

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2010-55521  
(P2010-55521A)

(43) 公開日 平成22年3月11日(2010.3.11)

(51) Int. Cl.	F I	テーマコード (参考)
<b>G06F 3/12 (2006.01)</b>	G06F 3/12	2C061
<b>B41J 29/00 (2006.01)</b>	B41J 29/00	5B021
<b>H04N 1/00 (2006.01)</b>	H04N 1/00	5C062

審査請求 未請求 請求項の数 15 O L (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)

(71) 出願人 00006747  
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  
F ターム (参考) 2C061 AP07 CL08 HJ06 HN04 HN06  
5B021 AA01 AA02 BB01 CC05 NN18  
5C062 AA02 AA05 AB20 AB22 AB38  
AB42 AC04 AC22 AC58 AF12  
AF14 BA00

(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

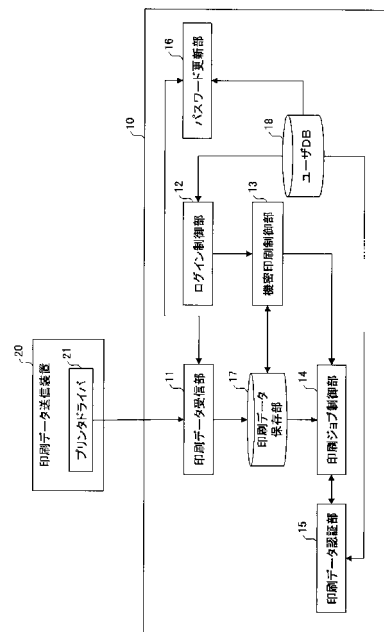
(57) 【要約】

【課題】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の提供を目的とする。

【解決手段】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手段と、操作者のユーザ識別情報及びパスワードの入力を受け付け、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手段と、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管理手段とに基づいて認証を行う手段と、認証された印刷データを印刷させる手段と、認証が行われるまでに、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手段とを有することにより上記課題を解決する。

【選択図】 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



**【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

10

20

30

40

50

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。

10

20

30

40

50

**【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として、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、スプールされ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。

10

20

30

40

50

## 【 0 0 0 6 】

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、スプールされ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。

## 【 0 0 0 7 】

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。

10

## 【 0 0 0 8 】

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】

## 【 0 0 0 9 】

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。

20

## 【 0 0 1 0 】

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。

30

## 【発明の効果】

## 【 0 0 1 1 】

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行うことができる。

## 【発明を実施するための最良の形態】

## 【 0 0 1 2 】

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。

40

## 【 0 0 1 3 】

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ーフェースとして用いられる。

50

## 【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に一意的なカード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。

10

20

## 【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。

30

## 【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)。

40

## 【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

50

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。

【 0 0 2 2 】

斯かる機密印刷を実行するために画像形成装置 1 0 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 1 0 は、印刷データ受信部 1 1、ログイン制御部 1 2、機密印刷制御部 1 3、印刷ジョブ制御部 1 4、印刷データ認証部 1 5、パスワード更新部 1 6、印刷データ保存部 1 7、及びユーザ DB 1 8 等を有する。これら各部は、画像形成装置 1 0 にインストールされたプログラムが CPU 1 0 1 に実行させる処理によって実現される。

【 0 0 2 3 】

印刷データ受信部 1 1 は、印刷データ送信装置 2 0 より送信される印刷データを受信し、印刷データ保存部 1 7 に保存する。印刷データ保存部 1 7 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 1 0 3 上に形成される。ログイン制御部 1 2 は、画像形成装置 1 0 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 DB 1 8 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 DB 1 8 は、例えば、記録媒体 1 0 3 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 DB 1 8 は、画像形成装置 1 0 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 1 3 は、印刷データ保存部 1 7 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 1 4 は、機密印刷制御部 1 3 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 1 0 5 に実行させる。印刷データ認証部 1 5 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 DB 1 8 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 1 6 は、印刷データに含まれているパスワードを、ユーザ DB 1 8 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 1 6 は、印刷データ受信部 1 1 による印刷データの受信に応じ、又は印刷データ保存部 1 7 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。

