(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2006-18761
(P2006-18761A)
(43)公開日　平成18年1月19日(2006.1.19)

(51)Int.Cl.			F I			テーマコード（参考）
G06T	1/00	(2006.01)	G06T	1/00	430J	5B047
H04N	1/00	(2006.01)	G06T	1/00	400G	5C062
H04N	1/10	(2006.01)	H04N	1/00	C	5C072
H04N	1/107	(2006.01)	H04N	1/10		

審査請求 有　請求項の数 7　ＯＬ　（全 14 頁）

(21)出願番号　特願2004-198343 (P2004-198343)
(22)出願日　平成16年7月5日 (2004.7.5)

(71)出願人　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　100081880
弁理士　渡部　敏彦
(72)発明者　本保　綱男
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

Ｆターム(参考)　5B047 AA01 AA25 BA02 BB02 BC05 BC09 BC11 BC16 BC23 CA23 CB22 DC06
5C062 AA05 AB06 AB07 AB17 AB29 AB42 AC21 AC22 AD06 AF12
5C072 AA01 BA02 BA04 DA02 EA05 LA02 RA16 UA02 UA06 UA11 UA13 VA10

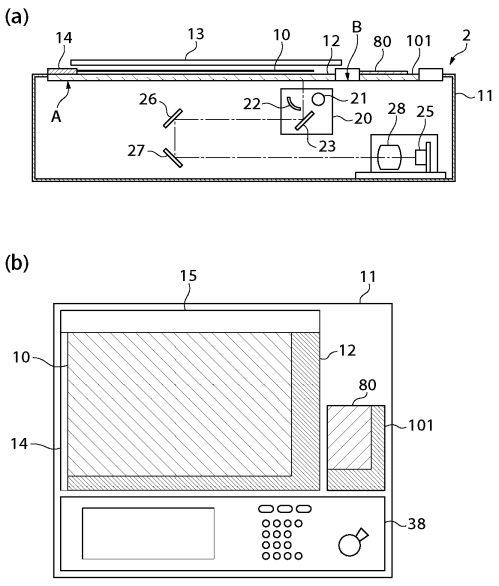
(54)【発明の名称】画像読取装置

(57)【要約】

【課題】　製造コストの増大を抑制しつつ精度の高い認証及び高い操作性を実現するセキュリティ機能を備える画像読取装置を提供する。

【解決手段】　画像読取装置１は、原稿１０を載置するプラテンガラス１２と、原稿１０の画像を読取る１次元のイメージセンサ２５と、該イメージセンサ２５により読取られたセキュリティ情報を予め記憶されたセキュリティ情報と照合するセキュリティデータ認証部４３とを備え、イメージセンサ２５は、認証カード８０のセキュリティ情報を読取る。

【選択図】　図２



【特許請求の範囲】
【請求項１】
原稿を載置する載置面と、該原稿の画像を読取るイメージセンサと、セキュリティ情報媒体から読取られたセキュリティ情報を予め記憶されたセキュリティ情報と照合する情報照合部とを備える画像読取装置において、
前記イメージセンサは、セキュリティ情報媒体のセキュリティ情報を読取ることを特徴とする画像読取装置。
【請求項２】
前記セキュリティ情報媒体を載置する他の載置面を有することを特徴とする請求項１記載の画像読取装置。
【請求項３】
前記載置面は、前記セキュリティ情報媒体を載置することを特徴とする請求項１記載の画像読取装置。
【請求項４】
前記セキュリティ情報は個人認証情報であることを特徴とする請求項１記載の画像読取装置。
【請求項５】
前記個人認証情報は指紋であることを特徴とする請求項４記載の画像読取装置。
【請求項６】
前記セキュリティ情報媒体は、個人を特定する情報が記載された印刷物であることを特徴とする請求項４記載の画像読取装置。
【請求項７】
所定のタイミングで読取られた前記載置面の画像において、所定の輝度レベルを超える輝度の画素の数に応じて所定のメッセージを表示する表示部を備えることを特徴とする請求項３記載の画像読取装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティ機能を備える画像読取装置に関する。
【背景技術】
【０００２】
ネットワーク社会の発展によって情報処理装置とネットワークとの融合が進展し、個人認証などのセキュリティ機能の必要性が増してきている。個人認証としては、鍵やＩＣ（集積回路）カードの他に、指紋などの生体情報による認証が注目されている。例えば、特許文献１には、指紋の読取方式としてプリズムなどの光学系を用いた読取方式が開示されており、特許文献２には、液晶表示装置のＴＦＴ（薄膜トランジスタ）素子に隣接してフォトダイオードを配置してＣＣＤ（電荷結合素子）のように画像を読出す技術が開示されている。また、特許文献３や特許文献４には、指紋識別の手法に関する技術が開示されている。さらに、特許文献５には、指紋認証結果に基づく情報処理装置の動作制御に関する技術が開示されている。
【特許文献１】特開平８－３１５１４３号公報
【特許文献２】特開平９－１８６３１２号公報
【特許文献３】特開平７－２２００７５号公報
【特許文献４】特開平１０－１５４２３１号公報
【特許文献５】特開平１０－６９３２４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、情報処理装置、特に、画像読取装置の分野においては、画像読取装置が有するセキュリティ機能の認証精度が低いことにより、該画像読取装置の操作が正当な権

限が与えられたユーザによって実行されたことを確認することができず、また、認証精度の高いセキュリティ機能を有するものであっても、認証を実行するための操作が煩雑であることにより操作性が低くなるという問題がある。加えて、画像読取装置が認証精度の高いセキュリティ機能を備えることにより、画像読取装置の製造コストが増大してしまうという問題がある。

