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

特許第5096266号
(P5096266)

(45)発行日　平成24年12月12日(2012.12.12)　(24)登録日　平成24年9月28日(2012.9.28)

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

請求項の数 15　(全 20 頁)

(21)出願番号　特願2008-222125 (P2008-222125)
(22)出願日　平成20年8月29日 (2008.8.29)
(65)公開番号　特開2010-55521 (P2010-55521A)
(43)公開日　平成22年3月11日 (2010.3.11)
審査請求日　平成23年6月13日 (2011.6.13)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　田中　沙樹
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　安島　智也

最終頁に続く

(54)【発明の名称】画像形成装置、印刷制御方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手段と、

操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手段と、

前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手段と、

認証された前記印刷データを印刷させる印刷制御手段と、

前記認証が行われるまでに、前記印刷データに含まれるユーザ識別情報に対応するパスワードを前記管理手段より取得し、取得されたパスワードによって当該印刷データに含まれているパスワードを更新するパスワード更新手段とを有する画像形成装置。

【請求項２】

前記パスワード更新手段は、前記印刷データの受信に応じ、又は前記印刷データの保存に応じ、前記印刷データに含まれているパスワードを更新する請求項１記載の画像形成装置。

【請求項３】

前記パスワード更新手段は、前記操作者のユーザ識別情報及びパスワードを特定する情

報の入力に応じ、前記印刷データに含まれているパスワードを更新する請求項１記載の画像形成装置。
【請求項４】
前記パスワード更新手段は、前記印刷制御手段が前記印刷データを印刷させる際に前記印刷データに含まれているパスワードを更新する請求項１記載の画像形成装置。
【請求項５】
ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手段と、
操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手段と、
前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手段と、
認証された前記印刷データを印刷させる印刷制御手段と、
前記認証が行われるまでに、前記印刷データに含まれているパスワードを前記管理手段に登録するパスワード登録手段とを有する画像形成装置。
【請求項６】
画像形成装置が実行する印刷制御方法であって、
ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手順と、
操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手順と、
前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手順と、
認証された前記印刷データを印刷させる印刷制御手順と、
前記認証が行われるまでに、前記印刷データに含まれるユーザ識別情報に対応するパスワードを前記管理手段より取得し、取得されたパスワードによって当該印刷データに含まれているパスワードを更新するパスワード更新手順とを有する印刷制御方法。
【請求項７】
前記パスワード更新手順は、前記印刷データの受信に応じ、又は前記印刷データの保存に応じ、前記印刷データに含まれているパスワードを更新する請求項６記載の印刷制御方法。
【請求項８】
前記パスワード更新手順は、前記操作者のユーザ識別情報及びパスワードを特定する情報の入力に応じ、前記印刷データに含まれているパスワードを更新する請求項６記載の印刷制御方法。
【請求項９】
前記パスワード更新手順は、前記印刷制御手順が前記印刷データを印刷させる際に前記印刷データに含まれているパスワードを更新する請求項６記載の印刷制御方法。
【請求項１０】
画像形成装置が実行する印刷制御方法であって、
ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手順と、
操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手順と、
前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて

、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手順と、
認証された前記印刷データを印刷させる印刷制御手順と、
前記認証が行われるまでに、前記印刷データに含まれているパスワードを前記管理手段に登録するパスワード登録手順とを有する印刷制御方法。
【請求項１１】
画像形成装置に、
ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手順と、
操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手順と、
前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手順と、
認証された前記印刷データを印刷させる印刷制御手順と、
前記認証が行われるまでに、前記印刷データに含まれるユーザ識別情報に対応するパスワードを前記管理手段より取得し、取得されたパスワードによって当該印刷データに含まれているパスワードを更新するパスワード更新手順とを実行させるためのプログラム。
【請求項１２】
前記パスワード更新手順は、前記印刷データの受信に応じ、又は前記印刷データの保存に応じ、前記印刷データに含まれているパスワードを更新する請求項１１記載のプログラム。
【請求項１３】
前記パスワード更新手順は、前記操作者のユーザ識別情報及びパスワードを特定する情報の入力に応じ、前記印刷データに含まれているパスワードを更新する請求項１１記載のプログラム。
【請求項１４】
前記パスワード更新手順は、前記印刷制御手順が前記印刷データを印刷させる際に前記印刷データに含まれているパスワードを更新する請求項１１記載のプログラム。
【請求項１５】
画像形成装置に、
ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手順と、
操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手順と、
前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手順と、
認証された前記印刷データを印刷させる印刷制御手順と、
前記認証が行われるまでに、前記印刷データに含まれているパスワードを前記管理手段に登録するパスワード登録手順とを実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像形成装置、印刷制御方法、及びプログラムに関し、特にユーザの認証に応じて印刷を実行する画像形成装置、印刷制御方法、及びプログラムに関する。
【背景技術】
【０００２】

従来、ユーザ名及びパスワードを含む印刷データをＰＣ（Personal Computer）から画像形成装置に送信し、画像形成装置内において当該ユーザ名及びパスワードに基づく認証が成功した場合に印刷ジョブが実行され、認証に失敗した場合には印刷ジョブの実行が拒否される技術が知られている（例えば、特許文献１、特許文献２）。当該技術によれば、オフィス等において共用される画像形成装置によって実行される印刷ジョブのセキュリティを向上させることができる。

【特許文献１】特開平１０－２０７６６１号公報

【特許文献２】特開２００６－０１８６５４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しかしながら、従来の技術では、印刷データのパスワード等は、ＰＣにおいて印刷指示が行われる際に設定される。また、画像形成装置において印刷データのパスワード等と照合されるパスワード等は、予めユーザ情報として画像形成装置内に設定される。このように、双方のパスワードは別々に（異なるタイミングで）設定される。したがって、印刷ジョブの実行時には双方のパスワードが一致しないことがある。この場合、正当なユーザであるにも拘わらず、印刷ジョブが実行されないという不都合が生じる。斯かる不都合が生じる可能性がある具体例して、例えば、以下のようなケースが挙げられる。

【０００４】

第一のケースは、ユーザが誤って、又は管理者によってパスワードが更新されていることを知らずに、印刷指示時に古いパスワードを入力した場合である。この場合、印刷データには古いパスワードが設定され、ユーザ情報として管理されているパスワードとは一致しない。

【０００５】

第二のケースは、ユーザ名及びパスワードが設定された印刷データが画像形成装置においてスプールされた後、その数日後にユーザが画像形成装置にログインし、スプールさている印刷データの印刷指示を行った場合である。この場合、印刷データにパスワード等が設定されてから画像形成装置において印刷指示が入力されるまでの間にユーザ情報として管理されているパスワードが更新されてしまうと、印刷データのパスワード等とユーザ情報のパスワード等は一致しない。

【０００６】

第三のケースは、ユーザ名及びパスワードが設定された印刷データが画像形成装置においてスプールされた後、ユーザが画像形成装置にログインし、スプールさている印刷データの印刷指示を行い、例えば、スケジュール機能又は印刷ジョブの蓄積状況等によりその数日後に印刷ジョブが開始される場合である。この場合、印刷指示が行われてから印刷ジョブが開始されるまでの間にユーザ情報として管理されているパスワードが更新されてしまうと、印刷ジョブの実行時に印刷データのパスワード等とユーザ情報のパスワード等は一致しない。

【０００７】

なお、一般的に、セキュリティ上の観点よりユーザ情報として管理されているパスワードは定期的に変更されることに鑑みれば、以上のような事態の発生は十分考えられる。

【０００８】

本発明は、上記の点に鑑みてなされたものであって、印刷データに含まれているパスワード等に基づく認証処理を適切に実行することのできる画像形成装置、印刷制御方法、及びプログラムの提供を目的とする。

【課題を解決するための手段】

【０００９】

そこで上記課題を解決するため、本発明は、ユーザ識別情報及びパスワードを含む印刷データを受信し、該印刷データを記憶装置に保存する印刷データ受信手段と、操作者のユーザ識別情報及びパスワードを特定する情報の入力を受け付け、ユーザ識別情報とパスワ

