(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4896595号
(P4896595)

(45)発行日　平成24年3月14日(2012.3.14)　(24)登録日　平成24年1月6日(2012.1.6)

(51)Int.Cl.		F I		
G06F 21/06	(2006.01)	G06F	21/06	186
H04N 1/00	(2006.01)	H04N	1/00	C
G06F 21/24	(2006.01)	H04N	1/00	107Z
G09C 1/00	(2006.01)	H04N	1/00	106C
		G06F	21/24	166A

請求項の数 12　(全 21 頁)　最終頁に続く

(21)出願番号　特願2006-158722 (P2006-158722)
(22)出願日　平成18年6月7日 (2006.6.7)
(65)公開番号　特開2007-220073 (P2007-220073A)
(43)公開日　平成19年8月30日 (2007.8.30)
審査請求日　平成21年1月7日 (2009.1.7)
(31)優先権主張番号　特願2006-10358 (P2006-10358)
(32)優先日　平成18年1月18日 (2006.1.18)
(33)優先権主張国　日本国(JP)

(73)特許権者　000136136
株式会社ＰＦＵ
石川県かほく市宇野気ヌ９８番地の２
(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100117075
弁理士　伊藤　剣太
(72)発明者　宮村　和俊
石川県かほく市宇野気ヌ９８番地の２　株式会社ＰＦＵ内
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】画像読取装置およびプログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークを介してサーバ装置と通信可能に接続され、動作ログを記録する記録手段を備えた画像読取装置において、
耐タンパー性を有するチップと、
前記サーバ装置へ情報を送信する送信手段と、
画像情報を一意に識別するための情報であり、当該画像読取装置固有の情報である機器固有情報を含む画像識別情報を生成する生成手段と、
高度センサと、
を備え、
前記動作ログは、前記高度センサで検出した高度を含み、
前記チップは、
当該画像読取装置固有の秘密鍵を格納する格納手段と、
前記生成手段で生成した前記画像識別情報を、当該画像読取装置で読み取った前記画像情報に付加する識別情報付加手段と、
前記格納手段で格納した前記秘密鍵で、前記記録手段で記録した前記動作ログおよび前記識別情報付加手段で前記画像識別情報が付加された前記画像情報を暗号化する暗号化手段と、
をさらに備えたこと
を特徴とする画像読取装置。

【請求項２】
ネットワークを介して通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段をさらに備え、
前記チップは、前記取得手段で取得した前記時刻情報を、前記記録手段で記録した前記動作ログに付加する付加手段をさらに備え、
前記暗号化手段は、前記秘密鍵で、前記付加手段で前記時刻情報が付加された前記動作ログを暗号化すること
を特徴とする請求項１に記載の画像読取装置。
【請求項３】
ネットワークを介して当該画像読取装置と通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段、
当該画像読取装置で前記画像情報が読み取られる度に、当該画像読取装置に予め格納されたシリアル番号を更新する更新手段
のいずれか１つをさらに備え、
前記画像識別情報は、前記機器固有情報と、前記取得手段で取得した前記時刻情報または前記更新手段で更新した前記シリアル番号とからなること
を特徴とする請求項１に記載の画像読取装置。
【請求項４】
前記動作ログは、当該画像読取装置で前記画像情報を読み取ったときの読取パラメータ、前記読み取ったときの読取枚数、前記読み取ったときの読取時刻、当該画像読取装置で発生したエラーに関する発生エラーコード、前記エラーが発生したときのエラー発生時刻、当該画像読取装置を操作する操作者を一意に識別するための情報である操作者識別情報のうち少なくとも１つを含むこと
を特徴とする請求項１から３のいずれか１つに記載の画像読取装置。
【請求項５】
温度センサ、湿度センサのうち少なくとも１つをさらに備え、
前記動作ログは、前記温度センサで検出した気温、前記温度センサで検出した装置温度、前記湿度センサで検出した湿度のうち少なくとも１つを含むこと
を特徴とする請求項１から４のいずれか１つに記載の画像読取装置。
【請求項６】
ネットワークを介してサーバ装置と通信可能に接続され、動作ログを記録する記録手段を備えた画像読取装置において、
耐タンパー性を有するチップと、
前記記録手段で記録した前記動作ログのハッシュ値を生成するハッシュ値生成手段と、
前記サーバ装置へ情報を送信する送信手段と、
画像情報を一意に識別するための情報であり、当該画像読取装置固有の情報である機器固有情報を含む画像識別情報を生成する生成手段と、
高度センサと、
を備え、
前記動作ログは、前記高度センサで検出した高度を含み、
前記チップは、
当該画像読取装置固有の秘密鍵を格納する格納手段と、
前記生成手段で生成した前記画像識別情報を、当該画像読取装置で読み取った前記画像情報に付加する識別情報付加手段と、
前記格納手段で格納した前記秘密鍵で、前記ハッシュ値生成手段で生成した前記ハッシュ値を暗号化する暗号化手段と
をさらに備え、
前記ハッシュ値生成手段は、前記識別情報付加手段で前記画像識別情報が付加された前記画像情報の前記ハッシュ値を生成すること
を特徴とする画像読取装置。

【請求項７】
ネットワークを介して通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段をさらに備え、
前記チップは、前記取得手段で取得した前記時刻情報を、前記記録手段で記録した前記動作ログに付加する付加手段をさらに備え、
前記ハッシュ値生成手段は、前記付加手段で前記時刻情報が付加された前記動作ログのハッシュ値を生成すること
を特徴とする請求項６に記載の画像読取装置。
【請求項８】
ネットワークを介して当該画像読取装置と通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段、
当該画像読取装置で前記画像情報が読み取られる度に、当該画像読取装置に予め格納されたシリアル番号を更新する更新手段
のいずれか１つをさらに備え、
前記画像識別情報は、前記機器固有情報と、前記取得手段で取得した前記時刻情報または前記更新手段で更新した前記シリアル番号とからなること
を特徴とする請求項６に記載の画像読取装置。
【請求項９】
前記動作ログは、当該画像読取装置で前記画像情報を読み取ったときの読取パラメータ、前記読み取ったときの読取枚数、前記読み取ったときの読取時刻、当該画像読取装置で発生したエラーに関する発生エラーコード、前記エラーが発生したときのエラー発生時刻、当該画像読取装置を操作する操作者を一意に識別するための情報である操作者識別情報のうち少なくとも１つを含むこと
を特徴とする請求項６から８のいずれか１つに記載の画像読取装置。
【請求項１０】
温度センサ、湿度センサのうち少なくとも１つをさらに備え、
前記動作ログは、前記温度センサで検出した気温、前記温度センサで検出した装置温度、前記湿度センサで検出した湿度のうち少なくとも１つを含むこと
を特徴とする請求項６から９のいずれか１つに記載の画像読取装置。
【請求項１１】
画像読取装置に、
画像情報を読み取る読取ステップと、
前記画像情報を一意に識別するための情報であり、当該画像読取装置固有の情報である機器固有情報を含む画像識別情報を生成する生成ステップと、
当該装置が備えた耐タンパー性を有するチップにて、前記生成ステップで生成した前記画像識別情報を、前記読取ステップで読み取った前記画像情報に付加する識別情報付加ステップと、
当該装置が備えた高度センサにて検出した高度を含む動作ログを記録する記録ステップと、
前記チップにて、当該チップに予め格納した当該装置固有の秘密鍵で、前記記録ステップで記録した前記動作ログおよび前記識別情報付加ステップで前記画像識別情報が付加された前記画像情報を暗号化する暗号化ステップと、
前記暗号化ステップで暗号化した前記動作ログおよび前記画像情報を、ネットワークを介して当該装置と通信可能に接続されたサーバ装置へ送信する送信ステップと、
を実行させること
を特徴とするプログラム。
【請求項１２】
画像読取装置に、
画像情報を読み取る読取ステップと、
画像情報を一意に識別するための情報であり、当該画像読取装置固有の情報である機器

固有情報を含む画像識別情報を生成する生成ステップと、
当該装置が備えた耐タンパー性を有するチップにて、前記生成ステップで生成した前記画像識別情報を、前記読取ステップで読み取った前記画像情報に付加する識別情報付加ステップと、
当該装置が備えた高度センサにて検出した高度を含む動作ログを記録する記録ステップと、
前記記録ステップで記録した前記動作ログのハッシュ値および前記識別情報付加ステップで前記画像識別情報が付加された前記画像情報の前記ハッシュ値を生成するハッシュ値生成ステップと、
前記チップにて、当該チップに予め格納した当該装置固有の秘密鍵で、前記ハッシュ値生成ステップで生成した前記ハッシュ値を暗号化する暗号化ステップと、
前記暗号化ステップで暗号化した前記動作ログの前記ハッシュ値および前記動作ログならびに前記暗号化ステップで暗号化した前記画像情報の前記ハッシュ値および前記画像識別情報が付加された前記画像情報を、ネットワークを介して当該装置と通信可能に接続されたサーバ装置へ送信する送信ステップと、
を実行させること
を特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、スキャナやプリンタ、複合機、ＦＡＸなどの画像読取装置、および当該画像読取装置に実行させるプログラムに関するものである。

