

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7013921号
(P7013921)

(45)発行日 令和4年2月1日(2022.2.1)

(24)登録日 令和4年1月24日(2022.1.24)

(51)国際特許分類	F I			
G 0 6 F 21/56 (2013.01)	G 0 6 F 21/56	3 5 0		
G 0 6 F 21/64 (2013.01)	G 0 6 F 21/64			

請求項の数 7 (全14頁)

(21)出願番号	特願2018-27114(P2018-27114)	(73)特許権者	000004260 株式会社デンソー 愛知県刈谷市昭和町1丁目1番地
(22)出願日	平成30年2月19日(2018.2.19)	(74)代理人	100140486 弁理士 鎌田 徹
(65)公開番号	特開2019-144752(P2019-144752 A)	(74)代理人	100170058 弁理士 津田 拓真
(43)公開日	令和1年8月29日(2019.8.29)	(72)発明者	岡部 達哉 愛知県刈谷市昭和町1丁目1番地 株式 会社デンソー内
審査請求日	令和2年12月9日(2020.12.9)	(72)発明者	奥野 英一 愛知県刈谷市昭和町1丁目1番地 株式 会社デンソー内
		(72)発明者	野尻 孝男 愛知県刈谷市昭和町1丁目1番地 株式 最終頁に続く

(54)【発明の名称】 検証端末

(57)【特許請求の範囲】

【請求項1】

プログラム又はデータの正当性検証を行う検証端末であって、
プログラム又はデータを格納する格納部(104)と、
前記格納部に格納されている自端末プログラム又は自端末データの自端末ハッシュ値を生成する検証値生成部(101)と、
前記自端末プログラム又は前記自端末データと同一のプログラム又はデータが格納されていると想定される端末であって、少なくとも1つの他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得する検証値取得部(102)と、
前記自端末ハッシュ値と前記他端末ハッシュ値との同一性に基づいて、前記自端末プログラム又は前記自端末データの健全性を検証する検証実行部(103)と、を備え、
前記検証値取得部は、2以上の他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得し、
前記検証実行部は、前記自端末ハッシュ値と前記他端末ハッシュ値との同一数が少なくとも過半数の場合に、前記自端末プログラム又は前記自端末データを健全であると判断する検証端末。

【請求項2】

請求項1に記載の検証端末であって、
前記検証値取得部は、乱数に基づいて前記他端末を選択する、検証端末。

【請求項3】

請求項 1 又は 2 に記載の検証端末であって、

前記検証実行部は、前記自端末ハッシュ値と前記他端末ハッシュ値とが同一でない場合に、前記自端末プログラム又は前記自端末データを健全であるとする判断を保留する、検証端末。

【請求項 4】

請求項 3 に記載の検証端末であって、

前記検証値取得部は、2 以上の他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得し、

前記検証実行部は、前記自端末ハッシュ値と同一の前記他端末ハッシュ値が過半数を超えない場合に、前記自端末プログラム又は前記自端末データを不健全であると判断する、検証端末。

10

【請求項 5】

請求項 3 に記載の検証端末であって、

前記検証実行部は、前記自端末ハッシュ値と前記他端末ハッシュ値とが同一でない場合に、ネットワークを経由してハッシュ値管理サーバーに健全性の問い合わせを行う、検証端末。

【請求項 6】

請求項 5 に記載の検証端末であって、

前記検証値取得部は、2 以上の他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得し、

前記検証実行部は、前記自端末ハッシュ値と前記他端末ハッシュ値とが全て同一でない場合に、ネットワークを経由してハッシュ値管理サーバーに健全性の問い合わせを行う、検証端末。

20

【請求項 7】

請求項 6 に記載の検証端末であって、

前記検証実行部は、前記ハッシュ値管理サーバーに格納されており、正当なプログラム又は正当なデータに対応するマスターハッシュ値を受信し、この受信したマスターハッシュ値と前記自端末ハッシュ値との同一性に基づいて、前記自端末プログラム又は前記自端末データの健全性を検証する、検証端末。

【発明の詳細な説明】

30

【技術分野】

【0001】

本開示は、プログラム又はデータの正当性検証を行う検証端末に関する。

【背景技術】

【0002】

自動車に通信端末を搭載し、ネットワークを介して又は直接他の車やインフラ装置やサーバーと通信を行うコネクテッドカーが普及すると、膨大な台数の端末のセキュリティを確保する必要がある。同様に、IoT 技術が更に展開されると、やはり膨大な台数の端末のセキュリティを確保する必要がある。

【0003】

40

セキュリティ確保の一つの観点として、コンピューターに格納されているプログラムの正当性を検証するものが提案されている（例えば、下記特許文献 1）。下記特許文献 1 に開示されている発明は、サーバーに格納されているプログラムとクライアントに格納されているプログラムとについて、暗号鍵を用いて差分を検出するものである。

