(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7581069号
(P7581069)

(45)発行日　令和6年11月12日(2024.11.12)

(24)登録日　令和6年11月1日(2024.11.1)

(51)国際特許分類			FI		
G06F	*21/55*	*(2013.01)*	G06F	21/55	
G06F	*21/57*	*(2013.01)*	G06F	21/57	350
G06F	*21/31*	*(2013.01)*	G06F	21/31	
B60R	*16/02*	*(2006.01)*	B60R	16/02	660Z

請求項の数　5　（全10頁）

(21)出願番号　特願2021-15054(P2021-15054)
(22)出願日　令和3年2月2日(2021.2.2)
(65)公開番号　特開2022-118486(P2022-118486A)
(43)公開日　令和4年8月15日(2022.8.15)
審査請求日　令和6年1月15日(2024.1.15)

(73)特許権者　000005348
株式会社ＳＵＢＡＲＵ
東京都渋谷区恵比寿一丁目２０番８号
(74)代理人　110000383
弁理士法人エビス国際特許事務所
(72)発明者　大嶋 宏典
東京都渋谷区恵比寿一丁目２０番８号
株式会社ＳＵＢＡＲＵ内
(72)発明者　飯波 久太郎
東京都渋谷区恵比寿一丁目２０番８号
株式会社ＳＵＢＡＲＵ内
(72)発明者　関 晃一
東京都渋谷区恵比寿一丁目２０番８号
株式会社ＳＵＢＡＲＵ内
審査官　三森 雄介

