

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-146338

(P2012-146338A)

(43) 公開日 平成24年8月2日(2012.8.2)

(51) Int.Cl. F I テーマコード (参考)  
**G06F 21/22 (2006.01)** G06F 21/22 112L 5B376  
**G06F 9/445 (2006.01)** G06F 9/06 610L

審査請求 有 請求項の数 13 O L (全 23 頁)

(21) 出願番号	特願2012-105954 (P2012-105954)	(71) 出願人	000006747
(22) 出願日	平成24年5月7日 (2012.5.7)		株式会社リコー
(62) 分割の表示	特願2008-36267 (P2008-36267)	(74) 代理人	100107766
	の分割		弁理士 伊東 忠重
原出願日	平成20年2月18日 (2008.2.18)	(74) 代理人	100070150
			弁理士 伊東 忠彦
		(72) 発明者	吉田 文幸
			東京都大田区中馬込1丁目3番6号 株式
			会社リコー内
		Fターム(参考)	5B376 AD11

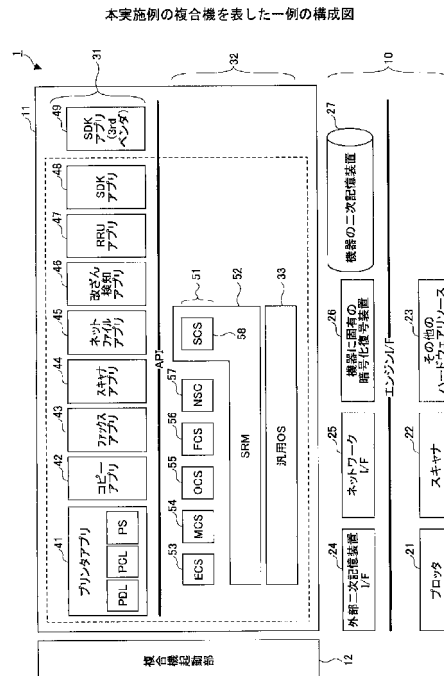
(54) 【発明の名称】 ソフトウェア改ざん検知方法、ソフトウェア改ざん検知プログラム及び機器

(57) 【要約】

【課題】 搭載されているソフトウェアの改ざんとソフトウェア構成の改ざんとを容易に検知可能なソフトウェア改ざん検知方法、ソフトウェア改ざん検知プログラム及び機器を提供することを目的とする。

【解決手段】 搭載されているソフトウェア11の改ざんを機器1が検知するソフトウェア改ざん検知方法であって、インストール手段が機器に固有の暗号化復号装置26を利用しインストール時における機器1のソフトウェア構成情報を暗号化して機器1の外部に保存する保存ステップと、改ざん検知手段46が機器の外部に保存したインストール時における機器のソフトウェア構成情報を機器に固有の暗号化復号装置26を利用して復号する復号ステップと、改ざん検知手段46がインストール時及び現在の機器のソフトウェア構成情報を比較し、ソフトウェア11の改ざんを検知する検知ステップとを有することにより上記課題を解決する。

【選択図】 図1



**【特許請求の範囲】****【請求項 1】**

機器に搭載されているソフトウェアの改ざんを前記機器が検知するソフトウェア改ざん検知方法であって、

前記ソフトウェアをインストールするインストール手段が、前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して前記機器の外部に保存する保存ステップと、

前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記機器の外部に保存したインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、

前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップと

を有することを特徴とするソフトウェア改ざん検知方法。

**【請求項 2】**

前記保存ステップは、前記インストール手段が、暗号化されている暗号鍵を、前記機器に固有の暗号化復号装置で復号するステップと、

前記インストール手段が、復号された暗号鍵で、インストール時における前記機器のソフトウェア構成情報を暗号化するステップと、

前記インストール手段が、暗号化された前記インストール時における前記機器のソフトウェア構成情報を前記機器の外部に保存するステップと

を有することを特徴とする請求項 1 記載のソフトウェア改ざん検知方法。

**【請求項 3】**

前記復号ステップは、前記改ざん検知手段が、暗号化されている前記インストール時における前記機器のソフトウェア構成情報を前記機器の外部から取得するステップと、

前記改ざん検知手段が、暗号化されている復号鍵を、前記機器に固有の暗号化復号装置で復号するステップと、

前記改ざん検知手段が、復号された復号鍵で、前記インストール時における前記機器のソフトウェア構成情報を復号するステップと

を有することを特徴とする請求項 1 又は 2 記載のソフトウェア改ざん検知方法。

**【請求項 4】**

前記検知ステップは、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報が一致しないときに前記ソフトウェアの改ざんを検知することを特徴とする請求項 1 乃至 3 何れか一項記載のソフトウェア改ざん検知方法。

**【請求項 5】**

前記機器に固有の暗号化復号装置は、内部から取り出しができない他の暗号 / 復号鍵を有しており、平文を前記他の暗号鍵で暗号化して返すインターフェースと、暗号化されたデータを前記他の復号鍵で復号して返すインターフェースとを有することを特徴とする請求項 1 乃至 4 何れか一項記載のソフトウェア改ざん検知方法。

**【請求項 6】**

前記インストール時における前記機器のソフトウェア構成情報はインストール用ファイル群に含まれることを特徴とする請求項 1 乃至 5 何れか一項記載のソフトウェア改ざん検知方法。

**【請求項 7】**

前記インストール時における前記機器のソフトウェア構成情報はインストール用ファイル群を用いて前記ソフトウェアをインストールしたあと、ファイル構成を取得するコマンドにより生成されることを特徴とする請求項 1 乃至 5 何れか一項記載のソフトウェア改ざん検知方法。

10

20

30

40

50

## 【請求項 8】

前記インストール時における前記機器のソフトウェア構成情報は携帯可能な記録媒体に保存されることを特徴とする請求項 1 乃至 7 何れか一項記載のソフトウェア改ざん検知方法。

## 【請求項 9】

前記インストール時における前記機器のソフトウェア構成情報はネットワーク経由で接続された外部サーバに保存されることを特徴とする請求項 1 乃至 7 何れか一項記載のソフトウェア改ざん検知方法。

## 【請求項 10】

前記機器の起動時又は前記機器を操作する操作者からの指示により、前記機器が前記ソフトウェアの改ざんを検知することを特徴とする請求項 1 乃至 9 何れか一項記載のソフトウェア改ざん検知方法。

10

## 【請求項 11】

搭載されているソフトウェアの改ざんを検知する機器に、

前記ソフトウェアをインストールするインストール手段が、前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して前記機器の外部に保存する保存ステップと、

前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記機器の外部に保存したインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、

20

前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップと

を実行させるためのソフトウェア改ざん検知プログラム。

## 【請求項 12】

前記保存ステップは、前記機器に、

前記インストール手段が、暗号化されている暗号鍵を、前記機器に固有の暗号化復号装置で復号するステップと、

前記インストール手段が、復号された暗号鍵で、インストール時における前記機器のソフトウェア構成情報を暗号化するステップと、

30

前記インストール手段が、暗号化された前記インストール時における前記機器のソフトウェア構成情報を前記機器の外部に保存するステップと

を実行させるための請求項 11 記載のソフトウェア改ざん検知プログラム。

## 【請求項 13】

前記復号ステップは、前記機器に、

前記改ざん検知手段が、暗号化されている前記インストール時における前記機器のソフトウェア構成情報を前記機器の外部から取得するステップと、

前記改ざん検知手段が、暗号化されている復号鍵を、前記機器に固有の暗号化復号装置で復号するステップと、

前記改ざん検知手段が、復号された復号鍵で、前記インストール時における前記機器のソフトウェア構成情報を復号するステップと

40

を実行させるための請求項 11 又は 12 記載のソフトウェア改ざん検知プログラム。

## 【請求項 14】

前記検知ステップは、前記機器に、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報が一致しないときに前記ソフトウェアの改ざんを検知させることを特徴とする請求項 11 乃至 13 何れか一項記載のソフトウェア改ざん検知プログラム。

## 【請求項 15】

前記機器に固有の暗号化復号装置は、内部から取り出しができない他の暗号 / 復号鍵を

50

有しており、平文を前記他の暗号鍵で暗号化して返すインターフェースと、暗号化されたデータを前記他の復号鍵で復号して返すインターフェースとを有することを特徴とする請求項 1 1 乃至 1 4 何れか一項記載のソフトウェア改ざん検知プログラム。

【請求項 1 6】

搭載されているソフトウェアの改ざんを検知する機器であって、  
前記機器に固有の暗号化復号装置と、  
前記ソフトウェアをインストールするインストール手段と、  
前記ソフトウェアの改ざんを検知する改ざん検知手段と  
を有し、

前記インストール手段は、前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して前記機器の外部に保存し、

前記改ざん検知手段は、前記機器の外部に保存したインストール時における前記機器のソフトウェア構成情報を前記機器に固有の暗号化復号装置を利用して復号し、前記インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較して、前記ソフトウェアの改ざんを検知することを特徴とする機器。

