに、フレーム送受信部３１０へ送る。

【００６９】

［１．４　受信ＩＤリスト］

図４は、ゲートウェイ３００が受信するメッセージＩＤのリストである受信ＩＤリストのデータ構成の一例を示す図である。この例では、各行にゲートウェイ３００がバス２００から受信して処理する対象であるメッセージのＩＤが含まれている。この例の受信ＩＤリストによる設定では、ゲートウェイ３００は、メッセージＩＤが「１」、「２」、「３」又は「４」のメッセージを受信する。受信ＩＤリストに含まれないＩＤを持つメッセージの受信は中止される。なお、この例におけるＩＤの値及びリストに含まれるＩＤの個数は説明のための例であり、ゲートウェイ３００で用いられる受信ＩＤリストの構成を限定するものではない。

【００７０】

［１．５　転送ルール］
図５は、ゲートウェイ３００で保持される転送ルールのデータ構成の一例を示す。この例では、各行にメッセージの転送元のバスと転送先のバス（この例では参照符号と同じ名称２００ａ及び２００ｂで示される）との組み合わせ、及び転送対象のメッセージのＩＤが含まれる。この例の転送ルールによる設定では、ゲートウェイ３００は、バス２００ａから受信するメッセージを、ＩＤが何であってもバス２００ｂに転送する。また、バス２００ｂから受信するメッセージは、ＩＤが「３」のメッセージのみバス２００ａに転送される。
【００７１】
［１．６　不正検知処理機能群の構成］
図６は、ゲートウェイ３００が備える不正検知処理機能群３７０の機能構成を示すブロック図である。不正検知処理機能群３７０は、不正検知部３７１と、メッセージ保存処理部３７２と、攻撃メッセージ情報保持部３７３と、通信パターン識別部３７４と、通信パターン判定部３７５とを含む。
【００７２】
なお、これらの機能構成要素も、ゲートウェイ３００において記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。
【００７３】
不正検知部３７１は、フレーム処理部３５０から受け取ったメッセージが攻撃メッセージであるか否かを判定する。
【００７４】
不正検知部３７１は、複数種類の判定機能を持つ。各判定機能では、あらかじめ設定されて記憶部に保存されている異なるルール（図示なし）が参照されて、このルールを用いて受信したメッセージがチェック、つまり、各メッセージがこのルールに適合するか否かが判定される。そして各判定機能の判定結果に基づいて、受信したメッセージが攻撃メッセージであるか否かが判定される。受信したメッセージが攻撃メッセージであれば、不正検知部３７１は不正の発生を検知する。
【００７５】
図７に、不正検知部３７１の構成の例を示す。図７は、不正検知部３７１の機能構成の一例を示すブロック図である。この例では、不正検知部３７１は、メッセージの所定のポイントをチェックする６種類の判定機能を持つ。具体的には、メッセージのＩＤフィールドをチェックする機能（ＩＤ判定機能）、メッセージのデータ長をチェックする機能（データ長判定機能）、メッセージが送信される周期（時間間隔）をチェックする機能（送信周期判定機能）、メッセージが送信される頻度をチェックする機能（送信頻度判定機能）、メッセージのデータフィールドの値（データ値）をチェックする機能（データ値判定機能）、これらの判定機能の判定結果、送信周期、頻度、データ値、又はデータ値の変化量などに基づいて車両の状態を認識し、車両状態をチェックする機能（車両状態判定機能）である。さらに不正検知部３７１は、受信したメッセージが攻撃メッセージであるか否かを、これらの判定機能による判定結果から総合的に判定する総合判定機能を持つ。総合判定機能の結果が、不正検知部３７１による不正の検知の結果となる。
【００７６】
なお、ゲートウェイ３００が備えるこれらの機能構成要素も、ゲートウェイ３００において記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。
【００７７】
図６の説明に戻って、不正検知部３７１は、通信パターン判定部３７５に、受信したメッセージが、攻撃メッセージの通信パターンに適合するか否かの判定を要求する。
【００７８】

メッセージ保存処理部３７２は、不正検知部３７１の判定結果を受けて、受信したメッセージが攻撃メッセージであり、かつ、保存が必要と判定した場合には、攻撃メッセージ情報保持部３７３へ、受信した攻撃メッセージ、攻撃メッセージを受信した時刻、同一ＩＤ又は特定の異なるＩＤを持つ他のメッセージとの受信時間の差、データ値の変化量等の攻撃メッセージに関する情報を攻撃メッセージ情報保持部３７３に保持させる。

【００７９】

攻撃メッセージ情報保持部３７３は、メッセージ保存処理部３７２より保存を指示された攻撃メッセージに関する情報を保持する。具体的には、ゲートウェイ３００が備える記憶部に記憶される。また、攻撃メッセージ情報保持部３７３は、通信パターン識別部３７４からの要求に応じて、保持している攻撃メッセージに関する情報を出力する。

【００８０】

通信パターン識別部３７４は、攻撃メッセージ情報保持部３７３から、攻撃メッセージに関する情報を取得し、受信した攻撃メッセージに見られるパターン（以下、通信パターン）を識別する。

【００８１】

通信パターンとは、例えばデータ値の変化に関するパターンである。より具体的な例としては、同一ＩＤ、つまり同じ種類のデータ値を表すデータフィールドの値（全体の場合も特定の部分の値の場合もある）の変化の有無に関するパターン、増加又は減少の量、割合若しくは頻度に関するパターン、他の特定のＩＤのメッセージとのデータ値との差分若しくは比に関するパターンが挙げられる。

【００８２】

また例えば、通信パターンとは攻撃メッセージの通信タイミングに関するパターンであり、例えば同一ＩＤの複数のメッセージの実際の送信時刻の間隔のばらつきに関するパターン、あるＩＤのメッセージのメッセージ同士、又はあるＩＤのメッセージと他の特定のＩＤのメッセージとの間の送信時刻の差分に関するパターンが挙げられる。より具体的な例として、攻撃メッセージが正常メッセージの直前又は直後に送信されるパターン、又は正常メッセージと攻撃メッセージとが一定の時間を空けて送信されるパターンとして識別されてもよい。

【００８３】

このような通信パターンの識別のために、通信パターン識別部３７４は、攻撃メッセージに関する情報を攻撃メッセージ情報保持部３７３から取得する。

【００８４】

攻撃メッセージに関する情報とは、個々の攻撃メッセージのデータ値、受信時刻などの、上述の通信パターンの識別に用いられる情報である。

【００８５】

通信パターン識別部３７４は、取得した情報の比較、統計的処理等を経て上記のような通信パターンを導出し識別する。識別に用いられる攻撃メッセージに関する情報の量は、例えば識別の処理の負荷と精度とを考慮して決定されてもよい。

【００８６】

また、通信パターン識別部３７４は、通信パターンを識別した後、識別の結果として得た通信パターンを示す情報と、その通信パターンの判定に必要な情報とを通信パターン判定部３７５へ通知する。通信パターンの判定に必要な情報とは、例えば、データフィールドの特定の部分の値が一定の値であるパターンであればその部分及び値、データ値の一定の割合での変化（増加又は減少）が見られるパターンであれば、その割合、データ値が他の特定のＩＤのメッセージのデータ値との一定の差であるパターンであればその一定の差分である。

【００８７】

このような通信パターン識別部３７４による通信パターンの識別は、各種のタイミングで実行し得る。例えば、攻撃メッセージに関する情報の追加に関連するタイミングであってもよい。より具体的には、攻撃メッセージ情報保持部３７３に攻撃メッセージに関する

情報が新たに保存される度に実行されてもよいし、又は攻撃メッセージ情報保持部３７３に保持されている攻撃メッセージに関する情報が一定量（容量又は件数）に達したときに実行されてもよい。また、攻撃メッセージに関する情報の追加とは関連しないタイミングであってもよい。例えば、一定の経過時間ごとに実行されてもよいし、車両が所定の状態になったとき、又は車両の状態が所定の変化をしたときでもよい。また、これらのような状況を組み合わせた条件が満たされたときでもよい。識別の実行のタイミングは、例えば識別の処理の負荷と、通信パターンの追加又は更新の必要性とを考慮して決定されてもよい。

【００８８】

通信パターン判定部３７５は、不正検知部３７１からの要求に応じて、受信したメッセージが、通信パターン識別部３７４による識別の結果として得られた通信パターンに適合するか否かを判定する。

【００８９】

通信パターン判定部３７５は、受信したメッセージの通信パターンへの適合に関する判定に、当該判定対象の受信したメッセージ以外に、例えばより古い受信したメッセージ、通信パターン識別部３７４から通知される識別した通信パターンを示す情報と、通信パターン別の判定に必要な情報等を用いる。

【００９０】

例えば、データフィールドの特定の部分の値が一定の値である通信パターンとの適合の判定は、受信したメッセージのデータフィールドの値が、通信パターン識別部３７４から通知された該当部分及びその部分の値と一致するか否かに基づいて行われる。

【００９１】

また例えば、データ値が一定の割合又は量で増加又は減少しているパターンとの適合は、一つ前に受信したメッセージのデータ値と、判定対象のメッセージのデータ値の差分又は比を算出し、その算出結果が通信パターン識別部３７４から通知された変化の割合又は量と整合するか否かに基づいて行われる。

【００９２】

また例えば、データ値が、他の特定のＩＤのメッセージのデータ値に対して一定の差又は比であるパターンとの適合、受信したメッセージのデータ値と、対応する周期で受信した他の特定のＩＤのメッセージのデータ値との差又は比を算出し、その算出結果が通信パターン識別部３７４から通知された差又は比と一致するか否かに基づいて行われる。

【００９３】

また例えば、攻撃メッセージが、他のメッセージの直前又は直後に送信されるパターン、又は、一定の時間経過後に送信されるパターンとの適合は、当該他のメッセージの送信時刻、判定対象の受信したメッセージの送信時刻との差分が所定の範囲にあるか否かに基づいて行われる。なお、ここでの他のメッセージは、同一ＩＤの前後のメッセージであってもよいし、他の特定のＩＤのメッセージであってもよい。

【００９４】

また、通信パターン識別部３７４は、データフィールドの値の変化又は通信タイミングに関する通信パターンを識別し、通信パターン判定部３７５は、受信したメッセージがこの通信パターンに適合するか否かを判定しているが、ゲートウェイ３００が備える不正検知処理機能群の構成はこれに限定されるものではない。ゲートウェイ３００は、不正検知処理機能群３７０に代えて、例えば図８に示すような、さらに通信パターン予測部３７６ａを含む不正検知処理機能群３７０ａを備えてもよい。図８は、本実施の形態における不正検知処理機能群の機能構成の他の例を示すブロック図である。不正検知処理機能群３７０ａの機能的構成要素のうち、不正検知処理機能群３７０と共通のものは共通の参照符号を用いて示し、その詳細な説明を省略する。

【００９５】

図８において、通信パターン識別部３７４ａは、統計的処理又は確率理論を用いて、攻撃メッセージに関する情報のＡＲ（ＡｕｔｏＲｅｇｒｅｓｓｉｖｅ）モデル、ＡＲＭＡ（

ＡｕｔｏＲｅｇｒｅｓｓｉｖｅ Ｍｏｖｉｎｇ Ａｖｅｒａｇｅ）モデル、ＨＭＭ（Ｈｉｄｄｅｎ Ｍａｒｋｏｖ Ｍｏｄｅｌ）、又はベイジアンモデル（Ｂａｙｅｓｉａｎ Ｉｎｆｅｒｅｎｃｅ）などのモデルを取得し、そのモデルを通信パターンとする。

