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

特許第4506850号
(P4506850)

(45)発行日　平成22年7月21日(2010.7.21)　(24)登録日　平成22年5月14日(2010.5.14)

(51)Int.Cl.			F I		
H04N	1/00	(2006.01)	H04N	1/00	107Z
H04N	1/44	(2006.01)	H04N	1/00	C
G06F	3/12	(2006.01)	H04N	1/44	
B41J	29/00	(2006.01)	G06F	3/12	K
B41J	29/38	(2006.01)	B41J	29/00	Z

請求項の数 14　(全 25 頁)　最終頁に続く

(21)出願番号　特願2008-36529(P2008-36529)
(22)出願日　平成20年2月18日(2008.2.18)
(65)公開番号　特開2009-194866(P2009-194866A)
(43)公開日　平成21年8月27日(2009.8.27)
審査請求日　平成20年2月19日(2008.2.19)

(73)特許権者　303000372
コニカミノルタビジネステクノロジーズ株式会社
東京都千代田区丸の内一丁目６番１号
(74)代理人　100117673
弁理士　中島　了
(72)発明者　福留　憲治
東京都千代田区丸の内一丁目６番１号　コニカミノルタビジネステクノロジーズ株式会社内

審査官　國分　直樹

最終頁に続く

(54)【発明の名称】画像管理装置、画像管理方法およびプログラム

(57)【特許請求の範囲】

【請求項１】

画像管理装置であって、

画像データをボックス内に格納する格納手段と、

画像送信要求を受け付ける手段と、

前記画像送信要求に応答して、セキュリティ情報を前記画像データに付与し、当該画像データを前記画像管理装置の前記格納手段から前記画像管理装置の外部装置へ送信する制御手段と、

を備え、

前記制御手段は、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする画像管理装置。

【請求項２】

請求項１に記載の画像管理装置において、

前記制御手段は、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする画像管理装置。

【請求項３】

請求項１または請求項２に記載の画像管理装置において、

前記画像データに付与される前記セキュリティ情報は、前記画像管理装置にログインして前記画像送信要求を付与したユーザに関するパスワード、前記ユーザの所属グループに関するパスワード、および前記画像データの格納先のボックスに関するパスワード、のうちの少なくとも１つを含むことを特徴とする画像管理装置。

【請求項４】

請求項１ないし請求項３のいずれかに記載の画像管理装置において、

前記制御手段は、前記格納手段の内部において前記画像データが移動またはコピーされ前記画像データの格納先が第１のボックスから第２のボックスへと変更された後に前記画像データが前記外部装置に送信される際には、格納先変更後における前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする画像管理装置。

【請求項５】

請求項４に記載の画像管理装置において、

前記格納先変更後における前記画像データのセキュリティ付与フラグの値は、前記格納先変更前における前記画像データのセキュリティ付与フラグの値と前記第１のボックスのセキュリティ付与フラグの値とに基づいて決定されることを特徴とする画像管理装置。

【請求項６】

請求項１ないし請求項３のいずれかに記載の画像管理装置において、

前記制御手段は、前記格納手段の内部において前記画像データが移動またはコピーされ前記画像データの格納先が第１のボックスから第２のボックスへと変更された後に前記画像データが前記外部装置に送信される際には、前記第２のボックスに設定されたセキュリティ付与フラグの値と格納先変更後における前記画像データに設定されたセキュリティ付与フラグの値とに基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする画像管理装置。

【請求項７】

請求項１または請求項２に記載の画像管理装置において、

前記制御手段は、前記ログイン中のユーザが前記画像データに対するアクセス権限を有することを確認した上で、前記画像データを送信することを特徴とする画像管理装置。

【請求項８】

請求項１または請求項２に記載の画像管理装置において、

前記制御手段は、

前記格納手段の内部において前記画像データが移動またはコピーされ前記画像データの格納先が第１のボックスから第２のボックスへと変更される際には、前記画像データに対するパスワード付与を行わず、

前記格納先の変更後に前記画像データが前記外部装置に送信される際に、前記パスワードを含む前記セキュリティ情報を前記画像データに付与することを特徴とする画像管理装置。

【請求項９】

画像管理装置の格納手段のボックス内に格納された画像データに関する画像管理方法であって、

a)画像送信要求を受け付けるステップと、

b)前記画像送信要求に応答して、セキュリティ情報を前記画像データに付与し、当該画像データを前記画像管理装置の前記格納手段から前記画像管理装置の外部装置へ送信するステップと、

を含み、

前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とする画像管理方法。

【請求項１０】

請求項９に記載の画像管理方法において、

前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とする画像管理方法。

【請求項１１】

請求項９または請求項１０に記載の画像管理方法において、

前記画像データに付与される前記セキュリティ情報は、前記画像管理装置にログインして前記画像送信要求を付与したユーザに関するパスワード、前記ユーザの所属グループに関するパスワード、および前記画像データの格納先のボックスに関するパスワード、のうちの少なくとも１つを含むことを特徴とする画像管理方法。

【請求項１２】

コンピュータに、

a)画像管理装置の格納手段のボックス内に格納された画像データに関する画像送信要求を受け付けるステップと、

b)前記画像送信要求に応答して、セキュリティ情報を前記画像データに付与し、当該画像データを前記画像管理装置の前記格納手段から前記画像管理装置の外部装置へ送信するステップと、

を実行させるためのプログラムであって、

前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とするプログラム。

【請求項１３】

請求項１２に記載のプログラムにおいて、

前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とするプログラム。

【請求項１４】

請求項１２または請求項１３に記載のプログラムにおいて、

前記画像データに付与される前記セキュリティ情報は、前記画像管理装置にログインして前記画像送信要求を付与したユーザに関するパスワード、前記ユーザの所属グループに関するパスワード、および前記画像データの格納先のボックスに関するパスワード、のうちの少なくとも１つを含むことを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、画像データを管理する画像管理装置に関する。

【背景技術】

【０００２】

ＭＦＰ等の装置において、当該装置で生成された画像データを当該装置内に保管する技術が存在する。例えば、当該画像データは、ＭＦＰ内の「ボックス」（フォルダとも表現される）に格納されて保管される。そして、当該装置内に保管される画像データは、例えばネットワークを介して外部装置（他のコンピュータ等）に送信され、当該外部装置から取り出され得る。

【０００３】

ところで、このような画像データに関して、当該画像データが外部装置に送信された後においても、セキュリティの確保が要求されることがある。

【０００４】

セキュリティを確保する技術としては、例えば特許文献１に記載の技術が存在する。特許文献１には、電子証明書を用いてスキャンデータを暗号化して送信する技術が記載され

ている。
【０００５】
また、特許文献２にはスキャン動作に関する次のような技術が記載されている。まず、スキャン動作を行う際にユーザがユーザコードを入力すると、ユーザコードに対応したパスワードが付加された状態でスキャンデータが外部コンピュータに保存される。そして、当該外部コンピュータでのスキャンデータの閲覧時に、ユーザコードに対応したパスワードが入力されると、当該スキャンデータが閲覧可能になる。
【０００６】
また、特許文献２においては、スキャンデータの閲覧に必要なパスワードを自動的に生成し、生成したパスワードを当該スキャンデータに付与するとともに、当該パスワードを電子メールで送信する技術も示されている。
【０００７】
【特許文献１】特開２００７－１６６０４９号公報
【特許文献２】特開２００６－８７０２５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、特許文献１の技術は、電子証明書の利用を必須要件とするものであり、必ずしも簡易な手法ではない。
【０００９】
また、上記特許文献２の技術は、スキャン動作に関するものであり、画像管理装置内に格納されている画像データを外部装置に送信する技術に関するものではない。また、メールを利用してパスワードを知らせる場合には、パスワードの漏洩リスクが存在する。
【００１０】
そこで、この発明の課題は、装置内に格納されている画像データを外部装置に送信する際のセキュリティ確保を簡易に実現することが可能な画像管理装置およびそれに関連する技術を提供することにある。
【課題を解決するための手段】
【００１１】
上記課題を解決すべく、請求項１の発明は、画像管理装置であって、画像データをボックス内に格納する格納手段と、画像送信要求を受け付ける手段と、前記画像送信要求に応答して、セキュリティ情報を前記画像データに付与し、当該画像データを前記画像管理装置の前記格納手段から前記画像管理装置の外部装置へ送信する制御手段とを備え、前記制御手段は、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする。
【００１２】
請求項２の発明は、請求項１の発明に係る画像管理装置において、前記制御手段は、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする。
【００１３】
請求項３の発明は、請求項１または請求項２の発明に係る画像管理装置において、前記画像データに付与される前記セキュリティ情報は、前記画像管理装置にログインして前記画像送信要求を付与したユーザに関するパスワード、前記ユーザの所属グループに関するパスワード、および前記画像データの格納先のボックスに関するパスワード、のうちの少なくとも１つを含むことを特徴とする。
【００１４】
請求項４の発明は、請求項１ないし請求項３のいずれかの発明に係る画像管理装置において、前記制御手段は、前記格納手段の内部において前記画像データが移動またはコピー

され前記画像データの格納先が第１のボックスから第２のボックスへと変更された後に前記画像データが前記外部装置に送信される際には、格納先変更後における前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする。

【００１５】

請求項５の発明は、請求項４の発明に係る画像管理装置において、前記格納先変更後における前記画像データのセキュリティ付与フラグの値は、前記格納先変更前における前記画像データのセキュリティ付与フラグの値と前記第１のボックスのセキュリティ付与フラグの値とに基づいて決定されることを特徴とする。

【００１６】

請求項６の発明は、請求項１ないし請求項３のいずれかの発明に係る画像管理装置において、前記制御手段は、前記格納手段の内部において前記画像データが移動またはコピーされ前記画像データの格納先が第１のボックスから第２のボックスへと変更された後に前記画像データが前記外部装置に送信される際には、前記第２のボックスに設定されたセキュリティ付与フラグの値と格納先変更後における前記画像データに設定されたセキュリティ付与フラグの値とに基づいて、前記セキュリティ情報を前記画像データに付与するか否かを決定することを特徴とする。

【００１７】

請求項７の発明は、請求項１または請求項２の発明に係る画像管理装置において、前記制御手段は、前記ログイン中のユーザが前記画像データに対するアクセス権限を有することを確認した上で、前記画像データを送信することを特徴とする。

【００１８】

請求項８の発明は、請求項１または請求項２の発明に係る画像管理装置において、前記制御手段は、前記格納手段の内部において前記画像データが移動またはコピーされ前記画像データの格納先が第１のボックスから第２のボックスへと変更される際には、前記画像データに対するパスワード付与を行わず、前記格納先の変更後に前記画像データが前記外部装置に送信される際に、前記パスワードを含む前記セキュリティ情報を前記画像データに付与することを特徴とする。