最終頁に続く

(54)【発明の名称】　車両用制御装置

(57)【特許請求の範囲】

【請求項１】

車両に搭載された制御対象を制御する制御部と、

前記車両内への人の不正侵入の有無を示す不正侵入情報を格納した記憶部と、

前記不正侵入情報に基づいて、前記制御部に対するセキュアブート処理の要否を、前記制御部の起動前に判定する要否判定部と、を備え、

前記不正侵入情報は、前記制御部の前回の起動後に実行される不正侵入判定処理によって生成されて前記記憶部に格納されるものであり、

前記要否判定部は、

前記不正侵入情報が前記車両への人の不正侵入ありを示す場合に、前記制御部の起動前に前記制御部に対するセキュアブート処理を実行し、

前記不正侵入情報が前記車両への人の不正侵入なしを示す場合に、前記制御部に対するセキュアブート処理を実行せずに、前記制御部の起動を許可する、

車両用制御装置。

【請求項２】

車両に搭載された制御対象を制御する制御部と、

前記車両内への人の不正侵入の有無を示す不正侵入情報を格納した記憶部と、

前記不正侵入情報に基づいて、前記制御部に対するセキュアブート処理の要否を、前記制御部の起動前に判定する要否判定部と、を備えた車両用制御装置であって、

前記不正侵入情報は、前記制御部の前回の起動後に実行される不正侵入判定処理によって

生成されて前記記憶部に格納されるものであり、
前記車両用制御装置が行う不正侵入判定処理は、
前記車両のドアの解錠時に使用されたキーと前記車両に予め登録されている認証キーとが一致するか否かを判定し、
前記使用されたキーと前記認証キーとが一致している場合に、前記車両への人の不正侵入なしを示す前記不正侵入情報を前記記憶部に格納し、
前記使用されたキーと前記認証キーとが一致していない場合に、前記車両への人の不正侵入ありを示す前記不正侵入情報を前記記憶部に格納し、
前記要否判定部は、
前記不正侵入情報が前記車両への人の不正侵入ありを示す場合に、前記制御部の起動前に前記制御部に対するセキュアブート処理を実行し、
前記不正侵入情報が前記車両への人の不正侵入なしを示す場合に、前記制御部に対するセキュアブート処理を実行せずに、前記制御部の起動を許可する、
車両用制御装置。
【請求項３】
前記車両用制御装置が行う不正侵入判定処理は、
カメラによって撮像された前記車両の乗員の画像に基づいて、当該乗員が正規ユーザであるか否かを判定し、
前記乗員が正規ユーザである場合に、前記車両への人の不正侵入なしを示す前記不正侵入情報を前記記憶部に格納し、
前記乗員が正規ユーザでない場合に、前記車両への人の不正侵入ありを示す前記不正侵入情報を前記記憶部に格納する、
請求項１記載の車両用制御装置。
【請求項４】
車両に搭載された制御対象を制御する制御部と、
前記車両内への人の不正侵入の有無を示す不正侵入情報を格納した記憶部と、
前記不正侵入情報に基づいて、前記制御部に対するセキュアブート処理の要否を、前記制御部の起動前に判定する要否判定部と、を備えた車両用制御装置であって、
前記不正侵入情報は、前記制御部の前回の起動後に実行される不正侵入判定処理によって生成されて前記記憶部に格納されるものであり、
前記車両用制御装置が行う不正侵入判定処理は、
前記車両のドアの解錠時に使用されたキーと前記車両に予め登録されている認証キーとが一致するか否かを判定すると共に、カメラによって撮像された前記車両の乗員の画像に基づいて、当該乗員が正規ユーザであるか否かを判定し、
前記使用されたキーと前記認証キーとが一致する場合且つ前記乗員が正規ユーザである場合に、前記車両への人の不正侵入なしを示す前記不正侵入情報を前記記憶部に格納し、
前記使用されたキーと前記認証キーとが一致していない場合又は前記乗員が正規ユーザでない場合に、前記車両への人の不正侵入ありを示す前記不正侵入情報を前記記憶部に格納し、
前記要否判定部は、
前記不正侵入情報が前記車両への人の不正侵入ありを示す場合に、前記制御部の起動前に前記制御部に対するセキュアブート処理を実行し、
前記不正侵入情報が前記車両への人の不正侵入なしを示す場合に、前記制御部に対するセキュアブート処理を実行せずに、前記制御部の起動を許可する、
車両用制御装置。
【請求項５】
前記制御部は、車載ネットワークを介して通信を行うことにより前記制御対象を制御し、
前記制御部と前記要否判定部は、前記車載ネットワークを介することなく前記記憶部と通信可能である、
請求項１～４のいずれか１項記載の車両用制御装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両用制御装置、特に、起動時に完全性の検証を行う車両用制御装置に関する。
【背景技術】
【０００２】
車両には、複数のＥＣＵ（Electronic Control Unit）を備えた車両用制御装置が搭載され、車両は、所定のプログラムに基づく各ＥＣＵの動作により制御されている。近年の自動運転技術における車両周囲の状況確認や自動走行（走る、曲がる、止まる等）等もＥＣＵによって制御されている。従って、例えば、ＥＣＵのプログラムが不正に改ざんされると、車両の安全な走行を阻害するおそれがある。
【０００３】
近年、車両がネットワークと通信可能に構成されるようになったことで、外部からの悪意ある攻撃により、ＥＣＵのプログラムが改ざんされる等の問題が顕在化してきている。また、ＥＣＵでは、着脱可能な不揮発性メモリに格納されたプログラムに基づいて制御を行う場合があり、例えば、車両の駐車中等にスリープ状態となったＥＣＵの不揮発性メモリを不正に交換する等のプログラムの改ざんも存在する。
【０００４】
そこで、ＥＣＵでは、起動（ブート）時にプログラムの完全性を検証することで、不正に改ざんされたプログラムが実行されることを阻止するセキュアブート処理を実行している。セキュアブート処理では、暗号技術を用いてプログラムの完全性の検証を行い、プログラムの改ざんがない場合にはＥＣＵの起動を許可し、プログラムの改ざんが検出された場合にはその状態でのＥＣＵの起動を阻止することができる。
【０００５】
一方、ＥＣＵには、起動開始から起動完了までの起動時間に厳しい制約がある（例えば、数十ｍｓから数百ｍｓ以内）。すなわち、ＥＣＵが制御を開始するまでの起動時間内にセキュアブート処理による検証を完了させることが要求される。このため、セキュアブート処理において、処理時間を短縮させる技術が提案されている（例えば、特許文献１）。
【０００６】
特許文献１には、ＥＣＵの停止時に他ＥＣＵから取得した情報と、ＥＣＵの起動時に他ＥＣＵから取得した情報との検証を行い、改ざんの可能性が低いと判断される場合には、セキュアブートによる検証領域を一部省略することにより、セキュアブート処理に要する時間を短縮することが開示されている。
【先行技術文献】
【特許文献】
【０００７】
【文献】特許第６６３９６１５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、特許文献１のセキュアブート処理では、ＥＣＵ起動時の検証において、他のＥＣＵとの通信を行って他のＥＣＵから得た状態情報を用いるため、他のＥＣＵの起動及び通信開始を待機する必要があり、セキュアブート処理に要する時間の短縮は十分とは言えない。
【０００９】
本発明は、このような状況に対処することを課題としている。すなわち、ＥＣＵ起動時の完全性を確保しながら、セキュアブート処理の処理時間を短縮させることなどを課題としている。
【課題を解決するための手段】

