

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2018年2月15日(15.02.2018)



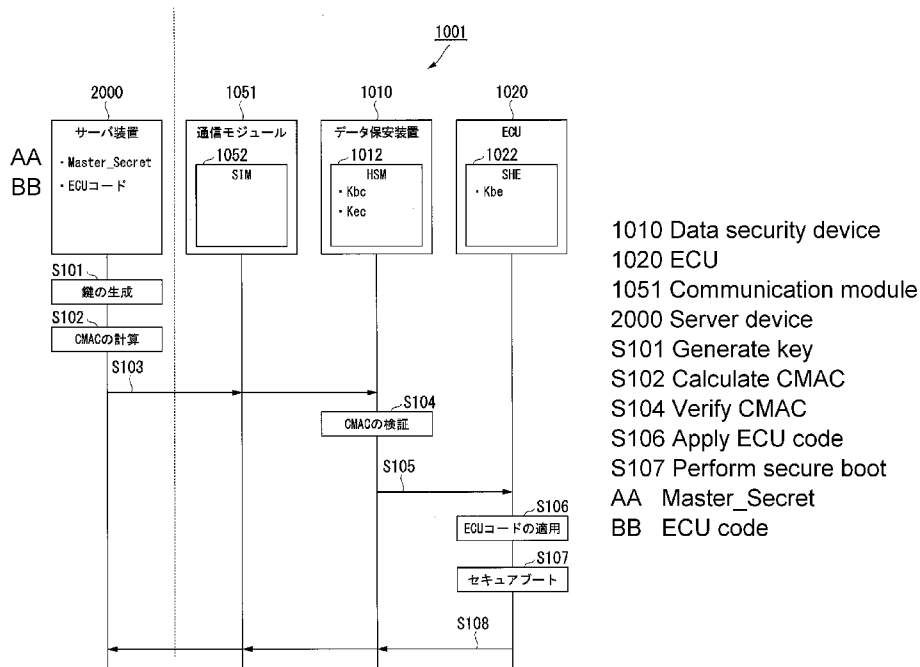
(10) 国際公開番号

WO 2018/029893 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) G06F 21/57 (2013.01)
- (21) 国際出願番号: PCT/JP2017/012720
- (22) 国際出願日: 2017年3月28日(28.03.2017)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2016-158121 2016年8月10日(10.08.2016) JP
- (71) 出願人: K D D I 株 式 会 社 (KDDI CORPORATION) [JP/JP]; 〒1638003 東京都新宿区西新宿二丁目3番2号 Tokyo (JP).
- (72) 発明者: 竹 森 敬 祐 (TAKEMORI Keisuke); 〒3568502 埼玉県ふじみ野市大原2丁目1番15号 株式会社K D D I 総合研究所内 Saitama (JP). 溝 口 誠 一 郎 (MIZOGUCHI Seichiro); 〒3568502 埼玉県ふじみ野市大原2丁目1番15号 株式会社K D D I 総合研究所内 Saitama (JP). 窪 田 歩 (KUBOTA Ayumu); 〒3568502 埼玉県ふじみ野市大原2丁目1番15号 株式会社K D D I 総合研究所内 Saitama (JP).
- (74) 代理人: 棚 井 澄 雄, 外 (TANAI Sumio et al.); 〒1006620 東京都千代田区丸の内一丁目9番2号 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ,

(54) Title: DATA PROVISION SYSTEM, DATA SECURITY DEVICE, DATA PROVISION METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: データ提供システム、データ保安装置、データ提供方法、及びコンピュータプログラム



(57) Abstract: A data provision system that comprises: a data provision device; and a data security device that is installed in a vehicle. The data provision device comprises: a vehicle interface that transmits/receives data to/from the vehicle; and an expected value calculation unit that calculates an expected value for application data that is to be applied by an on-board computer that is installed in the vehicle. The data provision device transmits the application data and the expected value to the vehicle by means of the vehicle interface. The data security device comprises: an interface unit that transmits/receives



BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))

data to/from a device that is external to the data security device; and a measurement unit that calculates a measured value for the application data as received from the data provision device by means of the interface unit and that verifies the measured value on the basis of the expected value as received from the data provision device by means of the interface unit. The data security device transmits application data for which the measured value has been successfully verified to the on-board computer by means of the interface unit.

(57) 要約: データ提供システムは、データ提供装置と、車両に搭載されるデータ保安装置とを備える。前記データ提供装置は、前記車両とデータを送受する車両インタフェースと、前記車両に搭載される車載コンピュータに適用される適用データの期待値を計算する期待値計算部と、を備え、前記適用データ及び前記期待値を前記車両インタフェースにより前記車両に送信する。前記データ保安装置は、前記データ保安装置の外部の装置とデータを送受するインタフェース部と、前記インタフェース部により前記データ提供装置から受信した前記適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した前記期待値に基づいて該測定値を検証する測定部と、を備え、前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車載コンピュータに送信する。

明 細 書

発明の名称：

データ提供システム、データ保安装置、データ提供方法、及びコンピュータプログラム

技術分野

[0001] 本発明は、データ提供システム、データ保安装置、データ提供方法、及びコンピュータプログラムに関する。

本願は、2016年8月10日に、日本に出願された特願2016-158121号に基づき優先権を主張し、その内容をここに援用する。

背景技術

[0002] 従来、自動車は、ECU (Electronic Control Unit：電子制御装置) を有し、ECUによってエンジン制御等の機能を実現する。ECUは、コンピュータの一種であり、コンピュータプログラムによって所望の機能を実現する。複数のECUをCAN (Controller Area Network) に接続して構成される車載制御システムについてのセキュリティ技術が例えば非特許文献1に記載されている。

先行技術文献

非特許文献

[0003] 非特許文献1：竹森敬祐、“セキュアエレメントを基点とした車載制御システムの保護 ―要素技術の整理と考察―”、電子情報通信学会、信学技報、vol. 114、no. 508、pp. 73-78、2015年3月

非特許文献2：STMicroelectronics、“AN4240 Application note”、[平成28年8月3日検索]、インターネット<URL：http://www.st.com/web/en/resource/technical/document/application_note/DM00075575.pdf>

非特許文献3：INTERNATIONAL STANDARD、ISO14229-1、「Road vehicles Unifieddiagnostic services (UDS) Part 1: Specification and requirements」、Second edition、2013-03-15

発明の概要

発明が解決しようとする課題

[0004] 自動車の車載制御システムのＥＣＵに適用される更新プログラム等のデータの信頼性を向上させることが一つの課題であった。

[0005] 本発明は、このような事情を考慮してなされたものであり、ＥＣＵ等の車載コンピュータに適用されるデータの信頼性を向上させることができるデータ提供システム、データ保安装置、データ提供方法、及びコンピュータプログラムを提供することを課題とする。

課題を解決するための手段

[0006] (１) 本発明の一態様は、データ提供装置と、車両に搭載されるデータ保安装置とを備え、前記データ提供装置は、前記車両とデータを送受する車両インタフェースと、前記車両に搭載される車載コンピュータに適用される適用データの期待値を計算する期待値計算部と、を備え、前記適用データ及び前記期待値を前記車両インタフェースにより前記車両に送信し、前記データ保安装置は、前記データ保安装置の外部の装置とデータを送受するインタフェース部と、前記インタフェース部により前記データ提供装置から受信した前記適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した前記期待値に基づいて該測定値を検証する測定部と、を備え、前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車載コンピュータに送信する、データ提供システムである。

(２) 本発明の一態様は、上記(１)のデータ提供システムにおいて、前記データ保安装置は、前記インタフェース部により、前記車載コンピュータに送信した前記適用データの車載コンピュータへの適用の可否を示すデータ適用結果を前記車載コンピュータから受信して前記データ提供装置へ転送する、データ提供システムである。

本発明の一態様においては、前記データ保安装置は、前記測定値の検証が合格した前記適用データと、当該適用データについてのメッセージ認証符号とを前記インタフェース部により前記車載コンピュータに送信してもよい。

本発明の一態様においては、前記メッセージ認証符号は、前記測定値の検証が合格した前記適用データを格納して前記車載コンピュータに伝送するパケットに関するメッセージ認証符号であってもよい。

本発明の一態様においては、前記データ保安装置は、前記測定値の検証が合格した前記適用データを複数のブロックに分割し、該ブロック毎に前記メッセージ認証符号を計算し、該ブロックと該メッセージ認証符号とを前記インタフェース部により前記車載コンピュータに送信してもよい。

[0007] (3) 本発明の一態様は、車両に搭載されるデータ保安装置であり、前記データ保安装置の外部の装置とデータを送受するインタフェース部と、前記インタフェース部によりデータ提供装置から受信した適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した期待値に基づいて該測定値を検証する測定部と、を備え、前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車両に搭載される車載コンピュータに送信する、データ保安装置である。

[0008] (4) 本発明の一態様は、データ提供装置と、車両に搭載されるデータ保安装置とを備えるデータ提供システムのデータ提供方法であって、前記データ提供装置が、前記車両に搭載される車載コンピュータに適用される適用データの期待値を計算し、前記データ提供装置が、前記適用データ及び前記期待値を、前記車両とデータを送受する車両インタフェースにより前記車両に送信し、前記データ保安装置が、前記データ保安装置の外部の装置とデータを送受するインタフェース部により前記データ提供装置から受信した前記適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した前記期待値に基づいて該測定値を検証し、前記データ保安装置が、前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車載コンピュータに送信する、データ提供方法である。

