(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6659180号
(P6659180)
(45)発行日　令和2年3月4日(2020.3.4)　(24)登録日　令和2年2月10日(2020.2.10)

(51)Int.Cl.　F I
G06F 21/57 (2013.01)　G06F 21/57 350
G06F 21/64 (2013.01)　G06F 21/64
G06F 21/53 (2013.01)　G06F 21/53

請求項の数 4　(全 13 頁)

(21)出願番号　特願2018-78151(P2018-78151)
(22)出願日　平成30年4月16日(2018.4.16)
(65)公開番号　特開2019-185575(P2019-185575A)
(43)公開日　令和1年10月24日(2019.10.24)
審査請求日　平成30年4月16日(2018.4.16)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100073759
弁理士　大岩　増雄
(74)代理人　100088199
弁理士　竹中　岑生
(74)代理人　100094916
弁理士　村上　啓吾
(74)代理人　100127672
弁理士　吉澤　憲治
(72)発明者　池頭　俊樹
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】制御装置および制御方法

(57)【特許請求の範囲】
【請求項１】
制御対象への制御処理を実行する制御処理部、
この制御処理部による上記制御対象の制御に用いられるデータを格納した第一の記憶領域、
上記制御処理部を起動するか否かを判定する検証判定部、
上記制御処理部の起動および停止を制御する起動制御部、
上記第一の記憶領域のデータに基づいて予め生成された、上記データの検証のための基準値を格納する第二の記憶領域、
外部機器と通信するための通信機能を有する通信制御部、
上記第一の記憶領域に記憶されたデータに基づいて、このデータを検証するための検証値を生成する検証値生成部、
および上記基準値と上記検証値とを比較することにより、上記データの検証を実行し、比較結果を上記第二の記憶領域に格納する検証実行部を備え、
上記検証値生成部および上記検証実行部は、上記制御処理部、上記検証判定部、上記起動制御部および上記通信制御部が動作する第一の処理環境からハードウェア的に隔離された第二の処理環境下で動作し、上記第二の記憶領域は、上記第二の処理環境下からのみアクセスを可能にされ、
上記起動制御部により上記制御処理部が停止される場合には、
上記起動制御部は、上記制御処理部を停止させるための停止処理を実行し、

上記停止処理には、上記通信制御部の上記通信機能を無効にした後、上記検証値生成部により上記検証値を生成させるとともに、上記検証実行部による上記比較結果を上記第二の記憶領域へ格納させる処理が含まれ、
上記起動制御部により上記制御処理部が起動される場合には、
上記起動制御部は、上記制御処理部を起動させるための起動処理を実行し、
上記起動処理には、上記検証実行部により、上記第二の記憶領域に格納された比較結果を上記検証判定部に送信させて、上記検証判定部による上記判定を行わせる処理が含まれ、
上記検証判定部による上記判定の結果が、検証合格であれば、上記制御処理部を起動し、
検証不合格であれば、上記制御処理部の起動を中止することを特徴とする制御装置。
【請求項２】
上記第一の処理環境下に、
上記制御処理部を起動する時刻になったことを起動指令として、上記起動制御部に通知する時間計測部を備え、
上記起動制御部は、上記制御処理部を停止させた後に、上記時間計測部から上記起動指令を受信した場合には、上記通信制御部の上記通信機能を有効とし、
上記通信制御部により、上記外部機器から上記制御処理部の起動要求を受信して、上記起動処理を実行することを特徴とする請求項１に記載の制御装置。
【請求項３】
上記第一の記憶領域に記憶されたデータは、複数の制御用プログラムデータを含み、
上記制御処理部は、上記複数の制御用プログラムデータに、それぞれ対応する上記制御処理を実行し、
上記検証実行部は、上記複数の制御用プログラムデータに対応して、上記検証値生成部により生成された複数の検証値と、上記第二の記憶領域に格納された複数の基準値とを比較し、それぞれの検証値について検証合格か検証不合格かを示す複数の比較結果を上記第二の記憶領域に格納し、
上記検証判定部は、上記制御処理部の起動に当たって、上記複数の比較結果に基づいて、複数の制御用プログラムデータについて判定し、上記起動制御部は、上記判定で上記検証合格が得られた検証値に対応する制御用プログラムデータが実行されるように限定し、上記制御処理部を起動させることを特徴とする請求項１または請求項２に記載の制御装置。
【請求項４】
制御対象への制御処理を第一の処理環境下で実行する制御処理部が停止される場合に、起動処理部が、上記第一の処理環境下で動作する通信制御部の通信機能を無効にする通信無効化ステップ、
この通信無効化ステップの実行後、上記第一の処理環境からハードウェア的に隔離された第二の処理環境下で動作する検証値生成部により、上記第一の処理環境下の第一の記憶領域のデータに基づいて検証値を生成する第一のステップ、
上記第一の記憶領域のデータに基づいて予め生成された基準値と上記検証値との比較処理を、検証実行部により上記第二の処理環境下で実行する第二のステップ、
この第二のステップで得られた比較結果を、上記検証実行部により、上記第二の処理環境下の第二の記憶領域に格納する第三のステップ、
上記制御処理部が起動される場合に、上記第二の記憶領域に格納された比較結果が、上記検証実行部から上記第一の処理環境下で動作する検証判定部に送信され、上記検証判定部が、上記比較結果に基づき、検証合格または検証不合格を判定する第四のステップ、
および起動制御部が、上記検証合格の場合には、上記制御処理部を起動するとともに、上記検証不合格の場合には、上記制御処理部の起動を中止する第五のステップを含むことを特徴とする制御方法。
【発明の詳細な説明】

