(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6973120号
(P6973120)
(45)発行日　令和3年11月24日(2021.11.24)　(24)登録日　令和3年11月8日(2021.11.8)

(51)Int.Cl.　　F I
H04L 12/28 (2006.01)　　H04L 12/28 200Z
G06F 21/44 (2013.01)　　G06F 21/44
H04L 12/28 100A

請求項の数 11　(全 17 頁)

(21)出願番号　特願2018-11780(P2018-11780)
(22)出願日　平成30年1月26日(2018.1.26)
(65)公開番号　特開2019-129500(P2019-129500A)
(43)公開日　令和1年8月1日(2019.8.1)
審査請求日　令和2年8月18日(2020.8.18)

(73)特許権者　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(74)代理人　110000280
特許業務法人サンクレスト国際特許事務所
(72)発明者　山下　哲生
大阪府大阪市中央区北浜四丁目５番３３号
住友電気工業株式会社内

審査官　野元　久道

(56)参考文献　国際公開第２０１３／１２２１７７（WO，A1）
特開２０１４－０９１４８７（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】なりすまし検出装置、検出方法、およびコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
通信ネットワークに属する複数の装置への電力供給を個別に制御する電源制御部と、
前記通信ネットワークの通信状態を取得する取得部と、
前記複数の装置のうちの１つの装置である対象装置の電力供給状態、および、前記通信ネットワークの通信状態に基づいて、前記対象装置を詐称する通信ノードの存在を検出する検出部と、を備え、
前記通信ネットワークは、車内の通信ネットワークであり、
前記複数の装置は、それぞれ車載制御装置であり、
前記電源制御部は、前記複数の装置が設置された車両の走行状態に基づいて、前記複数の装置への電力供給を個別に制御する、なりすまし検出装置。
【請求項２】
通信ネットワークに属する複数の装置への電力供給を個別に制御する電源制御部と、
前記通信ネットワークの通信状態を取得する取得部と、
前記複数の装置のうちの１つの装置である対象装置の電力供給状態、および、前記通信ネットワークの通信状態に基づいて、前記対象装置を詐称する通信ノードの存在を検出する検出部と、を備え、
前記通信ノードの存在が検出されると、前記電源制御部は、被詐称装置である前記対象装置の安全性のレベルが所定レベルよりも高いときには、前記対象装置への電力供給を遮断する、なりすまし検出装置。

【請求項３】
前記通信ノードの存在が検出されると、前記電源制御部は、被詐称装置である前記対象装置の安全性のレベルが所定レベルよりも高いときには、前記対象装置への電力供給を遮断する、請求項１に記載のなりすまし検出装置。
【請求項４】
前記通信ネットワークは、車内の通信ネットワークであり、
前記複数の装置は、それぞれ車載制御装置である、請求項２に記載のなりすまし検出装置。
【請求項５】
前記対象装置への電力供給が遮断された状態において、前記対象装置を送信元とした通信が生じている場合に、前記検出部は前記通信ノードの存在を検出する、請求項１から請求項４のいずれか１項に記載のなりすまし検出装置。
【請求項６】
前記通信ノードの存在が検出されると、被詐称装置である前記対象装置の識別情報を前記複数の装置のうちの前記対象装置以外の装置である非対象装置に通知する通知部をさらに備える、請求項１から請求項５のいずれか１項に記載のなりすまし検出装置。
【請求項７】
前記通知部は、前記識別情報を表示装置で表示する処理を実行する、請求項６に記載のなりすまし検出装置。
【請求項８】
複数の装置の属する通信ネットワークにおいて、前記複数の装置のうちの１つの装置である対象装置を詐称する通信ノードの存在を検出する方法であって、
前記複数の装置への電力供給を個別に制御するステップと、
前記通信ネットワークの通信状態を取得するステップと、
前記対象装置の電力供給状態、および、前記通信ネットワークの通信状態に基づいて、前記通信ノードの存在を検出するステップと、を備え、
前記通信ネットワークは、車内の通信ネットワークであり、
前記複数の装置は、それぞれ車載制御装置であり、
前記制御するステップは、前記複数の装置が設置された車両の走行状態に基づいて、前記複数の装置への電力供給を個別に制御するステップを含む、検出方法。
【請求項９】
複数の装置の属する通信ネットワークにおいて、前記複数の装置のうちの１つの装置である対象装置を詐称する通信ノードの存在を検出する方法であって、
前記複数の装置への電力供給を個別に制御するステップと、
前記通信ネットワークの通信状態を取得するステップと、
前記対象装置の電力供給状態、および、前記通信ネットワークの通信状態に基づいて、前記通信ノードの存在を検出するステップと、を備え、
前記制御するステップは、前記通信ノードの存在が検出された場合に、被詐称装置である前記対象装置の安全性のレベルが所定レベルよりも高いときには、前記対象装置への電力供給を遮断するステップを含む、検出方法。
【請求項１０】
なりすまし検出装置としてコンピュータを機能させるためのコンピュータプログラムであって、
前記コンピュータを、
通信ネットワークに属する複数の装置への電力供給を個別に制御する電源制御部と、
前記通信ネットワークの通信状態を取得する取得部と、
前記複数の装置のうちの１つの装置である対象装置の電力供給状態、および、前記通信ネットワークの通信状態に基づいて、前記対象装置を詐称する通信ノードの存在を検出する検出部、として機能させ、
前記通信ネットワークは、車内の通信ネットワークであり、

前記複数の装置は、それぞれ車載制御装置であり、
前記電源制御部は、前記複数の装置が設置された車両の走行状態に基づいて、前記複数の装置への電力供給を個別に制御する、コンピュータプログラム。
【請求項１１】
なりすまし検出装置としてコンピュータを機能させるためのコンピュータプログラムであって、
前記コンピュータを、
通信ネットワークに属する複数の装置への電力供給を個別に制御する電源制御部と、
前記通信ネットワークの通信状態を取得する取得部と、
前記複数の装置のうちの１つの装置である対象装置の電力供給状態、および、前記通信ネットワークの通信状態に基づいて、前記対象装置を詐称する通信ノードの存在を検出する検出部、として機能させ、
前記通信ノードの存在が検出されると、前記電源制御部は、被詐称装置である前記対象装置の安全性のレベルが所定レベルよりも高いときには、前記対象装置への電力供給を遮断する、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明はなりすまし検出装置、検出方法、およびコンピュータプログラムに関し、特に、車載装置への電力供給を制御するなりすまし検出装置、検出方法、およびコンピュータプログラムに関する。
【背景技術】
【０００２】
近年、自動車の技術分野においては、車両の高機能化が進行しており、多種多様な車載機器が車両に搭載されている。従って、車両には、各車載機器を制御するための制御装置である、所謂ＥＣＵ（Electronic Control Unit）が多数搭載されている。
ＥＣＵの種類には、例えば、アクセル、ブレーキ、ハンドルの操作に対してエンジンやブレーキ、ＥＰＳ（Electric Power Steering）等の制御を行う走行系に関わるもの、乗員によるスイッチ操作に応じて車内照明やヘッドライトの点灯／消灯と警報器の吹鳴等の制御を行うボディ系ＥＣＵ、運転席近傍に配設されるメータ類の動作を制御するメータ系ＥＣＵなどがある。
【０００３】
複数のＥＣＵを含む車内ネットワークに対して悪意ある第三者のアクセスが成功すると、車外装置を用いて送信元をいずれかのＥＣＵと詐称して（なりすまして）他のＥＣＵにメッセージを送信する場合が想定される。
【０００４】
この問題に対して、特許文献１には、ＣＡＮ（Controller Area Network）通信システムを構成する複数のＥＣＵの各々において、受信したフレームに含まれる送信元ＩＤが自身のＩＤである場合になりすましを検出する技術が開示されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１４－１１６２１号公報
【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では、ＥＣＵは自身が送信元と詐称されていることのみ検出するものであるため、すべてのＥＣＵについて送信元が詐称されているか否かを判定するためには、すべてのＥＣＵが検出処理を行う必要がある。そのため、全体としてＥＣＵの処理負荷が高くなることがある。

