

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7210238号
(P7210238)

(45)発行日 令和5年1月23日(2023.1.23)

(24)登録日 令和5年1月13日(2023.1.13)

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

請求項の数 10 (全11頁)

(21)出願番号	特願2018-214684(P2018-214684)	(73)特許権者	000001007 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
(22)出願日	平成30年11月15日(2018.11.15)	(74)代理人	100126240 弁理士 阿部 琢磨
(65)公開番号	特開2020-86516(P2020-86516A)	(74)代理人	100124442 弁理士 黒岩 創吾
(43)公開日	令和2年6月4日(2020.6.4)	(72)発明者	美馬 毅 東京都大田区下丸子3丁目30番2号キ ヤノン株式会社内
審査請求日	令和3年11月8日(2021.11.8)	審査官	岸野 徹

最終頁に続く

(54)【発明の名称】 情報処理装置、情報処理装置の制御方法、及び、プログラム

(57)【特許請求の範囲】

【請求項1】

第1CPUと、第2CPUと、省電力制御を行う電力制御プログラムを格納する第1メモリと、改ざん検知プログラムを格納する第2メモリと、を備える情報処理装置であって、前記第2CPUは、前記情報処理装置の起動に基づいて前記改ざん検知プログラムを実行し、

前記第1CPUは、前記第2CPUが実行するプログラムを、前記改ざん検知プログラムから前記電力制御プログラムに変更する変更プログラムを実行し、

前記第2CPUは、前記情報処理装置が省電力状態への移行条件を満たすことによって、前記電力制御プログラムによって前記第1CPUを省電力状態に移行させ、

前記第1CPUは、前記変更プログラムに基づいて、前記第2CPUのリセットベクタを前記第2メモリのアドレス領域から前記第1メモリのアドレス領域に切り替えることを特徴とする情報処理装置。

【請求項2】

前記第1CPUは、前記変更プログラムに基づいて、前記第2CPUが実行するプログラムを前記改ざん検知プログラムから前記電力制御プログラムに切り替えるとともに、前記第2CPUを再度起動させることを特徴とする請求項1に記載の情報処理装置。

【請求項3】

第1CPUと、第2CPUと、省電力制御を行う電力制御プログラムを格納する第1メモリと、改ざん検知プログラムを格納する第2メモリと、を備える情報処理装置であって、

10

20

前記第 2 CPU は、前記情報処理装置の起動に基づいて前記改ざん検知プログラムを実行し、

前記第 1 CPU は、前記第 2 CPU が実行するプログラムを、前記改ざん検知プログラムから前記電力制御プログラムに変更する変更プログラムを実行し、

前記第 2 CPU は、前記情報処理装置が省電力状態への移行条件を満たすことによって、前記電力制御プログラムによって前記第 1 CPU を省電力状態に移行させ、

前記第 1 CPU は、前記変更プログラムに基づいて、前記第 2 CPU が実行するプログラムを前記改ざん検知プログラムから前記電力制御プログラムに切り替えるとともに、前記第 2 CPU を再度起動させることを特徴とする情報処理装置。

【請求項 4】

前記第 2 CPU は、前記変更プログラムの改ざん検知を行い、

前記第 2 CPU は、前記変更プログラムが改ざんされていない場合に、前記第 1 CPU を起動させ、前記変更プログラムが改ざんされた場合に、前記第 1 CPU を起動しないことを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の情報処理装置。

【請求項 5】

前記第 2 CPU は、前記第 1 メモリに格納されている前記電力制御プログラムの改ざん検知を行うことを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の情報処理装置。

【請求項 6】

前記第 1 メモリは、画像処理プログラムを記憶し、

前記第 1 CPU は、前記変更プログラムを実行することで、前記第 2 CPU に前記画像処理プログラムを実行可能にすることを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載の情報処理装置。