【技術分野】
【０００１】
本願は、制御対象を制御する制御装置および制御方法に関するものである。
【背景技術】
【０００２】
従来から、車両に搭載される制御装置である、例えばＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）において、ＥＣＵ内部データの改ざん対策に関する技術が提案されている（例えば、特許文献１参照）。
通常、車両には複数のＥＣＵが搭載されており、各ＥＣＵ間は、通信接続されている。このため、外部からの不正な侵入を受けやすい。外部から不正な侵入を受け、ＥＣＵ内部データが改ざんされてしまうと、その結果として、ＥＣＵが外部から不正に遠隔操作されてしまうおそれがある。
【０００３】
データ改ざんの対策として、セキュアブート処理がある。このセキュアブート処理とは、暗号技術を用いてデータを検証し、データの改ざんを検知する技術である。ＥＣＵを起動する前に、ＥＣＵの内部データが改ざんされているか否かを検知することにより、ＥＣＵを高いセキュリティ強度で起動できるか否かを判断することができる。
しかしながら、車載用のＥＣＵは、起動開始から起動完了までの時間の制約が厳しい。そのため、ＥＣＵ起動時のセキュアブートには、高いセキュリティ強度および高速な処理が求められる。さらに、セキュアブート処理用のプログラム自体も改ざんされてしまうおそれがある。そのため、セキュアブート処理自体にも改ざんに対する高いセキュリティ強度が求められる。
【０００４】
特許文献１は、改ざん検出の対象とするアプリケーションプログラムを選別することで、セキュアブート処理時間を短縮している。また、特許文献１は、検証に用いるデータをイベント毎に更新することにより、セキュアブート処理も高いセキュリティ強度で起動することができるとしている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１７－３３２４８号公報（第５～１１頁、第２図）
【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、従来技術には、以下のような問題がある。
特許文献１では、セキュアブート処理時間を短縮するために、改ざん検出の対象とするアプリケーションプログラムを、システム管理者が予め選別することが必要である。
すなわち、事前に選別されなかったアプリケーションプログラムは、改ざん検出の対象とはならない。このため、事前に選別されなかったアプリケーションプログラムに対して攻撃者によって不正にデータが改ざんされた場合には、改ざんを検出することができないという問題がある。
また、セキュアブート処理自体の改ざんに対するセキュリティ強度を高めるためには、セキュアブートの検証に用いるデータ量を増加させる必要がある。また、検証値生成のための暗号鍵のデータ量を増加させる必要がある。
【０００７】
このように、改ざん検出の対象となるプログラムおよびデータの量を増加させることで、外部からシステム浸入し、データの改ざんを試みる攻撃者は、暗号化された検証値を解読することが困難となる。このため、改ざんに対するセキュリティ強度が向上する。
【０００８】
一方、改ざん検出の対象となるプログラムおよびデータの量を増加させた場合には、セ

キュアブート処理に要する時間が増大してしまうという問題がある。セキュアブート処理の時間短縮方法として、ＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）などの高速演算可能なハードウェアを用いる方法が知られている。しかしながら、データ量が多い場合には、ＨＳＭを使用したとしても、処理時間を十分に短縮できないという問題がある。

【０００９】

本願は、上記のような課題を解決するための技術を開示するものであり、高いセキュリティ強度および高速な起動を実現する制御装置および制御方法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】

