(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
2019年1月17日(17.01.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/012952 A1

(51) 国際特許分類:
G06F 21/12 (2013.01) *G09C 1/00* (2006.01)
G06F 21/64 (2013.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2018/023808

(22) 国際出願日: 2018年6月22日(22.06.2018)

(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 2017-136725 2017年7月13日(13.07.2017) JP

(71) 出願人: 株式会社デンソー (**DENSO CORPORATION**) [JP/JP]; 〒4488661 愛知県刈谷市昭和町１丁目１番地 Aichi (JP). トヨタ自動車株式会社(**TOYOTA JIDOSHA KABUSHIKI KAISHA**) [JP/JP]; 〒4718571 愛知県豊田市トヨタ町１番地 Aichi (JP).

(72) 発明者: 司代 尊裕 (**SHIDAI Takahiro**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP). 佐藤雄介(**SATOH Yusuke**); 〒4718571 愛知県豊田市トヨタ町１番地 トヨタ自動車株式会社内 Aichi (JP).

(74) 代理人: 金 順姫 (**JIN Shunji**); 〒4600003 愛知県名古屋市中区錦２丁目１３番１９号 瀧定ビル６階 Aichi (JP).

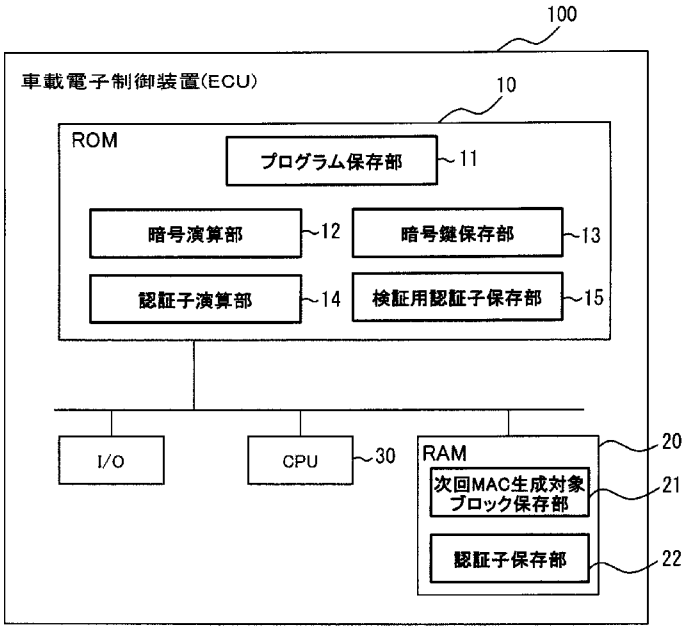
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

WO 2019/012952 A1

(54) **Title:** ELECTRONIC CONTROL DEVICE, PROGRAM TAMPERING DETECTION METHOD, PROGRAM FOR PROGRAM TAMPERING DETECTION METHOD, AND COMPUTER READABLE PERMANENT TANGIBLE RECORDING MEDIUM

(54) 発明の名称: 電子制御装置、プログラム改ざん検知方法、プログラム改ざん検知方法のプログラム、およびコンピュータ読み出し可能持続的有形記録媒体

[図1]



11... PROGRAM STORAGE UNIT
12... ENCRYPTION COMPUTING UNIT
13... ENCRYPTION KEY STORAGE UNIT
14... AUTHENTICATOR COMPUTING UNIT
15... VERIFICATION AUTHENTICATOR STORAGE UNIT
21... NEXT MAC GENERATION TARGET BLOCK STORAGE UNIT
22... AUTHENTICATOR STORAGE UNIT
100... VEHICLE-MOUNTED ELECTRONIC CONTROL DEVICE (ECU)

(57) **Abstract:** This electronic control device comprises: a storage unit (11, 15) which stores a plurality of divided programs obtained by dividing a program, and a verification authenticator; an encryption computing unit (12, 13, 30, 224) which generates partial authenticators for each of the plurality of divided programs by means of an encryption computa-

[続葉有]

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, 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))

tion; and a verification unit (14, 30, 224) which generates a computed authenticator by performing a logical operation using the plurality of partial authenticators, and verifies tampering of the program in accordance with whether or not the verification authenticator and the computed authenticator match.

(57) 要約:電子制御装置は、プログラムを分割した複数の分割プログラム、および検証用認証子を記憶する記憶部(１１、１５)と、暗号演算により前記複数の分割プログラムそれぞれの部分認証子を生成する暗号演算部(１２、１３、３０、２２４)と、複数の前記部分認証子を用いた論理演算を行って演算認証子を生成し、前記検証用認証子と前記演算認証子とが一致するか否かによって前記プログラムの改ざんを検証する検証部(１４、３０、２２４)とを有する。

明　細　書

発明の名称 ：

電子制御装置、プログラム改ざん検知方法、プログラム改ざん検知方法のプログラム、およびコンピュータ読み出し可能持続的有形記録媒体

関連出願の相互参照

[0001] 本出願は、２０１７年７月１３日に出願された日本特許出願番号２０１７－１３６７２５号に基づくもので、ここにその記載内容を援用する。

技術分野

[0002] 本開示は、プログラム改ざんを検知する電子制御装置、プログラム改ざん検知方法、プログラム改ざん検知方法のプログラム、およびコンピュータ読み出し可能持続的有形記録媒体に関するものである。

背景技術

[0003] 車両には、電子制御装置として、エンジン、ハンドル、ブレーキ等の制御を行う制御系ＥＣＵ（Electronic Control Unit）や、メータやパワーウインドウ等の制御を行うボデー系ＥＣＵや、ナビゲーション装置等の情報系ＥＣＵ等といった異なる種類のＥＣＵが搭載されている。これら、車両に搭載される車載ＥＣＵのプログラムには、例えば安全性を確保するため、起動時間に厳しい時間的制約が課せられるものが含まれる。

[0004] 特許文献１には、自動車等の組み込み機器において、ＯＳ（Operating System）等が第三者によって改ざんされる危険に対し、意図したＯＳ等のみを動作させるセキュアブート方法の開示が記載されている。同文献に記載のセキュアブート方法の開示は、高速かつ安全にシステムを起動させることを目的として、コンピュータが、システムのプログラム起動毎に、プログラムを複数に区分した部分プログラムのうち、検証対象となる部分プログラムを選択する選択工程と、選択した部分プログラムのハッシュ値を算出する算出工程と、算出したハッシュ値と正解ハッシュ値とが一致するかを判定し、一致する場合に起動処理を継続し、一致しない場合に起動処理を中断する検証工程

とを、実行するものである。

このように、特許文献１には、検証対象となるプログラム領域を複数の区分に分割し、各区分単位でプログラムの改ざんの有無の検証を順次実施することで、起動時間の制約を満しつつ、検証すべきすべてのプログラム領域を検証できることが記載されている。

[0005] 特許文献１に記載されているセキュアブート方法は、起動時の時間制約を満たすためにプログラム領域を分割した部分プログラムごとに、認証子として生成したハッシュ値と、あらかじめ記憶しておいた検証用認証子である正解ハッシュ値とを比較し、プログラムの改ざんの有無を検証する。

[0006] 無線インターフェースを経由して外部からの情報が自動車に提供される新たなサービスに伴って、自動車が外部と接続される機会も増える。このため、車載ＥＣＵのプログラムが改ざんのリスクも増大するといえる。したがって、安全なシステム起動のために、改ざんの有無を頻繁に検証することが必要になる。例えば、バッテリ接続時に起動する車載ＥＣＵの場合、バッテリ接続時にしか起動しないため、次回のバッテリ接続まで起動するタイミングがなく、その間にプログラムが改ざんされると改ざんがあったことに気付くのが遅れてしまう。したがって、スリープモードからのウェイクアップ起動（低消費電力モードから通常モードへの移行）時にも、改ざんの有無の検証を実施するようにすることで、改ざんに早期に気づくことが可能となる。

[0007] 一般に、スリープからのウェイクアップ起動時間の制約は、通常の起動時間の制約よりも厳しい。このため、スリープからウェイクアップ起動時における時間的制約を満たそうとすると、検証すべきプログラムの領域を細かく分けて、多数の部分プログラムに分割する必要がある。