10

【請求項 1 7】

前記インストール手段は、暗号化されている暗号鍵を、前記機器に固有の暗号化復号装置で復号し、復号された暗号鍵で、インストール時における前記機器のソフトウェア構成情報を暗号化し、暗号化された前記インストール時における前記機器のソフトウェア構成情報を前記機器の外部に保存することを特徴とする請求項 1 6 記載の機器。

20

【請求項 1 8】

前記改ざん検知手段は、暗号化されている前記インストール時における前記機器のソフトウェア構成情報を前記機器の外部から取得し、暗号化されている復号鍵を前記機器に固有の暗号化復号装置で復号し、復号された復号鍵で前記インストール時における前記機器のソフトウェア構成情報を復号することを特徴とする請求項 1 6 又は 1 7 記載の機器。

【請求項 1 9】

前記改ざん検知手段は、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とが一致しないときに前記ソフトウェアの改ざんを検知することを特徴とする請求項 1 6 乃至 1 8 何れか一項記載の機器。

30

【請求項 2 0】

前記機器に固有の暗号化復号装置は、内部から取り出しができない他の暗号 / 復号鍵を有しており、平文を前記他の暗号鍵で暗号化して返すインターフェースと、暗号化されたデータを前記他の復号鍵で復号して返すインターフェースとを有することを特徴とする請求項 1 6 乃至 1 9 何れか一項記載の機器。

【請求項 2 1】

前記インストール時における前記機器のソフトウェア構成情報はインストール用ファイル群に含まれることを特徴とする請求項 1 6 乃至 2 0 何れか一項記載の機器。

40

【請求項 2 2】

前記インストール時における前記機器のソフトウェア構成情報はインストール用ファイル群を用いて前記ソフトウェアをインストールしたあと、ファイル構成を取得するコマンドにより生成されることを特徴とする請求項 1 6 乃至 2 0 何れか一項記載の機器。

【請求項 2 3】

前記インストール時における前記機器のソフトウェア構成情報は携帯可能な記録媒体に保存されることを特徴とする請求項 1 6 乃至 2 2 何れか一項記載の機器。

【請求項 2 4】

前記インストール時における前記機器のソフトウェア構成情報はネットワーク経由で接続された外部サーバに保存されることを特徴とする請求項 1 6 乃至 2 2 何れか一項記載の

50

機器。

【請求項 25】

前記機器の起動時又は前記機器を操作する操作者からの指示により、前記ソフトウェアの改ざんを検知することを特徴とする請求項 16 乃至 24 何れか一項記載の機器。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ソフトウェア改ざん検知方法、ソフトウェア改ざん検知プログラム及び機器に係り、特に搭載されているソフトウェアの改ざんを検知するソフトウェア改ざん検知方法、ソフトウェア改ざん検知プログラム及び機器に関する。

10

【背景技術】

【0002】

例えば機器に搭載されているファームウェア（ソフトウェア）の改ざん検知方法としては従来からハッシュ値による改ざん検知方法が良く知られている（例えば特許文献 1 乃至 3 参照）。

【0003】

従来のハッシュ値による改ざん検知方法は、ファームウェアを機器へインストールするときに、そのファームウェアのハッシュ値を計算し、機器の二次記憶装置に予め保存しておく。そして、機器の起動時、従来のハッシュ値による改ざん検知方法はファームウェアのハッシュ値を再計算し、二次記憶装置に予め保存してあるハッシュ値と比較して不一致であれば改ざんがなされたものと判定し、異常時の処理を行っていた。

20

【発明の概要】

【発明が解決しようとする課題】

【0004】

従来のハッシュ値による改ざん検知方法は確かにファームウェア自体になされた改ざんを検知できる。しかし、従来のハッシュ値による改ざん検知方法はファームウェアとともに機器の二次記憶装置等に保存してあるハッシュ値も改ざんされると、ファームウェアの改ざんを検知できないという問題があった。

【0005】

また、従来のハッシュ値による改ざん検知方法はファームウェアとともに機器の二次記憶装置等に保存してあるハッシュ値も削除されると、ファームウェアの削除を検知できないという問題があった。上記問題は、ハッシュ値が個々のファームウェアの改ざんを検知できても機器全体のファームウェアの構成が変更されたことを検知できないことに起因するものである。

30

【0006】

ファームウェアとともに機器の二次記憶装置等に保存してあるハッシュ値も改ざんされるとファームウェアの改ざんを検知できないという上記問題については機器内に暗号／復号鍵を用意し、機器の二次記憶装置等に保存するハッシュ値を暗号化しておくことでハッシュ値の改ざんを防ぐことも考えられる。

【0007】

しかし、暗号／復号鍵が機器の二次記憶装置等に保存されるため、機器の二次記憶装置等に保存するハッシュ値を暗号化しておく改ざん検知方法は、悪意の第三者が、機器の二次記憶装置等から復号鍵を不正に入手し、暗号化されたハッシュ値を復号可能という問題が残されている。

40

【0008】

このように、従来のハッシュ値による改ざん検知方法は機器内に保存したハッシュ値の改ざんに対して無力であった。また、従来のハッシュ値による改ざん検知方法は機器全体のファームウェアの構成の改ざんに対して無力であった。さらに、従来のハッシュ値による改ざん検知方法は、改ざんを防ぐ為の暗号化によっても、上記のハッシュ値の改ざんや機器全体のファームウェアの構成の改ざんを完全に検知できるものではなかった。

50

## 【 0 0 0 9 】

本発明は上記の点に鑑みなされたもので、搭載されているソフトウェアの改ざんとソフトウェア構成の改ざんとを容易に検知可能なソフトウェア改ざん検知方法、ソフトウェア改ざん検知プログラム及び機器を提供することを目的とする。

## 【 課題を解決するための手段 】

## 【 0 0 1 0 】

上記課題を解決するため、本発明は、機器に搭載されているソフトウェアの改ざんを前記機器が検知するソフトウェア改ざん検知方法であって、前記ソフトウェアをインストールするインストール手段が、前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して前記機器の外部に保存する保存ステップと、前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記機器の外部に保存したインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップとを有することを特徴とする。

10

## 【 0 0 1 1 】

また、本発明は、搭載されているソフトウェアの改ざんを検知する機器に、前記ソフトウェアをインストールするインストール手段が、前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して前記機器の外部に保存する保存ステップと、前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記機器の外部に保存したインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップとを実行させるためのソフトウェア改ざん検知プログラムであることを特徴とする。

20

## 【 0 0 1 2 】

また、本発明は、搭載されているソフトウェアの改ざんを検知する機器であって、前記機器に固有の暗号化復号装置と、前記ソフトウェアをインストールするインストール手段と、前記ソフトウェアの改ざんを検知する改ざん検知手段とを有し、前記インストール手段は、前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して前記機器の外部に保存し、前記改ざん検知手段は、前記機器の外部に保存したインストール時における前記機器のソフトウェア構成情報を前記機器に固有の暗号化復号装置を利用して復号し、前記インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較して、前記ソフトウェアの改ざんを検知することを特徴とする。

30

## 【 0 0 1 3 】

なお、本発明の構成要素、表現または構成要素の任意の組合せを、方法、装置、システム、コンピュータプログラム、記録媒体、データ構造などに適用したのも本発明の態様として有効である。

40

## 【 発明の効果 】

## 【 0 0 1 4 】

本発明によれば、搭載されているソフトウェアの改ざんとソフトウェア構成の改ざんとを容易に検知可能なソフトウェア改ざん検知方法、ソフトウェア改ざん検知プログラム及び機器を提供可能である。

## 【 図面の簡単な説明 】

## 【 0 0 1 5 】

【 図 1 】 本実施例の複合機を表した一例の構成図である。

【 図 2 】 機器に固有の暗号化復号装置の特徴について説明する為の模式図である。

【 図 3 】 機器に固有の暗号化復号装置がある場合の暗号化データ保存方法について説明す

50

る為の模式図である。

【図 4】機器に固有の暗号化復号装置がある場合の暗号化データ復号方法について説明する為のシーケンス図である。

【図 5】本実施例の複合機にファームウェアを書き込む処理を説明する為のブロック図である。

【図 6】本実施例の複合機にファームウェアを書き込む処理を説明する為のシーケンス図である。

【図 7】本実施例の複合機に搭載されているファームウェアの改ざんを検知する処理を説明する為のシーケンス図である。

【図 8】実施例 1 の複合機を表した一例の構成図である。

10

【図 9】実施例 1 の複合機にファームウェアを書き込む処理を説明する為のブロック図である。

【図 10】実施例 1 の複合機にファームウェアを書き込む処理を説明する為のシーケンス図である。

【図 11】バージョンファイルの暗号化処理の手順を示すフローチャートである。

【図 12】実施例 1 の複合機におけるファームウェアの改ざんを検知する処理を説明する為のフローチャートである。

【図 13】改ざんを検知したときにオペレーションパネルに表示される画面の一例を表したイメージ図である。

【図 14】改ざんを検知しないときにオペレーションパネルに表示される画面の一例を表したイメージ図である。

20

【図 15】改ざんを検知したときにオペレーションパネルに表示される画面の一例を表したイメージ図である。

【図 16】実施例 2 の複合機を表した一例の構成図である。

【図 17】実施例 2 の複合機にファームウェアを書き込む処理を説明する為のブロック図である。

【図 18】実施例 2 の複合機にファームウェアを書き込む処理を説明する為のシーケンス図である。

【図 19】ファイル構成スナップショットの暗号化処理の手順を示すフローチャートである。

30

【図 20】実施例 2 の複合機におけるファームウェアの改ざんを検知する処理を説明する為のフローチャートである。

【発明を実施するための形態】

【0016】

次に、本発明を実施する為の最良の形態を、以下の実施例に基づき図面を参照しつつ説明していく。なお、本実施例では搭載されているソフトウェアの改ざんを検知する機器の一例として複合機を例に説明するが、ソフトウェア（ファームウェア）が搭載された組み込み機器等、如何なる機器であってもよい。

