

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2019-80234  
(P2019-80234A)

(43) 公開日 令和1年5月23日(2019.5.23)

(51) Int. Cl. F I テーマコード (参考)  
 H04L 12/28 (2006.01) H04L 12/28 200M 5K033  
 G06F 21/31 (2013.01) G06F 21/31

審査請求 未請求 請求項の数 10 O L (全 16 頁)

<p>(21) 出願番号 特願2017-207250 (P2017-207250)                  (22) 出願日 平成29年10月26日 (2017.10.26)</p>	<p>(71) 出願人 000003207                  トヨタ自動車株式会社                  愛知県豊田市トヨタ町1番地                  (74) 代理人 100107766                  弁理士 伊東 忠重                  (74) 代理人 100070150                  弁理士 伊東 忠彦                  (72) 発明者 越前 直哉                  愛知県豊田市トヨタ町1番地 トヨタ自動車株式会社内                  Fターム(参考) 5K033 AA05 AA08 BA06 DB20</p>
--	---

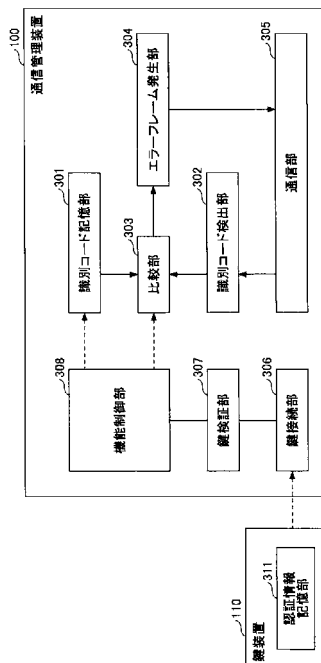
(54) 【発明の名称】 電子制御装置、通信管理方法、及びプログラム

(57) 【要約】

【課題】車載ネットワークにおいて、中継装置を介さない通信経路においても、不正な外部装置による通信を制限しつつ、正当な外部装置による通信を許可することができるようにする。

【解決手段】電子制御装置は、車載ネットワークに接続され、前記車載ネットワークにおける所定の通信を制限する電子制御装置であって、鍵装置の接続を受け付ける鍵接続部と、前記鍵接続部に接続された前記鍵装置を検証する鍵検証部と、前記鍵検証部による前記鍵装置の検証に成功した場合、前記車載ネットワークにおける前記所定の通信を許可する機能制御部と、を有する。

【選択図】 図3



**【特許請求の範囲】****【請求項 1】**

車載ネットワークに接続され、前記車載ネットワークにおける所定の通信を制限する電子制御装置であって、

鍵装置の接続を受け付ける鍵接続部と、

前記鍵接続部に接続された前記鍵装置を検証する鍵検証部と、

前記鍵検証部による前記鍵装置の検証に成功した場合、前記車載ネットワークにおける前記所定の通信を許可する機能制御部と、

を有する、電子制御装置。

**【請求項 2】**

前記鍵装置は、前記車載ネットワークに接続される外部装置による通信を許可する、請求項 1 に記載の電子制御装置。

**【請求項 3】**

前記鍵装置は、前記車載ネットワークに接続される外部装置による通信のうち、前記鍵装置に対応する前記所定の通信を許可する、請求項 1 に記載の電子制御装置。

**【請求項 4】**

前記所定の通信は X C P 通信を含む、請求項 1 又は 3 に記載の電子制御装置。

**【請求項 5】**

前記車載ネットワークに送信される通信フレームを受信する受信部と、

前記通信フレームに、前記所定の通信に対応する識別コードが含まれる場合、前記通信フレームにエラーを発生させる発生部と、

を有し、

前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記発生部による前記エラーの発生を中止させる、請求項 1 乃至 4 のいずれか一項に記載の電子制御装置。

**【請求項 6】**

前記受信部が受信した前記通信フレームに含まれる識別コードと、前記所定の通信に対応する識別コードとを比較し、比較結果を前記発生部に出力する比較部を有し、

前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記比較部による識別コードの比較を無効にする、請求項 5 に記載の電子制御装置。

**【請求項 7】**

前記鍵装置は、前記比較部による判定をバイパスするバイパス回路を含み、

前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記バイパス回路を有効にする、請求項 6 に記載の電子制御装置。

**【請求項 8】**

前記所定の通信に対応する識別コードを記憶する識別コード記憶部を有し、

前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記識別コード記憶部に記憶した前記識別コードのうち、少なくとも一部を無効にする、請求項 5 に記載の電子制御装置。

**【請求項 9】**

車載ネットワークに接続され、前記車載ネットワークにおける所定の通信を制限する電子制御装置が実行する通信管理方法であって、

前記電子制御装置が、

前記電子制御装置が備える鍵接続部に鍵装置が接続されている場合、前記鍵接続部に接続された前記鍵装置を検証するステップと、

前記鍵接続部に接続された前記鍵装置の検証に成功した場合、前記車載ネットワークにおける前記所定の通信を許可するステップと、

を実行する、通信管理方法。

**【請求項 10】**

車載ネットワークに接続され、前記車載ネットワークにおける所定の通信を制限する電

10

20

30

40

50

子制御装置に、

前記電子制御装置が備える鍵接続部に鍵装置が接続されている場合、前記鍵接続部に接続された前記鍵装置を検証するステップと、

前記鍵接続部に接続された前記鍵装置の検証に成功した場合、前記車載ネットワークにおける前記所定の通信を許可するステップと、

を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子制御装置、通信管理方法、及びプログラムに関する。

10

【背景技術】

【0002】

自動車等の車両に搭載される車載ネットワークにおいて、車載ネットワークに接続される外部装置による通信を制限する技術が知られている。

【0003】

例えば、外部装置と車載LAN(Local Area Network)との通信を中継する中継装置を有し、認証システムが外部装置を認証したときだけ、外部装置と車載LANとの間の通信を許可するように中継装置を制御するシステムが知られている(例えば、特許文献1参照)。

【0004】

20

また、複数のモジュール間で識別コード付きのメッセージを通信するネットワークにおいて、予め記憶した識別コードを含む通信フレームを検出したときに、ネットワークに対してエラーコードを出力する技術が知られている(例えば、特許文献2参照)。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】国際公開第2013/038478号