【０００４】

本発明の目的は、製造コストの増大を抑制しつつ精度の高い認証及び高い操作性を実現するセキュリティ機能を備える画像読取装置を提供することにある。

【課題を解決するための手段】

【０００５】

上記目的を達成するために、請求項１記載の画像読取装置は、原稿を載置する載置面と、該原稿の画像を読取るイメージセンサと、セキュリティ情報媒体から読取られたセキュリティ情報を予め記憶されたセキュリティ情報と照合する情報照合部とを備える画像読取装置において、前記イメージセンサは、セキュリティ情報媒体のセキュリティ情報を読取ることを特徴とする。

【０００６】

請求項２記載の画像読取装置は、請求項１記載の画像読取装置において、前記セキュリティ情報媒体を載置する他の載置面を有することを特徴とする。

【０００７】

請求項３記載の画像読取装置は、請求項１記載の画像読取装置において、前記載置面は、前記セキュリティ情報媒体を載置することを特徴とする。

【０００８】

請求項４記載の画像読取装置は、請求項１記載の画像読取装置において、前記セキュリティ情報は個人認証情報であることを特徴とする。

【０００９】

請求項５記載の画像読取装置は、請求項４記載の画像読取装置において、前記個人認証情報は指紋であることを特徴とする。

【００１０】

請求項６記載の画像読取装置は、請求項４記載の画像読取装置において、前記セキュリティ情報媒体は、個人を特定する情報が記載された印刷物であることを特徴とする。

【００１１】

請求項７記載の画像読取装置は、請求項３記載の画像読取装置において、所定のタイミングで読取られた前記載置面の画像において、所定の輝度レベルを超える輝度の画素の数に応じて所定のメッセージを表示する表示部を備えることを特徴とする。

【発明の効果】

【００１２】

請求項１記載の画像読取装置によれば、原稿の画像を読取るイメージセンサがセキュリティ情報媒体のセキュリティ情報を読取るので、セキュリティ情報を読取るための新たなイメージセンサを設ける必要が無く且つ認証の実行が容易であり、もって製造コストの増大を抑制しつつ精度の高い認証及び高い操作性を実現することができる。

【００１３】

請求項２記載の画像読取装置によれば、セキュリティ情報媒体を載置する他の載置面を有するので、更に精度の高い認証を実現することができる。

【００１４】

請求項３記載の画像読取装置によれば、載置面はセキュリティ情報媒体を載置するので、セキュリティ情報媒体を載置する新たな載置面を設ける必要がなく、製造コストの増大を更に抑制できる。

【００１５】

請求項４記載の画像読取装置によれば、セキュリティ情報は個人認証情報であるので、更に精度の高い認証を実現することができる。

【００１６】
請求項５記載の画像読取装置によれば、個人認証情報は指紋であるので、認証の実行が更に容易であり、加えて、更に精度の高い認証を実現することができる。
【００１７】
請求項６記載の画像読取装置によれば、セキュリティ情報媒体は、個人を特定する情報が記載された印刷物であるので、更に精度の高い認証を実現することができる。
【００１８】
請求項７記載の画像読取装置によれば、所定のタイミングで読取られた載置面の画像において所定の輝度レベルを超える輝度の画素の数に応じて所定のメッセージが表示されるので、載置面が汚れていることをユーザに通知することができ、もって精度の高い認証を維持することができる。
【発明を実施するための最良の形態】
【００１９】
以下、本発明の実施の形態を図面を参照しながら詳述する。
【００２０】
先ず、本発明の第１の実施の形態について説明する。
【００２１】
図１は、本発明の第１の実施の形態に係る画像読取装置の構成を概略的に示す図である。
【００２２】
図１に示すように、画像読取装置１は、原稿の画像等を光学的に読取り、読取った原稿の画像等を画像データに変換する読取部２と、後述する画像出力装置６０及び通信制御装置６１に接続され、読取部２によって読取られた画像データを処理する信号処理部３と、読取部２の作動を制御する制御部４と、信号処理部３に接続され、読取部２で読取られた画像データの分析、保存等を行う記憶部５とを備える。画像出力装置６０及び通信制御装置６１は、画像読取装置１と共にファクシミリ・複写システムを構成する。
【００２３】
図２は、図１の読取部２の構成を示す図であり、（Ａ）は読取部２の断面図であり、（Ｂ）は、原稿押さえを除いた状態で読取部２を上面からみた平面図である。
【００２４】
図２（Ａ）において、読取部２は読取部本体（筐体）１１を有し、この読取部本体１１の上面には、原稿１０を載置するプラテンガラス（載置面）１２が設けられている。このプラテンガラス１２上には開閉自在な原稿押さえ１３が設けられている。また、プラテンガラス１２の副走査開始側の端部の上には、主走査方向に沿って副走査レジプレート１４が設けられている。プラテンガラス１２の副走査終了側の端部より副走査方向に関して後方に、後述する認証カード（セキュリティ情報媒体）８０等を載置するセキュリティ情報読取部（他の載置面）１０１が設けられている。これにより、更に精度の高い認証を実現することができる。
【００２５】
プラテンガラス１２の下方には、副走査方向に移動可能なキャリッジ２０が設けられている。このキャリッジ２０内には、原稿１０をライン状に照明するためのランプ２１と、このランプ２１から出射された光を原稿１０に照射するリフレクタ２２と、原稿１０からの反射光を反射する第１ミラー２３とが設けられている。また、読取部本体１１内の底部には画像を読取る１次元のイメージセンサ２５が設けられ、読取部本体１１内には第１ミラー２３からの光をイメージセンサ２５へ導く第２ミラー２６および第３ミラー２７が設けられている。また、イメージセンサ２５の光路に関する前方には、イメージセンサ２５上に画像を結像させるレンズ２８が設けられている。
【００２６】
キャリッジ２０は後述するモータ４０によって副走査方向に往復運動する。また、第２ミラー２６および第３ミラー２７は、図示しない駆動装置によって、キャリッジ２０の移