[0009] (5) 本発明の一態様は、車両に搭載されるデータ保安装置のコンピュータに、前記データ保安装置の外部の装置とデータを送受するインタフェース部によりデータ提供装置から受信した適用データの測定値を計算し、前記イン

タフェース部により前記データ提供装置から受信した期待値に基づいて該測定値を検証し、前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車両に搭載される車載コンピュータに送信する、処理を実行させるコンピュータプログラムである。

発明の効果

[0010] 本発明によれば、ＥＣＵ等の車載コンピュータに適用されるデータの信頼性を向上させることができるという効果が得られる。

図面の簡単な説明

[0011] [図1]一実施形態に係るデータ提供システム及び自動車１００１の構成例を示す図である。

[図2]一実施形態に係るサーバ装置２０００の構成例を示す図である。

[図3]一実施形態に係るデータ保安装置１０１０の構成例を示す図である。

[図4]一実施形態に係るＥＣＵ１０２０の構成例を示す図である。

[図5]一実施形態に係るデータ提供方法の例を示すシーケンスチャートである。

[図6]一実施形態に係るデータ提供方法の実施例を示すフローチャートである。

[図7]一実施形態に係るデータ提供方法の実施例を示すフローチャートである。

[図8]一実施形態に係るデータ提供方法の実施例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

[0012] 以下、図面を参照し、本発明の実施形態について説明する。なお、以下に示す実施形態では、車両として自動車を例に挙げて説明する。

[0013] 図１は、一実施形態に係るデータ提供システム及び自動車１００１の構成例を示す図である。本実施形態では、車載コンピュータの一例として、自動車１００１に搭載されるＥＣＵ（電子制御装置）を挙げて説明する。

[0014] 図１において、自動車１００１は、データ保安装置１０１０と複数のＥＣ

U1020とを備える。ECU1020は、自動車1001に備わる車載コンピュータである。ECU1020は、自動車1001のエンジン制御等の制御機能を有する。ECU1020として、例えば、エンジン制御機能を有するECU、ハンドル制御機能を有するECU、ブレーキ制御機能を有するECUなどがある。データ保安装置1010は、自動車1001に搭載されたECU1020に適用されるデータのセキュリティ（保安）の機能を有する。

なお、自動車1001に搭載されたいずれかのECUをデータ保安装置1010として機能させてもよい。

[0015] データ保安装置1010と複数のECU1020とは、自動車1001に備わるCAN（Controller Area Network）1030に接続される。CAN1030は通信ネットワークである。CANは車両に搭載される通信ネットワークの一つとして知られている。データ保安装置1010は、CAN1030を介して、各ECU1020との間でデータを交換する。ECU1020は、CAN1030を介して、他のECU1020との間でデータを交換する。

[0016] なお、車両に搭載される通信ネットワークとして、CAN以外の通信ネットワークを自動車1001に備え、CAN以外の通信ネットワークを介して、データ保安装置1010とECU1020との間のデータの交換、及び、ECU1020同士との間のデータの交換が行われてもよい。例えば、LIN（Local Interconnect Network）が自動車1001に備えられてもよい。また、CANとLINとが自動車1001に備えられてもよい。また、自動車1001において、LINに接続するECU1020が備えられてもよい。また、データ保安装置1010は、CANとLINとに接続されてもよい。また、データ保安装置1010は、CANを介して該CANに接続されるECU1020との間でデータを交換し、また、LINを介して該LINに接続されるECU1020との間でデータを交換してもよい。また、ECU1020同士が、LINを介してデータを交換してもよい。

- [0017] 自動車1001に備わる車載コンピュータシステム1002は、データ保安装置1010と複数のECU1020とがCAN1030に接続されて構成される。本実施形態において、車載コンピュータシステム1002は、自動車1001の車載制御システムとして機能する。
- [0018] ゲートウェイ1070は、車載コンピュータシステム1002の内部と外部の間の通信を監視する。ゲートウェイ1070はCAN1030に接続される。また、ゲートウェイ1070は、車載コンピュータシステム1002の外部の装置の例として、インフォテインメント機器1040、TCU (Tele Communication Unit) 1050及び診断ポート1060と接続される。データ保安装置1010及びECU1020は、ゲートウェイ1070を介して、車載コンピュータシステム1002の外部の装置と通信を行う。
- [0019] なお、CAN1030の構成として、CAN1030が複数のバス（通信線）を備え、該複数のバスがゲートウェイ1070に接続されてもよい。この場合、一つのバスに、一つのECU1020又は複数のECU1020が接続される。また、同じバスにデータ保安装置1010とECU1020とが接続されてもよく、又は、データ保安装置1010が接続されるバスとECU1020が接続されるバスとが別個にされてもよい。
- [0020] 自動車1001は診断ポート1060を備える。診断ポート1060として、例えばOBD (On-board Diagnostics) ポートが使用されてもよい。診断ポート1060には、自動車1001の外部の装置を接続可能である。診断ポート1060に接続可能な自動車1001の外部の装置として、例えば、図1に示されるメンテナンスツール2100などがある。データ保安装置1010と、診断ポート1060に接続された装置、例えばメンテナンスツール2100とは、診断ポート1060及びゲートウェイ1070を介して、データが交換される。メンテナンスツール2100は、OBDポートに接続される従来の診断端末の機能を有していてもよい。
- [0021] 自動車1001はインフォテインメント (Infotainment) 機器1040を備える。インフォテインメント機器1040として、例えば、ナビゲーション機

能、位置情報サービス機能、音楽や動画などのマルチメディア再生機能、音声通信機能、データ通信機能、インターネット接続機能などを有するものが挙げられる。

[0022] 自動車1001は、TCU1050を備える。TCU1050は通信装置である。TCU1050は通信モジュール1051を備える。通信モジュール1051は、無線通信ネットワークを利用して無線通信を行う。通信モジュール1051は、SIM (Subscriber Identity Module) 1052を備える。SIM 1052は、無線通信ネットワークを利用するための情報が書き込まれたSIMである。通信モジュール1051は、SIM 1052を使用することにより該無線通信ネットワークに接続して無線通信を行うことができる。なお、SIM 1052として、eSIM (Embedded Subscriber Identity Module) が使用されてもよい。

[0023] データ保安装置1010は、ゲートウェイ1070を介して、TCU1050とデータを交換する。なお、TCU1050とデータ保安装置1010とを通信ケーブルで直接接続し、TCU1050とデータ保安装置1010は該通信ケーブルを介してデータを交換してもよい。例えば、USB (universal serial bus) ケーブルでTCU1050とデータ保安装置1010とを直接接続し、TCU1050とデータ保安装置1010は該USBケーブルを介してデータを交換してもよい。また、TCU1050とデータ保安装置1010とをUSBケーブル等の通信ケーブルで直接接続し、該通信ケーブルを介してTCU1050とデータ保安装置1010間のデータの交換を行う場合、TCU1050とデータ保安装置1010とのうち送信側の装置は、受信側の装置に送信するデータを一時的に蓄えるバッファを備えてもよい。

[0024] なお、TCU1050の他の接続形態として、例えば、TCU1050をインフォテインメント機器1040に接続し、データ保安装置1010が、ゲートウェイ1070及びインフォテインメント機器1040を介して、TCU1050とデータを交換してもよい。又は、TCU1050を診断ポート1

０６０に接続し、データ保装置１０１０が、ゲートウェイ１０７０及び診断ポート１０６０を介して、該診断ポート１０６０に接続されたＴＣＵ１０５０とデータを交換してもよい。又は、データ保装置１０１０が、ＳＩＭ１０５２を含む通信モジュール１０５１を備えてもよい。データ保装置１０１０がＳＩＭ１０５２を含む通信モジュール１０５１を備える場合には、自動車１００１はＴＣＵ１０５０を備えなくてもよい。

[0025] データ保装置１０１０は、メイン演算器１０１１とＨＳＭ（Hardware Security Module）１０１２とを備える。メイン演算器１０１１は、データ保装置１０１０の機能を実現させるためのコンピュータプログラムを実行する。ＨＳＭ１０１２は暗号処理機能等を有する。ＨＳＭ１０１２は耐タンパー性（Tamper Resistant）を有する。ＨＳＭ１０１２はセキュアエレメント（Secure Element：ＳＥ）の例である。ＨＳＭ１０１２は、データを記憶する記憶部１０１３を備える。メイン演算器１０１１はＨＳＭ１０１２を使用する。

[0026] ＥＣＵ１０２０は、メイン演算器１０２１とＳＨＥ（Secure Hardware Extension）１０２２とを備える。メイン演算器１０２１は、ＥＣＵ１０２０の機能を実現させるためのコンピュータプログラムを実行する。ＳＨＥ１０２２は暗号処理機能等を有する。ＳＨＥ１０２２は耐タンパー性を有する。ＳＨＥ１０２２はセキュアエレメントの例である。ＳＨＥ１０２２は、データを記憶する記憶部１０２３を備える。メイン演算器１０２１はＳＨＥ１０２２を使用する。

[0027] サーバ装置２０００は、通信回線を介して、自動車１００１のＴＣＵ１０５０の通信モジュール１０５１とデータを送受する。サーバ装置２０００は、自動車１００１のＴＣＵ１０５０の通信モジュール１０５１が利用する無線通信ネットワークを介して、該通信モジュール１０５１とデータを送受する。又は、サーバ装置２０００は、インターネット等の通信ネットワークと該無線通信ネットワークとを介して、該通信モジュール１０５１とデータを送受してもよい。また、例えば、サーバ装置２０００と通信モジュール１０