【0017】

図 1 は本実施例の複合機を表した一例の構成図である。図 1 の複合機 1 は種々のハードウェア 10 と、種々のソフトウェア 11 と、複合機起動部 12 とを含む構成である。

40

【0018】

ハードウェア 10 はプロッタ 21 と、スキャナ 22 と、その他のハードウェアリソース 23 と、外部二次記憶装置 I/F（インターフェース）24 と、ネットワーク I/F 25 と、機器に固有の暗号化復号装置 26 と、機器の二次記憶装置 27 とを含む構成である。

【0019】

外部二次記憶装置 I/F 24 は、例えば SD カードを外部から接続する為の SD カードスロットのように何らかの二次記憶装置を外部から接続する I/F である。ネットワーク I/F 25 は例えばインターネットや LAN 等のネットワーク経由で外部サーバ等の二次記憶装置に接続する I/F である。機器に固有の暗号化復号装置 26 は、例えばセキュリ

50

ティチップである T P M ( Trusted Platform Module ) により実現される。なお、機器に固有の暗号化復号装置 2 6 の詳細は後述する。

【 0 0 2 0 】

ソフトウェア 1 1 は、種々のアプリケーション 3 1 と、プラットフォーム 3 2 と、汎用 O S ( オペレーティングシステム ) 3 3 とを含む構成である。種々のアプリケーション 3 1 とプラットフォーム 3 2 とを構成するプログラムは、U N I X ( 登録商標 ) 等の汎用 O S 3 3 によりプロセス単位で並列的に実行される。

【 0 0 2 1 】

アプリケーション 3 1 は、プリンタアプリ 4 1 と、コピーアプリ 4 2 と、ファックスアプリ 4 3 と、スキャナアプリ 4 4 と、ネットファイルアプリ 4 5 と、改ざん検知アプリ 4 6 と、R R U アプリ 4 7 と、S D K アプリ 4 8 と、サードベンダの S D K アプリ 4 9 とを含む構成である。S D K アプリ 4 8 とサードベンダの S D K アプリ 4 9 とは、専用の S D K ( ソフトウェア開発キット ) を使用して開発されたプログラムである。なお、改ざん検知アプリ 4 6 の詳細は後述する。

10

【 0 0 2 2 】

プラットフォーム 3 2 は種々のコントロールサービス 5 1 と S R M ( システムリソースマネージャ ) 5 2 とを含む構成である。また、コントロールサービス 5 1 は E C S ( エンジンコントロールサービス ) 5 3 と、M C S ( メモリコントロールサービス ) 5 4 と、O C S ( オペレーションパネルコントロールサービス ) 5 5 と、F C S ( ファクシミリコントロールサービス ) 5 6 と、N C S ( ネットワークコントロールサービス ) 5 7 と、S C S ( システムコントロールサービス ) 5 8 とを含む構成である。なお、プラットフォーム 3 2 を構成するプログラムの詳細は例えば特開 2 0 0 2 - 8 4 3 8 3 号公報に記載されている為、説明を省略する。

20

【 0 0 2 3 】

複合機起動部 1 2 は、複合機 1 の電源投入時に最初に実行される。これにより、複合機 1 では汎用 O S 3 3 が起動され、アプリケーション 3 1 やプラットフォーム 3 2 が起動される。種々のアプリケーション 3 1 とプラットフォーム 3 2 とを構成するプログラムは H D D ( ハードディスクドライブ ) やメモリカード等の機器の二次記憶装置 2 7 に記憶されており、H D D やメモリカードから読み出されて、メモリ上で起動されることになる。

【 0 0 2 4 】

図 2 は機器に固有の暗号化復号装置の特徴について説明する為の模式図である。機器に固有の暗号化復号装置 2 6 は、ルート鍵 6 1 と、二つの I / F 6 2 , 6 3 とを含む構成である。ルート鍵 6 1 は、機器に固有の暗号化復号装置 2 6 から取り出すことのできない暗号 / 復号鍵である。機器に固有の暗号化復号装置 2 6 は、ルート鍵 6 1 を用いた暗号化復号処理機能を有する。

30

【 0 0 2 5 】

I / F 6 2 は平文データをルート鍵 6 1 で暗号化して返す I / F である。I / F 6 3 は暗号化された平文データをルート鍵 6 1 で復号して返す I / F である。なお、機器に固有の暗号化復号装置 2 6 はハードウェアが基板に直付けされており、且つ、取り外して別の機器に取り付けても利用できない。

40

【 0 0 2 6 】

図 3 は機器に固有の暗号化復号装置がある場合の暗号化データ保存方法について説明する為の模式図である。機器の二次記憶装置 2 7 にはルート鍵 6 1 で暗号化済の暗号 / 復号鍵と、暗号鍵で暗号化済の暗号化データとが記憶されている。機器の二次記憶装置 2 7 に記憶されている暗号化データは、図 4 のシーケンス図に示す処理手順に従い復号されて利用される。

【 0 0 2 7 】

図 4 は、機器に固有の暗号化復号装置がある場合の暗号化データ復号方法について説明する為のシーケンス図である。なお、以下の説明では、暗号化されたデータを「データ名称 + B L O B 」と言う。例えば暗号化された暗号 / 復号鍵は、鍵 B L O B とする。

50

## 【0028】

ステップS1に進み、データを使うソフト71は、鍵BLOBを機器に固有の暗号化復号装置26に送信し、ルート鍵61で復号させる。ステップS2に進み、機器に固有の暗号化復号装置26は、鍵BLOBから復号した復号鍵を、データを使うソフト71に送信する。ステップS3に進み、データを使うソフト71は受信した復号鍵で暗号化データを復号する。

## 【0029】

図3に示した暗号化データ保存方法は、機器の二次記憶装置27をまるごと取り外して別の機器に移動しても機器の二次記憶装置27に記憶されている鍵BLOBを復号できないため、暗号化データの解読もできない。また、図3に示した暗号化データ保存方法は機器に固有の暗号化復号装置26からルート鍵61を取り出すことができない為、ルート鍵61を盗まれる危険もない。

10

## 【0030】

なお、機器に固有の暗号化復号装置がない場合の従来の暗号化データ保存方法では、暗号/復号鍵と暗号化データとが両方、機器の二次記憶装置27に記憶されている為、機器の二次記憶装置27をまるごと取り外して別の機器に移動すると、機器の二次記憶装置27に記憶されている復号鍵で暗号化データを解読できてしまう。

## 【0031】

図5は本実施例の複合機にファームウェアを書き込む処理を説明する為のブロック図である。なお、図5のブロック図は説明に不要な部分を適宜省略している。

20

## 【0032】

複合機1のインストールアプリ80は、種々のファームウェア82を複合機1に書き込む(インストールする)為のツールである。種々のファームウェア82はインストール用ファイル群81に含まれる。また、インストール用ファイル群81にはルート鍵61で暗号化した暗号/復号鍵である鍵BLOB83と、ファームウェア構成情報84とが更に含まれる。なお、ファームウェア構成情報84はインストール用ファイル群81に含まれていてもよいし、生成してもよい。

## 【0033】

ファームウェア構成情報84は、複合機1に書き込む種々のファームウェア82を一意に特定する為の情報である。例えばファームウェア構成情報84は機器の二次記憶装置27のファイル構成リスト(UNIX(登録商標)のlsを実施した結果など)やファームウェア82のバージョン情報等である。

30

## 【0034】

図6は本実施例の複合機にファームウェアを書き込む処理を説明する為のシーケンス図である。ステップS11に進み、インストールアプリ80はインストール用ファイル群81を機器の二次記憶装置27に書き込む。ステップS12に進み、インストールアプリ80はインストール用ファイル群81に含まれる鍵BLOB83を機器に固有の暗号化復号装置26に送信し、ルート鍵61で鍵BLOBを復号させ、暗号鍵を得る。