【００１９】

請求項９の発明は、画像管理装置の格納手段のボックス内に格納された画像データに関する画像管理方法であって、a)画像送信要求を受け付けるステップと、b)前記画像送信要求に応答して、セキュリティ情報を前記画像データに付与し、当該画像データを前記画像管理装置の前記格納手段から前記画像管理装置の外部装置へ送信するステップとを含み、前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とする。

【００２０】

請求項１０の発明は、請求項９の発明に係る画像管理方法において、前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とする。

【００２１】

請求項１１の発明は、請求項９または請求項１０の発明に係る画像管理方法において、前記画像データに付与される前記セキュリティ情報は、前記画像管理装置にログインして前記画像送信要求を付与したユーザに関するパスワード、前記ユーザの所属グループに関するパスワード、および前記画像データの格納先のボックスに関するパスワード、のうちの少なくとも１つを含むことを特徴とする。

【００２２】

請求項１２の発明は、コンピュータに、a)画像管理装置の格納手段のボックス内に格納

された画像データに関する画像送信要求を受け付けるステップと、b)前記画像送信要求に応答して、セキュリティ情報を前記画像データに付与し、当該画像データを前記画像管理装置の前記格納手段から前記画像管理装置の外部装置へ送信するステップとを実行させるためのプログラムであって、前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とする。

【００２３】

請求項１３の発明は、請求項１２の発明に係るプログラムにおいて、前記ステップb)においては、前記画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、前記画像データに設定されたセキュリティ付与フラグの値に基づいて、前記セキュリティ情報を前記画像データに付与するか否かが決定されることを特徴とするプログラム。

【００２４】

請求項１４の発明は、請求項１２または請求項１３の発明に係るプログラムにおいて、前記画像データに付与される前記セキュリティ情報は、前記画像管理装置にログインして前記画像送信要求を付与したユーザに関するパスワード、前記ユーザの所属グループに関するパスワード、および前記画像データの格納先のボックスに関するパスワード、のうちの少なくとも１つを含むことを特徴とする。

【発明の効果】

【００２５】

請求項１ないし請求項１４に記載の発明によれば、画像データが外部装置へ送信される際には、セキュリティ情報が当該画像データに対して自動的に付与されるので、簡易にセキュリティを確保することができる。

【００２６】

また、ボックスに設定されたセキュリティ付与フラグの値に基づいて、セキュリティ情報を画像データに付与するか否かが決定されるので、全ての画像データに対してセキュリティ付与の是非を逐一指定する必要がない。すなわち、ボックス内の複数の画像データに対して一括的にセキュリティ付与の是非を決定することができる。

【００２７】

また特に、請求項２，１０，１３に記載の発明によれば、画像データの格納先のボックスに設定されたセキュリティ付与フラグの値がオフである場合、画像データに設定されたセキュリティ付与フラグの値に基づいて、セキュリティ情報を画像データに付与するか否かが決定されるので、セキュリティ情報の設定の是非を画像データごとに個別に決定することも可能である。

【００２８】

また特に、請求項５に記載の発明によれば、格納先変更後における画像データのセキュリティ付与フラグに、第１のボックスのセキュリティ付与フラグの値を反映させることができる。したがって、装置内部での格納先変更に起因するセキュリティの低下を防止することが可能である。

【００２９】

また特に、請求項７に記載の発明によれば、ログイン中のユーザが画像データに対するアクセス権限を有することを確認した上で、画像データが送信されるので、セキュリティが高いレベルで確保される。

【発明を実施するための最良の形態】

【００３０】

以下、本発明の実施形態を図面に基づいて説明する。

【００３１】

＜１．構成＞

図１は、マルチ・ファンクション・ペリフェラル（Multi Function Peripheral）（ＭＦＰとも略称する）１を備える画像送受信システム１００の構成を示す概略図である。

【００３２】
ＭＦＰ１は、ネットワークＮＷを介して外部装置（コンピュータ９０等）に接続されており、当該外部装置との間でデータの送受信が可能である。ＭＦＰ１は、外部装置（あるいは自機の操作入力部）から、自機内の画像データ（画像）の送信要求（画像送信要求とも称する）を受け付け、当該画像送信要求に応じて画像データ（画像）を外部装置へと送信する。なお、ネットワークＮＷは、ＬＡＮ（Local Area Network）およびインターネットなどの各種のネットワークを含む。
【００３３】
このＭＦＰ１は、画像管理装置として機能する。また、ＭＦＰ１は、画像形成装置としても機能する。
【００３４】
ＭＦＰ１は、スキャナ機能、プリンタ機能、コピー機能およびファクシミリ通信機能などを備える装置（複合機とも称する）である。具体的には、ＭＦＰ１は、画像読取部２と、印刷出力部３と、通信部４と、格納部５と、入出力部６と、コントローラ９とを備えており、これらの各部を複合的に動作させることによって、上記の各機能を実現する。
【００３５】
画像読取部２は、ＭＦＰ１の所定の位置に載置された原稿を光学的に読み取って、当該原稿の画像データ（原稿画像とも称する）を生成する処理部である。
【００３６】
印刷出力部３は、対象画像に関する画像データに基づいて紙などの各種の媒体に画像を印刷出力する出力部である。
【００３７】
通信部４は、公衆回線等を介したファクシミリ通信を行うことが可能な処理部である。さらに、通信部４は、通信ネットワークＮＷを介したネットワーク通信が可能である。このネットワーク通信では、ＴＣＰ／ＩＰ（Transmission Control Protocol / Internet Protocol）およびＦＴＰ（File Transfer Protocol）等の各種のプロトコルが利用され、当該ネットワーク通信を利用することによって、ＭＦＰ１は、所望の相手先との間で各種のデータを授受することが可能である。なお、ＭＦＰ１は、このネットワーク通信を利用することによって、電子メールの送受信を行うことも可能である。
【００３８】
格納部５は、ハードディスクドライブ（ＨＤＤ）等の格納装置で構成される。この格納部５には、画像読取部２等で生成された原稿画像（画像データ）が格納される。格納部５には複数のボックス（フォルダ）が設けられており、各画像データは複数のボックスのいずれかに格納される。また、格納部５には、ユーザ認証情報等も記憶されている。
【００３９】
入出力部６は、ＭＦＰ１に対する入力を受け付ける操作入力部６１と、各種情報の表示出力を行う表示部６２とを備えている。詳細には、ＭＦＰ１には操作パネル６３（図１１参照）が設けられている。この操作パネル６３は、液晶表示パネルに圧電センサ等が埋め込まれて構成されており、表示部６２の一部として機能するとともに、操作入力部６１の一部としても機能する。
【００４０】
コントローラ９は、ＭＦＰ１を統括的に制御する制御装置であり、ＣＰＵと、各種の半導体メモリ（ＲＡＭおよびＲＯＭ等）とを備えて構成される。コントローラ９の制御下において各種の処理部が動作することによって、ＭＦＰ１の各種の機能が実現される。例えば、コントローラ９の制御下において、画像読取部２を用いて所望の画像を光学的に読み取ることによって、原稿をスキャニングした画像（原稿画像）が取得され、スキャナ機能が実現される。また、コントローラ９は、次述するような各種の処理をも制御する。
【００４１】
コントローラ９は、ＣＰＵにおいて、ＲＯＭ（例えば、ＥＥＰＲＯＭ等）内に格納されている所定のソフトウエアプログラム（以下、単にプログラムとも称する）を実行するこ

とによって、各種の処理部を実現する。コントローラ９は、印刷制御システム（印刷制御装置とも称される）として機能する。

【００４２】

具体的には、コントローラ９は、ユーザ／グループ情報管理部１１と、ボックス管理部１２と、画像データ管理部１３と、セキュリティ付与部１４とを含む各種の処理部を実現する。

【００４３】

ユーザ／グループ情報管理部１１は、各ユーザ（個人ユーザ）に関する情報と、各グループに関する情報とを管理する処理部である。

【００４４】

ボックス管理部１２は、各ボックスに関する情報を管理する処理部である。ボックス管理部１２は、例えば、各ボックスの種別（プライベートボックス、グループボックス、パブリックボックス）、および各ボックスに対するセキュリティ付与フラグＦＢ（ＦＸ）の設定等を管理する。

【００４５】

画像データ管理部１３は、各画像データに関する情報を管理する処理部である。画像データ管理部１３は、各画像データに対するセキュリティ付与フラグＦＢ（ＦＹ）の設定等を管理する。

【００４６】

セキュリティ付与部（セキュリティ制御部とも称する）１４は、各画像データの外部装置への取出動作（送信動作）、および各画像データの自機内での移動動作およびコピー動作等を管理する処理部である。特に、セキュリティ付与部１４は、ユーザ／グループ情報管理部１１、ボックス管理部１２、および画像データ管理部１３との間で情報を授受しつつ、各画像データの外部装置への送信する送信動作時に各画像データＰＤに対してセキュリティ情報（パスワード等）を付与する処理を実行する。

【００４７】

これらの処理部を有するコントローラ９は、ＭＦＰ（画像管理装置）１にログイン中のユーザにより付与された画像送信要求に応答して格納部５から当該ＭＦＰの外部へと画像データが取り出される（送信される）際に、所定のユーザ等に関するパスワードなどを含むセキュリティ情報を、当該画像データに対して自動的に付与する。これにより、ユーザが画像データを取り出すたびに画像データに対するパスワード付与操作を行うことなく、送信先のコンピュータ９０にパスワード設定済みの画像データを簡易に送信することができる。特に、送信対象の画像データがパスワード未設定（未付与）の画像データであっても、自動的にパスワードが付与されるので、非常に簡便である。このような送信動作については、後に詳述する。

【００４８】

＜２．ユーザおよびグループ＞

図２は、ユーザとグループとの間の所属関係を示す図であり、各ユーザがいずれのグループに所属しているかが示されている。

【００４９】

例えば、ユーザＵＡは、グループＧ１に所属するとともにグループＧ３にも所属している。ユーザＵＢ，ＵＣも同様である。また、ユーザＵＤは、グループＧ２に所属するとともに、グループＧ３にも所属している。また、ユーザＵＥは、グループＧ２に所属している。

【００５０】

換言すれば、グループＧ１にはユーザＵＡ，ＵＢ，ＵＣが所属し、グループＧ２には、ユーザＵＤ，ＵＥが所属し、グループＧ３には、ユーザＵＡ，ＵＢ，ＵＣ，ＵＤが所属する。