【０００７】
本発明のある局面における目的は、容易な制御によって、対象装置を詐称する通信ノードの存在を検出することにより、なりすましの存在を高精度で検出するなりすまし検出装置、その検出方法、およびコンピュータプログラムを提供することである。
【課題を解決するための手段】
【０００８】
ある実施の形態に従うと、なりすまし検出装置は、通信ネットワークに属する複数の装置への電力供給を個別に制御する電源制御部と、通信ネットワークの通信状態を取得する取得部と、複数の装置のうちの１つの装置である対象装置の電力供給状態、および、通信ネットワークの通信状態に基づいて、対象装置を詐称する通信ノードの存在を検出する検出部と、を備える。
【０００９】
他の実施の形態に従うと、検出方法は、複数の装置の属する通信ネットワークにおいて、複数の装置のうちの１つの装置である対象装置を詐称する通信ノードの存在を検出する方法であって、複数の装置への電力供給を個別に制御するステップと、通信ネットワークの通信状態を取得するステップと、対象装置の電力供給状態、および、通信ネットワークの通信状態に基づいて、通信ノードの存在を検出するステップと、を備える。
【００１０】
他の実施の形態に従うと、コンピュータプログラムはなりすまし検出装置としてコンピュータを機能させるためのコンピュータプログラムであって、コンピュータを、通信ネットワークに属する複数の装置への電力供給を個別に制御する電源制御部と、通信ネットワークの通信状態を取得する取得部と、複数の装置のうちの１つの装置である対象装置の電力供給状態、および、通信ネットワークの通信状態に基づいて、対象装置を詐称する通信ノードの存在を検出する検出部、として機能させる。
【発明の効果】
【００１１】
この発明によると、対象装置の電力供給状態および通信ネットワークの通信状態に基づいて対象装置を詐称する通信ノードの存在を検出することにより、容易な制御によって高精度でなりすましの存在を検出することができる。
【図面の簡単な説明】
【００１２】
【図１】実施の形態にかかる車両の構成を表した概略図である。
【図２】中継装置の内部構成を示すブロック図である。
【図３】電源制御装置の内部構成を示すブロック図である。
【図４】第１の実施の形態にかかる検出処理の流れを表したフローチャートである。
【図５】第２の実施の形態にかかる検出処理の流れを表したフローチャートである。
【発明を実施するための形態】
【００１３】
［実施の形態の説明］
本実施の形態には、少なくとも以下のものが含まれる。すなわち、
（１）本実施の形態に含まれるなりすまし検出装置は、車内の通信ネットワークに属する複数の車載制御装置への電力供給を個別に制御する電源制御部と、通信ネットワークの通信状態を取得する取得部と、複数の車載制御装置のうちの１つの車載制御装置である対象装置の電力供給状態、および、通信ネットワークの通信状態に基づいて、対象装置を詐称する通信ノードの存在、つまり、なりすましの存在を検出する検出部と、を備える。
対象装置の電力供給状態および通信ネットワークの通信状態に基づいて対象装置を詐称する通信ノードの存在を検出することにより、容易な制御によって高精度でなりすましの存在を検出することができる。また、複数の車載制御装置への電力供給を個別に制御することによって、複数の車載制御装置のいずれも対象装置としてなりすましの存在を検出することができる。

【００１４】
（２）好ましくは、対象装置への電力供給が遮断された状態において、対象装置を送信元とした通信が生じている場合に、検出部は上記通信ノードの存在を検出する。
対象装置への電力供給が遮断されている場合には当該対象装置を送信元とした通信は生じないため、対象装置への電力供給が遮断されている状態においては、当該対象装置を送信元とした通信が生じているか否かという容易な判定によって高精度でなりすましの存在を検出できる。
【００１５】
（３）好ましくは、なりすまし検出装置は、通信ノードの存在が検出されると、被詐称装置である対象装置の識別情報を複数の車載制御装置のうちの対象装置以外の車載制御装置である非対象装置に通知する通知部をさらに備える。
被詐称装置である対象装置の識別情報が通知されることによって、非対象装置は当該対象装置を送信元とした送信メッセージに対処することができる。
【００１６】
（４）好ましくは、通知部は、識別情報を表示装置で表示する処理を実行する。
これにより、ユーザは、対象装置を表示装置の表示によって知ることができる。
【００１７】
（５）好ましくは、通信ノードの存在が検出されると、電源制御部は、被詐称装置である対象装置の安全性のレベルが所定レベルよりも高いときには、対象装置への電力供給を遮断する。
これにより、対象装置の安全性のレベルが高い場合に、当該車両における安全性を確保することができる。
【００１８】
（６）本実施の形態に含まれる検出方法は、（１）～（５）のいずれか１つに記載のなりすまし装置において、複数の車載制御装置のうちの１つの車載制御装置である対象装置を詐称する通信ノードの存在を検出する方法である。
かかる検出方法は、上記（１）～（５）のなりすまし検出装置と同様の効果を奏する。
【００１９】
（７）本実施の形態に含まれるコンピュータプログラムは、コンピュータを、（１）～（５）のいずれか１つに記載のなりすまし検出装置として機能させる。
かかるコンピュータプログラムは、上記（１）～（５）のなりすまし検出装置と同様の効果を奏する。
【００２０】
［実施の形態の詳細］
以下に、図面を参照しつつ、好ましい実施の形態について説明する。以下の説明では、同一の部品および構成要素には同一の符号を付してある。それらの名称および機能も同じである。したがって、これらの説明は繰り返さない。
【００２１】
＜第１の実施の形態＞
〔車両構成〕
図１は第１の実施の形態にかかる車両の構成を表した概略図である。
図１を参照して、本実施の形態にかかる車両１は、車外装置と通信するための車外通信機１５と、複数のＥＣＵ（Electronic Control Unit）３０Ａ，３０Ｂ，３０Ｃ，…と、車外装置と複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃ，…との通信を中継するＥＣＵである中継装置１０と、これらに電力を供給するバッテリ４０と、電源制御装置２０と、を含む。複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃ，…を代表させてＥＣＵ３０とも称する。複数のＥＣＵ３０それぞれを区別するときには、ＥＣＵ－１，ＥＣＵ－２，ＥＣＵ－３，…とも表現する。バッテリ４０は、メインバッテリおよびサブバッテリからなるものであってもよい。
【００２２】

