(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
2024年10月3日(03.10.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/201600 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号： PCT/JP2023/011933

(22) 国際出願日： 2023年3月24日(24.03.2023)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 株式会社ＳＵＢＡＲＵ (**SUBARU CORPORATION**) [JP/JP]; 〒1508554 東京都渋谷区恵比寿一丁目２０番８号 Tokyo (JP).

(72) 発明者: 飯波 久太郎 (**IINAMI, Hisataro**); 〒1508554 東京都渋谷区恵比寿一丁目２０番８号 株式会社ＳＵＢＡＲＵ内 Tokyo (JP).

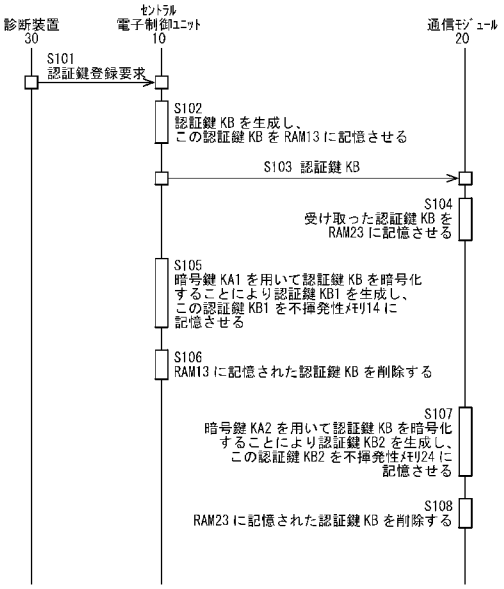
小松 優祐 (**KOMATSU, Yusuke**); 〒1508554 東京都渋谷区恵比寿一丁目２０番８号 株式会社ＳＵＢＡＲＵ内 Tokyo (JP).

(74) 代理人: 弁理士法人つばさ国際特許事務所 (**TSUBASA PATENT PROFESSIONAL CORPORATION**); 〒1600022 東京都新宿区新宿１丁目１５番９号さわだビル３階 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, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,

(54) **Title:** CONTROL SYSTEM AND VEHICLE

(54) 発明の名称： 制御システムおよび車両



10 Central electronic control unit
20 Communication module
30 Diagnostic device
S101 Authentication key registration request
S102 Generate authentication key KB, store authentication key KB in RAM 13
S103 Authentication key KB
S104 Store received authentication key KB in RAM 23
S105 Generate authentication key KB1 by encrypting authentication key KB with cryptographic key KA1, store authentication key KB1 in non-volatile memory 14
S106 Delete authentication key KB stored in RAM 13
S107 Generate authentication key KB2 by encrypting authentication key KB with cryptographic key KA2, store authentication key KB2 in non-volatile memory 24
S108 Delete authentication key KB stored in RAM 23

(57) **Abstract:** A control system according to an embodiment of the present disclosure comprises: a first control device including a first security circuit, in which a first cryptographic key is stored and to which access from the outside is restricted, and a first memory circuit; and a second control device including a second security circuit, in which a second cryptographic key is stored and to which access from the outside is restricted, and a second memory circuit. The first control device is capable of generating an authentication key to be used in an authentication process between the first control

WO 2024/201600 A1

[続葉有]

KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

device and the second control device, is capable of generating a first authentication key by encrypting the authentication key with a first cryptographic key, and is capable of storing the first authentication key in the first memory circuit. The first control device is capable of supplying the generated authentication key to the second control device. The second control device is capable of generating a second authentication key by encrypting the authentication key supplied from the first control device with a second cryptographic key, and is capable of storing the second authentication key in the second memory circuit.

(57) 要約:本開示の一実施の形態に係る制御システムは、第１の暗号鍵が記憶され、外部からのアクセスが制限された第１のセキュリティ回路と、第１の記憶回路とを有する第１の制御装置と、第２の暗号鍵が記憶され、外部からのアクセスが制限された第２のセキュリティ回路と、第２の記憶回路とを有する第２の制御装置とを備える。第１の制御装置は、第１の制御装置および第２の制御装置の間の認証処理に使用される認証鍵を生成可能であり、認証鍵を第１の暗号鍵を用いて暗号化することにより第１の認証鍵を生成可能であり、第１の認証鍵を第１の記憶回路に記憶させることが可能である。第１の制御装置は、生成した認証鍵を第２の制御装置に供給可能である。第２の制御装置は、第１の制御装置から供給された認証鍵を第２の暗号鍵を用いて暗号化することにより第２の認証鍵を生成可能であり、第２の認証鍵を第２の記憶回路に記憶させることが可能である。

明　細　書

発明の名称 ： 制御システムおよび車両

技術分野

[0001]　本開示は、認証鍵を用いて認証処理を行う制御システム、およびそのような制御システムを備えた車両に関する。

背景技術

[0002]　電子機器では、しばしば、鍵を用いてセキュリティを高める技術が用いられる。例えば特許文献１には、車両用マスタ装置における、セキュリティアクセス鍵の管理方法についての技術が開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特開２０２０－０２８１２０号公報

発明の概要

[0004]　本開示の一実施の形態に係る制御システムは、第１の制御装置と、第２の制御装置とを備えている。第１の制御装置は、第１の暗号鍵が記憶され、外部からのアクセスが制限された第１のセキュリティ回路と、第１の記憶回路とを有している。第２の制御装置は、第２の暗号鍵が記憶され、外部からのアクセスが制限された第２のセキュリティ回路と、第２の記憶回路とを有している。第１の制御装置は、第１の制御装置および第２の制御装置の間の認証処理に使用される認証鍵を生成可能であり、認証鍵を第１の暗号鍵を用いて暗号化することにより第１の認証鍵を生成可能であり、第１の認証鍵を第１の記憶回路に記憶させることが可能である。第１の制御装置は、生成した認証鍵を前記第２の制御装置に供給可能である。第２の制御装置は、第１の制御装置から供給された認証鍵を第２の暗号鍵を用いて暗号化することにより第２の認証鍵を生成可能であり、第２の認証鍵を第２の記憶回路に記憶させることが可能である。

[0005]　本開示の一実施の形態に係る車両は、上記制御システムを備えている。第

１の制御装置は、車両を制御する電子制御ユニットを含む。

図面の簡単な説明

[0006] 添付図面は、本開示をさらに理解するために設けられており、本明細書に組み込まれるとともに、本明細書の一部を構成するものである。図面は、一実施の形態を示し、明細書とともに、本開示の原理を説明する役割を果たす。

[0007] [図1]図１は、本開示の一実施の形態に係る制御システムの一構成例を表す説明図である。

[図2]図２は、図１に示したセントラル電子制御ユニットおよび通信モジュールの一構成例を表すブロック図である。

[図3]図３は、図１に示した制御システムの一動作例を表す説明図である。

[図4]図４は、図３に示した制御システムの一動作例を表すシーケンス図である。

[図5]図５は、図１に示した制御システムの他の一動作例を表す説明図である。

[図6A]図６Ａは、図５に示した制御システムの一動作例を表すシーケンス図である。

[図6B]図６Ｂは、図５に示した制御システムの一動作例を表す他のシーケンス図である。

発明を実施するための形態

[0008] 制御システムでは、セキュリティを高めつつ、利便性を高めることが望まれており、さらなる利便性の向上が期待されている。

[0009] セキュリティを高めつつ、利便性を高めることができる制御システムおよび車両を提供することが望ましい。

[0010] 以下、本開示のいくつかの例示的な実施の形態を、添付図面を参照して詳細に説明する。なお、以下の説明は、本開示の一具体例を示すものであり、本開示を限定するものと解釈されてはならない。例えば、数値、形状、材料、部品、各部品の位置および各部品の接続方法等を含む各要素は、一例にす

ぎず、本開示を限定するものと解釈されてはならない。また、以下の例示的な実施の形態において、本開示の最上位概念に基づく独立項に記載されていない構成要素は、任意的なものであり、必要に応じて設けられ得る。図面は模式的なものであり、原寸通りの図示を意図してはいない。本明細書および図面の全般において、略同じ機能および略同じ構成を有する構成要素については、同一の参照符号を付し、重複する説明を省略する。また、本開示の一実施の形態に直接関係の無い構成要素は、図面に図示してはいない。

[0011] ＜実施の形態＞

［構成例］

図１は、一実施の形態に係る制御システム（制御システム１）の一構成例を表すものである。この制御システム１は、車両９に設けられる。車両９は、自動車などの車両である。制御システム１は、セントラル電子制御ユニット（ＥＣＵ：Electronic Control Unit）１０と、複数の電子制御ユニット１９と、通信モジュール２０とを有している。

[0012] セントラル電子制御ユニット１０は、複数の電子制御ユニット１９の動作を制御することにより、車両９の動作を制御するように構成される。また、セントラル電子制御ユニット１０は、例えば、通信ケーブルを介して車外の診断装置３０（後述）に接続され、この診断装置３０と通信を行うことができるようになっている。また、このセントラル電子制御ユニット１０は、ＣＡＮ（Controller Area Network）９に接続され、ＣＡＮ９を介して通信モジュール２０と通信を行うようになっている。