【００１０】
このような課題を解決するために、本発明による車両用制御装置は、以下の構成を具備する。
すなわち、本発明の一態様は、車両に搭載された制御対象を制御する制御部と、前記車両内への不正侵入の有無を示す不正侵入情報を格納した記憶部と、前記不正侵入情報に基づいて、前記制御部の起動時におけるセキュアブート処理の要否を判定する要否判定部と、を備えた車両用制御装置を提供する。
【発明の効果】
【００１１】
このような特徴を有する車両用制御装置によれば、ＥＣＵ起動時の完全性を確保しながら、セキュアブート処理の処理時間を短縮させることができる。
【図面の簡単な説明】
【００１２】
【図１】本発明の実施形態に係る車両用制御装置を含む車両用制御システムの概略構成を示す説明図である。
【図２】本発明の実施形態に係る車両用制御装置の概略構成を示す説明図である。
【図３】本発明の実施形態に係る車両用制御装置におけるセキュアブート処理の要否判定処理及びＥＣＵ起動処理を示すフローチャートである。
【図４】本発明の実施形態に係る車両用制御装置における不正侵入判定処理を示すフローチャートである。
【発明を実施するための形態】
【００１３】
以下、図面を参照して本発明の実施形態を説明する。以下の説明で、異なる図における同一符号は同一機能の部位を示しており、各図における重複説明は適宜省略する。
【００１４】
図１に示すように、本発明の実施形態に係る車両用制御装置（ＥＣＵ）１０は、例えば、車両の走行に必要な種々の電子機器類（制御対象）に接続され、これらの電子機器類を制御するＥＣＵ（Electronic Control Unit）１０（例えば、乗員監視ＥＣＵ１０Ａ，車両監視ＥＣＵ１０Ｂ，駆動ＥＣＵ１０Ｃ，制動ＥＣＵ１０Ｄ，操舵ＥＣＵ１０Ｅ・・・を含み、全てのＥＣＵを示す場合には、単にＥＣＵ１０と記す）である。
【００１５】
このような各電子機器及びこれらを制御するＥＣＵ１０等は、ＣＡＮ（Controller Area Network）やＬＩＮ(Local Interconnect Network)等の車載ネットワーク３により相互に通信可能に接続されると共に、中継装置としてのセントラルゲートウェイ（ＣＧＷ）４に接続されて車両用制御システム１を構成する。以下の説明において、本実施形態にかかる車両用制御装置１０に直接関与しない電子機器等についての詳細な説明及び図示は省略する。
【００１６】
図１に示すように、車両用制御システム１に含まれるＥＣＵ１０は、車両に搭載された制御対象の電子機器に接続され、車載ネットワーク３から取得する情報（データ）に基づいて各々が接続された電子機器の動作を制御する。また、ＥＣＵ１０は、接続された電子機器の動作状態などの状態情報（データ）を車載ネットワーク３へ出力する。
【００１７】
例えば、乗員監視ＥＣＵ１０Ａは、車両に乗車している乗員を監視する乗員監視装置（ＤＭＳ:Driver Monitoring System）の一部を構成し、乗員監視装置に含まれるカメラ、マイク、座席シートに設けられる着座センサ、ドアの開閉センサ（いずれも図示せず）等の電子機器を制御することにより乗員を監視する。例えば、乗員監視ＥＣＵ１０Ａでは、カメラによって撮像された乗員の画像に基づいて車両の乗員が正規ユーザであるか否かを判定する。乗員監視ＥＣＵによる判定結果であるユーザ認証結果は、状態情報として車載ネットワーク３に出力される。

