(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7100502号
(P7100502)

(45)発行日　令和4年7月13日(2022.7.13)

(24)登録日　令和4年7月5日(2022.7.5)

(51)国際特許分類		FI		
G06F	21/12 (2013.01)	G06F	21/12	
G06F	8/65 (2018.01)	G06F	8/65	
G06F	21/64 (2013.01)	G06F	21/64	
H04L	9/32 (2006.01)	H04L	9/32	200B
H04N	1/00 (2006.01)	H04N	1/00	838

請求項の数　14　（全12頁）

(21)出願番号　特願2018-113101(P2018-113101)
(22)出願日　平成30年6月13日(2018.6.13)
(65)公開番号　特開2019-215754(P2019-215754A)
(43)公開日　令和1年12月19日(2019.12.19)
審査請求日　令和3年6月14日(2021.6.14)

(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
(74)代理人　110003281
特許業務法人大塚国際特許事務所
(72)発明者　八木 優一
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
審査官　岸野 徹

最終頁に続く

(54)【発明の名称】　情報処理装置とその制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置であって、
プログラムを記憶する記憶手段と、
前記記憶手段に記憶されている制御プログラムが改ざんされたかどうか検知する検知手段と、
前記検知手段が前記制御プログラムが改ざんされたことを検知したことに従って、前記制御プログラムを他のプログラムに更新する更新手段と、
前記更新手段により前記制御プログラムが更新された後に、前記情報処理装置の動作により使用される、ユーザにより設定された設定データを初期データに書き換える書き換え手段と、
を有することを特徴とする情報処理装置。
【請求項２】
前記記憶手段は更に、前記制御プログラムに対するデジタル署名及び復号鍵を記憶しており、
前記検知手段は、
前記記憶手段に記憶されている前記制御プログラムから第一のハッシュ値を算出し、前記復号鍵により前記デジタル署名から第二のハッシュ値を取得し、前記第一のハッシュ値と前記第二のハッシュ値とが一致しないときに前記制御プログラムが改ざんされたと検知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】
前記検知手段が前記制御プログラムが改ざんされたことを検知したことを示す情報を不揮発に記憶する手段を、更に有し、
前記書き換え手段は、前記更新手段による前記制御プログラムの更新の後、前記情報処理装置が起動されて前記情報が記憶されていることに応じて、前記制御プログラムの動作に使用されるユーザによって設定された前記設定データを初期データに書き換えることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記初期データは、前記情報処理装置の工場出荷時の設定データであることを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記書き換え手段による、前記設定データの初期データへの書き換えを実行させるか否かをユーザに選択させる選択手段を、更に有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】
前記制御プログラムはメインプログラムと更新プログラムとを含み、
前記検知手段が、前記メインプログラムが改ざんされ、前記更新プログラムが改ざんされていないことを検知した場合、前記更新手段は、前記更新プログラムを実行して前記メインプログラムを更新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】
前記検知手段が、前記メインプログラムと前記更新プログラムがともに改ざんされていることを検知した場合、前記更新手段は、前記更新プログラムを正当な更新プログラムに更新した後、当該正当な更新プログラムを実行して前記メインプログラムを更新することを特徴とする請求項６に記載の情報処理装置。
【請求項８】
前記更新手段は、前記メインプログラムを更新する場合、前記更新プログラムを実行し外部装置或いはサーバからメインプログラムをダウンロードして更新することを特徴とする請求項６に記載の情報処理装置。
【請求項９】
前記更新手段は、前記更新プログラムを更新する場合、前記更新プログラムを、前記情報処理装置の工場出荷時の更新プログラムに更新することを特徴とする請求項６に記載の情報処理装置。
【請求項１０】
前記設定データは、システム管理者ＩＤとパスワードの少なくとも一つを含むことを特徴とする請求項２乃至９のいずれか１項に記載の情報処理装置。
【請求項１１】
前記書き換え手段は、前記制御プログラムを更新した後の前記情報処理装置の最初の起動時に前記初期データに書き換えることを特徴とする請求項２乃至１０のいずれか１項に記載の情報処理装置。
【請求項１２】
前記初期データは、前記設定データよりも前に生成されたデータであることを特徴とする請求項２乃至１０のいずれか１項に記載の情報処理装置。
【請求項１３】
プログラムを記憶する記憶部を有する情報処理装置が実行する、改ざんされたプログラムの更新方法であって、
前記情報処理装置の検知手段が、前記記憶部に記憶されている制御プログラムが改ざんされたかどうか検知する検知工程と、
前記情報処理装置の更新手段が、前記検知工程で前記制御プログラムが改ざんされたことが検知されたことに従って、前記制御プログラムを他のプログラムに更新する更新工程と、

