

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7614881号
(P7614881)

(45)発行日 令和7年1月16日(2025.1.16)

(24)登録日 令和7年1月7日(2025.1.7)

(51)国際特許分類

G 0 6 F 21/64 (2013.01)

G 0 6 F 9/4401(2018.01)

G 0 6 F 9/445(2018.01)

F I

G 0 6 F 21/64

G 0 6 F 9/4401

G 0 6 F 9/445

請求項の数 10 (全10頁)

(21)出願番号	特願2021-24692(P2021-24692)	(73)特許権者	000001007
(22)出願日	令和3年2月18日(2021.2.18)		キャノン株式会社
(65)公開番号	特開2022-126549(P2022-126549 A)		東京都大田区下丸子3丁目30番2号
(43)公開日	令和4年8月30日(2022.8.30)	(74)代理人	100126240
審査請求日	令和6年2月8日(2024.2.8)		弁理士 阿部 琢磨
		(74)代理人	100223941
			弁理士 高橋 佳子
		(74)代理人	100159695
			弁理士 中辻 七朗
		(74)代理人	100172476
			弁理士 富田 一史
		(74)代理人	100126974
			弁理士 大朋 靖尚
		(72)発明者	山下 貴弘
			東京都大田区下丸子3丁目30番2号キ
			最終頁に続く

(54)【発明の名称】 情報処理装置

(57)【特許請求の範囲】

【請求項1】

情報処理装置であって、
第1プログラムを保持する不揮発性のメモリと、
第2プログラムと第3プログラムを格納するように構成された不揮発性のストレージと、
前記第1プログラムが有効であるか否かを検証する第1プロセッサと、
前記第1プログラムが有効である場合に、前記第1プログラムを実行する第2プロセッサと、
ネットワークを介して外部装置と通信する通信手段と、
を有し、
前記第2プロセッサは、
前記第2プログラムが有効であるか否かを検証し、
前記第2プログラムが有効である場合には、前記第2プログラムを実行し、前記第2プログラムが有効でない場合には、前記第3プログラムが有効であるか否かを検証し、
前記第3プログラムが有効である場合には、前記第3プログラムを用いて前記第2プログラムを上書きし、
前記第3プログラムが有効でないと判定されることによって、前記通信手段を介して第4プログラムを受信し、前記受信した前記第4プログラムの有効であるか否かを検証し、
前記第2プロセッサによって有効であると判定された前記第4プログラムによって、前記ストレージに記憶された前記有効でないと判定された前記第3プログラムを上書きするこ

とを特徴とする情報処理装置。

【請求項 2】

前記第 2 プロセッサは、前記有効でないと判断された前記第 2 プログラムを前記上書きされた前記第 3 プログラムで上書きす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】

前記第 2 プロセッサは、

前記上書きした前記第 2 プログラムを実行可能であることを特徴とする請求項 1 または 2 に記載の情報処理装置。

【請求項 4】

前記ストレージは、画像データを記憶するストレージであり、

前記第 2 プログラムおよび前記第 3 プログラムは、Loaderである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 プロセッサは、前記第 3 プログラムが有効である場合には、前記第 3 プログラムの全てのデータによって、前記ストレージに記憶された前記第 2 プログラムの上書きを実行する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】

前記不揮発性のメモリは、画像データを記憶しないメモリであり、

前記不揮発性のメモリに記憶された前記第 1 プログラムは、BIOSであ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】

前記ストレージは、第 5 プログラム、第 6 プログラム、第 7 プログラム、第 8 プログラムを記憶し、前記第 5 プログラムは、Kernelであり、前記第 6 プログラムは、前記 Kernelのバックアップであり、前記第 7 プログラムは、ファームウェアであり、前記第 8 プログラムは、前記ファームウェアのバックアップであ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】

