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

特許第4514215号
(P4514215)

(45)発行日　平成22年7月28日(2010.7.28)　(24)登録日　平成22年5月21日(2010.5.21)

(51)Int.Cl.		F I		
G06F 3/12	(2006.01)	G06F	3/12	K
B41J 29/38	(2006.01)	B41J	29/38	Z
H04N 1/21	(2006.01)	H04N	1/21	

請求項の数 15　(全 26 頁)

(21)出願番号　特願2005-109222 (P2005-109222)
(22)出願日　平成17年4月5日 (2005.4.5)
(65)公開番号　特開2006-293438 (P2006-293438A)
(43)公開日　平成18年10月26日 (2006.10.26)
審査請求日　平成20年3月27日 (2008.3.27)

(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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　川瀬　道夫
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

最終頁に続く

(54)【発明の名称】情報処理装置、画像形成装置、画像形成システム、情報処理方法、画像形成方法

(57)【特許請求の範囲】

【請求項１】

ネットワークを介して接続する画像形成装置から出力を行うために、画像データを生成する情報処理装置であって、

ユーザを認証するための認証情報の入力を受付けるＩＤ情報入力手段と、

前記認証情報を前記画像データに付加する認証情報付加手段と、

前記認証情報に基づいて、画像形成装置による前記画像データの出力を制御するための出力制限情報を生成する生成手段と、

前記ネットワークに接続する一の画像形成装置を選択する選択手段と、

前記認証情報が付加された画像データと、前記出力制限情報とを、前記ネットワークに接続し、前記画像形成装置に対するデータの送信を制御する装置に出力する出力手段と

を備えることを特徴とする情報処理装置。

【請求項２】

ネットワークを介して接続する画像形成装置から出力を行うために、受信した画像データを含むデータの送信を制御する情報処理装置であって、

受信した画像データに、ユーザを認証するための認証情報が付加されているか否かを判別する判別手段と、

前記判別手段により、前記画像データに前記認証情報が付加されていると判別された場合、出力先として選択されている画像形成装置に設定されているセキュリティ認証レベルを判定する制御手段と、

前記制御手段の判定に従い、選択されている前記画像形成装置に対する、前記画像データを含むデータの送信を制御する送信制御手段と
を備えることを特徴とする情報処理装置。
【請求項３】
前記画像形成装置のセキュリティ認証レベルの判定として、前記画像データに付加されている認証情報を前記画像形成装置が認証できないと前記制御手段が判定する場合、
前記送信制御手段は、前記画像データを含むデータを前記出力先として選択されている画像形成装置に送信しない
ことを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記認証情報には、前記ユーザの指紋、網膜パターン、音声に関する特徴量データが含まれることを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記認証情報の情報量に基づいて、当該認証情報の内容を識別する認証情報識別手段を更に備え、
前記制御手段は、前記認証情報識別手段の識別に従って、前記出力先として選択されている画像形成装置に設定されているセキュリティ認証レベルを判定することを特徴とする請求項２または３に記載の情報処理装置。
【請求項６】
画像データの出力を、ユーザを認証するための認証情報と、前記画像データの出力を制御するための出力制限情報と、に基づいて制御する画像形成装置であって、
受信した前記画像データに、ユーザを認証するための認証情報が付加されているか否か判別する付加判別手段と、
認証情報入力手段から入力された認証情報と、前記付加判別手段により判別された前記画像データに付加されている認証情報と、が一致するか否か判定する判定手段と、
前記認証情報入力手段から入力された認証情報と、前記付加判別手段により判別された前記認証情報とが一致している場合、前記出力制限情報に基づいて、前記画像データの画像形成を制御する画像形成制御手段と
を備えることを特徴とする画像形成装置。
【請求項７】
前記出力制限情報には、前記画像形成制御手段における印刷機能を制限するための情報が含まれること特徴とする請求項６に記載の画像形成装置。
【請求項８】
前記出力制限情報には、前記画像形成制御手段における画像形成出力の印刷範囲を制限するための情報が含まれることを特徴とする請求項６に記載の画像形成装置。
【請求項９】
前記出力制限情報には、前記情報処理装置から前記画像データを取得する回数を制限するための情報が含まれることを特徴とする請求項６に記載の画像形成装置。
【請求項１０】
受信した画像データを含むデータの送信を制御する情報処理装置と、ネットワークを介してデータの送受信を行う通信手段を更に備え、
前記認証情報が一致しない場合、当該通信手段は、前記情報処理装置に格納されている前記画像データに対するアクセスを禁止することを特徴とする請求項６に記載の画像形成装置。
【請求項１１】
前記認証情報が一致した場合に、前記画像形成制御手段は、暗号化された画像データを、出力制限情報に基づいて復号化するための制御を行い、当該認証情報が一致ない場合に、前記画像形成制御手段は暗号化された画像データの復号化を禁止する制御を行うことを特徴とする請求項６に記載の画像形成装置。
【請求項１２】