前記情報処理装置の書き換え手段が、前記更新工程で前記制御プログラムが更新された後に、前記情報処理装置の動作に使用される、ユーザによって設定された設定データを初期データに書き換える書き換え工程と、
を有することを特徴とする更新方法。
【請求項１４】
コンピュータを、請求項１乃至１２のいずれか１項に記載の情報処理装置の各手段のすべてとして機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置とその制御方法、及びプログラムに関するものである。
【背景技術】
【０００２】
ソフトウェアの脆弱性をついて、ソフトウェアを改ざんし、コンピュータを悪用する攻撃が問題となっている。そういった攻撃への対策として、耐タンパーモジュールを用いてプログラムのハッシュ値を計算して保存しておき、起動する度にプログラムのハッシュ値を再計算して検証を行うことで改ざんを検知する方法が提案されている。（特許文献１参照）。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２００８－２４４９９２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
特許文献１に記載された技術でプログラムの改ざんを検知した場合、情報処理装置を復旧するためにプログラムの書き換えを行うことになる。このプログラムの書き換えによって、プログラムのセキュリティは担保できる。しかし、改ざんされたプログラムが一時的に動作していることから、情報処理装置の設定データなどが不正に変更されている可能性があり、プログラムの書き換えだけでは情報処理装置のセキュリティを担保しているとは言えない。
【０００５】
本発明の目的は、上記従来技術の問題点の少なくとも一つを解決することにある。
【０００６】
本発明の目的は、プログラムの改ざんを検知し、プログラムの書き換えによって復旧した際に、設定データのセキュリティを担保する技術を提供することにある。
【課題を解決するための手段】
【０００７】
上記目的を達成するために本発明の一態様に係る情報処理装置は以下のような構成を備える。即ち、
情報処理装置であって、
プログラムを記憶する記憶手段と、
前記記憶手段に記憶されている制御プログラムが改ざんされたかどうか検知する検知手段と、
前記検知手段が前記制御プログラムが改ざんされたことを検知したことに従って、前記制御プログラムを他のプログラムに更新する更新手段と、
前記更新手段により前記制御プログラムが更新された後に、前記情報処理装置の動作により使用される、ユーザにより設定された設定データを初期データに書き換える書き換え手段と、を有することを特徴とする。
【発明の効果】

【０００８】
本発明によれば、プログラムの改ざんを検知し、プログラムの書き換えによって復旧した際に、設定データのセキュリティを担保することが可能となった。
【０００９】
本発明のその他の特徴及び利点は、添付図面を参照とした以下の説明により明らかになるであろう。なお、添付図面においては、同じ若しくは同様の構成には、同じ参照番号を付す。
【図面の簡単な説明】
【００１０】
添付図面は明細書に含まれ、その一部を構成し、本発明の実施形態を示し、その記述と共に本発明の原理を説明するために用いられる。
【図１】実施形態１に係る情報処理装置の構成を説明するブロック図。
【図２】実施形態１に係る情報処理装置の不揮発記憶部とＨＤＤに格納されているプログラム及びデータを説明する図。
【図３】実施形態１に係る情報処理装置が実行する処理を説明するフローチャート。
【図４】実施形態２に係る情報処理装置の操作部に表示される、設定データを工場出荷設定データに書き換えをか否かをユーザに選択させる画面の一例を示す図。
【図５】実施形態２に係る情報処理装置が実行する処理を説明するフローチャート。
【発明を実施するための形態】
【００１１】
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。
【００１２】
［実施形態１］
図１は、実施形態１に係る情報処理装置の構成を説明するブロック図である。
【００１３】
実施形態に係る情報処理装置は、例えばスキャン機能やプリント機能等、複数の機能が一体化された、いわゆるＭＦＰ（多機能型周辺装置）として実現される。この情報処理装置は、装置全体を制御するコントローラユニット（制御部）１００、スキャナ１１３、プリンタ１１４、操作部１０６を含む。スキャナ１１３は、原稿の画像を光学的に読み取って、その画像に対応する画像データを出力する。プリンタ１１４は、制御部１００から出力される画像データに基づいて、用紙等の記録媒体（シート）に画像を印刷する。操作部１０６は、ユーザからのジョブ実行等の指示などの入力を受け付けるためのテンキーや各種ハードキー等を含み、更に、ユーザへ装置情報やジョブの進捗情報等、或いは、情報処理装置が実行可能な機能の設定画面を表示する表示パネルを含む。
【００１４】
スキャナ１１３、プリンタ１１４はそれぞれ、制御部１００に含まれるスキャナ処理部１１１、プリンタ処理部１１２に接続される。操作部１０６は、制御部１００に含まれる操作部インタフェース（Ｉ／Ｆ）に接続される。そのような構成により、スキャナ処理部１１１、プリンタ処理部１１２、操作部１０６はそれぞれ、制御部１００から制御されて動作する。
【００１５】
制御部１００は、情報処理装置の各部を統括的に制御するＣＰＵ１０１を含む。ＣＰＵ１０１は、システムバス１０８を介して、ＲＡＭ１０２、不揮発記憶部１０３、ハードウェアディスクドライブ（ＨＤＤ）１０４、操作部Ｉ／Ｆ１０５、ネットワークＩ／Ｆ１０７と接続される。ＲＡＭ１０２は汎用的なＲＡＭであり、ＣＰＵ１０１のプログラムの格納領域および作業領域を提供するためのメモリである。またＲＡＭ１０２は、パラメータや設定データ等を一時的に記憶するためのメモリや、画像データをページ等、所定単位で記憶するための画像メモリとしても使用される。不揮発記憶部１０３は、例えばフラッシュ