【００９６】

通信パターン予測部３７６ａは、通信パターン識別部３７４ａが識別したモデルを通信パターンとして用いて、受信するメッセージのデータ値又は通信タイミングに関する予測値を算出する。

【００９７】

通信パターン判定部３７５ａは、通信パターン予測部３７６ａが算出した予測値と、受信したメッセージに関する情報とから、当該受信したメッセージが通信パターンに適合するか否か判定する。

【００９８】

なお、ここまで通信パターン判定部３７５又は通信パターン判定部３７５ａは、通信パターンに適合するか否かを判定する説明している。この「適合」の語は、比較されるデータ値又は時刻の一致のみをもって適合すると判定される意味に限定されない。例えば、所定の許容差内にあることをもって適合すると判定される意味を意図して本開示では「適合」の語が用いられる。

【００９９】

例えば、データフィールドの特定の部分の値が一定である通信パターンとの適合は、その一定の値と一致するか否かではなく、その値から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。

【０１００】

また例えば、データ値が一定の割合で増加する通信パターンとの適合は、その一定の割合で増加した結果の値から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。同様に、一定の割合で減少する通信パターンとの適合は、その一定の割合で減少した結果の値から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。

【０１０１】

また例えば、他のＩＤのメッセージのデータ値に対して一定の値を足した値である通信パターンとの適合は、当該他のＩＤのメッセージのデータ値に一定の値を足した結果の値から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。同様に、他のＩＤのメッセージのデータ値に対して一定の値を引いた値である通信パターンとの適合は、当該他のＩＤのメッセージのデータ値から一定の値を引いた結果の値から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。

【０１０２】

また例えば、攻撃メッセージが、他のメッセージの送信の直前に送信される通信パターンとの適合は、事前に定義された直前の時刻から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。同様に、攻撃メッセージが他のメッセージの送信の直後に送信される通信パターンとの適合は、事前に定義された直後の時刻から事前に設計されたマージンに入るか否かに基づいて判定されてもよい。攻撃メッセージが、他のメッセージの送信から一定の時間経過後に送信される通信パターンとの適合は、他のメッセージの送信から一定時間経過した時刻から事前に設計されたマージン入るか否かに基づいて判定されてもよい。

【０１０３】

さらに、通信パターン予測部３７６ａによってデータ値が予測される場合は、受信したメッセージのデータ値が、予測値から事前に設計されたマージンに収まっているか否かに基づいて通信パターンに一致するか否かが判定されてもよい。また、通信パターン予測部３７６ａによって通信タイミングが予測された場合には、受信したメッセージの送信又は受信の時刻や、他のメッセージとの送信又は受信時刻の差が、事前に設定したしきい値以下に収まっている否かに基づいて通信パターンに一致するか否かが判定されてもよい。

【０１０４】

なお、メッセージ保存処理部３７２は、受信したメッセージが攻撃メッセージであり、かつ、保存が必要と判定した場合に攻撃メッセージに関する情報を保存するとしたが、これに限定されない。通信パターン識別部３７４又は通信パターン識別部３７４ａによる識別に、正常メッセージに関する情報も必要な場合には、メッセージ保存処理部３７２は、正常メッセージに関する情報もさらに保存してもよい。この場合、例えば各メッセージについての不正検知部３７１の判定結果が各メッセージに関する情報としてあわせて保存されてもよい。

【０１０５】

なお、受信したメッセージはゲートウェイ３００の記憶部に保存される。ただし、記憶部の容量は有限であるため、メッセージの保存の要否については、例えば間引いた攻撃メッセージの情報に基づいても通信パターンの識別が可能な識別方法が用いられる場合には、保存されるメッセージが必要以上に多くならないよう各攻撃メッセージについて保存の要否が判定される。または、記憶部に保存されるメッセージの件数又は容量に上限をあらかじめ設定しておき、保存対象のメッセージが発生する度に、古いメッセージから消去する、先入れ先出し方式でメッセージの保存管理がなされてもよい。

【０１０６】

［１．７　ＥＣＵの構成］

図９は、車載ネットワークシステム１０に含まれるＥＣＵ１００の機能構成を示すブロック図である。ＥＣＵ１００は、フレーム送受信部１１０と、フレーム解釈部１２０と、受信ＩＤ判定部１３０と、受信ＩＤリスト保持部１４０と、フレーム処理部１５０と、データ取得部１７０と、フレーム生成部１８０とを備える。

【０１０７】

なお、これらの構成要素は機能構成要素であり、ＥＣＵ１００は、例えばプロセッサで実現される処理部、半導体メモリ等で実現される記憶部、入出力ポートで実現される入出力部等を備える情報処理装置として提供される。上記に挙げた各機能構成要素は、記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。

【０１０８】

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メッセージを送受信する。より具体的には、フレーム送受信部１１０は、バス２００に送出されたメッセージを１ｂｉｔずつ読み出し、読み出したメッセージをフレーム解釈部１２０に転送する。また、フレーム送受信部１１０は、フレーム生成部１８０より通知を受けたメッセージをバス２００に送出する。

【０１０９】

フレーム解釈部１２０は、フレーム送受信部１１０よりメッセージの値を受け取り、ＣＡＮプロトコルにおける各フィールドにマッピングするようにしてフレーム（メッセージ）の解釈を行う。この解釈においてＩＤフィールドと判断した一連の値を、フレーム解釈部１２０は受信ＩＤ判定部１３０へ転送する。

【０１１０】

フレーム解釈部１２０はさらに、受信ＩＤ判定部１３０から通知される判定結果に応じて、メッセージのＩＤフィールドの値及びＩＤフィールド以降に現れるデータフィールドをフレーム処理部１５０へ転送するか、メッセージの受信を中止するかを決定する。

【０１１１】

またフレーム解釈部１２０は、ＣＡＮプロトコルに則っていないメッセージと判断した場合は、エラーフレームを送信するようにフレーム生成部１８０へ要求する。

【０１１２】

またフレーム解釈部１２０は、他のノードが送信したエラーフレームを受信したと判断した場合、読取中のメッセージを破棄する。

【０１１３】

受信ＩＤ判定部１３０は、フレーム解釈部１２０からＩＤフィールドの値を受け取り、受信ＩＤリスト保持部１４０が保持しているメッセージＩＤのリストに従い、読み出したメッセージを受信するか否かの判定を行う。受信ＩＤ判定部１３０は、この判定の結果をフレーム解釈部１２０へ通知する。

【０１１４】

受信ＩＤリスト保持部１４０は、ＥＣＵ１００が受信するメッセージＩＤのリストである受信ＩＤリストを保持する。受信ＩＤリストは、図４と同様であり、ここでは説明を省略する。

【０１１５】

フレーム処理部１５０は、受信したメッセージのデータに応じた処理を行う。処理の内容は、各ＥＣＵ１００によって異なる。例えば、ＥＣＵ１００ａでは、時速が３０ｋｍを超えているときに、ドアが開いていることを示すメッセージを受信すると、アラーム音を鳴らすための処理を実行する。ＥＣＵ１００ｃは、ブレーキがかかっていないことを示すメッセージを受信しているときにドアが開くと、アラーム音を鳴らすための処理を実行する。これらの処理は説明を目的として挙げる例であり、ＥＣＵ１００は上記以外の処理を実行してもよい。このような処理を実行するために送出するフレームを、フレーム処理部１５０はフレーム生成部１８０に生成させる。

【０１１６】

データ取得部１７０は、各ＥＣＵ１００に接続されている機器状態又はセンサによる計測値等を示す出力データを取得し、フレーム生成部１８０に転送する。

【０１１７】

フレーム生成部１８０は、フレーム解釈部１２０から通知されたエラーフレーム送信の要求に従い、エラーフレームを構成してフレーム送受信部１１０へ送る。

【０１１８】

またフレーム生成部１８０は、データ取得部１７０より受け取ったデータの値に対してあらかじめ定められたメッセージＩＤを付けてメッセージフレームを構成し、フレーム送受信部１１０へ送る。

【０１１９】

［１．８　不正検知処理］

図１０は、不正検知処理機能群３７０での不正検知処理の一例を示すフロー図である。

【０１２０】

まず、不正検知部３７１は、フレーム処理部３５０からメッセージを受け取る（ステップＳ１００１）。

【０１２１】

メッセージを受け取った不正検知部３７１は、ＩＤ判定機能などの各種の判定機能を利用して、そのメッセージが攻撃メッセージであるか正常メッセージであるかの判定を行う。そして不正検知部３７１は、その判定の結果をメッセージ保存処理部３７２へ通知する。このとき、不正検知部３７１はさらに、通信パターン判定部３７５に、受信したメッセージが攻撃メッセージの通信パターンに適合するか否かの判定を依頼する。不正検知部３７１の総合判定機能は、ＩＤ判定機能などの各種の判定機能の判定の結果と、通信パターン判定部３７５による判定の結果とから総合的に、当該メッセージについての最終的な判定をする（ステップＳ１００２）。

【０１２２】

メッセージ保存処理部３７２は、不正検知部３７１から最終的な判定の結果として、受信したメッセージが攻撃メッセージであるとの通知を受けた場合（ステップＳ１００３でＹｅｓ）、ステップＳ１００４へ進む。メッセージ保存処理部３７２が受けた通知が、受信したメッセージが攻撃メッセージではないとの通知である場合、不正検知処理機能群３７０での不正検知処理は終了する（ステップＳ１００３でＮｏ）。

【０１２３】

ステップＳ１００３でＹｅｓの場合、メッセージ保存処理部３７２は、攻撃メッセージ

に関する情報を、攻撃メッセージ情報保持部３７３に保持させる（ステップＳ１００４）。

【０１２４】

攻撃メッセージ情報保持部３７３への攻撃メッセージに関する情報が保存された後、通信パターン識別部３７４は、通信パターンの識別を実行する条件が満たされているか否かを判定する（ステップＳ１００５）。識別が必要であるか否かの判定は、例えば保持される攻撃メッセージの件数が、通信パターンの識別が可能な程度にあるか否か基づいて実行される。

【０１２５】

ステップＳ１００５で、通信パターン識別部３７４が通信パターンの識別が必要であると判定した場合（ステップＳ１００５でＹｅｓ）、通信パターン識別部３７４は、攻撃メッセージ情報保持部３７３に保持されている攻撃メッセージに関連する情報から、攻撃パターンを識別する（ステップＳ１００６）。

【０１２６】

ステップＳ１００５で、通信パターン識別部３７４が通信パターンの識別が必要ではないと判定した場合（ステップＳ１００５でＮｏ）、不正検知処理機能群３７０での不正検知処理は終了する。

【０１２７】

識別された通信パターンは、ゲートウェイ３００の記憶部に保存され、通信パターン判定部３７５又は通信パターン判定部３７５ａによって、受信メッセージに対する判定にあたって参照される。そしてこの判定の結果は、不正検知処理（ステップＳ１００２）における、総合判定機能に用いられる。これにより、個々のメッセージが攻撃メッセージであるか否かの判定は、より高い精度で実行される。