[0013] 複数の電子制御ユニット１９は、セントラル電子制御ユニット１０からの指示に基づいて、車両９における各装置の動作を制御するように構成される。複数の電子制御ユニット１９は、例えば、エンジンなどのパワートレインを制御する電子制御ユニット１９、操舵装置や制動装置を制御する電子制御ユニット１９、車内外の照明、ドア、ワイパーなどを制御する電子制御ユニット１９、運転支援システムを制御する電子制御ユニット１９などを含んでいる。

[0014] 通信モジュール２０は、例えば、４Ｇ（4th Generation）や５Ｇ（5th Generation）などの移動通信を行うことにより、基地局と通信を行うように構成される。これにより、通信モジュール２０は、基地局を介して、インターネットに接続されたサーバ４０（後述）と通信を行うことができるようになっている。また、この通信モジュール２０は、ＣＡＮ９に接続され、ＣＡＮ９を介してセントラル電子制御ユニット１０と通信を行うようになっている。

[0015] この制御システム１では、セントラル電子制御ユニット１０および通信モジュール２０の間で認証処理を行うことができる。セントラル電子制御ユニット１０では、例えば、後述する不揮発性メモリ１４に、暗号化された認証鍵ＫＢ１が記憶され、通信モジュール２０では、例えば、後述する不揮発性メモリ２４に、暗号化された認証鍵ＫＢ２が記憶される。セントラル電子制御ユニット１０および通信モジュール２０は、これらの認証鍵ＫＢ１，ＫＢ２を用いて認証処理を行うことができるようになっている。

[0016] 図２は、セントラル電子制御ユニット１０および通信モジュール２０の一構成例を表すものである。

[0017] セントラル電子制御ユニット１０は、通信部１１と、記憶部１２と、セキュリティモジュール１５と、外部通信部１６と、処理部１７とを有している。

[0018] 通信部１１は、ＣＡＮ９を介して、通信モジュール２０と通信を行うように構成される。

[0019] 記憶部１２は、データを記憶するように構成される。記憶部１２は、ＲＡＭ１３と、不揮発性メモリ１４とを有している。ＲＡＭ１３は、例えばＤＲＡＭ（Dynamic Random Access Memory）を用いて構成され、セントラル電子制御ユニット１０の処理内容を一時的に記憶するように構成される。不揮発性メモリ１４は、例えばフラッシュメモリなどを用いて構成され、セントラル電子制御ユニット１０で実行されるソフトウェアや、暗号化された認証鍵ＫＢ１を記憶するように構成される。ＲＡＭ１３および不揮発性メモリ１４のメモリ領域は、セントラル電子制御ユニット１０の外部から、通信部１１

および処理部１７を介してアクセスされることができるようになっている。

[0020] セキュリティモジュール１５は、いわゆるＨＳＭ（Hardware Security Module）であり、データをセキュアなメモリ領域に記憶するように構成される。この例では、セキュリティモジュール１５には、暗号鍵ＫＡ１が記憶される。セキュリティモジュール１５は、セントラル電子制御ユニット１０の外部からのアクセスが制限されるように構成される。これにより、セキュリティモジュール１５は、記憶しているデータを容易に書き換えできないように、そして記憶しているデータが漏洩しないように、データを保護するようになっている。

[0021] 外部通信部１６は、例えば、車両９に不具合がある場合に、通信ケーブルを用いて、診断装置３０（後述）と通信を行うように構成される。

[0022] 処理部１７は、例えば、１または複数のプロセッサを用いて構成され、ソフトウェアを実行することによりセントラル電子制御ユニット１０の動作を制御するように構成される。

[0023] 通信モジュール２０は、通信部２１と、記憶部２２と、セキュリティモジュール２５と、無線通信部２６と、処理部２７とを有している。

[0024] 通信部２１は、ＣＡＮ９を介して、セントラル電子制御ユニット１０と通信を行うように構成される。

[0025] 記憶部２２は、データを記憶するように構成される。記憶部２２は、ＲＡＭ２３と、不揮発性メモリ２４とを有している。ＲＡＭ２３は、例えばＤＲＡＭを用いて構成され、通信モジュール２０の処理内容を一時的に記憶するように構成される。不揮発性メモリ２４は、例えばフラッシュメモリなどを用いて構成され、通信モジュール２０で実行されるソフトウェアや、暗号化された認証鍵ＫＢ２を記憶するように構成される。ＲＡＭ２３および不揮発性メモリ２４のメモリ領域は、通信モジュール２０の外部から、通信部２１および処理部２７を介してアクセスされることができるようになっている。

[0026] セキュリティモジュール２５は、いわゆるＨＳＭであり、データをセキュアなメモリ領域に記憶するように構成される。この例では、セキュリティモ

ジュール２５には、暗号鍵ＫＡ２が記憶される。セキュリティモジュール２５は、通信モジュール２０の外部からのアクセスが制限されるように構成される。これにより、セキュリティモジュール２５は、記憶しているデータを容易に書き換えできないように、そして記憶しているデータが漏洩しないように、データを保護するようになっている。

[0027] 無線通信部２６は、例えば、４Ｇや５Ｇなどの移動通信を行うことにより、基地局と通信を行うように構成される。これにより、無線通信部２６は、基地局を介して、インターネットに接続されたサーバ４０（後述）と通信を行うことができる。無線通信部２６は、例えば、更新用のソフトウェアを、サーバ４０からダウンロードすることができるようになっている。

[0028] 処理部２７は、例えば、１または複数のプロセッサを用いて構成され、ソフトウェアを実行することにより通信モジュール２０の動作を制御するように構成される。

[0029] この制御システム１では、セントラル電子制御ユニット１０は、診断装置３０からの指示に基づいて認証鍵ＫＢを生成する。そして、セントラル電子制御ユニット１０は、この認証鍵ＫＢを通信モジュール２０に送信する。セントラル電子制御ユニット１０は、暗号鍵ＫＡ１を用いてこの認証鍵ＫＢを暗号化することにより認証鍵ＫＢ１を生成し、この認証鍵ＫＢ１を不揮発性メモリ１４に記憶させる。同様に、通信モジュール２０は、暗号鍵ＫＡ２を用いてこの認証鍵ＫＢを暗号化することにより認証鍵ＫＢ２を生成し、この認証鍵ＫＢ２を不揮発性メモリ２４に記憶させる。これ以降、セントラル電子制御ユニット１０および通信モジュール２０は、不揮発性メモリ１４，２４に記憶されたこの認証鍵ＫＢ１，ＫＢ２を用いて認証処理を行うことができるようになっている。

[0030] ここで、セントラル電子制御ユニット１０は、本開示の一実施の形態における「第１の制御装置」の一具体例に対応する。暗号鍵ＫＡ１は、本開示の一実施の形態における「第１の暗号鍵」の一具体例に対応する。セキュリティモジュール１５は、本開示の一実施の形態における「第１のセキュリティ

回路」の一具体例に対応する。記憶部１２は、本開示の一実施の形態における「第１の記憶回路」の一具体例に対応する。通信モジュール２０は、本開示の一実施の形態における「第２の制御装置」の一具体例に対応する。暗号鍵ＫＡ２は、本開示の一実施の形態における「第２の暗号鍵」の一具体例に対応する。セキュリティモジュール２５は、本開示の一実施の形態における「第２のセキュリティ回路」の一具体例に対応する。記憶部２２は、本開示の一実施の形態における「第２の記憶回路」の一具体例に対応する。認証鍵ＫＢは、本開示の一実施の形態における「認証鍵」の一具体例に対応する。認証鍵ＫＢ１は、本開示の一実施の形態における「第１の認証鍵」の一具体例に対応する。認証鍵ＫＢ２は、本開示の一実施の形態における「第２の認証鍵」の一具体例に対応する。

[0031] ［動作および作用］

続いて、本実施の形態の制御システム１の動作および作用について説明する。

[0032] （全体動作概要）

まず、図１，２を参照して、制御システム１の動作を説明する。セントラル電子制御ユニット１０では、通信部１１は、ＣＡＮ９を介して、通信モジュール２０と通信を行う。記憶部１２は、データを記憶する。セキュリティモジュール１５は、データをセキュアなメモリ領域に記憶する。セキュリティモジュール１５は、暗号鍵ＫＡ１を記憶している。外部通信部１６は、例えば、車両９に不具合がある場合に、通信ケーブルを用いて、診断装置３０と通信を行う。処理部１７は、セントラル電子制御ユニット１０の動作を制御する。

[0033] 通信モジュール２０では、通信部２１は、ＣＡＮ９を介して、セントラル電子制御ユニット１０と通信を行う。記憶部２２は、データを記憶する。セキュリティモジュール２５は、データをセキュアなメモリ領域に記憶する。セキュリティモジュール２５は、暗号鍵ＫＡ２を記憶している。無線通信部２６は、移動通信を行うことにより、基地局を介して、インターネットに接