メモリのような汎用的な不揮発メモリで、例えば図２に示すように、ブートプログラム２１０と各プログラムを更新するための更新プログラム２２０、工場出荷前に後述の設定データ２４２をコピーした工場出荷設定データ２３１等を格納している。ＨＤＤ１０４には、メインプログラム２４０、設定データ２４２、画像データ、テーブルなどが格納される。情報処理装置の機能は、例えば、ＣＰＵ１０１が不揮発記憶部１０３に格納されたブートプログラム２１０を実行し、ブートプログラム２１０が更新プログラム２３０、或いはメインプログラム２４０をＲＡＭ１０２に展開して実行することにより実現される。

【００１６】

操作部Ｉ／Ｆ１０５は、操作部１０６との間で情報の入出力を行うためのインタフェースである。操作部Ｉ／Ｆ１０５は、ＣＰＵ１０１からの指示により、表示データを操作部１０６へ出力し、またユーザが操作部１０６上で入力した情報を、ＣＰＵ１０１へ伝送する。ネットワークＩ／Ｆ１０７は、有線や無線媒体のＬＡＮ１１５と接続され、情報処理装置とＬＡＮ１１５上の機器との間の情報の入出力を可能にする。ネットワークＩ／Ｆ１０７は、ＬＡＮ１１５に対応した構成を有し、例えば、無線距離が数十ｃｍ程度の近距離無線通信（ＮｅａｒＦｉｅｌｄＣｏｍｍｕｎｉｃａｔｉｏｎ）に対応した構成を有する場合もある。その場合には、携帯無線端末との間で相互に通信が行われる。

【００１７】

画像処理部１０９は汎用的な画像処理を実行し、例えばＬＡＮ１１５を介して外部から取得した画像データに対して、拡大／縮小、回転、変換等の処理を実行する。また画像処理部１０９は、ＬＡＮ１１５を介して受信したＰＤＬコードをビットマップデータへ展開する処理を実行する。また画像処理部１０９は、プリンタ処理部１１２を介してプリンタ１１４で印刷する場合に、ＨＤＤ１０４に圧縮・符号化されて記憶されている画像データをプリンタ処理部１１２で処理可能な形式にするための処理を実行する。デバイスＩ／Ｆ１１０は、スキャナ処理部１１１及びプリンタ処理部１１２を介してスキャナ１１３やプリンタ１１４に接続され、画像データの同期系／非同期系の変換や、設定データ、調整値等を伝送する。またデバイスＩ／Ｆ１１０は、スキャナ１１３やプリンタ１１４の状態情報をＣＰＵ１０１へ伝送する。その状態情報は、例えば、スキャナ１１３やプリンタ１１４で発生したジャムなどのエラー情報を含む。

【００１８】

スキャナ処理部１１１は、スキャナ１１３で読み取られて入力される画像データに対して、補正、加工、像域分離、変倍、２値化処理などのスキャン機能に対応した各種処理を行う。スキャナ１１３は、不図示の自動連続原稿給送装置と圧板読取装置を含み、原稿ガラス台に設置された原稿の読取りや、複数枚の原稿の両面読取りなども実行できる。またスキャナ１１３は、不図示の原稿カバーの開閉、原稿の有無、原稿サイズの検知等を行うセンサを有している。それらのセンサによる検知信号やスキャナ１１３の状態情報は、スキャナ処理部１１１とデバイスＩ／Ｆ１１０を介してＣＰＵ１０１へ送信され、ＣＰＵ１０１は、スキャナ１１３でのエラー発生やエラー解除等の状態を認識できる。