【００５１】

ユーザ／グループ情報管理部１１は、このようなユーザとグループとの所属関係（換言

すれば各グループのメンバー情報）に関する登録情報を格納部５に記憶して管理する。また、各種パスワードも同様に管理する。

【００５２】

＜３．ボックス構成（フォルダ構成）＞

図３は、格納部５内におけるボックス構成を示す概念図である。

【００５３】

上述したように、格納部５内に設けられる「ボックス」（フォルダ）には複数の種別、具体的には、プライベートボックス、グループボックス、およびパブリックボックス、の３種類の種別が存在する。プライベートボックスは、特定のユーザによるアクセスが許容されるボックスである。また、グループボックスは、特定のグループによるアクセスが許容されるボックスである。さらに、パブリックボックスは、不特定のユーザによるアクセスが許容されるボックスである。

【００５４】

以下では、図３に示すように、プライベートボックスＢＲ１，ＢＲ２，ＢＲ３，ＢＲ４，ＢＲ５，ＢＲ６とグループボックスＢＧ１，ＢＧ２，ＢＧ３，ＢＧ４とパブリックボックスＢＢ１とが格納部５に設けられているものとする。

【００５５】

また、図３においては、各ユーザＵＡ～ＵＥがアクセス可能な範囲が、それぞれ、破線の矩形領域で示されている。すなわち、各ユーザＵＡ～ＵＥは、それぞれ、対応する破線矩形内のボックスに対するアクセスが許可されている。

【００５６】

例えば、ユーザＵＡは、ユーザＵＡのプライベートボックスＢＲ１，ＢＲ６にアクセス可能である。

【００５７】

また、ユーザＵＡは、グループボックスＢＧ１，ＢＧ３，ＢＧ４にもアクセス可能である。グループボックスＢＧ１，ＢＧ４は、グループＧ１のメンバーからのアクセスが許可されているボックスであり、グループボックスＢＧ３は、グループＧ３のメンバーからのアクセスが許可されているボックスである。ユーザＵＡは、グループＧ１，Ｇ３のメンバーであるため、上述のように、グループボックスＢＧ１，ＢＧ３，ＢＧ４にもアクセス可能である。

【００５８】

さらに、ユーザＵＡは、パブリックボックスＢＢ１にもアクセス可能である。

【００５９】

なお、ユーザＵＡは、上記以外のボックスＢＲ２，ＢＲ３，ＢＲ４，ＢＲ５，ＢＧ２に対しては原則としてアクセスすることができない。

【００６０】

同様に、ユーザＵＢは、ユーザＵＢのプライベートボックスＢＲ２にアクセス可能である。また、ユーザＵＢは、グループボックスＢＧ１，ＢＧ３，ＢＧ４にもアクセス可能である。さらに、ユーザＵＢは、パブリックボックスＢＢ１にもアクセス可能である。ユーザＵＢは、これら以外のボックスＢＲ１，ＢＲ３，ＢＲ４，ＢＲ５，ＢＲ６，ＢＧ２に対しては原則としてアクセスすることができない。

【００６１】

ユーザＵＣについても同様である。ただし、ユーザＵＣは、ユーザＵＣのプライベートボックスＢＲ３にアクセス可能であるが、ユーザＵＢのプライベートボックスＢＲ２には原則としてアクセスすることはできない。

【００６２】

また、ユーザＵＤは、ユーザＵＤのプライベートボックスＢＲ４と、グループボックスＢＧ２，ＢＧ３と、パブリックボックスＢＢ１とにアクセス可能である。一方、ユーザＵＤは、これら以外のボックスＢＲ１，ＢＲ２，ＢＲ３，ＢＲ５，ＢＲ６，ＢＧ１，ＢＧ４に対しては原則としてアクセスすることができない。

【００６３】
また、ユーザＵＥは、ユーザＵＥのプライベートボックスＢＲ５と、グループボックスＢＧ２と、パブリックボックスＢＢ１とにアクセス可能である。一方、ユーザＵＥは、これら以外のボックスＢＲ１，ＢＲ２，ＢＲ３，ＢＲ４，ＢＲ６，ＢＧ１，ＢＧ３，ＢＧ４に対しては原則としてアクセスすることができない。
【００６４】
図４は、各ボックスに関する情報の一例を示す図である。
【００６５】
図４に示すように、各ボックスに関して、その識別番号（記号）を表す「ボックスＩＤ」と、その名称を表す「ボックス名」と、その種別を表す「ボックス種別」、そのボックスに対するアクセスが許容されているユーザおよびグループを表す「アクセス許容ユーザ／グループ」とが設定されている。また、各ボックスに関しては、それぞれ、セキュリティ情報を自動的に付与する（「オン」）か否（「オフ」）かを決定するフラグ（「セキュリティ付与フラグ」とも称する）ＦＢも設定されている。
【００６６】
例えば、図４では、プライベートボックスＢＲ１に関して、「ボックスＩＤ」＝０００１、「ボックス名」＝鈴木、「ボックス種別」＝プライベート、「アクセス許容ユーザ／グループ」＝ユーザＵＡ、「セキュリティ付与フラグ」＝オフ、の各情報が設定されている。
【００６７】
また、グループボックスＢＧ１に関しては、「ボックスＩＤ」＝０１０１、「ボックス名」＝営業１課、「ボックス種別」＝グループ、「アクセス許容ユーザ／グループ」＝グループＧ１、「セキュリティ付与フラグ」＝オフ、の各情報が設定されている。
【００６８】
＜４．画像データ構成＞
図５は、各画像データに関する情報の一例を示す図である。
【００６９】
図５に示すように、各画像データ（画像ファイル）に関して、その識別番号（記号）を表す「ファイルＩＤ」と、その名称を表す「ファイル名」と、その格納先のボックス名称を表す「ボックス名」とが設定されている。また、各画像データに関しては、それぞれ、セキュリティ情報を自動的に付与する（「オン」）か否（「オフ」）かを決定するためのフラグ（「セキュリティ付与フラグ」とも称する）ＦＢも設定されている。
【００７０】
例えば、図５では、画像データＰＤ１に関して、「ファイルＩＤ」＝０００１、「ファイル名」＝商品写真、「ボックス名」＝ボックスＢＲ１、「セキュリティ付与フラグ」＝オン、の各情報が設定されている。
【００７１】
また、各画像データＰＤは、当該各画像データＰＤがＭＦＰ１内に存在する際には、セキュリティ情報自体を有していない。換言すれば、画像データＰＤにはセキュリティ情報（パスワード等）自体は付与されていない。一方、当該各画像データＰＤがＭＦＰ１内に存在する際には、「セキュリティ付与フラグＦＢ」が、セキュリティ管理に関する情報（セキュリティ管理情報）として、各画像データＰＤに関連づけて記憶されている。この実施形態においては、このセキュリティ付与フラグＦＢ等を利用することによって、画像データＰＤを外部へ取り出す際にセキュリティ情報（パスワード等）を付与するか否かが管理される。
【００７２】
なお、「セキュリティ付与フラグ」としては、ボックスごとに設定されるセキュリティ付与フラグＦＢ（図４）と、画像データＰＤごとに設定されるセキュリティ付与フラグＦＢ（図５）とが存在する。後述するように、特定の画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）がオンの場合には、当該画像データＰＤが外部に取り出される際に当該

画像データＰＤに対して常にセキュリティ情報の付与動作（パスワードの自動付与動作等）が実行される。また、特定のボックスのセキュリティ付与フラグＦＢ（ＦＸ（図４））がオンの場合には、画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ（図５））の設定内容にかかわらず、当該ボックス内の画像データＰＤが外部に取り出される際には当該画像データＰＤに対して常にセキュリティ情報が付与される。一方、ボックスのセキュリティ付与フラグＦＢ（ＦＸ）がオフであり、且つ、画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）がオフである場合には、当該ボックス内の画像データＰＤが外部に取り出される際にも当該画像データＰＤに対するセキュリティ情報の付与動作は実行されない。

【００７３】

＜５．セキュリティ情報（パスワード）＞

上述したように、この実施形態においては、所定の条件が充足される場合には、画像データに対してセキュリティ情報が自動的に付与される。

【００７４】

画像データに対するセキュリティ情報を付与する手法としては、例えば、画像データに対してパスワードロック（パスワードによるデータアクセス制限機能）を用いることが挙げられる。なお、これに限定されず、例えば、画像データに対してパスワード入力を伴う電子署名情報の付与を行うようにしてもよい。

【００７５】

また、パスワードの種類としては、個人専用（ユーザ専用）のパスワードが例示される。ただし、これに限定されず、ユーザの所属グループに関するグループ共用のパスワードを用いるようにしてもよい。なお、個人専用のパスワードを用いることによれば、装置外部に取り出された画像データに関するセキュリティを高度に維持することが可能である。一方、グループ共用のパスワードを用いることによれば、セキュリティを確保しつつ、外部装置への送信操作を指示したユーザとは別の人物（詳細には、当該ユーザの同一グループに所属する別の人物）が、取り出し後の画像データを容易に閲覧することが可能である。また、ユーザ専用のパスワードとして、ＭＦＰ１への各ユーザのログイン用パスワードを用いてもよい。これによれば、パスワードを別途メール送信しなくても済む。また、自分のログイン用パスワードを忘れることは少ないと考えられ、忘却抑止効果も得られる。さらに、グループ共用のパスワードについても同様である。具体的には、グループ共用のパスワードとして、グループボックスへのアクセス許可用パスワードを用いてもよい。これによっても、同様の効果が得られる。

【００７６】

ここでは、図６のような設定画面を用いて、両者（個人専用のパスワードおよびグループ共用のパスワード）を選択的に利用するものとする。

【００７７】

図６は、パスワード種別を設定する設定画面を示す図である。ここでは、図６のような設定画面を用いて、いずれの種類のパスワードを利用するかが予め設定されるものとする。また、以下では、ユーザのパスワードを利用する場合、特に、各ユーザごとに予めＭＦＰ１に登録されたパスワードを用いるものとする。

【００７８】

具体的には、図２に示すように、ユーザＵＡのログイン中には、ユーザＵＡの登録済みパスワードＰＷａが利用されるものとする。同様に、ユーザＵＢのログイン中には、ユーザＵＢの登録済みパスワードＰＷｂが利用され、ユーザＵＣのログイン中には、ユーザＵＣの登録済みパスワードＰＷｃが利用される。また、ユーザＵＤのログイン中には、ユーザＵＤの登録済みパスワードＰＷｄが利用され、ユーザＵＥのログイン中には、ユーザＵＥの登録済みパスワードＰＷｅが利用される。このように、現在ログイン中のユーザのパスワードがセキュリティ情報として利用される。

【００７９】

さらに、ここでは、セキュリティ情報として画像データＰＤに自動的に付与される個人

パスワードは、各個人のログイン時のパスワードとは別の設定情報として定められているものを利用するものとする。ただし、これに限定されず、当該別の設定情報として設定される個人パスワードは、各個人のログイン時のパスワードと同じものであってもよい。あるいは、セキュリティ情報として自動的に付与される個人パスワードとして、各ユーザのログイン時のパスワードを常にそのまま用いるようにしてもよい。