【０１２８】

なお、不正検知処理機能群３７０における上記の不正検知処理のうち、不正検知部３７１による不正検知のステップと、通信パターン判定部３７５又は通信パターン判定部３７５ａとは各受信メッセージに対して実行されるが、それ以外のステップはステップＳ１００３又はステップＳ１００５での所定の条件が満たされた場合に実行されるため、必ずしも各受信メッセージに対しては実行されない。

【０１２９】

また、不正検知部３７１は、ＩＤ判定機能などの各種の判定機能の判定結果と、通信パターン判定部３７５による判定結果とから総合的に、受信メッセージが攻撃メッセージであるか否かの最終的な判定を実行すると説明したが、これに限定されない。例えば、各種の判定機能の判定結果から、一旦、判定を行い、その判定結果に応じて通信パターン判定部３７５による判定を行い、その後に、最終的な判定してもよい。また、その逆に、通信パターン判定部３７５による判定を先に行い、その結果に応じてＩＤ判定機能などの各種判定機能による判定を行ってもよい。

【０１３０】

また、受信したメッセージごとに、実行される判定が決定されてもよい。これにより、受信したメッセージに応じて、例えば不正検知部３７１におけるＩＤ判定機能などの各種の判定機能による判定のみでよいメッセージは、その結果によらず通信パターン判定部３７５による判定が実行されないようにすることができる。また、通信パターン判定部３７５による判定のみでよいメッセージには、その結果によらず、不正検知部３７１における各種の判定機能による判定が実行されないようにすることができる。

【０１３１】

これにより、判定結果や受信したメッセージに応じて、各種判定機能又は通信パターン判定部３７５による判定処理が省略できるため、不正検知処理機能群３７０全体での判定処理の高速化、及び省電力化の効果が期待できる。

【０１３２】

［１．９　転送処理］

図１１は、ゲートウェイ３００が行う転送処理の一例を示すフロー図である。この転送処理の内容は転送の方向によらず実質的に共通であるため、以下では、この転送処理について、ゲートウェイ３００がバス２００ａから受信したメッセージをバス２００ｂへ転送する場合を例に説明する。

【０１３３】

まず、フレーム送受信部３１０は、バス２００ａからメッセージを読み出す（ステップＳ１１０１）。フレーム送受信部３１０は、読み出したメッセージの各フィールドのデータをフレーム解釈部３２０へ転送する。

【０１３４】

次に、フレーム解釈部３２０は、受信ＩＤ判定部３３０と連携して、読み出したメッセージのＩＤフィールドの値（メッセージＩＤ）から、受信して処理する対象のメッセージであるか否かを判定する（ステップＳ１１０２）。処理する対象のメッセージではないとフレーム解釈部３２０が判定した場合（ステップＳ１１０２でＮＯ）、当該メッセージの転送は行われない。

【０１３５】

フレーム解釈部３２０は、ステップＳ１１０２で、受信して処理する対象のメッセージであると判定した場合には（ステップＳ１１０２でＹｅｓ）、フレーム処理部３５０へメッセージ内の各フィールドの値を転送する。その後、フレーム処理部３５０は、転送ルール保持部３６０に保持される転送ルールに従って、転送先のバスを決定する（ステップＳ１１０３）。

【０１３６】

フレーム処理部３５０は、フレーム解釈部３２０から受け取ったメッセージ内の各フィールドの値を不正検知処理機能群３７０へ通知し、攻撃メッセージであるか否かの判定を要求する。

【０１３７】

不正検知処理機能群３７０は、通知されたメッセージの各フィールドの値から、通知されたメッセージが攻撃メッセージであるか否かを判定し（ステップＳ１１０４）、その判定の結果をフレーム処理部３５０へ通知する。攻撃メッセージであると不正検知処理機能群３７０が判定した場合（ステップＳ１１０４でＹＥＳ）、当該メッセージの転送は行われない。

【０１３８】

ステップＳ１１０４でメッセージが攻撃メッセージではなく正常メッセージであると判定された場合（ステップＳ１１０４でＮｏ）、フレーム処理部３５０は、そのメッセージをステップＳ１１０３で決定した転送先のバスに、転送するようフレーム生成部３８０へ要求する。フレーム生成部３８０は、フレーム処理部３５０からの要求を受けて、指定された転送先が受信するようメッセージを生成し、このメッセージをフレーム送受信部３１０に送出させる（ステップＳ１１０５）。

【０１３９】

なお、上記の例では、受信したメッセージの転送先の決定（ステップＳ１１０３）の後にこのメッセージが攻撃メッセージであるかの判定（ステップＳ１１０４）がなされているが、これに限定されない。受信したメッセージが攻撃メッセージであるかの判定の後にこのメッセージの転送先の決定がなされてもよい。また、受信したメッセージの転送先の決定と攻撃メッセージであるかの判定が並行して行われてもよい。

【０１４０】

［１．１０　効果］

本実施の形態では、不正検知処理機能群３７０は、車載ネットワークシステムのネットワークを流れるメッセージを監視し、受信したメッセージが、通信パターンに一致するかどうかを判定することで、攻撃メッセージであるか否かを判定する。通信パターンとは、攻撃メッセージの特徴を示す、メッセージのデータ値の変化又は通信タイミングに関するパターンである。このような通信パターンは、攻撃メッセージとすでに判定したメッセー

ジに関する情報に基づいて識別して取得される。これにより従来の不正検知の技術で用いられていたような、例えば一の受信メッセージに関する情報からのみでは正常メッセージであるか攻撃メッセージであるかの判定が困難であったメッセージに関しても、より高い精度で判定することが可能になる。その結果、車載ネットワークシステムの安全が高められる。

【０１４１】

（実施の形態２）

［２．概要］

実施の形態２として、不正検知処理の対象の受信メッセージに関する情報、つまり受信したメッセージのデータ値又は受信時刻を算出するために基準として利用されるメッセージ（以下、基準メッセージともいう）の決定に、上述の通信パターンを利用する不正検知処理機能群について図面を参照しながら説明する。このような不正検知処理機能群は、図３における不正検知処理機能群３７０に代えてゲートウェイに含まれ得る。なお、この不正検知処理機能群を含むゲートウェイ、及びこのゲートウェイを備える車載ネットワークシステムは実施の形態１と基本的に共通でよいため、その構成についての説明を省略する。

【０１４２】

［２．１　不正検知処理機能群の構成］

図１２は、本実施の形態における不正検知処理機能群３７０ｂの機能構成を示すブロック図である。図１２において、図６と同じ構成要素については同じ符号を用い、説明を省略する。また、同じ構成要素の一部については、図示を省略する。以下、不正検知処理機能群３７０ｂについて、不正検知処理機能群３７０との差異点を中心に説明する。

【０１４３】

不正検知処理機能群３７０ｂは、実施の形態１における不正検知処理機能群３７０の構成に加え、基準メッセージ決定部３７７ｂ、及び基準メッセージ候補保持部３７８ｂを含む。また、不正検知処理機能群３７０ｂは、不正検知部３７１に代えて不正検知部３７１ｂを、通信パターン判定部３７５に代えて通信パターン判定部３７５ｂを含む。これらの構成要素も機能構成要素であり、ゲートウェイにおいて記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。

【０１４４】

基準メッセージ決定部３７７ｂは、不正検知部３７１ｂの送信周期判定機能による同一ＩＤで１つ前のメッセージからの送信時間の差の算出、及びデータ値判定機能による同一ＩＤで１つ前のメッセージからの変化量の算出において基準として用いられる基準メッセージを決定する。

【０１４５】

例えば、周期的に送信されるメッセージについて、受信予定時刻Ｔの前後に時間長αのマージンが考慮されている場合、そのマージン内に複数のメッセージが送信される場合がある。このとき、基準メッセージ決定部３７７ｂは、これらの複数のメッセージから基準メッセージとして用いるメッセージを決定する。

【０１４６】

不正検知部３７１ｂは、受信したメッセージから、次の受信周期に移ったことを認識したとき、基準メッセージ決定部３７７ｂに基準メッセージの取得を要求する。

【０１４７】

基準メッセージ決定部３７７ｂは、基準メッセージ候補保持部３７８ｂから基準メッセージの候補となるメッセージに関する情報を取得し、その候補から基準メッセージとして用いるメッセージを決定して不正検知部３７１ｂへ通知する。

【０１４８】

基準メッセージ決定部３７７ｂは、基準メッセージを決定するときに、通信パターン判定部３７５ｂへ基準メッセージの候補を通知する。

【０１４９】
通信パターン判定部３７５ｂは、候補である各メッセージがいずれかの通信パターンに一致するか否か、又は各通信パターンとの近さの判定を実行する。
【０１５０】
基準メッセージ決定部３７７ｂは、通信パターン判定部３７５ｂが判定した結果から、いずれかの通信パターンと一致する、又は所定の程度を超えて近いと判定されたメッセージを候補から外す。この段階で残った候補のメッセージが１つである場合は、基準メッセージ決定部３７７ｂはそのメッセージを基準メッセージとして決定する。また、基準メッセージ決定部３７７ｂは、複数のメッセージが候補に残った場合は、事前に決定されたルールに従って基準メッセージを決定する。
【０１５１】
事前に決定されたルールに従って、例えば、実際の受信時刻が受信予定時刻Ｔに最も近いメッセージが基準メッセージとして決定されてもよい。また例えば、候補のメッセージのうちで、受信予定時刻Ｔより遅い時刻に送信されたメッセージであって、実際の受信時刻が受信予定時刻Ｔに最も近いメッセージが基準メッセージとして決定されてもよい。または逆に、受信予定時刻Ｔより早い時刻に受信されたメッセージであって、実際の受信時刻が受信予定時刻Ｔに最も近いメッセージが基準メッセージとして決定されてもよい。さらに別の例として、１つ前又は２つ前に送信されたメッセージが受信予定時刻Ｔに対して遅れていたか早かったかに応じて、受信予定時刻Ｔより遅い時刻のメッセージを選択するか、早い時刻のメッセージを選択するかが切り替えられてもよい。また、メッセージが連続して送信されていたか否かに応じて、実際の受信時刻が受信予定時刻Ｔにより近いメッセージを選択するか、より遠いメッセージを選択するかが切り替えられてもよい。
【０１５２】
また、事前に決定されたルールは、データ値を用いて基準メッセージが決定されるルールでもよい。
【０１５３】
例えば、同一ＩＤ又は特定の異なるＩＤを持つ、同じ種類のデータ量を表す他のメッセージのデータ値と近いメッセージを基準メッセージとして決定してもよいし、同じ種類のデータ量を表す他のメッセージのデータ値から算出される値に近いデータ値を含むメッセージを基準メッセージとして決定してもよい。データの変化量が予測できる場合には、その予測値と比較して、近いデータ値のメッセージを基準メッセージとして決定してもよい。
【０１５４】
基準メッセージ候補保持部３７８ｂは、基準メッセージ決定部３７７ｂに提示される基準メッセージ候補を保持する。
【０１５５】
不正検知部３７１ｂは、受信したメッセージから、基準メッセージの候補となるメッセージに関する情報を、基準メッセージ候補保持部３７８ｂへ通知する。基準メッセージ候補保持部３７８ｂは、不正検知部３７１ｂから通知を受けた基準メッセージの候補となるメッセージに関する情報を保持しておき、基準メッセージ決定部３７７ｂからの要求に応じて、基準メッセージの候補となるメッセージに関する情報を基準メッセージ決定部３７７ｂに通知する。
【０１５６】
なお、上記では不正検知部３７１ｂは、受信したメッセージから、次の受信周期に移ったことを認識したとき、基準メッセージ決定部３７７ｂに対して、基準メッセージの取得を依頼すると説明したが、これに限定されない。例えば、受信予定時刻Ｔのマージン内に１つめのメッセージが受信されたときに、受信したメッセージを基準メッセージ候補としてそのメッセージに関する情報を基準メッセージ候補保持部３７８ｂに保持させ、以降、その受信予定時刻Ｔのマージン内にメッセージを受信する度に、基準メッセージ決定部３７７ｂに基準メッセージの決定を要求してもよい。