続されたサーバ４０と通信を行う。無線通信部２６は、例えば、更新用のソフトウェアを、サーバ４０からダウンロードすることができる。処理部２７は、通信モジュール２０の動作を制御する。

[0034]（詳細動作）

以下に、制御システム１の動作について、詳細に説明する。

[0035] 制御システム１は、セントラル電子制御ユニット１０および通信モジュール２０の間の認証処理で使用される認証鍵ＫＢ１，ＫＢ２を登録する。以下に、この動作について詳細に説明する。

[0036] 図３は、認証鍵ＫＢ１，ＫＢ２が記憶される場合における車両９の一例を表すものである。例えば、車両９に不具合がある場合には、車両９の所有者は、この車両９をディーラに持ち込む。ディーラの作業員は、この例では、通信ケーブル８を介して、診断装置３０を、車両９のセントラル電子制御ユニット１０に接続し、診断装置３０は、車両９を診断する。この例では、診断装置３０は、セントラル電子制御ユニット１０の故障を検出する。ディーラの作業員は、セントラル電子制御ユニット１０を交換する。この場合には、制御システム１は、診断装置３０からの指示に基づいて、セントラル電子制御ユニット１０および通信モジュール２０の間の認証処理で使用される認証鍵ＫＢ１，ＫＢ２を登録する。

[0037] 図４は、制御システム１における認証鍵ＫＢ１，ＫＢ２の登録処理の一例を表すものである。

[0038] まず、診断装置３０は、車両９のセントラル電子制御ユニット１０に対して認証鍵の登録要求を行う（ステップＳ１０１）。セントラル電子制御ユニット１０の外部通信部１６は、この登録要求を受け取る。

[0039] 次に、セントラル電子制御ユニット１０の処理部１７は、診断装置３０からの認証鍵の登録要求に基づいて、認証鍵ＫＢを生成し、この認証鍵ＫＢをＲＡＭ１３に記憶させる（ステップＳ１０２）。

[0040] 次に、セントラル電子制御ユニット１０の通信部１１は、ステップＳ１０２において生成した認証鍵ＫＢを通信モジュール２０に供給する（ステップ

Ｓ１０３）。通信モジュール２０の通信部２１は、この認証鍵ＫＢを受け取る。

[0041] そして、通信モジュール２０の処理部２７は、受け取った認証鍵ＫＢをＲＡＭ２３に記憶させる（ステップＳ１０４）。

[0042] セントラル電子制御ユニット１０の処理部１７は、セキュリティモジュール１５に記憶された暗号鍵ＫＡ１を用いて、ＲＡＭ１３に記憶された認証鍵ＫＢを暗号化することにより認証鍵ＫＢ１を生成し、この認証鍵ＫＢ１を不揮発性メモリ１４に記憶させる（ステップＳ１０５）。

[0043] そして、セントラル電子制御ユニット１０の処理部１７は、ＲＡＭ１３に記憶された認証鍵ＫＢを削除する（ステップＳ１０６）。

[0044] 同様に、通信モジュール２０の処理部２７は、セキュリティモジュール２５に記憶された暗号鍵ＫＡ２を用いて、ＲＡＭ２３に記憶された認証鍵ＫＢを暗号化することにより認証鍵ＫＢ２を生成し、この認証鍵ＫＢ２を不揮発性メモリ２４に記憶させる（ステップＳ１０７）。

[0045] そして、通信モジュール２０の処理部２７は、ＲＡＭ２３に記憶された認証鍵ＫＢを削除する（ステップＳ１０８）。

[0046] 以上で、この処理は終了する。

[0047] このようにして、セントラル電子制御ユニット１０の不揮発性メモリ１４には、暗号鍵ＫＡ１を用いて暗号化された認証鍵ＫＢ１が記憶され、通信モジュール２０の不揮発性メモリ２４には、暗号鍵ＫＡ２を用いて暗号化された認証鍵ＫＢ２が記憶される。

[0048] 制御システム１では、セントラル電子制御ユニット１０および通信モジュール２０は、これ以降、この認証鍵ＫＢ１，ＫＢ２を用いて認証処理を行うことができる。以下に、この動作について説明する。

[0049] 図５は、認証鍵ＫＢ１，ＫＢ２を用いた認証処理を行う場合における車両９の一例を表すものである。例えば、複数の電子制御ユニット１９のうちのある電子制御ユニット１９において実行されるソフトウェアの更新用のソフトウェアが準備された場合には、車両９の通信モジュール２０は、サーバ４

０から、この更新用のソフトウェアをダウンロードする。そして、車両９のセントラル電子制御ユニット１０および通信モジュール２０は、認証鍵ＫＢ１，ＫＢ２を用いて認証処理を行い、この認証処理が成功した場合には、セントラル電子制御ユニット１０は、この更新用のソフトウェアを用いて、電子制御ユニット１９のソフトウェアを更新する。

[0050] 図６Ａ，６Ｂは、制御システム１における認証鍵ＫＢ１，ＫＢ２を用いた認証処理の一例を表すものである。

[0051] まず、サーバ４０は、車両９の通信モジュール２０に対して、更新用のソフトウェアを送信する（ステップＳ２０１）。通信モジュール２０の無線通信部２６は、この更新用のソフトウェアを受信する。

[0052] 次に、通信モジュール２０の通信部２１は、セントラル電子制御ユニット１０に対して、認証要求を行う（ステップＳ２０２）。セントラル電子制御ユニット１０の通信部１１は、この認証要求を受け取る。

[0053] 通信モジュール２０の処理部２７は、ＲＡＭ２３のアクセス制限を行う（ステップＳ２０３）。これにより、例えば、通信モジュール２０の外部からのＲＡＭ２３のメモリ領域へのアクセスが一時的に制限される。

[0054] 同様に、セントラル電子制御ユニット１０の処理部１７は、ＲＡＭ１３のアクセス制限を行う（ステップＳ２０４）。これにより、例えば、セントラル電子制御ユニット１０の外部からのＲＡＭ１３のメモリ領域へのアクセスが一時的に制限される。

[0055] 次に、セントラル電子制御ユニット１０の処理部１７は、複数桁の乱数を含む乱数データを生成し、生成した乱数データをＲＡＭ１３に記憶させる（ステップＳ２０５）。

[0056] 次に、セントラル電子制御ユニット１０の通信部１１は、この乱数データを通信モジュール２０に対して供給する（ステップＳ２０６）。通信モジュール２０の通信部１１は、この乱数データを受け取る。

[0057] 次に、通信モジュール２０の処理部２７は、ステップＳ２０６において受け取った乱数データをＲＡＭ２３に記憶させる（ステップＳ２０７）。

[0058] 次に、通信モジュール２０の処理部２７は、セキュリティモジュール２５に記憶された暗号鍵ＫＡ２を用いて、不揮発性メモリ２４に記憶された認証鍵ＫＢ２を復号することにより認証鍵ＫＢ２１を生成し、この認証鍵ＫＢ２１をＲＡＭ１３に記憶させる（ステップＳ２０８）。この認証鍵ＫＢ２１は、ステップＳ１０２において生成された認証鍵ＫＢと同じである。

[0059] そして、通信モジュール２０の処理部２７は、この復号された認証鍵ＫＢ２１を用いて、ステップＳ２０７においてＲＡＭ２３に記憶された乱数データを暗号化する（ステップＳ２０９）。

[0060] 同様に、セントラル電子制御ユニット１０の処理部１７は、セキュリティモジュール１５に記憶された暗号鍵ＫＡ１を用いて、不揮発性メモリ１４に記憶された認証鍵ＫＢ１を復号することにより認証鍵ＫＢ１１を生成し、この認証鍵ＫＢ１１をＲＡＭ１３に記憶させる（ステップＳ２１０）。この認証鍵ＫＢ１１は、ステップＳ１０２において生成された認証鍵ＫＢと同じである。

[0061] そして、セントラル電子制御ユニット１０の処理部１７は、この復号された認証鍵ＫＢ１１を用いて、ステップＳ２０５においてＲＡＭ１３に記憶された乱数データを暗号化する（ステップＳ２１１）。

[0062] 次に、通信モジュール２０の通信部１１は、ステップＳ２０９において暗号化された乱数データを、セントラル電子制御ユニット１０に対して供給する（ステップＳ２１２）。セントラル電子制御ユニット１０の通信部１１は、この暗号化された乱数データを受け取る。

[0063] 次に、セントラル電子制御ユニット１０の処理部１７は、ステップＳ２１１において暗号化された乱数データと、ステップＳ２１２において通信モジュール２０から受け取った暗号化された乱数データとを比較することにより、認証処理を行う（ステップＳ２１３）。すなわち、これらの乱数データが同じである場合には、通信モジュール２０において用いられた認証鍵ＫＢ２１と、セントラル電子制御ユニット１０において用いられた認証鍵ＫＢ１１が同じであることを意味するので、処理部１７は、これらの乱数データを比

