(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3月28日(28.03.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/059148 A1

(51) 国際特許分類:
G06F 21/57 (2013.01)　*G06F 9/4401* (2018.01)

(21) 国際出願番号：　PCT/JP2018/034355

(22) 国際出願日：　2018年9月18日(18.09.2018)

(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 2017-180250　2017年9月20日(20.09.2017)　JP

(71) 出願人：ＮＥＣプラットフォームズ株式会社 **(NEC PLATFORMS, LTD.)** [JP/JP]；〒2138511 神奈川県川崎市高津区北見方二丁目６番１号 Kanagawa (JP).

(72) 発明者：神藤 雅弘**(JINDO Masahiro)**；〒2138511 神奈川県川崎市高津区北見方二丁目６番１号ＮＥＣプラットフォームズ株式会社内 Kanagawa (JP).

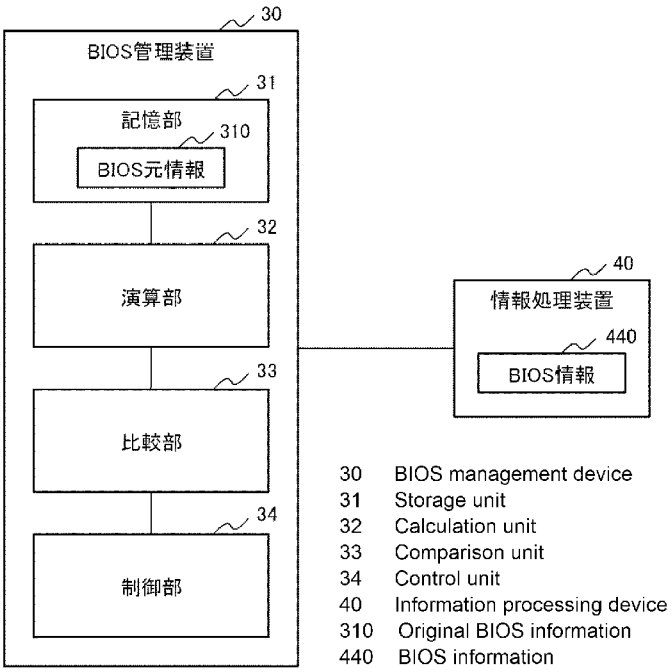
(74) 代理人：下坂　直樹 **(SHIMOSAKA Naoki)**；〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(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, 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, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

WO 2019/059148 A1

(54) Title: BIOS MANAGEMENT DEVICE, BIOS MANAGEMENT SYSTEM, BIOS MANAGEMENT METHOD, AND BIOS MANAGEMENT PROGRAM-STORED RECORDING MEDIUM

(54) 発明の名称：ＢＩＯＳ管理装置、ＢＩＯＳ管理システム、ＢＩＯＳ管理方法、及び、ＢＩＯＳ管理プログラムが格納された記録媒体



(57) Abstract: This BIOS management device 30 raises robustness against an unauthorized alteration of a BIOS by being provided with: a storage unit 31 which stores original BIOS information 310 used as original information of BIOS information 440 when the BIOS information 440 referred to by an information processing device 40 is stored in the information

［続葉有］

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))

processing device 40; a calculation unit 32 which executes different calculation processes on the BIOS information 440 and the original BIOS information 310, every time the information processing device 40 is activated; a comparison unit 33 which compares a first result obtained by executing the calculation process on the BIOS information 440 with a second result obtained by executing the calculation process on the original BIOS information 310; and a control unit 34 which controls the information processing device 40 to finish the activation by using the BIOS information 440, when the first result matches the second result.

(57) 要約:ＢＩＯＳ管理装置３０は、情報処理装置４０が参照するＢＩＯＳ情報４４０が、情報処理装置４０に格納された際にＢＩＯＳ情報４４０の元情報として使用されたＢＩＯＳ元情報３１０を記憶している記憶部３１と、情報処理装置４０が起動する度に異なる演算処理を、ＢＩＯＳ情報４４０とＢＩＯＳ元情報３１０とに対して実行する演算部３２と、ＢＩＯＳ情報４４０に対して当該演算処理が実行された第一の結果と、ＢＩＯＳ元情報３１０に対して当該演算処理が実行された第二の結果と、を比較する比較部３３と、当該第一及び第二の結果が一致する場合に、ＢＩＯＳ情報４４０を実行することによって起動を完了するように情報処理装置４０を制御する制御部３４と、を備えることによって、ＢＩＯＳの不正な改ざんに対する堅牢性を高める。

明　細　書

発明の名称 ：

ＢＩＯＳ管理装置、ＢＩＯＳ管理システム、ＢＩＯＳ管理方法、及び、ＢＩＯＳ管理プログラムが格納された記録媒体

技術分野

[0001] 本願発明は、ＢＩＯＳ（Basic Input Output System）の正当性を検証する技術に関する。

背景技術

[0002] サーバ装置等の情報処理装置を起動し、起動中及び起動後におけるその動作全般を制御するプログラムであるＢＩＯＳが、マルウェア等によって不正に改ざんされた場合、ユーザが知らないうちに機密情報が漏えいするなど、重大なセキュリティ問題が発生する可能性がある。したがって、ＢＩＯＳを不正な改ざんから保護するとともに、情報処理装置が起動する際に使用するＢＩＯＳの正当性を保証する技術への期待が高まってきている。

[0003] このような技術に関連する技術として、特許文献１には、安全なブートプロセスを介して、サーバまたはパーソナルコンピュータに記憶された情報を保護するシステムが開示されている。このシステムは、情報の処理及び記憶に関してプロセッサから分離されたコントローラを有し、当該コントローラは暗号化サービスモジュールを有する。このシステムは、ファームウェアの正当性を検証するために、当該コントローラと当該プロセッサとの間で暗号化情報を通信する。

[0004] また、特許文献２には、外部デバイスからの入力修正コマンドを検証した後に、内部ＢＩＯＳデータを修正する許可を与えるＢＩＯＳチップが開示されている。このＢＩＯＳチップは、内部ＢＩＯＳデータを保持する第１フラッシュメモリユニットと、セキュリティデータを保持する第２フラッシュメモリユニットと、当該外部装置、第１フラッシュメモリユニット、及び、第２フラッシュメモリユニットに接続された集積コード管理装置とを備える。

この集積コード管理装置は、修正コマンドを受信し、セキュリティデータを第２フラッシュメモリユニットに保存する。当該集積コード管理装置は、セキュリティデータを暗号化した暗号化データを生成し、その暗号化データを、復号を行う外部装置に送信する。そして、このＢＩＯＳチップは、外部装置によって復号された復号データを、元のセキュリティデータと比較するために集積コード管理装置へ返信する。そして、このＢＩＯＳチップは、復号データとセキュリティデータとが一致する場合に、内部ＢＩＯＳデータが、外部装置から提供されるデータに置き換えられることを許可する。

[0005] また、特許文献３には、ＢＩＯＳを実行して起動するときに、チェックサムエラーを検出する情報処理端末が開示されている。この情報処理端末は、当該チェックサムエラーを検出した場合に、自動的にＢＩＯＳの設定を初期化し、その初期化が終了した場合に、自動的にＢＩＯＳを再実行することによって再起動する。

先行技術文献

特許文献

[0006] 特許文献1：特開2011-243231号公報

特許文献2：特開2002-55725号公報

特許文献3：特開2011-81617号公報

発明の概要

発明が解決しようとする課題

[0007] 情報処理装置が起動する際に使用するＢＩＯＳの正当性を保証するために、例えば、起動時に、マスクＲＯＭ（Read Only Memory）等に格納されているチェック用プログラムによって、ＢＩＯＳの正当性をチェックすることが行なわれている。あるいは、セキュリティチェック用の専用ハードウェアであるＴＰＭ（Trusted Platform Module）を搭載し、ＴＰＭの中に格納された、正当なＢＩＯＳから求められたハッシュ値を用いて、ＢＩＯＳの正当性をチェックすることなども行なわれている。

