(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5387724号
(P5387724)
(45)発行日　平成26年1月15日(2014.1.15)　(24)登録日　平成25年10月18日(2013.10.18)

(51)Int.Cl.　　F I
*G06F 21/12 (2013.01)*　　G06F 21/22 112L
*G06F 9/445 (2006.01)*　　G06F 9/06 610L

請求項の数 13　(全 19 頁)

(21)出願番号　特願2012-105954(P2012-105954)
(22)出願日　平成24年5月7日(2012.5.7)
(62)分割の表示　特願2008-36267(P2008-36267)の分割
原出願日　平成20年2月18日(2008.2.18)
(65)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)
審査請求日　平成24年6月4日(2012.6.4)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100107766
弁理士　伊東　忠重
(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

審査官　平井　誠

最終頁に続く

(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)【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、前記機器の外部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し、
前記機器のソフトウェア構成情報は、前記ソフトウェアのバージョン情報であること
を特徴とする機器。
【請求項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に含まれる各ソフトウェアのバージョン情報が前記機器の外部に暗号化されて保存されたものであること
を特徴とする請求項１記載の機器。
【請求項３】
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又は２記載の機器。
【請求項４】
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３記載の機器。
【請求項５】
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乃至４何れか一項記載の機器。
【請求項６】
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５何れか一項記載の機器。
【請求項７】
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に未調査の前記バージョン情報が残る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６記載の機器。
【請求項８】
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７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、前記機器の外部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である前記ソフトウェアのバージョン情報を、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、前記機器の外部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である前記ソフトウェアのバージョン情報を、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。
【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。
【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。
【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。
【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。

【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。

【０００９】

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】

【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、前記機器の外部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である前記ソフトウェアのバージョン情報を、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。

【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、前記機器の外部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である前記ソフトウェアのバージョン情報を、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。

【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、前記機器の外部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し、前記機器のソフトウェア構成情報は、前記ソフトウェアのバージョン情報であることを特徴とする。

【００１３】

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ものも本発明の態様として有効である。

【発明の効果】

【００１４】

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】

【００１５】
【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。
【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。
【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。
【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。
【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／Ｆ２５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／Ｆ２４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／Ｆ２５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、例えばセキュリティチップであるＴＰＭ（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２６の詳細は後述する。

【００２０】

ソフトウェア１１は、種々のアプリケーション３１と、プラットフォーム３２と、汎用ＯＳ（オペレーティングシステム）３３とを含む構成である。種々のアプリケーション３１とプラットフォーム３２とを構成するプログラムは、ＵＮＩＸ（登録商標）等の汎用ＯＳ３３によりプロセス単位で並列的に実行される。

【００２１】

アプリケーション３１は、プリンタアプリ４１と、コピーアプリ４２と、ファックスアプリ４３と、スキャナアプリ４４と、ネットファイルアプリ４５と、改ざん検知アプリ４６と、ＲＲＵアプリ４７と、ＳＤＫアプリ４８と、サードベンダのＳＤＫアプリ４９とを含む構成である。ＳＤＫアプリ４８とサードベンダのＳＤＫアプリ４９とは、専用のＳＤＫ（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４６の詳細は後述する。

【００２２】

プラットフォーム３２は種々のコントロールサービス５１とＳＲＭ（システムリソースマネージャ）５２とを含む構成である。また、コントロールサービス５１はＥＣＳ（エンジンコントロールサービス）５３と、ＭＣＳ（メモリコントロールサービス）５４と、ＯＣＳ（オペレーションパネルコントロールサービス）５５と、ＦＣＳ（ファクシミリコントロールサービス）５６と、ＮＣＳ（ネットワークコントロールサービス）５７と、ＳＣＳ（システムコントロールサービス）５８とを含む構成である。なお、プラットフォーム３２を構成するプログラムの詳細は例えば特開２００２－８４３８３号公報に記載されている為、説明を省略する。