第 1 プログラムを保持する不揮発性のメモリと、第 2 プログラムと第 3 プログラムを格納するように構成された不揮発性のストレージと、前記第 1 プログラムが有効であるか否かを検証する第 1 プロセッサと、前記第 1 プログラムが有効である場合に、前記第 1 プログラムを実行する第 2 プロセッサと、ネットワークを介して外部装置と通信する通信手段と、を有する情報処理装置の制御方法であって、

前記第 2 プロセッサは、

前記第 2 プログラムが有効であるか否かを検証し、

前記第 2 プログラムが有効である場合には、前記第 2 プログラムを実行し、前記第 2 プログラムが有効でない場合には、前記第 3 プログラムが有効であるか否かを検証し、

前記第 3 プログラムが有効である場合には、前記第 3 プログラムを用いて前記第 2 プログラムを上書きし、

前記第 3 プログラムが有効でないと判定されることによって、前記通信手段を介して第 4 プログラムを受信し、前記受信した前記第 4 プログラムの有効であるか否かを検証し、前記第 2 プロセッサによって有効であると判定された前記第 4 プログラムによって、前記ストレージに記憶された前記有効でないと判定された前記第 3 プログラムを上書きすることを特徴とする情報処理装置の制御方法。

【請求項 9】

請求項 8 に記載の制御方法を、コンピュータに実行させるためのプログラム。

【請求項 10】

請求項 9 に記載のプログラムを格納したコンピュータで読み取り可能な記憶媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置および情報処理装置の制御方法に関する。

【背景技術】

【0002】

近年の画像形成装置においては、プログラム起動の際に起動対象のプログラムについて署名検証処理等を行うことにより、プログラムが正常なものか否かの判定を行うことで、改ざんされたプログラムの起動を防止する改ざん検知機能を有するものがある。また、この際に改ざんが検知された場合は、バックアップとなるプログラムを上書きすることで、改ざんされたプログラムを修復する修復機能を有するものもある。

【0003】

先行文献1においては、バックアッププログラムを上書き後、上書きした対象に対して再度改ざん検知処理を行うことにより、上書き先となる領域やデバイスの書き込み不良を検知する手法が公開されている。

10

【先行技術文献】

【特許文献】

【0004】

【文献】特開2020-95470号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、バックアッププログラム自体が改ざんされている場合に、改ざんを検知することなく上書きをしてしまうと、改ざんされたプログラムで上書きをしてしまうおそれがある。

20

【課題を解決するための手段】

【0006】

本発明は、情報処理装置であって、第1プログラムを保持する不揮発性のメモリと、第2プログラムと第3プログラムを格納するように構成された不揮発性のストレージと、前記第1プログラムが有効であるか否かを検証する第1プロセッサと、前記第1プログラムが有効である場合に、前記第1プログラムを実行する第2プロセッサと、ネットワークを介して外部装置と通信する通信手段と、を有し、前記第2プロセッサは、前記第2プログラムが有効であるか否かを検証し、前記第2プログラムが有効である場合には、前記第2プログラムを実行し、前記第2プログラムが有効でない場合には、前記第3プログラムが有効であるか否かを検証し、前記第3プログラムが有効である場合には、前記第3プログラムを用いて前記第2プログラムを上書きし、前記第3プログラムが有効でないと判定されることによって、前記通信手段を介して第4プログラムを受信し、前記受信した前記第4プログラムの有効であるか否かを検証し、前記第2プロセッサによって有効であると判定された前記第4プログラムによって、前記ストレージに記憶された前記有効でないと判定された前記第3プログラムを上書きすることを特徴とする。

30

【発明の効果】

【0007】

本発明によれば、バックアッププログラムの改ざんを検知することができる。また、改ざんされたプログラムで上書きすることを抑止することができる。

40

【図面の簡単な説明】

【0008】

【図1】画像形成装置のハード構成を示すブロック図

【図2】画像形成装置の起動処理の概略フローチャート

【図3】HDDに保存されるソフトウェアを示すブロック図

【図4】ソフトウェアの改ざん判定とバックアップを用いた上書き処理のフローチャート

【図5】ソフトウェアの改ざん判定とバックアップを用いた上書き処理の別フローチャート

【発明を実施するための形態】

【0009】

50

添付図面を参照して本発明の各実施例を詳しく説明する。なお、以下の実施例は特許請求の範囲に係る発明を限定するものではなく、また各実施例で説明されている特徴の組み合わせのすべてが本発明の解決手段に必須のものとは限らない。本実施形態では、情報処理装置の一例として画像処理装置を用いて説明するがこれに限らない。