[0008] 特許文献１に記載のセキュアブート方法は、各部分プログラムに対して一つずつの検証用認証子（正解ハッシュ値）をあらかじめ記憶しておく必要がある。このため、部分プログラムの数が増加すると、記憶領域に記憶される検証用認証子の数も増加する。したがって、多数の検証用認証子が限られた記憶領域（メモリ）における多くの領域を占めるという問題が発生する。

先行技術文献

特許文献

[0009] 特許文献1：特開２０１５－２２５２１号公報

発明の概要

[0010] 本開示は、起動時間の制約を満たしつつ、検証用認証子を記憶するために消費される記憶領域を抑制する、改ざんの検証対象プログラムを分割した分割プログラム毎にプログラムの改ざんを検知する処理を行なう電子制御装置、プログラム改ざん検知方法、プログラム改ざん検知方法のプログラム、およびコンピュータ読み出し可能持続的有形記録媒体を提供することを目的とする。

[0011] 本開示の第一の態様において、電子制御装置は、プログラムを分割した複数の分割プログラム、および検証用認証子を記憶する記憶部と、暗号演算により前記複数の分割プログラムそれぞれの部分認証子を生成する暗号演算部と、複数の前記部分認証子を用いた論理演算を行って演算認証子を生成し、前記検証用認証子と前記演算認証子とが一致するか否かによって前記プログラムの改ざんを検証する検証部とを有する。

[0012] 上記の電子制御装置は、分割プログラムから生成された部分認証子を複数用いた論理演算によって生成された演算認証子と、あらかじめ同じ論理演算を行って生成された検証用認証子と、が一致するか否かにより、プログラムの改ざんの有無を検証する。この構成によって、記憶部にあらかじめ記憶しておく検証用認証子の数を分割プログラムの数よりも少なくすることができる。したがって、起動時間の制約を満たすためにプログラムの分割数を増やしても、検証用認証子の記憶に要する記憶部（メモリ）の消費量が少ない電子制御装置となる。

[0013] 本開示の第二の態様において、プログラム改ざん検知方法は、プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成することと、複数の前記部分認証子を用いて論理演算を行って演算認証子を生成することと、前記演算認証子と、あらかじめ求めた検証用認証子とが

一致するか否かを判定することとを有する。

[0014] 上記のプログラム改ざん検知方法は、分割プログラムから生成された部分認証子を複数用いた論理演算によって生成された演算認証子と、あらかじめ同じ論理演算を行って生成された検証用認証子と、が一致するか否かにより、プログラムの改ざんの有無を検証する。この構成によって、あらかじめ記憶しておく検証用認証子の数を分割プログラムの数よりも少なくすることができる。したがって、起動時間の制約を満たすためにプログラムの分割数を増やしても、検証用認証子の記憶に要する記憶部（メモリ）の消費量が少なくなる。

[0015] 本開示の第三の態様において、プログラムは、プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成することと、複数の前記部分認証子を用いて論理演算を行って演算認証子を生成することと、前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定することとを有するプログラム改ざん検知方法をコンピュータに実行させる。

[0016] 上記のプログラム改ざん検知方法は、分割プログラムから生成された部分認証子を複数用いた論理演算によって生成された演算認証子と、あらかじめ同じ論理演算を行って生成された検証用認証子と、が一致するか否かにより、プログラムの改ざんの有無を検証する。この構成によって、あらかじめ記憶しておく検証用認証子の数を分割プログラムの数よりも少なくすることができる。したがって、起動時間の制約を満たすためにプログラムの分割数を増やしても、検証用認証子の記憶に要する記憶部（メモリ）の消費量が少なくなる。

[0017] 本開示の第四の態様において、プログラムは、プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成することと、複数の前記部分認証子を用いて論理演算を行って演算認証子を生成することと、前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定することとを有するプログラム改ざん検知方法を、電子制御装置が起

動する際にコンピュータに実行させる。

[0018] 上記のプログラム改ざん検知方法は、分割プログラムから生成された部分認証子を複数用いた論理演算によって生成された演算認証子と、あらかじめ同じ論理演算を行って生成された検証用認証子と、が一致するか否かにより、プログラムの改ざんの有無を検証する。この構成によって、あらかじめ記憶しておく検証用認証子の数を分割プログラムの数よりも少なくすることができる。したがって、起動時間の制約を満たすためにプログラムの分割数を増やしても、検証用認証子の記憶に要する記憶部（メモリ）の消費量が少なくなる。

[0019] 本開示の第五の態様において、プログラムは、プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成することと、複数の前記部分認証子を用いて論理演算を行って演算認証子を生成することと、前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定することとを有するプログラム改ざん検知方法を、電子制御装置の低消費電力モードから通常モードに移行する際にコンピュータに実行させる。

[0020] 上記のプログラム改ざん検知方法は、分割プログラムから生成された部分認証子を複数用いた論理演算によって生成された演算認証子と、あらかじめ同じ論理演算を行って生成された検証用認証子と、が一致するか否かにより、プログラムの改ざんの有無を検証する。この構成によって、あらかじめ記憶しておく検証用認証子の数を分割プログラムの数よりも少なくすることができる。したがって、起動時間の制約を満たすためにプログラムの分割数を増やしても、検証用認証子の記憶に要する記憶部（メモリ）の消費量が少なくなる。

[0021] 本開示の第六の態様において、コンピュータにより実行されるインストラクションを含むコンピュータ読み出し可能持続的有形記録媒体において、当該インストラクションは、プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成することと、複数の前記部分認証子を用いて論理演算を行って演算認証子を生成することと、前記演算認証子と

、あらかじめ求めた検証用認証子とが一致するか否かを判定することとを有する。

[0022] 上記のコンピュータ読み出し可能持続的有形記録媒体は、分割プログラムから生成された部分認証子を複数用いた論理演算によって生成された演算認証子と、あらかじめ同じ論理演算を行って生成された検証用認証子と、が一致するか否かにより、プログラムの改ざんの有無を検証する。この構成によって、あらかじめ記憶しておく検証用認証子の数を分割プログラムの数よりも少なくすることができる。したがって、起動時間の制約を満たすためにプログラムの分割数を増やしても、検証用認証子の記憶に要する記憶部（メモリ）の消費量が少なくなる。

図面の簡単な説明

[0023] 本開示についての上記目的およびその他の目的、特徴や利点は、添付の図面を参照しながら下記の詳細な記述により、より明確になる。その図面は、

[図1]本開示の実施形態１に係る電子制御装置の構成を説明するブロック図であり、

[図2]図１の電子制御装置によるプログラムの改ざんチェック処理の概要を模式的に示す説明図であり、

[図3]図１の電子制御装置の動作を説明するフローチャートであり、

[図4]本開示の実施形態２に係る電子制御装置の構成を説明するブロック図である。

発明を実施するための形態

[0024]（実施形態１）

１．電子制御装置（ＥＣＵ）の構成

本実施形態の電子制御装置の構成について以下に説明する。

[0025] 図１に示すように、電子制御装置１００は、ＲＯＭ（Read Only Memory）１０、ＲＡＭ（Random Access Memory）２０、ＣＰＵ（Central Processing Unit）３０、Ｉ／Ｏ（Input / Output）、およびこれらの構成を接続するバスラインなどから構成されている。

[0026] なお、本実施形態は、メッセージ認証コード（Message Authentication Code、MAC）を用いた暗号演算を用いることを主眼として記載しているが、本開示はＨＡＳＨ関数（Hash function）を用いた演算（ＳＨＡ－２５６など）をはじめ、その他の演算も含むものである。

[0027] ＲＯＭ１０は、改ざんチェック用のプログラム保存部１１、暗号演算部１２、暗号鍵保存部１３、認証子演算部１４、および検証用認証子保存部１５を備えている。

[0028] プログラム保存部１１（本開示の「記憶部」に相当）には、改ざんチェック対象のプログラムが、複数のブロックに分割された分割プログラムとして記憶されている。プログラムの分割数は、電子制御装置１００の用途や起動時間等を考慮して決定すればよい。

