

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6494821号  
(P6494821)

(45) 発行日 平成31年4月3日(2019.4.3)

(24) 登録日 平成31年3月15日(2019.3.15)

|              |       |           |        |       |         |
|--------------|-------|-----------|--------|-------|---------|
| (51) Int.Cl. |       | F I       |        |       |         |
| HO 4 L       | 12/28 | (2006.01) | HO 4 L | 12/28 | 2 0 0 M |
| HO 4 L       | 12/70 | (2013.01) | HO 4 L | 12/28 | 1 0 0 A |
|              |       |           | HO 4 L | 12/70 | 1 0 0 Z |

請求項の数 8 (全 38 頁)

|              |                               |           |                                 |
|--------------|-------------------------------|-----------|---------------------------------|
| (21) 出願番号    | 特願2018-20034 (P2018-20034)    | (73) 特許権者 | 514136668                       |
| (22) 出願日     | 平成30年2月7日(2018.2.7)           |           | パナソニック インテレクチュアル プロ             |
| (65) 公開番号    | 特開2018-182725 (P2018-182725A) |           | パティ コーポレーション オブ アメリ             |
| (43) 公開日     | 平成30年11月15日(2018.11.15)       |           | カ                               |
| 審査請求日        | 平成30年12月25日(2018.12.25)       |           | Panasonic Intellectual          |
| (31) 優先権主張番号 | 特願2017-76637 (P2017-76637)    |           | Property Corporation of America |
| (32) 優先日     | 平成29年4月7日(2017.4.7)           |           | アメリカ合衆国 90503 カリフォル             |
| (33) 優先権主張国  | 日本国(JP)                       |           | ニア州, トーランス, スイート 200,           |
| 早期審査対象出願     |                               |           | 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】 不正通信検知基準決定方法、不正通信検知基準決定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に用いる基準メッセージの決定方法であって、

前記車載ネットワークシステムに対する攻撃メッセージに関する情報から、前記攻撃メッセージの特徴を示す通信パターンを識別する通信パターン識別ステップと、

前記ネットワークに送出されたメッセージが、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、

前記ネットワークに送出されるメッセージが攻撃メッセージであるか否かの判定の基準に用いる基準メッセージを、前記通信パターン判定ステップにおける判定結果を用いて決定する基準メッセージ決定ステップとを含む、

不正通信検知基準決定方法。

## 【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、前記ネットワークに送出された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、

前記基準メッセージ決定ステップでは、前記複数のメッセージのそれぞれが含むデータ値に基づいて前記複数のメッセージから選択される一のメッセージを前記基準メッセージとして決定する、

請求項 1 に記載の不正通信検知基準決定方法。

10

20

## 【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の割合に関するパターン、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基準決定方法。

## 【請求項 4】

さらに、前記基準メッセージ決定ステップにおいて、

前記通信パターン判定ステップにおける判定結果で、通信パターンに適合しないと判定されたメッセージがないために基準メッセージが決定できない場合、前記通信パターン判定ステップにおける判定結果を用いずに所定のルールに従って、前記基準メッセージを決定する、

請求項 1 から 3 のいずれか一項に記載の不正通信検知基準決定方法。

## 【請求項 5】

さらに、前記基準メッセージ決定ステップにおいて、

前記通信パターン判定ステップにおける判定結果で、通信パターンに適合しないと判定されたメッセージが複数ある場合、前記通信パターンに適合しないと判定された複数のメッセージから所定のルールに従って選択される一のメッセージを前記基準メッセージとして決定する、

請求項 1 から 3 のいずれか一項に記載の不正通信検知基準決定方法。

## 【請求項 6】

前記所定のルールは、前記送出されたメッセージの送信時刻若しくは受信時刻、又はデータ値に関する所定のルールである

請求項 4 又は 5 に記載の不正通信検知基準決定方法。

## 【請求項 7】

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に用いる基準メッセージの決定システムであって、

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、

前記車載ネットワークシステムに対する攻撃メッセージに関する情報から、前記攻撃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特徴を示す通信パターンを識別し、

前記ネットワークに送出されたメッセージが、識別された前記通信パターンに適合するか否かを判定し、

前記ネットワークに送出されるメッセージが攻撃メッセージであるか否かの判定の基準に用いる基準メッセージを、前記通信パターンに適合するか否かの判定の結果を用いて決定する、

不正通信検知基準決定システム。

## 【請求項 8】

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基準決定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】

10

20

30

40

50

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。

10

【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、予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。

20

【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。

30

【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ために基準として利用されるメッセージを決定する不正通信検知基準決定方法、不正通信検知基準決定等を提供することを目的とする。

40

【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基準決定方法は、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に用いる基準メッセージの決定方法であって、前記車載ネットワークシステムに対する攻撃メッセージに関する情報から、前記攻撃メッセージの特徴を示す通信パターンを識別する通信パターン識別ステップと、前記ネットワークに送出されたメッセージが、前記通信パ

50

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、前記ネットワークに送出されるメッセージが攻撃メッセージであるか否かの判定の基準に用いる基準メッセージを、前記通信パターン判定ステップにおける判定結果を用いて決定する基準メッセージ決定ステップとを含む。

【 0 0 0 9 】

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】

10

【 0 0 1 0 】

本開示の一態様に係る不正通信検知基準決定方法等によれば、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ための基準となるメッセージを決定することができる。

【図面の簡単な説明】

【 0 0 1 1 】

【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。

20

【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。

30

【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。

40

【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

50

る。

【図 2 1】図 2 1 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 2 2】図 2 2 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 2 3】図 2 3 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 2 4】図 2 4 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 2 5】図 2 5 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 2 6】図 2 6 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基準決定方法は、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に用いる基準メッセージの決定方法であって、前記車載ネットワークシステムに対する攻撃メッセージに関する情報から、前記攻撃メッセージの特徴を示す通信パターンを識別する通信パターン識別ステップと、前記ネットワークに送出されたメッセージが、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、前記ネットワークに送出されるメッセージが攻撃メッセージであるか否かの判定の基準に用いる基準メッセージを、前記通信パターン判定ステップにおける判定結果を用いて決定する基準メッセージ決定ステップとを含む。

【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の判定に基準として用いられる基準メッセージが適切に選択される。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、前記ネットワークに送出された複数のメッセージの受信時刻に関するパターンが識別され、前記基準メッセージ決定ステップでは、前記複数のメッセージのそれぞれの、前記受信時刻に関するパターンに基づく受信予定時刻と、実際の受信時刻との比較の結果に基づいて前記複数のメッセージから選択される一のメッセージを前記基準メッセージとして決定してもよい。