【００２３】

複合機起動部１２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ＯＳ３３が起動され、アプリケーション３１やプラットフォーム３２が起動される。種々のアプリケーション３１とプラットフォーム３２とを構成するプログラムはＨＤＤ（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２７に記憶されており、ＨＤＤ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。

【００２４】

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２６は、ルート鍵６１と、二つのＩ／Ｆ６２，６３とを含む構成である。ルート鍵６１は、機器に固有の暗号化復号装置２６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２６は、ルート鍵６１を用いた暗号化復号処理機能を有する。

【００２５】

Ｉ／Ｆ６２は平文データをルート鍵６１で暗号化して返すＩ／Ｆである。Ｉ／Ｆ６３は暗号化された平文データをルート鍵６１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２６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。

【００２６】

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２７にはルート鍵６１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２７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。

【００２７】
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＋ＢＬＯＢ」と言う。例えば暗号化された暗号／復号鍵は、鍵ＢＬＯＢと言う。
【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。
【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。
【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。
【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。
【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るときの複合機１の構成は図１と同様である。

【００３８】

ステップＳ２１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Ｓ２２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Ｓ２３に進み、改ざん検知アプリ４６は、外部の二次記憶装置９１からファームウェア構成情報ＢＬＯＢを取り出す。ステップＳ２４に進み、改ざん検知アプリ４６はファームウェア構成情報ＢＬＯＢを復号鍵で復号して、ファームウェア構成情報８４を得る。

【００３９】

そして、ステップＳ２５に進み、改ざん検知アプリ４６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３１のファームウェア構成情報と、ファームウェア構成情報ＢＬＯＢを復号鍵で復号して得たファームウェア構成情報８４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Ｓ２５の処理の具体的内容は後述する。

【実施例１】

【００４０】

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８２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９１はＵＳＢメモリやＳＤカード等の「携帯可能な二次記憶装置」であるものとする。

【００４１】

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／Ｆ２５が無い点で図１の構成図と異なる。

【００４２】

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８４がバージョンファイル８６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８６は、対応するファームウェア８２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。

【００４３】

バージョンファイル８６は、ファームウェア８２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８０は、バージョンファイル８６の生成に関与しない。バージョンファイル８６は、ファームウェア構成情報８４の一例である。

【００４４】

図１０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Ｓ３１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８５を機器の二次記憶装置２７に書き込む。ステップＳ３２に進み、インストールアプリ８０は図１１に示すバージョンファイル８６の暗号化処理を行う。図１１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。

【００４５】

ステップＳ４１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８５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Ｓ４２に進み、インストールアプリ８０は全てのバージョンファイル８６を出力したか否かを判定する。

【００４６】
全てのバージョンファイル８６を出力していない（出力していないバージョンファイル８６が残っている）と判定すると、インストールアプリ８０はステップＳ４３に進み、インストール用ファイル群８５に含まれるバージョンファイル８６を一つ選択する。
【００４７】
ステップＳ４４に進み、インストールアプリ８０は選択したバージョンファイル８６の中身を「バージョン出力ファイル」に出力し、ステップＳ４２に戻る。インストールアプリ８０は、全てのバージョンファイル８６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Ｓ４２～Ｓ４４の処理を繰り返し行う。全てのバージョンファイル８６を出力した（出力していないバージョンファイル８６が残っていない）と判定すると、インストールアプリ８０はステップＳ４５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ＢＬＯＢを生成する。
【００４８】
図１０のステップＳ３３に進み、インストールアプリ８０はバージョン出力ファイルＢＬＯＢを、外部二次記憶装置Ｉ／Ｆ２４経由で接続されるＳＤカード等の携帯可能な二次記憶装置１０１に保存する。携帯可能な二次記憶装置１０１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）３１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。
【００４９】
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１０１にバージョン出力ファイル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。
【００５０】
図１２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。
【００５１】
ステップＳ５１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Ｓ５２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Ｓ５３に進み、改ざん検知アプリ４６は、外部二次記憶装置Ｉ／Ｆ２４経由で接続される携帯可能な二次記憶装置１０１からバージョン出力ファイルＢＬＯＢを取り出す。ステップＳ５４に進み、改ざん検知アプリ４６はバージョン出力ファイルＢＬＯＢを復号鍵で復号し、バージョン出力ファイルを得る。
【００５２】
ステップＳ５５に進み、改ざん検知アプリ４６は機器の二次記憶装置２７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８６を全て調査したか否かを判定する。
【００５３】
全てのバージョンファイル８６を調査していない（調査していないバージョンファイル８６が残っている）と判定すると、改ざん検知アプリ４６はステップＳ５６に進み、機器の二次記憶装置２７からバージョンファイル８６を一つ取り出す。改ざん検知アプリ４６はステップＳ５７に進み、取り出したバージョンファイル８６からバージョン文字列を取り出す。
【００５４】
ステップＳ５８に進み、改ざん検知アプリ４６はステップＳ５４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Ｓ５９に進み、改ざん検知アプリ４６はステップＳ５７で取り出したバージョン文字列とステップＳ５８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。
【００５５】