【0010】

(実施例1)

図1は、画像形成装置1のハード構成図である。本図を用いて、画像形成装置1の構成を説明する。中央演算処理装置(以下CPU)101は、画像形成装置1を稼働させるためのソフトウェアを動作させる。システムバス102は、CPU101が他のユニットにアクセスするための通路であり、他のユニット同士がアクセスするための通路である。

10

【0011】

ハードディスクユニット(以下HDD)103は、画像形成装置1のソフトウェア及び、画像形成装置1が動作するために必要な各種プログラム、データベース、スキャナで生成した画像データやプリンタで印刷に用いる画像データ等を記憶する。SATAコントローラは、HDD103に対するリード、ライトを制御する。なお、ここではHDDを例に挙げるが、例えば、SSD等の不揮発性の半導体記憶装置であってもよい。

【0012】

Random Access Memory(以下RAM)104は、画像形成装置1のプログラムが展開され、プログラム動作時の変数や、各ユニットからDynamic Memory Access(以下DMA)で転送されるデータの格納領域である。

20

【0013】

ネットワークコントローラ105とネットワークコントローラI/F106は、画像形成装置1とネットワーク上の他の機器と通信を行う。USBホストコントローラ107とUSBホストI/F108は、画像形成装置1とUSBデバイスとの通信を制御する。このUSBホストI/F108はUSBケーブルを使用してUSBデバイスと接続される。USBデバイスの形態によっては、USBケーブルは使用せず直接接続される形態となる。

【0014】

ディスプレイ111は画像形成装置1の動作状況をユーザー等が確認できるように表示する。ディスプレイコントローラ110は、ディスプレイに表示制御を行う。

【0015】

30

入力部113は、画像形成装置1へのユーザーからの指示を受け付ける。入力部コントローラ112は、入力部113を制御する。入力部113は具体的にはキーボードやマウス、テンキー、カーソルキー、タッチパネルや、操作部キーボードといった入力システムである。入力部113がタッチパネルである場合は、物理的にはディスプレイ111の表面に装着された実装形態になる。

【0016】

リアルタイムクロック(以下RTC)114は、画像形成装置1の時計機能、アラーム機能、タイマ機能等を持つ。不揮発メモリ115は書き換え可能なメモリである。不揮発メモリ115は、BIOS等のプログラムを記憶し、少なくともスキャナで生成した画像データやプリンタで印刷に用いる画像データ等を記憶しない。

40

【0017】

不揮発メモリ120は、不揮発メモリ115のバックアップとしてBIOS等のプログラムを記憶する。

【0018】

CPLD109は、CPU101を介して、基盤回路上の信号線のLow/High状況を読み取る、または、CPU101がLow/High状況の設定を変更可能にするユニットである。CPLD109はプログラマブルなロジックデバイスであり、画像形成装置1上で電力関係のOFF/ONを制御可能にしているユニットである。CPLD109の内部には、General Purpose Input Output(以下GPIO)が存在する。CPU101は、そのGPIOレジスタの設定値を変更することで、電力

50

関係のOFF／ONを可能としている。

【0019】

画像形成装置1には、システムバス102とスキャナI／F116を介してスキャナ117が接続される。また、画像形成装置1には、システムバス102とプリンタI／F118を介してプリンタ119が接続される。