5 1 との間が V P N (Virtual Private Network) 回線等の専用回線で接続され、該専用回線でデータが送受されてもよい。例えば、S I M 1 0 5 2 に対応する無線通信ネットワークによって、V P N 回線等の専用回線が提供されてもよい。なお、サーバ装置 2 0 0 0 と自動車 1 0 0 1 とが通信ケーブルで接続されてもよい。例えば、サーバ装置 2 0 0 0 と自動車 1 0 0 1 のゲートウェイ 1 0 7 0 とが通信ケーブルで接続するように構成されてもよい。

[0028] サーバ装置 2 0 0 0 は、E C U 1 0 2 0 に適用される E C U コード (E C U c o d e) を自動車 1 0 0 1 に提供する。E C U コードは、E C U 1 0 2 0 に適用されるデータの例である。E C U コードは、E C U 1 0 2 0 にインストールされる更新プログラム等のコンピュータプログラムであってもよく、又は、E C U 1 0 2 0 に設定されるパラメータ設定値などの設定データであってもよい。

[0029] 図 2 は、サーバ装置 2 0 0 0 の構成例を示す図である。図 2 において、サーバ装置 2 0 0 0 は、通信部 2 0 1 1 と記憶部 2 0 1 2 と期待値計算部 2 0 1 3 と検証部 2 0 1 4 と鍵生成部 2 0 1 5 と暗号処理部 2 0 1 6 とを備える。通信部 2 0 1 1 は、通信回線を介して、他の装置と通信を行う。通信部 2 0 1 1 は車両インタフェースに対応する。記憶部 2 0 1 2 は、データを記憶する。期待値計算部 2 0 1 3 は、E C U コードについての期待値を計算する。検証部 2 0 1 4 は、E C U 1 0 2 0 の測定値の検証に係る処理を行う。鍵生成部 2 0 1 5 は、鍵を生成する。暗号処理部 2 0 1 6 は、データの暗号化及び暗号化データの復号を行う。

[0030] サーバ装置 2 0 0 0 の機能は、該サーバ装置 2 0 0 0 が備える C P U (Central Processing Unit) がコンピュータプログラムを実行することにより実現される。なお、サーバ装置 2 0 0 0 として、汎用のコンピュータ装置を使用して構成されてもよく、又は、専用のハードウェア装置として構成されてもよい。

[0031] 図 3 は、データ保安装置 1 0 1 0 の構成例を示す図である。図 3 において、データ保安装置 1 0 1 0 は、メイン演算器 1 0 1 1 と H S M 1 0 1 2 とイ

インタフェース部20とを備える。メイン演算器1011は、制御部21と記憶部22とを備える。HSM1012は、記憶部1013と暗号処理部32と測定部33とを備える。

[0032] インタフェース部20は、自データ保安装置1010の外部の装置とデータを送受する。インタフェース部20は、CAN1030を介してデータを送受するインタフェースを備える。メイン演算器1011は、インタフェース部20を介して、データ保安装置1010以外の他の装置とデータの送受を行う。

[0033] 制御部21は、データ保安装置1010の制御を行う。記憶部22は、データを記憶する。記憶部1013は、データを記憶する。暗号処理部32は、データの暗号化及び暗号化データの復号を行う。測定部33は、ECUコード等のデータの測定値を計算し、該測定値を期待値に基づいて検証する。

[0034] 図4は、ECU1020の構成例を示す図である。図4において、ECU1020は、メイン演算器1021とSHE1022とインタフェース部40とを備える。メイン演算器1021は、制御部41と記憶部42とを備える。SHE1022は、記憶部1023と暗号処理部52と測定部53とを備える。

[0035] インタフェース部40は、自ECU1020の外部の装置とデータを送受する。インタフェース部40は、CAN1030を介してデータを送受するインタフェースを備える。メイン演算器1021は、インタフェース部40を介して、自ECU1020以外の他の装置とデータの送受を行う。

[0036] 制御部41は、ECU1020の制御を行う。記憶部42は、データを記憶する。記憶部1023は、データを記憶する。暗号処理部52は、データの暗号化及び暗号化データの復号を行う。測定部53は、ECUコード等のデータの測定値を計算し、該測定値を期待値に基づいて検証する。

[0037] なお、本実施形態では、データ保安装置1010にHSMが使用されているが、データ保安装置1010においてHSMの代わりにSHEが使用されてもよい。なお、SHEについては、例えば非特許文献2に記載されている

。

[0038] 次に図5を参照して、本実施形態に係るデータ提供方法の例を説明する。

図5は、本実施形態に係るデータ提供方法の例を示すシーケンスチャートである。

[0039] サーバ装置2000は、マスタ鍵Master__Secretと、ECU1020のECUコードとを予め記憶部2012に格納している。ECU1020のECUコードは、ECU1020に適用する予定のECUコードを含む。データ保安装置1010は、署名鍵Kbc及び暗号鍵Kecを予めHSM1012の記憶部1013に格納している。ECU1020は、署名鍵Kbeを予めSHE1022の記憶部1023に格納している。

[0040] 以下、サーバ装置2000は、通信部2011により、自動車1001のTCU1050と通信を行い、TCU1050及びゲートウェイ1070を介して、自動車1001のCAN1030に接続されるデータ保安装置1010との間でデータを送受する。なお、サーバ装置2000とデータ保安装置1010との間の通信路として、暗号化通信路が使用されてもよい。例えば、サーバ装置2000とデータ保安装置1010は、暗号化通信路の一例として、https (hypertext transfer protocol secure) 通信を行ってもよい。

[0041] (ステップS101) サーバ装置2000の鍵生成部2015は、自動車1001に搭載されているデータ保安装置1010の署名鍵Kbc及び暗号鍵Kec、並びに、ECU1020の署名鍵Kbeを生成する。

[0042] 鍵生成部2015の鍵生成方法の例を説明する。鍵生成部2015は、記憶部2012に格納されているマスタ鍵Master__Secretと、鍵生成対象装置の識別子UNIT__IDと、変数Nkとを使用して、次式により鍵(共通鍵)を生成する。

共通鍵=ダイジェスト(Master__Secret、UNIT__ID、Nk)

[0043] 但し、鍵生成対象装置がデータ保安装置1010である場合には、UNI

T__IDはデータ保安装置1010の識別子SecU__IDである。鍵生成対象装置がECU1020である場合には、UNIT__IDはECU1020の識別子ECU__IDである。ダイジェスト(Master__Secret、UNIT__ID、Nk)は、マスタ鍵Master__Secretと識別子UNIT__IDと変数Nkとから生成されるダイジェスト値である。ダイジェスト値として、例えば、ハッシュ(hash)関数により算出される値、排他的論理和演算により算出される値、又は、CMAC(Cipher-based Message Authentication Code)などが挙げられる。例えば、共通鍵は、マスタ鍵Master__Secretと識別子UNIT__IDと変数Nkとを入力値に使用して算出されるハッシュ関数値である。

[0044] 変数Nkの値が異なれば、ダイジェスト値は異なる。変数Nkの値を変えることによって、同じマスタ鍵Master__Secretと識別子UNIT__IDとから、異なる共通鍵を生成することができる。例えば、署名鍵用の変数Nkの値をNk__aとし、暗号鍵用の変数Nkの値をNk__bとする。鍵生成部2015は、マスタ鍵Master__Secretと、データ保安装置1010の識別子SecU__IDと、変数Nk__a、Nk__bとを使用して、

署名鍵Kbc=ダイジェスト(Master__Secret、SecU__ID、Nk__a)、

暗号鍵Kec=ダイジェスト(Master__Secret、SecU__ID、Nk__b)、

により、データ保安装置1010の署名鍵Kbcと暗号鍵Kecとを異なる鍵として生成する。また、鍵生成部2015は、マスタ鍵Master__Secretと、ECU1020の識別子ECU__IDと、変数Nk__aとを使用して、

署名鍵Kbe=ダイジェスト(Master__Secret、ECU__ID、Nk__a)、

により、ECU1020の署名鍵Kbeを生成する。記憶部2012は、デ

ータ保安装置1010の署名鍵Kbc及び暗号鍵Kec、並びに、ECU1020の署名鍵Kbeを格納する。データ保安装置1010のHSM1012の記憶部1013は、サーバ装置2000と同じ鍵生成方法によって生成された署名鍵Kbc及び暗号鍵Kecを予め格納している。ECU1020のSHE1022の記憶部1023は、サーバ装置2000と同じ鍵生成方法によって生成された署名鍵Kbeを予め格納している。

[0045] なお、本実施形態に係る鍵（共通鍵）の生成方法の他の例として、署名鍵をハッシュ関数により算出される値とし、暗号鍵を排他的論理和演算により算出される値としてもよい。又は、その逆、つまり、署名鍵を排他的論理和演算により算出される値とし、暗号鍵をハッシュ関数により算出される値としてもよい。

[0046] （ステップS102）サーバ装置2000の期待値計算部2013は、自動車1001に搭載されているECU1020に適用する予定のECUコードのCMACを、データ保安装置1010の署名鍵Kbcにより計算する。この計算結果のCMACは、該ECUコードについての期待値である。なお、本実施形態では、ECUコードの測定値の一例として、CMACを使用する。期待値計算部2013が計算したECUコードの期待値（CMAC）は、該ECUコードの測定値（CMAC）の検証に使用される。記憶部2012は、ECUコードの期待値（CMAC）を格納する。