[0029] なお、「分割」とは、記憶領域で区切るなどして、プログラムの部分の開始点が特定されていればよく、プログラム自体を分割する必要は必ずしもない。

[0030] 暗号演算部１２（本開示の「暗号演算部」に相当）は、暗号演算プログラムが保存された領域である。暗号演算は、暗号演算部１２のプログラムを読み込んだＣＰＵ（暗号演算部）３０によって実施される。本実施形態では、ＣＭＡＣ（Cipher-based MAC）などのメッセージ認証コード（Message Authentication Code、MAC）を用いた暗号演算プログラムが暗号演算部１２に保存されている。ＭＡＣ以外の暗号演算としては、ＨＡＳＨ関数（Hash function）を用いた演算（ＳＨＡ－２５６など）が挙げられる。暗号演算により、複数の分割プログラムそれぞれの部分認証子を生成する。

[0031] 暗号鍵保存部１３は、暗号演算部１２が暗号演算を実施する際に必要となる、ＭＡＣ演算の暗号鍵が記憶された領域である。なお、暗号演算部１２が暗号演算プログラムとして、ＨＡＳＨ関数（Hash function）を用いた演算を行う場合は、暗号鍵は不要なので暗号鍵保存部１３を用いる必要はない。

[0032] 認証子演算部１４（本開示の「検証部」に相当）は、改ざんチェック用のプログラム保存部１１の各分割プログラムについて生成された、複数の部分

認証子を用いて演算認証子を生成する論理演算プログラムが記憶された領域である。論理演算は、認証子演算部１４のプログラムを読み込んだＣＰＵ（検証部）３０によって実施される。認証子演算部１４において用いられる論理演算については、図２および図３を参照して後に説明する。また、プログラムの改ざんの有無の検証についても、図２および図３を参照して後に説明する。

[0033] 検証用認証子保存部１５（本開示の「記憶部」に相当）は、改ざんを検証する対象であるプログラム保存部１１に記憶された検証対象のプログラムの検証用認証子が保存された領域である。検証用認証子は、プログラム保存部１１のプログラムについて、所定の暗号演算および論理演算をあらかじめ行うことにより生成されたものである。

[0034] 電子制御装置１００は、ＲＯＭ１０に保存されているプログラム保存部１１を書き換え可能な機能（リプログラム機能）を備えていてもよい。この場合、プログラム保存部１１の書き換えにより、検証用認証子も変化するから、併せて検証用認証子保存部１５も書き換える必要がある。リプログラム機能を備えている場合、外部から接続される可能性が高くなるから、検証用認証子の記憶に要する領域を増大させることなく、プログラム保存部１１の分割数を増やすことができる電子制御装置１００は有用である。

[0035] ＲＡＭ２０は、次回ＭＡＣ生成対象ブロック保存部２１および認証子保存部２２を備えている。

[0036] 次回ＭＡＣ生成対象ブロック保存部２１には、ブロック番号やＲＯＭ１０におけるアドレス等、次にＭＡＣ生成の対象となる分割プログラムを特定できる情報が保存される。

[0037] 認証子保存部２２には、認証子が生成される毎に、新たな認証子が上書き保存される。

[0038] ＣＰＵ３０は、プログラムを実行する装置であり、プログラム保存部１１のプログラム改ざんを検証する際には、暗号演算部１２および認証子演算部１４の各プログラムを実行する。

２．改ざんチェック処理

上述した構成を備えた電子制御装置１００による、プログラムの改ざんチェック処理について、図２を参照して説明する。

[0039] 図２に示すように、ＲＯＭ１０のプログラム保存部１１に書かれたプログラムをチェック対象とする改ざんチェック処理では、ＭＡＣ演算および論理演算が行われる。以下、ＭＡＣ演算および論理演算について順に説明する。

２．１．ＭＡＣ演算

ＭＡＣ演算は、メッセージ認証コード（ＭＡＣ）を用いた暗号演算であり、暗号演算部１２のプログラムの実行として、暗号鍵保存部１３の暗号鍵を用いて、ＲＯＭ１０の改ざんチェック領域１０Ａのブロック１～ブロックｎの各分割プログラムを対象として行われる。ＭＡＣ演算の結果として、ブロック１～ブロックｎの各分割プログラムそれぞれに対してＭＡＣ１～ＭＡＣｎ（部分認証子）が生成される。生成されたＭＡＣは、例えば、AES（Advanced Encryption Standard）１２８の暗号アルゴリズムを用いた演算の場合は、１２８ビットである。なお、SHA（Secure Hash Algorithm）－２５６のＨＡＳＨ関数を用いた演算の場合は、生成されるＨＡＳＨ値は、２５６ビットである。

[0040] ＲＯＭ１０は、ｎ個の部分プログラムが保存されたプログラム保存部１１が置かれた改ざんチェック領域１０Ａと、それ以外の非改ざんチェック領域１０Ｂとに分かれている。

[0041] 改ざんチェック領域１０Ａには、ブロック１～ブロックｎに分割された部分プログラムが保存されている。以下では、ブロック１～ブロックｎの部分プログラムを、適宜、ブロック１～ブロックｎということもある。

[0042] 非改ざんチェック領域１０Ｂには、検証用認証子が保存されている。検証用認証子は、演算によってあらかじめ生成されたものであり、認証子［１－ｎ］（演算用認証子）と比較して、ブロック１～ブロックｎが改ざんされたものが含まれるか否かの判定に用いられるから、重要性の高いデータである。このため、ＲＯＭ１０の非改ざんチェック領域１０Ｂはセキュア領域とし

て構成されている。セキュア領域とは、記憶されている情報へのアクセスが困難であって、情報を保護する機能が高い領域をいう。

[0043] 図２には、非改ざんチェック領域１０Ｂの全部がセキュア領域として構成された例を示す。しかし、非改ざんチェック領域１０Ｂはセキュア領域ではなく、改ざんチェック領域１０Ａと同程度の情報保護機能の領域であってもよい、また、一部をセキュア領域としてもよい。

[0044] なお、図２では省略しているが、ＲＯＭ１０の非改ざんチェック領域１０Ｂには、暗号演算部１２、暗号鍵保存部１３および認証子演算部１４（図１参照）も置かれている。

２．２．論理演算

ブロックｘ（ｘは２～ｎの整数）の暗号演算によってＭＡＣｘが算出されると、ＲＡＭ２０の認証子保存部２２に記憶されている認証子とＭＡＣｘとの論理演算が行われて、認証子［１－ｘ］が生成され、認証子保存部２２に上書きされる。併せて、次回ＭＡＣ生成対象ブロック保存部２１にブロックｘ＋１を特定するブロック番号ｘ＋１が保存される。

[0045] 論理演算としては、論理積（ＡＮＤ演算）、論理積の否定（ＮＡＮＤ演算）、論理和（ＯＲ演算）、論理和の否定（ＮＯＲ演算）、排他的論理和（ＸＯＲ演算）および、排他的論理和の否定（ＸＮＯＲ演算＝一致論理）が挙げられる。これらのうちでは、排他的論理和および排他的論理和の否定が、真理値表における０と１との数が同じであることから、論理演算の繰り返しによって、０または１の一方に収束しないという点において好ましい。

２．３．ＭＡＣ演算と論理演算との関係

ＭＡＣ演算および論理演算はそれぞれ、２．１および２．２で説明したように実施される。以下では、ＭＡＣがブロック番号順に生成される場合、ＭＡＣ演算により生成される部分認証子と、論理演算により生成される演算認証子とが、それぞれ、どのように用いられるかについて、順次実施されるブロック１～ブロックｎの演算処理に沿って順に説明する。

[0046] ブロック１のＭＡＣ１は、最初に生成される部分認証子である。このため

、ＭＡＣ１が生成された時点では、複数の部分認証子を用いた論理演算を行うことができない。そこで、認証子［１］（演算認証子）として、ブロック１のＭＡＣ１がＲＡＭ２０の認証子保存部２２に保存される。併せて、次回ＭＡＣ生成対象ブロック保存部２１の次回ＭＡＣ生成対象ブロックを２にする。

[0047] 続いて、ブロック２のＭＡＣ２が生成されると、認証子保存部２２の認証子［１］とＭＡＣ２との論理演算を行って生成された認証子［１－２］（演算認証子）が認証子保存部２２に上書き保存される。併せて、次回ＭＡＣ生成対象ブロック保存部２１の次回ＭＡＣ生成対象ブロックを３にする。

[0048] 認証子［１］はＭＡＣ１と同一だから、ＭＡＣ２と認証子［１］との論理演算は、２つの部分認証子を用いて行われたものである。

[0049] さらに、ブロック３のＭＡＣ３が生成されると、認証子保存部２２の認証子［１－２］とＭＡＣ３との論理演算を行って生成された認証子［１－３］（演算認証子）が認証子保存部２２に上書き保存される。併せて、次回ＭＡＣ生成対象ブロック保存部２１の次回ＭＡＣ生成対象ブロックを４にする。