ステップＳ５９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。

【００５６】

ステップＳ５９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４６はステップＳ５５に戻る。なお、ステップＳ５９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４６はステップＳ６０に進み、図１３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。

【００５７】

図１３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１３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。

【００５８】

また、ステップＳ５５において、全てのバージョンファイル８６を調査した（調査していないバージョンファイル８６が残っていない）と判定すると、改ざん検知アプリ４６はステップＳ６１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。

【００５９】

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４６はステップＳ６２に進み、図１４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。

【００６０】

図１４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１４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。

【００６１】

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４６はステップＳ６３に進み、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。なお、ステップＳ６３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。

【００６２】

図１５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１５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。

【００６３】

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】

【００６４】

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２７のファイル構成を表すファイル構成リスト（例えばＵＮＩＸ（登録商標）のｌｓ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９１は「外部サーバ」であるものとする。

【００６５】

図１６は実施例２の複合機を表した一例の構成図である。図１６の複合機１は外部二次記憶装置Ｉ／Ｆ２４が無い点で図１の構成図と異なる。

【００６６】
図１７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１７のブロック図は、ファームウェア構成情報８４の代わりに機器の二次記憶装置２７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８９を利用する点で図５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。
【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。
【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。
【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。
【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。

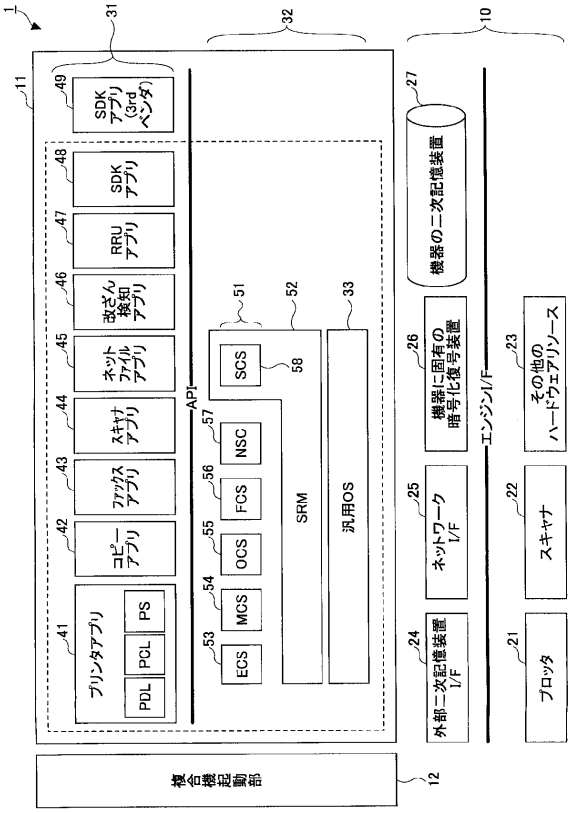
【００７６】
ステップＳ９６に進み、改ざん検知アプリ４６は、ステップＳ９４で取得したファイル構成スナップショット８９とステップＳ９５で取得したファイル構成スナップショットとを比較し、一致しているか否かを判定する。ステップＳ９６は現在の複合機１のファイル構成スナップショットと、ファームウェアをインストールした後のファイル構成スナップショット８９とが一致しているか否かを判定するものである。
【００７７】
ステップＳ９６においてファイル構成スナップショット８９が一致していなければ、改ざん検知アプリ４６はステップＳ９７に進み、図１３又は図１５に示すような画面をオペレーションパネル等に出力して、複合機１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。
【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。
【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
４８　ＳＤＫアプリ
４９　サードベンダのＳＤＫアプリ
５１　コントロールサービス
５２　ＳＲＭ（システムリソースマネージャ）
５３　ＥＣＳ（エンジンコントロールサービス）
５４　ＭＣＳ（メモリコントロールサービス）
５５　ＯＣＳ（オペレーションパネルコントロールサービス）
５６　ＦＣＳ（ファクシミリコントロールサービス）
５７　ＮＣＳ（ネットワークコントロールサービス）
５８　ＳＣＳ（システムコントロールサービス）
６１　ルート鍵
８０　インストールアプリ
８１，８５，８８　インストール用ファイル群
８２　ファームウェア
８３　ルート鍵で暗号化した暗号鍵／復号鍵（鍵ＢＬＯＢ）
８４　ファームウェア構成情報
８６　バージョンファイル
８７　ファイル構成出力アプリ
８９　ファイル構成スナップショット
９１　外部の二次記憶装置
１０１　携帯可能な二次記憶装置
１８１　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