【請求項 7】

前記変更プログラムを記憶する第 3 のメモリを有することを特徴とする請求項 1 乃至 6 のいずれか 1 項に記載の情報処理装置。

【請求項 8】

前記第 1 メモリは、揮発性の記憶媒体であることを特徴とする請求項 1 乃至 7 のいずれか 1 項に記載の情報処理装置。

【請求項 9】

前記第 2 メモリは、不揮発性の記憶媒体であることを特徴とする請求項 1 乃至 8 のいずれか 1 項に記載の情報処理装置。

【請求項 10】

第 1 CPU と、第 2 CPU と、省電力制御を行う電力制御プログラムを格納する第 1 メモリと、改ざん検知プログラムを格納する第 2 メモリと、を備える情報処理装置の制御方法であって、

前記第 2 CPU は、前記情報処理装置の起動に基づいて前記改ざん検知プログラムを実行し、

前記第 1 CPU は、前記第 2 CPU が実行するプログラムを、前記改ざん検知プログラムから前記電力制御プログラムに変更する変更プログラムを実行し、

前記第 2 CPU は、前記情報処理装置が省電力状態への移行条件を満たすことによって、前記電力制御プログラムによって前記第 1 CPU を省電力状態に移行させ、

前記第 1 CPU は、前記第 2 CPU のリセットベクタを、前記第 2 メモリのアドレス領域から前記第 1 メモリのアドレス領域に切り替えることで前記制御を行うことを特徴とする情報処理装置の制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置、情報処理装置の制御方法、及び、プログラムに関するものである。

【背景技術】

10

20

30

40

50

【 0 0 0 2 】

情報処理装置に搭載するCPUが実行する起動プログラムの改竄を検知する手法が知られている（たとえば特許文献1）。

【 0 0 0 3 】

例えば特許文献1では、起動プログラムを実行するCPU自身では、起動プログラムの改竄を検知できないため、起動プログラムを実行するCPUとは異なるCPUにより、前記起動プログラムの改竄の有無を検証する。

【先行技術文献】

【特許文献】

【 0 0 0 4 】

【文献】国際公開WO 2 0 0 9 - 0 1 3 8 2 5号公報

【発明の概要】

【発明が解決しようとする課題】

【 0 0 0 5 】

情報処理装置は、世の中の高性能化への要求に対応し、同時に複数の処理をスムーズに実行できるよう、今や複数のCPUが搭載されているのが一般的であり、CPU毎にそれぞれ異なる処理プログラムを実行させている。

【 0 0 0 6 】

その為、起動プログラムの改竄検証の機能を情報処理装置に備える場合、情報処理装置の何れかのCPUについて、元々行っていた処理プログラムの他に、起動プログラムの改竄検証のプログラムを実行させることが考えられる。

【 0 0 0 7 】

この場合、改竄検証プログラムを実行させるCPUには、最初は改竄検証プログラムを実行させて、検証完了後に処理プログラムに切り換えて実行させるように、動作プログラムを制御する。

【 0 0 0 8 】

しかしながら、動作プログラムが改竄されると、切替対象の処理プログラムとは別のプログラムに切り換えられる場合がある。

【課題を解決するための手段】

【 0 0 0 9 】

本発明は、第1CPUと、第2CPUと、省電力制御を行う電力制御プログラムを格納する第1メモリと、改ざん検知プログラムを格納する第2メモリと、を備える情報処理装置であって、前記第2CPUは、前記情報処理装置の起動に基づいて前記改ざん検知プログラムを実行し、前記第1CPUは、前記第2CPUが実行するプログラムを、前記改ざん検知プログラムから前記電力制御プログラムに変更する変更プログラムを実行し、前記第2CPUは、前記情報処理装置が省電力状態への移行条件を満たすことによって、前記電力制御プログラムによって前記第1CPUを省電力状態に移行させ、前記第1CPUは、前記第2CPUのリセットベクタを、前記第2メモリのアドレス領域から前記第1メモリのアドレス領域に切り替えることで前記制御を行うことを特徴とする。