【背景技術】

【０００２】

これまで、ネットワーク対応の画像読取装置内でログ情報を記録する技術として、例えば特許文献１や特許文献２などが開示されている。特許文献１には、原稿読取条件や送信条件・送信先等の履歴情報を保存し、必要に応じてその履歴情報を利用することにより、システムの再利用時の作業性、および使用状況の確認や異常発生時におけるメンテナンス等の作業性を向上させることができるネットワーク対応スキャナ装置などに関する技術が開示されている。特許文献２には、ログ情報を記録し、ユーザが頻繁に利用する読み取りモードをデフォルト値として反映させることができるネットワークスキャナ装置の管理方法などに関する技術が開示されている。

【０００３】

一方、各企業が個別に進めて来たセキュリティ強化について、ＰＣプラットフォームを提供する技術を持つ企業が集まり、より高い信頼性と安全性を持った新たなハードウェア／ソフトウェアをつくる取り組みを、一つの業界団体として行うものとして、ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）がある。ＴＣＧでは、コンピューティング・プラットフォームに向けて、セキュリティチップに関するＴＰＭ（Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ）チップの仕様を作成している（特許文献３等参照。）。

【０００４】

【特許文献１】特開平１１－３３１４６９号公報
【特許文献２】特開２００３－１８９０５４号公報
【特許文献３】特開２００５－３１７０２６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、上述した特許文献１や特許文献２に記載の技術では、履歴情報やログ情報が不正に改竄される可能性を排除できておらず、ゆえに履歴情報やログ情報の信頼性や否偽証性（偽りがないこと）を確保することができていなかったという問題点があった。

【０００６】
本発明では、上記問題点に鑑みてなされたものであって、例えばセキュリティや保守を目的として動作ログを分析する場合などにおいて、動作ログの信頼性や否偽証性（偽りがないこと）を確保することができる画像読取装置およびプログラムを提供することを目的とするものである。
【課題を解決するための手段】
【０００７】
上述した課題を解決し目的を達成するために、本発明にかかる画像読取装置は、ネットワークを介してサーバ装置と通信可能に接続され、動作ログを記録する記録手段を備えた画像読取装置において、耐タンパー性を有するチップと、前記サーバ装置へ情報を送信する送信手段とを備え、前記チップは、当該画像読取装置固有の秘密鍵を格納する格納手段と、前記格納手段で格納した前記秘密鍵で、前記記録手段で記録した前記動作ログを暗号化する暗号化手段とをさらに備えたことを特徴とする。
【０００８】
ここで、「耐タンパー性」とは、チップに対する物理的攻撃（ＩＣメモリーへの侵入・改竄等）に抵抗する機能をいい、外部からの不当なアクセスに対し、物理的な仕組みによってアクセスできないようにする他、分解して解析するなどがあった場合には、チップそのものが回路的に破壊されるような、偽造・変造・改竄等を防止する手段などを備えたものを含む。
【０００９】
また、本発明にかかる画像読取装置は、前記の画像読取装置において、ネットワークを介して通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段をさらに備え、前記チップは、前記取得手段で取得した前記時刻情報を、前記記録手段で記録した前記動作ログに付加する付加手段をさらに備え、前記暗号化手段は、前記秘密鍵で、前記付加手段で前記時刻情報が付加された前記動作ログを暗号化することを特徴とする。
【００１０】
また、本発明にかかる画像読取装置は、前記の画像読取装置において、温度センサ、湿度センサ、高度センサのうち少なくとも１つをさらに備えたことを特徴とする。
【００１１】
また、本発明にかかる画像読取装置は、前記の画像読取装置において、前記動作ログは、原稿を読み取ったときの読取パラメータ、読取枚数、読取時刻、発生エラーコード、エラー発生時刻、操作者識別情報、気温、装置温度、湿度、高度のうち少なくとも１つを含むことを特徴とする。
【００１２】
また、本発明にかかる画像読取装置は、前記の画像読取装置において、画像情報を一意に識別するための情報である画像識別情報を生成する生成手段をさらに備え、前記チップは、前記生成手段で生成した前記画像識別情報を、当該画像読取装置で読み取った前記画像情報に付加する識別情報付加手段をさらに備え、前記暗号化手段は、前記秘密鍵で、前記識別情報付加手段で前記画像識別情報が付加された前記画像情報を暗号化することを特徴とする。
【００１３】
また、本発明にかかる画像読取装置は、前記の画像読取装置において、前記動作ログは、当該画像読取装置で前記画像情報を読み取ったときの読取パラメータ、前記読み取ったときの読取枚数、前記読み取ったときの読取時刻、当該画像読取装置で発生したエラーに関する発生エラーコード、前記エラーが発生したときのエラー発生時刻、当該画像読取装置を操作する操作者を一意に識別するための情報である操作者識別情報のうち少なくとも１つを含むことを特徴とする。
【００１４】
また、本発明にかかる画像読取装置は、前記の画像読取装置において、温度センサ、湿

度センサ、高度センサのうち少なくとも１つをさらに備え、前記動作ログは、前記温度センサで検出した気温、前記温度センサで検出した装置温度、前記湿度センサで検出した湿度、前記高度センサで検出した高度のうち少なくとも１つを含むことを特徴とする。

【００１５】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、ネットワークを介して当該画像読取装置と通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段、当該画像読取装置で前記画像情報が読み取られる度に、当該画像読取装置に予め格納されたシリアル番号を更新する更新手段のいずれか１つをさらに備え、前記画像識別情報は、当該画像読取装置固有の情報である機器固有情報と、前記取得手段で取得した前記時刻情報または前記更新手段で更新した前記シリアル番号とからなることを特徴とする。

【００１６】

また、本発明にかかる画像読取装置は、ネットワークを介してサーバ装置と通信可能に接続され、動作ログを記録する記録手段を備えた画像読取装置において、耐タンパー性を有するチップと、前記記録手段で記録した前記動作ログのハッシュ値を生成するハッシュ値生成手段と、前記サーバ装置へ情報を送信する送信手段と、を備え、前記チップは、当該画像読取装置固有の秘密鍵を格納する格納手段と、前記格納手段で格納した前記秘密鍵で、前記ハッシュ値生成手段で生成した前記ハッシュ値を暗号化する暗号化手段とをさらに備えたことを特徴とする。

【００１７】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、ネットワークを介して通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段をさらに備え、前記チップは、前記取得手段で取得した前記時刻情報を、前記記録手段で記録した前記動作ログに付加する付加手段をさらに備え、前記ハッシュ値生成手段は、前記付加手段で前記時刻情報が付加された前記動作ログのハッシュ値を生成することを特徴とする。

【００１８】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、温度センサ、湿度センサ、高度センサのうち少なくとも１つをさらに備えたことを特徴とする。

【００１９】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、前記動作ログは、原稿を読み取ったときの読取パラメータ、読取枚数、読取時刻、発生エラーコード、エラー発生時刻、操作者識別情報、気温、装置温度、湿度、高度のうち少なくとも１つを含むことを特徴とする。

【００２０】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、画像情報を一意に識別するための情報である画像識別情報を生成する生成手段をさらに備え、前記チップは、前記生成手段で生成した前記画像識別情報を、当該画像読取装置で読み取った前記画像情報に付加する識別情報付加手段をさらに備え、前記ハッシュ値生成手段は、前記識別情報付加手段で前記画像識別情報が付加された前記画像情報の前記ハッシュ値を生成することを特徴とする。

【００２１】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、前記動作ログは、当該画像読取装置で前記画像情報を読み取ったときの読取パラメータ、前記読み取ったときの読取枚数、前記読み取ったときの読取時刻、当該画像読取装置で発生したエラーに関する発生エラーコード、前記エラーが発生したときのエラー発生時刻、当該画像読取装置を操作する操作者を一意に識別するための情報である操作者識別情報のうち少なくとも１つを含むことを特徴とする。

【００２２】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、温度センサ、湿

度センサ、高度センサのうち少なくとも１つをさらに備え、前記動作ログは、前記温度センサで検出した気温、前記温度センサで検出した装置温度、前記湿度センサで検出した湿度、前記高度センサで検出した高度のうち少なくとも１つを含むことを特徴とする。

