(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2010-178047
(P2010-178047A)
(43)公開日　平成22年8月12日(2010.8.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 1/00	(2006.01)	H04N	1/00	C	5B285
G06F 21/20	(2006.01)	G06F	15/00	330D	5C062
G06F 1/00	(2006.01)	G06F	1/00	370E	

審査請求 有　請求項の数 10　ＯＬ　（全 25 頁）

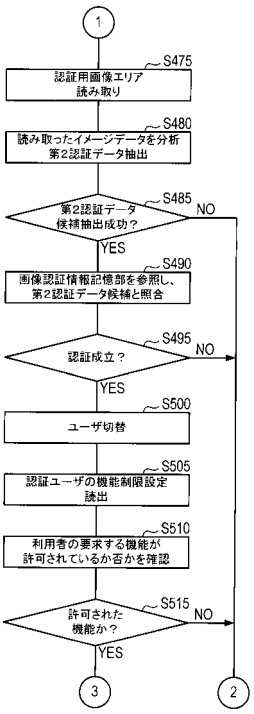
(21)出願番号　特願2009-18215(P2009-18215)
(22)出願日　平成21年1月29日(2009.1.29)

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110000578
名古屋国際特許業務法人
(72)発明者　白井　孝明
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内

Ｆターム(参考)　5B285 AA01 BA04 CB41 CB83
5C062 AA02 AA05 AA30 AA35 AB02
AB17 AC02 AC07 AC09 AC22
AC64 AF12

(54)【発明の名称】画像処理装置およびプログラム

(57)【要約】
【課題】入力情報を利用者が手作業で入力しなくても、所定の機能の利用が許可された利用者か否かを判別するための認証処理を実施可能な画像処理装置の提供。
【解決手段】ＭＦＰは、認証用画像エリアを読み取り（Ｓ４７５）、読み取ったイメージデータを分析して、第２認証データを抽出する（Ｓ４８０）。抽出に成功した場合（Ｓ４８５：ＹＥＳ）、抽出した第２認証データの候補と画像認証情報記憶部に記憶された第２認証データとの照合を行う（Ｓ４９０）。照合の結果、認証が成立したと判断された場合（Ｓ４９５：ＹＥＳ）、認証ユーザに対する機能制限設定を読み出す（Ｓ５０５）。そして、利用しようとしている機能について、ログイン中の利用者による利用が許可された機能であると判断された場合（Ｓ５１５：ＹＥＳ）、利用者の要求する機能を作動させる。
【選択図】図９



【特許請求の範囲】
【請求項１】
読取対象物から画像を読み取り可能な読取手段と、
前記読取対象物上での範囲があらかじめ設定された第１領域にある処理対象画像を、前記読取手段で読み取ることにより、前記処理対象画像を取得する処理対象画像取得手段と、
前記読取対象物上での範囲があらかじめ設定され、その範囲が前記第１領域とは異なる範囲とされた第２領域にある認証用画像を、前記読取手段で読み取ることにより、前記認証用画像を取得する認証用画像取得手段と、
前記認証用画像取得手段によって取得された前記認証用画像が、あらかじめ定められた認証条件を満たす画像であるか否かを判断する判断手段と、
前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、前記処理対象画像取得手段によって取得された前記処理対象画像が処理対象とされる所定の機能について、当該機能を作動させる制御を実行する機能制御手段と
を備えたことを特徴とする画像処理装置。
【請求項２】
前記読取対象物上の前記第２領域となる範囲を、利用者が指定した範囲に変更可能な範囲変更手段
を備えることを特徴とする請求項１に記載の画像処理装置。
【請求項３】
前記処理対象画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側にある前記第１領域から前記処理対象画像を取得し、
前記認証用画像取得手段は、前記読取対象物が有する表裏両面のうち、裏面側にある前記第２領域から前記認証用画像を取得する
ことを特徴とする請求項１または請求項２に記載の画像処理装置。
【請求項４】
前記処理対象画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側にある前記第１領域から前記処理対象画像を取得し、
前記認証用画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側にあって前記第１領域とは異なる範囲にある前記第２領域から前記認証用画像を取得する
ことを特徴とする請求項１または請求項２に記載の画像処理装置。
【請求項５】
前記処理対象画像取得手段は、前記読取対象物が有する表裏両面のうち、両方の面にある前記第１領域から前記処理対象画像を取得し、
前記認証用画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側または裏面側にあって前記第１領域とは異なる範囲にある前記第２領域から前記認証用画像を取得する
ことを特徴とする請求項１または請求項２に記載の画像処理装置。
【請求項６】
前記認証用画像取得手段は、前記処理対象画像取得手段による前記処理対象画像の取得を開始する前に、前記第２領域から前記認証用画像の取得を完了し、前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、前記処理対象画像取得手段は、前記処理対象画像の取得を開始する
ことを特徴とする請求項１～請求項５のいずれかに記載の画像処理装置。
【請求項７】
前記処理対象画像が処理対象とされる所定の機能を、複数の利用者それぞれが利用可能か否かの設定を、各利用者に対応付けて記憶する設定記憶手段と、
前記認証用画像が前記複数の利用者のいずれに対応する画像であるのかを特定して、特定された利用者に対応付けて前記所定の機能を利用可能である旨の設定が前記設定記憶手段に記憶されていれば、前記特定された利用者は、前記所定の機能を利用可能と判定する

利用者別制限判定手段と
を備え、
前記機能制御手段は、前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、さらに、前記利用者別制限判定手段により、前記特定された利用者が前記所定の機能を利用可能と判定されたら、前記所定の機能を作動させる制御を実行する
ことを特徴とする請求項１～請求項６のいずれかに記載の画像処理装置。
【請求項８】
前記読取手段は、前記読取対象物が有する表裏両面の内、いずれか一方の面から画像を読み取る第１イメージセンサと、他方の面から画像を読み取る第２イメージセンサとを備え、前記第１イメージセンサおよび第２イメージセンサが並行して作動可能に構成されている
ことを特徴とする請求項１～請求項７のいずれかに記載の画像処理装置。
【請求項９】
前記第２イメージセンサは、前記第１イメージセンサが前記一方の面から前記処理対象画像の読み取りを開始する前に、前記他方の面から前記認証用画像の読み取りを完了可能な位置にあり、
前記認証用画像取得手段は、前記他方の面にある認証用画像を、前記第２イメージセンサで読み取ることにより、前記認証用画像を取得する
ことを特徴とする請求項８に記載の画像処理装置。
【請求項１０】
読取対象物から画像を読み取り可能な読取手段を備えた画像処理装置に内蔵された制御部を、
前記読取対象物上での範囲があらかじめ設定された第１領域にある処理対象画像を、前記読取手段で読み取ることにより、前記処理対象画像を取得する処理対象画像取得手段と、
前記読取対象物上での範囲があらかじめ設定され、その範囲が前記第１領域とは異なる範囲とされた第２領域にある認証用画像を、前記読取手段で読み取ることにより、前記認証用画像を取得する認証用画像取得手段と、
前記認証用画像取得手段によって取得された前記認証用画像が、あらかじめ定められた認証条件を満たす画像であるか否かを判断する判断手段と、
前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、前記処理対象画像取得手段によって取得された前記処理対象画像が処理対象とされる所定の機能について、当該機能を作動させる制御を実行する機能制御手段
として機能させることを特徴とする画像処理装置用のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像処理装置が備える各種機能について、その利用を許可するか否か等を利用者に対応付けて設定可能な画像処理装置と、そのような画像処理装置用のプログラムに関する。
【背景技術】
【０００２】
従来、プリント機能、スキャン機能、コピー機能、ファクシミリ送受信機能、あるいはデータ転送機能といった複数種の機能を有する画像処理装置が知られている。また、この種の画像処理装置において採用される技術として、利用者の認証を行って、認証の成立した利用者だけが所定の機能を利用できるようにする仕組みも、既に提案されている（例えば、特許文献１参照。）。
【０００３】
このような認証機能を持つ画像処理装置の場合、利用者が操作パネルからユーザアカウ

ント名やパスワードをキー入力すると、それらの入力情報に基づく認証処理が行われる。そして、認証が成立した場合にだけ、利用者は所定の機能を利用することができる状態になる。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００５－６５０５３号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかしながら、上記のような従来技術の場合、認証機能を利用する際に、利用者は操作パネル等からユーザアカウント名やパスワードを手作業で入力しなければならないため、その入力操作が煩わしいという問題があった。特に、この種の画像処理装置では、キーの総数が比較的少ない操作パネルを採用している場合も多いため、そのような場合、複雑なユーザアカウント名やパスワードを入力する際には相応の手間がかかるという問題があり、それ故、入力ミスが発生しやすいといった問題もあった。

【０００６】

本発明は、上記問題を解決するためになされたものであり、その目的は、ユーザアカウント名やパスワードのような入力情報を利用者が手作業で入力しなくても、所定の機能の利用が許可された利用者か否かを判別するための認証処理を実施可能な画像処理装置と、そのような画像処理装置用のプログラムを提供することにある。

【課題を解決するための手段】

【０００７】

以下、本発明において採用した構成について説明する。

【０００８】

請求項１に記載の画像処理装置は、読取対象物から画像を読み取り可能な読取手段と、前記読取対象物上での範囲があらかじめ設定された第１領域にある処理対象画像を、前記読取手段で読み取ることにより、前記処理対象画像を取得する処理対象画像取得手段と、前記読取対象物上での範囲があらかじめ設定され、その範囲が前記第１領域とは異なる範囲とされた第２領域にある認証用画像を、前記読取手段で読み取ることにより、前記認証用画像を取得する認証用画像取得手段と、前記認証用画像取得手段によって取得された前記認証用画像が、あらかじめ定められた認証条件を満たす画像であるか否かを判断する判断手段と、前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、前記処理対象画像取得手段によって取得された前記処理対象画像が処理対象とされる所定の機能について、当該機能を作動させる制御を実行する機能制御手段とを備えたことを特徴とする。

【０００９】

このように構成された画像処理装置によれば、認証用画像が認証条件を満たす画像であった場合に、処理対象画像が処理対象とされる所定の機能を作動させることができる。そのため、上記所定の機能を作動させることができる利用者を、認証条件を満たす認証用画像を第２領域に形成できる利用者に制限することができる。

【００１０】

したがって、認証を行うために、利用者がユーザアカウント名やパスワードを手作業で入力せざるを得なかった従来技術とは異なり、利用者が手作業で入力操作を行う手間を省くことができ、画像処理装置の使い勝手を向上させることができる。

【００１１】

また、本発明の画像処理装置の場合、認証用画像は処理対象画像とは別領域から読み取られるので、認証用画像と処理対象画像が同じ領域から読み取られるものとは異なり、処理対象画像の中に認証用画像が含まれてしまうことがない。

【００１２】

したがって、例えば、処理対処画像が人手に渡るような機能（例えば、ファクシミリ送信機能など）を利用した場合であっても、認証用画像まで人手に渡ってしまうことはないので、認証用画像が第三者によって不正な認証に利用される危険性を低減することができる。

【００１３】

請求項２に記載の画像処理装置は、請求項１に記載の画像処理装置において、前記読取対象物上の前記第２領域となる範囲を、利用者が指定した範囲に変更可能な範囲変更手段を備えることを特徴とする。