【0016】

これにより、攻撃メッセージと正常メッセージとのそれぞれの受信時刻に現れる特徴をに基づくことで、基準メッセージがより高い精度で選択される。

【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、前記ネットワークに送出された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、前記基準メッセージ決定ステップでは、前記複数のメッセージのそれぞれが含むデータ値に基づいて前記複数のメッセージから選択される一のメッセージを前記基準メッ

10

20

30

40

50

セージとして決定してもよい。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の割合に関するパターン、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。

#### 【0018】

これにより、攻撃メッセージと正常メッセージとのそれぞれのデータ値に現れる特徴をに基づくことで、基準メッセージがより高い精度で選択される。

10

#### 【0019】

また例えば、さらに、前記基準メッセージ決定ステップにおいて、前記通信パターン判定ステップにおける判定結果で、通信パターンに適合しないと判定されたメッセージがないために基準メッセージが決定できない場合、前記通信パターン判定ステップにおける判定結果を用いずに所定のルールに従って、前記基準メッセージを決定してもよい。もしくは、さらに、前記基準メッセージ決定ステップにおいて、前記通信パターン判定ステップにおける判定結果で、通信パターンに適合しないと判定されたメッセージが複数ある場合、前記通信パターンに適合しないと判定された複数のメッセージから所定のルールに従って選択される一のメッセージを前記基準メッセージとして決定してもよい。より具体的には、前記所定のルールは、前記送出されたメッセージの送信時刻若しくは受信時刻、又はデータ値に関する所定のルールであってもよい。

20

#### 【0020】

これにより、受信時刻又はデータ値の特徴に基づくのみでは、基準メッセージの候補が選択できない場合であっても、基準メッセージを用意して不正検知を実行することができる。

#### 【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。

30

#### 【0022】

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。

40

#### 【0023】

また、本開示の一態様に係る不正通信検知基準決定システムは、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通信の検知に用いる基準メッセージの決定システムであって、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、前記車載ネットワークシステムに対する攻撃メッセージに関する情報から、前記攻撃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特徴を示す通信パターンを識別し、前記ネットワークに送出されたメッセージが、識別された前記通信パターンに適合するか否かを判定し、前記ネットワークに送出されるメッセージが攻撃メッセージであるか否かの判定の基準に用いる基準メ

50

ッセージを、前記通信パターンに適合するか否かの判定の結果を用いて決定する。

【 0 0 2 4 】

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の判定に基準として用いられる基準メッセージが適切に選択される。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。

【 0 0 2 5 】

また、本開示の一態様に係るプログラムは、上記の不正通信検知基準決定システムにおいて、前記 1 個以上のプロセッサに上記の不正通信検知基準決定方法のいずれかを実施させるためのプログラムである。

【 0 0 2 6 】

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の判定に基準として用いられる基準メッセージが適切に選択される。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。

【 0 0 2 7 】

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。

【 0 0 2 8 】

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。

【 0 0 2 9 】

( 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。

【 0 0 3 0 】

[ 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 1 0 の全体構成を示すブロック図である。

【 0 0 3 1 】

車載ネットワークシステム 1 0 は、CAN ネットワークで構成され、ECU 1 0 0 ( 図中の ECU 1 0 0 a、ECU 1 0 0 b、ECU 1 0 0 c、及び ECU 1 0 0 d 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 ECU 1 0 0 ともいう ) と、バス 2 0 0 ( 図中のバス 2 0 0 a 及びバス 2 0 0 b 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 2 0 0 ともいう ) と、ゲートウェイ 3 0 0 とを含む。

【 0 0 3 2 】

ECU 1 0 0 a はエンジン 1 0 1 に、ECU 1 0 0 b はブレーキ 1 0 2 に、ECU 1 0 0 c はドア開閉センサ 1 0 3 に、ECU 1 0 0 d はウィンドウ開閉センサ 1 0 4 にそれぞれ接続されている。ECU 1 0 0 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 2 0 0 に送出している。例えば ECU 1 0 0 a は、エンジン 1 0 1 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 2 0 0 に送出する。また、各 ECU 1 0 0 は、他の ECU 1 0 0 が送信したメッセージをバス 2 0 0 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。

【 0 0 3 3 】

ゲートウェイ 3 0 0 は、ECU 1 0 0 a 及び ECU 1 0 0 b が接続されているバス 2 0 0 a と、ECU 1 0 0 c 及び ECU 1 0 0 d が接続されているバス 2 0 0 b とを接続して

10

20

30

40

50

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。

#### 【0034】

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。

#### 【0035】

##### [ 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。

#### 【0036】

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 Transmission 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、Cyclic 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。

#### 【0037】

SOF は、1 bit 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 ECU 100 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 ECU 100 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。

#### 【0038】

ID とは、メッセージが含むデータの種別を示す 11 bit 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。

#### 【0039】

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 1 bit のドミナントである。

#### 【0040】

IDE と r は、それぞれ 1 bit のドミナントである。

#### 【0041】

DLC は、続くデータフィールドの長さを示す 4 bit の値である。

#### 【0042】

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 64 bit 長で、8 bit 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。

#### 【0043】

10

20

30

40

50



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。

【0044】

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。

【0045】

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。

【0046】

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。

【0047】

EOFは7bitのレセシブ固定で、メッセージの終了を示す。

【0048】

[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。

【0049】

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。

【0050】

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。

【0051】

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。

【0052】

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。

【0053】

10

20

30

40

50

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。

【0054】

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。

【0055】

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。

【0056】

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。

【0057】

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。

【0058】

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。

【0059】

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。

【0060】

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。

【0061】

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。

【0062】

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。

【0063】

[ 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

10

20

30

40

50

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。

【0064】

[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。

10

【0065】

[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。

【0066】

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。

20

【0067】

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。

【0068】

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、予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。

30

【0069】

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。

40

【0070】

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。

【0071】

50

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。

【0072】

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。

【0073】

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。

10

【0074】

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。

【0075】

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。

20

【0076】

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。

30

【0077】

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。

【0078】

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。

【0079】

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。

40

【0080】

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。

【0081】

50

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。

10

#### 【0082】

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。

#### 【0083】

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。

20

#### 【0084】

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。

#### 【0085】

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。

#### 【0086】

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。

30

#### 【0087】

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。

40

#### 【0088】

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 376 a を含む不正検知処理機能群 370 a 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 370 a 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。

