(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 12 月 3 日(03.12.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/182103 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *H04L 12/28* (2006.01)
B60R 16/023 (2006.01)

(21) 国際出願番号: PCT/JP2015/002614

(22) 国際出願日: 2015 年 5 月 25 日(25.05.2015)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2014-110908 2014 年 5 月 29 日(29.05.2014) JP
特願 2014-251551 2014 年 12 月 12 日(12.12.2014) JP

(71) 出願人: パナソニックＩＰマネジメント株式会社 **(PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.)** [JP/JP]; 〒5406207 大阪府大阪市中央区城見２丁目１番６１号 Osaka (JP).

(72) 発明者: 田邉　正人 **(TANABE, Masato)**. 安齋　潤 **(ANZAI, Jun)**. 北村　嘉彦 **(KITAMURA, Yoshihiko)**.

(74) 代理人: 藤井　兼太郎，外 **(FUJII, Kentaro** et al.); 〒5406207 大阪府大阪市中央区城見２丁目１番６１号パナソニックＩＰマネジメント株式会社内 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

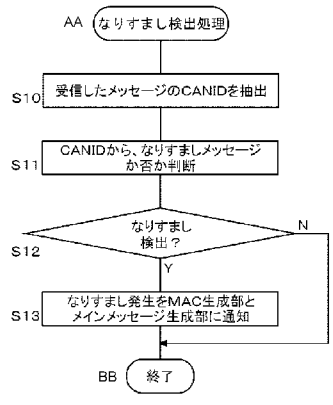
添付公開書類:
— 国際調査報告（条約第 21 条(3)）

WO 2015/182103 A1

(54) **Title**: TRANSMISSION DEVICE, RECEPTION DEVICE, TRANSMISSION METHOD, AND RECEPTION METHOD

(54) 発明の名称 : 送信装置、受信装置、送信方法および受信方法

[図5]



S10 Extract CANID of received message
S11 Determine from CANID whether message is spoofed
S12 Spoof detection?
S13 Notify MAC generation unit and main message generation unit of spoof occurrence
AA Spoof detection process
BB End

(57) **Abstract**: This transmission device has a detection unit, a generation unit, and a transmission unit. When the detection unit has detected a match between the communication rules for a message that has been broadcast transmitted to a network by another transmission device and the communication rules of a message that the present transmission device broadcast transmits to the network, the generation unit generates an abnormality notification message. Then, the transmission unit broadcast transmits the abnormality notification message to the network.

(57) 要約: 送信装置は、検出部と、生成部と、送信部と、を有する。検出部が、他の送信装置によりネットワークへブロードキャスト送信されたメッセージの通信規則と本送信装置がネットワークへブロードキャスト送信するメッセージの通信規則との一致を検出した場合、生成部は、異常通知メッセージを生成する。そして、送信部は、この異常通知メッセージをネットワークへブロードキャスト送信する。

明　細　書

発明の名称 ： 送信装置、受信装置、送信方法および受信方法

技術分野

[0001] 本発明は、バスで接続された通信システムにおける送信装置、受信装置、送信方法および受信方法に関する。

背景技術

[0002] 車載ネットワークとしてＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が普及している。ＣＡＮはバス型ネットワークを採用したシリアル通信プロトコルである。バスに接続される各ノードからのメッセージは、バスに接続される全てのノードにブロードキャストされる。当該メッセージには送信元ノード及び宛先ノードの識別情報が含まれない。したがって受信ノードにおいて、正しい通信相手から来たメッセージであるか否かを単純に判断することはできない。

[0003] メッセージの完全性を保証したり、ＣＡＮに接続された不正機器からのリプレイ攻撃を防御したりするため、メッセージ認証コード（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ；ＭＡＣ）を用いる方法が提案されている。例えば通常のメッセージを生成および送信する度にそのメッセージに対するＭＡＣを生成し、ＭＡＣを含むメッセージを送信する方法が提案されている（例えば特許文献１参照）。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１３－９８７１９号公報

発明の概要

[0005] 本発明は、ブロードキャスト送信される通信システムにおけるセキュリティを、負荷の増大を抑制しつつ向上させる技術を提供する。

[0006] 本発明の一態様に係る送信装置は、検出部と、生成部と、送信部と、を有する。検出部は、他の送信装置によりネットワークへブロードキャスト送信

されたメッセージの通信規則が、本送信装置が保持するメッセージの通信規則と一致するか否かを検出する。生成部は、異常を検出したことを通知するための異常通知メッセージを生成する。送信部は、生成部が生成したメッセージをネットワークへブロードキャスト送信する。検出部が、他の送信装置によりネットワークへブロードキャスト送信されたメッセージの通信規則と本送信装置がネットワークへブロードキャスト送信するメッセージの通信規則との一致を検出した場合、生成部は、異常通知メッセージを生成し、送信部が、この異常通知メッセージをネットワークへブロードキャスト送信する。

[0007] なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、コンピュータプログラム、又はコンピュータプログラムを記録した記録媒体などの間で変換したものもまた、本発明の態様として有効である。

[0008] 本発明によれば、ブロードキャスト送信される通信システムにおけるセキュリティを、負荷の増大を抑制しつつ向上させることができる。

図面の簡単な説明

[0009] [図1]ＣＡＮで使用される標準フォーマットのデータフレームの一例を示す図

[図2]本発明の実施の形態に係るＣＡＮシステムの構成の一例を示す図

[図3]本発明の実施の形態に係るＥＣＵの構成例を示す図

[図4]異常検出後に制御を続ける方式にてＭＡＣを別メッセージで送信する場合における、メッセージ処理部のなりすまし検出およびメッセージ送信に必要な機能を示すブロック図

[図5]図４のメッセージ処理部による、なりすまし検出処理を示すフローチャート

[図6]図４のメッセージ処理部によってなりすましが検出された後のメッセージ送信処理を示すフローチャート

[図7]異常検出後に制御を続ける方式にてメインメッセージを先に受信しＭＡＣメッセージを後に受信する場合における、メッセージ処理部のメッセージ

受信に必要な機能を示すブロック図

[図8]図７のメッセージ処理部によるメインメッセージ受信処理を示すフローチャート

[図9]図７のメッセージ処理部によるＭＡＣメッセージ受信処理を示すフローチャート

[図10]異常検出後に制御を続ける方式にてＭＡＣメッセージを先に受信しメインメッセージを後に受信する場合における、メッセージ処理部のメッセージ受信に必要な機能を示すブロック図

[図11]図１０のメッセージ処理部によるＭＡＣメッセージ受信処理を示すフローチャート

[図12]図１０のメッセージ処理部によるメインメッセージ受信処理を示すフローチャート

[図13]異常検出後に制御を続ける方式にてＭＡＣをメインメッセージに含めて送信する場合における、メッセージ処理部のなりすまし検出およびメッセージ送信に必要な機能を示すブロック図

[図14]図１３のメッセージ処理部による、なりすまし検出後のＭＡＣ付きメインメッセージ送信処理を示すフローチャート

[図15]異常検出後に制御を続ける方式にてＭＡＣ付きメインメッセージを受信する場合における、メッセージ処理部のメッセージ受信に必要な機能を示すブロック図

[図16]図１５のメッセージ処理部によるＭＡＣ付きメインメッセージ受信処理を示すフローチャート

[図17]異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部のなりすまし検出および不正通知メッセージ送信に必要な機能を示すブロック図

[図18]不正通知メッセージのフォーマット例を示す図

[図19]図１７のメッセージ処理部によるなりすまし検出処理および不正通知メッセージ送信処理を示すフローチャート

[図20]異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部の不正通知メッセージ受信に必要な機能を示すブロック図

[図21]異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部による不正通知メッセージ受信処理を示すフローチャート

[図22]異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部によるメインメッセージ受信処理を示すフローチャート

[図23]２つのＣＡＮシステムがゲートウェイ装置を介して接続された統合システムの構成例を示す図

[図24]図２３のゲートウェイ装置が保持するホワイトリストの一例を示す図

[図25]統合システム内の異なるＣＡＮシステム間におけるなりすましを検出する第１の構成例を説明するためのタイミングチャート

[図26]統合システム内でなりすましを検出するための第２の構成例を採用する場合におけるホワイトリストの一例を示す図

[図27]統合システム内の異なるＣＡＮシステム間におけるなりすましを検出する第２の構成例を説明するためのタイミングチャート

[図28]統合システム内の異なるＣＡＮシステム間におけるなりすましを検出する第３の構成例を説明するためのタイミングチャート

発明を実施するための形態

[0010] 本発明の実施の形態の説明に先立ち、従来の送信装置における課題を簡単に説明する。従来の送信装置では、通常のメッセージを生成および送信する度にＭＡＣを生成する。この場合、ノードの負荷が大きくなり消費電力も増大する。またメッセージの数が増えるためバスの占有率も増大する。

[0011] 本発明の実施の形態は、車両内に搭載される複数のＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）がノードとして接続された車載ネットワークであって、メッセージＩＤとデータと認証コードとしてのＭＡＣとが含まれるメッセージがブロードキャストされるものに関する。以下このようなネットワークとしてのＣＡＮシステムを例示して本発明の実施の形態を説明する。上述のようにＣＡＮはバス型ネットワークを採用しており、バス

に接続される各ＥＣＵからのメッセージはバスに接続される全てのＥＣＵにブロードキャストされる。近年、車両の電装化が進み一台の車両に搭載されるＥＣＵの数やＥＣＵが扱うデータ量が増えており、ＣＡＮバスのトラフィック量が増えている。またＥＣＵの増加および高度化に伴いバッテリの消費電力が増えている。

[0012] 図１は、ＣＡＮで使用される標準フォーマットのデータフレームの一例を示す図である。このデータフォーマットは次の規格文書に記載されている。ＩＳＯ １１８９８－１：２００３ Ｒｏａｄ ｖｅｈｉｃｌｅｓ －－ Ｃｏｎｔｒｏｌｌｅｒ ａｒｅａ ｎｅｔｗｏｒｋ（ＣＡＮ）－－Ｐａｒｔ １： Ｄａｔａ ｌｉｎｋ ｌａｙｅｒ ａｎｄ ｐｈｙｓｉｃａｌ ｓｉｇｎａｌｌｉｎｇ

[0013] 図１のデータフレームはＳＯＦ、ＩＤフィールド、ＲＴＲ、ＩＤＥ、ｒ０、ＤＬＣ、データフィールド、ＣＲＣデリミタ、Ａｃｋ、Ａｃｋデリミタ及びＥＯＦを含む。各ボックス内の数字はビット数を示す。またボックスの上が開放されている項目は常に「０」をとる項目であり、ボックスの下が開放されている項目は常に「１」をとる項目である。上下が開放されていない項目は「０」と「１」の両方をとりうる項目である。

[0014] 本実施の形態では主にＩＤフィールドＦ１とデータフィールドＦ２に注目する。ＩＤフィールドＦ１に格納されるＩＤ（以下適宜、ＣＡＮＩＤともいう）は、メッセージの種類および優先度を表す識別情報である。本明細書では送信可能な状態のデータフレームをメッセージと呼ぶ。ＣＡＮにおけるメッセージは車両内の特定の処理対象の特定の通知事項に関するメッセージである。当該処理対象には特定の監視対象および特定の制御対象が含まれる。例えば車両内の特定の処理対象に関するメッセージとして、速度情報を含むメッセージ、又はドアの開閉を指示するメッセージ等がある。また同じ処理対象に対して複数の通知事項が設定されることがある。例えば１つのメーターに対してエンジン回転数を通知するための通知事項、及びエンジン水温を通知するための通知事項など複数の通知事項が設定可能である。

[0015] ＣＡＮＩＤは、送信されるメッセージに含まれる特定の処理対象の特定の通知事項に関連づけられている。メッセージを受信したＥＣＵでは、そのＣＡＮＩＤに基づいてメッセージに含まれる特定の通知事項の内容を判断する。データフィールドＦ２には最大６４ビットのデータを格納できる。

[0016] 図１に示すようにＣＡＮのデータフレームには送信先ＩＤおよび受信先ＩＤが含まれない。したがって受信側のＥＣＵは、正しい通信相手から来たメッセージであるか否か判断できない。例えばエンジン回転数を含むメッセージはエンジンＥＣＵから送信される。当該メッセージに付与されるＣＡＮＩＤと同じＣＡＮＩＤが付与されたメッセージが、不正なＥＣＵから送信されると、受信側のＥＣＵは正当なエンジンＥＣＵからのメッセージであるか不正なＥＣＵからのメッセージであるか判別できない。すなわち、不正なＥＣＵが送信ＥＣＵになりすまして不正な情報を含むメッセージを送信したとしても、受信側のＥＣＵでは、正当なメッセージとして処理してしまい、その後の処理（補機の制御など）に悪影響が及んでしまう。例えば、不正なＥＣＵがエンジンＥＣＵになりすましてエンジン回転数を含むメッセージを送信することにより、それを受信したメーターＥＣＵの制御に悪影響が及ぶといったことが挙げられる。

[0017] このようにＣＡＮプロトコルでは、なりすましが容易である。またメッセージがＣＡＮバスに対してブロードキャスト送信されるため、ユニキャスト送信よりも盗聴が容易である。

[0018] これらの脅威に対して本実施の形態ではＭＡＣを用いることでＣＡＮメッセージを認証する。ＭＡＣは認証対象のデータと共通鍵とに所定のＭＡＣアルゴリズムを適用して生成される。共通鍵はＣＡＮに接続されたＥＣＵ間で事前に共有される秘密の鍵である。ＭＡＣ生成アルゴリズムにはハッシュ関数を使う方式（ＨＭＡＣ）やブロック暗号アルゴリズムを使う方式（ＯＭＡＣ／ＣＭＡＣ、ＣＢＣ－ＭＡＣ、ＰＭＡＣ）などがある。受信側のＥＣＵではメッセージに含まれる認証対象のデータと自己が保持する共通鍵に、送信側のＥＣＵで使用されたＭＡＣアルゴリズムを適用してＭＡＣを算出する。

この算出したＭＡＣと受信したＭＡＣが一致していれば認証が成功したと判定し、不一致であれば認証が失敗したと判定する。

[0019] したがって共通鍵が漏洩しなければ不正なＥＣＵや悪意がある発信元などからのメッセージは認証されないことになる。正当なメッセージとＭＡＣを受信した不正なＥＣＵなどからの再送攻撃に対しては認証対象のデータにカウンタ値などを含めることにより対処できる。本実施の形態では送信側のＥＣＵで生成されるＭＡＣのデータ長を６４ビット以下とする。６４ビットを超えるＭＡＣが算出される場合、その任意の６４ビット又はそれ以下のビットを抽出して使用する。

[0020] 以下本明細書ではデータフィールドに、特定の処理対象の特定の通知事項に関する情報（以下適宜、通常データという）を含みＭＡＣを含まないメッセージをメインメッセージという。メインメッセージは通常の処理を行うために送信されるメッセージである。通常データは、特定の処理対象の特定の機能に関する制御値などが該当する。データフィールドに通常データを含まずＭＡＣを含むメッセージをＭＡＣメッセージという。データフィールドに通常データとＭＡＣの両方を含むメッセージをＭＡＣ付きメインメッセージという。メインメッセージ、ＭＡＣメッセージ及びＭＡＣ付きメインメッセージは通常のメッセージである。通常のメッセージ以外に、あるＣＡＮＩＤを含むメッセージが不正なメッセージであることを通知するためのメッセージがある。以下このメッセージを不正通知メッセージという。また、ＭＡＣメッセージとＭＡＣ付きメインメッセージと不正通知メッセージとのうち、少なくともいずれか１つを含むメッセージを異常通知メッセージという。異常通知メッセージとは、上述のような「なりすまし」などによる異常を検出した際に、異常を検出したことを他のＥＣＵへ通知するためのメッセージである。詳細後述する通り、以下の実施の形態において、ＭＡＣを受信した時点で受信側のＥＣＵが異常（なりすましによる不正）の発生を判断できるため、ＭＡＣメッセージおよびＭＡＣ付きメインメッセージも実質的に異常通知メッセージに含まれる。

[0021] ＣＡＮの性質上、基本的にあるＩＤのメッセージを送信するＥＣＵは一意に定められる。このＣＡＮのブロードキャストの性質を利用することにより、自らが送信すべきＩＤのメッセージが他のＥＣＵに送信されていないか監視することで、不正なメッセージ送信を検出できる。以下この検出方法を利用して恒常的にＭＡＣを送信することなく、セキュリティを確保する方法を検討する。

[0022] 図２は、本発明の実施の形態に係るＣＡＮシステム５００の構成の一例を示す図である。当該ＣＡＮシステム５００では、ＣＡＮバス２００に複数のＥＣＵ１００（図２ではＥＣＵ１（１００ａ）、ＥＣＵ２（１００ｂ）、ＥＣＵ３（１００ｃ）及びＥＣＵ４（１００ｄ））が接続されている。ＣＡＮではＣＳＭＡ／ＣＡ（Ｃａｒｒｉｅｒ Ｓｅｎｓｅ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ ｗｉｔｈ Ｃｏｌｌｉｓｉｏｎ Ａｖｏｉｄａｎｃｅ）と呼ばれるアクセス制御方式が採用されており、ＣＡＮバス２００に対して最初に送信を開始したＥＣＵ１００が送信権を取得する。なお同時に複数のＥＣＵ１００が送信した場合は通信調停（ｂｕｓ ａｒｂｉｔｒａｔｉｏｎ）が行われる。ＣＡＮではＣＡＮＩＤの値が小さいほうが優先される。

[0023] 図３は、本発明の実施の形態に係るＥＣＵ１００の構成例を示す図である。ＥＣＵ１００は、アプリケーション処理部１０、メッセージ処理部３０及び送受信部５０を有する。これらの構成はハードウエア的には任意のプロセッサ、メモリ及びその他のＬＳＩで実現でき、ソフトウエア的にはメモリにロードされたプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがってこれらの機能ブロックがハードウエアのみ、ソフトウエアのみ又はそれらの組合せによっていろいろな形で実現できることは当業者には理解されるところである。

[0024] アプリケーション処理部１０は例えば、プロセッサ、メモリ及びメモリにロードされたアプリケーションプログラムによって実現される。メッセージ処理部３０は例えば、プロセッサ、メモリ、メモリにロードされたメッセージ処理プログラム及びＣＡＮコントローラによって実現される。なおＣＡＮ

コントローラに全ての機能を実装する構成も可能である。送受信部５０は例えば、トランシーバにより実現される。

[0025] アプリケーション処理部１０は各ＥＣＵ１００の処理対象（例えばエンジン、ステアリング、ブレーキ又はその他の各種補機）と接続し、それらの処理対象からステータス情報または指示情報を取得する。アプリケーション処理部１０は当該処理対象から取得した情報をもとに、ＣＡＮにおいてブロードキャスト送信すべきデータを生成し、メッセージ処理部３０に渡す。またアプリケーション処理部１０は、ＣＡＮバス２００から受信されたメインメッセージ又はＭＡＣ付きメインメッセージに含まれるデータをメッセージ処理部３０から受け取り、当該データに応じて当該処理対象を処理する。

[0026] メッセージ処理部３０はメッセージ送信時にメッセージを生成するとともに、メッセージ受信時にメッセージを解析する。メッセージ処理部３０の具体的な構成は後述する。

[0027] 送受信部５０は、メッセージ処理部３０により生成されたメッセージをＣＡＮバス２００へブロードキャスト送信する。送受信部５０は、他のＥＣＵ１００で生成されＣＡＮバス２００へブロードキャスト送信されたメッセージをＣＡＮバス２００から受信する。送受信部５０は受信したメッセージをメッセージ処理部３０に渡す。

[0028] 本実施の形態では正規の送信側のＥＣＵ１００が、自己が送信すべきメッセージが自己以外の装置から他のＥＣＵ１００に送信されていることを検出した場合、受信側のＥＣＵ１００に対して異常を通知する。これにより不正制御が行われることを防止する。正規の送信側のＥＣＵ１００による不正メッセージの検出後、不正メッセージに含まれるＩＤにより特定される処理対象の機能について、制御を続ける方式とフェイルセーフ制御に移行する方式が考えられる。まず制御を続ける方式から説明する。

[0029] 図４は、異常検出後に制御を続ける方式にてＭＡＣを別メッセージで送信する場合における、メッセージ処理部３０のなりすまし検出およびメッセージ送信に必要な機能を示すブロック図である。図４では受信に関する機能は

省略して描いている。図４のメッセージ処理部３０はメッセージ解析部３１、ＣＡＮＩＤ抽出部３２、なりすまし検出部３４、ＭＡＣ生成部３５、メインメッセージ生成部３６、データフィールド抽出部３７及びＭＡＣメッセージ生成部３８を有する。

[0030] 図５は、図４のメッセージ処理部３０による、なりすまし検出処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からメッセージを受信し、メッセージ解析部３１に渡す。ＣＡＮＩＤ抽出部３２は、メッセージ解析部３１により受信されたメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（図５のＳ１０）。ＣＡＮＩＤ抽出部３２は抽出したＣＡＮＩＤをなりすまし検出部３４に渡す。

[0031] なりすまし検出部３４はＣＡＮＩＤ抽出部３２から渡されたＣＡＮＩＤと、自己のＥＣＵ１００が送信するメッセージに含めるべきＣＡＮＩＤとを比較して、なりすましを検出する（Ｓ１１）。ここで、自己が送信するＩＤは複数あることが一般的であり、複数のＩＤ（ＩＤ群）はリスト化されて（ＩＤリスト）、各ＥＣＵのメモリに保存されているものとする。したがって、なりすまし検出部３４は、ＩＤリストの全ＩＤについてＣＡＮＩＤとの比較を行う。

[0032] 両者のＣＡＮＩＤが一致する場合は、受信されたメッセージがなりすましメッセージであると判定する。なりすましが検出された場合（Ｓ１２のＹ）、なりすまし検出部３４はなりすまし発生をＭＡＣ生成部３５及びメインメッセージ生成部３６に通知する（Ｓ１３）。なりすましが検出されない場合（Ｓ１２のＮ）、ステップＳ１３の処理はスキップされる。

[0033] 図６は、図４のメッセージ処理部３０によってなりすましが検出された後のメッセージ送信処理を示すフローチャートである。メインメッセージ生成部３６はなりすまし検出部３４からなりすまし発生の通知を受けると、なりすまされたＣＡＮＩＤで特定される処理対象の機能に関する正当なデータをアプリケーション処理部１０から取得する。メインメッセージ生成部３６は取得したデータをＣＡＮメッセージのデータフィールドに格納する。また当