【発明の効果】

【 0 0 1 0 】

本発明によれば、改竄検証済みのプログラムを使って起動されたCPUにより、起動時に実行される改竄検知プログラムから適切な処理プログラムに切り換えることができる。

【図面の簡単な説明】

【 0 0 1 1 】

【図1】本実施例における複合機100のブロック図。

【図2】本実施例におけるCPU102から見たメモリアドレスマップの一例。

【図3】本実施例1におけるCPU102の動作プログラム切り換え制御を説明するフローチャート。

【図4】本実施例2におけるCPU102の動作プログラム切り換え制御を説明するフロ

10

20

30

40

50

ーチャート。

【発明を実施するための形態】

【0012】

以下、添付図面を参照して本発明の実施形態を詳しく説明する。尚、以下の実施形態は特許請求の範囲に係る本発明を限定するものでなく、また本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。尚、実施形態に係る情報処理装置として複合機（デジタル複合機/MFP/Multi Function Peripheral）を例に説明する。しかしながら適用範囲は複合機に限定はせず、情報処理装置であればよい。

【実施例1】

【0013】

<情報処理装置100>

図1に本実施形態を説明するための複合機100のブロック図を示す。SOC20は複合機100の制御を行うための後述する101~114のモジュールで構成される。

【0014】

CPU101は、複合機100の各種ソフトウェアプログラムを実行し、複合機100の各種制御を行なうプロセッサである。CPU102は、改竄検知用のソフトウェアプログラムと、CPU101が実行するプログラムとは別のアプリケーションプログラムを実行し、複合機100の改竄検知と一部のアプリケーションの制御を行うプロセッサである。

【0015】

ROM103は、リードオンリーメモリで、複合機100の固定パラメータ等を格納している。又、ROM103は、前記改竄検知用のソフトウェアプログラムや後述の公開鍵などが格納されている。なお、ROM103は外部からのI/Fからは書き換えられないように論理回路で構成されたMASK ROMもしくは製造時に一度だけ書き込みが可能なOTP ROMで構成されているものとする。ここでOTPとは(One Time Programmable ROM)のことである。

【0016】

RAM104(揮発性の記憶媒体)は、ランダムアクセスメモリで、CPU101とCPU102が複合機100を制御する際に、プログラムや一時的なデータの格納などに使用される。HDD制御部105は、HDD115(不揮発性の記憶媒体)に対してデータを読み書きする制御を行う。例えばRAM104に格納されている画像データをシステムバス114経由で、HDD115に書き出して格納することができる。

【0017】

フラッシュメモリ制御部106は、フラッシュメモリ116に対してデータを読み書きする制御を行う。起動時に、フラッシュメモリ116に格納されているプログラムを読み出してシステムバス114経由でRAM104へ展開することができる。

【0018】

ネットワークI/F制御部107は、ネットワーク117上の他のデバイスやサーバーと、データの送受信を制御する。外部ポート制御部108は、SOC20の入出力ポート制御部である。例えば出力ポートを制御することによりLED118を必要に応じて点灯し、ソフトウェアやハードウェアの異常を外部に伝えることが可能である。

【0019】

スキャナI/F制御部109は、スキャナ119による原稿の読み取りを制御する。プリンタI/F制御部110は、プリンタ120による印刷処理を制御する。

【0020】

画像処理部111は、スキャナ118から読み取った画像データをシェーディング補正したり、プリンタ119に出力するためにハーフトーン処理やスムージング処理したりする処理部である。

【0021】

パネル制御部112は、タッチパネル式の操作パネル121を制御し、各種情報の表示

10

20

30

40

50

、使用者からの指示入力を制御する。リセットベクタ制御部 113 は、CPU 102 のリセットベクタ（電源投入後に実行するプログラムを読みだす為に、リセット解除後に参照するアドレス値）の設定を変更する制御部であり、レジスタで構成されている。リセットベクタ制御部 113 のレジスタ設定は、CPU 101 により行われる。

【0022】

システムバス 114 は、接続されているモジュールを相互に接続する。このシステムバス 114 を介して、CPU 101 や CPU 102 からの制御信号や各装置間のデータ信号が送受信される。