【００１０】

本願に開示される制御装置は、制御対象への制御処理を実行する制御処理部、この制御処理部による制御対象の制御に用いられるデータを格納した第一の記憶領域、制御処理部を起動するか否かを判定する検証判定部、制御処理部の起動および停止を制御する起動制御部、第一の記憶領域のデータに基づいて予め生成された、データの検証のための基準値を格納する第二の記憶領域、外部機器と通信するための通信機能を有する通信制御部、第一の記憶領域に記憶されたデータに基づいて、このデータを検証するための検証値を生成する検証値生成部、および基準値と検証値とを比較することにより、データの検証を実行し、比較結果を第二の記憶領域に格納する検証実行部を備え、検証値生成部および検証実行部は、制御処理部、検証判定部、起動制御部および通信制御部が動作する第一の処理環境からハードウェア的に隔離された第二の処理環境下で動作し、第二の記憶領域は、第二の処理環境下からのみアクセスを可能にされ、起動制御部により制御処理部が停止される場合には、起動制御部は、制御処理部を停止させるための停止処理を実行し、停止処理には、通信制御部の通信機能を無効にした後、検証値生成部により検証値を生成させるとともに、検証実行部による比較結果を第二の記憶領域へ格納させる処理が含まれ、起動制御部により制御処理部が起動される場合には、起動制御部は、制御処理部を起動させるための起動処理を実行し、起動処理には、検証実行部により、第二の記憶領域に格納された比較結果を検証判定部に送信させて、検証判定部による判定を行わせる処理が含まれ、検証判定部による判定の結果が、検証合格であれば、制御処理部を起動し、検証不合格であれば、制御処理部の起動を中止するようにしたものである。

【発明の効果】

【００１１】

本願に開示される制御装置によれば、高いセキュリティ強度および高速な起動を実現することができる。

【図面の簡単な説明】

【００１２】

【図１】実施の形態１による車載制御装置を示す機能ブロック図である。

【図２】実施の形態１による車載制御装置の制御処理部の停止および起動処理を示すフローチャートである。

【図３】実施の形態１による車載制御装置のハードウェア構成を示す図である。

【発明を実施するための形態】

【００１３】

実施の形態１.

以下に、制御装置の具体例として、制御対象を車両および車載機器とする車載制御装置（ＥＣＵ）に適用する場合について、図を用いて詳細に説明する。

【００１４】

図１は、実施の形態１による車載制御装置を示す機能ブロック図である。

図１において、車載制御装置１０は、後述する起動制御部１００、制御処理部１０１、不揮発性記憶部１０２、検証値生成部１０３、検証実行部１０４、検証判定部１０５、通信制御部１０６および時間計測部１０７を有する。

【００１５】
また、車載制御装置１０は、第一の処理環境２０ａと第二の処理環境２０ｂとを有する。第二の処理環境２０ｂは、第一の処理環境２０ａとは、ハードウェア的に隔離された処理環境である。例えば、第二の処理環境２０ｂとしては、ＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）を使用することができる。
第一の処理環境２０ａは、起動制御部１００、制御処理部１０１、不揮発性記憶部１０２内の第一の記憶領域１０２ａ、検証判定部１０５、通信制御部１０６および時間計測部１０７を有する。
第二の処理環境２０ｂは、不揮発性記憶部１０２内の第二の記憶領域１０２ｂ、検証値生成部１０３および検証実行部１０４を有する。この第二の記憶領域１０２ｂは、第二の処理環境２０ｂからのみアクセス可能に設定されている。
【００１６】
車載制御装置１０は、車両の制御を行う。車載制御装置１０は、車両内部の他の制御装置と、例えばＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を介して接続されている。
起動制御部１００は、車載制御装置１０の制御処理部１０１の起動および停止を制御する機能を有している。さらに、起動制御部１００は、制御処理部１０１の停止処理および起動処理を統括制御する機能も有している。
ここで、制御処理部１０１が起動していない状態とは、車載制御装置１０がスリープ状態、または車載制御装置１０の電源がオフとなっている状態である。
【００１７】
制御処理部１０１は、車内に搭載されている制御対象の機器を制御する機能を有している。なお、図１では、制御対象の機器を図示しておらず、以下の説明では、制御対象の機器のことを、単に制御対象と称する。車内に搭載されている制御対象とは、アクチュエーター等である。
具体的には、制御処理部１０１は、制御対象に対応した制御用プログラムデータを不揮発性記憶部１０２の第一の記憶領域１０２ａから読み出して、読み出したプログラムを実行することで、制御対象の制御を行う。
【００１８】
不揮発性記憶部１０２は、第一の記憶領域１０２ａと第二の記憶領域１０２ｂとを有している。第一の記憶領域１０２ａと第二の記憶領域１０２ｂは、物理的に隔離されている。
【００１９】
第一の記憶領域１０２ａは、制御処理部１０１が制御処理を実行するための制御用プログラムデータを格納する領域である。第一の記憶領域１０２ａは、制御処理部１０１の通常の動作時に使用するデータが格納されている領域である。
【００２０】
第二の記憶領域１０２ｂは、セキュアブート処理（改ざん検出処理）で使用する期待値（基準値）と検証値と、これらの期待値および検証値の比較結果を格納する領域である。期待値は、例えば、車載制御装置１０の開発段階において、第一の記憶領域１０２ａのデータに基づいて、検証値と同一の算出方法で生成される。
【００２１】
ここで、第一の記憶領域１０２ａに格納されたデータは、上述したように、制御処理部１０１が制御処理を実行するための制御用プログラムデータである。そのため、第一の記憶領域１０２ａに格納されたデータが不正に改ざんされてしまった場合には、制御対象の動作および車両全体の制御に重大な問題が生じるおそれがある。
【００２２】
第二の処理環境２０ｂ内に設けられた検証値生成部１０３は、第一の記憶領域１０２ａに格納された、通常の動作時に使用されるデータに基づいて、セキュアブート処理で使用する検証値を生成する機能を有している。検証値は、例えば、ＭＡＣ（Ｍｅｓｓａｇｅ

Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）、ハッシュなどを使用することができる。

【００２３】

第二の処理環境２０ｂ内に設けられた検証実行部１０４は、第二の記憶領域１０２ｂに格納されている期待値と、第一の記憶領域１０２ａのデータを基に検証値生成部１０３により生成された検証値とが、一致するか否かの検証を実行する。

【００２４】

第一の処理環境２０ａ内に設けられた検証判定部１０５は、検証実行部１０４の比較結果に基づいて、制御処理部１０１が制御対象に対する制御処理を実行してよいか否かを判定する。

【００２５】

検証実行部１０４による比較結果として、期待値と検証値が一致している場合には、検証判定部１０５は、第一の記憶領域１０２ａのデータは改ざんされていないと判定する。以下、この検証判定結果を「検証合格」と称する。

また、検証結果として期待値と検証値が一致していない場合には、検証判定部１０５は、第一の記憶領域１０２ａのデータが改ざんされていると判定する。以下、この検証判定結果を「検証不合格」と称する。

【００２６】

検証判定結果は、検証判定部１０５から起動制御部１００に出力される。起動制御部１００は、検証判定部１０５から出力された検証判定結果に基づいて、「検証合格」の場合には、制御処理部１０１の起動を実行し、「検証不合格」の場合には、制御処理部１０１の起動を中止する。

【００２７】

なお、以上の説明では、制御処理部１０１の起動を中止する場合には、制御処理部１０１の全ての機能の実行を中止するものとした。

しかしながら、実施の形態１における中止処理は、これに限られるものではない。例えば、制御処理部１０１の一部の機能の実行を制限した状態で、制御処理部１０１の起動を実行するようにしてもよい。

【００２８】

通信制御部１０６は、図示しない通信線を介して、車内に搭載されている他の機器と接続されている。通信制御部１０６は、起動制御部１００からの出力に基づいて、車載制御装置１０と外部機器との通信機能を有効化または無効化する機能を備えている。

【００２９】

時間計測部１０７は、起動制御部１００および通信制御部１０６に、所定の時刻となったことを通知する時計機能、または、ある時刻から所定の時間が経過したことを通知するタイマー機能を有している。

【００３０】

起動制御部１００および時間計測部１０７は、車載制御装置１０がスリープ状態または電源オフ状態であっても継続して起動可能なように構成されている。例えば、起動制御部１００および時間計測部１０７には、車載制御装置１０がスリープ状態または電源オフ状態であっても、電池または車内のバッテリー電源から電力が継続して供給されるようになっている。

【００３１】

次に、動作について説明する。

制御処理部１０１の停止時および起動時に実行される処理について、図２を用いて詳細に説明する。

図２は、起動制御部１００により、制御処理部１０１を停止および起動する場合の処理の流れを示している。

【００３２】

ステップＳ２０１において、起動制御部１００は、制御処理部１０１の停止処理を開始

する。制御処理部１０１の停止処理は、車載制御装置１０がスリープ状態または電源オフ状態となる直前に、自動的に実行されるように設定されている。

【００３３】

次に、ステップＳ２０２において、起動制御部１００は、通信制御部１０６に対して、現在の通信状態の問い合わせを行う。通信制御部１０６は、車載制御装置１０と外部機器との通信が有効となっているか否かを確認して、その確認結果を起動制御部１００に出力する。