[0050] 認証子［１－２］は、ＭＡＣ１とＭＡＣ２とを用いた論理演算により生成されたものであるから、認証子［１－２］とＭＡＣ３との論理演算は、３つの部分認証子ＭＡＣ１、ＭＡＣ２およびＭＡＣ３を用いて行われたものである。本開示において、論理演算に用いられた「複数の部分認証子」には、先の論理演算で用いられた部分認証子が含まれる。

[0051] ブロックＸのＭＡＣＸ（Ｘ＝４～ｎ－１）が生成された場合の演算処理は、ブロック３と同様である。

[0052] 最後に、ブロックｎのＭＡＣｎが生成されると、認証子保存部２２の認証子［１－ｎ-１］とＭＡＣｎとの論理演算を行って生成された認証子［１－ｎ］（演算認証子）が認証子保存部２２に上書き保存される。併せて、次回ＭＡＣ生成対象ブロック保存部２１の次回ＭＡＣ生成対象ブロックを１に初期化する。

[0053] 認証子［１－ｎ-１］は、ＭＡＣ１～ＭＡＣｎ-１を用いた論理演算により

生成されたものであるから、認証子［１－ｎ-１］とＭＡＣｎとの論理演算は、部分認証子ＭＡＣ１～ＭＡＣｎのすべてを用いて行われたものである。

[0054] 認証子［１－ｎ］は、ブロック１～ブロックｎのＭＡＣ１～ＭＡＣｎ（部分認証子）のすべてを用いて行われた論理演算の結果として、生成された演算認証子である。したがって、ブロック１～ブロックｎのいずれかが改ざんされた場合、ＭＡＣ１～ＭＡＣｎのいずれかを介して、認証子［１－ｎ］に当該改ざんが反映される。したがって、改ざんがある場合、認証子［１－ｎ］と、事前の演算によって求められた検証用認証子とは一致しない。

[0055] そこで、認証子［１－ｎ］と検証用認証子とを比較して、一致しない場合にはプログラムの改ざん有、一致する場合にはプログラムの改ざん無、と判断することができる。当該比較によって、プログラムの改ざん有と判断した場合には、電子制御装置１００（図１参照）の起動を中止したり、警告表示を出したりする。

[0056] 電子制御装置１００は、ＭＡＣ１～ＭＡＣｎのすべてを用いた演算を行って認証子［１－ｎ］（演算認証子）生成し、検証用認証子とを比較して、プログラム保存部１１（図１参照）の改ざんの有無を判断する。このため、ＲＯＭ１０の検証用認証子保存部１５には一つの検証用認証子を保存すれば足りる。

[0057] したがって、従来のように、分割したブロック毎にプログラムの改ざんの有無を検証する、ブロック数と同じ数の検証用認証子が必要なものよりも、ブロック数ｎから１を引いたｎ－１個の検証用認証子の記憶容量を削減することができる。

[0058] 例えば、部分認証子であるＭＡＣ１～ＭＡＣｎとして１２８ビットのものを用いた場合、（ｎ－１）×１２８ビットの記憶容量を削減することができる。電子制御装置１００によれば、改ざん検証の対象となるプログラムの分割数が多くなるほど、ＲＯＭ１０の記憶容量の削減効果が高くなる。プログラムの分割数の増大は、起動処理が中断した場合に、それまでの処理が無駄になることを防止し、電子制御装置１００の起動時間を短縮するために有効

である。

[0059] 図２では、検証用認証子が一つである場合記載した。このように、検証用認証子を一つにすることは、ＲＯＭ１０の検証用認証子保存部１５の記憶容量を削減する観点から好ましいといえる。

[0060] ただし、検証用認証子保存部１５に保存される検証用認証子の数は、一つに限られず、複数としてもよい、検証用認証子を複数とする場合、ブロック１～ブロックｎを複数のグループに分け、各グループ用の検証用認証子をあらかじめＲＯＭ１０に記憶しておく。そして、各グループの部分認証子をすべて用いた論理演算による検証用認証子を生成し、検証用認証子と比較し、当該グループに含まれる分割プログラムの改ざんの有無を判断する。

[0061] 認証子［１］～認証子［１－ｎ］の算出を連続して、一度で行うことが出来ない場合、暗号演算や論理演算の途中で改ざんチェック処理が中止される。この場合、認証子保存部２２には、中止されるまでの改ざんチェック処理によって得られた認証子（演算認証子）が保存されている。また、次回ＭＡＣ生成対象ブロック保存部２１には、認証子が得られた論理演算の次に、ＭＡＣ生成対象となるブロックが保存されている。したがって、中止される迄の改ざんチェック処理で、認証子を生成した論理演算の次の暗号演算から再開することができる。そして、再開した暗号演算に続く論理演算では、認証子保存部２２の認証子を用いることができため、中断されるまでに完了したブロックに対する暗号処理および論理演算の結果を有効に用いることができる。

[0062] したがって、プログラムを分割して、改ざんチェック処理を行うことによって、プログラム検証に要する時間を短縮することが可能になる。

[0063] ＲＡＭ２０は、低消費電力モードから通常モードへの起動（Ｗａｋｅ　Ｕｐ起動）において、初期化されない非初期化領域２０Ａと、初期化される初期領域２０Ｂとからなっている。非初期化領域２０Ａには、次回ＭＡＣ生成対象ブロック保存部２１と認証子保存部２２とが置かれている。このため、認証子１～認証子［１－ｎ］が算出される毎に書き換えられた次回ＭＡＣ生

成対象ブロック保存部２１、および認証子保存部２２に書き込まれた情報は、Ｗａｋｅ　Ｕｐ起動時に維持される。したがって、認証子１～認証子［１－ｎ］の演算途中で、再起動が生じた場合、再起動前に記録された次回ＭＡＣ生成対象ブロック保存部２１および認証子保存部２２の情報に基づいて、改ざんチェック処理を再開することができる。

[0064] 次回ＭＡＣ生成対象ブロック保存部２１および認証子保存部２２が保存される領域は、Ｗａｋｅ　Ｕｐ起動時に初期化されない領域であれば、改ざんチェック処理の中断から素早く再開することができる。このため、次回ＭＡＣ生成対象ブロック保存部２１および認証子保存部２２を、ＥＥＰＲＯＭやＤａｔａ　Ｆｌａｓｈ等の書き換え可能な不揮発性メモリに保存してもよい。ただし、処理速度は、例示の不揮発性メモリよりもＲＡＭ２０の方が速いため、電子制御装置１００の起動時における時間制約を満たすことができる場合に限って、前記例示の不揮発性メモリを使用できる。

[0065] 本開示は、電子制御装置を複数備えた電子制御装置ユニットとして実施することもできる。電子制御装置を複数備えた電子制御装置ユニットは、起動時における時間的制約が異なる電子制御装置が組み合わせて用いられることが多い。したがって、記憶部に記憶されている分割プログラムの分割数を、複数の電子制御装置の用途や、移動時の時間的制約に応じて、異ならせることが好ましい。これにより、電子制御装置の各起動時間の制約を満たしつつ、電子制御装置ユニットにおける記憶部全体としてメモリの消費量を抑制することができる。

３．プログラム改ざん検知方法

図３を参照して、上述した電子制御装置１００によるプログラム改ざん検知方法について、説明する。

[0066] プログラム改ざん検知方法は、ＣＰＵ３０が暗号演算部１２および認証子演算部１４（図１参照）のプログラムを読み込んで実行するものであり、電子制御装置１００の起動時、低消費電力モードから通常モードに移行する際等にコールされる。低消費電力モードは、電子制御装置１００が、通常モー

ドにおいて行う処理の一部を行わない、消費電力が通常モードよりも小さい状態をいう。実行中のプログラムがメモリに保存され一時的に停止するスリープモードは、低消費電力モードの一例である。