【0004】

自動車に搭載されている ECU (Electronic Control Unit) に格納されているプログラムの改竄防止の観点からは、メンテナンスの際に不正なプログラムが入り込まないようにするものが提案されている（例えば、下記特許文献 2）。下記特許文献 2 に開示されている発明は、メンテナンスの際に認証プロセスを走らせることで、正規の作業員によるメンテナンスを担保している。

50

【0005】

1台の自動車に搭載されているECUは相当な数になっており、相互に通信を行うことで運転制御を実現している。この観点から、車載ECUを繋ぐネットワークに流れる不正なデータを検出することが提案されている（例えば、下記特許文献3）。下記特許文献3に開示されている発明は、車内ネットワークを流れるデータの正当性を各ECUにおいて検証するものである。

【先行技術文献】

【特許文献】

【0006】

【文献】特開2012-165289号公報

10

特開2013-168007号公報

特開2017-112594号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

特許文献1に記載されているように、クライアントサーバー型で中央集権的に管理する手法は、上記したように膨大な端末のセキュリティを確保する場合に、ネットワーク負荷が過大になることや、常時接続を担保しなければならないといった別の技術的課題が発生する。

【0008】

20

ネットワーク負荷の課題を解決するためには、車載端末やIoT端末のようにエッジ側での対処が必要になる。しかしながら、特許文献2に記載されているように、メンテナンスの際の正当性を確認する手法では、メンテナンス後のプログラム改竄を検出することができない。また、特許文献3に記載されているように、車内ネットワークを流れるデータの正当性をECUが検証する手法では、不正なデータ検出がECUのプログラムに起因するのか、不正なトラフィックに起因するのかを検出することができない。

【0009】

本開示は、ネットワーク負荷を極力低減しつつ、端末に格納されているプログラム又はデータの改竄を早期に検出することを目的とする。

【課題を解決するための手段】

30

【0010】

本開示は、プログラム又はデータの正当性検証を行う検証端末であって、プログラム又はデータを格納する格納部(104)と、格納部に格納されている自端末プログラム又は自端末データの自端末ハッシュ値を生成する検証値生成部(101)と、自端末プログラム又は自端末データと同一のプログラム又はデータが格納されていると想定される端末であって、少なくとも1つの他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得する検証値取得部(102)と、自端末ハッシュ値と他端末ハッシュ値との同一性に基づいて、自端末プログラム又は自端末データの健全性を検証する検証実行部(103)と、を備える。

【0011】

40

本開示においては、自端末プログラムと他端末プログラム又は自端末データと他端末データとが同一であるのが正常であるとの前提条件で、自端末ハッシュ値と他端末ハッシュ値との同一性を確認している。自端末プログラム又は自端末データと、他端末プログラム又は他端末データとが共に改竄もされておらず最新のバージョンであるといった健全性が確保されていれば、自端末ハッシュ値と他端末ハッシュ値とが同一になるので、自端末プログラム又は自端末データの健全性を検証することができる。このように、自端末と他端末との間の通信のみで自端末プログラム又は自端末データの健全性を検証することができるので、ネットワーク負荷を低減することができると共に、他端末を選択して比較することによるランダム性も確保できる。更に、自端末ハッシュ値と他端末ハッシュ値とを随時比較することができるので、プログラムやデータをダウンロードした場合のみならず、その

50

後においても検証を継続することができる。

【 0 0 1 2 】

尚、「課題を解決するための手段」及び「特許請求の範囲」に記載した括弧内の符号は、後述する「発明を実施するための形態」との対応関係を示すものであって、「課題を解決するための手段」及び「特許請求の範囲」が、後述する「発明を実施するための形態」に限定されることを示すものではない。