較することにより、認証処理を行うことができる。

[0064] 認証処理が成功した場合には、セントラル電子制御ユニット１０の通信部１１は、通信モジュール２０に対して、ソフトウェアの更新許可通知を行う（ステップＳ２１４）。通信モジュール２０の通信部１１は、この更新許可通知を受け取る。

[0065] 次に、通信モジュール２０の処理部２７は、ＲＡＭ２３に記憶された認証鍵ＫＢ２１および乱数データを削除する（ステップＳ２１５）。そして、通信モジュール２０の処理部２７は、ステップＳ２０３において行ったＲＡＭ２３のアクセス制限を解除する（ステップＳ２１６）。これにより、例えば、通信モジュール２０の外部からのＲＡＭ２３のメモリ領域へのアクセスは許可される。

[0066] 同様に、セントラル電子制御ユニット１０の処理部１７は、ＲＡＭ１３に記憶された認証鍵ＫＢ１１および乱数データを削除する（ステップＳ２１７）。そして、セントラル電子制御ユニット１０の処理部１７は、ステップＳ２０４において行ったＲＡＭ１３のアクセス制限を解除する（ステップＳ２１８）。これにより、例えば、セントラル電子制御ユニット１０の外部からのＲＡＭ１３のメモリ領域へのアクセスは許可される。

[0067] 次に、通信モジュール２０の通信部２１は、ステップＳ２０１において受信した更新用のソフトウェアを、セントラル電子制御ユニット１０に対して供給する（ステップＳ２１９）。セントラル電子制御ユニット１０の通信部１１は、この更新用のソフトウェアを受け取る。

[0068] そして、セントラル電子制御ユニット１０の処理部１７は、ステップＳ２２０において受け取った更新用のソフトウェアを用いて、更新対象である電子制御ユニット１９のソフトウェアを更新する（ステップＳ２２０）。

[0069] 以上により、この処理は終了する。ここで、認証鍵ＫＢ１１は、本開示の一実施の形態における「第３の認証鍵」の一具体例に対応する。認証鍵ＫＢ２１は、本開示の一実施の形態における「第４の認証鍵」の一具体例に対応する。

[0070] このように、制御システム１では、第１の暗号鍵（暗号鍵ＫＡ１）が記憶され、外部からのアクセスが制限された第１のセキュリティ回路（セキュリティモジュール１５）と、第１の記憶回路（記憶部１２）とを有するセントラル電子制御ユニット１０と、第２の暗号鍵（暗号鍵ＫＡ２）が記憶され、外部からのアクセスが制限された第２のセキュリティ回路（セキュリティモジュール２５）と、第２の記憶回路（記憶部２２）とを有する通信モジュール２０とを備えるようにした。セントラル電子制御ユニット１０は、セントラル電子制御ユニット１０および通信モジュール２０の間の認証処理に使用される認証鍵ＫＢを生成可能であり、認証鍵ＫＢを第１の暗号鍵（暗号鍵ＫＡ１）を用いて暗号化することにより第１の認証鍵（認証鍵ＫＢ１）を生成可能であり、第１の認証鍵（認証鍵ＫＢ１）を第１の記憶回路（記憶部１２）に記憶させることが可能であるようにした。セントラル電子制御ユニット１０は、生成した認証鍵ＫＢを通信モジュール２０に供給可能なようにした。通信モジュール２０は、セントラル電子制御ユニット１０から供給された認証鍵ＫＢを第２の暗号鍵（暗号鍵ＫＡ２）を用いて暗号化することにより第２の認証鍵（認証鍵ＫＢ２）を生成可能であり、第２の認証鍵（認証鍵ＫＢ２）を第２の記憶回路（記憶部２２）に記憶させることが可能なようにした。これにより、セキュリティを高めつつ、利便性を高めることができる。

[0071] すなわち、セキュリティを高めるためには、生成した認証鍵をセキュリティモジュール１５，２５に記憶させる方法もあり得る。この場合、例えば、診断装置３０が、セキュリティモジュール１５に認証鍵を記憶させるためには、セキュリティモジュール１５に記憶された暗号鍵ＫＡ１を使用する必要がある。よって、診断装置３０は、この暗号鍵ＫＡ１を記憶しておく必要がある。すなわち、診断装置３０は、複数の車両９の暗号鍵ＫＡ１をそれぞれ管理する必要があるので、管理コストがかかり、利便性を損なってしまう。

[0072] 一方、本実施の形態にかかる制御システム１では、セキュリティモジュール１５に認証鍵を記憶させるのではなく、セキュリティモジュール１５に記憶された暗号鍵ＫＡ１を用いて認証鍵ＫＢを暗号化することにより認証鍵Ｋ

Ｂ１を生成し、この認証鍵ＫＢ１を記憶部１２に記憶させるようにした。同様に、制御システム１では、セキュリティモジュール２５に記憶された暗号鍵ＫＡ２を用いて認証鍵ＫＢを暗号化することにより認証鍵ＫＢ２を生成し、この認証鍵ＫＢ２を記憶部２２に記憶させるようにした。これにより、診断装置３０は、暗号鍵ＫＡ１，ＫＡ２を記憶する必要がないので、管理コストを抑えることができ、利便性を高めることができる。

[0073] また、制御システム１では、セントラル電子制御ユニット１０は、生成した認証鍵（認証鍵ＫＢ）を第１の記憶回路（記憶部１２）に一旦記憶させることが可能であり、第１の認証鍵（認証鍵ＫＢ１）を第１の記憶回路（記憶部１２）に記憶させた後に、第１の記憶回路（記憶部１２）に記憶された認証鍵（認証鍵ＫＢ）を削除可能であるようにした。通信モジュール２０は、セントラル電子制御ユニット１０から供給された認証鍵（認証鍵ＫＢ）を第２の記憶回路（記憶部２２）に一旦記憶させることが可能であり、第２の認証鍵（認証鍵ＫＢ２）を第２の記憶回路（記憶部２２）に記憶させた後に、第２の記憶回路（記憶部２２）に記憶された認証鍵（認証鍵ＫＢ）を削除可能であるようにした。これにより、制御システム１では、記憶部１２では、暗号化された認証鍵ＫＢ１が記憶されるとともに暗号化されていない認証鍵ＫＢは削除され、記憶部２２では、暗号化された認証鍵ＫＢ２が記憶されるとともに暗号化されていない認証鍵ＫＢは削除されるので、セキュリティを高めることができる。

[0074] また、制御システム１では、セントラル電子制御ユニット１０は、診断装置３０からの指示に基づいて認証鍵ＫＢを生成可能なようにした。すなわち、例えば、セントラル電子制御ユニット１０が故障した場合に、診断装置３０からの指示に基づいて認証鍵ＫＢを生成する。これにより、例えば以前の認証鍵ＫＢをそのまま使用し続けることなく、認証鍵ＫＢを再度生成することができるので、セキュリティを高めることができる。

[0075] また、制御システム１では、セントラル電子制御ユニット１０は、第１の認証鍵（認証鍵ＫＢ１）を第１の暗号鍵（暗号鍵ＫＡ１）を用いて復号する

ことにより第３の認証鍵（認証鍵ＫＢ１１）を生成可能であり、第３の認証鍵（認証鍵ＫＢ１１）に基づいて第１の処理を行うことが可能であるようにした。また、通信モジュール２０は、第２の認証鍵（認証鍵ＫＢ２）を第２の暗号鍵（暗号鍵ＫＡ２）を用いて復号することにより第４の認証鍵（認証鍵ＫＢ２１）を生成可能であり、第４の認証鍵（認証鍵ＫＢ２１）に基づいて第２の処理を行うことが可能であるようにした。そして、セントラル電子制御ユニット１０および通信モジュール２０は、第１の処理および第２の処理を行うことにより、認証処理を行うようにした。これにより、例えば、認証鍵ＫＢ１１および認証鍵ＫＢ２１が互いに同じである場合に、認証処理が成功し、認証処理が成功した場合に所定の処理を行うことができるので、セキュリティを高めることができる。

[0076] ［効果］

以上のように本実施の形態では、第１の暗号鍵が記憶され、外部からのアクセスが制限された第１のセキュリティ回路と、第１の記憶回路とを有するセントラル電子制御ユニットと、第２の暗号鍵が記憶され、外部からのアクセスが制限された第２のセキュリティ回路と、第２の記憶回路とを有する通信モジュールとを備えるようにした。セントラル電子制御ユニットは、セントラル電子制御ユニットおよび通信モジュールの間の認証処理に使用される認証鍵を生成可能であり、認証鍵を第１の暗号鍵を用いて暗号化することにより第１の認証鍵を生成可能であり、第１の認証鍵を第１の記憶回路に記憶させることが可能であるようにした。セントラル電子制御ユニットは、生成した認証鍵を通信モジュールに供給可能なようにした。通信モジュールは、セントラル電子制御ユニットから供給された認証鍵を第２の暗号鍵を用いて暗号化することにより第２の認証鍵を生成可能であり、第２の認証鍵を第２の記憶回路に記憶させることが可能なようにした。これにより、セキュリティを高めつつ、利便性を高めることができる。

