(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2020-144531
(P2020-144531A)
(43)公開日　令和2年9月10日(2020.9.10)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/57	(2013.01)	G06F	21/57	350
H04L 9/32	(2006.01)	H04L	9/00	675A
H04L 9/08	(2006.01)	H04L	9/00	601E
G06F 21/12	(2013.01)	G06F	21/12	
B60R 16/02	(2006.01)	B60R	16/02	66OW

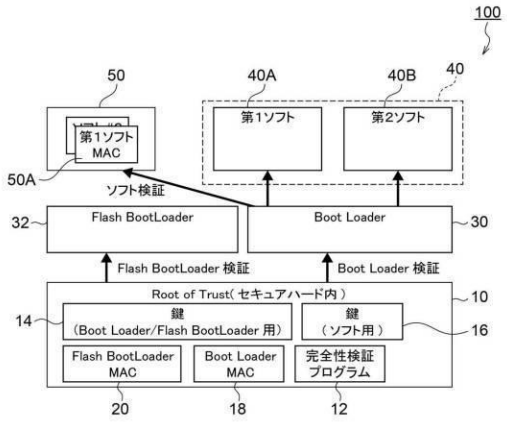
審査請求 未請求　請求項の数 7　ＯＬ　（全 11 頁）

(21)出願番号　特願2019-39703(P2019-39703)
(22)出願日　平成31年3月5日(2019.3.5)

(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　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(74)代理人　100099025
弁理士　福田　浩志
(72)発明者　後藤　慶太
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内
(72)発明者　佐藤　雄介
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内

(54)【発明の名称】車両用制御装置、車両用制御装置の起動方法及び記録媒体

(57)【要約】　（修正有）
【課題】起動時の検証を迅速に実行できる車両用制御装置、車両用制御装置の起動方法及び記録媒体を提供する。
【解決手段】車両用制御装置１００は、起動プログラムであるBootLoader３０及びFlashBootLoader３２を含む重要領域内のプログラムの完全性を検証するための完全性検証プログラム１２、鍵１４、BootLoaderMAC１８及びFlashBootLoaderMAC２０と、起動プログラムにより重要領域内のプログラムが起動した状態で、非重要領域内の制御プログラム４０の完全性を検証するための鍵１６及び第１ソフトＭＡＣ５０Ａ等を格納したフラッシュＲＯＭ５０と、を含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
起動プログラムを含む重要領域内のプログラムの完全性を検証する第１検証部と、
前記起動プログラムにより前記重要領域内のプログラムが起動した状態で、非重要領域内のプログラムの完全性を検証する第２検証部と、
を含む車両用制御装置。
【請求項２】
前記第１検証部は完全性検証プログラム、重要領域用鍵及び前記重要領域内のプログラムの検証用署名を、
前記第２検証部は非重要領域用鍵及び非重要領域内のプログラムの検証用署名を、各々備える請求項１に記載の車両用制御装置。
【請求項３】
前記第１検証部は、前記完全性検証プログラム及び前記重要領域用鍵を用いて生成した前記重要領域内のプログラムの署名が前記重要領域内の検証用署名と一致する場合に前記重要領域内のプログラムが完全性を有すると判定する請求項２に記載の車両用制御装置。
【請求項４】
前記第２検証部は、前記第１検証部が前記重要領域内のプログラムが完全性を有すると判定した後、前記非重要領域用鍵を用いて生成した前記非重要領域内のプログラムの署名が前記非重要領域内の検証用署名と一致する場合に前記非重要領域内のプログラムが完全性を有すると判定する請求項３に記載の車両用制御装置。
【請求項５】
前記重要領域用鍵は、車両用制御装置が搭載される車両毎に異なる鍵であり、
前記非重要領域用鍵は、同型式の車両用制御装置で同一の鍵である請求項２～４のいずれか１項に記載の車両用制御装置。
【請求項６】
起動プログラムを含む重要領域内のプログラムの完全性を検証する第１検証工程と、
前記起動プログラムにより前記重要領域内のプログラムが起動した状態で、非重要領域内のプログラムの完全性を検証する第２検証工程と、
を含む車両用制御装置の起動方法。
【請求項７】
起動プログラムを含む重要領域内のプログラムの完全性を検証するための完全性検証プログラム、重要領域用鍵及び前記重要領域内のプログラムの検証用署名、並びに非重要領域内のプログラムの完全性を検証するための非重要領域用鍵及び非重要領域内のプログラムの検証用署名を記録した記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両用制御装置、車両用制御装置の起動方法及び記録媒体に関する。
【背景技術】
【０００２】
車両用制御装置であるＥＣＵ（Electronic Control Unit）はプログラムに基づいて動作する半導体装置である。従って、ＥＣＵにインストールされているプログラムが正常でないと、正常な動作はおぼつかない。
【０００３】
ＥＣＵのプログラムのインストールは車両の製造者によって行われ、当該プログラムのアップデート等の保守は車両の製造者又は販売店によって行われる。しかしながら、当該プログラムのアップデート時に、錯誤により非正規のプログラムがインストールされるおそれが皆無とは言えない。また、近年のように車両がネットワークと接続可能に構成されたことで、外部からの悪意ある攻撃により、ＥＣＵに不正なプログラムがインストールされる又は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た。