## 【0035】

ステップS13に進み、インストールアプリ80はファームウェア構成情報84を暗号鍵で暗号化し、ファームウェア構成情報BLOBを生成する。ステップS14及びS15に進み、インストールアプリ80はファームウェア構成情報BLOBを、外部二次記憶装置I/F24経由で接続されるSDカードやネットワークI/F25経由で接続される外部サーバ等の外部の二次記憶装置91に保存する。

40

## 【0036】

本実施例の複合機1では、複合機1以外の外部の二次記憶装置91に保存しておくことで悪意の第三者による改ざんを防ぐことができる。

## 【0037】

図7は本実施例の複合機に搭載されているファームウェアの改ざんを検知する処理を説明する為のシーケンス図である。なお、ファームウェアの改ざんを検知する処理を実行す

50

るときの複合機 1 の構成は図 1 と同様である。

【 0 0 3 8 】

ステップ S 2 1 に進み、改ざん検知アプリ 4 6 は機器の二次記憶装置 2 7 から鍵 B L O B 8 3 を取り出す。ステップ S 2 2 に進み、改ざん検知アプリ 4 6 は鍵 B L O B 8 3 を機器に固有の暗号化復号装置 2 6 に送信し、ルート鍵 6 1 で鍵 B L O B を復号させ、復号鍵を得る。ステップ S 2 3 に進み、改ざん検知アプリ 4 6 は、外部の二次記憶装置 9 1 からファームウェア構成情報 B L O B を取り出す。ステップ S 2 4 に進み、改ざん検知アプリ 4 6 はファームウェア構成情報 B L O B を復号鍵で復号して、ファームウェア構成情報 8 4 を得る。

【 0 0 3 9 】

そして、ステップ S 2 5 に進み、改ざん検知アプリ 4 6 は、現在の複合機 1 に搭載されている種々のアプリケーション 3 1 のファームウェア構成情報と、ファームウェア構成情報 B L O B を復号鍵で復号して得たファームウェア構成情報 8 4 とを比較し、その比較結果が異なるときに、改ざんがあったことを検知する。なお、ステップ S 2 5 の処理の具体的内容は後述する。

【 実施例 1 】

【 0 0 4 0 】

実施例 1 の複合機 1 は、搭載されているファームウェアの改ざんを検知する処理を起動時に毎回実行するものとする。また、ファームウェア構成情報は「各ファームウェア 8 2 のバージョン文字列を格納したテキストファイル」であるものとする。さらに、外部の二次記憶装置 9 1 は U S B メモリや S D カード等の「携帯可能な二次記憶装置」であるものとする。

【 0 0 4 1 】

図 8 は実施例 1 の複合機を表した一例の構成図である。図 8 の複合機 1 はネットワーク I / F 2 5 が無い点で図 1 の構成図と異なる。

【 0 0 4 2 】

図 9 は実施例 1 の複合機にファームウェアを書き込む処理を説明する為のブロック図である。図 9 のブロック図はファームウェア構成情報 8 4 がバージョンファイル 8 6 に置き換えられている点で図 5 のブロック図と異なっている。バージョンファイル 8 6 は、対応するファームウェア 8 2 のバージョン文字列が記載されたテキストファイルである。

【 0 0 4 3 】

バージョンファイル 8 6 は、ファームウェア 8 2 を複合機 1 にインストールする前に予め手動または自動で生成されるファイルである。インストールアプリ 8 0 は、バージョンファイル 8 6 の生成に関与しない。バージョンファイル 8 6 は、ファームウェア構成情報 8 4 の一例である。

【 0 0 4 4 】

図 1 0 は実施例 1 の複合機にファームウェアを書き込む処理を説明する為のシーケンス図である。ステップ S 3 1 に進み、インストールアプリ 8 0 はインストール用ファイル群 8 5 を機器の二次記憶装置 2 7 に書き込む。ステップ S 3 2 に進み、インストールアプリ 8 0 は図 1 1 に示すバージョンファイル 8 6 の暗号化処理を行う。図 1 1 は、バージョンファイルの暗号化処理の手順を示すフローチャートである。

【 0 0 4 5 】

ステップ S 4 1 に進み、インストールアプリ 8 0 はインストール用ファイル群 8 5 に含まれる鍵 B L O B 8 3 を機器に固有の暗号化復号装置 2 6 に送信し、ルート鍵 6 1 で鍵 B L O B を復号させ、暗号鍵を得る。ステップ S 4 2 に進み、インストールアプリ 8 0 は全てのバージョンファイル 8 6 を出力したか否かを判定する。

【 0 0 4 6 】

全てのバージョンファイル 8 6 を出力していない（出力していないバージョンファイル 8 6 が残っていると判定すると、インストールアプリ 8 0 はステップ S 4 3 に進み、インストール用ファイル群 8 5 に含まれるバージョンファイル 8 6 を一つ選択する。

10

20

30

40

50

## 【 0 0 4 7 】

ステップ S 4 4 に進み、インストールアプリ 8 0 は選択したバージョンファイル 8 6 の中身を「バージョン出力ファイル」に出力し、ステップ S 4 2 に戻る。インストールアプリ 8 0 は、全てのバージョンファイル 8 6 の中身を「バージョン出力ファイル」に出力するまでステップ S 4 2 ~ S 4 4 の処理を繰り返し行う。全てのバージョンファイル 8 6 を出力した（出力していないバージョンファイル 8 6 が残っていない）と判定すると、インストールアプリ 8 0 はステップ S 4 5 に進み、バージョン出力ファイルを暗号鍵で暗号化してバージョン出力ファイル B L O B を生成する。

## 【 0 0 4 8 】

図 1 0 のステップ S 3 3 に進み、インストールアプリ 8 0 はバージョン出力ファイル B L O B を、外部二次記憶装置 I / F 2 4 経由で接続される S D カード等の携帯可能な二次記憶装置 1 0 1 に保存する。携帯可能な二次記憶装置 1 0 1 は、複合機 1 に搭載されているアプリケーション（ファームウェア）3 1 の改ざんを検知する時に、複合機 1 に取り付けられるものである。

10

## 【 0 0 4 9 】

実施例 1 の複合機 1 では、複合機 1 以外の携帯可能な二次記憶装置 1 0 1 にバージョン出力ファイル B L O B を保存しておくことで、悪意の第三者による改ざんを防ぐことができる。

## 【 0 0 5 0 】

図 1 2 は実施例 1 の複合機におけるファームウェアの改ざんを検知する処理を説明する為のフローチャートである。なお、ファームウェアの改ざんを検知する処理を実行するときの複合機 1 の構成は図 8 と同様である。

20

## 【 0 0 5 1 】

ステップ S 5 1 に進み、改ざん検知アプリ 4 6 は機器の二次記憶装置 2 7 から鍵 B L O B 8 3 を取り出す。ステップ S 5 2 に進み、改ざん検知アプリ 4 6 は鍵 B L O B 8 3 を機器に固有の暗号化復号装置 2 6 に送信し、ルート鍵 6 1 で鍵 B L O B を復号させ、復号鍵を得る。ステップ S 5 3 に進み、改ざん検知アプリ 4 6 は、外部二次記憶装置 I / F 2 4 経由で接続される携帯可能な二次記憶装置 1 0 1 からバージョン出力ファイル B L O B を取り出す。ステップ S 5 4 に進み、改ざん検知アプリ 4 6 はバージョン出力ファイル B L O B を復号鍵で復号し、バージョン出力ファイルを得る。

30

## 【 0 0 5 2 】

ステップ S 5 5 に進み、改ざん検知アプリ 4 6 は機器の二次記憶装置 2 7 に記憶されている現在の複合機 1 に搭載されている種々のファームウェアのバージョンファイル 8 6 を全て調査したか否かを判定する。

## 【 0 0 5 3 】

全てのバージョンファイル 8 6 を調査していない（調査していないバージョンファイル 8 6 が残っている）と判定すると、改ざん検知アプリ 4 6 はステップ S 5 6 に進み、機器の二次記憶装置 2 7 からバージョンファイル 8 6 を一つ取り出す。改ざん検知アプリ 4 6 はステップ S 5 7 に進み、取り出したバージョンファイル 8 6 からバージョン文字列を取り出す。

40

## 【 0 0 5 4 】

ステップ S 5 8 に進み、改ざん検知アプリ 4 6 はステップ S 5 4 で得たバージョン出力ファイルから、該当するファームウェアのバージョン文字列を取り出す。ステップ S 5 9 に進み、改ざん検知アプリ 4 6 はステップ S 5 7 で取り出したバージョン文字列とステップ S 5 8 で取り出したバージョン文字列とを比較し、一致しているか否かを判定する。

## 【 0 0 5 5 】

ステップ S 5 9 は現在の複合機 1 に搭載されている種々のファームウェアのバージョン文字列と、インストール時、複合機 1 に搭載された種々のファームウェアのバージョン文字列とが一致しているか否かを判定するものである。