【００２３】

また、本発明にかかる画像読取装置は、前記の画像読取装置において、ネットワークを介して当該画像読取装置と通信可能に接続された時刻管理を行うタイムサーバ装置から時刻情報を取得する取得手段、当該画像読取装置で前記画像情報が読み取られる度に、当該画像読取装置に予め格納されたシリアル番号を更新する更新手段のいずれか１つをさらに備え、前記画像識別情報は、当該画像読取装置固有の情報である機器固有情報と、前記取得手段で取得した前記時刻情報または前記更新手段で更新した前記シリアル番号とからなることを特徴とする。

【００２４】

また、本発明はプログラムに関するものであり、本発明にかかるプログラムは、画像読取装置に、動作ログを記録する記録ステップと、当該装置が備えた耐タンパー性を有するチップにて、当該チップに予め格納した当該装置固有の秘密鍵で、前記記録ステップで記録した前記動作ログを暗号化する暗号化ステップと、前記暗号化ステップで暗号化した前記動作ログを、ネットワークを介して当該装置と通信可能に接続されたサーバ装置へ送信する送信ステップと、を実行させることを特徴とする。

【００２５】

また、本発明にかかるプログラムは、前記のプログラムにおいて、画像読取装置に、画像情報を読み取る読取ステップと、前記画像情報を一意に識別するための情報である画像識別情報を生成する生成ステップと、前記チップにて、前記生成ステップで生成した前記画像識別情報を、前記読取ステップで読み取った前記画像情報に付加する識別情報付加ステップと、をさらに実行させ、前記暗号化ステップは、前記チップにて、前記秘密鍵で、前記識別情報付加ステップで前記画像識別情報が付加された前記画像情報を暗号化し、前記送信ステップは、前記暗号化ステップで暗号化した前記画像情報を前記サーバ装置へ送信することを特徴とする。

【００２６】

また、本発明にかかるプログラムは、画像読取装置に、動作ログを記録する記録ステップと、前記記録ステップで記録した前記動作ログのハッシュ値を生成するハッシュ値生成ステップと、当該装置が備えた耐タンパー性を有するチップにて、当該チップに予め格納した当該装置固有の秘密鍵で、前記ハッシュ値生成ステップで生成した前記ハッシュ値を暗号化する暗号化ステップと、前記暗号化ステップで暗号化した前記ハッシュ値および前記動作ログを、ネットワークを介して当該装置と通信可能に接続されたサーバ装置へ送信する送信ステップと、を実行させることを特徴とする。

【００２７】

また、本発明にかかるプログラムは、前記のプログラムにおいて、画像読取装置に、画像情報を読み取る読取ステップと、画像情報を一意に識別するための情報である画像識別情報を生成する生成ステップと、前記チップにて、前記生成ステップで生成した前記画像識別情報を、前記読取ステップで読み取った前記画像情報に付加する識別情報付加ステップと、をさらに実行させ、前記ハッシュ値生成手段は、前記識別情報付加ステップで前記画像識別情報が付加された前記画像情報の前記ハッシュ値を生成し、前記送信ステップは、前記暗号化ステップで暗号化した前記ハッシュ値および前記画像識別情報が付加された前記画像情報を前記サーバ装置へ送信することを特徴とする。

【発明の効果】

【００２８】

本発明は、例えばセキュリティや保守を目的として動作ログを分析する場合などにおいて、動作ログの信頼性や否偽証性（偽りがないこと）を確保することができる等の効果を奏する。また、本発明は、画像情報がどういう経路を通ったかをマッピングすることができるので、画像情報のトレーサビリティーを確保することができる等の効果を奏する。

【発明を実施するための最良の形態】
【００２９】
以下に、本発明にかかる画像読取装置およびプログラムの実施の形態を図面に基づいて詳細に説明する。なお、本実施の形態により本発明が限定されるものではない。特に、本実施の形態においては、耐タンパー性を有するチップとしてＴＰＭチップを一例に挙げて説明するが、本発明は本実施の形態に限定されるものではない。
【００３０】
［本発明の概要（その１）］
図１は本発明の基本原理を示す原理構成図である。本発明は概略的に以下の基本的特徴を有する。本システムは、概略的に、スキャナやプリンタ、複合機、ＦＡＸなどの画像読取装置１００とサーバ装置２００とをネットワーク３００を介して通信可能に接続して構成されている。画像読取装置１００は、特徴として、当該画像読取装置固有の秘密鍵を格納した耐タンパー性を有するチップであるＴＰＭチップ１０を備えている。なお、本システムは、図示の如く、時刻管理を行うタイムサーバ装置４００を、ネットワーク３００を介して通信可能に接続して構成してもよい。
【００３１】
そして、画像読取装置１００は、まず、当該画像読取装置が動作した際の動作ログを記録する（ステップＳ－１）。つぎに、画像読取装置１００は、定期的に又は外部からの要求があったときに、ＴＰＭチップ１０で、記録した動作ログを、当該画像読取装置固有の秘密鍵で暗号化する（ステップＳ－２）。つぎに、画像読取装置１００は、暗号化した動作ログを、ネットワーク３００を介してサーバ装置２００へ送信する（ステップＳ－３）。
【００３２】
一方、サーバ装置２００は、画像読取装置１００から送信された動作ログを受信して（ステップＳ－４）、蓄積する（ステップＳ－５）。
【００３３】
ここで、本システムにおいてタイムサーバ装置４００が図示の如くネットワーク３００を介して通信可能に接続して構成されている場合、画像読取装置１００は、タイムサーバ装置４００から時刻情報を取得し、取得した時刻情報を、ステップＳ－１で記録した動作ログに付加し、時刻情報が付加された動作ログである時刻付動作ログをＴＰＭチップ１０で暗号化し、暗号化した時刻付動作ログをサーバ装置２００へ送信してもよい。
【００３４】
また、画像読取装置１００は、温度センサ、湿度センサ、高度センサなどのうち少なくとも１つをさらに備えてもよい。
【００３５】
また、動作ログは、原稿を読み取ったときの読取パラメータ（例えば原稿サイズ、給紙条件（ＡＤＦ／ＦＢ／片面／両面）、解像度、カラー／モノクロなど）、読取枚数、読取時刻、発生エラーコード、エラー発生時刻、操作者を一意に識別するための操作者識別情報、気温、装置温度、湿度、高度のうち少なくとも１つを含んでもよい。
【００３６】
［本発明の概要（その２）］
図２は本発明の基本原理を示す原理構成図である。本発明が概略的に以下の基本的特徴を有する。スキャナやプリンタ、複合機、ＦＡＸなどの画像読取装置１００は、まず、当該画像読取装置が備えた画像処理部で、画像情報（画像データ）を読み取る（ステップＴ－１）。
【００３７】
そして、画像読取装置１００は、ステップＴ－１で読み取った画像情報を一意に識別するための情報である画像ＩＤなどの画像識別情報を生成し、ＴＰＭチップ１０で、生成した画像識別情報をステップＴ－１で読み取った画像情報に付加することで、画像情報および画像識別情報からなる画像ファイルを作成する。具体的には、画像識別情報が例えば当

該画像読取装置固有の情報である機器固有情報とシリアル番号とで構成される場合には、画像読取装置１００は、ＴＰＭチップ１０で、当該画像読取装置が備えた機器情報ファイルから機器固有時情報を取得する（ステップＴ－２）と共に、ステップＴ－１で画像情報が読み取られた際にカウンターで生成（更新）されたシリアル番号を取得し（ステップＴ－３）、取得した機器固有情報およびシリアル番号を組み合わせて画像識別情報を作成し、作成した画像識別情報を動作ログの一部として当該画像読取装置の所定の記憶領域（ログ保存領域）に保存（記録）する。なお、ＴＰＭチップ１０で収集した動作ログ自体は、画像読取装置１００が備えるハードディスク等の記憶装置に蓄積し、ＴＰＭチップ１０では当該動作ログのハッシュ値及び／又は動作ログの格納場所を示すアドレスを蓄積してもよい。また、当該動作ログのハッシュ値及び／又は動作ログの格納場所を示すアドレスは、ＴＰＭチップ１０固有の秘密鍵で暗号化した上で、ハードディスク等の記憶装置に蓄積してもよい。

【００３８】

ここで、画像識別情報は機器固有情報と時刻情報とで構成されてもよい。時刻情報は、ネットワークを介して画像読取装置１００と通信可能に接続された時刻管理を行うタイムサーバ装置から当該画像読取装置が取得したものでもよい。カウンターは、当該画像読取装置で画像情報が読み取られる度に当該画像読取装置に予め格納されたシリアル番号を更新する更新手段であり、例えばＴＰＭチップ１０が備えたモノトニックカウンターなどである。