【００１８】
車両監視ＥＣＵ１０Ｂは、車両のドアの開閉センサやキーセンサに接続され、ドアの開閉、ドアのロック又はアンロック、開閉時のキーの照合等を制御することにより車両を監視する。例えば、車両監視ＥＣＵは、車両のドア開閉状態や、ドアの解錠時に使用されたキーと車両に予め登録されている認証キーとが一致するか否かを判定し、ドアの開閉履歴や認証キー照合結果を状態情報として車載ネットワーク３に出力する。
【００１９】
駆動ＥＣＵ１０Ｃ、制動ＥＣＵ１０Ｄ及び操舵ＥＣＵ１０Ｅは、車載ネットワーク３から情報を取得し、車両の走行を制御する。また、駆動ＥＣＵ１０Ｃ、制動ＥＣＵ１０Ｄ及び操舵ＥＣＵ１０Ｅに接続された電子機器の状態を示す状態情報（例えば、車両の車速情報、フットブレーキの踏み込み量を示す情報、サイドブレーキのオン、オフ情報、ステアリングの操舵角の情報）を車載ネットワーク３に出力する。
この他、車両用制御システムには車両の走行に必要な種々の電子機器を制御する複数のＥＣＵ１０が含まれるが、図１においては図示を省略する。
【００２０】
図２に示すように、車両用制御装置としてのＥＣＵ１０は、制御対象に接続され、ＣＰＵ（Central Processing Unit）２０、第１記憶部３０、第２記憶部４０及びＨＳＭ（Hardware Security Module）５０を備えている。
【００２１】
ＣＰＵ２０は、第１記憶部３０に格納されたプログラムに基づいて種々の処理を実行する。本実施形態では、ＣＰＵ２０は、第１記憶部３０に格納されたプログラムを例えば第２記憶部４０等のメモリに読み込んで実行することにより、図２に示す制御部２１、状態情報取得部２２、不正侵入判定部２３、及び要否判定部２４として機能することができる。
【００２２】
制御部２１は、第１記憶部３０に格納された制御プログラムに基づいて、ＥＣＵ１０を起動させ、制御対象を制御するための処理を実行する。
【００２３】
状態情報取得部２２は、車載ネットワーク３を介して、車載ネットワーク３に接続された他のＥＣＵ１０から車両の状態情報を取得する。状態情報取得部２２が取得する状態情報には、乗員監視ＥＣＵ１０Ａによるユーザ認証結果や車両監視ＥＣＵ１０Ｂによる認証キー照合結果が含まれる。
【００２４】
不正侵入判定部２３は、状態情報取得部２２が取得した状態情報に基づいて車両内への不正侵入の有無を判定する。また、不正侵入判定部２３は、判定結果に基づく不正侵入情報を生成し、生成した不正侵入情報を第２記憶部４０に記憶させる。不正侵入判定部２３は、不正侵入情報として、不正侵入があったとの判定結果を得た場合には、セキュアブート処理を実行するためにフラグＯＮを第２記憶部４０に記憶させる。
【００２５】
また、不正侵入判定部２３は、不正侵入がなかったとの判定結果を得た場合には、セキュアブートを処理が不要であるとするフラグＯＦＦを第２記憶部４０に記憶させる。不正侵入判定部２３による不正侵入判定処理については後述する。
【００２６】
要否判定部２４は、前回の制御部２１によるＥＣＵ１０の起動時に第２記憶部４０に記憶された不正侵入情報に基づいて、制御部２１の起動時、すなわち、制御部２１がＥＣＵ１０を起動させる際のセキュアブート処理の要否を判定する。例えば、第２記憶部４０にフラグＯＮが記憶されている場合には、セキュアブート処理を要すると判定し、第２記憶部４０にフラグＯＦＦが記憶されている場合には、セキュアブート処理を要しないと判定する。要否判定部２４による判定結果は、後述するＨＳＭ５０に通知される。
【００２７】
第１記憶部３０は、不揮発性メモリ（例えば、フラッシュメモリ）によって構成するこ