該データに対応するＣＡＮＩＤをＩＤフィールドに格納する。メインメッセージ生成部３６はＣＡＮメッセージのその他の項目の値を確定してメインメッセージを完成させる。メインメッセージ生成部３６は生成したメインメッセージを送受信部５０に渡し、送受信部５０は当該メインメッセージをＣＡＮバス２００へブロードキャスト送信する（図６のＳ２０）。

[0034] ＣＡＮＩＤ抽出部３２は、送信されたメインメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（Ｓ２１）。ＣＡＮＩＤ抽出部３２は抽出したＣＡＮＩＤをＭＡＣ生成部３５に渡す。データフィールド抽出部３７は、送信されたメインメッセージのデータフィールドに格納されたデータを抽出する（Ｓ２２）。データフィールド抽出部３７は抽出したデータをＭＡＣ生成部３５に渡す。

[0035] ＭＡＣ生成部３５は、抽出されたＣＡＮＩＤ及びデータをもとにＭＡＣを生成する（Ｓ２３）。具体的には少なくとも抽出されたＣＡＮＩＤ及びデータを含む認証対象に、保持する共通鍵３５ａを使用して所定のＭＡＣアルゴリズムを適用する。これにより当該認証対象に対するＭＡＣが生成される。ＭＡＣ生成部３５は生成したＭＡＣをＭＡＣメッセージ生成部３８に渡す。

[0036] ＭＡＣメッセージ生成部３８はＭＡＣ生成部３５から取得したＭＡＣをＣＡＮメッセージのデータフィールドに格納する。また上記データに対するＭＡＣを含むメッセージであることを示すＣＡＮＩＤをＩＤフィールドに格納する。例えば上記データそのものを含むメッセージであることを示すＣＡＮＩＤの値から所定の固定値を減算した値が使用されてもよい。ＭＡＣメッセージ生成部３８はＣＡＮメッセージのその他の項目の値を確定してＭＡＣメッセージを完成させる。ＭＡＣメッセージ生成部３８は生成したＭＡＣメッセージを送受信部５０に渡し、送受信部５０は当該ＭＡＣメッセージをＣＡＮバス２００へブロードキャスト送信する（Ｓ２４）。

[0037] 図６では、なりすまされたＣＡＮＩＤで特定される処理対象の機能の正当なデータを含むメインメッセージを先に送信し、当該正当なデータを少なくとも対象とするＭＡＣを含むＭＡＣメッセージを後に送信する例を説明した

。この点、当該ＭＡＣメッセージを先に送信し、当該メインメッセージを後に送信することとしても良い。

[0038] 図７は、異常検出後に制御を続ける方式にてメインメッセージを先に受信しＭＡＣメッセージを後に受信する場合における、メッセージ処理部３０のメッセージ受信に必要な機能を示すブロック図である。図７ではなりすまし検出およびメッセージ送信に関する機能は省略して描いている。図７のメッセージ処理部３０はメッセージ解析部４１、ＣＡＮＩＤ抽出部４２、データフィールド抽出部４３、モード切替部４４、ＭＡＣ生成部４５、ＭＡＣ比較部４６、データ受渡部４７及びメインメッセージ一時保持部４８を有する。

[0039] 図８は、図７のメッセージ処理部３０によるメインメッセージ受信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からメインメッセージを受信し、メッセージ解析部４１に渡す。メッセージ解析部４１はメインメッセージを受信すると、当該メインメッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（図８のＳ３０）。

[0040] 異常検出後に制御を続ける方式における縮退モードとは、メインメッセージに含まれる特定の処理対象の特定の機能に関するデータを、ＭＡＣの検証に成功したことを条件として、当該機能に関する処理に使用するモードである。したがってＭＡＣの検証に失敗した場合、当該機能に関するデータは使用されずに破棄される。通常モードでは、メインメッセージに含まれる当該データは、ＭＡＣの検証を行うことなく当該機能に関する処理に使用される。

[0041] ステップＳ３０にて縮退モードに移行中でなく通常モードの場合（Ｓ３０のＮ）、メッセージ解析部４１により受信されたメインメッセージに対して、データフィールド抽出部４３が、このメインメッセージのデータフィールドに格納されたデータを抽出してデータ受渡部４７に渡す。データ受渡部４７は、データフィールド抽出部４３から取得したデータをアプリケーション処理部１０に渡す（Ｓ３１）。アプリケーション処理部１０は取得したデー

タに応じて処理対象を処理する。

[0042] ステップＳ３０にて縮退モードに移行中の場合（Ｓ３０のＹ）、メッセージ解析部４１は、受信されたメインメッセージをデータフィールド抽出部４３には渡さず、処理が保留される（Ｓ３２）。

[0043] メッセージ解析部４１は、メインメッセージ一時保持部４８にメインメッセージが保持されているか否か判断する（Ｓ３３）。保持されている場合（Ｓ３３のＹ）、メインメッセージ一時保持部４８に保持されているメインメッセージの数がｎ個以上であるか否か判断する（Ｓ３４）。ｎはメインメッセージ一時保持部４８に保持されるメインメッセージの上限数を規定したパラメータである。例えばｎ＝３に設定される。

[0044] メインメッセージの数がｎ個以上、保持されている場合（Ｓ３４のＹ）、メッセージ解析部４１は、メインメッセージ一時保持部４８に保持されている複数のメインメッセージの内、最も古いメインメッセージを破棄する（Ｓ３５）。メッセージ解析部４１は受信した新しいメインメッセージをメインメッセージ一時保持部４８に格納する（Ｓ３６）。即ちメインメッセージ一時保持部４８はＦＩＦＯ（ＦＩＲＳＴ－ＩＮ　ＦＩＲＳＴ－ＯＵＴ）で管理される。メインメッセージ一時保持部４８に格納されたメインメッセージに含まれるデータに対するＭＡＣの生成処理は、メッセージ解析部４１から指示があるまで保留される。

[0045] ステップＳ３４にて、メインメッセージ一時保持部４８に保持されているメインメッセージの数がｎ個未満である場合（Ｓ３４のＮ）、ステップＳ３５はスキップされ、メッセージ解析部４１は受信した新しいメインメッセージをメインメッセージ一時保持部４８に格納する（Ｓ３６）。

[0046] ステップＳ３３にて、メインメッセージ一時保持部４８にメインメッセージが保持されていない場合（Ｓ３３のＮ）、メッセージ解析部４１は受信した新しいメインメッセージをメインメッセージ一時保持部４８に格納する（Ｓ３６）。

[0047] 図９は、図７のメッセージ処理部３０によるＭＡＣメッセージ受信処理を

示すフローチャートである。送受信部５０はＣＡＮバス２００からＭＡＣメッセージを受信し、メッセージ解析部４１に渡す。メッセージ解析部４１はＭＡＣメッセージを受信すると、当該メインメッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（図９のＳ４０）。縮退モードに移行中でない場合（Ｓ４０のＮ）、モード切替部４４は通常モードから縮退モードに切り替える（Ｓ４１）。縮退モードに移行中の場合（Ｓ４０のＹ）、縮退モードを継続する。このように異常検出後に制御を続ける方式では、受信側のＥＣＵ１００でＭＡＣが受信されたタイミングで縮退モードに移行する。

[0048] メッセージ解析部４１は、メインメッセージ一時保持部４８にメインメッセージが保持されているか否か判断する（Ｓ４２）。保持されている場合（Ｓ４２のＹ）、メッセージ解析部４１は受信したＭＡＣメッセージをデータフィールド抽出部４３に渡し、データフィールド抽出部４３は、取得したＭＡＣメッセージのデータフィールドからＭＡＣを抽出する（Ｓ４３）。データフィールド抽出部４３は抽出したＭＡＣをＭＡＣ比較部４６に渡す。

[0049] メインメッセージ一時保持部４８に保持されるメインメッセージのＭＡＣが生成済みでない場合（Ｓ４４のＮ）、ＣＡＮＩＤ抽出部４２は、メッセージ解析部４１により受信されてメインメッセージ一時保持部４８に保持されているメインメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（Ｓ４５）。ＣＡＮＩＤ抽出部４２は抽出したＣＡＮＩＤをＭＡＣ生成部４５に渡す。データフィールド抽出部４３は、メッセージ解析部４１により受信されてメインメッセージ一時保持部４８に保持されているメインメッセージのデータフィールドに格納されたデータを抽出する（Ｓ４６）。データフィールド抽出部４３は抽出したデータをＭＡＣ生成部４５及びデータ受渡部４７に渡す。

[0050] ＭＡＣ生成部４５は、抽出されたＣＡＮＩＤ及びデータをもとにＭＡＣを生成する（Ｓ４７）。生成方法は送信側のＭＡＣ生成部３５の生成方法と同じである。受信側のＭＡＣ生成部４５は、送信側のＭＡＣ生成部３５が保持

する共通鍵３５ａと同じ共通鍵４５ａを保持している。ＭＡＣ生成部４５は生成したＭＡＣをＭＡＣ比較部４６に渡す。

[0051] ＭＡＣ比較部４６はＭＡＣ生成部４５により生成されたＭＡＣと、データフィールド抽出部４３により抽出されたＭＡＣとを比較する（Ｓ４８）。両者のＭＡＣが一致した場合（Ｓ４９のＹ）、ＭＡＣ比較部４６はＭＡＣの検証が成功したと判定し、データ受渡部４７に検証が成功した旨を通知する。データフィールド抽出部４３は、ＭＡＣの検証が成功したメインメッセージのデータフィールドからデータを抽出してデータ受渡部４７に渡す。データ受渡部４７はデータフィールド抽出部４３から渡されたデータをアプリケーション処理部１０に渡す（Ｓ４１０）。アプリケーション処理部１０は取得したデータに応じて処理対象を処理する。

[0052] メッセージ解析部４１は、メインメッセージ一時保持部４８にメインメッセージが保持されているか否か判断する（Ｓ４１２）。保持されている場合（Ｓ４１２のＹ）、メッセージ解析部４１はメインメッセージ一時保持部４８に保持されているメッセージを破棄する（Ｓ４１３）。メインメッセージ一時保持部４８にメインメッセージが保持されていない場合（Ｓ４１２のＮ）、ステップＳ４１３の処理がスキップされる。

[0053] ステップＳ４９にて、両者のＭＡＣが一致しない場合（Ｓ４９のＮ）、ＭＡＣ比較部４６はＭＡＣの検証が失敗したと判定し、データ受渡部４７に検証が失敗した旨を通知する。データ受渡部４７はデータフィールド抽出部４３から渡されたデータをアプリケーション処理部１０に渡さない。メッセージ解析部４１は受信したＭＡＣメッセージを破棄する（Ｓ４１１）。

[0054] ステップＳ４４にて、メインメッセージ一時保持部４８に保持されているメインメッセージのＭＡＣが生成済みである場合（Ｓ４４のＹ）、ステップＳ４５～ステップＳ４７の処理がスキップされる。

[0055] ステップＳ４２にて、メインメッセージ一時保持部４８にメインメッセージが保持されていない場合（Ｓ４２のＮ）、メッセージ解析部４１は受信したＭＡＣメッセージを破棄する（Ｓ４１１）。

[0056] なおＭＡＣメッセージが受信された際、メインメッセージ一時保持部４８に複数のメインメッセージが保持されている場合、新しいメインメッセージから順にＭＡＣが生成され、受信されたＭＡＣメッセージに含まれるＭＡＣと比較される。受信したＭＡＣメッセージに対応するメインメッセージが見つかった時点で当該メインメッセージに含まれるデータに応じた処理が実行される。それと共にメインメッセージ一時保持部４８に保持されている残りのメインメッセージが破棄される。

[0057] 図１０は、異常検出後に制御を続ける方式にてＭＡＣメッセージを先に受信しメインメッセージを後に受信する場合における、メッセージ処理部３０のメッセージ受信に必要な機能を示すブロック図である。図１０ではなりすまし検出およびメッセージ送信に関する機能は省略して描いている。図１０のメッセージ処理部３０は、図７のメッセージ処理部３０のメインメッセージ一時保持部４８がＭＡＣメッセージ一時保持部４８ａに置き換わった構成である。

[0058] 図１１は、図１０のメッセージ処理部３０によるＭＡＣメッセージ受信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からＭＡＣメッセージを受信し、メッセージ解析部４１に渡す。メッセージ解析部４１はＭＡＣメッセージを受信すると、当該ＭＡＣメッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（図１１のＳ５０）。縮退モードに移行中でない場合（Ｓ５０のＮ）、モード切替部４４は通常モードから縮退モードに切り替える（Ｓ５１）。縮退モードに移行中の場合（Ｓ５０のＹ）、縮退モードを継続する。

[0059] メッセージ解析部４１は、ＭＡＣメッセージ一時保持部４８ａに保持されているＭＡＣメッセージの数がｎ個以上であるか否か判断する（Ｓ５２）。ｎはＭＡＣメッセージ一時保持部４８ａに保持されるＭＡＣメッセージの上限数を規定したパラメータである。例えばｎ＝３に設定される。

[0060] ＭＡＣメッセージの数がｎ個以上、保持されている場合（Ｓ５２のＹ）、メッセージ解析部４１は、ＭＡＣメッセージ一時保持部４８ａに保持されて

いる複数のＭＡＣメッセージの内、最も古いＭＡＣメッセージを破棄する（Ｓ５３）。メッセージ解析部４１は受信した新しいＭＡＣメッセージをＭＡＣメッセージ一時保持部４８ａに格納する（Ｓ５４）。即ちＭＡＣメッセージ一時保持部４８ａはＦＩＦＯ（ＦＩＲＳＴ－ＩＮ　ＦＩＲＳＴ－ＯＵＴ）で管理される。ステップＳ５２にて、ＭＡＣメッセージ一時保持部４８ａに保持されているＭＡＣメッセージの数がｎ個未満である場合（Ｓ５２のＮ）、ステップＳ５３がスキップされ、メッセージ解析部４１は受信した新しいＭＡＣメッセージをＭＡＣメッセージ一時保持部４８ａに格納する（Ｓ５４）。

[0061] メインメッセージが受信されるとデータフィールド抽出部４３は、先に受信されたＭＡＣメッセージのデータフィールドに格納されたＭＡＣを抽出してＭＡＣ比較部４６に渡す（Ｓ５５）。

[0062] 図１２は、図１０のメッセージ処理部３０によるメインメッセージ受信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からメインメッセージを受信し、メッセージ解析部４１に渡す。メッセージ解析部４１はメインメッセージを受信すると、当該メインメッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（図１２のＳ６０）。

[0063] 縮退モードに移行中であり（Ｓ６０のＹ）且つＭＡＣメッセージが受信済みである場合（Ｓ６１のＹ）、ＣＡＮＩＤ抽出部４２は、メッセージ解析部４１により受信されたメインメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（Ｓ６２）。ＣＡＮＩＤ抽出部４２は抽出したＣＡＮＩＤをＭＡＣ生成部４５に渡す。データフィールド抽出部４３は、メッセージ解析部４１により受信されたメインメッセージのデータフィールドに格納されたデータを抽出する（Ｓ６３）。データフィールド抽出部４３は抽出したデータをＭＡＣ生成部４５及びデータ受渡部４７に渡す。

[0064] ＭＡＣ生成部４５は、抽出されたＣＡＮＩＤ及びデータをもとにＭＡＣを生成する（Ｓ６４）。ＭＡＣ生成部４５は生成したＭＡＣをＭＡＣ比較部４

６に渡す。ＭＡＣ比較部４６はＭＡＣ生成部４５により生成されたＭＡＣと、データフィールド抽出部４３によりＭＡＣメッセージのデータフィールドから抽出されたＭＡＣとを比較する（Ｓ６５）。両者のＭＡＣが一致した場合（Ｓ６６のＹ）、ＭＡＣ比較部４６はＭＡＣの検証が成功したと判定し、データ受渡部４７に検証が成功した旨を通知する。データ受渡部４７は当該通知を受けると、データフィールド抽出部４３から渡され保留していたデータをアプリケーション処理部１０に渡す（Ｓ６７）。アプリケーション処理部１０は取得したデータに応じて処理対象を処理する。

[0065] ステップＳ６６にて、両者のＭＡＣが一致しない場合（Ｓ６６のＮ）、ＭＡＣ比較部４６はＭＡＣの検証が失敗したと判定し、データ受渡部４７に検証が失敗した旨を通知する。データ受渡部４７は、データフィールド抽出部４３から渡されたデータをアプリケーション処理部１０に渡さない。ステップＳ６１にて、ＭＡＣメッセージが受信済みでない場合（Ｓ６１のＮ）、メッセージ解析部４１は受信したメインメッセージを破棄する（Ｓ６８）。ステップＳ６０にて、縮退モードに移行中でない場合（Ｓ６０のＮ）、ステップＳ６１～ステップＳ６６がスキップされ、受信されたメインメッセージから抽出されたデータはアプリケーション処理部１０に渡される（Ｓ６７）。アプリケーション処理部１０は取得したデータに応じて処理対象を処理する。

[0066] なおメインメッセージが受信された際、ＭＡＣメッセージ一時保持部４８ａに複数のＭＡＣメッセージが保持されている場合、新しいＭＡＣから順に、メインメッセージに含まれるデータから生成されるＭＡＣと比較される。ＭＡＣが一致した時点で当該メインメッセージに含まれるデータに応じた処理が実行される。それと共にＭＡＣメッセージ一時保持部４８ａに保持されている残りのＭＡＣメッセージが破棄される。

[0067] 以上、正当なデータを含むメインメッセージを先に送信し、当該メインメッセージに対するＭＡＣメッセージを後に送信する場合と、正当なデータを含むメインメッセージに対するＭＡＣメッセージを先に送信し、当該メイン

メッセージを後に送信する場合を説明した。両者の送信方法のどちらを採用してもよいが、後者の送信方法を採用した方が縮退モードに移行するタイミングが早くなる。受信側のＥＣＵ１００ではＭＡＣメッセージの受信を契機として縮退モードに移行するためである。当該ＭＡＣメッセージと当該メインメッセージの間に、攻撃者により不正メッセージが挿入された場合でも既に縮退モードに移行しているため、当該不正メッセージによる不正な制御を防止できる。

[0068] 図１３は、異常検出後に制御を続ける方式にてＭＡＣをメインメッセージに含めて送信する場合における、メッセージ処理部３０のなりすまし検出およびメッセージ送信に必要な機能を示すブロック図である。図１３では受信に関する機能は省略して描いている。図１３のメッセージ処理部３０は、図４のメッセージ処理部３０からＭＡＣメッセージ生成部３８が省略された構成である。

[0069] 図１４は、図１３のメッセージ処理部３０による、なりすまし検出後のＭＡＣ付きメインメッセージ送信処理を示すフローチャートである。メインメッセージ生成部３６は、なりすまし検出部３４からなりすまし発生の通知を受けると、なりすまされたＣＡＮＩＤで特定される処理対象の機能に関する正当なデータをアプリケーション処理部１０から取得する。メインメッセージ生成部３６は取得したデータをＣＡＮメッセージのデータフィールドに格納してメインメッセージを生成する（Ｓ２０ａ）。

[0070] ＣＡＮＩＤ抽出部３２は、生成されたメインメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（Ｓ２１ａ）。ＣＡＮＩＤ抽出部３２は抽出したＣＡＮＩＤをＭＡＣ生成部３５に渡す。データフィールド抽出部３７は、生成されたメインメッセージのデータフィールドに格納されたデータを抽出する（Ｓ２２ａ）。データフィールド抽出部３７は抽出したデータをＭＡＣ生成部３５に渡す。

[0071] ＭＡＣ生成部３５は、抽出されたＣＡＮＩＤ及びデータをもとにＭＡＣを生成する（Ｓ２３ａ）。ＭＡＣ生成部３５は生成したＭＡＣをメインメッセ

ージ生成部３６に渡す。メインメッセージ生成部３６はＭＡＣ生成部３５から取得したＭＡＣを、上記メインメッセージのデータフィールドに追加で格納する。メインメッセージ生成部３６はＭＡＣを追加したＭＡＣ付きメインメッセージを送受信部５０に渡し、送受信部５０は当該ＭＡＣ付きメインメッセージをＣＡＮバス２００へブロードキャスト送信する（Ｓ２４ａ）。

[0072] 図１５は、異常検出後に制御を続ける方式にてＭＡＣ付きメインメッセージを受信する場合における、メッセージ処理部３０のメッセージ受信に必要な機能を示すブロック図である。図１５ではなりすまし検出およびメッセージ送信に関する機能は省略して描いている。図１５のメッセージ処理部３０は、図７のメッセージ処理部３０のメインメッセージ一時保持部４８が省略された構成である。また図１０のメッセージ処理部３０のＭＡＣメッセージ一時保持部４８ａが省略された構成でもある。

[0073] 図１６は、図１５のメッセージ処理部３０によるＭＡＣ付きメインメッセージ受信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からメッセージを受信し、メッセージ解析部４１に渡す。メッセージ解析部４１は送受信部５０から取得したメッセージにＭＡＣが含まれるか否か判定する（図１６のＳ３９８）。ＭＡＣが含まれるか否かは、例えばデータ長符号（ＤＬＣ：ＤａｔａＬｅｎｇｔｈＣｏｄｅ）、ＣＡＮＩＤ、又はデータフィールド内にＭＡＣを含むか否かを示すフラグを参照することにより判定できる。

[0074] ＭＡＣが含まれる場合（Ｓ３９８のＹ）、メッセージ解析部４１は受信したＭＡＣ付きメインメッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（Ｓ４０）。縮退モードに移行中でない場合（Ｓ４０のＮ）、モード切替部４４は通常モードから縮退モードに切り替える（Ｓ４１）。縮退モードに移行中の場合（Ｓ４０のＹ）、縮退モードを継続する。

[0075] ＣＡＮＩＤ抽出部４２は、メッセージ解析部４１により受信されたＭＡＣ付きメインメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（Ｓ４５

ａ）。ＣＡＮＩＤ抽出部４２は抽出したＣＡＮＩＤをＭＡＣ生成部４５に渡す。データフィールド抽出部４３は、メッセージ解析部４１により受信されたＭＡＣ付きメインメッセージのデータフィールドからＭＡＣとデータを抽出する（Ｓ４６ａ）。データフィールド抽出部４３は抽出したＭＡＣをＭＡＣ比較部４６に渡し、抽出したデータをＭＡＣ生成部４５及びデータ受渡部４７に渡す。

[0076] ＭＡＣ生成部４５は、抽出されたＣＡＮＩＤ及びデータをもとにＭＡＣを生成する（Ｓ４７）。ＭＡＣ比較部４６はＭＡＣ生成部４５により生成されたＭＡＣと、データフィールド抽出部４３により抽出されたＭＡＣとを比較する（Ｓ４８）。両者のＭＡＣが一致した場合（Ｓ４９のＹ）、ＭＡＣ比較部４６はＭＡＣの検証が成功したと判定し、データ受渡部４７に検証が成功した旨を通知する。データ受渡部４７はデータフィールド抽出部４３から渡されたデータをアプリケーション処理部１０に渡す（Ｓ４１０）。アプリケーション処理部１０は取得したデータに応じて処理対象を処理する。