【特許文献2】特開2002-94535号公報

【発明の概要】

【発明が解決しようとする課題】

30

【0006】

特許文献1に開示された技術では、中継装置によって、外部装置に対する通信許可が行われるので、中継装置を介さない通信経路では外部装置に対する通信を制限することができないという問題がある。このようなシステムでは、例えば、不正な外部装置が、中継装置ではなく、車載LANに直接接続された場合等に、不正な外部装置による通信を制限することができない場合がある。

【0007】

一方、特許文献2に開示された技術では、予め記憶した識別コードを含む通信フレームに対してエラーコードが出力されるので、中継装置を介さない通信経路においても、当該識別コードを用いて通信を行う不正な外部装置による通信を制限することができる。ただし、この方法では、当該識別コードを用いて通信を行う正当な外部装置による通信に対しても、通信が制限されてしまうという問題がある。

40

【0008】

本発明の実施の形態は、上記の問題点に鑑みてなされたものであって、車載ネットワークにおいて、中継装置を介さない通信経路においても、不正な外部装置による通信を制限しつつ、正当な外部装置による通信を許可することができるようにする。

【課題を解決するための手段】

【0009】

上記の課題を解決するため、本発明の一実施形態に係る電子制御装置は、車載ネットワークに接続され、前記車載ネットワークにおける所定の通信を制限する電子制御装置であ

50

って、鍵装置の接続を受け付ける鍵接続部と、前記鍵接続部に接続された前記鍵装置を検証する鍵検証部と、前記鍵検証部による前記鍵装置の検証に成功した場合、前記車載ネットワークにおける前記所定の通信を許可する機能制御部と、を有する。

【0010】

電子制御装置は、鍵装置の接続を受け付けし、鍵装置の検証に成功した場合、車載ネットワークにおける所定の通信を許可する。従って、電子制御装置は、不正な利用者が車載ネットワークに接続する不正な外部装置による通信を制限しつつ、鍵装置を有する正当な利用者による所定の通信を許可することができるようになる。

【0011】

上述の実施形態において、前記鍵装置は、前記車載ネットワークに接続される外部装置による通信を許可しても良い。

10

【0012】

これにより、電子制御装置は、鍵装置を有する正当な利用者が、車載ネットワークに接続する正当な外部装置による通信を許可することができる。

【0013】

上述の実施形態において、前記鍵装置は、前記車載ネットワークに接続される外部装置による通信のうち、前記鍵装置に対応する前記所定の通信を許可しても良い。

【0014】

これにより、電子制御装置は、鍵装置を有する正当な利用者が、車載ネットワークに接続する正当な外部装置による通信のうち、所定の通信を許可することができる。

20

【0015】

上述の実施形態において、前記所定の通信はXCP通信を含むものであって良い。

【0016】

これにより、電子制御装置は、鍵装置を有する正当な利用者が、車載ネットワークに接続する正当な外部装置による通信のうち、XCP通信を許可することができる。

【0017】

上述の実施形態において、電子制御装置は、前記車載ネットワークに送信される通信フレームを受信する受信部と、前記通信フレームに、前記所定の通信に対応する識別コードが含まれる場合、前記通信フレームにエラーを発生させる発生部と、を有し、前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記発生部による前記エラーの発生を中止させても良い。

30

【0018】

これにより、電子制御装置は、所定の通信に対応する識別コードを含む通信フレームに対してエラーを発生させることにより、所定の通信を制限することができる。また、電子制御装置は、正当な鍵装置が接続されたとき、所定の通信に対応する識別コードを含む通信フレームに対するエラーの発生を中止させることにより、所定の通信の制限を解除することができる。

【0019】

上述の実施形態において、電子制御装置は、前記受信部が受信した前記通信フレームに含まれる識別コードと、前記所定の通信に対応する識別コードとを比較し、比較結果を前記発生部に出力する比較部を有し、前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記比較部による識別コードの比較を無効にしても良い。

40

【0020】

これにより、電子制御装置は、比較部の機能を有効、又は無効に制御することにより、所定の通信に対する制限を容易に解除することができる。

【0021】

本発明の他の実施形態では、前記鍵装置は、前記比較部による判定をバイパスするバイパス回路を含み、前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記バイパス回路を有効にする。

【0022】

50

これにより、電子制御装置は、論理回路を用いて、比較部による識別コードの比較を無効にすることができる。

【0023】

上述の各実施形態において、電子制御装置は、前記所定の通信に対応する識別コードを記憶する識別コード記憶部を有し、前記機能制御部は、前記鍵検証部による前記鍵装置の検証に成功したとき、前記識別コード記憶部に記憶した前記識別コードのうち、少なくとも一部を無効にしても良い。

【0024】

これにより、電子制御装置は、正当な鍵装置が接続されたとき、識別コード記憶部に記憶した識別コードのうち、少なくとも一部の識別コードを用いて通信を行う、所定の通信を許可することができる。

10

【0025】

本発明の他の実施形態は、通信管理方法、又はプログラムによって実現される。

【発明の効果】

【0026】

本発明の実施の形態によれば、車載ネットワークにおいて、中継装置を介さない通信経路においても、不正な外部装置による通信を制限しつつ、正当な外部装置による通信を許可することができるようになる。

【図面の簡単な説明】

【0027】

20

【図1】一実施形態に係る車載通信システムのシステム構成の例を示す図である。

【図2】第1の実施形態に係る通信管理装置のハードウェア構成の例を示す図である。

【図3】第1の実施形態に係る通信管理装置の機能構成の例を示す図である。

【図4】第1の実施形態に係る通信管理装置の処理の流れを示すフローチャートである。

【図5】第1の実施形態に係る識別コードについて説明するための図である。

【図6】第2の実施形態に係る通信管理装置、及び鍵装置の機能構成の例を示す図である。

【図7】第2の実施形態に係る通信管理装置の処理の流れを示すフローチャートである。

【図8】第2の実施形態に係る識別コードについて説明するための図である。

【発明を実施するための形態】

30

【0028】

以下、図面を参照して発明を実施するための形態について説明する。

【0029】

<システム構成>

図1は、一実施形態に係る車載通信システムのシステム構成の例を示す図である。車載通信システム1は、例えば、自動車等の車両10に搭載される。また、車載通信システム1は、車載ネットワーク130に接続された、通信管理装置100、及び1つ以上のECU (Electric Control Unit) 120-1~120-3を有する。なお、以下の説明の中で、1つ以上のECU 120-1~120-3のうち、任意のECUを示す場合、「ECU 120」を用いる。また、図1に示すECU 120の数は一例であり、ECU 120の数は他の数であって良い。