動に追従して同一方向に関し、キャリッジ２０の１／２の速度で移動されるようになっている。これにより、原稿面とイメージセンサ２５間の距離が変化することなく、原稿面を走査することができるようになっている。

【００２７】

尚、図中、「Ａ」は第一の読取り走査開始位置、「Ｂ」は第二の読取り走査開始位置を夫々示し、原稿１０の画像を読取る場合のキャリッジ２０の走査開始位置は第一の読取り走査開始位置であり、認証カード８０のセキュリティ情報を読取る場合のキャリッジ２０の走査開始位置は第二の読取り走査開始位置である。また、画像読取装置１の電源投入直後や、ジョブの終了後には、キャリッジ２０は第一の読取り走査開始位置に位置する。

【００２８】

原稿１０は、副走査レジプレート１４及びプラテンガラス１２上に設けられた主走査レジプレート１５に沿って、プラテンガラス１２上に載置され、認証カード８０はセキュリティ情報読取部１０１上に載置される（図２（Ｂ））。イメージセンサ２５は、プラテンガラス１２上に載置された原稿１０の画像を読取り、更に、セキュリティ情報読取部１０１上に載置された認証カード８０のセキュリティ情報を読取る。これにより、セキュリティ情報を読取るための新たなイメージセンサを設ける必要が無く且つ認証の実行が容易となる。

【００２９】

図３は、画像読取装置１の信号処理部３および制御部４を説明するのに用いられるブロック図である。

【００３０】

図３に示すように、信号処理部３は、イメージセンサ２５の出力信号をディジタルの画像データに変換するアナログ－ディジタル変換部（以下、「Ａ／Ｄ変換部」と記す）３１と、該Ａ／Ｄ変換部３１の出力画像データに対してシェーディング補正を行うシェーディング補正部３２と、該シェーディング補正部３２の出力画像データに対して画像処理を施す画像処理部３３と、画像読取装置１全体を制御する中央処理部（以下、「ＣＰＵ」と記す）３４と、これらイメージセンサ２５、Ａ／Ｄ変換部３１、シェーディング補正部３２、画像処理部３３およびＣＰＵ３４に対してタイミング信号を供給するタイミング信号発生部３５とを備える。ＣＰＵ３４は、プログラム等を格納したリード・オンリー・メモリ（以下、「ＲＯＭ」と記す）と、ワーキングエリアとなるランダム・アクセス・メモリ（以下、「ＲＡＭ」と記す）とを有する。記憶部５はセキュリティ情報読取部１０１で読取られたセキュリティ情報の検出、保存等を行う。

【００３１】

画像読取装置１の制御部４は、キー入力によって画像読取装置１を操作する操作部３８と、画像読取装置１のステータス情報や、操作部３８により入力されたデータ等を表示する表示部３７と、表示部３７を制御する表示制御部３６と、前記副走査方向に移動可能なキャリッジ２０を駆動するモータ４０と、モータ４０の作動を制御するモータ制御部３９からなる。

【００３２】

また、画像処理部３３の出力画像データは、画像読取装置１と共にファクシミリ・複写システムを構成する通信制御装置６１及び画像出力装置６０に送られ、通信制御装置６１による画像送信、画像出力装置６０による画像出力が可能になっている。また、通信制御装置６１の受信画像は画像出力装置６０によって出力される。ＣＰＵ３４は図示しないバスを介して通信制御装置６１と画像出力装置６０に接続されている。

【００３３】

図４は、図１における記憶部５の構成を説明するブロック図である。

【００３４】

図４において、記憶部５は、イメージセンサ２５により読取られたセキュリティ情報を予め記憶されたセキュリティ情報と照合するセキュリティデータ認証部（情報照合部）４３と、プログラム／ワークメモリ４４とを備える。セキュリティデータ認証部４３は、セ

キュリティ情報の特徴を抽出する特徴抽出部４５と、抽出された特徴を照合する照合部４６とを有する。プログラム／ワークメモリ４４は、セキュリティ情報を保存し／又は読出す保存・読出部４７およびセキュリティ情報を認証するために実行されるアプリケーションプログラムを格納するプログラム格納部５０で構成される。保存・読出部４７は、ユーザ登録データを読出すデータ読出部４８と、読出されたユーザ登録データを格納するデータ格納部４９とを有する。

【００３５】

図５は、セキュリティ情報が記載された認証カードの一例を示す図である。

【００３６】

図５に示すように、認証カード８０には個人を特定し得る顔写真や氏名等のＩＤ情報（個人認証情報）が記載されており、加えて、該ＩＤ情報が所定の方法でバーコード８１に変換し併記されている。これにより、更に精度の高い認証を実現することができる。

【００３７】

図６は、図２の読取部２を用いてセキュリティ情報を登録する方法を説明するフローチャートである。

【００３８】

図６において、ユーザは、操作部３８上に設けられた図示しないボタン等の操作により、ユーザによるセキュリティ情報の登録が可能となるユーザ登録モード設定を行い（ステップＳ６１）、セキュリティ情報読取部１０１に認証カード８０を載置する（ステップＳ６２）。

【００３９】

ユーザにより操作部３８上の図示しない読取ボタンが押下されると（ステップＳ６３）、キャリッジ２０は第二の走査開始位置に移動する（ステップＳ６４）。その後、ランプ２１を点灯させてキャリッジ２０を走査することにより、セキュリティ情報読取部１０１に載置された認証カード８０を読取る（ステップＳ６５）。

【００４０】

ステップＳ６５において読取られた認証カードデータは、画像処理部３３を介して記憶部５内の特徴抽出部４５に送信され、該特徴抽出部４５でバーコード８１が抽出されて所定の手段でユーザデータに変換される（ステップＳ６６）。

【００４１】

次に、データ格納部４９内に予め登録されているユーザ登録データをデータ読出部４８に読出し（ステップＳ６７）、読み出されたユーザ登録データ内に特徴抽出部４５で変換されたユーザデータと一致するものがあるか否かを判別し（ステップＳ６８）、ユーザデータと一致するものがない場合は、データ格納部５０にユーザデータを格納すると共に表示部３７に「新規登録」のメッセージを表示して（ステップＳ６９）、本処理を終了する。