ードとの対応情報を管理する管理手段に基づいて該ユーザの認証を行うユーザ認証手段と、前記操作者のユーザ識別情報と一致するユーザ識別情報を含む前記印刷データについて、当該印刷データに含まれるユーザ識別情報及びパスワードと前記管理手段とに基づいて認証を行う印刷データ認証手段と、認証された前記印刷データを印刷させる印刷制御手段と、前記認証が行われるまでに、前記印刷データに含まれるユーザ識別情報に対応するパスワードを前記管理手段より取得し、取得されたパスワードによって当該印刷データに含まれているパスワードを更新するパスワード更新手段とを有することを特徴とする。

【００１０】

このような画像形成装置では、印刷データに含まれているパスワード等に基づく認証処理を適切に実行することができる。

【発明の効果】

【００１１】

本発明によれば、印刷データに含まれているパスワード等に基づく認証処理を適切に実行することができる。

【発明を実施するための最良の形態】

【００１２】

以下、図面に基づいて本発明の実施の形態を説明する。図１は、本発明の実施の形態における画像形成装置のハードウェア構成例を示す図である。図１において、画像形成装置１０は、スキャン、コピー、及び印刷等の複数の機能を一台の筐体において実現する複合機であり、ＣＰＵ１０１、メモリ１０２、記録媒体１０３、ネットワークＩ／Ｆ１０４、画像出力部１０５、画像処理部１０６、外部デバイスＩ／Ｆ１０７、表示部１０８、及び操作部１０９等を有する。

【００１３】

画像形成装置１０での機能を実現するプログラムは、ＨＤＤ（Hard Disk Drive）等の不揮発性の記録媒体１０３に記録（インストール）される。記録媒体１０３は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。メモリ１０２は、プログラムの起動指示があった場合に、記録媒体１０３からプログラムを読み出して格納する。ＣＰＵ１０１は、メモリ１０２に格納されたプログラムに従って画像形成装置１０に係る機能を実現する。ネットワークＩ／Ｆ１０４は、ネットワークに接続するためのインタフェースとして用いられる。

【００１４】

表示部１０８は、ＬＣＤ（Liquid Crystal Display）等によって構成され、操作画面やメッセージ等を表示させる。操作部１０９は、ハード的なボタン（キー）によって構成され、ユーザによる操作入力を受け付ける入力手段である。なお、表示部１０８及び操作部１０９は、オペレーションパネルとして一体的に構成されてもよい。

【００１５】

画像処理部１０６は、画像データを出力（印刷）等する際に必要とされる各種の画像処理を実行する。画像出力部１０５は、画像データの出力（印刷）を行う。

【００１６】

外部デバイスＩ／Ｆ１０７は、認証のためのユーザ情報の入力に用いられるカードリーダーと接続するためのインタフェースであり、例えば、ＵＳＢポート（ＵＳＢホストインタフェース）又はシリアルポート等によって構成される。カードリーダー３０は、カード５０から情報を読み取るいわゆるカードリーダーであり、外部デバイスＩ／Ｆ１０７と接続可能なハードウェアインタフェース（例えば、ＵＳＢコネクタ又はシリアルインタフェース等）を備える。但し、カードリーダー３０は、画像形成装置１０に内蔵されていてもよい。カードリーダー３０は、接触型又は非接触型のいずれであってもよい。カード５０は、ＩＣカードに限定されず、磁気カード等、少なくとも各カード５０に一意なカードＩＤ（カード番号）が記録可能なものであればよい。カードＩＤは、一般的に、Ｕｎｉｖｅｒｓａｌ　ＩＤ又はＣａｒｄ　Ｓｅｒｉａｌ　Ｎｕｍｂｅｒと呼ばれる。カード５０の具体例の一部としては、Ｐｒｏｘｉｍｉｔｙカード、Ｍｉｆａｒｅカード、Ｊａｖａ（登録

商標）Ｃａｒｄ等が挙げられる。

【００１７】

本実施の形態において、カード５０は各ユーザに配布されていることとする。但し、運用上必要とされるセキュリティのレベルに応じて、複数のユーザによって一枚のカード５０を共用させてもよい。なお、各ユーザに配布されるカード５０は一種類に限定されなくてもよい。上記のようにカードリーダー３０は、ＵＳＢ等によって簡便に画像形成装置１０に接続することが可能である。したがって、それぞれ対応するカード５０の種類（Ｐｒｏｘｉｍｉｔｙカード、Ｍｉｆａｒｅカード、Ｊａｖａ（登録商標）Ｃａｒｄ等）が異なる複数のカードリーダー３０を画像形成装置１０に同時に接続させてもよい。この場合、複数種類のカード５０を同時に利用することができる。

【００１８】

同図において、画像形成装置１０は、ネットワーク（有線又は無線の別を問わない。）を介して印刷データ送信装置２０と接続されている。印刷データ送信装置２０は、ユーザによる印刷指示の入力に応じて、印刷指示の対象とされた文書データを画像形成装置１０に解釈可能な印刷データに変換し、当該印刷データの印刷要求（印刷ジョブ）を画像形成装置１０に送信するコンピュータである。

【００１９】

本実施の形態において、印刷データ送信装置２０は、機密印刷の実行を画像形成装置１０に要求する。図２は、機密印刷の概要を説明するための図である。

【００２０】

機密印刷を行う場合、ユーザは、印刷指示と共にユーザ名（ユーザＩＤ）及びパスワードを印刷データ送信装置２０に入力する（Ｓ１１）。印刷データ送信装置２０は、印刷対象とされた文書データの印刷データを生成し、当該印刷データにユーザ名及びパスワードを含めて画像形成装置１０に送信する（Ｓ１２）。画像形成装置１０は、ユーザ名及びパスワードを含む印刷データを受信すると、直ちに印刷は実行せずに当該印刷データを記録媒体１０３に保存する。その後、ユーザが画像形成装置１０にログインし、保存されている印刷データの印刷を指示すると（Ｓ１３）、画像形成装置１０は、当該印刷データの印刷を実行する（Ｓ１４）。

【００２１】

このような機密印刷によれば、印刷指示を行ったユーザが画像形成装置１０の側に居ることが確認された場合にのみ印刷が実行される。したがって、特に、機密性の高い文書を印刷する際の情報漏洩の防止に有効である。

【００２２】

斯かる機密印刷を実行するために画像形成装置１０は次のような機能構成を有する。図３は、第一の実施の形態における画像形成装置の機能構成例を示す図である。同図において、画像形成装置１０は、印刷データ受信部１１、ログイン制御部１２、機密印刷制御部１３、印刷ジョブ制御部１４、印刷データ認証部１５、パスワード更新部１６、印刷データ保存部１７、及びユーザＤＢ１８等を有する。これら各部は、画像形成装置１０にインストールされたプログラムがＣＰＵ１０１に実行させる処理によって実現される。

【００２３】

印刷データ受信部１１は、印刷データ送信装置２０より送信される印刷データを受信し、印刷データ保存部１７に保存する。印刷データ保存部１７は、印刷データをスプールしておくための記憶領域であり、例えば、記録媒体１０３上に形成される。ログイン制御部１２は、画像形成装置１０に対する操作者（ユーザ）のログイン処理を制御する。ログイン処理の際に、ユーザＤＢ１８に登録されているユーザ名及びパスワードに基づいて操作者の認証が行われる。ユーザＤＢ１８は、例えば、記録媒体１０３を用いてユーザごとにユーザ情報を管理するデータベースである。ユーザ情報の一部としてユーザ名及びパスワードが含まれている。なお、ユーザＤＢ１８は、画像形成装置１０とネットワークを介して接続するコンピュータにおいて一元的に管理されていてもよい。機密印刷制御部１３は、印刷データ保存部１７に保存されている印刷データに関する印刷ジョブの実行要求を操

作者より受け付けるための処理を制御する。印刷ジョブ制御部１４は、機密印刷制御部１３によって受け付けられた印刷ジョブの実行要求に応じ、印刷データの印刷を画像出力部１０５に実行させる。印刷データ認証部１５は、印刷データに含まれているユーザ名及びパスワードを、ユーザＤＢ１８に登録されているユーザ名及びパスワードと照合することにより印刷データの認証を行う。パスワード更新部１６は、印刷データに含まれているパスワードを、ユーザＤＢ１８に登録されているパスワードによって必要に応じて更新する（書き換える）。第一の実施の形態において、パスワード更新部１６は、印刷データ受信部１１による印刷データの受信に応じ、又は印刷データ保存部１７への印刷データの保存に応じ、当該印刷データのパスワードを更新する。