【0020】

サブCPU122とサブROM123およびサブRAM124を備えたEC(Embedded Controller)121は、不揮発メモリ115内のBIOSプログラムの正当性を検証する。EC121は通電がなされた時点で、サブCPU122はサブROM123内のプログラムを実行する。それによってサブCPU122は不揮発メモリ115上のECFWを読み出してサブRAM124に展開する。サブCPU122はサブRAM124上に展開されたプログラムを使用して、不揮発メモリ115の改ざん有無を検証する。EC121はバックアップ用途の不揮発メモリ120とも接続されている。不揮発メモリ115が正しくない状態であると判断した場合、EC121は不揮発メモリ120の内容(例えば、BIOS)の改ざん有無を検証し、改ざんが無ければ不揮発メモリ120の内容を不揮発メモリ115に上書きコピーする。なお、この時、不揮発メモリ120の全ての内容を不揮発メモリ115に上書きコピーしてもよい。

【0021】

図2は画像形成装置の起動処理の概略を示すフローチャートである。本フローチャートは、画像形成装置1の電源スイッチがオンされることによって、サブCPU122がサブROM123に記憶されたプログラムを実行し、ECFWをサブRAM124に展開し、展開したプログラムを用いて実行する。

【0022】

EC121はリセット解除され不揮発メモリ115に記録されたEC121用ソフトウェアを読み出して動作を開始する(S201)。EC121は不揮発メモリ115に記録されたBIOSの改ざん有無を判定し、問題が無い場合はCPU101をリセット解除し、BIOS処理を開始させる。続いてCPU101はBIOS処理を実行する(S202)。

【0023】

CPU101はHDD103に保存されている各ソフトウェアの改ざん有無判定の他、各ハードウェアの初期化処理を行う。各ソフトウェアの改ざん判定処理の詳細は図4で説明する。Loaderが改ざんされていない場合、CPU101はLoader処理を開始する(S203)。次にCPU101はKernelの改ざん判定を行う。Kernelが改ざんされていない場合、CPU101は、Kernelの処理を開始する(S204)。次にCPU101はファームウェアの改ざん判定を行い、問題が無いファームウェアを順次起動する。(S205)。

【0024】

図3はHDD103に含まれるソフトウェアを図示したものである。HDD103内にはLoader301およびKernel303およびファームウェア305が含まれており、それぞれのバックアップも含む。(Loader302、Kernel304、ファームウェア306)

図4は本発明の特徴となる、図3記載のプログラムを起動する際に行う、改ざん判定処理並びに復旧上書き処理のフローチャートである。このフローにおいてソフトウェアおよびソフトウェアのバックアップという二種類のソフトウェアが登場する。これらは図3に記載のものに相当し、例えばソフトウェアがLoader301の場合、ソフトウェアのバックアップは302を指す。

【0025】

同様にして、ソフトウェアがKernel303に対してはソフトウェアのバックアップは304を指し、ソフトウェアがファームウェア305の場合は、ソフトウェアのバックアップは306を指す。

10

20

30

40

50

【0026】

なお、これらソフトウェアを検証する主体は図2の起動フローに記載の前段のソフトウェアである。例えばLoader 301を検証するソフトウェアはその前段のBIOSとなる。下記はそのケースについて記載するが、同様にLoader 301はKernel 303の検証および上書きを行い、Kernel 303はファームウェア305の検証および上書きを行う。なお、CPUは、HDD 103から読み出されたその他のプログラムを用いて改ざん判定を行ってもよい。

【0027】

ここでは、例として、Loader 301の改ざん検知について説明するが、Kernel 303、ファームウェア305も各々に対応する検証ソフトウェアを用いて同様の改ざん検知を行う。

10

【0028】

BIOSはLoader 301をHDD 103から読み出し、改ざんの有無を検証する(S401)。検証手段については明記しないが、例えば公開鍵による署名検証処理を行い、あらかじめ保存された正解値と比較することで改ざん有無を検証する。