【発明の効果】

【 0 0 1 3 】

本開示によれば、ネットワーク負荷を極力低減しつつ、端末に格納されているプログラム又はデータの改竄を早期に検出することができる。

10

【図面の簡単な説明】

【 0 0 1 4 】

【図 1】図 1 は、本実施形態の基本概念を説明するための図である。

【図 2】図 2 は、本実施形態である検証端末の機能的な構成を説明するための図である。

【図 3】図 3 は、検証端末の情報処理を説明するためのフローチャートである。

【図 4】図 4 は、検証端末の情報処理を説明するためのフローチャートである。

【図 5】図 5 は、検証端末の情報処理を説明するためのフローチャートである。

【図 6】図 6 は、検証端末の情報処理を説明するためのフローチャートである。

【図 7】図 7 は、検証端末の情報処理の結果を受けて表示される画面の例を示す図である。

【図 8】図 8 は、検証端末の情報処理の結果を受けて表示される画面の例を示す図である。

20

【図 9】図 9 は、検証端末の情報処理の結果を受けて表示される画面の例を示す図である。

【図 10】図 10 は、検証端末の情報処理の結果を受けて表示される画面の例を示す図である。

【図 11】図 11 は、検証端末の情報処理の結果を受けて表示される画面の例を示す図である。

【図 12】図 12 は、検証端末の情報処理の結果を受けて表示される画面の例を示す図である。

【図 13】図 13 は、本実施形態において端末間及び端末サーバー間の情報授受を説明するための図である。

【発明を実施するための形態】

30

【 0 0 1 5 】

以下、添付図面を参照しながら本実施形態について説明する。説明の理解を容易にするため、各図面において同一の構成要素に対しては可能な限り同一の符号を付して、重複する説明は省略する。

【 0 0 1 6 】

図 1 を参照しながら、本実施形態の基本概念を説明する。本実施形態は自動車に搭載される検証端末を例示しているが、本開示の技術的思想は全ての分散された情報端末のセキュリティ確保のために応用されうるものである。一例ではあるが、ゲームソフトをダウンロードする情報端末や、携帯電話、スマートフォン、IoT 機器といった各種情報端末のセキュリティ確保に用いることができる。

40

【 0 0 1 7 】

図 1 に示される例では、自動運転車 10、20、21、22、23 と、管理サーバー 30 とによって構成される検証網を示している。自動運転車 10 が、自己のプログラム又はデータの健全性を判断するものとする。自動運転車 20、21、22、23 は、自動運転車 10 と同種の自動運転車であり、自動運転車 10、20、21、22、23 には、全て同じプログラム又はデータが格納されていることが期待される関係となっている。

【 0 0 1 8 】

自動運転車 20、21 は、正常な自動運転車であり、正常なハッシュ値が格納されているものとする。自動運転車 22 は、異常状態にある自動運転車であり、異常なハッシュ値が格納されている。自動運転車 23 は、正常な自動運転車であり、格納されているプログラ

50

ム又はデータが最新版に更新されているものであって、最新版に対応する正常なハッシュ値が格納されている。

【 0 0 1 9 】

自動運転車 1 0 に格納されているプログラム又はデータのハッシュ値が正常である場合、自動運転車 2 0 , 2 1 に格納されているプログラム又はデータのハッシュ値と照合すると、互いに整合性が取れており同一であることが確認される。

【 0 0 2 0 】

一方、自動運転車 1 0 に格納されているプログラム又はデータのハッシュ値が正常である場合であって、自動運転車 2 2 に格納されているプログラム又はデータのハッシュ値と照合すると、互いに整合性が取れず同一であることが確認できない。この場合、自動運転車 1 0 は、自動運転車 2 0 , 2 1 に格納されているプログラム又はデータのハッシュ値と整合性が取れていることから、整合性が取れていないのが 1 台に対して整合性が取れているのが 2 台であることを根拠に、自動運転車 2 2 に格納されているプログラム又はデータが不健全であると判断することができる。

10

【 0 0 2 1 】

更に、自動運転車 1 0 に格納されているプログラム又はデータに対して、更新されている新しいプログラム又はデータが格納されている自動運転車 2 3 を考えると、多数決によつての判断がし難くなる場合も想定される。このような場合、自動運転車 1 0 は、管理サーバー 3 0 に自己のハッシュ値を送信すると共に、マスターハッシュ値の送信を要求することができる。マスターハッシュ値とは、自動運転車 1 0 , 2 0 , 2 1 , 2 2 , 2 3 において格納されるべき最新且つ正当なプログラム又はデータから算出されるハッシュ値である。自動運転車 1 0 においては、自己のハッシュ値とマスターハッシュ値とを比較して、自己のプログラム又はデータの正当性や最新性を確認することができる。

20

【 0 0 2 2 】

自動運転車 1 0 , 2 0 , 2 1 , 2 2 , 2 3 の相互におけるハッシュ値の送受信や、自動運転車 1 0 と管理サーバー 3 0 との間におけるハッシュ値の送受信には、既知の暗号化技術を用いることができる。

【 0 0 2 3 】

続いて、図 2 を参照しながら、本実施形態に係る検証端末 1 0 A の機能的な構成要素について説明する。検証端末 1 0 A は、自動運転車 1 0 に搭載される通信可能な情報端末である。検証端末 1 0 A は、ハードウェア的な構成要素として、CPU といった演算部、RAM や ROM といった記憶部、データの授受を行うためのインターフェイス部を備えるコンピュータとして構成されている。検証端末 1 0 A は、自動運転車 2 0 , 2 1 , 2 2 , 2 3 に搭載されている同様の検証端末と相互に情報送受信可能なように構成されている。検証端末 1 0 A は、管理サーバー 3 0 とも相互に情報送受信可能なように構成されている。続いて、制御装置の機能的な構成要素について説明する。