[0008] しかしながら、高度な改ざん機能を備えたマルウェア等は、例えば、上述したチェックに用いられるデータを、改ざん後のＢＩＯＳから求められるデータではなく、正当なＢＩＯＳから求められる値に擬装することなどによって、チェックを巧妙にすり抜ける場合がある。したがって、このような高度な改ざん機能を備えたマルウェアからＢＩＯＳを保護することができるように、ＢＩＯＳの不正な改ざんに対する堅牢性を高めることが課題である。特許文献１乃至３が示す技術は、このような課題を解決するのに、十分であるとは言えない。本願発明の主たる目的は、この問題を解決するＢＩＯＳ管理装置等を提供することである。

課題を解決するための手段

[0009] 本願発明の一態様に係るＢＩＯＳ管理装置は、情報処理装置が参照するＢＩＯＳ（Basic Input Output System）情報が、前記情報処理装置に格納された際に前記ＢＩＯＳ情報の元情報として使用されたＢＩＯＳ元情報を記憶している記憶手段と、前記情報処理装置が起動する度に異なる演算処理を、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して実行する演算手段と、前記ＢＩＯＳ情報に対して前記演算処理が実行された第一の結果と、前記ＢＩＯＳ元情報に対して前記演算処理が実行された第二の結果と、を比較する比較手段と、前記第一及び第二の結果が一致する場合に、前記ＢＩＯＳ情報を実行することによって起動を完了するように前記情報処理装置を制御する制御手段と、を備える。

[0010] 上記目的を達成する他の見地において、本願発明の一態様に係るＢＩＯＳ管理方法は、第一の情報処理装置が参照するＢＩＯＳ情報が前記第一の情報処理装置に格納された際に、前記ＢＩＯＳ情報の元情報として使用されたＢＩＯＳ元情報が記憶手段に記憶されている場合に、第二の情報処理装置によって、前記第一の情報処理装置が起動する度に異なる演算処理を、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して実行し、前記ＢＩＯＳ情報に対して前記演算処理が実行された第一の結果と、前記ＢＩＯＳ元情報に対して前記演算処理が実行された第二の結果と、を比較し、前記第一及び第二の結果

が一致する場合に、前記ＢＩＯＳ情報を実行することによって起動を完了するように前記第一の情報処理装置を制御する。

[0011] また、上記目的を達成する更なる見地において、本願発明の一態様に係るＢＩＯＳ管理プログラムは、情報処理装置が参照するＢＩＯＳ情報が、前記情報処理装置に格納された際に前記ＢＩＯＳ情報の元情報として使用されたＢＩＯＳ元情報を記憶している記憶手段にアクセス可能なコンピュータに、前記情報処理装置が起動する度に異なる演算処理を、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して実行する演算機能と、前記ＢＩＯＳ情報に対して前記演算処理が実行された第一の結果と、前記ＢＩＯＳ元情報に対して前記演算処理が実行された第二の結果と、を比較する比較機能と、前記第一及び第二の結果が一致する場合に、前記ＢＩＯＳ情報を実行することによって起動を完了するように前記情報処理装置を制御する制御機能と、をコンピュータに実行させるためのプログラムである。

[0012] 更に、本願発明は、係るＢＩＯＳ管理プログラム（コンピュータプログラム）が格納された、コンピュータ読み取り可能な、不揮発性の記録媒体によっても実現可能である。

発明の効果

[0013] 本願発明は、ＢＩＯＳの不正な改ざんに対する堅牢性を高めることを可能とする。

図面の簡単な説明

[0014] [図1]本願発明の第１の実施形態に係るＢＩＯＳ管理システム１の構成を概念的に示すブロック図である。

[図2A]本願発明の第１の実施形態に係るＢＩＯＳ管理システム１の動作を示すフローチャート（１／２）である。

[図2B]本願発明の第１の実施形態に係るＢＩＯＳ管理システム１の動作を示すフローチャート（２／２）である。

[図3]本願発明の第２の実施形態に係るＢＩＯＳ管理装置３０の構成を概念的に示すブロック図である。

[図4]本願発明の各実施形態に係るＢＩＯＳ管理装置を実行可能な情報処理装置９００の構成を示すブロック図である。

発明を実施するための形態

[0015] 以下、本願発明の実施の形態について図面を参照して詳細に説明する。

[0016] ＜第１の実施形態＞

図１は、本願発明の第１の実施の形態に係るＢＩＯＳ管理システム１の構成を概念的に示すブロック図である。ＢＩＯＳ管理システム１は、大別して、ＢＩＯＳ管理装置１０、及び、本体系装置（情報処理装置）２０を有している。ＢＩＯＳ管理システム１は、例えば、１つのサーバ装置として構成されてもよい。

[0017] 本体系装置２０は、様々なアプリケーション（ソフトウェア）を実行することによって、様々なサービスを提供する装置である。本体系装置２０は、ＣＰＵ（Central Processing Unit）２１、主記憶２２、Ｉ／Ｏ（Input / Output）制御部（チップセット）２３、及び、ＢＩＯＳ－ＲＯＭ２４を備える。ＣＰＵ２１は、ＢＩＯＳ管理システム１の電源がオンされたときに、ＢＩＯＳ－ＲＯＭ２４に格納されているＢＩＯＳ情報２４０を、Ｉ／Ｏ制御部２３を介して読み出す。そしてＣＰＵ２１は、読み出したＢＩＯＳ情報２４０を参照及び実行することによって、本体系装置２０を起動する処理を行う。尚、ＢＩＯＳ－ＲＯＭ２４は、例えば、書き換え可能であって不揮発性を有するメモリであるフラッシュＲＯＭである。

[0018] ＢＩＯＳ管理装置（ＢＭＣ：Baseboard Management Controller）１０は、本体系装置２０に対して、動作環境や障害処理などに関する制御を行なう。ＢＩＯＳ管理装置１０は、ＢＩＯＳ管理システム１の電源オン／オフに伴い、ＢＩＯＳ情報２４０の実行開始／実行中止を制御する機能を備える。ＢＩＯＳ管理装置１０は、また、ユーザがコンソール端末（不図示）を使用して、ＢＩＯＳ管理システム１の状態を監視する際に、当該コンソール端末との間における情報の入出力を制御する機能を備える。ＢＩＯＳ管理装置１０は、また、ＢＩＯＳ情報２４０をＢＩＯＳ－ＲＯＭ２４へ格納する（ＢＩＯＳ

情報２４０を更新する）ことを制御する機能を備える。

[0019] ＢＩＯＳ管理装置１０は、記憶部１１、演算部１２、比較部１３、及び、制御部１４を備える。記憶部１１における記憶制御機能、演算部１２、比較部１３、及び、制御部１４は、図４を参照してＢＩＯＳ管理装置１０のハードウェア構成例に関して後述するように、例えば、ＢＩＯＳ管理装置１０の機能を実現するＢＭＣファームウェアに実装されてもよい。

[0020] 記憶部１１は、不揮発メモリ等の、不揮発性を有する記憶デバイスである。記憶部１１には、ＢＩＯＳ元情報１１０が格納されている。ＢＩＯＳ元情報１１０は、ＢＩＯＳ情報２４０として、本体系装置２０におけるＢＩＯＳ－ＲＯＭ２４へ格納される元情報である。