【００１９】

プリンタ処理部１１２は、印刷する画像データに対して、プリンタ１１４の出力特性に対応した出力補正、解像度変換、画像の印刷位置の調整などのプリント機能に対応した処理を行う。プリンタ１１４は、用紙を収納するための給紙カセットを少なくとも１つ含む。各給紙カセットの用紙残量、トナーの有無などを検知するセンサがプリンタ１１４に設けられている。センサからの検知信号やプリンタ１１４の状態情報は、プリンタ処理部１１２とデバイスＩ／Ｆ１１０を介してＣＰＵ１０１へ送信され、ＣＰＵ１０１は、プリンタ１１４でのエラー発生やエラー解除等の状態を認識できる。

【００２０】

図２は、実施形態１に係る情報処理装置の不揮発記憶部１０３とＨＤＤ１０４に格納されているプログラム及びデータを説明する図である。

【００２１】

ＣＰＵ１０１は、情報処理装置に電源が投入されると、ブートプログラム２１０を実行し

起動処理を行う。このブートプログラムの中には、改ざん検知処理部２１１と改ざん検知用公開鍵２１２（復号鍵）が含まれる。改ざん検知用公開鍵２１２は、後述の更新プログラム用デジタル署名２３０、メインプログラム用デジタル署名２４１の作成に使用した秘密鍵と対をなす公開鍵である。秘密鍵は、例えば、情報処理装置の製造者が管理する秘密鍵である。

【００２２】

更新プログラム２２０のプログラム更新制御部２２１は、図示しない外部装置やインターネット上のサーバ等から、メインプログラム２４０、または、更新プログラム２２０の、更新用プログラムとそれと対をなすデジタル署名を取得し、不揮発記憶部１０３、ＨＤＤ１０４に格納されたプログラム、デジタル署名を書き換える。

【００２３】

更新プログラム用デジタル署名２３０は、一般的に知られたハッシュ関数を用いて更新プログラム２２０のハッシュ値を算出し、算出したハッシュ値を前述の秘密鍵により暗号化したデータである。更新プログラム用デジタル署名２３０は、ブートプログラム２１０の改ざん検知処理部２１１が、更新プログラム２２０をＲＡＭ１０２に展開して実行する前に使用される。改ざん検知処理部２１１は、更新プログラム２２０のハッシュ値を算出し、更に、改ざん検知用公開鍵２１２を用いて更新プログラム用デジタル署名２３０を復号してハッシュ値を取得する。そして、算出したハッシュ値と、復号して取得したハッシュ値が一致するか否かで、更新プログラム２２０が正当なプログラムであるか否かを判定する。

【００２４】

工場出荷設定データ２３１は、製造者が情報処理装置を出荷する前に、後述の設定データ２４２を格納したものである。改ざん検知フラグ２３２は、プログラム毎に、改ざん検知処理部２１１がプログラムの改ざんを検知した時にオン「１」にするフラグである。改ざん検知処理部２１１は、改ざん検知フラグがオンの状態でプログラムの正当性が確認できると、改ざん検知フラグをオフ「０」にする。

【００２５】

起動プログラム設定２３３は、ブートプログラム２１０が、更新プログラム２２０を起動するか、メインプログラム２４０を起動するかを判断するために使用する設定である。ユーザの指示に基づきメインプログラム２４０のプログラムの更新を行う際に、起動プログラム設定２３３を更新プログラムに設定する。そして更新プログラム２２０によりメインプログラムの更新が完了すると、起動プログラム設定２３３をメインプログラム２４０に設定する。

【００２６】

メインプログラム２４０は、制御部１００、操作部１０６、スキャナ１１３、プリンタ１１４を制御し、コピー機能を実現するコピー処理部、外部装置から送られているデータをプリントするプリント処理部などが含まれる。メインプログラム２４０には、プログラム以外に操作部に表示されるメッセージ用の言語データやプリントの色調整に使用するカラープロファイルといったデータが含まれていてもよい。

【００２７】

メインプログラム用デジタル署名２４１は、一般的に知られたハッシュ関数を用いてメインプログラム２４０のハッシュ値を算出し、算出したハッシュ値を前述の秘密鍵により暗号化したデータである。メインプログラム用デジタル署名２４１は、ブートプログラムの改ざん検知処理部２１１が、メインプログラム２４０をＲＡＭ１０２に展開し実行する前に使用する。改ざん検知処理部２１１は、メインプログラム２４０のハッシュ値を算出し、さらに、改ざん検知用公開鍵２１２を用いてメインプログラム用デジタル署名２４１を復号してハッシュ値を取得する。そして算出したハッシュ値と復号して取得したハッシュ値が一致するか否かで、メインプログラム２４０が正当なプログラムであるか否かを判定する。