[0077] ステップＳ４９にて、両者のＭＡＣが一致しない場合（Ｓ４９のＮ）、ＭＡＣ比較部４６はＭＡＣの検証が失敗したと判定し、データ受渡部４７に検証が失敗した旨を通知する。データ受渡部４７はデータフィールド抽出部４３から渡されたデータをアプリケーション処理部１０に渡さない。

[0078] ステップＳ３９８にて、ＭＡＣが含まれない場合（Ｓ３９８のＮ）、メッセージ解析部４１は、受信されたメッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（Ｓ３９９）。縮退モードに移行中でなく通常モードの場合（Ｓ３９９のＮ）、データフィールド抽出部４３はメッセージ解析部４１により受信されたメッセージのデータフィールドに格納されたデータを抽出してデータ受渡部４７に渡す。データ受渡部４７はデータフィールド抽出部４３から取得したデータをアプリケーション処理部１０に渡す（Ｓ４１０）。アプリケーション処理部１０は取得したデータに応じて処理対象を処理する。ステップＳ３９９にて、縮退モードに移行中の場合（Ｓ３９９のＹ）、メッセージ解析部４１に

より受信されたメッセージに含まれるデータは、アプリケーション処理部１０に渡されない。当該受信されたメッセージは破棄されるか、図示しないメッセージ一時保持部に一時保持される。

[0079] 以上に説明したＭＡＣをメインメッセージに含めて送信する方式は、送信すべき通常データの量が少ない場合に有効である。ＭＡＣをメインメッセージに含めて送信する方式はＭＡＣを別のメッセージで送信する方式と比較し、基本的にメッセージ数を減らす効果がある。しかしながら通常データの量が多い場合、６４ビットのデータフィールドに通常データとＭＡＣを併存させるのが難しくなる。その場合、両者の少なくとも一方を複数に分割する必要があり、メッセージの数が増える。またＭＡＣを別メッセージで送信する方式のほうが通常、メッセージ処理部３０の処理を単純化できる。したがって必ずしも、ＭＡＣをメインメッセージに含めて送信する方式が、ＭＡＣを別のメッセージで送信する方式より有利というわけではない。したがって通常データの量などが考慮されたうえで、両者が使い分けられて設定されるのが好ましい。

[0080] 次に、正規の送信側のＥＣＵ１００による不正メッセージの検出後、不正メッセージに含まれるＩＤにより特定される処理対象の機能について、フェイルセーフ制御に移行する方式を説明する。この方式では、不正メッセージを検出した正規の送信側のＥＣＵ１００が不正通知メッセージを送信する。受信側のＥＣＵ１００は不正通知メッセージを受信すると予め定められた縮退モードへと移行し、フェイルセーフ制御を行う。

[0081] 上述のように異常検出後に制御を続ける方式における縮退モードは、メインメッセージに含まれる特定の機能に関するデータを、ＭＡＣの検証に成功したことを条件として、当該機能の処理に使用するモードを意味した。

[0082] これに対して異常検出後にフェイルセーフ制御に移行する方式における縮退モードは、不正通知メッセージによって通知されたＣＡＮＩＤのメインメッセージに含まれる特定の機能に関するデータの値を信用せず、予め規定されたフェイルセーフ制御を行うモードを意味する。フェイルセーフ制御とは

、特定の処理対象の特定の機能を当該処理対象を安全に処理するために、予め安全性を考慮して規定されたデフォルト値に応じて行われる制御である。

[0083] なお重要な処理対象の重要な機能に関連するメッセージに不正が発生した場合については、当該機能に関してのみフェイルセーフ制御に移行させるのではなく、当該処理対象全体または車両全体をフェイルセーフ制御に移行させてもよい。例えば車両が安全に停止できるよう車両内の全ての処理対象に関する制御値を予め安全性を考慮して規定されたデフォルト値に設定してもよい。

[0084] 図１７は、異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部３０のなりすまし検出および不正通知メッセージ送信に必要な機能を示すブロック図である。図１７では受信に関する機能は省略して描いている。図１７のメッセージ処理部３０はメッセージ解析部３１、ＣＡＮＩＤ抽出部３２、なりすまし検出部３４、ＭＡＣ生成部３５、不正通知メッセージ生成部３６ａ、データフィールド抽出部３７及びカウンタ値記憶部３９を有する。

[0085] 図１８は、不正通知メッセージのフォーマット例を示す図である。不正通知メッセージのフォーマットは、図１のＣＡＮメッセージのフォーマットと同じフォーマットである。図１８のＣＡＮヘッダは、図１のＳＯＦからＤＬＣまでに相当する。図１８のデータフィールドＦ２には異常が発生したＣＡＮＩＤ、再送攻撃を防ぐためのカウンタ値、及びＭＡＣが格納される。当該ＭＡＣは、当該ＣＡＮＩＤ及び当該カウンタ値を対象として生成されたＭＡＣである。

[0086] 当該ＣＡＮＩＤは、なりすまし検出部３４により検出される不正メッセージに含まれるＣＡＮＩＤである。当該カウンタ値には、各ＥＣＵ１００において各ＣＡＮＩＤのメッセージが送信された回数を用いることができる。カウンタ値記憶部３９は各ＣＡＮＩＤのメッセージの送信回数をカウンタ値として記憶している。即ち、あるＣＡＮＩＤのメッセージが送信される度に当該ＣＡＮＩＤのカウンタ値がインクリメントされる。上記のデータフィール

ドＦ２に格納されるカウンタ値には、異常通知メッセージの送信回数が使用される。

[0087] なお不正通知メッセージのデータフィールドＦ２に格納されるデータのフォーマットは、図１８の例に限るものではない。例えばカウンタ値を含まないフォーマットも可能である。この場合、図１７のカウンタ値記憶部３９は不要となる。またカウンタ値の代わりに乱数を用いてもよい。なお不正通知メッセージのデータフィールドＦ２には、異常が発生したＣＡＮＩＤを特定するための情報が含まれていればよく、当該ＣＡＮＩＤそのものを含めないフォーマットも可能である。

[0088] 図１９は、図１７のメッセージ処理部３０によるなりすまし検出処理および不正通知メッセージ送信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からメッセージを受信し、メッセージ解析部３１に渡す。ＣＡＮＩＤ抽出部３２は、メッセージ解析部３１により受信されたメッセージのＩＤフィールドからＣＡＮＩＤを抽出する（図１９のＳ１０）。ＣＡＮＩＤ抽出部３２は、抽出したＣＡＮＩＤをなりすまし検出部３４に渡す。

[0089] なりすまし検出部３４はＣＡＮＩＤ抽出部３２から渡されたＣＡＮＩＤと、自己のＥＣＵ１００が送信するメッセージに含めるべきＣＡＮＩＤとを比較して、なりすましを検出する（Ｓ１１）。両者のＣＡＮＩＤが一致する場合、受信されたメッセージがなりすましメッセージであると判定する。なりすましが検出された場合（Ｓ１２のＹ）、なりすまし検出部３４はなりすまし発生を不正通知メッセージ生成部３６ａに通知する（Ｓ１４）。

[0090] 不正通知メッセージ生成部３６ａは、なりすましが検出されたＣＡＮＩＤを含むデータを生成し、不正通知メッセージのデータフィールドに格納するとともに（Ｓ１５）、ＭＡＣ生成部３５に渡す。当該データは例えば、なりすましが検出されたＣＡＮＩＤと、当該ＣＡＮＩＤのメッセージの送信回数を示すカウンタ値との組み合わせで生成される。

[0091] ＭＡＣ生成部３５は不正通知メッセージ生成部３６ａにより生成されたデータをもとにＭＡＣを生成する（Ｓ１６）。ＭＡＣ生成部３５は生成したＭ

ＡＣを不正通知メッセージ生成部３６ａに渡す。不正通知メッセージ生成部３６ａはＭＡＣ生成部３５により生成されたＭＡＣを、不正通知メッセージのデータフィールドに追加で格納する（Ｓ１７）。不正通知メッセージ生成部３６ａは生成した不正通知メッセージを送受信部５０に渡し、送受信部５０は当該不正通知メッセージをＣＡＮバス２００へブロードキャスト送信する（Ｓ１８）。

[0092] 図２０は、異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部３０の不正通知メッセージ受信に必要な機能を示すブロック図である。図２０ではなりすまし検出およびメッセージ送信に関する機能は省略して描いている。図２０のメッセージ処理部３０は、図１５のメッセージ処理部３０にカウンタ値記憶部４９が追加された構成である。カウンタ値記憶部４９は各ＣＡＮＩＤのメッセージの受信回数をカウンタ値として記憶している。即ち、あるＣＡＮＩＤのメッセージが受信され、ＭＡＣの検証に成功する度に当該ＣＡＮＩＤのカウンタ値がインクリメントされる。

[0093] 図２１は、異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部３０による不正通知メッセージ受信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００から不正通知メッセージを受信し、メッセージ解析部４１に渡す。データフィールド抽出部４３はメッセージ解析部４１により受信された不正通知メッセージのデータフィールドを抽出する（図２０のＳ７０）。データフィールド抽出部４３は、抽出したデータフィールドに含まれるデータとＭＡＣを分離する（Ｓ７１）。データフィールド抽出部４３は、抽出および分離したデータをＭＡＣ生成部４５に渡し、抽出および分離したＭＡＣをＭＡＣ比較部４６に渡す。

[0094] ＭＡＣ生成部４５は、分離されたデータに含まれる異常が発生したＣＡＮＩＤと、カウンタ値記憶部４９から取得される当該ＣＡＮＩＤのカウンタ値をもとにＭＡＣを生成する（Ｓ７２）。ＭＡＣ生成部４５は生成したＭＡＣをＭＡＣ比較部４６に渡す。

[0095] なお当該カウンタ値として、受信された不正通知メッセージのデータフィ

ールドに含まれているカウンタ値をそのまま使用してもよい。この場合、例えば受信されたカウンタ値がカウンタ値記憶部４９から取得される当該ＣＡＮＩＤのカウンタ値より大きく、且つＭＡＣの検証に成功した場合に、カウンタ値記憶部４９に記憶されるカウンタ値を、受信されたカウンタ値の値に更新することで、送信側のＥＣＵと受信側のＥＣＵにおけるカウンタ値のずれを防ぐことができる。

[0096] さらに、単に受信されたカウンタ値とカウンタ値記憶部４９から取得される当該ＣＡＮＩＤのカウンタ値の大小を比較するのみではなく、次に示す内容でもセキュリティ強度を高めることができる。

[0097] すなわち、受信されたカウンタ値がカウンタ値記憶部４９から取得される当該ＣＡＮＩＤのカウンタ値より大きく、カウンタ値記憶部４９から取得される当該ＣＡＮＩＤのカウンタ値に、任意の値を足したものより小さい範囲に入っているカウンタ値のみを更新の対象にするなどである。

[0098] ＭＡＣ比較部４６はＭＡＣ生成部４５により生成されたＭＡＣと、データフィールド抽出部４３により抽出および分離されたＭＡＣとを比較する（Ｓ７３）。両者のＭＡＣが一致した場合（Ｓ７４のＹ）、モード切替部４４は通常モードから縮退モード（フェイルセーフ制御）に移行する（Ｓ７５）。両者のＭＡＣが一致しない場合（Ｓ７４のＮ）、通常モードに維持される。

[0099] 図２２は、異常検出後にフェイルセーフ制御に移行する方式にて、メッセージ処理部３０によるメインメッセージ受信処理を示すフローチャートである。送受信部５０はＣＡＮバス２００からメインメッセージを受信し、メッセージ解析部４１に渡す。メッセージ解析部４１はメインメッセージを受信すると、当該メッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能が縮退モードに移行中であるか否か判定する（図２２のＳ８０）。縮退モードに移行中でなく通常モードの場合（Ｓ８０のＮ）、受信されたメインメッセージに含まれるデータはアプリケーション処理部１０に渡され、アプリケーション処理部１０は渡されたデータに応じて処理対象を処理する（Ｓ８１）。縮退モードに移行中の場合（Ｓ８０のＹ）、メッセージ解析部４１

は受信したメインメッセージを破棄する（Ｓ８２）。当該メッセージに含まれるＣＡＮＩＤにより特定される処理対象の機能は、フェイルセーフ制御が維持される。

[0100] 以上説明したように本実施の形態によれば、なりすましメッセージが検出された際、ＭＡＣメッセージ、ＭＡＣ付きメインメッセージ又は不正通知メッセージを送信する。これにより、通常データを含むメッセージを送信する度にＭＡＣを生成および送信することなくセキュリティを向上させることができる。恒常的なＭＡＣの生成および送信処理が不要であるため、各ＥＣＵ１００でのＭＡＣの生成およびＭＡＣの検証にかかる処理負荷を軽減できる。またＣＡＮバス２００の占有率の増加を抑制できる。

[0101] また不正通知メッセージを通常のＣＡＮメッセージのフォーマットで生成するため、ＣＡＮコントローラ等のハードウエア資源に変更を加えることなく、且つ規格で規定された処理内容を変更することなく実装できる。したがって導入コストを低く抑えることができる。

[0102] 以上、本発明を実施の形態をもとに説明した。実施の形態は例示であり、それらの各構成要素や各処理プロセスの組み合わせにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

[0103] たとえば変形例の１つとして、以下のような例がある。すなわち、上述の実施の形態では、受信側のＥＣＵ１００が異常検出後の不正通知メッセージを受信した際に「フェイルセーフ制御へ移行する方式」について詳細を説明したが、本変形例は、受信側のＥＣＵ１００が不正通知メッセージを受信した際に「制御を続ける方式」へ移行する処理フローを採用する例である。

[0104] この場合、メッセージ処理部３０のなりすまし検出および不正通知メッセージ送信に必要な機能ブロック、不正通知メッセージのフォーマット例、処理フローは、上記実施の形態の説明で用いた図１７から図１９に示される構成や内容と同じ構成、内容にて実現される。また、不正通知メッセージ受信に必要な機能の構成および処理フローも図２０および図２１に示すものと同

様である。

[0105] ただし、受信側のＥＣＵ１００における処理は、図２１に示すステップＳ７０からステップＳ７３までは同じ処理を行い、ＭＡＣ比較部４６がＭＡＣ生成部４５により生成されたＭＡＣとデータフィールド抽出部４３により抽出および分離されたＭＡＣとを比較し（Ｓ７３）、両者のＭＡＣが一致した場合、ＭＡＣの検証が成功したと判定し、「制御を続ける方式」における縮退モードに移行する。

[0106] 不正通知メッセージ受信後に「制御を続ける方式」に移行する場合、異常が検出された後に、送信側のＥＣＵ１００からはメインメッセージとＭＡＣメッセージとを分けて送信する場合と、ＭＡＣ付きメインメッセージを送信する場合がある。メインメッセージとＭＡＣメッセージとを分けて送信する場合、メッセージ処理部３０のメッセージ送信に必要な機能の構成および処理フローは図４および図６に示すものと同様である。ＭＡＣ付きメインメッセージを送信する場合、メッセージ処理部３０のメッセージ送信に必要な機能の構成および処理フローは図１３および図１４に示すものと同様である。

[0107] また、受信側ＥＣＵ１００において、メインメッセージを先に受信し、ＭＡＣメッセージを後に受信する場合と、ＭＡＣメッセージを先に受信し、メインメッセージを後に受信する場合と、ＭＡＣ付きメインメッセージを受信する場合がある。

[0108] メインメッセージを先に受信し、ＭＡＣメッセージを後に受信する場合、メッセージ処理部３０のメッセージ受信に必要な機能の構成および処理フローは、図７から図９に示すものと同様である。

[0109] ＭＡＣメッセージを先に受信し、メインメッセージを後に受信する場合、メッセージ処理部３０のメッセージ受信に必要な機能の構成および処理フローは、図１０から図１２に示すものと同様である。

[0110] ＭＡＣ付きメインメッセージを受信する場合、メッセージ処理部３０のメッセージ受信に必要な機能の構成および処理フローは、図１５から図１６に示すものと同様である。

[0111] この変形例を採用しても、上記実施の形態にて説明したものと同様にセキュリティを向上させることができる。

[0112] なお、任意のＥＣＵ１００（受信側のＥＣＵ１００）において、それぞれ異なるＣＡＮＩＤを含むメッセージを複数受信し、複数の当該メッセージに対して異常が検出された後に「制御を続ける方式」に移行した場合、移行後さらに「フェイルセーフ制御へ移行する方式」に移行してもよい。

[0113] また、上述の実施の形態においては、なりすましが検出された後にＭＡＣが送信される内容を例示して説明したが、次のような場合に受信側のＥＣＵ１００が、フェイルセーフ制御に移行する構成としてもよい。

[0114] すなわち、送信側のＥＣＵ１００と受信側のＥＣＵ１００との間でメッセージにＭＡＣが付与されるタイミングを共有させておくことを前提に、送信側のＥＣＵ１００から定期的にＭＡＣを送信し、受信側のＥＣＵ１００において、本来ＭＡＣを受信すべきタイミングでＭＡＣの検証に失敗した場合である。

[0115] もしくは、送信側のＥＣＵ１００と受信側のＥＣＵ１００との間でメッセージにＭＡＣが付与されるタイミングを共有させておくことを前提に、送信側のＥＣＵ１００から定期的にＭＡＣを送信し、受信側のＥＣＵ１００において、本来ＭＡＣを受信すべきタイミングで送信側のＥＣＵ１００からＭＡＣが送信されなかった場合である。

[0116] これらの構成により、ＣＡＮシステム５００の動作中に正規のＥＣＵ１００に対する改ざんや不正な取り外しなどによる異常状態の検出や安全性の確保が可能となる。

[0117] あるいは、ＣＡＮシステム５００が起動し通信が開始される際に、初めて送信するＣＡＮＩＤのメッセージに対してＭＡＣを付与して送信する構成としてもよい。この構成によれば、システムの起動時における正規のＥＣＵ１００に対する改ざんや不正な取り外しなどに起因する異常状態の検出や安全性の確保が可能となる。

[0118] 上述の実施の形態では、あらかじめ設定された規則として、送信側のＥＣ

Ｕ１００が本来送信するＣＡＮＩＤを当該ＥＣＵ１００自身は受信しないという事象を規定し、この規則に反した事象（この場合、本来送信するＣＡＮＩＤを受信すること）の発生を異常が発生した（あるいは不正が検出された）こととして説明した。

[0119] このような、あらかじめ設定（あるいは規定）された規則を通信規則と称すると、当該通信規則にはその他にもいくつかの種類が考えられ、たとえば以下のものが適用可能である。

[0120] 通信規則の一例としては、送信側のＥＣＵ１００において、ＣＡＮバス２００に任意のＣＡＮＩＤのメッセージが送信される周期を通信規則として保持する例がある。本例では、当該ＣＡＮＩＤのメッセージが送信される周期があらかじめ通信規則として設定された周期と不一致であった場合に、これを不正なメッセージとして検出することが可能である。

[0121] 通信規則の一例としては、送信側のＥＣＵ１００において、ＣＡＮバス２００に任意のＣＡＮＩＤのメッセージが送信される最大頻度を通信規則として保持する例がある。本例では、当該ＣＡＮＩＤのメッセージが送信される頻度があらかじめ通信規則として設定された最大頻度と不一致であった場合に、これを不正なメッセージとして検出することが可能である。

[0122] また、通信規則の別の例としては、送信側のＥＣＵ１００において、あるＣＡＮＩＤのメッセージのフォーマットを通信規則として保持する例がある。フォーマットとしては、メッセージのデータサイズなどが挙げられる。本例では、ＣＡＮバス２００に送信された当該ＣＡＮＩＤのメッセージのデータサイズが、あらかじめ通信規則として設定されたデータサイズと不一致であった場合に、これを不正として検出することが可能である。

[0123] また、通信規則の別の例としては、送信側のＥＣＵ１００において、あるＣＡＮＩＤのメッセージに含まれるデータの値の範囲や変化量などを通信規則として保持する例がある。本例では、当該ＣＡＮＩＤのメッセージにＣＡＮバス２００に送信された当該ＣＡＮＩＤのメッセージに含まれるデータの値が、あらかじめ通信規則として規定されている値と不一致であった場合に

、これを不正として検出することが可能である。

[0124] 上述の実施の形態では単一のＣＡＮバス２００で構成されるＣＡＮシステム５００を説明した。以下、複数のＣＡＮシステムをゲートウェイ装置を介して接続した統合システムに拡張する例を説明する。

[0125] 複数のＣＡＮシステムにゲートウェイ装置が介在する状態において、ゲートウェイ装置がメッセージの送信者になる場合がある。

[0126] これは、複数のＣＡＮシステムのうち任意の一つのＣＡＮシステムにおけるＥＣＵからゲートウェイ装置を介して該複数のＣＡＮシステム内の他のＣＡＮシステムにおけるＥＣＵへメッセージを送信する場合である。

[0127] なぜなら、ゲートウェイ装置が一度このメッセージを受信してから該他のＣＡＮシステムへメッセージを送信し直す（転送する）ためであり、他のＣＡＮシステムにおいてはゲートウェイ装置がメッセージの送信者となる。

[0128] そのため、上述した単一のＣＡＮバス２００で構成されるＣＡＮシステム５００のように「自らが送信すべきＩＤのメッセージが他のＥＣＵに送信されていないか監視することで、不正なメッセージ送信を検出」することができなくなる。そこで、ゲートウェイ装置を介して複数のＣＡＮシステムを接続した統合システムでは、ゲートウェイ装置に記憶されているホワイトリストを利用することによって対処させることができる。以下にその詳細を説明する。

[0129] 図２３は、２つのＣＡＮシステムがゲートウェイ装置３００を介して接続された統合システム５００ａの構成例を示す図である。第１ＣＡＮバス２００ａにはＥＣＵ１（１００ａ）、ＥＣＵ２（１００ｂ）及びＥＣＵ３（１００ｃ）が接続されている。第２ＣＡＮバス２００ｂにはＥＣＵ４（１００ｄ）、ＥＣＵ５（１００ｅ）及びＥＣＵ６（１００ｆ）が接続されている。第１ＣＡＮバス２００ａと第２ＣＡＮバス２００ｂの間にゲートウェイ装置３００が接続される。