とができる。第１記憶部３０には、ＥＣＵ１０が作動する際にＣＰＵ２０によって実行されるプログラムが格納されている。なお、第１記憶部３０として、例えば、ＳＤカードなどの着脱可能な記憶媒体を適用することもできる。

【００２８】

第２記憶部４０は、いわゆるＲＡＭとして用いることができる。また、第２記憶部４０には、不正侵入情報判定部によって生成された不正侵入情報を記憶させる。

【００２９】

ＨＳＭ５０は、ＥＣＵ１０の起動時に、起動対象のプログラム（すなわち、ＣＰＵ２０によって実行されるプログラム）が適正であるか否かを検証するセキュアブート処理を実行する。本実施形態におけるＨＳＭ５０では、要否判定部２４による判定結果が、セキュアブート処理を要するとの結果である場合に、ＨＳＭ５０によるセキュアブート処理が実行される。

【００３０】

セキュアブート処理による検証の結果、プログラムが適正である場合には、ＨＳＭ５０は制御部２１に対してＥＣＵ１０の起動を許可する。検証の結果、プログラムが適正でない場合には、ＨＳＭ５０は制御部２１に対してＥＣＵ１０の起動を許可しない。

【００３１】

例えば、ＨＳＭ５０が、第１記憶部３０に格納されたプログラムが改ざんされていることを検出した場合、ＨＳＭ５０は制御部２１に対して起動不可を通知する。制御部２１は、ＨＳＭ５０からの通知に基づき、起動許可が通知された場合に限りプログラムを起動する。これにより、ＥＣＵ１０が不正なプログラムに基づいて起動されることを抑制することができる。

【００３２】

一方、要否判定部２４による判定結果がセキュアブート処理を要しないとの結果である場合には、ＨＳＭ５０では、セキュアブート処理を少なくとも一部実行せずに、制御部２１によるＥＣＵ１０の起動を許可する。

【００３３】

続いて、このように構成された車両用制御装置（ＥＣＵ）１０における処理フローについて、図３及び図４のフローチャートを用いて説明する。

【００３４】

[セキュアブート処理の要否判定処理及びＥＣＵ起動処理について]

図３は、車両用制御装置（ＥＣＵ）１０におけるセキュアブート処理の要否判定処理及びＥＣＵ起動処理を示すフローチャートである。セキュアブート処理の対象であるＥＣＵ１０が起動開始すると、要否判定部２４が、第２記憶部４０に記憶されているフラグがＯＮ又はＯＦＦであるかを確認する（ステップＳ１０１）。

【００３５】

ステップＳ１０１のフラグの確認処理において、要否判定部２４は、第２記憶部４０にフラグＯＮが記憶されている場合には、ＨＳＭ５０にセキュアブート処理を要する旨を通知し、ＨＳＭ５０にてセキュアブート処理を実行する（ステップＳ１０２）。要否判定部２４は、第２記憶部４０にフラグＯＦＦが記憶さている場合には、ＨＳＭ５０にセキュアブート処理を要しない旨の通知を行い、ＨＳＭ５０はセキュアブート処理を実行せずに制御部２１にＥＣＵ１０の起動を許可する。