【０００４】
特許文献１には、ＥＣＵの起動時にプログラムの完全性を検証し、当該検証に成功した場合にＥＣＵの起動（ブート）を許可するセキュアブート方法の発明が開示されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１５－０２２５２１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に開示されているセキュアブート方法は、ＥＣＵの全プログラムの検証が成功した場合にＥＣＵの起動を許可するため、ＥＣＵの起動に時間がかかるという問題があった。
【０００７】
本発明は、上記事実を考慮し、起動時の検証を迅速に実行できる車両用制御装置、車両用制御装置の起動方法及び記録媒体を提供することを目的とする。
【課題を解決するための手段】
【０００８】
上記課題を解決するために、請求項１に記載の車両用制御装置は、起動プログラムを含む重要領域内のプログラムの完全性を検証する第１検証部と、前記起動プログラムにより前記重要領域内のプログラムが起動した状態で、非重要領域内のプログラムの完全性を検証する第２検証部と、を含んでいる。
【０００９】
請求項１に記載の車両用制御装置によれば、車両用制御装置の起動プログラムを含む重要領域内のプログラムの完全性を非重要領域に対して優先的に検証する。
【００１０】
請求項２に記載の車両用制御装置は、請求項１に記載の車両用制御装置において、前記第１検証部は完全性検証プログラム、重要領域用鍵及び前記重要領域内のプログラムの検証用署名を、前記第２検証部は非重要領域用鍵及び非重要領域内のプログラムの検証用署名を、各々備える。
【００１１】
請求項２に記載の車両用制御装置によれば、第１検証部は重要領域内のプログラムの検証に必要な構成を、第２検証部は非重要領域内のプログラムの検証に必要な構成を各々備えることにより、重要領域内のプログラムの検証とは別に非重要領域内のプログラムの検証を実行できる。
【００１２】
請求項３に記載の車両用制御装置は請求項２に記載の車両用制御装置において、前記第１検証部は、前記完全性検証プログラム及び前記重要領域用鍵を用いて生成した前記重要領域内のプログラムの署名が前記重要領域内の検証用署名と一致する場合に前記重要領域内のプログラムが完全性を有すると判定する。
【００１３】
請求項３に記載の車両用制御装置によれば、重要領域用鍵により生成した重要領域内のプログラムの署名が検証用署名と一致した場合に当該プログラムが完全性を有すると判定できる。
【００１４】
請求項４に記載の車両用制御装置は、請求項３に記載の車両用制御装置において、前記第２検証部は、前記第１検証部が前記重要領域内のプログラムが完全性を有すると判定した後、前記非重要領域用鍵を用いて生成した前記非重要領域内のプログラムの署名が前記非重要領域内の検証用署名と一致する場合に前記非重要領域内のプログラムが完全性を有すると判定する。