## 【 0 0 5 6 】

50

ステップ S 5 9 においてバージョン文字列が一致していれば、改ざん検知アプリ 4 6 はステップ S 5 5 に戻る。なお、ステップ S 5 9 においてバージョン文字列が一致していなければファームウェアが改ざんされたと判定し、改ざん検知アプリ 4 6 はステップ S 6 0 に進み、図 1 3 に示すような画面をオペレーションパネル等に出力して、複合機 1 を停止する。

【 0 0 5 7 】

図 1 3 は改ざんを検知したときにオペレーションパネルに表示される画面の一例を表したイメージ図である。図 1 3 の画面には、操作者に異常を検知した旨を通知する為のコメントと、異常を検知したファームウェアの情報とが含まれる。

【 0 0 5 8 】

また、ステップ S 5 5 において、全てのバージョンファイル 8 6 を調査した（調査していないバージョンファイル 8 6 が残っていない）と判定すると、改ざん検知アプリ 4 6 はステップ S 6 1 に進み、バージョン出力ファイルに未調査のバージョン文字列が残っていないか否かを判定する。

【 0 0 5 9 】

バージョン出力ファイルに未調査のバージョン文字列が残っていなければ、改ざん検知アプリ 4 6 はステップ S 6 2 に進み、図 1 4 に示すような画面をオペレーションパネル等に出力して、複合機 1 の立ち上げ（起動）を続行する。

【 0 0 6 0 】

図 1 4 は改ざんを検知しないときにオペレーションパネルに表示される画面の一例を表したイメージ図である。図 1 4 の画面には、操作者に異常を検知しなかった旨を通知する為のコメントが含まれる。

【 0 0 6 1 】

一方、バージョン出力ファイルに未調査のバージョン文字列が残っていれば、改ざん検知アプリ 4 6 はステップ S 6 3 に進み、図 1 5 に示すような画面をオペレーションパネル等に出力して、複合機 1 を停止する。なお、ステップ S 6 3 において複合機 1 を停止する理由はバージョン出力ファイルに未調査のバージョン文字列が残っている場合、複合機 1 からファームウェアが削除された（ファームウェア構成が改ざんされた）可能性が高いからである。

【 0 0 6 2 】

図 1 5 は改ざんを検知したときにオペレーションパネルに表示される画面の一例を表したイメージ図である。図 1 5 の画面には、操作者に異常（ファームウェアの削除）を検知した旨を通知する為のコメントと、削除されたファームウェアの情報とが含まれる。

【 0 0 6 3 】

以上、実施例 1 の複合機 1 では、搭載されているファームウェアの改ざんと、ファームウェア構成の改ざんとを容易に検知可能である。

【 実施例 2 】

【 0 0 6 4 】

実施例 2 の複合機 1 は、搭載されているファームウェアの改ざんを検知する処理を操作者からの指示により実行するものとする。また、ファームウェア構成情報は「複合機 1 にファームウェアがインストールされた後の機器の二次記憶装置 2 7 のファイル構成を表すファイル構成リスト（例えば U N I X（登録商標）の l s を実施した結果など）」であるものとする。更に、外部の二次記憶装置 9 1 は「外部サーバ」であるものとする。

【 0 0 6 5 】

図 1 6 は実施例 2 の複合機を表した一例の構成図である。図 1 6 の複合機 1 は外部二次記憶装置 I / F 2 4 が無い点で図 1 の構成図と異なる。

【 0 0 6 6 】

図 1 7 は実施例 2 の複合機にファームウェアを書き込む処理を説明する為のブロック図である。図 1 7 のブロック図は、ファームウェア構成情報 8 4 の代わりに機器の二次記憶装置 2 7 のファイル構成を表したファイル構成スナップショット 8 9 を利用する点で図 5

10

20

30

40

50

のブロック図と異なっている。

【0067】

ファイル構成スナップショット89は、ファイル構成出力アプリ87によって例えばUNIX（登録商標）のlsなどを実施することにより生成される。ファイル構成スナップショット89は、複合機1にファームウェアがインストールされた後の機器の二次記憶装置27のファイル構成を表すファイル構成リストである。

【0068】

図18は実施例2の複合機にファームウェアを書き込む処理を説明する為のシーケンス図である。ステップS71に進み、インストールアプリ80はインストール用ファイル群88を機器の二次記憶装置27に書き込む。ステップS72に進み、インストールアプリ80は図19に示すファイル構成スナップショット89の暗号化処理を行う。

10

【0069】

図19は、ファイル構成スナップショットの暗号化処理の手順を示すフローチャートである。ステップS81に進み、インストールアプリ80はインストール用ファイル群88に含まれる鍵BLOB83を機器に固有の暗号化復号装置26に送信し、ルート鍵61で鍵BLOBを復号させ、暗号鍵を得る。ステップS82に進み、インストールアプリ80はファイル構成スナップショット89をファイルに出力する。

【0070】

ステップS83に進み、インストールアプリ80はファイル構成スナップショット89を出力したファイルを暗号鍵で暗号化してファイル構成スナップショットBLOBを生成する。

20

【0071】

更に図18のステップS73に進み、インストールアプリ80はファイル構成スナップショットBLOBを、ネットワークI/F25経由で接続される外部サーバ181に送出する。ステップS74に進み、外部サーバ181はファイル構成スナップショットBLOBを例えば外部サーバ181内の二次記憶装置に保存する。

【0072】

実施例2の複合機1では、複合機1以外の外部サーバ181内の二次記憶装置にファイル構成スナップショットBLOBを保存しておくことで悪意の第三者による改ざんを防ぐことができる。

30

【0073】

図20は実施例2の複合機におけるファームウェアの改ざんを検知する処理を説明する為のフローチャートである。なお、ファームウェアの改ざんを検知する処理を実行するときの複合機1の構成は図16と同様である。

【0074】

ステップS91に進み、改ざん検知アプリ46は機器の二次記憶装置27から鍵BLOB83を取り出す。ステップS92に進み、改ざん検知アプリ46は鍵BLOB83を機器に固有の暗号化復号装置26に送信し、ルート鍵61で鍵BLOBを復号させ、復号鍵を得る。ステップS93に進み、改ざん検知アプリ46はネットワークI/F25経由で接続される外部サーバ181からファイル構成スナップショットBLOBを取り出す。ステップS94に進み、改ざん検知アプリ46はファイル構成スナップショットBLOBを復号鍵で復号し、ファイル構成スナップショット89を得る。

40

【0075】

ステップS95に進み、改ざん検知アプリ46は現在の複合機1の機器の二次記憶装置27のファイル構成を表すファイル構成リストであるファイル構成スナップショットを取得する。

【0076】

ステップS96に進み、改ざん検知アプリ46は、ステップS94で取得したファイル構成スナップショット89とステップS95で取得したファイル構成スナップショットとを比較し、一致しているか否かを判定する。ステップS96は現在の複合機1のファイル

50

構成スナップショットと、ファームウェアをインストールした後のファイル構成スナップショット 89 とが一致しているか否かを判定するものである。

【0077】

ステップ S96 においてファイル構成スナップショット 89 が一致していなければ、改ざん検知アプリ 46 はステップ S97 に進み、図 13 又は図 15 に示すような画面をオペレーションパネル等に出力して、複合機 1 を停止する。

【0078】

ステップ S96 においてファイル構成スナップショット 89 が一致していれば、改ざん検知アプリ 46 はステップ S98 に進み、図 16 に示すような画面をオペレーションパネル等に出力して、複合機 1 の動作を続行する。

10

【0079】

以上、実施例 2 の複合機 1 では、搭載されているファームウェアの改ざんと、ファームウェア構成の改ざんとを容易に検知可能である。

【0080】

本発明は、具体的に開示された実施例に限定されるものではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。

【0081】

なお、図 1、図 8 及び図 16 では点線によって囲まれているファームウェアが改ざん検知対象となる。また、現在の複合機 1 のファームウェア構成情報は、インストール時に機器の二次記憶装置 27 へ記憶したものであっても、ファームウェアの改ざんを検知する処理を行う度に生成するようにしてもよい。

20

【0082】

インストール時、機器の二次記憶装置 27 に記憶したファームウェア構成情報を現在のファームウェア構成情報として利用する場合はファームウェアがアップデート（更新）される度、機器の二次記憶装置 27 へ記憶したファームウェア構成情報を更新する仕組みが必要である。また、ファームウェアがアップデート（更新）される場合も、本実施例の複合機 1 はファームウェアのインストール時と同様に処理すればよい。

【符号の説明】

【0083】

- 1 複合機
- 10 ハードウェア
- 11 種々のソフトウェア
- 12 複合機起動部
- 21 プロッタ
- 22 スキャナ
- 23 その他のハードウェアリソース
- 24 外部二次記憶装置 I/F（インターフェース）
- 25 ネットワーク I/F
- 26 機器に固有の暗号化復号装置
- 27 機器の二次記憶装置
- 31 種々のアプリケーション
- 32 プラットフォーム
- 33 汎用 OS（オペレーティングシステム）
- 41 プリンタアプリ
- 42 コピーアプリ
- 43 ファックスアプリ
- 44 スキャナアプリ
- 45 ネットファイルアプリ
- 46 改ざん検知アプリ
- 47 RRU アプリ