【００１４】

このように構成された画像処理装置によれば、第２領域となる範囲を利用者が指定した範囲に変更できるので、第２領域の範囲が固定されているものとは異なり、利用者にとって都合の良い範囲を第２領域にすることができる。

【００１５】

請求項３に記載の画像処理装置は、請求項１または請求項２に記載の画像処理装置において、前記処理対象画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側にある前記第１領域から前記処理対象画像を取得し、前記認証用画像取得手段は、前記読取対象物が有する表裏両面のうち、裏面側にある前記第２領域から前記認証用画像を取得することを特徴とする。

【００１６】

このように構成された画像処理装置によれば、読取対象物上にある表裏両面から、処理対象画像および認証用画像をそれぞれ独立に読み取ることができる。したがって、同一面内で第１領域および第２領域を重ならないように設ける場合に比べ、画像の読み取り範囲についての制約を減らすことができる。

【００１７】

請求項４に記載の画像処理装置は、請求項１または請求項２に記載の画像処理装置において、前記処理対象画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側にある前記第１領域から前記処理対象画像を取得し、前記認証用画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側にあって前記第１領域とは異なる範囲にある前記第２領域から前記認証用画像を取得することを特徴とする。

【００１８】

このように構成された画像処理装置によれば、読取対象物上にある表面側から処理対象画像および認証用画像を読み取ることができるので、第１領域および第２領域が互いに異なる面内にある場合より、読取手段の構造を簡素化することができる。

【００１９】

請求項５に記載の画像処理装置は、請求項１または請求項２に記載の画像処理装置において、前記処理対象画像取得手段は、前記読取対象物が有する表裏両面のうち、両方の面にある前記第１領域から前記処理対象画像を取得し、前記認証用画像取得手段は、前記読取対象物が有する表裏両面のうち、表面側または裏面側にあって前記第１領域とは異なる範囲にある前記第２領域から前記認証用画像を取得することを特徴とする。

【００２０】

このように構成された画像処理装置によれば、読取対象物が有する表裏両面から処理対象画像を読み取って、それらの処理対象画像が処理対象とされる所定の機能を作動させることができる。

【００２１】

請求項６に記載の画像処理装置は、請求項１～請求項５のいずれかに記載の画像処理装置において、前記認証用画像取得手段は、前記処理対象画像取得手段による前記処理対象画像の取得を開始する前に、前記第２領域から前記認証用画像の取得を完了し、前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、前記処理対象画像取得手段は、前記処理対象画像の取得を開始することを特徴とする。

【００２２】

このように構成された画像処理装置によれば、判断手段によって認証用画像が認証条件を満たす画像であると判断された場合に、処理対象画像の取得を開始するので、認証が成立しない場合に、無駄に処理対象画像の取得を開始してしまうことがない。

【００２３】

請求項７に記載の画像処理装置は、請求項１～請求項６のいずれかに記載の画像処理装置において、前記処理対象画像が処理対象とされる所定の機能を、複数の利用者それぞれが利用可能か否かの設定を、各利用者に対応付けて記憶する設定記憶手段と、前記認証用画像が前記複数の利用者のいずれに対応する画像であるのかを特定して、特定された利用者に対応付けて前記所定の機能を利用可能である旨の設定が前記設定記憶手段に記憶されていれば、前記特定された利用者は、前記所定の機能を利用可能と判定する利用者別制限判定手段とを備え、前記機能制御手段は、前記判断手段によって前記認証用画像が前記認証条件を満たす画像であると判断された場合に、さらに、前記利用者別制限判定手段により、前記特定された利用者が前記所定の機能を利用可能と判定されたら、前記所定の機能を作動させる制御を実行することを特徴とする。

【００２４】

このように構成された画像処理装置によれば、複数の利用者それぞれについて、所定の機能を利用可能か否かを個別に設定することができる。

【００２５】

請求項８に記載の画像処理装置は、請求項１～請求項７のいずれかに記載の画像処理装置において、前記読取手段は、前記読取対象物が有する表裏両面の内、いずれか一方の面から画像を読み取る第１イメージセンサと、他方の面から画像を読み取る第２イメージセンサとを備え、前記第１イメージセンサおよび第２イメージセンサが並行して作動可能に構成されていることを特徴とする。

【００２６】

このように構成された画像処理装置によれば、読取対象物上にある表裏両面から、処理対象画像および認証用画像を読み取る際、第１イメージセンサおよび第２イメージセンサを並行して利用できる。したがって、単一のイメージセンサで処理対象画像および認証用画像を順に読み取る構成に比べ、迅速な読み取りが可能となる。また、読取対象物上にある表裏両面を単一のイメージセンサで読み取り可能な位置まで読取対象物を搬送する場合に比べ、読取対象物の搬送機構も簡素化することができる。

【００２７】

請求項９に記載の画像処理装置は、請求項８に記載の画像処理装置において、前記第２イメージセンサは、前記第１イメージセンサが前記一方の面から前記処理対象画像の読み取りを開始する前に、前記他方の面から前記認証用画像の読み取りを完了可能な位置にあり、前記認証用画像取得手段は、前記他方の面にある認証用画像を、前記第２イメージセンサで読み取ることにより、前記認証用画像を取得することを特徴とする。

【００２８】

このように構成された画像処理装置によれば、第１イメージセンサで処理対象画像の読み取りを開始する前に、第２イメージセンサで認証用画像を読み取ることができる。したがって、認証用画像の迅速な読み取りが可能となり、認証が成立しない場合に、第１イメージセンサによる処理対象画像の読み取りを開始しないようにすることもできる。

【００２９】

請求項１０に記載の画像処理装置用のプログラムは、読取対象物から画像を読み取り可能な読取手段を備えた画像処理装置に内蔵された制御部を、前記読取対象物上での範囲があらかじめ設定された第１領域にある処理対象画像を、前記読取手段で読み取ることにより、前記処理対象画像を取得する処理対象画像取得手段と、前記読取対象物上での範囲があらかじめ設定され、その範囲が前記第１領域とは異なる範囲とされた第２領域にある認証用画像を、前記読取手段で読み取ることにより、前記認証用画像を取得する認証用画像取得手段と、前記認証用画像取得手段によって取得された前記認証用画像が、あらかじめ定められた認証条件を満たす画像であるか否かを判断する判断手段と、前記判断手段によ

って前記認証用画像が前記認証条件を満たす画像であると判断された場合に、前記処理対象画像取得手段によって取得された前記処理対象画像が処理対象とされる所定の機能について、当該機能を作動させる制御を実行する機能制御手段として機能させることを特徴とする。

【００３０】

このように構成された画像処理装置用のプログラムによれば、読取対象物から画像を読み取り可能な読取手段を備えた画像処理装置に内蔵された制御部を、請求項１に記載の画像処理装置が備える各手段として機能させることができる。

【００３１】

なお、この画像処理装置用のプログラムは、さらに、読取対象物から画像を読み取り可能な読取手段を備えた画像処理装置に内蔵された制御部を、請求項２～請求項９のいずれかに記載の画像処理装置が備える各手段として機能させるプログラムとして構成されていてもよい。

【図面の簡単な説明】

【００３２】

【図１】（ａ）は画像処理装置の内部構成を示すブロック図、（ｂ）はスキャナ部の概略構造を示す説明図。

【図２】（ａ）は機能制限情報記憶部に記憶された情報の一例を示す説明図、（ｂ）は画像認証情報記憶部に記憶された情報の一例を示す説明図。

【図３】（ａ）は処理対象画像エリアおよび認証用画像エリアの設定例（その１）を示す説明図、（ｂ）は処理対象画像エリアおよび認証用画像エリアの設定例（その２）を示す説明図。

【図４】（ａ）は処理対象画像エリアおよび認証用画像エリアの設定例（その３）を示す説明図、（ｂ）は処理対象画像エリアおよび認証用画像エリアの設定例（その４）を示す説明図。

【図５】主処理のフローチャート。

【図６】ユーザ登録処理のフローチャート。

【図７】ファンクションロック処理のフローチャート。

【図８】機能制御処理のフローチャート（その１）。

【図９】機能制御処理のフローチャート（その２）。

【発明を実施するための形態】

【００３３】

次に、本発明の実施形態について一例を挙げて説明する。

【００３４】

［画像処理装置の構成］

ＭＦＰ１は、プリント機能、スキャン機能、コピー機能、ＦＡＸ（ファクシミリ）機能、ｉ－ＦＡＸ（インターネットファクシミリ）機能、およびＳｃａｎＴｏＵＳＢ機能（原稿から読み取った画像のデータをＵＳＢストレージデバイスへ転送する機能）などを備えた複合機で、図１（ａ）に示すように、制御部１１、スキャナ部１２、プリンタ部１３、記憶部１４、ＬＡＮ用通信部１５、ＰＳＴＮ用通信部１６、ＵＳＢインターフェース部１７、操作部１８、および表示部１９などを備えている。

【００３５】

これらの内、制御部１１は、ＣＰＵ、ＲＯＭ、ＲＡＭ等を備えたマイクロコンピュータを中心に構成され、ＭＦＰ１各部に対する制御は、この制御部１１によって実行されている。

【００３６】

スキャナ部１２は、第１イメージセンサ１２Ａ、第２イメージセンサ１２Ｂ、原稿搬送装置１２Ｃなどを備えている。第１イメージセンサ１２Ａおよび第２イメージセンサ１２Ｂは、双方とも読取対象物から光学的に画像を読み取り可能なデバイスである。原稿搬送装置１２Ｃは、複数枚の原稿を１枚ずつ搬送可能な装置である。