【００８０】

なお、画像データＰＤに自動的に付与されるパスワードとして、グループ共用のパスワードを利用する場合には、例えば、各グループごとに予めＭＦＰ１に登録されたパスワードを用いればよい。具体的には、図２に示すように、グループＧ１のメンバーのログイン中には、グループＧ１の登録済みパスワードＰＷ１が利用されればよい。同様に、グループＧ２のメンバーのログイン中には、グループＧ２の登録済みパスワードＰＷ２が利用されればよく、グループＧ３のメンバーのログイン中には、グループＧ３の登録済みパスワードＰＷ３が利用されればよい。

【００８１】

また、複数の所属グループを有するユーザがログインしている際には、あらかじめ設定された順位にしたがって、いずれのグループに関するパスワードを利用するかを決定すればよい。

【００８２】

また、この実施形態においては、プライベートボックスからの取り出しの場合、グループボックスからの取り出しの場合、およびパブリックボックスからの取り出しの場合のいずれであっても、それぞれ上記の２種類のうちの一方のパスワードを用いて、取り出し対象の画像データに対してセキュリティ情報が付与されるものとする。すなわち、装置全体においてグループ共用のパスワードと個人専用のパスワードとが二者択一的に切り替えられて付与されるものとする。

【００８３】

＜６．動作＞

＜６－１．ボックスへの格納動作＞

つぎに、ＭＦＰ１における動作について説明する。

【００８４】

画像データの外部装置への取出動作について説明する前に、図７のフローチャートを参照しながら、画像データをボックスへ格納する動作について説明する。ここでは、スキャン動作によって生成される画像（画像データＰＤ）のセキュリティ付与フラグＦＢ（ＦＹ）が、全スキャンデータに対する一括的な保護設定と、ボックスのセキュリティ付与フラグＦＢ（ＦＸ）の設定とに基づいて、自動的にオンに設定される場合を例示する。

【００８５】

まず、図７のステップＳ１１において、或るユーザ（例えばユーザＵＡ）がＭＦＰ１にログインする。

【００８６】

そして、ステップＳ１２において、ユーザＵＡは操作入力部６１を用いて「スキャンｔｏＨＤＤ」などのメニュー項目を選択して、当該メニュー項目に対応する動作をＭＦＰ１に実行させる。具体的には、ＭＦＰ１は、まず、画像読取部２によって光学的に読み取られた原稿画像に関する画像データ（スキャンデータ）ＰＤを生成する。そして、ＭＦＰ１は、ステップＳ１３～Ｓ１６の動作において、生成した画像データＰＤを格納部５内のハードディスクドライブ（ＨＤＤ）に格納する動作を実行する。

【００８７】

ステップＳ１３，Ｓ１４においては、画像読取部２によって生成された画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）を、オンに設定すべきか否かが決定される。

【００８８】

具体的には、全スキャンデータに対する一括的な保護設定がオンに指定されていること（いずれのスキャンデータを外部に取り出す際にもセキュリティ情報を付与すべき旨がユ

ーザによって予め一括的に指定されていること）がステップＳ１３で確認されると、ステップＳ１５に進む。当該一括保護指定の有無は、不図示の設定画面を用いて、ＭＦＰ１のスキャン動作に対して一括的に設定される。

【００８９】

ステップＳ１５では、画像データＰＤのセキュリティ付与フラグＦＢがオン（ＯＮ）に変更されて、画像データＰＤが格納対象のボックス（例えば、ボックスＢＲ１）に格納される。したがって、例えば、ＭＦＰ１のスキャン動作全体に関する上記の一括保護指定がなされている場合には、全てのスキャン動作に対して画像データＰＤのセキュリティ付与フラグＦＢがオンにされる。

【００９０】

また、セキュリティ情報を付与すべき旨の設定がユーザによって選択されていない場合であっても、画像データＰＤの格納先のボックスのセキュリティ付与フラグＦＢ（ＦＸ）がオンであることがステップＳ１４で確認されると、ステップＳ１５に進む。

【００９１】

ステップＳ１５では、上述のように、画像データＰＤのセキュリティ付与フラグＦＢがオン（ＯＮ）に変更されて、当該画像データＰＤが格納対象のボックスに格納される。

【００９２】

したがって、ユーザは、そのセキュリティ付与フラグＦＢの値をオンに設定したボックス内に画像データＰＤを格納することなどによって、画像データＰＤのセキュリティ付与フラグＦＢを自動的にオンに設定することができる。これによれば、後述するように、画像データＰＤの外部送信時において容易にセキュリティを維持することが可能になる。

【００９３】

一方、上記の一括保護設定がなされていない場合であって、且つ、画像データＰＤの格納対象のボックスのセキュリティ付与フラグＦＢ（ＦＸ）がオンでない場合には、ステップＳ１６に進む。ステップＳ１６では、画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）をオフ（ＯＦＦ）に維持したまま、当該画像データが格納対象のボックスに格納される。

【００９４】

このようにして、スキャン画像がＭＦＰ１の格納部５内に格納される。

【００９５】

ただし、各画像データＰＤのセキュリティ付与フラグＦＢの値は、上記のような自動設定動作によって決定される場合に限定されない。各画像データＰＤのセキュリティ付与フラグＦＢの値は、様々な動作によって適宜の値（「オン」または「オフ」）に設定された状態で、各画像データＰＤがそれぞれの格納先のボックスに格納される。

【００９６】

例えば、画像データＰＤのセキュリティ付与フラグＦＢは、最初の格納時には「オン」に設定されていたとしても、設定変更画面（不図示）を用いたユーザ操作に応じて、「オン」から「オフ」に事後的に変更され得る。

【００９７】

あるいは逆に、画像データＰＤのセキュリティ付与フラグＦＢは、最初の格納時には「オフ」に設定されていたとしても、同様の設定変更画面を用いたユーザ操作に応じて「オフ」から「オン」へと事後的に変更され得る。

【００９８】

また、ここでは、スキャン画像（画像データＰＤ）のセキュリティ付与フラグＦＢが上記の一括保護指定に応じて自動的にオンに設定される場合（ステップＳ１３，Ｓ１５）を例示したが、これに限定されない。例えば、画像データＰＤのセキュリティ付与フラグＦＢは、一括保護指定に応じて自動的にオンに設定されないようにしてもよい。より詳細には、画像データＰＤのセキュリティ付与フラグＦＢは、ユーザによる設定操作に応じてのみオンに設定されるようにしてもよい。

【００９９】

同様に、ここでは、スキャン画像（画像データＰＤ）のセキュリティ付与フラグＦＢが、ボックスのセキュリティ付与フラグＦＢの設定にも応じて自動的にオンに設定される場合（ステップＳ１４，Ｓ１５）を例示したが、これに限定されない。例えば、画像データＰＤのセキュリティ付与フラグＦＢは、ボックスのセキュリティ付与フラグＦＢに応じてオンにされないようにしてもよい。より詳細には、ボックスのセキュリティ付与フラグＦＢは、ユーザによる設定操作に応じてのみオンに設定されるようにしてもよい。

【０１００】

以上のような様々な動作によって、各画像データＰＤのセキュリティ付与フラグＦＢは、その値が「オン」または「オフ」に適宜に設定された状態で、それぞれの格納先のボックスに格納される。

【０１０１】

＜６－２．外部への取出動作（外部アクセス）＞

次に、ボックスに格納されている画像データを装置外部へと取り出す動作（送信動作）について、図８のフローチャートを参照しながら説明する。ここでは、ＭＦＰ１のボックスＢＲ１内の画像データＰＤが、ＭＦＰ１の外部装置であるコンピュータ９０へと、ユーザＵＡによって取り出される場合について説明する。

【０１０２】

まず、ステップＳ２１において、ユーザＵＡが外部のコンピュータ９０（図１参照）からネットワークを介してＭＦＰ１にログインする。

【０１０３】

そして、ステップＳ２２において、ログイン中のユーザＵＡはコンピュータ９０の操作画面を利用して、ＭＦＰ１のボックスＢＲ１内の画像データＰＤを、コンピュータ９０の所定のフォルダに移動（ないしコピー）するための操作を実行する。例えば、ユーザＵＡは、コンピュータ９０のマウスのドラッグ操作を伴って、コンピュータ９０の操作画面においてボックスＢＲ１内の画像データＰＤのアイコンをコンピュータ９０の所定のフォルダ内へと移動させる操作を行う。そして、コンピュータ９０は、ユーザＵＡによる当該操作に応答して、画像データＰＤを送信すべき旨のデータ転送指令（画像送信要求）をＭＦＰ１に送信する。

【０１０４】

ＭＦＰ１は、当該操作に伴って、コンピュータ９０から当該画像データＰＤのデータ転送指令（画像送信要求）を受信すると、ステップＳ２３～Ｓ２６において、転送対象の画像データＰＤを格納部５からコンピュータ９０へと転送する動作を実行する。

【０１０５】

具体的には、まず、ステップＳ２３，Ｓ２４において、転送対象の画像データＰＤに対してセキュリティ情報を付与すべきか否かが決定される。詳細には、画像データＰＤの格納先のボックスに設定されたセキュリティ付与フラグＦＢ（ＦＸ）の値と、画像データＰＤ自体に設定されたセキュリティ付与フラグＦＢ（ＦＹ）の値との双方に基づいて決定される。

【０１０６】

より詳細には、（画像データＰＤの格納先である）ボックスＢＲ１のセキュリティ付与フラグＦＢ（ＦＸ）がオン（ＯＮ）であることがステップＳ２３で確認される場合には、セキュリティ情報を付与すべきであると判断されてステップＳ２５に進む。また、ボックスＢＲ１のセキュリティ付与フラグＦＢがオフであっても、画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）がオンであることがステップＳ２４で確認される場合には、セキュリティ情報を付与すべきであると判断されてステップＳ２５に進む。このように、ボックスＢＲ１のセキュリティ付与フラグＦＢ（ＦＸ）と画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）との少なくとも一方がオンである場合には、セキュリティ情報を付与すべきであると判断されてステップＳ２５に進む。

【０１０７】

ステップＳ２５では、画像データＰＤに対してセキュリティ情報が付与され、当該セキ

ュリティ情報が付与された状態の画像データＰＤがＭＦＰ１からコンピュータ９０へと転送される。なお、画像データＰＤに付与されるセキュリティ情報としては、上述のような情報が用いられる。例えば、画像データＰＤは、ユーザＵＡに関するパスワードが付与された状態で、コンピュータ９０内の指定された転送先フォルダへと転送される。

