(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4845902号
(P4845902)
(45)発行日　平成23年12月28日(2011.12.28)　(24)登録日　平成23年10月21日(2011.10.21)

(51)Int.Cl.　　F I
H04N 1/44 (2006.01)　　H04N 1/44
H04N 1/00 (2006.01)　　H04N 1/00　C

請求項の数 6　(全 14 頁)

(21)出願番号　特願2008-15502(P2008-15502)
(22)出願日　平成20年1月25日(2008.1.25)
(65)公開番号　特開2009-177630(P2009-177630A)
(43)公開日　平成21年8月6日(2009.8.6)
審査請求日　平成22年6月30日(2010.6.30)

(73)特許権者　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　110001243
特許業務法人　谷・阿部特許事務所
(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　三留　綾
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

審査官　渡辺　努

最終頁に続く

(54)【発明の名称】画像処理装置、画像処理方法、プログラム、および記憶媒体

(57)【特許請求の範囲】
【請求項１】
原稿のスキャンにより得られた原稿画像内の２次元コードをデコードして元情報を得るデコード手段と、
前記デコード手段で得られた元情報の中に、前記原稿画像を他の装置に出力するために特定のパスワードの入力が必要であることを示す情報が含まれているかどうか判断する判断手段と、
パスワードの入力要求を表示する表示手段と、
前記原稿画像を電子ファイルに変換して他の装置に出力する制御手段と、を備え、
前記制御手段は、
前記判断手段で元情報の中に前記原稿画像を他の装置に出力するために特定のパスワードの入力が必要であることを示す情報が含まれていると判断された場合に、前記表示手段にパスワードの入力要求を表示し、
前記表示手段でのパスワードの入力要求の表示後に、前記特定のパスワードが入力された場合に、前記原稿画像を、閲覧のために前記特定のパスワードの入力を要とする電子ファイルに変換して前記他の装置に出力し、
前記表示手段でのパスワードの入力要求の表示後に、前記特定のパスワードが入力されなかった場合に、前記原稿画像を前記他の装置に出力せず、
前記判断手段で元情報の中に前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれていないと判断された場合に、前記原稿画像を、

閲覧のためにパスワードの入力を要しない電子ファイルに変換して前記他の装置に出力する
ことを特徴とする画像処理装置。
【請求項２】
原稿のスキャンにより得られた原稿画像内の２次元コードをデコードして元情報を得るデコード手段と、
前記デコード手段で得られた元情報の中に、前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれているかどうか判断する判断手段と、
前記判断手段で元情報の中に前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれていると判断された場合に、前記パスワードの入力要求を表示する表示手段と、
前記原稿画像を電子ファイルに変換する変換手段と、
前記変換手段での変換により得られた電子ファイルを他の装置に出力する出力手段と、
を備え、
前記変換手段は、
前記パスワードの入力要求に対して前記パスワードの入力が行われた場合には、前記原稿画像を、閲覧のために前記パスワードの入力を要しない電子ファイルに変換し、
前記パスワードの入力要求に対して前記パスワードの入力が行われなかった場合には、前記原稿画像を、閲覧のために前記パスワードの入力を要する電子ファイルに変換する
ことを特徴とする画像処理装置。
【請求項３】
原稿のスキャンにより得られた原稿画像内の２次元コードをデコードして元情報を得るデコードステップと、
前記デコードステップで得られた元情報の中に、前記原稿画像を他の装置に出力するために特定のパスワードの入力が必要であることを示す情報が含まれているかどうか判断する判断ステップと、
パスワードの入力要求を表示する表示ステップと、
前記原稿画像を電子ファイルに変換して他の装置に出力する制御ステップと、
を含み、
前記制御ステップは、
前記判断ステップで元情報の中に前記原稿画像を他の装置に出力するために特定のパスワードの入力が必要であることを示す情報が含まれていると判断された場合に、前記表示ステップでパスワードの入力要求を表示し、
前記表示ステップでのパスワードの入力要求の表示後に、前記特定のパスワードが入力された場合に、前記原稿画像を、閲覧のために前記特定のパスワードの入力を要とする電子ファイルに変換して前記他の装置に出力し、
前記表示ステップでのパスワードの入力要求の表示後に、前記特定のパスワードが入力されなかった場合に、前記原稿画像を前記他の装置に出力せず、
前記判断ステップで元情報の中に前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれていないと判断された場合に、前記原稿画像を、閲覧のためにパスワードの入力を要しない電子ファイルに変換して前記他の装置に出力する
ことを特徴とする画像処理方法。
【請求項４】
原稿のスキャンにより得られた原稿画像内の２次元コードをデコードして元情報を得るデコードステップと、
前記デコードステップで得られた元情報の中に、前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれているかどうか判断する判断ステップと、