【００３７】
このスキャナ部１２において、第１イメージセンサ１２Ａは、図１（ｂ）に示すように、原稿搬送装置１２Ｃによって原稿が搬送される際に原稿表面Ｄ１から画像を読み取り可能な位置に配設されている。また、第２イメージセンサ１２Ｂは、原稿搬送装置１２Ｃによって原稿が搬送される際に原稿裏面Ｄ２から画像を読み取り可能な位置に配設されている。これにより、このスキャナ部１２では、第１イメージセンサ１２Ａおよび第２イメージセンサ１２Ｂを利用して、原稿の表裏両面の読み取り処理を並列に実行可能となっている。
【００３８】
ただし、第１イメージセンサ１２Ａおよび第２イメージセンサ１２Ｂは、原稿搬送方向について距離Ｌ１だけ離れた位置に配設されているので、原稿の読み取りを行う際には、第２イメージセンサ１２Ｂが、第１イメージセンサ１２Ａよりも先行して原稿裏面Ｄ２から画像の読み取りを開始するように制御される。そして、その後、原稿表面Ｄ１が第１イメージセンサ１２Ａと対向する位置に到達した時点で、第１イメージセンサ１２Ａが原稿表面Ｄ１から画像の読み取りを開始するように制御される。
【００３９】
プリンタ部１３は、ＭＦＰ１のコピー機能を利用した際にスキャナ部１２で読み取った画像を印刷したり、ＭＦＰ１のＦＡＸ機能を利用した際に受信画像を印刷したりするのに利用される部分である。
【００４０】
記憶部１４は、ハードディスク装置や不揮発性メモリによって構成される不揮発性記憶領域、ＲＡＭによって構成される一時記憶領域を備えてなる。記憶部１４の不揮発性記憶領域内には、機能制限情報記憶部１４Ａ、画像認証情報記憶部１４Ｂなどが確保され、これにより、機能制限情報記憶部１４Ａおよび画像認証情報記憶部１４Ｂに記憶された情報（情報の内容については後述。）は、ＭＦＰ１への電力供給が途絶えたときにも保持されるようになっている。また、一時記憶領域には、スキャナ用イメージバッファ１４Ｃなどが確保され、スキャナ部１２によって読み取られた画像を表すデータを記憶する際に利用される。
【００４１】
ＬＡＮ用通信部１５は、ＬＡＮ（Local Area Network）に接続するための通信インターフェース装置によって構成され、このＬＡＮ用通信部１５により、ＭＦＰ１は、ＬＡＮを介して通信可能な他の機器とデータ通信可能となっている。また、ＭＦＰ１が接続されたＬＡＮがゲートウェイを介してインターネットなどのＷＡＮ（Wide Area Network）に接続されていれば、ＭＦＰ１は、ＷＡＮを介して通信可能な他の機器ともデータ通信を行うことができ、例えば、ＭＦＰ１が備えるｉ－ＦＡＸ機能を利用する際には、ＬＡＮ用通信部１５を介してデータの送受信が行われる。
【００４２】
ＰＳＴＮ用通信部１６は、ＦＡＸモデムや音声ＣＯＤＥＣなど、公衆回線（Public Switched Telephone Networks；ＰＳＴＮ）に接続する上で必要となる各種機器によって構成されている。このＰＳＴＮ用通信部１６により、ＭＦＰ１は、公衆回線を介して通信可能な他の機器（例えば、ファクシミリ装置）と通信可能で、例えば、ＭＦＰ１が備えるＦＡＸ機能を利用する際には、ＰＳＴＮ用通信部１６を介してデータの送受信が行われる。
【００４３】
ＵＳＢインターフェース部１７は、ＵＳＢストレージデバイスを接続可能なインターフェースで、例えば、ＭＦＰ１が備えるＳｃａｎＴｏＵＳＢ機能を利用する際に、スキャナ部１２で読み取った画像を表すデータを、ＵＳＢインターフェース部１７に接続されたＵＳＢストレージデバイスへと転送することができる。
【００４４】
［認証機能の概要］
次に、上記ＭＦＰ１において実行される具体的な処理の詳細を説明するのに先立って、

上記ＭＦＰ１が備える認証機能の概要について説明する。

【００４５】

このＭＦＰ１では、ＭＦＰ１の利用時に利用者の認証を行い、認証の成立した利用者だけが所定の機能を利用できるようになっている。この状態が、後述するファンクションロック機能の起動中に相当する。また、利用者の認証を行う方法としては、２通りの認証方法（以下、第１，第２の認証方法と称する。）を利用することができる。

【００４６】

第１の認証方法は、利用者が操作部１８での操作によってユーザ名を選択するとともに、そのユーザ名に対応する第１認証データ（いわゆるパスワードに相当）を入力することによって認証を行う方法である。第２の認証方法は、スキャナ部１２を使用して、原稿上において任意に設定された認証用画像エリアから認証用画像を読み取ることによって認証を行う方法である。以下、これら２通りの認証方法について、さらに詳しく説明する。

【００４７】

まず、上記第１の認証方法による認証を実行可能とするため、ＭＦＰ１が備える記憶部１４の機能制限情報記憶部１４Ａには、図２（ａ）に示すように、「ユーザ名」、「第１認証データ」、「ＦＡＸ送信」、「ｉ－ＦＡＸ送信」、「コピー」、および「ＳｃａｎＴｏＵＳＢ」、以上６項目を１組とするデータが、複数の利用者それぞれに対応づけて複数組記憶されている。そして、各項目に対して、ユーザ名毎に使用を許可するか否かを示す情報、また、許可する場合には、その使用制限回数が記憶される。

【００４８】

これらのデータのうち、「ユーザ名」および「第１認証データ」は、上記第１の認証方法による認証を行う際にＭＦＰ１が参照するデータで、ＭＦＰ１の管理者が任意に設定した文字列が記憶されている。

【００４９】

これら「ユーザ名」および「第１認証データ」は、管理者がＭＦＰ１への登録作業を行った後、管理者から個々の利用者へと知らされる。そして、個々の利用者がＭＦＰ１を利用する際、上記第１の認証方法による認証を行う場合には、利用者が、操作部１８での操作により、ユーザ名を選択するとともに第１認証データを入力する。

【００５０】

そして、これらの情報が入力されると、ＭＦＰ１は、それらの入力情報と機能制限情報記憶部１４Ａに記憶された情報とを照合し、両者の組み合わせが一致すれば認証を成立させる。

【００５１】

認証が成立した場合、続いて、利用者により選択された機能について、ＭＦＰ１は、「ＦＡＸ送信」、「ｉ－ＦＡＸ送信」、「コピー」、および「ＳｃａｎＴｏＵＳＢ」の各項目を参照し、これら各項目に対応する各機能について、認証の成立した利用者が利用可能な機能か否か、利用可能な機能である場合は、上限として何回まで利用可能かを判断する。

【００５２】

これら「ＦＡＸ送信」、「ｉ－ＦＡＸ送信」、「コピー」、および「ＳｃａｎＴｏＵＳＢ」の各項目に記憶された内容は、「ユーザ名」および「第１認証データ」同様、管理者が事前にＭＦＰ１への登録作業を行ったものである。

【００５３】

以上のような認証方法について、具体例を交えて説明すると、例えば、機能制限情報記憶部１４Ａに、図２（ａ）に例示したデータが記憶されている場合、利用者が、操作部１８での操作により、ユーザ名“Ｕｓｅｒ１”を選択するとともに、第１認証データとして“１１１１”を入力すると、認証が成立する。

【００５４】

そして、このユーザ名“Ｕｓｅｒ１”の認証が成立した場合であれば、ＭＦＰ１は、機能制限情報記憶部１４Ａに記憶された情報を参照し、「ＦＡＸ送信」、「ｉ－ＦＡＸ送信

」、および「コピー」の各機能については、記憶された上限回数までの利用を許可する一方、「ＳｃａｎＴｏＵＳＢ」については、その利用を禁止する。

【００５５】

他のユーザ名が選択された場合も同様の認証処理が行われるが、どの機能の利用が許可されるかは、機能制限情報記憶部１４Ａに記憶された情報に応じて変わり、例えば、ユーザ名“Ｕｓｅｒ３”の認証が成立した場合であれば、「コピー」については記憶された上限回数までの利用が許可されるものの、「ＦＡＸ送信」、「ｉ－ＦＡＸ送信」、および「ＳｃａｎＴｏＵＳＢ」については、その利用が禁止される。

【００５６】

なお、ＭＦＰ１の起動直後、認証が成立しなかった場合、あるいは、認証成立後に所定のタイムアウト時間が経過した場合等には、ＭＦＰ１は、Ｐｕｂｌｉｃモードで作動する。この場合、機能制限情報記憶部１４Ａに記憶された情報については、ユーザ名“Ｐｕｂｌｉｃ”に対応する各項目が参照され、各機能の利用を許可するか否かの判断が行われる。

【００５７】

すなわち、このＭＦＰ１は、認証が成立していない状態であっても、管理者が利用を許可している機能については、その機能を利用することができる。Ｐｕｂｌｉｃモードでの作動時にどのような機能の利用が許可されるかについては、管理者の設定次第となるが、特定の利用者の認証が成立した場合より、利用できる機能がさらに制限される設定とするのが一般的である。

【００５８】

さて次に、上記第２の認証方法について説明する。第２の認証方法による認証を実行可能とするため、ＭＦＰ１が備える記憶部１４の画像認証情報記憶部１４Ｂには、図２（ｂ）に示すように、「ユーザ名」および「第２認証データ」、以上２項目を１組とするデータが、複数の利用者それぞれに対応づけて複数組記憶されている。

【００５９】

これらのデータのうち、「ユーザ名」は、機能制限情報記憶部１４Ａに記憶された「ユーザ名」と同一の文字列で、この項目をキーにして、機能制限情報記憶部１４Ａおよび画像認証情報記憶部１４Ｂが関連付けられている。

【００６０】

また、「第２認証データ」は、認証用画像のデータそのもの、または認証用画像であるか否かを判定するために必要となるデータ（例えば、認証用画像がバーコードの画像であれば、そのバーコードによって表されるバイナリデータ、あるいは、認証用画像が文字列の画像であれば、その文字列に対してＯＣＲ処理を施すことによって得られるテキストデータ等）で、本実施形態の場合は、印鑑の印影を表す画像データが「第２認証データ」として記憶されている。

【００６１】

本実施形態のように、印影を表す画像データを「第２認証データ」とする場合、管理者は、個々の利用者から提出された印影をスキャナ部１２で読み取って画像データ化し、ＭＦＰ１への登録作業を行い、これにより、第２の認証方法が利用可能となる。

【００６２】

そして、個々の利用者がＭＦＰ１を利用する際、上記第２の認証方法による認証を行う場合には、利用者が、操作部１８での操作により、スキャナ部１２での画像読み取りを伴う機能（例えば、ＦＡＸ送信機能、コピー機能等）を作動させる。

【００６３】

このような操作が行われると、ＭＦＰ１は、スキャナ部１２を使用して、原稿上において任意に設定された認証用画像エリアから画像を読み取り、読み取った画像の中から認証用画像を抽出する。そして、抽出された認証用画像を表す画像データ（もしくは、抽出された認証用画像から変換されたバイナリデータやテキストデータ）と画像認証情報記憶部１４Ｂに記憶された第２認証データとを照合し、両者が一致すれば認証を成立させる。