40

【0030】

ECU 120は、車両10に搭載され、例えば、車両制御系、ボディー系、マルチメディア系等の予め定められた機能を制御する電子制御装置である。ECU 120は、例えば、CPU (Central Processing Unit)、RAM (Random Access Memory)、フラッシュROM (Read Only Memory)、及び通信インタフェース等を含み、所定のプログラムを実行することにより、予め定められた機能を制御する。また、ECU 120は、例えば、CAN (Controller Area Network)、XCP (Universal Calibration Protocol) 等の所定の通信プロトコルを用いて、車載ネットワーク130に接続された他の装置と通信可能である。

50

## 【 0 0 3 1 】

例えば、ECU 120は、XCPのスレーブ（以下、XCPスレーブと呼ぶ）として機能し、車載ネットワーク130に接続される外部ツール140等のXCPのマスター（以下、XCPマスターと呼ぶ）とXCP通信が可能である。なお、外部ツール140は、外部装置の一例である。

## 【 0 0 3 2 】

XCPは、車載ネットワーク130に接続する外部ツール140等を用いて、車両10に搭載される1つ以上のECU120にアクセスし、測定やキャリブレーションを行うための測定/キャリブレーション用のプロトコルの一例である。XCPでは、マスター・スレーブ通信方式が採用されており、XCPマスターが送信するコマンドに対して、コマンドを受信したXCPスレーブが、コマンドに対するレスポンスを送信することにより、通信が行われる。

## 【 0 0 3 3 】

XCPは、車載ネットワーク130において、XCPマスターからXCPスレーブへの送信であること、及びXCPスレーブからXCPマスターへの送信であることを区別することができる様々な通信システムで用いることができる。例えば、CANでは、XCPマスターからXCPスレーブへの送信であることを示すCANのIDと、XCPスレーブからXCPマスターへの送信であることを示すCANのIDとを割り当てることにより、XCP通信が可能である。

## 【 0 0 3 4 】

また、ECU120は、例えば、他のECUと、例えば、CAN等の車載ネットワーク用の通信プロトコルを用いて通信可能である。なお、ECU120は、CAN以外の通信プロトコルを用いて、他のECUと通信するものであっても良い。

## 【 0 0 3 5 】

通信管理装置（電子制御装置）100は、車載ネットワーク130に接続され、車載ネットワーク130における所定の通信を制限する電子制御装置である。例えば、通信管理装置100は、車載ネットワーク130に接続される不正な外部ツール140による通信を制限する機能を有している。

## 【 0 0 3 6 】

例えば、通信管理装置100は、車載ネットワーク130において、XCPマスターからXCPスレーブへの送信であることを示すCANのIDを含む通信フレームを検知すると、当該通信フレーム内においてエラーフレームを発生させる。これにより、通信管理装置100は、車載ネットワーク130に接続された不正な外部ツール140が、XCPプロトコルを用いて、ECU120と通信することを制限することができる。

## 【 0 0 3 7 】

ただし、これだけでは、車載ネットワーク130に、XCPプロトコルを用いて通信を行う正当な外部ツール140が接続されたときであっても、通信が制限されてしまうという問題がある。

## 【 0 0 3 8 】

そこで、本実施形態に係る通信管理装置100は、鍵装置110の接続を受け付ける鍵接続部を有しており、鍵接続部に正当な利用者が有する鍵装置110が接続された場合、車載ネットワーク130における所定の通信（例えば、XCP通信）を許可する。これにより、通信管理装置100は、不正な利用者が車載ネットワーク130に接続する不正な外部ツール140に対しては通信の制限を維持しつつ、鍵装置110を有する正当なユーザが、車載ネットワーク130に正当な外部ツール140を接続する際には、通信を許可することができる。

## 【 0 0 3 9 】

このように、本実施形態に係る鍵装置110は、車載ネットワーク130に接続される外部ツール140による通信を許可する機能を有している。また、鍵装置110は、車載ネットワーク130に接続される外部ツール140による通信のうち、鍵装置110に対

10

20

30

40

50

応する所定の通信（例えば、XCP通信）を許可する機能を有していても良い。なお、鍵装置110は、例えば、所定の情報を記憶した電子的な鍵であっても良いし、物理的な形状により解錠を行う鍵等であっても良い。ここでは、鍵装置110が、所定の情報を記憶した電子的な鍵であるものとして、以下の説明を行う。

#### 【0040】

##### [第1の実施形態]

##### <ハードウェア構成>

続いて、第1の実施形態に係る通信管理装置100のハードウェア構成について説明する。図2は、第1の実施形態に係る通信管理装置のハードウェア構成の例を示す図である。通信管理装置100は、例えば、CPU201、RAM202、フラッシュROM203、接続端子204、通信I/F205、ロジック回路206、及びシステムバス207等を有する。

10

#### 【0041】

CPU201は、フラッシュROM203等に格納されたプログラムやデータ等をRAM202上に読み出し、処理を実行することで、通信管理装置100の各機能を実現する演算装置である。RAM202は、CPU201のワークエリア等として用いられる揮発性のメモリである。フラッシュROM203は、例えば、OS(Operating System)、プログラム、及び各種データ等を記憶する不揮発性のメモリである。

#### 【0042】

接続端子204は、通信管理装置100に鍵装置110を接続するためのインタフェースである。例えば、鍵装置110が、認証情報を記憶した記憶装置である場合、接続端子204は、鍵装置110を通信管理装置100に電氣的に接続するためのコネクタ等である。また、鍵装置110が、物理的な形状に基づいて解錠を行う鍵である場合には、接続端子204は、鍵装置110の形状に対応する構造を有する。

20

#### 【0043】

通信I/F205は、通信管理装置100を車載ネットワーク130に接続する、例えば、CANトランシーバ等の通信インタフェースである。

#### 【0044】

ロジック回路206は、通信管理装置100が実現する各機能の少なくとも一部を実現するための論理回路であり、例えば、専用の集積回路や、プログラミング可能な集積回路等によって実現される。通信管理装置100が実現する各機能は、CPU201によって実行されるプログラムによって実現されるものであっても良いし、ロジック回路206によって実現されるものであっても良い。システムバス207は、上記の各構成要素に共通に接続され、例えば、アドレス信号、データ信号、各種制御信号等を伝達する。

