(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2005-149237
(P2005-149237A)
(43)公開日　平成17年6月9日(2005.6.9)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 1/00	G06F	1/00	370E	2C061
B41J 29/38	B41J	29/38	Z	2H027
G03G 21/04	G06F	3/12	K	5B021
G06F 3/12	G06F	15/00	330B	5B085
G06F 15/00	H04N	1/00	C	5C062

審査請求 未請求　請求項の数 11　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2003-387171 (P2003-387171)
(22)出願日　平成15年11月17日 (2003.11.17)

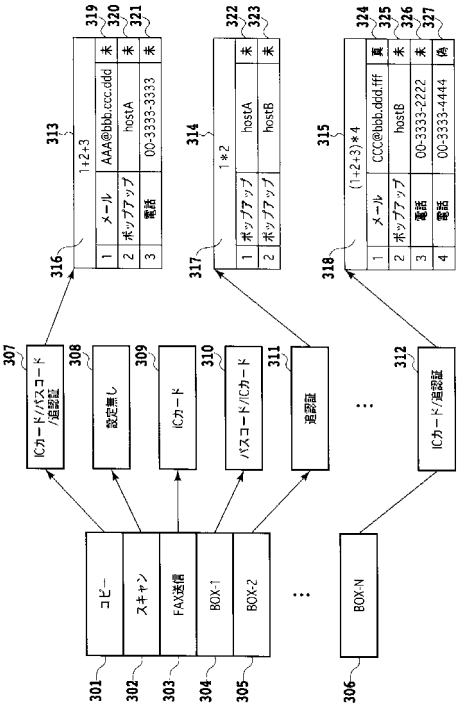
(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　一色　直広
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

Ｆターム(参考)　2C061 AP01 AP03 AP04 AP07 AQ06
CL08 HK11 HN04 HN15 HP00
2H027 EJ03 EJ04 EJ08 EJ09 EJ13
5B021 AA05 AA19 BB04 NN18
5B085 AE02 AE03 AE12 AE23

最終頁に続く

(54)【発明の名称】画像処理システム及び個人認証方法及び画像形成装置

(57)【要約】
【課題】　従来の個人認証方法に加えて、第３者に追認証を要求することにより、より強固なセキュリティを実現すること。
【解決手段】　認証方法管理テーブルの領域３０１～３０６には、各機能またはボックス使用時の個人認証方法設定の有無、第３者への追認証の有無の設定が記述された領域３０７～３０９へのリンクが記述される。例えば領域３０７の記述は、ＩＣカードおよびパスコードよる認証の他に追認証が必要であることを示す。この領域には、認証先テーブル３１３へのリンクが記述される。テーブル３１３は、認証論理式３１６と、第３者への認証要求先である認証先エントリ３１９～３２１で構成される。認証論理式３１６は、認証先エントリ３１９～３２１からどのような認証を受ければ、結果的に認証されると判断されるかを規定する。
【選択図】　図３



【特許請求の範囲】
【請求項１】
システム上の個人認証情報を外部からの個人認証情報と照合して個人認証を行う個人認証手段を備えた画像処理システムにおいて、
システムが有する複数種類の画像処理機能またはシステムが格納している複数種類の情報毎に、前記個人認証手段による前記個人認証および／または第３者による個人認証を行うかを、その認証方法とともに設定する認証方法設定手段と、
前記設定された認証方法に従って、前記個人認証手段による前記個人認証および／または前記第３者による前記個人認証を行ない、その認証結果に従って前記複数種類の画像処理機能または前記複数種類の情報毎に使用またはアクセスを許可する追認証手段と
を備えたことを特徴とする画像処理システム。
【請求項２】
前記追認証手段は、前記第３者による前記個人認証を行うことが前記認証方法設定手段により設定されているときは、その設定された方法に従って外部装置に接続して、該外部装置を介して前記第３者による前記個人認証を要求することを特徴とする請求項１に記載の画像処理システム。
【請求項３】
前記外部装置および前記第３者は複数であり、これら複数の第３者による認証結果の論理式に従ってセキュリティレベルが設定されることを特徴とする請求項２に記載の画像処理システム。
【請求項４】
前記認証方法設定手段は、前記個人認証手段による前記個人認証の認証方法を複数有しており、前記複数種類の画像処理機能または前記複数種類の情報毎に、０個以上の前記認証方法を選択して設定することを特徴とする請求項１乃至３のいずれかに記載の画像処理システム。
【請求項５】
前記認証方法設定手段は、前記第３者による前記個人認証の認証方法を複数有しており、前記複数種類の画像処理機能または前記複数種類の情報毎に、０個以上の前記認証方法を選択して設定することを特徴とする請求項１乃至４のいずれかに記載の画像処理システム。
【請求項６】
システム上の個人認証情報を外部からの個人認証情報と照合して個人認証を行う個人認証手段を備えた画像処理システムにおける個人認証方法において、
前記画像処理システムが有する複数種類の画像処理機能または該システムが格納している複数種類の情報毎に、前記個人認証手段による前記個人認証および／または第３者による個人認証を行うかを、その認証方法とともに設定する認証方法設定ステップと、
前記設定された認証方法に従って、前記個人認証手段による前記個人認証および／または前記第３者による前記個人認証を行ない、その認証結果に従って前記複数種類の画像処理機能または前記複数種類の情報毎に使用またはアクセスを許可する追認証ステップと
を備えたことを特徴とする個人認証方法。
【請求項７】
前記追認証ステップにおいて、前記第３者による前記個人認証を行うことが前記認証方法設定ステップにおいて設定されているときは、その設定された方法に従って外部装置に接続して、該外部装置を介して前記第３者による前記個人認証を要求することを特徴とする請求項６に記載の個人認証方法。
【請求項８】
前記外部装置および前記第３者は複数であり、これら複数の第３者による認証結果の論理式に従ってセキュリティレベルが設定されることを特徴とする請求項７に記載の個人認証方法。
【請求項９】

前記認証方法設定ステップにおいて、前記個人認証手段による前記個人認証の認証方法として、複数の認証方法の中から０個以上をそれぞれ前記複数種類の画像処理機能または前記複数種類の情報毎に別個に選択して設定することを特徴とする請求項６乃至８のいずれかに記載の個人認証方法。

【請求項１０】

前記認証方法設定ステップにおいて、前記第３者による前記個人認証の認証方法として、複数の認証方法の中から０個以上をそれぞれ前記複数種類の画像処理機能または前記複数種類の情報毎に別個に選択して設定することを特徴とする請求項６乃至９のいずれかに記載の個人認証方法。