【００２８】

設定データ２４２は、情報処理装置が動作するために必要なデータを格納している。例えば、装置固有のシリアル番号や、プリンタ１１４のレジ調整値、ユーザが設定するシステム管理者ＩＤやパスワード、といった情報処理装置のあらゆる情報を格納している。

【００２９】

図３は、実施形態１に係る情報処理装置が実行する処理を説明するフローチャートである。このフローチャートで示す処理は、ＣＰＵ１０１が不揮発記憶部１０３のブートプログラムを実行してＨＤＤ１０４に格納されているプログラムをＲＡＭ１０２に展開し、その展開したプログラムを実行することにより実現される。尚、この処理は、情報処理装置の電源を入れた際、或いは、更新プログラムがプログラムを書き換えた後などに情報処理装置を再起動することにより開始される。

【００３０】

まずＳ３０１でＣＰＵ１０１は、起動プログラム設定２３３に基づいて起動するプログラムを判定する。ここでメインプログラムを起動するように設定されていた場合はＳ３０２に進み、更新プログラムを起動するように設定されていた場合はＳ３０５に進む。Ｓ３０２でＣＰＵ１０１は、改ざん検知処理部２１１によって、メインプログラム２４０のハッシュ値を算出し、更に、改ざん検知用公開鍵２１２を用いてメインプログラム用デジタル署名２４１を復号してハッシュ値を取得する。そしてＳ３０３に進みＣＰＵ１０１は、算出したハッシュ値と復号して取得したハッシュ値とが一致するか否かに基づいて、メインプログラム２４０が改ざんされているか否かを判定する。ここで改ざんされた正当なプログラムではないと判定した場合はＳ３０４に進むが、正当なプログラムと判定した場合、つまり改ざんされていないと判定した場合はＳ３０９に進む。Ｓ３０４でＣＰＵ１０１は、改ざん検知フラグ２３２をオン「１」にしてＳ３０５に進む。

【００３１】

Ｓ３０５でＣＰＵ１０１は、改ざん検知処理部２１１によって、更新プログラム２２０のハッシュ値を算出し、更に、改ざん検知用公開鍵２１２を用いて更新プログラム用デジタル署名２３０を復号してハッシュ値を取得する。そしてＳ３０６に進みＣＰＵ１０１は、算出したハッシュ値と復号して取得したハッシュ値が一致するか否かに基づいて、更新プログラム２２０が正当なプログラムであるか否かを判定する。ここで正当なプログラムでないと判定した場合、つまり改ざんされていると判定した場合は、Ｓ３０８に進むが、正当なプログラムと判定した場合、つまり更新プログラム２２０が改ざんされていないと判定した場合はＳ３０７に進む。Ｓ３０７でＣＰＵ１０１は、ＲＡＭ１０２に更新プログラム２２０を展開して更新プログラム２２０を起動しフローチャートを終了する。

【００３２】

こうして更新プログラム２２０が起動されると、上述の外部装置やインターネット上のサーバ等からメインプログラム２４０をダウンロードして、改ざんされているメインプログラムを、正当なメインプログラムで更新する。こうしてメインプログラムの更新が終了すると、起動プログラム設定２３３を、メインプログラム２４０を起動するように設定して、情報処理装置が再起動される。そして、その場合は、Ｓ３０１→Ｓ３０２→Ｓ３０３→Ｓ３０９に処理が進むことになる。この処理は後述する。

【００３３】

一方、メインプログラム２４０と更新プログラム２２０の両方が改ざんされているときはＳ３０８に進みＣＰＵ１０１は、改ざん検知フラグ２３２をオン「１」にして、この処理を終了する。この場合、ユーザは、不揮発記憶部１０３の更新プログラム２２０と更新プログラム用デジタル署名２３０を正当な情報に書き換える。そして起動プログラム設定２３３を、更新プログラム２２０を起動するように設定して、情報処理装置を再起動する。その場合は、Ｓ３０１→Ｓ３０５→Ｓ３０６→Ｓ３０７に処理が進む。そして更新プログラム２２０が起動されると、上述の外部装置やインターネット上のサーバ等からメインプログラム２４０をダウンロードして、改ざんされているメインプログラムを、正当なメインプログラムで更新することができる。