前記判断ステップで元情報の中に前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれていると判断された場合に、前記パスワードの入力要求を表示する表示ステップと、
前記原稿画像を電子ファイルに変換する変換ステップと、
前記変換ステップでの変換により得られた電子ファイルを他の装置に出力する出力ステップと、
を含み、
前記変換ステップは、
前記パスワードの入力要求に対して前記パスワードの入力が行われた場合には、前記原稿画像を、閲覧のために前記パスワードの入力を要しない電子ファイルに変換し、
前記パスワードの入力要求に対して前記パスワードの入力が行われなかった場合には、前記原稿画像を、閲覧のために前記パスワードの入力を要する電子ファイルに変換することを特徴とする画像処理方法。
【請求項５】
請求項３又は請求項４に記載の画像処理方法をコンピュータに実行させるためのプログラム。
【請求項６】
請求項５に記載のプログラムを記憶したコンピュータで読み取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証情報が含まれる原稿を処理する画像処理装置、画像処理方法、プログラム、および記憶媒体に関する。
【背景技術】
【０００２】
特許文献１は、微小スペースに多量のデータを記録することができる二次元コードの一種であるＱＲコード（商標）について開示している。
【０００３】
特許文献２は、複製動作を制御することができるグリフコード（商標）について開示している。
【０００４】
【特許文献１】特開平１０－３１２４４７号公報
【特許文献２】特開２００３－２８０４６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
特許文献１や特許文献２に開示されている技術を用いることによって、カードや原稿などの紙媒体に、電子的な制御を行うための情報を持たせることが可能となり、紙媒体に対するアクセス制御が実現できる。
【０００６】
特許文献２に開示されている技術をＭＦＰ（複合機）に適用すると、ＭＦＰは、スキャン時に原稿上の２次元コードを検知し、それをデコードすることによって原稿に対する認証情報を得る。その認証結果に基づいて、ＭＦＰは、上記原稿を扱う処理の継続や中止を制御することができる。
【０００７】
ＭＦＰが、処理の継続が可能と判断した場合、ＭＦＰに搭載されている送信機能を用いることによって、原稿を電子データに変換したり、ファイルサーバや、ＰＣ上に送信したりすることができる。
【０００８】
そのような場合、ＭＦＰが生成した電子データ上には原稿が持っていた認証情報が、２

次元コードという「画像」で保持されることになる。

【０００９】

そのため、これらの電子データは、ＭＦＰが送信した先のファイルサーバやＰＣ上で認証制御を行うことができなくなり、認証情報を持っていた原稿であっても、閲覧や複製が自由に行われてしまうという危険性がある。

【００１０】

また、上記のようなフローで電子データにも認証制御を適用する場合には、再び画像を解析しなければならない。

【課題を解決するための手段】

【００１１】

上記課題を解決するために、本発明に係る画像処理装置は、原稿のスキャンにより得られた原稿画像内の２次元コードをデコードして元情報を得るデコード手段と、前記デコード手段で得られた元情報の中に、前記原稿画像を他の装置に出力するために特定のパスワードの入力が必要であることを示す情報が含まれているかどうか判断する判断手段と、パスワードの入力要求を表示する表示手段と、前記原稿画像を電子ファイルに変換して他の装置に出力する制御手段と、を備え、前記制御手段は、前記判断手段で元情報の中に前記原稿画像を他の装置に出力するために特定のパスワードの入力が必要であることを示す情報が含まれていると判断された場合に、前記表示手段にパスワードの入力要求を表示し、前記表示手段でのパスワードの入力要求の表示後に、前記特定のパスワードが入力された場合に、前記原稿画像を、閲覧のために前記特定のパスワードの入力を要とする電子ファイルに変換して前記他の装置に出力し、前記表示手段でのパスワードの入力要求の表示後に、前記特定のパスワードが入力されなかった場合に、前記原稿画像を前記他の装置に出力せず、前記判断手段で元情報の中に前記原稿画像を他の装置に出力するためにパスワードの入力が必要であることを示す情報が含まれていないと判断された場合に、前記原稿画像を、閲覧のためにパスワードの入力を要しない電子ファイルに変換して前記他の装置に出力することを特徴とする。

【発明の効果】

【００１２】

ＭＦＰの送信機能を用いて認証情報が含まれる原稿をスキャンし、電子データを生成して、ファイルサーバやＰＣ上に送信する場合、原稿に設定されていた認証情報を、電子データにも適用することできる。これにより、ＭＦＰによりスキャンされた原稿上の情報に対して厳密なセキュリティを確保することができる。

【発明を実施するための最良の形態】

【００１３】

以下では、図面を参照して本発明を実施するための最良の形態について説明する。

（実施形態１）

図１は、実施形態１のシステム図である。実施形態１のシステムには、少なくともＭＦＰ１３１とクライアントコンピュータ１１１とが含まれている。

【００１４】

ＭＦＰ１３１は、スキャン、プリント、コピー、送信が可能となっている。ＭＦＰ１３１のその他の機能については、以下の実施形態に関する説明により明らかにされる。

【００１５】

クライアントコンピュータ１１１は、ネッワーク１０１を介して、ＭＦＰ１３１の送信したデータを、受信し保存することができる。また、クライアントコンピュータ１１１は、保存したデータを表示することができる。クライアントコンピュータ１１１のその他の機能については実施形態に関する説明により明らかにされる。