各ＥＣＵ３０は、中継装置１０において終端する車内通信線１６によって接続されて、中継装置１０とともに車内の通信ネットワーク４を構成する。通信ネットワーク４はＥＣＵ３０同士の通信を可能とする、バス型の通信ネットワーク（たとえば、ＣＡＮ（Controller Area Network））よりなる。この通信方式のネットワークでは、データフレームと呼ばれるフォーマットに情報を格納して送受信される。

【００２３】

通信ネットワーク４は、ＣＡＮだけでなく、ＬＩＮ（Local Interconnect Network）、ＣＡＮＦＤ（ＣＡＮ with Flexible Data Rate）、Ｅｔｈｅｒｎｅｔ（登録商標）、又はＭＯＳＴ（Media Oriented Systems Transport：ＭＯＳＴは登録商標）などの通信規格を採用するネットワークであってもよい。

【００２４】

ＥＣＵ３０は、たとえば、アクセル、ブレーキ、ハンドルの操作に対してエンジンやブレーキ、ＥＰＳ（Electric Power Steering）等の制御を行うパワー・トレイン系ＥＣＵ、スイッチ操作に応じて車内照明やヘッドライトの点灯／消灯と警報器の吹鳴等の制御を行うボディ系ＥＣＵ、運転席近傍に配設されるメータ類の動作を制御するメータ系ＥＣＵなどである。

【００２５】

中継装置１０は、さらに、所定規格の通信線を介して車外通信機１５と接続されている。または、中継装置１０は、車外通信機１５を搭載していてもよい。車外通信機１５は、インターネット等の広域通信網２を介して、車外装置と無線通信する。車外装置は、たとえば、ＥＣＵ３０の更新用プログラムを保存するサーバ５である。または、車外通信機１５は図示しないプラグを有し、当該プラグに接続された車外装置と有線にて通信してもよい。車外通信機１５は、ユーザが所有する携帯電話機、スマートフォン、タブレット型端末、ノートＰＣ（Personal Computer）等の装置であってもよい。

【００２６】

中継装置１０は、車外装置から車外通信機１５が受信した情報をＥＣＵ３０に中継する。また、中継装置１０は、ＥＣＵ３０から受信した情報を車外通信機１５に中継する。車外通信機１５は、中継された情報を車外装置に無線送信する。

【００２７】

バッテリ４０は、電力線１８を介して電源制御装置２０と接続され、電源制御装置２０は、電力線１７Ａ，１７Ｂ，１７Ｃ，…を介してＥＣＵ３０Ａ，３０Ｂ，３０Ｃ…それぞれと接続されている。電力線１７Ａ，１７Ｂ，１７Ｃ，…を代表させて電力線１７とも称する。

【００２８】

中継装置１０は、さらに、車内通信線１６を介して電源制御装置２０と接続されている。または、中継装置１０は、電源制御装置２０を搭載していてもよい。電源制御装置２０は、バッテリ４０からＥＣＵ３０への電力供給を制御する。

【００２９】

〔中継装置の構成〕

図２は、中継装置１０の内部構成を示すブロック図である。

図２に示すように、中継装置１０は、制御部１１、記憶部１２、および車内通信部１３などを備える。

【００３０】

中継装置１０の制御部１１は、ＣＰＵ（Central Processing Unit）を含むマイコンからなる。マイコンの種類は特定の種類に限定されない。制御部１１のＣＰＵは、記憶部１２に記憶された１または複数のプログラムを読み出して各種処理を実行するための機能を有している。

制御部１１のＣＰＵは、たとえば時分割で複数のプログラムを切り替えて実行することにより、複数のプログラムを並列的に実行可能である。

【００３１】

制御部１１のＣＰＵは、１または複数の大規模集積回路（ＬＳＩ）を含む。複数のＬＳＩを含むＣＰＵでは、複数のＬＳＩが協働して当該ＣＰＵの機能を実現する。

【００３２】

制御部１１のＣＰＵが実行するコンピュータプログラムは、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの記録媒体に記録した状態で譲渡することもできるし、サーバコンピュータなどのコンピュータ装置からのダウンロードによって譲渡することもできる。

【００３３】

記憶部１２は、フラッシュメモリ若しくはＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）などの不揮発性のメモリ素子よりなる。

記憶部１２は、制御部１１のＣＰＵが実行するプログラムまたは実行に必要なデータなどを記憶する記憶領域を有する。

【００３４】

車内通信部１３には車内通信線１６が接続されている。車内通信部１３は、ＣＡＮなどの所定の通信規格に則って、ＥＣＵ３０と通信する通信装置よりなる。

車内通信部１３は、制御部１１のＣＰＵから与えられた情報を所定のＥＣＵ３０宛てに送信し、ＥＣＵ３０が送信元の情報を制御部１１のＣＰＵに与える。

【００３５】

車外通信機１５は、アンテナと、アンテナからの無線信号の送受信を実行する通信回路とを含む無線通信機よりなる。車外通信機１５は、携帯電話網等の広域通信網２に接続されることにより車外装置との通信が可能である。

車外通信機１５は、図示しない基地局により形成される広域通信網２を介して、制御部１１のＣＰＵから与えられた情報をサーバ５等の車外装置に送信するとともに、車外装置から受信した情報を制御部１１のＣＰＵに与える。

【００３６】

〔電源制御装置の構成〕

図３は、電源制御装置２０の内部構成を示すブロック図である。

図３に示すように、電源制御装置２０は、制御部２１、記憶部２２、および車内通信部２３などを備える。

【００３７】

電源制御装置２０の制御部２１はＣＰＵを含むマイコンからなる。マイコンの種類は特定の種類に限定されない。制御部２１のＣＰＵは、記憶部２２に記憶された１または複数のプログラムを読み出して、各種処理を実行するための機能を有している。