【００３４】

一方、Ｓ３０３でメインプログラム２４０が正当なプログラムであると判定した場合はＳ３０９でＣＰＵ１０１は、改ざん検知フラグ２３２がオンか否かを判定する。ここで、改ざん検知フラグ２３２がオン「１」と判定した場合はＳ３１０に進み、オンでないと判定した場合はＳ３１２に進む。Ｓ３０３でメインプログラムの改ざんが検知できず、Ｓ３０９で改ざん検知フラグ２３２がオンということは、メインプログラムの改ざんを検知した後に、改ざんされたメインプログラムが書き換えられて復旧したことを意味する。従って、この場合は、Ｓ３１０でＣＰＵ１０１は、設定データ２４２の領域を工場出荷設定データ２３１に書き換える。即ち、設定データ２４２を初期データに初期化する。そしてＳ３１１に進んでＣＰＵ１０１は、改ざん検知フラグ２４２をオフ「０」にする。そしてＳ３１２に進みＣＰＵ１０１は、ＲＡＭ１０２にメインプログラムを展開し、そのメインプログラムを起動して、この処理を終了する。

【００３５】

以上説明したように実施形態１によれば、プログラムの改ざんを検出したときは、その設定データ等も初期データに書き換えることにより、情報処理装置のセキュリティを担保することができる。

【００３６】

［実施形態２］

上述の実施形態１では、プログラムの改ざんを検知し、プログラムの書き換えによって復旧した場合に、自動的に設定データ２４２を工場出荷設定データ２３１に書き換えていた。これに対して実施形態２では、自動的に設定データ２４２を書き換えるのではなく、ユーザの選択により書き換えを実行するかどうか選択できる例で説明する。尚、実施形態２に係る情報処理装置のハードウェア構成などは前述の実施形態１と同じであるため、その説明を省略する。

【００３７】

図４は、実施形態２に係る情報処理装置の操作部１０６に表示される、設定データ２４２を工場出荷設定データ２３１に書き換えるか否かをユーザに選択させる画面の一例を示す図である。

【００３８】

この画面４００で、ユーザが「はい」４０１を選択すると実施形態１と同様の処理が実行される。一方、ユーザが「いいえ」４０２を選択すると、設定データ２４２を工場出荷設定データ２３１に書き換えることなく、メインプログラムを起動する。

【００３９】

図５は、実施形態２に係る情報処理装置による処理を説明するフローチャートである。このフローチャートで示す処理は、ＣＰＵ１０１が不揮発記憶部１０３のブートプログラムを実行してＨＤＤ１０４に格納されているプログラムをＲＡＭ１０２に展開し、その展開したプログラムを実行することにより実現される。尚、この処理は、情報処理装置の電源を入れた際、或いは、更新プログラムがプログラムを書き換えた後などに情報処理装置を再起動することにより開始される。尚、図５において、前述の図３のフローチャートと共通する部分は同じ参照番号を付して、それらの説明を省略する。

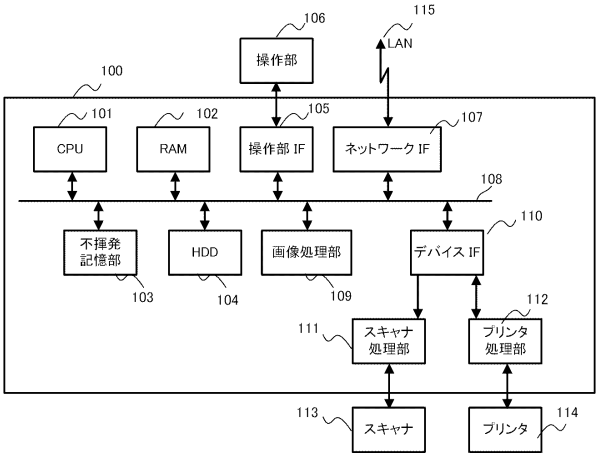
【００４０】

Ｓ３０３でＣＰＵ１０１は、メインプログラムの改ざんを検知しないときはＳ３０９に進みＣＰＵ１０１は、改ざん検知フラグ２３２がオンかどうか判定する。ここで改ざん検知フラグ２３２がオンのときはＳ５０１に進み、そうでないときはＳ３１２に進む。Ｓ３０３でメインプログラムの改ざんを検知せずにＳ３０９で改ざんフラグがオンということは、メインプログラムの改ざんを検知した後に、改ざんされたプメインログラムが書き換えられ復旧したことを意味している。Ｓ５０１でＣＰＵ１０１は、例えば図４に示すような、設定データ２４２を工場出荷設定データ２３１に書き換えるか否かを選択する画面４００を操作部１０６に表示させて、ユーザの選択結果を受け取る。ここで「はい」４０１が選択がされた場合はＳ３１０に進み、前述の実施形態１と同様の処理を行う。一方、「いいえ」４０２が選択がされた場合はＳ３１０をスキップしてＳ３１１に進み、ＣＰＵ１０