【００３９】

動作ログは例えば画像識別情報に加えて、さらにその他のログ項目を含んでもよい。その他のログ項目は、例えば、画像情報を読み取ったときの読取パラメータ、画像情報を読み取ったときの読取枚数、画像情報を読み取ったときの読取時刻、画像読取装置１００で発生したエラーに関する発生エラーコード、エラーが発生したときのエラー発生時刻、当該画像読取装置を操作する操作者を一意に識別するための情報である操作者識別情報、当該画像読取装置が備えた温度センサで検出された気温、当該温度センサで検出された装置温度、当該画像読取装置が備えた湿度センサで検出された湿度、当該画像読取装置が備えた高度センサで検出された高度などを含んでもよい。

【００４０】

図２の説明に戻り、画像読取装置１００は、ＴＰＭチップ１０で、画像ファイルを、当該ＴＰＭチップの秘密鍵ファイルに格納された秘密鍵で暗号化する（ステップＴ－４）。

【００４１】

そして、画像読取装置１００は、ステップＴ－４で暗号化した画像ファイルを、例えば当該画像読取装置と通信可能に接続されたパーソナルコンピュータやサーバ装置へ送信する（ステップＴ－５）。これにより、パーソナルコンピュータやサーバ装置は、画像情報と共に、動作ログを蓄積することができる。

【００４２】

以上、本発明にかかる画像読取装置１００によれば、蓄積された動作ログを見ることで、例えば或る画像ＩＤの画像情報がどの画像読取装置から出力されたものであるかを特定することが可能になるので、画像情報（画像データ）のトレーサビリティーを確保することができる。また、画像読取装置１００によれば、例えば画像ＩＤが付加された画像情報を暗号化して他の装置へ送信するので、伝送路上での画像ＩＤの改竄を検出することができ、その結果、画像データの信頼性の度合いを向上させることができる。

【００４３】

［本発明の概要（その３）］

図３は本発明の基本原理を示す原理構成図である。本発明が概略的に以下の基本的特徴を有する。なお、［本発明の概要（その１）］での説明と同様のものについては、その説明を省略する場合がある。

【００４４】

まず、画像読取装置１００は、当該画像読取装置が動作した際の動作ログを記録する（

ステップＵ－１）。つぎに、画像読取装置１００は、ステップＵ－１で記録した動作ログのハッシュ値を生成する（ステップＵ－２）。つぎに、画像読取装置１００は、定期的に又は外部からの要求があったときに、ＴＰＭチップ１０で、生成したハッシュ値を、当該画像読取装置固有の秘密鍵で暗号化する（ステップＵ－３）。つぎに、画像読取装置１００は、暗号化したハッシュ値および動作ログを、ネットワーク３００を介してサーバ装置２００へ送信する（ステップＵ－４）。

【００４５】

一方、サーバ装置２００は、画像読取装置１００から送信されたハッシュ値および動作ログを受信して（ステップＵ－５）、蓄積する（ステップＵ－６）。

【００４６】

ここで、本システムにおいてタイムサーバ装置４００が図示の如くネットワーク３００を介して通信可能に接続して構成されている場合、画像読取装置１００は、タイムサーバ装置４００から時刻情報を取得し、取得した時刻情報を、ステップＳ－１で記録した動作ログに付加し、時刻情報が付加された動作ログである時刻付動作ログのハッシュ値を生成し、生成したハッシュ値をＴＰＭチップ１０で暗号化し、暗号化したハッシュ値および時刻付動作ログをサーバ装置２００へ送信してもよい。

【００４７】

［本発明の概要（その４）］

図４は本発明の基本原理を示す原理構成図である。本発明が概略的に以下の基本的特徴を有する。なお、［本発明の概要（その２）］での説明と同様のものについては、その説明を省略する場合がある。

【００４８】

まず、画像読取装置１００は、当該画像読取装置が備えた画像処理部で、画像情報（画像データ）を読み取る（ステップＶ－１）。

【００４９】

つぎに、画像読取装置１００は、ステップＶ－１で読み取った画像情報を一意に識別するための情報である画像ＩＤなどの画像識別情報を生成し、ＴＰＭチップ１０で、生成した画像識別情報をステップＶ－１で読み取った画像情報に付加することで、画像情報および画像識別情報からなる画像ファイルを作成する。具体的には、画像識別情報が例えば当該画像読取装置固有の情報である機器固有情報とシリアル番号とで構成される場合には、画像読取装置１００は、ＴＰＭチップ１０で、当該画像読取装置が備えた機器情報ファイルから機器固有時情報を取得する（ステップＶ－２）と共に、ステップＶ－１で画像情報が読み取られた際にカウンターで生成（更新）されたシリアル番号を取得し（ステップＶ－３）、取得した機器固有情報およびシリアル番号を組み合わせて画像識別情報を作成し、作成した画像識別情報を動作ログの一部として当該画像読取装置の所定の記憶領域（ログ保存領域）に保存（記録）する。

【００５０】

つぎに、画像読取装置１００は、画像ファイルのハッシュ値を生成する（ステップＶ－４）。つぎに、画像読取装置１００は、ＴＰＭチップ１０で、ハッシュ値を、当該ＴＰＭチップの秘密鍵ファイルに格納された秘密鍵で暗号化する（ステップＶ－５）。

【００５１】

そして、画像読取装置１００は、ステップＶ－５で暗号化したハッシュ値および画像ファイルを、例えば当該画像読取装置と通信可能に接続されたパーソナルコンピュータやサーバ装置へ送信する（ステップＶ－６）。

【００５２】

以上、本発明にかかる画像読取装置１００によれば、蓄積された動作ログを見ることで、例えば或る画像ＩＤの画像情報がどの画像読取装置から出力されたものであるかを特定することが可能になるので、画像情報（画像データ）のトレーサビリティーを確保することができる。また、画像読取装置１００によれば、例えば画像ＩＤが付加された画像情報を電子署名して他の装置へ送信するので、伝送路上での画像ＩＤの改竄を検出することが

でき、その結果、画像データの信頼性の度合いを向上させることができる。

【００５３】

［システム構成］

次に、本システムの構成について図５から図７を用いて説明する。図５は、本発明が適用される画像読取装置１００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図５に示すように、画像読取装置１００は、概略的に、機構ユニット１１０、制御ユニット１２０、光学ユニット１３０を少なくとも備えて構成されている。そして、これらのユニット毎に、ユニットに関する情報を収集しそれらを記憶する耐タンパー性を有するチップであるＴＰＭチップ１０を搭載する。ＴＰＭチップ１０には、署名・暗号化に必要な秘密鍵などが格納されている他、指紋等の個人認証機能も搭載されていてもよい。また、ＴＰＭチップ１０は、外部から容易に取り外しできない形で各ユニットの筐体内に取り付けられており、取り外すとそのユニットは動作ができないようになっている。

【００５４】

機構ユニット１１０は、モータ、センサ等を含む自動給紙部／フラットベット部と、ＴＰＭチップ１０とがユニットインターフェース部を介して相互に接続されている。制御ユニット１２０は、ＭＰＵと、制御プログラムを格納したメモリ装置と、画像処理部と、指紋取得部と、外部インターフェース部と、ＲＡＭと、ＴＰＭチップ１０とがユニットインターフェース部を介して相互に接続されている。光学ユニット１３０は、ＣＣＤ、光源等を含む光学系装置と、ＴＰＭチップ１０とがユニットインターフェース部を介して相互に接続されている。

【００５５】

ここで、各ユニット（機構ユニット１１０、制御ユニット１２０、光学ユニット１３０）において、各種のセンサ（温度センサ、湿度センサ、高度センサ）を備えてユニットの環境（温度、湿度、高度など）を測定してもよい。

【００５６】

図６は、本発明が適用されるＴＰＭチップ１０の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。図６に示すように、ＴＰＭチップ１０は、ＭＰＵ１１と、ユニットを制御するための制御プログラム１２と、動作ログや時刻付動作ログなどを暗号化するための秘密鍵ファイル１３と、ユニットの機体識別番号を少なくとも含むユニット情報を格納するユニット情報ファイル１４と、個人認証用の指紋情報などを格納する個人認証情報ファイル１５と、ユニットの環境（温度、湿度、高度など）に関する測定値、ユニットの動作時の設定情報および動作結果を含む動作ログなどを格納するＲＡＭ１６と、を少なくとも備えて構成される。