【００１６】

また、以下で説明する実施形態において、図１に示されているように、ネットワーク１０１に、複数のクライアントコンピュータ１１１、１１２、複数のＭＦＰ１３１、１３２、およびファイルサーバ１２１が接続されていても良い。

【００１７】
＜実施形態１における処理フロー（図２）＞
次に、実施形態１における処理フロー（図２）について説明を行う。
【００１８】
図１のＭＦＰ１１１、１１２は、操作画面上に表示された「送信モード」「印刷モード」等の選択をユーザから受付けた上で、ＭＦＰの操作画面上に表示されたスタートボタンの選択をユーザから受付けることができる。
【００１９】
図２は、ＭＦＰの操作画面上に表示されたスタートボタンの選択をユーザから受付けると開始する処理のフローチャートを示している。また、図２に示されているフローチャートにおける各ステップの処理は、ＭＦＰ内のＣＰＵにより統括的に制御される。
【００２０】
ステップＳ２００１で、ＭＦＰは、原稿台の原稿をスキャンし、電気信号としての原稿画像を生成する。
【００２１】
次に、ステップＳ２００２で、ＭＦＰは、原稿画像から２次元コードの存在領域を検知する。
【００２２】
次に、ステップＳ２００３で、ＭＦＰは、ステップＳ２００２で検知された２次元コードをデコードし、ステップＳ２００４に処理が進む。
【００２３】
なお、ステップＳ２００２やステップＳ２００３で２次元コードの検知やデコードができなかった場合には、適宜、ＭＦＰは、エラー表示を操作画面上に行う。
【００２４】
ここで、本発明に係る実施形態におけるデコードおよびコード化という言葉の定義について図６を用いて説明する。図６は、２次元コードの中に含まれている情報（元情報）を示す図である。元情報がコード画像化されることにより２次元コードはできている。
【００２５】
例えば、２次元コードは、「スキャン：条件付許可（パスワードが正しければ許可）、パスワード：ａｂｃｄｅｆｇ」という元情報がコード画像化されることによりできている。
【００２６】
そこで、本発明に係る実施形態では、ある情報を「元情報をコード画像化して２次元コードを生成すること」を「コード化」と定義している。また、本発明に係る実施形態では、２次元コードを「２次元コードから元情報を得ること」を「デコード」と称している。以上が、本発明に係る実施形態におけるデコードとコード化の定義である。
【００２７】
ステップＳ２００４で、ＭＦＰは、ステップＳ２００１で生成されたビットマップ形式の原稿画像と、ステップＳ２００３で得られた元情報と、ステップＳ２００２で検知した２次元コードの存在領域とをメモリに格納する。このとき、ＭＦＰは、ステップＳ２００１で生成された原稿画像をビットマップ形式でメモリに格納する。
【００２８】
次に、ステップＳ２００５で、ＭＦＰは、スタートボタンの選択を受付ける前に「送信モード」の選択を受付けていたか、「印刷モード」の選択を受付けていたか否かを判断する。
【００２９】
ステップＳ２００５で、「印刷モード」の選択を受けていたと判断された場合、ステップＳ２００７に処理が進む。ステップＳ２００７でＭＦＰが行う処理を、図３に示す。
【００３０】
図３のステップＳ３００１で、ＭＦＰは、ステップ２００４でメモリに格納した情報の

中に動作制限のための認証情報があるかを検索し、ステップＳ３００２に処理が進む。
【００３１】
ここでは、動作制限のための認証情報を「許可」「禁止」「パスワード入力による条件付許可」の３つを例に挙げて説明する。動作制限のための認証情報に、「許可」「禁止」「パスワード入力による条件付許可」の３つ以外の認証情報が含まれていても良い。
【００３２】
ステップＳ３００２で、ＭＦＰが、「許可」と判断した場合には、ステップＳ３００３に処理が進む。
【００３３】
ステップＳ３００３で、ＭＦＰは、通常のコピー処理を行う。
【００３４】
ステップＳ３００２で、ＭＦＰが、「禁止」と判断した場合には、ステップＳ３００４に処理が進む。
【００３５】
ステップＳ３００４で、ＭＦＰは、ジョブをキャンセルする。
【００３６】
ステップＳ３００２で、ＭＦＰが、「パスワード入力による条件付許可」と判断した場合には、ステップＳ３００５に処理が進む。
【００３７】
ステップＳ３００５で、ＭＦＰは、ジョブの先頭ページか否かを判断する。ステップＳ３００５で先頭ページであると判断された場合には、ステップＳ３００６に処理が進む。
【００３８】
ステップＳ３００６で、ＭＦＰは、操作画面上にパスワード入力要求画面を表示し、ユーザにパスワードの入力を促す。
【００３９】
次に、ステップＳ３００６で、図７に示されている処理が実行される。すなわち、ステップＳ７００１で、ＭＦＰが、パスワードの入力を検知するか否かを判断する。
【００４０】
ステップＳ７００１で、パスワードの入力が検知されなかったと判断された場合に、ステップＳ７００２で、ＭＦＰは、ジョブをキャンセルする。
【００４１】
一方、ステップＳ７００１で、パスワードの入力が検知されたと判断された場合に、ステップＳ３００７に処理が進む。
【００４２】
ステップＳ３００７で、ＭＦＰは、ステップＳ２００４でメモリに格納したパスワード情報と、ステップＳ３００６で入力されたパスワードとを比較することで認証を行い、ステップＳ３００８に処理が進む。
【００４３】
ステップＳ３００８で、ＭＦＰが、認証ＯＫ（成功）と判断した場合、ステップＳ３００９に処理が進み、通常のコピー処理を行う。
【００４４】
ステップＳ３００８で、ＭＦＰが、認証ＮＧ（失敗）と判断した場合、ステップＳ３０１０に処理が進み、ジョブをキャンセルする。
【００４５】
ステップＳ３００５で、ＭＦＰが、先頭ページではないと判断した場合、ステップＳ３０１１に処理が進む。
【００４６】
ステップＳ３０１１で、ＭＦＰは、ステップＳ２００４でメモリに格納したパスワードが、そのジョブの１ページ前と同じパスワードか否かを判断する。ステップＳ３０１１で、ＭＦＰが、同じパスワードと判断した場合には、ステップＳ３００９に処理が進み、Ｍ