【0023】

HDD 115 は、ハードディスクドライブで一部のアプリケーション、各種データを格納する。フラッシュメモリ 116 は、BIOS、ブートローダー、カーネル、アプリケーションを格納する。なお、HDD 115 とフラッシュメモリ 116 は同一のストレージモジュールであっても良いものとする。

10

【0024】

<改竄されたプログラムへ切り替えられる仕組み>

ここで、本実施例の課題である CPU が実行するプログラムが、改竄されたプログラムへ切り替えられてしまうメカニズムについて説明する。

【0025】

図 2 に、CPU 102 から見た各格納手段のメモリアドレスマップ（論理アドレスマップ）の一例を示す。

20

【0026】

図 2 に示すメモリアドレスマップにおいて、アドレス 0×00000 より ROM 103 のアドレス領域、アドレス 0×01000 よりフラッシュメモリ 116 のアドレス領域が、それぞれ割り当てられている。また、アドレス 0×10000 より RAM 104 のアドレス領域、アドレス 0×20000 より HDD 115 のアドレス領域、がそれぞれ割り当てられている。

【0027】

本実施例では、CPU 102 に、最初は改竄検証プログラムを実行させて、検証完了後は別の処理プログラムを実行させるように、動作プログラムを切り換える場合を例にとり説明する。

30

【0028】

図 2 において、プログラム 201 ~ 203 は、CPU 102 が実行するプログラムを示し、リセットベクタ 204 ~ 206 は、CPU 102 が起動後に最初に参照する、プログラムが格納されている参照先（アドレス値）を示している。

【0029】

プログラム 201 は、CPU 102 が最初に実行する改竄検証プログラムであり、ROM 103 のアドレス領域のリセットベクタ 204 が示すアドレス値の 0×00000 より格納されている。

【0030】

プログラム 202 は、CPU 102 が検証完了後に実行する別の処理プログラムであり、フラッシュメモリ 116 のアドレス領域のリセットベクタ 205 が示すアドレス値の 0×01000 より格納されている。

40

【0031】

CPU 102 に実行させる別の処理プログラムは、例えば、情報処理装置 100 の消費電力を低減させるために、CPU 101 のスリープ制御（通常状態、スリープ状態への移行制御）を行う処理プログラムや、画像処理プログラムなどである。CPU 101 がスリープ状態へ移行する条件を満たした場合に、前記別の処理プログラムが実行される。

【0032】

プログラム 203 は、CPU 102 が検証完了後に、改竄者が実行させる目的で予め格納した改竄された処理プログラムであり、HDD 115 のアドレス領域のリセットベクタ

50

206が示すアドレス値の0x02000より格納されている。

【0033】

つまりCPU102のリセットベクタは、最初は改竄検証プログラム(プログラム201)が格納されているリセットベクタ204に設定され、検証完了後、別の処理プログラム(プログラム202)が格納されているリセットベクタ205へ、本来は設定される。

【0034】

しかしながら、CPU102のリセットベクタの設定は、CPU101の動作プログラムにより、リセットベクタ制御部113のレジスタ値を変更することにより行われる。このCPU101の動作プログラムが改竄されると、改竄者にリセットベクタ設定を変更されるおそれがある。

10

【0035】

図2に示す例では、改竄された処理プログラムであるプログラム203が格納されているリセットベクタ206へ変更されてしまうと、CPU102は改竄された処理プログラムであるプログラム203へと動作プログラムを切り換えられてしまう。

【0036】

また、リセットベクタは、改竄されたプログラム203以外の、HDD115またはRAM104の中の改竄されていない処理プログラムのアドレスに切り換えられてしまうこともある。