[0077] 本実施の形態では、セントラル電子制御ユニットは、生成した認証鍵を第１の記憶回路に一旦記憶させることが可能であり、第１の認証鍵を第１の記

憶回路に記憶させた後に、第１の記憶回路に記憶された認証鍵を削除可能であるようにした。通信モジュールは、セントラル電子制御ユニットから供給された認証鍵を第２の記憶回路に一旦記憶させることが可能であり、第２の認証鍵を第２の記憶回路に記憶させた後に、第２の記憶回路に記憶された認証鍵を削除可能であるようにした。これにより、セキュリティを高めることができる。

[0078] 本実施の形態では、セントラル電子制御ユニットは、診断装置からの指示に基づいて認証鍵を生成可能なようにしたので、セキュリティを高めることができる。

[0079] 本実施の形態では、セントラル電子制御ユニットは、第１の認証鍵を第１の暗号鍵を用いて復号することにより第３の認証鍵を生成可能であり、第３の認証鍵に基づいて第１の処理を行うことが可能であるようにした。通信モジュールは、第２の認証鍵を第２の暗号鍵を用いて復号することにより第４の認証鍵を生成可能であり、第４の認証鍵に基づいて第２の処理を行うことが可能であるようにした。そして、セントラル電子制御ユニットおよび通信モジュールは、第１の処理および第２の処理を行うことにより、認証処理を行うようにした。これにより、セキュリティを高めることができる。

[0080] 以上、本開示の実施の形態について添付図面を参照しつつ一例を説明したが、本開示は上記実施の形態に決して限定されるものではない。当業者であれば、添付の請求の範囲によって定義される範囲から逸脱することなく、各種変形や変更をなし得ることが理解される。本開示は、そのような各種変形や変更が、添付の請求の範囲およびその均等物の範囲に属する限り、それらを包含することを意図するものである。

[0081] 例えば、上記実施の形態では、図６Ａ，６Ｂに示した方法で認証処理を行うようにしたが、これに限定されるものではなく、セントラル電子制御ユニット１０の記憶部２２に記憶された認証鍵ＫＢ１、および通信モジュール２０の記憶部２２に記憶された認証鍵ＫＢ２を用いた認証方法であれば、どのようなものであってもよい。

[0082] 例えば、上記実施の形態では、セントラル電子制御ユニット１０および通信モジュール２０が認証処理を行うようにしたが、これに限定されるものではなく、車両９における他の様々な回路が認証処理を行うようにしてもよい。

[0083] 例えば、上記実施の形態では、本技術を車両９に適用したが、これに限定されるものではなく、車両９以外に適用してもよい。

[0084] 本明細書中に記載された効果はあくまで例示であり、本開示の効果は、本明細書中に記載された効果に限定されない。よって、本開示に関して、他の効果が得られてもよい。

[0085] さらに、本開示は、以下の態様を取り得る。

[0086] （１）

第１の暗号鍵が記憶され、外部からのアクセスが制限された第１のセキュリティ回路と、第１の記憶回路とを有する第１の制御装置と、

第２の暗号鍵が記憶され、外部からのアクセスが制限された第２のセキュリティ回路と、第２の記憶回路とを有する第２の制御装置と

を備え、

前記第１の制御装置は、前記第１の制御装置および前記第２の制御装置の間の認証処理に使用される認証鍵を生成可能であり、前記認証鍵を前記第１の暗号鍵を用いて暗号化することにより第１の認証鍵を生成可能であり、前記第１の認証鍵を前記第１の記憶回路に記憶させることが可能であり、

前記第１の制御装置は、生成した前記認証鍵を前記第２の制御装置に供給可能であり、

前記第２の制御装置は、前記第１の制御装置から供給された前記認証鍵を前記第２の暗号鍵を用いて暗号化することにより第２の認証鍵を生成可能であり、前記第２の認証鍵を前記第２の記憶回路に記憶させることが可能である

制御システム。

（２）

前記第１の制御装置は、生成した前記認証鍵を前記第１の記憶回路に一旦記憶させることが可能であり、前記第１の認証鍵を前記第１の記憶回路に記憶させた後に、前記第１の記憶回路に記憶された前記認証鍵を削除可能であり、

前記第２の制御装置は、前記第１の制御装置から供給された前記認証鍵を前記第２の記憶回路に一旦記憶させることが可能であり、前記第２の認証鍵を前記第２の記憶回路に記憶させた後に、前記第２の記憶回路に記憶された前記認証鍵を削除可能である

前記（１）に記載の制御システム。

（３）

前記第１の制御装置は、外部装置からの指示に基づいて前記認証鍵を生成可能である

前記（１）または（２）に記載の制御システム。

（４）

前記第１の制御装置は、前記第１の認証鍵を前記第１の暗号鍵を用いて復号することにより第３の認証鍵を生成可能であり、前記第３の認証鍵に基づいて第１の処理を行うことが可能であり、

前記第２の制御装置は、前記第２の認証鍵を前記第２の暗号鍵を用いて復号することにより第４の認証鍵を生成可能であり、前記第４の認証鍵に基づいて第２の処理を行うことが可能であり、

前記第１の制御装置および前記第２の制御装置は、前記第１の処理および前記第２の処理を行うことにより、前記認証処理を行う

前記（１）から（３）のいずれかに記載の制御システム。

（５）

請求項１から請求項４のいずれか一項に記載の制御システムを備え、

前記第１の制御装置は、車両を制御する電子制御ユニットを含む

車両。

[0087] 図２に示す処理部１７は、少なくとも１つのプロセッサ（例えば、中央演

算処理装置（ＣＰＵ））、少なくとも１つの特定用途向け集積回路（ＡＳＩＣ）および／または少なくとも１つのフィールドプログラマブルゲートアレイ（ＦＰＧＡ）等の、少なくとも１つの半導体集積回路を含む回路によって実施可能である。少なくとも１つのプロセッサは、少なくとも１つの非一時的かつ有形のコンピュータ可読媒体から指示を読み込むことによって、図２に示す処理部１７における各種機能のうちの全部または一部を実行するように構成可能である。そのような媒体は、ハードディスク等の各種磁気媒体、ＣＤまたはＤＶＤ等の各種光媒体、揮発性メモリまたは不揮発性メモリ等の各種半導体メモリ（すなわち、半導体回路）を含む様々な形態をとり得るが、これらには限定されない。揮発性メモリは、ＤＲＡＭおよびＳＲＡＭを含み得る。不揮発性メモリは、ＲＯＭおよびＮＶＲＡＭを含み得る。ＡＳＩＣは、図２に示す処理部１７における各種機能のうちの全部または一部を実行するように特化された集積回路（ＩＣ）である。ＦＰＧＡは、図２に示す処理部１７における各種機能のうちの全部または一部を実行するように、製造後に構成可能に設計された集積回路である。なお、以上では、処理部１７を例に挙げて説明したが、これに限定されるものではなく、処理部２７についても同様である。

請求の範囲

[請求項1] 第１の暗号鍵が記憶され、外部からのアクセスが制限された第１のセキュリティ回路と、第１の記憶回路とを有する第１の制御装置と、

第２の暗号鍵が記憶され、外部からのアクセスが制限された第２のセキュリティ回路と、第２の記憶回路とを有する第２の制御装置と

を備え、

前記第１の制御装置は、前記第１の制御装置および前記第２の制御装置の間の認証処理に使用される認証鍵を生成可能であり、前記認証鍵を前記第１の暗号鍵を用いて暗号化することにより第１の認証鍵を生成可能であり、前記第１の認証鍵を前記第１の記憶回路に記憶させることが可能であり、

前記第１の制御装置は、生成した前記認証鍵を前記第２の制御装置に供給可能であり、

前記第２の制御装置は、前記第１の制御装置から供給された前記認証鍵を前記第２の暗号鍵を用いて暗号化することにより第２の認証鍵を生成可能であり、前記第２の認証鍵を前記第２の記憶回路に記憶させることが可能である

制御システム。

[請求項2] 前記第１の制御装置は、生成した前記認証鍵を前記第１の記憶回路に一旦記憶させることが可能であり、前記第１の認証鍵を前記第１の記憶回路に記憶させた後に、前記第１の記憶回路に記憶された前記認証鍵を削除可能であり、

前記第２の制御装置は、前記第１の制御装置から供給された前記認証鍵を前記第２の記憶回路に一旦記憶させることが可能であり、前記第２の認証鍵を前記第２の記憶回路に記憶させた後に、前記第２の記憶回路に記憶された前記認証鍵を削除可能である

請求項１に記載の制御システム。

[請求項3] 前記第１の制御装置は、外部装置からの指示に基づいて前記認証鍵

を生成可能である

請求項１に記載の制御システム。

[請求項4] 前記第１の制御装置は、前記第１の認証鍵を前記第１の暗号鍵を用いて復号することにより第３の認証鍵を生成可能であり、前記第３の認証鍵に基づいて第１の処理を行うことが可能であり、