【００２４】

以下、画像形成装置１０の処理手順について説明する。図４は、第一の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図である。

【００２５】

印刷データ送信装置２０において、プリンタドライバ２１は、機密印刷ジョブの実行要求の入力に応じ、ユーザ名及びパスワードをユーザに入力させる（Ｓ１０１）。ユーザ名及びパスワードは、認証情報入力画面を介して入力される。

【００２６】

図５は、プリンタドライバが表示させる認証情報入力画面の表示例を示す図である。同図において、認証情報入力画面４１０は、ユーザ名入力領域４１１及びパスワード入力領域４１２等を有する。プリンタドライバ２１は、認証情報入力画面４１０を介して入力されたユーザ名及びパスワードを印刷データに設定して画像形成装置１０に送信する。但し、パスワードは必ずしも入力されなくてもよい。パスワードが入力されない場合、プリンタドライバ２１は、ユーザ名のみを印刷データに設定する。なお、認証情報入力画面４１０は、印刷条件を設定させる印刷設定画面上の所定のボタンが押下されると表示される。

【００２７】

続いて、プリンタドライバ２１は、印刷対象とされた文書データの印刷データを生成すると共に入力されたユーザ名及びパスワードを当該印刷データに設定し、当該印刷データを画像形成装置１０に送信する（Ｓ１０２）。

【００２８】

画像形成装置１０の印刷データ受信部１１は、印刷データを受信すると、当該印刷データに設定されているパスワードの検査をパスワード更新部１６に実行させる（Ｓ１０３）。パスワード更新部１６は、印刷データにパスワードが設定されているか否かを判定し、パスワードが含まれていない場合は、当該印刷データに設定されているユーザ名に対応するパスワードをユーザＤＢ１８より取得し、当該パスワードを印刷データに設定する（Ｓ１０４）。また、印刷データにパスワードが設定されている場合は、当該パスワードがユーザＤＢ１８において当該印刷データに設定されているユーザ名に対応するものと一致するか否かを判定し、一致しない場合はユーザＤＢ１８に登録されているパスワードによって印刷データに設定されているパスワードを更新する（Ｓ１０５）。パスワード更新部１６によるパスワードの検査が終了すると、印刷データ受信部１１は、印刷データを印刷データ保存部１７に保存する。保存された印刷データに関する印刷ジョブは、印刷データの受信に応じて同期的には実行されない。すなわち、当該印刷ジョブは、ロックされた状態となる。なお、パスワード更新部１６によるパスワードの検査は、印刷データ保存部１７への印刷データの保存に応じて行われてもよい。

【００２９】

その後、ユーザが、画像形成装置１０の操作者として操作部１０９に配置されているログインボタンを押下すると、ログイン制御部１２は、ログイン画面を表示部１０８に表示させる。

【００３０】

図６は、画像形成装置におけるログイン画面の表示例を示す図である。同図において、ログイン画面５１０には、ユーザ名及びパスワードの入力、又はカード５０のセットを促

すメッセージが表示されている。

【００３１】

ログイン画面５１０が表示部１０８に表示されている状態において、ユーザによってカード５０がカードリーダー３０にセットされると、又はユーザによってログイン画面５１０を介してユーザ名及びパスワードが入力されると（Ｓ１０６）、ログイン制御部１２は、カード３０のカードＩＤに基づいて特定されるユーザ名及びパスワード、又はユーザによって入力されたユーザ名及びパスワードを、ユーザＤＢ１８に登録されているユーザ名及びパスワードの一覧と照合することにより、ユーザの認証を行う（Ｓ１０７）。認証に失敗すると、ログイン制御部１２は、ユーザのログインを拒否し、エラー画面を表示部１０８に表示させる。

【００３２】

認証に成功すると、機密印刷制御部１３は、認証されたユーザ（以下、「ログインユーザ」という。）のユーザ名と一致するユーザ名が設定されている印刷データ（すなわち、ログインユーザが機密印刷を要求した印刷データ）を印刷データ保存部１７より検索し、当該検索結果を含む印刷データ一覧画面を表示部１０８に表示させる（Ｓ１０８）。

【００３３】

図７は、印刷データ一覧画面の表示例を示す図である。同図において、印刷データ一覧画面５２０は、印刷データ一覧表示領域５２１、印刷ボタン５２２、及び削除ボタン５２３等を有する。

【００３４】

印刷データ一覧表示領域５２１には、印刷データ保存部１７に保存されている印刷データのうち、ログインユーザに係る印刷データ（の文書名）の一覧が表示される。削除ボタン５２３が押下されると、機密印刷制御部１３は、印刷データ一覧表示領域５２１において選択されている印刷データを印刷データ保存部１７より削除する。したがって、この場合、当該印刷データに係る印刷ジョブはキャンセルされる。

【００３５】

印刷ボタン５２２が押下されると、機密印刷制御部１３は、印刷データ一覧表示領域５２１において選択されている印刷データに関する印刷ジョブの実行を印刷ジョブ制御部１４に要求する（Ｓ１０９）。

【００３６】

印刷ジョブ制御部１４は、印刷ジョブの対象とされた印刷データの認証を印刷データ認証部１５に実行させる（Ｓ１１０）。印刷データ認証部１５は、印刷データに含まれているユーザ名及びパスワードと、ユーザＤＢ１８に登録されているユーザ名及びパスワードの一覧と照合することにより、印刷データの認証を行う。印刷データが認証されると、印刷ジョブ制御部１４は、印刷データの印刷を画像出力部１０５に実行させる（Ｓ１１１）。なお、ユーザＤＢ１８に、ユーザごとに印刷ジョブに関する権限が設定されている場合、印刷ジョブ制御部１４は、当該権限に応じて印刷ジョブの実行を制限してもよい。例えば、ログインユーザに印刷ジョブの実行権限が無い場合は、印刷ジョブ制御部１４は、印刷データが認証された場合であっても印刷ジョブの実行を拒否する。また、例えば、ログインユーザにカラー印刷の実行権限が無い場合であって、印刷データがカラー印刷に係るものである場合、印刷ジョブ制御部１４は、印刷ジョブの実行を拒否する。

【００３７】

上述したように、第一の実施の形態における画像形成装置１０によれば、印刷データの受信に応じて、又は印刷データ保存部１７への保存に応じて印刷データのパスワードについてユーザＤＢ１８に登録されているパスワードとの整合性が図られる。したがって、ユーザが誤って、又はパスワードが管理者によって更新されたことを知らずに古いパスワードを印刷データに設定してしまった場合であっても、印刷データの認証は成功し、円滑に印刷ジョブが実行される可能性を高めることができる。

【００３８】

続いて、第二の実施の形態について説明する。図８は、第二の実施の形態における画像

形成装置の機能構成例を示す図である。図８中、図３と同一部分には同一符号を付し、その説明は適宜省略する。第二の実施の形態では、画像形成装置１０を画像形成装置１０ａとして説明する。

【００３９】

第二の実施の形態と第一の実施の形態との主な相違点は、印刷データに含まれているパスワードの更新のタイミングにある。第二の実施の形態では、印刷データに含まれているパスワードの更新が、ユーザによる画像形成装置１０ａへのログインの成功に応じて（ログイン時に）行われる。すなわち、図８におけるパスワード更新部１６は、機密印刷制御部１３からの要求に応じてパスワードの更新を実行するように構成されている。

【００４０】

以下、画像形成装置１０ａの処理手順について説明する。図９は、第二の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図である。

【００４１】

ステップＳ２０１では、ステップＳ１０１と同様に、印刷データ送信装置２０のプリンタドライバ２１が、認証情報入力画面４１０（図５参照）を介してユーザ名及びパスワードをユーザに入力させる。続いて、プリンタドライバ２１は、印刷対象とされた文書データの印刷データを生成すると共に入力されたユーザ名及びパスワードを当該印刷データに設定し、当該印刷データを画像形成装置１０に送信する（Ｓ２０２）。画像形成装置１０ａの印刷データ受信部１１は、印刷データを受信すると、当該印刷データを印刷データ保存部１７に保存する。