【 0 0 2 4 】

以下、画像形成装置 1 0 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。

【 0 0 2 5 】

印刷データ送信装置 2 0 において、プリンタドライバ 2 1 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（S 1 0 1）。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。

【 0 0 2 6 】

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 4 1 0 は、ユーザ名入力領域 4 1 1 及びパスワード入力領域 4 1 2 等を有する。プリンタドライバ 2 1 は、認証情報入力画面 4 1 0 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 1 0 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 2 1 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 4 1 0 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。

【 0 0 2 7 】

続いて、プリンタドライバ 2 1 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 1 0 に送信する（S 1 0 2）。

【 0 0 2 8 】

画像形成装置 1 0 の印刷データ受信部 1 1 は、印刷データを受信すると、当該印刷デー

10

20

30

40

50

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 ( S 1 0 3 ) 。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 DB 18 より取得し、当該パスワードを印刷データに設定する ( S 1 0 4 ) 。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 DB 18 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 DB 18 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 ( S 1 0 5 ) 。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。

10

20

30

40

50

**【 0 0 2 9 】**

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。

**【 0 0 3 0 】**

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。

**【 0 0 3 1 】**

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 ( S 1 0 6 ) 、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 DB 18 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 ( S 1 0 7 ) 。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。

**【 0 0 3 2 】**

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 ( S 1 0 8 ) 。

**【 0 0 3 3 】**

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。

**【 0 0 3 4 】**

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。

**【 0 0 3 5 】**

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 ( S 1 0 9 ) 。

**【 0 0 3 6 】**



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 (S 110)。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 DB 18 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 (S 111)。なお、ユーザ DB 18 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も、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。

10

#### 【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 DB 18 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。

20

#### 【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。

30

#### 【0041】

ステップ S 201 では、ステップ S 101 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 (S 202)。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。

40

#### 【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 (S 203)、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 DB 18 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 (S 204)。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

50

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DB 18 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DB 18 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DB 18 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）。

10

【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DB 18 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DB 18 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。

20

【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。

30

【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。

40

【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）

50

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 DB 18 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。

10

#### 【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 DB 18 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 DB 18 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 DB 18 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)。

20

#### 【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 DB 18 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 DB 18 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。

30

#### 【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。

40

#### 【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 DB 18 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 DB 18 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 DB 1

50

8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、本実施の形態における画像形成装置10では、操作者は、カード50をカードリーダー30にセットする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121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

【0062】

得する。

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

10

20

30

40

50

、ユーザ情報取得部 1 2 2 は、対応情報管理部 1 2 5 において、カレントカード I D に対応付けられているユーザ名を対応情報管理部 1 2 5 より取得する。なお、カード効力とは、カード 5 0 の有効性を示す情報をいう。カード 5 0 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 5 0 が無効の場合、当該カード 5 0 を利用した認証は無効とされる。

**【 0 0 6 6 】**

ここで、パスワードは、必ずしも対応情報管理部 1 2 5 に登録されているとは限らない。カレント I D 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 1 2 2 は、ログイン画面 5 1 0 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。

10

**【 0 0 6 7 】**

ユーザ名が取得できなかった場合（ S 5 0 4 N o ）、ユーザ情報取得部 1 2 2 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（ S 5 0 4 で Y e s ）、ユーザ情報取得部 1 2 2 は、対応情報管理部 1 2 5 において、カレントカード I D 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 5 0 が有効であるか否かを判定する（ S 5 0 5 ）。カード 5 0 が無効である場合（ S 5 0 5 で N o ）、ユーザ情報取得部 1 2 2 は、認証エラーであると判定する。