【0037】

<CPU102の動作プログラム切り換えシーケンス>

20

次に、本実施例の特徴であるCPU102に動作させるプログラムの切り換え制御について説明する。

【0038】

図3に、本実施例1における、複合機100の電源投入直後からの、CPU102に動作させるプログラム、及びプログラム切り換えシーケンスのフローチャートを示す。

【0039】

まず始めに、複合機100の電源が投入されると、複合機100内の各モジュールをリセットし、その後、CPU102のみリセット状態を解除することにより、CPU102が起動する。複合機100内の各モジュールのリセット制御は、例えばリセット制御IC等を使用して、各モジュールへ供給するリセット信号の論理を所望のタイミングで切り替えることにより行う(S301)。

30

【0040】

CPU102のリセットが解除されると、CPU102のリセットベクタ204~206の示すアドレス領域に格納されているプログラムをCPU102は読み込み、読み込んだプログラムで実行するよう起動する。

【0041】

CPU102のリセットベクタ204~206は、リセット後の初期状態では、ROM103のアドレス領域を示すリセットベクタ204に設定されている。よってCPU102は、リセットベクタ204が示すアドレス領域であるROM103に格納されている、改竄検知プログラムであるプログラム201を読み込み、プログラム201に従って動作する状態で起動する(S302)。

40

【0042】

次に、改竄検知プログラムに従って動作しているCPU102により、フラッシュメモリ116に格納されているプログラムについて、改竄の有無を検証する(S303)。S303において改竄の検証がされるプログラムは、CPU101の起動時に実行されるプログラムである。S303では、フラッシュメモリ116に格納されているプログラムをRAM104に読み込み、読み込んだプログラムの改竄の有無を検証する。なお、S303において、フラッシュメモリ116に格納されているプログラム202をRAM104に読み込んでよい。

【0043】

50

本実施例において、改竄の有無の検証（以下、改竄検証）は、一般的によく使用される公開鍵暗号方式を応用したデジタル署名（以下、署名）を使用して実施する場合を例にとり説明する。勿論、デジタル署名以外の改竄検証を行うプログラムであっても構わない。

【0044】

署名データは、CPU101に実行させるプログラムの一部または全体について、ハッシュ関数を使用して算出されたハッシュ値であり、暗号鍵の対となる公開鍵と共に、予め製品出荷時のタイミング等でROM103へ格納されている。

【0045】

一方、CPU101に実行されるプログラムは、後にソフトウェア更新などで書き換えられる事を想定し、ROMライター等で書き換え可能なフラッシュメモリ116に、署名データと共に格納されている。フラッシュメモリ116に格納されている署名データは、外部からアクセスされるおそれがあるため、暗号鍵の対となるもう一方の秘密鍵を使用して暗号化されている。

【0046】

改竄検知プログラムであるプログラム201で動作しているCPU102は、まず始めに、フラッシュメモリ116に格納されている暗号化された署名データをリードして、RAM104へ格納する。次に、ROM103に格納されている公開鍵を使用して、暗号化された署名データをデコードする。そして、デコードした署名データと、ROM103に予め格納されている署名データと比較することにより署名データが改竄されているか否かを検証する。

【0047】

CPU102は、署名データを比較して、少しでも違いがあれば「改竄有り」と判断し、一致していれば「改竄無し」と判断する（S304）。

【0048】

S304において、「改竄有り」と判断された場合には、改竄検知通知処理を行う（S305）。本実施例の複合機100においては、外部ポート制御部108を経由してLED118に供給される出力ポートを制御することにより、LED118を点灯させることにより、改竄が有ることを外部に通知する。

【0049】

S304において、「改竄無し」と判断された場合には、CPU101のリセット状態を解除する（S306）。CPU101のリセット状態の解除は、CPU101に供給するリセット信号の論理を「解除」を伝える値へ切り替えることにより行う。

【0050】

CPU101のリセットが解除されると、CPU101はフラッシュメモリ116のリセットベクタ（CPU101のリセットベクタは不変）が示すアドレス領域に格納されているプログラムを読み込み、RAM104に展開する。そして、リセット状態が解除されたCPU101は、RAM104に展開したプログラムを実行することにより、CPU101の起動処理を行う（S307）。