【請求項１１】

個人データの照合で個人認証を行う第１の個人認証手段と、

第３者に認証を要求し要求を受けた第３者が認証を行う第３者認証要求手段と、

各機能毎又は各情報毎に、前記第３者認証要求手段で認証を行うか否かを設定する認証方法設定手段とを有することを特徴とする画像形成装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は画像処理システム及び該システムにおける個人認証方法及び画像形成装置に関する。

【背景技術】

【０００２】

近年、複写機やプリンタの機能が進化し、統合され、ＦＡＸ機能や文書サーバ機能をも取り込んだ複合機が普及している。

【０００３】

このような複合機が、例えば会社等におかれ使用されるとき、コピーカウントやプリントカウント等の課金管理や、文書サーバ上の文書を引き出ためのセキュリティ管理のために、操作者の個人認証を行う必要がある。

【０００４】

従来、このような個人認証の典型的な方法としては、個人ＩＤとパスワードによる認証方法や、ＩＤカードによる認証方法がある。

【０００５】

個人ＩＤとパスワードによる認証方法は、ユーザが機器を使用時に機器のパネルを操作して、予め発行され、機器本体上または機器の接続されているネットワーク上の認証システムに登録されている個人ＩＤとパスワードを入力することにより、前記認証システムが個人ＩＤとパスワードの照合を行い使用者の認証を行うものである。

【０００６】

また、ＩＤカードによる認証方法は、個人情報をＩＤカードに登録しておき、機器に接続されたＩＤカード読取装置にＩＤカードを挿入することにより、機器がＩＤカード上の情報をスキャンし、その情報を基に機器本体上または機器の接続されているネットワーク上の認証システムで予め登録されている情報と照合してＩＤカードの使用者を認証するものである。最近では、ＩＣカードを使用した非接触型の読取装置が登場し、ＩＤカードを挿入せずに、読取装置にかざすだけで必要な情報の読取が行えるものもある。

【０００７】

さらには、セキュリティを向上させるために、ＩＤカードとパスワードを併用して認証を行う方法もある（特許文献１）。

【０００８】

【特許文献１】特開２０００－１０４４１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】
前述のような、個人ＩＤとパスワードによる認証方法では、個人ＩＤとパスワードが盗まれ、不正に使用される場合がある。また、ＩＤカードを使用した場合でも、ＩＤカードの盗難、偽造等によって不正に入手したカードが不正使用される場合がある。さらには、パスワードとＩＤカードを併用した場合においてもパスワードとＩＤカードが盗まれてしまえば、不正アクセスが可能となってしまう。等のようなキュリティ上の問題点がある。
【００１０】
本発明は上記問題点を解決するためになされたものであり、その目的は、個人ＩＤとパスワードによる認証方法やＩＤカードによる認証方法のようなシステム上に配置された個人データとの照合のみで個人認証を行なう個人認証方法に加えて、第３者に対して追認証を要求することにより、より強固なセキュリティを実現することのできる画像処理システム及び該システムにおける個人認証方法及び画像形成装置を提供することである。
【課題を解決するための手段】
【００１１】
上記目的を達成するための本発明に係る画像処理システムは、システムが有する複数種類の画像処理機能またはシステムが格納している複数種類の情報毎に、前記個人認証手段による前記個人認証および／または第３者による個人認証を行うかを、その認証方法とともに設定する認証方法設定手段と、前記設定された認証方法に従って、前記個人認証手段による前記個人認証および／または前記第３者による前記個人認証を行ない、その認証結果に従って前記複数種類の画像処理機能または前記複数種類の情報毎に使用またはアクセスを許可する追認証手段とを備えた構成を採用した。
【００１２】
また、本発明に係る画像処理システムにおける個人認証方法は、前記画像処理システムが有する複数種類の画像処理機能または該システムが格納している複数種類の情報毎に、前記個人認証手段による前記個人認証および／または第３者による個人認証を行うかを、その認証方法とともに設定する認証方法設定ステップと、前記設定された認証方法に従って、前記個人認証手段による前記個人認証および／または前記第３者による前記個人認証を行ない、その認証結果に従って前記複数種類の画像処理機能または前記複数種類の情報毎に使用またはアクセスを許可する追認証ステップとを備えた構成を採用した。
【発明の効果】
【００１３】
かかる構成を採用した本発明によれば、個人ＩＤとパスワードによる認証方法やＩＤカードによる認証方法のようなシステム上に配置された個人認証情報の照合のみで個人認証を行なう個人認証方法に加えて、第３者に対して追認証を要求することにより、より強固なセキュリティを実現することができる効果がある。
【発明を実施するための最良の形態】
【００１４】
本発明を適用するのに好適なカラー複合画像形成装置１００の構成について図１を参照しながら説明する。なお、本発明が適用可能な画像処理システムとしては、カラー複合画像形成装置のみならず、プリンタ単体機、複写機単体機、ＦＡＸ単体機及びこれらの白黒機器の場合であっても良いことは言うまでもない。
【００１５】
図１は、本発明の適用可能な、カラー複合画像形成装置の構成を示す側断面図である。
図中、２０１はイメージスキャナ部で、原稿をスキャンし、デジタル信号処理を行う。２００はプリンタ部で、イメージスキャナ２０１読み取った画像及び、コントローラ部１０００で生成処理された画像を用紙にフルカラーで印刷出力する。
【００１６】
イメージスキャナ部２０１において、２０２は原稿圧板を兼ねたデジタイザである。デジタイザ２０２は、スキャン動作前にその上に載置された原稿２０４の所望の点を、付属のペンで押すことにより原稿上の領域を指定するのに用いられる。