**【 0 0 6 8 】**

カード 5 0 が有効である場合（ S 5 0 5 で Y e s ）、ユーザ情報取得部 1 2 2 は、対応情報管理部 1 2 5 においてカレントカード I D 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（ S 5 0 6 ）。パスワードが登録されていない場合（ S 5 0 6 で N o ）、ユーザ情報取得部 1 2 2 は、図 1 6 に示されるパスワード画面 5 5 0 を表示部 1 0 8 に表示させる（ S 5 0 7 ）。パスワード画面 5 5 0 においてユーザによって入力ボタン 5 5 1 が押下され、パスワードが入力された後（ S 5 0 8 で Y e s ）、 C a n c e l ボタン 5 5 3 ではなく（ S 5 0 9 で N o ）、 O K ボタン 5 5 2 が押下されると（ S 5 1 0 で Y e s ）、認証制御部 1 2 3 は、ステップ S 5 0 3 において取得されたユーザ名及びステップ S 5 0 8 で入力されたパスワードをユーザ D B 1 8 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（ S 5 1 2 ）。

20

**【 0 0 6 9 】**

一方、対応情報管理部 1 2 5 においてカレントカード I D に対してパスワードが登録されている場合（ S 5 0 6 で Y e s ）、ユーザ情報取得部 1 2 2 は、当該パスワードを取得する（ S 5 1 1 ）。続いて、認証制御部 1 2 3 は、ステップ S 5 0 3 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 D B 1 8 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（ S 5 1 2 ）。

30

**【 0 0 7 0 】**

認証に成功した場合（ S 5 1 6 で Y e s ）、パスワード登録部 1 2 4 は、パスワード画面 5 5 0 のチェックボタン 5 5 4 の状態に基づいて、パスワード画面 5 5 0 に入力されたパスワードの登録（保存）の要否を判定する（ S 5 1 7 ）。チェックボタン 5 5 4 がチェックされている場合（ S 5 1 7 で Y e s ）、パスワード登録部 1 2 4 は、当該パスワードをカレントカード I D に対応させて対応情報管理部 1 2 5 に登録する（ S 5 1 8 ）。一方、チェックボタン 5 5 4 がチェックされていない場合（ S 5 1 7 で N o ）、パスワード登録部 1 2 4 は、対応情報管理部 1 2 5 においてカレントカード I D に対して登録されているパスワードを削除する（ S 5 1 9 ）。但し、カレントカード I D 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。

40

**【 0 0 7 1 】**

一方、ログイン画面 5 1 0 が表示されている状態において、カードリーダー 3 0 にカード 5 0 はセットされずに（ S 5 0 1 で N o ）、ログイン画面 5 1 0 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（ S 5 1 3 で Y e s ）、 L o g i n ボタン 5 1 1 が押下された場合（ S 5 1 4 で Y e s ）について説明する。この場合、ユーザ情報取得部 1 2 2 は、ログイン画面 5 1 0 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

50

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が否かを判定する(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】

10

20

30

40

50

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。 10

【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。 20

【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】

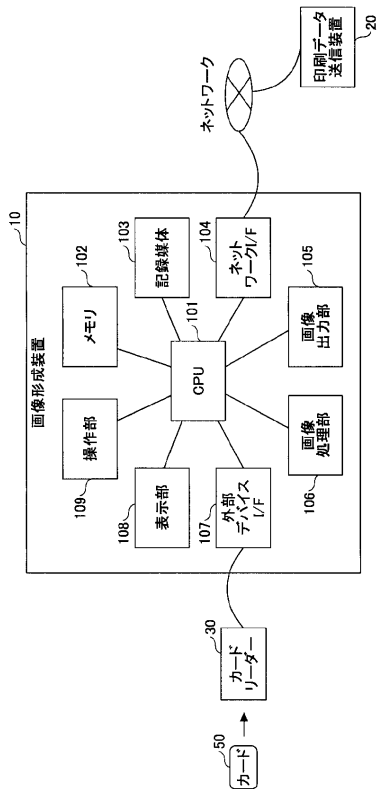
【0082】

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	30
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	40
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	50