【００５７】

図７は、本発明が適用されるサーバ装置２００およびタイムサーバ装置４００の構成の一例を示すブロック図であり、該構成のうち本発明に関係する部分のみを概念的に示している。サーバ装置２００およびタイムサーバ装置４００のハードウェア構成は、一般に市販されるワークステーション、パーソナルコンピュータ等の情報処理装置およびその付属装置により構成してもよい。また、サーバ装置２００およびタイムサーバ装置４００の各機能は、ハードウェア構成中のＣＰＵなどの制御装置と、ハードディスク装置、メモリ装置（ＲＡＭ、ＲＯＭなど）などの記憶装置と、入力装置と、出力装置と、入出力インターフェースと、通信制御インターフェース、および、それらを制御するプログラム等により実現される。

【００５８】

［システムの処理（その１）］

次に、このように構成された本実施の形態における本システムの処理の一例について、図８を参照して詳細に説明する。なお、以下の説明において、画像読取装置１００は、温度センサ、湿度センサ、高度センサを備えているものとする。

【００５９】

まず、画像読取装置１００は、当該画像読取装置が動作した際の動作ログを記録する（記録手段：ステップＳＡ－１）。ここで、動作ログには、原稿を読み取ったときの読取パラメータ（例えば原稿サイズ、給紙条件（ＡＤＦ／ＦＢ／片面／両面）、解像度、カラー／モノクロなど）、読取枚数、読取時刻、発生エラーコード、エラー発生時刻、操作者識別情報、気温、装置温度、湿度、高度のうち少なくとも１つが含まれる。

【００６０】

つぎに、画像読取装置１００は、ネットワーク３００を介して、タイムサーバ装置４００から時刻情報を取得する（取得手段：ステップＳＡ－２）。具体的には、まず、画像読取装置１００は、取得部で、時刻情報の提供要求を、ネットワーク３００を介してタイムサーバ装置４００へ行う（ステップＳＡ－２－１）。つぎに、タイムサーバ装置４００は、画像読取装置１００から送信された提供要求を受信し（ステップＳＡ－２－２）、当該タイムサーバ装置で管理している時刻情報を、ネットワーク３００を介して画像読取装置１００へ送信する（ステップＳＡ－２－３）。つぎに、画像読取装置１００は、取得部で、タイムサーバ装置４００から送信された時刻情報を受信する（ステップＳＡ－２－４）。ここで、画像読取装置１００がリアルタイムクロックをさらに備えている場合、画像読取装置１００は、当該リアルタイムクロックの精度に応じて、前回の時刻取得時から一定時間が経過していたら、時刻情報の取得を行ってもよい。

【００６１】

つぎに、画像読取装置１００は、ステップＳＡ－２で取得した時刻情報を、ステップＳＡ－１で記録した動作ログに付加する（付加手段：ステップＳＡ－３）。

【００６２】

つぎに、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＡ－３で時刻情報が付加された動作ログである時刻付動作ログを、当該画像読取装置固有の秘密鍵で暗号化する（ステップＳＡ－４）。

【００６３】

つぎに、画像読取装置１００は、ステップＳＡ－４で暗号化した時刻付動作ログを、ネットワーク３００を介してサーバ装置２００へ送信する（送信手段：ステップＳＡ－５）。

【００６４】

つぎに、サーバ装置２００は、画像読取装置１００から送信された時刻付動作ログを受信する（ステップＳＡ－６）。

【００６５】

つぎに、サーバ装置２００は、ステップＳＡ－６で受信した時刻付動作ログを蓄積する（ステップＳＡ－７）。

【００６６】

これにて、メイン処理の説明を終了する。

【００６７】

［システムの処理（その２）］

ここでは、上述したように構成された本実施の形態における本システムの処理の一例について、図９および図１０を参照して詳細に説明する。なお、以下の説明において、画像読取装置１００は、シリアル番号を生成・更新するカウンター、タイムサーバ装置から時刻情報を取得する時刻取得部、温度センサ、湿度センサ、高度センサを備えているものとする。

【００６８】

まず、画像読取装置１００は、画像情報を読み取る（ステップＳＢ－１）。

【００６９】

つぎに、画像読取装置１００は、ステップＳＢ－１で読み取った画像情報に対応する画像識別情報を生成する（生成手段：ステップＳＢ－２（画像識別情報生成処理））。ここで、画像読取装置１００が行う画像識別情報生成処理の一例について図１０を参照して説明する。

【００７０】
まず、画像読取装置１００は、ＴＰＭチップ１０で、機器固有情報を収集（取得）する（ステップＳＣ－１）。
【００７１】
つぎに、画像読取装置１００は、ＴＰＭチップ１０で、カウンターで更新した後のシリアル番号を取得する（ステップＳＣ－２）。なお、画像読取装置１００は、シリアル番号を取得する代わりに、時刻取得部で、タイムサーバ装置から時刻情報を取得してもよい。なお、時刻情報の取得の仕方については、上述した図８に示すステップＳＡ－２と同じである。
【００７２】
つぎに、画像読取装置１００は、ステップＳＣ－１で収集した機器固有情報と、ステップＳＣ－２で取得したシリアル番号（時刻情報）とを組み合わせて、画像識別情報を作成する（ステップＳＣ－３）。
【００７３】
これにて、画像識別情報生成処理の説明を終了する。
【００７４】
図９に戻り、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＢ－１で読み取った画像情報に、ステップＳＢ－２で生成した画像識別情報を付加する（識別情報付加手段：ステップＳＢ－３）。
【００７５】
つぎに、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＢ－３で画像識別情報が付加された画像情報（画像ファイル）を、当該ＴＰＭチップに格納された秘密鍵で暗号化する（暗号化手段：ステップＳＢ－４）。
【００７６】
つぎに、画像読取装置１００は、ステップＳＢ－４で暗号化した画像ファイルを、サーバ装置２００へ送信する（送信手段：ステップＳＢ－５）。
【００７７】
これにて、メイン処理の説明を終了する。
【００７８】
なお、画像読取装置１００は、上述した図９に示すメイン処理を実行すると共に、動作ログをＴＰＭチップ１０で収集し、収集した動作ログをＴＰＭチップ１０で秘密鍵を用いて暗号化し、暗号化した動作ログをサーバ装置２００へ送信してもよい。ここで、画像読取装置１００は、動作ログを収集するにあたり、ＴＰＭチップ１０で、読取パラメータ、読取枚数、読取時刻、発生エラーコード、エラー発生時刻、操作者識別情報、気温、装置温度、湿度、高度などをその他のログ項目として取得してもよい。そして、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＢ－１で生成した画像識別情報と、取得したその他のログ項目とを組み合わせて、動作ログを作成してもよい。
【００７９】
［システムの処理（その３）］
次に、このように構成された本実施の形態における本システムの処理の一例について、図１１を参照して詳細に説明する。なお、［システムの処理（その１）］での説明と同様のものについては、その説明を省略する場合がある。また、以下の説明において、画像読取装置１００は、温度センサ、湿度センサ、高度センサを備えているものとする。
【００８０】
まず、画像読取装置１００は、当該画像読取装置が動作した際の動作ログを記録する（記録手段：ステップＳＤ－１）。
【００８１】
つぎに、画像読取装置１００は、ネットワーク３００を介して、タイムサーバ装置４００から時刻情報を取得する（取得手段：ステップＳＤ－２）。
【００８２】

つぎに、画像読取装置１００は、ステップＳＤ－２で取得した時刻情報を、ステップＳＤ－１で記録した動作ログに付加する（付加手段：ステップＳＡ－３）。

【００８３】

つぎに、画像読取装置１００は、ステップＳＤ－３で時刻情報が付加された動作ログである時刻付動作ログのハッシュ値を生成する（ハッシュ値生成手段：ステップＳＤ－４）。

【００８４】

つぎに、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＤ－４で生成したハッシュ値を、当該画像読取装置固有の秘密鍵で暗号化する（ステップＳＤ－５）。

【００８５】

つぎに、画像読取装置１００は、ステップＳＤ－４で暗号化したハッシュ値および時刻付動作ログを、ネットワーク３００を介してサーバ装置２００へ送信する（送信手段：ステップＳＤ－６）。

【００８６】

つぎに、サーバ装置２００は、画像読取装置１００から送信されたハッシュ値および時刻付動作ログを受信する（ステップＳＤ－７）。

【００８７】

つぎに、サーバ装置２００は、ステップＳＤ－７で受信したハッシュ値および時刻付動作ログを蓄積する（ステップＳＤ－８）。ここで、画像読取装置１００は、受信した動作ログ（具体的には時刻付動作ログ）を蓄積する前または後に、当該動作ログに付いている電子署名（ハッシュ値）が妥当なものであるかを検証してもよい。つまり、画像読取装置１００は、受信した動作ログを蓄積する前または後に、当該動作ログの検証を行ってもよい。