【００１７】
以下、イメージスキャナ部２０１の構成及び原稿スキャン動作を説明する。
原稿台ガラス（以下「プラテン」と称す。）２０３上に原稿２０４を置き、操作部１０１０より複写又はスキャン動作のスタートを指示すると、ハロゲンランプ２０５からの光で原稿２０４が照射される。原稿からの反射光はミラー２０６、２０７に導かれ、レンズ２０８により３ラインセンサ（以下「ＣＣＤ」と称す。）２１０上に結像する。
【００１８】
ＣＣＤ２１０は光情報をレッド（Ｒ）、グリーン（Ｇ）、ブルー（Ｂ）成分に分解し、その光情報を表わす信号を増幅回路（図示せず）によって増幅した後、画像信号処理部２０９に送る。
【００１９】
なお、ハロゲンランプ２０５、ミラー２０６は速度ｖで、ミラー２０７は速度ｖ／２でラインセンサの電気的走査方向（以下、「主走査方向」と称す。）に対して垂直方向（以下、「副走査方向」と称す。）に機械的に動き、原稿全面を走査する。
【００２０】
画像信号処理部２０９では、読み取られた信号を電気的に処理し、原稿種にしたがった適切な画像処理が行われ、ビデオ信号としてコントローラ部１０００に送る。
【００２１】
コントローラ部１０００はカラー複合画像形成装置１００内の各機器の制御を統括すると共に、主に外部から通知されるＰＤＬデータ、ＦＡＸデータ、リモートプリントデータ及びイメージスキャナ部２０１から通知される画像データから、印刷するべき画像データを生成し、プリンタ部２００へマゼンタ（Ｍ）、シアン（Ｃ）、イエロー（Ｙ）、ブラック（ＢＫ）の各ビデオ信号として通知する。
【００２２】
以下、プリンタ部２００の構成及び印刷動作を説明する。
プリンタ部２００に送られたビデオ信号は、レーザドライバ２１２でレーザ駆動信号に変換され、半導体レーザ（図示せず）を駆動する。レーザ光はポリゴンミラー２１４、ｆ－θレンズ２１５、ミラー２１６を介し、帯電器２１１によって一様な電位に帯電された感光ドラム２１７上を走査して静電潜像を形成する。
【００２３】
２１９～２２２は現像器であり、マゼンタ現像器２１９、シアン現像機２２０、イエロー現像器２２１、ブラック現像器２２２より構成される。これら４つの現像器が交互に感光ドラム２１７に接し、感光ドラム２１７上に形成されたＭ、Ｃ、Ｙ、ＢＫ各色成分に対応した静電潜像を対応するトナーで現像する。
【００２４】
２２３は転写ドラムで、用紙カセット２２４または２２５より給紙された用紙を転写ドラム２２３に巻き付け、感光ドラム２１７上に現像されたトナー像を用紙に転写する。
【００２５】
このようにしてＭ、Ｃ、Ｙ、ＢＫの４色によって形成された画像が順次転写された後に、用紙は定着ユニット２２６を通過して排紙される。
【００２６】
図２はコントローラ部１０００上に構成されるカラー複合画像形成装置の制御システムを説明するブロック図である。なお本発明の機能が実行されるのであれば単体の機器であっても、複数の機器からなるシステムであっても、ＬＡＮ等のネットワークを介して処理が行われるシステムであっても本発明を適用できることは言うまでもない。
【００２７】
コントローラ部１０００において、１００１はＣＰＵで、ＲＯＭ１００３のプログラム用ＲＯＭに記憶された制御プログラム等或いはハードディスク（ＨＤ）１００６に記憶され、起動時にＲＡＭ１００２にロードされる制御プログラム等に基づいて、システムバス１００４に接続される各種のデバイスとのアクセスを総括的に制御する。

【００２８】
このＣＰＵ１００１の主な制御内容として、イメージスキャナ部２０１からのビデオ信号入力をスキャナＩ／Ｆを介して受取りＲＡＭ１００２に形成するイメージバッファへ格納を行う制御、外部ネットワーク２０００からＩ／Ｏ１００７を介して入力されるＰＤＬ等の印刷用データを解釈し、ＲＡＭ１００２に形成するイメージバッファへ画像を形成する制御、電話回線２００１から電話Ｉ／Ｆ１０１３を介して入力されるＦＡＸデータをＦＡＸ部１００９で解釈し、ＲＡＭ１００２に形成するイメージバッファへ画像を形成する制御、ＲＡＭ１００２上のイメージバッファ上の出力画像を、印刷部インタフェース１００８を介して接続されるプリント部（プリンタエンジン）２００に、出力情報としてＹ、Ｃ、Ｍ、Ｂｋの各ビデオ信号を出力する制御等がある。

【００２９】
ＲＯＭ１００３のプログラムＲＯＭは、図４、図５のフローチャートで示されるようなＣＰＵ１００１の制御プログラム等を記憶する。ＲＯＭ１００３のデータＲＯＭは、例えば紙幣や有価証券などの特定画像の特徴を抽出したリファレンスデータ等を記憶する。ＣＰＵ１００１は、Ｉ／Ｏ１０１２を介して外部ネットワーク２０００に接続されているホストコンピュータ２２２２等の外部機器との通信処理が可能である。なお、図２では外部機器とのＣＰＵ１００１による通信を外部ネットワーク２０００を介して行うとしているが、インターフェース（図示せず）を介して外部機器と直接接続して通信を行っても良いことは言うまでもない。

【００３０】
ＲＡＭ１００２は、ＣＰＵ１２の主メモリ、ワークエリア等として機能し、増設ポート（図示せず）に接続されるオプションＲＡＭによりメモリ容量を拡張することができるように構成されている。なお、ＲＡＭ１００２は、ＰＤＬ画像、ＦＡＸ画像、スキャン画像が記憶されるイメージバッファ領域、環境データ格納領域等として用いられる。前述したＨＤ１００６は、メモリコントローラ（ＭＣ）１００５によりアクセスを制御される。ＨＤ１００６は、ＰＤＬデータ解析時に使用するフォントデータ等の格納や、ＲＡＭ１００２のイメージバッファ内画像の一時保存、また各種イメージデータを格納し文書サーバとして動作するための文書ボックス等として使用される。また、前述した操作部１０１０には、操作のためのスイッチおよびＬＥＤ表示器等が配置されている。

【００３１】
文書ボックスには、作成されたＰＤＬ画像、ＦＡＸ画像、スキャン画像や外部ネットワーク２００より通知される画像等の画像が保存される。保存された画像は、操作部１０１０の操作や、外部ネットワークに接続されたホストコンピュータからの指示により、外部ネットワーク２０００上の機器への転送、プリント部２００での印刷出力、ＦＡＸ部１００９を介したＦＡＸ送信を行うことができる。

【００３２】
電話認証部１０１１は、電話Ｉ／Ｆ１０１３を介して電話回線２００１へ接続し、後述する電話認証タスクを実行する。また、電話認証部１０１１はＩ／Ｏ１０１２を介して外部ネットワークに２０００に接続し、ＩＰ電話網を使用した電話認証を行うことも可能である。