[0021] ＢＩＯＳ管理装置１０は、例えば、図４に示す入出力インタフェース９０９を介して、通信ネットワークに接続された外部の装置からＢＩＯＳ元情報１１０を取得する。記憶部１１は、あるいは、図４に示す記録媒体（アップデート媒体）９０７を介して、ＢＩＯＳ元情報１１０を取得する。尚、記録媒体９０７は、ＢＩＯＳ元情報１１０が格納された記憶領域の他、ＢＩＯＳ元情報１１０に関する付属情報等が格納されたヘッダ領域を含んでいる。

[0022] 演算部１２は、ＢＩＯＳ管理システム１の電源がオンされることによって本体系装置２０の起動が開始する度に異なる演算処理を、ＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに対して実行する機能を備える。

[0023] より具体的には、演算部１２は、例えば、本体系装置２０が起動した時間に基づく乱数を発生する。但し、演算部１２は、時計等の計時機能を有するデバイス（不図示）を備えることとする。そして、演算部１２は、生成した乱数を使用することによって、本体系装置２０の起動が開始する度に異なる暗号鍵１２０と復号鍵１２１とを生成する。暗号鍵１２０及び復号鍵１２１の生成については、例えばＲＳＡ（Rivest-Shamir-Adleman cryptosystem）等の既存の技術を使用可能であるので、本願では、その詳細な説明を省略する。

[0024] 演算部１２は、生成した暗号鍵１２０を用いて、記憶部１１に格納されて

いるＢＩＯＳ元情報１１０を暗号化する。演算部１２は、生成した暗号鍵１２０を本体系装置２０に送信し、暗号鍵１２０によりＢＩＯＳ－ＲＯＭ２４に格納されているＢＩＯＳ情報２４０を暗号化するように、本体系装置２０を制御する。演算部１２は、暗号鍵１２０により暗号化されたＢＩＯＳ元情報１１０とＢＩＯＳ情報２４０とを、生成した復号鍵１２１を用いて復号する。

[0025] 比較部１３は、演算部１２によってＢＩＯＳ情報２４０に関して復号された結果（第一の結果）と、演算部１２によってＢＩＯＳ元情報１１０に関して復号された結果（第二の結果）とが一致するか否かを確認する。比較部１３は、この比較結果を、制御部１４へ入力する。

[0026] 制御部１４は、比較部１３から入力された比較結果が、第一及び第二の結果が一致することを示す場合、ＢＩＯＳ－ＲＯＭ２４に格納されているＢＩＯＳ情報２４０は、マルウェア等による改ざんが行なわれていない正当なＢＩＯＳ情報であると判定する。この場合、制御部１４は、ＢＩＯＳ情報２４０を実行することによって起動を完了するように本体系装置２０を制御する。

[0027] 制御部１４は、比較部１３から入力された比較結果が、第一及び第二の結果が一致しないことを示す場合、ＢＩＯＳ－ＲＯＭ２４に格納されているＢＩＯＳ情報２４０は、マルウェア等による改ざんが行なわれた可能性がある不正なＢＩＯＳ情報であると判定する。この場合、制御部１４は、ＢＩＯＳ情報２４０による起動を中止するように本体系装置２０を制御する。

[0028] この場合、制御部１４は、改ざんが行なわれた可能性があるＢＩＯＳ情報２４０を、正当なＢＩＯＳ情報に更新し、更新したＢＩＯＳ情報２４０を実行することによって起動を完了するように本体系装置２０を制御するようにしてもよい。即ち、制御部１４は、ＢＩＯＳ－ＲＯＭ２４に格納されているＢＩＯＳ情報２４０を、記憶部１１に格納されているＢＩＯＳ元情報１１０に更新する。そして制御部１４は、ＢＩＯＳ元情報１１０に更新したＢＩＯＳ情報２４０を実行することによって起動を完了するように本体系装置２０

を制御する。

[0029] 次に、図２Ａ及び図２Ｂのフローチャートを参照して、本実施形態に係るＢＩＯＳ管理システム１の動作（処理）について詳細に説明する。

[0030] 例えばユーザによって、ＢＩＯＳ管理システム１の電源がオンされることにより、本体系装置２０の起動が開始する（ステップＳ１０１）。演算部１２は、本体系装置２０が起動した時間に基づく乱数を生成し、生成した乱数を使用することによって、暗号鍵１２０及び復号鍵１２１を生成する（ステップＳ１０２）。

[0031] 演算部１２は、本体系装置２０に生成した暗号鍵１２０を送信し、暗号鍵１２０によりＢＩＯＳ情報２４０を暗号化するように、本体系装置２０を制御する（ステップＳ１０３）。演算部１２は、暗号鍵１２０を使用して、ＢＩＯＳ元情報１１０を暗号化する（ステップＳ１０４）。

[0032] 所定の時間内に、演算部１２が、本体系装置２０から、ＢＩＯＳ情報２４０が暗号化された情報を入手しない場合（ステップＳ１０５でＮｏ）、処理はステップＳ１１０へ進む。所定の時間内に、演算部１２が、本体系装置２０から、ＢＩＯＳ情報２４０が暗号化された情報を入手した場合（ステップＳ１０５でＹｅｓ）、演算部１２は、暗号化されたＢＩＯＳ情報２４０、及び、暗号化されたＢＩＯＳ元情報１１０を、生成した復号鍵１２１により復号する（ステップＳ１０６）。

[0033] 比較部１３は、ＢＩＯＳ情報２４０に関して復号された結果（第一の結果）と、ＢＩＯＳ元情報１１０に関して復号された結果（第二の結果）とを比較する（ステップＳ１０７）。第一及び第二の結果が一致する場合（ステップＳ１０８でＹｅｓ）、制御部１４は、ＢＩＯＳ－ＲＯＭ２４に格納されているＢＩＯＳ情報２４０を実行することによって起動を完了するように、本体系装置２０を制御し（ステップＳ１０９）、全体の処理は終了する。

[0034] 第一及び第二の結果が一致しない場合（ステップＳ１０８でＮｏ）、制御部１４は、ＢＩＯＳ情報２４０を実行することによる、本体系装置２０の起動を中止する（ステップＳ１１０）。制御部１４は、ＢＩＯＳ－ＲＯＭ２４

に格納されているＢＩＯＳ情報２４０を、記憶部１１に格納されているＢＩＯＳ元情報１１０に更新する（ステップＳ１１１）。制御部１４は、ＢＩＯＳ元情報１１０に更新されたＢＩＯＳ情報２４０を実行することにより起動を完了するように、本体系装置２０を制御し（ステップＳ１１２）、全体の処理は終了する。

[0035] 本実施形態に係るＢＩＯＳ管理装置１０は、ＢＩＯＳの不正な改ざんに対する堅牢性を高めることができる。その理由は、ＢＩＯＳ管理装置１０は、本体系装置２０が起動する度に異なる演算処理を、ＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに対して実行し、その２つの演算処理の結果が一致する場合に、ＢＩＯＳ情報２４０を実行することによって起動を完了するように本体系装置２０を制御するからである。

[0036] 以下に、本実施形態に係るＢＩＯＳ管理装置１０によって実現される効果について、詳細に説明する。

[0037] 情報処理装置が起動する際に使用するＢＩＯＳの正当性を保証するために、例えば、起動時に、チェック用プログラムによって、ＢＩＯＳの正当性をチェックすることが行なわれている。あるいは、ＴＰＭを搭載し、ＴＰＭの中に格納された、正当なＢＩＯＳから求められたハッシュ値を用いて、ＢＩＯＳの正当性をチェックすることなども行なわれている。しかしながら、高度な改ざん機能を備えたマルウェア等は、例えば、上述したチェックに用いられるデータを、改ざん後のＢＩＯＳから求められるデータではなく、正当なＢＩＯＳから求められる値に擬装することなどによって、チェックを巧妙にすり抜ける場合がある。