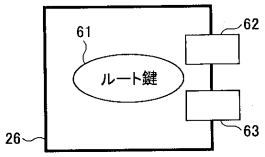
【図１】

本実施例の複合機を表した一例の構成図



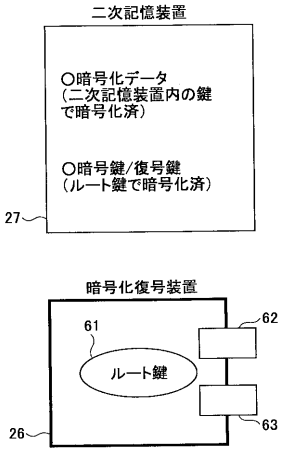

【図２】

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



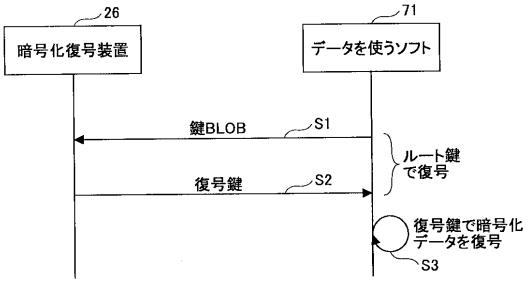

【図３】

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



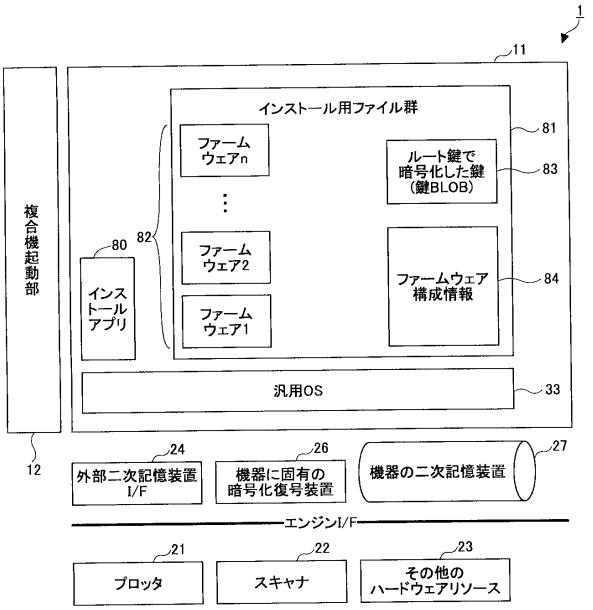

【図４】

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



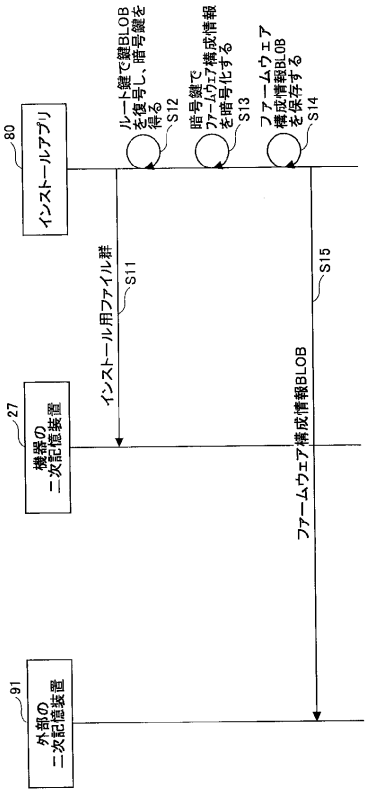