制御部２１のＣＰＵは、たとえば時分割で複数のプログラムを切り替えて実行することにより、複数のプログラムを並列的に実行可能である。

【００３８】

制御部２１のＣＰＵは、１または複数の大規模集積回路（ＬＳＩ）を含む。複数のＬＳＩを含むＣＰＵでは、複数のＬＳＩが協働して当該ＣＰＵの機能を実現する。

【００３９】

制御部２１のＣＰＵが実行するコンピュータプログラムは、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの記録媒体に記録した状態で譲渡することもできるし、サーバコンピュータなどのコンピュータ装置からのダウンロードによって譲渡することもできる。

【００４０】

記憶部２２は、フラッシュメモリ若しくはＥＥＰＲＯＭなどの不揮発性のメモリ素子よりなる。

記憶部２２は、制御部２１のＣＰＵが実行するプログラムおよび実行に必要なデータなどを記憶する記憶領域を有する。

【００４１】

車内通信部２３には車内通信線１６が接続されている。車内通信部２３は、ＣＡＮなどの所定の通信規格に則って、中継装置１０と通信する通信装置よりなる。

車内通信部２３は、制御部２１のＣＰＵから与えられた情報を所定の中継装置１０宛て

に送信し、中継装置１０が送信元の情報を制御部２１のＣＰＵに与える。

【００４２】

電源制御装置２０は、さらに、バッテリ４０と電力線１８を介して接続されたメインスイッチ２５と、ＥＣＵ３０Ａに電力線１７Ａを介して接続された第１個別スイッチ２７Ａ、ＥＣＵ３０Ｂに電力線１７Ｂを介して接続された第２個別スイッチ２７Ｂ、ＥＣＵ３０Ｃに電力線１７Ｃを介して接続された第３個別スイッチ２７Ｃ、…と、を含み、個別スイッチ２７Ａ，２７Ｂ，２７Ｃ，…は、それぞれメインスイッチ２５および電力線１８を介してバッテリ４０と接続されている。個別スイッチ２７Ａ，２７Ｂ，２７Ｃ，…を代表させて個別スイッチ２７とも称する。

【００４３】

メインスイッチ２５および個別スイッチ２７は電力供給を許容、遮断する機能を有する回路であって、たとえば、トランジスタ、ＦＥＴ（Field Effect Transistor：電界効果トランジスタ）、および、リレー回路、などを含む回路である。

【００４４】

電源制御装置２０は、さらに、メインスイッチ２５を駆動するための第１駆動回路２４と、個別スイッチ２７それぞれを独立して駆動するための第２駆動回路２６と含む。これら駆動回路２４，２６は制御部２１に接続されて、制御部２１の制御に従ってそれぞれメインスイッチ２５および個別スイッチ２７を駆動する。

【００４５】

メインスイッチ２５の駆動は、ＯＮ状態またはＯＦＦ状態を他方状態に切り替えることである。第１駆動回路２４は、制御部２１のＣＰＵからの制御信号に従って、メインスイッチ２５をＯＮ状態からＯＦＦ状態、または、ＯＦＦ状態からＯＮ状態に切り替える。従って、メインスイッチ２５は、ＯＮ状態、または、ＯＦＦ状態のいずれか一方の状態を採る。

【００４６】

個別スイッチ２７の駆動は、一例として、それぞれ独立して、ＯＮ状態またはＯＦＦ状態を他方状態に切り替えることである。第２駆動回路２６は、制御部２１のＣＰＵからの制御信号に従って、個別スイッチ２７を個別に、ＯＮ状態からＯＦＦ状態、または、ＯＦＦ状態からＯＮ状態に切り替える。従って、ＥＣＵ３０Ａ，３０Ｂ，３０Ｃそれぞれに対応した個別スイッチ２７Ａ，２７Ｂ，２７Ｃは、以下のＯＮ状態またはＯＦＦ状態の組合せを採り得る。

１）ＥＣＵ３０Ａ（ＯＮ）、ＥＣＵ３０Ｂ（ＯＮ）、ＥＣＵ３０Ｃ（ＯＮ）
２）ＥＣＵ３０Ａ（ＯＮ）、ＥＣＵ３０Ｂ（ＯＮ）、ＥＣＵ３０Ｃ（ＯＦＦ）
３）ＥＣＵ３０Ａ（ＯＮ）、ＥＣＵ３０Ｂ（ＯＦＦ）、ＥＣＵ３０Ｃ（ＯＮ）
４）ＥＣＵ３０Ａ（ＯＮ）、ＥＣＵ３０Ｂ（ＯＦＦ）、ＥＣＵ３０Ｃ（ＯＦＦ）
５）ＥＣＵ３０Ａ（ＯＦＦ）、ＥＣＵ３０Ｂ（ＯＮ）、ＥＣＵ３０Ｃ（ＯＮ）
６）ＥＣＵ３０Ａ（ＯＦＦ）、ＥＣＵ３０Ｂ（ＯＮ）、ＥＣＵ３０Ｃ（ＯＦＦ）
７）ＥＣＵ３０Ａ（ＯＦＦ）、ＥＣＵ３０Ｂ（ＯＦＦ）、ＥＣＵ３０Ｃ（ＯＮ）
８）ＥＣＵ３０Ａ（ＯＦＦ）、ＥＣＵ３０Ｂ（ＯＦＦ）、ＥＣＵ３０Ｃ（ＯＦＦ）

【００４７】

メインスイッチ２５がＯＮ状態の場合、個別スイッチ２７がＯＮ状態のＥＣＵ３０にのみバッテリ４０から電力が供給される。上記１）ではＥＣＵ３０Ａ，３０Ｂ，３０Ｃに電力が供給される。上記２）ではＥＣＵ３０Ａ，３０Ｂに電力が供給され、ＥＣＵ３０Ｃには供給されない。

【００４８】

メインスイッチ２５がＯＦＦ状態の場合、個別スイッチ２７の状態に関わらず、すべてのＥＣＵ３０にバッテリ４０から電力が供給されない。

【００４９】

車両１には、ユーザ（ドライバー）が操作可能な、図示しない電源スイッチが備えられ、制御部２１は、電源スイッチに対して電源ＯＮの操作が行われると第１駆動回路２４に

メインスイッチ２５をＯＮ状態にさせる。また、電源ＯＦＦの操作が行われると第１駆動回路２４にメインスイッチ２５をＯＦＦ状態にさせる。

制御部２１は、後述する中継装置１０での検出処理に従って個別スイッチ２７を個別に駆動する。そのため、制御部２１は、個別スイッチ２７を個別に駆動することによって各ＥＣＵ３０への電力供給を制御する電源制御部２１１を含む。この機能は、制御部２１のＣＰＵが記憶部２２に記憶されているプログラムを読み出して実行することによって、主にＣＰＵによって実現される。