【００４２】

その後、ユーザが、画像形成装置１０ａの操作者として操作部１０９に配置されているログインボタンを押下すると、ログイン制御部１２は、ログイン画面５１０（図６参照）を表示部１０８に表示させる。ログイン画面５１０が表示部１０８に表示されている状態において、ユーザによってカード５０がカードリーダー３０にセットされると、又はユーザによってログイン画面５１０を介してユーザ名及びパスワードが入力されると（Ｓ２０３）、ログイン制御部１２は、カード３０のカードＩＤに基づいて特定されるユーザ名及びパスワード又はユーザによって入力されたユーザ名及びパスワードを、ユーザＤＢ１８に登録されているユーザ名及びパスワードの一覧と照合することにより、ユーザの認証を行う（Ｓ２０４）。認証に失敗すると、ログイン制御部１２は、ユーザのログインを拒否し、エラー画面を表示部１０８に表示させる。

【００４３】

認証に成功すると、機密印刷制御部１３は、認証されたユーザ（ログインユーザ）のユーザ名と一致するユーザ名が設定されている印刷データ（すなわち、ログインユーザが機密印刷を要求した印刷データ）を印刷データ保存部１７より検索する（Ｓ２０５）。続いて、パスワード更新部１６は、検索された各印刷データについて印刷データにパスワードが設定されているか否かを判定する。パスワード更新部１６は、パスワードが含まれていない印刷データについては、当該印刷データに設定されているユーザ名に対応するパスワードをユーザＤＢ１８より取得し、当該パスワードを当該印刷データに設定する（Ｓ２０６）。また、パスワードが設定されている印刷データについては、当該パスワードがユーザＤＢ１８において当該印刷データに設定されているユーザ名に対応するものと一致するか否かを判定し、一致しない場合はユーザＤＢ１８に登録されているパスワードによって印刷データに設定されているパスワードを更新する（Ｓ２０７）。続いて、機密印刷制御部１３は、ステップＳ２０５における検索結果を含む印刷データ一覧画面５２０（図７参照）を表示部１０８に表示させる（Ｓ２０８）。

【００４４】

ステップＳ２０９～Ｓ２１１については、図４のステップＳ１０９～Ｓ１１１と同様でよいため、ここでの説明は省略する。

【００４５】

上述したように、第二の実施の形態における画像形成装置１０ａによれば、ユーザのロ

グインに応じて、印刷データのパスワードについてユーザＤＢ１８に登録されているパスワードとの整合性が図られる。したがって、例えば、ユーザが印刷データ送信装置２０において印刷指示を行ってから、画像形成装置１０ａにログインするまでの間にユーザＤＢ１８におけるパスワードが変更された場合であっても、印刷データの認証は成功し、円滑に印刷ジョブが実行される可能性を高めることができる。

【００４６】

続いて、第三の実施の形態について説明する。図１０は、第三の実施の形態における画像形成装置の機能構成例を示す図である。図１０中、図３又は図８と同一部分には同一符号を付し、その説明は適宜省略する。第三の実施の形態では、画像形成装置１０を画像形成装置１０ｂとして説明する。

【００４７】

第三の実施の形態と第一又は第二の実施の形態との主な相違点は、印刷データに含まれているパスワードの更新のタイミングにある。第三の実施の形態では、印刷データに含まれているパスワードの更新が印刷ジョブの実行時に行われる。すなわち、図１０におけるパスワード更新部１６は、印刷ジョブ制御部１４からの要求に応じてパスワードの更新を実行するように構成されている。

【００４８】

以下、画像形成装置１０ｂの処理手順について説明する。図１１は、第三の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図である。

【００４９】

ステップＳ３０１では、ステップＳ１０１又はＳ２０１と同様に、印刷データ送信装置２０のプリンタドライバ２１が、認証情報入力画面４１０（図５参照）を介してユーザ名及びパスワードをユーザに入力させる。続いて、プリンタドライバ２１は、印刷対象とされた文書データの印刷データを生成すると共に入力されたユーザ名及びパスワードを当該印刷データに設定し、当該印刷データを画像形成装置１０ｂに送信する（Ｓ３０２）。画像形成装置１０の印刷データ受信部１１は、印刷データを受信すると、当該印刷データを印刷データ保存部１７に保存する。

【００５０】

その後、ユーザが、画像形成装置１０ｂの操作者として操作部１０９に配置されているログインボタンを押下すると、ログイン制御部１２は、ログイン画面５１０（図６参照）を表示部１０８に表示させる。ログイン画面５１０が表示部１０８に表示されている状態において、ユーザによってカード５０がカードリーダー３０にセットされると、又はユーザによってログイン画面５１０を介してユーザ名及びパスワードが入力されると（Ｓ３０３）、ログイン制御部１２は、カード３０のカードＩＤに基づいて特定されるユーザ名及びパスワード、又はユーザによって入力されたユーザ名及びパスワードを、ユーザＤＢ１８に登録されているユーザ名及びパスワードの一覧と照合することにより、ユーザの認証を行う（Ｓ３０４）。認証に失敗すると、ログイン制御部１２は、ユーザのログインを拒否し、エラー画面を表示部１０８に表示させる。

【００５１】

認証に成功すると、機密印刷制御部１３は、認証されたユーザ（ログインユーザ）のユーザ名と一致するユーザ名が設定されている印刷データ（すなわち、ログインユーザが機密印刷を要求した印刷データ）を印刷データ保存部１７より検索し、当該検索結果を含む印刷データ一覧画面５２０（図７参照）を表示部１０８に表示させる（Ｓ３０５）。印刷データ一覧画面５２０において印刷ボタン５２２が押下されると、機密印刷制御部１３は、印刷データ一覧表示領域５２１において選択されている印刷データに関する印刷ジョブの実行を印刷ジョブ制御部１４に要求する。

【００５２】

印刷ジョブ制御部１４は、当該印刷データに設定されているパスワードの検査をパスワード更新部１６に実行させる（Ｓ３０７）。パスワード更新部１６は、当該印刷データにパスワードが設定されているか否かを判定し、パスワードが含まれていない印刷データに

ついては、当該印刷データに設定されているユーザ名に対応するパスワードをユーザＤＢ１８より取得し、当該パスワードを当該印刷データに設定する（Ｓ３０８）。また、パスワードが設定されている印刷データについては、当該パスワードがユーザＤＢ１８において当該印刷データに設定されているユーザ名に対応するものと一致するか否かを判定し、一致しない場合はユーザＤＢ１８に登録されているパスワードによって印刷データに設定されているパスワードを更新する（Ｓ３０９）。

【００５３】

パスワード更新部１６によるパスワードの検査が終了すると、図４のステップＳ１１０～Ｓ１１１と同様の処理が実行される（Ｓ３１０、Ｓ３１１）。

【００５４】

上述したように、第三の実施の形態における画像形成装置１０ｂによれば、ユーザのログインに応じて、印刷データのパスワードについてユーザＤＢ１８に登録されているパスワードとの整合性が図られる。したがって、例えば、ユーザが印刷データ送信装置２０において印刷指示を行ってから、画像形成装置１０ｂに印刷ジョブが実行されるまでの間にユーザＤＢ１８におけるパスワードが変更された場合であっても、印刷データの認証は成功し、円滑に印刷ジョブが実行される可能性を高めることができる。

【００５５】

続いて、第四の実施の形態について説明する。図１２は、第四の実施の形態における画像形成装置の機能構成例を示す図である。図１２中、図３と同一部分には同一符号を付し、その説明は適宜省略する。第四の実施の形態では、画像形成装置１０を画像形成装置１０ｃとして説明する。

【００５６】

第四の実施の形態と第一の実施の形態との主な相違点は、パスワード更新部１６によってパスワードが更新される対象である。すなわち、第四の実施の形態では、印刷データに含まれているパスワードによってユーザＤＢ１８のパスワードが更新される。