【００６４】
認証が成立した場合には、第１の認証方法の場合と同様に、ＭＦＰ１は、機能制限情報記憶部１４Ａに記憶された「ＦＡＸ送信」、「ｉ－ＦＡＸ送信」、「コピー」、および「ＳｃａｎＴｏＵＳＢ」の各項目を参照して、選択された機能について、認証の成立した利用者が利用可能な機能か否か、利用可能な機能である場合は、上限として何回まで利用可能かを判断することになる。
【００６５】
なお、認証が成立しなかった場合、あるいは、利用者が利用しようとした機能の利用が禁止されていた場合、ＭＦＰ１は、認証用画像の読み取りについては実行するものの、利用者が利用しようとした機能そのものが実行されることはない。
【００６６】
以上説明したような認証方法のうち、第１の認証方法を使用するか否かは、ＭＦＰ１において管理者が任意に設定することができる。また、第１の認証方法を使用する設定とした場合であっても、第１の認証方法だけを利用するか、第１，第２の認証方法を併用するかは、ＭＦＰ１において管理者が任意に設定することができる。
【００６７】
さらに、第２の認証方法を利用する設定とした場合、原稿上のどの範囲を認証用画像エリアとして利用するのかについては、管理者が任意に設定できる。以下、この認証用画像エリアの設定例について、いくつかの具体的事例を挙げて説明する。
【００６８】
図３（ａ）は、処理対象画像エリアおよび認証用画像エリアの設定例（その１）を示す説明図である。この設定例（その１）は、原稿の表裏両面に処理対象画像（例えば、コピー対象となる画像）が描かれている場合についての設定例であり、原稿表面Ｄ１に第１処理対象画像エリアＡ１、原稿裏面Ｄ２に第２処理対象画像エリアＡ２が設けられている。また、原稿裏面Ｄ２の一部には、認証用画像エリアＡ３が設けられている。
【００６９】
図３（ａ）において、原稿表面Ｄ１と原稿裏面Ｄ２が距離Ｌ１だけずれた位置に描いてあるのは、同時に読み取られる原稿上の位置を横方向に並べて描いてあるためである。すなわち、このＭＦＰ１の場合、既に説明したとおり、原稿裏面Ｄ２が原稿表面Ｄ１よりも先行して読み取られるが、図３（ａ）では、同時に読み取られる原稿上の位置を横方向に並べて描いてあるので、原稿表面Ｄ１と原稿裏面Ｄ２とでは、読み取りの開始タイミングに距離Ｌ１分のずれが生じている。
【００７０】
また、認証用画像エリアＡ３は、図３（ａ）中に示した距離Ｌ２の範囲に設定されており、この距離Ｌ２は、距離Ｌ２＝距離Ｌ１－距離Ｌ３を満たすような距離とされている。そして、原稿搬送装置１２Ｃが所定の速度で原稿を搬送した場合に、原稿を距離Ｌ３だけ搬送する際に要する時間が、第２の認証方法で認証を完了するまでに要する時間を上回ることになるように、原稿搬送速度と距離Ｌ３の関係が最適化されている。
【００７１】
以上のような前提の下、ＭＦＰ１で認証用画像エリアＡ３の範囲（距離Ｌ２）を、利用者が任意に設定する際には、上記のような距離Ｌ３を考慮した範囲内でしか、認証用画像エリアＡ３の範囲（距離Ｌ２）を設定できないようにしてある。
【００７２】
具体的には、操作部１８において利用者が任意に距離Ｌ２の値を入力するか、あるいは、距離Ｌ２として選択可能ないくつかの候補がプリセット値として用意されていて、その中から利用者が所望の値を選択する、といった方法で距離Ｌ２を設定できるが、いずれの方法であっても、その上限値は距離Ｌ３が過小にならない範囲内でしか入力または選択ができないようになっている。
【００７３】
このようにしておけば、認証用画像エリアＡ３の読み取りを完了してから、引き続いて

第２処理対象画像エリアＡ２の読み取りを開始する際、同時に第２の認証方法による認証を開始することにより、その後、第１処理対象画像エリアＡ１の読み取りを開始する前の時点で、第２の認証方法による認証を完了させることができるようになる。

【００７４】

したがって、この認証処理の結果、認証が不成立となった場合には、第１処理対象画像エリアＡ１の読み取りを無駄に実施しなくても済む。なお、利用者が、上記のように決められた範囲内で任意の範囲を認証用画像エリアＡ３に設定すると、原稿裏面Ｄ２の残りの範囲は、第２処理対象画像エリアＡ２とされる。

【００７５】

ところで、以上の説明においては、原稿搬送装置１２Ｃが所定の一定速度で原稿を搬送するとの前提で、距離Ｌ３を最適化することにより、第１処理対象画像エリアＡ１の無駄な読み取りを回避できる旨を説明したが、原稿が所定の位置に到来した時点で一時的に搬送を停止できる場合には、距離Ｌ２の範囲の読み取りが完了した時点で原稿搬送を一時停止してもよい。

【００７６】

このような構成とした場合は、認証用画像エリアＡ３の読み取りが完了した時点で読み取りを一時停止し、第２処理対象画像エリアＡ２の読み取りを行うことなく、認証処理だけを実行できるので、認証不成立時には、一定速度で原稿を搬送する場合同様、第１処理対象画像エリアＡ１の無駄な読み取りを回避できるのはもちろんのこと、一定速度で原稿を搬送する場合とは異なり、第２処理対象画像エリアＡ２の無駄な読み取りも回避することができる。

【００７７】

しかも、原稿搬送を一時停止した後、原稿搬送を再開するに当たっては、第２の認証方法で認証を完了した後に、原稿搬送を再開すればよいので、上述のように原稿搬送速度と距離Ｌ３の関係を最適化する必要はなく、距離Ｌ１の範囲内であれば、所望の範囲を認証用画像エリアＡ３として設定できるようになる。

【００７８】

次に、上記とは別の設定例（その２）について、図３（ｂ）を参照しつつ説明する。図３（ｂ）は、処理対象画像エリアおよび認証用画像エリアの設定例（その２）を示す説明図である。

【００７９】

この設定例（その２）も、原稿の表裏両面に処理対象画像（例えば、コピー対象となる画像）が描かれている場合についての設定例であり、原稿表面Ｄ１に第１処理対象画像エリアＡ１、原稿裏面Ｄ２に第２処理対象画像エリアＡ２が設けられている。また、原稿裏面Ｄ２の一部には、認証用画像エリアＡ３が設けられている。さらに、設定例（その１）とは異なる点として、上述した距離Ｌ３の範囲には、未使用エリアＡ４が設けられている。

【００８０】

認証用画像エリアＡ３の設定方法は、上記設定例（その１）と同様な方法とすればよく、認証用画像エリアＡ３が決まれば、それに応じて未使用エリアＡ４の範囲も決まる。また、この設定例（その２）の場合、第２処理対象画像エリアＡ２の範囲は不変となる。

【００８１】

このような未使用エリアＡ４を設けると、先に説明したような、原稿搬送装置１２Ｃが所定の一定速度で原稿を搬送することと、認証不成立時に第１処理対象画像エリアＡ１および第２処理対象画像エリアＡ２双方についての無駄な読み取りを回避することを、両立して実現することができる。

【００８２】

すなわち、認証用画像エリアＡ３の読み取りを完了した後、原稿搬送の一時停止は実施しないものの、未使用エリアＡ４の読み取りは行わないことで、無駄な読み取りを回避することができる。そして、原稿を距離Ｌ３だけ搬送する間に認証処理を完了し、認証が成

立した場合には、第１処理対象画像エリアＡ１および第２処理対象画像エリアＡ２の読み取りを同時に開始する。

【００８３】

このような構成を採用すれば、第２処理対象画像エリアＡ２は、未使用エリアＡ４の分だけ狭くなるものの、原稿搬送の一時停止を実施しなくても済むので、一時停止することなく迅速に処理が進行する印象を利用者に与えることができ、且つ、認証不成立時の無駄な読み取りを回避することが可能となる。

【００８４】

次に、上記とは別の設定例（その３）について、図４（ａ）を参照しつつ説明する。図４（ａ）は、処理対象画像エリアおよび認証用画像エリアの設定例（その３）を示す説明図である。

【００８５】

この設定例（その３）も、原稿の表裏両面に処理対象画像（例えば、コピー対象となる画像）が描かれている場合についての設定例であるが、設定例（その１）および設定例（その２）とは異なる点として、認証用画像エリアＡ３が原稿表面Ｄ１に設けられている。認証用画像エリアＡ３の設定方法は、上記設定例（その１）と同様な方法とすればよく、認証用画像エリアＡ３が決まれば、それに応じて第１処理対象画像エリアＡ１の範囲も決まる。

【００８６】

このような位置に認証用画像エリアＡ３を設けても、認証を行う上では、何ら問題は生じない。ただし、このような位置に認証用画像エリアＡ３を設けた場合、第２処理対象画像エリアＡ２に関しては、認証が成立するか否かを問わず、先行して読み取りを行わなければならないので、その分だけＭＦＰ１の記憶領域を使用することになる。特に認証が成立しなかった場合には、最終的に破棄されることになるデータであっても読み取りを行うことになるので、いくらか無駄な処理を行うことにはなる。

【００８７】

このように認証が成立するか否かを問わず、先行してデータの読み取りを行った後、第２の認証方法で認証が成立しなかった場合に、先行して読み取ったデータを有効利用するには、第２の認証方法で認証が成立しなかったら、利用者が事後的に第１の認証方法での認証を実施できるように構成してもよい。この場合、第１の認証方法で認証が成立すれば、所期の機能を作動させることができるようにする。このような構成を採用しておけば、先行して読み取ったデータを無駄にすることなく利用することもできる。

【００８８】

また、このような位置に認証用画像エリアＡ３を設けた場合、所定の一定速度で原稿を搬送するのであれば、第１処理対象画像エリアＡ１に関しても、認証が成立するか否かを問わず、先行して読み取りを行わなければならないので、その分だけＭＦＰ１の記憶領域を使用することになる。ただし、この点は、先に説明した通り、原稿搬送の一時停止を実施することもできるので、この場合は、第１処理対象画像エリアＡ１については、無駄な読み取りを回避することも可能となる。

【００８９】

次に、上記とは別の設定例（その４）について、図４（ｂ）を参照しつつ説明する。図４（ｂ）は、処理対象画像エリアおよび認証用画像エリアの設定例（その４）を示す説明図である。

【００９０】

この設定例（その４）は、原稿表面Ｄ１に処理対象画像（例えば、コピー対象となる画像）が描かれ、原稿裏面Ｄ２には処理対象画像が描かれていない場合についての設定例である。

【００９１】

この事例の場合、利用者は、ＭＦＰ１において原稿裏面Ｄ２が認証用画像エリアＡ３である旨の設定を事前に行っている。そして、原稿の読み取りを行う際には、ＭＦＰ１にお

いて片面読み取りを実行する旨の指令を入力する。

【００９２】

片面読み取りの実行が指令された場合、第２の認証方法による認証を実施する旨が設定されていなければ、ＭＦＰ１は、第１イメージセンサ１２Ａのみを利用して読み取りを実行する。

【００９３】

一方、第２の認証方法による認証を実施する旨が設定されていれば、片面読み取りの実行が指令された場合であっても、ＭＦＰ１は、第１イメージセンサ１２Ａおよび第２イメージセンサ１２Ｂの双方を利用して読み取りを実行する。

【００９４】

このような構成にすれば、原稿の表裏を処理対象画像エリアＡ１と認証用画像エリアＡ３として使い分けることができるので、一方の面に処理対象画像エリアＡ１またはＡ２と認証用画像エリアＡ３とが共存する場合に比べ、認証用画像エリアＡ３の範囲を、利用者にとってわかりやすいものとすることができる。

【００９５】

なお、この事例のように、原稿の表裏を処理対象画像エリアＡ１と認証用画像エリアＡ３として使い分ける場合であっても、他の例のように、一部を認証用画像エリアＡ３として、残りは未使用エリアＡ４とする構成にしてもよい。また、原稿の表裏いずれを認証用画像エリアＡ３としてもよい。

【００９６】

さらに、原稿の表裏いずれか一方の全面が認証用画像エリアＡ３として設定される場合であっても、例えば、本実施形態のように、印影を表す画像データを「第２認証データ」とする場合などは、「第２認証データ」となる画像のサイズがある程度限られたサイズになる。したがって、このような場合であれば、認証用画像エリアＡ３全体を読み取ってから、「第２認証データ」となる画像の有無を解析しなくてもよい。具体例を挙げれば、例えば、図４（ｂ）に示した距離Ｌ４の範囲を対象に、この範囲を少しずつずらしながら、画像の読み取りと解析を繰り返してもよい。このように認証用画像エリアＡ３の一部を対象に画像の読み取りと解析を繰り返せば、認証用画像エリアＡ３全体を読み取ってから解析を行う場合より、読み取り時に必要となるスキャナ用イメージバッファ１４Ｃの空き領域を低減でき、メモリの利用効率を上げることができる。