【０１０８】

図９に示すように、ボックスＢＲ１のセキュリティ付与フラグＦＢ（ＦＸ）がオフであっても、画像データＰＤ１のセキュリティ付与フラグＦＢ（ＦＹ）がオンである場合には、画像データＰＤ１は、ユーザＵＡに関するパスワードが付与された状態でコンピュータ９０へと転送される。

【０１０９】

また、図１０に示すように、ボックスＢＲ１のセキュリティ付与フラグＦＢ（ＦＸ）がオンである場合には、当該ボックスＢＲ１内の画像データＰＤ１，ＰＤ２は、いずれも、ユーザＵＡに関するパスワードが付与された状態でコンピュータ９０へと転送される。すなわち、画像データＰＤ１，ＰＤ２のセキュリティ付与フラグＦＢがオンであるか否かにかかわらず、当該ボックスＢＲ１内の画像データＰＤ１，ＰＤ２は、いずれも、ユーザＵＡに関するパスワードが付与された状態でコンピュータ９０へと転送される。

【０１１０】

その後、転送された画像データＰＤをコンピュータ９０等で閲覧する際には、セキュリティ情報に基づく認証動作が求められる。具体的には、パスワード入力が求められる。閲覧ユーザは、正規のパスワードを入力することによって、当該画像データＰＤを閲覧することが可能である。

【０１１１】

以上のような動作によれば、ＭＦＰ１内に格納された画像データＰＤが外部のコンピュータ９０に転送される場合において、ログイン中のユーザに関するパスワードが当該画像データＰＤに対して自動的に付与される。したがって、転送後の画像データＰＤのセキュリティ確保を簡易に実現することができる。また、上記従来技術のようにメールでパスワードを報知する必要がないため、メール送信に伴うパスワードの漏洩リスクを回避できる。

【０１１２】

また特に、ボックスのセキュリティ付与フラグＦＢ（ＦＸ）の値（オンであるかオフであるか）に基づいて、セキュリティ情報を画像データに付与するか否かが決定されるので、全ての画像データに対してセキュリティ付与の是非を逐一指定する必要がない。すなわち、ボックス内の複数の画像データに対して一括的にセキュリティ付与の是非を決定することができる。

【０１１３】

さらに、画像データＰＤに設定されたセキュリティ付与フラグＦＢ（ＦＹ）の値にも基づいて、セキュリティ情報を画像データＰＤに付与するか否かが決定されるので、セキュリティ付与の是非を画像データごとに個別に指定することも可能である。

【０１１４】

なお、上述したように、セキュリティ情報としては、例えば、個人専用（ユーザ専用）のパスワード、あるいは、ユーザの所属グループに関するグループ共用のパスワード等が用いられる。例えば、ユーザＵＡ個人専用のパスワードを画像データＰＤに付加することによれば、装置外部に取り出された画像データＰＤに関するセキュリティを高度に維持することが可能である。あるいは、ユーザＵＡの所属グループであるグループＧ１のパスワードを画像データＰＤに付加することによれば、セキュリティを確保しつつ、ユーザＵＡの所属グループＧ１内の他人（例えばユーザＵＢ等）も、取り出し後の画像データを容易に閲覧することが可能である。

【０１１５】

さて一方、ボックスＢＲ１のセキュリティ付与フラグＦＢと画像データＰＤのセキュリティ付与フラグＦＢとの両方がオフ（ＯＦＦ）である場合には、セキュリティ情報を付与

すべきではないと判断されて、ステップＳ２３，Ｓ２４から、ステップＳ２６に進む。
【０１１６】
ステップＳ２６では、当該画像データに対してセキュリティ情報が付与されることなく、当該画像データがＭＦＰ１からコンピュータ９０へと転送される。
【０１１７】
例えば、図９に示すように、ボックスＢＲ１のセキュリティ付与フラグＦＢがオフであり、且つ、画像データＰＤ２のセキュリティ付与フラグＦＢもオフである場合には、画像データＰＤ２は、パスワードが付与されない状態で、そのままコンピュータ９０へと転送される。
【０１１８】
この場合には、転送された画像データＰＤ（ＰＤ２）をコンピュータ９０等で閲覧する際に、セキュリティ情報に基づく認証動作は求められない。すなわち、パスワード入力を求められることがない。したがって、セキュリティの確保が不要な場合には、転送後の画像データＰＤにさらに容易にアクセスすることが可能になる。
【０１１９】
また、上記の動作は、ユーザＵＡ（あるいはユーザの所属グループ）のパスワードが予め設定されていることを前提にして実行される。一方、ユーザＵＡ（あるいはユーザの所属グループ）のパスワードが設定されていない場合には、セキュリティ付与フラグＦＢの値にかかわらず、常に転送を許可しないようにすることが好ましい。例えば、ユーザＵＡのパスワードの設定の有無をステップＳ２２とステップＳ２３との間で判断し、ユーザＵＡ（あるいはユーザの所属グループ）のパスワードが設定されていない場合には、画像データの転送を行うことなく図７の処理を終了するようにすればよい。これによれば、セキュリティの低下を回避することができる。
【０１２０】
例えば、図９および図１０に示すように画像データＰＤ３のセキュリティ付与フラグＦＢ（ＦＹ）がオンである場合であっても、付与すべきパスワード（具体的には、ユーザＵＡのパスワードあるいはグループＧ１のパスワード等）が設定されていない場合には、画像データＰＤ３の転送は許可されないことが好ましい。
【０１２１】
また、上記の動作は、プライベートボックス、グループボックス、およびパブリックボックスのいずれに関しても同様に適用される。ただし、セキュリティ確保の観点から、各ボックス内の画像データＰＤを取り出すことが可能なユーザは、当該画像データＰＤに対するアクセス権限を有している者に制限されることが好ましい。換言すれば、コントローラ９は、ログイン中のユーザが画像データＰＤに対するアクセス権限を有していることを確認した上で、画像データを送信することが好ましい。なお、画像データＰＤに対するアクセス権限の有無は、画像データＰＤ自体に設定されたアクセス権限情報に基づいて決定されてもよく、および／または、当該画像データＰＤの格納先ボックスに設定されたアクセス権限情報に基づいて決定されてもよい。
【０１２２】
＜６－３．外部への取出動作（自機操作）＞
上記においては、外部装置（コンピュータ９０）からの転送指令に基づいて画像データＰＤをＭＦＰ１の外部へと転送する場合を例示したが、これに限定されない。
【０１２３】
例えば、図１１に示すように、ＭＦＰ１の操作入力部６１（操作パネル６３等）による操作入力に応じて、外部装置へと画像データを転送するようにしてもよい。詳細には、ＭＦＰ１のログインユーザが、操作パネル６３に表示される操作画面を操作することによって、ＭＦＰ１は、当該ログインユーザによる画像送信要求を受け付ける。そして、ＭＦＰ１は、当該画像送信要求に応答して、ＦＴＰ送信動作あるいは外部装置へのメール送信動作等によって、画像データを外部装置へ転送するようにしてもよい。
【０１２４】

＜６－４．内部でのコピー動作等＞

つぎに、画像データをＭＦＰ１の内部でコピーする動作について、図１２のフローチャートを参照しながら説明する。なお、ここでは、コピー動作について詳細に説明するが、画像データをＭＦＰ１の内部で移動する動作（移動動作）についても同様である。

【０１２５】

まず、ステップＳ３１において、或るユーザ（例えばユーザＵＡ）がＭＦＰ１の操作入力部６１を操作して、ＭＦＰ１にログインする。

【０１２６】

そして、ステップＳ３２において、ユーザＵＡは操作入力部６１の操作画面を利用して、ＭＦＰ１内の或るボックス（ここではプライベートボックスＢＲ１）内の画像データＰＤを、ＭＦＰ１内の別のボックス（ここではグループボックスＢＧ１）にコピーするための操作を実行する。

【０１２７】

ＭＦＰ１は、ユーザＵＡの当該操作に応答して、ステップＳ３３～Ｓ３６において、コピー対象（転送対象）の画像データＰＤをボックスＢＲ１からボックスＢＧ１へとコピー（転送）する動作を実行する。

【０１２８】

具体的には、まず、ステップＳ３３，Ｓ３４においては、転送対象の画像データＰＤに関して、当該画像データＰＤのセキュリティ付与フラグをオンにすべきか否かが決定される。詳細には、格納先の変更後における画像データ（コピー先の画像データ）ＰＤのセキュリティ付与フラグＦＢが、格納先の変更前における画像データ（コピー元の画像データ）ＰＤのセキュリティ付与フラグＦＢの値と、ボックスＢＲ１のセキュリティ付与フラグＦＢの値とに基づいて決定される。

【０１２９】

より詳細には、（画像データＰＤの格納先である）ボックスＢＲ１のセキュリティ付与フラグＦＢ（ＦＸ）がオン（ＯＮ）であることがステップＳ３３で確認される場合には、ステップＳ３５に進む。また、ボックスＢＲ１のセキュリティ付与フラグＦＢ（ＦＸ）がオフであっても、画像データＰＤのセキュリティ付与フラグＦＢ（ＦＹ）がオンであることがステップＳ３４で確認される場合には、ステップＳ３５に進む。このように、ボックスＢＲ１のセキュリティ付与フラグＦＢと画像データＰＤのセキュリティ付与フラグＦＢとの少なくとも一方がオンである場合には、ステップＳ３５に進む。

【０１３０】

ステップＳ３５では、画像データＰＤのセキュリティ付与フラグＦＢがオン状態に維持され或いはオン状態に変更されて、画像データＰＤが新たなボックスにコピーされる。

【０１３１】

ただし、画像データＰＤの内部移動時には、画像データＰＤに対してセキュリティ情報自体は付与されない。セキュリティ情報自体は、その後に、画像データＰＤがＭＦＰ１の外部に取り出される際に、条件に応じて画像データＰＤに対して付与される。具体的には、図１２の動作の後に、図８と同様の動作が実行される。すなわち、画像データＰＤのセキュリティ付与フラグＦＢ、および当該画像データＰＤの格納先のボックスのセキュリティ付与フラグＦＢの設定内容に応じて、セキュリティ情報の付与の有無が決定され画像データＰＤが取り出される。

【０１３２】

例えば、図１３に示すように、画像データＰＤがプライベートボックスＢＲ１からグループボックスＢＧ１へとユーザＵＡの操作によってコピーされた後に、さらに、コンピュータ９０を用いて同じユーザＵＡによってＭＦＰ１の外部へと取り出される場合を想定する。この場合には、画像データＰＤは、図８に示すような動作によって、例えばユーザＵＡに関するパスワード設定を伴ってコンピュータ９０へと転送される。なお、これに限定されず、グループＧ１に関するパスワードが設定されて画像データＰＤがコンピュータ９０へと送信されるようにしてもよい。