ＦＰは、通常のコピー処理を行う。

【００４７】

ステップＳ３０１１で、ＭＦＰが、そのジョブの１ページ前と別のパスワードと判断した場合には、ステップＳ３０１２に処理が進み、ＭＦＰはジョブをキャンセルする。

【００４８】

そして、ＭＦＰは、ステップＳ３００１からステップＳ３０１２までをそのジョブの全てのページが終了するまで繰り返す。すなわち、ステップＳ３０１３で、ＭＦＰは、最終ページの処理か否かを判断する。そして、ステップＳ３０１３で、最終ページの処理でないと判断された場合には、ステップＳ３００１に処理が進む。一方、ステップＳ３０１３で最終ページの処理であると判断された場合には、全ての処理が終了する。

【００４９】

ステップＳ２００５で、ＭＦＰが、「送信モード」の選択を受けていたと判断した場合、ステップＳ２００６に処理が進む。ステップＳ２００６でＭＦＰが行う処理を、図４に示す。

【００５０】

ステップＳ４００１で、ＭＦＰは、ステップ２００４でメモリに格納した情報の中に動作制限のための認証情報があるかを検索し、ステップＳ４００２に処理が進む。

【００５１】

ここでは、動作制限のための認証情報を「許可」「禁止」「パスワード入力による条件付許可」の３つを例に挙げて説明する。動作制限のための認証情報に、「許可」「禁止」「パスワード入力による条件付許可」の３つ以外の認証情報が含まれていても良い。

【００５２】

ステップＳ４００２で、ＭＦＰが、「許可」と判断した場合には、ステップＳ４００３に処理が進む。

【００５３】

ステップＳ４００３で、ＭＦＰは、通常の送信処理を行う。

【００５４】

ステップＳ４００２で、ＭＦＰが、「禁止」と判断した場合には、ステップＳ４００４に処理が進む。

【００５５】

ステップＳ４００４で、ＭＦＰは、ジョブをキャンセルする。

【００５６】

ステップＳ４００２で、ＭＦＰが、「パスワード入力による条件付許可」と判断した場合には、ステップＳ４００５に処理が進む。

【００５７】

ステップＳ４００５で、ＭＦＰは、ジョブの先頭ページか否かを判断する。そして、ステップＳ４００５で、ＭＦＰが、先頭ページであると判断した場合には、ステップＳ４００６に処理が進む。