第１情報処理装置と、第２情報処理装置と、複数の画像形成装置と、を備える画像形成システムであって、
前記第１情報処理装置は、
ユーザを認証するための認証情報の入力を受付けるＩＤ情報入力手段と、
前記認証情報を前記画像データに付加する認証情報付加手段と、
前記認証情報に基づいて、画像形成装置による前記画像データの出力を制御するための出力制限情報を生成する生成手段と、
前記ネットワークに接続する一の画像形成装置を選択する選択手段と、
前記認証情報が付加された画像データと、前記出力制限情報とを、前記ネットワークに接続し、前記画像形成装置に対するデータの送信を制御する前記第２情報処理装置に出力する出力手段とを備え、
前記第２情報処理装置は、
受信した画像データに、ユーザを認証するための認証情報が付加されているか否かを判別する判別手段と、
前記判別手段により、前記画像データに前記認証情報が付加されていると判別された場合、出力先として選択されている画像形成装置に設定されているセキュリティ認証レベルを判定する制御手段と、
前記制御手段の判定に従い、を選択されている前記画像形成装置に対する、前記画像データを含むデータの送信を制御する送信制御手段とを備え、
前記画像形成装置は、
受信した前記画像データに、ユーザを認証するための認証情報が付加されているか否か判別する付加判別手段と、
認証情報入力手段から入力された認証情報と、前記付加判別手段により判別された前記画像データに付加されている認証情報と、が一致するか否か判定する判定手段と、
前記認証情報入力手段から入力された認証情報と、前記付加判別手段により判別された前記認証情報とが一致している場合、前記出力制限情報に基づいて、前記画像データの画像形成を制御する画像形成制御手段とを備える
ことを特徴とする画像形成システム。

【請求項１３】
ネットワークを介して接続する画像形成装置から出力を行うために、画像データを生成する情報処理方法であって、
ユーザを認証するための認証情報の入力を受付けるＩＤ情報入力工程と、
前記認証情報を前記画像データに付加する認証情報付加工程と、
前記認証情報に基づいて、画像形成装置による前記画像データの出力を制御するための出力制限情報を生成する生成工程と、
前記ネットワークに接続する一の画像形成装置を選択する選択工程と、
前記認証情報が付加された画像データと、前記出力制限情報とを、前記ネットワークに接続し、前記画像形成装置に対するデータの送信を制御する装置に出力する出力工程と
を備えることを特徴とする情報処理方法。

【請求項１４】
ネットワークを介して接続する画像形成装置から出力を行うために、受信した画像データを含むデータの送信を制御する情報処理方法であって、
受信した画像データに、ユーザを認証するための認証情報が付加されているか否かを判別する判別工程と、
前記判別工程により、前記画像データに前記認証情報が付加されていると判別された場合、出力先として選択されている画像形成装置に設定されているセキュリティ認証レベルを判定する制御工程と、
前記制御手段の判定に従い、選択されている前記画像形成装置に対する、前記画像データを含むデータの送信を制御する送信制御工程と
を備えることを特徴とする情報処理方法。