【００３４】

続いて、起動制御部１００は、ステップＳ２０２において、通信が無効（ステップＳ２０２：ＮＯ）であった場合は、処理をステップＳ２０４に進める。

一方、起動制御部１００は、ステップＳ２０２において、通信が有効（ステップＳ２０２：ＹＥＳ）であった場合は、処理をステップＳ２０３に進める。

【００３５】

ステップＳ２０３（通信無効化ステップ）において、起動制御部１００は、通信制御部１０６に対して、通信を無効化する命令を出力する。起動制御部１００は、通信制御部１０６によって通信が無効化されたことを確認した後、処理をステップＳ２０４に進める。

【００３６】

ステップＳ２０４（第一のステップ）において、起動制御部１００は、第二の処理環境２０ｂ内の検証値生成部１０３に対して、検証値を生成する命令を出力する。

これを受けて、検証値生成部１０３は、不揮発性記憶部１０２の第一の処理環境２０ａ内の第一の記憶領域１０２ａから、セキュアブート処理における検証に用いるデータを読み出し、読み出したデータに基づいて検証値を生成する。

【００３７】

例えば、検証値がＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）であり、第二の処理環境２０ｂがＨＳＭ（Ｈａｒｄｗａｒｅ Ｓｅｃｕｒｉｔｙ Ｍｏｄｕｌｅ）である場合、検証値生成部１０３は、検証値ＭＡＣを生成する。

【００３８】

次いで、ステップＳ２０４５において、検証実行部１０４は、第二の記憶領域１０２ｂから期待値を読み出し、生成された検証値と期待値が一致するか否かを比較する（第二のステップ）。

ここで、期待値と検証値が一致している場合には、第一の記憶領域１０２ａのデータは改ざんされておらず、「一致」と判定する。

一方、期待値と検証値が一致していない場合には、検証判定部１０５は、第一の記憶領域１０２ａのデータは改ざんされており、「不一致」であると判定する。

そして、この比較結果を、第二の記憶領域１０２ｂに格納する（第三のステップ）。

【００３９】

このように、実施の形態１の車載制御装置１０は、制御処理部１０１を停止する前に、ステップＳ２０３で、通信機能を無効化した後に、ステップＳ２０４にて、セキュアブート処理で使用する検証値を生成するとともに、ステップＳ２０４５において、比較結果を格納する。

【００４０】

次に、ステップＳ２０５において、起動制御部１００は、制御処理部１０１による制御処理の動作を停止させる。

制御処理部１０１の動作停止に伴って、車載制御装置１０は、スリープ状態または電源オフ状態に移行する。ここで、起動制御部１００および時間計測部１０７は、車載制御装置１０がスリープ状態または電源オフ状態であっても、継続して起動するように設定されている。