[0047] （ステップS103）サーバ装置2000は、通信部2011により、ECU1020に適用されるECUコードと、期待値計算部2013が計算した期待値（CMAC）とを、データ保安装置1010に送信する。データ保安装置1010は、サーバ装置2000から送信された、ECUコードと期待値（CMAC）とを受信する。

[0048] （ステップS104）データ保安装置1010の制御部21は、サーバ装置2000から受信した期待値のCMACをHSM1012に渡し、該CMACをHSM1012における測定値の期待値に設定する。制御部21は、サーバ装置2000から受信したECUコードをHSM1012に渡し、HS

M1012にECUコードの測定を実行させる。HSM1012の測定部33は、記憶部1013に格納している署名鍵Kbcにより、ECUコードの測定値を計算する。本実施形態では、測定値の一例としてCMACを使用する。

よって、測定部33は、記憶部1013に格納している署名鍵Kbcにより、ECUコードのCMACを計算する。

[0049] 測定部33は、期待値のCMACと、計算した測定値のCMACとを比較する。この比較の結果、両者が一致する場合には測定値（CMAC）の検証が合格であり、両者が一致しない場合には測定値（CMAC）の検証が不合格である。HSM1012は、測定値の検証結果「合格又は不合格」を制御部21に渡す。制御部21は、ECUコードの測定値の検証結果が合格である場合に、ステップS105に処理を進める。一方、制御部21は、ECUコードの測定値の検証結果が不合格である場合には、図5の処理を終了する。

[0050] なお、ECUコードの測定値の検証結果が不合格である場合には、制御部21は、所定のエラー処理を実行してもよい。例えば、制御部21は、ECUコードの測定値の検証結果が不合格であることを示すエラーメッセージを、サーバ装置2000に送信してもよい。サーバ装置2000は、該エラーメッセージに応じて、所定のエラー処理を実行してもよい。例えば、サーバ装置2000は、ECUコードと期待値（CMAC）とをデータ保安装置1010に再送信したり、又は、期待値（CMAC）を再生成してデータ保安装置1010に送信したりしてもよい。

[0051] （ステップS105）データ保安装置1010の制御部21は、ECUコードの測定値の検証が合格したECUコードを、インタフェース部20によりECU1020に送信する。ECU1020は、データ保安装置1010から送信されたECUコードを受信する。

[0052] （ステップS106）ECU1020の制御部41は、データ保安装置1010から受信したECUコードを自ECU1020に適用する。

[0053] (ステップS107) ECU1020の制御部41は、ECUコードの適用後に、セキュアブートを実行する。このセキュアブートでは、SHE1022の測定部53は、記憶部1023に格納している署名鍵KbeによりECUコードの測定値を計算する。本実施形態では、測定値の一例として、CMACを使用する。よって、測定部53は、記憶部1023に格納している署名鍵Kbeにより、ECUコードのCMACを計算する。測定部53は、該計算結果のCMACと期待値との比較を行う。制御部41は、セキュアブートの実行前に、予め、期待値をSHE1022に設定する。該計算結果のCMACと期待値との比較の結果、両者が一致する場合にはセキュアブート結果が合格であり、両者が一致しない場合にはセキュアブート結果が不合格である。SHE1022は、セキュアブート結果を制御部41に渡す。制御部41は、セキュアブート結果が合格である場合にECUコードの実行を進める。一方、制御部41は、セキュアブート結果が不合格である場合にはECUコードの実行を停止する。

なお、ECU1020のセキュアブートで使用される期待値は、サーバ装置2000又はデータ保安装置1010からECU1020に予め供給される。サーバ装置2000がECU1020にセキュアブートで使用される期待値を供給する場合、サーバ装置2000の期待値計算部2013がECU1020の署名鍵KbeによりECUコードの期待値(CMAC)を計算する。ECU1020の署名鍵Kbeは、予め、ECU1020とサーバ装置2000間で共有される。また、サーバ装置2000は、「ECU1020のセキュアブートで使用される期待値(CMAC)」の期待値(CMAC)を、上記ステップS102と同様にデータ保安装置1010の署名鍵Kbcにより計算する。そして、サーバ装置2000は、この計算結果のCMACと「ECU1020のセキュアブートで使用される期待値(CMAC)」とを上記ステップS103と同様にデータ保安装置1010に送信してもよい。データ保安装置1010は、サーバ装置2000から受信した「ECU1020のセキュアブートで使用される期待値(CMAC)」と該期待値のC

MACについて、上記ステップS104と同様に、自己の署名鍵Kbcにより検証を行う。データ保安装置1010は、上記ステップS105と同様に、該検証が合格した場合に、サーバ装置2000から受信した「ECU1020のセキュアブートで使用される期待値(CMAC)」をECU1020に送信する。「ECU1020のセキュアブートで使用される期待値(CMAC)」は、ECU1020に適用されるデータの例である。

一方、データ保安装置1010がECU1020にセキュアブートで使用される期待値を供給する場合には、データ保安装置1010は、期待値計算部を有し、ECU1020の署名鍵KbeによりECUコードの期待値(CMAC)を計算する。ECU1020の署名鍵Kbeは、予め、ECU1020とデータ保安装置1010間で共有される。

[0054] (ステップS108) ECU1020の制御部41は、インタフェース部40により、セキュアブート結果「合格又は不合格」をデータ保安装置1010に送信する。データ保安装置1010は、ECU1020から受信したセキュアブート結果「合格又は不合格」をサーバ装置2000に転送する。セキュアブート結果「合格又は不合格」は、ECUコードのECU1020への適用の可否を示すデータ適用結果に対応する。

[0055] サーバ装置2000は、通信部2011により、データ保安装置1010から送信されたセキュアブート結果「合格又は不合格」を受信する。サーバ装置2000は、データ保安装置1010から受信したセキュアブート結果「合格又は不合格」に応じて、所定の処理を実行する。例えば、セキュアブート結果が合格である場合には、その旨を記録する。

一方、セキュアブート結果が不合格である場合には、サーバ装置2000は、所定のエラー処理を実行してもよい。例えば、エラー処理として、サーバ装置2000は、ECUコードと期待値(CMAC)とをデータ保安装置1010に再送信したり、又は、期待値(CMAC)を再生成してデータ保安装置1010に送信したりしてもよい。また、該エラー処理を、セキュアブート結果が合格になるまで繰り返す、又は、所定回数だけ繰り返してもよ

い。

[0056] なお、上記したステップS 1 0 7のECUコードの適用後のセキュアブートは、必須ではなく、実行しなくてもよい。

[0057] 次に、上述した図5のデータ提供方法の変形例を説明する。

[0058] <データ提供方法の変形例1>

ステップS 1 0 3において、サーバ装置2 0 0 0は、暗号処理部2 0 1 6によりECUコードを暗号化して、データ保安装置1 0 1 0に送信する。この暗号化に用いる鍵は、データ保安装置1 0 1 0の暗号鍵K e cである。データ保安装置1 0 1 0は、サーバ装置2 0 0 0から受信した暗号化データを、HSM1 0 1 2の暗号処理部3 2により、記憶部1 0 1 3に格納されている暗号鍵K e cで復号して、ECUコードを取得する。

[0059] <データ提供方法の変形例2>

ステップS 1 0 5において、データ保安装置1 0 1 0は、HSM1 0 1 2の暗号処理部3 2によりECUコードを暗号化して、ECU1 0 2 0に送信する。この暗号化に用いる鍵は、予め、データ保安装置1 0 1 0とECU1 0 2 0間で共有される。ECU1 0 2 0は、データ保安装置1 0 1 0から受信した暗号化データを、SHE1 0 2 2の暗号処理部5 2により、記憶部1 0 2 3に格納されている該当の鍵で復号して、ECUコードを取得する。

[0060] <データ提供方法の変形例3>

ステップS 1 0 5において、ECUコードは、CAN1 0 3 0のパケットに格納されて、データ保安装置1 0 1 0からECU1 0 2 0に伝送される。データ保安装置1 0 1 0は、該パケットに、該パケットについてのCMACをさらに含める。該CMACの生成に使用する鍵は、予め、データ保安装置1 0 1 0とECU1 0 2 0間で共有される。ECU1 0 2 0は、データ保安装置1 0 1 0から受信したパケットに含まれるCMACを、該当の鍵で検証する。ECU1 0 2 0は、該CMACの検証が合格した場合に当該ECUコードを適用する。一方、ECU1 0 2 0は、該CMACの検証が不合格である場合には当該ECUコードを適用しない。

[0061] なお、ECUコードを格納するパケットに含めるCMACとして、該ECUコードの全て又は一部についてのCMACが使用されてもよい。例えば、データ保安装置1010は、ECUコードを一定サイズのブロックに分割し、ブロック毎にCMACを計算して、該ブロックと該CMACとをパケットに格納してもよい。ECU1020は、ブロック毎にCMACを検証しながらECUコードを取得する。該CMACの生成に使用する鍵は、予め、データ保安装置1010とECU1020間で共有される。

[0062] <データ提供方法の変形例4>

ステップS108において、ECU1020からサーバ装置2000に送信するセキュアブート結果「合格又は不合格」は所定値とする。例えば、合格は「1」であり、不合格は「0」である。