【００３３】
ＩＣカード読取部１０１４は、ＩＣカード上のデータを接触又は非接触で読取、読み取った情報をＩＣカードＩ／Ｆ１０８８を介して、ＲＡＭ１００２上に格納する。

【００３４】
このように構成されたカラー複合画像形成装置における個人認証方法について、図３乃至図５を参照して説明する。

【００３５】
図３は、カラー複合画像形成装置１００上のＲＡＭ１００２上に作成される、各機能及び文書ボックスに対する認証方法を管理する認証方法管理テーブルの一例である。

【００３６】

この管理テーブルの領域３０１～３０３には、各コピー、スキャン、ＦＡＸ送信機能を使用時の、本カラー複合画像形成装置１００上で行う個人認証方法設定の有無と、第３者への認証（追認証）の有無の設定が記述された領域３０７～３０９へのリンクが記述されている。即ち、コピー機能使用時の、個人認証方法設定の有無と、第３者への認証の有無の設定は領域３０７に記述され、領域３０１には領域３０７へのリンクが記述される。また、スキャン機能使用時の、個人認証方法設定の有無と、第３者への認証の有無の設定が領域３０８に記述され、領域３０２には領域３０８へのリンクが記述される。また、ＦＡＸ送信機能使用時の、個人認証方法設定の有無と、第３者への認証の有無の設定が領域３０９に記述され、領域３０３には領域３０９へのリンクが記述される。

【００３７】

さらに、領域３０４、３０５及び３０６には文書ボックスにアクセスする際の、本カラー複合画像形成装置１００上で行う個人認証方法設定の有無と、第３者への認証の有無の設定が記述された領域へのリンクが記述されている。即ち、ＩＤ番号１の文書ボックス（Ｂｏｘ－１）にアクセスする際の、個人認証方法設定の有無と、第３者への認証の有無の設定が領域３１０に記述され、領域３０４には領域３１０へのリンクが記述される。また、ＩＤ番号２の文書ボックス（Ｂｏｘ－２）にアクセスする際の、個人認証方法設定の有無と、第３者への認証の有無の設定が領域３１１に記述され、領域３０５には領域３１１へのリンクが記述される。

【００３８】

以下同様に、ＩＤ番号Ｎまでの文書ボックス（Ｂｏｘ－Ｎ）にアクセスする際の、個人認証方法設定の有無と、第３者への認証の有無の設定が記述された領域３１１，…３１２があり、これら領域３１１，３１２へのリンクが領域３０５から領域３０６の間に記述される。

【００３９】

本カラー複合画像形成装置１００上で行う個人認証方法には、ＩＣカードによる認証方法とパスコードによる認証方法がある。なお、本実施例では、ＩＣカードによる認証方法とパスコードによる認証方法があるとしているが（領域３０７，３０９，３１０，３１２参照）、指紋認証や虹彩認証等、他の認証方式を使用しても良いことは言うまでも無い。

【００４０】

本カラー複合画像形成装置１００上では、各機能、各文書ボックス毎にその機能を使用可能な、又は文書ボックスにアクセス可能な個人ＩＤ及びそれに付随する個人情報が管理者により登録されており、これらのデータはＨＤ１００６上に保存され、必要に応じてＲＡＭ１００２上に読み出される。また、個人ＩＤに付随する個人情報の中にはパスコードが含まれており、このパスコードは個人ＩＤを持つユーザにのみ知らされている。

【００４１】

上述したＩＣカードによる認証方法では、ＩＣカードに個人ＩＤが登録されており、ユーザがＩＣカード読取部１０１４にＩＣカードをかざすことにより、ＩＣカードに登録されている個人ＩＤが読み出され、ＲＡＭ１００２上に書き込まれる。ＣＰＵ１００１は、ＲＡＭ１００２に書き込まれた、ＩＣカードに登録された個人ＩＤと、上述の各機能毎又は各文書ボックス毎に登録されているアクセス可能な個人ＩＤと照合し、一致するものがあればその機能を使用可能、又は文書ボックスにアクセス可能として認証する。

【００４２】

また、パスコードによる認証方法は、上述のＩＣカードによる認証が行なわれた後、操作パネル１０１０上のＬＣＤにパスコードの入力を促す画面を表示し、ユーザが操作パネル１０１０を操作してパスコードを入力されるのを待つ。ユーザがパスコードを入力すると、入力されたパスコードと、ＩＣカードによって認証された個人ＩＤに付随しているパスコードの照合を行い、一致していれば認証される。

【００４３】

各機能及び各文書ボックスの、個人認証方法設定の有無と、第３者への認証の有無の設定が記述される領域３０７～３１２には、「ＩＣカード」、「パスコード」、「追認証」

のうち０個以上の設定が記述される。０個の時には設定無しとして扱われ、第１の認証及び第３者への認証が必要ないことを示す。「ＩＣカード」が記述されている時は、個人認証方法としてＩＣカードによる認証が必要であることを示す。「パスコード」が記述されている時は、個人認証方法としてパスコードによる認証が必要であることを示す。但し、「パスコード」が単独で記述されることは無く、常に「ＩＣカード」と共に記述される。「追認証」が記述されている時は、第３者への認証が必要であることを示す。

【００４４】

即ち、領域３０７は、ＩＣカードによる認証とパスコードよる認証と第３者への認証が必要であることを示し、領域３０８はいずれの認証も必要ないことを示し、領域３０９はＩＣカードによる認証のみ必要であることを示し、領域３１０はＩＣカードによる認証とパスコードによる認証が必要であることを示し、領域３１１は第３者への認証が必要であることを示し、領域３１２はＩＣカードによる認証と第３者への認証が必要であることを示す。

【００４５】

第３者への認証が必要な、個人認証方法設定の有無と、第３者への認証の有無の設定が記述される領域には、後述する第３者への認証先テーブルへのリンクが記述される。即ち、図３の例では、領域３０７、３１１及び３１２には、それぞれ第３者認証先設定テーブル３１３、３１４及び３１５へのリンクが記述されている。

【００４６】

第３者認証先設定テーブル３１３、３１４及び３１５はそれぞれ、認証論理式３１６、３１７及び３１８と、１つ以上の認証先エントリ３１９～３２７で構成されている。認証論理式３１６、３１７及び３１８は、複数の認証先からそれぞれどのような認証を受ければ、結果として認証されると判断されるかを規定する論理式で、後述の認証先ＩＤを使用して記述される。各認証論理式の「＋」は論理和を表し、「＊」は論理積を表す。論理積は論理和よりも演算の優先順位は高く、「（」と「）」で囲まれた演算の優先順位が最も高い。また、認証先ＩＤへの認証要求が認証されたならば認証論理式の認証先ＩＤの論理値は真であり、認証要求が認証されなければ偽となる。