[0038] 例えば、図１に示す例では、ＢＩＯＳ情報２４０がＢＩＯＳ元情報１１０と一致することをもって、ＢＩＯＳ情報２４０が不正に改ざんされていない正当なＢＩＯＳ情報であることを保証可能である。この場合、ＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とを単に比較するのみでは、ＢＩＯＳ情報２４０が正当なＢＩＯＳ情報であることを保証するのに十分であるとは言えない。なぜなら、ＢＩＯＳ情報２４０がＢＩＯＳ－ＲＯＭ２４から読み出され

る際に、ＢＩＯＳ情報２４０を不正に改ざんしたマルウェアは、ＢＩＯＳ情報２４０が改ざんされる前の状態でＢＩＯＳ－ＲＯＭ２４から読み出されるように擬装する可能性があるからである。

[0039] また、ＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに対して所定の演算処理（例えば暗号化処理及び復号処理等）を行うことによって、ＢＩＯＳ情報２４０を不正に改ざんしたマルウェアが上述したような擬装を行いにくくすることができる。しかしながら、その演算処理の内容が固定されている場合、マルウェアは、当該演算処理に対応した擬装を行なう可能性がある。したがって、このような高度な改ざん機能や擬装機能を備えたマルウェアからＢＩＯＳを保護することができるように、ＢＩＯＳの不正な改ざんに対する堅牢性を高めることが課題である。

[0040] このような課題に対して、本実施形態に係るＢＩＯＳ管理装置１０は、記憶部１１と、演算部１２と、比較部１３と、制御部１４と、を備え、例えば図１乃至図３を参照して上述した通り動作する。即ち、記憶部１１は、本体系装置（情報処理装置）２０が参照するＢＩＯＳ情報２４０が、本体系装置２０に格納された際にＢＩＯＳ情報２４０の元情報として使用されたＢＩＯＳ元情報１１０を記憶している。演算部１２は、本体系装置２０が起動する度に異なる演算処理（例えば暗号化処理及び復号処理）を、ＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに対して実行する。比較部１３は、ＢＩＯＳ情報２４０に対して当該演算処理が実行された第一の結果と、ＢＩＯＳ元情報１１０に対して演算処理が実行された第二の結果と、を比較する。そして、制御部１４は、当該第一及び第二の結果が一致する場合に、ＢＩＯＳ情報２４０を実行することによって起動を完了するように本体系装置２０を制御する。

[0041] 即ち、本実施形態に係るＢＩＯＳ管理装置１０がＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに対して行なう演算処理の内容は、本体系装置２０が起動する度に異なる。このため、ＢＩＯＳ情報２４０を不正に改ざんしたマルウェアが、このように毎回異なる演算処理に対応した擬装を行なうことは

、非常に困難となる。したがって、本実施形態に係るＢＩＯＳ管理装置１０は、ＢＩＯＳの不正な改ざんに対する堅牢性を高めることができる。

[0042] また、本実施形態に係る演算部１２がＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに対して実行する演算処理は、暗号化処理及び復号処理に限定されない。演算部１２は、例えば、本体系装置２０が起動する度に異なるハッシュ関数を、本体系装置２０が起動した時間に基づく乱数を使用して生成する。そして演算部１２は、生成したハッシュ関数を使用して、ＢＩＯＳ情報２４０とＢＩＯＳ元情報１１０とに関するハッシュ値を求めてもよい。

[0043] また、本実施形態に係るＢＩＯＳ管理装置１０は、ＢＩＯＳ情報２４０が不正に改ざんされていることを検出した場合、ＢＩＯＳ情報２４０を実行することによる、本体系装置２０の起動を中止する。ＢＩＯＳ管理装置１０は、こののち、改ざんされたＢＩＯＳ情報２４０を、ＢＩＯＳ元情報１１０に更新し、更新されたＢＩＯＳ情報２４０を実行することにより起動を完了するように、本体系装置２０を制御可能である。したがって、本実施形態に係るＢＩＯＳ管理装置１０は、改ざんされたＢＩＯＳ情報２４０を復旧する作業を自動で行なうので、ユーザの負担を軽減するとともに、復旧に要する時間を短縮することができる。

[0044] ＜第２の実施形態＞

図３は、本願発明の第２の実施形態に係るＢＩＯＳ管理装置３０の構成を概念的に示すブロック図である。

[0045] 実施形態に係るＢＩＯＳ管理装置３０は、記憶部３１、演算部３２、比較部３３、及び、制御部３４を備えている。

[0046] 記憶部３１は、情報処理装置が参照するＢＩＯＳ情報４４０が、情報処理装置４０に格納された際にＢＩＯＳ情報４４０の元情報として使用されたＢＩＯＳ元情報３１０を記憶している。

[0047] 演算部３２は、情報処理装置４０が起動する度に異なる演算処理を、ＢＩＯＳ情報４４０とＢＩＯＳ元情報３１０とに対して実行する。

[0048] 比較部３３は、ＢＩＯＳ情報４４０に対して当該演算処理が実行された第

一の結果と、ＢＩＯＳ元情報３１０に対して当該演算処理が実行された第二の結果と、を比較する。

[0049] 制御部３４は、当該第一及び第二の結果が一致する場合に、ＢＩＯＳ情報４４０を実行することによって起動を完了するように情報処理装置４０を制御する。

[0050] 本実施形態に係るＢＩＯＳ管理装置３０は、ＢＩＯＳの不正な改ざんに対する堅牢性を高めることができる。その理由は、ＢＩＯＳ管理装置３０は、情報処理装置４０が起動する度に異なる演算処理を、ＢＩＯＳ情報４４０とＢＩＯＳ元情報３１０とに対して実行し、その２つの演算処理の結果が一致する場合に、ＢＩＯＳ情報４４０を実行することによって起動を完了するように情報処理装置４０を制御するからである。

[0051] ＜ハードウェア構成例＞

上述した各実施形態において図１、及び、図３に示したＢＩＯＳ管理装置における各部は、専用のＨＷ（ＨａｒｄＷａｒｅ）（電子回路）によって実現することができる。また、図１、及び、図３において、少なくとも、下記構成は、ソフトウェアプログラムの機能（処理）単位（ソフトウェアモジュール）と捉えることができる。

・記憶部１１、及び、３１における記憶制御機能、

・演算部１２、及び、３２、

・比較部１３、及び、３３、

・制御部１４、及び、３４。

[0052] 但し、これらの図面に示した各部の区分けは、説明の便宜上の構成であり、実装に際しては、様々な構成が想定され得る。この場合のハードウェア環境の一例を、図４を参照して説明する。

[0053] 図４は、本願発明の各実施形態に係るＢＩＯＳ管理装置を実行可能な情報処理装置９００（コンピュータ）の構成を例示的に説明する図である。即ち、図４は、図１、及び、図３に示したＢＩＯＳ管理装置を実現可能なコンピュータ（情報処理装置）の構成であって、上述した実施形態における各機能