- 1 2 3 認証制御部
- 1 2 4 パスワード登録部
- 1 2 5 対応情報管理部

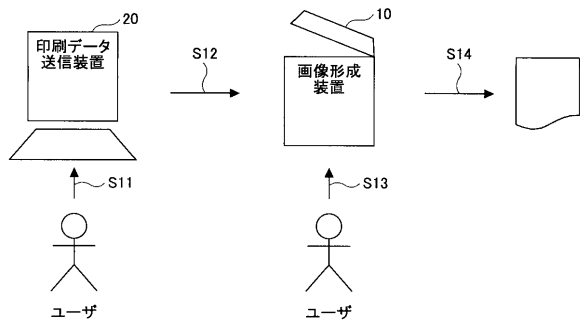
【 図 1 】

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 】

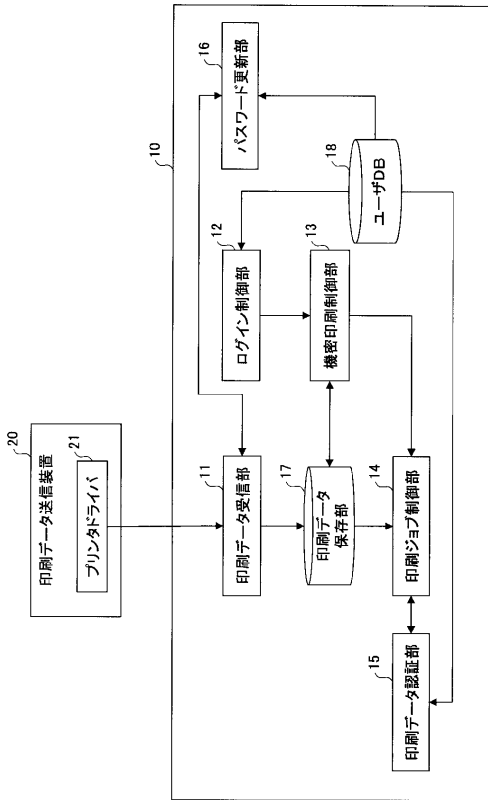
機密印刷の概要を説明するための図





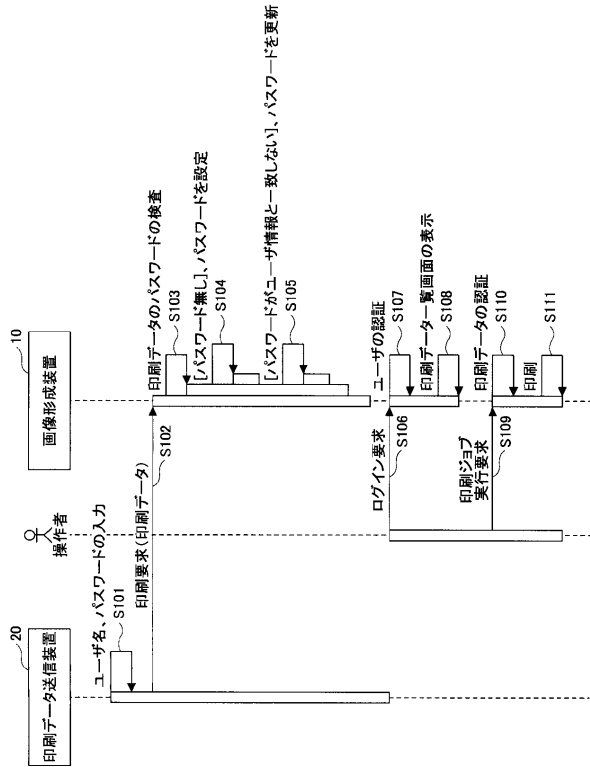
【 図 3 】

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



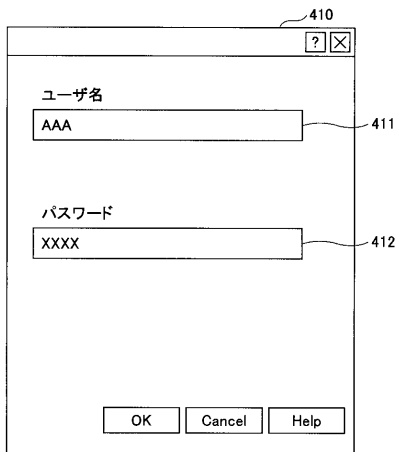
【 図 4 】