【００９７】

以上説明したような設定例（その１）～（その４）について、どのような設定とするかは、利用者が任意にいずれか一つを選択することができる。ただし、上記設定例（その１）～（その４）のうち、いずれか一つの設定しかできない構成になっていてもよい。

【００９８】

［ＭＦＰにおいて実行される処理］

次に、上述したような機能を実現するためにＭＦＰ１において実行される処理について、図５～図９のフローチャートに基づいて説明する。

【００９９】

図５は、ＭＦＰ１において実行される主処理のフローチャートである。この主処理は、ＭＦＰ１の電源スイッチがオンにされたことを契機として、制御部１１が備えるＣＰＵによって実行される処理である。

【０１００】

この処理を開始すると、ＭＦＰ１は、キー入力を待つ状態になり（Ｓ１０５）、キー入力があったか否かを判定し（Ｓ１１０）、キー入力がなかった場合は（Ｓ１１０：ＮＯ）、Ｓ１０５へと戻る。これにより、キー入力がない間は、Ｓ１０５～Ｓ１１０を繰り返すことで、キー入力を待ち受けることになる。

【０１０１】

そして、キー入力があった場合は（Ｓ１１０：ＹＥＳ）、ＭＦＰ１は、キーに対応付けられたイベントが発生したことを検知して、イベントに対応する処理を実行し（Ｓ１１５

）、Ｓ１０５へと戻る。

【０１０２】

Ｓ１１５において、イベントの発生を検知した場合に、どのような処理が実行されるかは、操作されたキー（またはキーの組み合わせ）によって変わるが、本発明の要部に関連する処理としては、ユーザ登録処理、ファンクションロック処理、および機能制御処理などが実行される。以下、これらの各処理について説明する。

【０１０３】

まず、ユーザ登録処理について説明する。図６は、ユーザ登録処理のフローチャートである。ユーザ登録処理は、Ｓ１１５において、イベントの発生を検知した場合に実行される処理の一つであり、ＭＦＰ１の管理者が、ユーザ登録を行うためのキー操作を行うことでユーザ登録開始イベントが発生したら、そのユーザ登録開始イベントの発生を契機として実行される。

【０１０４】

この処理を開始すると、ＭＦＰ１は、まず、新規登録か否かを判断する（Ｓ２０５）。管理者は、ＭＦＰ１が備える操作部１８で所定のキーを操作することにより、新規ユーザの登録か登録済みユーザについての変更かの指示をＭＦＰ１に対して与えることができ、Ｓ２０５では、操作部１８でのキー操作に基づいて、新規登録か否かが判断される。

【０１０５】

Ｓ２０５において、新規登録でないと判断された場合（Ｓ２０５：ＮＯ）、ＭＦＰ１は、変更対象ユーザを選択するための入力操作を受け付けて（Ｓ２１０）、Ｓ２１５へと進む。一方、Ｓ２０５において、新規登録であると判断された場合（Ｓ２０５：ＹＥＳ）、ＭＦＰ１は、Ｓ２１０を実行することなく、Ｓ２１５へと進む。

【０１０６】

こうしてＳ２１５へと進むと、ＭＦＰ１は、ユーザ名についての設定を受け付ける（Ｓ２１５）。新規登録の場合、管理者は、Ｓ２１５において新たなユーザ名を入力することになる。また、登録済み情報の変更の場合、管理者は、必要があれば、Ｓ２１５においてユーザ名の一部または全部を修正することになる。そして、いずれの場合とも、Ｓ２１５において入力されたユーザ名は、機能制限情報記憶部１４Ａに記憶される。

【０１０７】

続いて、ＭＦＰ１は、第１認証データについての設定を受け付ける（Ｓ２２０）。新規登録の場合、管理者は、Ｓ２２０において新たなユーザに対応する第１認証データを入力することになる。また、登録済み情報の変更の場合、管理者は、必要があれば、Ｓ２２０において登録済みユーザに対応する第１認証データを修正することになる。そして、いずれの場合とも、Ｓ２２０において入力された第１認証データは、機能制限情報記憶部１４Ａに記憶される。

【０１０８】

続いて、ＭＦＰ１は、機能・動作制限についての設定を受け付ける（Ｓ２２５）。本実施形態において、機能・動作制限について設定できる項目は、図２（ａ）に示した「ＦＡＸ送信」、「ｉ－ＦＡＸ送信」、「コピー」、および「ＳｃａｎＴｏＵＳＢ」、以上の４項目である。

【０１０９】

新規登録の場合、管理者は、Ｓ２２５において新たなユーザに対応する機能・動作制限について、その設定を入力することになる。また、登録済み情報の変更の場合、管理者は、必要があれば、Ｓ２２５において登録済みユーザに対応する機能・動作制限について、その設定を修正することになる。そして、いずれの場合とも、Ｓ２２５において入力された機能・動作制限についての設定は、機能制限情報記憶部１４Ａに記憶される。

【０１１０】

続いて、ＭＦＰ１は、第２認証データを設定するか否かを判断する（Ｓ２３０）。管理者は、ＭＦＰ１が備える操作部１８で所定のキーを操作することにより、第２認証データを設定するか否かの指示をＭＦＰ１に対して与えることができ、Ｓ２３０では、操作部１

８でのキー操作に基づく判断が行われる。

【０１１１】

Ｓ２３０において第２認証データを設定すると判断された場合（Ｓ２３０：ＹＥＳ）、ＭＦＰ１は、第２認証データについての設定を受け付ける（Ｓ２３５）。新規登録の場合、管理者は、Ｓ２３５において新たなユーザに対応する第２認証データを入力することになる。また、登録済み情報の変更の場合、管理者は、必要があれば、Ｓ２３５において登録済みユーザに対応する第２認証データを修正することになる。そして、いずれの場合とも、Ｓ２３５において入力された第２認証データは、画像認証情報記憶部１４Ｂに記憶される。

【０１１２】

本実施形態の場合、Ｓ２３５において、管理者は、個々の利用者から受け取った印鑑の印影をスキャナ部１２にセットして、操作部１８において第２認証データの抽出を指令するキー操作を実施する。これを受けて、ＭＦＰ１は、スキャナ部１２で画像を読み取って、読み取った画像の中から朱肉相当の色を持つ画素を抽出することにより、第２認証データとなる印影の画像を切り出し、このデータが画像認証情報記憶部１４Ｂに記憶される。

【０１１３】

そして、Ｓ２３５を終えたら、Ｓ２４０へと進む。なお、Ｓ２３０において第２認証データを設定しないと判断された場合（Ｓ２３０：ＮＯ）、ＭＦＰ１は、Ｓ２３５を実行することなく、Ｓ２４０へと進む。

【０１１４】

こうしてＳ２４０へと進んだら、ＭＦＰ１は、ユーザ登録終了か否かを判断する（Ｓ２４０）。管理者は、ＭＦＰ１が備える操作部１８で所定のキーを操作することにより、ユーザ登録終了か否かの指示をＭＦＰ１に対して与えることができ、Ｓ２４０では、操作部１８でのキー操作に基づく判断が行われる。

【０１１５】

Ｓ２４０においてユーザ登録終了ではないと判断された場合（Ｓ２４０：ＮＯ）、Ｓ２０５へと戻る。これにより、Ｓ２０５以降の処理が再び実行され、さらに新規登録または登録済みユーザについての変更が行われることになる。また、Ｓ２４０においてユーザ登録終了であると判断された場合（Ｓ２４０：ＹＥＳ）、図６に示すユーザ登録処理を終了する。

【０１１６】

次に、ファンクションロック処理について説明する。図７は、ファンクションロック処理のフローチャートである。ファンクションロック処理は、Ｓ１１５において、イベントの発生を検知した場合に実行される処理の一つであり、ＭＦＰ１の管理者が、ファンクションロック機能の起動を指令するためのキー操作を行うことでファンクションロック機能起動イベントが発生したら、そのファンクションロック機能起動イベントの発生を契機として実行される。

【０１１７】

この処理を開始すると、ＭＦＰ１は、まず、ファンクションロック機能の起動に必要となる設定があるか否かを判断する（Ｓ３０５）。ファンクションロック機能の起動に必要となる設定とは、例えば、先にユーザ登録処理で登録した情報などである。

【０１１８】

すなわち、少なくとも１つはユーザ名が登録され、且つ、登録済みユーザ名に対応付けて機能・動作制限に関する情報が登録されている場合に、Ｓ３０５では、ファンクションロック機能の起動に必要となる設定があると判断する。

【０１１９】

Ｓ３０５において、ファンクションロック機能の起動に必要となる設定がないと判断された場合（Ｓ３０５：ＮＯ）、図７に示すファンクションロック処理を終了する。一方、Ｓ３０５において、ファンクションロック機能の起動に必要となる設定があると判断された場合（Ｓ３０５：ＹＥＳ）、ＭＦＰ１は、ファンクションロック機能を起動する（Ｓ３

１０）。ファンクションロック機能を起動した旨は、例えば、ＭＦＰ１のメモリ上においてフラグとして保持され、以降に実行される他の処理において参照される。

【０１２０】

続いて、ＭＦＰ１は、第２認証データの登録数が０より大であるか否かを判断する（Ｓ３１５）。すなわち、第２認証データが少なくとも１つは登録されているか否かを判断する。Ｓ３１５において、第２認証データの登録数が０であると判断された場合（Ｓ３１５：ＮＯ）、第２の認証方法を利用できないので、そのまま図７に示すファンクションロック処理を終了する。この場合、第１の認証方法のみが有効になる。

【０１２１】

一方、第２認証データの登録数が０より大であると判断された場合は（Ｓ３１５：ＹＥＳ）、第２の認証方法を利用できるので、第２認証データを用いた「自動認証」（すなわち、第２の認証方法による認証；以下、自動認証とも言う。）を有効にするか否かを、管理者に問い合わせるためのメッセージを表示部１９に表示し（Ｓ３２０）、管理者からの指令を受け付ける状態になる。ここで、管理者は、自動認証をオンにするかオフにするかを、操作部１８での操作によって指令することができる。

【０１２２】

管理者からの指令を受け付けたら、引き続いて、ＭＦＰ１は、管理者からの指令に基づいて自動認証をオンにするか否かを判断する（Ｓ３２５）。Ｓ３２５において、自動認証をオンにしないと判断された場合（Ｓ３２５：ＮＯ）、管理者は第２の認証方法を利用しない設定を選択したことになるので、そのまま図７に示すファンクションロック処理を終了する。この場合、第１の認証方法のみが有効になる。

【０１２３】

一方、Ｓ３２５において、自動認証をオンにすると判断された場合（Ｓ３２５：ＹＥＳ）、管理者は第２の認証方法を利用する設定を選択したことになるので、この場合は、自動認証機能の設定をオンにして（Ｓ３３０）、認証用画像エリアを有効化して（Ｓ３３５）、図７に示すファンクションロック処理を終了する。この場合、第１，第２の認証方法双方が有効になる。

【０１２４】

なお、Ｓ３３５によって有効化される認証用画像エリアは、先に図３および図４に例示したようなエリアであり、設定例（その１）～（その４）のうち、いずれの設定例に示したようなエリアとするか、各設定例中の距離Ｌ２をどの程度とするかは、Ｓ３３０において、管理者が自動認証機能の設定をオンにする際、操作部１８での操作により、管理者が任意に設定することになる。また、予め距離Ｌ２が設定されている場合には、変更の操作が管理者によりなされない限り、その設定を用いるような構成であってもよい。