30

#### 【0045】

##### <機能構成>

続いて、通信管理装置100の機能構成について説明する。図3は、第1の実施形態に係る通信管理装置の機能構成の例を示す図である。

#### 【0046】

通信管理装置100は、例えば、識別コード記憶部301、識別コード検出部302、比較部303、エラーフレーム発生部304、通信部305、鍵接続部306、鍵検証部307、及び機能制御部308を有する。

40

#### 【0047】

識別コード記憶部(記憶部)301は、例えば、図2のフラッシュROM、又はロジック回路206に含まれるレジスタ等によって実現され、通信管理装置100が通信を制限する所定の通信に対応する識別コードを記憶している。例えば、通信管理装置100が、XCP通信を制限する場合、識別コード記憶部301は、前述した、XCPマスターからXCPスレーブへの送信であることを示す識別コードを記憶している。

#### 【0048】

識別コード検出部302は、例えば、図2のCPU201で実行されるプログラム、又

50

はロジック回路 206 等によって実現され、通信部 305 が受信する通信フレームに含まれる識別コードを検出する。例えば、通信部 305 が C A N トランシーバである場合、識別コード検出部 302 は、通信フレームに含まれる C A N の I D を検出する。

【0049】

比較部 303 は、例えば、図 2 の C P U 201 で実行されるプログラム、又はロジック回路 206 によって実現される。比較部 303 は、識別コード検出部 302 が検出した識別コードと、識別コード記憶部 301 が記憶している識別コードとを比較し、比較結果をエラーフレーム発生部 304 に出力する。

【0050】

ここで、比較部 303 が出力する比較結果が、2つの識別コードが一致したことを示す場合、通信部 305 が受信する通信フレームに、所定の通信に対応する識別コードが含まれていることを示している。一方、比較部 303 が出力する比較結果が、2つの識別コードが一致しないことを示す場合、通信部 305 が受信する通信フレームには、所定の通信に対応する識別コードが含まれていないことを示している。

10

【0051】

エラーフレーム発生部 304 は、例えば、図 2 の C P U 201 で実行されるプログラム、又はロジック回路 206 等によって実現される。エラーフレーム発生部 304 は、比較部 303 から出力される比較結果が、通信部 305 が受信する通信フレームに、所定の通信に対応する識別コードが含まれていることを示す場合、当該通信フレームにエラーを発生させる。例えば、通信部 305 が C A N トランシーバである場合、エラーフレーム発生部 304 は、当該通信フレーム内において、6ビットのドミナントで構成されるエラーフラグを含むエラーフレームを送信する。

20

【0052】

一方、エラーフレーム発生部 304 は、比較部 303 から出力される比較結果が、通信部 305 が受信する通信フレームに、所定の通信に対応する識別コードが含まれていないことを示す場合、当該通信フレームにエラーを発生させない。

【0053】

通信部（受信部）305 は、例えば、図 2 に示す C P U 201 で実行されるプログラム、及び通信 I / F 205 等によって実現され、例えば、C A N 通信、X C P 通信等の所定の通信を実行する。例えば、通信部 305 は、車載ネットワーク 130 に送信される通信フレームを受信する受信部として機能する。

30

【0054】

鍵接続部 306 は、例えば、図 2 の接続端子 204 によって実現され、通信管理装置 100 への鍵装置 110 の接続を受け付ける。

【0055】

鍵検証部 307 は、例えば、図 2 の C P U 201 で実行されるプログラム、又はロジック回路 206 等によって実現され、鍵接続部 306 に鍵装置 110 が接続されている場合、鍵接続部 306 に接続された鍵装置 110 が正当な鍵装置 110 であるかを検証する。

【0056】

例えば、図 3 に示すように、鍵装置 110 が、認証情報を記憶する認証情報記憶部 311 を有する電子的な鍵である場合、鍵検証部 307 は、鍵装置 110 から、認証情報記憶部 311 に記憶された認証情報を取得する。

40

【0057】

また、鍵検証部 307 は、登録済の鍵装置 110 の認証情報をフラッシュ R O M 203 等に予め記憶しておき、鍵装置 110 から取得した認証情報が、フラッシュ R O M 203 等に認証情報として記憶されている場合、鍵装置 110 の検証を成功させる。一方、鍵検証部 307 は、鍵装置 110 から取得した認証情報が、フラッシュ R O M 203 等に認証情報として記憶されていない場合、鍵装置 110 の検証を失敗させる。

【0058】

別の一例として、例えば、鍵装置 110 が、物理的な形状を利用して解錠を行う鍵であ

50



る場合、鍵検証部 307 は、鍵装置 110 による解錠が成功したか否かにより、鍵装置 110 の検証を行うもの等であっても良い。

【0059】

機能制御部 308 は、例えば、図 2 の CPU 201 で実行されるプログラム、又はロジック回路 206 等によって実現され、鍵検証部 307 による鍵装置 110 の検証に成功した場合、通信管理装置 100 が通信を制限する所定の通信を許可する。例えば、機能制御部 308 は、鍵検証部 307 による鍵装置 110 の検証に成功した場合、エラーフレーム発生部 304 による、エラーの発生を中止させる。

【0060】

機能制御部 308 が、エラーフレーム発生部 304 によるエラーの発生を中止させる方法としては、例えば、比較部 303 による識別コードの比較を無効にするのもであっても良い。また、機能制御部 308 が、エラーフレーム発生部 304 によるエラーの発生を中止させる方法は、識別コード記憶部 301 に記憶した識別コードを無効にするのもであっても良い。この場合、機能制御部 308 は、識別コード記憶部に記憶した識別コードのうち少なくとも 1 つを無効にするのもであっても良い。

【0061】

< 処理の流れ >

続いて、図 4、5 を用いて、第 1 の実施形態に係る通信管理装置 100 が実行する通信管理方法の流れについて説明する。

【0062】

なお、ここでは、一例として、ECU 120、及び外部ツール 140 が送信する通信フレームには、図 5 (a) に示すように、通信の用途に応じて異なる識別コードが含まれているものとする。