【0051】

CPU102のリセットベクタの設定は、改竄検証対象であるCPU101に実行させるプログラムにおいて行われる。CPU102のリセットベクタ設定が改竄されると、フラッシュメモリ116に格納される署名データは、正確値であるROM103に格納される署名データとの比較で違いが発生するため、リセットベクタの改竄を検知することができる。

【0052】

CPU101の起動が完了すると、CPU101は、読み込んだ改竄検証済みのプログラムに従って、CPU102をリセットする（S308）。CPU102のリセットは、CPU101に供給するリセット信号の論理を「リセット」を伝える値へ切り替えることにより行う。

【0053】

10

20

30

40

50

そして、CPU101は改竄検証済みのプログラムに従って、CPU102のリセットベクタ204～206をリセットベクタ205へ切り替える(S309)。改竄検証済みのプログラムには、CPU102のリセットベクタとして、リセットベクタ205を示すリセット制御部113のレジスタ設定値がプログラミングされている。そのため、前記レジスタ値をリセット制御部113のレジスタへ設定することにより、CPU102にはリセットベクタ205が設定される。

【0054】

その後、CPU101は、CPU102のリセット信号の論理を切り替えて、CPU102のリセット状態を解除することにより、CPU102は再度起動される(S310)。

【0055】

CPU102のリセットが解除されると、CPU102はリセットベクタ205の示すアドレス領域に格納されているプログラムを読み込み、読み込んだプログラムで実行するよう起動する。リセットベクタ205が示すアドレス領域であるRAM104には、CPU102に実行させる改竄検知プログラムとは別の処理プログラムが格納されている。

【0056】

前記CPU102に実行させる別の処理プログラムは、複合機100の電源投入直後は、フラッシュメモリ116に格納されている。

【0057】

このフラッシュメモリ116のアクセス速度は遅い為、改竄検証済みのプログラムで動作している状態のCPU101により、CPU102に実行させる別の処理プログラムは、アクセス速度の速いRAM104へ事前に格納されている。

【0058】

よってCPU102は、リセットベクタ205が示すアドレス領域であるRAM104に格納されている、別の処理プログラムであるプログラム202を読み込み、別の処理プログラムであるプログラム202に従って動作する状態で起動する(S311)。

【0059】

以上説明してきたように、実施例1の複合機100は、CPU102に動作させるプログラムを切り換える際に、改竄検証済みのプログラムで動作するCPU101によって、CPU102のリセットベクタ204～206を切り換えるよう制御する。

【0060】

つまりCPU102は、改竄検証済みのリセットベクタの示すアドレス領域に格納されたプログラムを読み込み起動する。そのため、改竄者にリセットベクタ設定を改竄されて、CPU102が改竄されたプログラムが格納されたアドレス領域から起動し、改竄されたプログラムが実行されることを低減することができる。

【実施例2】

【0061】

第1の実施形態では、改竄検証済みのプログラムで動作するCPU101によって、CPU102のリセットベクタを切り換えることにより、CPU102に動作させるプログラムを別の処理プログラムへ切り換える制御について説明した。

【0062】

しかし、別の処理プログラムであるプログラム202が、フラッシュメモリ116に格納されている場合は、フラッシュメモリ116へ書き込み器具等で外部より書き込む事が可能であるため、改竄されてしまうおそれがある。

【0063】

その為、改竄検証済みのプログラムで動作するCPU101によって、CPU102のリセットベクタを切り換えても、CPU102は改竄されたプログラムで起動される恐れがある。

【0064】

第2の実施形態では、上記課題を解決するために、フラッシュメモリ116に格納されているCPU102に実行させる別の処理プログラム(プログラム202)についても改

10

20

30

40

50

鼠検証を行う。以下、第2の実施形態について、複合機を例に説明する。第2の実施形態の複合機を説明するに辺り、第1の実施形態の複合機と同じモジュール、処理については同一の番号を付与し、説明を割愛する。