[0067] Ｓ１０では、ＲＡＭ２０の次回ＭＡＣ生成対象ブロック保存部２１に記録されているブロック番号を参照して、ブロック番号が１以外であるか否かが判定される。そして、次回ＭＡＣ生成対象ブロック保存部２１のブロック番号が１以外ではない場合（１である場合）には（Ｓ１０：ＮＯ）Ｓ２０（暗号演算ステップ）に処理が移行され、次回ＭＡＣ生成対象ブロック保存部２１のブロック番号が１以外である場合には（Ｓ１０：ＹＥＳ）Ｓ５０（暗号演算ステップ）に移行する。

[0068] Ｓ２０では、ＭＡＣ生成対象ブロックであるブロック１の分割プログラムのＭＡＣ１を生成し、Ｓ３０に移行する。

[0069] Ｓ３０では、Ｓ２０で生成されたＭＡＣ１をＲＡＭ２０の認証子保存部２２に、認証子として記憶し、Ｓ４０（認証子演算ステップ）に移行する。

[0070] Ｓ４０では、ＲＡＭ２０の次回ＭＡＣ生成対象ブロック保存部２１に、次回ＭＡＣ生成対象ブロックとして、Ｓ２０においてＭＡＣを生成した部分プログラムのブロック番号に１を加えたブロック番号を書き込んで（設定して）、本処理を終了する。

[0071] Ｓ５０では、ＭＡＣ生成対象ブロックである、ブロック番号ｘ（ｘは２～ｎの整数）の分割プログラムのＭＡＣｘを生成して、Ｓ６０（認証子演算ステップ）に移行する。

[0072] Ｓ６０では、認証子演算部１４が、Ｓ５０で生成されたＭＡＣとＲＡＭ２０の認証子保存部２２に記憶されている認証子［１－（ｘ－１）］との論理演算を行い、認証子［１－（ｘ）］を算出し、Ｓ７０に移行する。

[0073] Ｓ７０では、ＲＡＭ２０の認証子保存部２２に、生成された認証子［１－ｘ］を記憶し、Ｓ８０に移行する。

[0074] Ｓ８０では、Ｓ５０でＭＡＣが生成されたブロックが最終ブロックか否か、すなわち、ＭＡＣが生成されたブロックのブロック番号ｘが、分割プログ

ラムのブロック数ｎと等しい（ｘ＝ｎ）か否かが判断される。

[0075] ｘ＝ｎである場合には（Ｓ８０：Ｙｅｓ）、Ｓ７０で認証子保存部２２に記憶された認証子［１－ｎ］は、すべての分割プログラムの部分認証子を用いた論理演算の結果得られたものである。すべての分割プログラムのなかに、改ざんされたプログラムが含まれるか否かを検証する検証用認証子として用いることができる。そこで、Ｓ９０（検証ステップ）に移行する。

[0076] ｘ＝ｎでない場合には、Ｓ４０に移行する。

[0077] Ｓ９０では、認証子保存部２２に保存されている認証子［１－ｎ］と、検証用認証子保存部１５に保存されている検証用認証子と、を比較する。

[0078] Ｓ１００（検証ステップ）では、Ｓ９０において比較した値が一致したか否を判断する。

一致する場合には（Ｓ１００：ＹＥＳ）Ｓ１１０に処理が移行され、一致しない場合には（Ｓ１００：ＹＥＳ）Ｓ１２０に処理が移行される。

[0079] Ｓ１１０では、改ざんチェック結果を改ざんなしに設定し、Ｓ１３０に移行する。

[0080] Ｓ１２０では、改ざんチェック結果を改ざんありに設定し、Ｓ１３０に移行する。

[0081] Ｓ１３０では、次回ＭＡＣ生成対象ブロック保存部２１のブロック番号を１に初期化して、本処理を終了する。

[0082] 本開示は、上述したプログラム改ざん検知方法をコンピュータに実行させるプログラムとして実施することもできる。当該プログラムは、電子制御装置が起動する際や、低消費電力モードから通常モードに移行する際に実行される。

[0083] 以上のように、本実施形態の電子制御装置によれば、プログラムを分割した分割プログラム毎に必要となる各部分認証子そのものではなく、複数の部分認証子を用いて論理演算を行って得られる演算認証子を検証用認証子との比較対象とし、プログラムの改ざんの有無を検知する。これにより、記憶すべき検証用認証子の数を削減し、ＲＯＭの大量消費を抑えることが可能にな

る。

（実施形態２）

セキュリティチップを利用する電子制御装置（ＥＣＵ）に本開示を適用する形態について説明する。

[0084] 図４に示すように、本実施形態の電子制御装置２００は、ＲＯＭ２１０、セキュリティチップ２２０、ＲＡＭ２０、ＣＰＵ３０、およびＩ／Ｏおよびこれらの構成を接続するバスラインを備えている。

[0085] 電子制御装置２００は、ＲＯＭ１０に代えて、ＲＯＭ２１０およびセキュリティチップ２２０を備えている構成において、電子制御装置１００と異なっている。ＲＯＭ１０の各部のうち、ＲＯＭ２１０に配置されているのはプログラム保存部１１のみである。プログラム保存部１１以外は、耐タンパー性（記憶データを解析する困難さ）が高いセキュリティチップ２２０に置かれている。

[0086] セキュリティチップ２２０は、セキュア（Ｓｅｃｕｒｅ）ＣＰＵ２２４、セキュア（Ｓｅｃｕｒｅ）ＲＡＭ２２３、セキュアインターフェース（Ｓｅｃｕｒｅ　Ｉ／Ｆ）、ハードウェアＩＰモジュール（ＨＷＩＰ）２２１、およびセキュア（Ｓｅｃｕｒｅ）ＲＯＭ２２２を備えている。ハードウェアＩＰモジュール２２１は、暗号演算部１２を有している。セキュア（Ｓｅｃｕｒｅ）ＲＯＭ２２２は、暗号鍵保存部１３、認証子演算部１４および検証用認証子保存部１５を有している。セキュア（Ｓｅｃｕｒｅ）ＲＡＭ２２３は、次回ＭＡＣ生成対象ブロック保存部２１、および認証子保存部２２を有している。そして、実施形態１においては、図２の各種暗号演算や図３のフローの処理はＣＰＵ３０が実行していたが、本実施形態においてはセキュア（Ｓｅｃｕｒｅ）ＣＰＵ２２４がこれを実行する。

[0087] 以上のように、プログラム改ざんの有無を検証する処理に用いられるプログラム（および演算認証子や次回ＭＡＣ生成対象ブロック等の一時データ）、暗号鍵、および検証用認証子をセキュリティチップ２２０に記憶することにより、これらプログラム（および上記一時データ）、暗号鍵、および検証

用認証子にアクセスされることを防止することができる。

[0088] 本開示の電子制御装置の形態の例として、半導体、電子回路、モジュール、マイクロコンピュータが挙げられる。またこれらにアンテナや通信用インターフェースなど、必要な機能を追加してもよい。また、カーナビゲーションシステム、スマートフォン、パーソナルコンピュータ、携帯情報端末のような形態をとることも可能である。

[0089] 加えて、本開示は、上述の専用のハードウェアで実現できるだけでなく、メモリやハードディスク等の記録媒体に記録したプログラム、及びこれを実行可能な専用又は汎用ＣＰＵ及びメモリ等を有する汎用のハードウェアとの組み合わせとしても実現できる。

[0090] 専用や汎用のハードウェアの記憶領域（外部記憶装置（ハードディスク、ＵＳＢメモリ等）、内部記憶装置（ＲＡＭ，ＲＯＭ等））に格納されるプログラムは、記録媒体を介して、あるいは記録媒体を介さずにサーバから通信回線を経由して上述の専用又は汎用のハードウェア（本開示の「コンピュータ」に相当」に提供することもできる。これにより、プログラムのアップグレードを通じて常に最新の機能を提供することができる。

[0091] 本開示にかかる電子制御装置は、車載用電子制御装置（ＥＣＵ）として用いることができる。もちろん、車載用以外の電子制御装置も本開示に含むものである。

[0092] ここで、この出願に記載されるフローチャート、あるいは、フローチャートの処理は、複数のセクション（あるいはステップと言及される）から構成され、各セクションは、たとえば、Ｓ１０と表現される。さらに、各セクションは、複数のサブセクションに分割されることができる、一方、複数のセクションが合わさって一つのセクションにすることも可能である。さらに、このように構成される各セクションは、デバイス、モジュール、ミーンズとして言及されることができる。