を実現可能なハードウェア環境を表す。

[0054] 図４に示した情報処理装置９００は、構成要素として下記を備えている。

・ＣＰＵ（Ｃｅｎｔｒａｌ＿Ｐｒｏｃｅｓｓｉｎｇ＿Ｕｎｉｔ）９０１、

・ＲＯＭ（Ｒｅａｄ＿Ｏｎｌｙ＿Ｍｅｍｏｒｙ）９０２、

・ＲＡＭ（Ｒａｎｄｏｍ＿Ａｃｃｅｓｓ＿Ｍｅｍｏｒｙ）９０３、

・ハードディスク（記憶装置）９０４、

・外部装置との通信インタフェース９０５、

・バス９０６（通信線）、

・ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ＿Ｄｉｓｃ＿Ｒｅａｄ＿Ｏｎｌｙ＿Ｍｅｍｏｒｙ）等の記録媒体９０７に格納されたデータを読み書き可能なリーダライタ９０８、

・入出力インタフェース９０９。

[0055] 即ち、上記構成要素を備える情報処理装置９００は、これらの構成がバス９０６を介して接続された一般的なコンピュータである。情報処理装置９００は、ＣＰＵ９０１を複数備える場合もあれば、マルチコアにより構成されたＣＰＵ９０１を備える場合もある。

[0056] そして、上述した実施形態を例に説明した本願発明は、図４に示した情報処理装置９００に対して、次の機能を実現可能なコンピュータプログラムを供給する。その機能とは、その実施形態の説明において参照したブロック構成図（図１、及び、図３）における上述した構成、或いはフローチャート（図２Ａ及び図２Ｂ）の機能である。本願発明は、その後、そのコンピュータプログラムを、当該ハードウェアのＣＰＵ９０１に読み出して解釈し実行することによって達成される。また、当該装置内に供給されたコンピュータプログラムは、読み書き可能な揮発性のメモリ（ＲＡＭ９０３）、または、ＲＯＭ９０２やハードディスク９０４等の不揮発性の記憶デバイスに格納すれば良い。

[0057] また、前記の場合において、当該ハードウェア内へのコンピュータプログラムの供給方法は、現在では一般的な手順を採用することができる。その手

順としては、例えば、ＣＤ－ＲＯＭ等の各種記録媒体９０７を介して当該装置内にインストールする方法や、インターネット等の通信回線を介して外部よりダウンロードする方法等がある。そして、このような場合において、本願発明は、係るコンピュータプログラムを構成するコード或いは、そのコードが格納された記録媒体９０７によって構成されると捉えることができる。

[0058] 以上、上述した実施形態を模範的な例として本願発明を説明した。しかしながら、本願発明は、上述した実施形態には限定されない。即ち、本願発明は、本願発明のスコープ内において、当業者が理解し得る様々な態様を適用することができる。

[0059] この出願は、２０１７年９月２０日に出願された日本出願特願２０１７－１８０２５０を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0060] １　ＢＩＯＳ管理システム
１０　ＢＩＯＳ管理装置
１１　記憶部
１１０　ＢＩＯＳ元情報
１２　演算部
１２０　暗号鍵
１２１　復号鍵
１３　比較部
１４　制御部
２０　本体系装置
２１　ＣＰＵ
２２　主記憶
２３　Ｉ／Ｏ制御部
２４　ＢＩＯＳ－ＲＯＭ
２４０　ＢＩＯＳ情報

３０　ＢＩＯＳ管理装置

３１　記憶部

３１０　ＢＩＯＳ元情報

３２　演算部

３３　比較部

３４　制御部

４０　情報処理装置

４４０　ＢＩＯＳ情報

９００　情報処理装置

９０１　ＣＰＵ

９０２　ＲＯＭ

９０３　ＲＡＭ

９０４　ハードディスク（記憶装置）

９０５　通信インタフェース

９０６　バス

９０７　記録媒体

９０８　リーダライタ

９０９　入出力インタフェース

請求の範囲

[請求項1] 情報処理装置が参照するＢＩＯＳ（Basic Input Output System）情報が、前記情報処理装置に格納された際に前記ＢＩＯＳ情報の元情報として使用されたＢＩＯＳ元情報を記憶している記憶手段と、

前記情報処理装置が起動する度に異なる演算処理を、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して実行する演算手段と、

前記ＢＩＯＳ情報に対して前記演算処理が実行された第一の結果と、前記ＢＩＯＳ元情報に対して前記演算処理が実行された第二の結果と、を比較する比較手段と、

前記第一及び第二の結果が一致する場合に、前記ＢＩＯＳ情報を実行することによって起動を完了するように前記情報処理装置を制御する制御手段と、

を備えるＢＩＯＳ管理装置。

[請求項2] 前記演算手段は、前記情報処理装置が起動する度に異なる暗号鍵及び復号鍵を生成したのち、生成した前記暗号鍵を使用して、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して暗号化を実行し、暗号化した前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して前記復号鍵を使用して復号を実行する、

請求項１に記載のＢＩＯＳ管理装置。

[請求項3] 前記演算手段は、前記情報処理装置が起動する度に異なるハッシュ関数を生成したのち、生成した前記ハッシュ関数を使用して、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに関するハッシュ値を求める、

請求項１に記載のＢＩＯＳ管理装置。

[請求項4] 前記演算手段は、前記情報処理装置が起動した時間に基づく乱数を生成し、生成した前記乱数を使用した前記演算処理を実行する、

請求項１乃至請求項３のいずれか一項に記載のＢＩＯＳ管理装置。

[請求項5] 前記制御手段は、前記第一及び第二の結果が一致しない場合、前記情報処理装置の起動を中止する、

請求項１乃至請求項４のいずれか一項に記載のＢＩＯＳ管理装置。

[請求項6] 前記制御手段は、前記第一及び第二の結果が一致しない場合、前記ＢＩＯＳ情報を、前記記憶手段に記憶されている前記ＢＩＯＳ元情報に更新したのち、更新された前記ＢＩＯＳ情報を実行するように前記情報処理装置を制御する、

請求項１乃至請求項４のいずれか一項に記載のＢＩＯＳ管理装置。

[請求項7] 請求項１乃至請求項６のいずれか一項に記載のＢＩＯＳ管理装置と、

前記情報処理装置と、

を含むＢＩＯＳ管理システム。

[請求項8] 前記演算手段は、前記ＢＩＯＳ情報に対して前記演算処理を実行するように、前記情報処理装置を制御し、

前記情報処理装置は、前記演算処理を実行することによって得られた結果を、前記演算手段に入力する、

請求項７に記載のＢＩＯＳ管理システム。

[請求項9] 第一の情報処理装置が参照するＢＩＯＳ情報が前記第一の情報処理装置に格納された際に、前記ＢＩＯＳ情報の元情報として使用されたＢＩＯＳ元情報が記憶手段に記憶されている場合に、

第二の情報処理装置によって、

前記第一の情報処理装置が起動する度に異なる演算処理を、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して実行し、

前記ＢＩＯＳ情報に対して前記演算処理が実行された第一の結果と、前記ＢＩＯＳ元情報に対して前記演算処理が実行された第二の結果と、を比較し、

前記第一及び第二の結果が一致する場合に、前記ＢＩＯＳ情報を実行することによって起動を完了するように前記第一の情報処理装置を制御する、

ＢＩＯＳ管理方法。

[請求項10] 情報処理装置が参照するＢＩＯＳ情報が、前記情報処理装置に格納された際に前記ＢＩＯＳ情報の元情報として使用されたＢＩＯＳ元情報を記憶している記憶手段にアクセス可能なコンピュータに、