【００１５】
請求項４に記載の車両用制御装置によれば、非重要領域用鍵により生成した非重要領域内のプログラムの署名が検証用署名と一致した場合に当該プログラムが完全性を有すると判定できる。
【００１６】
請求項５に記載の車両用制御装置は、請求項２～４のいずれか１項に記載の車両用制御装置において、前記重要領域用鍵は、車両用制御装置が搭載される車両毎に異なる鍵であり、前記非重要領域用鍵は、同型式の車両用制御装置で同一の鍵である。
【００１７】
請求項５に記載の車両用制御装置によれば、重要領域用鍵を車両毎に異なる鍵にすることにより、第三者による重要領域用鍵の悪用を防止する。
【００１８】
上記課題を解決するために、請求項６に記載の車両用制御装置の起動方法は、起動プログラムを含む重要領域内のプログラムの完全性を検証する第１検証工程と、前記起動プログラムにより前記重要領域内のプログラムが起動した状態で、非重要領域内のプログラムの完全性を検証する第２検証工程と、を含んでいる。
【００１９】
請求項６に記載の車両用制御装置の起動方法によれば、車両用制御装置の起動プログラムを含む重要領域内のプログラムの完全性を非重要領域に対して優先的に検証する。
【００２０】
上記課題を解決するために、請求項７に記載の記録媒体は、起動プログラムを含む重要領域内のプログラムの完全性を検証するための完全性検証プログラム、重要領域用鍵及び前記重要領域内のプログラムの検証用署名、並びに非重要領域内のプログラムの完全性を検証するための非重要領域用鍵及び非重要領域内のプログラムの検証用署名を記録する。
【００２１】
請求項７に記載の記録媒体によれば、重要領域内及び非重要領域内の各々のプログラムの検証に必要な構成を必要に応じて持ち運べるという効果を奏する。
【発明の効果】
【００２２】
請求項１に記載の車両用制御装置によれば、重要領域内のプログラムの完全性を非重要領域に対して優先的に検証することにより、起動時の検証を迅速に実行できるという効果を奏する。
【００２３】
請求項２に記載の車両用制御装置によれば、重要領域内のプログラムの検証とは別に非重要領域内のプログラムの検証を実行できるようにすることにより、起動時の検証を迅速に実行できるという効果を奏する。
【００２４】
請求項３に記載の車両用制御装置によれば、重要領域用鍵により生成した重要領域内のプログラムの署名が検証用署名と一致した場合、当該プログラムの改ざんはないことを検証できるという効果を奏する。
【００２５】
請求項４に記載の車両用制御装置によれば、非重要領域用鍵により生成した非重要領域内のプログラムの署名が検証用署名と一致した場合、当該プログラムの改ざんはないことを検証できるという効果を奏する。
【００２６】
請求項５に記載の車両用制御装置によれば、重要領域用鍵を車両毎に異なる鍵にすることにより、セキュリティを担保できるという効果を奏する。
【００２７】
請求項６に記載の車両用制御装置の起動方法によれば、重要領域内のプログラムの完全性を非重要領域に対して優先的に検証することにより、起動時の検証を迅速に実行できる