【００４２】

ユーザデータと一致するものがあった場合は（ステップＳ６８でＹＥＳ）、表示部３７に「登録済み」のメッセージを表示して（ステップＳ７０）、本処理を終了する。

【００４３】

図７は、画像読取装置１にて画像を読取り、画像データを画像出力装置６０に送信する方法を説明するフローチャートである。

【００４４】

図７において、ユーザは原稿１０をプラテンガラス１２に載置し、操作部３８上の図示しない読取ボタンを押下する（ステップＳ７１）。第一の走査開始位置に位置するキャリッジ２０はランプ２１を点灯し（ステップＳ７２）、副走査レジプレート１４とプラテンガラス１２との接触面に存在する図示しない標準白色板を読取り、シェーディングデータを生成し、更に、キャリッジ２０を副走査方向に移動させながら原稿１０の画像を読取る（ステップＳ７３）。読取った原稿１０の画像データは、図３に示すように、イメージセンサ２５、A/D変換部３１、及びシェーディング補正部３２を介して画像形成装置３３に

送信され、該画像処理部３３にて所定の画像処理が施されて、画像処理部３３内の図示しないワークメモリに書き込まれる。

【００４５】

原稿１０の画像を読取った後、キャリッジ２０はランプ２１を消し、第二の走査開始位置に移動する（ステップＳ７４）。ユーザは、セキュリティ情報読取り部１０１に認証カード８０を載置し、操作部３８内の図示しない読取ボタンを押下する（ステップＳ７５）。第二の走査開始位置にあるキャリッジ２０はランプ２１を点灯させ、副走査方向に移動しながら認証カード８０のＩＤ情報等を読取る（ステップＳ７６）。認証カード８０のＩＤ情報を読取った後、キャリッジ２０はランプ２１を消し、第一の走査開始位置へ移動する。読取られた認証カードデータは、画像処理部３３で所定の画像処理が施され、記憶部５へ送信される。さらに、該送信された認証カードデータは記憶部５内の特徴抽出部４５でバーコード８１が抽出されて所定の手段でユーザデータに変換される（ステップＳ７７）。

【００４６】

次に、データ読出部４８にて、データ格納部４９内に予め登録されているユーザ登録データを読出し（ステップＳ７８）、読出されたユーザ登録データ内に、特徴抽出部４５で変換されたユーザデータと一致するものがあるか否かを判別し（ステップＳ７９）、ユーザデータと一致するものがある場合は、画像処理部３３内のワークメモリに格納されている画像データを画像出力装置６０へ送信し、本処理を終了する（ステップＳ８０）。

【００４７】

ユーザデータと一致するものがない場合は（ステップＳ７９でＮＯ）、ユーザは画像読取装置１を使用する権限がないと判断され、表示部３７にその旨のメッセージを表示すると共に（ステップＳ８１）、画像処理部３３内の図示しないワークメモリに格納されている画像データを消去して（ステップＳ８２）、本処理を終了する。

【００４８】

上述したように、本実施の形態によれば、イメージセンサ２５は原稿１０の画像だけでなく認証カード８０のセキュリティ情報も読取るので、セキュリティ情報を読取るための新たなイメージセンサを設ける必要が無く且つ認証の実行が容易であり、もって製造コストの増大を抑制しつつ精度の高い認証及び高い操作性を実現することができる。

【００４９】

尚、本実施の形態では、先に原稿１０の画像を読取り、次に認証カード８０のＩＤ情報等を読取ったが、この順番が入れ替わっても同様の効果が得られることは言うまでもない。

【００５０】

また、本実施の形態では、セキュリティ情報媒体として認証カード８０のような、個人情報が印刷されている媒体を使用したが、より精度良く個人を特定できる指紋を検出しても同様の効果を奏することができる。この場合、セキュリティ情報読取部１０１にユーザの手を置くことにより指紋を読取らせても良いし、より指紋の検出を容易にするべく、例えば、図８に示すように、セキュリティ情報読取部１０１の代わりに、ユーザの指紋を読取る指紋検出エリア７１～７５を有するセキュリティ情報読取部７０が設けられてもよい。これにより、認証の実行が容易となり、加えて更に精度の高い認証を実現することができる。

【００５１】

セキュリティ情報読取部７０は、指紋検出エリア７１～７５以外はマスクされており、画像が読取れないようになっている。また、ユーザは、指紋検出エリア７１に所定の指を置いて当該指の指紋のみを読取らせても良いし、指紋検出エリア７１～７５全てを使用してもよい。指紋を用いたユーザデータの登録及び画像読取装置１の動作に関しては本実施の形態と同様である。