30

40

50

4 8	S D K アプリ	
4 9	サードベンダの S D K アプリ	
5 1	コントロールサービス	
5 2	S R M (システムリソースマネージャ)	
5 3	E C S (エンジンコントロールサービス)	
5 4	M C S (メモリコントロールサービス)	
5 5	O C S (オペレーションパネルコントロールサービス)	
5 6	F C S (ファクシミリコントロールサービス)	
5 7	N C S (ネットワークコントロールサービス)	
5 8	S C S (システムコントロールサービス)	10
6 1	ルート鍵	
8 0	インストールアプリ	
8 1 , 8 5 , 8 8	インストール用ファイル群	
8 2	ファームウェア	
8 3	ルート鍵で暗号化した暗号鍵 / 復号鍵 ( 鍵 B L O B )	
8 4	ファームウェア構成情報	
8 6	バージョンファイル	
8 7	ファイル構成出力アプリ	
8 9	ファイル構成スナップショット	
9 1	外部の二次記憶装置	20
1 0 1	携帯可能な二次記憶装置	
1 8 1	外部サーバ	

## 【先行技術文献】

## 【特許文献】

## 【0084】

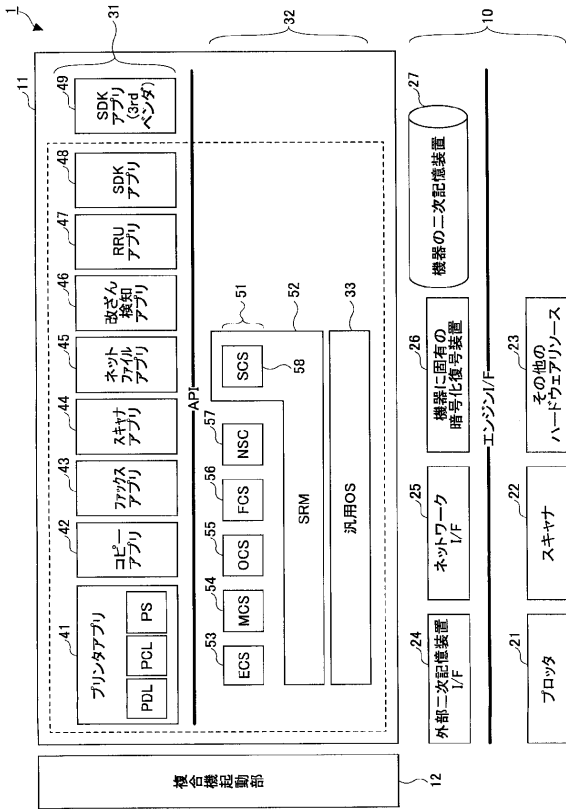
【特許文献1】特開2004-213057号公報

【特許文献2】特開2005-84989号公報

【特許文献3】特開2007-41694号公報

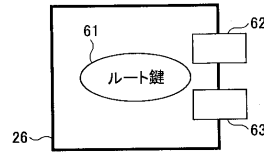
【 図 1 】

本実施例の複合機を表した一例の構成図



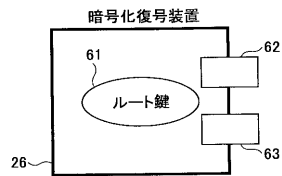
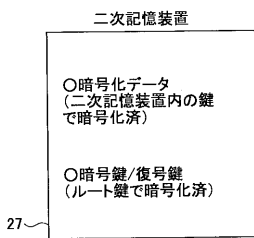
【 図 2 】