30

【 0 0 2 4 】

検証端末 1 0 A は、検証値生成部 1 0 1 と、検証値取得部 1 0 2 と、検証実行部 1 0 3 と、格納部 1 0 4 と、を備えている。格納部 1 0 4 は、プログラムやデータ、プログラム又はデータから算出されるハッシュ値を格納する部分である。

40

【 0 0 2 5 】

検証値生成部 1 0 1 は、格納部 1 0 4 に格納されている自端末プログラム又は自端末データの自端末ハッシュ値を生成する部分である。

【 0 0 2 6 】

検証値取得部 1 0 2 は、自端末プログラム又は自端末データと同一のプログラム又はデータが格納されていると想定される端末であって、少なくとも 1 つの他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得する部分である。本実施形態の場合、他端末とは、自動運転車 2 0 , 2 1 , 2 2 , 2 3 に搭載されている端末である。

【 0 0 2 7 】

50

検証実行部 103 は、自端末ハッシュ値と他端末ハッシュ値との同一性に基づいて、自端末プログラム又は自端末データの健全性を検証する部分である。

【0028】

本実施形態においては、自端末プログラムと他端末プログラム又は自端末データと他端末データとが同一であるのが正常であるとの前提条件で、自端末ハッシュ値と他端末ハッシュ値との同一性を確認している。自端末プログラム又は自端末データと、他端末プログラム又は他端末データとが共に改竄もされておらず最新のバージョンであるといった健全性が確保されていれば、自端末ハッシュ値と他端末ハッシュ値とが同一になるので、自端末プログラム又は自端末データの健全性を検証することができる。このように、自端末と他端末との間の通信のみで自端末プログラム又は自端末データの健全性を検証することができるので、ネットワーク負荷を低減することができると共に、他端末を選択して比較することによるランダム性も確保できる。更に、自端末ハッシュ値と他端末ハッシュ値とを随時比較することができるので、プログラムやデータをダウンロードした場合のみならず、その後においても検証を継続することができる。

10

【0029】

本実施形態において、検証値取得部 102 は、2 以上の他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得し、検証実行部 103 は、自端末ハッシュ値と他端末ハッシュ値との同一数が少なくとも過半数の場合に、自端末プログラム又は自端末データを健全であると判断することができる。2 以上の他端末における他端末ハッシュ値を比較し、少なくとも過半数の同一性をもって検証するので、確実に自端末プログラム又は自端末データの健全性を検証することができる。

20

【0030】

本実施形態において、検証値取得部 102 は、乱数に基づいて他端末を選択することができる。乱数に基づいて他端末を選択するので、他端末を選択して比較することによるランダム性をより高めることができる。

【0031】

本実施形態において、検証実行部 103 は、自端末ハッシュ値と他端末ハッシュ値とが同一でない場合に、自端末プログラム又は自端末データを健全であるとする判断を保留することができる。

【0032】

自端末ハッシュ値と他端末ハッシュ値とが同一でない場合でも、自端末プログラム又は自端末データが不健全であるのか、他端末側が不健全であるのかを判断することができない場合もある。そこで、自端末プログラム又は自端末データを健全であるとする判断を保留することで、更に他の他端末における他端末ハッシュ値と比較をしたり、管理サーバーに格納されているハッシュ値と比較したりといった手法を組み込むことができる。

30

【0033】

本実施形態において、検証値取得部 102 は、2 以上の他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得し、検証実行部 103 は、自端末ハッシュ値と同一の他端末ハッシュ値が過半数を超えない場合に、自端末プログラム又は自端末データを不健全であると判断することができる。

40

【0034】

自端末ハッシュ値と同一の他端末ハッシュ値が過半数を超えない場合には、自端末ハッシュ値が少数派なので、改竄されていたりアップデートされていなかったりといった不健全な状態である蓋然性が高いと判断することも可能であるので、自端末プログラム又は自端末データを不健全であると判断することができる。

【0035】

本実施形態において、検証実行部 103 は、自端末ハッシュ値と他端末ハッシュ値とが同一でない場合に、ネットワークを経由してハッシュ値管理サーバーである管理サーバー 30 に健全性の問い合わせを行うことができる。