【０１５７】
この場合、基準メッセージ決定部３７７ｂは、新たに受信したメッセージを基準メッセージ候補とし、基準メッセージ候補保持部３７８ｂが保持している基準メッセージの候補とどちらを基準メッセージ候補として残すかを決定する。この決定は、上述の基準メッセージの決定に用いられるルールに従って行われる。この決定の結果残された基準メッセージの候補が、基準メッセージ候補保持部３７８ｂに引き続き保持される。その後、次の受信周期に移った時点で残っている基準メッセージ候補が、次に用いられる基準メッセージとなる。

【０１５８】
これにより、基準メッセージの候補として保持されるのは常に１つのメッセージのみでよいため、候補を保持するためのリソースを節約することが可能となる。

【０１５９】
なお、基準メッセージ決定部３７７ｂは、基準メッセージの候補から基準メッセージを決定するときに、通信パターン判定部３７５ｂの判定結果から、候補メッセージのいくつかを候補から外し、残った候補のメッセージから事前に決定されたルールに従って基準メッセージを決定すると説明したが、これに限定されない。例えば基準メッセージ決定部３７７ｂは、まず事前に決定されたルールに従って候補を絞った後に、通信パターン判定部３７５ｂに通信パターンの判定を要求し、その判定結果に応じて基準メッセージを決定してもよい。また、通信パターン判定部３７５ｂで全ての候補メッセージが、何らかの通信パターンに一致すると判定された場合、又は事前に決定されたルールでの判定の結果、全ての候補メッセージが基準メッセージにならないと判定された場合、つまり、全ての候補のメッセージが基準メッセージにふさわしくないと判定された場合には、基準メッセージ決定部３７７ｂは、基準メッセージがないと決定してもよい。または、全ての候補のメッセージが基準メッセージにふさわしくないと判定された場合に利用するルールを別途定義しておき、基準メッセージ決定部３７７ｂは、そのルールに従って基準メッセージを決定してもよい。

【０１６０】
別途定義されるこのルールは、専用に定義されるルールであってもよい。例えば、事前に決定された基準メッセージを決定するためのルールや、通信パターンの判定時に、基準メッセージのふさわしさをスコア化し、そのスコアに基づいて基準メッセージを決定するというルールであってもよい。

【０１６１】
また、通信パターン判定部３７５ｂで全ての候補のメッセージが何らかの通信パターンに一致すると判定した場合に、全ての候補のメッセージに対して、再度、事前に決定されたルールを適用し、基準メッセージを決定するというルールが定義されてもよい。また、逆に、事前に決定されたルールで判断した結果、全ての候補のメッセージが基準メッセージにならないと判定された場合、全ての候補のメッセージに対して、再度、通信パターン判定部３７５ｂに問い合わせを行い、その結果に応じて基準メッセージを決定するというルールが定義されてもよい。

【０１６２】
また、実施の形態１における図８に示される構成と同様に、通信パターンとの適合の判定に、攻撃メッセージに関する情報をモデル化し、そのモデルを通信パターンとして用いられる構成であってもよい。図１３は、本実施の形態において、通信パターンとの適合の判定に、攻撃メッセージに関する情報をモデル化して取得したモデルを通信パターンとして判定する不正検知処理機能群３７０ｃの構成の一例を示す図である。不正検知処理機能群３７０ｃは、実施の形態１におけるゲートウェイ３００に、不正検知処理機能群３７０ｂに代えて含まれうる。

【０１６３】
通信パターン判定部３７５ｃは、通信パターン判定部３７５ｂと同じ機能を備え、さらに、通信パターン予測部３７６ｃによる予測値を用いて通信パターンを判定する機能を備

える。
【０１６４】
通信パターン予測部３７６ｃは、通信パターン予測部３７６ａと同じ機能を備え、通信パターン判定部３７５ｃからの要求に応じて予測値を通知する機能を備える。
【０１６５】
この予測値は、通信パターン予測部３７６ｃが、通信パターン識別部３７４ｃが識別したモデルを通信パターンとして用いて算出するものである。
【０１６６】
通信パターン識別部３７４ｃは、通信パターン識別部３７４ａと同じ機能を備える。
【０１６７】
不正検知処理機能群３７０ｃのこれらの構成要素も機能構成要素であり、ゲートウェイにおいて記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。
【０１６８】
［２．２　不正検知処理］シーケンス
図１４は、不正検知処理機能群３７０ｂでの不正検知処理の一例を示すフロー図である。図１０と共通のステップについては、図１４において同じ参照符号を用いて示し、一部説明を省略する。
【０１６９】
まず、不正検知部３７１ｂは、フレーム処理部３５０からメッセージを受け取る（ステップＳ１００１）。
【０１７０】
メッセージを受け取った不正検知部３７１ｂは、周期的に送信されるメッセージの受信周期が次に移ったかどうかを判定する（ステップＳ１４０２）。
【０１７１】
ステップＳ１４０２において、不正検知部３７１ｂが次の受信周期に移っていると判定した場合には、新しい基準メッセージを決定する（ステップＳ１４０３）。
【０１７２】
ステップＳ１４０３で新しい基準メッセージを決定した後、又はステップＳ１４０２において次の受信周期に移っていないと判定した場合に、不正検知処理を行う（ステップＳ１４０４）。
【０１７３】
不正検知部３７１ｂは、ＩＤ判定機能などの各種の判定機能を利用して、受信したメッセージが攻撃メッセージであるか正常メッセージであるかの判定を行う。このとき、不正検知部３７１ｂの各種の判定機能は、必要に応じて、ステップＳ１４０３で決定された基準メッセージを用いて判定を行う。そして不正検知部３７１は、その判定の結果をメッセージ保存処理部３７２へ通知する。
【０１７４】
ステップＳ１４０４のその他の処理は、図１０のステップＳ１００２の不正検知処理と同様である。
【０１７５】
ステップＳ１００３以降の処理は、図１０と共通であるため、説明を省略する。
【０１７６】
［２．３　効果］
本実施の形態では、不正検知処理機能群３７０ｂでの不正検知処理において、不正検知部３７１ｂの各種判定機能が利用する基準メッセージを決定する際に、候補のメッセージが通信パターンに適合するか否かを判定し、通信パターンに適合しない候補のメッセージから基準メッセージを決定する。これにより、従来起こり得た、攻撃メッセージを基準メッセージとして用いた結果、不正検知が正しくできない状況の発生を抑える、より高い精

度で攻撃メッセージであるか否かの判定をすることができる。その結果、車載ネットワークシステムの安全が高められる。

【０１７７】

（実施の形態３）

［３．概要］

ここでは、実施の形態３として、不正検知処理機能群の一部の機能が車両の外のサーバに配置され、ゲートウェイとサーバとが通信する車載ネットワークシステムについて、図面を参照しながら説明する。

【０１７８】

［３．１　車載ネットワークシステムの全体構成］

図１５は、本実施の形態における車載ネットワークシステム１０ａの全体構成を示すブロック図である。図１５において、図１に示される車載ネットワークシステム１０と共通の構成要素については共通の参照符号を用いて示し、その説明を省略する。

【０１７９】

車載ネットワークシステム１０ａは、ＣＡＮネットワークで構成され、ＥＣＵ１００（図中のＥＣＵ１００ａ、ＥＣＵ１００ｂ、ＥＣＵ１００ｃ、及びＥＣＵ１００ｄであり、以下ではこれらを集合的に、又は特定しない一部を指して、以下ではＥＣＵ１００ともいう）と、バス２００（図中のバス２００ａ及びバス２００ｂであり、以下ではこれらを集合的に、又は特定しない一方を指して、以下ではバス２００ともいう）と、ゲートウェイ３００ｄと、外部ネットワーク４００と、サーバ５００とを含む。

【０１８０】

ゲートウェイ３００ｄは、ＥＣＵ１００ａ及びＥＣＵ１００ｂが接続されているバス２００ａと、ＥＣＵ１００ｃ及びＥＣＵ１００ｄが接続されているバス２００ｂとを接続している。ゲートウェイ３００ｄは一方のバスから受信したメッセージを、もう一方のバスに転送する機能を持つ。ゲートウェイ３００ｄもまた、ＣＡＮネットワーク上ではひとつのノードである。

【０１８１】

外部ネットワーク４００は、ゲートウェイ３００とサーバ５００とが通信するための通信ネットワークである。外部ネットワーク４００の通信方法は、有線であっても無線であってもよい。また、無線通信方式は例えば既存技術であるＷｉ－Ｆｉ、３Ｇ、又はＬＴＥであってもよい。

【０１８２】

サーバ５００は、外部ネットワーク４００を介してゲートウェイ３００ｄと通信を行う。

【０１８３】

ゲートウェイ３００ｄとサーバ５００とは、それぞれが実施の形態１における不正検知処理機能群３７０の一部の機能を分担して備え、ゲートウェイ３００ｄとサーバ５００が連携して動作することで上述の不正検知処理を実行する。

【０１８４】

［３．２　ゲートウェイの構成］

図１６は、ゲートウェイ３００ｄの機能構成の一例を示すブロック図である。図１６において、図３と共通の構成要素については共通の参照符号で示し、説明を省略する。以下、ゲートウェイ３００ｄについて、ゲートウェイ３００との差異点を中心に説明する。

【０１８５】

ゲートウェイ３００ｄは、ゲートウェイ３００の構成における不正検知処理機能群３７０に代えて不正検知処理機能群３７０ｄを備え、また、さらに外部通信部３９０とを備える点が異なる。これらの構成要素も機能構成要素であり、ゲートウェイ３００ｄにおいて記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。