前記第２の制御装置は、前記第２の認証鍵を前記第２の暗号鍵を用いて復号することにより第４の認証鍵を生成可能であり、前記第４の認証鍵に基づいて第２の処理を行うことが可能であり、

前記第１の制御装置および前記第２の制御装置は、前記第１の処理および前記第２の処理を行うことにより、前記認証処理を行う

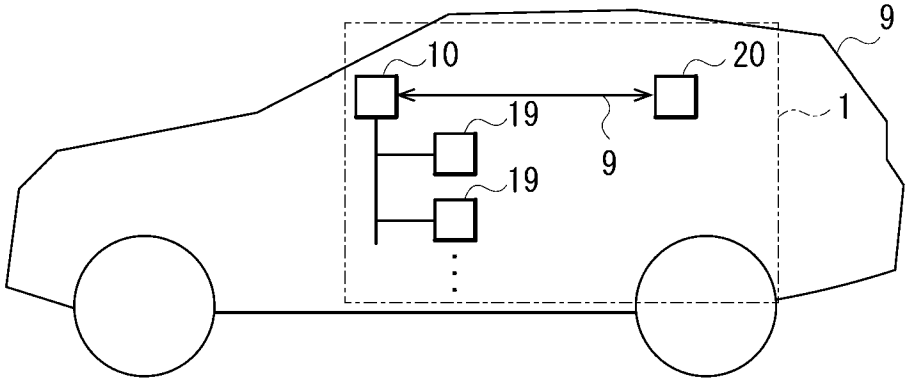
請求項１に記載の制御システム。

[請求項5] 請求項１から請求項４のいずれか一項に記載の制御システムを備え、

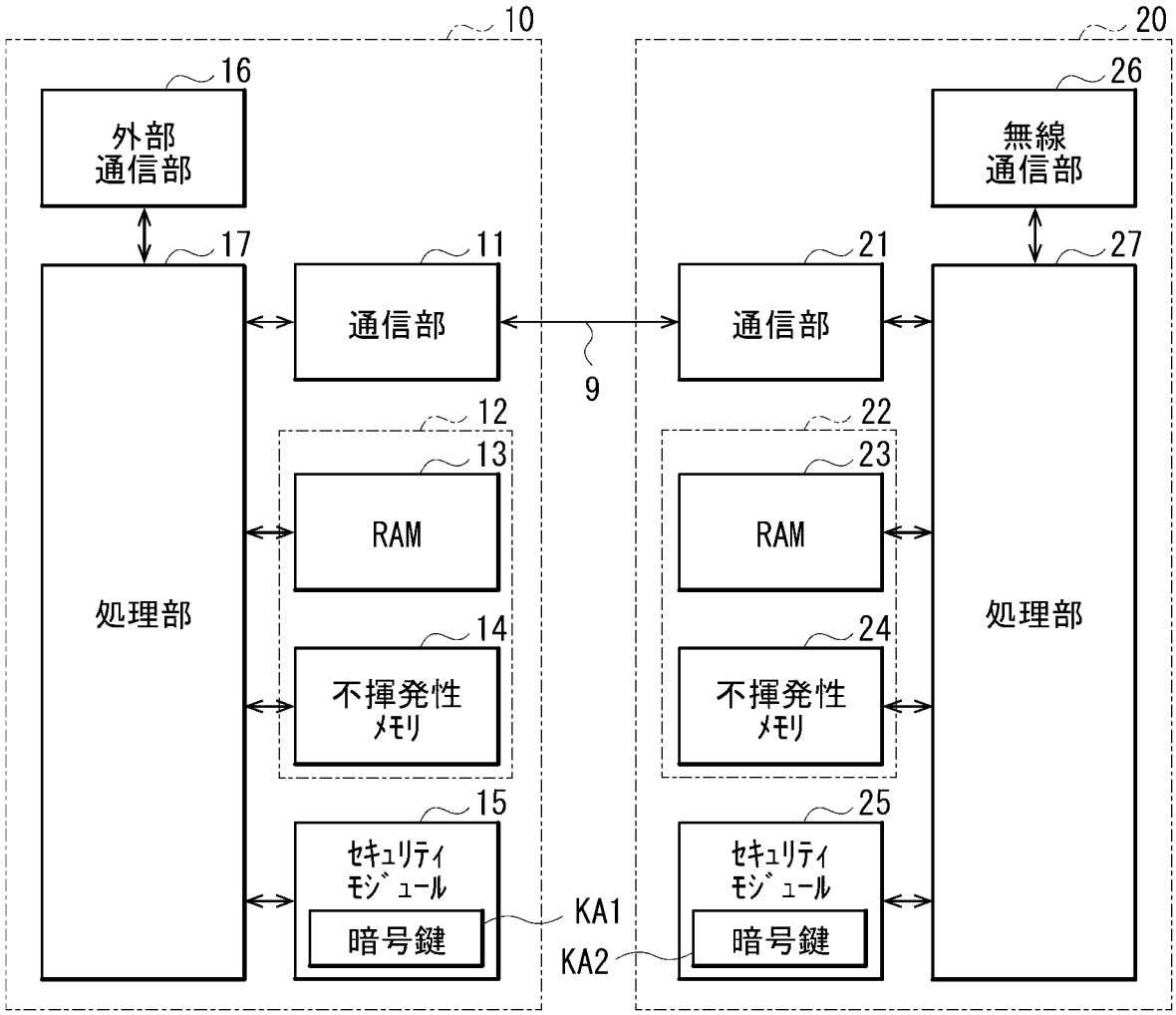
前記第１の制御装置は、車両を制御する電子制御ユニットを含む

車両。

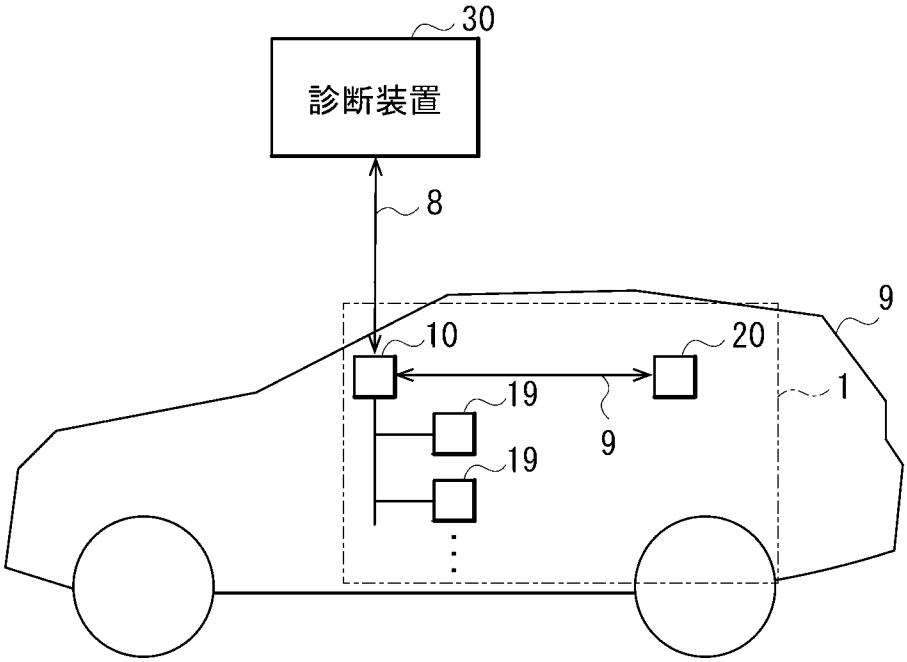
[図1]