【0036】

50

自端末ハッシュ値と他端末ハッシュ値とが同一でない場合、自端末プログラムが不健全な可能性があるため、ネットワークを経由して管理サーバー 30 に健全性の問い合わせを行い、自端末プログラム又は自端末データの健全性を検証する。自端末ハッシュ値と他端末ハッシュ値とが同一の場合には健全性の問い合わせを実行しないので、ネットワーク負荷を低減することができる。

【0037】

本実施形態において、検証値取得部 102 は、2 以上の他端末に格納されている他端末プログラム又は他端末データの他端末ハッシュ値を取得し、検証実行部 103 は、自端末ハッシュ値と他端末ハッシュ値とが全て同一でない場合に、ネットワークを経由してハッシュ値管理サーバーである管理サーバー 30 に健全性の問い合わせを行うことができる。

10

【0038】

自端末ハッシュ値と他端末ハッシュ値とが全て同一でない場合、自端末プログラム又は自端末データと、他端末プログラム又は他端末データのどちらが不健全であるかが分からないので、ネットワークを経由して管理サーバー 30 に健全性の問い合わせを行い、自端末プログラム又は自端末データの健全性を検証することができる。

【0039】

本実施形態において、検証実行部 103 は、ハッシュ値管理サーバーである管理サーバー 30 に格納されており、正当なプログラム又は正当なデータに対応するマスターハッシュ値を受信し、この受信したマスターハッシュ値と自端末ハッシュ値との同一性に基づいて、自端末プログラム又は自端末データの健全性を検証することができる。

20

【0040】

正当なプログラム又は正当なデータに対応するマスターハッシュ値と、自端末ハッシュ値との同一性に基づいて判断するので、より確実に自端末プログラム又は自端末データの健全性を判断することができる。

【0041】

続いて、図 3 を参照しながら、検証端末 10A の情報処理について説明する。ステップ S101 では、検証値取得部 102 が、イベント開始タイミングであるか否かを判断する。イベント開始タイミングが到来していなければ、ステップ S101 の判断を繰り返し、イベント開始タイミングが到来していれば、ステップ S102 の処理に進む。

【0042】

ステップ S102 では、検証値生成部 101 が、ハードウェア選択処理を実行する。ステップ S102 のハードウェア選択処理については、図 4 を参照しながら説明する。

30

【0043】

図 4 のステップ S151 では、検証値生成部 101 が周囲の自動運転車や情報端末の RSSI (Received Signal Strength Indicator) を取得する。RSSI は、Wi-Fi ネットワークにおける受信信号強度を示すものである。RSSI が大きいものを選択することで、近隣の端末を特定することができる。尚、近隣の端末を特定するという観点からは、GPS 情報を用いることもできる。

【0044】

ステップ S151 に続くステップ S152 では、同一種類のハードウェアを検出する。例えば、図 1 に示される例では、自動運転車 20, 21, 22, 23 を同一種類のハードウェアとして検出する。

40

【0045】

ステップ S152 に続くステップ S153 では、ステップ S152 で検出したハードウェアからより少ない数のハードウェアを抽出する。例えば、図 1 に示される例では、自動運転車 20, 21, 22, 23 を同一種類のハードウェアとして検出した上で、自動運転車 21 及び自動運転車 22 を抽出する。ステップ S153 の処理が終了すると、ハードウェア選択処理を終了し、図 3 のステップ S103 の処理に進む。

【0046】

ステップ S103 では、検証値生成部 101 及び検証値取得部 102 がハッシュ値取得処

50

理を実行する。ハッシュ値取得処理については、図5を参照しながら説明する。

【0047】

図5のステップS201では、検証値生成部101が自端末ハッシュ値を計算する。ステップS201に続くステップS202では、検証値取得部102が、ステップS102において抽出したハードウェア（例えば、自動運転車21及び自動運転車22）にハッシュ値を送信する。ハッシュ値を受信した他のハードウェアは、自己が算出したハッシュ値を返信する。

【0048】

ステップS202に続くステップS203では、検証値取得部102が、他のハードウェアが送信したハッシュ値を受信する。ステップS203に続くステップS204では、検証値取得部102が、ハッシュ値比較結果を取得する。ハッシュ値比較結果は、他のハードウェアから受信したハッシュ値と、自己のハッシュ値とを検証値取得部102が比較算出してもよく、他のハードウェアにおいて比較算出されてもよい。

【0049】

ステップS204に続くステップS205では、検証値取得部102が、ハッシュ値比較結果が所定数以上取得できたか否かを判断する。ハッシュ値比較結果が所定数集まらなければステップS204の処理に戻り、ハッシュ値比較結果が所定数集まればハッシュ値比較処理を終了し、図3のステップS104の処理に進む。