50

## 【 0 0 8 9 】

図 8 において、通信パターン識別部 3 7 4 a 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 ( Auto Regressive ) モデル、ARMA ( Auto Regressive 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。

## 【 0 0 9 0 】

通信パターン予測部 3 7 6 a は、通信パターン識別部 3 7 4 a 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。

10

## 【 0 0 9 1 】

通信パターン判定部 3 7 5 a は、通信パターン予測部 3 7 6 a 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を判定する。

## 【 0 0 9 2 】

なお、ここまで通信パターン判定部 3 7 5 又は通信パターン判定部 3 7 5 a 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。

20

## 【 0 0 9 3 】

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。

## 【 0 0 9 4 】

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。

## 【 0 0 9 5 】

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。

30

## 【 0 0 9 6 】

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に入るか否かに基づいて判定されてもよい。

40

## 【 0 0 9 7 】

さらに、通信パターン予測部 3 7 6 a 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 3 7 6 a 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

50

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。

【 0 0 9 8 】

なお、メッセージ保存処理部 3 7 2 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 3 7 4 又は通信パターン識別部 3 7 4 a 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 3 7 2 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 3 7 1 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。

10

【 0 0 9 9 】

なお、受信したメッセージはゲートウェイ 3 0 0 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予め設定しておき、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。

【 0 1 0 0 】

[ 1 . 7 E C U の構成 ]

20

図 9 は、車載ネットワークシステム 1 0 に含まれる E C U 1 0 0 の機能構成を示すブロック図である。E C U 1 0 0 は、フレーム送受信部 1 1 0 と、フレーム解釈部 1 2 0 と、受信 I D 判定部 1 3 0 と、受信 I D リスト保持部 1 4 0 と、フレーム処理部 1 5 0 と、データ取得部 1 7 0 と、フレーム生成部 1 8 0 とを備える。

【 0 1 0 1 】

なお、これらの構成要素は機能構成要素であり、E C U 1 0 0 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。

30

【 0 1 0 2 】

フレーム送受信部 1 1 0 は、バス 2 0 0 に対して、C A N 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 1 1 0 は、バス 2 0 0 に送出されたメッセージを 1 b i t ずつ読み出し、読み出したメッセージをフレーム解釈部 1 2 0 に転送する。また、フレーム送受信部 1 1 0 は、フレーム生成部 1 8 0 より通知を受けたメッセージをバス 2 0 0 に送出する。

【 0 1 0 3 】

フレーム解釈部 1 2 0 は、フレーム送受信部 1 1 0 よりメッセージの値を受け取り、C A N 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 I D フィールドと判断した一連の値を、フレーム解釈部 1 2 0 は受信 I D 判定部 1 3 0 へ転送する。

40

【 0 1 0 4 】

フレーム解釈部 1 2 0 はさらに、受信 I D 判定部 1 3 0 から通知される判定結果に応じて、メッセージの I D フィールドの値及び I D 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 1 5 0 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。

【 0 1 0 5 】

またフレーム解釈部 1 2 0 は、C A N 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 1 8 0 へ要求する。

【 0 1 0 6 】

50

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。

【0107】

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。

【0108】

受信 ID リスト保持部 140 は、ECU 100 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。

10

【0109】

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 ECU 100 によって異なる。例えば、ECU 100 a では、時速が 30 km 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。ECU 100 c 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、ECU 100 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。

20

【0110】

データ取得部 170 は、各 ECU 100 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。

【0111】

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。

【0112】

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予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。

30

【0113】

[ 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。

【0114】

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）。

【0115】

メッセージを受け取った不正検知部 371 では、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）。

40

【0116】

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 3

50



70での不正検知処理は終了する(ステップS1003でNo)。

【0117】

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)。

【0118】

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に基づいて実行される。

10

【0119】

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ら、攻撃パターンを識別する(ステップS1006)。

【0120】

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。

20

【0121】

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。

【0122】

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。

30

【0123】

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、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。

40

【0124】

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。

【0125】

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

50

処理の高速化、及び省電力化の効果が期待できる。

【 0 1 2 6 】

[ 1 . 9 転送処理 ]

図 1 1 は、ゲートウェイ 3 0 0 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 3 0 0 がバス 2 0 0 a から受信したメッセージをバス 2 0 0 b へ転送する場合を例に説明する。

【 0 1 2 7 】

まず、フレーム送受信部 3 1 0 は、バス 2 0 0 a からメッセージを読み出す（ステップ S 1 1 0 1）。フレーム送受信部 3 1 0 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 3 2 0 へ転送する。

10

【 0 1 2 8 】

次に、フレーム解釈部 3 2 0 は、受信 ID 判定部 3 3 0 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 S 1 1 0 2）。処理する対象のメッセージではないとフレーム解釈部 3 2 0 が判定した場合（ステップ S 1 1 0 2 で N O）、当該メッセージの転送は行われない。

【 0 1 2 9 】

フレーム解釈部 3 2 0 は、ステップ S 1 1 0 2 で、受信して処理する対象のメッセージであると判断した場合には（ステップ S 1 1 0 2 で Y e s）、フレーム処理部 3 5 0 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 3 5 0 は、転送ルール保持部 3 6 0 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 S 1 1 0 3）。

20

【 0 1 3 0 】

フレーム処理部 3 5 0 は、フレーム解釈部 3 2 0 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 3 7 0 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。

【 0 1 3 1 】

不正検知処理機能群 3 7 0 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 S 1 1 0 4）、その判定の結果をフレーム処理部 3 5 0 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 3 7 0 が判定した場合（ステップ S 1 1 0 4 で Y E S）、当該メッセージの転送は行われない。

30

【 0 1 3 2 】

ステップ S 1 1 0 4 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 S 1 1 0 4 で N o）、フレーム処理部 3 5 0 は、そのメッセージをステップ S 1 1 0 3 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 3 8 0 へ要求する。フレーム生成部 3 8 0 は、フレーム処理部 3 5 0 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 3 1 0 に送出させる（ステップ S 1 1 0 5）。

40

【 0 1 3 3 】

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 S 1 1 0 3）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 S 1 1 0 4）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。

【 0 1 3 4 】

[ 1 . 1 0 効果 ]