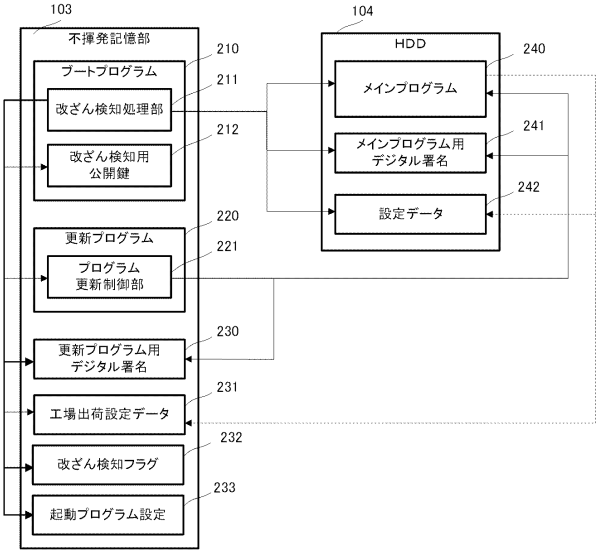
１は改ざん検知フラグ２４２をオフ「０」にしてＳ３１２に進む。
【００４１】
以上説明したように実施形態２によれば、情報処理装置がプログラムの改ざんを検知し、プログラムの書き換えによって復旧した際に、設定データのセキュリティを担保することが可能となった。また設定データを、工場出荷時の設定データに書き換えるかどうかをユーザが選択できるので、ユーザは、設定データが工場出荷時の設定データに書き換えられたかどうかを認識できる。
【００４２】
（その他の実施形態）
本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読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。
【００４３】
本発明は上記実施形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために、以下の請求項を添付する。
【符号の説明】
【００４４】
１０１…ＣＰＵ、１０３…不揮発記憶部、１０５…操作部、２１０…ブートプログラム、２１１…改ざん検知処理部、２１２…改ざん検知用公開鍵、２３０…更新プログラム用デジタル署名、２３１…工場出荷設定データ、２３２…改ざん検知フラグ、２４０…メインプログラム、２４１…メインプログラム用デジタル署名、２４２…設定データ

【図面】

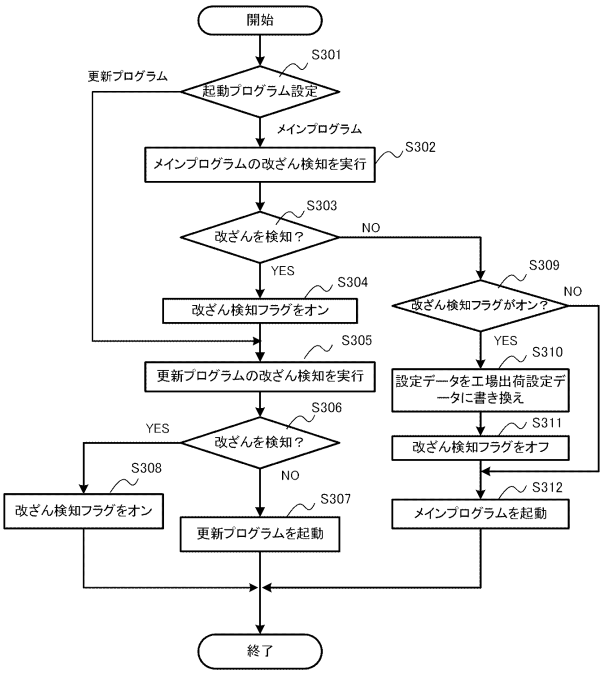
【図１】


106
操作部
115
LAN
100
101
CPU
102
RAM
105
操作部 IF
107
ネットワーク IF
108
110
不揮発
記憶部
103
HDD
104
画像処理部
109
デバイス IF
111
スキャナ
処理部
112
プリンタ
処理部
113
スキャナ
114
プリンタ