【0063】

例えば、ECU 120 が、ブレーキ制御用の通信フレームを送信する場合、送信する通信フレームには識別コード「0x10」が含まれる。また、ECU 120 が、サスペンション制御用の通信フレームを送信する場合、送信する通信フレームには識別コード「0x20」が含まれる。さらに、外部ツール 140 が XCP 用の通信フレームを送信する場合、送信する通信フレームには識別コード「0x30」が含まれる。

【0064】

また、ここでは、図 5 (b) に示すように、通信フレーム 520 は、データ 522 の前に、識別コード 521 を有しているものとする。

【0065】

さらに、ここでは、通信管理装置 100 は、識別コード「0x30」を含む通信フレームを用いて通信が行われる XCP 通信を制限するものとする。例えば、通信管理装置 100 は、図 5 (b) に示す通信フレーム 520 のように、識別コード 521 に「0x30」が含まれる場合、データ 522 内において、エラーフレームを送信することにより、通信フレームにエラーを発生させる。

【0066】

図 4 は、第 1 の実施形態に係る通信管理装置の処理の流れを示すフローチャートである。

【0067】

ステップ S401 において、通信管理装置 100 の通信部 305 が、車載ネットワーク 130 に送信される通信フレームを受信すると、通信管理装置 100 は、ステップ S402 以降の処理を実行する。

【0068】

ステップ S402 において、通信管理装置 100 の鍵検証部 307 は、鍵接続部 306 に鍵装置 110 が接続されているか否かを判断する。鍵装置 110 が接続されている場合、通信管理装置 100 は、処理をステップ S403 に移行させる。一方、鍵装置 110 が接続されていない場合、通信管理装置 100 は、処理をステップ S404 に移行させる。

10

20

30

40

50

## 【 0 0 6 9 】

ステップ S 4 0 2 からステップ S 4 0 3 に移行すると、通信管理装置 1 0 0 の鍵検証部 3 0 7 は、鍵接続部 3 0 6 に接続された鍵装置 1 1 0 を検証する。例えば、鍵検証部 3 0 7 は、鍵接続部 3 0 6 に接続された鍵装置 1 1 0 から、認証情報記憶部 3 1 1 に記憶された認証情報を読み出し、読み出した認証情報が、予め記憶した登録済の鍵装置 1 1 0 の認証情報に含まれる場合、鍵装置 1 1 0 の検証を成功させる。

## 【 0 0 7 0 】

鍵装置 1 1 0 の検証に成功した場合、通信管理装置 1 0 0 は、処理をステップ S 4 0 6 に移行させる。一方、鍵装置 1 1 0 の検証に成功しなかった場合、通信管理装置 1 0 0 は、処理をステップ S 4 0 4 に移行させる。

10

## 【 0 0 7 1 】

ステップ S 4 0 4 に移行すると、通信管理装置 1 0 0 の比較部 3 0 3 は、通信部 3 0 5 が受信した通信フレームから識別コード検出部 3 0 2 検出した識別コードと、識別コード記憶部 3 0 1 に記憶された識別コードとを比較する。

## 【 0 0 7 2 】

識別コード検出部 3 0 2 検出した識別コードと、識別コード記憶部 3 0 1 に記憶された識別コードとが一致した場合、すなわち、受信した通信フレームが所定の識別コード「0 x 3 0」を含む場合、通信管理装置 1 0 0 は、処理をステップ S 4 0 5 に移行させる。一方、識別コード検出部 3 0 2 検出した識別コードと、識別コード記憶部 3 0 1 に記憶された識別コードとが一致しない場合、すなわち、受信した通信フレームが所定の識別コード「0 x 3 0」を含まない場合、通信管理装置 1 0 0 は、処理を終了させる。

20

## 【 0 0 7 3 】

ステップ S 4 0 5 に移行すると、通信管理装置 1 0 0 のエラーフレーム発生部 3 0 4 は、通信部 3 0 5 が受信した通信フレームにおいて、エラーフレームを送信することにより、通信フレームにエラーを発生させる。

## 【 0 0 7 4 】

一方、ステップ S 4 0 3 からステップ S 4 0 6 に移行すると、通信管理装置 1 0 0 の機能制御部 3 0 8 は、識別コード記憶部 3 0 1 に記憶された識別コードを無効にする、又は比較部 3 0 3 による識別コードの比較を無効にする。これにより、通信管理装置 1 0 0 は、ステップ S 4 0 4、S 4 0 5 に示す、エラーフレームの発生処理を中止させる。

30

## 【 0 0 7 5 】

上記の処理により、通信管理装置 1 0 0 は、通信管理装置 1 0 0 に鍵装置 1 1 0 が接続されていない場合、及び鍵装置 1 1 0 の検証に成功しなかった場合には、所定の識別コードを含む通信フレームに対してエラーを発生させる。これにより、通信管理装置 1 0 0 は、正当な鍵装置 1 1 0 を有していない不正な利用者が、車載ネットワーク 1 3 0 に外部ツール 1 4 0 を接続したとき、外部ツール 1 4 0 による所定の通信（例えば、X C P 通信）を制限することができる。

## 【 0 0 7 6 】

一方、通信管理装置 1 0 0 は、通信管理装置 1 0 0 に鍵装置 1 1 0 が接続されており、かつ鍵装置 1 1 0 の検証に成功した場合には、所定の識別コードを含む通信フレームに対して、エラーを発生させない。これにより、通信管理装置 1 0 0 は、正当な鍵装置 1 1 0 を有する正当な利用者が、通信管理装置 1 0 0 に鍵装置 1 1 0 を接続したとき、外部ツール 1 4 0 による所定の通信の制限を解除することができる。

40

## 【 0 0 7 7 】

[ 第 2 の実施形態 ]

第 2 の実施形態では、通信管理装置 1 0 0 を論理回路で構成する場合に好適な実施形態について説明する。

## 【 0 0 7 8 】

< ハードウェア構成 >

第 2 の実施形態に係る通信管理装置 1 0 0 は、例えば、図 2 に示す第 1 の実施形態に係

50

る通信管理装置100のハードウェア構成のうち、CPU201、RAM202、及びフラッシュROMを有していなくても良い。第2の実施形態では、例えば、図6に示すような、通信管理装置100の機能構成を、主にロジック回路206で実現している。