【図５】

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



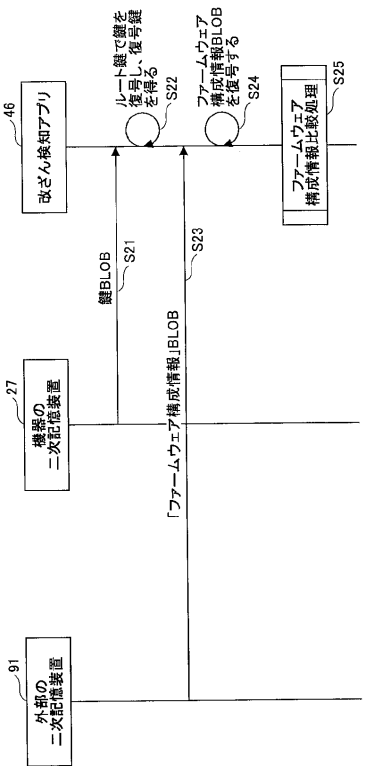

【図６】

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



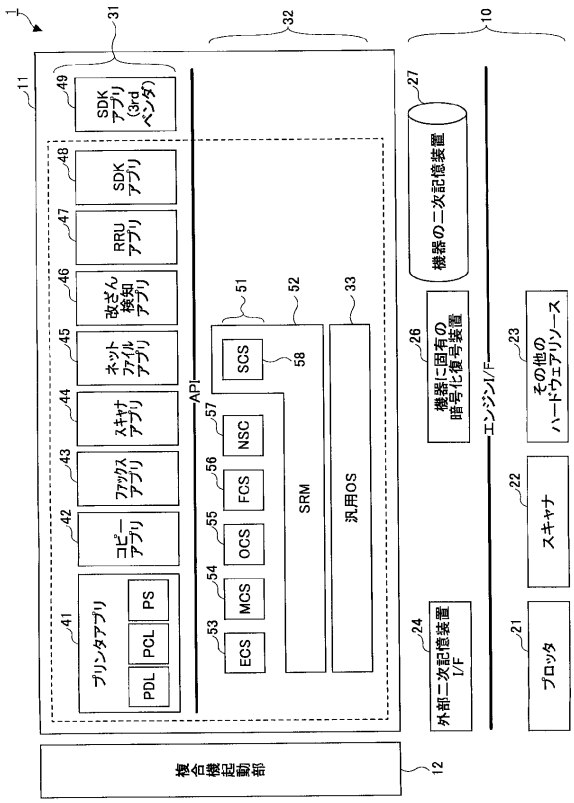

【図７】

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



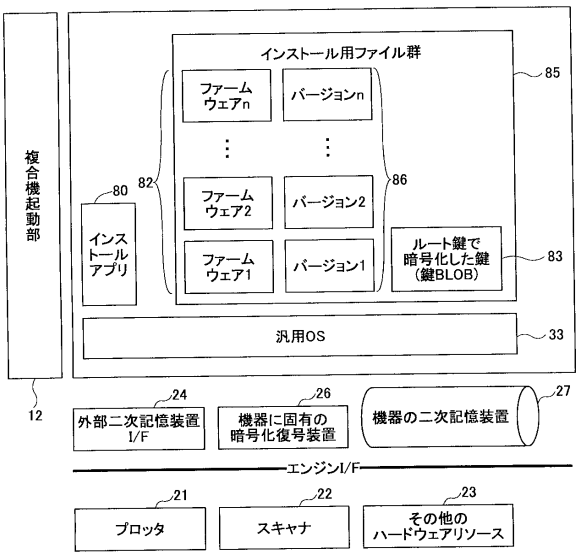

【図８】

実施例１の複合機を表した一例の構成図



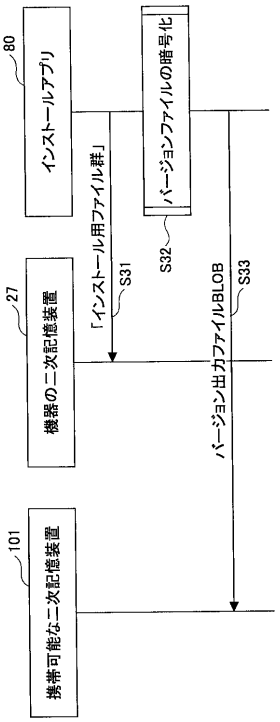
【図９】