【0050】

ステップS104では、検証実行部103がハッシュ値判定処理を実行する。ハッシュ値判定処理については、図6を参照しながら説明する。

【0051】

ステップS251では、検証実行部103が、自端末ハッシュ値と異なる値の他端末ハッシュ値が過半数あるか否かを判断する。自端末ハッシュ値と異なる値のハッシュ値が過半数あれば、ステップS252の処理に進む。自端末ハッシュ値と異なる値のハッシュ値が過半数なければ、ステップS253の処理に進む。

【0052】

ステップS252では、検証実行部103が表示画面に異常表示を行う。異常表示の例について、図7、図8、図9に示す。図7に示される例は、検証端末10Aが自動運転車に搭載されている場合の例である。異常発生を告知すると共に、異常の可能性に言及し、ディーラーに行き対処するように提案している。図8に示される例も、検証端末10Aが自動運転車に搭載されている場合の例である。異常発生を告知すると共に、異常の可能性に言及し、自動運転から手動運転に切り替えるとともにディーラーに行き対処するように提案している。図9に示される例は、検証端末10Aが携帯端末である場合や、AIスピーカーといったIoT機器に搭載される場合の例である。異常発生を告知すると共に、異常の可能性に言及し、メーカーに連絡して対処するように提案している。

【0053】

ステップS253では、検証実行部103が、自端末ハッシュ値と他端末ハッシュ値とが全て同一であるか否かを判断する。自端末ハッシュ値と他端末ハッシュ値とが全て同一であれば、ステップS254の処理に進む。自端末ハッシュ値と他端末ハッシュ値とが全て同一でなければ、ステップS255の処理に進む。

【0054】

ステップS254では、検証実行部103が表示画面に正常表示を行う。正常表示の例について、図10に示す。図10に示される例では、制御ソフトウェアが正常である旨を表示している。

【0055】

ステップS255では、検証値取得部102が、管理サーバー30からマスターハッシュ値を取得する。ステップS255に続くステップS256では、検証実行部103が、自端末ハッシュ値とマスターハッシュ値とが同一であるか否かを判断する。自端末ハッシュ値とマスターハッシュ値とが同一であれば、ステップS254の処理に進む。自端末ハッ

10

20

30

40

50

シユ値とマスターハッシュ値とが同一でなければ、ステップ S 2 5 7 の処理に進む。

【 0 0 5 6 】

ステップ S 2 5 7 では、検証実行部 1 0 3 が表示画面に警告表示を行う。警告表示の例について図 1 1、図 1 2 に示す。図 1 1 に示される例は、検証端末 1 0 A が自動運転車に搭載されている場合の例である。制御ソフトウェアが最新でないことを告知し、ディーラーに行き対処するように提案している。図 1 2 に示される例は、検証端末 1 0 A が携帯端末である場合や、AIスピーカーといったIoT機器に搭載される場合の例である。インストールされているソフトウェアが最新のものでないことを告知し、アップデートを行うことを提案している。

【 0 0 5 7 】

ステップ S 2 5 2、ステップ S 2 5 4、ステップ S 2 5 7 の処理が終了すると、ハッシュ値判定処理を終了する。

【 0 0 5 8 】

図 1 3 に示されるシーケンス図は、自動運転車間や自動運転車と管理サーバーとの間の情報の授受を示すものである。自動運転車 1 0 は、ステップ S 3 0 1 においてハードウェア選択処理を実行する。ハードウェア選択処理については、説明済であるので詳細説明を省略する。図 1 3 の例の場合は、自動運転車 2 0 を選択している。

【 0 0 5 9 】

ステップ S 3 0 1 に続くステップ S 3 0 2 では、自動運転車 1 0 が自端末ハッシュ値を計算している。続いて、自動運転車 1 0 は自動運転車 2 0 と通信接続を行う。ステップ S 3 0 3 では、自動運転車 1 0 から自動運転車 2 0 にハッシュ値が送信される。

【 0 0 6 0 】

ステップ S 3 3 1 では、自動運転車 2 0 が自端末ハッシュ値を計算している。ステップ S 3 0 3 では、自動運転車 2 0 が自端末ハッシュ値を、自動運転車 1 0 にとっての他端末ハッシュ値として送信している。他端末ハッシュ値を受信すると、自動運転車 1 0 は自動運転車 2 0 との通信を切断する。

【 0 0 6 1 】

ステップ S 3 3 3 では、自動運転車 2 0 がハッシュ値の比較を行う。ハッシュ値が異なっているという比較結果であれば、管理サーバー 3 0 と通信接続を行う。ステップ S 3 3 4 では、比較 NG 情報、送信アドレス（自動運転車 1 0 のアドレス）、受信アドレス（自動運転車 2 0 のアドレス）を送信する。ステップ S 3 5 1 では、管理サーバー 3 0 が NG 情報を記録する。