【0065】

< CPU102の動作プログラム切り換えシーケンス >

図4に、本実施例2における、複合機100の電源投入直後からの、CPU102に動作させるプログラム、及びプログラム切り換えシーケンスのフローチャートを示す。

【0066】

図4に示すフローチャートにおいて、S301～S302の処理は、本実施例1のフローチャート(図3)における処理と同様であるため、説明を割愛する。

10

【0067】

CPU102が改竄検知プログラムに従って動作する状態で起動すると、CPU102は、フラッシュメモリ116に格納されているCPU101に動作させるプログラムと、CPU102の別の処理プログラムについて、改竄の有無を検証する(S403)。

【0068】

ROM103には、CPU101に動作させるプログラムの署名データの他に、CPU102に動作させる別の処理プログラム(プログラム202)の署名データが予め格納されている。

【0069】

一方、フラッシュメモリ116には、CPU101に動作させるプログラムの暗号化された署名データの他に、CPU102に動作させる別の処理プログラム(プログラム202)の暗号化された署名データが予め格納されている。

20

【0070】

改竄検知プログラム(プログラム201)で動作しているCPU102は、まず始めにフラッシュメモリ116に格納されているCPU101に動作させるプログラムの暗号化された署名データをデコードする。そしてROM103に格納されているCPU101に動作させるプログラムの署名データと一致しているか否かを確認することにより、CPU101に動作させるプログラムの改竄の有無を検証する。

【0071】

次にCPU102は、フラッシュメモリ116に格納されているCPU102に動作させる別の処理プログラム(プログラム202)の暗号化された署名データをデコードする。そしてROM103に格納されている別の処理プログラム(プログラム202)の署名データと一致しているか否かを確認することにより、CPU102に動作させる別の処理プログラム(プログラム202)の改竄の有無を検証する。

30

【0072】

図4に示すフローチャートにおいて、S305～S311の処理は、本実施例1のフローチャート(図3)における処理と同様であるため、説明を割愛する。

【0073】

以上説明してきたように、実施例2の複合機100では、CPU102は、改竄検証済みの別の処理プログラムであるプログラム202により動作するよう制御する。

40

【0074】

つまり、CPU102に実行させるプログラムを別の処理プログラム(プログラム202)に切り換える際に、CPU102のリセットベクタを実施例1と同じリセットベクタ205で設定した場合であっても、プログラム202の改竄検証を行うことができる。

【0075】

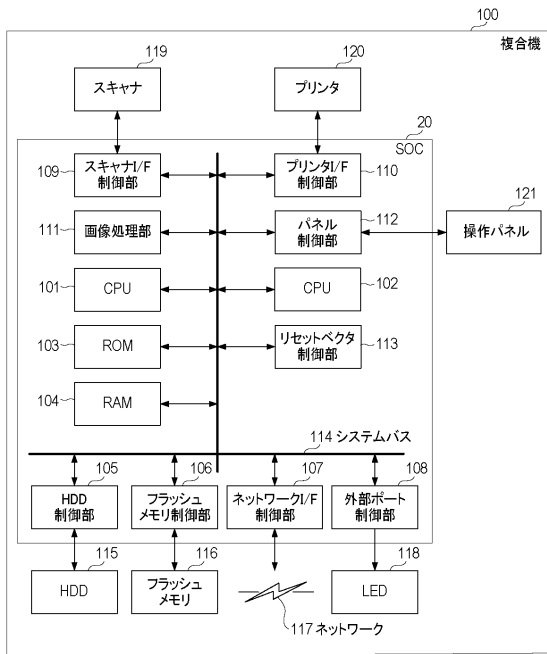
(その他の実施形態)

本発明は、上述の実施形態の1以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける1つ以上のプロセッサがプログラムを読み出し実行する処理でも実現可能である。また、1以上の機能を実現する回路(例えば、ASIC)によっても実現可能である。