【００５８】

ステップＳ４００６で、ＭＦＰは、操作画面上にパスワード入力要求画面を表示し、ユーザにパスワードの入力を促す。

【００５９】

次に、ステップＳ４００６で、図７に示されている処理が実行される。すなわち、ステップＳ７００１で、ＭＦＰが、パスワードの入力を検知するか否かを判断する。

【００６０】

ステップＳ７００１で、パスワードの入力が検知されなかったと判断された場合に、ステップＳ７００２で、ＭＦＰは、ジョブをキャンセルする。

【００６１】

一方、ステップＳ７００１で、パスワードの入力が検知されたと判断された場合に、ステップＳ４００７に処理が進む。

【００６２】
ステップＳ４００７で、ＭＦＰは、ステップＳ２００４でメモリに格納したパスワード情報と、ステップＳ４００６で入力されたパスワードとを比較することで認証を行い、ステップＳ４００８に処理が進む。
【００６３】
ステップＳ４００８で、ＭＦＰが、認証が完了したと判断した場合、ステップＳ４００９に処理が進む。
【００６４】
ステップＳ４００９で、ＭＦＰは、ステップＳ２００４でメモリに格納したビットマップ形式の原稿画像を、同じくメモリに格納したパスワードを用いて、暗号化ＰＤＦを生成する。
【００６５】
ここで、「ビットマップ形式の原稿画像とパスワードとを用いて暗号化ＰＤＦを生成する」とは、どういうことかを詳しく説明する。本実施形態においては、暗号化ＰＤＦは、ＰＤＦ（Ｐｏｒｔａｂｌｅ　Ｄｏｃｕｍｅｎｔ　Ｆｏｒｍａｔ）ファイルの一種である。そして、上記「ビットマップ形式の原稿画像とパスワードとを用いて暗号化ＰＤＦを生成する」とは、以下のような意味である。すなわち、ビットマップ形式の原稿画像をＰＤＦ形式に変換してＰＤＦファイルを生成し、当該ＰＤＦ形式の原稿画像の閲覧を制限するためにＰＤＦファイルに対して、パスワードを付加することを意味する。このパスワード付加によって、暗号化ＰＤＦが生成されるのである。なお、この暗号化ＰＤＦは、送信先の装置(例えばＰＣ)上で、ユーザから閲覧指示があった場合には、付加されているパスワードと、送信先の装置上でユーザから入力されたパスワードが一致する場合に、ＰＤＦ形式の原稿画像が表示される。一方、それらが一致しない場合には、ＰＤＦ形式の原稿画像は、表示されない。ＭＦＰは、生成した暗号化ＰＤＦを、「送信モード」で設定された宛先に送信する。
【００６６】
なお、本発明に係る実施形態の記載では、ＭＦＰに読み込まれた原稿画像から生成される電子データを記録する電子ファイルの一例として、ＰＤＦファイルを用いて説明を行う。しかし、暗号化が可能な電子ファイルであれば、どのような電子ファイルでも本発明に係る実施形態に適用することができる。
【００６７】
ステップＳ４００８で、ＭＦＰが、認証が完了しなかったと判断した場合、ステップＳ４０１０に処理が進む。
【００６８】
ステップＳ４０１０で、ＭＦＰは、ジョブをキャンセルする。
【００６９】
ステップＳ４００５で、ＭＦＰが、先頭ページではないと判断した場合、ステップＳ４０１１に処理が進む。
【００７０】
ステップＳ４０１１で、ＭＦＰは、ステップＳ２００４でメモリに格納したパスワードが、そのジョブの１ページ前と同じパスワードか否かを判断する。ステップＳ４０１１で、ＭＦＰが、同じパスワードと判断した場合には、ステップＳ４００９に処理が進む。そして、ＭＦＰは、ステップＳ２００４でメモリに格納したビットマップ形式の原稿画像を、同じくメモリに格納したパスワードを用いて暗号化ＰＤＦを生成し、「送信モード」で設定された宛先に送信する。
【００７１】
ステップＳ４０１１で、そのジョブの１ページ前と別のパスワードと判断した場合には、ステップＳ４０１２に処理が進む。
【００７２】
ステップＳ４０１２で、ＭＦＰは、ジョブをキャンセルする。

【００７３】
ＭＦＰは、ステップＳ４００１からステップＳ４０１２までを全てのページが終了するまで繰り返す。すなわち、ステップＳ４０１３で、ＭＦＰは、最終ページの処理か否かを判断する。そして、ステップＳ４０１３で、最終ページの処理でないと判断された場合には、ステップＳ４００１に処理が進む。一方、ステップＳ４０１３で最終ページの処理であると判断された場合には、全ての処理が終了する。
【００７４】
以上のように処理を行うことで、ＭＦＰが、認証情報の埋め込まれている原稿をスキャンして電子データを生成し、ファイルサーバやＰＣに送信した場合であっても認証情報を適用することができる。また、原稿上の情報に対するセキュリティポリシーを電子データが引き継ぐことができる。
【００７５】
（実施形態２）
実施形態２も、図１に示した、システム図と同一の構成で実現される。
【００７６】
＜実施形態２における処理フロー（図５）＞
実施形態２では、実施形態１で説明した「送信モード」の選択をユーザから受付けた場合の処理が異なる。よって、図４に置き換わる部分のみ、図５を用いて説明する。
【００７７】
図２のステップＳ２００５で「送信モード」の選択を受けていたと判断した場合、ステップＳ２００６に処理が進む。ステップＳ２００６で、ＭＦＰが行なう処理を、図５に示す。
【００７８】
ステップＳ５００１で、ＭＦＰは、ステップＳ２００４でメモリに格納した情報の中に動作制限のための認証情報があるかを判断する。ここで、動作制限のための認証情報を「許可」「禁止」「パスワード入力による条件付許可」の３つを例に挙げて説明する。動作制限のための認証情報に、「許可」「禁止」「パスワード入力による条件付許可」の３つ以外の認証情報が含まれていても良い。
【００７９】
ステップＳ５００２で、ＭＦＰが、「許可」と判断した場合には、ステップＳ５００３に処理が進む。
【００８０】
ステップＳ５００３で、ＭＦＰは、通常の送信処理を行う。
【００８１】
ステップＳ５００２で、ＭＦＰが、「禁止」と判断した場合には、ステップＳ５００４に処理が進む。
【００８２】
ステップＳ５００４で、ＭＦＰは、ジョブをキャンセルする。
【００８３】
ステップＳ５００２で、ＭＦＰが、「パスワード入力による条件付許可」と判断した場合には、ステップＳ５００５に処理が進む。
【００８４】
ステップＳ５００５で、ＭＦＰは、ジョブの先頭ページか否かを判断する。ステップＳ５００５で、ＭＦＰが、ジョブの先頭ページであると判断した場合には、ステップＳ５００６に処理が進む。
【００８５】
ステップＳ５００６で、ＭＦＰは、操作画面上にパスワード入力要求画面を表示し、ユーザにパスワードの入力を促す。
【００８６】
次に、ステップＳ５００６で、図７に示されている処理が実行される。すなわち、ステ