【００８８】

これにて、メイン処理の説明を終了する。

【００８９】

［システムの処理（その４）］

ここでは、上述したように構成された本実施の形態における本システムの処理の一例について、図１２を参照して詳細に説明する。なお、［システムの処理（その２）］での説明と同様のものについては、その説明を省略する場合がある。また、以下の説明において、画像読取装置１００は、シリアル番号を生成・更新するカウンター、タイムサーバ装置から時刻情報を取得する時刻取得部、温度センサ、湿度センサ、高度センサを備えているものとする。

【００９０】

まず、画像読取装置１００は、画像情報を読み取る（ステップＳＥ－１）。

【００９１】

つぎに、画像読取装置１００は、ステップＳＥ－１で読み取った画像情報に対応する画像識別情報を生成する（生成手段：ステップＳＥ－２（画像識別情報生成処理））。

【００９２】

つぎに、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＥ－１で読み取った画像情報に、ステップＳＥ－２で生成した画像識別情報を付加する（識別情報付加手段：ステップＳＥ－３）。

【００９３】

つぎに、画像読取装置１００は、ステップＳＥ－３で画像識別情報が付加された画像情報（画像ファイル）のハッシュ値を生成する（ハッシュ値生成手段：ステップＳＥ－４）。

【００９４】

つぎに、画像読取装置１００は、ＴＰＭチップ１０で、ステップＳＥ－４で生成したハッシュ値を、当該ＴＰＭチップに格納された秘密鍵で暗号化する（暗号化手段：ステップＳＥ－５）。

【００９５】
つぎに、画像読取装置１００は、ステップＳＥ－５で暗号化したハッシュ値およびステップＳＥ－３で画像識別情報が付加された画像情報（画像ファイル）を、サーバ装置２００へ送信する（送信手段：ステップＳＥ－６）。
【００９６】
これにて、メイン処理の説明を終了する。
【００９７】
なお、画像読取装置１００は、上述した図１２に示すメイン処理を実行すると共に、動作ログをＴＰＭチップ１０で収集し、収集した動作ログのハッシュ値を生成し、生成したハッシュ値をＴＰＭチップ１０で秘密鍵を用いて暗号化し、暗号化したハッシュ値および動作ログをサーバ装置２００へ送信してもよい。
【００９８】
［本実施の形態のまとめ及びその他の実施の形態］
以上説明したように、本実施の形態の本システムにおいて、画像読取装置１００は、当該画像読取装置が動作した際の動作ログを記録し、記録した動作ログをＴＰＭチップ１０で暗号化し、暗号化した動作ログを、ネットワーク３００を介してサーバ装置２００へ送信する。また、画像読取装置１００は、当該画像読取装置が動作した際の動作ログを記録し、記録した動作ログのハッシュ値を生成し、生成したハッシュ値をＴＰＭチップ１０で暗号化し、暗号化したハッシュ値および動作ログを、ネットワーク３００を介してサーバ装置２００へ送信する。つまり、電子署名にてデータ送信を行う。一方、本システムにおいて、サーバ装置２００は、画像読取装置１００から送信された情報（動作ログ、ハッシュ値）を受信し、受信した情報（動作ログ、ハッシュ値）を蓄積する。これにより、例えばセキュリティや保守を目的として動作ログを分析する場合などにおいて、動作ログの信頼性や否偽証性（偽りがないこと）を確保することができる。
【００９９】
ここで、例えば不法侵入者が画像読取装置１００で原稿を読み取りデータ化し、当該データのみを持ち去った場合、原稿自体は持ち去られていないため、通常、画像読取装置１００に記録されたログをチェックすることで画像読取装置１００が不正に使用されたかを確認していた。しかし、従来では、当該ログが容易に改竄可能な状態にあったので、当該ログの信頼性は低く、故に不正に使用されたかの確認結果の信頼性も低かった。ところが、画像読取装置１００を導入すれば、耐タンパー性を有するＴＰＭチップ１０でログの電子署名を行うので、ログが偽りなく当該画像読取装置にて生成されたものであることを証明することができる。
【０１００】
また、或る者の誤動作や悪意により、ログが書換えられる可能性を排除することができ、その結果、保守の効率を高めることができる。また、サーバ装置２００が保守のサービスセンターに設置されている場合、当該センターで、サーバ装置２００に蓄積された多量の動作ログを分析することにより、例えば或る装置でエラー発生頻度が高いなどの傾向を容易に調査することができる。
【０１０１】
また、本システムにおいて、画像読取装置１００は、温度センサ、湿度センサ、高度センサを備えているので、画像読取装置１００が使用されている環境（気候や地域など）に関する情報も正確に得ることができる。
【０１０２】
また、画像読取装置１００は、画像情報を読み取り、ＴＰＭチップ１０で画像識別情報を生成し、生成した画像識別情報をＴＰＭチップ１０で画像情報に付加し、画像識別情報が付加された画像情報をＴＰＭチップ１０で秘密鍵により暗号化し、暗号化した画像情報をサーバ装置２００へ送信する。また、画像読取装置１００は、画像情報を読み取り、ＴＰＭチップ１０で画像識別情報を生成し、生成した画像識別情報をＴＰＭチップ１０で画像情報に付加し、画像識別情報が付加された画像情報のハッシュ値を生成し、生成したハ

ッシュ値をＴＰＭチップ１０で秘密鍵により暗号化し、暗号化したハッシュ値および画像情報を、ネットワーク３００を介してサーバ装置２００へ送信する。つまり、電子署名にてデータ送信を行う。これにより、サーバ装置２００に蓄積された動作ログを見ることで、例えば或る画像ＩＤの画像情報がどの画像読取装置から出力されたものであるかを特定することが可能になるので、画像情報（画像データ）のトレーサビリティーを確保することができる。また、画像読取装置１００によれば、例えば画像ＩＤが付加された画像情報を暗号化して他の装置へ送信するので、伝送路上での画像ＩＤの改竄を検出することができ、その結果、画像データの信頼性の度合いを向上させることができる。

【０１０３】

また、本発明は、上述した実施の形態以外にも、特許請求の範囲の書類に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてよいものである。例えば、本実施の形態において説明した各処理のうち、自動的に行なわれるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行なわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。

【０１０４】

この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種の登録データや検索条件等のパラメータを含む情報、画面例、データベース構成については、特記する場合を除いて任意に変更することができる。

【０１０５】

また、図示の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。例えば、制御装置の各部または各装置が備える処理機能については、その全部または任意の一部を、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）および当該ＣＰＵにて解釈実行されるプログラムにて実現することができ、あるいは、ワイヤードロジックによるハードウェアとして実現することも可能である。なお、プログラムは、後述する記録媒体に記録されており、必要に応じて制御装置に機械的に読み取られる。すなわち、ＲＯＭまたはＨＤなどの記憶装置には、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）と協働してＣＰＵに命令を与え、各種処理を行うためのコンピュータプログラムが記録されている。このコンピュータプログラムは、ＲＡＭ等にロードされることによって実行され、ＣＰＵと協働して制御装置を構成する。また、このコンピュータプログラムは、任意のネットワークを介して接続されたアプリケーションプログラムサーバに記録されてもよく、必要に応じてその全部または一部をダウンロードすることも可能である。

【０１０６】

また、本発明にかかるプログラムを、コンピュータ読み取り可能な記録媒体に格納することもできる。ここで、「記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等の任意の「可搬用の物理媒体」や、各種コンピュータシステムに内蔵されるＲＯＭ、ＲＡＭ、ＨＤ等の任意の「固定用の物理媒体」、あるいは、ＬＡＮ、ＷＡＮ、インターネットに代表されるネットワークを介してプログラムを送信する場合の通信回線や搬送波のように、短期にプログラムを保持する「通信媒体」を含むものとする。また、「プログラム」とは、任意の言語や記述方法にて記述されたデータ処理方法であり、ソースコードやバイナリコード等の形式を問わない。なお、「プログラム」は必ずしも単一的に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）に代表される別個のプログラムと協働してその機能を達成するものをも含む。なお、本実施の形態に示した各装置において記録媒体を読み取るための具体的な構成、読み取り手順、あるいは、読み取り後のインストール手順等については、周知の構成や手順を用いることができる。

【０１０７】

さらに、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷等に応じた任意の単位で、機能的または物理的に分散・統合して構成す

ることができる。例えば、各データベースを独立したデータベース装置として独立に構成してもよく、また、処理の一部をＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）を用いて実現してもよい。

【産業上の利用可能性】

【０１０８】

以上のように、本発明にかかる画像読取装置およびプログラムは、産業上の多くの分野、特に情報処理、画像処理産業等の分野で広く実施することができ、特にスキャナやプリンタ、複合機、ＦＡＸなどに極めて有用である。