[0130] ゲートウェイ装置３００は、例えば通信トラフィックの増大を防止するなどのために第１ＣＡＮバス２００ａと第２ＣＡＮバス２００ｂとの間に配置

される。ゲートウェイ装置３００にはホワイトリスト３１０が保持されている。このホワイトリストには、ゲートウェイ装置３００を介して異なるＣＡＮシステムへ転送されることがあらかじめ許可されるメッセージと、当該メッセージの転送方向（「第１ＣＡＮバス２００ａから第２ＣＡＮバス２００ｂへ」または「第２ＣＡＮバス２００ｂから第１ＣＡＮバス２００ａへ」などメッセージの送信方向）と、メッセージのＣＡＮＩＤとが紐づけられて保持（記憶）されている。

[0131] 図２４は、図２３のゲートウェイ装置３００が保持するホワイトリスト３１０の一例を示す。図２４のホワイトリスト３１０には、第１ＣＡＮバス２００ａから第２ＣＡＮバス２００ｂへの転送を許可するメッセージのＣＡＮＩＤが登録されている。ＣＡＮＩＤ＝０ｘ０３及び０ｘ０４のメッセージはＥＣＵ１（１００ａ）で生成されるメッセージである。ＣＡＮＩＤ＝０ｘ１１及び０ｘ１２のメッセージはＥＣＵ２（１００ｂ）で生成されるメッセージである。ＣＡＮＩＤ＝０ｘ２１のメッセージはＥＣＵ３（１００ｃ）で生成されるメッセージである。また、図示する例では、転送方向は全て第１ＣＡＮバス２００ａから第２ＣＡＮバス２００ｂへ向かう方向である（但し、上述のように、各メッセージに対して個別に紐づけられていても良い）。

[0132] ゲートウェイ装置３００は、ホワイトリスト３１０に登録されたＣＡＮＩＤのメッセージを第１ＣＡＮバス２００ａから受信すると第２ＣＡＮバス２００ｂに転送する。具体的にはゲートウェイ装置３００は、第１ＣＡＮバス２００ａに送信された当該ＣＡＮＩＤのメッセージを一度受信し、第２ＣＡＮバス２００ｂに送信し直す。したがって第２ＣＡＮバス２００ｂにおいてはゲートウェイ装置３００が当該メッセージの送信者となる。

[0133] 以下、第２ＣＡＮバス２００ｂに接続された不正なＥＣＵ６（１００ｆ）がＥＣＵ１（１００ａ）になりすまして、ＣＡＮＩＤ＝０ｘ０３のメッセージを送信するケースを考える。このケースは、正常状態においては、ＥＣＵ１（１００ａ）からゲートウェイ装置３００を介してＥＣＵ４（１００ｄ）およびＥＣＵ５（１００ｅ）へメッセージを送信するのが正しいケースであ

る。しかしながら、ＥＣＵ６（１００ｆ）からＥＣＵ４（１００ｄ）およびＥＣＵ５（１００ｅ）へのメッセージ送信は、単一のＣＡＮバスである第２ＣＡＮバス２００ｂにて接続されるシステム内での処理であるため、ＥＣＵ６（１００ｆ）からゲートウェイ装置３００を介してＥＣＵ１（１００ａ）へ送信されることが無い。そこで、ゲートウェイ装置３００がホワイトリストを利用して不正なＥＣＵのなりすましを検出する。以下になりすましの検出処理および検出後の対応処理について、詳細説明する。

[0134] 第１の構成例は、ゲートウェイ装置３００がなりすましを検出した後、ゲートウェイ装置３００が異常対応を行うものである。即ちゲートウェイ装置３００が、ＥＣＵ１００のメッセージ処理部３０における、なりすまし検出機能およびメッセージ送信機能を搭載する例である。

[0135] 図２５は、統合システム５００ａ内の異なるＣＡＮシステム間におけるなりすましを検出する第１の構成例を説明するためのタイミングチャートである。第２ＣＡＮバス２００ｂに接続された不正なＥＣＵがなりすましメッセージを送信すると、ゲートウェイ装置３００が当該なりすましメッセージを受信し、異常を検出する（Ｐ１１）。ゲートウェイ装置３００は異常を検出すると異常対応処理を実行する（Ｐ１２）。例えばホワイトリスト３１０に登録されているＣＡＮＩＤと同一のＣＡＮＩＤのメッセージを、第２ＣＡＮバス２００ｂから受信した場合、異常と判断できる。ゲートウェイ装置３００は異常対応処理として上述の不正通知メッセージを第２ＣＡＮバス２００ｂに送信する。

[0136] なお異常対応処理として正当なデータを含むメインメッセージと、当該メインメッセージに対応するＭＡＣメッセージを送信する処理も考えられる。ただしこの方法では、ゲートウェイ装置３００がＥＣＵ１（１００ａ）、ＥＣＵ２（１００ｂ）及びＥＣＵ３（１００ｃ）から各機能に関する正当なデータを収集する必要がある。したがって異常対応処理としては上述の不正通知メッセージを送信する処理のほうが簡便である。第１の構成例では、ゲートウェイ装置３００がなりすましを検出して異常対応を行うことから即時応

答性が高い。

[0137] 第２の構成例は、ゲートウェイ装置３００がなりすましメッセージを正規の送信ＥＣＵであるＥＣＵ１（１００ａ）が接続された第１ＣＡＮバス２００ａに転送し、当該正規の送信ＥＣＵが異常対応を行うものである。第２の構成例は、ゲートウェイ装置３００が保持するホワイトリスト３１０に登録されている全てのＣＡＮＩＤのメッセージを双方向に転送するように設定することにより実現できる。

[0138] 図２６は、統合システム５００ａ内でなりすましを検出するための第２の構成例を採用する場合におけるホワイトリスト３１０の一例を示す。このホワイトリスト３１０に登録されているＣＡＮＩＤのメッセージは、第１ＣＡＮバス２００ａと第２ＣＡＮバス２００ｂ間で双方向に転送される。ただし通常は、第２ＣＡＮバス２００ｂに接続されたＥＣＵから当該ＣＡＮＩＤのメッセージが送信されることはないため、第２ＣＡＮバス２００ｂから第１ＣＡＮバス２００ａへの転送処理は発生しない。第２ＣＡＮバス２００ｂに接続されたＥＣＵから不正なりすましメッセージが送信されたときのみ、第２ＣＡＮバス２００ｂから第１ＣＡＮバス２００ａへの転送処理が発生する。

[0139] 図２７は、統合システム５００ａ内の異なるＣＡＮシステム間におけるなりすましを検出する第２の構成例を説明するためのタイミングチャートである。第２ＣＡＮバス２００ｂに接続された不正なＥＣＵがなりすましメッセージを送信すると、ゲートウェイ装置３００は当該なりすましメッセージを受信し、第１ＣＡＮバス２００ａに転送する（Ｐ２１）。正規の送信ＥＣＵであるＥＣＵ１（１００ａ）は当該なりすましメッセージを検出することにより異常を検出して（Ｐ２２）、異常対応処理を実行する（Ｐ２３）。ＥＣＵ１（１００ａ）は、正当なデータを含むメッセージなどの異常対応メッセージを送信し、ゲートウェイ装置３００は当該異常対応メッセージを受信し、第２ＣＡＮバス２００ｂに転送する（Ｐ２４）。第２の構成例では、ホワイトリスト３１０を改良するだけで済むためゲートウェイ装置３００の機能

追加を最低限に抑えることができる。

[0140] 第３の構成例は、ゲートウェイ装置３００がなりすましを検出し、正規の送信ＥＣＵであるＥＣＵ１（１００ａ）に通知し、当該正規の送信ＥＣＵが異常対応を行うものである。ゲートウェイ装置３００はＥＣＵ１００のメッセージ処理部３０における、なりすまし検出機能を搭載する。またゲートウェイ装置３００は図２３のホワイトリスト３１０を保持することを前提とする。

[0141] 図２８は、統合システム５００ａ内の異なるＣＡＮシステム間におけるなりすましを検出する第３の構成例を説明するためのタイミングチャートである。第２ＣＡＮバス２００ｂに接続された不正なＥＣＵがなりすましメッセージを送信すると、ゲートウェイ装置３００は当該メッセージを受信し、異常を検出する（Ｐ３１）。ゲートウェイ装置３００は異常を検出すると、なりすまし検出通知を正規の送信ＥＣＵであるＥＣＵ１（１００ａ）に送信する。このなりすまし検出通知は、ゲートウェイ装置３００で新たに生成されるメッセージである。当該メッセージは、ＣＡＮメッセージのフォーマットに準拠したメッセージである。

[0142] ＥＣＵ１（１００ａ）は当該なりすまし検出通知を受信すると異常対応処理を実行する（Ｐ３２）。ＥＣＵ１（１００ａ）は、正当なデータを含むメッセージなどの異常対応メッセージを送信し、ゲートウェイ装置３００は当該異常対応メッセージを受信し、第２ＣＡＮバス２００ｂに転送する（Ｐ３３）。第３の構成例では、ホワイトリスト３１０を書き換えずに、正規の送信ＥＣＵに異常対応処理を委ねることができる。

[0143] 本発明の一態様の概要は、次の通りである。本発明のある態様は、送信装置である。この装置は、検出部と、生成部と、送信部とを有する。検出部は、他の送信装置によりネットワークへブロードキャスト送信されたメッセージの通信規則が、本送信装置が保持する当該メッセージの通信規則と一致するか否かを検出する。生成部は、異常を検出したことを通知するための異常通知メッセージを生成する。送信部は、生成部が生成したメッセージをネッ

トワークへブロードキャスト送信する。検出部が、他の送信装置によりネットワークへブロードキャスト送信されたメッセージの通信規則と本送信装置がネットワークへブロードキャスト送信するメッセージの通信規則との一致を検出した場合、生成部は、異常通知メッセージを生成する。そして、送信部は、この異常通知メッセージをネットワークへブロードキャスト送信する。

[0144] この態様によると、自己が保持するメッセージの通信規則と一致する通信規則のメッセージを受信すると不正通知メッセージを送信することにより、不正発生をネットワークに接続された他の装置に通知して他の装置のセキュリティを向上させることができる。またこの不正なメッセージの検出処理と不正通知メッセージの送信処理は軽負荷な処理であり、送信装置の負荷の増大を抑えることができる。

[0145] 本発明の別の態様もまた、送信装置である。この装置は、検出部と、生成部と、送信部とを有する。検出部は、他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置がネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致するか否かを検出する。生成部は、異常を検出したことを通知するための異常通知メッセージを生成する。送信部は、生成部が生成したメッセージをネットワークへブロードキャスト送信する。検出部が、他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報と本送信装置がネットワークへブロードキャスト送信するメッセージに含めるべき識別情報との一致を検出した場合、生成部は、異常通知メッセージを生成する。そして、送信部は、この異常通知メッセージをネットワークへブロードキャスト送信する。「識別情報」はＣＡＮＩＤであってもよい。「検出部」は図１７のなりすまし検出部３４であってもよい。「生成部」は図１７の不正通知メッセージ生成部３６ａであってもよく、図１３のメインメッセージ生成部でもよく、図４のＭＡＣメッセージ生成部３８であってもよい。「送信部」は図３の送受信部５０であってもよい。

[0146] この態様によると、自己が送信するメッセージに含めるべき識別情報を含むメッセージを受信すると不正通知メッセージを送信することにより、不正発生をネットワークに接続された他の装置に通知して他の装置のセキュリティを向上させることができる。またこの不正なメッセージの検出処理と不正通知メッセージの送信処理は軽負荷な処理であり、送信装置の負荷の増大を抑えることができる。

[0147] 本発明の別の態様もまた、送信装置である。この装置は、第１生成部と、第２生成部と、送信部とを有する。第１生成部は、他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置がネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報と、当該識別情報で特定される処理対象の通知事項に関する正当なデータを含むメッセージを生成する。第２生成部は、正当なデータを少なくとも対象としたメッセージ認証コードを生成する。送信部は、第１生成部において生成したメッセージと、第２生成部において生成したメッセージ認証コードをネットワークへブロードキャスト送信する。「識別情報」はＣＡＮＩＤであってもよい。「第１生成部」は図４のメインメッセージ生成部３６であってもよい。「第２生成部」は図４のＭＡＣ生成部３５であってもよい。「送信部」は図３の送受信部５０であってもよい。

[0148] この態様によると、自己が送信するメッセージに含めるべき識別情報を含むメッセージを受信すると、正当なデータを含むメッセージとＭＡＣを送信することにより、不正発生をネットワークに接続された他の装置に通知して他の装置のセキュリティを向上させることができる。またそれ以外の場合は、ＭＡＣを生成および送信しないことにより、送信装置の負荷の増大を抑制できる。

[0149] 本発明の別の態様もまた、送信装置である。この装置は、メッセージ生成部と、送信部とを有する。メッセージ生成部は、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含む

メッセージを生成する。送信部は、メッセージ生成部において生成したメッセージをネットワークへブロードキャスト送信する。メッセージ生成部は、他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置がネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報を含むメッセージが不正なメッセージであることを通知するための不正通知メッセージを、通常のメッセージと同じフォーマットで生成する。そして、送信部は、この不正通知メッセージをネットワークへブロードキャスト送信する。「識別情報」はＣＡＮＩＤであってもよい。「メッセージ生成部」は図１７の不正通知メッセージ生成部３６ａであってもよい。「送信部」は図３の送受信部５０であってもよい。

[0150] この態様によると、自己が送信するメッセージに含めるべき識別情報を含むメッセージを受信すると不正通知メッセージを送信することにより、不正発生をネットワークに接続された他の装置に通知して他の装置のセキュリティを向上させることができる。またこの不正なメッセージの検出処理と不正通知メッセージの送信処理は軽負荷な処理であり、送信装置の負荷の増大を抑えることができる。

[0151] また、送信装置は識別情報を少なくとも対象としたメッセージ認証コードを生成するメッセージ認証コード生成部をさらに有してもよい。メッセージ生成部は、メッセージ認証コード生成部において生成したメッセージ認証コードを不正通知メッセージに含めてもよい。「メッセージ認証コード生成部」は図１７のＭＡＣ生成部３５であってもよい。

[0152] この態様によると、不正通知メッセージにＭＡＣを含めることにより不正通知メッセージの信頼性を向上させることができる。

[0153] 本発明のさらに別の態様は、受信装置である。この装置は、受信部と、処理部とを有する。受信部は、ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する。処理部は、受信部において受信したメッセージを処

理する。受信部が、ネットワークからメッセージを認証するためのメッセージ認証コードを受信すると、処理部は、メッセージに含まれるデータを、メッセージ認証コードを用いた検証なしに有効とするモードから、メッセージ認証コードを用いた検証に成功したことを条件として有効とするモードに切り替える。「識別情報」はＣＡＮＩＤであってもよい。「受信部」は図３の送受信部５０であってもよい。「処理部」は図７のメッセージ処理部３０であってもよい。

[0154] この態様によると、ＭＡＣの受信に起因してＭＡＣを用いた検証なしに有効とするモードから、ＭＡＣを用いた検証に成功したことを条件として有効とするモードに切り替えることにより、受信装置の負荷の増大を抑制しつつセキュリティを向上させることができる。

[0155] 本発明のさらに別の態様もまた、受信装置である。この装置は、受信部と、処理部とを有する。受信部は、ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する。処理部は、受信部において受信したメッセージを処理する。受信部が、ネットワークから識別情報を含むメッセージが不正なメッセージであることを通知するためのメッセージであり、通常のメッセージと同じフォーマットで生成された不正通知メッセージを受信すると、処理部は、識別情報を含むメッセージに含まれるデータを無効とするモードに切り替える。「識別情報」はＣＡＮＩＤであってもよい。「受信部」は図３の送受信部５０であってもよい。「処理部」は図２０のメッセージ処理部３０であってもよい。

[0156] この態様によると、不正通知メッセージの受信に起因して、不正通知メッセージで通知された識別情報を含むメッセージに含まれるデータを無効とするモードに切り替えることにより、受信装置の負荷の増大を抑制しつつセキュリティを向上させることができる。

[0157] なお処理部は、不正通知メッセージに、識別情報を少なくとも対象としたメッセージ認証コードが含まれている場合、当該メッセージ認証コードを用

いた検証に成功したことを条件として、識別情報を含むメッセージに含まれるデータを無効とするモードに切り替えてもよい。

[0158] この態様によると、ＭＡＣの検証に成功したことを条件として、不正通知メッセージで通知された識別情報を含むメッセージに含まれるデータを無効とするモードに切り替えることにより、モード切替処理の信頼性を向上させることができる。

[0159] 本発明のさらに別の態様もまた、受信装置である。この装置は、受信部と、処理部とを有する。受信部は、ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する。処理部は、受信部において受信したメッセージを処理する。受信部が、ネットワークから識別情報を含むメッセージが不正なメッセージであることを通知するためのメッセージであり、通常のメッセージと同じフォーマットで生成された不正通知メッセージを受信すると、処理部は、受信部が受信した不正通知メッセージに、識別情報を少なくとも対象としたメッセージ認証コードが含まれている場合、メッセージ認証コードを用いた検証に成功したことを条件として、識別情報を含むメッセージに含まれるデータを、メッセージ認証コードの検証なしに有効とするモードから、メッセージ認証をコードを用いた検証に成功したことを条件として有効とするモードに切り替える。「識別情報」はＣＡＮＩＤであってもよい。「受信部」は図３の送受信部５０であってもよい。「処理部」は図２０のメッセージ処理部３０であってもよい。

[0160] この態様によると、不正通知メッセージを受信した際、ＭＡＣの検証に成功したことを条件として、ＭＡＣを含むメッセージに含まれるデータを、ＭＡＣの検証なしに有効とするモードから、ＭＡＣの検証に成功したことを条件として有効とするモードに切り替えることにより、受信装置の負荷の増大を抑制しつつセキュリティを向上させることができる。

[0161] 本発明のさらに別の態様は、送信方法である。この方法は、第１ステップと、第２ステップと、第３ステップとを有する。第１ステップでは、他の送

信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置がネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報と、当該識別情報で特定される処理対象の通知事項に関する正当なデータを含むメッセージを生成する。第２ステップでは、正当なデータを少なくとも対象としたメッセージ認証コードを生成する。第３ステップでは、第１ステップにおいて生成したメッセージと、第２ステップにおいて生成したメッセージ認証コードとをネットワークへブロードキャスト送信する。

[0162] この態様によると、自己が送信するメッセージに含めるべき識別情報を含むメッセージを受信すると、正当なデータを含むメッセージとＭＡＣを送信することにより、不正発生をネットワークに接続された他の装置に通知して他の装置のセキュリティを向上させることができる。またそれ以外の場合は、ＭＡＣを生成および送信しないことにより、送信装置の負荷の増大を抑制できる。

[0163] 本発明のさらに別の態様もまた、送信方法である。この方法は、第１ステップと、第２ステップとを有する。第１ステップでは、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを生成する。第２ステップでは、第１ステップにおいて生成したメッセージをネットワークへブロードキャスト送信する。第１ステップでは、他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置がネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報を含むメッセージが不正なメッセージであることを通知するための不正通知メッセージを、通常のメッセージと同じフォーマットで生成する。第２ステップでは、不正通知メッセージをネットワークへブロードキャスト送信する。

[0164] この態様によると、自己が送信するメッセージに含めるべき識別情報を含むメッセージを受信すると不正通知メッセージを送信することにより、不正

発生をネットワークに接続された他の装置に通知して他の装置のセキュリティを向上させることができる。またこの不正なメッセージの検出処理と不正通知メッセージの送信処理は軽負荷な処理であり、送信装置の負荷の増大を抑えることができる。

[0165] 本発明のさらに別の態様は、受信方法である。この方法は、第１ステップと、第２ステップとを有する。第１ステップでは、ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する。第２ステップでは、第１ステップにおいて受信したメッセージを処理する。第１ステップで、ネットワークからメッセージに含まれる識別情報を少なくとも対象としたメッセージ認証コードを受信すると、第２ステップは、メッセージに含まれるデータを、メッセージ認証コードを用いた検証なしに有効とするモードから、メッセージ認証コードを用いた検証に成功したことを条件として有効とするモードに切り替える。

[0166] この態様によると、ＭＡＣの受信に起因してＭＡＣを用いた検証なしに有効とするモードから、ＭＡＣを用いた検証に成功したことを条件として有効とするモードに切り替えることにより、受信装置の負荷の増大を抑制しつつセキュリティを向上させることができる。

[0167] 本発明のさらに別の態様もまた、受信方法である。この方法は、第１ステップと、第２ステップとを有する。第１ステップでは、ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する。第２ステップでは、第１ステップにおいて受信したメッセージを処理する。第１ステップで、ネットワークから識別情報を含むメッセージが不正なメッセージであることを通知するためのメッセージであり、通常のメッセージと同じフォーマットで生成された不正通知メッセージを受信すると、第２ステップでは、識別情報を含むメッセージに含まれるデータを無効とするモードに切り替える。

[0168] この態様によると、不正通知メッセージの受信に起因して、不正通知メッ

セージで通知された識別情報を含むメッセージに含まれるデータを無効とするモードに切り替えることにより、受信装置の負荷の増大を抑制しつつセキュリティを向上させることができる。

産業上の利用可能性

[0169] 本発明は、ＣＡＮに利用可能である。

符号の説明

[0170] １０　アプリケーション処理部
３０　メッセージ処理部
３１　メッセージ解析部
３２　ＣＡＮＩＤ抽出部
３４　なりすまし検出部
３５　ＭＡＣ生成部
３５ａ　共通鍵
３６　メインメッセージ生成部
３６ａ　不正通知メッセージ生成部
３７　データフィールド抽出部
３８　ＭＡＣメッセージ生成部
３９　カウンタ値記憶部
４１　メッセージ解析部
４２　ＣＡＮＩＤ抽出部
４３　データフィールド抽出部
４４　モード切替部
４５　ＭＡＣ生成部
４５ａ　共通鍵
４６　ＭＡＣ比較部
４７　データ受渡部
４８　メインメッセージ一時保持部
４８ａ　ＭＡＣメッセージ一時保持部

４９　　カウンタ値記憶部

５０　　送受信部

１００，１００ａ，１００ｂ，１００ｃ，１００ｄ，１００ｅ，１００ｆ　ＥＣＵ

２００　　ＣＡＮバス

２００ａ　　第１ＣＡＮバス

２００ｂ　　第２ＣＡＮバス

３００　　ゲートウェイ装置

３１０　　ホワイトリスト

５００　　ＣＡＮシステム

５００ａ　　統合システム

請求の範囲

[請求項1] 他の送信装置によりネットワークへブロードキャスト送信されたメッセージの通信規則が、本送信装置が保持する当該メッセージの通信規則と一致するか否かを検出する検出部と、