【００５０】

〔検出処理〕

車両１の走行中には、通信ネットワーク４では数多くのデータフレームが送受信されている。中継装置１０の制御部１１は、通信ネットワーク４におけるＥＣＵ３０間の通信を制御する通信制御部１１１を有する（図２）。この機能は、制御部１１のＣＰＵが記憶部１２に記憶されているプログラムを読み出して実行することによって、主にＣＰＵによって実現される。

【００５１】

通信ネットワーク４で送受信されるデータフレームには送信元のＥＣＵを示す識別情報（ＩＤ）が含まれる。悪意ある第三者の通信ノードが通信ネットワーク４にアクセスし、送信元のＩＤを詐称してあるＥＣＵ３０（たとえばＥＣＵ３０Ａ）のＩＤとしたデータフレームを通信ネットワーク４に送信すると、当該データフレームを受信した他のＥＣＵ３０は、当該データフレームの送信元を上記ＥＣＵ３０（たとえばＥＣＵ３０Ａ）と認識する。この状態は、あるＥＣＵ３０が上記通信ノードによってなりすまされている状態であって、当該あるＥＣＵ３０が被詐称ＥＣＵとなる。以降の説明では、送信元を詐称した通信を詐称通信とも称する。

【００５２】

本実施の形態においては、中継装置１０がなりすまし検出装置として機能する。なりすまし検出装置として機能する中継装置１０の制御部１１は、複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃのうちの１台のＥＣＵ（たとえばＥＣＵ３０Ａ）について、当該ＥＣＵを被詐称ＥＣＵとした詐称通信の存在、つまり、当該ＥＣＵを詐称する通信ノード（なりすまし）の存在を検出する検出処理を実行する。以降の説明において、被詐称ＥＣＵとした詐称通信を検出する対象となる、複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃのうちの１台のＥＣＵを対象ＥＣＵ、対象ＥＣＵ以外のＥＣＵを非対象ＥＣＵと称する。

【００５３】

複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃのうちの１台のＥＣＵが対象ＥＣＵとされる。対象ＥＣＵは、複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃの中から予め規定された順に決定されてもよい。これにより、複数のＥＣＵ３０Ａ，３０Ｂ，３０Ｃすべてが、順に、対象ＥＣＵとして、詐称通信の存在が検出される。

【００５４】

他の例として、対象ＥＣＵは、後述する、被詐称ＥＣＵである可能性のあるＥＣＵの判定結果に基づいて決定されてもよい。これにより、被詐称ＥＣＵである可能性のあるＥＣＵを対象ＥＣＵとして詐称通信の存在が検出されるため、高精度で詐称通信の存在が検出される。

【００５５】

図２を参照して、中継装置１０の制御部１１は、検出処理を実行するための機能として、通信制御部１１１と、取得部１１２と、検出部１１３と、通知部１１４と、を有する。これら機能は、制御部１１のＣＰＵが記憶部１２に記憶されているプログラムを読み出して実行することによって、主にＣＰＵによって実現される。

【００５６】

検出処理は、対象ＥＣＵに対する電力供給を遮断、許容する電源制御処理を含む。通信制御部１１１は、対象ＥＣＵの個別スイッチ２７のＯＮ／ＯＦＦ状態を独立して切り替えることを指示する制御信号を車内通信部１３に渡し、電源制御装置２０に送信させる。こ

の制御信号に従って、電源制御装置２０の電源制御部２１１は、対象ＥＣＵの個別スイッチ２７のＯＮ／ＯＦＦ状態を切り替える。これらの機能により、電源制御処理が実行される。

【００５７】

好ましくは、電源制御処理は対象ＥＣＵの個別スイッチ２７をＯＮ状態からＯＦＦ状態に切り替えることの可否を、車両１の走行状態に基づいて判定する処理を含む。たとえば、対象ＥＣＵが車両１の現在の走行状態に必要な機能を制御するＥＣＵである場合、切替が否と判定される。車両１の現在の走行状態に必要であっても、後述する検出処理に要する時間程度であれば電力供給が遮断されてもよい場合には、切替が可と判定される。通信制御部１１１は、切替が可と判定した場合に、対象ＥＣＵの個別スイッチ２７をＯＦＦ状態とする制御信号を電源制御装置２０に送信させる。

【００５８】

さらに、通信制御部１１１は、通信ネットワーク４の通信状態を取得する。通信ネットワーク４の通信状態は、各ＥＣＵ３０について当該ＥＣＵ３０のＩＤが送信元ＩＤであるデータフレームが車内通信線１６で転送されているか否か、つまり、対象ＥＣＵを送信元とする通信が生じているか否かの判定結果を含む。通信制御部１１１は、車内通信部１３によって受信された、車内通信線１６で転送されるすべてのデータフレームを解析して、各データフレームに含まれる送信元ＩＤを取得することによって、各ＥＣＵ３０について当該ＥＣＵ３０を送信元とするデータフレームが車内通信線１６で転送されているか否かを判定可能である。取得部１１２は、通信制御部１１１から通信ネットワーク４の通信状態を取得する。

【００５９】

上記のように、被詐称ＥＣＵである可能性のあるＥＣＵの判定結果に基づいて対象ＥＣＵを特定する場合、取得部１１２は、通信制御部１１１から取得した通信ネットワーク４の通信状態より、各ＥＣＵ３０についての当該ＥＣＵ３０を送信元とするデータフレームの転送頻度を特定する。転送頻度は、たとえば、所定時間内における同一のＥＣＵ３０を送信元としたデータフレームの転送回数、または、同一のＥＣＵ３０を送信元としたデータフレームの転送間隔などである。

【００６０】

通信制御部１１１は、取得部１１２で特定された各ＥＣＵ３０の当該ＥＣＵ３０を送信元とするデータフレームの転送頻度に基づいて上記判定を実行する。一例として、電源制御部２１１は、データフレームの転送頻度が、予め記憶している閾値より高い送信元のＥＣＵが被詐称ＥＣＵの可能性があると判定する。本来のＥＣＵ３０から送信されるデータフレームに加えて送信元を参詐称したデータフレームが追加されることによって、当該ＥＣＵ３０を送信元とするデータフレームの転送頻度が高くなっている可能性があるためである。閾値は、学習によってＥＣＵ３０ごとに設定されるものであってもよい。

【００６１】

検出部１１３は、対象ＥＣＵの電源状態と通信ネットワーク４の通信状態とに基づいて、当該対象ＥＣＵについて当該対象ＥＣＵを被詐する通信ノードの存在を検出する。具体的に、検出部１１３は、対象ＥＣＵの個別スイッチ２７がＯＦＦ状態において、当該対象ＥＣＵを送信元とする通信が生じている場合に、当該対象ＥＣＵを被詐する通信ノードが存在すると検出する。そうでない場合には、当該通信ノードの存在が検出されない。電力供給が遮断されている対象ＥＣＵからはデータフレームが送信されることがないため、対象ＥＣＵの個別スイッチ２７がＯＦＦ状態において当該対象ＥＣＵを送信元とするデータフレームが転送されている場合には、そのデータフレームの真の送信元は対象ＥＣＵではないためである。