という効果を奏する。
【００２８】
請求項７に記載の記録媒体によれば、車両の製造者が重要領域内及び非重要領域内の各々のプログラムの検証に必要な構成を車両にインストールできるという効果を奏する。
【図面の簡単な説明】
【００２９】
【図１】本発明の実施の形態に係る車両用制御装置の起動時の状態を示すブロック図である。
【図２】本発明の実施の形態において、検証領域の区分の一例を示した表である。
【図３】検証に用いる鍵の保管及び検証ルートの一例を示したブロック図である。
【図４】本発明の実施の形態に係る車両用制御装置の重要領域の完全性の検証の一例を示したフローチャートである。
【図５】本発明の実施の形態に係る車両用制御装置の非重要領域の完全性の検証の一例を示したフローチャートである。
【発明を実施するための形態】
【００３０】
以下、図１～図５を用いて、本実施の形態に係る車両用制御装置１００について説明する。図１は、本実施の形態に係る車両用制御装置１００の起動時の状態を示すブロック図である。
【００３１】
図１に示した車両用制御装置１００は、一般にＥＣＵと呼称される半導体装置であり、車両に搭載されている機器を制御する第１ソフト４０Ａ、第２ソフト４０Ｂ等の制御ソフトウェア４０がインストールされている。
【００３２】
車両用制御装置１００を起動するには、BootLoader３０（以下、「ＢＬ３０」と略記）及びFlashBootLoader３２（以下、「ＦＢＬ３２」と略記）の各々を用いる。ＢＬ３０は、車両用制御装置１００のＲＯＭ（Read only memory）等の記憶装置に格納された車両用制御装置１００のソフトウェアを、ＦＢＬ３２は車両用制御装置１００のフラッシュメモリに格納された車両用制御装置１００のソフトウェアを、車両用制御装置１００の起動時に各々車両用制御装置１００の主記憶に呼び出すプログラムである。従って、ＢＬ３０及びＦＢＬ３２の各々は、本実施の形態に係る車両用制御装置１００において、起動時に最初に実行されるプログラムである。
【００３３】
Root of Trust１０（以下、「ＲｏＴ１０」と略記）には、完全性検証プログラム１２、ＢＬ３０とＦＢＬ３２との検証で用いる鍵１４、制御ソフトウェア４０の検証で用いる鍵１６、BootLoaderMAC１８（以下、「ＢＬＭＡＣ１８」と略記）及びFlashBootLoadcrMAC２０（以下、「ＦＢＬＭＡＣ２０」と略記）が格納される。ＢＬＭＡＣ１８はＢＬ３０を、ＦＢＬＭＡＣ２０はＦＢＬ３２を、各々鍵１４で認証する際に用いられるＭＡＣ（メッセージ認証コード）である。鍵１４、１６は、公開鍵でも共通鍵でもよいが、公開鍵の場合、後述するようにＭＡＣではなくハッシュ値を用いて検証する。また、共通鍵を用いた場合の方が、公開鍵を用いた場合よりも、若干ながら処理が高速になる。
【００３４】
完全性検証プログラム１２、鍵１４、１６、ＢＬＭＡＣ１８及びＦＢＬＭＡＣ２０を格納したＲｏＴ１０は、セキュアハードドライブにて保護され、車両の出荷後は、変更不能に構成されている。
【００３５】
本実施の形態では、ＢＬ３０及びＦＢＬ３２の各々が格納された領域を最も重要な領域とし、車両用制御装置１００の起動又はリセット時に、制御ソフトウェア４０の起動前に完全性検証プログラム１２内でＢＬ３０及びＦＢＬ３２の完全性を検証する。
【００３６】