【０１２５】

次に、機能制御処理について説明する。図８および図９は、機能制御処理のフローチャートである。機能制御処理は、Ｓ１１５において、イベントの発生を検知した場合に実行される処理の一つであり、ＭＦＰ１の利用者（管理者以外でも可）が、ＭＦＰ１の機能を利用するためのキー操作を行うことで機能開始要求イベントが発生したら、その機能開始要求イベントの発生を契機として実行される。

【０１２６】

なお、機能制御処理によって作動させることになる機能は、例えば、コピー機能、ＦＡＸ機能など、ＭＦＰ１が備える複数種の機能が対象となり、それら複数種の機能毎に細部の制御は異なるものとなる。ただし、本発明の要部に相当する認証に関連する処理や機能作動させるか否かを振り分ける処理については、上記複数種の機能のいずれであっても同等な手順となる共通の処理なので、以下の説明では、上記複数種の機能を特に区別することなく説明する。

【０１２７】

この処理を開始すると、ＭＦＰ１は、まず、ファンクションロック機能の起動を確認し（Ｓ４０５）、ファンクションロック機能が起動中か否かを判断する（Ｓ４１０）。具体

的には、ファンクションロック機能が起動されている場合、その旨を表す情報が、先に説明したＳ３１０によって保存されているので、Ｓ４０５では、その情報を取得することで、制御部１１はファンクションロック機能の起動を確認でき、Ｓ４１０では、取得した情報に基づく判断を行う。

【０１２８】

Ｓ４１０において、ファンクションロック機能が起動中であると判断された場合（Ｓ４１０：ＹＥＳ）、ログイン中のユーザを確認し（Ｓ４１５）、ログイン中のユーザに対する機能制限設定を読み出す（Ｓ４２０）。

【０１２９】

具体的には、特定の利用者がログインしている状態（特定の利用者が第１の認証方法を利用して認証済みとなっている状態）にある場合、そのユーザ名が所定の記憶領域に格納されているので、Ｓ４１５では、ユーザ名が格納された記憶領域からユーザ名を読み取ることで、そのユーザ名を取得し、これにより、制御部１１は、その時点でログイン中の利用者を確認できる。また、既に説明した通り、ＭＦＰ１の起動直後、認証が成立しなかった場合、あるいは、認証成立後に所定のタイムアウト時間が経過した場合等、ＭＦＰ１はＰｕｂｌｉｃモードで作動していることもあるが、この場合、上記ユーザ名が格納された記憶領域には、Ｐｕｂｌｉｃモードに対応する情報（例えば、ユーザ名“Ｐｕｂｌｉｃ”、あるいは文字列以外の制御コードなどでも可。）が格納されているので、Ｓ４１５では、ユーザ名が格納された記憶領域からユーザ名を読み取り、これにより、制御部１１は、その時点でＭＦＰ１がＰｕｂｌｉｃモードで作動していることを確認できる。

【０１３０】

そして、Ｓ４２０では、取得したユーザ名（またはＰｕｂｌｉｃモードに対応する情報）をキーにして機能制限情報記憶部１４Ａに記憶された情報を検索し、その中からユーザ名（またはＰｕｂｌｉｃモードに対応する情報）が一致する１組の情報を読み出す。

【０１３１】

そして、Ｓ４２０で読み出した１組の情報に基づいて、利用しようとしている機能（機能開始要求イベントの発生時に指示された機能）について、ログイン中の利用者による利用が許可された機能か否かを判断する（Ｓ４２５）。具体例を挙げると、例えば、図２（ａ）に例示したユーザ名“Ｕｓｅｒ１”でログイン中、利用しようとしている機能が「ＦＡＸ送信」である場合、Ｓ４２５では、許可された機能であると判断する。また、ユーザ名“Ｕｓｅｒ３”でログイン中、利用しようとしている機能が「ＦＡＸ送信」である場合、Ｓ４２５では、許可された機能ではないと判断する。

【０１３２】

Ｓ４２５において、許可された機能であると判断された場合（Ｓ４２５：ＹＥＳ）、ＭＦＰ１は、利用者の要求する機能を作動させて（Ｓ４３０）、図８に示す機能制御処理を終了する。また、Ｓ４１０において、ファンクションロック機能が起動中でないと判断された場合も（Ｓ４１０：ＮＯ）、利用者の要求する機能を作動させて（Ｓ４３０）、図７に示す機能制御処理を終了する。

【０１３３】

このＳ４３０により、利用者の要求する機能、例えば、プリント機能、スキャン機能、コピー機能、ＦＡＸ機能、ｉ－ＦＡＸ機能、ＳｃａｎＴｏＵＳＢ機能などを作動させるための制御が行われる。その際、処理対象画像の読み取りを伴う機能（例えば、コピー機能）を作動させる際には、第１処理対象画像エリアＡ１や第２処理対象画像エリアＡ２の読み取りも、Ｓ４３０によって実行されることになる。なお、これら各機能を作動させる制御自体は、従来のＭＦＰと同等な制御となるので、これ以上の詳細な説明については省略する。

【０１３４】

一方、Ｓ４２５において、許可された機能ではないと判断された場合（Ｓ４２５：ＮＯ）、ＭＦＰ１は、「自動認証機能」の確認を行い（Ｓ４３５）、自動認証がオンか否かを判断する（Ｓ４４０）。具体的には、自動認証機能がオンとなっている場合、先に説明し

たＳ３３０によって、その旨の設定がなされているので、Ｓ４３５では、その設定を表す情報を取得することで、制御部１１は自動認証機能がオンかどうかを確認でき、Ｓ４４０では、取得した情報に基づく判断を行う。

【０１３５】

Ｓ４４０において、自動認証がオンではないと判断された場合（Ｓ４４０：ＮＯ）、ＭＦＰ１は、利用者の要求する機能の作動を拒否して（Ｓ４４５）、図８に示す機能制御処理を終了する。すなわち、Ｓ４２５において第１の認証方法による機能制限を受けた場合で、且つ、自動認証機能がオフとなっていて第２の認証方法による認証を受けることができない場合は、それ以上、機能制限を解除する術がないので、Ｓ４４５へと進むことになる。なお、Ｓ４４５では、表示部１９に作動を拒否する旨のメッセージ等を表示する。

【０１３６】

一方、Ｓ４４０において、自動認証がオンであると判断された場合（Ｓ４４０：ＹＥＳ）、ＭＦＰ１は、利用者の要求する機能の「自動認証」可否を確認し（Ｓ４５０）、「自動認証」が可能か否かを判断する（Ｓ４５５）。

【０１３７】

「自動認証」が可能な機能か否かは、スキャナ部１２での読み取りを伴う機能か否かに基づいてあらかじめ取り決められており、例えば、ＦＡＸ送信機能であれば「自動認証」が可能、プリント機能であれば「自動認証」が不可能、といった取り決めになっている。Ｓ４５０では、その取り決めを示す情報を取得することで、制御部１１は「自動認証」が可能か不可能かを確認でき、Ｓ４５５では、取得した情報に基づいて「自動認証」が可能か否かを判断する。

【０１３８】

Ｓ４５５において、「自動認証」が不可能な機能であると判断された場合（Ｓ４５５：ＮＯ）、ＭＦＰ１は、利用者の要求する機能の作動を拒否して（Ｓ４４５）、図８に示す機能制御処理を終了する。

【０１３９】

一方、Ｓ４５５において、「自動認証」が可能な機能であると判断された場合（Ｓ４５５：ＹＥＳ）、ＭＦＰ１は、認証用画像エリアの設定を確認し（Ｓ４６０）、第２認証データを読み取るための設定変更が必要か否かを判断する（Ｓ４６５）。

【０１４０】

認証用画像エリアＡ３については、既に説明した通り、原稿の表裏いずれの面とするか、および、そのいずれかの面において原稿端部からの距離Ｌ２がどの程度か、以上が管理者によって事前に設定されているので、Ｓ４６０では、その設定を取得することで、制御部１１は認証用画像エリアを確認でき、必要があれば、スキャナ部１２を制御するためのパラメータ等をセットして、認証用画像エリアＡ３の範囲設定、範囲変更などを行う。

【０１４１】

そして、Ｓ４６５では、「利用者の要求する機能が片面読み取りで、原稿表面Ｄ１しか読み取らない設定になっていて、且つ、認証用画像エリアＡ３が原稿裏面Ｄ２に設定されている。」、または「利用者の要求する機能が片面読み取りで、原稿裏面Ｄ２しか読み取らない設定になっていて、且つ、認証用画像エリアＡ３が原稿表面Ｄ１に設定されている。」、以上の条件となっている場合に、第２認証データを読み取るための設定変更が必要と判断する。すなわち、片面読み取りの設定がなされているにもかかわらず、両面読み取りが必要となるケースが、Ｓ４６５において設定変更を要すると判断されるケースとなる。

【０１４２】

Ｓ４６５において、設定変更が必要と判断された場合（Ｓ４６５：ＹＥＳ）、ＭＦＰ１は、認証用画像エリアを読み取ることができるように読み取り設定を変更し（Ｓ４７０）、図９に示すＳ４７５へと進む。また、Ｓ４６５において、設定変更は不要と判断された場合（Ｓ４６５：ＮＯ）、ＭＦＰ１は、Ｓ４７０による読み取り設定の変更を実行することなく、図９に示すＳ４７５へと進む。以下、図９へと進んで説明を続ける。