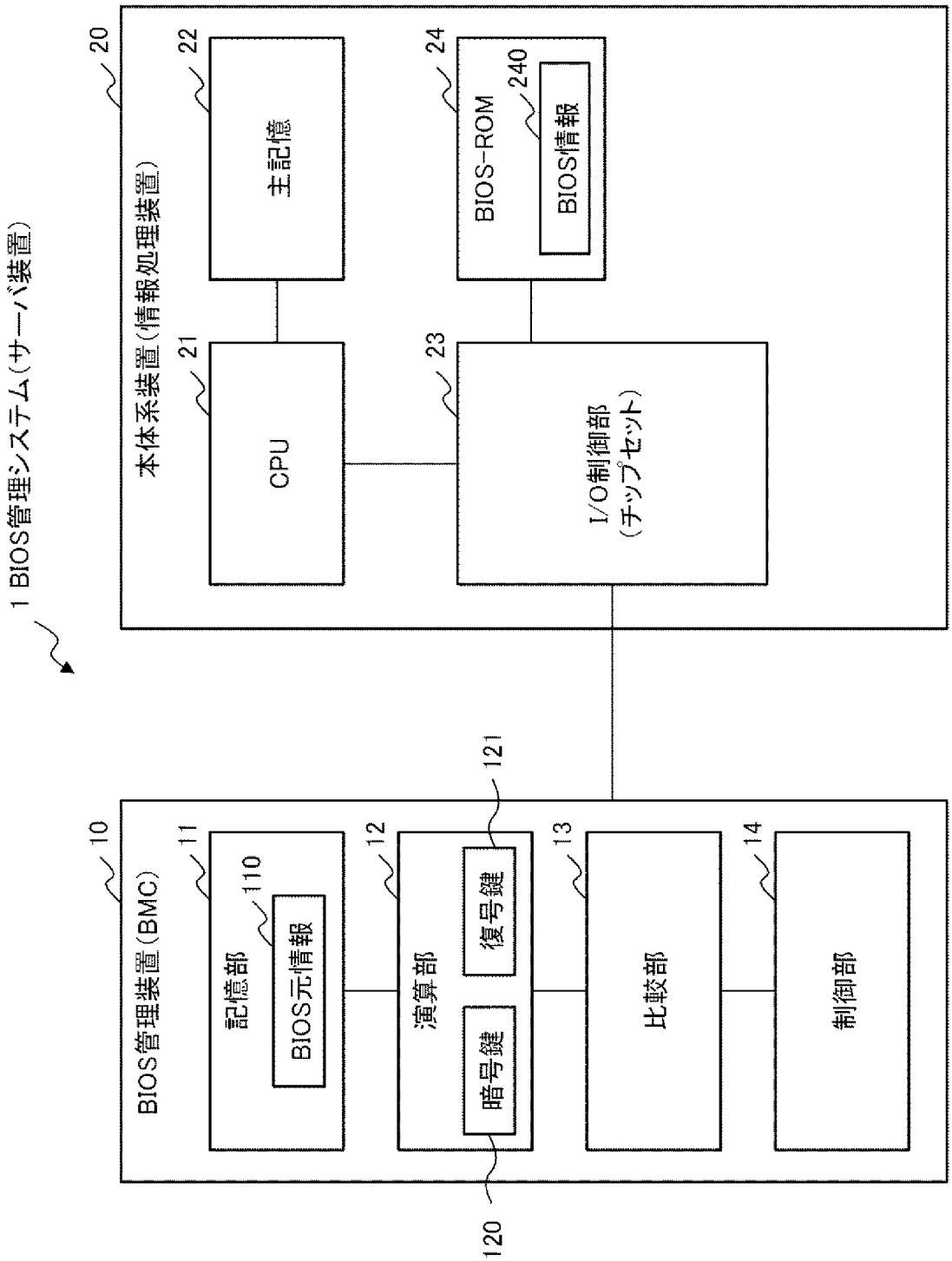
前記情報処理装置が起動する度に異なる演算処理を、前記ＢＩＯＳ情報と前記ＢＩＯＳ元情報とに対して実行する演算機能と、

前記ＢＩＯＳ情報に対して前記演算処理が実行された第一の結果と、前記ＢＩＯＳ元情報に対して前記演算処理が実行された第二の結果と、を比較する比較機能と、

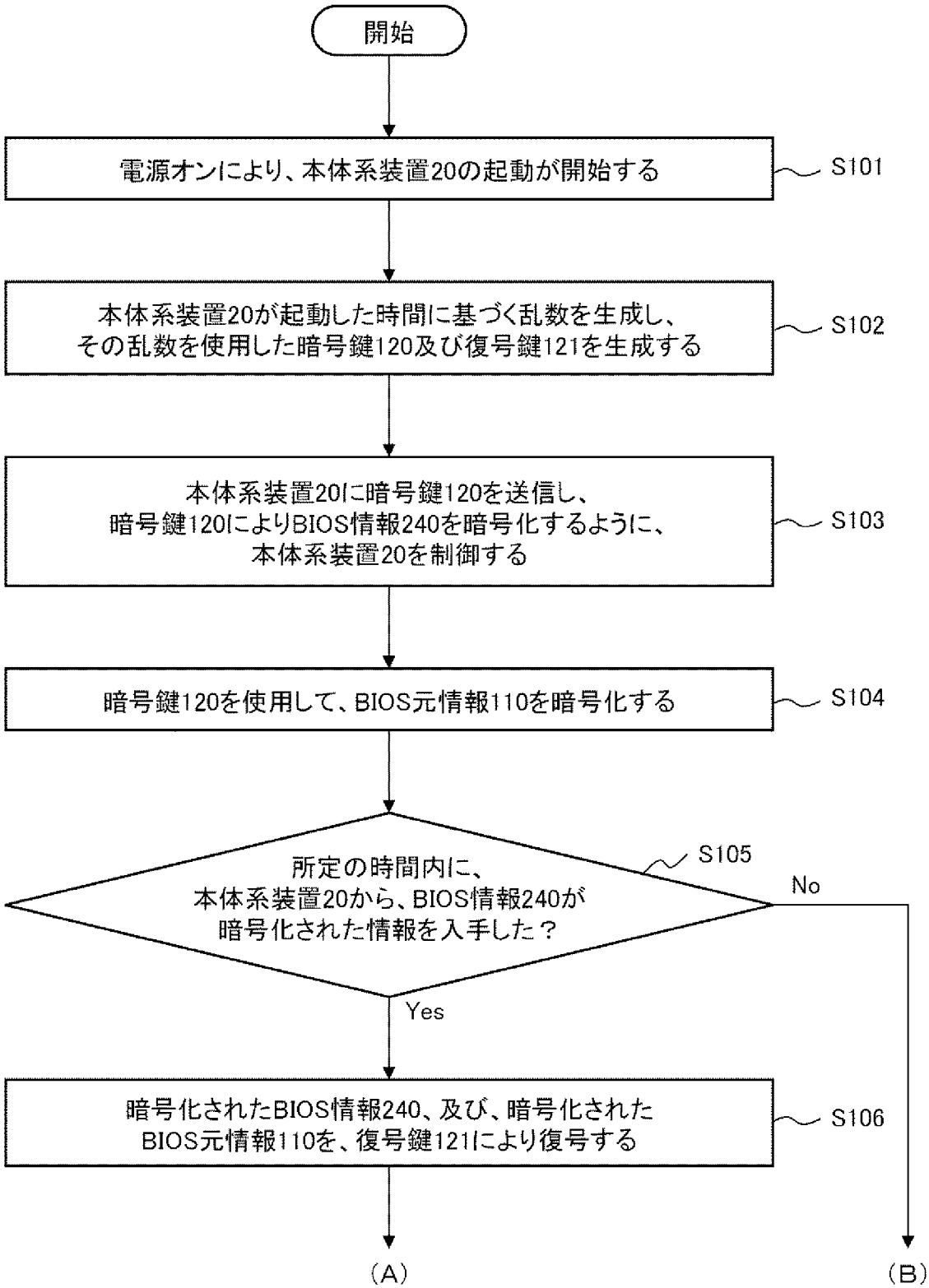
前記第一及び第二の結果が一致する場合に、前記ＢＩＯＳ情報を実行することによって起動を完了するように前記情報処理装置を制御する制御機能と、