本実施の形態では、不正検知処理機能群 3 7 0 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

50

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。

#### 【 0 1 3 5 】

( 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 3 7 0 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。

#### 【 0 1 3 6 】

#### [ 2 . 1 不正検知処理機能群の構成 ]

図 1 2 は、本実施の形態における不正検知処理機能群 3 7 0 b の機能構成を示すブロック図である。図 1 2 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 3 7 0 b について、不正検知処理機能群 3 7 0 との差異点を中心に説明する。

#### 【 0 1 3 7 】

不正検知処理機能群 3 7 0 b は、実施の形態 1 における不正検知処理機能群 3 7 0 の構成に加え、基準メッセージ決定部 3 7 7 b、及び基準メッセージ候補保持部 3 7 8 b を含む。また、不正検知処理機能群 3 7 0 b は、不正検知部 3 7 1 に代えて不正検知部 3 7 1 b を、通信パターン判定部 3 7 5 に代えて通信パターン判定部 3 7 5 b 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。

#### 【 0 1 3 8 】

基準メッセージ決定部 3 7 7 b は、不正検知部 3 7 1 b 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。

#### 【 0 1 3 9 】

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 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 3 7 7 b 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。

#### 【 0 1 4 0 】

不正検知部 3 7 1 b 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 3 7 7 b に基準メッセージの取得を要求する。

#### 【 0 1 4 1 】

基準メッセージ決定部 3 7 7 b は、基準メッセージ候補保持部 3 7 8 b 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 3 7 1 b へ通知する。

## 【 0 1 4 2 】

基準メッセージ決定部 3 7 7 b 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 3 7 5 b へ基準メッセージの候補を通知する。

## 【 0 1 4 3 】

通信パターン判定部 3 7 5 b 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。

## 【 0 1 4 4 】

基準メッセージ決定部 3 7 7 b は、通信パターン判定部 3 7 5 b 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、また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  
10  
セージ決定部 3 7 7 b 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  
セージ決定部 3 7 7 b 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。

## 【 0 1 4 5 】

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  
20  
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。

## 【 0 1 4 6 】

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。

## 【 0 1 4 7 】

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。  
30

## 【 0 1 4 8 】

基準メッセージ候補保持部 3 7 8 b は、基準メッセージ決定部 3 7 7 b に提示される基準メッセージ候補を保持する。

## 【 0 1 4 9 】

不正検知部 3 7 1 b 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 3 7 8 b へ通知する。基準メッセージ候補保持部 3 7 8 b は、不正検知部 3 7 1 b 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 3 7 7 b 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 3 7 7 b に通知する。  
40

## 【 0 1 5 0 】

なお、上記では不正検知部 3 7 1 b 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 3 7 7 b 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  
50

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。

【0151】

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。

10

【0152】

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。そのため、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。

【0153】

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。

20

【0154】

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。

30

【0155】

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。

40

【0156】

また、図 8 に示される実施の形態 1 における構成と同様に、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 に代えて含まれる。

50

## 【 0 1 5 7 】

通信パターン判定部 3 7 5 c は、通信パターン判定部 3 7 5 b と同じ機能を備え、更に、通信パターン予測部 3 7 6 c 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。

## 【 0 1 5 8 】

通信パターン予測部 3 7 6 c は、通信パターン予測部 3 7 6 a と同じ機能を備え、通信パターン判定部 3 7 5 c からの要求に応じて予測値を通知する機能を備える。

## 【 0 1 5 9 】

この予測値は、通信パターン予測部 3 7 6 c が、通信パターン識別部 3 7 4 c 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。

10

## 【 0 1 6 0 】

通信パターン識別部 3 7 4 c は、通信パターン識別部 3 7 4 a と同じ機能を備える。

## 【 0 1 6 1 】

不正検知処理機能群 3 7 0 c 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。

## 【 0 1 6 2 】

## [ 2 . 2 不正検知処理 ]

図 1 4 は、不正検知処理機能群 3 7 0 b での不正検知処理の一例を示すフロー図である。図 1 0 と共通のステップについては、図 1 4 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。

20

## 【 0 1 6 3 】

まず、不正検知部 3 7 1 b は、フレーム処理部 3 5 0 からメッセージを受け取る（ステップ S 1 0 0 1 ）。

## 【 0 1 6 4 】

メッセージを受け取った不正検知部 3 7 1 b 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 S 1 4 0 2 ）。

## 【 0 1 6 5 】

ステップ S 1 4 0 2 において、不正検知部 3 7 1 b 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 S 1 4 0 3 ）。

30

## 【 0 1 6 6 】

ステップ S 1 4 0 3 で新しい基準メッセージを決定した後、またはステップ S 1 4 0 2 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 S 1 4 0 4 ）。

## 【 0 1 6 7 】

不正検知部 3 7 1 b 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 3 7 1 b の各種の判定機能は、必要に応じて、ステップ S 1 4 0 3 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 3 7 1 は、その判定の結果をメッセージ保存処理部 3 7 2 へ通知する。

40

## 【 0 1 6 8 】

ステップ S 1 4 0 4 のその他の処理は、図 1 0 のステップ S 1 0 0 2 の不正検知処理と同様である。

## 【 0 1 6 9 】

ステップ S 1 0 0 3 以降の処理は、図 1 0 と共通であるため、説明を省略する。

## 【 0 1 7 0 】

## [ 2 . 3 効果 ]

本実施の形態では、不正検知処理機能群 3 7 0 b での不正検知処理において、不正検知部 3 7 1 b 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

50

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。

#### 【 0 1 7 1 】

( 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。

10

#### 【 0 1 7 2 】

#### [ 3 . 1 車載ネットワークシステムの全体構成 ]

図 1 5 は、本実施の形態における車載ネットワークシステム 1 0 a の全体構成を示すブロック図である。図 1 5 において、図 1 に示される車載ネットワークシステム 1 0 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。

#### 【 0 1 7 3 】

車載ネットワークシステム 1 0 a は、CAN ネットワークで構成され、ECU 1 0 0 ( 図中の ECU 1 0 0 a、ECU 1 0 0 b、ECU 1 0 0 c、及び ECU 1 0 0 d 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 ECU 1 0 0 ともいう ) と、バス 2 0 0 ( 図中のバス 2 0 0 a 及びバス 2 0 0 b 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 2 0 0 ともいう ) と、ゲートウェイ 3 0 0 d と、外部ネットワーク 4 0 0 と、サーバ 5 0 0 とを含む。