ップＳ７００１で、ＭＦＰが、パスワードの入力を検知するか否かを判断する。
【００８７】
ステップＳ７００１で、パスワードの入力が検知されなかったと判断された場合に、ステップＳ７００２で、ＭＦＰは、ジョブをキャンセルする。
【００８８】
一方、ステップＳ７００１で、パスワードの入力が検知されたと判断された場合に、ステップＳ５００７に処理が進む。
【００８９】
ステップＳ５００７で、ＭＦＰは、ステップＳ２００４でメモリに格納したパスワード情報と、ステップＳ５００６で入力されたパスワードとを比較することで認証を行う。
【００９０】
ステップＳ５００８で、ＭＦＰが、認証が完了したと判断した場合、ステップＳ５００９に処理が進む。
【００９１】
ステップＳ５００９で、ＭＦＰは、通常の送信処理を行う。ここでは、実施形態１のように、ＭＦＰが、ステップＳ２００４でメモリに格納したビットマップ形式の原稿画像を、同じくメモリに格納したパスワードを用いて暗号化ＰＤＦを生成するという処理は行わない。
【００９２】
ステップＳ５００８で、ＭＦＰが、認証が完了しなかったと判断した場合は、ステップＳ５０１０に処理が進む。
【００９３】
ステップＳ５０１０で、ＭＦＰは、ジョブをキャンセルする。
【００９４】
ステップＳ５００５で、ＭＦＰが先頭ページではないと判断した場合、ステップＳ５０１２に処理が進む。
【００９５】
ステップＳ５０１２で、ＭＦＰがステップＳ２００４でメモリに格納したパスワードが、そのジョブの１ページ前と同じパスワードか否かを判断する。ステップＳ５０１２で、ＭＦＰが、同じパスワードと判断した場合には、ステップＳ５０１３に処理が進む。
【００９６】
ステップＳ５０１３で、ＭＦＰは、ステップＳ５００６で、ユーザによるパスワード入力を検知したか否かを判断する。
【００９７】
ステップＳ５０１３で、ＭＦＰが、パスワード入力を検知していた場合、ステップＳ５００９に処理が進み、ＭＦＰは、通常の送信処理を行う。
【００９８】
ステップＳ５０１３で、ＭＦＰが、パスワード入力を検知していなかった場合、ステップＳ５０１１に処理が進む。そして、Ｓ５０１１で、ＭＦＰは、ステップＳ２００４でメモリに格納したビットマップ形式の原稿画像を、同じくメモリに格納したパスワードを用いて暗号化ＰＤＦを生成し、「送信モード」で設定された宛先に送信する。
【００９９】
ステップＳ５０１２で、ＭＦＰが、そのジョブの１ページ前と別のパスワードと判断した場合に、ステップＳ５０１４に処理が進む。
【０１００】
ステップＳ５０１４で、ＭＦＰは、ジョブをキャンセルする。
【０１０１】
ＭＦＰは、ステップＳ５００１からステップＳ５０１４までをそのジョブの全てのページが終了するまで繰り返す。すなわち、ステップＳ５０１５で、ＭＦＰは、最終ページの処理か否かを判断する。そして、ステップＳ５０１５で、最終ページの処理でないと判断

された場合には、ステップＳ５００１に処理が進む。一方、ステップＳ５０１５で最終ページの処理であると判断された場合には、全ての処理が終了する。

【０１０２】

以上のように処理を行うことで、ＭＦＰが、認証情報の埋め込まれている原稿をスキャンして電子データを生成し、ファイルサーバやＰＣに送信する場合に次のような制御が可能となる。

【０１０３】

一度、ＭＦＰによって原稿にアクセスするための認証が許可されたユーザは、以後、パスワード入力が不要となるため、ユーザの利便性が向上する。これは、主に、ＭＦＰを操作するユーザが、ＭＦＰの送信機能を用いて自分のＰＣを宛先に原稿を送信する場合に有効な手段である。ＭＦＰを操作するユーザと、「送信モード」の宛先が同一か否かは、別途利用可能なログイン機能などを用いて判断してもよい。