【請求項１５】
画像データの出力を、ユーザを認証するための認証情報と、前記画像データの出力を制御するための出力制限情報と、に基づいて制御する画像形成装置における画像形成方法であって、
受信した前記画像データに、ユーザを認証するための認証情報が付加されているか否か判別する付加判別工程と、
認証情報入力手段から入力された認証情報と、前記付加判別工程により判別された前記画像データに付加されている認証情報と、が一致するか否か判定する判定工程と、
前記認証情報入力手段から入力された認証情報と、前記付加判別工程により判別された前記認証情報とが一致している場合、前記出力制限情報に基づいて、前記画像データの画像形成を制御する画像形成制御工程と
を備えることを特徴とする画像形成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像形成技術に関し、特に、画像形成の際、ユーザの個人情報を認証して画像形成を行う画像形成技術に関するものである。
【背景技術】
【０００２】
近年、様々な情報を載せたＷＷＷ（World Wide Web）サーバと、このサーバへＨＴＴＰ(Hyper Text Transfer Protocol)でアクセスするための専用ソフトウェア（以後、「ブラウザ」と呼ぶ）を搭載したコンピュータとをネットワークで接続し、ＷＷＷサーバ上の情報を、そのコンピュータから参照することが可能になっている。また、このブラウザはＷＷＷサーバ上の情報をコンピュータに取り込んで格納することができる。従って、このデータを印刷したいユーザは、印刷機能を有するプリンタ装置等に、コンピュータ内に一時的に格納されているデータを出力して印刷させることにより、ＷＷＷサーバの各種データを印刷することが可能である。
【０００３】
しかしながら、従来のプリンタ装置は、ＷＷＷサーバから取得したデータを印刷する際、情報管理がなされているか否かに関わらず、常に固定的な画像処理を行って印刷するものであった。このために、重要なデータに関しては、本人を確認する認証機能と連携して、印刷処理を行うプリンタ装置の重要性が増してきている。
【０００４】
情報管理におけるセキュリティの観点から、アクセス権の異なるユーザに対し、文書サーバに格納された文書開示管理を文書構成単位で行えるプリンタシステムなどが提案されている。例えば、プリントジョブのセキュリティを確保するためにＢＯＸ（ボックス）という機能がある。この機能は、画像出力機器においてパスワード等のＩＤ認証を用いて、送付された画像データを特定ユーザにのみ開放する機能で、不特定のユーザに画像出力された情報の漏洩を防ぐことが可能となる。
【０００５】
上述の従来技術として、例えば、以下の特許文献１、２に示されるものがある。
【特許文献１】特開平１０－８３２６３号公報
【特許文献２】特開２００３－９４７７７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、情報管理において一般的に使用されているパスワードは、ある一定の複雑なキー操作の組み合わせであったり、ＩＤ入力であったり、または特定の認証用カードを用いることにより、本人を確認するものであったため、キー操作の方法が漏洩したり、認証用カードやＩＤが盗まれるなどのリスクがあった。一旦パスワード情報さえ入手して

しまえばＢＯＸ（ボックス）機能を用いたとしても、誰でも情報を入手することが可能となってしまう。

【０００７】

従来のネットワークプリンタにおけるＢＯＸ（ボックス）機能では、ジョブ投入の際にセキュリティレベルに関係無く、画像出力先を自由に選定でき、誤って出力先を選定しまった場合もその画像形成装置にデータは送付されてしまうことになるので、パスワード情報が漏洩していた場合、このジョブのセキュリティは確保されないという問題点があった。

【０００８】

また、本人を確認するための個人認証と、セキュリティレベルを任意に設定する機能等、画像形成装置の使用態様に応じて複数種の情報管理を行うものではなかった。例えば、暗号化された画像データを読み取り、個人認証、システム認証判定の結果に応じて復号化してプリントアウトする機能がないため、セキュリティ管理機能が未対応のセキュリティ設定が画像データに組み込まれた場合、違法な複製を防止することはできなかった。

【０００９】

以上の問題点を鑑みて、ユーザの個人認証を行うためのＩＤ情報と、画像データの出力を制御する出力制限情報とに基づいて、出力先のセキュリティ環境に応じた画像形成を可能にする画像形成技術を提供することを目的とする。