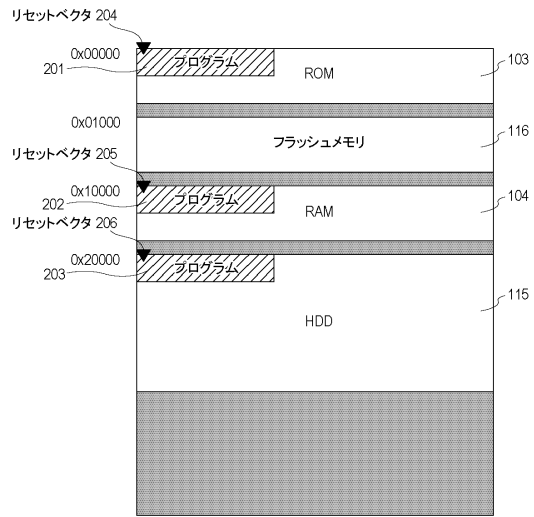
50

【 図 面 】

【 図 1 】



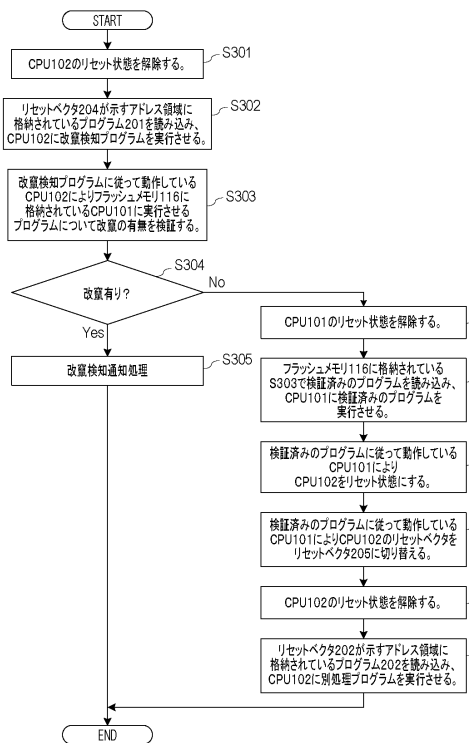
【 図 2 】



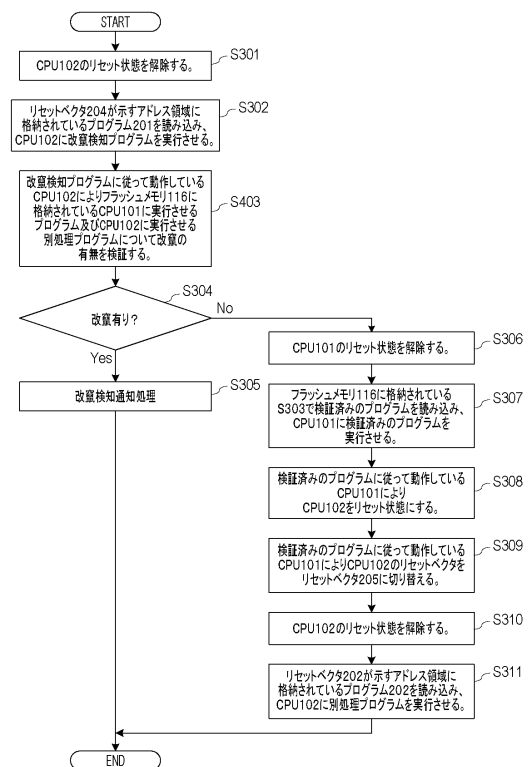
10

20

【 図 3 】



【 図 4 】



30

40

50

フロントページの続き

- (56)参考文献 特開2018-045310(JP,A)
国際公開第2009/013825(WO,A1)
特開2015-106771(JP,A)
特開2020-071723(JP,A)
特開2011-008432(JP,A)
特許第4279902(JP,B2)
米国特許出願公開第2015/0074387(US,A1)
米国特許出願公開第2011/0044451(US,A1)
米国特許出願公開第2020/0134232(US,A1)
特開2014-021953(JP,A)
特開2012-181882(JP,A)
特開2008-244992(JP,A)
特開2004-326307(JP,A)
特開2016-107570(JP,A)
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/51
G06F 21/64