【００４７】

各認証先エントリは、左から認証先ＩＤ、認証要求方法、認証先、認証結果が記述される。認証ＩＤは上述の認証論理式を記述するために使用される。カラー複合画像形成装置１００は認証要求方法として、電子メールによる認証要求、ポップアップ表示による認証要求と、電話による認証要求とを持っており、いずれかひとつが認証要求方法として記述される。各認証要求については後述する。

【００４８】

認証先には、上述の認証要求方法による認証先が、各認証要求方法に適合した内容で記述される。即ち、電子メールによる認証要求の認証先には電子メールアドレスが、ポップアップ表示による認証要求の認証先には、ポップアップを表示するホスト名又はＩＰアドレスが、電話による認証要求の認証先には、電話番号又は短縮ダイヤル番号が、それぞれ記述される。認証結果には、上述の認証要求よって要求された認証先での認証結果が後述する各認証タスクにより登録される。

【００４９】

例えば第３者認証先設定テーブル３１５は、ＩＤ番号Ｎの文書ボックスへアクセスする際に行なわれる第３者への認証の認証先が記述されており、認証先ＩＤが１の「ＣＣＣ@ｂｂｂ．ｄｄｄ．ｆｆｆ」へ電子メールによる認証要求を行い、認証先ＩＤが２の「ｈｏｓｔＢ」へポップアップによる認証要求を行い、認証先ＩＤが３の「００－３３３３－２２２２」へ電話による認証要求を行い、認証先ＩＤが４の「００－３３３３－４４４４」へ認証要求を行う。そして、認証論理式３１８に従えば、認証先ＩＤが１又は２又は３の認証要求の少なくとも１つが認証され、且つ認証先ＩＤが４の認証要求が認証されたときのみ、第３者への認証要求が認証されたと判断されることになる。

【００５０】

ところで、領域３０７～３１２の、個人認証方法設定の有無と、第３者への認証の有無の登録は、管理者又は文書ボックス作成者により、操作部１０１０又は、外部ネットワーク２０００に接続された機器から行うことができる。さらに、個人認証方法設定の有無と、第３者への認証の有無の設定領域に第３者への認証要求が必要であると設定したときには、第３者認証設定テーブルが作成され、設定者、作成された第３者認証テーブルの認証論理式と１つ以上の認証先エントリを登録しなければならない。

【００５１】

ここで、カラー複合画像形成装置１００が図３の認証方法管理テーブルに登録された内容に基づいて認証を行い、操作者により指定された機能を実行する動作を図４のフローチャートに従って説明する。

【００５２】

カラー複合画像形成装置１００は、電源が投入され各種初期化が終了すると（ステップＳ４０１）ステップＳ４０２で操作パネル１０１０から、操作者が操作が行なわれるのを待つ。ステップＳ４０３で、操作者が操作パネル１０１０を操作し、コピー動作又はスキャン動作又はＦＡＸ送信動作又は文書ボックスへのアクセス動作が指定されると、ステップＳ４０４でいずれの動作が指定されたか判断し、認証方法管理テーブルを参照して指定動作の認証方法を読み出す。即ち、例えばコピー動作が指定された場合は領域３０１に記述されたリンクをたどり、領域３０７に登録されている設定内容を読み出す。

【００５３】

ステップＳ４０５では、ステップＳ４０４で読み出した認証方法に、「ＩＣカード」が記述されていれば、ステップＳ４０６へ進み、記述されていなければステップＳ４０９へ進む。

【００５４】

ステップＳ４０６ではＩＣカードによる認証方法を行い、ステップＳ４０７へ進む。

【００５５】

ステップＳ４０７では、ステップＳ４０６で行ったＩＣカードによる認証方法により認証されたか否かを判断し、認証されていればステップＳ４０９へ進み、認証されていなければステップＳ４０８へ進んで認証不可を表示する。

【００５６】

ステップＳ４０９では、ステップＳ４０４で読み出した認証方法に、「パスコード」が記述されていれば、ステップＳ４１０へ進み、記述されていなければステップＳ４１２へ進む。

【００５７】

ステップＳ４１０ではパスコードによる認証方法を行い、ステップＳ４１１へ進む。

【００５８】

ステップＳ４１１では、ステップＳ４１０で行ったパスコードによる認証方法により認証されたか否かを判断し、認証されていればステップＳ４１２へ進み、認証されていなければステップＳ４０８へ進んで認証不可を表示する。

【００５９】

ステップＳ４１２では、ステップＳ４０４で読み出した認証方法に、「追認証」が記述されていなければステップＳ４１５へ進み、記述されていればステップＳ４１３へ進む。

【００６０】

ステップＳ４１３では、後述する図５の追認証ルーチンにより、第３者への認証を行い、ステップＳ４１４へ進む。追認証ルーチンを呼び出すときには、ステップＳ４０４で読み出している領域に記述されている第３者認証先テーブルへのリンクをたどり、その内容が追認証ルーチンに入力として渡される。即ち、例えば、ステップＳ４０３でコピー動作が指定されている時には、第３者認証先設定テーブル３１３の内容が追認証ルーチンへの入力として渡される。

【００６１】

ステップＳ４１４では、ステップＳ４１３で行った第３者への認証により認証されたか

否かを判断し、認証されていればステップＳ４１５へ進み、認証されていなければステップＳ４０８へ進んで認証不可を表示する。

【００６２】

ステップＳ４１５には、すべての指定された認証方法で認証された場合（認証論理式３１３が成立したとき）のみ到達し、ステップＳ４０３で指定された動作を行った後、ステップＳ４０２へ戻る。

【００６３】

ステップＳ４０８には、指定された認証方法のいずれかで認証されなかった場合に到達し、操作パネル１０１０上のＬＣＤに、認証がされなかった旨を表示して、操作者に認証されなかったことを伝え、ステップＳ４０２へ戻る。なお、認証がされなかった旨を表示するときに、合わせて、どの認証方法にて認証されなかったのかを表示してもよい。さらに、第３者への認証によって認証されなかった場合には、認証されなかった認証先を表示してもよい。

【００６４】

続いてステップＳ４１３で実行される追認証ルーチンの動作を図５のフローチャートにしたがって説明する。

【００６５】

追認証ルーチンでは、入力として渡された第３者認証テーブルの内容に従い、この第３者認証テーブルに登録されている各認証先エントリの認証先へ指定された認証要求方法で認証要求を行う。