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



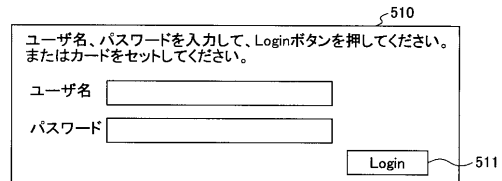
【 図 5 】

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



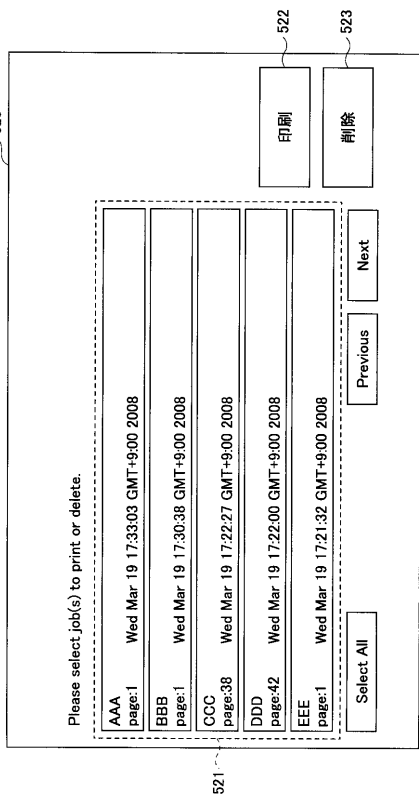
【 図 6 】

画像形成装置におけるログイン画面の表示例を示す図



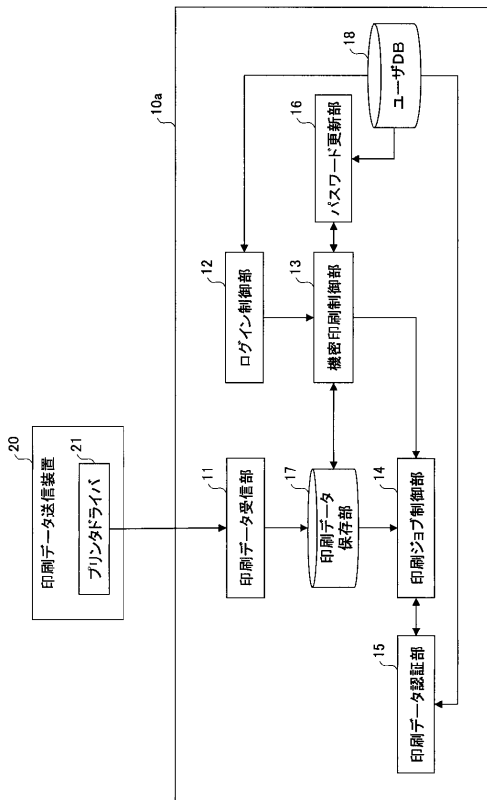
【 図 7 】

印刷データ一覧画面の表示例を示す図



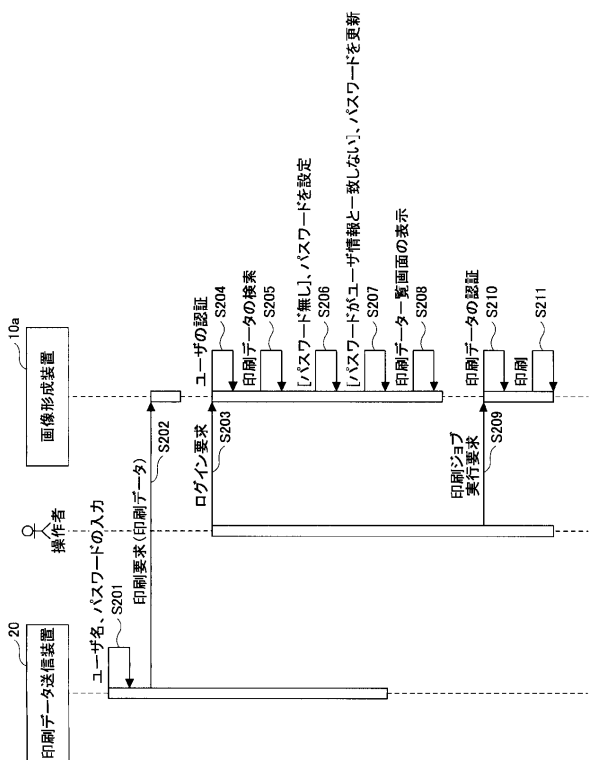
【 図 8 】

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