[0063] <データ提供方法の変形例5>

ステップS108において、ECU1020からサーバ装置2000に送信するセキュアブート結果「合格又は不合格」は、ステップS107のセキュアブートで計算された結果のECUコードのCMACとする。サーバ装置2000の検証部2014は、ステップS103でデータ保安装置1010に送信したECUコードのCMACを、ECU1020の署名鍵K_{be}により計算する。サーバ装置2000の検証部2014は、該計算結果のCMACと、ECU1020のセキュアブート結果のCMACとを比較する。サーバ装置2000の検証部2014は、該比較の結果、両者が一致する場合にはECU1020のセキュアブート結果が合格であると判断し、両者が一致しない場合にはECU1020のセキュアブート結果が不合格であると判断する。

[0064] <データ提供方法の変形例6>

サーバ装置2000は、検証値（例えば、乱数）を予めECU1020に供給する。ステップS108において、ECU1020は、セキュアブート結果が合格である場合にはセキュアブート結果「合格」に検証値を含め、一方、セキュアブート結果が不合格である場合にはセキュアブート結果「不合

格」に検証値を含めない。サーバ装置 2000 の検証部 2014 は、ECU 1020 のセキュアブート結果「合格」に含まれる検証値と、予め ECU 1020 に供給した元の検証値とを比較する。サーバ装置 2000 の検証部 2014 は、該比較の結果、両者が一致する場合には ECU 1020 のセキュアブート結果が合格であると判断し、両者が一致しない場合には ECU 1020 のセキュアブート結果が不合格であると判断する。

[0065] <データ提供方法の変形例 7>

上記のデータ提供方法の変形例 4, 5, 6 のいずれか複数を組合せて適用する。

[0066] <データ提供方法の変形例 8>

上記のデータ提供方法の変形例 4, 5, 6, 7 において、ECU 1020 は、SHE 1022 の暗号処理部 52 によりセキュアブート結果を暗号化して、サーバ装置 2000 に送信する。この暗号化に用いる鍵は、予め、サーバ装置 2000 と ECU 1020 間で共有される。サーバ装置 2000 は、ECU 1020 からの暗号化データを、暗号処理部 2016 により、記憶部 2012 に格納されている該当の鍵で復号して、セキュアブート結果を取得する。なお、該暗号化に用いる鍵として、セキュアブート結果が合格である場合にのみ SHE 1022 で使用可能となる暗号鍵が、使用されてもよい。この場合、セキュアブート結果「合格」が該暗号鍵により暗号化されてもよい。

[0067] 次に、上述した図 5 のデータ提供方法におけるデータ保安装置 1010 と ECU 1020 間の実施例を説明する。図 6 から図 8 は、本実施形態に係るデータ提供方法の実施例を示すフローチャートである。本実施例では、非特許文献 3 に記載される 15 章の「Non-volatile server memory programming process」において、「15.2.1.2 Programming step of phase #1 — Download of application software and data」の手順と、「15.2.1.3 Post-Programming step of phase #1 — Re-synchronization of vehicle network」の手順と、を利用する。図 6 及び図 7 には、非特許文献 3 に記載される「15.2.1.

2 Programming step of phase #1 — Download of application software and data」の図33の「graphically depicts the functionality embedded in the programming step of phase #1.」における適用例が示されている。

図8には、非特許文献3に記載される「15.2.1.3 Post-Programming step of phase #1 — Re-synchronization of vehicle network」の図34の「graphically depicts the functionality embedded in the post-programming step of phase #1.」における適用例が示されている。

[0068] 図6において、符号S1001で示されるステップは、データ保安装置1010のセキュリティ・アクセス (Security Access) の処理に対応する。図7において、符号S1002で示されるステップは、データ保安装置1010のECUコードのブロック毎の復号及び電子署名の検証の処理に対応する。図7において、符号S1003で示されるステップは、ECU1020のECUコードの検証の処理に対応する。図8において、符号S1004で示されるステップは、ECU1020のECUコードの適用後のセキュアブートの処理に対応する。

[0069] 上述した実施形態によれば、データ保安装置1010は、サーバ装置2000から提供されたECUコードの期待値 (CMAC) に基づいて、該ECUコードの測定値 (CMAC) を検証し、この測定値 (CMAC) の検証が合格したECUコードをECU1020に送信する。これにより、ECU1020に適用されるECUコードの信頼性を向上させることができる。また、サーバ装置2000がECU1020にセキュアブートで使用される期待値を供給する場合、データ保安装置1010は、ECUコードと同様に、サーバ装置2000から受信した「ECU1020のセキュアブートで使用される期待値」と該期待値の期待値 (CMAC) について検証を行う。これにより、ECU1020に適用される「セキュアブートで使用される期待値」の信頼性を向上させることができる。

[0070] 上述した実施形態において、サーバ装置2000はデータ提供装置に対応する。

- [0071] なお、メンテナンスツール２１００が、サーバ装置２０００と同様の機能を備えてもよい。メンテナンスツール２１００は、サーバ装置２０００と同様のデータ提供方法により、診断ポート１０６０及びデータ保安装置１０１０を介してＥＣＵ１０２０にＥＣＵコードを提供する。
- [0072] また、自動車１００１のＴＣＵ１０５０又はゲートウェイ１０７０が、データ保安装置１０１０の機能を有してもよい。
- [0073] 以上、本発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施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変更等も含まれる。
- [0074] 上述した実施形態では、データ保安装置１０１０やＥＣＵ１０２０にＨＳＭやＳＨＥが使用されたが、ＨＳＭ及びＳＨＥ以外の暗号処理チップが使用されてもよい。データ保安装置１０１０に対して、例えば「ＴＰＭ（Trusted Platform Module）*f*」と呼ばれる暗号処理チップが使用されてもよい。ＴＰＭ*f*は耐タンパー性を有する。ＴＰＭ*f*はセキュアエレメントの例である。ＥＣＵ１０２０に対して、例えば「ＴＰＭ*t*」と呼ばれる暗号処理チップが使用されてもよい。ＴＰＭ*t*は耐タンパー性を有する。ＴＰＭ*t*はセキュアエレメントの例である。
- [0075] 上述した実施形態は、自動車の製造工場において、自動車の製造工程で自動車に搭載されたＥＣＵに適用されてもよい。また、上述した実施形態は、自動車の整備工場や販売店等において、自動車に搭載されているＥＣＵに適用されてもよい。
- [0076] 上述した実施形態では、車両として自動車を例に挙げたが、原動機付自転車や鉄道車両等の自動車以外の他の車両にも適用可能である。
- [0077] また、上述した各装置の機能を実現するためのコンピュータプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行するようにしてもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものであってもよい。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM、フラッシュメモリ等の書き込み可能な不揮発性メモリ、DVD (Digital Versatile Disc) 等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

[0078] さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（例えばDRAM (Dynamic Random Access Memory)）のように、一定時間プログラムを保持しているものも含むものとする。

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。

さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

産業上の利用可能性

[0079] 本発明によれば、ECU等の車載コンピュータに適用されるデータの信頼性を向上させることができるという効果が得られる。

符号の説明

[0080] 22, 42, 2012…記憶部、2013…期待値計算部、2014…検証部、32, 52, 2016…暗号処理部、20, 40…インタフェース部、21, 41…制御部、33, 53…測定部、1001…自動車、1002…車載コンピュータシステム、1010…データ保安装置、1011, 102

1…メイン演算器、1012…HSM、1013, 1023…記憶部、1020…ECU、1022…SHE、1030…CAN、1040…インフォテイメント機器、1050…TCU、1051…通信モジュール、1052…SIM、1060…診断ポート、1070…ゲートウェイ、2000…サーバ装置、2011…通信部、2015…鍵生成部、2100…メンテナンスツール

請求の範囲

- [請求項1] データ提供装置と、車両に搭載されるデータ保安装置とを備え、
前記データ提供装置は、
前記車両とデータを送受する車両インタフェースと、
前記車両に搭載される車載コンピュータに適用される適用データの
期待値を計算する期待値計算部と、を備え、前記適用データ及び前記
期待値を前記車両インタフェースにより前記車両に送信し、
前記データ保安装置は、
前記データ保安装置の外部の装置とデータを送受するインタフェー
ス部と、
前記インタフェース部により前記データ提供装置から受信した前記
適用データの測定値を計算し、前記インタフェース部により前記デー
タ提供装置から受信した前記期待値に基づいて該測定値を検証する測
定部と、を備え、前記測定値の検証が合格した前記適用データを前記
インタフェース部により前記車載コンピュータに送信する、
データ提供システム。
- [請求項2] 前記データ保安装置は、前記インタフェース部により、前記車載コ
ンピュータに送信した前記適用データの前記車載コンピュータへの適
用の可否を示すデータ適用結果を前記車載コンピュータから受信して
前記データ提供装置へ転送する、
請求項1に記載のデータ提供システム。
- [請求項3] 前記データ保安装置は、前記測定値の検証が合格した前記適用デー
タと、当該適用データについてのメッセージ認証符号とを前記インタ
フェース部により前記車載コンピュータに送信する、
請求項1又は2のいずれか1項に記載のデータ提供システム。
- [請求項4] 前記メッセージ認証符号は、前記測定値の検証が合格した前記適用
データを格納して前記車載コンピュータに伝送するパケットに関する
メッセージ認証符号である、

請求項3に記載のデータ提供システム。

[請求項5]