【００４１】
以上の処理によって、制御処理部１０１の停止処理は、終了する。
この段階で、セキュアブート処理において使用する比較結果が導出されており、第二の記憶領域１０２ｂに格納された状態となっている。
【００４２】
次に、起動制御部１００による制御処理部１０１の起動処理について説明する。
ステップＳ２０６において、時間計測部１０７は、制御処理部１０１による制御処理を起動する所定の時刻となったことを、起動指令として、起動制御部１００に通知する。
ここで、所定の時刻とは、例えば、運転者が日常的に車両のエンジンを始動する時刻の直前（例えば１時間前）とする。または、運転者が選択した時刻を所定の時刻として、設定可能としてもよい。
【００４３】
また、所定の時刻ではなく、ある時刻から所定の時間（例えば１時間～１２時間）が経過したタイミングで、時間計測部１０７が起動制御部１００に起動指令を通知するようにしてもよい。
ここで、ある時刻とは、例えば、エンジンが停止した時刻または車載制御装置１０がスリープまたは電源オフとなった時刻とすればよい。また、所定の時間は、運転者が任意の時間を設定可能としてもよい。
【００４４】
次に、ステップＳ２０７において、起動制御部１００は、車載制御装置１０のスリープ状態を解除または電源オフ状態を解除する。これによって、車載制御装置１０は、起動状態となる。
続いて、ステップＳ２０７において、起動制御部１００は、通信制御部１０６に対して、通信機能を有効化する命令を出力する。通信制御部１０６は、起動制御部１００からの出力に基づいて、車載制御装置１０と外部との通信機能を、無効状態から有効状態に変更する。
【００４５】
次に、ステップＳ２０８において、起動制御部１００は、車載制御装置１０に対して、通信線および通信制御部１０６を介して、外部機器から制御処理部１０１の起動要求があったか否かを判断する。
そして、起動要求があった場合（ステップＳ２０８：ＹＥＳ）には、起動制御部１００は、制御処理部１０１の起動処理を開始する。
【００４６】
一方、ステップＳ２０８において、制御処理部１０１の起動要求がない場合（ステップＳ２０８：ＮＯ）には、起動制御部１００は、制御処理部１０１の起動処理を実行しない。
ここで、外部機器からの制御処理部１０１の起動要求とは、例えば、ＣＡＮ通信を介して、車載制御装置１０以外の他のＥＣＵから出力される起動要求などである。
【００４７】
次いで、制御処理部１０１の起動処理について説明する。
ステップＳ２０９（第四のステップ）において、制御処理部１０１の起動を要求された起動制御部１００は、第二の処理環境２０ｂ内の検証実行部１０４と検証判定部１０５に対して、比較結果を検証する命令を出力する。
ステップＳ２０９において、検証実行部１０４により、第二の記憶領域１０２ｂから比較結果が読み出され、第一の処理環境２０ａ内の検証判定部１０５に出力される。
【００４８】
ステップＳ２１０（第四のステップ）において、検証判定部１０５は、比較結果から第一の記憶領域１０２ａのデータが改ざんされているか否かを判定する。検証判定部１０５は、検証判定の結果を、起動制御部１００に出力する。
具体的には、検証判定部１０５は、比較結果が「一致」の場合には、「検証合格」と判

定する（ステップＳ２１０：ＹＥＳ）。
一方、比較結果が「不一致」の場合には、「検証不合格」であると判定する（ステップＳ２１０：ＮＯ）。検証判定の結果は、検証判定部１０５から起動制御部１００に出力される。
【００４９】
起動制御部１００は、検証判定の結果に基づいて、制御処理部１０１を起動させるか否かを制御する。検証判定の結果が「検証合格」の場合（ステップＳ２１０：ＹＥＳ）には、起動制御部１００は、制御処理部１０１を起動させる（ステップＳ２１１、第五のステップ）。起動された制御処理部１０１は、制御対象の制御を開始する。
【００５０】
一方、検証判定の結果が「検証不合格」の場合（ステップＳ２１０：ＮＯ）には、起動制御部１００は、制御処理部１０１の起動を中止する（ステップＳ２１２、第五のステップ）。
このようにすることにより、制御処理部１０１が、改ざんされたデータに基づいて制御対象を制御することを防止することができる。
【００５１】
なお、以上の説明では、ステップＳ２１０において、検証判定部１０５が実施する検証判定を、「検証合格・検証不合格」の二段階の判定とした。また、制御処理部１０１の起動を中止する場合には、制御処理部１０１の全ての機能の実行を中止するとした。しかしながら、本実施の形態１は、これらのような処理に限られるものではない。
【００５２】
例えば、検証実行結果に基づく検証判定の段階を、「検証合格・検証一部不合格」の二段階、または、「検証合格・検証一部不合格・検証不合格」の三段階としてもよい。
そして、検証一部不合格と判定された場合には、例えば、起動制御部１００は、検証不合格となった一部のデータまたはプログラムに対応する制御処理部１０１の一部の機能の実行を制限した状態で、制御処理部１０１の起動を行うようにしてもよい。
【００５３】
具体的には、以下に説明するように、制御用プログラムデータ毎に検証を行うことによって、検証合格となった制御用プログラムデータに対応する制御処理を実行し、検証不合格となった制御用プログラムデータに対応する制御処理を実行しないように制限して、制御処理部１０１の起動を行うようにすればよい。
【００５４】
第一の記憶領域１０２ａに、複数の制御対象または複数の制御処理に対応した複数の制御用プログラムデータが存在する場合が想定される。その場合は、検証値生成部１０３は、複数の制御用プログラムデータにそれぞれ対応した複数の検証値を生成する。
【００５５】
続いて、検証実行部１０４は、複数の制御用プログラムデータにそれぞれ対応した複数の検証値と、複数の検証値のそれぞれに対応して予め第二の記憶領域１０２ｂに格納された期待値とを比較する。これらの複数の比較結果は、第二の記憶領域１０２ｂに格納される。
【００５６】
次に、検証実行部１０４は、第二の記憶領域１０２ｂに格納された比較結果を検証判定部１０５に出力する。
検証判定部１０５は、検証実行部１０４からの複数の比較結果に基づいて、複数の制御用プログラムデータそれぞれについて、検証合格か不合格かを判定する。そして、検証結果が全て「一致」の場合には、検証判定部１０５は、第一の記憶領域１０２ａのデータは改ざんされておらず、「検証合格」であると判定する。
一方、一部の比較結果に「不一致」が含まれている場合には、検証判定部１０５は、第一の記憶領域１０２ａのデータは部分的に改ざんされており、「検証一部不合格」であると判定する。