【０１４３】
Ｓ４７５へと進むと、ＭＦＰ１は、認証用画像エリアの読み取りを実行する（Ｓ４７５）。そして、読み取ったイメージデータを分析して、第２認証データを抽出する（Ｓ４８０）。本実施形態の場合、Ｓ４８０では、読み取った画像の中から朱肉相当の色を持つ画素を検索・抽出することにより、第２認証データとなる印影の画像を切り出す。
【０１４４】
続いて、ＭＦＰ１は、第２認証データの候補となる画像の抽出に成功したか否かを判断する（Ｓ４８５）。Ｓ４８５において、抽出に成功していないと判断された場合（Ｓ４８５：ＮＯ）、図８に示すＳ４４５へと進むことになり、ＭＦＰ１は、利用者の要求する機能の作動を拒否して（Ｓ４４５）、図８に示す機能制御処理を終了する。
【０１４５】
一方、Ｓ４８５において、抽出に成功したと判断された場合（Ｓ４８５：ＹＥＳ）、ＭＦＰ１は、画像認証情報記憶部１４Ｂを参照し、Ｓ４８０で抽出した第２認証データの候補と画像認証情報記憶部１４Ｂに記憶された第２認証データとの照合を行う（Ｓ４９０）。Ｓ４９０では、公知の印鑑照合技術と同様な技術を任意に採用できるが、一例を挙げれば、照合対象となる２つの印影のうち、一方を回転させながら、両者の一致度（画素が重なる程度や共通する特徴点の有無など）を計測し、両者が同じ印鑑の印影であるか否かを判定する、といった照合方法を採用すればよい。
【０１４６】
そして、Ｓ４９０を終えたら、ＭＦＰ１は、第２の認証方法による認証が成立したか否かを判断する（Ｓ４９５）。Ｓ４９５では、Ｓ４９０による照合の結果、登録済みの印影と読み取った印影が、同じ印鑑の印影であると判定された場合に、認証が成立したと判断する。
【０１４７】
Ｓ４９５において認証が成立しないと判断された場合（Ｓ４９５：ＮＯ）、図８に示すＳ４４５へと進むことになり、ＭＦＰ１は、利用者の要求する機能の作動を拒否して（Ｓ４４５）、図８に示す機能制御処理を終了する。
【０１４８】
一方、Ｓ４９５において、認証が成立したと判断された場合（Ｓ４９５：ＹＥＳ）、ＭＦＰ１は、ユーザの切り替えを実行する（Ｓ５００）。このＳ５００では、例えば、現在ログイン中の利用者が、ユーザ名“Ｕｓｅｒ１”の利用者であっても、Ｓ４９０での照合により、ユーザ名“Ｕｓｅｒ３”に対応する印影について同一の印影である旨の照合結果が得られれば、ログイン中の利用者をユーザ名“Ｕｓｅｒ３”の利用者に切り替える処理が行われる。
【０１４９】
その上で、ＭＦＰ１は、認証ユーザ（切り替え後のユーザ）に対する機能制限設定を読み出す（Ｓ５０５）。そして、利用しようとしている機能について、ログイン中の利用者による利用が許可された機能か否かを確認し（Ｓ５１０）、許可された機能か否かを判断する（Ｓ５１５）。例えば、ユーザ名“Ｕｓｅｒ１”の場合であれば、Ｓ５１０では、要求されている機能（例えば、コピー機能）について、機能制限情報記憶部１４Ａからユーザ名“Ｕｓｅｒ１”に対応する機能制限設定が確認され、Ｓ５１５において、許可された機能か否かが判断される。
【０１５０】
Ｓ５１５において、許可された機能であると判断された場合（Ｓ５１５：ＹＥＳ）、図８に示すＳ４３０へと進むことになり、ＭＦＰ１は、利用者の要求する機能を作動させて（Ｓ４３０）、図８に示す機能制御処理を終了する。
【０１５１】
一方、Ｓ５１５において、許可された機能ではないと判断された場合（Ｓ５１５：ＮＯ）、図８に示すＳ４４５へと進むことになり、ＭＦＰ１は、利用者の要求する機能の作動を拒否して（Ｓ４４５）、図８に示す機能制御処理を終了する。

【０１５２】
なお、以上説明した実施形態において、スキャナ部１２は本発明でいう読取手段に相当する。Ｓ４３０において処理対象画像の読み取り処理を実行する制御部１１は本発明でいう処理対象画像取得手段に相当する。Ｓ４７５を実行する制御部１１は本発明でいう認証用画像取得手段に相当する。Ｓ４８０～Ｓ４９５を実行する制御部１１は本発明でいう判断手段に相当する。Ｓ４３０を実行する制御部１１は本発明でいう機能制御手段に相当する。Ｓ４６０～Ｓ４７０を実行する制御部１１は本発明でいう範囲変更手段に相当する。機能制御情報記憶部１４Ａは本発明でいう設定記憶手段に相当する。Ｓ５０５～Ｓ５１５を実行する制御部１１は利用者別制限判定手段に相当する。
【０１５３】
［効果］
以上説明した通り、上記ＭＦＰ１によれば、認証用画像が認証条件を満たす画像であった場合に、処理対象画像が処理対象とされる所定の機能を作動させることができる。そのため、上記所定の機能を作動させることができる利用者を、認証条件を満たす認証用画像を認証用画像エリアＡ３（本発明でいう第２領域に相当）に形成できる利用者だけに制限することができる。また、図２（ａ）に示すように利用者毎に利用回数を管理して、事前に取り決められた上限回数以上の利用を制限する、といったことも実現できる。
【０１５４】
したがって、認証を行うために、利用者がユーザアカウント名やパスワードを手作業で入力せざるを得なかった従来技術（すなわち、上記第１の認証方法しか利用できない技術）とは異なり、第２の認証方法を利用すれば、利用者が手作業で入力操作を行う手間を省くことができ、ＭＦＰ１の使い勝手を向上させることができる。
【０１５５】
また、上記ＭＦＰ１の場合、認証用画像は処理対象画像とは別領域（例えば、認証用画像は認証用画像エリアＡ３、処理対象画像は第１処理対象画像エリアＡ１および第２処理対象画像エリアＡ２）から読み取られるので、認証用画像と処理対象画像が同じ領域から読み取られるものとは異なり、処理対象画像の中に認証用画像が含まれてしまうことがない。
【０１５６】
したがって、例えば、処理対処画像が人手に渡るような機能（例えば、ファクシミリ送信機能など）を利用した場合であっても、認証用画像まで人手に渡ってしまうことはないので、認証用画像が第三者によって不正な認証に利用される危険性を低減することができる。
【０１５７】
また、上記ＭＦＰ１によれば、認証用画像エリアＡ３となる範囲を、例えば図３および図４に例示した通り、利用者が指定した範囲に変更できるので、認証用画像エリアＡ３の範囲が固定されているものとは異なり、利用者にとって都合の良い範囲を認証用画像エリアＡ３にすることができる。
【０１５８】
また、上記ＭＦＰ１によれば、図４（ｂ）に例示したような設定にすることで、原稿（本発明でいう読取対象物に相当）上にある表裏両面から、処理対象画像および認証用画像をそれぞれ独立に読み取ることができる。したがって、同一面内で第１領域および第２領域を重ならないように設ける場合に比べ、画像の読み取り範囲についての制約を減らすことができる。
【０１５９】
また、上記ＭＦＰ１によれば、図３（ａ）、同図（ｂ）、図４（ａ）に例示したような設定にすることで、原稿が有する表裏両面から処理対象画像を読み取って、それらの処理対象画像が処理対象とされる所定の機能を作動させることもできる。
【０１６０】
さらに、上記ＭＦＰ１によれば、図３に例示した距離Ｌ２，Ｌ３と原稿の搬送速度との

関係を最適化することで、認証用画像が認証条件を満たす画像であると判断された場合には、第１処理対象画像エリアＡ１から処理対象画像の取得を開始する一方、認証が成立しない場合には、第１処理対象画像エリアＡ１から処理対象画像の取得を中止することができる。したがって、第１処理対象画像エリアＡ１については、無駄に処理対象画像の取得を開始してしまうことがない。

【０１６１】

また、上記ＭＦＰ１によれば、図２（ａ）に例示した機能制限情報記憶部１４Ａを備えているので、複数の利用者それぞれについて、所定の機能を利用可能か否かを個別に設定することができる。

【０１６２】

また、上記ＭＦＰ１によれば、原稿の表裏両面から、処理対象画像および認証用画像を読み取る際、第１イメージセンサ１２Ａおよび第２イメージセンサ１２Ｂを並行して利用できる。したがって、単一のイメージセンサで処理対象画像および認証用画像を順に読み取る構成に比べ、迅速な読み取りが可能となる。また、原稿の表裏両面を単一のイメージセンサで読み取り可能な位置まで、原稿を原稿搬送装置によって搬送することで、両面読取機能を実現している場合に比べ、原稿搬送装置の機構も簡素化することができる。

【０１６３】

［変形例等］

以上、本発明の実施形態について説明したが、本発明は上記の具体的な一実施形態に限定されず、この他にも種々の形態で実施することができる。

【０１６４】

例えば、上記ＭＦＰ１においては、片面読取機能および両面読取機能を有するＭＦＰを例示したが、本発明は、片面読取機能のみを備えるＭＦＰにおいても採用可能である。この場合は、原稿の表面側から処理対象画像および認証用画像を読み取ることになるが、このように処理対象画像エリア（第１領域）および認証用画像エリア（第２領域）が同一面内にあれば、単一のイメージセンサで対処可能となるので、両エリアが互いに異なる面内にある場合より、スキャナ部１２の構造を簡素化することができる。

【０１６５】

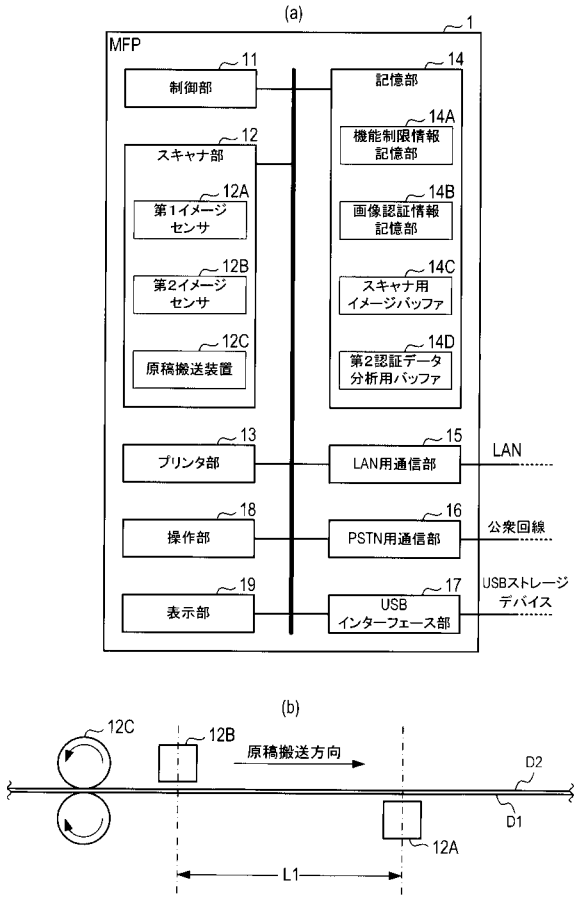
また、上記実施形態では、認証用画像として印鑑による印影を利用する例を示したが、認証用画像については、印影に限らない。具体的には、手書きの文字、印刷された文字、指紋、バーコードや二次元コードのような機械読み取り可能なコードなど、光学的に読み取り可能な画像であればなんでもよい。ただし、手書き文字の場合は、さらに手書き文字の解析を行うサイン認証技術を採用して、筆跡の特徴部を抽出するなどの対処が必要となる。また、指紋の場合も、指紋の照合を行う指紋認証技術を採用することが必要となる。さらに、バーコードや二次元コードの場合も、それらのコードを解析する技術を採用することになる。

【符号の説明】

【０１６６】

１・・・ＭＦＰ、１１・・・制御部、１２・・・スキャナ部、１２Ａ・・・第１イメージセンサ、１２Ｂ・・・第２イメージセンサ、１２Ｃ・・・原稿搬送装置、１３・・・プリンタ部、１４・・・記憶部、１４Ａ・・・機能制限情報記憶部、１４Ｂ・・・画像認証情報記憶部、１４Ｃ・・・スキャナ用イメージバッファ、１５・・・ＬＡＮ用通信部、１６・・・ＰＳＴＮ用通信部、１７・・・ＵＳＢインターフェース部、１８・・・操作部、１９・・・表示部、Ａ１・・・第１処理対象画像エリア、Ａ２・・・第２処理対象画像エリア、Ａ３・・・認証用画像エリア、Ａ４・・・未使用エリア。