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



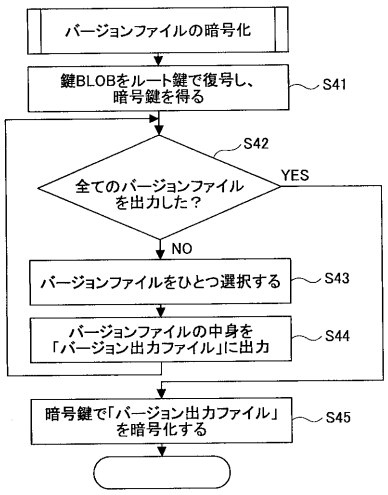

【図１０】

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



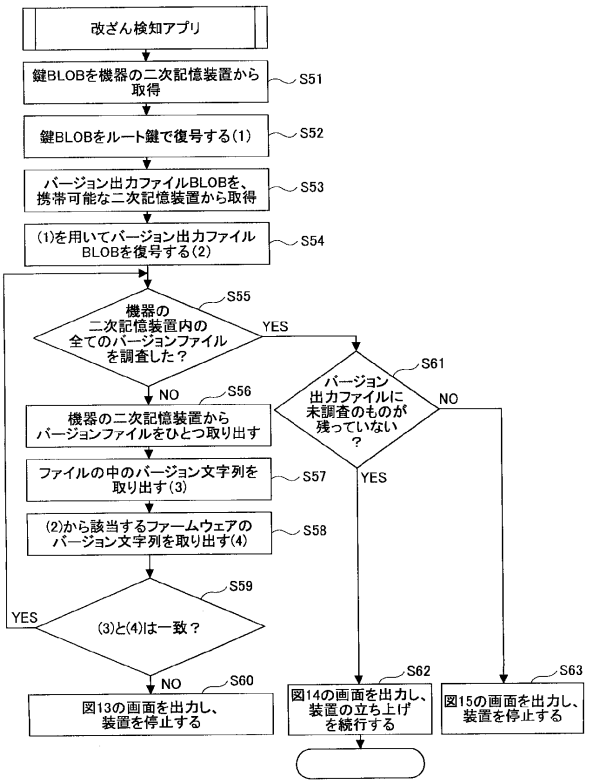

【図１１】

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



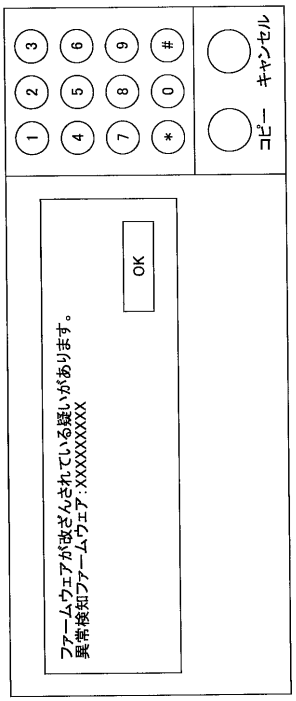

【図１２】

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



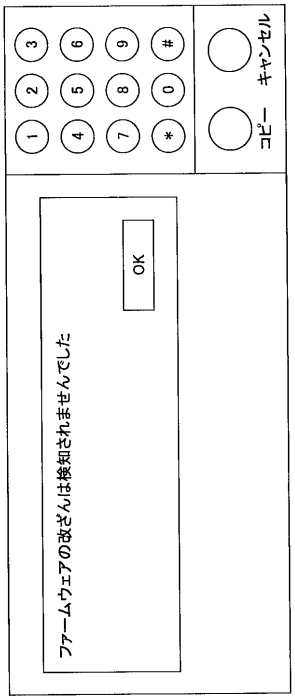
【図１３】