【０１３３】
また、画像データＰＤがグループボックスＢＧ１へコピーされると、グループＧ１のメンバーが（特にユーザＵＡ以外のユーザ（ＵＢ，ＵＣ）も）、画像データＰＤにアクセスすることが可能になる。
【０１３４】
そのため、例えば、図１４に示すように、画像データＰＤがボックスＢＲ１からボックスＢＧ１へとユーザＵＡの操作によってコピーされた後に、さらに、今度は別のユーザＵＢによってコンピュータ９０へと取り出される場合も想定される。この場合には、画像データＰＤは、図８に示すような動作によって、例えば「ユーザＵＢ」に関するパスワード設定を伴ってコンピュータ９０へと転送される。なお、これに限定されず、（ユーザに関するパスワードではなく、）ユーザＵＢの所属グループであるグループＧ１に関するパスワードが設定された画像データＰＤがコンピュータ９０へと送信されるようにしてもよい。
【０１３５】
その後、転送された画像データＰＤをコンピュータ９０等で閲覧する際には、セキュリティ情報に基づく認証動作が求められる。具体的には、パスワード入力が求められる。閲覧ユーザは、正規のパスワードを入力することによって、当該画像データＰＤを閲覧することが可能である。したがって、ＭＦＰ１内に格納された画像データＰＤが外部のコンピュータ９０に転送される場合であっても、転送後の画像データＰＤのセキュリティ確保を簡易に実現することができる。
【０１３６】
特に、プライベートボックスＢＲ１のセキュリティ付与フラグＦＢがオンである場合には、図１２の動作によって、グループボックスＢＧ１にコピーされた画像データＰＤ（すなわち格納先変更後における画像データＰＤ）のセキュリティ付与フラグＦＢは、オンに設定される。すなわち、格納先変更後における画像データＰＤのセキュリティ付与フラグＦＢの値に、ボックスＢＲ１のセキュリティ付与フラグの値を反映させることができる。したがって、装置内部での画像データＰＤの格納先が変更された後に当該画像データＰＤが外部へ送信される場合でも、画像データＰＤに関するセキュリティの低下を防止することが可能である。
【０１３７】
また、格納先変更前における画像データＰＤのセキュリティ付与フラグＦＢがオンである場合には、格納先変更後における画像データＰＤのセキュリティ付与フラグＦＢも、オンに設定される。すなわち、格納先変更後における画像データＰＤのセキュリティ付与フラグＦＢの値に、格納先変更前における画像データＰＤのセキュリティ付与フラグＦＢの値を反映させることができる。したがって、画像データＰＤに関するセキュリティの低下を防止することが可能である。特に、コピーが複数世代にわたって繰り返されたとしても、セキュリティの低下を防止することが可能である。
【０１３８】
一方、ボックスＢＲ１のセキュリティ付与フラグＦＢと画像データＰＤのセキュリティ付与フラグＦＢとの両方がオフ（ＯＦＦ）である場合には、ステップＳ３６に進む。
【０１３９】
ステップＳ３６では、画像データＰＤのセキュリティ付与フラグＦＢがオフ状態に維持されて、画像データＰＤがコピー先の新たなボックス（例えばグループボックスＢＧ１）にコピーされる。
【０１４０】
また、ステップＳ３６の後に、画像データＰＤが外部に移動される場合には、当該画像データＰＤのコピー先のボックスのセキュリティ付与フラグＦＢに依存して、セキュリティ付与の有無が決定される。すなわち、グループボックスＢＧ１のセキュリティ付与フラグＦＢがオンの場合にはステップＳ２５の動作が実行され、グループボックスＢＧ１のセキュリティ付与フラグＦＢがオフの場合には、ステップＳ２６の動作が実行される（図８

）。

【０１４１】

また、上述の内部でのコピー動作（および移動動作）は、プライベートボックス、グループボックス、およびパブリックボックスのいずれに関しても同様に適用される。ただし、ＭＦＰ１は、コピー指令を付与するユーザが少なくともコピー元のボックスに対するアクセス権限を有していることを条件に、コピー動作を許可することが好ましい。また、ＭＦＰ１は、コピー指令を付与するユーザがコピー先のボックスに対するアクセス権限をも有していることを条件に、コピー動作を許可することが好ましい。また、コピー先の画像データＰＤをＭＦＰ１の外部へ送信する動作は、当該コピー先のボックスのアクセス権限を有するユーザに対してのみ許可されることが好ましい。

【０１４２】

以上のように、画像データＰＤが装置内部でボックスＢＲ１から別のボックスＢＧ１へとコピー（あるいは移動）する際には、未だ画像データＰＤに対してパスワードロックをかけることを行わず、その後に画像データＰＤが外部装置に送信される際に、画像データＰＤに対してパスワードロックをかけることが行われる。これによれば、装置内部でのコピー動作等における制約を最小限に止めることができる。

【０１４３】

また、その後、画像データＰＤがボックスＢＧ１から装置外部へと取り出される際には、当該画像データＰＤの取出指示者であるユーザに関するパスワードが当該画像データＰＤに対して付与される。これによれば、画像データＰＤが外部へと取り出される際に、当該画像データＰＤのセキュリティ確保を簡易に実現することができる。なお、上述したように、画像データＰＤがボックスＢＧ１から装置外部へと取り出される際に、当該画像データＰＤの取出指示者であるユーザの所属グループに関するパスワードが当該画像データＰＤに対して付与されてもよい。これによれば、同一グループの他のユーザが画像データＰＤを容易に閲覧することが可能である。

【０１４４】

＜７．その他＞

以上、この発明の実施の形態について説明したが、この発明は上記説明した内容のものに限定されるものではない。

【０１４５】

たとえば、上記実施形態においては、装置内部で画像データＰＤをコピーする際に画像データＰＤのセキュリティ付与フラグＦＢの値を、ボックスのセキュリティ付与フラグＦＢの値に応じて自動的にオンに変更する場合（ステップＳ３３，Ｓ３５）を例示したが、これに限定されない。具体的には、装置内部でのコピー動作等の際には、画像データＰＤのセキュリティ付与フラグＦＢの設定内容を変更せずに維持するようにしてもよい。

【０１４６】

また、上記実施形態においては、画像データＰＤが装置内部でコピーされる際には画像データＰＤに対するセキュリティ情報自体は付与されない場合を例示したが、これに限定されない。例えば、画像データＰＤが装置内部でコピーされる際にも、画像データＰＤに対してセキュリティ情報（パスワード等）自体が自動的に付与されるようにしてもよい。

【０１４７】

また、上記実施形態においては、グループ共用のパスワードと個人専用のパスワードとが装置全体において二者択一的に切り替えられて設定される場合を例示しているが、これに限定されない。

【０１４８】

具体的には、取り出し対象のボックス種別に応じて、設定すべきパスワードを変更するようにしてもよい。具体的には、１）プライベートボックスからの取り出しには「個人専用のパスワード」を設定し、２）グループボックスからの取り出しには「グループ共用のパスワード」を設定するようにしてもよい。

【０１４９】

また、上記実施形態においては、ユーザあるいはグループに関するパスワードが画像データＰＤに付与される場合を例示したが、これに限定されない。例えば、ボックス自体に設定されたパスワード（ボックスに関するパスワード）が、画像データＰＤに自動的に付与されてＭＦＰ１の外部装置へ送信されてもよい。より詳細には、ボックスＢＧ１内の画像データＰＤが外部のコンピュータ９０に送信される際には、ボックスごとに設定されているパスワード（ここではボックスＢＧ１自体に設定されているパスワード）が画像データＰＤに自動的に付与されるようにしてもよい。

【図面の簡単な説明】

【０１５０】

【図１】ＭＦＰを備える画像送受信システムの構成を示す概略図である。

【図２】各ユーザの所属グループを示す図である。

【図３】格納部内におけるボックス構成を示す概念図である。

【図４】各ボックスに関する情報の一例を示す図である。

【図５】各画像データに関する情報の一例を示す図である。

【図６】パスワード種別を設定する設定画面を示す図である。

【図７】画像データをボックスへ格納する動作を示すフローチャートである。

【図８】ボックス内の画像データを装置外部へと取り出す動作を示すフローチャートである。

【図９】ボックス内の画像データを装置外部へと取り出す動作を示す概念図である（ボックスのセキュリティ付与フラグがオフの場合）。

【図１０】ボックス内の画像データを装置外部へと取り出す動作を示す概念図である（ボックスのセキュリティ付与フラグがオンの場合）。

【図１１】ＭＦＰの操作入力部により受け付けられた画像送信要求に応答して、画像データが外部装置へ転送される動作を示す概念図である。

【図１２】画像データの内部コピー動作を示すフローチャートである。

【図１３】内部コピー動作と外部取り出し動作とが同一人物によって実行される様子を示す概念図である。

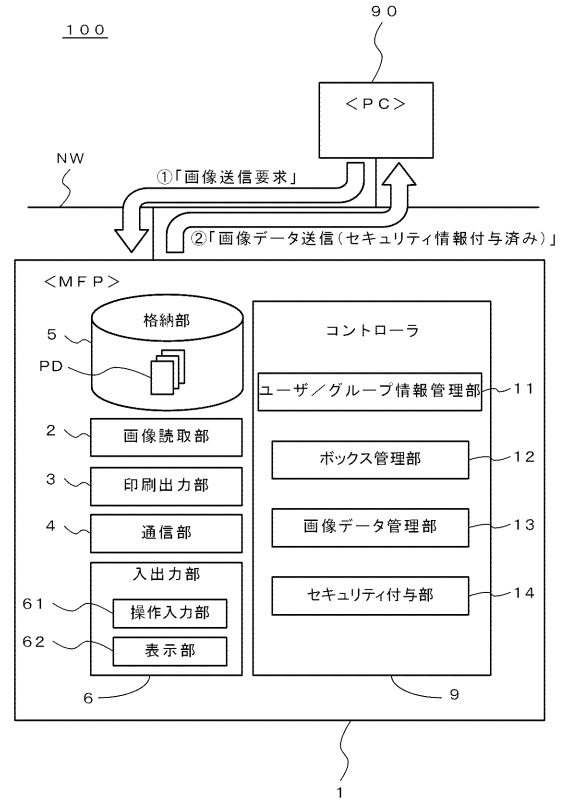
【図１４】内部コピー動作と外部取り出し動作とが異なる人物によって実行される様子を示す概念図である。