20

#### 【 0 1 7 4 】

ゲートウェイ 3 0 0 d は、ECU 1 0 0 a 及び ECU 1 0 0 b が接続されているバス 2 0 0 a と、ECU 1 0 0 c 及び ECU 1 0 0 d が接続されているバス 2 0 0 b とを接続している。ゲートウェイ 3 0 0 d 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 3 0 0 d もまた、CAN ネットワーク上ではひとつのノードである。

#### 【 0 1 7 5 】

外部ネットワーク 4 0 0 は、ゲートウェイ 3 0 0 とサーバ 5 0 0 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 4 0 0 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、3 G、又は LTE であってもよい。

30

#### 【 0 1 7 6 】

サーバ 5 0 0 は、外部ネットワーク 4 0 0 を介してゲートウェイ 3 0 0 d と通信を行う。

#### 【 0 1 7 7 】

ゲートウェイ 3 0 0 d とサーバ 5 0 0 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 3 7 0 の一部の機能を分担して備え、ゲートウェイ 3 0 0 d とサーバ 5 0 0 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。

40

#### 【 0 1 7 8 】

#### [ 3 . 2 ゲートウェイの構成 ]

図 1 6 は、ゲートウェイ 3 0 0 d の機能構成の一例を示すブロック図である。図 1 6 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 3 0 0 d について、ゲートウェイ 3 0 0 との差異点を中心に説明する。

#### 【 0 1 7 9 】

ゲートウェイ 3 0 0 d は、ゲートウェイ 3 0 0 の構成における不正検知処理機能群 3 7 0 に代えて不正検知処理機能群 3 7 0 d を備え、また、さらに外部通信部 3 9 0 とを備える点異なる。これらの構成要素も機能構成要素であり、ゲートウェイ 3 0 0 d において

50

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。

#### 【0180】

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。

#### 【0181】

外部通信部390は、サーバ500との通信を行う。

#### 【0182】

[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。

#### 【0183】

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。

#### 【0184】

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。

#### 【0185】

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。

#### 【0186】

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。

#### 【0187】

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。

#### 【0188】

[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。

#### 【0189】



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。

【0190】

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。

【0191】

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。

【0192】

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。

【0193】

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。

【0194】

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。

【0195】

[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。

【0196】

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。

【0197】

## 〔 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る構築される形態も、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。

## 【 0 1 9 8 】

( 1 ) 上記の実施の形態では、不正検知処理機能群 3 7 0 c は、不正検知部 3 7 1 と、メッセージ保存処理部 3 7 2 と、攻撃メッセージ情報保持部 3 7 3 と、通信パターン識別部 3 7 4 c と、通信パターン判定部 3 7 5 c と、通信パターン予測部 3 7 6 c と、基準メッセージ決定部 3 7 7 b と、基準メッセージ候補保持部 3 7 8 b とを備えると説明したが、これに限定されない。

10

## 【 0 1 9 9 】

図 2 0 に示すように、不正検知部 3 7 1 と、メッセージ保存処理部 3 7 2 f と、攻撃メッセージ情報保持部 3 7 3 f と、通信パターン識別部 3 7 4 f と、通信パターン判定部 3 7 5 f と、通信パターン予測部 3 7 6 c と、基準メッセージ決定部 3 7 7 b と、基準メッセージ候補保持部 3 7 8 b と、車両状態認識部 3 7 9 f 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 ( 3 7 0 、 3 7 0 a 、 3 7 0 b 、 3 7 0 d 、 3 7 0 e ) が、さらに車両状態認識部 3 7 9 f を備えてもよい ( 図示なし ) 。

## 【 0 2 0 0 】

ここで、車両状態認識部 3 7 9 f は、車両がどのような状態であるかを C A N 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 3 7 9 f 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 O F F ) 」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。

20

## 【 0 2 0 1 】

例えばメッセージ保存処理部 3 7 2 f 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 3 7 9 f 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 3 7 2 f 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。

30

## 【 0 2 0 2 】

また、通信パターン識別部 3 7 4 f 及び通信パターン判定部 3 7 5 f は、車両状態認識部 3 7 9 f 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。

## 【 0 2 0 3 】

より具体的な例を挙げると、通信パターン識別部 3 7 4 f 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 3 7 5 f は、「運転支援モード」又は「自動運転モード」の時に、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 3 7 4 f 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 3 7 5 f は、「走行中」の時に通信パターンを判定する。

40

## 【 0 2 0 4 】

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、E C U 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 E C U からの制御信号も不要である。したがって、自

50

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。

【0205】

(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。

【0206】

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。

【0207】

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。

【0208】

(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。

【0209】

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。

【0210】

(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。

【0211】

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。

【0212】

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

10

20

30

40

50

であるかどうかの判定を依頼してもよい。

【0213】

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。

【0214】

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。

10

【0215】

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。

【0216】

20

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。

【0217】

(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。

30

【0218】

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。

【0219】

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。

【0220】

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。

40

【0221】

(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。

【0222】

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

50

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。

【0223】

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。

【0224】

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。

【0225】

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予め計算しておき、どの系列が予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。

【0226】

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。

【0227】

(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。

【0228】

(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。

【0229】

(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。

【0230】

(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。

【0231】

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 Interconne

10

20

30

40

50

ct 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。

【0232】

(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。

10

【0233】

(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。

【0234】

20

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。

【0235】

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りコンフィギュラブル・プロセッサを利用してもよい。

【0236】

30

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。

【0237】

(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。

40

【0238】

(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。

【0239】

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

50

れているデジタル信号であるとしてもよい。

【0240】

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。

【0241】

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。

【0242】

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。

【0243】

(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。

【0244】

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基準として用いられるメッセージの決定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の基準として用いられるメッセージが決定される。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基準決定システムと呼ぶ。したがって、不正通信検知基準決定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。

【0245】

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、又は不正通信検知基準決定システムのプロセッサに実行されて、不正通信検知基準決定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。

【0246】

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】

【0247】

本発明にかかる不正通信検知基準決定方法等は、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ための基準メッセージを決定する。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】