本実施の形態において、鍵１４、１６が共通鍵の場合のＢＬ３０の完全性の検証の手順は、以下の通りである。
（１）鍵１４によりＢＬ３０のＭＡＣを生成する。
（２）生成したＭＡＣをＲｏＴ１０内のＢＬＭＡＣ１８と比較する。
（３）比較した結果が一致した場合、ＢＬ３０は完全性を有すると判定する。
【００３７】
ＢＬ３０が完全性を有する場合、ＦＢＬ３２の完全性を以下の手順で検証する。
（１）鍵１４によりＦＢＬ３２のＭＡＣを生成する。
（２）生成したＭＡＣをＲｏＴ１０内のＦＢＬＭＡＣ２０と比較する。
（３）比較した結果が一致した場合、ＦＢＬ３２は完全性を有すると判定する。
【００３８】
ＢＬ３０及びＦＢＬ３２が完全性を有する場合、ＢＬ３０を起動し、ＢＬ３０内で制御ソフトウェア４０の完全性を以下の手順で検証する。
（１）鍵１４又は鍵１６により第１ソフト４０ＡのＭＡＣを生成する。
（２）生成したＭＡＣをフラッシュＲＯＭ５０内の第１ソフトＭＡＣ５０Ａと比較する。
（３）比較した結果が一致した場合、第１ソフト４０Ａは完全性を有すると判定し、第１ソフト４０Ａを実行する。
（４）以下、上記（１）～（３）と同様に鍵１６を用いて、第２ソフト４０Ｂ以降の各々の制御ソフトウェア４０のＭＡＣを生成し、生成したＭＡＣをフラッシュＲＯＭ５０内の制御ソフトウェア４０の各々のＭＡＣと比較して制御ソフトウェア４０の各々の完全性を検証し、完全性を有する制御ソフトウェア４０を順次実行する。
【００３９】
図２は、検証領域の区分の一例を示した表である。図２に示したように、本実施の形態に係る車両用制御装置１００は、検証領域を重要領域と非重要領域とに区分している。重要領域は車両が走行中は検証実施が不可能な領域であり、本実施の形態では、上述のＢＬ３０及びＦＢＬ３２がインストールされた領域等が該当する。特にＢＬ３０及びＦＢＬ３２がインストールされた領域は、最初に検証されるべき領域であるから、ＥＣＵである車両用制御装置１００の起動前に検証することを要する。
【００４０】
また、車両のエンジン、ブレーキ、操舵機構及びトランスミッション等の車両の走行に直接係る構成の制御ソフトウェア４０がインストールされた領域も、重要領域に含めてもよいが、重要領域を多くすると、起動前の検証に時間を要する。
【００４１】
ＢＬ３０及びＦＢＬ３２がインストールされた領域は、セキュリティ上でも非常に重要な領域なので、検証に用いる鍵１４は、車両毎に専用のものが用意される。また、当該領域が改ざんされた場合は、車両用制御装置１００の起動を行わない。
【００４２】
非重要領域は、車両が走行中でも検証実施が可能な領域であり、本実施の形態では、上述の制御ソフトウェア４０のうち、車両の走行及び安全に直接関係しない空調、音響機器及びナビゲーションシステム等のプログラムがインストールされた領域が該当する。
【００４３】
非重要領域は、重要領域ほど重大なセキュリティが求められないので、検証に用いる鍵１６は、同一形式の全ての車両用制御装置１００で共通である。また、当該領域が改ざんされた場合は、問題のあるソフトウェアを実行しない等のフェールセーフが行われる。
【００４４】
非重要領域は、車両用制御装置１００の起動前でも検証は可能だが、本実施の形態では起動前は重要領域のみ検証を行って車両が走行可能な状態へ逸早く移行させている。重要領域の検証が完了しても、非重要領域の検証は完了していないが、車両は走行可能な状態なので、実用上は車両用制御装置１００の起動時の検証が迅速かつ円滑に実行されることになる。

【００４５】
図３は、検証に用いる鍵１４、１６の保管及び検証ルートの一例を示したブロック図である。図３に示したように、セキュア領域であるＲｏＴ１０では、Bootプログラムである ＢＬ３０及びＦＢＬ３２が上述のように完全性検証プログラム１２内で完全性を検証された後、図３の(１)に示したように、重要領域用の鍵１４を取り出して重要領域４２内の実行プログラムＡの完全性の検証を実施する。
【００４６】
そして、図３の(２)に示したように、(１)での検証の結果から実行プログラムＡの署名（ＭＡＣ又はハッシュ値）を生成し、図３の（３）で、（２）で生成した署名と実行プログラムＡの作成時に計算した実行プログラムＡ内の署名とを比較し、両者が一致した場合、実行プログラムＡは完全性を有すると判定する。
【００４７】
非重要領域６０では、図３の（４）に示したように、非重要領域６０用の鍵１６を取り出して非重要領域６０内の実行プログラムＢの完全性の検証を実施する。
【００４８】
そして、図３の(５)に示したように、(４)での検証の結果から実行プログラムＢの署名を生成し、図３の（６）で、（５）で作成した署名と実行プログラムＢの作成時に計算した実行プログラムＢ内の署名とを比較し、両者が一致した場合、実行プログラムＢは完全性を有すると判定する。
【００４９】
完全性の検証で用いる鍵１４、１６は、前述のように、共通鍵方式でも公開鍵方式でもよい。例えば、共通鍵方式は、ＲｏＴ１０内の鍵１４と完全性検証プログラム１２とを利用して、例えば、重要領域４２内のソフトウェアの署名であるＭＡＣを生成する。そして、生成したＭＡＣと検証対象であるソフトウェア内のＭＡＣとを比較し、両者が一致した場合、検証対象のソフトウェアが完全性を有すると判定して、当該ソフトウェアを起動する。
【００５０】
プログラムの署名の暗号化を秘密鍵で行い、暗号化された署名の復号化を公開鍵で行う公開鍵方式では、以下のようにソフトウェアの完全性を検証する。例えば、ＲｏＴ１０内の完全性検証プログラム１２又はハッシュ値演算用プログラム等を用いて、重要領域４２又は非重要領域内のソフトウェアの署名であるハッシュ値を生成し、公開鍵である鍵１４を用いて当該ソフトウェアの暗号化された署名を復号化してハッシュ値を得る。そして、生成したハッシュ値と復号化したハッシュ値とを比較し、両者が一致した場合、検証対象のソフトウェアが完全性を有すると判定して、当該ソフトウェアを起動する。
【００５１】
図４は、本実施の形態に係る車両用制御装置１００の重要領域４２の完全性の検証の一例を示したフローチャートである。図４に示した処理は、車両用制御装置１００の起動又はリセット時に開始される。
【００５２】
ステップ４００では、重要領域４２のプログラム改ざんの検知に係るプログラムを起動する。当該プログラムは、例えば完全性検証プログラム１２である。
【００５３】
ステップ４０２では、重要領域４２の検証を開始し、ステップ４０４で重要領域４２の検証用の鍵１４を取り出す。鍵１４は、前述のように、車両毎に個別に設けられた専用鍵である。
【００５４】
ステップ４０６では、鍵１４を用いて重要領域４２のソフトウェア（プログラム）の完全性を上述のように検証し、当該ソフトウェアの改ざんの有無をチェックする。
【００５５】
ステップ４０８ではステップ４０６でのチェック結果の妥当性を判定する。ステップ４