前記データ保安装置は、前記測定値の検証が合格した前記適用データを複数のブロックに分割し、該ブロック毎に前記メッセージ認証符号を計算し、該ブロックと該メッセージ認証符号とを前記インタフェース部により前記車載コンピュータに送信する、

請求項3又は4のいずれか1項に記載のデータ提供システム。

[請求項6]

車両に搭載されるデータ保安装置であり、

前記データ保安装置の外部の装置とデータを送受するインタフェース部と、

前記インタフェース部によりデータ提供装置から受信した適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した期待値に基づいて該測定値を検証する測定部と、を備え、

前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車両に搭載される車載コンピュータに送信する、

データ保安装置。

[請求項7]

データ提供装置と、車両に搭載されるデータ保安装置とを備えるデータ提供システムのデータ提供方法であって、

前記データ提供装置が、前記車両に搭載される車載コンピュータに適用される適用データの期待値を計算し、

前記データ提供装置が、前記適用データ及び前記期待値を、前記車両とデータを送受する車両インタフェースにより前記車両に送信し、

前記データ保安装置が、前記データ保安装置の外部の装置とデータを送受するインタフェース部により前記データ提供装置から受信した前記適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した前記期待値に基づいて該測定値を検証し、

前記データ保安装置が、前記測定値の検証が合格した前記適用デー

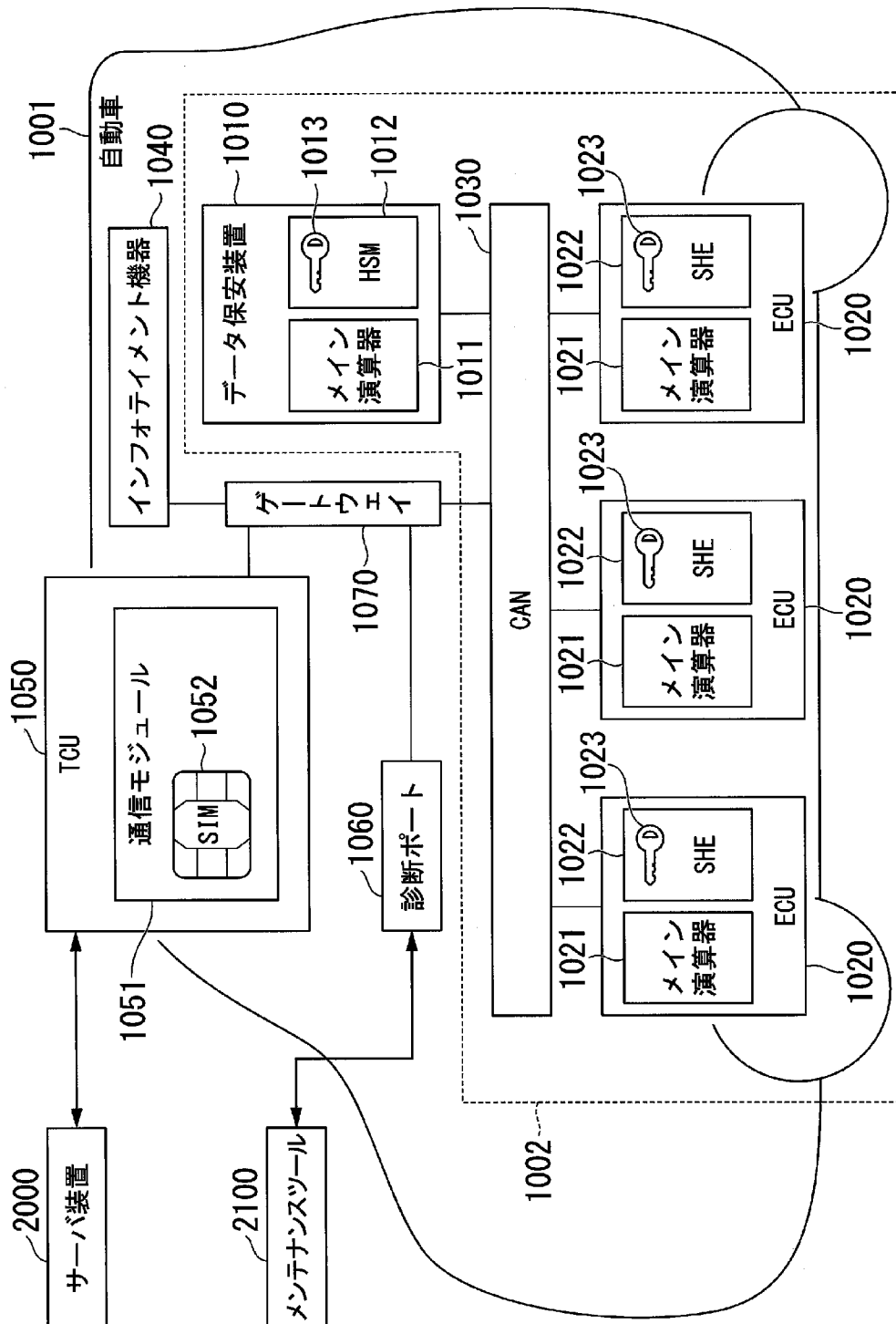
タを前記インタフェース部により前記車載コンピュータに送信する、
データ提供方法。

[請求項8]

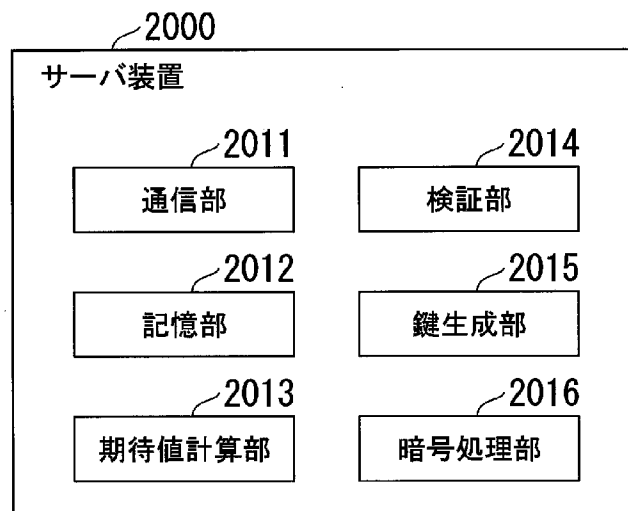
車両に搭載されるデータ保安装置のコンピュータに、
前記データ保安装置の外部の装置とデータを送受するインタフェース部によりデータ提供装置から受信した適用データの測定値を計算し、前記インタフェース部により前記データ提供装置から受信した期待値に基づいて該測定値を検証し、

前記測定値の検証が合格した前記適用データを前記インタフェース部により前記車両に搭載される車載コンピュータに送信する、
処理を実行させるコンピュータプログラム。

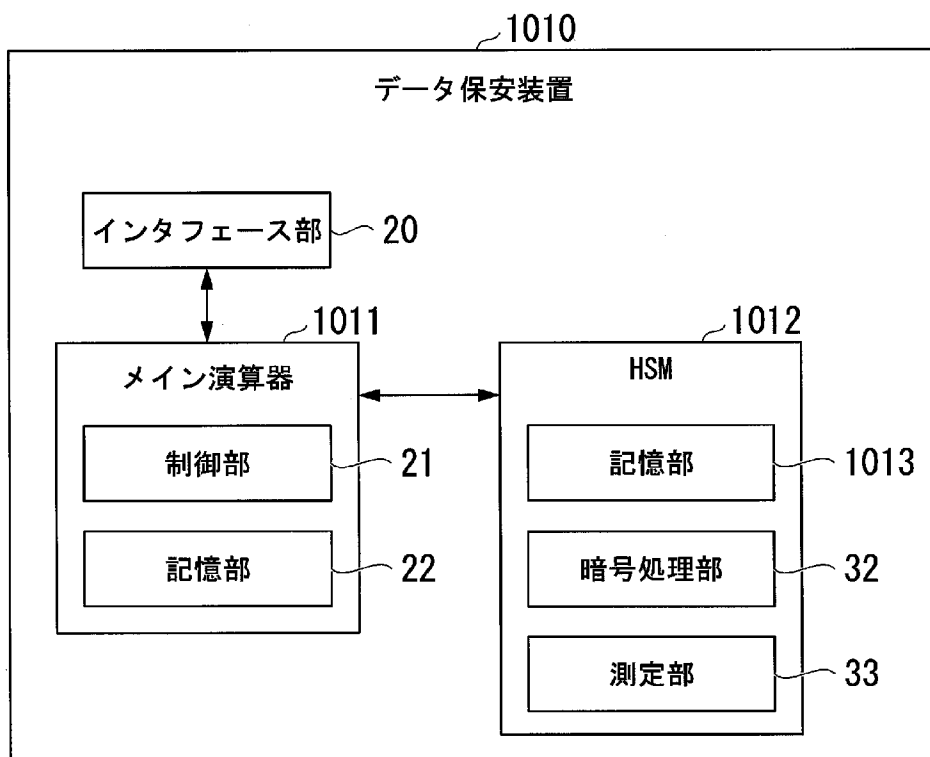
[図1]