【0248】

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

10

20

30

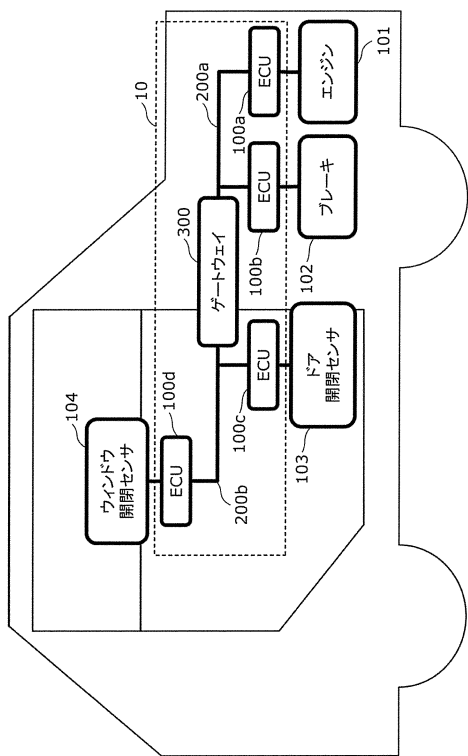
40

50

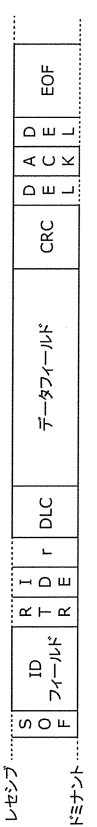
|  |               |    |
|--|---------------|----|
| 1 0 3  | ドア開閉センサ       |    |
| 1 0 4  | ウィンドウ開閉センサ    |    |
| 1 1 0  | フレーム送受信部      |    |
| 1 2 0  | フレーム解釈部       |    |
| 1 3 0  | 受信 I D 判定部    |    |
| 1 4 0  | 受信 I D リスト保持部 |    |
| 1 5 0  | フレーム処理部       |    |
| 1 7 0  | データ取得部        |    |
| 1 7 1  | 送信データ取得部      |    |
| 1 8 0  | フレーム生成部       | 10 |
| 2 0 0、2 0 0 a、2 0 0 b  | バス            |    |
| 3 0 0、3 0 0 d  | ゲートウェイ        |    |
| 3 1 0  | フレーム送受信部      |    |
| 3 2 0  | フレーム解釈部       |    |
| 3 3 0  | 受信 I D 判定部    |    |
| 3 4 0  | 受信 I D リスト保持部 |    |
| 3 5 0  | フレーム処理部       |    |
| 3 6 0  | 転送ルール保持部      |    |
| 3 7 0、3 7 0 a、3 7 0 b、3 7 0 c、3 7 0 d、3 7 0 e、3 7 0 f、3 7 0 g、 |               |    |
| 3 7 0 h、3 7 0 i、3 7 0 j  | 不正検知処理機能群     | 20 |
| 3 7 1、3 7 1 b、3 7 1 g、3 7 1 h、3 7 1 i                          | 不正検知部         |    |
| 3 7 2、3 7 2 d、3 7 2 f  | メッセージ保存処理部    |    |
| 3 7 3、3 7 3 d、3 7 3 f  | 攻撃メッセージ情報保持部  |    |
| 3 7 4、3 7 4 a、3 7 4 c、3 7 4 d、3 7 4 f                          | 通信パターン識別部     |    |
| 3 7 5、3 7 5 a、3 7 5 b、3 7 5 c、3 7 5 d、3 7 5 e、3 7 5 f、3 7 5 g、 |               |    |
| 3 7 5 h  | 通信パターン判定部     |    |
| 3 7 6 a、3 7 6 c、3 7 6 e  | 通信パターン予測部     |    |
| 3 7 7 b  | 基準メッセージ決定部    |    |
| 3 7 8 b  | 基準メッセージ候補保持部  |    |
| 3 7 9 f  | 車両状態認識部       | 30 |
| 3 8 0  | フレーム生成部       |    |
| 3 9 0  | 外部通信部         |    |
| 4 0 0  | 外部ネットワーク      |    |
| 5 0 0  | サーバ           |    |