機器に固有の暗号化復号装置の特徴について説明する為の模式図



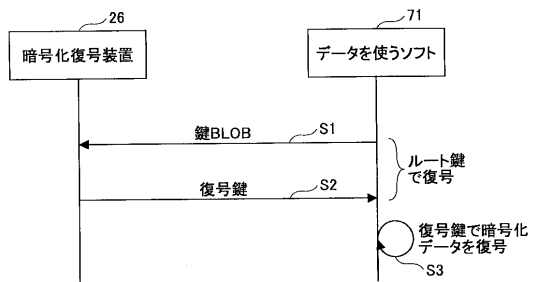
【 図 3 】

機器に固有の暗号化復号装置がある場合の暗号化データ保存方法について説明する為の模式図



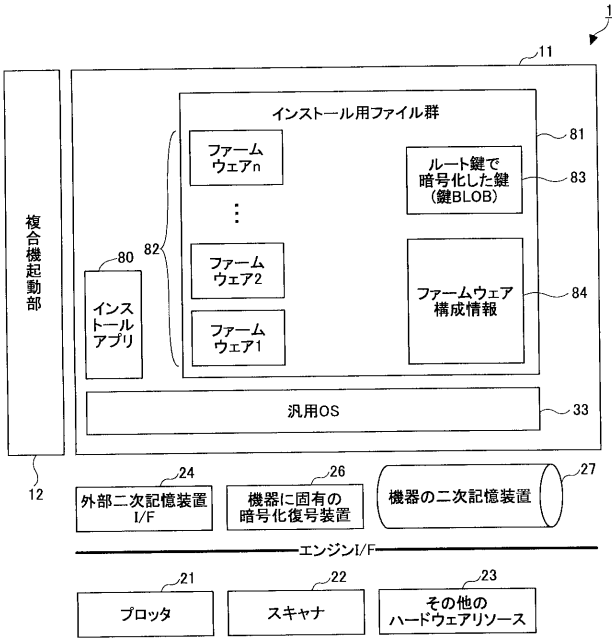
【 図 4 】

機器に固有の暗号化復号装置がある場合の暗号化データ復号方法について説明する為のシーケンス図



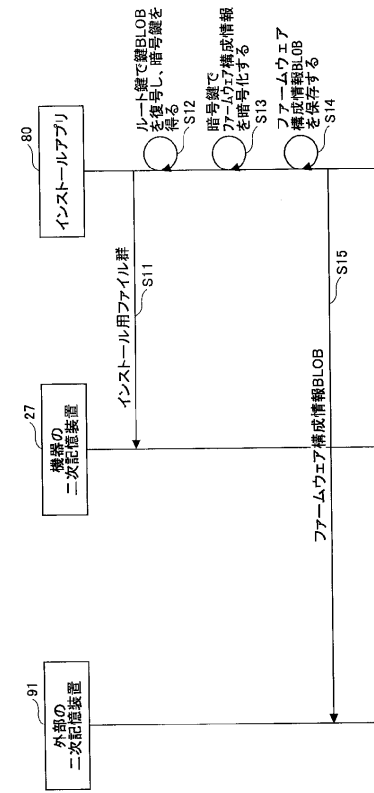
【図5】

本実施例の複合機にファームウェアを書き込む処理を説明する為のブロック図



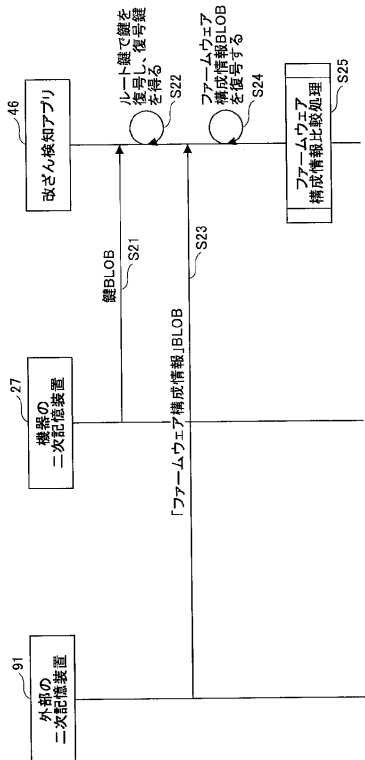
【図6】

本実施例の複合機にファームウェアを書き込む処理を説明する為のシーケンス図



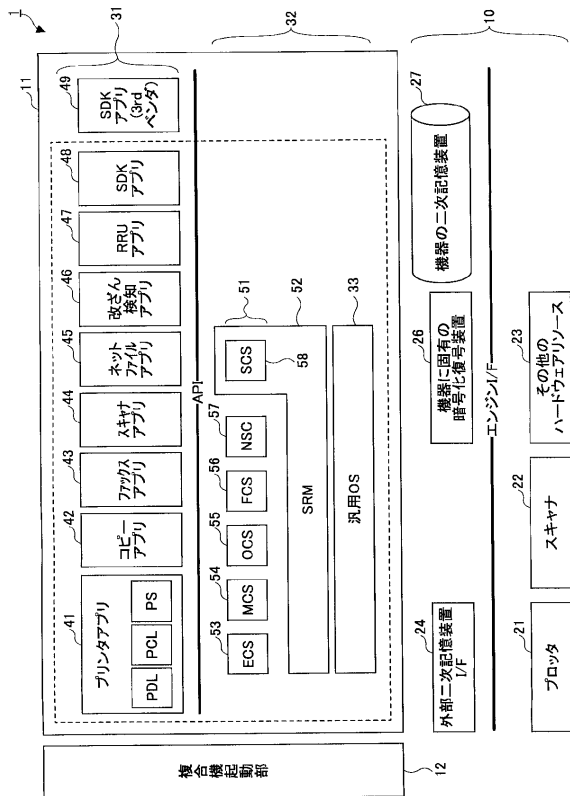
【図7】

本実施例の複合機に搭載されているファームウェアの改ざんを検知する処理を説明する為のシーケンス図



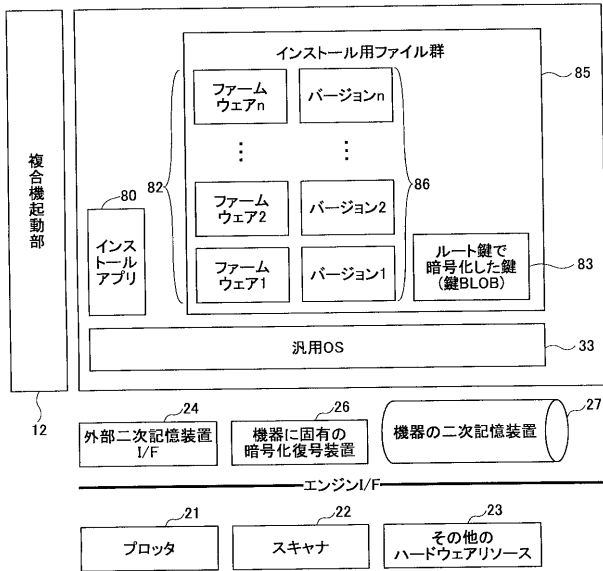
【図8】

実施例1の複合機を表した一例の構成図



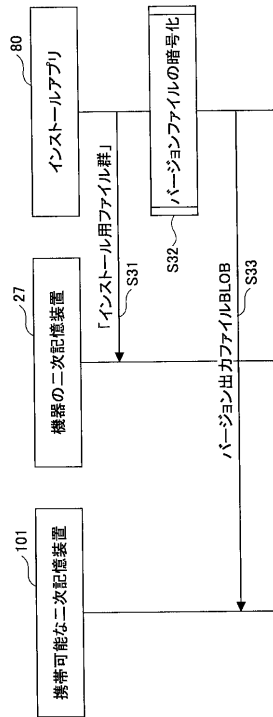
【 図 9 】

実施例1の複合機にファームウェアを書き込む処理を説明する為のブロック図



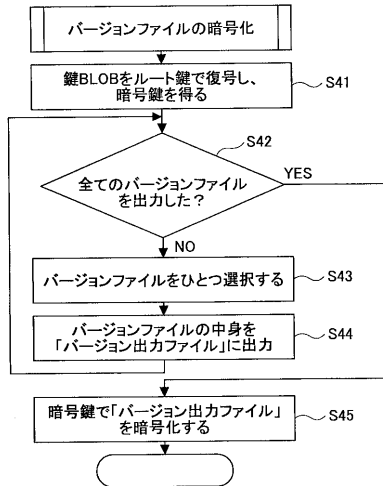
【 図 1 0 】

実施例1の複合機にファームウェアを書き込む処理を説明する為のシーケンス図



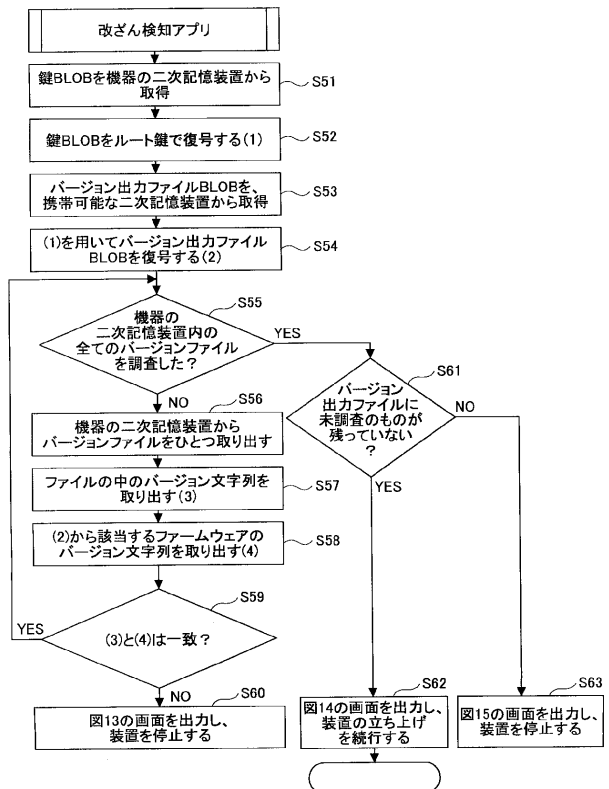
【 図 1 1 】

バージョンファイルの暗号化処理の手順を示すフローチャート



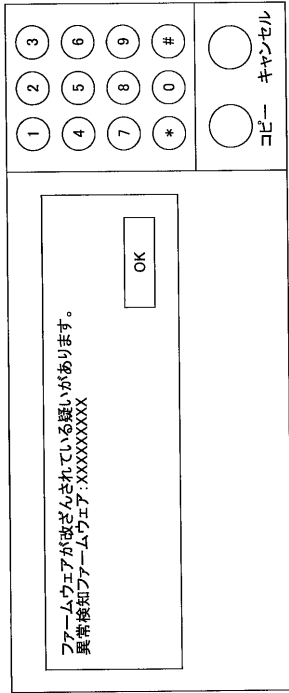
【 図 1 2 】

実施例1の複合機におけるファームウェアの改ざんを検知する処理を説明する為のフローチャート



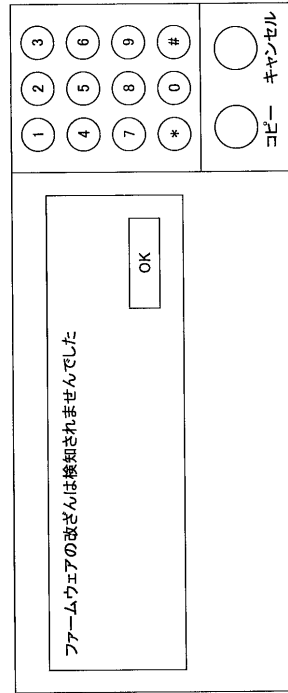
【 図 1 3 】

改ざんを検知したときにオペレーションパネルに表示される画面の一例を表したイメージ図



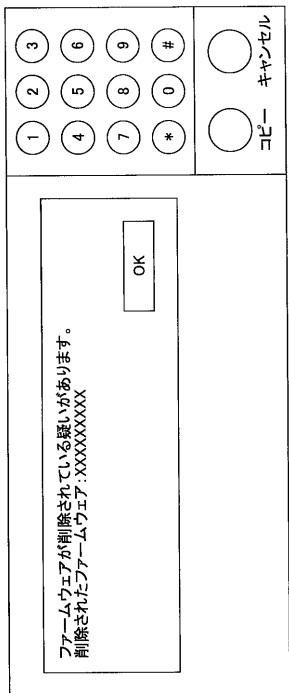
【 図 1 4 】

改ざんを検知しないときにオペレーションパネルに表示される画面の一例を表したイメージ図



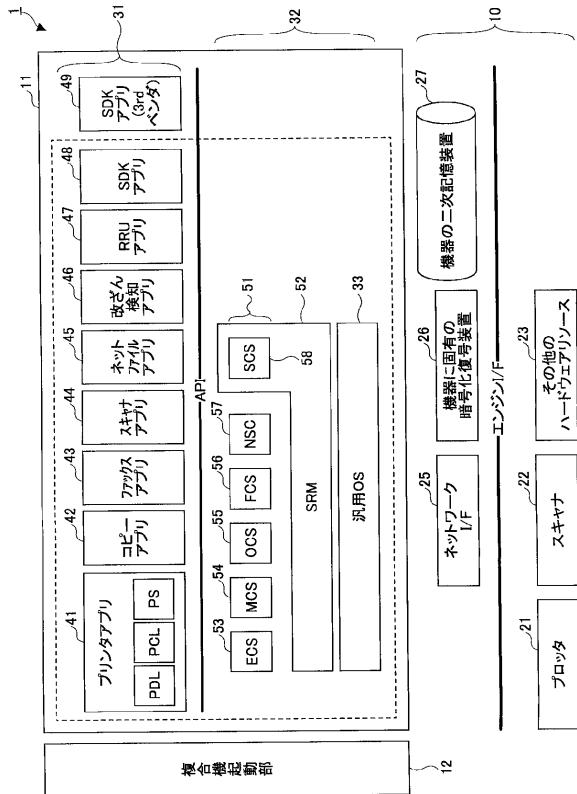
【 図 1 5 】

改ざんを検知したときにオペレーションパネルに表示される画面の一例を表したイメージ図



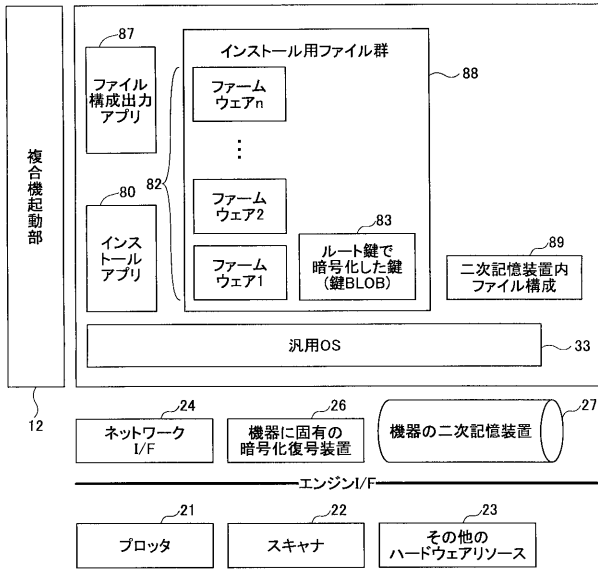
【 図 1 6 】

実施例2の複合機を表した一例の構成図



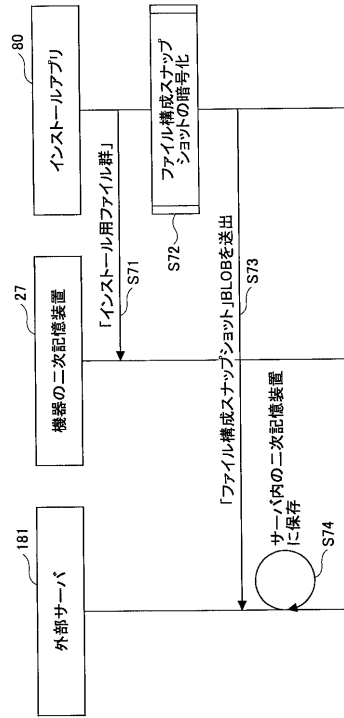
【 図 1 7 】

実施例2の複合機にファームウェアを書き込む処理を説明する為のブロック図



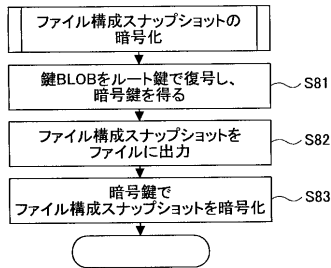
【 図 1 8 】

実施例2の複合機にファームウェアを書き込む処理を説明する為のシーケンス図



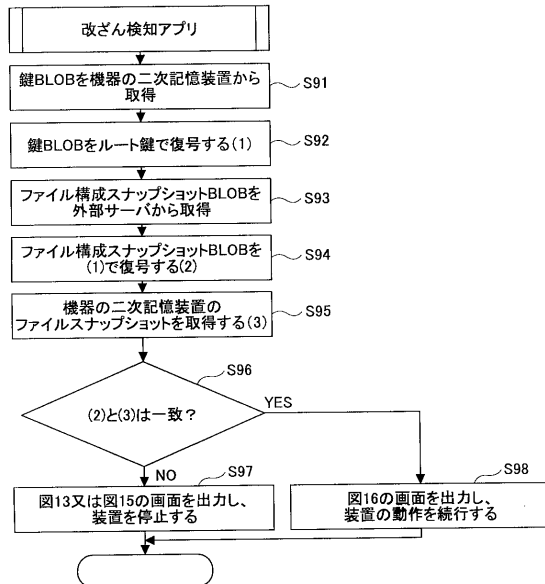
【 図 1 9 】

ファイル構成スナップショットの暗号化処理の手順を示すフローチャート



【 図 2 0 】

実施例2の複合機におけるファームウェアの改ざんを検知する処理を説明する為のフローチャート



## 【手続補正書】

【提出日】平成24年6月4日(2012.6.4)

## 【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

## 【特許請求の範囲】

## 【請求項1】

搭載されているソフトウェアの改ざんを検知する機器であって、  
前記機器に固有の暗号化復号装置と、  
前記ソフトウェアの改ざんを検知する改ざん検知手段と  
を有し、

前記改ざん検知手段は、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に暗号化されて保存されたインストール時における前記機器のソフトウェア構成情報を前記機器に固有の暗号化復号装置を利用して復号し、前記インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較して、前記ソフトウェアの改ざんを検知すること  
を特徴とする機器。

## 【請求項2】

前記機器に固有の暗号化復号装置を利用し、インストール時における前記機器のソフトウェア構成情報を暗号化して、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に保存するインストール手段を更に有すること  
を特徴とする請求項1記載の機器。

## 【請求項3】

前記インストール手段は、暗号化されている暗号鍵を、前記機器に固有の暗号化復号装置で復号し、復号された暗号鍵で、インストール時における前記機器のソフトウェア構成情報を暗号化し、暗号化された前記インストール時における前記機器のソフトウェア構成情報を、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に保存すること  
を特徴とする請求項2記載の機器。