【0079】

<機能構成>

図6は、第2の実施形態に係る通信管理装置、及び鍵装置の機能構成の例を示している。

【0080】

通信管理装置100は、例えば、鍵接続部610、比較器620、識別コード検出器630、エラーフレーム発生器640、及び通信部650等を有する。

10

【0081】

鍵接続部610は、例えば、図2の接続端子204によって実現され、鍵装置110の接続を受け付ける。

【0082】

比較器620は、例えば、図2のロジック回路206によって実現され、例えば、鍵検証回路621、識別コード比較回路622、及び切替回路623を含む。なお、鍵検証回路621、及び切替回路623は、比較器620の外部に設けられているものであっても良い。また、切替回路623は、識別コード比較回路622に含まれているものであっても良い。

【0083】

20

鍵検証回路(鍵検証部)621は、鍵接続部610に鍵装置110が接続されている場合、鍵接続部610に接続された鍵装置110を検証し、検証結果を切替回路623に出力する。例えば、鍵検証回路621は、鍵装置110が有する認証コード601を取得して、鍵検証回路621に予め設定された認証情報との比較することにより、鍵装置110を検証する。或いは、鍵装置110は、鍵装置110を認証するための複数の接点を有し、鍵検証回路621は、鍵接続部610に接続された鍵装置110の接点の論理値を、予め設定された論理値と比較することにより、鍵装置110を検証するもの等であっても良い。なお、鍵検証回路621は、鍵検証部の一例である。

【0084】

識別コード比較回路(比較部)622は、識別コードのパターンを論理回路として有しており、識別コード検出器630から出力される識別コードを1ビット単位で論理比較する。これにより、例えば、プログラムの書換え等により、識別コードが無効化されることを防止することができる。また、識別コード比較回路622は、論理比較により、識別コードの全てのビットが一致した場合、エラーフレーム発生器640にエラーを発生させる。なお、識別コード比較回路622は、比較部の一例である。

30

【0085】

切替回路(機能制御部)623は、鍵検証回路621からの検証結果が、鍵装置110の検証に成功したことを示す場合、識別コード比較回路622による識別コードの比較を無効にすると共に、鍵装置110のバイパス回路602を有効にする。これにより、切替回路623は、エラーフレーム発生器640による、エラーの発生を中止させる。一方、切替回路623は、鍵検証回路621からの検証結果が、鍵装置110の検証に失敗したことを示す場合、識別コード比較回路622による識別コードの比較を有効にする。なお、切替回路623は、機能制御部の一例である。

40

【0086】

識別コード検出器630は、例えば、図2のロジック回路206によって実現され、通信部650が受信する通信フレームに含まれる識別コードを検出して、例えば、1ビット単位で比較器620に出力する。

【0087】

エラーフレーム発生器(発生部)640は、例えば、図2のロジック回路206によって実現され、識別コード比較回路622から出力される制御信号に従って、通信フレーム

50

内にエラーを発生させる。なお、エラーフレーム発生器 640 は、発生部の一例である。

【0088】

通信部（受信部）650 は、例えば、図2の通信I/F205等によって実現され、例えば、CAN通信、XCP通信等の所定の通信を実行する。例えば、通信部650は、車載ネットワーク130に送信される通信フレームを受信する受信部として機能する。

【0089】

上記の構成により、比較器620は、鍵接続部610に鍵装置110が接続されていない場合、及び鍵装置110の検証に失敗した場合には、識別コード比較回路622が有効となる。これにより、比較器620は、通信部650が受信した通信フレームが、所定の識別コードを含むとき、エラーフレーム発生器640に、エラーを発生させる。

10

【0090】

一方、比較器620は、鍵接続部610に鍵装置110が接続され、鍵装置110の検証に成功した場合には、識別コード比較回路622による識別コードの比較を無効にして、バイパス回路602を有効にする。これにより、鍵装置110のバイパス回路602は、比較器620の一部として機能し、エラーフレーム発生器640によるエラーの発生を中止させる。

【0091】

鍵装置110は、例えば、専用の集積回路等により、認証コード601、バイパス回路602等を実現している。

【0092】

認証コード601は、鍵装置110を認証するための情報であり、不揮発性のメモリ等に記憶されたものであっても良いし、認証コードのパターンを論理回路として有しているものであっても良い。

20

【0093】

バイパス回路602は、切替回路623による制御に応じて、比較器620の一部として機能して、識別コード比較回路622による識別コードの比較をバイパスすることにより、比較器620の識別コード比較回路622の機能を無効にする。

【0094】

< 処理の流れ >

続いて、図7、8を用いて、第2の実施形態に係る通信管理装置100による通信管理方法の流れについて説明する。

30

【0095】

図7は、第2の実施形態に係る通信管理装置の処理の流れを示すフローチャートである。なお、ここでは、第1の実施形態と同様に、ECU120、及び外部ツール140が送信する通信フレームには、通信の用途に応じて異なる識別コードが含まれているものとする。

【0096】

ステップS701において、通信部650が、車載ネットワーク130に送信される通信フレームを受信すると、通信管理装置100は、ステップS702以降の処理を実行する。

40

【0097】

ステップS702、S703において、鍵検証回路621は、鍵接続部610に鍵装置110が接続されている場合、鍵接続部610に接続されている鍵装置110を検証し、検証結果を切替回路623に出力する。また、切替回路623は、鍵検証回路621から出力される検証結果に応じて、処理を分岐させる。

【0098】

例えば、鍵検証回路621が、鍵装置110の検証に成功した場合、切替回路623は、処理をステップS706に移行させる。一方、鍵装置110の検証に成功しなかった場合、切替回路623は、処理をステップS704に移行させる。

【0099】

50

ステップS704に移行すると、識別コード比較回路622は、識別コード検出器630が検出する識別コードを、1ビット単位で比較することにより、通信部650が受信する通信フレームに所定の識別コードが含まれるか否かを判定する。

【0100】

例えば、図8(a)に示すように、通信部650が受信する通信フレーム810には、識別コード811と、データ812とが含まれる。第1の実施形態では、比較部303が、識別コード811の全体を比較単位として、所定の識別コードの有無を判定していたが、第2の実施形態では、識別コード比較回路622が、1ビットを比較単位として、所定の識別コードの有無を判定する。例えば、識別コード比較回路622は、識別コード検出器630から、1ビットずつ出力される識別コード811を、論理回路として有する識別コードのパターンと順次に比較し、全てのビットが一致した場合、通信フレームに所定の識別コードが含まれると判定する。