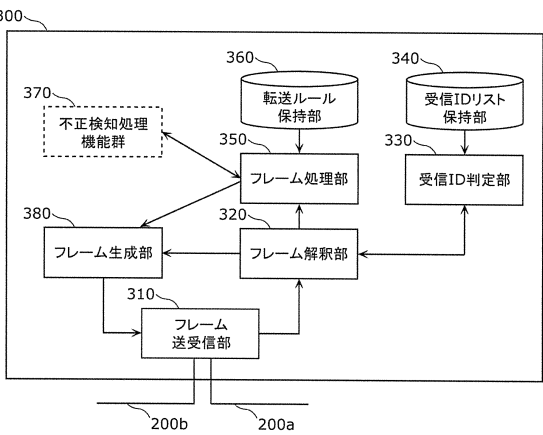
【図 1】



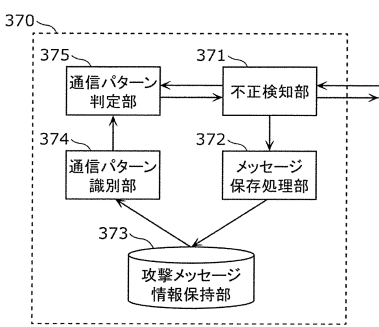
【図 2】



【図 3】



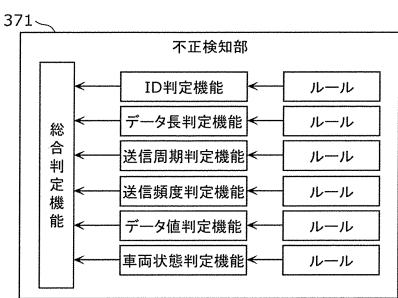
【図 6】



【図 4】

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

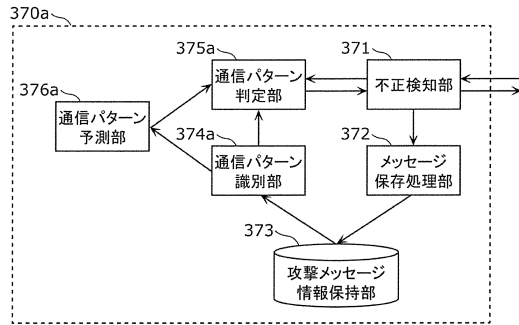
【図 7】



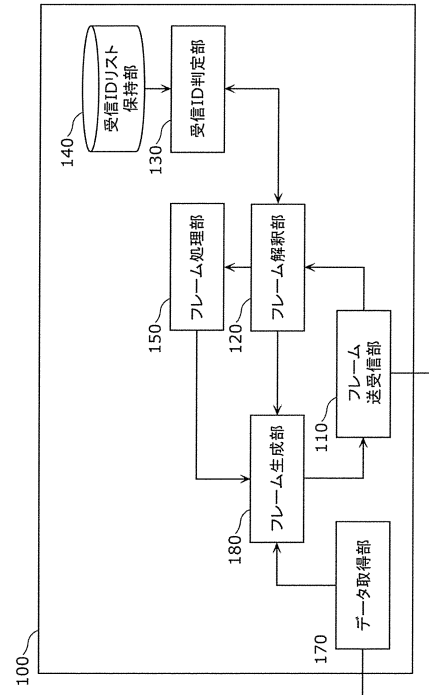
【図 5】

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

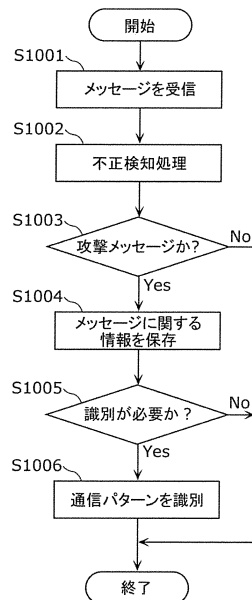
【図 8】



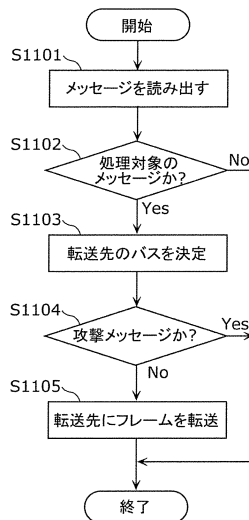
【図 9】



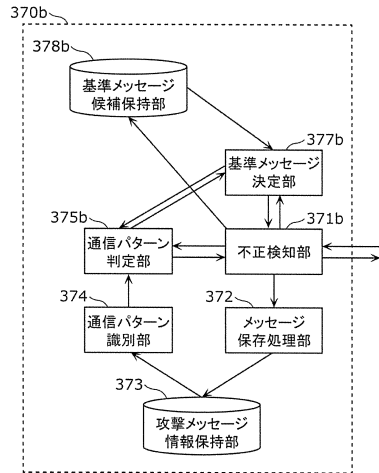
【図 10】



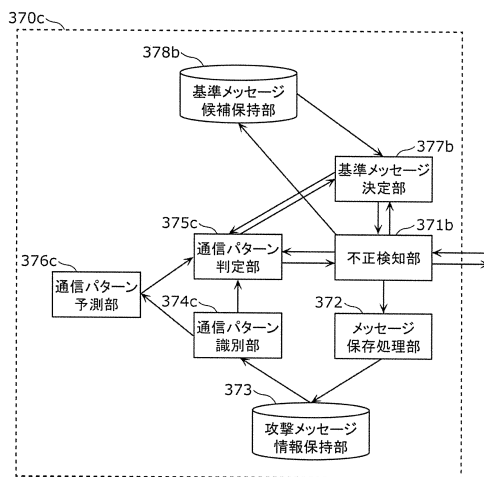
【図 11】



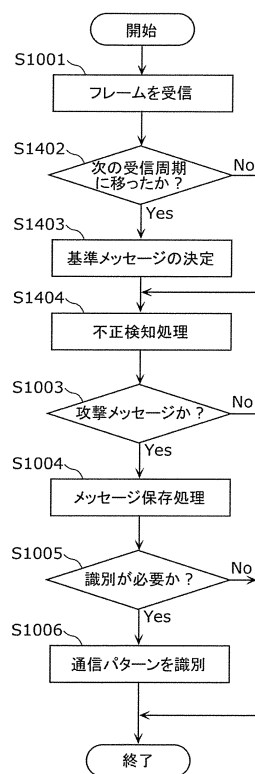
【図 12】



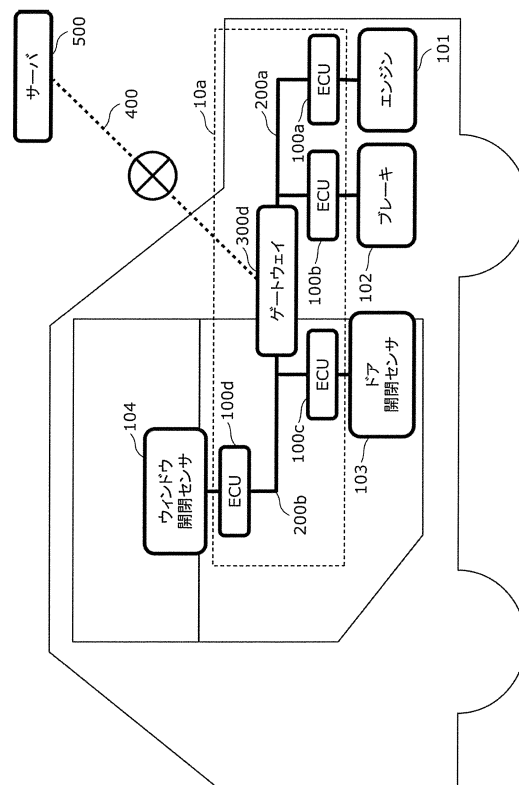
【図 13】



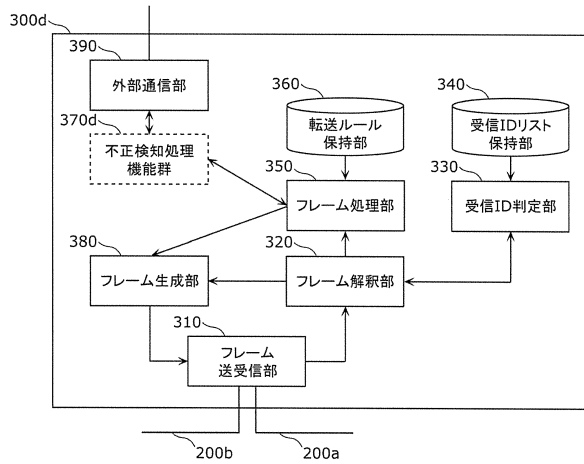
【図 14】



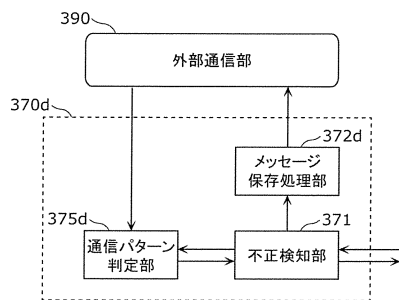
【図 15】



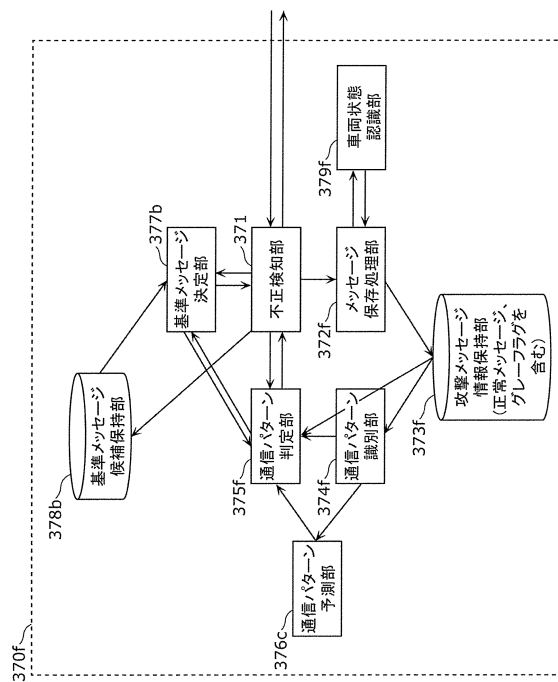