【課題を解決するための手段】

【００１０】

上記目的を達成するべく、本発明にかかる情報処理装置は、主として以下の構成を備えることを特徴とする。

【００１１】

すなわち、ネットワークを介して接続する画像形成装置から出力を行うために、画像データを生成する情報処理装置は、

ユーザを認証するための認証情報の入力を受付けるＩＤ情報入力手段と、

前記認証情報を前記画像データに付加する認証情報付加手段と、

前記認証情報に基づいて、画像形成装置による前記画像データの出力を制御するための出力制限情報を生成する生成手段と、

前記ネットワークに接続する一の画像形成装置を選択する選択手段と、

前記認証情報が付加された画像データと、前記出力制限情報とを、前記ネットワークに接続し、前記画像形成装置に対するデータの送信を制御する装置に出力する出力手段と

を備えることを特徴とする。

【００１２】

あるいは、ネットワークを介して接続する画像形成装置から出力を行うために、受信した画像データを含むデータの送信を制御する情報処理装置は、

受信した画像データに、ユーザを認証するための認証情報が付加されているか否かを判別する判別手段と、

前記判別手段により、前記画像データに前記認証情報が付加されていると判別された場合、出力先として選択されている画像形成装置に設定されているセキュリティ認証レベルを判定する制御手段と、

前記制御手段の判定に従い、選択されている前記画像形成装置に対する、前記画像データを含むデータの送信を制御する送信制御手段と

を備えることを特徴とする。

【００１３】

あるいは、本発明にかかる画像形成装置は、画像データの出力を、ユーザを認証するための認証情報と、前記画像データの出力を制御するための出力制限情報と、に基づいて制御する画像形成装置であって、

受信した前記画像データに、ユーザを認証するための認証情報が付加されているか否か判別する付加判別手段と、

認証情報入力手段から入力された認証情報と、前記付加判別手段により判別された前記画像データに付加されている認証情報と、が一致するか否か判定する判定手段と、

前記認証情報入力手段から入力された認証情報と、前記付加判別手段により判別された前記認証情報とが一致している場合、前記出力制限情報に基づいて、前記画像データの画像形成を制御する画像形成制御手段と

を備えることを特徴とする。

【発明の効果】

【００１４】

本発明によれば、ユーザの個人認証を行うためのＩＤ情報と、画像データの出力を制御する出力制限情報とに基づいて、出力先のセキュリティ環境に応じた画像形成が可能になる。

【発明を実施するための最良の形態】

【００１５】

（第１実施形態）

図１は、本発明の第１実施形態にかかる画像形成システムの構成を示す図である。１０１，１０９はユーザが通常使用する情報処理装置（以下、「パーソナルコンピュータ」という）であり、画像データ（文書データ）を作成生成し、ネットワーク上の他のコンピュータとの間で電子メールの授受等を行うことができる。１０１、１０９のパーソナルコンピュータは、キーボードを通じてキー入力によるＩＤ登録部を有する。更に、パーソナルコンピュータ１０１等には、ユーザ個人の認証情報を入力するためのＩＤ情報入力装置１２１も備えている。１０２はプリンタサーバであり、プリントキューの管理、ユーザアカウントの管理等を行っている。また、プリンタサーバ１０２はネットワーク１１２（インターネットやＬＡＮなどを含む）に接続され、各種画像データや文書データを保持している。

【００１６】

このプリンタサーバ１０２には後述する画像データに付加されたＩＤ情報を判別する機能を有し、更には判別したＩＤ情報のセキュリティレベルをも判別可能である。

【００１７】

１０７、１０８、１１０は、大型の液晶タッチパネルを有し、スキャナ機能とプリンタ機能を併有する画像形成装置である。すなわち、単体としては複写機能を有する他、光磁気ディスクユニット１１４、１１５を接続することにより、電子ファイリング装置としての機能をも有する。また、画像形成装置１０７、１０８、１１０はコンピュータ１０１、１０９用のプリンタとしても機能し、コンピュータ１０１、１０９等で作成されたドキュメントに係わる画像形成用コマンドデータ等をネットワーク１１２経由で受信し、ビットマップの画像データに展開して印刷を行う。