[0093] 本開示は、実施例に準拠して記述されたが、本開示は当該実施例や構造に限定されるものではないと理解される。本開示は、様々な変形例や均等範囲

内の変形をも包含する。加えて、様々な組み合わせや形態、さらには、それらに一要素のみ、それ以上、あるいはそれ以下、を含む他の組み合わせや形態をも、本開示の範疇や思想範囲に入るものである。

請求の範囲

[請求項1] プログラムを分割した複数の分割プログラム、および検証用認証子を記憶する記憶部（１１、１５）と、

暗号演算により前記複数の分割プログラムそれぞれの部分認証子を生成する暗号演算部（１２、１３、３０、２２４）と、

複数の前記部分認証子を用いた論理演算を行って演算認証子を生成し、前記検証用認証子と前記演算認証子とが一致するか否かによって前記プログラムの改ざんを検証する検証部（１４、３０、２２４）と、

を有する電子制御装置。

[請求項2] 前記記憶部（１１）に記憶されている前記検証用認証子が一つであり、

前記検証部（１４、３０、２２４）が、すべての前記部分認証子を用いた論理演算を行って一つの演算認証子を生成し、

前記検証部（１４、３０、２２４）は、前記一つの検証用認証子と前記一つの演算認証子とが一致するか否かによって前記プログラムの改ざんの有無を検証する、

請求項１に記載の電子制御装置。

[請求項3] 前記検証部（１４、３０、２２４）が行う前記論理演算が、排他的論理和（ＸＯＲ演算）または排他的論理和の否定（ＸＮＯＲ演算）であり、

排他的論理和は、ＸＯＲ演算と定義され、

排他的論理和の否定は、ＸＮＯＲ演算と定義される、

請求項１または２に記載の電子制御装置。

[請求項4] プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成すること（Ｓ２０、Ｓ５０）と、

複数の前記部分認証子を用いて論理演算を行って演算認証子を生成すること（Ｓ６０）と、

前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定すること（Ｓ９０、Ｓ１００）と、

を有するプログラム改ざん検知方法。

[請求項5] 電子制御装置が起動する際に、部分認証子の生成と、演算認証子の生成と、判定を実行する、

請求項４に記載のプログラム改ざん検知方法。

[請求項6] 電子制御装置が低消費電力モードから通常モードに移行する際に、部分認証子の生成と、演算認証子の生成と、判定を実行する、

請求項４に記載のプログラム改ざん検知方法。

[請求項7] プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成すること（Ｓ２０、Ｓ５０）と、

複数の前記部分認証子を用いて論理演算を行って演算認証子を生成すること（Ｓ６０）と、

前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定すること（Ｓ９０、Ｓ１００）と、

を有するプログラム改ざん検知方法をコンピュータに実行させるプログラム。

[請求項8] プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成すること（Ｓ２０、Ｓ５０）と、

複数の前記部分認証子を用いて論理演算を行って演算認証子を生成すること（Ｓ６０）と、

前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定すること（Ｓ９０、Ｓ１００）と、

を有するプログラム改ざん検知方法を電子制御装置が起動する際にコンピュータに実行させるプログラム。

[請求項9] プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成すること（Ｓ２０、Ｓ５０）と、

複数の前記部分認証子を用いて論理演算を行って演算認証子を生成

すること（Ｓ６０）と、

前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定すること（Ｓ９０、Ｓ１００）と、

を有するプログラム改ざん検知方法を電子制御装置の低消費電力モードから通常モードに移行する際にコンピュータに実行させるプログラム。

[請求項10] コンピュータにより実行されるインストラクションを含むコンピュータ読み出し可能持続的有形記録媒体において、当該インストラクションは、

プログラムを分割した複数の分割プログラムそれぞれの部分認証子を暗号演算により生成すること（Ｓ２０、Ｓ５０）と、

複数の前記部分認証子を用いて論理演算を行って演算認証子を生成すること（Ｓ６０）と、

前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定すること（Ｓ９０、Ｓ１００）とを有する、

コンピュータ読み出し可能持続的有形記録媒体。

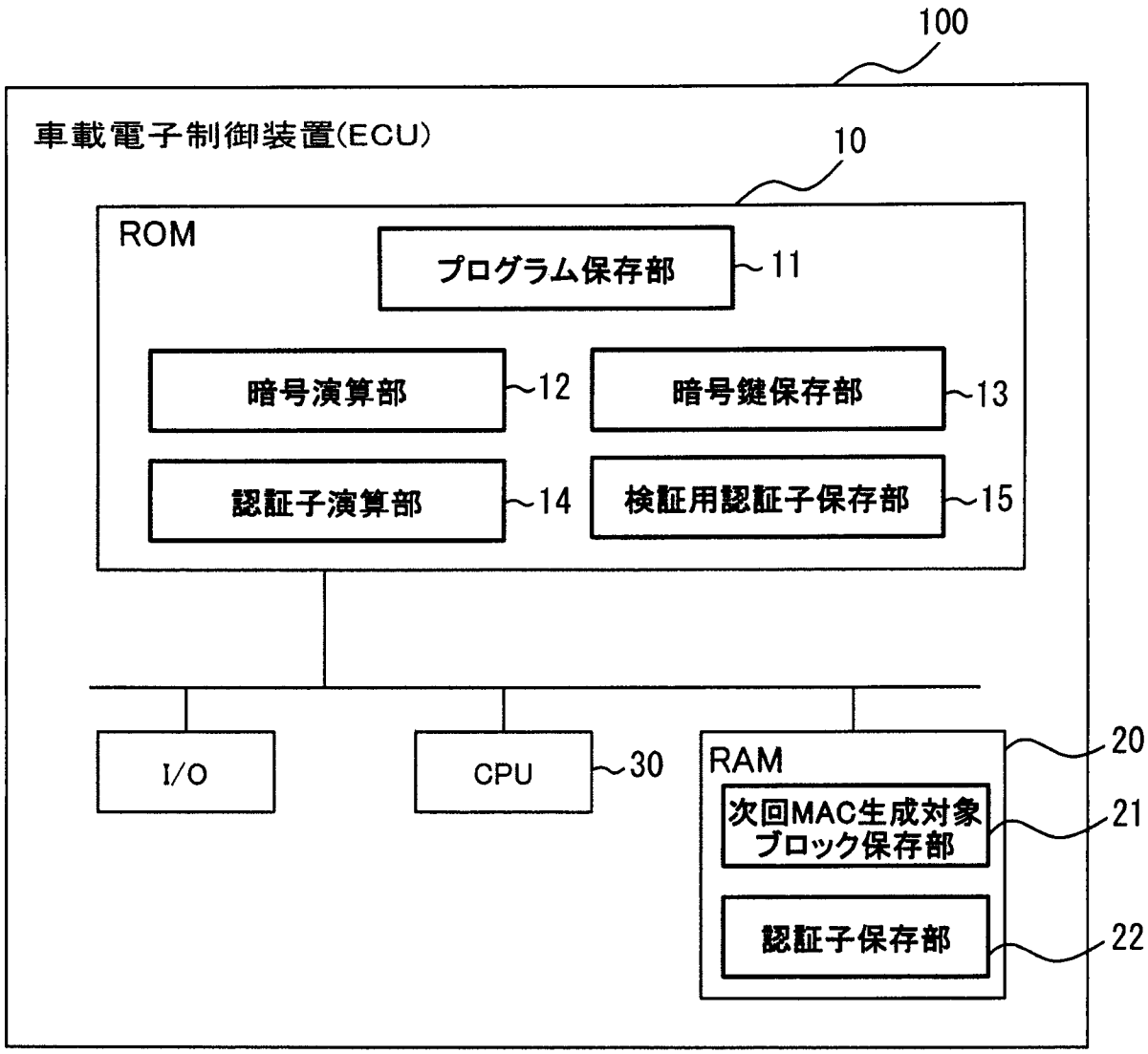
[請求項11] 電子制御装置が起動する際に、コンピュータは、当該インストラクションを実行する、