9
10
20
19
1
9
19

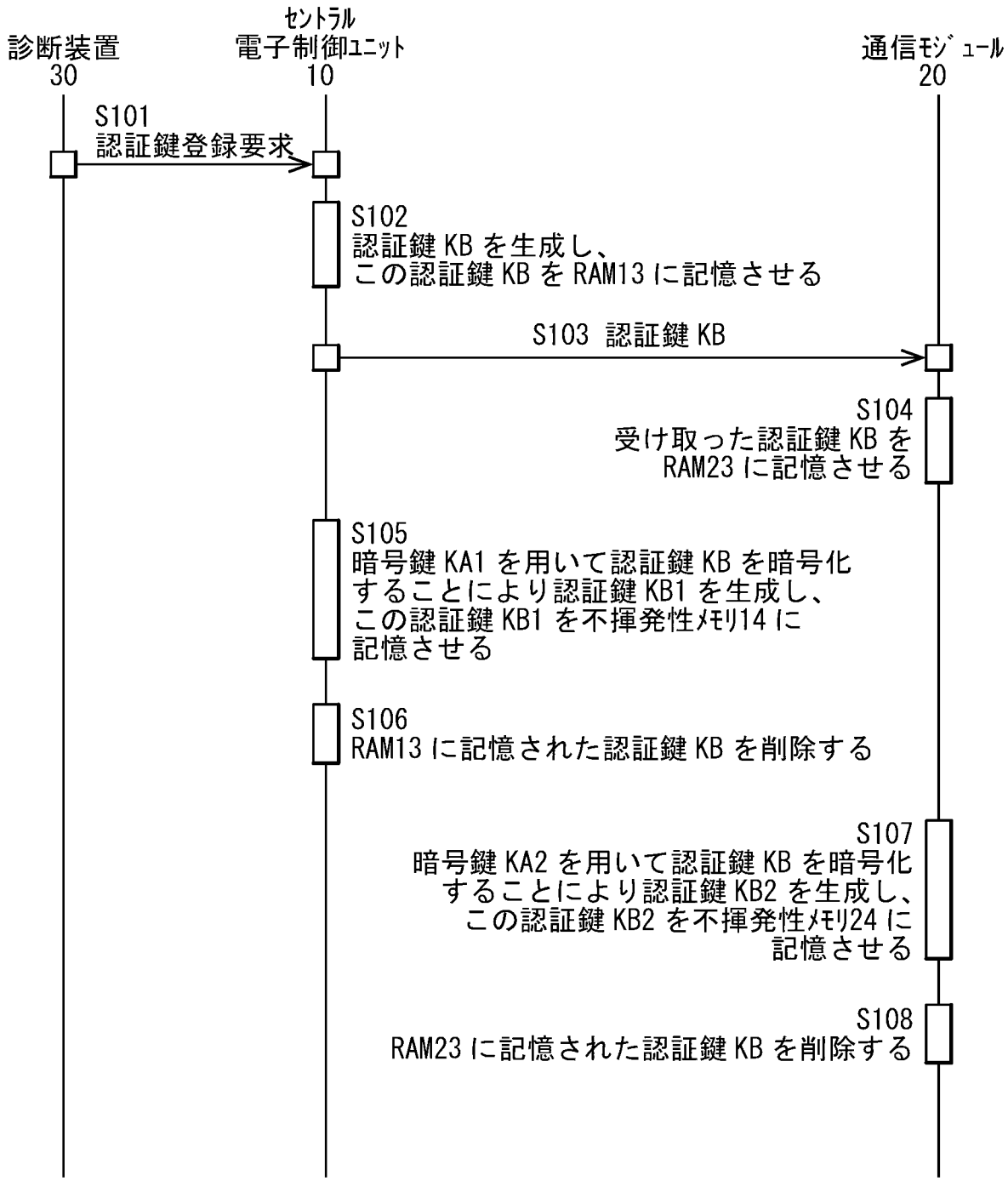
[図2]


10
20
16
外部
通信部
26
無線
通信部
17
11
21
27
通信部
通信部
9
12
22
13
23
RAM
RAM
処理部
処理部
14
24
不揮発性
メモリ
不揮発性
メモリ
15
25
セキュリティ
モジュール
セキュリティ
モジュール
KA1
暗号鍵
KA2
暗号鍵

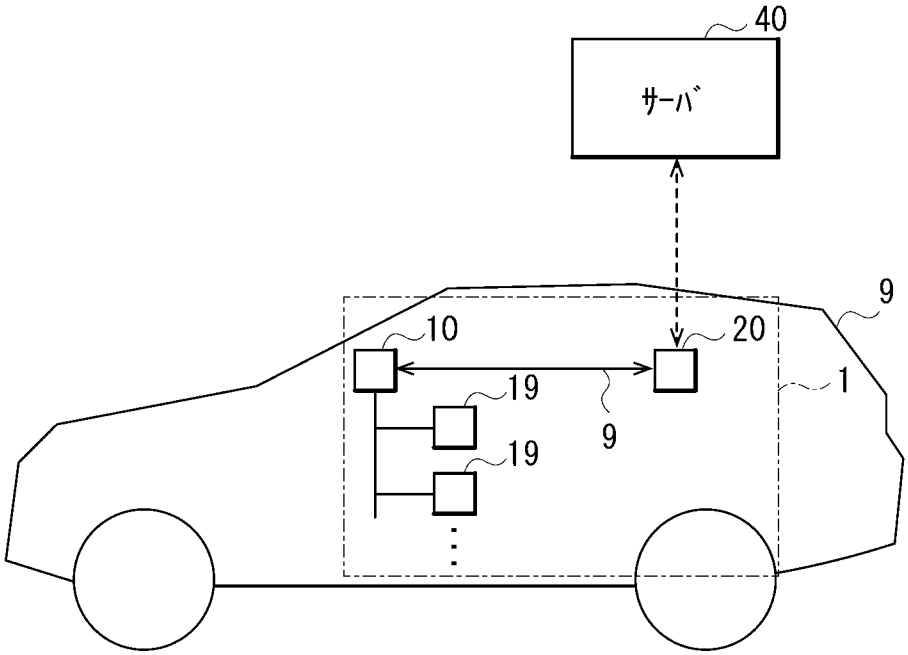
[図3]



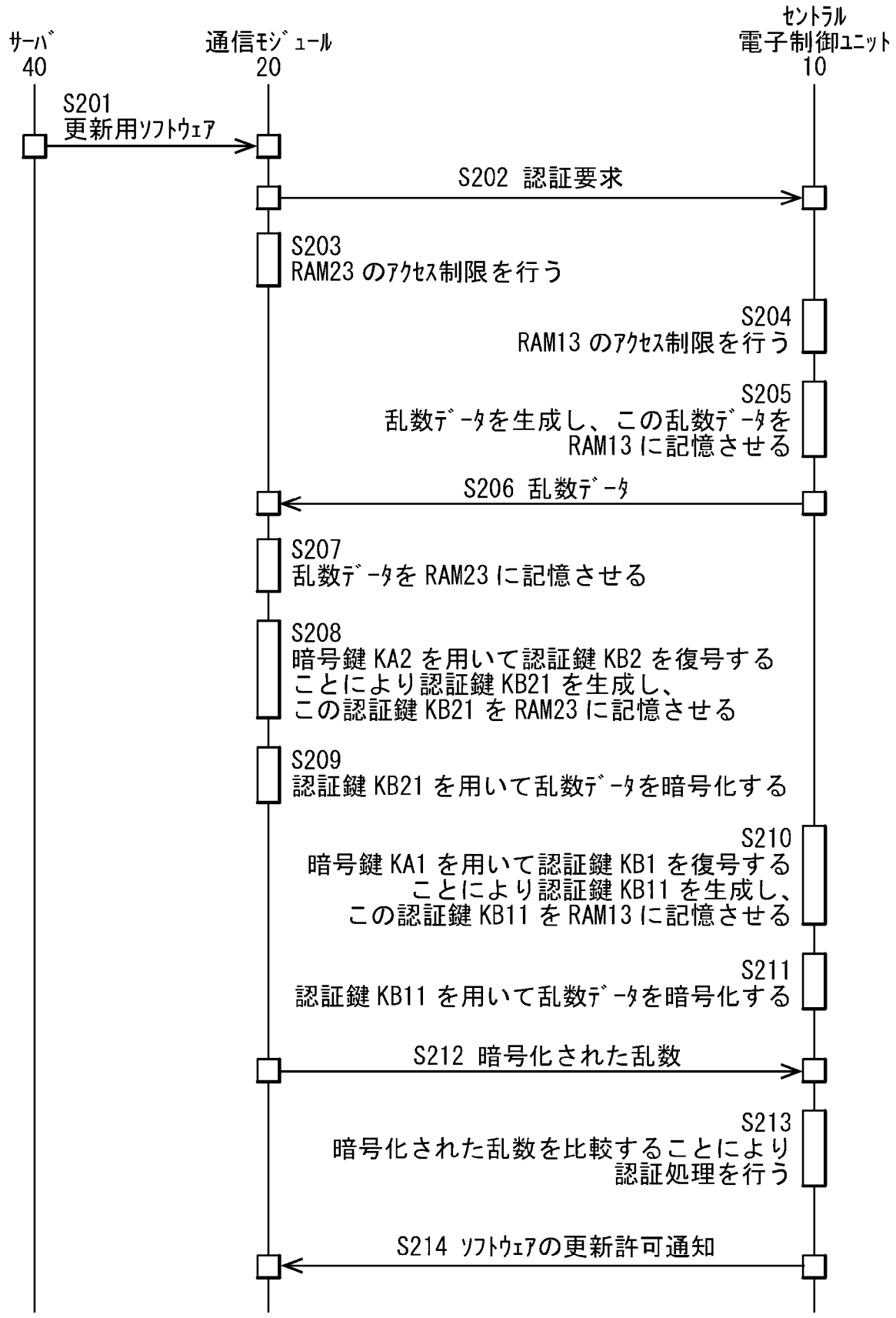
[図4]


診断装置
30
セントラル
電子制御ユニット
10
通信モジュール
20
S101
認証鍵登録要求
S102
認証鍵 KB を生成し、
この認証鍵 KB を RAM13 に記憶させる
S103 認証鍵 KB
S104
受け取った認証鍵 KB を
RAM23 に記憶させる
S105
暗号鍵 KA1 を用いて認証鍵 KB を暗号化
することにより認証鍵 KB1 を生成し、
この認証鍵 KB1 を不揮発性メモリ14 に
記憶させる
S106
RAM13 に記憶された認証鍵 KB を削除する
S107
暗号鍵 KA2 を用いて認証鍵 KB を暗号化
することにより認証鍵 KB2 を生成し、
この認証鍵 KB2 を不揮発性メモリ24 に
記憶させる
S108
RAM23 に記憶された認証鍵 KB を削除する