【００３６】

ＨＳＭ５０によるセキュアブート処理では、例えば、第１記憶部３０等において、ＥＣＵ１０による制御対象の制御を実行する際にＣＰＵ２０が実行するプログラムが格納された全領域を検証する。これにより、ＥＣＵ１０の起動時に、起動対象となるプログラムが適正であるか否かを検証する。検証の結果、プログラムが適正でない場合には、ＨＳＭ５０は制御部２１に対してＥＣＵ１０の起動を許可せず（ステップＳ１０４）、処理を終了する。

【００３７】

セキュアブート処理による検証の結果、プログラムが適正である場合には、ＨＳＭ５０は制御部２１に対してＥＣＵ１０の起動を許可する（ステップＳ１０５）。起動が成功したＥＣＵ１０は、通常動作を開始、すなわち、制御対象に対する制御を実施する（ステップＳ１０６）。ＥＣＵ１０では、通常動作と併行して、不正侵入判定部２３により、不正侵入判定処理を実施する（ステップＳ１０７）。不正侵入判定処理については後述する。

【００３８】

不正侵入判定部２３により不正侵入なしと判定された場合には（ステップＳ１０８）、不正侵入情報として、フラグＯＦＦを第２記憶部４０に記憶し（ステップＳ１０９）、処理を終了する。不正侵入判定部２３により不正侵入ありと判定された場合には（ステップＳ１０８）、不正侵入情報として、フラグＯＮを第２記憶部４０に記憶し（ステップＳ１１０）、処理を終了する。

【００３９】

不正侵入判定部２３によって第２記憶部４０に記憶された不正侵入情報（フラグＯＮ又はフラグＯＦＦ）は、ＥＣＵ１０の次回の起動時に、セキュアブート処理の要否を判定する際に用いられる。

【００４０】

なお、ステップＳ１０１の不正侵入情報（セキュアブート継続フラグ）の確認処理に先立って、セキュアブート処理に関するプログラムやデータが格納された記憶領域についての検証を実行しても良い。このような処理を行うことにより、不正侵入情報の確認処理等の完全性をより確実なものとすることができる。

【００４１】

［不正侵入判定処理について］

図４は、不正侵入判定部２３による不正侵入判定処理に係るフローチャートである。

不正侵入判定部２３は、状態情報取得部２２から取得した車両の状態情報に基づいて、車両に対する不正侵入の有無を判定する。具体的には、不正侵入判定部２３は、車両監視ＥＣＵ１０Ｂによる認証キー照合結果を示す状態情報を取得し、車両のドアの解錠時に使用されたキーと車両に予め登録されている認証キーとが一致するかを判定する（ステップＳ２０１）。解錠時に使用されたキーと認証キーとが一致していなかった場合には不正侵入ありと判定し（ステップＳ２０４）、不正侵入判定処理を終了する。

【００４２】

一方、不正侵入判定部２３は、解錠時に使用されたキーと認証キーとが一致していた場合には、乗員監視ＥＣＵ１０Ａからのユーザ認証結果を示す状態情報を取得し、車両に乗車した乗員が正規ユーザであるかを判定する（ステップＳ２０２）。

【００４３】

不正侵入判定部２３は、車両時乗車したユーザが正規ユーザでない場合には、不正侵入ありと判定し（ステップＳ２０４）、不正侵入判定処理を終了する。不正侵入判定部２３は、車両に乗車した乗員が正規ユーザであると判定した場合には不正侵入なしと判定し（ステップＳ２０３）、不正侵入判定処理を終了する。

【００４４】

なお、不正侵入判定処理が終了すると、図３のフローチャートのステップＳ１０８に進み、不正侵入判定部２３は、不正侵入判定処理による判定結果に従って、フラグＯＮ又はフラグＯＦＦを第２記憶部４０に記憶する（図３のステップＳ１０９、ステップＳ１１０）。

【００４５】

上述した不正侵入判定処理は一例であり、必ずしも上述のようにセキュアブート処理対象のＥＣＵにおいて実施する必要はない。不正侵入判定処理を、例えば、乗員監視ＥＣＵ１０Ａ又は車両監視ＥＣＵ１０Ｂ等のセキュアブート処理対象のＥＣＵ以外のＥＣＵによって実行し、その結果をセキュアブート処理対象のＥＣＵに出力してもよい。