請求項１０に記載のコンピュータ読み出し可能持続的有形記録媒体。

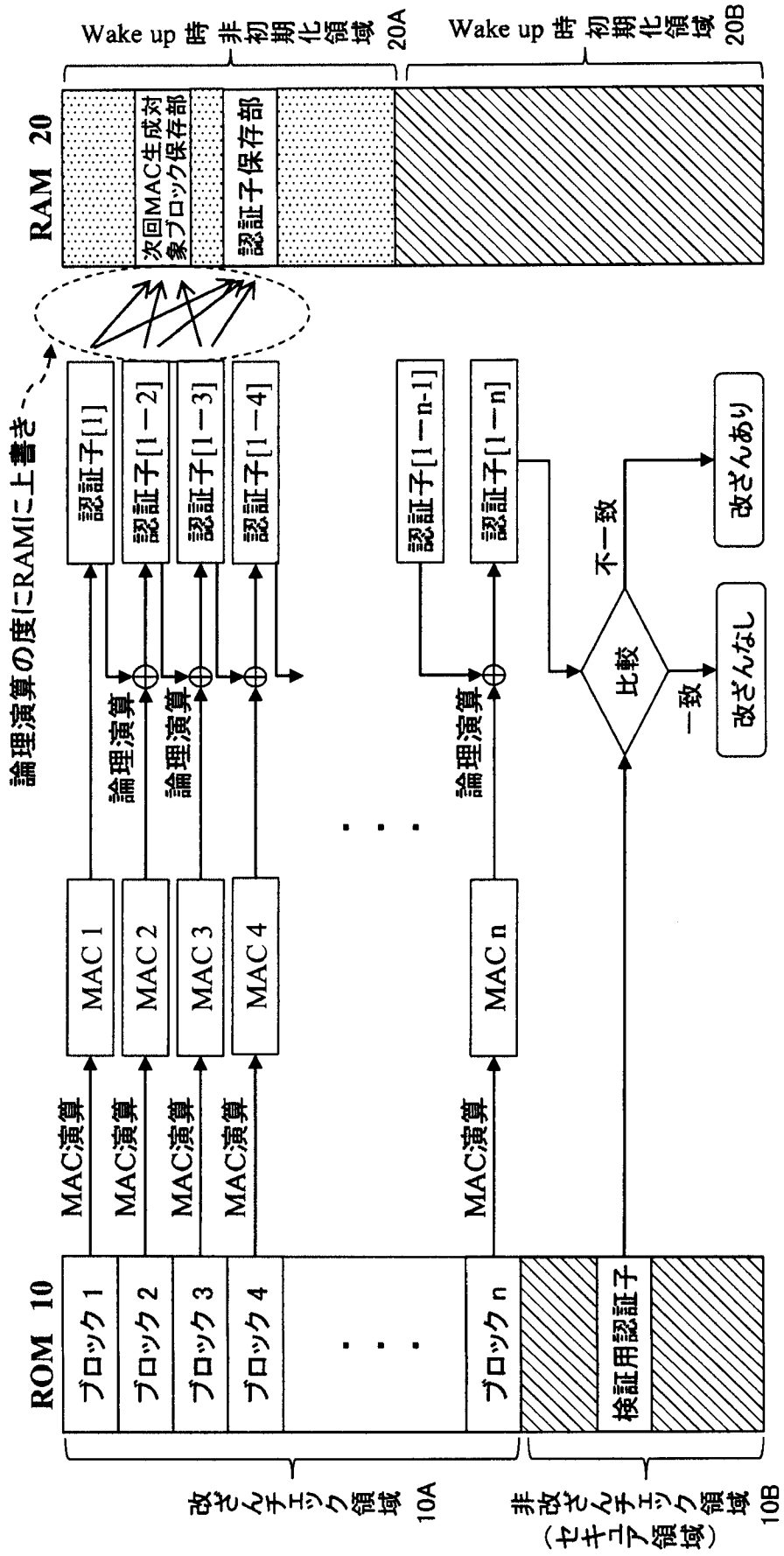
[請求項12] 電子制御装置が低消費電力モードから通常モードに移行する際に、コンピュータは、当該インストラクションを実行する、

請求項１０に記載のコンピュータ読み出し可能持続的有形記録媒体。

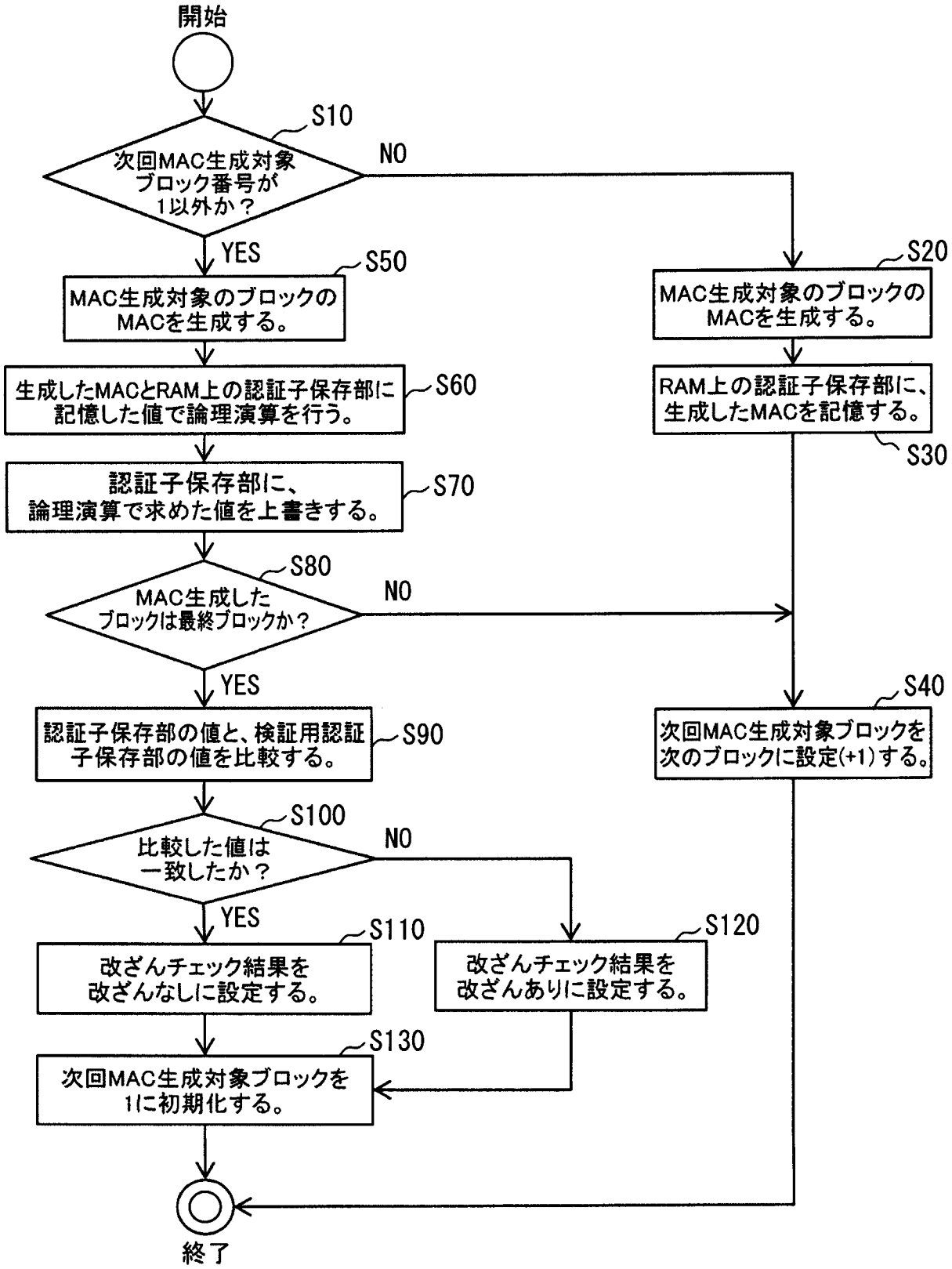
[図1]


100
車載電子制御装置(ECU)
10
ROM
プログラム保存部
11
暗号演算部
12
暗号鍵保存部
13
認証子演算部
14
検証用認証子保存部
15
I/O
CPU
30
RAM
20
次回MAC生成対象ブロック保存部
21
認証子保存部
22