【符号の説明】

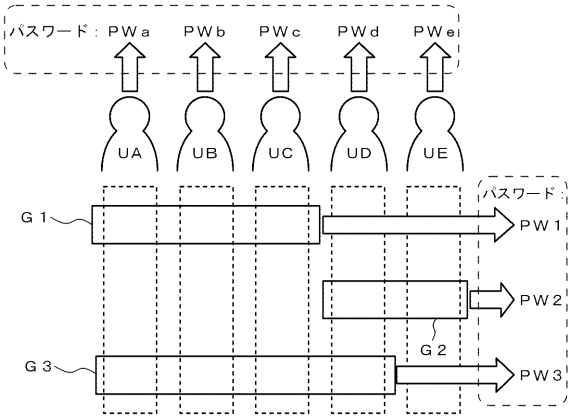
【０１５１】

１　ＭＦＰ
６３　操作パネル
９０　コンピュータ
ＢＢ１　パブリックボックス
ＢＧ１～ＢＧ４　グループボックス
ＢＲ１～ＢＲ６　プライベートボックス
ＦＢ　セキュリティ付与フラグ
Ｇ１～Ｇ３　グループ
ＵＡ～ＵＥ　ユーザ

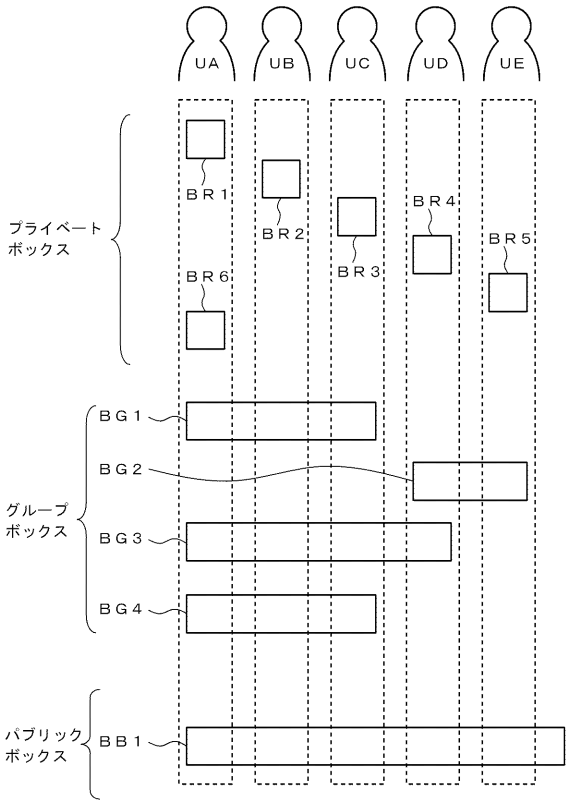
【図１】


100
90
＜PC＞
NW
①「画像送信要求」
②「画像データ送信（セキュリティ情報付与済み）」
＜MFP＞
格納部
5
PD
コントローラ
ユーザ／グループ情報管理部
11
2
画像読取部
ボックス管理部
12
3
印刷出力部
4
通信部
画像データ管理部
13
入出力部
61
操作入力部
セキュリティ付与部
14
62
表示部
6
9
1

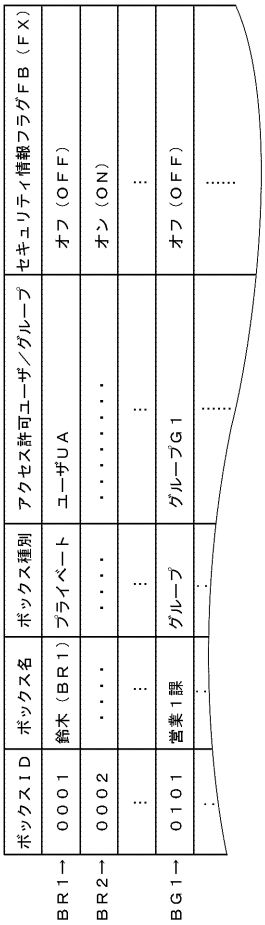
【図２】


パスワード：PWa
PWb
PWc
PWd
PWe
UA
UB
UC
UD
UE
パスワード：
G1
PW1
PW2
G2
G3
PW3

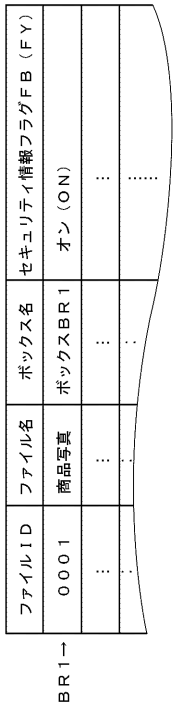
【図３】


UA
UB
UC
UD
UE
プライベート
ボックス
BR1
BR2
BR3
BR4
BR5
BR6
グループ
ボックス
BG1
BG2
BG3
BG4
パブリック
ボックス
BB1

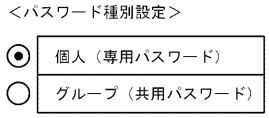
【図４】


ボックスID
ボックス名
ボックス種別
アクセス許可ユーザ／グループ
セキュリティ情報フラグFB（FX）
0001
鈴木（BR1）
プライベート
ユーザUA
オフ（OFF）
0002
オン（ON）
0101
営業1課
グループ
グループG1
オフ（OFF）
BR1→
BR2→
BG1→

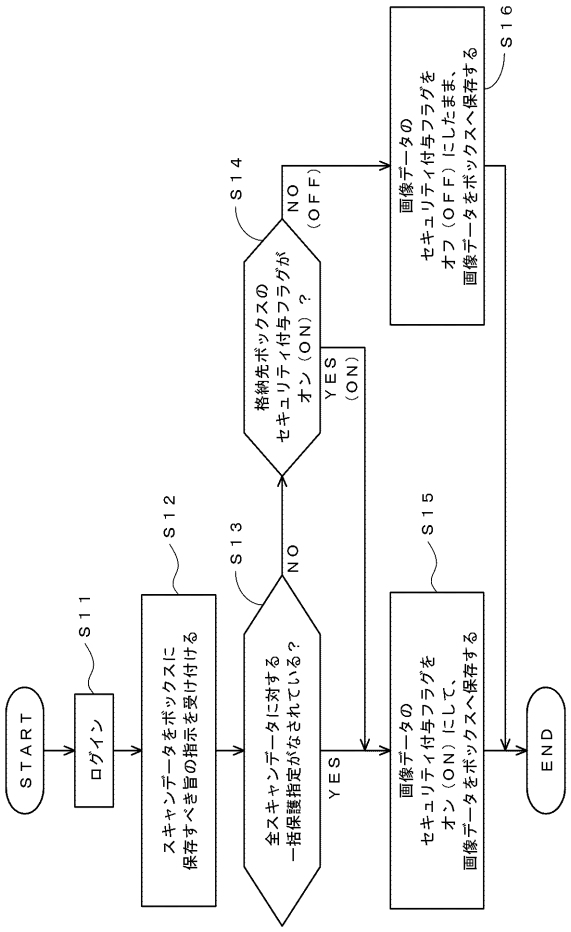
【図５】


ファイルＩＤ
ファイル名
ボックス名
セキュリティ情報フラグＦＢ（ＦＹ）
０００１
商品写真
ボックスＢＲ１
オン（ＯＮ）
ＢＲ１→

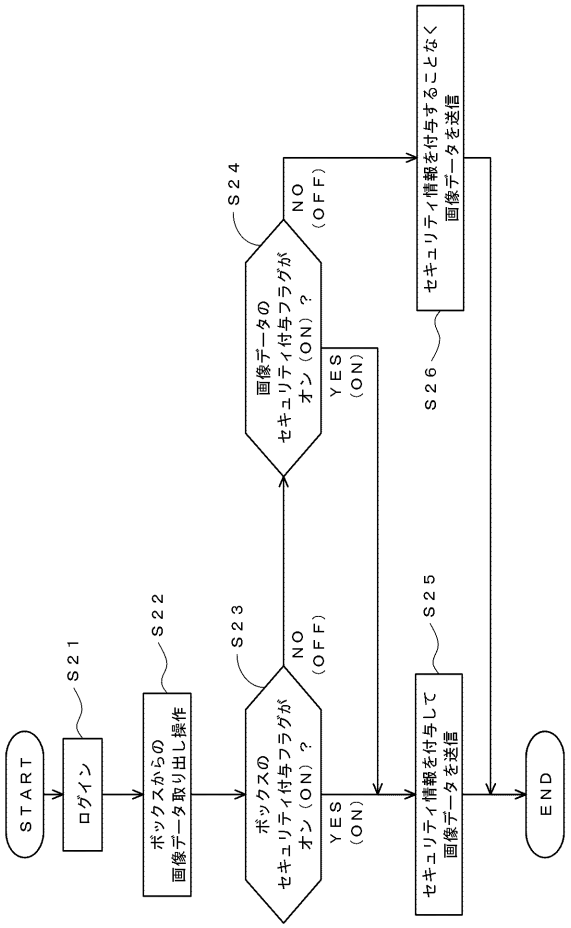
【図６】


<パスワード種別設定>
個人（専用パスワード）
グループ（共用パスワード）

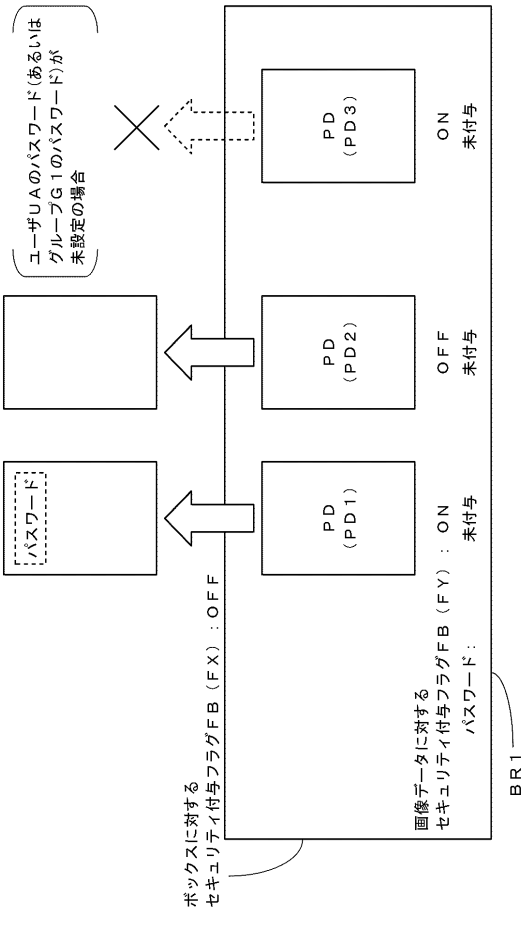
【図７】


ＳＴＡＲＴ
ＳＴＡＲＴ
ログイン
Ｓ１１
スキャンデータをボックスに
保存すべき旨の指示を受け付ける
Ｓ１２
全スキャンデータに対する
一括保護指定がなされている？
Ｓ１３
ＮＯ
ＹＥＳ
格納先ボックスの
セキュリティ付与フラグが
オン（ＯＮ）？
Ｓ１４
ＮＯ
（ＯＦＦ）
ＹＥＳ
（ＯＮ）
画像データの
セキュリティ付与フラグを
オン（ＯＮ）にして、
画像データをボックスへ保存する
Ｓ１５
画像データの
セキュリティ付与フラグを
オフ（ＯＦＦ）にしたまま、
画像データをボックスへ保存する
Ｓ１６
ＥＮＤ
ＥＮＤ