【００５２】

次に、本発明の第２の実施の形態について説明する。

【００５３】
図９は、本発明の第２の実施の形態に係る画像読取装置における読取部の構成を示す図である。尚、図９の読取部６は、その構成が図２の読取部２と基本的に同じであり、読取部２からセキュリティ情報読取部１０１が削除されている以外は同様であるので、異なる部分のみを説明し、同様の部分の説明を省略する。
【００５４】
図９に示すように、読取部６は読取部本体（筐体）１１１を有し、この読取部本体１１の上面には、原稿１０を載置すると共に認証カード８０を載置するプラテンガラス１１２が設けられている。これにより、認証カード８０を載置する新たな載置面を設ける必要がなく、製造コストの増大を更に抑制できる。
【００５５】
図１０は、図９の読取部６を用いてセキュリティ情報を登録する方法を説明するフローチャートである。
【００５６】
図１０において、ユーザは、操作部３８上に設けられた図示しないボタン等の操作により、ユーザによるセキュリティ情報の登録が可能となるユーザ登録モード設定を行い（ステップＳ１０１）、プラテンガラス１１２上の所定位置に認証カード８０を載置する（ステップＳ１０２）。
【００５７】
ユーザにより、操作部３８上の図示しない読取ボタンが押下されると（ステップＳ１０３）、キャリッジ２０はランプ２１を点灯する。さらに、キャリッジ２０を副走査方向に移動させることにより、プラテンガラス１１２上に載置された認証カード８０を読取る（ステップＳ１０４）。
【００５８】
ステップＳ１０４において読取られた認証カードデータは、画像処理部３３を介して、記憶部５内の特徴抽出部４５に送信され、該特徴抽出部４５でバーコード８１が抽出されて所定の手段でユーザデータに変換される（ステップＳ１０５）。
【００５９】
次に、データ格納部４９内に予め登録されているユーザ登録データを読出し（ステップＳ１０６）、読み出されたユーザ登録データ内に特徴抽出部４５で変換されたユーザデータと一致するものがあるか否かを判別し（ステップＳ１０７）、ユーザデータと一致するものがない場合は、データ格納部５０にユーザデータを格納すると共に表示部３７に「新規登録」のメッセージを表示し（ステップＳ１０８）、本処理を終了する。
【００６０】
ユーザデータと一致するものがあった場合は（ステップＳ１０７でＹＥＳ）、表示部３７に「登録済み」のメッセージを表示して（ステップＳ１０９）、本処理を終了する。
【００６１】
図１１は、図９の読取部６で画像を読取り、読取られた画像データを画像出力装置６０に送信する方法を説明するフローチャートである。
【００６２】
図１１において、ユーザは原稿１０をプラテンガラス１１２に載置し、操作部３８上の図示しない読取ボタンを押下する（ステップＳ１１１）。走査開始位置としての副走査レジプレート１４直下に位置するキャリッジ２０はランプ２１を点灯し（ステップＳ１１２）、副走査レジプレート１４のプラテンガラス１１２との接触面に存在する図示しない標準白色板を読取り、シェーディングデータを生成し、更に、キャリッジ２０を副走査方向に移動させながら原稿１０の画像を読取る（ステップＳ１１３）。読取った原稿１０の画像データは、図３に示すように、イメージセンサ１２５、A/D変換部３１、シェーディング補正部３２を介して画像処理部３３に送信され、画像処理部３３にて所定の画像処理が施されて、画像処理部３３内の図示しないワークメモリに書き込まれる。
【００６３】

原稿１０の画像を読取った後、キャリッジ２０はランプ２１を消し、走査開始位置に移動する（ステップＳ１１４）。ユーザは、原稿１０を取り除いた後、認証カード８０をプラテンガラス１１２上の所定位置に載置し、操作部３８内の図示しない読取ボタンを押下する（ステップＳ１１５）。走査開始位置にあるキャリッジ２０はランプ２１を点灯し、副走査方向に移動しながら認証カード８０のＩＤ情報等を読取る（ステップＳ１１６）。認証カード８０のＩＤ情報を読取った後、キャリッジ２０はランプ２１を消し、走査開始位置へ移動する。読取られた認証カードデータは、画像処理部３３で所定の画像処理が施され、記憶部５へ送られる。記憶部５内の特徴抽出部４５でバーコード８１が抽出されて、所定の手段でユーザデータに変換される（ステップＳ１１７）。

【００６４】

データ読出部４８にて、データ格納部４９内に予め登録されているユーザ登録データを読出し（ステップＳ１１８）、読出されたユーザ登録データ内に、特徴抽出部４５で変換されたユーザデータと一致するものがあるか否かを判別し（ステップＳ１１９）、ユーザデータと一致するものがある場合は、画像処理部３３内のワークメモリに格納されている画像データを画像出力装置６０へ送信し、本処理を終了する（ステップＳ１２０）。

【００６５】

ユーザデータと一致するものがない場合は（ステップＳ１１９でＮＯ）、ユーザは画像読取装置１を使用する権限がないと判断され、表示部３７にメッセージを表示すると共に（ステップＳ１２１）、画像処理部３３内のワークメモリに格納されている画像データを消去し（ステップＳ１２２）、本処理を終了する。

【００６６】

尚、本実施の形態では、先に原稿１０の画像を読取り、次に認証カード８０のＩＤ情報等を読取ったが、この順番が入れ替わっても同様の効果が得られることは言うまでもない。

【００６７】

また、セキュリティ情報が認証カード８０のＩＤ情報等ではなく、ユーザの指紋であっても図１０及び図１１の処理と同様の手順で実施可能である。この場合、セキュリティ情報を読取るために、原稿読取領域としてのプラテンガラス１１２に指等が載せられるので、プラテンガラス１１２に汚れがつき易く、画像の読取りに影響する可能性がある。そのため、所定のタイミングで、プラテンガラス１１２自身を読取ることによりプラテンガラス１１２の汚れを検知する機能を有することが好ましい。

【００６８】

以下、プラテンガラス１１２の汚れ検知機能について説明する。

【００６９】

図１２は、図４における記憶部５の変形例を説明するブロック図である。

【００７０】

図１２において、記憶部１４２は、プラテンガラス１１２で読取られたセキュリティ情報を認証するセキュリティデータ認証部１４３と、プログラム／ワークメモリ１４４と、プラテンガラス１１２を読取った画像から汚れ具合を検出する原稿領域汚れ検出部１５１とを備える。セキュリティデータ認証部１４３は、セキュリティ情報の特徴を抽出する特徴抽出部１４５と、抽出された特徴を照合する照合部１４６とを有する。プログラム／ワークメモリ１４４は、セキュリティ情報を保存及び／又は読出す保存・読出部１４７およびセキュリティ情報を認証するために実行されるアプリケーションプログラムを格納するプログラム格納部１５０で構成される。保存・読出部１４７は、ユーザ登録データを読出すデータ読出部１４８と、読出されたユーザ登録データを格納するデータ格納部１４９とを有する。