【００４６】

以上述べたように、本実施形態に係る車両用制御装置によれば、車両に対する不正侵入

の有無を判定することで、制御対象の制御に用いられるプログラムに対する改ざんの可能性を判断する。そして、プログラムに対する改ざんの可能性がある場合にセキュアブート処理を実行する一方で、プログラムに対する改ざんの可能性がない場合にはセキュアブート処理を一部又は全部省略することができる。

【００４７】

このように、プログラムに対する改ざんの可能性の有無に応じてセキュアブート処理の要否を決定するので、プログラムに対する改ざんの可能性が低い場合には、ＥＣＵの起動開始から起動完了までに要する時間の短縮を図ることができる。一方で、プログラムに対する改ざんの可能性が高い場合には、セキュアブート処理を実行することで、改ざんに対する安全性を確保することができる。

【００４８】

すなわち、車両を監視状態に基づく不正侵入の判定結果に応じ、セキュアブート処理の検証範囲を柔軟に変更することができるので、ＥＣＵ起動時の完全性とセキュアブート処理に要する時間の短縮とを両立させることができる。

【００４９】

また、ＥＣＵの起動が成功した際に、不正侵入判定処理を行って不正侵入情報を記憶させておき、この不正侵入情報を次回の起動時におけるセキュアブート処理の要否判定に用いるので、ＥＣＵの起動時に車両用制御システム１に含まれる他のＥＣＵとの間で通信を行う必要がない。

【００５０】

さらに、例えば、第１記憶部３０がＳＤカード等の着脱可能な記憶媒体である場合には、車両への不正侵入により第１記憶部３０そのものが交換されることによる改ざんも考えられるが、不正侵入判定処理に基づいてセキュアブート処理の要否を判定するので、このような改ざんへの対策となり得る。

【００５１】

本発明の実施の形態について図面を参照して詳述してきたが、具体的な構成はこれらの実施の形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計の変更等があっても本発明に含まれる。また、上述の各実施の形態は、その目的及び構成等に特に矛盾や問題がない限り、互いの技術を流用して組み合わせることが可能である。

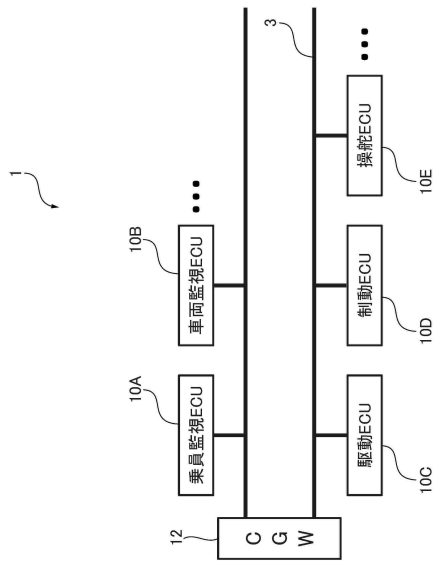
【符号の説明】

【００５２】

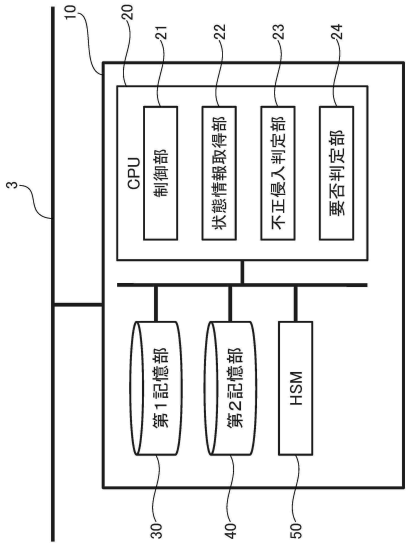
１：車両用制御システム，３：車載ネットワーク，１０：車両用制御装置（ＥＣＵ），１０Ａ：乗員監視ＥＣＵ，１０Ｂ：車両監視ＥＣＵ，１０Ｃ：駆動ＥＣＵ，１０Ｄ：制動ＥＣＵ，１０Ｅ：操舵ＥＣＵ，２０：ＣＰＵ，２１：制御部，２２：状態情報取得部，２３：不正侵入判定部，２４：要否判定部，３０：第１記憶部，４０：第２記憶部，５０：ＨＳＭ