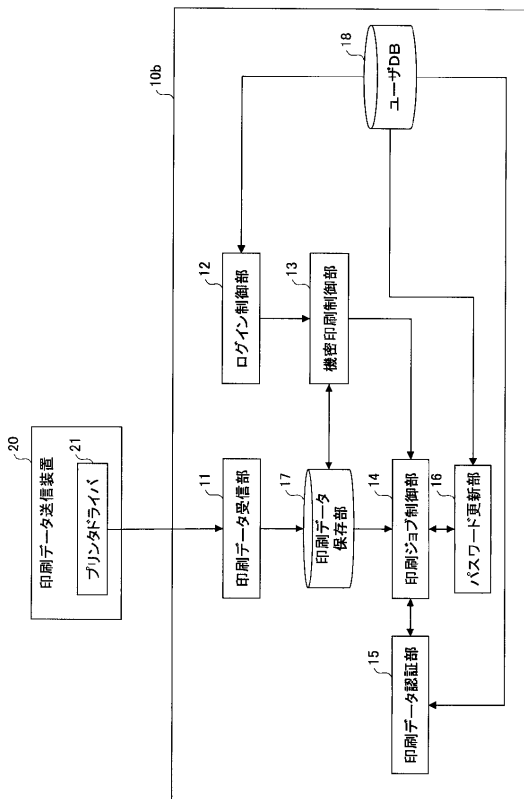
【 図 9 】

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



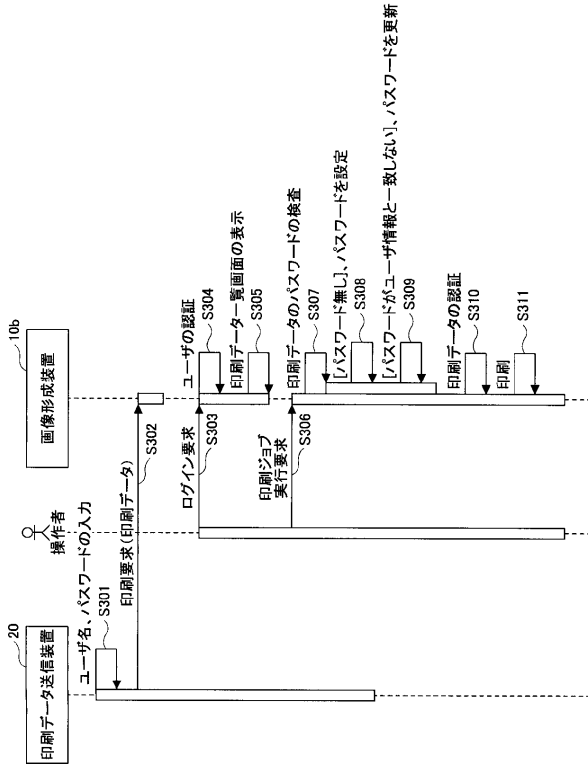
【 図 10 】

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



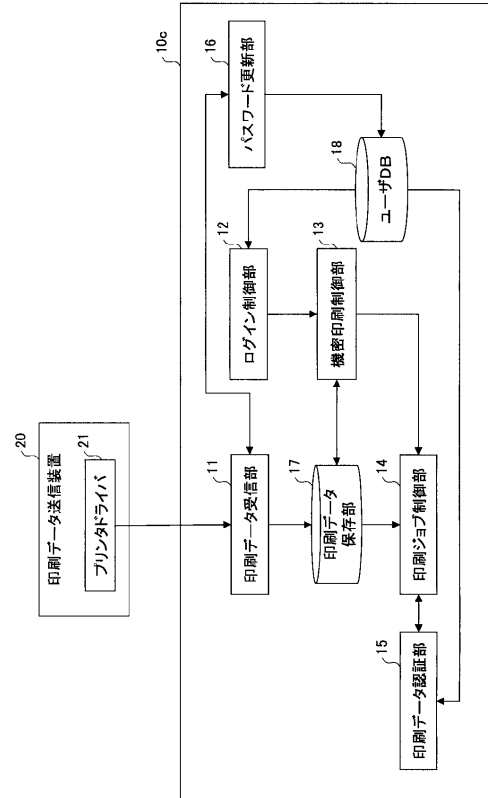
【図 1 1】

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



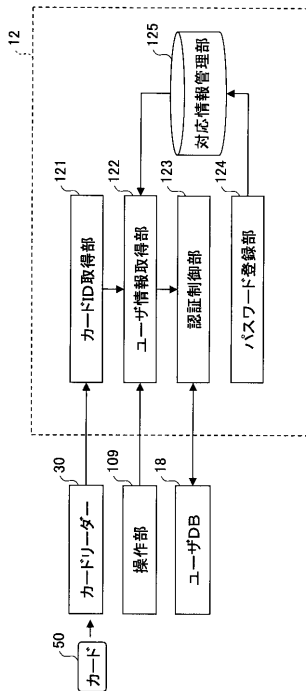
【図 1 2】