【００７１】

原稿領域汚れ検出部１５１は、所定のタイミングでプラテンガラス１１２から読取られた画像の画素のうち、所定の輝度レベル以上の輝度を有する画素の数を汚れデータとして抽出する汚れデータ抽出部１５２と、初期状態におけるプラテンガラス１１２から読取ら

れた画像の画素のうち、所定の輝度レベル以上の輝度を有する画素の数を初期汚れデータとして格納する汚れデータ格納部１５４と、初期汚れデータを汚れデータ格納部１５４から読出し、初期汚れデータを汚れデータと比較する汚れデータ比較部１５３とを有する。

【００７２】

図１３は、プラテンガラス１１２の汚れを検知する方法を説明するフローチャートである。ここでは、画像読取装置１の電源投入時にプラテンガラス１１２の汚れ検知を行う場合を説明する。

【００７３】

図１３において、画像読取装置１の電源が投入されると（ステップＳ１３１）、キャリッジ２０が走査開始位置に移動し、ランプ２１を点灯し、図示しない標準白色板を読取ることによりシェーディングデータを生成するなどの初期設定を行う（ステップＳ１３２）。次に、ランプ２１を点灯させながらキャリッジ２０を副走査方向に移動し、プラテンガラス１１２を読取る（ステップＳ１３３）。読取られた画像の画素のうち、所定の輝度レベル以上の輝度を有する画素の数を汚れデータとして抽出する（ステップＳ１３４）。さらに、汚れデータ格納部１５４に格納されている初期汚れデータを読出し（ステップＳ１３５）、汚れデータ抽出部１５２にて抽出された汚れデータが、読出された初期汚れデータ以上であるか否かを判別する（ステップＳ１３６）。

【００７４】

汚れデータが初期汚れデータ以下である場合は、本処理を終了し、汚れデータが初期汚れデータ以上である場合は、表示部３７に「プラテンガラスを清掃してください」のメッセージを表示して（ステップＳ１３７）、本処理を終了する。