【0029】

改ざんされていると判断した場合(S402のYes)、続いてBIOSはバックアップとなるLOADER 302をHDD 103から読み出し、バックアップの改ざん有無を検証する(S403)。バックアップも改ざんされていると判断した場合(S404のYes)、BIOSはエラー通知を行い、起動処理を止める(S405)。エラー通知とは例えばディスプレイ111に対して、エラー情報を表示する、ブザーを鳴らすといった操作を行うことである。

20

【0030】

バックアップの改ざんがない場合(S404のNo)、BIOSは改ざんの無かったLOADER 302を用いて、改ざんされているLoader 301に対する上書き処理をHDD 103に実行させる。それによりLoader 301を改ざんの無い状態とする(S406)。バックアップでLoader 301を上書きした後、もしくはS402にて改ざんが無いと判定された場合(S402のNo)、Loader 301は実行可能であり、BIOSはLoader 301を起動し、Loader 301の処理を開始する。

【0031】

図4では、S404のソフトウェアのバックアップの改ざん検知を、S402のソフトウェアの改ざんの検知後に、行っているが、S404のソフトウェアのバックアップの改ざん検知をS402のソフトウェアの改ざんの検知前又は並行に行っても良い。

30

【0032】

図5は、図4に記載のフローに加え、エラー表示(S405)を行う前にさらにネットワーク通信によってバックアップファイルを取得し、それを用いる処理のフローチャートである。図4との差分は三か所である(S508、S509、S510)。それ以外のステップについては図4の各処理と等しい。本フローもソフトウェアおよびソフトウェアのバックアップという二種類のソフトウェアが登場する。

【0033】

これらは図3に記載のものに相当し、例えばソフトウェアがLoader 301の場合、ソフトウェアのバックアップは302を指す。同様にして、ソフトウェアがKernel 303に対してはソフトウェアのバックアップは304を指し、ソフトウェアがファームウェア305の場合は、ソフトウェアのバックアップは306を指す。なお、これらソフトウェアを検証する主体は図2の起動フローに記載の前段のソフトウェアである。例えばLoader 301を検証するソフトウェアはその前段のBIOSとなる。下記はそのケースについて記載するが、同様にLoader 301はKernel 303の検証および上書きを行い、Kernel 303はファームウェア305の検証および上書きを行う。

40

【0034】

バックアップであるLoader 302も改ざんされていた場合(S504のYes)

50

、BIOSはネットワークコントローラ105を制御し、外部ネットワークから不図示のLoaderを受信する(S508)。通信先は予め設定されたサーバでも良いし、ユーザーによって設定されたユーザー管理のサーバでも良い。

【0035】

S508によって取得した不図示のLoaderに対して改ざん有無の検証を行う(S509)。この検証方法はS501およびS503と同一のものである。S509の結果、不図示のLoaderが改ざんされていると判断した場合(S510のYes)、S405と同様の処理を行い、エラー通知をして動作を停止する。一方で、改ざんが無いと判断した場合(S510のNo)、S406と同様に不図示のLoaderをLoader301に上書きすることでLoader301を改ざんの無い状態とする(S506)。

10

【0036】

図5では、S503、S504を実行してからS508～S510を実行するが、逆でもよい。また、S508～S510を行い、S503、S504を行わない構成であってもよい。

【0037】

また、図5では、S504、S510のソフトウェアのバックアップの改ざん検知を、S502のソフトウェアの改ざんの検知後に、検知前又は並行に行ってもよい。

【0038】

なお図4、図5は、BIOSにも適応可能である。ただし、BIOSの場合には、S402およびS502は、不揮発メモリ115から読み出したBIOSに対して改ざん検知を行う。S404、S504は、不揮発メモリ120から読み出したバックアップに対して改ざん検知を行う。S406、S506は、不揮発メモリ120に記憶されたデータを読み出して不揮発メモリ115に上書きを行う。

20

【0039】

(その他の実施形態)

以上、本発明の様々な例と実施形態を示して説明したが、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるものではない。