を実現させるためのＢＩＯＳ管理プログラムが格納された記録媒体。

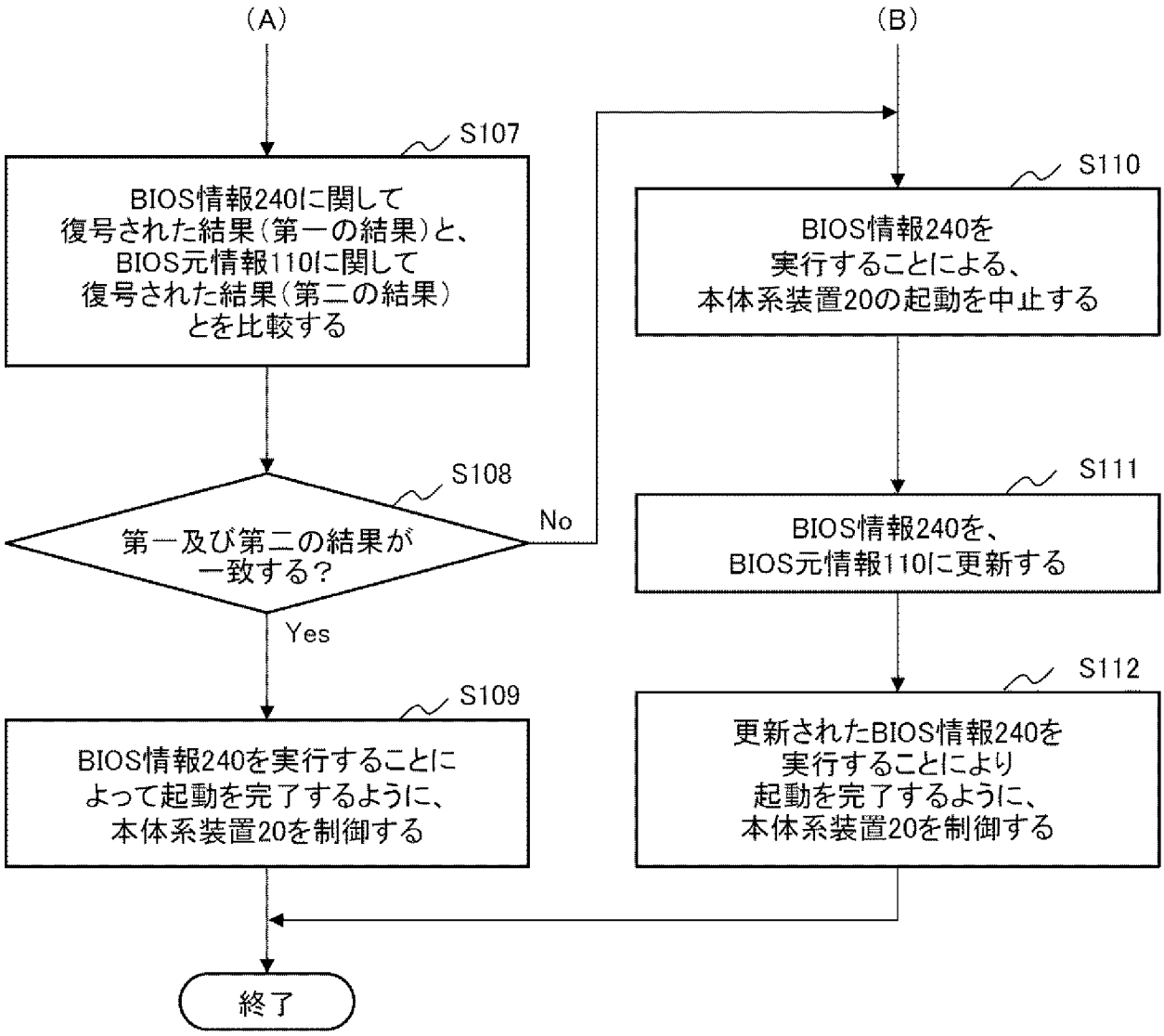
[図1]


1 BIOS管理システム（サーバ装置）
20
本体系装置（情報処理装置）
22
主記憶
24
BIOS-ROM
240
BIOS情報
21
CPU
23
I/O制御部
（チップセット）
121
10
BIOS管理装置（BMC）
11
記憶部
110
BIOS元情報
12
演算部
復号鍵
暗号鍵
13
比較部
14
制御部
120

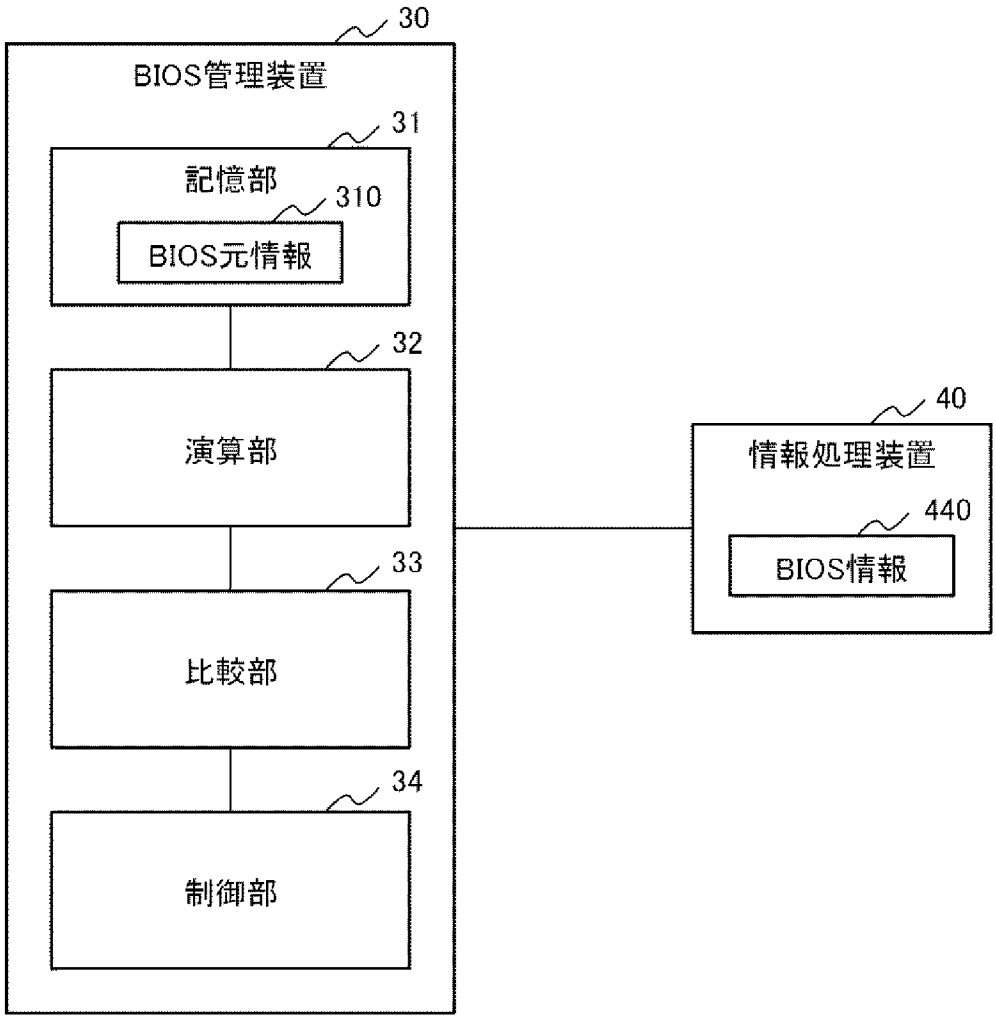
[図2A]