【００６６】

追認証ルーチンが実行されると（ステップＳ５０１）、入力された第３者認証テーブルに登録されている認証エントリに登録されているすべての認証先へ認証要求を行うまで、ステップＳ５０２～Ｓ５０９を繰り返す。

【００６７】

ステップＳ５０２では、認証先エントリをひとつ読み出し、ステップＳ５０３へ進む。

【００６８】

ステップＳ５０３では、ステップＳ５０２で読み出した認証先エントリ認証要求方法が電子メールによる要求であれば、ステップＳ５０４へ進み、異なる認証方法が指定されている場合はステップＳ５０５へ進む。

【００６９】

ステップＳ５０４では、ステップＳ５０２で読み出した認証先エントリの認証先ＩＤと認証先に登録されている電子メールアドレスを読み出し、読み出した認証先ＩＤと電子メールアドレスを入力として、電子メール承認タスクを起動する。

【００７０】

電子メール承認タスクは、入力された認証先ＩＤを持つ認証先エントリの認証結果欄に認証結果がまだ決定していないことを示す「未」を記述した後、ＩＣカードによる認証方法によって使用された個人ＩＤより、使用者を判別し、この使用者がステップＳ４０３で指定した動作を行うための認証を要求している旨のメール文書を作成し、入力された電子メールアドレスに送信する。なお、ＩＣカードによる認証が行なわれていない場合は、使用者不明とする。

【００７１】

認証要求の電子メールを受け取った認証者は、認証する又は認証しないを記述したメールを返信メールとして返信することにより、認証の可否をカラー複合画像形成装置１００へ通知する。認証可否を通知された電子メール認証タスクは、認証されていれば入力された認証先ＩＤを持つ認証先エントリの認証結果欄に「真」を記述し、認証されていなければ入力された認証先ＩＤを持つ認証先エントリの認証結果欄に「偽」を記述する。

【００７２】

ステップＳ５０５では、ステップＳ５０２で読み出した認証先エントリ認証要求方法がポップアップによる要求であれば、ステップＳ５０６へ進み、異なる認証方法が指定され

ている場合はステップＳ５０７へ進む。

【００７３】

ステップＳ５０６では、ステップＳ５０２で読み出した認証先エントリの認証先ＩＤと認証先に登録されているホスト名又はＩＰアドレスを読み出し、読み出した認証先ＩＤとホストを入力として、ポップアップ認証タスクを起動する。

【００７４】

ポップアップ認証タスクは、入力された認証先ＩＤを持つ認証先エントリの認証結果欄に認証結果がまだ決定していないことを示す「未」を記述した後、ＩＣカードによる認証方法によって使用された個人ＩＤより、使用者を判別し、入力されたホストのディスプレイに、この使用者がステップＳ４０３で指定した動作を行うための認証を要求している旨のポップアップ画面を表示する。なお、ＩＣカードによる認証が行なわれていない場合は、使用者不明とする。

【００７５】

認証要求のポップアップ画面の表示されたホストの使用者は、ポップアップ画面上にある、認証ボタンまたは認証しないボタンをクリックすることにより、認証の可否をカラー複合画像形成装置１００へ通知する。認証可否を通知されたポップアップ認証タスクは、認証されていれば入力された認証先ＩＤを持つ認証先エントリの認証結果欄に「真」を記述し、認証されていなければ入力された認証先ＩＤを持つ認証先エントリの認証結果欄に「偽」を記述する。

【００７６】

ステップＳ５０７では、ステップＳ５０２で読み出した認証先エントリ認証要求方法がポップアップによる要求であれば、ステップＳ５０８へ進み、異なる認証方法が指定されている場合はステップＳ５０９へ進む。

【００７７】

ステップＳ５０８では、ステップＳ５０２で読み出した認証先エントリの認証先ＩＤと認証先に登録されている電話番号を読み出し、読み出した認証先ＩＤと電話番号を入力として、電話認証タスクを起動する。

【００７８】

電話認証タスクは、入力された認証先ＩＤを持つ認証先エントリの認証結果欄に認証結果がまだ決定していないことを示す「未」を記述した後、電話認証部１０１１で実行される。ＩＣカードによる認証方法によって使用された個人ＩＤより、使用者を判別し、電話Ｉ／Ｆ１０１３を介して、入力された電話番号に電話をかけ、電話を受けた人物に、この使用者がステップＳ４０３で指定した動作を行うための認証を要求している旨を音声で伝える。なお、ＩＣカードによる認証が行なわれていない場合は、使用者不明とする。

【００７９】

さらに、続けて認証要求に対して認証するなら「１」を、認証しないなら「２」をダイヤルするように伝え、認証者がダイヤルするまで待つ。電話を受けた認証者は、指定された番号をダイヤルすることにより認証の可否をカラー複合画像形成装置１００へ通知する。認証可否を通知された電話認証タスクは、認証されていれば入力された認証先ＩＤを持つ認証先エントリの認証結果欄に「真」を記述し、認証されていなければ入力された認証先ＩＤを持つ認証先エントリの認証結果欄に「偽」を記述する。

【００８０】

ステップＳ５０９では、入力として渡された第３者認証先テーブルに、認証要求の行なわれていない認証先エントリがあれば、ステップＳ５０２で読み出す認証先エントリ先を１つ進め、ステップＳ５０２へ戻って、ここまでの動作を繰り返す。すべての認証先エントリの認証先へ認証要求が行なわれていれば、ステップＳ５１０へ進む。

【００８１】

ステップＳ５１０では、入力された第３者認証先テーブルの認証論理式を参照し、この認証論理式の結果が出るまで、ステップＳ５０４、Ｓ５０６及びＳ５０８で起動した各認証タスクからの認証結果を待つ。各認証先エントリの認証結果の欄が、「未」であれば、

その認証先エントリの認証要求結果はまだ出ていないことを示し、「真」又は「偽」であれば既に認証の可否が通知されていることを示しているので、既に認証の可否が通知している結果を使用して認証論理式を評価する。

【００８２】

認証結果の出ていない認証先エントリがあった場合でも、認証論理式の評価結果が出次第、ステップＳ５１１へ進む。例えば、本追認証タスクに入力された第３者認証先テーブルが３１５で示すテーブルであった場合、認証論理式３１８は（１＋２＋３）＊４であるため、認証ＩＤが４の認証先エントリの認証結果が「偽」であれば、（１＋２＋３）の演算結果に関係なく認証しない旨の判断をすることができる。そこで、認証ＩＤが４の認証先エントリの認証結果に「偽」が記述された場合、認証ＩＤが１から３の認証先エントリの認証結果を待つことなく、本追認証ルーチンの認証結果を認証しないと判断する。