10

【0101】

通信部650が受信する通信フレームに所定の識別コードが含まれる場合、識別コード比較回路622は、ステップS705において、エラーフレーム発生器640に、エラーフレームを送信させる。これにより、例えば、図8(a)に示す通信フレーム810のデータ812においてエラーが発生し、通信フレーム810が無効となる。一方、通信部650が受信する通信フレームに所定の識別コードが含まれない場合、通信管理装置100は、処理を終了させる。

【0102】

また、ステップS703からステップS706に移行すると、切替回路623は、識別コード比較回路622による識別コードの比較を無効にすると共に、鍵接続部306に接続された鍵装置110のバイパス回路602を有効にする。例えば、切替回路623は、識別コード検出器630から出力される識別コードの出力先を、識別コード比較回路622から、バイパス回路602に切替える。

20

【0103】

これにより、バイパス回路602は、例えば、識別コード比較回路622による識別コードの比較をバイパスして、識別コード比較回路622による識別コードの比較を無効にする。

【0104】

上記の処理により、通信管理装置100は、第1の実施形態と同様に、通信管理装置100に鍵装置110が接続されていない場合、及び鍵装置110の検証に成功しなかった場合には、所定の識別コードを含む通信フレームに対してエラーを発生させる。これにより、通信管理装置100は、正当な鍵装置110を有していない不正な利用者が、車載ネットワーク130に外部ツール140を接続したとき、外部ツール140による所定の通信(例えば、XCP通信)を制限することができる。

30

【0105】

また、通信管理装置100は、第1の実施形態と同様に、通信管理装置100に鍵装置110が接続されており、かつ鍵装置110の検証に成功した場合には、所定の識別コードを含む通信フレームに対して、エラーを発生させない。これにより、通信管理装置100は、正当な鍵装置110を有する正当な利用者が、通信管理装置100に鍵装置110を接続したとき、外部ツール140による所定の通信の制限を解除することができる。

40

【0106】

また、別の一例として、図7のステップS706において、鍵装置110が有するバイパス回路602は、識別コード比較回路622の機能の一部を無効にするものであっても良い。

【0107】

例えば、識別コード比較回路622は、図8(b)に示す第1の通信プロトコル用の識別コード「0x30」のパターンと、第2の通信プロトコル用の識別コード「0x310」とパターンとを論理回路として有しているものとする。

50

## 【 0 1 0 8 】

一方、バイパス回路 6 0 2 は、図 8 ( b ) に示すように、第 2 の通信プロトコル用の識別コード「 0 x 3 1 」のパターンを論理回路として有し、識別コード検出器 6 3 0 から出力される識別コードを 1 ビット単位で論理比較する。また、バイパス回路 6 0 2 は、論理比較により、識別コードの全てのビットが一致した場合、エラーフレーム発生器 6 4 0 にエラーを発生させる。

## 【 0 1 0 9 】

このようにして、通信管理装置 1 0 0 に鍵装置 1 1 0 を接続することにより、通信管理装置 1 0 0 が通信を制限する複数の通信プロトコルのうち、所定の通信プロトコルによる通信のみを許可することもできる。

10

## 【 0 1 1 0 】

以上、本発明の各実施形態によれば、車載ネットワーク 1 3 0 において、中継装置を介さない通信経路においても、不正な外部ツール 1 4 0 による通信を制限しつつ、正当な外部装置 4 0 による通信を許可することができるようになる。

## 【 0 1 1 1 】

以上、本発明の実施形態について説明したが、本発明は上記の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、様々な変形や変更が可能である。

## 【 符号の説明 】

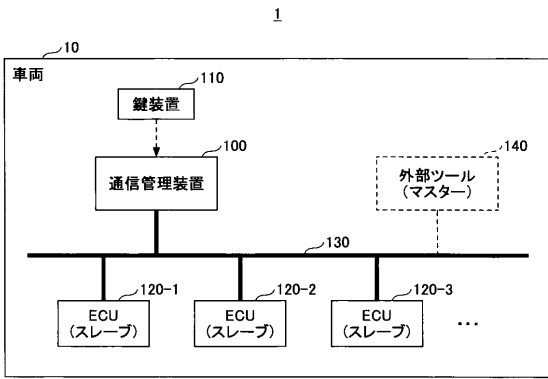
## 【 0 1 1 2 】

20

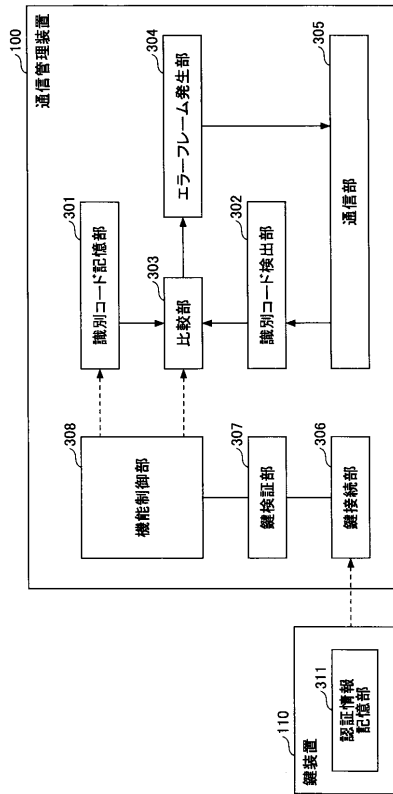
1	車載通信システム
1 0 0	通信管理装置 ( 電子制御装置 )
1 1 0	鍵装置
1 4 0	外部ツール ( 外部装置 )
3 0 1	識別コード記憶部
3 0 3	比較部
3 0 4	エラーフレーム発生部 ( 発生部 )
3 0 5、6 5 0	通信部 ( 受信部 )
3 0 6、6 1 0	鍵接続部
3 0 7	鍵検証部
3 0 8	機能制御部
6 0 2	バイパス回路
6 2 1	鍵検証回路 ( 鍵検証部の一例 )
6 2 2	識別コード比較回路 ( 比較部の一例 )
6 2 3	切替回路 ( 機能制御部の一例 )
6 4 0	エラーフレーム発生器 ( 発生部の一例 )