【０１８６】
不正検知処理機能群３７０ｄは、受信したメッセージが攻撃メッセージであるか否かの判定を、サーバ５００と通信し、連携して実行する。不正検知処理機能群３７０ｄに含まれる構成の詳細は後述する。
【０１８７】
外部通信部３９０は、サーバ５００との通信を行う。
【０１８８】
［３．３　不正検知処理機能群の構成］
図１７は、不正検知処理機能群３７０ｄの機能構成の一例を示すブロック図である。図１７において、図６と共通の構成要素は共通の参照符号で示し、説明を省略する。
【０１８９】
不正検知処理機能群３７０ｄは、不正検知部３７１と、メッセージ保存処理部３７２ｄと、通信パターン判定部３７５ｄとを含む。
【０１９０】
メッセージ保存処理部３７２ｄは、不正検知部３７１の判定結果を受けて、受信したメッセージが攻撃メッセージであり、保存が必要と判定した場合には、外部通信部３９０を介してサーバ５００と通信を行い、サーバ５００に攻撃メッセージに関する情報を送信して保存させる。正常メッセージの保存、メッセージの保存の要否の判定については、実施の形態１と同様である。
【０１９１】
通信パターン判定部３７５ｄは、不正検知部３７１からの判定要求に応じて、受信したメッセージが通信パターンに適合するか否かを判定する。通信パターン判定部３７５ｄはこの判定を、外部通信部３９０を介してサーバ５００と通信を行い、サーバ５００で実行された通信パターンの識別の結果を受信し、その受信した結果を用いて行う。
【０１９２】
なお、サーバ５００での通信パターンの識別では、通信パターン識別部３７４ａのように統計的処理又は確率理論を用いて、攻撃メッセージに関する情報のモデルを取得し、そのモデルを通信パターンとしてもよい。この場合には、ゲートウェイ３００ｄは不正検知処理機能群３７０ｄに代えて、図１８に示すように、通信パターン予測部３７６ｅをさらに含む不正検知処理機能群３７０ｅを備えてもよい。図１８は、本実施の形態における不正検知処理機能群の機能構成の他の例を示すブロック図である。
【０１９３】
通信パターン予測部３７６ｅは、サーバ５００が識別したモデルを、外部通信部３９０を介して受信し、このモデルを通信パターンとして用いて通信パターン予測部３７６ａがするように予測値を算出する。通信パターン判定部３７５ｅは、その予測値と、受信したメッセージに関する情報から、通信パターンに一致するか否かを判定してもよい。
【０１９４】
［３．４　サーバの構成］
図１９は、サーバ５００の機能構成の一例を示すブロック図である。サーバ５００は、攻撃メッセージ情報保持部３７３ｄと、通信パターン識別部３７４ｄとを備える。これらの構成要素は機能構成要素であって、サーバ５００は、いわゆるサーバコンピュータであり、プロセッサ等の情報処理装置、半導体メモリ等の記憶装置、入出力ポートを含む入出力部等を備える１台以上のコンピュータで実現される。上記に挙げた各機能構成要素は、記憶部に保持されるプログラムの処理部による読み出し及び実行、記憶部による所定のデータの保持、若しくは入出力部を介してのデータの送受信、又はこれらの組み合わせで実現される。
【０１９５】
攻撃メッセージ情報保持部３７３ｄは、ゲートウェイ３００ｄのメッセージ保存処理部３７２ｄから保存を指示された攻撃メッセージに関する情報を保持する。また、通信パターン識別部３７４ｄからの要求に応じて、保持している攻撃メッセージに関する情報を出

力する。
【０１９６】
通信パターン識別部３７４ｄは、攻撃メッセージ情報保持部３７３ｄから、攻撃メッセージに関する情報を取得し、受信した攻撃メッセージに見られる通信パターンを識別する。具体的な識別方法は、上述の各実施の形態の通信パターン識別部と同じであるため、説明を省略する。
【０１９７】
また、通信パターン識別部３７４ｄは、ゲートウェイ３００ｄの通信パターン判定部３７５ｄ、又は通信パターン予測部３７６ｅからの要求に応じて、識別した通信パターンを送信する。
【０１９８】
なお、サーバ５００は、複数の車両と通信し、各車両に対して不正検知処理機能群の一部の機能を担ってもよい。この場合、サーバ５００は、それぞれの車両に対して個別の攻撃メッセージ情報保持部３７３ｄ及び通信パターン識別部３７４ｄを備えてもよいし、通信する複数の車両に対して、一組の攻撃メッセージ情報保持部３７３ｄ及び通信パターン識別部３７４ｄを備えてもよい。またサーバ５００は、通信する複数の車両の一部に対して一組の攻撃メッセージ情報保持部３７３ｄ及び通信パターン識別部３７４ｄを備えてもよい。複数の車両に対して一組を備える場合、攻撃メッセージ情報保持部３７３ｄは、各車両から取得した攻撃メッセージに関する情報を、各車両を識別する情報と一緒に保持する。
【０１９９】
また、通信パターン識別部３７４ｄは、各車両から受信した情報から通信パターンを個別に識別し、個別の識別結果を各車両へ送信してもよいし、各車両からの情報を統合したものを用いて通信パターンを識別し、各車両へその識別の結果を送信してもよい。
【０２００】
ここで、各車両からの情報を統合する方法は、例えば全ての車両からの情報を統合してもよいし、各車両の製造メーカ又は車種、さらに型式、グレードごとに統合してもよい。または、各車両の車両クラス（大きさ、排気量等）ごと、各車両の所在地ごと、又は各車両が持つ機能（自動運転機能、運転支援機能、通信機能等）ごとに統合してもよい。または、各車両上のＥＣＵ等で実行されるファームウェア又はソフトウェアの種類、若しくはさらにそのバージョンごとに統合してもよい。また、これらの統合方法の組み合わせでもよい。
【０２０１】
［３．５　効果］
本実施の形態では、ゲートウェイ３００と車両の外部のサーバ５００サーバ５００が通信し、不正検知処理機能群３７０ｄ又は不正検知処理機能群３７０ｅの一部の機能が、サーバ５００によって担われる。
【０２０２】
従来では、個々の車両で収集される情報のみから通信パターンが識別され、判定可能な通信パターンが限られていた。しかし、本実施の形態においては、サーバ５００に情報を保持することで、複数の車両の情報から通信パターンを識別することが可能にある。これにより、より多くの攻撃メッセージに基づいて通信パターンが迅速に、又はより高い精度で識別される。そして各車両ではこの通信パターンが用いられることで、より高い精度での攻撃メッセージであるか否かの識別をすることができる。その結果、車載ネットワークシステムの安全が高められる。また、攻撃メッセージに関する情報がサーバ５００に保持されるため、ゲートウェイ３００に大容量の情報保持装置を備える必要が無く、各車両の製造及び維持コストを抑えることも可能となる。
【０２０３】
［４．　その他の変形例］
本発明は、上記で説明した各実施の形態に限定されないのはもちろんであり、本開示の

趣旨を逸脱しない限り、当業者が思いつく各種変形を実施の形態に施したもの、及び異なる実施の形態における構成要素を組み合わせて構築される形態も、本発明の範囲内に含まれる。例えば以下のような変形例も本発明に含まれる。

【０２０４】

（１）上記の実施の形態では、不正検知処理機能群３７０ｃは、不正検知部３７１と、メッセージ保存処理部３７２と、攻撃メッセージ情報保持部３７３と、通信パターン識別部３７４ｃと、通信パターン判定部３７５ｃと、通信パターン予測部３７６ｃと、基準メッセージ決定部３７７ｂと、基準メッセージ候補保持部３７８ｂとを備えると説明したが、これに限定されない。

【０２０５】

図２０に示すように、不正検知部３７１と、メッセージ保存処理部３７２ｆと、攻撃メッセージ情報保持部３７３ｆと、通信パターン識別部３７４ｆと、通信パターン判定部３７５ｆと、通信パターン予測部３７６ｃと、基準メッセージ決定部３７７ｂと、基準メッセージ候補保持部３７８ｂと、車両状態認識部３７９ｆとを備えてもよい。また、他の実施の形態における不正検知処理機能群（３７０、３７０ａ、３７０ｂ、３７０ｄ、３７０ｅ）が、さらに車両状態認識部３７９ｆを備えてもよい（図示なし）。

【０２０６】

ここで、車両状態認識部３７９ｆは、車両がどのような状態であるかをＣＡＮメッセージの内容、又は各種スイッチの状態などから認識する。車両状態認識部３７９ｆが認識する状態としては、例えば、車両の自動運転に関する状態である。より具体的には、例えば車両が現在、運転者が運転行動（認知、判断及び操作）のほぼ全般を行って車両を操作し走行している「通常走行モード」か、車両が運転行動の一部を補助・支援している「運転支援モード」か、運転者は運転行動をせずに車両が自動運転している「自動運転モード」か等である。または、車両の「走行中」、「停車中」、又は「駐車中（エンジンＯＦＦ）」のいずれかの状態であってもよい。また、これらの状態のうち、並立可能な複数の状態が認識されてもよい。または、自動運転を実現するための各種の機能（以下、自動運転機能ともいう）のうち１つ以上の機能の有効又は無効という状態であってもよい。

【０２０７】

例えばメッセージ保存処理部３７２ｆは、攻撃メッセージに関する情報に加えて、その時に車両状態認識部３７９ｆが認識して出力する、状態を示す情報を一緒に保存してもよい。また、メッセージ保存処理部３７２ｆは、特定の状態を示す情報を受信した場合のみ、攻撃メッセージに関する情報を保存してもよい。

【０２０８】

また、通信パターン識別部３７４ｆ及び通信パターン判定部３７５ｆは、車両状態認識部３７９ｆが出力した情報が示す所定の異なる状態に応じてそれぞれが動作してもよい。

【０２０９】

より具体的な例を挙げると、通信パターン識別部３７４ｆは、「通常走行モード」の間、又は「通常走行モード」から「運転支援モード」又は「自動運転モード」へ切り替わるタイミングで、通信パターンを識別する。一方、通信パターン判定部３７５ｆは、「運転支援モード」又は「自動運転モード」の時に、が通信パターンを判定する。別の例として、通信パターン識別部３７４ｆは、「停車中」又は「駐車中」の時に通信パターンを識別し、通信パターン判定部３７５ｆは、「走行中」の時に通信パターンを判定する。

【０２１０】

これにより、車両が攻撃を判定しやすい状態にあるとき、攻撃メッセージに関する情報の収集及び保持及び通信パターンの識別が実行され、車両が攻撃の判定が難しい状態にあるときに通信パターンを使った判定を行うことができる。より具体的には、車両で自動運転機能が実行されていないときは、ＥＣＵが接続されるセンサの出力情報には不要なものがあり、アクチュエータ等に対するＥＣＵからの制御信号も不要である。したがって、自動運転機能が実行されているときに比べてノード間の通信が少なく、攻撃メッセージは他のメッセージに紛れにくいため、攻撃の判定の精度が上がりやすい。その結果、更なる不

正検知精度の向上や、処理コストを低減することが可能となる。

【０２１１】

（２）不正検知処理機能群３７０は、不正検知部３７１と、メッセージ保存処理部３７２と、攻撃メッセージ情報保持部３７３と、通信パターン識別部３７４と、通信パターン判定部３７５とを備えると説明したが、これに限定されない。不正検知処理機能群はより少ない構成要素で構成されてもよい。例えば図２１に示すように、不正検知部３７１ｇと通信パターン判定部３７５ｇとを備える不正検知処理機能群３７０ｇであってもよい。

【０２１２】

また、不正検知処理機能群３７０ｂは、不正検知部３７１と、メッセージ保存処理部３７２と、攻撃メッセージ情報保持部３７３と、通信パターン識別部３７４と、通信パターン判定部３７５と、基準メッセージ決定部３７７ｂと、基準メッセージ候補保持部３７８ｂとを備えると説明したが、これに限定されない。例えば図２２に示すように、より少ない構成要件である不正検知部３７１ｈと、通信パターン判定部３７５ｈと、基準メッセージ決定部３７７ｂと、基準メッセージ候補保持部３７８ｂとを備える不正検知処理機能群３７０ｈであってもよい。