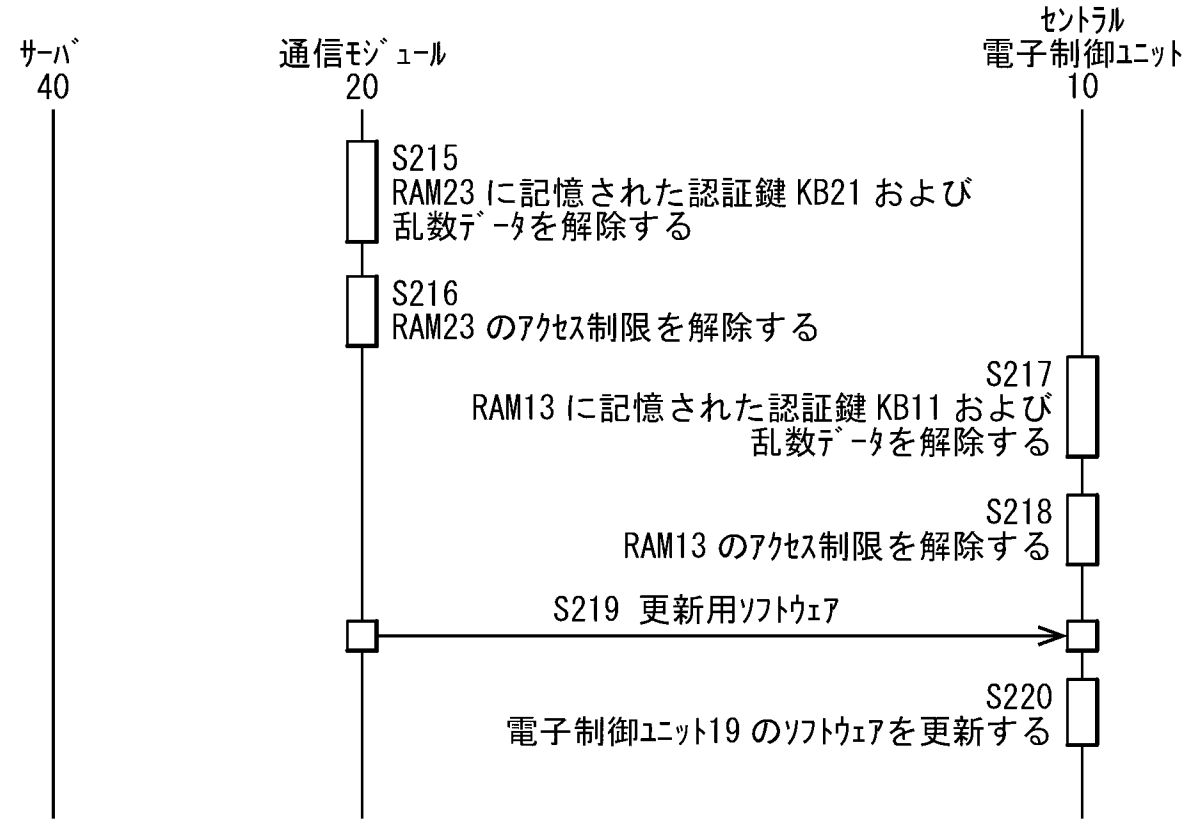
[図5]



[図6A]


サーバ
40
通信モジュール
20
セントラル
電子制御ユニット
10
S201
更新用ソフトウェア
S202 認証要求
S203
RAM23 のアクセス制限を行う
S204
RAM13 のアクセス制限を行う
S205
乱数データを生成し、この乱数データを
RAM13 に記憶させる
S206 乱数データ
S207
乱数データを RAM23 に記憶させる
S208
暗号鍵 KA2 を用いて認証鍵 KB2 を復号する
ことにより認証鍵 KB21 を生成し、
この認証鍵 KB21 を RAM23 に記憶させる
S209
認証鍵 KB21 を用いて乱数データを暗号化する
S210
暗号鍵 KA1 を用いて認証鍵 KB1 を復号する
ことにより認証鍵 KB11 を生成し、
この認証鍵 KB11 を RAM13 に記憶させる
S211
認証鍵 KB11 を用いて乱数データを暗号化する
S212 暗号化された乱数
S213
暗号化された乱数を比較することにより
認証処理を行う
S214 ソフトウェアの更新許可通知

[図6B]


ｻｰﾊﾞ
40
通信ﾓｼﾞｭｰﾙ
20
ｾﾝﾄﾗﾙ
電子制御ﾕﾆｯﾄ
10
S215
RAM23 に記憶された認証鍵 KB21 および
乱数ﾃﾞｰﾀを解除する
S216
RAM23 のｱｸｾｽ制限を解除する
S217
RAM13 に記憶された認証鍵 KB11 および
乱数ﾃﾞｰﾀを解除する
S218
RAM13 のｱｸｾｽ制限を解除する
S219 更新用ｿﾌﾄｳｪｱ
S220
電子制御ﾕﾆｯﾄ19 のｿﾌﾄｳｪｱを更新する

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/011933

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i
FI: H04L9/08 C

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)

H04L9/08

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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 2017-130908 A (KDDI CORP.) 27 July 2017 (2017-07-27) paragraphs [0023]-[0046], [0085]-[0123]	1-5
Y	JP 2018-196080 A (DENSO CORPORATION) 06 December 2018 (2018-12-06) paragraphs [0001]-[0037]	1-5
Y	JP 2021-135817 A (HITACHI ASTEMO, LTD.) 13 September 2021 (2021-09-13) paragraphs [0015]-[0045]	1-5
Y	WO 2016/075865 A1 (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 19 May 2016 (2016-05-19) paragraphs [0030]-[0037], [0102]-[0122]	3, 5
A	菅島健司他. セキュアかつ効率的な車載鍵管理の提案. 2016年暗号と情報セキュリティシンポジウム. 19 January 2016, pp. 1-6, non-official translation (SUGASHIMA, Takeshi et al. Approaches for Secure and Efficient In-Vehicle Key Management. Proceedings of the 2016 Symposium on Cryptography and Information Security.) 4. Proposed Method, 5. Evaluation and Analysis	1-5

☐ 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	Date of mailing of the international search report
05 June 2023	**13 June 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/011933

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2017-130908 A	27 July 2017	US 2019/0028267 A1 paragraphs [0054]-[0088], [0124]-[0164] WO 2017/126322 A1 EP 3407534 A1 CN 108496322 A	
JP 2018-196080 A	06 December 2018	(Family: none)	
JP 2021-135817 A	13 September 2021	(Family: none)	
WO 2016/075865 A1	19 May 2016	US 2017/0134164 A1 paragraphs [0052]-[0058], [0120]-[0139] EP 3219553 A1 CN 106458112 A	

国際調査報告

国際出願番号
PCT/JP2023/011933

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/08(2006.01)i
FI: H04L9/08 C

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（ＩＰＣ））

H04L9/08

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	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３年

国際調査で使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 2017-130908 A (KDDI株式会社) 27.07.2017 (2017-07-27) 段落[0023]-[0046], [0085]-[0123]	1-5
Y	JP 2018-196080 A (株式会社デンソー) 06.12.2018 (2018-12-06) 段落[0001]-[0037]	1-5
Y	JP 2021-135817 A (日立Ａｓｔｅｍｏ株式会社) 13.09.2021 (2021-09-13) 段落[0015]-[0045]	1-5
Y	WO 2016/075865 A1 (パナソニック　インテレクチュアル　プロパティ　コーポレーション　オブ　アメリカ) 19.05.2016 (2016-05-19) 段落[0030]-[0037], [0102]-[0122]	3, 5
A	菅島健司 他, セキュアかつ効率的な車載鍵管理の提案, 2016年暗号と情報セキュリティシンポジウム, 2016.01.19, pp.1-6 4 提案手法, 5 評価と分析	1-5

☐ 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、国際出願日以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抵触するものではなく、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	国際調査報告の発送日
05.06.2023	13.06.2023

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
中里　裕正 5S 9364
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2023/011933

引用文献	公表日	パテントファミリー文献	公表日
JP 2017-130908 A	27.07.2017	US 2019/0028267 A1 段落[0054]-[0088], [0124]-[0164] WO 2017/126322 A1 EP 3407534 A1 CN 108496322 A	
JP 2018-196080 A	06.12.2018	（ファミリーなし）	
JP 2021-135817 A	13.09.2021	（ファミリーなし）	
WO 2016/075865 A1	19.05.2016	US 2017/0134164 A1 段落[0052]-[0058], [0120]-[0139] EP 3219553 A1 CN 106458112 A	