異常を検出したことを通知するための異常通知メッセージを生成する生成部と、

前記生成部が生成したメッセージを前記ネットワークへブロードキャスト送信する送信部と、を備え、

前記検出部が、他の送信装置によりネットワークへブロードキャスト送信されたメッセージの通信規則と本送信装置が前記ネットワークへブロードキャスト送信するメッセージの通信規則との一致を検出した場合、前記生成部が、前記異常通知メッセージを生成し、前記送信部が、前記異常通知メッセージを前記ネットワークへブロードキャスト送信する、

送信装置。

[請求項2] 他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置が前記ネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致するか否かを検出する検出部と、

異常を検出したことを通知するための異常通知メッセージを生成する生成部と、

前記生成部が生成したメッセージを前記ネットワークへブロードキャスト送信する送信部と、を備え、

前記検出部が、他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報と本送信装置が前記ネットワークへブロードキャスト送信するメッセージに含めるべき識別情報との一致を検出した場合、前記生成部が、前記異常通知メッセージを生成し、前記送信部が、前記異常通知メッセージを前記ネットワーク

へブロードキャスト送信する、

送信装置。

[請求項3] 他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置が前記ネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報と、当該識別情報で特定される処理対象の通知事項に関する正当なデータを含むメッセージを生成する第１生成部と、

前記正当なデータを少なくとも対象としたメッセージ認証コードを生成する第２生成部と、

前記第１生成部において生成したメッセージと、前記第２生成部において生成したメッセージ認証コードとを前記ネットワークへブロードキャスト送信する送信部と、

を備える、

送信装置。

[請求項4] 特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを生成するメッセージ生成部と、

前記メッセージ生成部において生成したメッセージをネットワークへブロードキャスト送信する送信部と、を備え、

前記メッセージ生成部は、他の送信装置により前記ネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置が前記ネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報を含むメッセージが不正なメッセージであることを通知するための不正通知メッセージを、通常のメッセージと同じフォーマットで生成し、

前記送信部は、前記不正通知メッセージを前記ネットワークへブロードキャスト送信する、

送信装置。

[請求項5] 前記識別情報を少なくとも対象としたメッセージ認証コードを生成するメッセージ認証コード生成部を、さらに備え、
前記メッセージ生成部は、前記メッセージ認証コード生成部において生成したメッセージ認証コードを前記不正通知メッセージに含める、請求項４に記載の送信装置。

[請求項6] ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する受信部と、
前記受信部において受信したメッセージを処理する処理部と、を備え、
前記受信部は、前記ネットワークから前記メッセージを認証するためのメッセージ認証コードを受信し、
前記受信部が前記メッセージ認証コードを受信すると、前記処理部は、メッセージ認証コードを用いた検証なしに前記メッセージに含まれるデータを有効とするモードから、メッセージ認証コードを用いた検証に成功したことを条件として前記メッセージに含まれるデータを有効とするモードへ切り替える、
受信装置。

[請求項7] ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する受信部と、
前記受信部において受信したメッセージを処理する処理部と、を備え、
前記受信部は、通常のメッセージと同じフォーマットであり前記識別情報を含むメッセージが不正なメッセージであることを通知するための不正通知メッセージを前記ネットワークから受信し、
前記処理部は、前記受信部が前記不正通知メッセージを受信すると、前記識別情報を含むメッセージに含まれるデータを無効とするモード

に切り替える、

受信装置。

[請求項8] 前記処理部は、前記不正通知メッセージに、前記識別情報を少なくとも対象としたメッセージ認証コードが含まれている場合、当該メッセージ認証コードを用いた検証に成功したことを条件として、前記識別情報を含むメッセージに含まれるデータを無効とするモードに切り替える、

請求項７に記載の受信装置。

[請求項9] ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する受信部と、

前記受信部において受信したメッセージを処理する処理部と、を備え、

前記受信部は、前記ネットワークから前記識別情報を含むメッセージが不正なメッセージであることを通知するためのメッセージであり、通常のメッセージと同じフォーマットで生成された不正通知メッセージを受信し、

前記処理部は、前記受信部が受信した前記不正通知メッセージに、前記識別情報を少なくとも対象としたメッセージ認証コードが含まれている場合、前記メッセージ認証コードを用いた検証に成功したことを条件として前記識別情報を含むメッセージに含まれるデータをメッセージ認証コードの検証なしに有効とするモードから、メッセージ認証コードを用いた検証に成功したことを条件として前記識別情報を含むメッセージに含まれるデータを有効とするモードへ切り替える、

受信装置。

[請求項10] 他の送信装置によりネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置が前記ネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場

合、当該識別情報と、当該識別情報で特定される処理対象の通知事項に関する正当なデータを含むメッセージを生成する第１ステップと、

前記正当なデータを少なくとも対象としたメッセージ認証コードを生成する第２ステップと、

前記第１ステップにおいて生成したメッセージと、前記第２ステップにおいて生成したメッセージ認証コードを前記ネットワークへブロードキャスト送信する第３ステップと、を備えた、

送信方法。

[請求項11] 特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを生成する第１ステップと、

前記第１ステップにおいて生成したメッセージをネットワークへブロードキャスト送信する第２ステップと、を備え、

前記第１ステップでは、他の送信装置により前記ネットワークへブロードキャスト送信されたメッセージに含まれる識別情報が、本送信装置が前記ネットワークへブロードキャスト送信するメッセージに含めるべき識別情報と一致する場合、当該識別情報を含むメッセージが不正なメッセージであることを通知するための不正通知メッセージを、通常のメッセージと同じフォーマットで生成し、

前記第２ステップでは、前記不正通知メッセージを前記ネットワークへブロードキャスト送信する、

送信方法。

[請求項12] ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する第１ステップと、

前記第１ステップにおいて受信したメッセージを処理する第２ステップと、を備え、

前記第１ステップは、前記ネットワークから前記メッセージに含まれ

る識別情報を少なくとも対象としたメッセージ認証コードを受信し、

前記第２ステップは、前記メッセージ認証コードが受信されると前記メッセージに含まれるデータを、メッセージ認証コードを用いた検証なしに有効とするモードから、メッセージ認証コードを用いた検証に成功したことを条件として有効とするモードに切り替える、

受信方法。

[請求項13] ネットワークから、特定の処理対象の特定の通知事項に関連づけられた識別情報および当該通知事項に関するデータを含むメッセージを受信する第１ステップと、

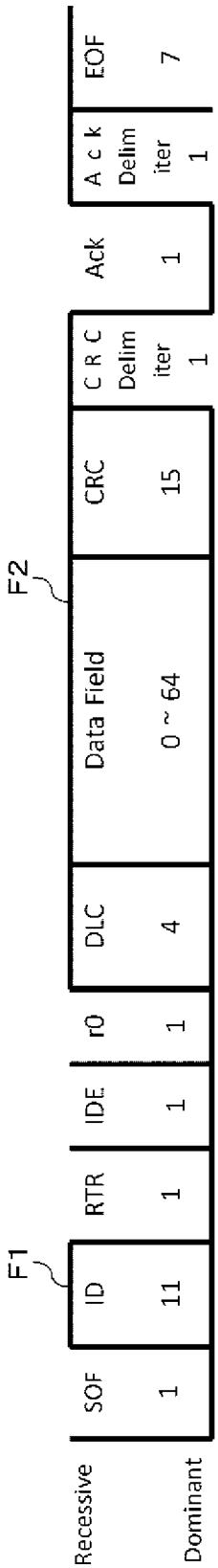
前記第１ステップにおいて受信したメッセージを処理する第２ステップと、を備え、

前記第１ステップは、前記ネットワークから前記識別情報を含むメッセージが不正なメッセージであることを通知するためのメッセージであり、通常のメッセージと同じフォーマットで生成された不正通知メッセージを受信し、

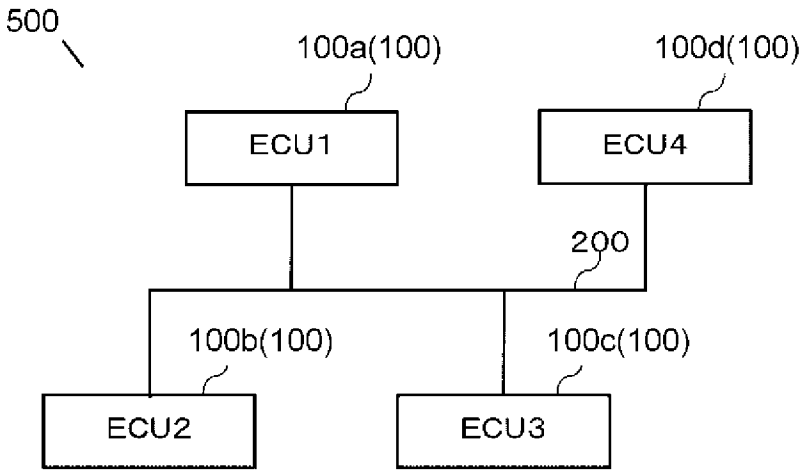
前記第２ステップは、前記不正通知メッセージが受信されると、前記識別情報を含むメッセージに含まれるデータを無効とするモードに切り替える、

受信方法。

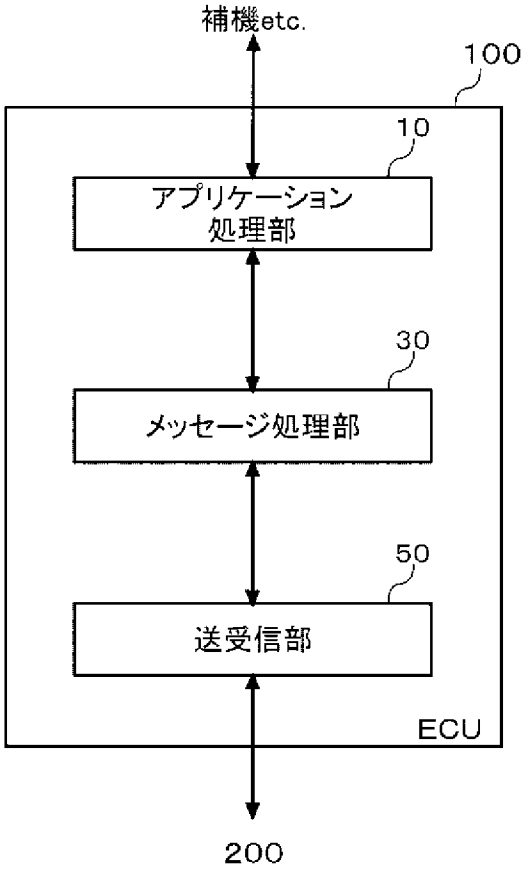
[図1]


F1
F2
SOF
ID
RTR
IDE
r0
DLC
Data Field
CRC
CRC Delim iter
Ack
Ack Delim iter
EOF
1
11
1
1
1
4
0 ~ 64
15
1
1
7
Recessive
Dominant

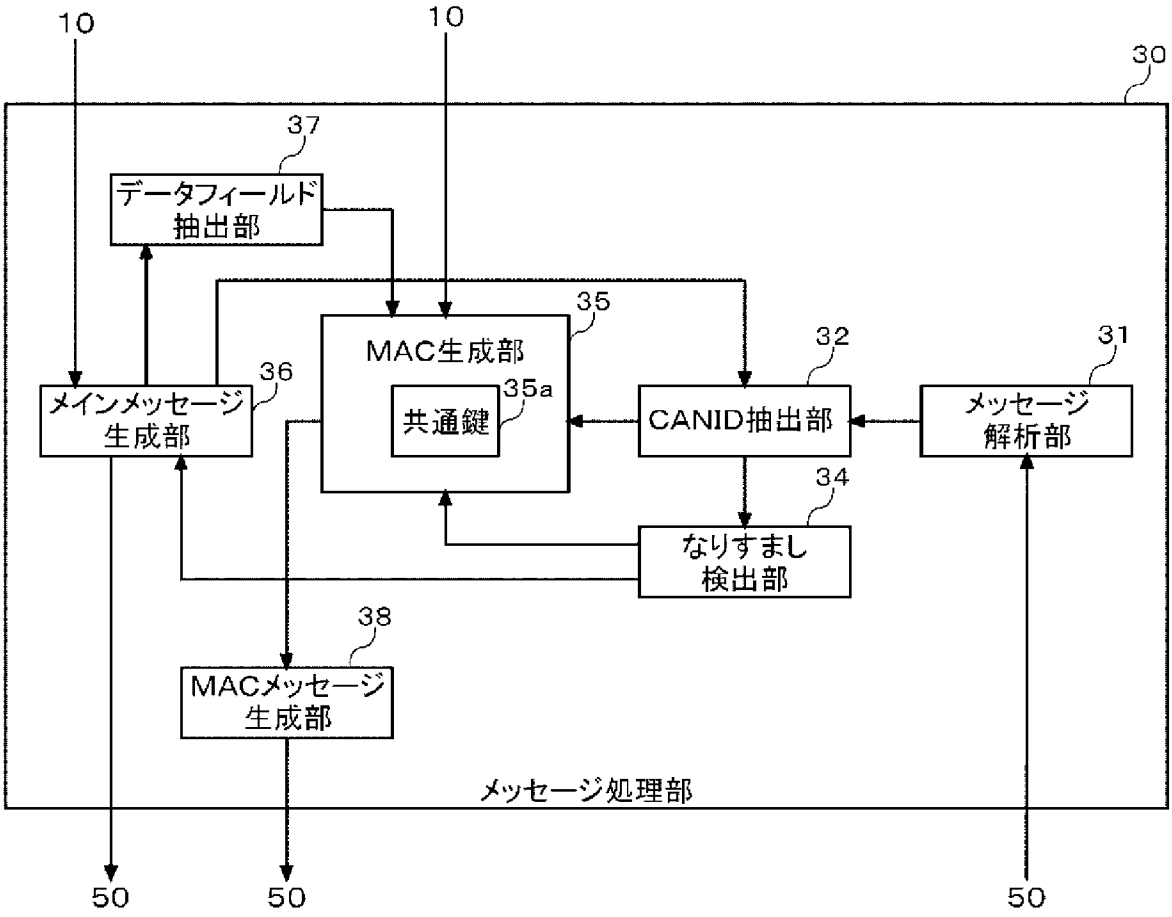
[図2]


500
100a(100)
100d(100)
ECU1
ECU4
200
100b(100)
100c(100)
ECU2
ECU3

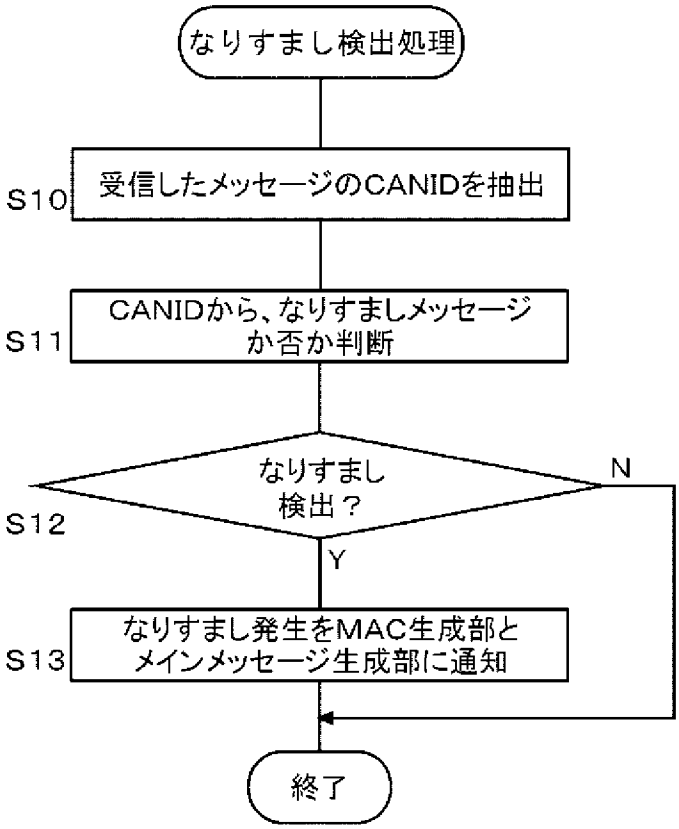
[図3]


補機etc.
100
10
アプリケーション
処理部
30
メッセージ処理部
50
送受信部
ECU
200

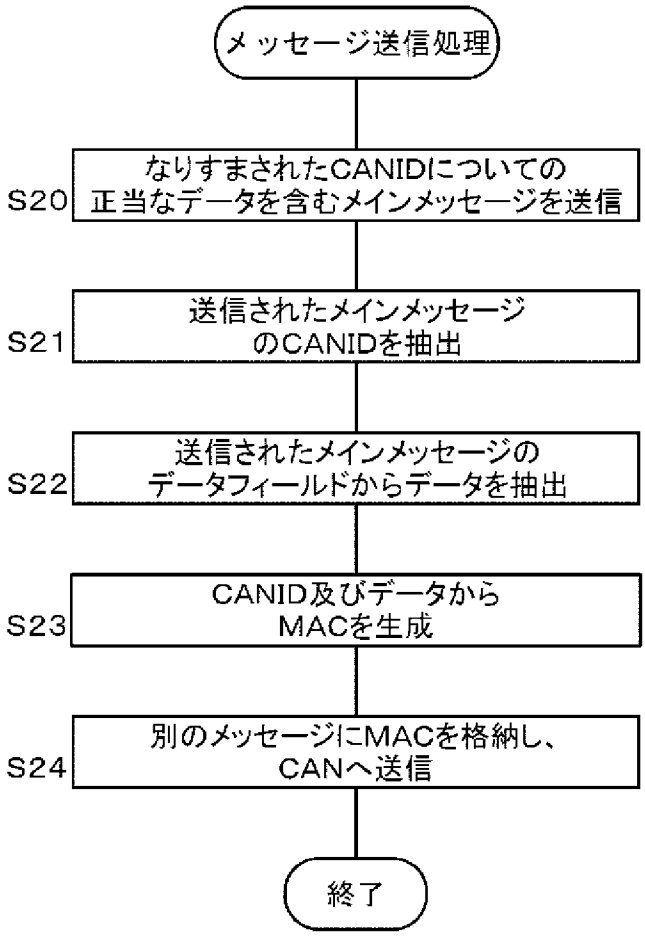
[図4]


10
10
30
37
データフィールド
抽出部
35
MAC生成部
32
31
36
メインメッセージ
生成部
35a
共通鍵
CANID抽出部
メッセージ
解析部
34
なりすまし
検出部
38
MACメッセージ
生成部
メッセージ処理部
50
50
50

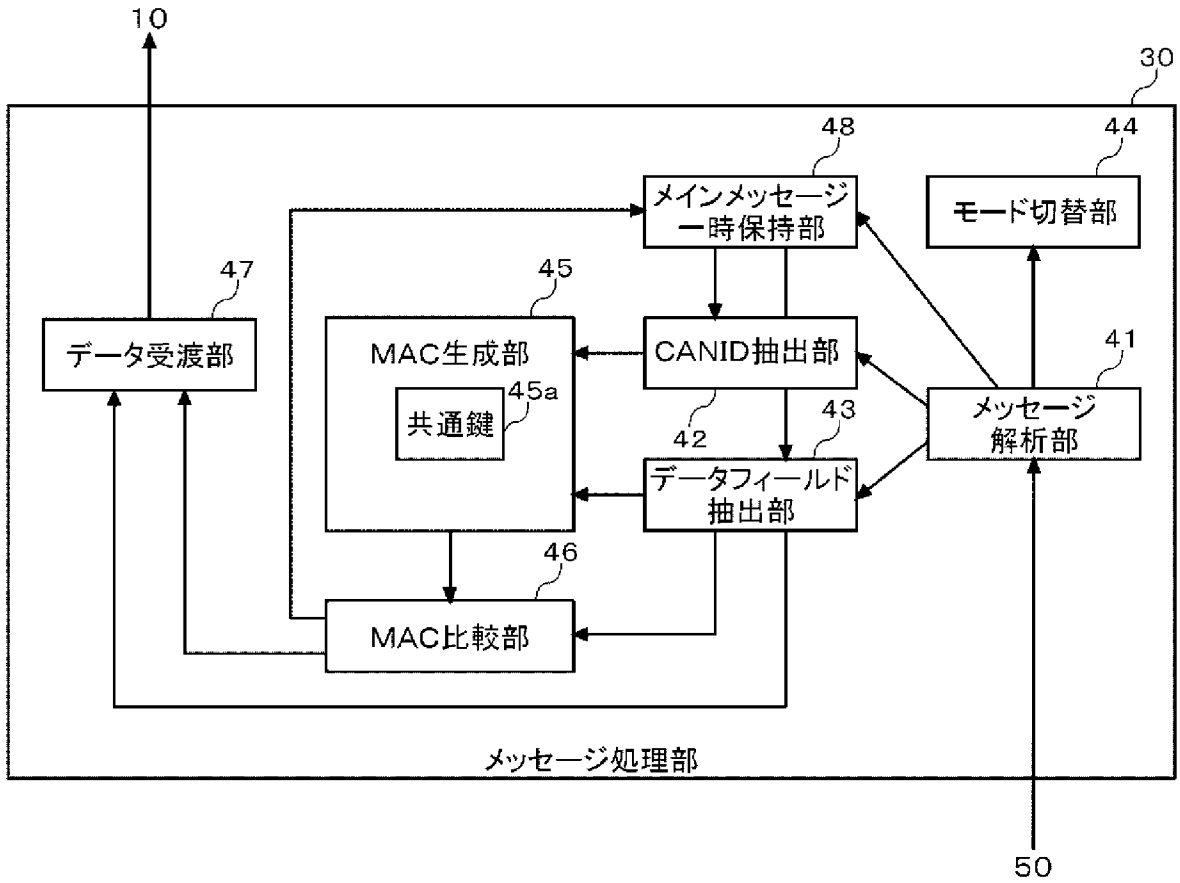
[図5]


なりすまし検出処理
S10
受信したメッセージのCANIDを抽出
S11
CANIDから、なりすましメッセージ
か否か判断
S12
なりすまし
検出？
N
Y
S13
なりすまし発生をMAC生成部と
メインメッセージ生成部に通知
終了