【 0 0 6 2 】

ステップ S 3 0 4 では、自動運転車 1 0 がハッシュ値の比較を行う。ハッシュ値が異なっているという比較結果であれば、管理サーバー 3 0 と通信接続を行う。ステップ S 3 0 5 では、比較 NG 情報、送信アドレス（自動運転車 2 0 のアドレス）、受信アドレス（自動運転車 1 0 のアドレス）を送信し、マスターハッシュ値を要求する。ステップ S 3 5 2 では、管理サーバー 3 0 が NG 情報を記録する。

【 0 0 6 3 】

ステップ S 3 0 6 では、自動運転車 1 0 が、マスターハッシュ値と自端末ハッシュ値との比較を行い、正当性を検証する。

【 0 0 6 4 】

以上、具体例を参照しつつ本実施形態について説明した。しかし、本開示はこれらの具体例に限定されるものではない。これら具体例に、当業者が適宜設計変更を加えたものも、本開示の特徴を備えている限り、本開示の範囲に包含される。前述した各具体例が備える各要素およびその配置、条件、形状などは、例示したものに限定されるわけではなく適宜変更することができる。前述した各具体例が備える各要素は、技術的な矛盾が生じない限り、適宜組み合わせを変えることができる。

【 符号の説明 】

【 0 0 6 5 】

10

20

30

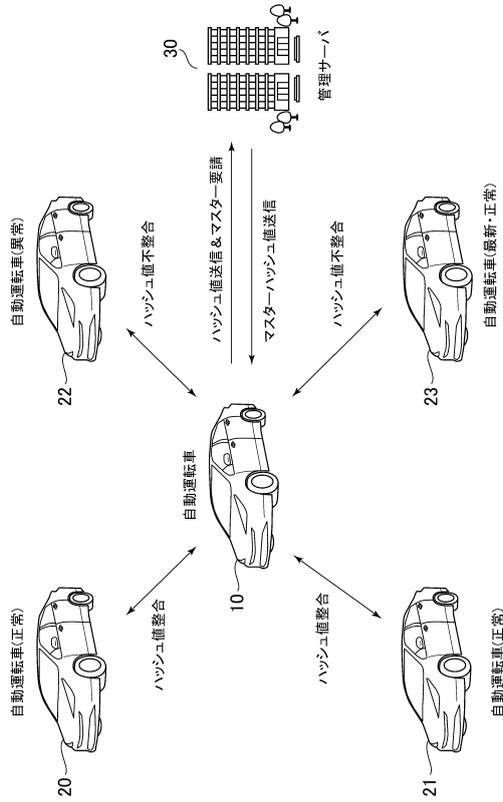
40

50

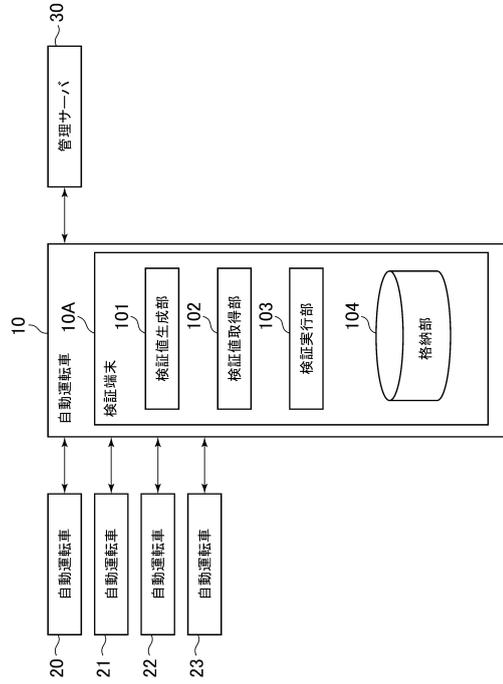
- 10A : 検証端末
- 101 : 検証値生成部
- 102 : 検証値取得部
- 103 : 検証実行部
- 104 : 格納部