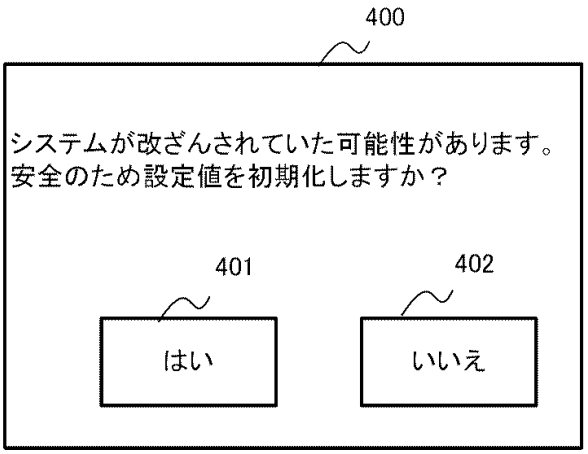
【図２】


103
不揮発記憶部
ブートプログラム
210
改ざん検知処理部
211
改ざん検知用
公開鍵
212
更新プログラム
220
プログラム
更新制御部
221
更新プログラム用
デジタル署名
230
工場出荷設定データ
231
改ざん検知フラグ
232
起動プログラム設定
233
104
HDD
240
メインプログラム
241
メインプログラム用
デジタル署名
242
設定データ

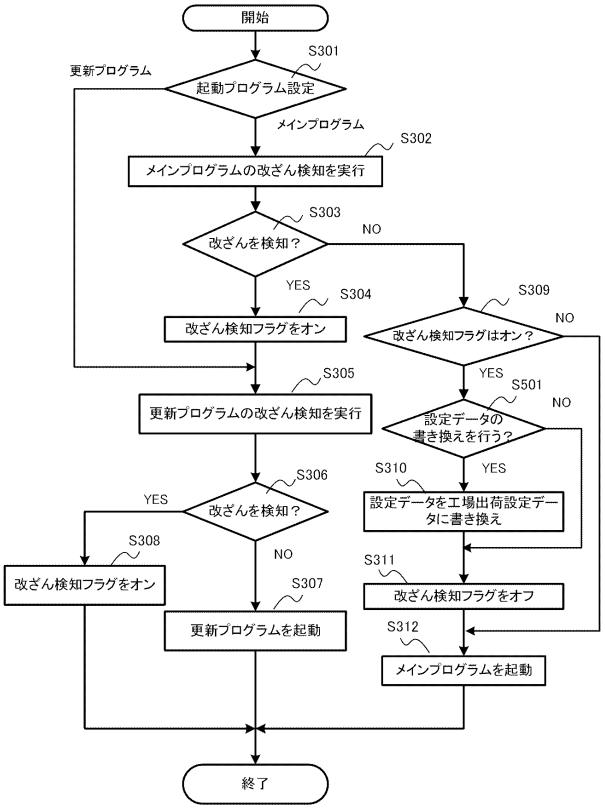
【図３】


開始
S301
更新プログラム
起動プログラム設定
メインプログラム
S302
メインプログラムの改ざん検知を実行
S303
改ざんを検知？
NO
YES
S304
改ざん検知フラグをオン
S309
改ざん検知フラグがオン？
NO
YES
S305
更新プログラムの改ざん検知を実行
S310
設定データを工場出荷設定データに書き換え
S306
YES
改ざんを検知？
S311
改ざん検知フラグをオフ
S308
NO
改ざん検知フラグをオン
S307
更新プログラムを起動
S312
メインプログラムを起動
終了

【図４】


400
システムが改ざんされていた可能性があります。
安全のため設定値を初期化しますか？
401
はい
402
いいえ

【図５】


開始
S301
起動プログラム設定
更新プログラム
メインプログラム
S302
メインプログラムの改ざん検知を実行
S303
改ざんを検知？
NO
YES
S304
改ざん検知フラグをオン
S309
改ざん検知フラグはオン？
NO
YES
S305
更新プログラムの改ざん検知を実行
S501
設定データの書き換えを行う？
NO
YES
S306
改ざんを検知？
YES
S310
設定データを工場出荷設定データに書き換え
S308
改ざん検知フラグをオン
NO
S307
更新プログラムを起動
S311
改ざん検知フラグをオフ
S312
メインプログラムを起動
終了

フロントページの続き

(56)参考文献 特開２０１１－１０８１６７（ＪＰ，Ａ）
特開２００６－２９３８８２（ＪＰ，Ａ）
特開２０１５－１５６０５５（ＪＰ，Ａ）
特開２０１１－０７９１３８（ＪＰ，Ａ）
特開２０１６－１９２１７５（ＪＰ，Ａ）
特開２０１０－１５２８７７（ＪＰ，Ａ）
特開２０１８－０８１５７７（ＪＰ，Ａ）
米国特許出願公開第２０１２／０１３７１２６（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／１２
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｆ ８／６５
Ｈ０４Ｎ １／００