開始
電源オンにより、本体系装置20の起動が開始する
S101
本体系装置20が起動した時間に基づく乱数を生成し、
その乱数を使用した暗号鍵120及び復号鍵121を生成する
S102
本体系装置20に暗号鍵120を送信し、
暗号鍵120によりBIOS情報240を暗号化するように、
本体系装置20を制御する
S103
暗号鍵120を使用して、BIOS元情報110を暗号化する
S104
所定の時間内に、
本体系装置20から、BIOS情報240が
暗号化された情報を入手した？
S105
No
Yes
暗号化されたBIOS情報240、及び、暗号化された
BIOS元情報110を、復号鍵121により復号する
S106
(A)
(B)

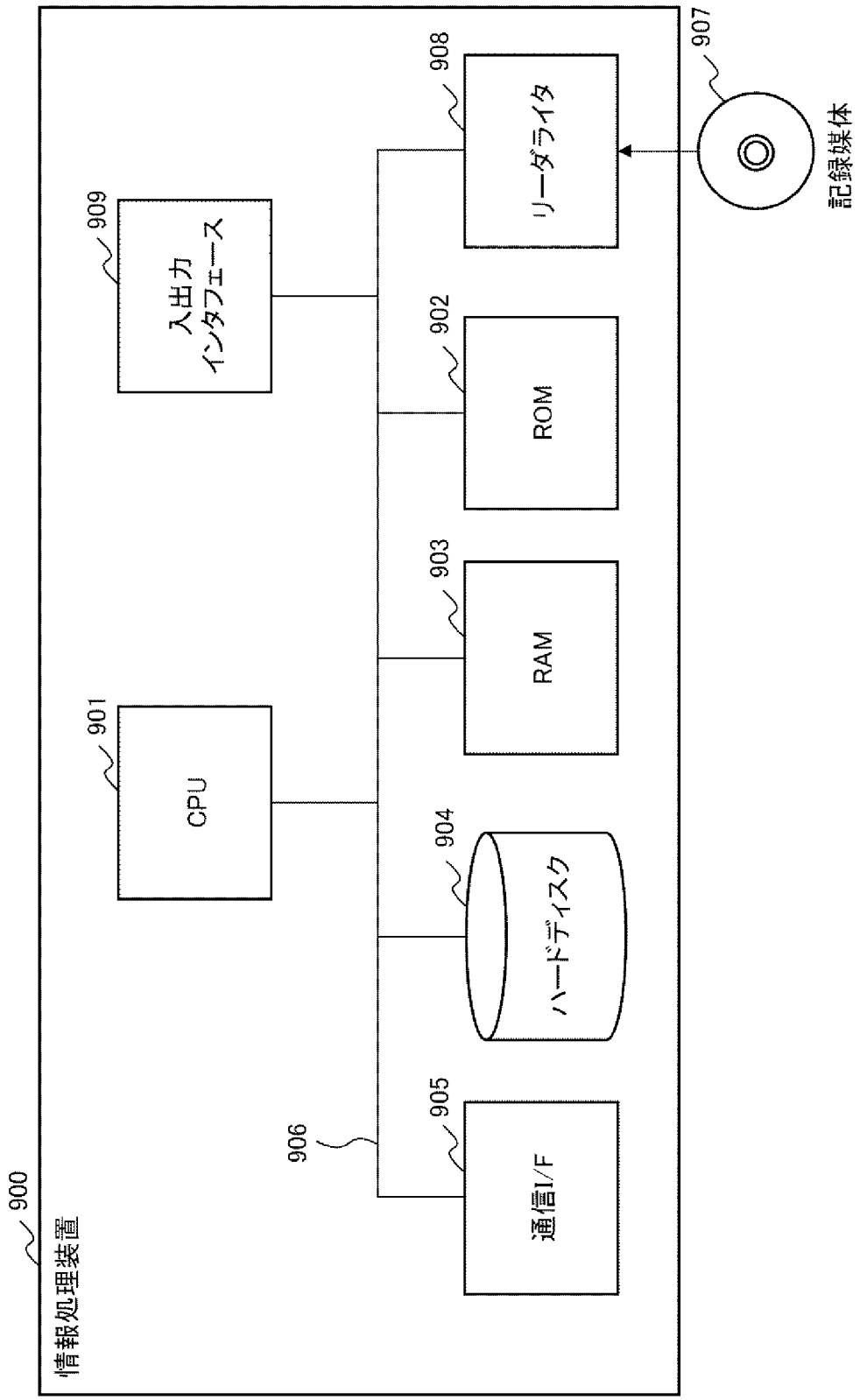
[図2B]


(A)
(B)
S107
BIOS情報240に関して
復号された結果(第一の結果)と、
BIOS元情報110に関して
復号された結果(第二の結果)
とを比較する
S108
第一及び第二の結果が
一致する?
No
Yes
S109
BIOS情報240を実行することに
よって起動を完了するように、
本体系装置20を制御する
S110
BIOS情報240を
実行することによる、
本体系装置20の起動を中止する
S111
BIOS情報240を、
BIOS元情報110に更新する
S112
更新されたBIOS情報240を
実行することにより
起動を完了するように、
本体系装置20を制御する
終了

[図3]


30
BIOS管理装置
31
記憶部
310
BIOS元情報
32
演算部
33
比較部
34
制御部
40
情報処理装置
440
BIOS情報

[図4]


900
情報処理装置
901
CPU
902
ROM
903
RAM
904
ハードディスク
905
通信I/F
906
907
記録媒体
908
リーダライタ
909
入出力
インタフェース

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/034355

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/57(2013.01)i, G06F9/4401(2018.01)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. G06F21/57, G06F9/4401

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.
A	JP 2004-164640 A (MICROSOFT CORPORATION) 10 June 2004, paragraphs [0044]-[0048], [0053]-[0062], fig. 6, 8 & US 2004/0093372 A1, paragraphs [0062]-[0066], [0072]-[0081], fig. 6, 8 & EP 1418725 A2	1-10
A	JP 2012-48488 A (TOYOTA INFOTECHNOLOGY CENTER CO., LTD. et al.) 08 March 2012, paragraphs [0033]-[0036], fig. 4 (Family: none)	1-10
A	JP 2016-10031 A (KDDI CORPORATION et al.) 18 January 2016, paragraphs [0059]-[0071] (Family: none)	1-10

☐ 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
06 December 2018 (06.12.2018)	18 December 2018 (18.12.2018)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０３４３５５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/57(2013.01)i, G06F9/4401(2018.01)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.　G06F21/57, G06F9/4401

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
A	JP 2004-164640 A (マイクロソフト　コーポレイション) 2004.06.10, 段落[0044]-[0048], [0053]-[0062], 図6, 図8 & US 2004/0093372 A1, 段落[0062]-[0066], [0072]-[0081], FIG.6, FIG.8 & EP 1418725 A2	1-10
A	JP 2012-48488 A (株式会社トヨタＩＴ開発センター他) 2012.03.08, 段落[0033]-[0036], 図4 (ファミリーなし)	1-10
A	JP 2016-10031 A (ＫＤＤＩ株式会社他) 2016.01.18,	1-10

☑　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
０６．１２．２０１８	１８．１２．２０１８

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　９５５５
宮司　卓佳
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
	段落[0059]-[0071]（ファミリーなし）	