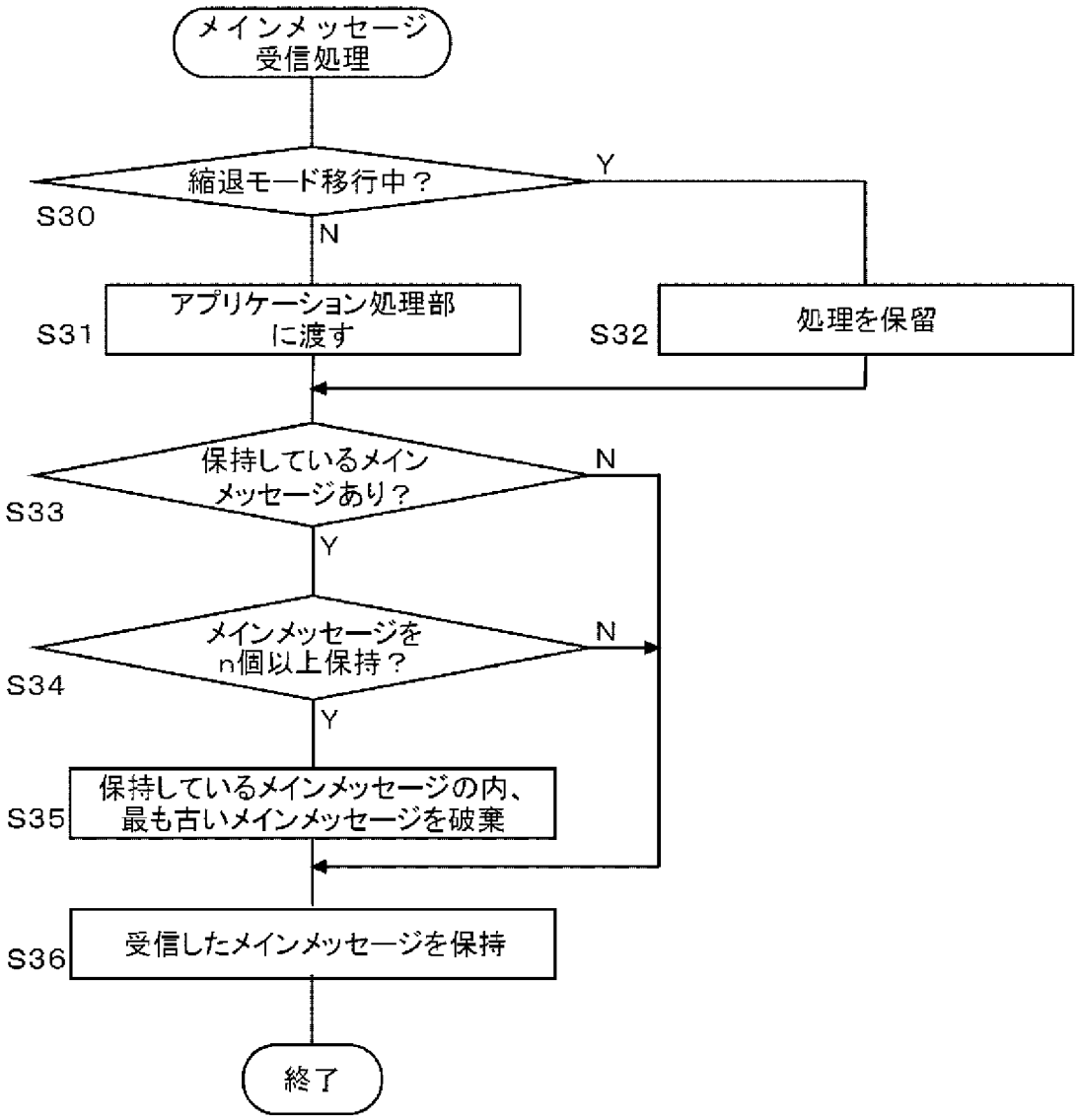
[図6]


メッセージ送信処理
S20
なりすまされたCANIDについての
正当なデータを含むメインメッセージを送信
S21
送信されたメインメッセージ
のCANIDを抽出
S22
送信されたメインメッセージの
データフィールドからデータを抽出
S23
CANID及びデータから
MACを生成
S24
別のメッセージにMACを格納し、
CANへ送信
終了

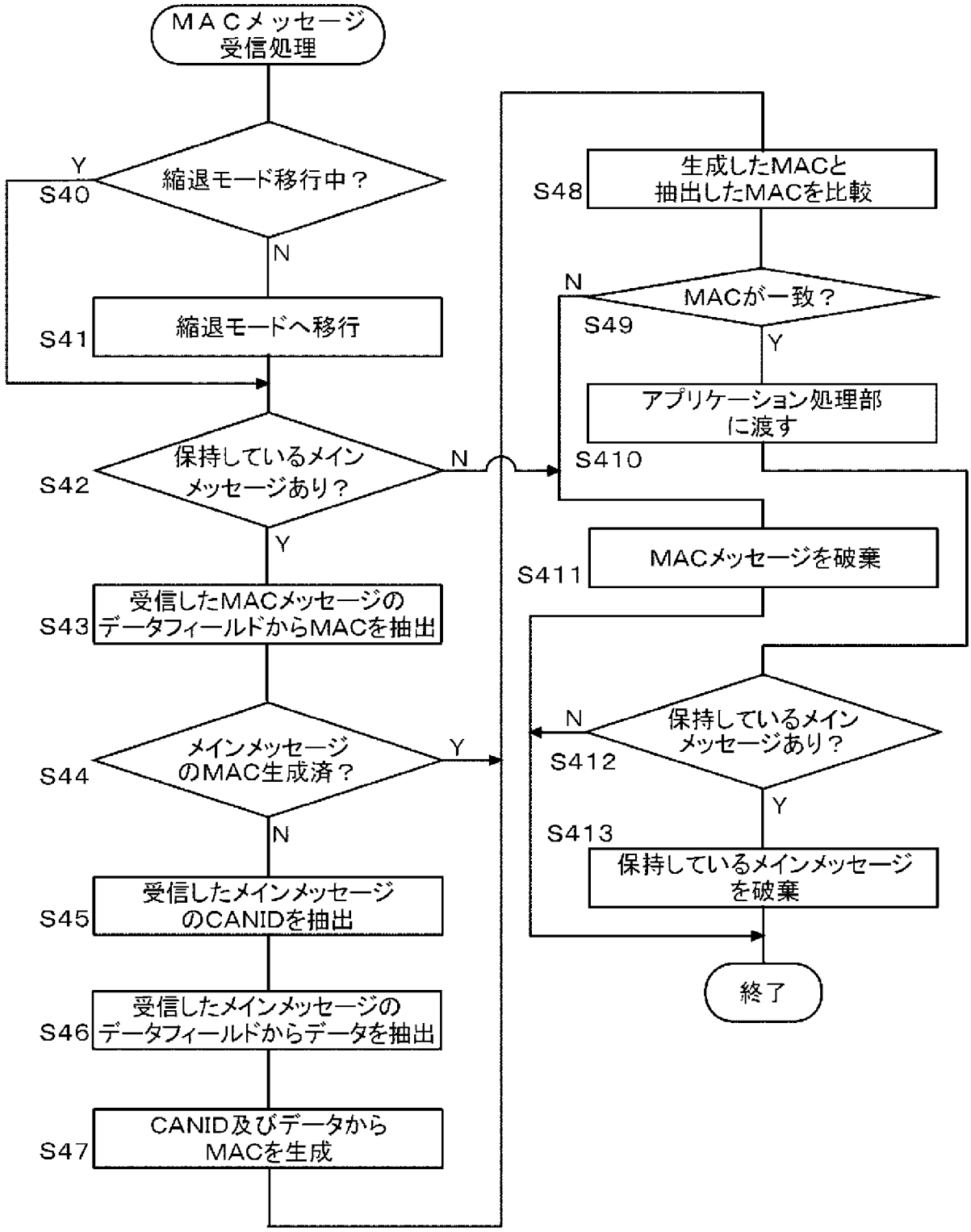
[図7]


10
30
48
44
メインメッセージ一時保持部
モード切替部
47
45
データ受渡部
MAC生成部
CANID抽出部
41
共通鍵
45a
42
43
メッセージ解析部
データフィールド抽出部
46
MAC比較部
メッセージ処理部
50

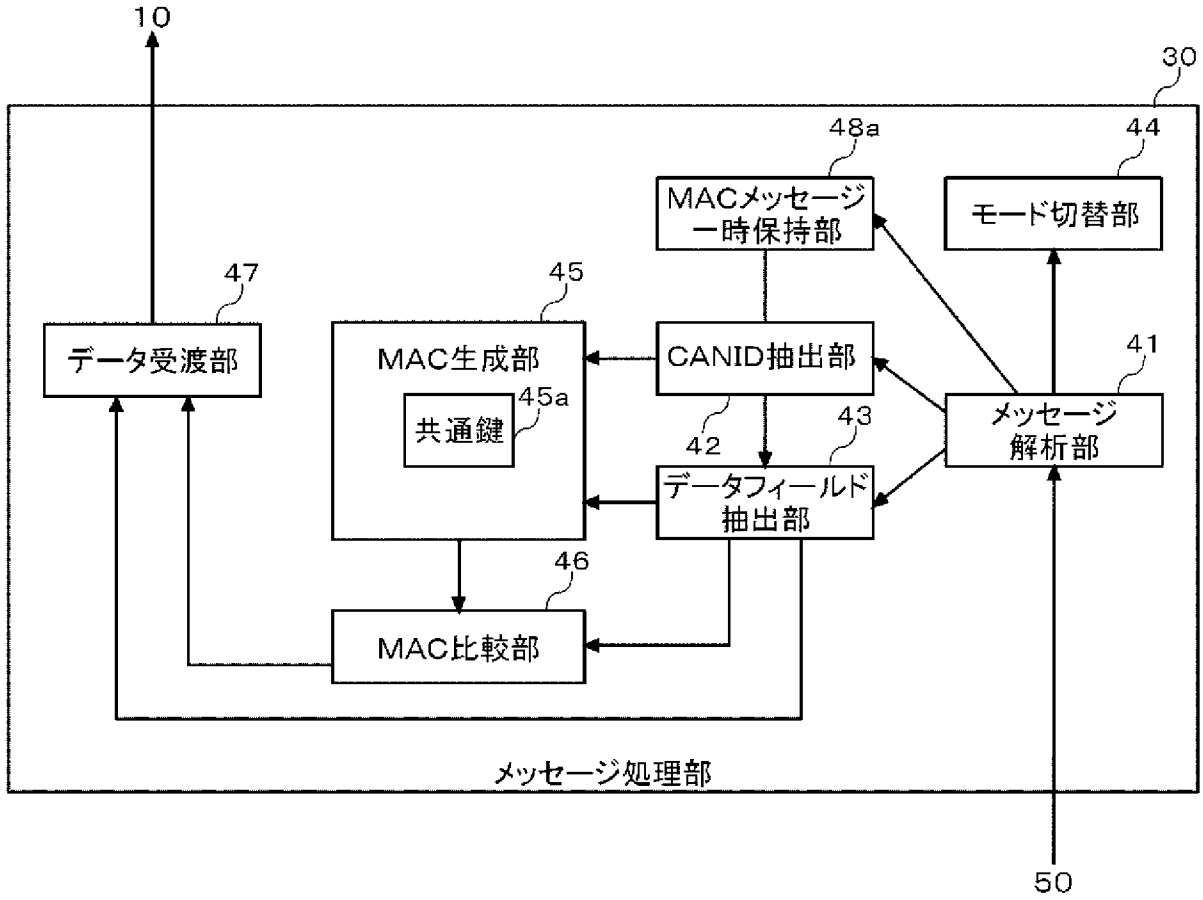
[図8]


メインメッセージ
受信処理
縮退モード移行中？
S30
Y
N
アプリケーション処理部
に渡す
S31
処理を保留
S32
保持しているメイン
メッセージあり？
S33
N
Y
メインメッセージを
n個以上保持？
S34
N
Y
保持しているメインメッセージの内、
最も古いメインメッセージを破棄
S35
受信したメインメッセージを保持
S36
終了

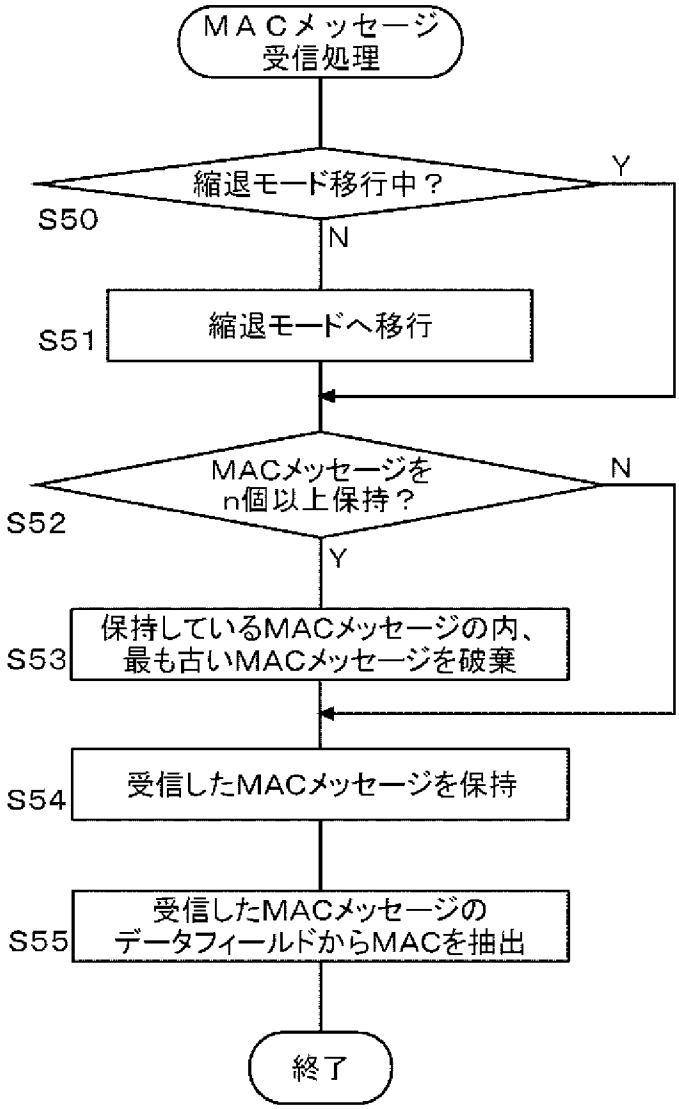
[図9]


MACメッセージ
受信処理
S40
縮退モード移行中？
Y
N
S41
縮退モードへ移行
S42
保持しているメイン
メッセージあり？
N
Y
S43
受信したMACメッセージの
データフィールドからMACを抽出
S44
メインメッセージ
のMAC生成済？
Y
N
S45
受信したメインメッセージ
のCANIDを抽出
S46
受信したメインメッセージの
データフィールドからデータを抽出
S47
CANID及びデータから
MACを生成
S48
生成したMACと
抽出したMACを比較
S49
MACが一致？
N
Y
S410
アプリケーション処理部
に渡す
S411
MACメッセージを破棄
S412
保持しているメイン
メッセージあり？
N
Y
S413
保持しているメインメッセージ
を破棄
終了

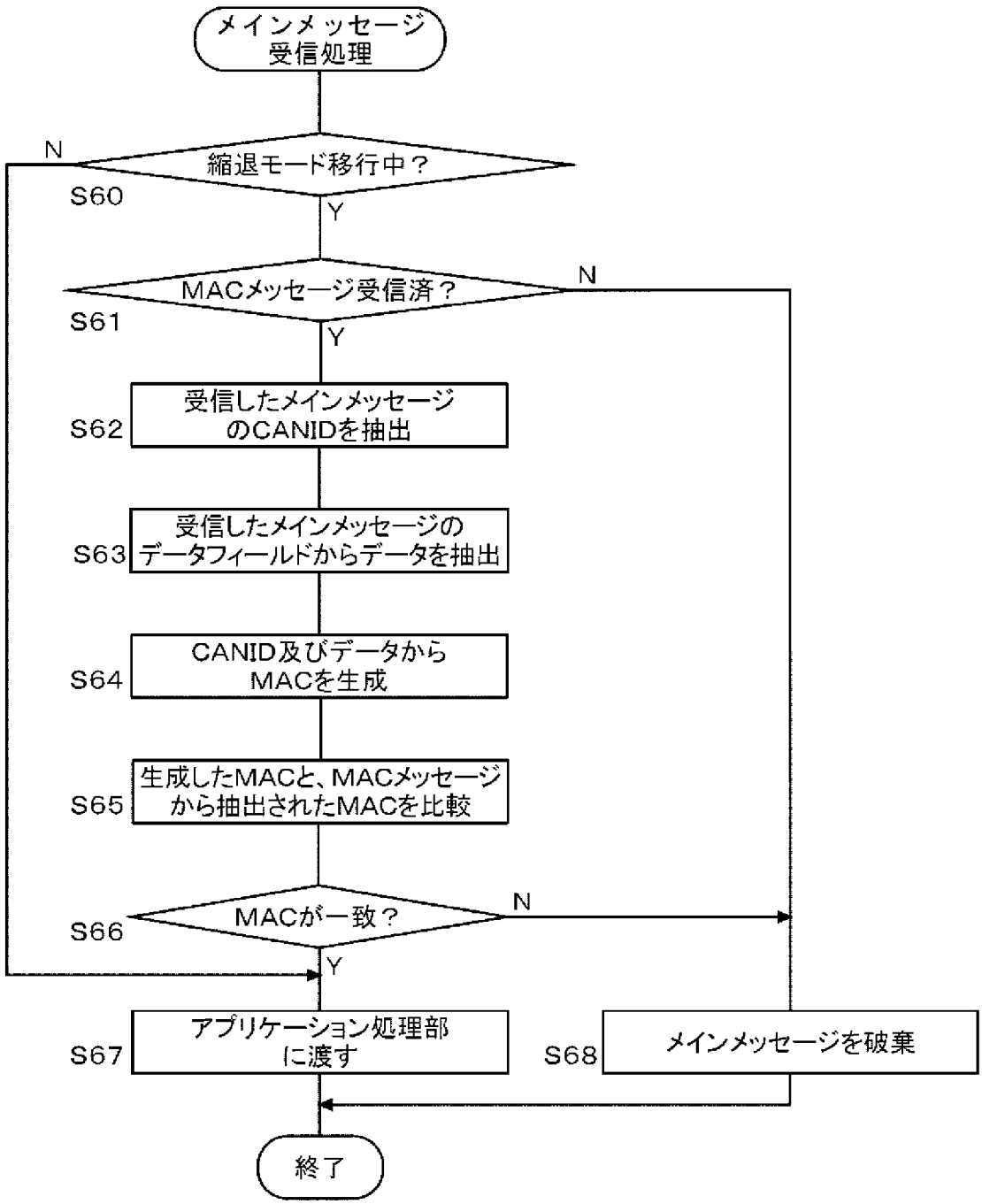
[図10]


10
30
48a
44
MACメッセージ一時保持部
モード切替部
47
45
データ受渡部
MAC生成部
CANID抽出部
41
共通鍵
45a
42
43
メッセージ解析部
データフィールド抽出部
46
MAC比較部
メッセージ処理部
50

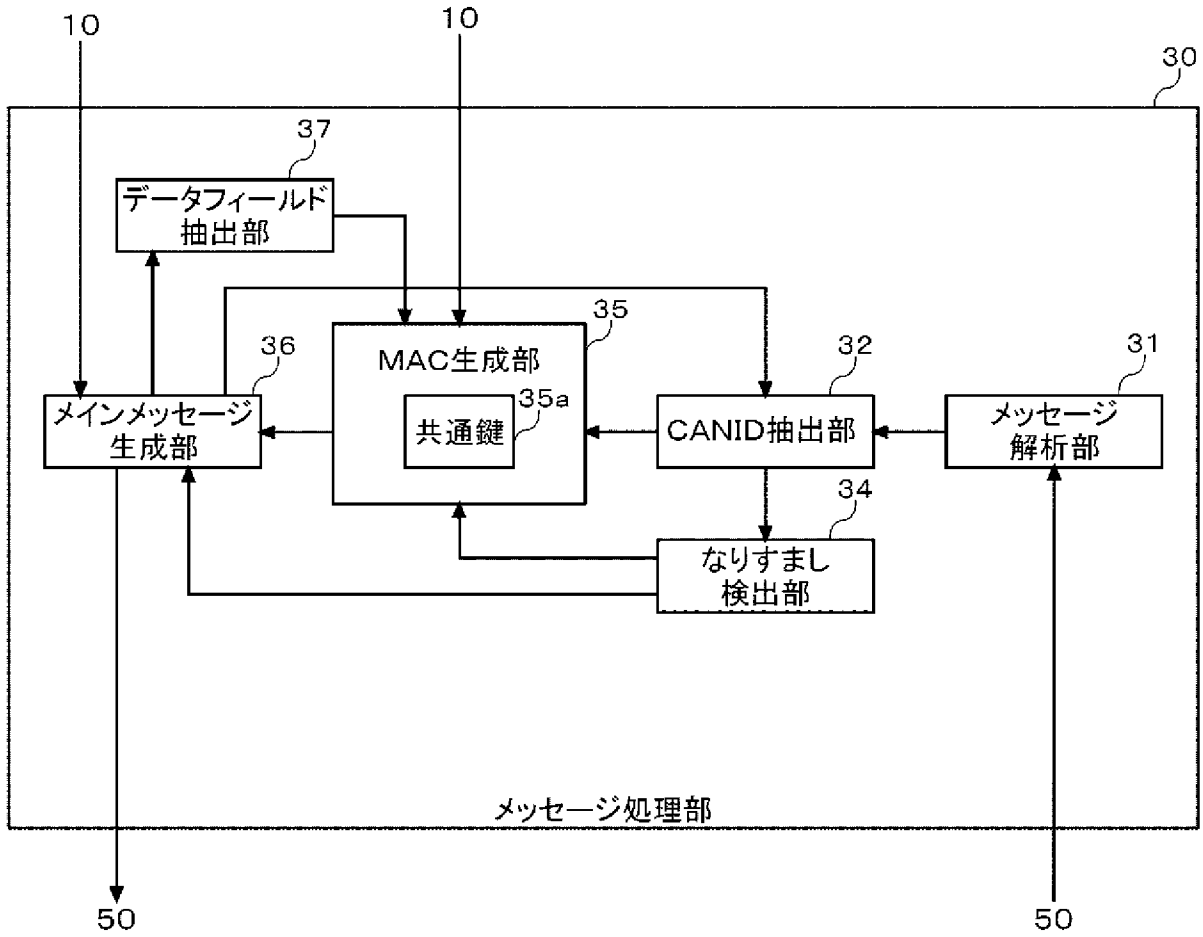
[図11]


MACメッセージ
受信処理
縮退モード移行中？
Y
S50
N
S51
縮退モードへ移行
MACメッセージを
n個以上保持？
N
S52
Y
S53
保持しているMACメッセージの内、
最も古いMACメッセージを破棄
S54
受信したMACメッセージを保持
S55
受信したMACメッセージの
データフィールドからMACを抽出
終了