【００５７】

第四の実施の形態の処理手順は、第一の実施の形態（図４）とほぼ同様でよい。但し、ステップＳ１０４において、パスワード更新部１６は、印刷データに含まれているユーザ名に対応するパスワードがユーザＤＢ１８に登録されているか否かを判定し、パスワードが登録されていない場合は、当該印刷データに設定されているパスワードをユーザＤＢ１８に登録する。また、ステップＳ１０５において、パスワード更新部１６は、印刷データに含まれているパスワードがユーザＤＢ１８において当該印刷データに設定されているユーザ名に対応するものと一致するか否かを判定し、一致しない場合は印刷データに設定されているパスワードによってユーザＤＢ１８に登録されているパスワードを更新する。

【００５８】

上述したように、第四の実施の形態における画像形成装置１０ｃによれば、印刷データの送信に伴って（印刷指示に伴って）、ユーザＤＢ１８のパスワードを更新することができる。したがって、セキュリティの向上を手軽に図ることができる。

【００５９】

ところで、本実施の形態にける画像形成装置１０では、操作者は、カード５０をカードリーダー３０にセットことによってログインすることができる。以下、カード５０によるログイン（カード認証）を実現するためのログイン制御部１２の構成及び処理手順について説明する。

【００６０】

図１３は、ログイン制御部の構成例を示す図である。同図においてログイン制御部１２は、カードＩＤ取得部１２１、ユーザ情報取得部１２２、認証制御部１２３、パスワード登録部１２４、及び対応情報管理部１２５等を有する。

【００６１】

カードＩＤ取得部１２１は、カードリーダー３０がカード５０より読み取ったカードＩＤをカードリーダー３０より取得する。ユーザ情報取得部１２２は、カードＩＤ取得部１

２１によって取得されたカードＩＤに対応するユーザ名を対応情報管理部１２５より取得すると共に、操作部１０９に対してユーザによって入力されるパスワードを操作部１０９より取得する。対応情報管理部１２５は、カードＩＤとユーザ情報との対応情報を管理する、記録媒体１０３における記憶領域である。認証制御部１２３は、ユーザ情報取得部１２２によって取得されたユーザ名及びパスワードに基づく操作者（ユーザ）の認証処理をユーザＤＢ１８に登録されているユーザ情報に基づいて実行する。パスワード登録部１２４は、認証時においてパスワードを毎回入力する煩雑さを排除することを目的として、パスワードをカードＩＤに対応させて対応情報管理部１２５に登録する。したがって、パスワードが対応情報管理部１２５に登録されている場合、ユーザ情報取得部１２２は、操作部１０９からではなく、対応情報管理部１２５よりカードＩＤに対応するパスワードを取得する。

【００６２】

以下、ログイン制御部１２の処理手順について説明する。図１４は、ログイン制御部による処理手順を説明するためのフローチャートである。

【００６３】

ユーザ情報取得部１２２が、表示部１０８にログイン画面５１０（図６参照）を表示させている状態において、ユーザによってカード５０がカードリーダー３０にセットされると（Ｓ５０１でＹｅｓ）、カードＩＤ取得部１２１は、カードリーダー３０がカードより読み取ったカードＩＤをカードリーダー３０より取得する（Ｓ５０２）。なお、カードリーダー３０へのカード５０のセットとは、カードリーダー３０へカード５０を挿入したり、カード５０を翳したりといったように、カードリーダー３０がカード５０に記録されている情報を読み取れる状態にすることをいう。

【００６４】

続いて、ユーザ情報取得部１２２は、取得されたカードＩＤ（以下、「カレントカードＩＤ」という。）に対応するユーザ名を対応情報管理部１２５より取得する（Ｓ５０３）。

【００６５】

図１５は、対応情報管理部が管理する対応情報の例を示す図である。同図において、対応情報１７０は、ユーザごとに、ユーザ名、カードＩＤ、パスワード、及びカード効力を対応付けて（関連付けて）保持する情報である。したがって、ステップＳ５０３において、ユーザ情報取得部１２２は、対応情報管理部１２５において、カレントカードＩＤに対応付けられているユーザ名を対応情報管理部１２５より取得する。なお、カード効力とは、カード５０の有効性を示す情報をいう。カード５０が有効の場合、当該カードＩを利用した認証は有効とされる。カード５０が無効の場合、当該カード５０を利用した認証は無効とされる。

【００６６】

ここで、パスワードは、必ずしも対応情報管理部１２５に登録されているとは限らない。カレントＩＤに対してパスワードが登録されている場合、ユーザ情報取得部１２２は、ログイン画面５１０において、パスワードの入力欄にパスワードの入力は不要であることを示す記号（例えば、「＊＊＊＊＊＊＊＊＊＊」）を表示させる。

【００６７】

ユーザ名が取得できなかった場合（Ｓ５０４Ｎｏ）、ユーザ情報取得部１２２は、認証エラーであると判定する。ユーザ名が取得できた場合（Ｓ５０４でＹｅｓ）、ユーザ情報取得部１２２は、対応情報管理部１２５において、カレントカードＩＤに対応付けられているカード効力の値（有効又は無効）を参照し、カード５０が有効であるか否かを判定する（Ｓ５０５）。カード５０が無効である場合（Ｓ５０５でＮｏ）、ユーザ情報取得部１２２は、認証エラーであると判定する。

【００６８】

カード５０が有効である場合（Ｓ５０５でＹｅｓ）、ユーザ情報取得部１２２は、対応情報管理部１２５においてカレントカードＩＤに対してパスワードが登録されているか否

かを判定する（Ｓ５０６）。パスワードが登録されていない場合（Ｓ５０６でＮｏ）、ユーザ情報取得部１２２は、図１６に示されるパスワード画面５５０を表示部１０８に表示させる（Ｓ５０７）。パスワード画面５５０においてユーザによって入力ボタン５５１が押下され、パスワードが入力された後（Ｓ５０８でＹｅｓ）、Ｃａｎｃｅｌボタン５５３ではなく（Ｓ５０９でＮｏ）、ＯＫボタン５５２が押下されると（Ｓ５１０でＹｅｓ）、認証制御部１２３は、ステップＳ５０３において取得されたユーザ名及びステップＳ５０８で入力されたパスワードをユーザＤＢ１８に登録されているユーザ名及びパスワードと照合することにより、認証処理を実行する（Ｓ５１２）。

【００６９】

一方、対応情報管理部１２５においてカレントカードＩＤに対してパスワードが登録されている場合（Ｓ５０６でＹｅｓ）、ユーザ情報取得部１２２は、当該パスワードを取得する（Ｓ５１１）。続いて、認証制御部１２３は、ステップＳ５０３において取得されたユーザ名及び当該パスワードをユーザＤＢ１８に登録されているユーザ名及びパスワードと照合することにより、認証処理を実行する（Ｓ５１２）。

【００７０】

認証に成功した場合（Ｓ５１６でＹｅｓ）、パスワード登録部１２４は、パスワード画面５５０のチェックボタン５５４の状態に基づいて、パスワード画面５５０に入力されたパスワードの登録（保存）の要否を判定する（Ｓ５１７）。チェックボタン５５４がチェックされている場合（Ｓ５１７でＹｅｓ）、パスワード登録部１２４は、当該パスワードをカレントカードＩＤに対応させて対応情報管理部１２５に登録する（Ｓ５１８）。一方、チェックボタン５５４がチェックされていない場合（Ｓ５１７でＮｏ）、パスワード登録部１２４は、対応情報管理部１２５においてカレントカードＩＤに対して登録されているパスワードを削除する（Ｓ５１９）。但し、カレントカードＩＤに対してパスワードが登録されていない場合、削除は不要である。

【００７１】

一方、ログイン画面５１０が表示されている状態において、カードリーダー３０にカード５０はセットされずに（Ｓ５０１でＮｏ）、ログイン画面５１０にユーザ名及び必要に応じてパスワードが入力された後（Ｓ５１３でＹｅｓ）、Ｌｏｇｉｎボタン５１１が押下された場合（Ｓ５１４でＹｅｓ）について説明する。この場合、ユーザ情報取得部１２２は、ログイン画面５１０に入力されたユーザ名及びパスワードを取得し（但し、カレントＩＤに対してパスワードが登録されている場合、当該パスワードが取得される）、認証制御部１２３は、当該ユーザ名及びパスワードをユーザＤＢ１８に登録されているユーザ名及びパスワードと照合することにより、認証処理を実行する（Ｓ５１５）。続いて、上述したステップＳ５１６以降の処理が実行される。