【図面の簡単な説明】

【０１０９】

【図１】本発明の基本原理を示す原理構成図である。

【図２】本発明の基本原理を示す原理構成図である。

【図３】本発明の基本原理を示す原理構成図である。

【図４】本発明の基本原理を示す原理構成図である。

【図５】本発明が適用される画像読取装置１００の構成の一例を示すブロック図である。

【図６】本発明が適用されるＴＰＭチップ１０の構成の一例を示すブロック図である。

【図７】本発明が適用されるサーバ装置２００およびタイムサーバ装置４００の構成の一例を示すブロック図である。

【図８】本実施の形態における本システムのメイン処理の一例を示すフローチャートである。

【図９】本実施の形態における本システムのメイン処理の一例を示すフローチャートである。

【図１０】本実施の形態における本システムの画像識別情報生成処理の一例を示すフローチャートである。

【図１１】本実施の形態における本システムのメイン処理の一例を示すフローチャートである。

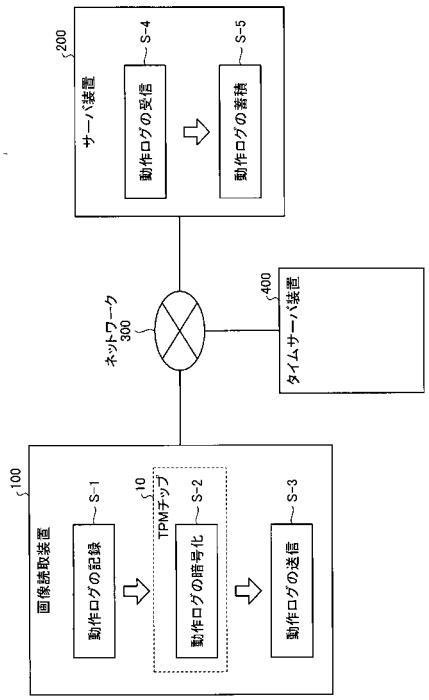
【図１２】本実施の形態における本システムのメイン処理の一例を示すフローチャートである。

【符号の説明】

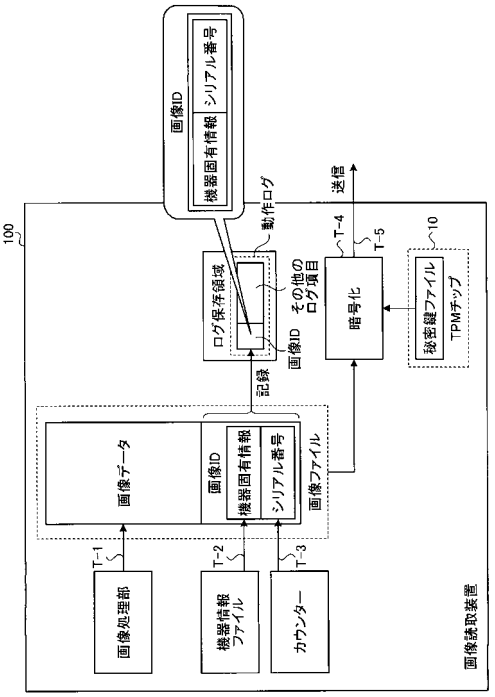
【０１１０】

１００　画像読取装置
　１０　耐タンパー性を有するチップ（ＴＰＭチップ）
　１１　ＭＰＵ
　１２　制御プログラム
　１３　秘密鍵ファイル
　１４　ユニット情報ファイル
　１５　個人認証情報ファイル
　１６　ＲＡＭ
１１０　機構ユニット
１２０　制御ユニット
１３０　光学ユニット
２００　サーバ装置
３００　ネットワーク
４００　タイムサーバ装置

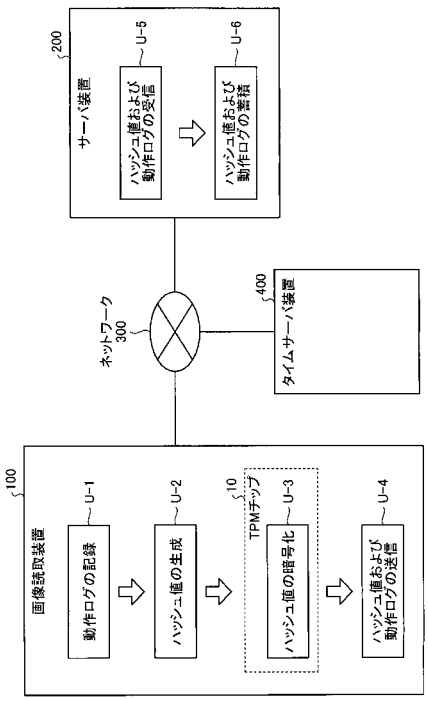
【図１】


200
サーバ装置
S-4
動作ログの受信
S-5
動作ログの蓄積
ネットワーク
300
400
タイムサーバ装置
100
画像読取装置
S-1
動作ログの記録
10
TPMチップ
S-2
動作ログの暗号化
S-3
動作ログの送信

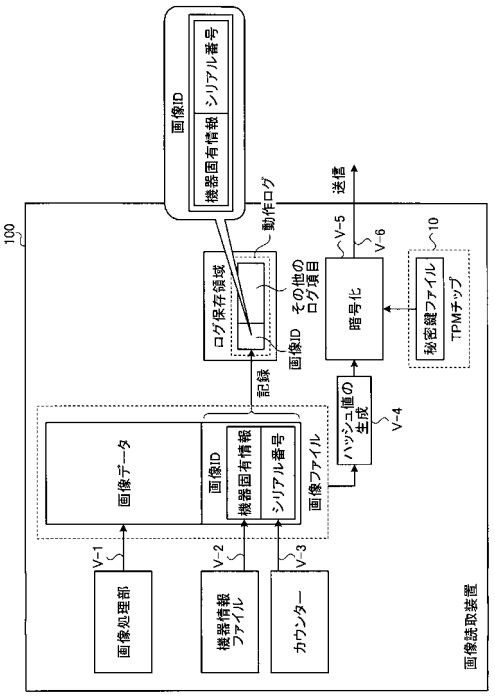
【図２】


100
画像ID
機器固有情報
シリアル番号
動作ログ
送信
ログ保存領域
記録
画像ID
その他の
ログ項目
T-4
T-5
暗号化
10
秘密鍵ファイル
TPMチップ
画像データ
画像ID
機器固有情報
シリアル番号
画像ファイル
T-1
T-2
T-3
画像処理部
機器情報
ファイル
カウンター
画像読取装置

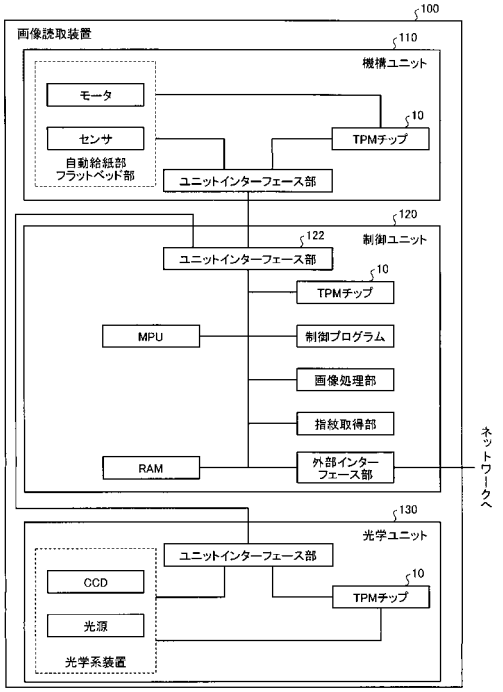
【図３】


200
サーバ装置
U-5
ハッシュ値および
動作ログの受信
U-6
ハッシュ値および
動作ログの蓄積
ネットワーク
300
400
タイムサーバ装置
100
画像読取装置
U-1
動作ログの記録
U-2
ハッシュ値の生成
10
TPMチップ
U-3
ハッシュ値の暗号化
U-4
ハッシュ値および
動作ログの送信

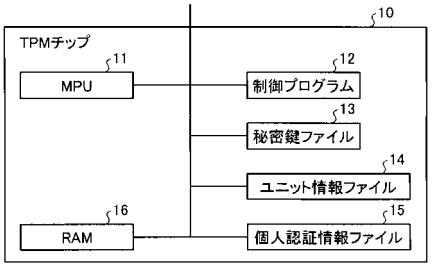
【図４】


100
画像ID
機器固有情報
シリアル番号
動作ログ
送信
ログ保存領域
記録
画像ID
その他の
ログ項目
V-5
V-6
暗号化
10
秘密鍵ファイル
TPMチップ
ハッシュ値の
生成
V-4
画像データ
画像ID
機器固有情報
シリアル番号
画像ファイル
V-1
V-2
V-3
画像処理部
機器情報
ファイル
カウンター
画像読取装置