【０２１３】

上記において、通信パターン判定部３７５ｇ及び通信パターン判定部３７５ｈは、事前に通信パターンに関する情報を保持しており、その情報を用いて、通信パターンに適合しているか否かの判定をする。これにより、攻撃メッセージ情報の保持が不要となり、攻撃メッセージを保持するための攻撃メッセージ情報保持装置の分のコストを節約することができる。

【０２１４】

（３）不正検知処理機能群３７０は、不正検知部３７１と、メッセージ保存処理部３７２と、攻撃メッセージ情報保持部３７３と、通信パターン識別部３７４と、通信パターン判定部３７５とを備えると説明したが、これに限定されない。図２３のように、不正検知部３７１ｉと、通信パターン判定部３７５ｇと、車両状態認識部３７９ｆとを備える不正検知処理機能群３７０ｉであってもよい。この場合、不正検知部３７１ｉは、車両状態認識部３７９ｆが認識した車両の状態に応じて、通信パターン判定部３７５ｇの判定結果を不正検知処理で利用するかどうかを決定する。

【０２１５】

これにより、通信パターン判定部３７５ｇによる判定処理を適切なタイミングで行うことが可能となり、例えば不要なタイミングでの判定処理を省くことができる。

【０２１６】

（４）上記実施の形態では、ＥＣＵ１００は、フレーム送受信部１１０と、フレーム解釈部１２０と、受信ＩＤ判定部１３０と、受信ＩＤリスト保持部１４０と、フレーム処理部１５０と、データ取得部１７０と、フレーム生成部１８０とを備えると説明したが、本開示における車載ネットワークシステムが備えるＥＣＵの構成はこれに限定されるものではない。

【０２１７】

例えば、図２４に示すＥＣＵ１００ｅのように、車載ネットワークシステムが備えるＥＣＵはさらに不正検知処理機能群３７０を備えてもよい。この場合、攻撃メッセージであるか否かの判定を、フレーム処理部１５０が不正検知処理機能群３７０へ要求してもよいし、フレーム解釈部１２０が要求してもよい。

【０２１８】

また、図２５に示すＥＣＵ１００ｆのように、車載ネットワークシステムが備えるＥＣＵは、フレーム送受信部１１０と、フレーム解釈部１２０と、フレーム生成部１８０とで構成されてもよい。この場合、フレーム解釈部１２０は、例えばＩＤによらず全てのメッセージを受信し、全てのメッセージについて不正検知処理機能群３７０へ攻撃メッセージであるかどうかの判定を依頼してもよい。

【０２１９】

また、ＥＣＵ１００は、図２５の構成に加えて、受信ＩＤ判定部１３０と、受信ＩＤリスト保持部１４０とを備え、受信ＩＤリスト保持部が保持する受信ＩＤリストに記載されたメッセージＩＤを持つメッセージのみを受信し、そのメッセージに関して、不正検知処理機能群３７０へ攻撃メッセージであるか否かの判定を依頼してもよい。なお、不正検知処理機能群３７０は、上述の３７０ａ～３７０ｉのいずれに代えられてもよい。

【０２２０】

これにより、ゲートウェイだけでなく、ＥＣＵでも、バスに送信されているメッセージが攻撃メッセージであるか否かを判定できる。その結果、例えば車載ネットワークシステムにおける不正通信のための仕組の冗長性が向上し、より高度に安全が確保される。

【０２２１】

さらに、図２６に示すＥＣＵ１００ｇのように、車載ネットワークシステムが備えるＥＣＵは、バス２００へ送信するデータを他の接続機器又は外部等から取得する送信データ取得部１７１を備えてもよい。ＥＣＵ１００ｇが備える不正検知処理機能群３７０ｊは、送信データ取得部１７１から受信したデータが攻撃メッセージであるか否かについても判定し、攻撃メッセージではないと判定した場合のみ、フレーム生成部１８０へメッセージの送信を依頼してもよい。なお、不正検知処理機能群３７０ｊの構成は、不正検知処理機能群３７０、３７０ａ～３７０ｉのいずれと共通であってもよい。

【０２２２】

これにより、例えばカーナビゲーションと一緒に利用されるＥＣＵが、乗っ取られたカーナビゲーションから攻撃メッセージが送信されるような場合において、そのメッセージのネットワークへの拡散を抑制することができる。または、車外から送り込みが試みられる攻撃メッセージの車載ネットワークシステム内部への侵入を抑制することができる。

【０２２３】

（５）上記実施の形態では、不正の検知に応じたアクションとして、受信したメッセージを転送しない例を示したが、これに限定されない。例えば上述の不正検知処理機能群を備えるゲートウェイ又はＥＣＵは、メッセージの受信中に不正検知処理を行い、攻撃メッセージであると判定した時点で、エラーフレームを送信することで、ネットワークから受信中のメッセージを無効化してもよい。

【０２２４】

これにより、攻撃メッセージが見つかったバスに接続された他のＥＣＵが攻撃メッセージを受信することを防止することができる。同様のアクションは、転送しないメッセージに対しても適用できる。

【０２２５】

また、上述の不正検知処理機能群を備えるゲートウェイ又はＥＣＵはさらに、不正の発生のユーザ若しくは外部のサーバ等への通知、不正の発生のログへの記録、又は車両のフェールセーフモードへの移行を実行してもよい。

【０２２６】

これにより、不正検知後の柔軟な対応が可能となる。また攻撃メッセージと判定した複数のメッセージをデータの１以上の系列として扱い、各系列について、データの値や受信間隔の集合を不正なラベルとして学習してもよい。

【０２２７】

（６）上記実施の形態では、メッセージ保存処理部３７２は、受信したメッセージが攻撃メッセージであり、かつ、保存が必要と判定した場合には、攻撃メッセージに関連する情報を保存すると説明したが、これに限定されない。例えばメッセージ保存処理部３７２はさらに、メッセージの受信時には攻撃メッセージとも正常メッセージとも判定できなかったメッセージをグレーメッセージとして、これに関する情報を保存してもよい。

【０２２８】

グレーメッセージとして保持されているメッセージには、所定のタイミングで、再び正常メッセージか攻撃メッセージかの判定が行われる。また、この結果として新たに攻撃メッセージと判定されたメッセージから通信パターンが識別されてもよいし、グレーメッセ

ージとして保存されていた情報を、攻撃メッセージに関連する情報として保存し直し、他の攻撃メッセージに関連する情報と一緒に用いて通信パターンの識別が行われてもよい。

【０２２９】

グレーメッセージを判定するタイミングとしては、例えば１０件のメッセージなど、事前に決定された数の攻撃メッセージに関する情報が保存されたときでもよいし、１分など、事前に決定された時間ごと、または車両状態認識部３７９ｆにより判定される車両の状態が切り替わったときでもよい。

【０２３０】

また、グレーメッセージに対する正常メッセージか攻撃メッセージかの判定方法としては、再度、不正検知部３７１によりメッセージごとに判定を行ってもよいし、複数のグレーメッセージをデータの１以上の系列とみて、その系列が正常メッセージの系列か、攻撃メッセージの系列かを判定してもよい。例えば、単純にデータ値が一定の範囲内に収まるグレーメッセージ同士を１つの系列として複数の系列に分け、各系列について正常メッセージの系列か、攻撃メッセージの系列かを判定してもよい。または、グレーメッセージを時系列に並べたときに、データ値が一定の大きさ以上に変化するメッセージを別系列のデータであると判定することで複数の系列に分け、正常メッセージの系列か、攻撃メッセージの系列かを判定してもよい。または、機械学習の分野におけるクラスタリングの手法を用いて系列を分け、正常メッセージの系列か、攻撃メッセージの系列かを判定してもよい。

【０２３１】

正常メッセージの系列か、攻撃メッセージの系列かを判定する方法としては、例えば、正常メッセージの一つ前のメッセージとの受信時刻の差の分散値などの統計量をあらかじめ計算しておき、どの系列があらかじめ計算された統計量と近いかに基づいて、正常メッセージの系列か、攻撃メッセージの系列かを判定してもよいし、正常メッセージの系列の受信時刻差と、評価対象メッセージの系列の受信時刻差の密度比推定を介した異常度の算出により攻撃メッセージの系列を求めてもよい。

【０２３２】

また、通信パターンを識別するタイミングは、グレーメッセージから攻撃メッセージへ保存し直した直後でもよいし、他のタイミングであってもよい。

【０２３３】

（７）上記実施の形態では、標準フォーマットのＩＤにおける例を示したが、拡張フォーマットのＩＤであってもよい。

【０２３４】

（８）上記実施の形態では、メッセージは平文で送信される例を示したが、暗号化されていてもよい。またメッセージにメッセージ認証コードを含んでいてもよい。

【０２３５】

（９）上記実施の形態では、正常モデルと、受信ログとを平文で保持している例を示したが、これらを暗号化して保持していてもよい。

【０２３６】

（１０）上記の実施の形態では、ＣＡＮプロトコルに従って通信するネットワーク通信システムの例として車載ネットワークを示した。本発明に係る技術は、車載ネットワークでの利用に限定されるものではなく、ロボット、産業機器等のネットワークその他、車載ネットワーク以外のＣＡＮプロトコルに従って通信するネットワーク通信システムに利用してもよい。

【０２３７】

また、車載ネットワークとしてＣＡＮプロトコルを用いていたが、これに限るものではない。例えば、ＣＡＮ－ＦＤ（ＣＡＮ ｗｉｔｈ Ｆｌｅｘｉｂｌｅ Ｄａｔａ Ｒａｔｅ）、ＦｌｅｘＲａｙ、Ｅｔｈｅｒｎｅｔ、ＬＩＮ（Ｌｏｃａｌ Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｎｅｔｗｏｒｋ）、ＭＯＳＴ（Ｍｅｄｉａ Ｏｒｉｅｎｔｅｄ Ｓｙｓｔｅｍｓ Ｔｒａｎｓｐｏｒｔ）などを用いてもよい。あるいはこれらのネットワークをサブネット

ワークとして、組み合わせたネットワークであってもよい。

【０２３８】

（１１）上記の実施の形態における各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、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、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭまたはハードディスクユニットには、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、各装置は、その機能を達成する。ここで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、コンピュータ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。

【０２３９】

（１２）上記の実施の形態における各装置は、構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。ＲＡＭには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、システムＬＳＩは、その機能を達成する。

【０２４０】

また、上記の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、一部又は全てを含むように１チップ化されてもよい。

【０２４１】

また、ここでは、システムＬＳＩとしたが、集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

【０２４２】

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よい。バイオ技術の適用等が可能性としてありえる。

【０２４３】

（１３）上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしてもよい。ＩＣカード又はモジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。ＩＣカード又はモジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、ＩＣカード又は前記モジュールは、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よい。

【０２４４】

（１４）本発明は、上記に示す方法であるとしてもよい。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よいし、コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０２４５】

また、本発明は、コンピュータプログラム又はデジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ（登録商標）　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されているデジタル信号であるとしてもよい。