【図 16】



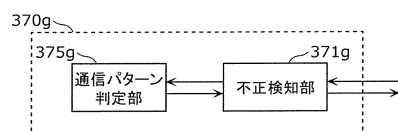
【図 17】



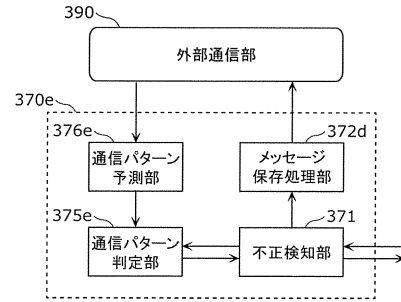
【図 20】



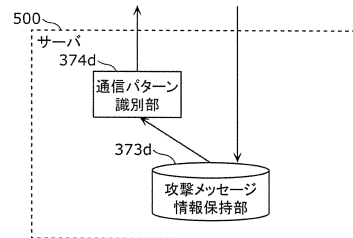
【図 21】



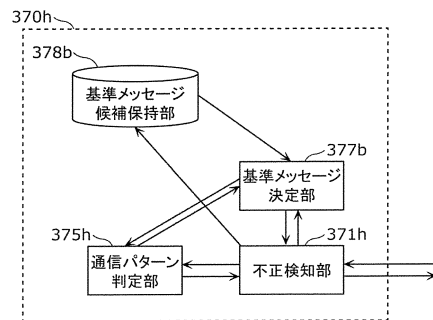
【図 18】



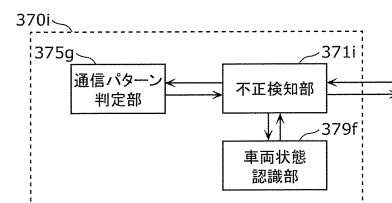
【図 19】



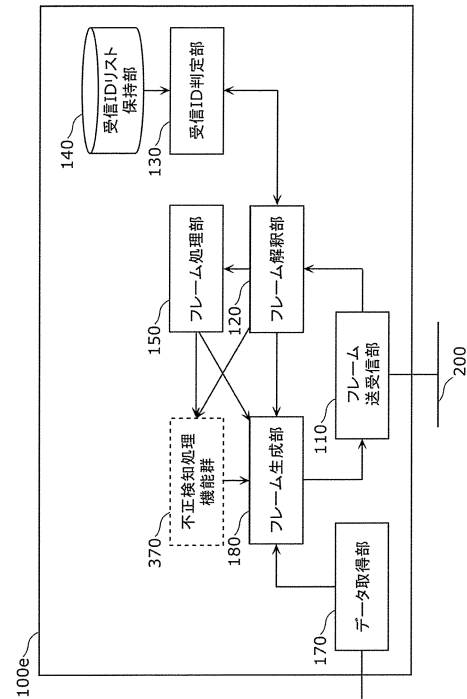
【図 22】



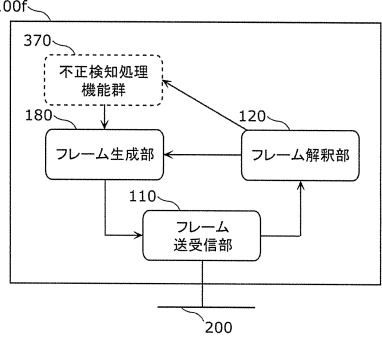
【図 23】



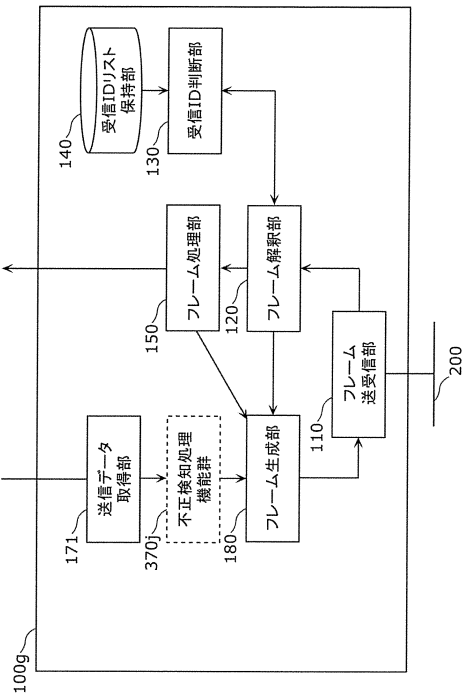
【図 2 4】



【図 2 5】



【図 2 6】



---

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 1 0 0 6 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 1 0 0 6 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 1 0 0 6 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 2 0 1 4 - 1 4 6 8 6 8 ( J P , A )

国際公開第 2 0 0 4 / 0 5 4 1 9 7 ( W O , A 1 )

(58)調査した分野(Int.Cl. , D B 名)

H 0 4 L 1 2 / 2 8

H 0 4 L 1 2 / 7 0