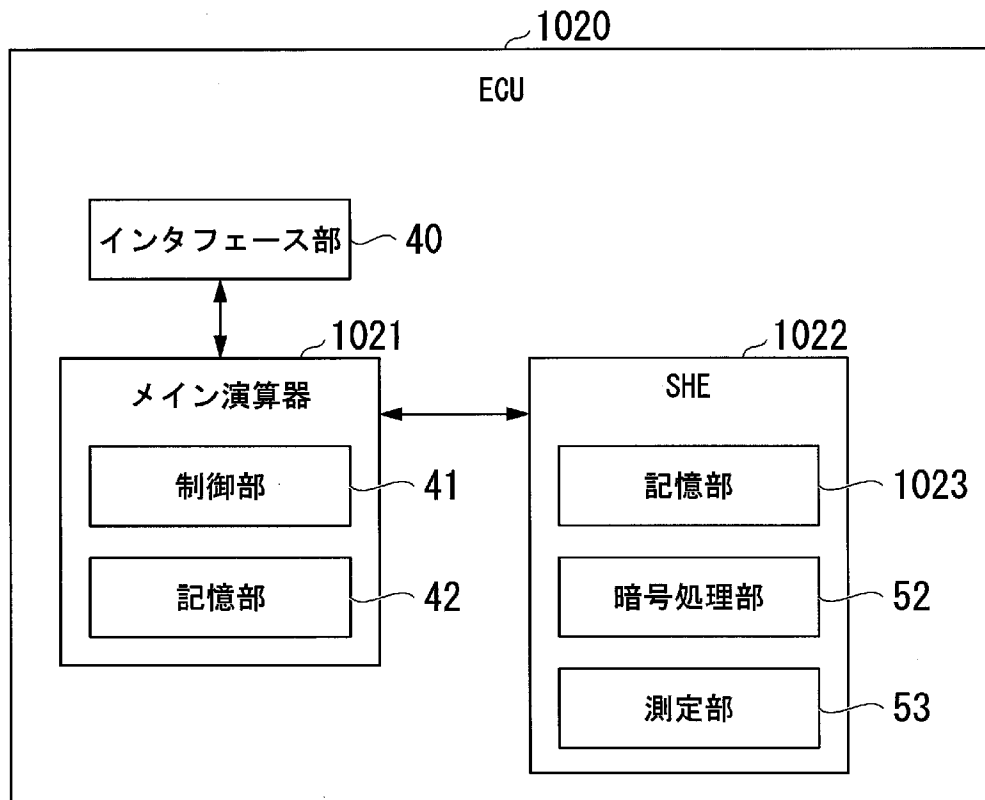
[図2]



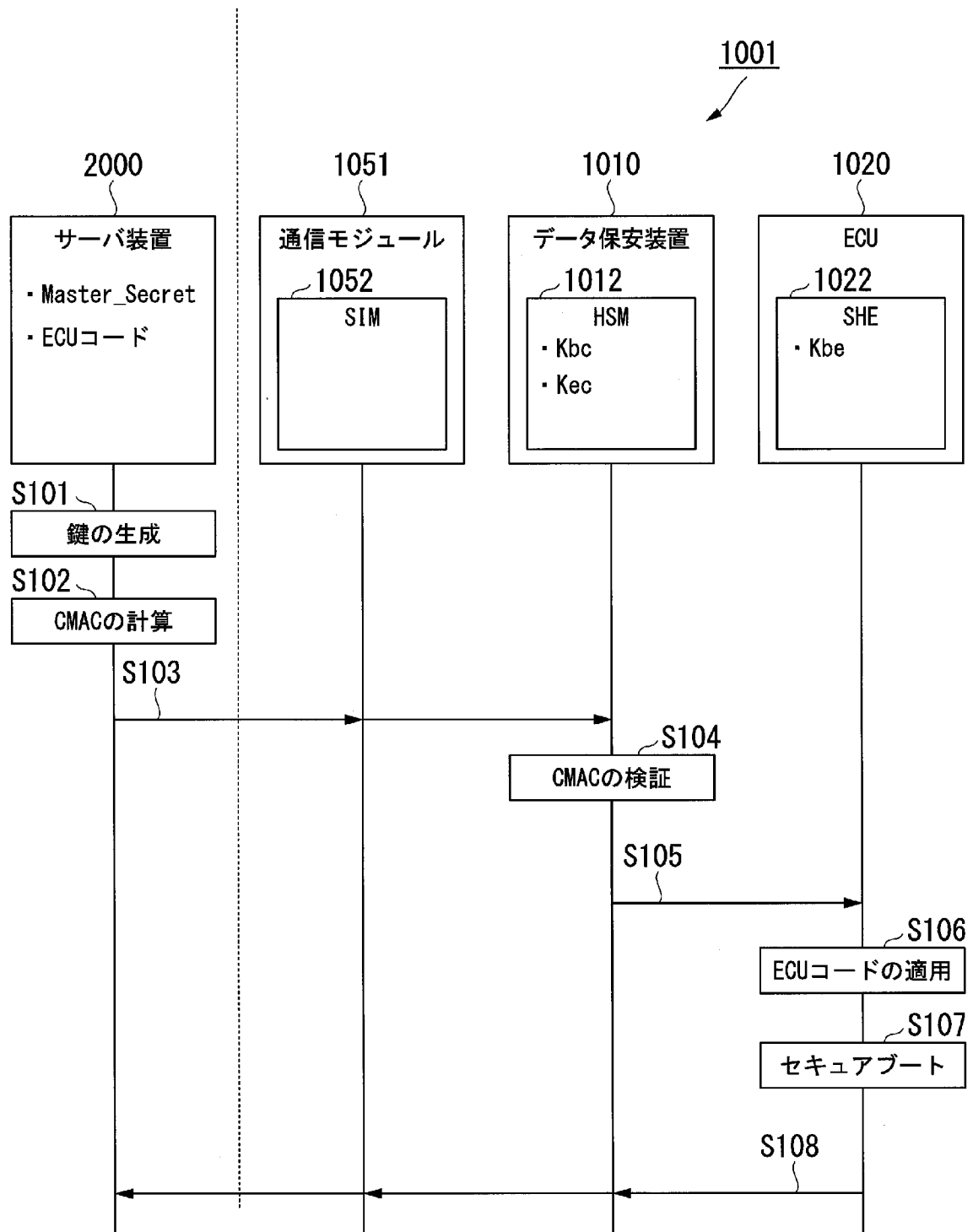
[図3]



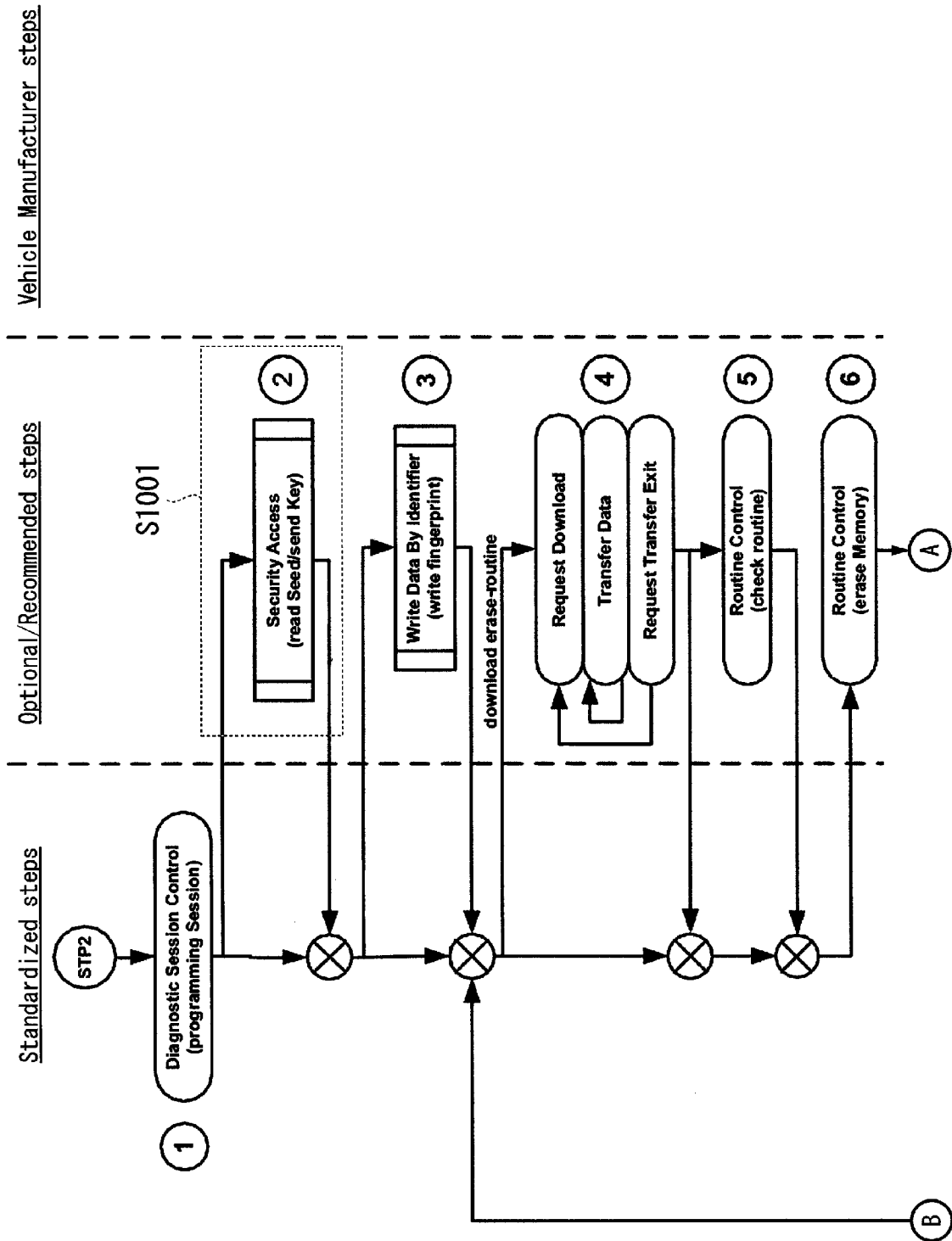
[図4]