【図面】

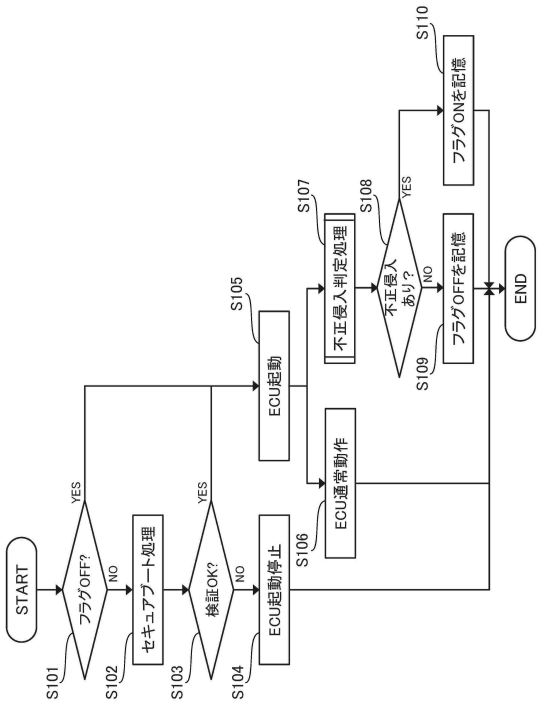
【図１】


1
3
12
C
G
W
10A
乗員監視ECU
10B
車両監視ECU
10C
駆動ECU
10D
制動ECU
10E
操舵ECU

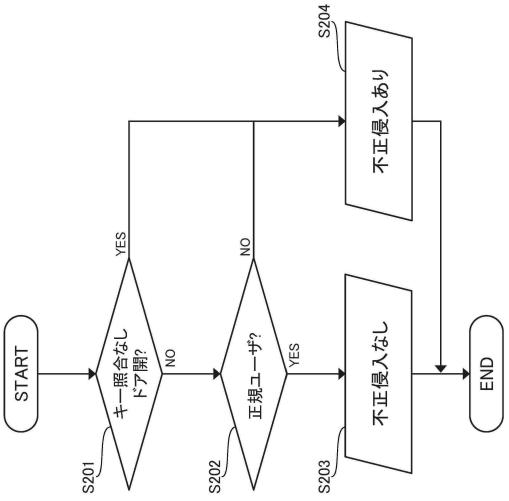
【図２】


3
10
20
CPU
制御部
21
状態情報取得部
22
不正侵入判定部
23
要否判定部
24
第1記憶部
30
第2記憶部
40
HSM
50

【図３】


START
フラグOFF?
S101
YES
NO
セキュアブート処理
S102
検証OK?
S103
YES
NO
ECU起動停止
S104
ECU起動
S105
ECU通常動作
S106
不正侵入判定処理
S107
不正侵入あり?
S108
YES
NO
フラグOFFを記憶
S109
フラグONを記憶
S110
END

【図４】


START
キー照合なしドア開?
S201
YES
NO
正規ユーザ?
S202
NO
YES
不正侵入なし
S203
不正侵入あり
S204
END

フロントページの続き

(56)参考文献 国際公開第２０２０／１５８３７７（WO，Ａ１）
特開２００４－２７６７８２（ＪＰ，Ａ）
特開２０１９－０６６９８４（ＪＰ，Ａ）
国際公開第２００９／０１３８３１（WO，Ａ１）
特開２０１８－１９５３２９（ＪＰ，Ａ）
特開２０１０－２０８３５３（ＪＰ，Ａ）
国際公開第２０１５／１７４５２６（WO，Ａ１）
特開２０１８－１７３７２１（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３０－２１／５７
Ｂ６０Ｒ １６／００－１７／０２