## 【請求項4】

前記改ざん検知手段は、暗号化されている前記インストール時における前記機器のソフトウェア構成情報を、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置から取得し、暗号化されている復号鍵を前記機器に固有の暗号化復号装置で復号し、復号された復号鍵で前記インストール時における前記機器のソフトウェア構成情報を復号することを特徴とする請求項1乃至3何れか一項記載の機器。

## 【請求項5】

前記改ざん検知手段は、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とが一致しないときに前記ソフトウェアの改ざんを検知すること  
を特徴とする請求項1乃至4何れか一項記載の機器。

## 【請求項6】

前記機器に固有の暗号化復号装置は、内部から取り出しができない他の暗号/復号鍵を有しており、平文を前記他の暗号鍵で暗号化して返すインターフェースと、暗号化されたデータを前記他の復号鍵で復号して返すインターフェースとを有すること  
を特徴とする請求項1乃至5何れか一項記載の機器。

## 【請求項7】

前記インストール時における前記機器のソフトウェア構成情報はインストール用ファイル群に含まれること

を特徴とする請求項 1 乃至 6 何れか一項記載の機器。

【請求項 8】

前記インストール時における前記機器のソフトウェア構成情報はインストール用ファイル群を用いて前記ソフトウェアをインストールしたあと、ファイル構成を取得するコマンドにより生成されること

を特徴とする請求項 1 乃至 6 何れか一項記載の機器。

【請求項 9】

前記インストール時における前記機器のソフトウェア構成情報は携帯可能な記録媒体に保存されること

を特徴とする請求項 1 乃至 8 何れか一項記載の機器。

【請求項 10】

前記インストール時における前記機器のソフトウェア構成情報はネットワーク経由で接続された外部サーバに保存されること

を特徴とする請求項 1 乃至 8 何れか一項記載の機器。

【請求項 11】

前記機器の起動時又は前記機器を操作する操作者からの指示により、前記ソフトウェアの改ざんを検知すること

を特徴とする請求項 1 乃至 10 何れか一項記載の機器。

【請求項 12】

機器に搭載されているソフトウェアの改ざんを前記機器が検知するソフトウェア改ざん検知方法であって、

前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に暗号化されて保存されたインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、

前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップと

を有することを特徴とするソフトウェア改ざん検知方法。

【請求項 13】

搭載されているソフトウェアの改ざんを検知する機器に、

前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に暗号化されて保存されたインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、

前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップと

を実行させるためのソフトウェア改ざん検知プログラム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正の内容】

【0010】

上記課題を解決するため、本発明は、機器に搭載されているソフトウェアの改ざんを前記機器が検知するソフトウェア改ざん検知方法であって、前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に暗号化されて保存されたインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、前記改ざん検知手

段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップとを有することを特徴とする。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

また、本発明は、搭載されているソフトウェアの改ざんを検知する機器に、前記ソフトウェアの改ざんを検知する改ざん検知手段が、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に暗号化されて保存されたインストール時における前記機器のソフトウェア構成情報を、前記機器に固有の暗号化復号装置を利用して復号する復号ステップと、前記改ざん検知手段が、インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較し、前記ソフトウェアの改ざんを検知する検知ステップとを実行させるためのソフトウェア改ざん検知プログラムであることを特徴とする。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

また、本発明は、搭載されているソフトウェアの改ざんを検知する機器であって、前記機器に固有の暗号化復号装置と、前記ソフトウェアの改ざんを検知する改ざん検知手段とを有し、前記改ざん検知手段は、前記ソフトウェアを記憶している記憶装置とは異なる記憶装置に暗号化されて保存されたインストール時における前記機器のソフトウェア構成情報を前記機器に固有の暗号化復号装置を利用して復号し、前記インストール時における前記機器のソフトウェア構成情報と現在の前記機器のソフトウェア構成情報とを比較して、前記ソフトウェアの改ざんを検知することを特徴とする。