【図１】



【図２】

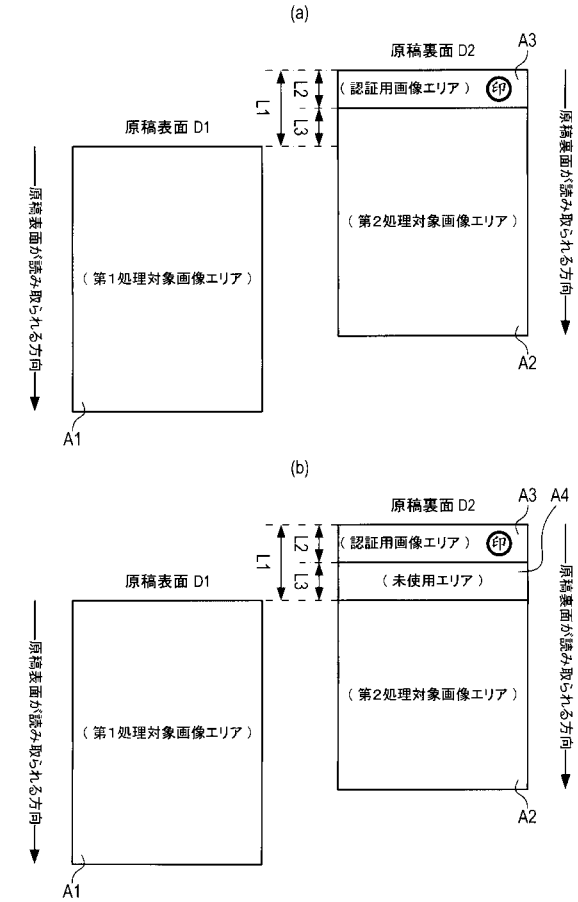
(a)

ユーザ名	第1認証データ	FAX送信	i-FAX送信	コピー	ScanToUSB
User1	1111	許可(n件迄)	許可(m件迄)	許可(n部迄)	×
User2	2222	許可(n件迄)	許可(m件迄)	許可(n部迄)	×
User3	3333	×	×	許可(n部迄)	×
⋮	⋮	⋮	⋮	⋮	⋮
Public	(None)				

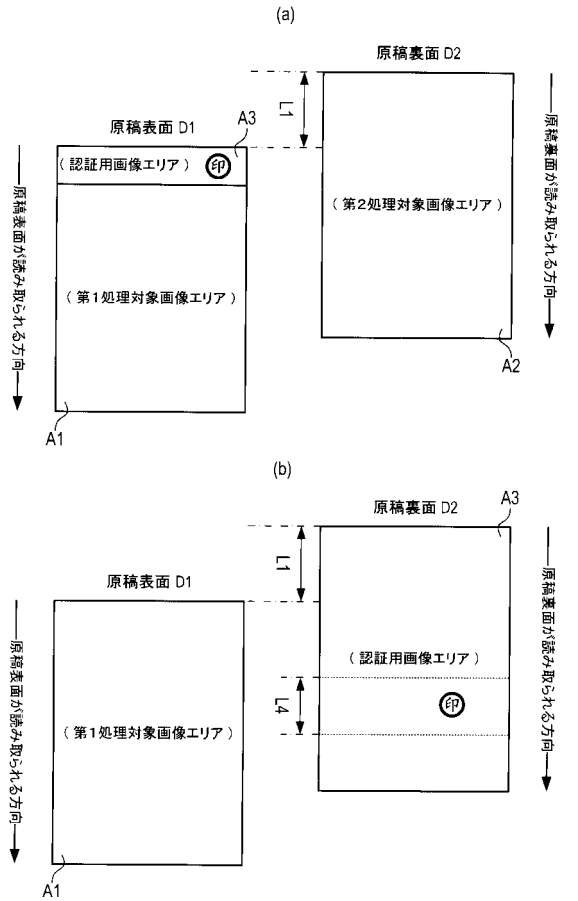
(b)

ユーザ名	第2認証データ
User1	認証用画像データ#1
User2	認証用画像データ#2
User3	認証用画像データ#3
⋮	⋮
Public	(None)

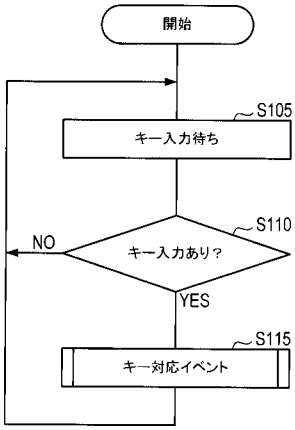
【図３】



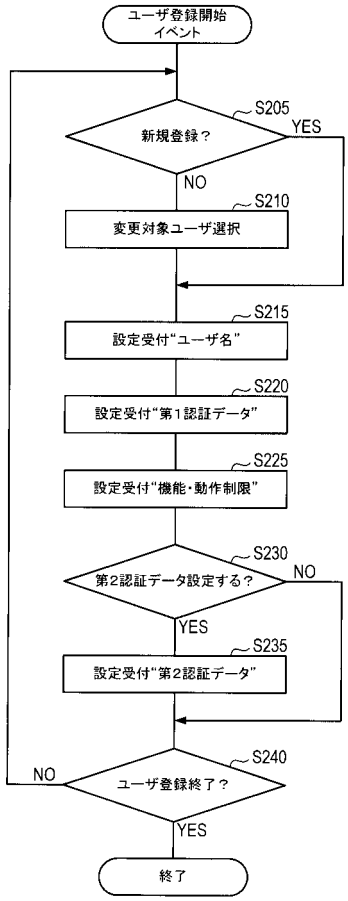
【図４】



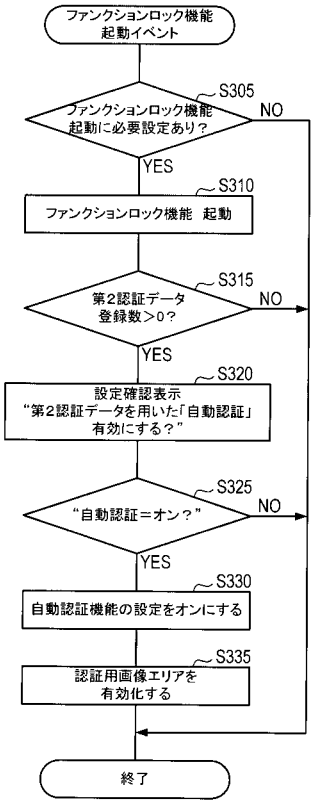
【図５】


開始
S105
キー入力待ち
S110
キー入力あり？
NO
YES
S115
キー対応イベント

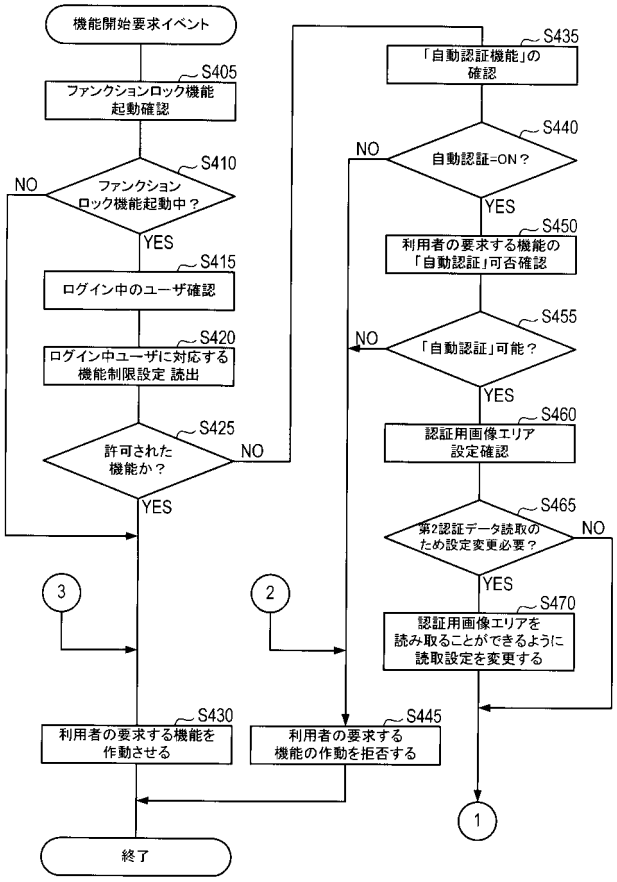
【図６】


ユーザ登録開始
イベント
S205
新規登録？
YES
NO
S210
変更対象ユーザ選択
S215
設定受付“ユーザ名”
S220
設定受付“第１認証データ”
S225
設定受付“機能・動作制限”
S230
第２認証データ設定する？
NO
YES
S235
設定受付“第２認証データ”
S240
ユーザ登録終了？
NO
YES
終了

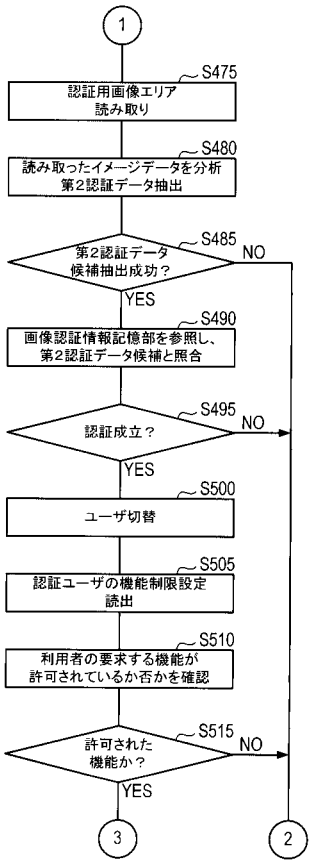
【図７】


ファンクションロック機能
起動イベント
S305
ファンクションロック機能
起動に必要設定あり？
NO
YES
S310
ファンクションロック機能 起動
S315
第２認証データ
登録数＞0？
NO
YES
S320
設定確認表示
“第２認証データを用いた「自動認証」
有効にする？”
S325
“自動認証＝オン？”
NO
YES
S330
自動認証機能の設定をオンにする
S335
認証用画像エリアを
有効化する
終了

【図８】


機能開始要求イベント
S405
ファンクションロック機能
起動確認
S410
ファンクション
ロック機能起動中？
NO
YES
S415
ログイン中のユーザ確認
S420
ログイン中ユーザに対応する
機能制限設定 読出
S425
許可された
機能か？
NO
YES
3
2
S430
利用者の要求する機能を
作動させる
S445
利用者の要求する
機能の作動を拒否する
終了
S435
「自動認証機能」の
確認
S440
自動認証=ON？
NO
YES
S450
利用者の要求する機能の
「自動認証」可否確認
S455
「自動認証」可能？
NO
YES
S460
認証用画像エリア
設定確認
S465
第２認証データ読取の
ため設定変更必要？
NO
YES
S470
認証用画像エリアを
読み取ることができるように
読取設定を変更する
1

【図９】


1
S475
認証用画像エリア
読み取り
S480
読み取ったイメージデータを分析
第2認証データ抽出
S485
第2認証データ
候補抽出成功？
NO
YES
S490
画像認証情報記憶部を参照し、
第2認証データ候補と照合
S495
認証成立？
NO
YES
S500
ユーザ切替
S505
認証ユーザの機能制限設定
読出
S510
利用者の要求する機能が
許可されているか否かを確認
S515
許可された
機能か？
NO
YES
3
2