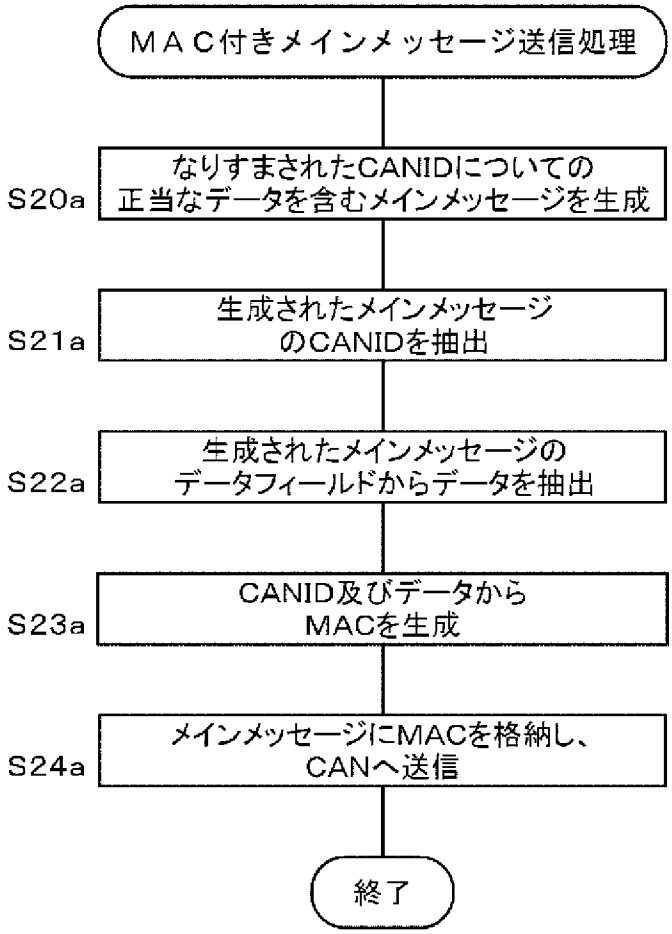
[図12]


メインメッセージ
受信処理
縮退モード移行中？
S60
N
Y
MACメッセージ受信済？
S61
N
Y
受信したメインメッセージ
のCANIDを抽出
S62
受信したメインメッセージの
データフィールドからデータを抽出
S63
CANID及びデータから
MACを生成
S64
生成したMACと、MACメッセージ
から抽出されたMACを比較
S65
MACが一致？
S66
N
Y
アプリケーション処理部
に渡す
S67
メインメッセージを破棄
S68
終了

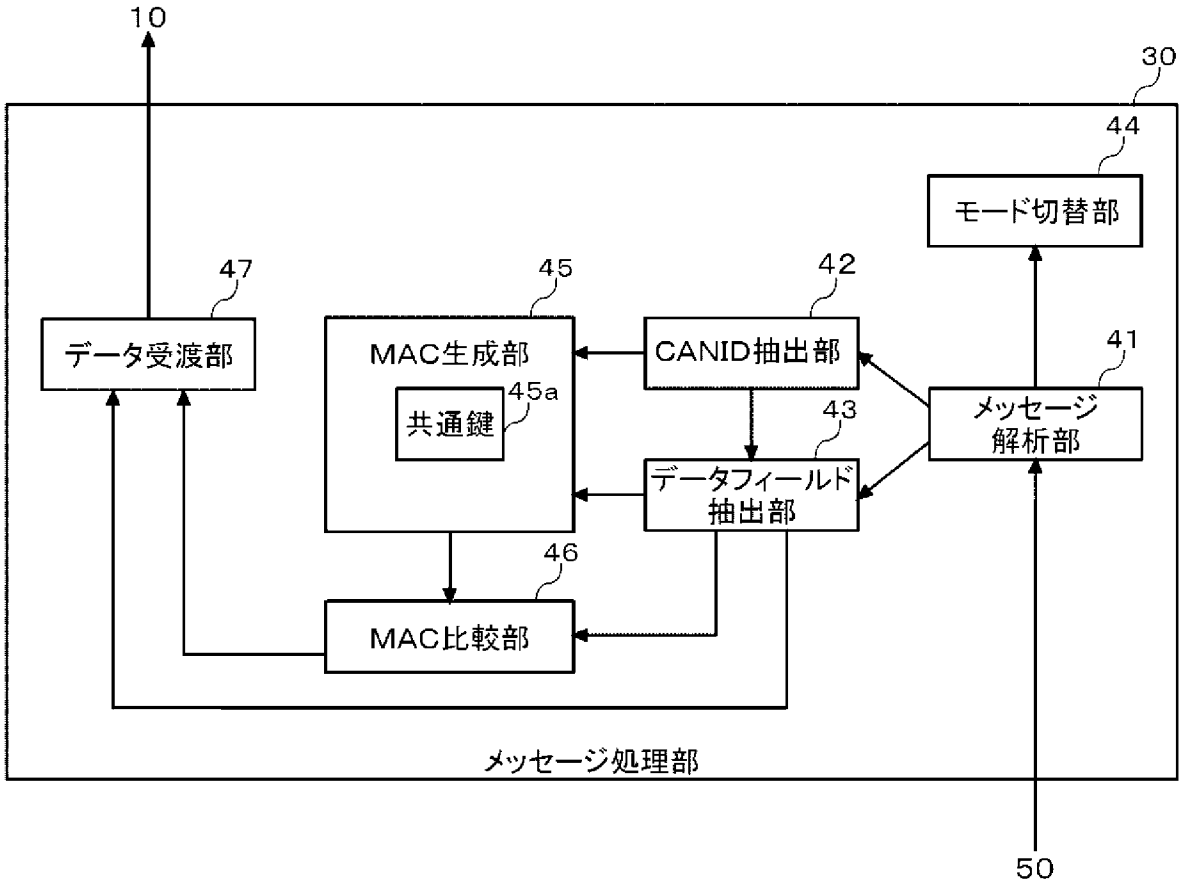
[図13]


10
10
30
37
データフィールド
抽出部
35
MAC生成部
36
32
31
メインメッセージ
生成部
35a
共通鍵
CANID抽出部
メッセージ
解析部
34
なりすまし
検出部
メッセージ処理部
50
50

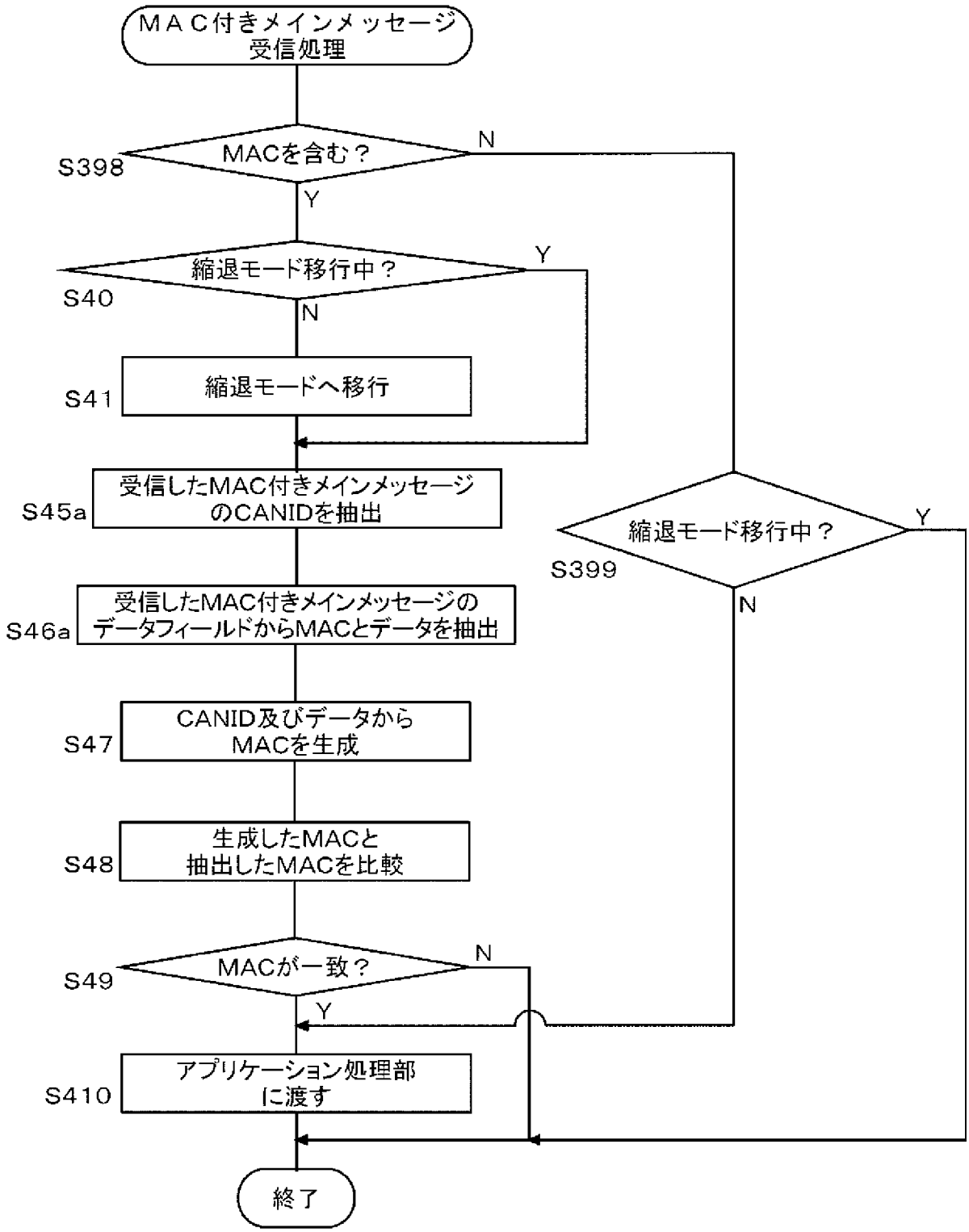
[図14]


ＭＡＣ付きメインメッセージ送信処理
S20a
なりすまされたCANIDについての
正当なデータを含むメインメッセージを生成
S21a
生成されたメインメッセージ
のCANIDを抽出
S22a
生成されたメインメッセージの
データフィールドからデータを抽出
S23a
CANID及びデータから
MACを生成
S24a
メインメッセージにMACを格納し、
CANへ送信
終了

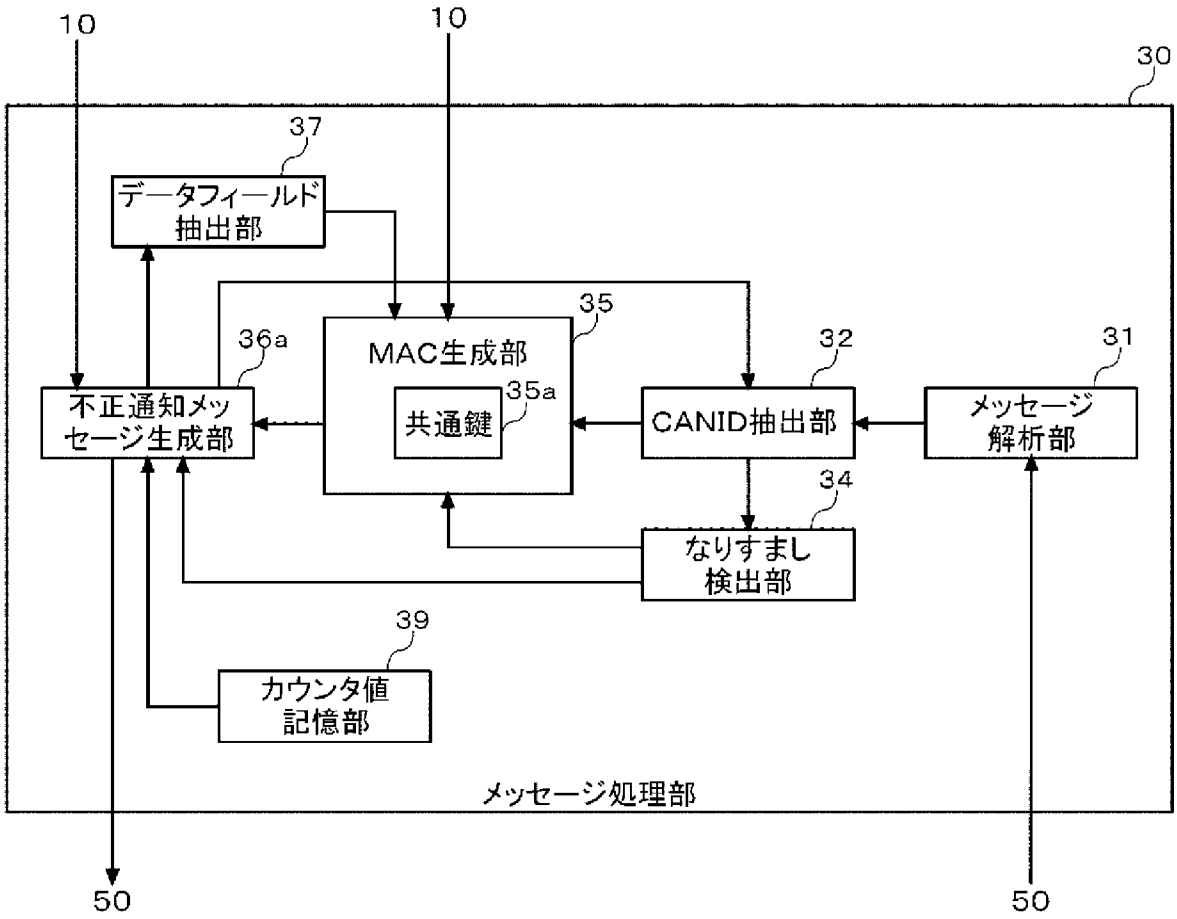
[図15]


10
30
44
モード切替部
47
45
42
データ受渡部
MAC生成部
CANID抽出部
41
45a
共通鍵
43
メッセージ
解析部
データフィールド
抽出部
46
MAC比較部
メッセージ処理部
50

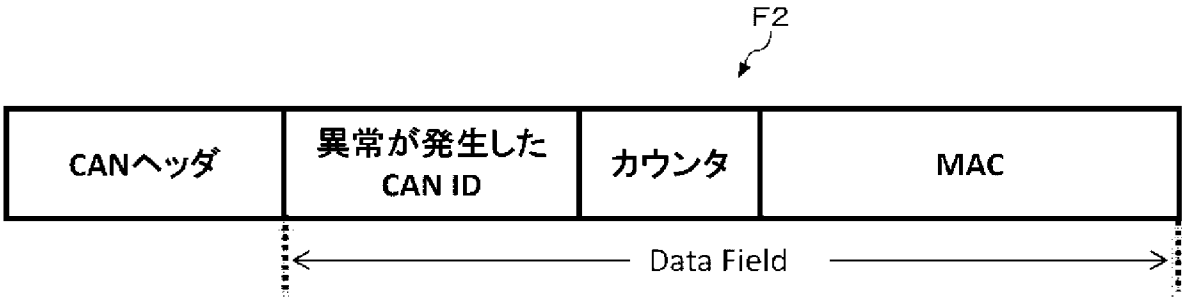
[図16]


ＭＡＣ付きメインメッセージ
受信処理
S398
MACを含む？
N
Y
S40
縮退モード移行中？
Y
N
S41
縮退モードへ移行
S45a
受信したMAC付きメインメッセージ
のCANIDを抽出
S46a
受信したMAC付きメインメッセージの
データフィールドからMACとデータを抽出
S47
CANID及びデータから
MACを生成
S48
生成したMACと
抽出したMACを比較
S49
MACが一致？
N
Y
S410
アプリケーション処理部
に渡す
終了
S399
縮退モード移行中？
Y
N

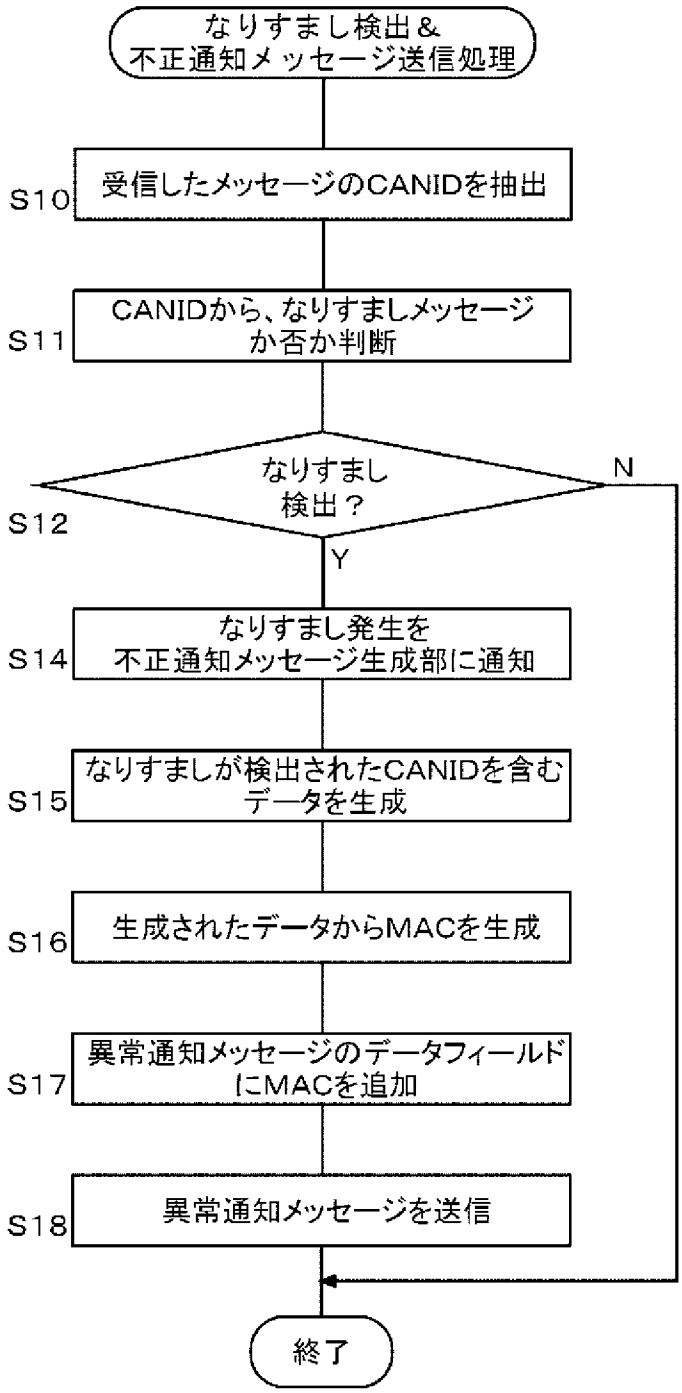
[図17]


10
10
30
37
データフィールド
抽出部
35
36a
MAC生成部
32
31
不正通知メッ
セージ生成部
35a
共通鍵
CANID抽出部
メッセージ
解析部
34
なりすまし
検出部
39
カウンタ値
記憶部
メッセージ処理部
50
50

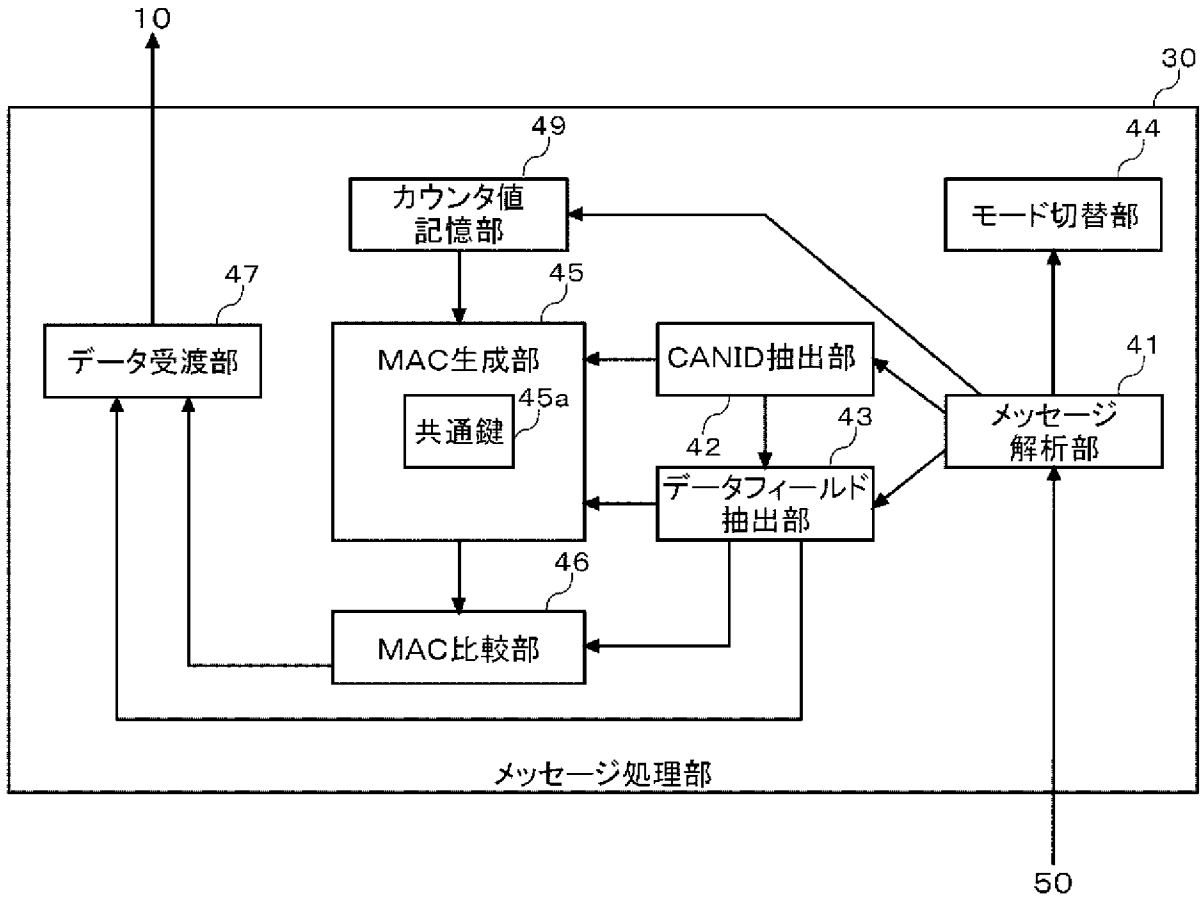
[図18]