【図面】

【図1】



【図2】



10

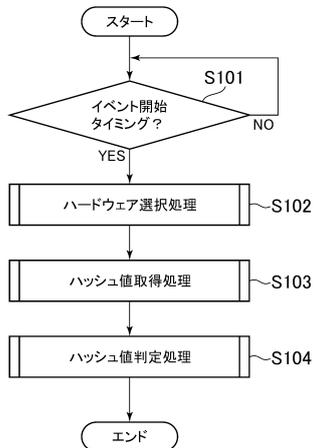
20

30

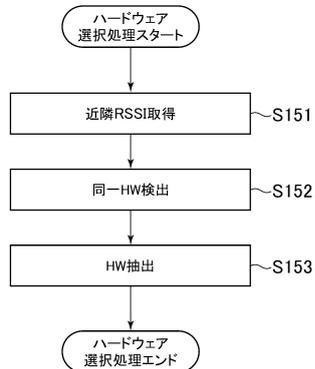
40

50

【 図 3 】



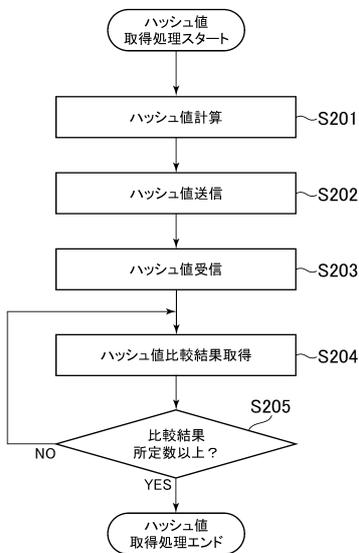
【 図 4 】



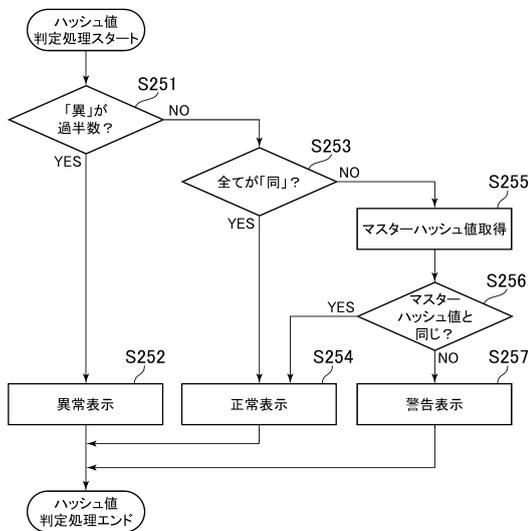
10

20

【 図 5 】



【 図 6 】



30

40

50

【 図 7 】

【 図 8 】

10

制御ソフトウェアに「異常」があります。
可能性: 不正な改竄、古いソフトウェア
対処: 至急ディーラーにお越しください。

制御ソフトウェアに「異常」があります。
可能性: 不正な改竄、古いソフトウェア
対処: 手動運転に切り替えます。
至急ディーラーにお越しください。

20

【 図 9 】

【 図 10 】

30

ソフトウェアに「異常」があります。
可能性: 不正な改竄、不正なコピー
対処: 至急メーカーにお問い合わせください。

制御ソフトウェアは正常です。

40

50

【 図 1 1 】

制御ソフトウェアは最新のバージョンではありません。
お早めにディーラーにお越しください。

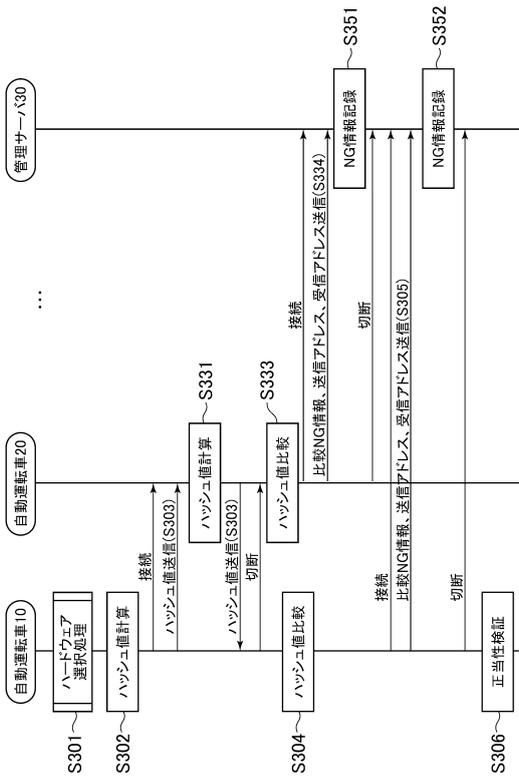
【 図 1 2 】

ソフトウェアは最新のバージョンではありません。
今すぐアップデートを行ってください。

10

20

【 図 1 3 】



30

40

50

フロントページの続き

会社デンソー内

審査官 平井 誠

- (56)参考文献 特開 2 0 1 9 - 0 4 6 2 6 2 (J P , A)
特開 2 0 0 6 - 0 4 8 5 7 5 (J P , A)
特開 2 0 0 4 - 0 0 5 5 8 5 (J P , A)
特開 2 0 1 7 - 2 2 0 2 3 6 (J P , A)
- (58)調査した分野 (Int.Cl. , D B 名)
G 0 6 F 2 1 / 0 0 - 8 8