【０２４６】

また、本発明は、コンピュータプログラム又はデジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

【０２４７】

また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、上記コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムに従って動作するとしてもよい。

【０２４８】

また、プログラム又はデジタル信号を記録媒体に記録して移送することにより、又はプログラム又はデジタル信号を、ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０２４９】

（１５）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０２５０】

以上、一つ又は複数の態様に係る車載ネットワークにおける、不正メッセージによる不正制御を目的とする不正通信検知のための技術について実施の形態及びその変形例に基づいて説明した。これらの各実施の形態及びその変形例では、車載ネットワークシステムに接続されて通信するゲートウェイ若しくはＥＣＵ、又はこれらとサーバコンピュータとの組み合わせによって不正通信検知が実行される。このような不正通信検知を実行する、１個以上のプロセッサ及び記憶部を含むシステムを、本開示では不正通信検知システムと呼ぶ。したがって、不正通信検知システムは車載ネットワークシステムに接続される１台のゲートウェイのように１個の装置によって実現されるものも、このようなゲートウェイとＥＣＵとの組み合わせ、又はゲートウェイ若しくはＥＣＵと遠隔にあるサーバコンピュータとの組み合わせのように複数個の装置によって実現されるものも含む。

【０２５１】

また、この技術は、上記各実施の形態又はその変形例において、各構成要素が実行する処理のステップの一部又は全部を含む方法として、又は不正通信検知システムのプロセッサに実行されて、不正通信検知システムがこの方法を実施させるためのプログラムとしても実現可能である。

【０２５２】

また、上記実施の形態又はその変形例において、特定の構成要素が実行する処理を特定の構成要素の代わりに別の構成要素が実行してもよい。また、複数の処理の順序が変更されてもよいし、複数の処理が並行して実行されてもよい。

【産業上の利用可能性】

【０２５３】

本発明に係る不正通信検知方法等は、攻撃メッセージの通信パターンを識別し、受信したメッセージを通信パターンに適合するか否かを判定することで不正を検知する。これにより従来では、正常メッセージと攻撃メッセージの識別が困難であったメッセージに関しても、精度よく、正常なメッセージを識別することができ、車載ネットワークの保護が可能となる。

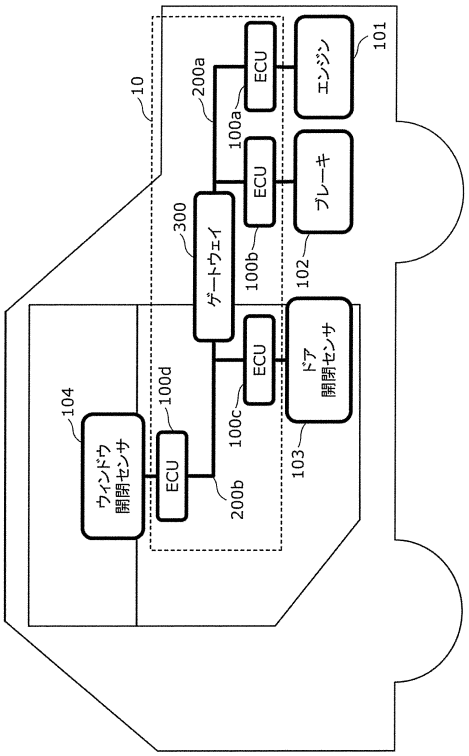
【符号の説明】

【０２５４】

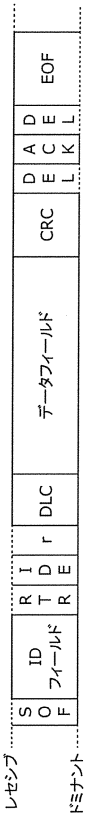
１０、１０ａ　車載ネットワークシステム
１００、１００ａ、１００ｂ、１００ｃ、１００ｄ、１００ｅ、１００ｆ、１００ｇ　ＥＣＵ
１０１　エンジン
１０２　ブレーキ
１０３　ドア開閉センサ
１０４　ウィンドウ開閉センサ
１１０　フレーム送受信部

１２０　フレーム解釈部
１３０　受信ＩＤ判定部
１４０　受信ＩＤリスト保持部
１５０　フレーム処理部
１７０　データ取得部
１７１　送信データ取得部
１８０　フレーム生成部
２００、２００ａ、２００ｂ　バス
３００、３００ｄ　ゲートウェイ
３１０　フレーム送受信部
３２０　フレーム解釈部
３３０　受信ＩＤ判定部
３４０　受信ＩＤリスト保持部
３５０　フレーム処理部
３６０　転送ルール保持部
３７０、３７０ａ、３７０ｂ、３７０ｃ、３７０ｄ、３７０ｅ、３７０ｆ、３７０ｇ、３７０ｈ、３７０ｉ、３７０ｊ　不正検知処理機能群
３７１、３７１ｂ、３７１ｇ、３７１ｈ、３７１ｉ　不正検知部
３７２、３７２ｄ、３７２ｆ　メッセージ保存処理部
３７３、３７３ｄ、３７３ｆ　攻撃メッセージ情報保持部
３７４、３７４ａ、３７４ｃ、３７４ｄ、３７４ｆ　通信パターン識別部
３７５、３７５ａ、３７５ｂ、３７５ｃ、３７５ｄ、３７５ｅ、３７５ｆ、３７５ｇ、３７５ｈ　通信パターン判定部
３７６ａ、３７６ｃ、３７６ｅ　通信パターン予測部
３７７ｂ　基準メッセージ決定部
３７８ｂ　基準メッセージ候補保持部
３７９ｆ　車両状態認識部
３８０　フレーム生成部
３９０　外部通信部
４００　外部ネットワーク
５００　サーバ

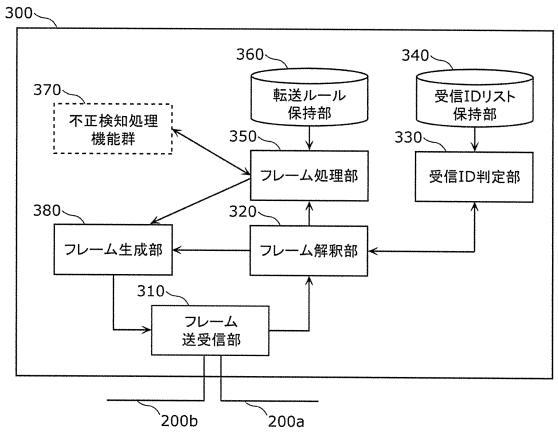
【図１】



【図２】



【図３】



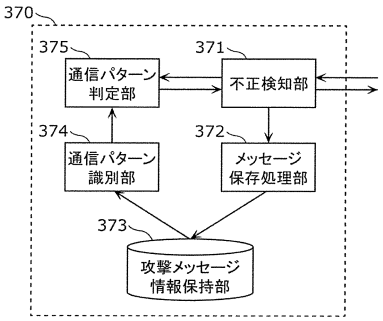
【図４】

受信IDリスト
1
2
3
4

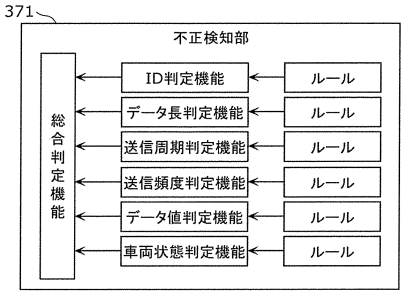
【図５】

転送元	転送先	ID
200a	200b	*
200b	200a	3

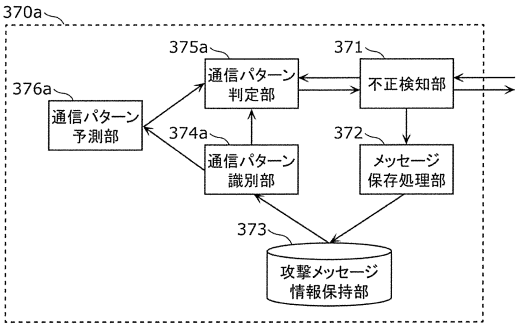
【図６】



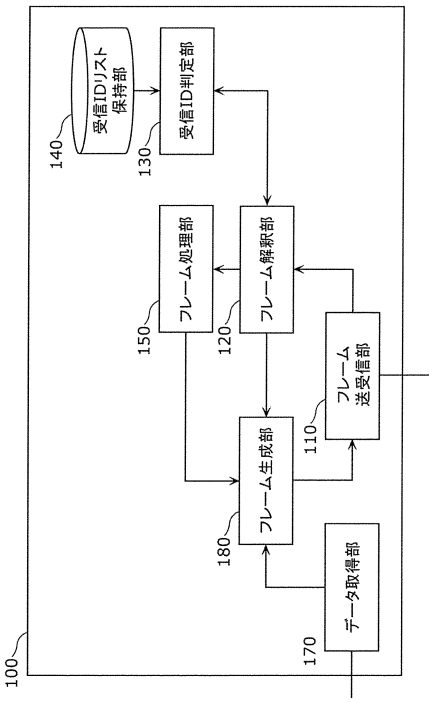
【図７】



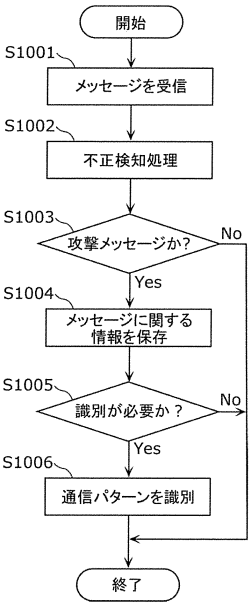
【図８】


370a
375a
通信パターン
判定部
371
不正検知部
376a
通信パターン
予測部
374a
通信パターン
識別部
372
メッセージ
保存処理部
373
攻撃メッセージ
情報保持部

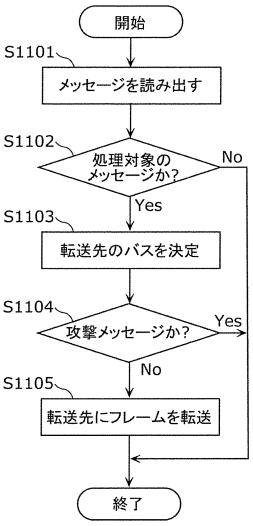
【図９】


受信IDリスト
保持部
140
受信ID判定部
130
フレーム処理部
150
フレーム解釈部
120
フレーム
送受信部
110
フレーム生成部
180
データ取得部
170
100

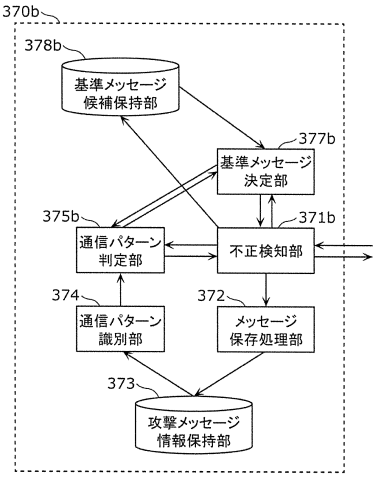
【図１０】


開始
S1001
メッセージを受信
S1002
不正検知処理
S1003
攻撃メッセージか?
No
Yes
S1004
メッセージに関する
情報を保存
S1005
識別が必要か？
No
Yes
S1006
通信パターンを識別
終了