【００７５】

これにより、プラテンガラス１１２が汚れていることをユーザに通知することができ、もって更に精度の高い認証を維持することができる。

【図面の簡単な説明】

【００７６】

【図１】本発明の第１の実施の形態に係る画像読取装置の構成を概略的に示す図である。

【図２】図１の読取部の構成を示す図であり、（Ａ）は読取部の断面図であり、（Ｂ）は、原稿押さえを除いた状態で読取部を上面からみた平面図である。

【図３】画像読取装置の信号処理部および制御部を説明するのに用いられるブロック図である。

【図４】図４は、図１における記憶部の構成を説明するブロック図である。

【図５】セキュリティ情報が記載された認証カードの一例を示す図である。

【図６】図２の読取部を用いてセキュリティ情報を登録する方法を説明するフローチャートである。

【図７】画像読取装置にて画像を読取り、画像データを画像出力装置に送信する方法を説明するフローチャートである。

【図８】セキュリティ情報読取部の変形例を示す図である。

【図９】本発明の第２の実施の形態に係る画像読取装置における読取部の構成を示す図である。

【図１０】図９の読取部を用いてセキュリティ情報を登録する方法を説明するフローチャートである。

【図１１】図９の読取部で画像を読取り、読取られた画像データを画像出力装置に送信する方法を説明するフローチャートである。

【図１２】図４における記憶部の変形例を説明するブロック図である。

【図１３】プラテンガラスの汚れを検知する方法を説明するフローチャートである。

【符号の説明】

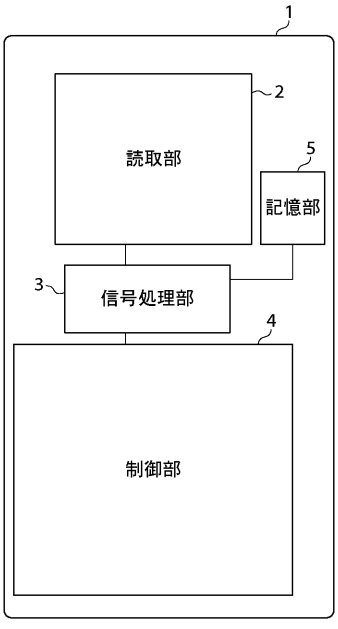
【００７７】

１　画像読取装置

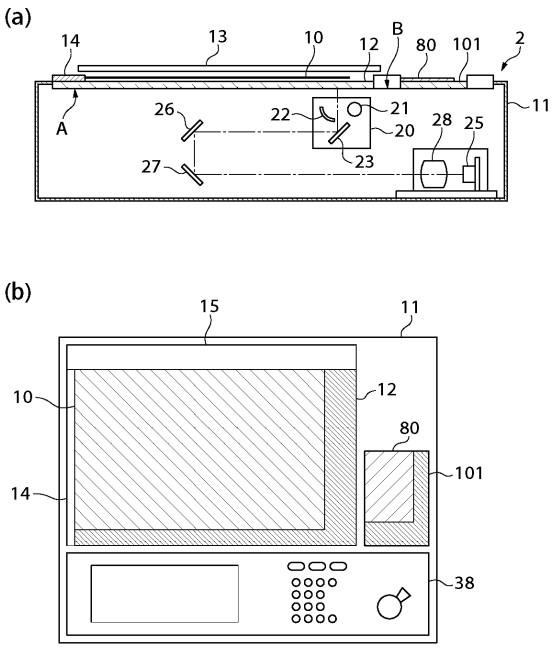
２　読取部

３　信号処理
４　制御部
５　記憶部
１２　プラテンガラス
２５　イメージセンサ
２８　レンズ
４３　セキュリティデータ認証部

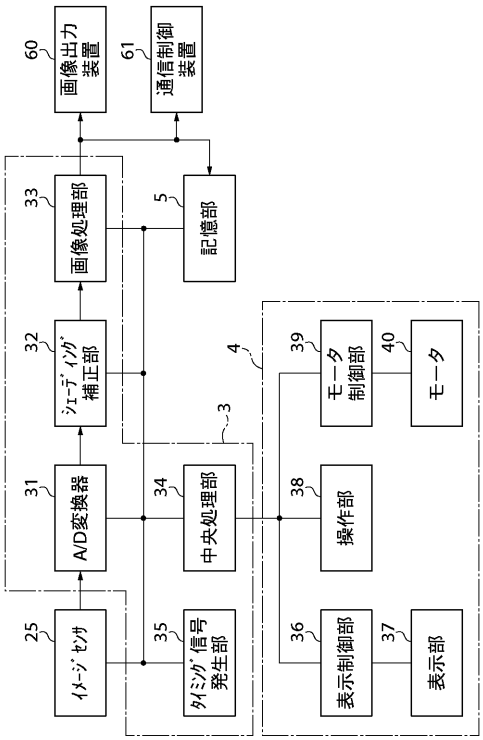
【図１】



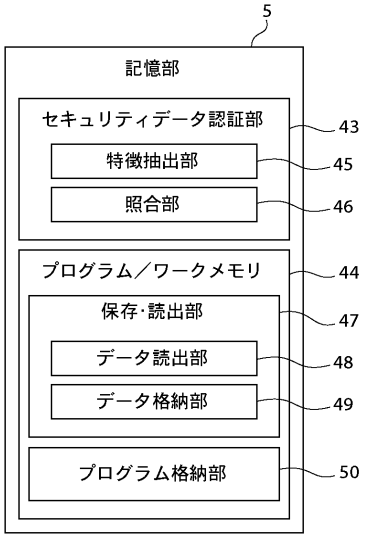
【図２】



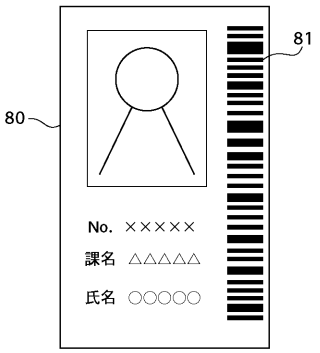
【図３】


60
画像出力装置
61
通信制御装置
33
画像処理部
5
記憶部
32
ｼｪｰﾃﾞｨﾝｸﾞ補正部
4
39
モータ制御部
40
モータ
3
31
A/D変換器
34
中央処理部
38
操作部
25
ｲﾒｰｼﾞｾﾝｻ
35
ﾀｲﾐﾝｸﾞ信号発生部
36
表示制御部
37
表示部

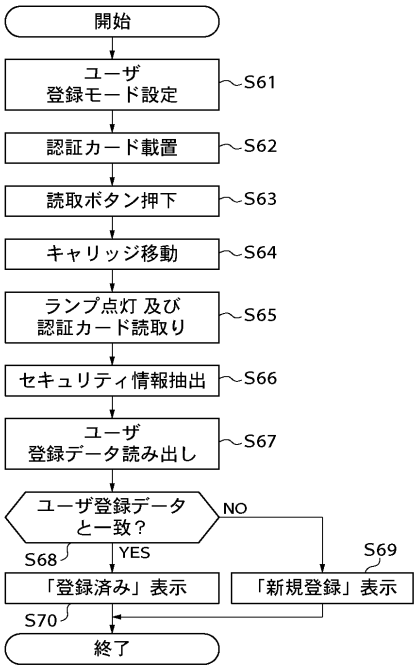
【図４】


5
記憶部
セキュリティデータ認証部
43
特徴抽出部
45
照合部
46
プログラム／ワークメモリ
44
保存･読出部
47
データ読出部
48
データ格納部
49
プログラム格納部
50

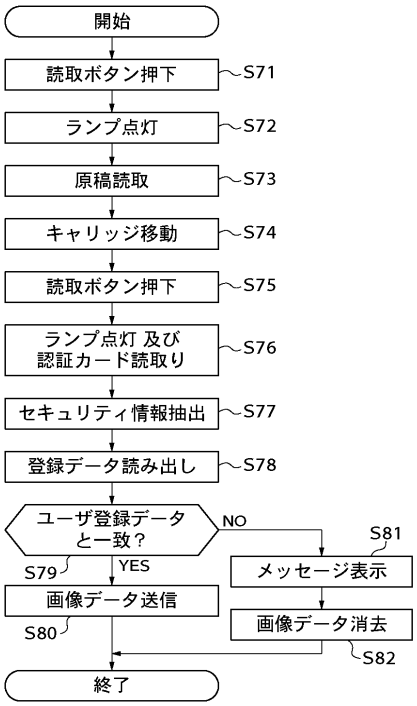
【図５】


81
80
No. ×××××
課名 △△△△△
氏名 ○○○○○

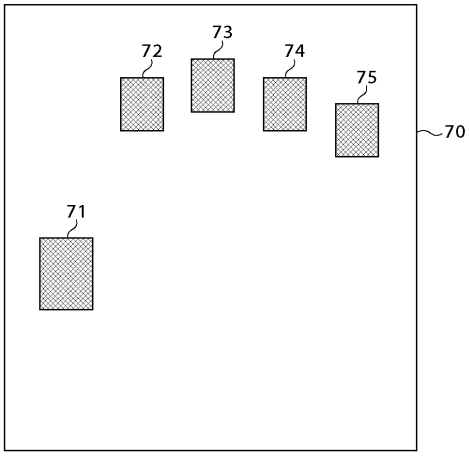
【図６】


開始
ユーザ登録モード設定
S61
認証カード載置
S62
読取ボタン押下
S63
キャリッジ移動
S64
ランプ点灯 及び認証カード読取り
S65
セキュリティ情報抽出
S66
ユーザ登録データ読み出し
S67
ユーザ登録データと一致？
NO
YES
S68
「登録済み」表示
S69
「新規登録」表示
S70
終了