【００８３】

一方で、認証ＩＤが４の認証先エントリの認証結果に「真」が記述された場合は、認証ＩＤ１から３の認証先エントリの認証結果が出て、「真」又は「偽」が記述されるまで待った後に、認証論理式３１８を演算して判断する。つまり、認証先ＩＤが４の認証先エントリの認証結果を、他の認証先ＩＤの認証先エントリの認証結果よりも重視して判断している。

【００８４】

第３者認証先テーブルが３１３で示すテーブルであった場合、認証論理式３１６は（１＋２＋３）であるため、認証ＩＤ１から３の認証先エントリの認証結果が出た後に認証論理式３１６を演算して判断する必要がある。また、第３者認証先テーブルが３１４で示すテーブルであった場合、認証論理式３１７は論理積（１＊２）であるため、認証ＩＤが１および２の認証先エントリのいずれかの認証結果が「偽」であれば、残りの認証先エントリの認証結果に関係なく認証しない旨の判断をすることができる。

【００８５】

このように、認証論理式が論理積を含んで表される場合には、論理和のみで表される場合よりもセキュリティレベルが高い、したがって、認証論理式の設定如何によりセキュリティレベルを設定することができる。例えば、論理積をとる対象の認証先エントリの数を増やせば増やすほど、セキュリティレベルを高レベルとすることができる。

【００８６】

ステップＳ５１１では、認証結果に「未」が記述されている認証先エントリの認証要求を行っている各タスクに終了通知を行い、本追認証ルーチンを終了する。このとき、終了通知を受けた各認証タスクは、認証先に認証の必要がなくなったことを通知した後、終了する。

【００８７】

以上、本実施例によれば、機能毎、文書ボックス毎の認証方法として、本カラー複合画像形成装置１００上で行う個人認証方法であるＩＣカードによる認証及びパスコードによる従来の認証に加えて、複数の第３者への認証を設定することができ、認証論理式で設定したセキュリティレベルに応じてより強固なセキュリティを実現することができる。

【図面の簡単な説明】

【００８８】

【図１】本発明に係る画像処理システムの一例であるカラー複合画像形成装置の構成を示す図である。

【図２】図１のカラー複合画像形成装置が備えるコントローラ部の構成を示すブロック図である。

【図３】図１のカラー複合画像形成装置が備えるＲＡＭに作成される認証方法管理テーブルの一例を説明する説明図である。

【図４】図１のカラー複合画像形成装置により本発明に係る個人認証方法を実施したときの同カラー複合画像形成装置の動作を示すフローチャートである。

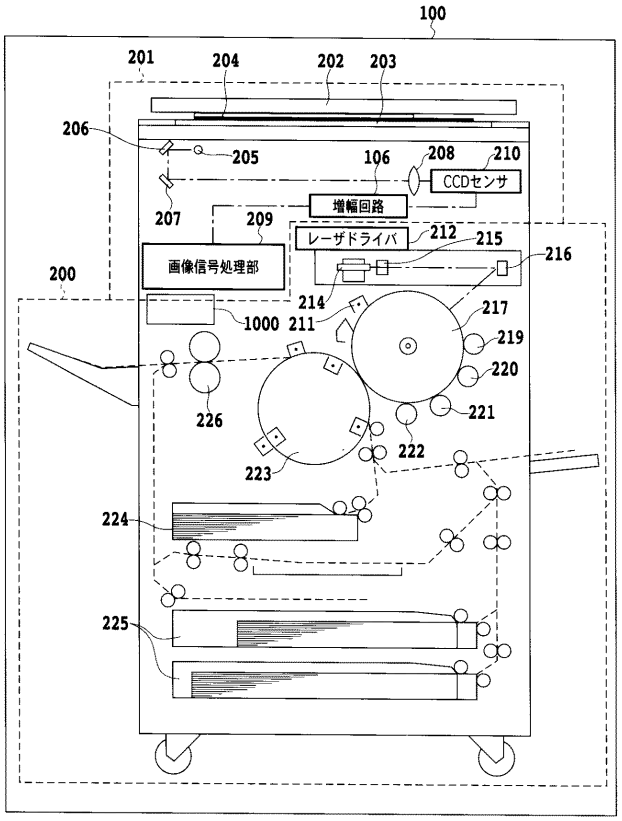
【図５】図４中の追認証ルーチンの動作を示すフローチャートである。

【符号の説明】

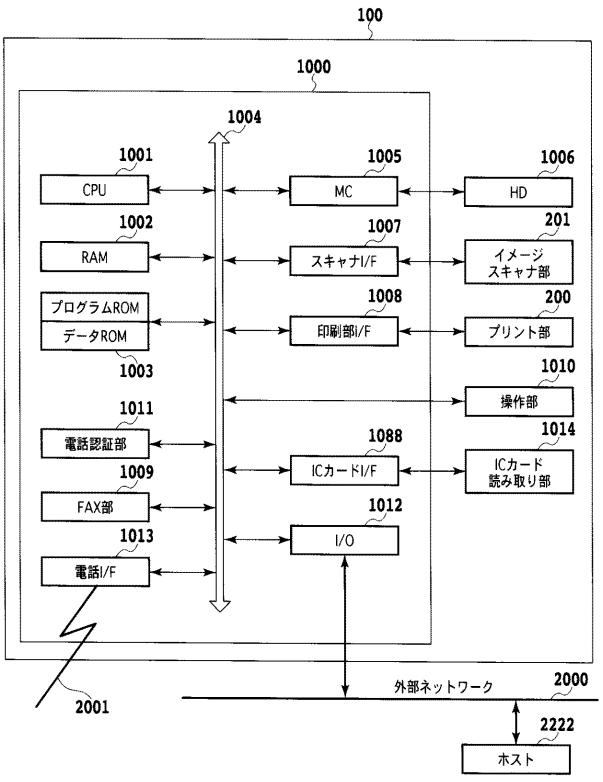
【００８９】

２００　プリンタ部
２０１　イメージスキャナ部
１０００　コントローラ部
１００１　ＣＰＵ
１００２　ＲＡＭ
１０１１　電話認証部
１０１４　ＩＣカード読取部
２０００　外部ネットワーク