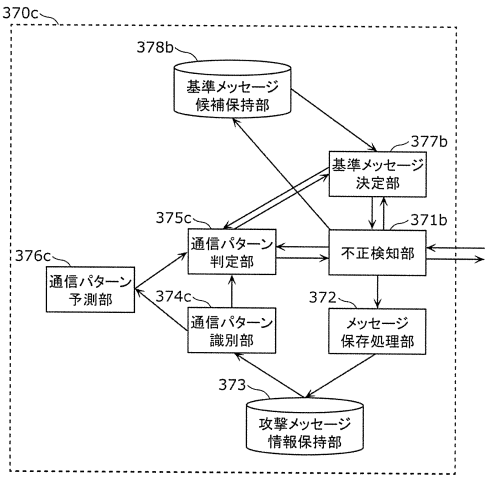
【図１１】


開始
S1101
メッセージを読み出す
S1102
処理対象の
メッセージか?
No
Yes
S1103
転送先のパスを決定
S1104
攻撃メッセージか?
Yes
No
S1105
転送先にフレームを転送
終了

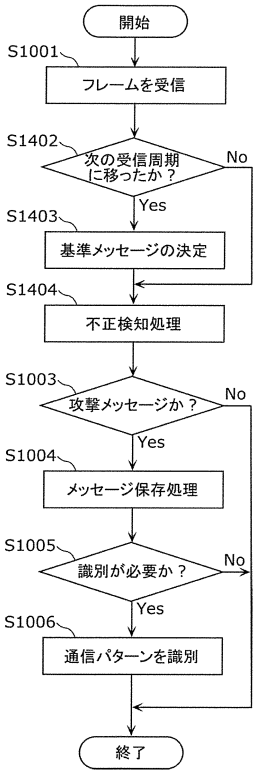
【図１２】



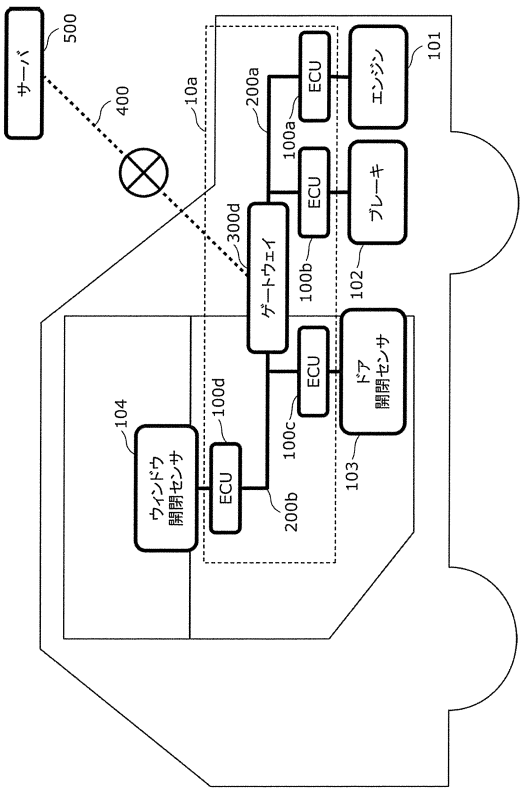
【図１３】



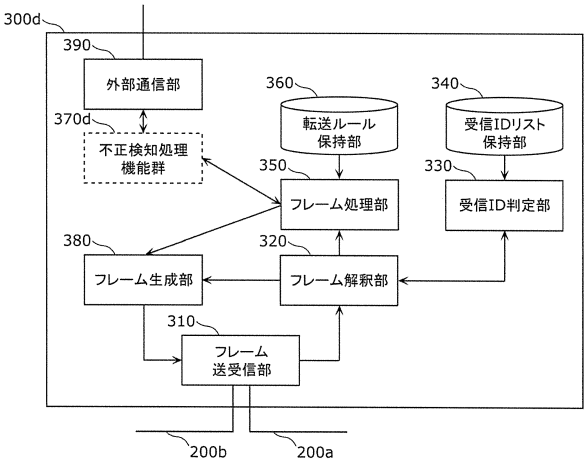
【図１４】



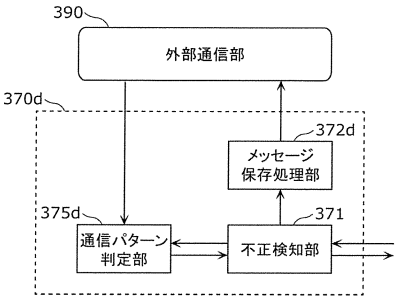
【図１５】



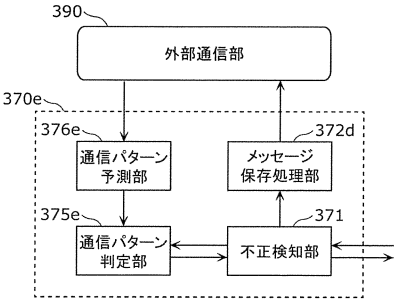
【図１６】



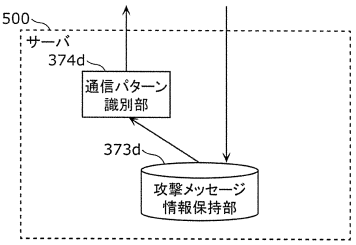
【図１７】



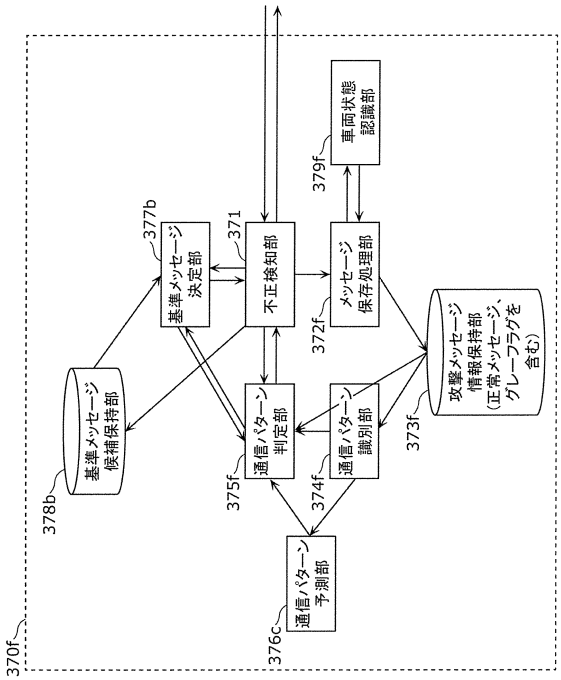
【図１８】



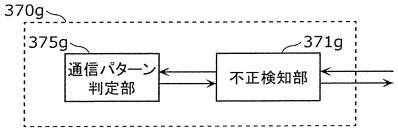
【図１９】



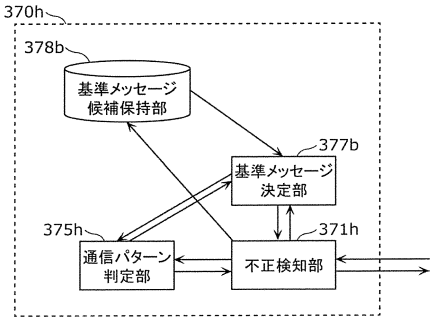
【図２０】



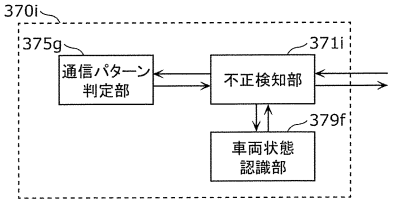
【図２１】



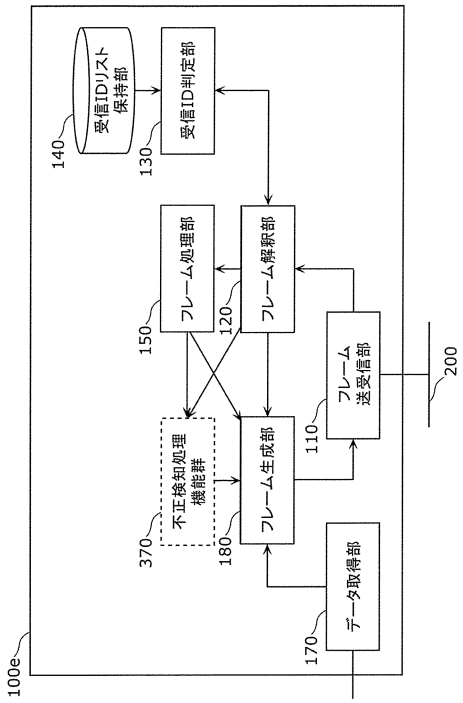
【図２２】



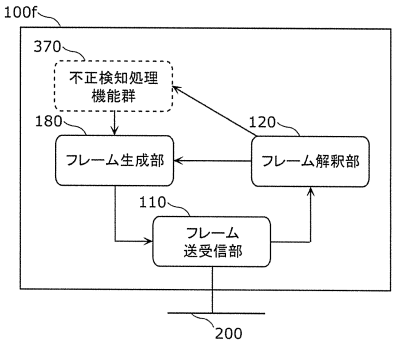
【図２３】



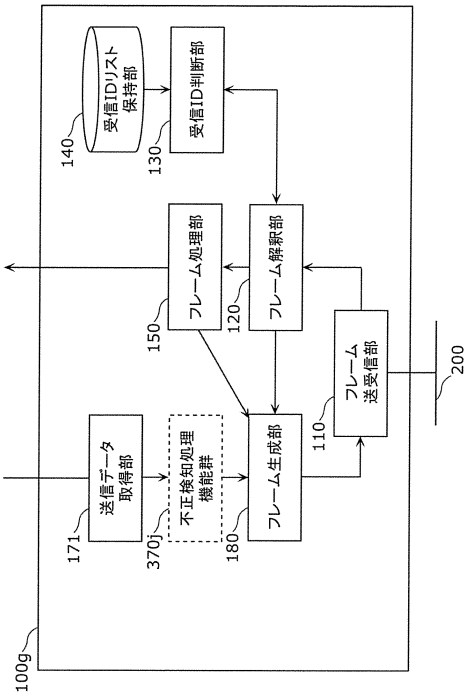
【図２４】


受信IDリスト保持部
140
受信ID判定部
130
フレーム処理部
150
フレーム解釈部
120
フレーム送受信部
110
200
不正検知処理機能群
370
フレーム生成部
180
データ取得部
170
100e

【図２５】


100f
370
不正検知処理機能群
180
フレーム生成部
120
フレーム解釈部
110
フレーム送受信部
200

【図２６】


受信IDリスト保持部
140
受信ID判断部
130
フレーム処理部
150
フレーム解釈部
120
フレーム送受信部
110
200
送信データ取得部
171
不正検知処理機能群
370
フレーム生成部
180
100g

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　前田　学
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　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
(72)発明者　国宗　大介
大阪府門真市大字門真１００６番地　パナソニックデバイスシステムテクノ株式会社内

審査官　大石　博見

(56)参考文献　特開２０１４－１４６８６８（ＪＰ，Ａ）
米国特許出願公開第２００４／０１１１５０８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２８
Ｈ０４Ｌ　１２／６６