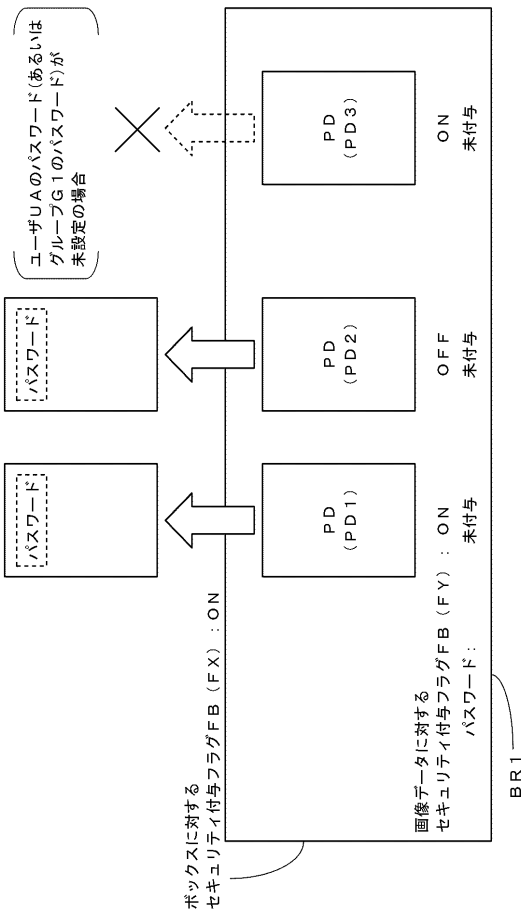
【図８】


ＳＴＡＲＴ
ＳＴＡＲＴ
ログイン
Ｓ２１
ボックスからの
画像データ取り出し操作
Ｓ２２
ボックスの
セキュリティ付与フラグが
オン（ＯＮ）？
Ｓ２３
ＮＯ
（ＯＦＦ）
ＹＥＳ
（ＯＮ）
セキュリティ情報を付与して
画像データを送信
Ｓ２５
画像データの
セキュリティ付与フラグが
オン（ＯＮ）？
Ｓ２４
ＮＯ
（ＯＦＦ）
ＹＥＳ
（ＯＮ）
セキュリティ情報を付与することなく
画像データを送信
Ｓ２６
ＥＮＤ
ＥＮＤ

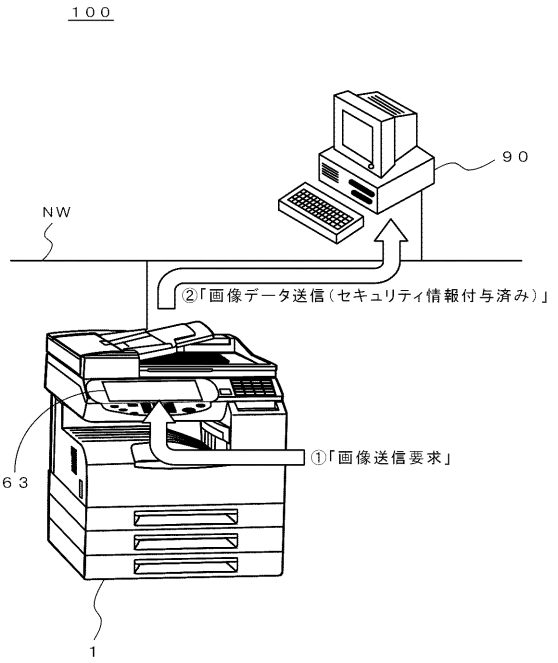
【図９】


ユーザＵＡのパスワード（あるいは
グループＧ１のパスワード）が
未設定の場合
パスワード
ＰＤ
（ＰＤ１）
ＰＤ
（ＰＤ２）
ＰＤ
（ＰＤ３）
ＯＮ
未付与
ＯＦＦ
未付与
ＯＮ
未付与
ボックスに対する
セキュリティ付与フラグＦＢ（ＦＸ）：ＯＦＦ
画像データに対する
セキュリティ付与フラグＦＢ（ＦＹ）：ＯＮ
パスワード：
ＢＲ１

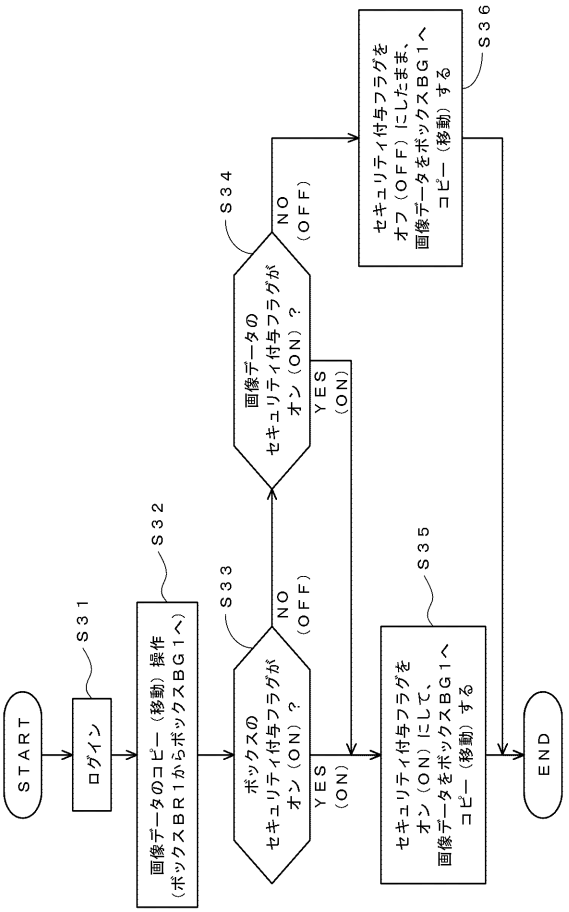
【図１０】



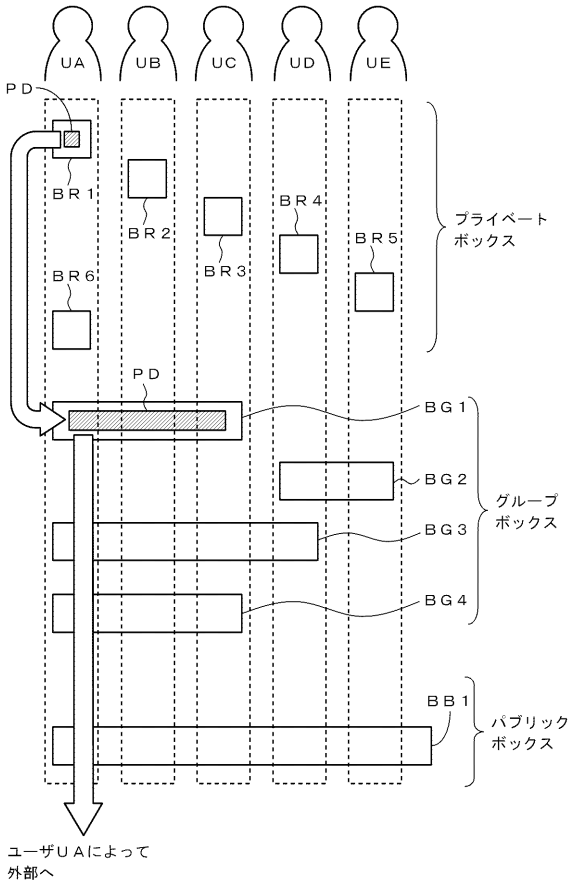
【図１１】



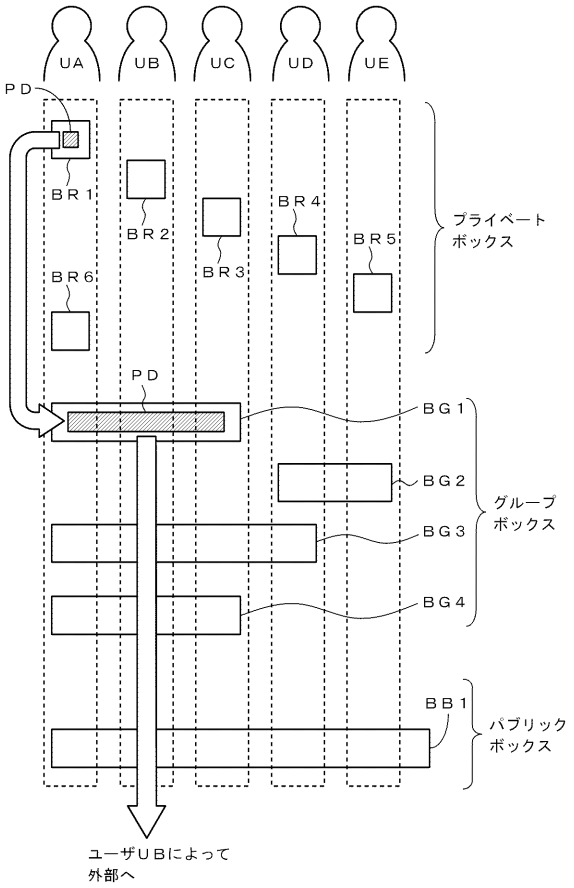
【図１２】



【図１３】



【図１４】


UA
UB
UC
UD
UE
ＰＤ
ＢＲ１
ＢＲ２
ＢＲ３
ＢＲ４
ＢＲ５
ＢＲ６
プライベート
ボックス
ＰＤ
ＢＧ１
ＢＧ２
ＢＧ３
ＢＧ４
グループ
ボックス
ＢＢ１
パブリック
ボックス
ユーザＵＢによって
外部へ

フロントページの続き

(51)Int.Cl. FI
B41J 29/38 Z

(56)参考文献 特開平０８－０９８００８（ＪＰ，Ａ）
特開２００７－０６７８４０（ＪＰ，Ａ）
特開２００６－２２９４２９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ１／００
Ｈ０４Ｎ１／４４
Ｇ０６Ｆ３／１２
Ｂ４１Ｊ２９／３８
Ｇ０６Ｆ１２／００