【０１０４】

また、ＭＦＰを操作するユーザが原稿の認証情報を知らない場合でも、ＭＦＰの送信機能を利用することができる。これは、主に、ＭＦＰを操作するユーザがＭＦＰの送信機能を用いて、自分以外のＰＣを宛先に原稿を送信する場合に有効な手段である。ＭＦＰで原稿に対する認証制御は行われないが、送信先のＰＣ上では必ず認証制御が行われるため、原稿上の情報に対するセキュリティを守った上で、ユーザの操作性を向上させることができる。

【０１０５】

＜その他の実施形態＞

二次元コードを用いて上記実施形態を説明したが、一次元コードや電子透かしやステガノグラフィーであってもよい。

【０１０６】

また、上記実施形態では、データを格納する媒体としてメモリを用いて説明を行ったが、データを格納できる媒体（例えば、ＨＤＤやＲＡＭ）であれば、メモリに代わることができる。

【０１０７】

また、上記実施形態では、ＭＦＰがスキャンすることを前提に説明したが、スキャンとは、原稿上の画像を光学的に読取ることを意味する。例えば、デジタルカメラによる撮影などであっても本発明の目的を達成することができる。

【０１０８】

また、上記実施形態では、画像の読取、情報の処理、画像のシート上への印字の何れもが可能なＭＦＰを取り上げて説明したが、画像の読取、情報処理、画像のシート上への印字を行う装置が夫々、別の装置であっても構わない。

【０１０９】

なお、本明細書では、少なくとも情報の処理を行うことができる装置を画像処理装置と称する。さらには、少なくとも情報の処理、及び、画像のシート上への印字とを行うことができる装置を画像形成装置と称する。

【０１１０】

また本発明の目的は、上記実施形態で示したフローチャートの手順を実現するプログラムコードを記憶した記憶媒体から、コンピュータが、そのプログラムコードを読出し実行することによっても達成される。この場合、記憶媒体から読み出されたプログラムコード自体が上述した実施形態の機能を実現することになる。そのため、このプログラムコードやプログラムコードを記憶した記憶媒体も本発明を構成することができる。

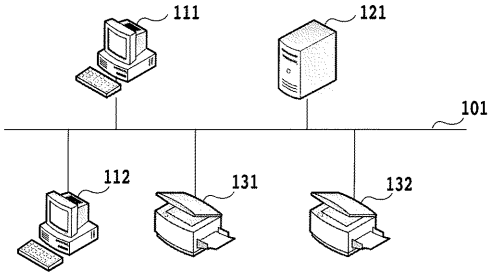
【０１１１】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

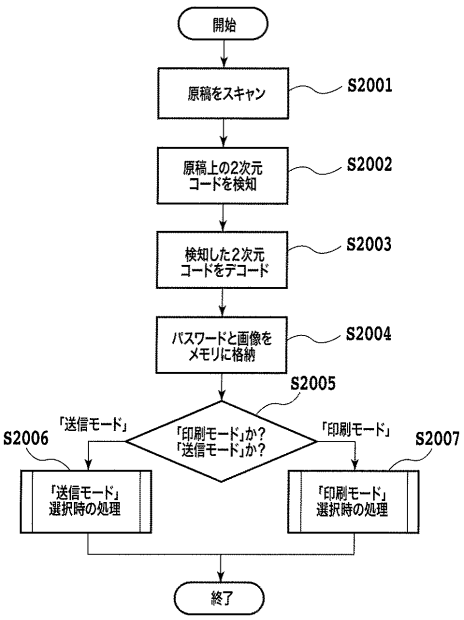
【図面の簡単な説明】

【０１１２】
【図１】システム図を示す図である。
【図２】実施形態１に係るフローチャートである。
【図３】実施形態１に係るフローチャートである。
【図４】実施形態１に係るフローチャートである。
【図５】実施形態２に係るフローチャートである。
【図６】デコードおよびコード化の例を示す図である。
【図７】パスワードの入力検知のフローチャートである。
【符号の説明】
【０１１３】
１０１　ネットワーク
１１１　クライアントコンピュータ
１１２　クライアントコンピュータ
１２１　ファイルサーバ
１３１　ＭＦＰ
１３２　ＭＦＰ