【００５７】
続いて、検証判定部１０５は、「検証合格」と判定された制御用プログラムデータに対応する制御処理を起動許可制御処理に指定し、「検証一部不合格」と判定された制御用プログラムデータのうち「不一致」に対応する制御処理を起動不許可制御処理に指定する。
起動制御部１００は、検証判定部１０５によって起動許可制御処理に指定された制御処理に限定して、制御処理部１０１の起動を実行する。
これにより、検証不合格となった制御用プログラムデータに対応する制御処理の実行を制限した状態で、制御処理部１０１を起動することができる。
【００５８】
なお、車載制御装置１０は、ハードウェアの一例を図３に示すように、プロセッサ１１と記憶装置１２から構成される。
記憶装置１２は図示していないが、ランダムアクセスメモリ等の揮発性記憶装置と、フラッシュメモリ等の不揮発性の補助記憶装置とを具備する。また、フラッシュメモリの代わりにハードディスクの補助記憶装置を具備してもよい。
プロセッサ１１は、記憶装置１２から入力されたプログラムを実行する。この場合、補助記憶装置から揮発性記憶装置を介してプロセッサ１１にプログラムが入力される。また、プロセッサ１１は、演算結果等のデータを記憶装置１２の揮発性記憶装置に出力してもよいし、揮発性記憶装置を介して補助記憶装置にデータを保存してもよい。
【００５９】
また、上述の実施の形態１の説明では、制御装置を車載制御装置として使用する例について説明した。
しかしながら、制御装置は、これに限られるものでない。例えば、高いセキュリティ強度を有し、かつ、高速な起動を必要とする、通信線に接続された制御装置に利用することができる。
【００６０】
実施の形態１によれば、制御処理に用いるデータが改ざんされているか否かを確認するために行うセキュアブート処理において、以下のような効果が得られる。
従来の制御装置においては、制御処理を起動する前に、セキュアブート処理に用いる検証値を生成していた。これに対して、実施の形態１の制御装置は、制御処理が停止する前に、セキュアブート処理に用いる比較結果を生成する構成を有している。そして、制御処理が起動する前に、予め生成した比較結果を用いて、セキュアブート処理を行うようにしている。
これにより、制御処理を起動する前に行うセキュアブート処理の処理時間を、従来に比べて短縮することができる。
【００６１】
また、改ざん検出の対象となるプログラムおよびデータの量を増加させた場合、あるいはセキュアブート処理自体に用いるデータ量を増加させた場合であっても、高いセキュリティ強度を有しつつ、制御装置の起動時に実行されるセキュアブート処理の処理時間を短縮することができる。
【００６２】
また、このように、セキュアブート処理に用いる検証値だけでなく、検証値と期待値の比較結果を、時間制約の厳しい制御装置の起動の前ではなく、制御装置の停止前に予め生成しておくことにより、検証値生成のための暗号鍵のデータ量を十分に確保することができる。そのため、セキュアブート処理の信頼度を高めることができる。
【００６３】
さらに、実施の形態１の制御装置は、第一の処理環境２０ａと、第一の処理環境２０ａから隔離された第二の処理環境２０ｂとを有し、第二の処理環境２０ｂ内でセキュアブート処理に用いる検証値の生成、検証値の格納、検証値と期待値の比較結果の格納、およびセキュアブートによる検証を実行する構成にしている。
そして、比較結果が格納される第二の記憶領域１０２ｂは、第二の処理環境２０ｂから

のみアクセス可能に設定されている。これにより、セキュアブート処理自体のセキュリティ強度と信頼度を高めることができる。

【００６４】

さらに、実施の形態１の制御装置は、制御装置の通信機能を無効化した状態で、検証値の生成および検証値と期待値の比較結果の格納を行う構成にしている。これにより、通信線を介した外部からの攻撃によるデータの改ざんを防ぐことができる。