【００６２】

通知部１１４は、検出部１１３において当該対象ＥＣＵを被詐する通信ノードの存在が検出された場合に、被詐称ＥＣＵである対象ＥＣＵを非対象ＥＣＵに通知する。

好ましくは、通知部１１４は、検出結果、および／または、被詐称ＥＣＵをユーザに通

知する処理を実行する。ユーザに通知する処理は、たとえば、図示しない表示装置で表示するための処理や、図示しないブザー等の音声出力装置で音声出力するための処理である。表示装置は、たとえば、インジケータ、ナビゲーション装置のディスプレイ、または、マルチファンクションディスプレイ、などの、車内のユーザが視認可能な表示装置である。この場合、通知部１１４は検出結果の出力を指示するコマンドを含むデータフレームを生成し、車内通信部１３に上記の表示装置や音声出力装置を制御するＥＣＵ３０に対して当該データフレームを送信させる。

【００６３】

または、ユーザに通知する処理は、予め登録された通信装置に送信する処理であってもよい。通信装置は、たとえば、スマートフォン、携帯電話、および、タブレット端末などである。この場合、通知部１１４は検出結果を表したメッセージの指定した通信装置への送信を指示するデータフレームを生成し、車外通信機１５に、指定された通信装置へメッセージを送信させる。

【００６４】

図４は、制御部１１が実行する第１の実施の形態にかかる検出処理の流れを表したフローチャートである。中継装置１０の制御部１１は、記憶部１２に記憶されているプログラムを読み出して実行することによって図４のフローチャートに表された処理を実行する。中継装置１０の制御部１１は、車両１の停車中に図４に示された検出処理を繰り返し実行する。

【００６５】

図４を参照して、制御部１１は通信ネットワーク４の通信状態を取得し、各ＥＣＵ３０を送信元としたデータフレームの転送頻度を予め記憶している閾値と比較する。この比較に基づいて、各ＥＣＵ３０について被詐称ＥＣＵである可能性の有無を判定する（ステップＳ１０１）。

【００６６】

あるＥＣＵ３０について、当該ＥＣＵ３０を送信元としたデータフレームの転送頻度が閾値よりも高い場合、制御部１１は当該ＥＣＵ３０が被詐称ＥＣＵである可能性が有ると判定する（ステップＳ１０１でＹＥＳ）。この場合、制御部１１は、当該ＥＣＵ３０を対象ＥＣＵとして以降の処理を実行する。

【００６７】

制御部１１は、車両１の走行状態に基づいて対象ＥＣＵの個別スイッチ２７をＯＦＦ状態に切り替えることの可否を判定する（ステップＳ１０３）。切替が可能な状態である場合（ステップＳ１０３でＹＥＳ）、制御部１１は、当該個別スイッチ２７をＯＦＦ状態とすることを電源制御装置２０に指示する（ステップＳ１０５）。これにより、対象ＥＣＵに対する電力供給が遮断される。

【００６８】

制御部１１は、通信ネットワーク４の通信状態に基づいて、対象ＥＣＵに対する電力供給が遮断されている状態において通信ネットワーク４で対象ＥＣＵを送信元とする通信が生じているか否かを判定する（ステップＳ１０７）。通信ネットワーク４において対象ＥＣＵを送信元とするデータフレームが転送されている場合（ステップＳ１０７でＹＥＳ）、制御部１１は対象ＥＣＵを詐称する通信ノードの存在を検出する（ステップＳ１０９）。

【００６９】

そうでない場合には（ステップＳ１０７でＮＯ）、制御部１１は、対象ＥＣＵを詐称する通信ノードの存在を検出せず、対象ＥＣＵの個別スイッチ２７をＯＮ状態に戻すことを電源制御装置２０に指示する（ステップＳ１１９）。これにより、対象ＥＣＵに対する電力供給が再開される。

【００７０】

詐称通信の存在が検出されると、制御部１１は、非対象ＥＣＵに被詐称ＥＣＵである対象ＥＣＵ（のＩＤ）を通知する（ステップＳ１１１）。これにより、非対象ＥＣＵは、被

詐称ＥＣＵが送信元であるデータフレームを破棄する、などの予め規定された処理を実行することができる。

【００７１】

好ましくは、ステップＳ１１１で制御部１１は、インジケータ、ナビゲーション装置のディスプレイ、または、マルチファンクションディスプレイ、などの、車内のユーザが視認可能な表示装置や、ブザー等の音声出力装置によって、検出結果、および／または、被詐称ＥＣＵを通知する。これにより、運転者などの車内のユーザはＥＣＵ３０になりすましたデータフレームを送信している通信ノードの存在を知ることができる。

【００７２】

また、好ましくは、ステップＳ１１１で制御部１１は、予め登録された通信装置にメッセージを送信することによって検出結果、および／または、被詐称ＥＣＵを通知する。これにより、ユーザが車外であっても、ＥＣＵ３０になりすましたデータフレームを送信している通信ノードの存在を知ることができる。

【００７３】

通知の後、制御部１１は、対象ＥＣＵの個別スイッチ２７をＯＮ状態に戻すことを電源制御装置２０に指示する（ステップＳ１１３）。これにより、対象ＥＣＵに対する電力供給が再開される。

【００７４】

〔第１の実施の形態の効果〕

第１の実施の形態にかかる車両１は、ＥＣＵ３０ごとの個別スイッチ２７を有し、電源制御装置２０がＥＣＵ３０ごとに独立して個別スイッチ２７のＯＮ／ＯＦＦを切り替える。これにより、各ＥＣＵ３０を個別に対象ＥＣＵとして、対象ＥＣＵへの電力供給を遮断させることができる。

【００７５】

対象ＥＣＵへの電力供給が遮断された状態において対象ＥＣＵを送信元とするデータフレームが車内通信線１６で転送されている場合、当該データフレームの真の送信元は対象ＥＣＵではない。そのため、対象ＥＣＵの個別スイッチ２７がＯＦＦ状態において、当該対象ＥＣＵを送信元とする通信が生じているか否かの判定結果に基づいて、当該ＥＣＵを詐称する通信ノードの存在、すなわちなりすましの存在を容易に検出できる。

【００７６】

電源制御装置２０がＥＣＵ３０ごとに独立して個別スイッチ２７のＯＮ／ＯＦＦを切り替えることによって、いずれのＥＣＵ３０についても、それぞれを対象ＥＣＵとして当該対象ＥＣＵを詐称する通信ノードの存在、すなわちなりすましの存在を検出できる。