０８の判定が問題ない（妥当な）場合は、ステップ４１０で車両のイグニッションスイッチのオンを許可する。そして、ステップ４１２でＥＵＣである車両用制御装置１００の起動を行って、手順を非重要領域の完全性の検証に移行する。

【００５６】

ステップ４０８の判定が問題ありの場合は、ステップ４１４でステップ４０８での問題ありの判定回数（失敗回数）が規定値以下か否かを判定する。規定値は、車両用制御装置１００の仕様等によるが、一例として２～３回である。

【００５７】

ステップ４１４で失敗回数が規定値以下と判定した場合は、ステップ４１６で車両用制御装置１００の起動を停止する。そして、ステップ４１８で再度の改ざんチェックを行う決定をして、手順をステップ４０２に移行する。

【００５８】

ステップ４１４で失敗回数が規定値を超えた場合は、ステップ４２０で車両用制御装置１００の起動を停止して処理を終了する。

【００５９】

図５は、本実施の形態に係る車両用制御装置１００の非重要領域６０の完全性の検証の一例を示したフローチャートである。ステップ５００では図４のステップ４１２の手順で車両用制御装置１００が起動し、ステップ５０２では車両用制御装置１００が動作を開始し、車両が走行可能な状態になる。

【００６０】

ステップ５０４では、車両用制御装置１００の動作中のバックグラウンドで非重要領域６０の完全性の検証を開始する。

【００６１】

ステップ５０６で非重要領域６０の検証用の鍵１６を取り出す。鍵１６は、前述のように、同型式の車両用制御装置１００に共通の鍵である。

【００６２】

ステップ５０８では、鍵１６を用いて非重要領域６０のソフトウェア（プログラム）の完全性を上述のように検証し、当該ソフトウェアの改ざんの有無をチェックする。

【００６３】

ステップ５１０ではステップ５０８でのチェック結果の妥当性を判定する。ステップ５０８の判定が問題ない（妥当な）場合は、ステップ５１２で車両用制御装置１００の動作を継続して、車両用制御装置１００のソフトウェアの完全性の検証処理を終了する。

【００６４】

ステップ５１０での判定が問題ありの場合は、ステップ５１４でステップ５１０での問題ありの判定回数（失敗回数）が規定値以下か否かを判定する。規定値は、車両用制御装置１００の仕様等によるが、一例として２～３回である。

【００６５】

ステップ５１４で失敗回数が規定値以下と判定した場合は、ステップ５１６で車両用制御装置１００の動作を継続する。そして、ステップ５１８で再度の改ざんチェックを行う決定をして、手順をステップ５０４に移行する。