F2
CANヘッダ
異常が発生した
CAN ID
カウンタ
MAC
Data Field

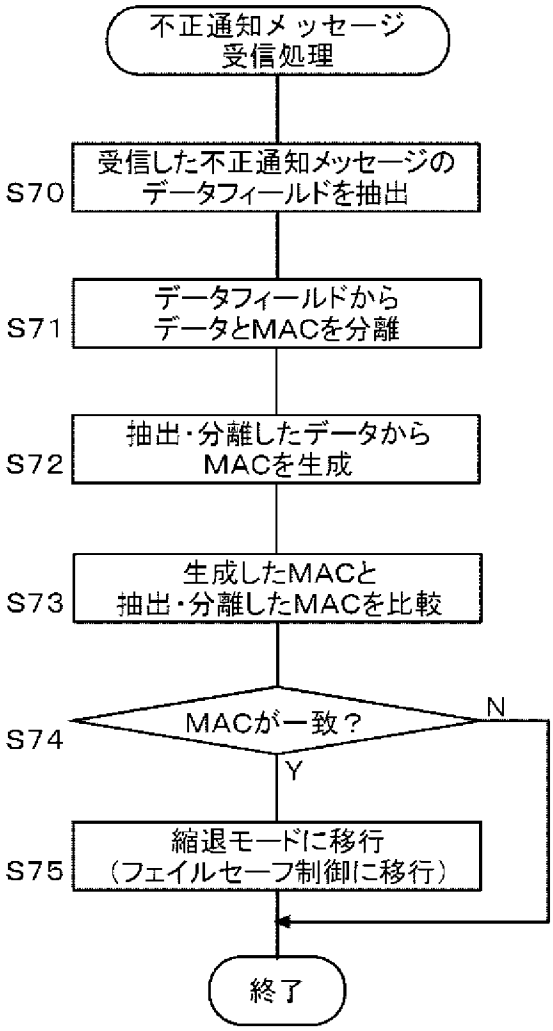
[図19]


なりすまし検出＆
不正通知メッセージ送信処理
S10
受信したメッセージのCANIDを抽出
S11
CANIDから、なりすましメッセージ
か否か判断
S12
なりすまし
検出？
N
Y
S14
なりすまし発生を
不正通知メッセージ生成部に通知
S15
なりすましが検出されたCANIDを含む
データを生成
S16
生成されたデータからMACを生成
S17
異常通知メッセージのデータフィールド
にMACを追加
S18
異常通知メッセージを送信
終了

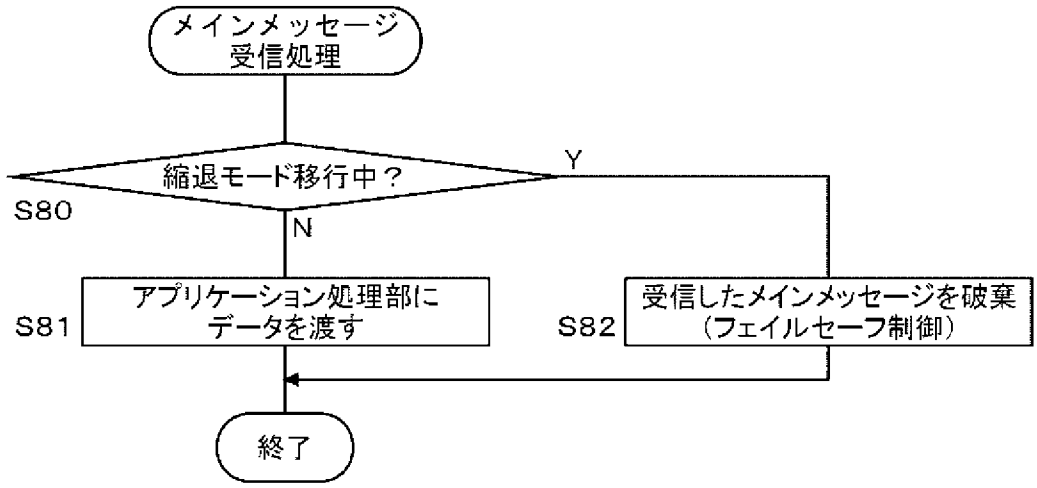
[図20]


10
30
49
カウンタ値
記憶部
44
モード切替部
47
45
データ受渡部
MAC生成部
CANID抽出部
41
45a
共通鍵
42
43
メッセージ
解析部
データフィールド
抽出部
46
MAC比較部
メッセージ処理部
50

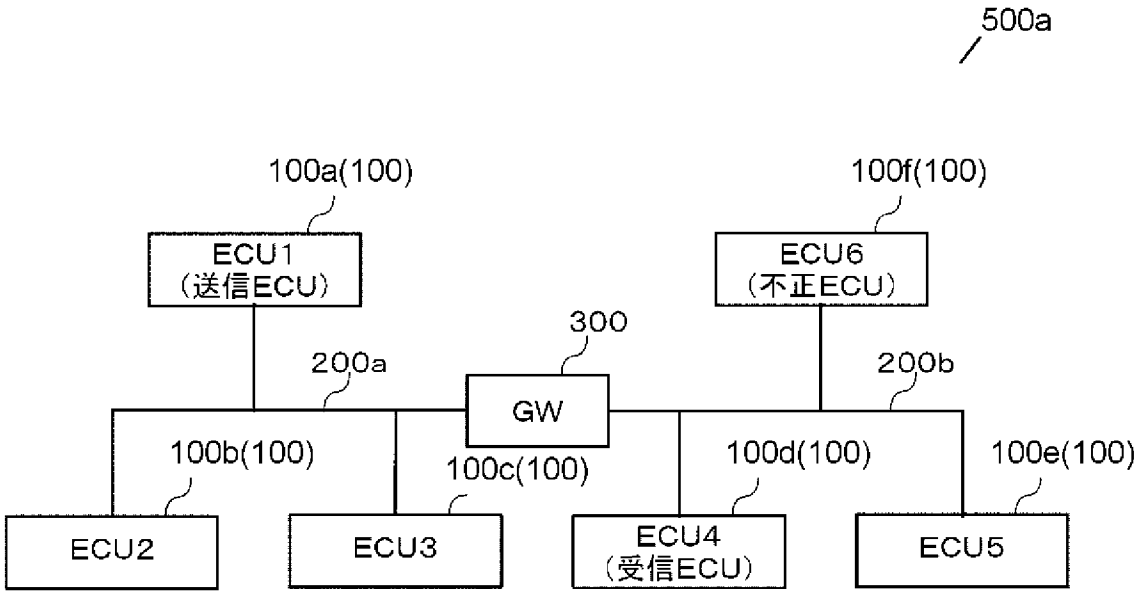
[図21]


不正通知メッセージ
受信処理
S70
受信した不正通知メッセージの
データフィールドを抽出
S71
データフィールドから
データとMACを分離
S72
抽出・分離したデータから
MACを生成
S73
生成したMACと
抽出・分離したMACを比較
S74
MACが一致？
N
Y
S75
縮退モードに移行
（フェイルセーフ制御に移行）
終了

[図22]


メインメッセージ
受信処理
縮退モード移行中？
Y
S80
N
S81
アプリケーション処理部に
データを渡す
S82
受信したメインメッセージを破棄
（フェイルセーフ制御）
終了

[図23]

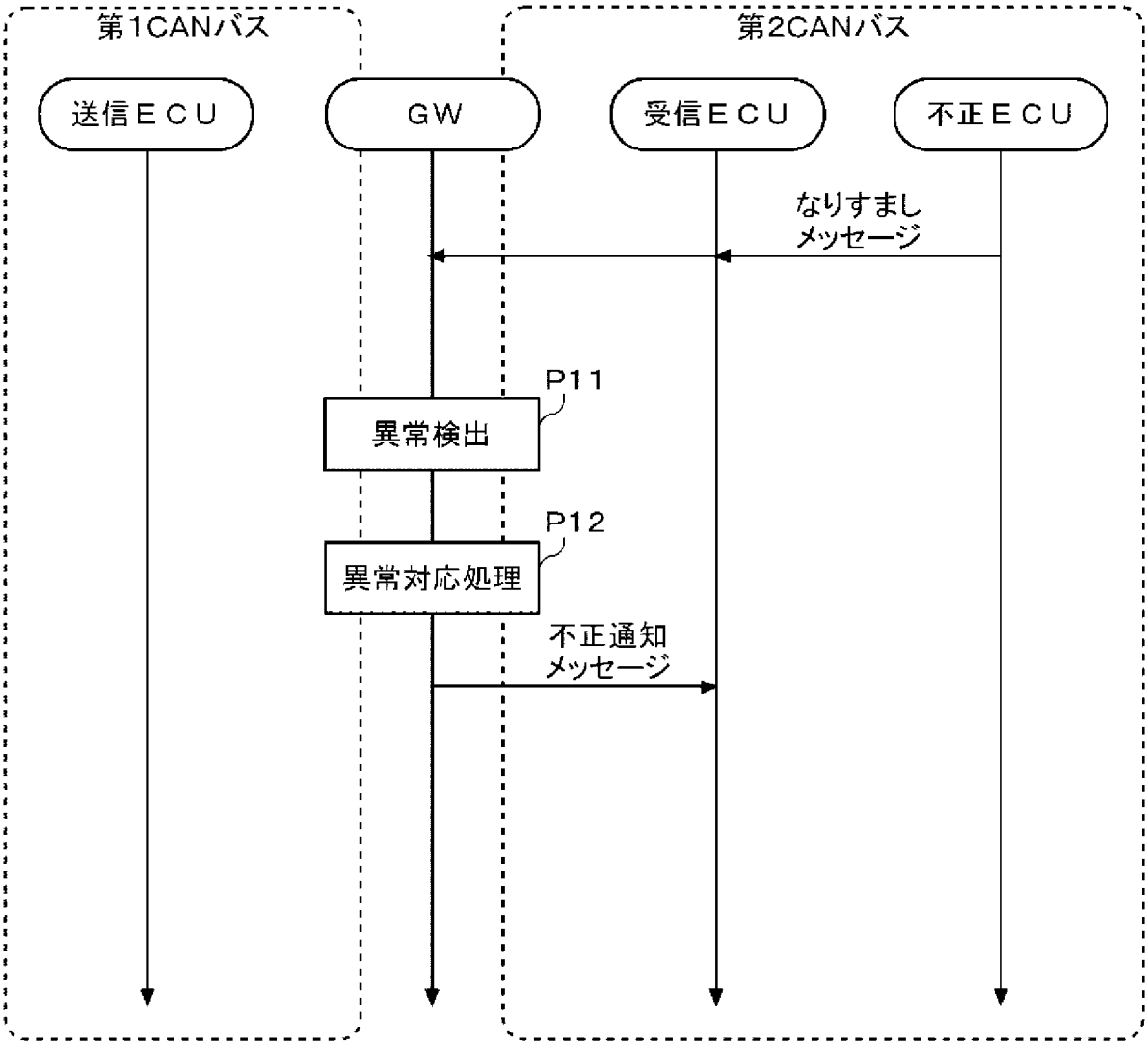


[図24]

310

第1CANバス200aから第2CANバス200bに転送するメッセージのCANID
0x03(ECU1)
0x04(ECU1)
0x11(ECU2)
0x12(ECU2)
0x21(ECU3)

[図25]

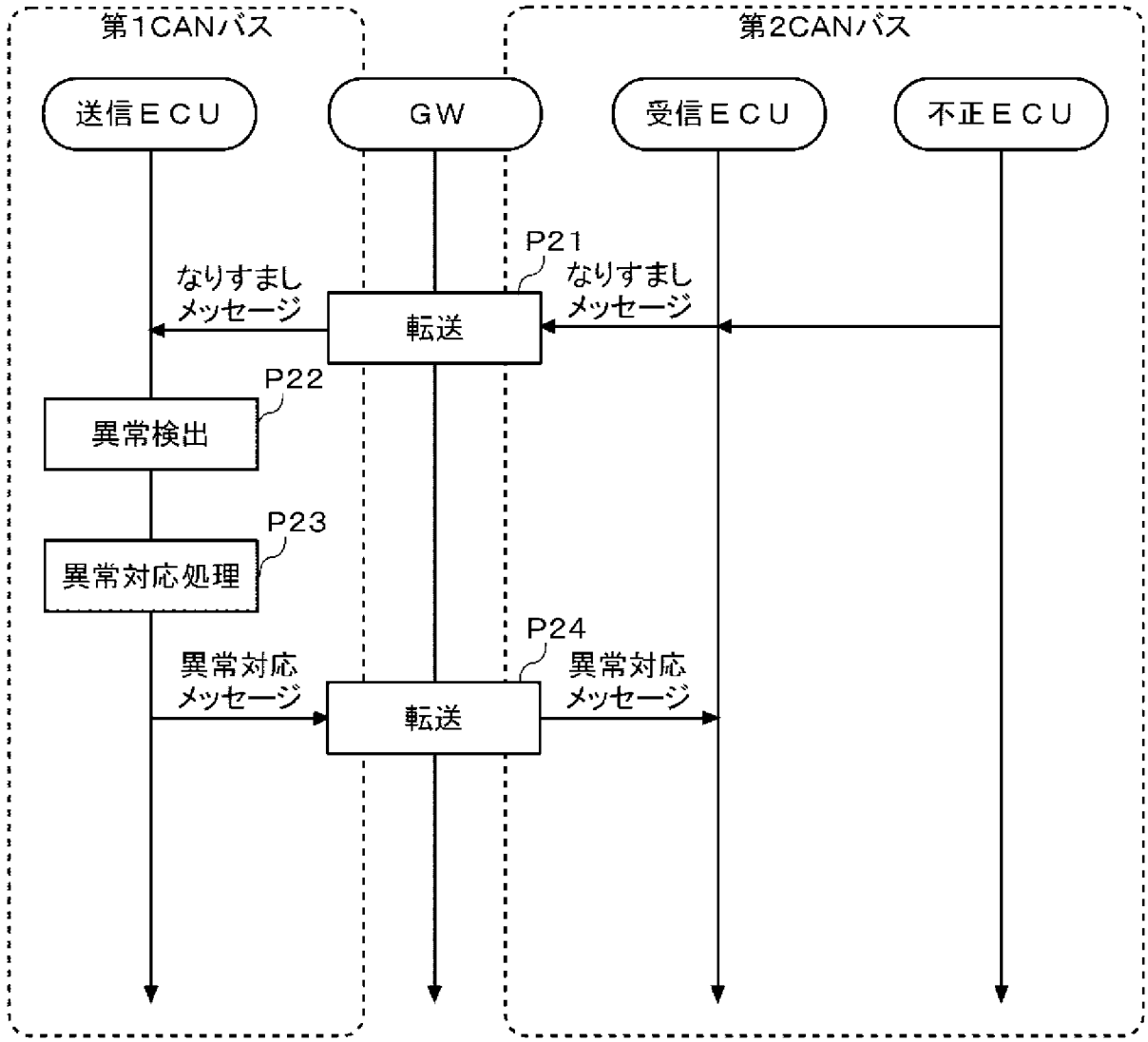


[図26]

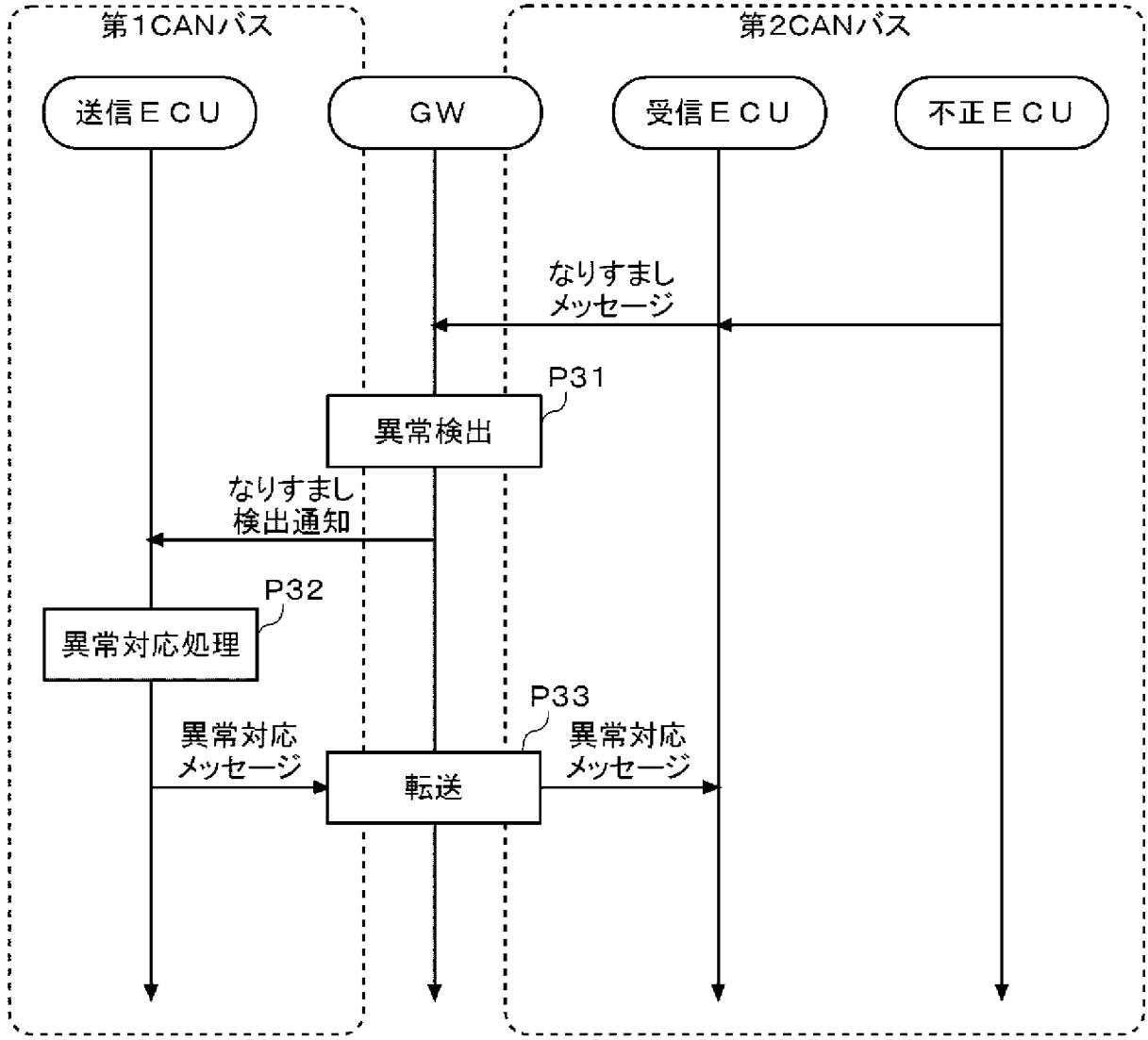
310

第1CANバス200aと第2CANバス200b間で双方向に転送するメッセージのCANID
0x03（ECU1）
0x04（ECU1）
0x11（ECU2）
0x12（ECU2）
0x21（ECU3）

[図27]


第1CANバス
第2CANバス
送信ＥＣＵ
GW
受信ＥＣＵ
不正ＥＣＵ
P21
なりすまし
メッセージ
なりすまし
メッセージ
転送
P22
異常検出
P23
異常対応処理
P24
異常対応
メッセージ
異常対応
メッセージ
転送

[図28]


第1CANバス
第2CANバス
送信ＥＣＵ
GW
受信ＥＣＵ
不正ＥＣＵ
なりすまし
メッセージ
P31
異常検出
なりすまし
検出通知
P32
異常対応処理
P33
異常対応
メッセージ
転送
異常対応
メッセージ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/002614

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *B60R16/023*(2006.01)i, *H04L12/28*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/32, B60R16/023, H04L12/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2014-11621 A (Toyota Motor Corp.), 20 January 2014 (20.01.2014), paragraphs [0019] to [0034] (Family: none)	1-2,4,7,11, 13 3,5,8,10 6,9,12
Y A	JP 2013-98719 A (Toyota InfoTechnology Center, Co., Ltd. et al.), 20 May 2013 (20.05.2013), paragraphs [0025] to [0051] & US 2014/0310530 A1 & WO 2013/065689 A1 & EP 2775660 A1 & CN 104025506 A	3,5,8,10 6,9,12
X A	JP 2006-210995 A (Murata Machinery Ltd.), 10 August 2006 (10.08.2006), paragraphs [0037] to [0038]; fig. 6 & US 2006/0112271 A1 & GB 2423679 A & CN 1783853 A	6,12 9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2015 (10.08.15)	18 August 2015 (18.08.15)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/002614

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-285962 A (Toshiba Carrier Corp.), 12 October 2001 (12.10.2001), paragraphs [0017] to [0040] (Family: none)	1-13
A	JP 2004-229125 A (Sony Corp.), 12 August 2004 (12.08.2004), paragraphs [0011] to [0020], [0037] to [0051] & US 2004/0205210 A1	6,9,12
P,X	WO 2014/199687 A1 (Hitachi Automotive Systems, Ltd.),	1-2,4,7,11, 13
P,A	18 December 2014 (18.12.2014), paragraphs [0056] to [0073], [0088] to [0090] (Family: none)	3,5-6,8-10, 12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／００２６１４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, B60R16/023(2006.01)i, H04L12/28(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, B60R16/023, H04L12/28

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X	JP 2014-11621 A (トヨタ自動車株式会社)	1-2, 4, 7, 11,
	2014.01.20, 段落 0019-0034	13
Y	(ファミリーなし)	3, 5, 8, 10
A		6, 9, 12
Y	JP 2013-98719 A (株式会社トヨタ IT 開発センター, 他)	3, 5, 8, 10
A	2013.05.20, 段落 0025-0051	6, 9, 12
	& US 2014/0310530 A1 & WO 2013/065689 A1 & EP 2775660 A1	
	& CN 104025506 A	

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１０．０８．２０１５	１８．０８．２０１５

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４５３８
金沢　史明
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X A	JP 2006-210995 A (村田機械株式会社) 2006.08.10, 段落 0037-0038, 図 6 & US 2006/0112271 A1 & GB 2423679 A & CN 1783853 A	6,12 9
A	JP 2001-285962 A (東芝キヤリア株式会社) 2001.10.12, 段落 0017-0040 (ファミリーなし)	1-13
A	JP 2004-229125 A (ソニー株式会社) 2004.08.12, 段落 0011-0020, 0037-0051 & US 2004/0205210 A1	6,9,12
P,X P,A	WO 2014/199687 A1 (日立オートモティブシステムズ株式会社) 2014.12.18, 段落 0056-0073, 0088-0090 (ファミリーなし)	1-2,4,7,11,13 3,5-6,8-10,12