30

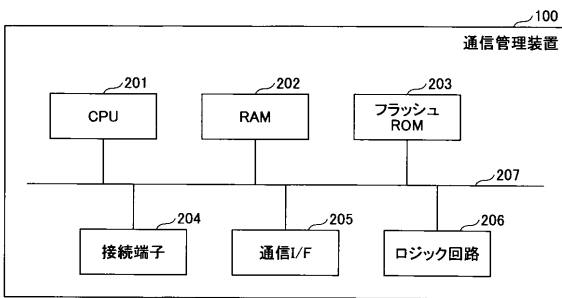
【 図 1 】



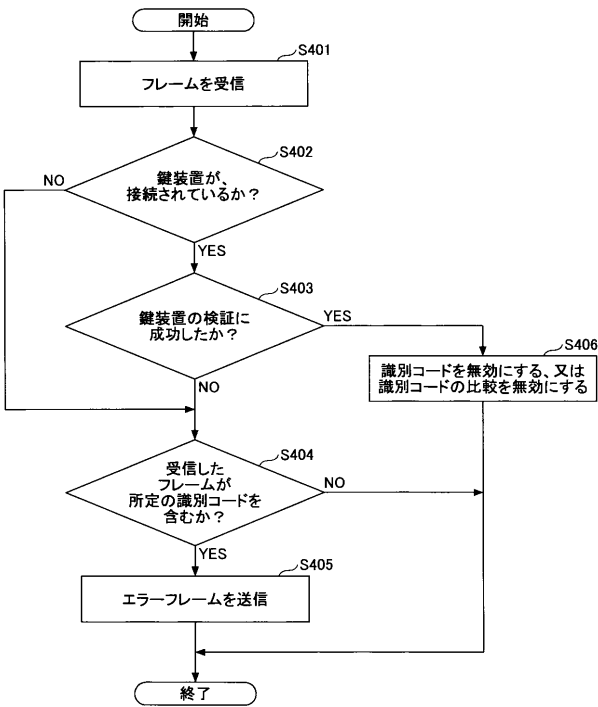
【 図 3 】



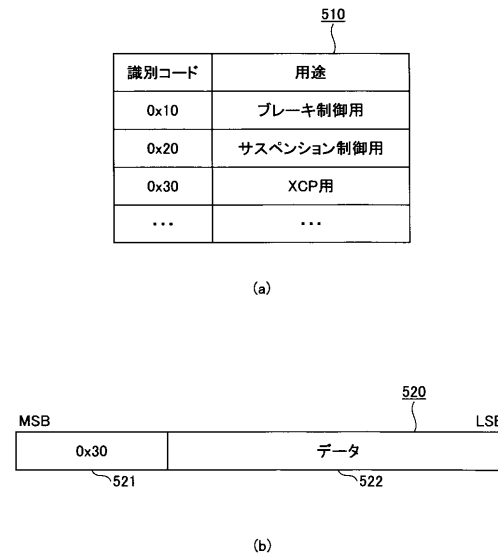
【 図 2 】



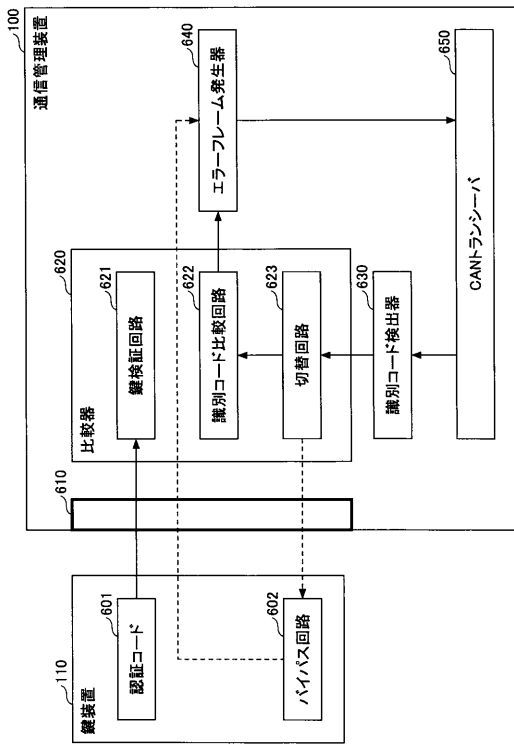
【 図 4 】



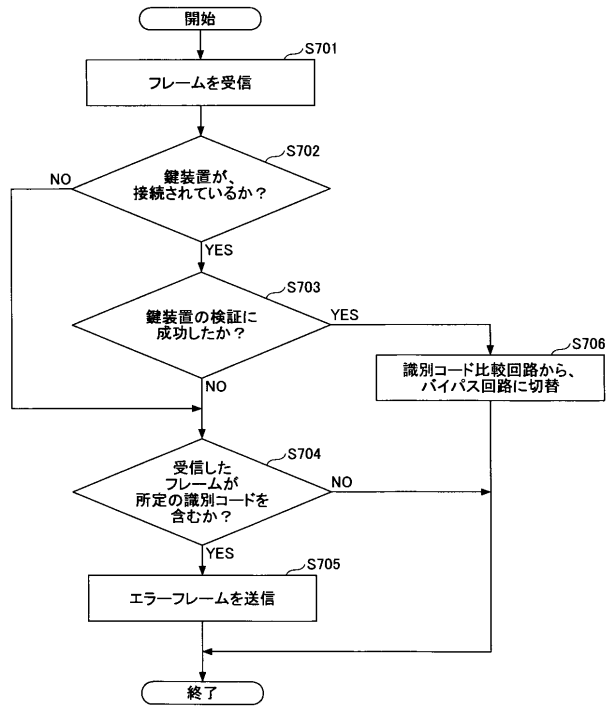
【 図 5 】



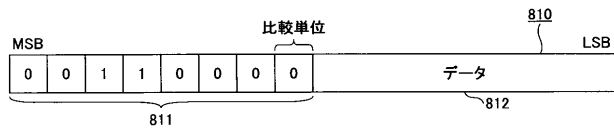
【図6】



【図7】



【図8】



(a)

識別コード	用途
0x30	第1の通信プロトコル用
0x31	第2の通信プロトコル用
...	...

(b)

識別コード	用途
0x31	第2の通信プロトコル用
...	...

(c)