【0040】

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。

30

【符号の説明】

【0041】

101 CPU

103 HDD

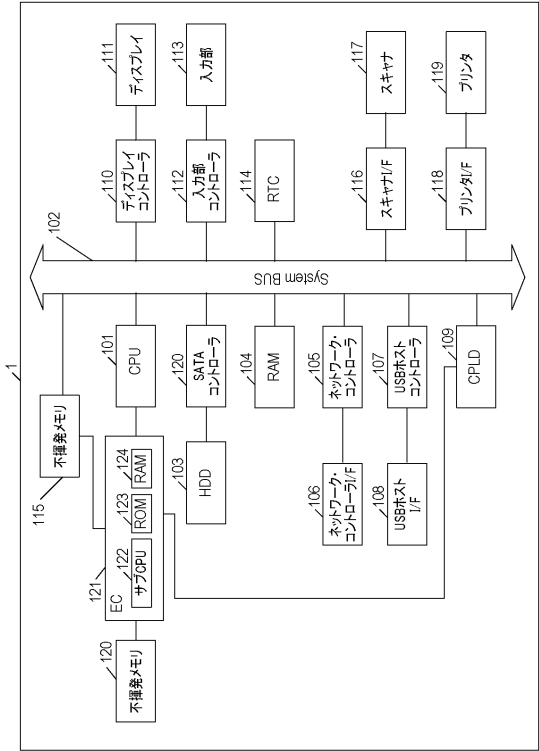
115 不揮発メモリ

120 不揮発メモリ

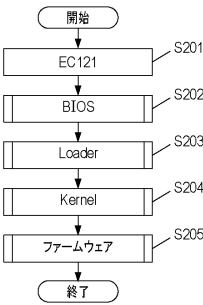
124 RAM

40

【図面】
【図 1】



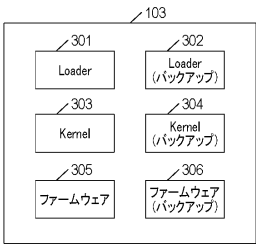
【図 2】



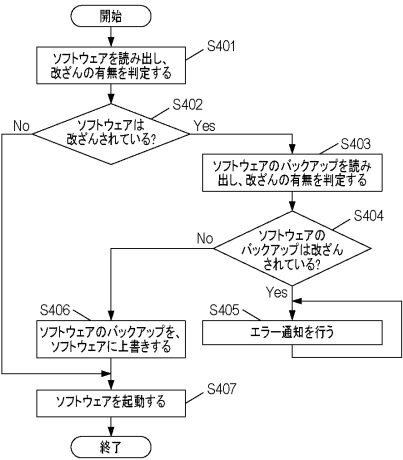
10

20

【図 3】



【図 4】

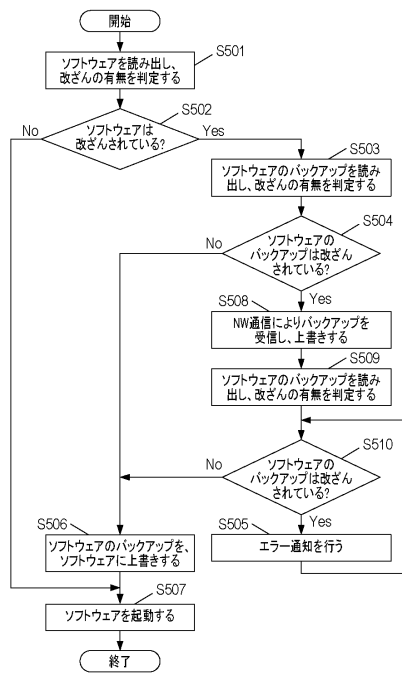


30

40

50

【図 5】



フロントページの続き

ヤノン株式会社内

審査官 中里 裕正

- (56)参考文献 特開 2019-212114 (JP, A)
特開 2013-178733 (JP, A)
特開 2013-084078 (JP, A)
特開 2017-108255 (JP, A)
特開 2020-181540 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
G 0 6 F 2 1 / 6 4
G 0 6 F 9 / 4 4 0 1
G 0 6 F 9 / 4 4 5