【００６５】

さらに、実施の形態１の制御装置は、制御装置の通信状態を、通信無効状態から通信有効状態に復帰させる手段として、制御装置内に時間計測部を備え、時間計測部で計測した所定の時間に基づいて制御装置を通信有効状態とする構成にしている。

これにより、通信線を介した外部からの攻撃を受けることなく、制御装置の通信状態を、通信無効状態から通信有効状態に復帰させることが可能となる。

【００６６】

本開示は、例示的な実施の形態が記載されているが、実施の形態に記載された様々な特徴、態様、および機能は特定の実施の形態の適用に限られるのではなく、単独で、または様々な組み合わせで実施の形態に適用可能である。

従って、例示されていない無数の変形例が、本願明細書に開示される技術の範囲内において想定される。例えば、少なくとも１つの構成要素を変形する場合、追加する場合または省略する場合が含まれるものとする。

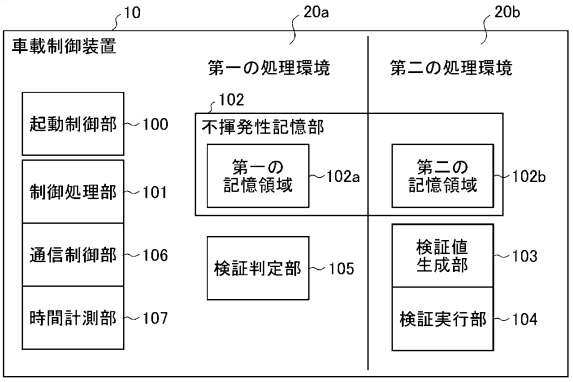
【符号の説明】

【００６７】

１０　車載制御装置、１１　プロセッサ、１２　記憶装置、２０ａ　第一の処理環境、
２０ｂ　第二の処理環境、１００　起動制御部、１０１　制御処理部、
１０２　不揮発性記憶部、１０２ａ　第一の記憶領域、１０２ｂ　第二の記憶領域、
１０３　検証値生成部、１０４　検証実行部、１０５　検証判定部、
１０６　通信制御部、１０７　時間計測部

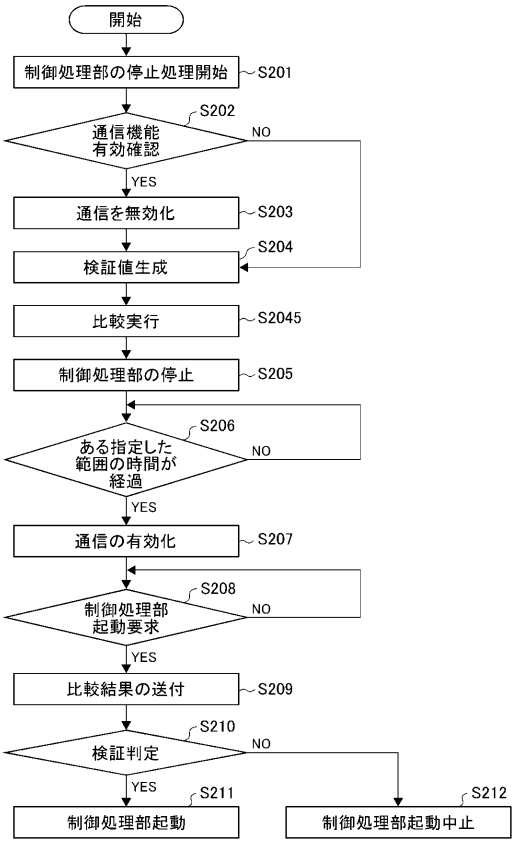
【図１】

図１



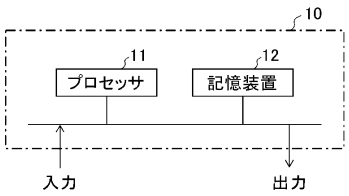
【図２】

図２



【図３】

図３



フロントページの続き

(72)発明者　松井　俊憲
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　田中　啓介

(56)参考文献　特開２０１７－０３３２４８（ＪＰ，Ａ）
特開２０１２－０３２９２５（ＪＰ，Ａ）
特開２０１５－０５５８９８（ＪＰ，Ａ）
国際公開第２０１６／１８５５７７（WO，Ａ１）
特開２０１５－０２９２４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ８／００－８／３８
Ｇ０６Ｆ８／６０－８／７７
Ｇ０６Ｆ９／４４－９／４４５、９／４５１
Ｇ０６Ｆ１２／１４
Ｇ０６Ｆ２１／００－２１／８８