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



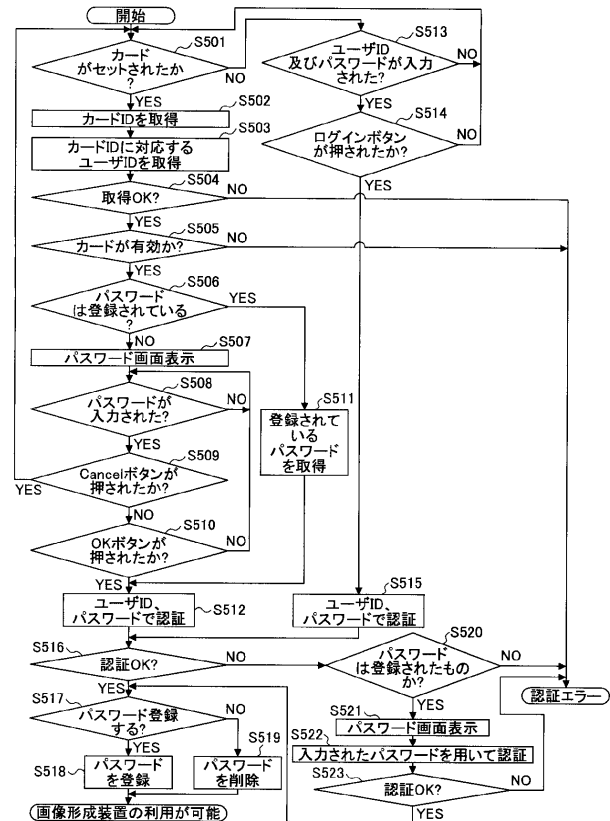
【図 1 3】

ログイン制御部の構成例を示す図



【図 1 4】

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 1 5 】

対応情報管理部が管理する対応情報の例を示す図

170

ユーザ名	カードID	パスワード	カード効力
...	...		有効
...	...	...	有効
...	...		無効
...	...	..	..

【 図 1 6 】

パスワード画面の表示例を示す図

550

パスワードを入力してください。

パスワード   551

パスワードを保存する 554

552

553