【００６６】

ステップ５１４で失敗回数が規定値を超えた場合は、ステップ５２０で問題のあるソフトウェアを起動しない等のフェールセーフを行って、車両用制御装置１００のソフトウェアの完全性の検証処理を終了する。

【００６７】

以上説明したように、本実施の形態に係る車両用制御装置１００は、重要領域４２のソフトウェアの完全性の検証を優先して行って、車両用制御装置１００を起動した後、非重要領域６０のソフトウェアの完全性の検証を行う。重要領域４２の検証後、車両用制御装置１００を起動することにより、起動時の検証が迅速に実行される。

【００６８】

本実施の形態では、車両用制御装置１００の起動後も、車両用制御装置１００のバックグラウンドでは非重要領域６０の完全性の検証が行われるが、車両が走行可能な状態なので、実用上は問題がない。

【００６９】

全プログラムの検証を実施する為には、全車両同じ鍵を用いた改ざん検知技術、又はハッシュ関数のような処理負荷の低い技術を採用する必要があるが、これらの技術はセキュリティ上の脆弱性を有している。

【００７０】

また、本実施の形態は、重要領域の検証に用いる鍵１４は各車両に専用品を設定し、かつ鍵１４を車両の製造者以外は変更できないセキュア領域であるＲｏＴ１０に格納することにより、高度なセキュリティを実現している。

【００７１】

本発明に係るプログラム等は、外部に流出しないように厳重な管理下に置くという条件付きで、記録媒体に格納して提供することも可能である。例えば、ＲｏＴ１０に格納される完全性検証プログラム１２、鍵１４、１６、ＢＬＭＡＣ１８、ＦＢＬＭＡＣ２０及びフラッシュＲＯＭ５０内の制御ソフトウェア４０の各々のＭＡＣを、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＤＶＤ－ＲＯＭ（Digital Versatile Disc Read Only Memory）、及びＵＳＢ（Universal Serial Bus）メモリ等の非一時的記録媒体に記録された形態で提供してもよい。

【００７２】

なお、特許請求の範囲の構成のうち、起動プログラムはBootLoader３０及びFlashBootLoader３２に、同第１検証部はＲｏＴ１０に、同第２検証部はＲｏＴ１０及びフラッシュＲＯＭ５０に、同完全性検証プログラムは完全性検証プログラム１２に、同重要領域用鍵は鍵１４に、同重要領域内のプログラムの検証用署名はBootLoaderMAC１８及びFlashBootLoaderMAC２０に、同非重要領域用鍵は鍵１６に、同非重要領域内の検証用署名は第１ソフトＭＡＣ５０Ａ等に各々対応する。

【００７３】

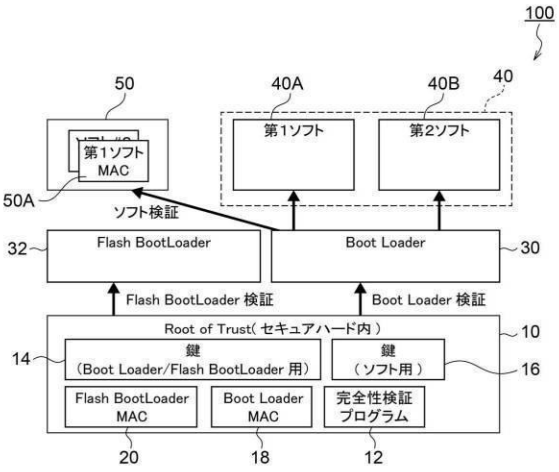
本発明は、上記の形態例に限定されるものではなく、上記の形態例以外にも、その主旨を逸脱しない範囲内において種々変形して実施可能であることは勿論である。

【符号の説明】

【００７４】

１０　Root of Trust
１２　完全性検証プログラム
１４、１６　鍵
１８　BootLoaderMAC
２０　FlashBootLoaderMAC
３０　BootLoader
３２　FlashBootLoader
４０　制御ソフトウェア
４０Ａ　第１ソフト
４０Ｂ　第２ソフト
４２　重要領域
６０　非重要領域
１００　車両用制御装置
５０　フラッシュＲＯＭ
５０Ａ　第１ソフトＭＡＣ