【００７２】

また、ステップＳ５１６において、認証に失敗した場合（Ｓ５１６でＮｏ）、ユーザ情報取得部１２２は、認証に利用されたパスワードは、対応情報管理部１２５に登録されていたものか否かを判定する（Ｓ５２０）。当該判定は、対応情報管理部１２５に登録されていたパスワード（以下、「登録パスワード」という。）を用いた場合にそのことを示す情報をメモリ１０２に記録しておき、当該情報に基づいて行えばよい。認証に利用されたパスワードは登録パスワードでない場合（Ｓ５２０でＮｏ）、認証制御部１２３は、認証エラーであると判定する。

【００７３】

認証に利用されたパスワードは登録パスワードである場合（Ｓ５２０でＹｅｓ）、ユーザ情報取得部１２２は、改めてパスワード画面５５０を表示部１０８に表示させ、ユーザに新たなパスワードを入力させる（Ｓ５２１）。ここで、登録パスワードで認証に失敗した場合に、改めてユーザにパスワードを入力させるのは以下の理由による。

【００７４】

近年、セキュリティ向上のためにパスワードを定期的に変更することが多くなってきている。したがって、ユーザＤＢ１８のパスワードが更新されているにもかかわらず対応情

報管理部１２５に登録されているパスワードが古いといった不整合が発生しうる。斯かる不整合に対して簡便に対処可能とするため、ステップＳ５２１において新たなパスワード（変更されているパスワード）を入力させる機会をユーザに与えるのである。

【００７５】

改めて表示されたパスワード画面５５０に対してパスワードが入力されると、ユーザ情報取得部１２２は、パスワード画面５５０に入力されたパスワードを取得し、認証制御部１２３は、ステップＳ５０３において取得されたユーザ名及び当該パスワードをユーザＤＢ１８に登録されているユーザ名及びパスワードと照合することにより、認証処理を実行する（Ｓ５２２）。

【００７６】

認証に失敗した場合（Ｓ５２３でＮｏ）、認証制御部１２３は、認証エラーであると判定する。認証に成功した場合（Ｓ５２３でＹｅｓ）、ステップＳ５１７以降の処理が実行される。したがって、チェックボタン５５４がチェックされている場合は、対応情報管理部１２５に登録されているパスワードは、新たなパスワードによって更新される。

【００７７】

このように、画像形成装置１０は、カードＩＤとユーザ名との対応情報を管理しており、カードＩＤに基づいてユーザ名を判定することができる。また、画像形成装置１０における認証にはカードＩＤのセットだけでなくパスワードの入力も必要とされる。したがって、カードＩＤのみが記録されているカード５０であっても、ＰＩＮ（Personal Identification Number：個人暗証番号）を使用する高機能なＩＣカードと同等のセキュリティレベルによる認証処理を実現することができる。

【００７８】

また、画像形成装置１０は、カードＩＤに対応させてパスワードを保存しておくことができ、当該パスワードを認証に利用することができるため、カード５０利用時におけるパスワードの入力する手間を省くことができ、利便性を向上させることができる。

【００７９】

また、登録パスワードとユーザＤＢ１８において管理されているパスワードとの間に不整合が生じた場合であっても、認証処理の一連の流れの中でユーザに新たなパスワードを入力させる機会が与えられるため、簡便にシステムの一貫性を保つことが可能である。

【００８０】

以上、本発明の実施例について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【図面の簡単な説明】

【００８１】

【図１】本発明の実施の形態における画像形成装置のハードウェア構成例を示す図である。

【図２】機密印刷の概要を説明するための図である。

【図３】第一の実施の形態における画像形成装置の機能構成例を示す図である。

【図４】第一の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図である。

【図５】プリンタドライバが表示させる認証情報入力画面の表示例を示す図である。

【図６】画像形成装置におけるログイン画面の表示例を示す図である。

【図７】印刷データ一覧画面の表示例を示す図である。

【図８】第二の実施の形態における画像形成装置の機能構成例を示す図である。

【図９】第二の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図である。

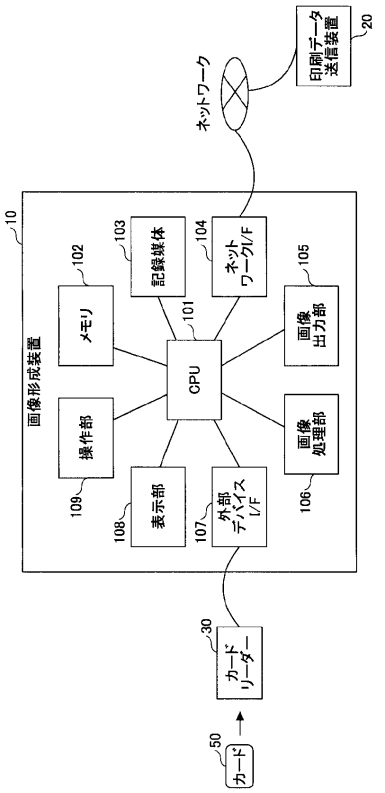
【図１０】第三の実施の形態における画像形成装置の機能構成例を示す図である。

【図１１】第三の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図である。

【図１２】第四の実施の形態における画像形成装置の機能構成例を示す図である。
【図１３】ログイン制御部の構成例を示す図である。
【図１４】ログイン制御部による処理手順を説明するためのフローチャートである。
【図１５】対応情報管理部が管理する対応情報の例を示す図である。
【図１６】パスワード画面の表示例を示す図である。
【符号の説明】
【００８２】
１０、１０ａ、１０ｂ　　画像形成装置
１１　　印刷データ受信部
１２　　ログイン制御部
１３　　機密印刷制御部
１４　　印刷ジョブ制御部
１５　　印刷データ認証部
１６　　パスワード更新部
１７　　印刷データ保存部
１８　　ユーザＤＢ
２０　　印刷データ送信装置
３０　　カードリーダー
５０　　カード
１０１　　ＣＰＵ
１０２　　メモリ
１０３　　記録媒体
１０４　　ネットワークＩ／Ｆ
１０５　　画像出力部
１０６　　画像処理部
１０７　　外部デバイスＩ／Ｆ
１０８　　表示部
１０９　　操作部
１２１　　カードＩＤ取得部
１２２　　ユーザ情報取得部
１２３　　認証制御部
１２４　　パスワード登録部
１２５　　対応情報管理部