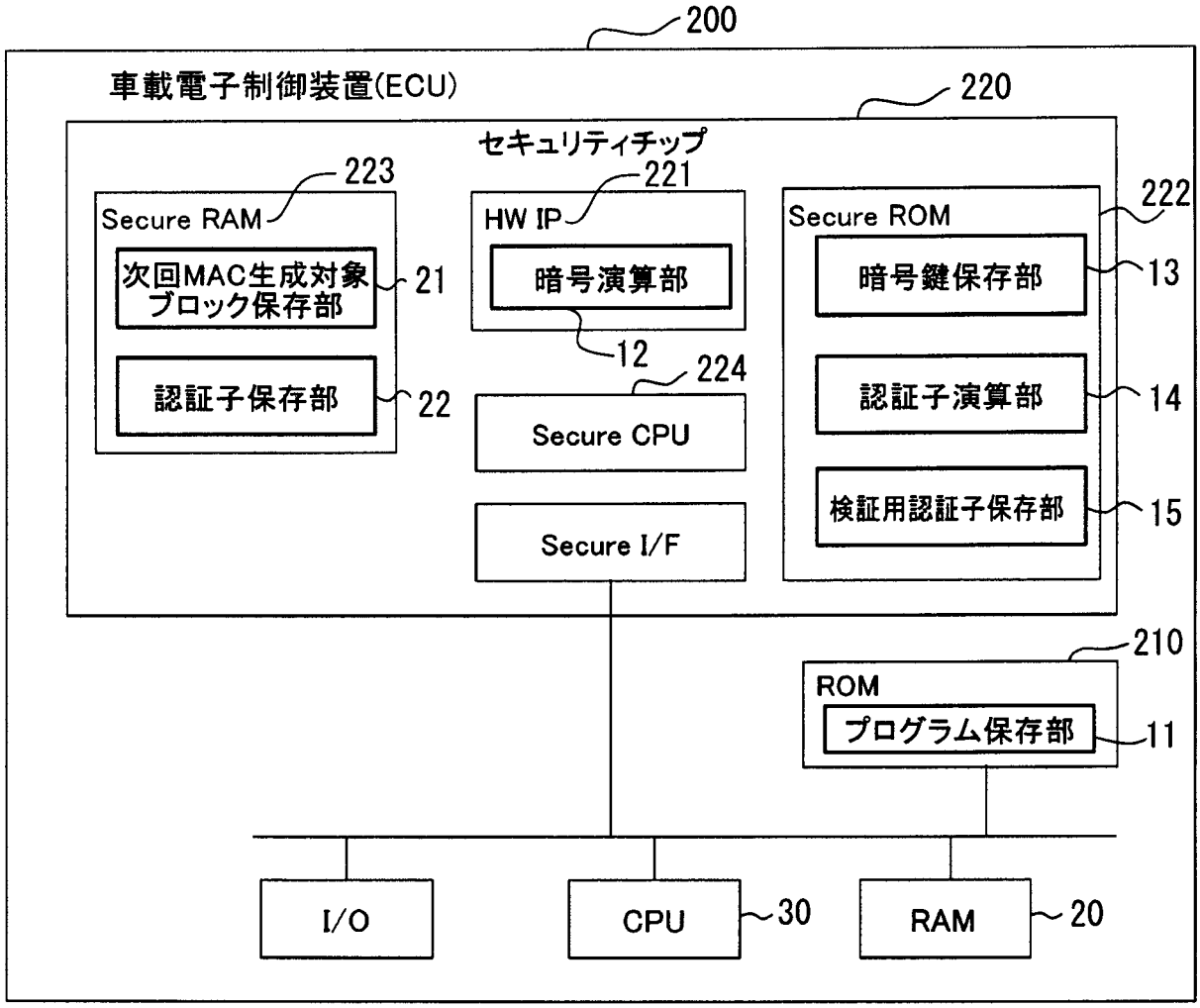
[図2]


Wake up 時 非初期化領域 20A
Wake up 時 初期化領域 20B
RAM 20
次回MAC生成対象ブロック保存部
認証子保存部
論理演算の度にRAMに上書き
認証子[1]
認証子[1－2]
認証子[1－3]
認証子[1－4]
認証子[1－n-1]
認証子[1－n]
論理演算
論理演算
論理演算
論理演算
MAC 1
MAC 2
MAC 3
MAC 4
MAC n
MAC演算
MAC演算
MAC演算
MAC演算
MAC演算
比較
不一致
一致
改ざんあり
改ざんなし
ROM 10
ブロック 1
ブロック 2
ブロック 3
ブロック 4
ブロック n
検証用認証子
改ざんチェック領域 10A
非改ざんチェック領域（セキュア領域） 10B

[図3]


開始
S10
次回MAC生成対象ブロック番号が1以外か？
NO
YES
S50
MAC生成対象のブロックのMACを生成する。
S20
MAC生成対象のブロックのMACを生成する。
生成したMACとRAM上の認証子保存部に記憶した値で論理演算を行う。
S60
RAM上の認証子保存部に、生成したMACを記憶する。
S30
認証子保存部に、論理演算で求めた値を上書きする。
S70
S80
MAC生成したブロックは最終ブロックか？
NO
YES
S40
次回MAC生成対象ブロックを次のブロックに設定(+1)する。
認証子保存部の値と、検証用認証子保存部の値を比較する。
S90
S100
比較した値は一致したか？
NO
YES
S110
改ざんチェック結果を改ざんなしに設定する。
S120
改ざんチェック結果を改ざんありに設定する。
S130
次回MAC生成対象ブロックを1に初期化する。
終了

[図4]


200
車載電子制御装置(ECU)
220
セキュリティチップ
223
Secure RAM
次回MAC生成対象ブロック保存部
21
認証子保存部
22
221
HW IP
暗号演算部
12
224
Secure CPU
Secure I/F
222
Secure ROM
暗号鍵保存部
13
認証子演算部
14
検証用認証子保存部
15
210
ROM
プログラム保存部
11
I/O
CPU
30
RAM
20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/023808

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/12(2013.01)i, G06F21/64(2013.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)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)
Int.Cl. G06F21/12, G06F21/64, G09C1/00, H04L9/32

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	1971-2018
Registered utility model specifications of Japan	1996-2018
Published registered utility model applications of Japan	1994-2018

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	WO 2016/185577 A1 (FUJITSU LTD.) 24 November 2016, paragraphs [0010]-[0087], fig. 1-15 & US 2018/0096132 A1, paragraphs [0013]-[0105], fig. 1-15 & EP 3299986 A1	1-12
Y	JP 2017-509082 A (OBERTHUR TECHNOLOGIES) 30 March 2017, paragraphs [0016]-[0166], fig. 2-3b & US 2017/0109546 A1, paragraphs [0016]-[0188], fig. 2-3b & WO 2015/145071 A1 & EP 3123387 A1 & FR 3019347 A1 & CN 106133739 A & KR 10-2016-0136386 A	1-12
Y	JP 2015-90682 A (CANON INC.) 11 May 2015, claims 1-4, paragraphs [0017]-[0029], [0031]-[0042], fig. 2, 3 & US 2015/0124279 A1, paragraphs [0022]-[0034], [0036]-[0047], fig. 2A-3B & CN 104639782 A	6, 9, 12

☐ 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 21 August 2018 (21.08.2018)	Date of mailing of the international search report 28 August 2018 (28.08.2018)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０２３８０８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/12(2013.01)i, G06F21/64(2013.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)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（ＩＰＣ））

Int.Cl.　G06F21/12, G06F21/64, G09C1/00, H04L9/32

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	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８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	WO 2016/185577 A1 (富士通株式会社) 2016.11.24, 段落［００１０］－［００８７］, 図１－１５ & US 2018/0096132 A1, 段落［００１３］－［０１０５］, 図１－１５ & EP 3299986 A1	1-12
Y	JP 2017-509082 A (オベルトゥル　テクノロジ) 2017.03.30, 段落［００１６］－［０１６６］, 図２－３ｂ & US 2017/0109546 A1, 段落［００１６］－［０１８８］, 図２－３ｂ & WO 2015/145071 A1 & EP 3123387 A1 & FR 3019347 A1 & CN 106133739 A & KR 10-2016-0136386 A	1-12

☑　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	国際調査報告の発送日
２１．０８．２０１８	２８．０８．２０１８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｓ　４４４０
打出　義尚
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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 2015-90682 A（キヤノン株式会社）2015.05.11，請求項１－４，段落［００１７］－［００２９］，［００３１］－［００４２］，図２，３ & US 2015/0124279 A1，段落［００２２］－［００３４］，［００３６］－［００４７］，図２Ａ－３Ｂ & CN 104639782 A	6，9，12