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



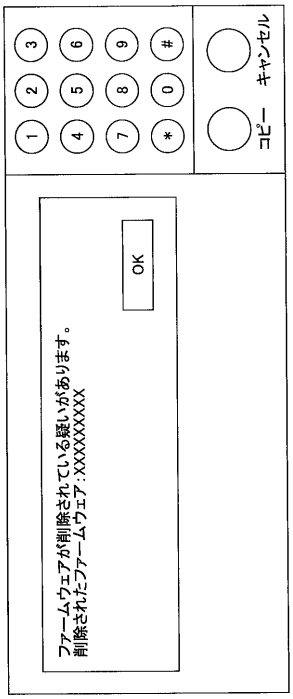

【図１４】

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



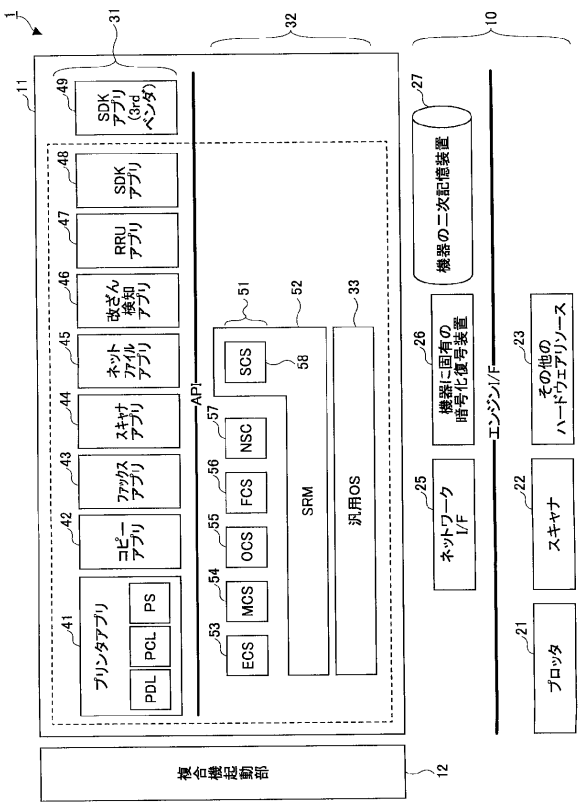

【図１５】

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



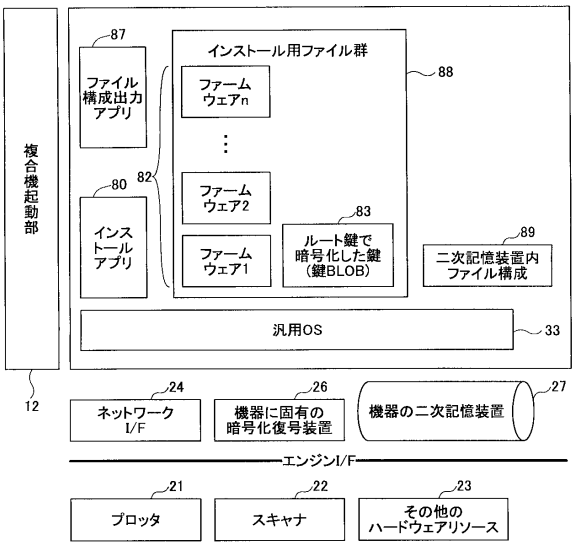

【図１６】

実施例２の複合機を表した一例の構成図



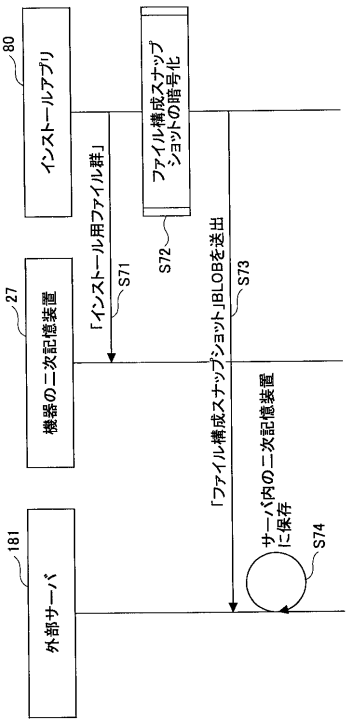
【図１７】

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