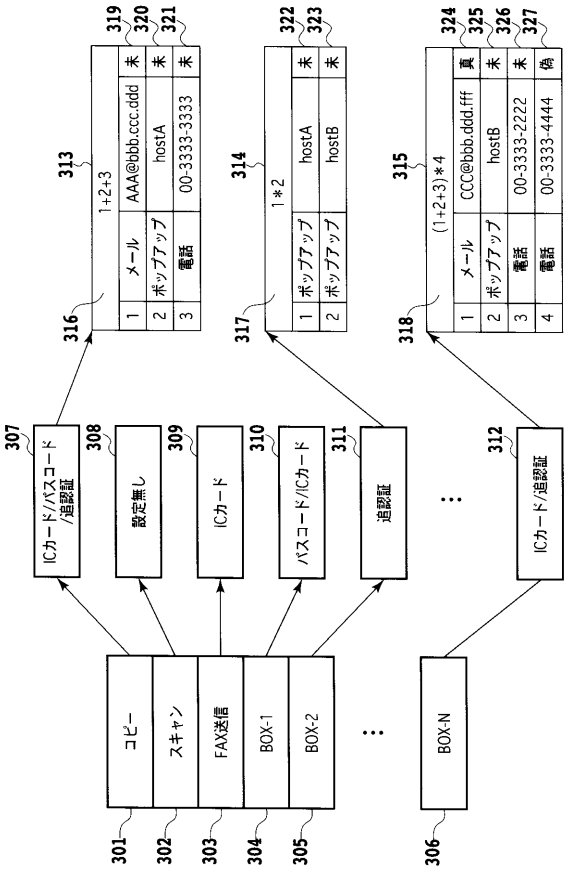
【図１】



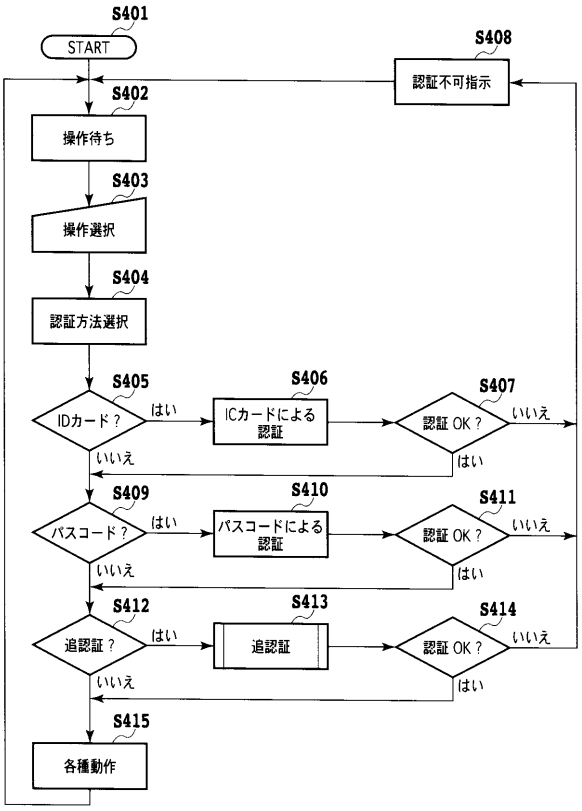
【図２】



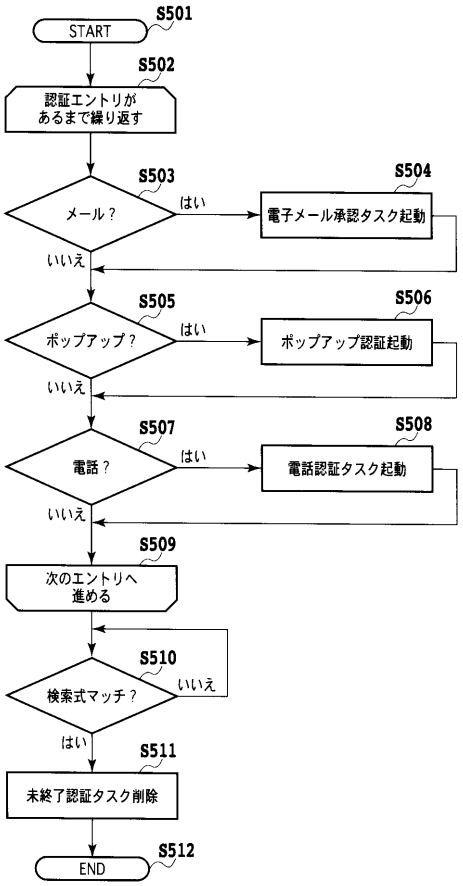
【図３】


319
320
321
322
323
324
325
326
327
313
314
315
1+2+3
1*2
(1+2+3)*4
未
未
未
未
未
真
未
未
偽
1
2
3
1
2
1
2
3
4
メール
ポップアップ
電話
ポップアップ
ポップアップ
メール
ポップアップ
電話
電話
AAA@bbb.ccc.ddd
hostA
00-3333-3333
hostA
hostB
CCC@bbb.ddd.fff
hostB
00-3333-2222
00-3333-4444
316
317
318
307
308
309
310
311
312
ICカード/パスコード/追認証
設定無し
ICカード
パスコード/ICカード
追認証
ICカード/追認証
コピー
スキャン
FAX送信
BOX-1
BOX-2
BOX-N
301
302
303
304
305
306

【図４】


S401
START
S402
操作待ち
S403
操作選択
S404
認証方法選択
S405
IDカード？
はい
いいえ
S406
ICカードによる認証
S407
認証 OK？
いいえ
はい
S408
認証不可指示
S409
パスコード？
はい
いいえ
S410
パスコードによる認証
S411
認証 OK？
いいえ
はい
S412
追認証？
はい
いいえ
S413
追認証
S414
認証 OK？
いいえ
はい
S415
各種動作

【図５】


S501
START
S502
認証エントリがあるまで繰り返す
S503
メール？
はい
いいえ
S504
電子メール承認タスク起動
S505
ポップアップ？
はい
いいえ
S506
ポップアップ認証起動
S507
電話？
はい
いいえ
S508
電話認証タスク起動
S509
次のエントリへ進める
S510
検索式マッチ？
いいえ
はい
S511
未終了認証タスク削除
S512
END

フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
H04N 1/00	G03G 21/00 390	

Fターム(参考) 5C062 AA02 AA05 AA13 AA35 AB17 AB38 AC02 AF12