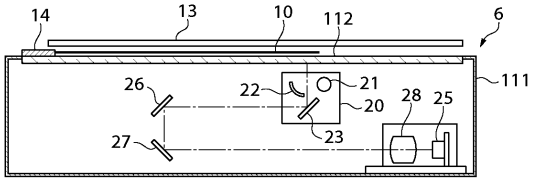
【図７】


開始
読取ボタン押下
S71
ランプ点灯
S72
原稿読取
S73
キャリッジ移動
S74
読取ボタン押下
S75
ランプ点灯 及び
認証カード読取り
S76
セキュリティ情報抽出
S77
登録データ読み出し
S78
ユーザ登録データ
と一致？
NO
S81
メッセージ表示
S79
YES
画像データ送信
画像データ消去
S80
S82
終了

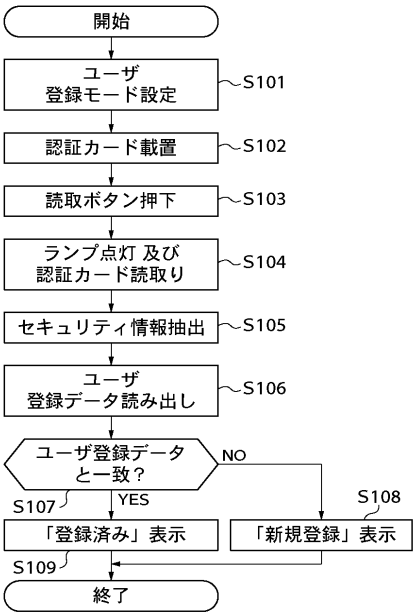
【図８】


72
73
74
75
70
71

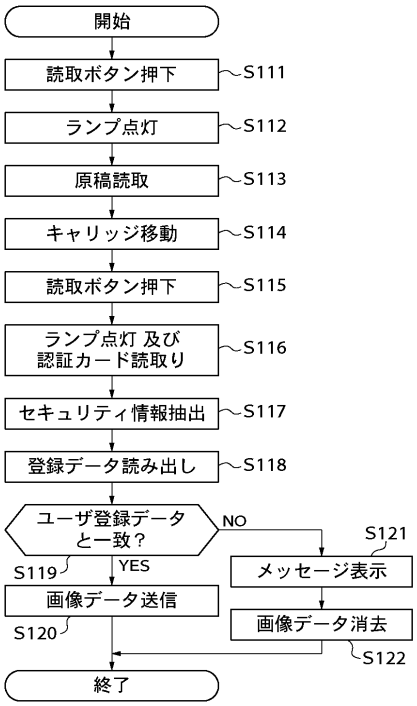
【図９】


14
13
10
112
6
111
26
22
21
20
28
25
27
23

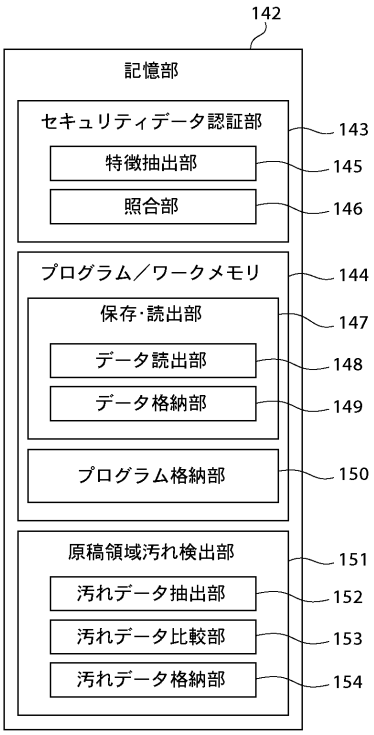
【図１０】


開始
ユーザ
登録モード設定
S101
認証カード載置
S102
読取ボタン押下
S103
ランプ点灯 及び
認証カード読取り
S104
セキュリティ情報抽出
S105
ユーザ
登録データ読み出し
S106
ユーザ登録データ
と一致？
NO
S107
YES
S108
「登録済み」表示
「新規登録」表示
S109
終了

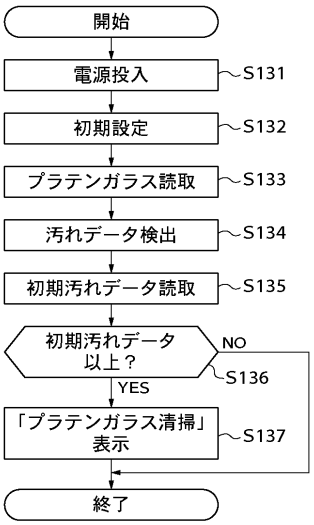
【図１１】


開始
読取ボタン押下
S111
ランプ点灯
S112
原稿読取
S113
キャリッジ移動
S114
読取ボタン押下
S115
ランプ点灯 及び
認証カード読取り
S116
セキュリティ情報抽出
S117
登録データ読み出し
S118
ユーザ登録データ
と一致？
NO
S121
メッセージ表示
S119
YES
画像データ送信
S120
画像データ消去
S122
終了

【図１２】


142
記憶部
セキュリティデータ認証部
143
特徴抽出部
145
照合部
146
プログラム／ワークメモリ
144
保存･読出部
147
データ読出部
148
データ格納部
149
プログラム格納部
150
原稿領域汚れ検出部
151
汚れデータ抽出部
152
汚れデータ比較部
153
汚れデータ格納部
154

【図１３】


開始
電源投入
S131
初期設定
S132
プラテンガラス読取
S133
汚れデータ検出
S134
初期汚れデータ読取
S135
初期汚れデータ
以上？
NO
S136
YES
「プラテンガラス清掃」
表示
S137
終了