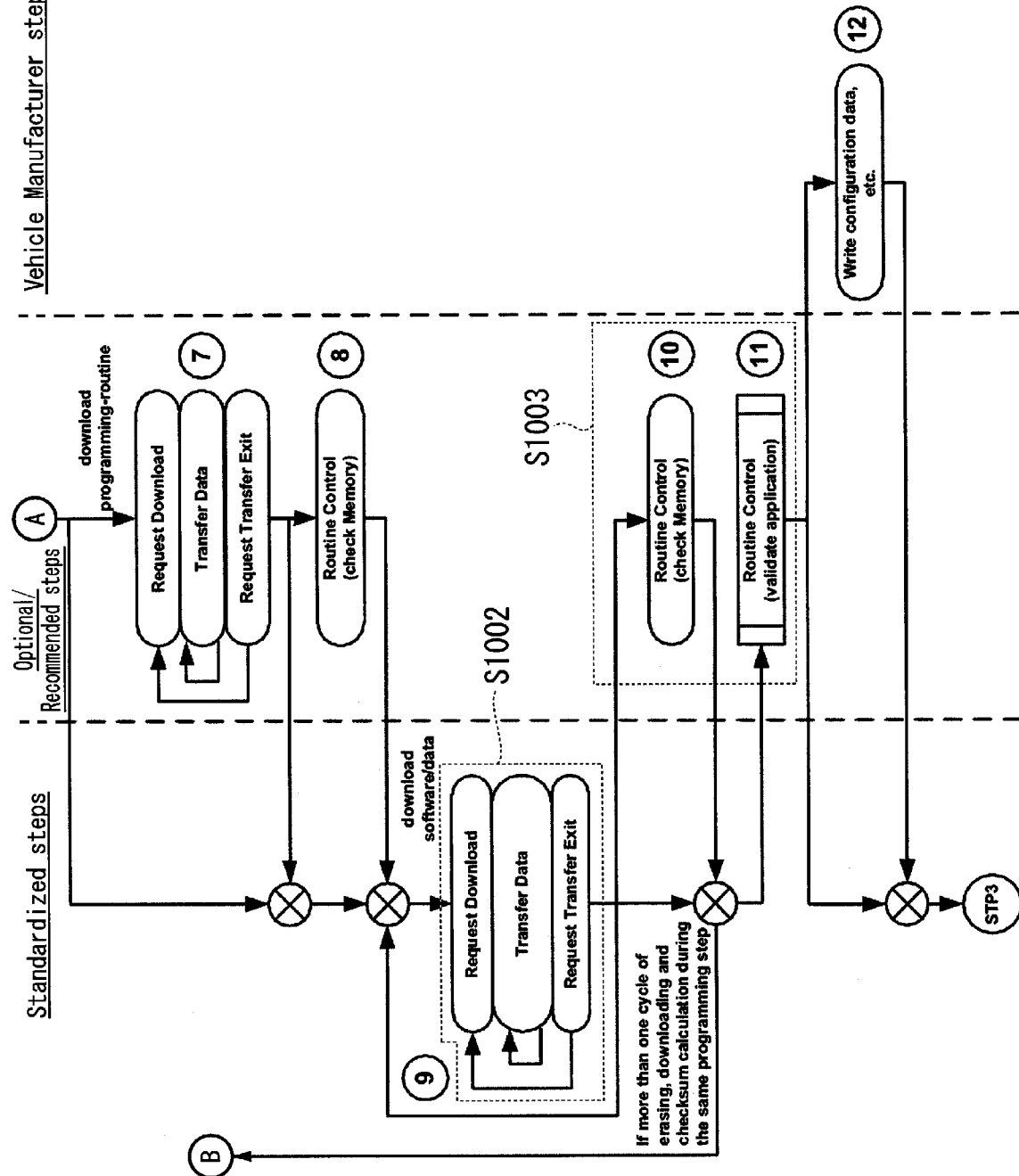
[図5]



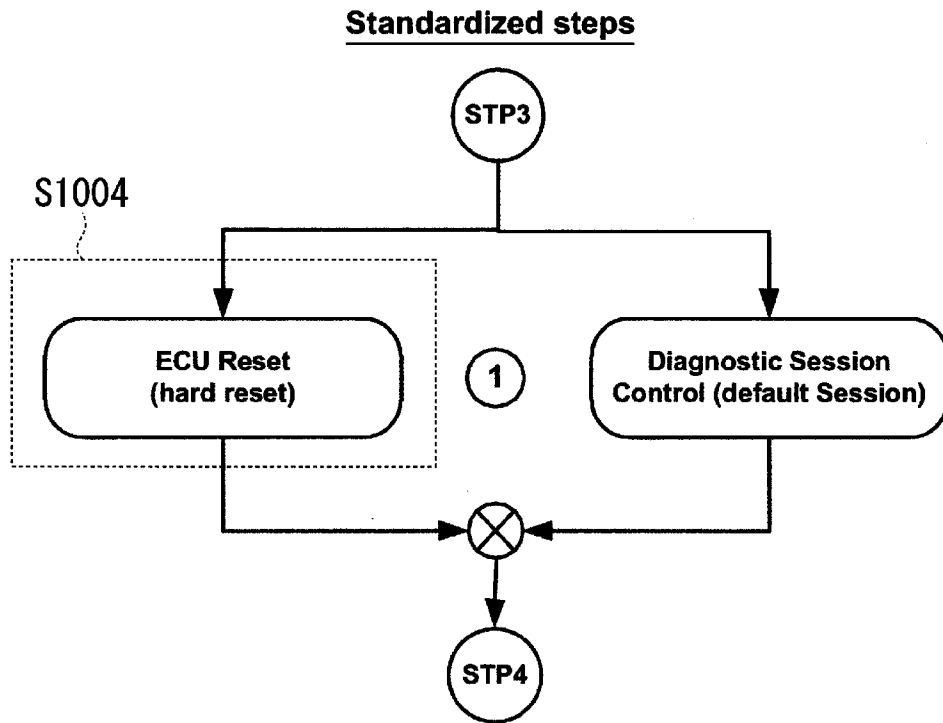
[図6]



Vehicle Manufacturer steps



[図8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/012720

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01)i, G06F21/57(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32, G06F21/57

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2016-72675 A (KDDI Corp.), 09 May 2016 (09.05.2016), paragraphs [0014] to [0019], [0020] to [0023], [0031] to [0033], [0056]; fig. 2 to 3 (Family: none)	1-8
Y	JP 2013-192091 A (Denso Corp.), 26 September 2013 (26.09.2013), paragraphs [0015] to [0016], [0019], [0023] to [0024]; fig. 1 (Family: none)	1-8
Y	Keisuke TAKEMORI et al., "Protection for Automotive Control System Using Secure Boot and Authentication", IEICE Technical Report, 12 September 2014 (12.09.2014), vol.114, no.225, pages 47 to 54	1-8



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
01 June 2017 (01.06.17)

Date of mailing of the international search report
13 June 2017 (13.06.17)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/012720

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Keisuke TAKEMORI et al., "Key Managements for ECU and Code Authentications Using Tamper-resistant Secure Element", IEICE Technical Report, 10 December 2015 (10.12.2015), vol.115, no.366, pages 227 to 232	2-5
Y	US 2012/0093312 A1 (INFINEON TECHNOLOGIES AG), 19 April 2012 (19.04.2012), paragraphs [0044] to [0053]; fig. 6 to 7B & DE 102010042539 A & CN 102457380 A	3-5

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/32(2006.01)i, G06F21/57(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/32, G06F21/57

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017年

国際調査で利用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2016-72675 A (KDD I 株式会社) 2016.05.09, 段落 [0014] - [0019]、[0020] - [0023]、 [0031] - [0033]、[図2] - [図3] (ファミリーなし)	1 - 8
Y	JP 2013-192091 A (株式会社デンソー) 2013.09.26, 段落 [0015] - [0016]、[0019]、 [0023] - [0024]、[図1] (ファミリーなし)	1 - 8

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

01.06.2017

国際調査報告の発送日

13.06.2017

国際調査機関の名称及びあて先

日本国特許庁 (I S A/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

青木 重徳

電話番号 03-3581-1101 内線 3546

5 S

4 2 2 9

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	竹森 敬祐 ほか，セキュアブート+認証による車載制御システムの保護，電子情報通信学会技術研究報告，2014.09.12， V o l . 1 1 4 N o . 2 2 5 , p p . 4 7 - 5 4	1 - 8
Y	竹森 敬祐 ほか，セキュアエレメントを活用した ECU 認証とコード認証の鍵管理，電子情報通信学会技術研究報告，2015.12.10， V o l . 1 1 5 N o . 3 6 6 , p p . 2 2 7 - 2 3 2	2 - 5
Y	US 2012/0093312 A1 (INFINEON TECHNOLOGIES AG) 2012.04.19， 段落 [0044] - [0053]、F I G 6 - 7 B & DE 102010042539 A & CN 102457380 A	3 - 5