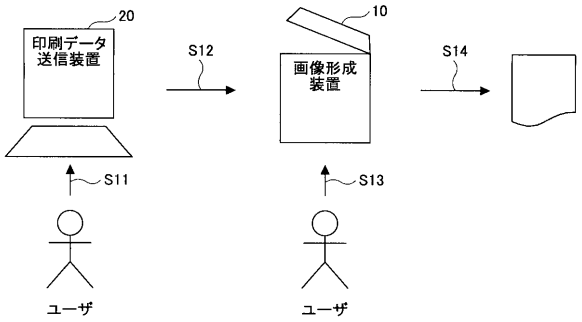
【図１】

本発明の実施の形態における画像形成装置のハードウェア構成例を示す図



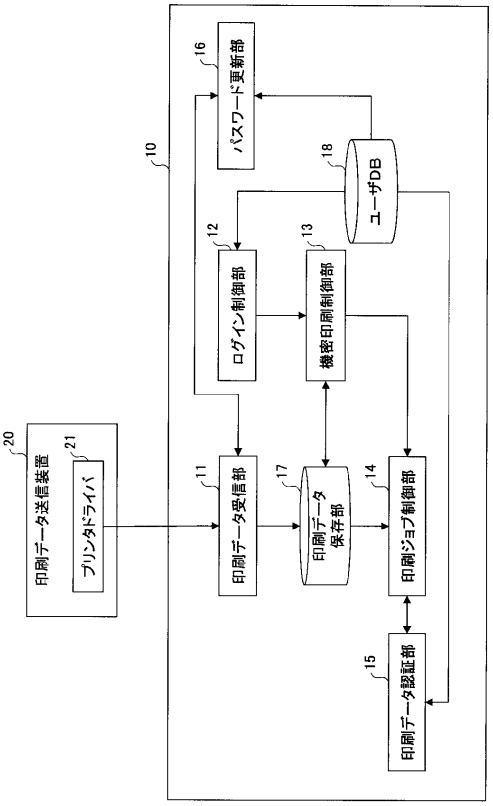
【図２】

機密印刷の概要を説明するための図



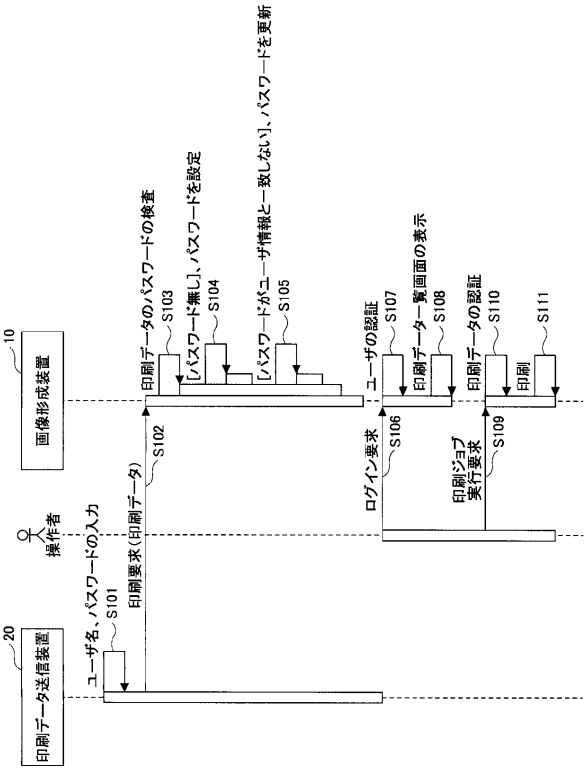
【図３】

第一の実施の形態における画像形成装置の機能構成例を示す図



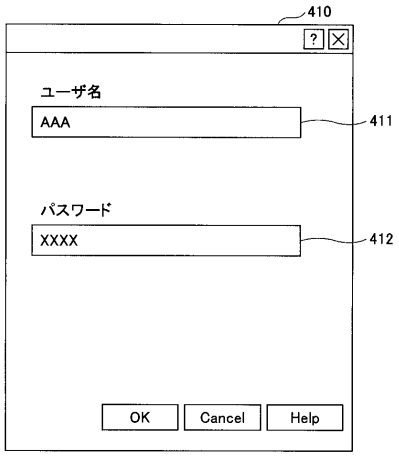
【図４】

第一の実施の形態における画像形成装置が実行する処理を説明するためのシーケンス図



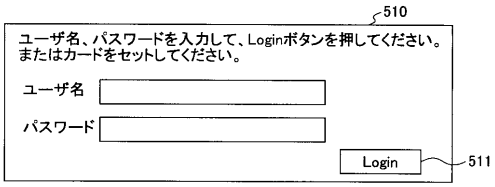
【図５】

プリンタドライバが表示させる認証情報入力画面の表示例を示す図



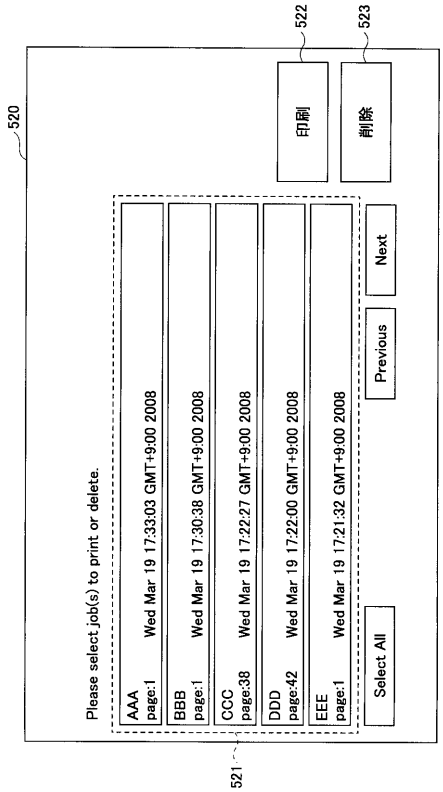
【図６】

画像形成装置におけるログイン画面の表示例を示す図



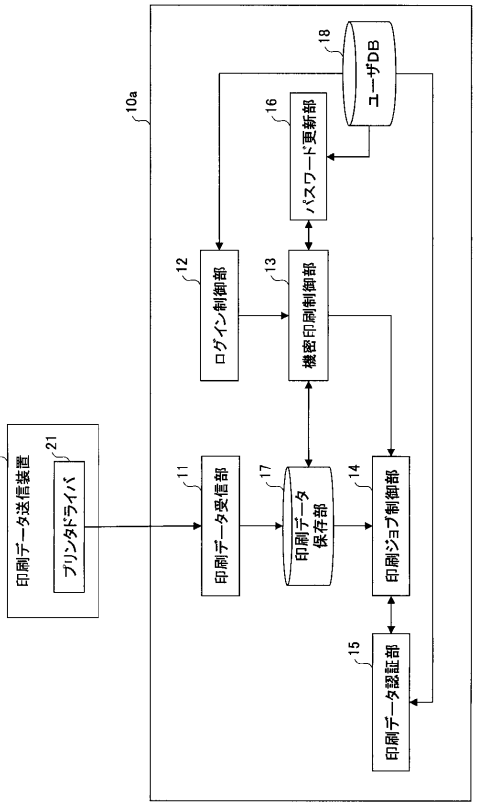
【図７】

印刷データー覧画面の表示例を示す図

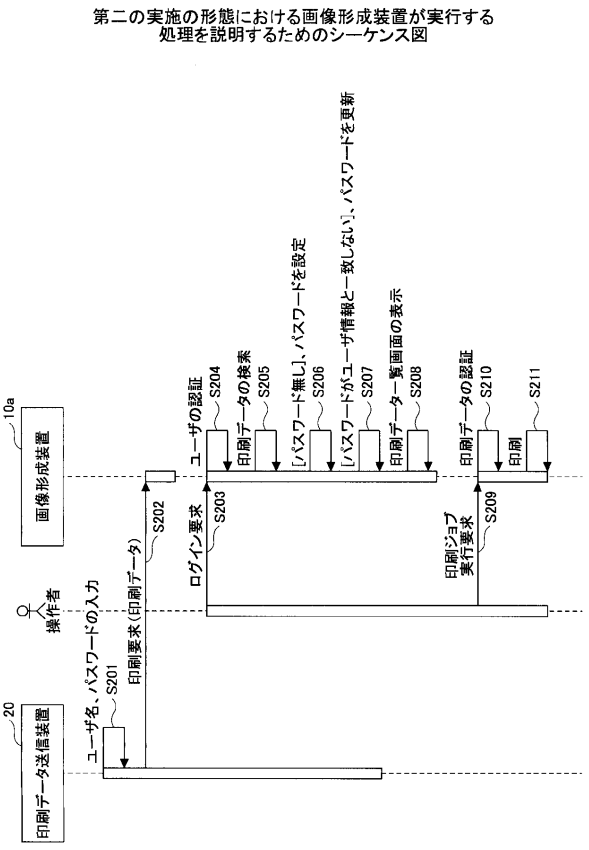


【図８】

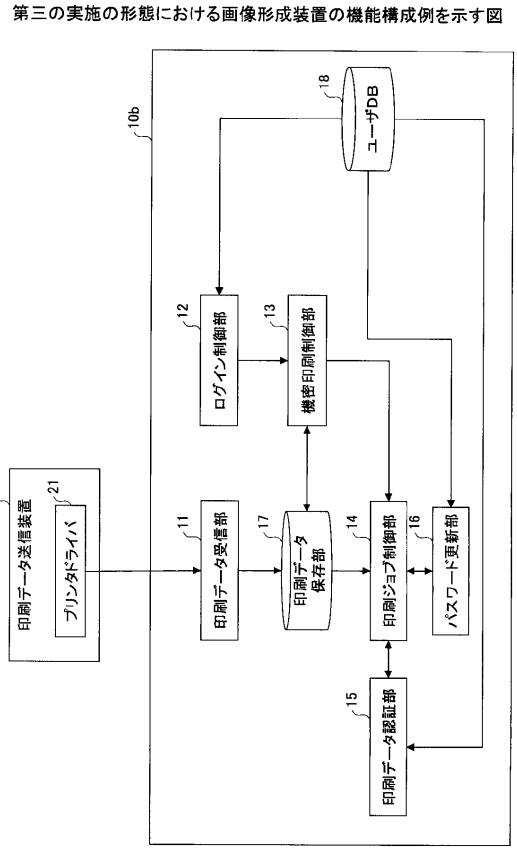