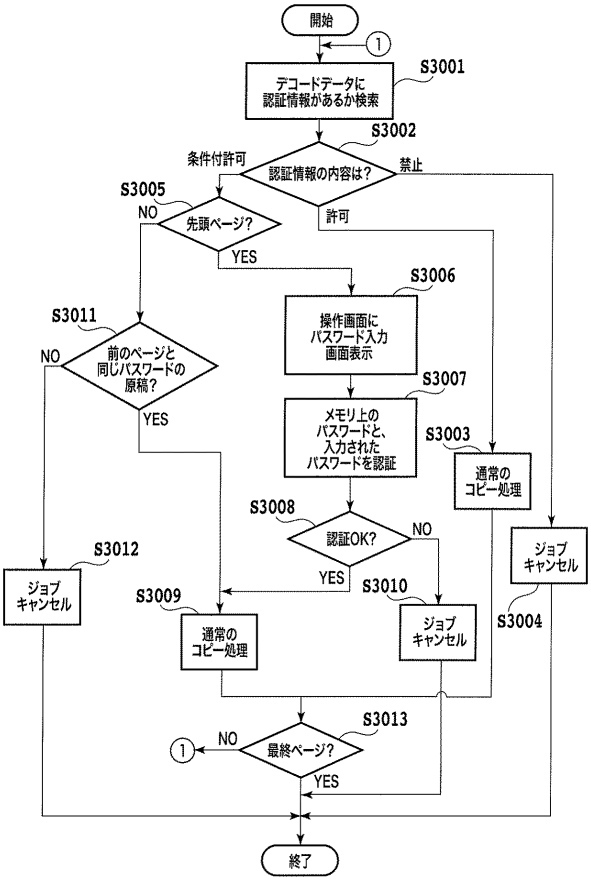
【図１】



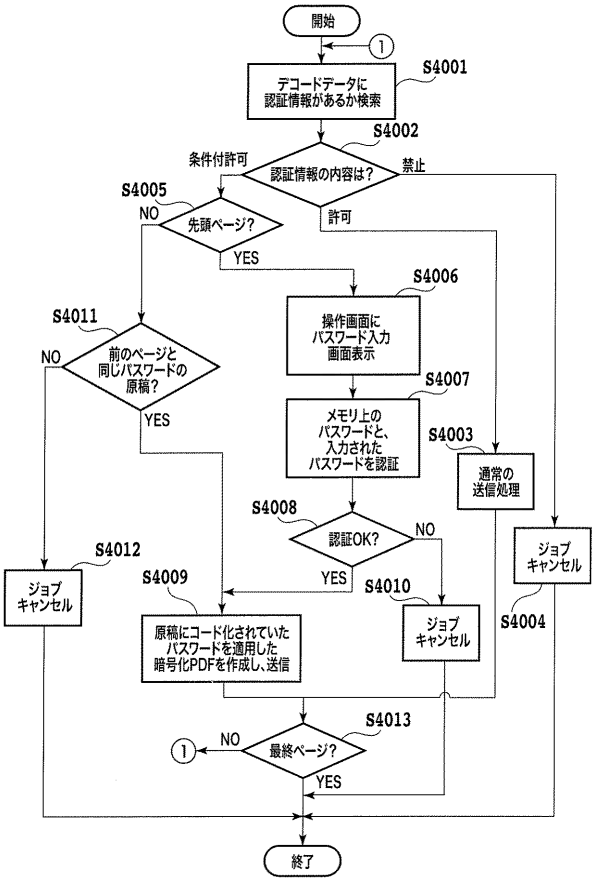
【図２】



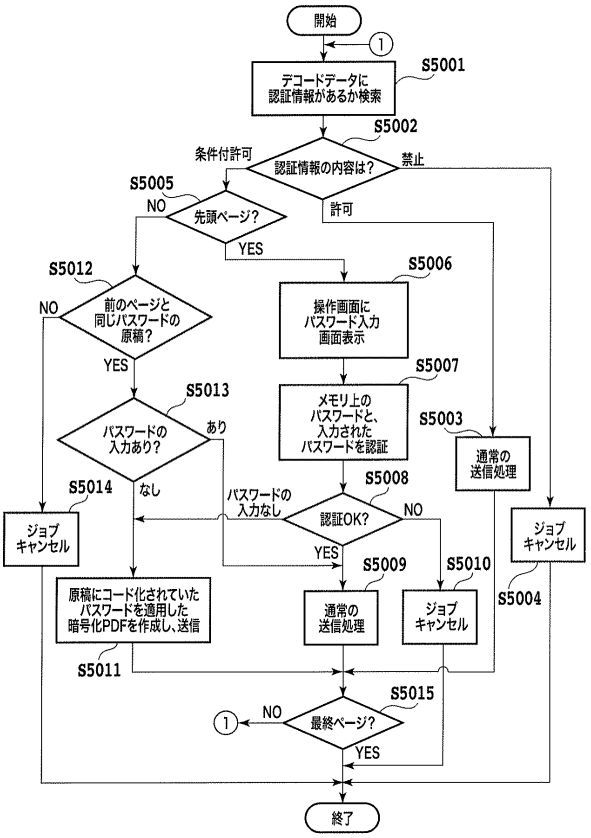
【図３】



【図４】



【図５】

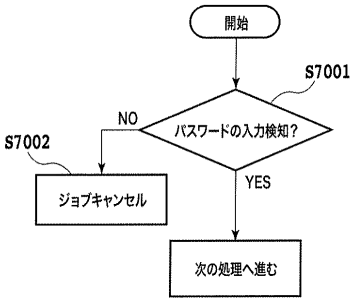


【図６】

元情報の例

スキャン：条件付許可（パスワードが正しければ許可）
パスワード：abcdefg

【図７】



フロントページの続き

(56)参考文献 特開２００７－１９５００５（ＪＰ，Ａ）
特開２００８－０１１１４９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　１／４４
Ｈ０４Ｎ　１／００