【００７７】

＜第２の実施の形態＞

第２の実施の形態では、中継装置１０は、検出処理において、対象ＥＣＵの安全性のレベルに応じた電源制御処理を実行する。安全性のレベルは、たとえば、ＩＳＯ（International Organization for Standardization（国際標準化機構））の規定するＩＳＯ２６２６２機能安全規格が知られている。ＩＳＯ ２６２６２規格は、機能安全の指標としてＡＳＩＬ（Automotive Safety Integrity Level：安全性要求レベル）を規定し、各安全要求にＱＭ（Quality Management），Ａ，Ｂ，Ｃ，Ｄのレベルを割り当てる。Ｄが割り当てられた機能は最も高いレベルの安全方策が求められ、Ａが割り当てられた機能は最も低い。ＱＭが割り当てられた機能は、安全性と関連がないことを指す。この場合、中継装置１０の制御部１１は、ＥＣＵ３０ごとのＡＳＩＬのレベルを予め記憶している。

【００７８】

図５は、制御部１１が実行する第２の実施の形態にかかる検出処理の流れを表したフローチャートである。第２の実施の形態にかかる検出処理は、図４の第１の実施の形態にかかる検出処理と比較してステップＳ２０１の処理が含まれている点が異なる。そこで、ここでは第１の実施の形態にかかる検出処理と異なる点を説明する。

【００７９】

図５を参照して、制御部１１は、詐称通信の存在が検出され、非対象ＥＣＵに被詐称ＥＣＵである対象ＥＣＵ（のＩＤ）を通知すると（ステップＳ１１１）、対象ＥＣＵのＡＳＩＬレベルが所定レベル以上高い（たとえば「Ｄ」である）場合には（ステップＳ２０１でＹＥＳ）、対象ＥＣＵの個別スイッチ２７をＯＮ状態に戻すことを電源制御装置２０に指示することなくＯＦＦ状態を維持して、一連の検出動作を終了する。これにより、対象ＥＣＵへの電力供給が遮断された状態が維持され、対象ＥＣＵはデータフレームを送信することがなくなる。すなわち、被詐称ＥＣＵである対象ＥＣＵは通信ネットワーク４から切り離される。

【００８０】

好ましくは、上記ステップＳ１１１での通知の際に、被詐称ＥＣＵである対象ＥＣＵのＡＳＩＬレベルが所定レベル以上高い場合には（ステップＳ２０１でＹＥＳ）、制御部１１は、非対象ＥＣＵに対して対象ＥＣＵを送信元とするデータフレームを受信しないように通知してもよい。

【００８１】

〔第２の実施の形態の効果〕

第２の実施の形態にかかる電源制御処理を含む検出処理が実行されることによって、安全性のレベルの高いＥＣＵを詐称する通信ノードの存在が検出された場合には当該詐称通信の解消の有無に関わらずに被詐称ＥＣＵである対象ＥＣＵが通信ネットワーク４から切り離される。または、当該検出以降は非対象ＥＣＵが被詐称ＥＣＵである対象ＥＣＵを送信元とするデータフレームを受信しなくなる。これにより、車両における安全性を確保することができる。

【００８２】

＜変形例＞

第２の実施の形態の変形例として、詐称通信が解消された場合（図４のステップＳ１１５でＹＥＳの場合に）、被詐称ＥＣＵであった対象ＥＣＵの安全性のレベルに応じた電源制御処理を実行してもよい。すなわち、第２の実施の形態にかかる検出処理の変形例では、詐称通信が解消された場合であっても（ステップＳ１１５でＹＥＳ）、被詐称ＥＣＵであった対象ＥＣＵのＡＳＩＬレベルが所定レベル以上高い（たとえば「Ｄ」である）場合には、ステップＳ１１７で非対象ＥＣＵに当該対象ＥＣＵのＩＤを通知することなく、また、ステップＳ１１９で対象ＥＣＵの個別スイッチ２７をＯＮ状態に戻すことを電源制御装置２０に指示することなく、一連の検出動作を終了する。

【００８３】

これにより、被詐称ＥＣＵであった対象ＥＣＵの安全性のレベルが所定レベル以上高い場合には、詐称通信が解消された場合であっても電力供給が遮断された状態が維持され、対象ＥＣＵはデータフレームを送信することがなくなる。すなわち、被詐称ＥＣＵであった対象ＥＣＵは通信ネットワーク４から切り離される。また、詐称通信が解消された場合であっても非対象ＥＣＵは被詐称ＥＣＵであった対象ＥＣＵについての詐称通信への対処を維持する。これにより、車両における安全性を確保することができる。

【００８４】

＜第３の実施の形態＞

中継装置１０に替えて電源制御装置２０がなりすまし検出装置として機能してもよい。この場合、電源制御装置２０の制御部２１１は、図３に示されたように、取得部２１２、検出部２１３、および、通知部２１４を有し、以上の検出処理を実行してもよい。さらには、中継装置１０と電源制御装置２０とが、協働して検出処理を実行してもよい。すなわち、なりすまし検出装置は、複数の車載装置によって実現されてもよい。

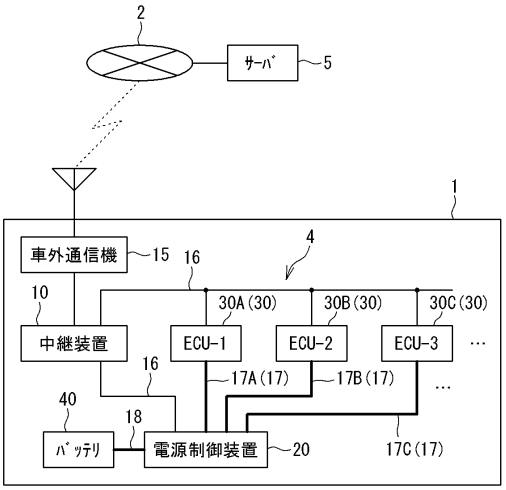
【００８５】

開示された特徴は、１つ以上のモジュールによって実現される。たとえば、当該特徴は、回路素子その他のハードウェアモジュールによって、当該特徴を実現する処理を規定したソフトウェアモジュールによって、または、ハードウェアモジュールとソフトウェアモジュールとの組み合わせによって実現され得る。