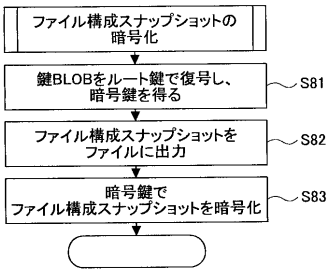

【図１８】

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



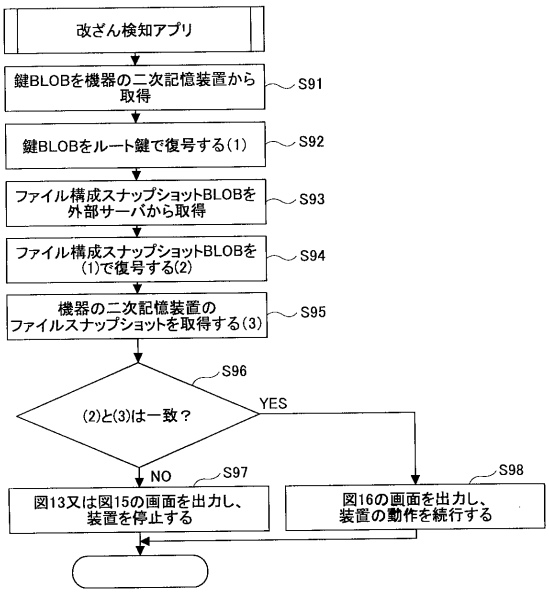

【図１９】

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




【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



フロントページの続き

(56)参考文献　特開２００４－２８０２８４（ＪＰ，Ａ）
特開平１０－３３３９０２（ＪＰ，Ａ）
特開２００３－２０２９３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１