第二の実施の形態における画像形成装置の機能構成例を示す図



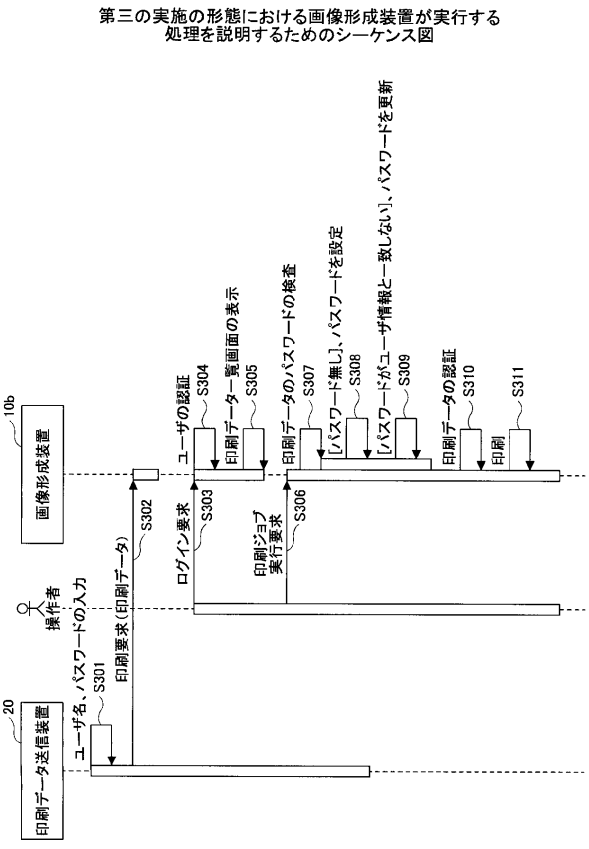
【図９】



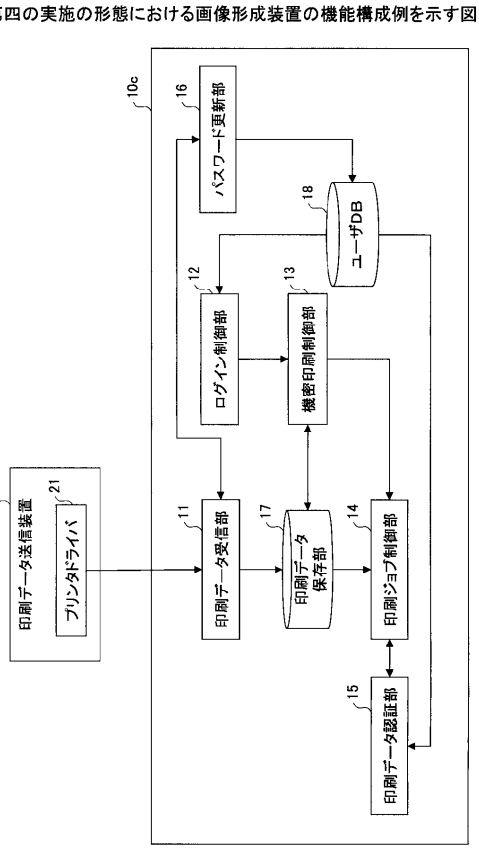
【図１０】



【図１１】

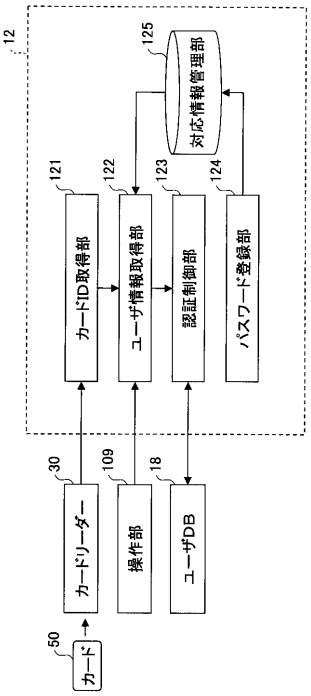


【図１２】



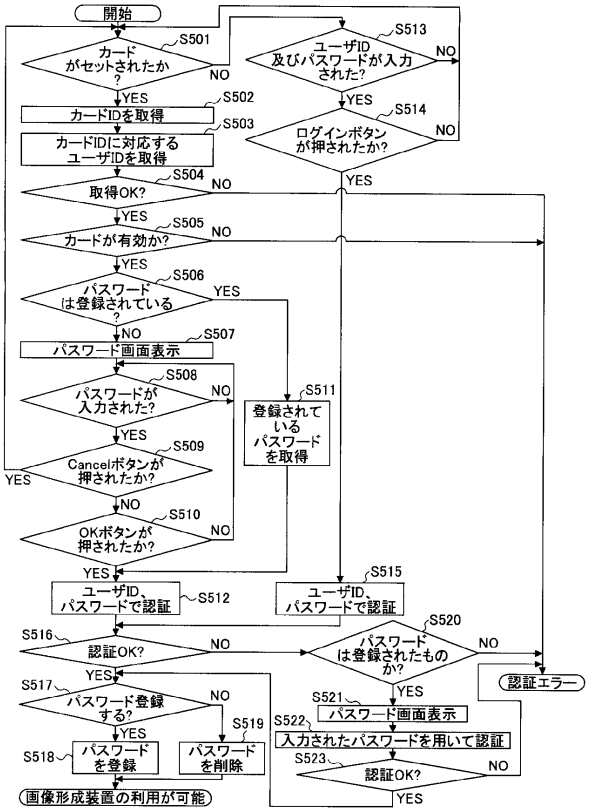
【図１３】

ログイン制御部の構成例を示す図



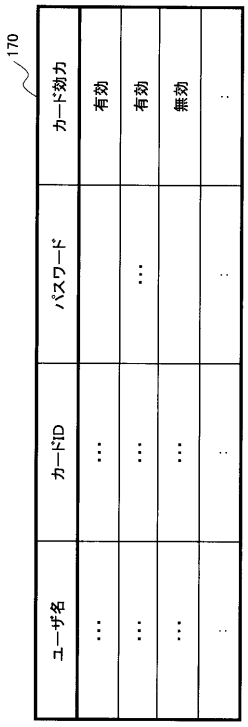
【図１４】

ログイン制御部による処理手順を説明するためのフローチャート



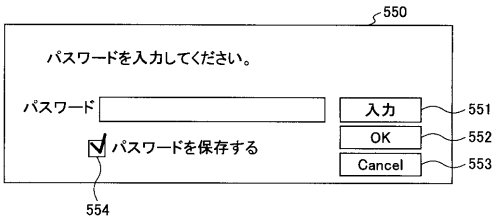
【図１５】

対応情報管理部が管理する対応情報の例を示す図



【図１６】

パスワード画面の表示例を示す図



フロントページの続き

(56)参考文献 特開２００６－１６４０４２（ＪＰ，Ａ）
特開２００７－０１１９４２（ＪＰ，Ａ）
特開２００７－１５６７７０（ＪＰ，Ａ）
特開２００７－１８４８０３（ＪＰ，Ａ）
特開２００７－２３７６８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　３／１２
Ｂ４１Ｊ　２９／００
Ｈ０４Ｎ　　１／００