【図１】

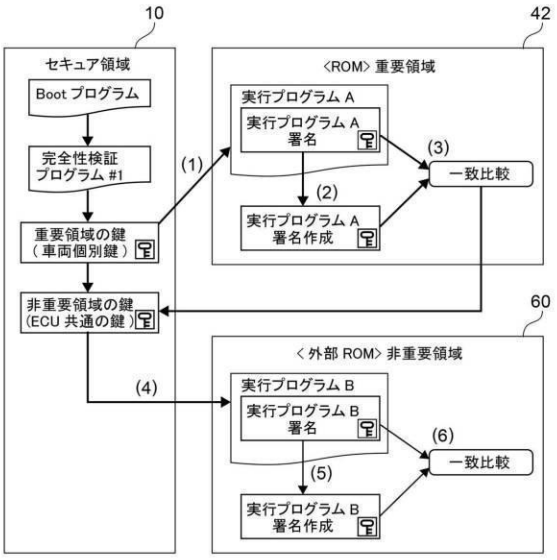


【図２】

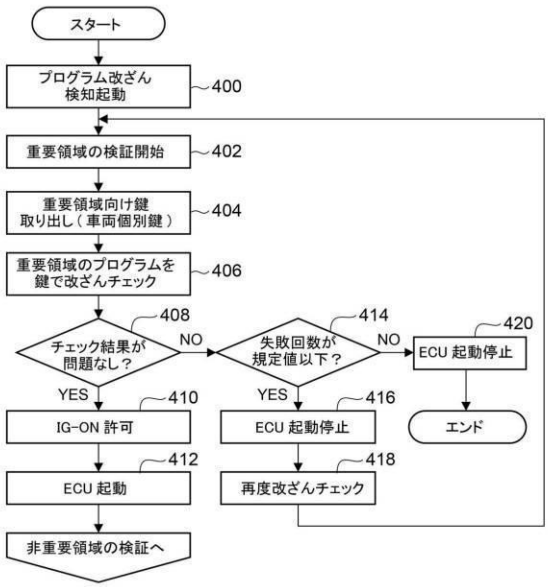
○ 必須　△ 任意　× 不可

安全性・セキュリティ性 ＼ 起動時間	ECU 起動前				走行中			
	鍵		改ざん時対応	検証実施	鍵		改ざん時対応	検証実施
重要領域	車両毎の鍵		起動不可	○	車両毎の鍵		起動不可	×
非重要領域	全 ECU で共通		フェールセーフ	△	全 ECU で共通		フェールセーフ	○

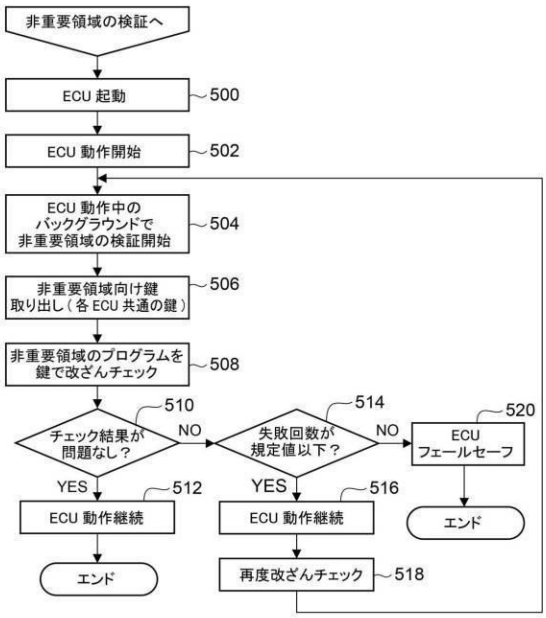
【図３】



【図４】



【図５】


非重要領域の検証へ
ECU 起動
500
ECU 動作開始
502
ECU 動作中の
バックグラウンドで
非重要領域の検証開始
504
非重要領域向け鍵
取り出し（各 ECU 共通の鍵）
506
非重要領域のプログラムを
鍵で改ざんチェック
508
510
チェック結果が
問題なし？
NO
514
失敗回数が
規定値以下？
NO
520
ECU
フェールセーフ
YES
512
ECU 動作継続
エンド
YES
516
ECU 動作継続
再度改ざんチェック
518