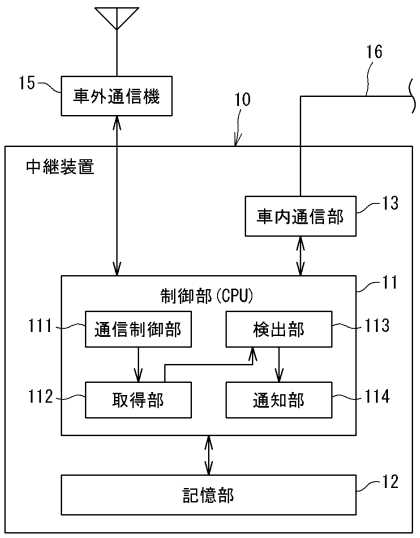
【００８６】
上述の動作をコンピュータに実行させるための、１つ以上のソフトウェアモジュールの組み合わせであるプログラムとして提供することもできる。このようなプログラムは、コンピュータに付属するフレキシブルディスク、ＣＤ－ＲＯＭ（Compact Disk-Read Only Memory）、ＲＯＭ、ＲＡＭおよびメモリカードなどのコンピュータ読取り可能な記録媒体にて記録させて、プログラム製品として提供することもできる。あるいは、コンピュータに内蔵するハードディスクなどの記録媒体にて記録させて、プログラムを提供することもできる。また、ネットワークを介したダウンロードによって、プログラムを提供することもできる。
【００８７】
なお、本開示にかかるプログラムは、コンピュータのオペレーティングシステム（ＯＳ）の一部として提供されるプログラムモジュールのうち、必要なモジュールを所定の配列で所定のタイミングで呼出して処理を実行させるものであってもよい。その場合、プログラム自体には上記モジュールが含まれずＯＳと協働して処理が実行される。このようなモジュールを含まないプログラムも、本開示にかかるプログラムに含まれ得る。
【００８８】
また、本開示にかかるプログラムは他のプログラムの一部に組込まれて提供されるものであってもよい。その場合にも、プログラム自体には上記他のプログラムに含まれるモジュールが含まれず、他のプログラムと協働して処理が実行される。このような他のプログラムに組込まれたプログラムも、本開示にかかるプログラムに含まれ得る。提供されるプログラム製品は、ハードディスクなどのプログラム格納部にインストールされて実行される。なお、プログラム製品は、プログラム自体と、プログラムが記録された記録媒体とを含む。
【００８９】
今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。
【符号の説明】
【００９０】
１　車両
２　広域通信網
４　通信ネットワーク
５　サーバ
１０　中継装置
１１　制御部
１２　記憶部
１３　車内通信部
１５　車外通信機
１６　車内通信線
１７，１７Ａ，１７Ｂ，１７Ｃ　電力線
１８　電力線
２０　電源制御装置
２１　制御部
２２　記憶部
２３　車内通信部
２４　第１駆動回路
２５　メインスイッチ
２６　第２駆動回路
２７　個別スイッチ

２７Ａ　第１個別スイッチ
２７Ｂ　第２個別スイッチ
２７Ｃ　第３個別スイッチ
３０，３０Ａ，３０Ｂ，３０Ｃ　ＥＣＵ
４０　バッテリ
１１１　通信制御部
１１２　取得部
１１３　検出部
１１４　通知部
２１１　電源制御部
２１２　取得部
２１３　検出部
２１４　通知部

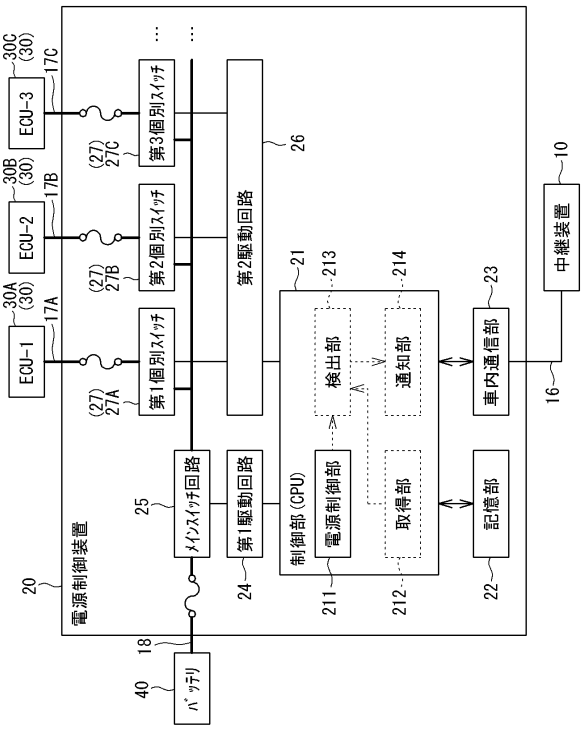
【図１】
図１



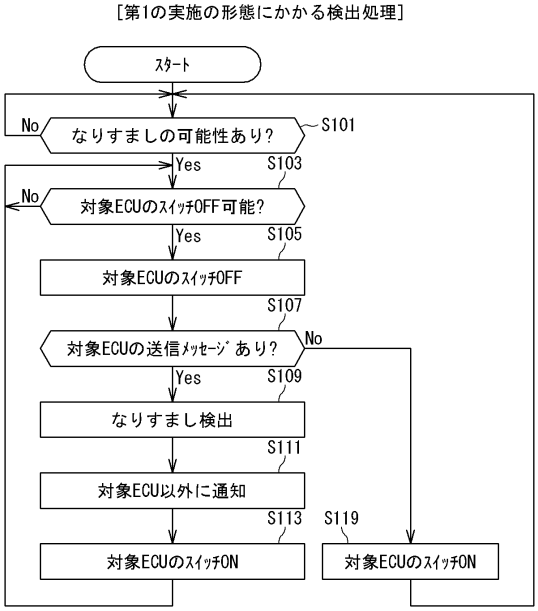
【図２】
図２



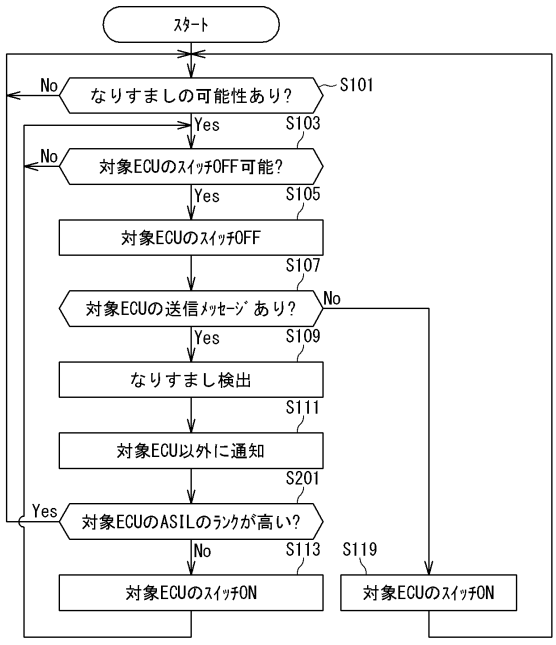
【図３】
図３



【図４】
図４



【図５】
図５



フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　１２／２８
Ｇ０６Ｆ　２１／４４