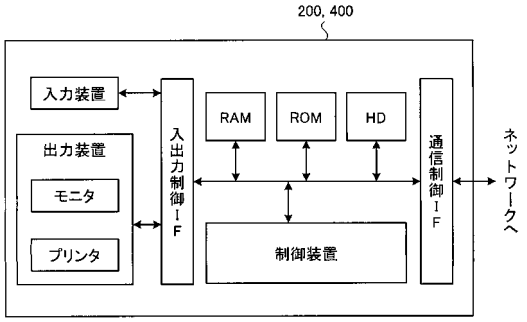
【図５】


100
画像読取装置
110
機構ユニット
モータ
センサ
自動給紙部
フラットベッド部
10
TPMチップ
ユニットインターフェース部
120
制御ユニット
122
ユニットインターフェース部
10
TPMチップ
MPU
制御プログラム
画像処理部
指紋取得部
RAM
外部インターフェース部
ネットワークへ
130
光学ユニット
ユニットインターフェース部
CCD
光源
光学系装置
10
TPMチップ

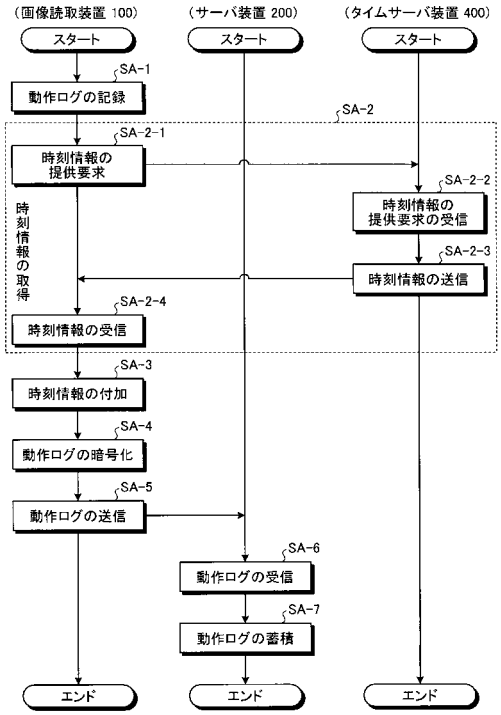
【図６】


10
TPMチップ
11
MPU
12
制御プログラム
13
秘密鍵ファイル
14
ユニット情報ファイル
16
RAM
15
個人認証情報ファイル

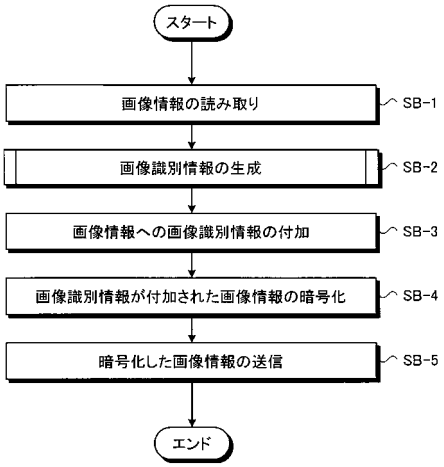
【図７】


200, 400
入力装置
出力装置
モニタ
プリンタ
入出力制御I/F
RAM
ROM
HD
制御装置
通信制御I/F
ネットワークへ

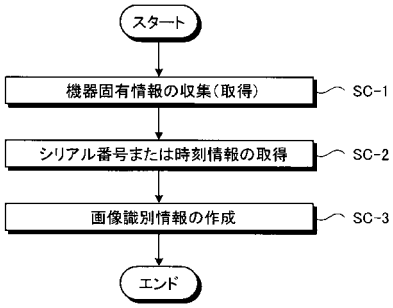
【図８】


(画像読取装置 100)
(サーバ装置 200)
(タイムサーバ装置 400)
スタート
スタート
スタート
SA-1
動作ログの記録
SA-2
SA-2-1
時刻情報の提供要求
SA-2-2
時刻情報の提供要求の受信
SA-2-3
時刻情報の送信
時刻情報の取得
SA-2-4
時刻情報の受信
SA-3
時刻情報の付加
SA-4
動作ログの暗号化
SA-5
動作ログの送信
SA-6
動作ログの受信
SA-7
動作ログの蓄積
エンド
エンド
エンド

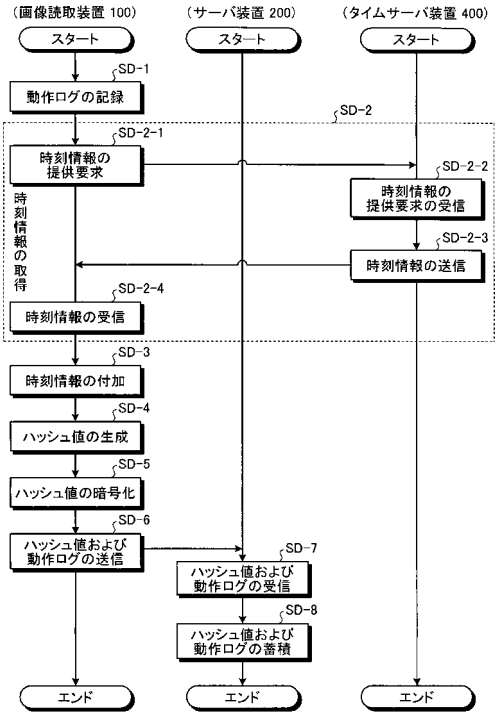
【図９】


スタート
画像情報の読み取り
SB-1
画像識別情報の生成
SB-2
画像情報への画像識別情報の付加
SB-3
画像識別情報が付加された画像情報の暗号化
SB-4
暗号化した画像情報の送信
SB-5
エンド

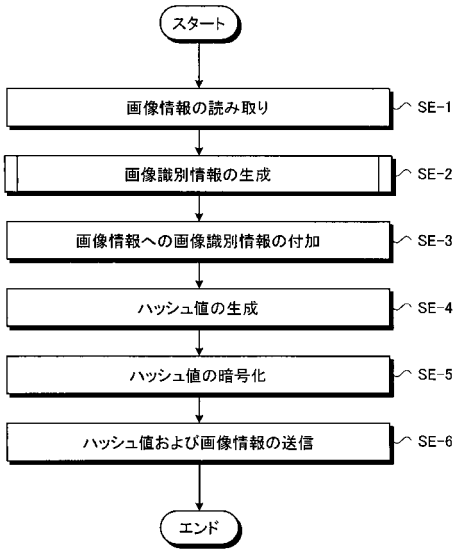
【図１０】


スタート
機器固有情報の収集（取得）
SC-1
シリアル番号または時刻情報の取得
SC-2
画像識別情報の作成
SC-3
エンド

【図１１】


（画像読取装置 100）
（サーバ装置 200）
（タイムサーバ装置 400）
スタート
スタート
スタート
SD-1
動作ログの記録
SD-2
SD-2-1
時刻情報の提供要求
SD-2-2
時刻情報の提供要求の受信
SD-2-3
時刻情報の送信
時刻情報の取得
SD-2-4
時刻情報の受信
SD-3
時刻情報の付加
SD-4
ハッシュ値の生成
SD-5
ハッシュ値の暗号化
SD-6
ハッシュ値および動作ログの送信
SD-7
ハッシュ値および動作ログの受信
SD-8
ハッシュ値および動作ログの蓄積
エンド
エンド
エンド

【図１２】


スタート
画像情報の読み取り
SE-1
画像識別情報の生成
SE-2
画像情報への画像識別情報の付加
SE-3
ハッシュ値の生成
SE-4
ハッシュ値の暗号化
SE-5
ハッシュ値および画像情報の送信
SE-6
エンド

フロントページの続き

(51)Int.Cl. FI
G09C 1/00 640B

審査官 児玉 崇晶

(56)参考文献 特開２００１－３５０７１７（ＪＰ，Ａ）
特開２００２－１６９９０９（ＪＰ，Ａ）
特開２００５－３０１１２２（ＪＰ，Ａ）
特開２００５－１９１７６５（ＪＰ，Ａ）
特開２００５－３３９３１２（ＪＰ，Ａ）
特開２００５－３５３０８７（ＪＰ，Ａ）
特開２００５－２３５１５９（ＪＰ，Ａ）
特開２００３－３３７９２３（ＪＰ，Ａ）
特開２００５－１４４９００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／０６
Ｇ０６Ｆ ２１／２４
Ｇ０９Ｃ １／００
Ｈ０４Ｎ １／００