【００１８】

画像形成装置１１０は、ＩＤ情報入力装置１２１を備え、このＩＤ情報入力装置１２１により、画像形成装置１１０は、ユーザの個人情報を認証するためのＩＤ情報を入力することができる。また、画像形成装置１１０は操作部１７２（図９）から、キー入力により、個人情報として、パスワードや暗号化された個人コードに関する情報を入力する入力部を備えており、処理するべき画像データに付加されているＩＤ情報の情報量や、要求されるセキュリティ認証レベルに応じて、両者を選択的に使用することが可能である。

【００１９】

画像形成装置１０８は、いずれのＩＤ認証部を有さないセキュリティレベルの最も低い画像形成装置となる。

【００２０】

画像形成装置１０７は、操作部１７２（図９）から、キー入力により、個人情報として、パスワードや暗号化された個人コードに関する情報を入力する入力部を備えているが、ＩＤ情報入力装置１２１は備えていないものとする。

【００２１】

上述の画像形成システムは、システム立上げ時に各画像形成装置１０７、１０８、１１０より、各画像形成装置のセキュリティレベルがサーバ１０２に通知され、プリントサーバ１０２は各画像形成装置のセキュリティレベルを把握している。

【００２２】

ここで、ＩＤ情報入力装置１２１は、例えば、指紋読取装置、指紋情報センサとして画像形成システムを構成することができる。本実施形態においては、よりセキュリティの高い画像形成システムを提供するために、ＩＤ情報入力装置１２１として指紋情報により認証するための指紋読取装置を用いた例で説明する（以下の説明では、「指紋読取装置」を指示するものとする）。尚、本発明の趣旨は、認証情報の照合に用いるデータとして本実施形態においては、指紋を検出しているが、これに限定されるものではなく、例えば、人間の網膜パターンや音声など他の方式によりにより、個人の生体情報による個人認証を行う方法であっても良く、もちろん、公知の公開鍵番号など、通常の数字や文字情報の組み合わせによるＩＤ情報でも本発明の実施は可能である。

【００２３】

（指紋読取装置の説明）

ここで、図２を参照して指紋読取装置１２１の構成を説明する。指紋読み取り部１７６はユーザの指紋を撮像し、アンプ１７７は、ユーザの指紋に対応するアナログ画像信号を増幅させる。Ａ／Ｄ変換部１７８は、アンプ１７７で増幅された指紋のアナログデータをデジタルデータに変換し、指紋情報処理部１７９は、デジタルデータに変換された指紋情報の特徴量データを抽出する。そして外部Ｉ／Ｆ１８０を経由して、パーソナルコンピュータへ抽出された指紋特徴量データを出力する。個人を認証する際には、パーソナルコンピュータ１０１に記録されている個人情報データを所定のタイミングで読み出して、Ａ／Ｄ変換部１７８、指紋情報処理部１７９を介して入力されるユーザの指紋に対応する特徴量データと比較して、予め登録されているユーザであるか否かを判断することも可能である。

【００２４】

図３は指紋読取部１７６の詳細を説明する図である。ＬＥＤ５０１は、所定の強度の光を、平板ガラス５０２の上面である読み取り面５０３に照射する。読み取り面５０３には、ユーザの指５０４が置かれる。読み取り面５０３にあたって反射した反射光のうち、指紋凸部のものは平板ガラス５０２の反射面５０５にて全反射し、指紋凹部のものは平板ガラス５０２を透過する。反射面５０５にて全反射した指紋凸部の反射光は折り返しミラー５０６で折り返され、レンズ５０７で集光される。レンズ５０７で集光された反射光は、更に、折り返しミラー５０８で再度折り返され、読み取りセンサ５０９に入射される。読み取りセンサ５０９は、光の入力に応じて蓄電容量が変化する半導体素子（フォトダイオード）を用いて、光（画像）信号を電気信号に変換するものである。

【００２５】

（ドキュメントデータの印刷）

次に、ネットワーク１１２に接続されたパーソナルコンピュータ１０１、１０９から受信したドキュメントデータ（画像データ（または文書データ）ともいう）を画像形成装置において印刷する手順について説明する。

【００２６】

パーソナルコンピュータ１０１、１０９により作成されたドキュメントデータは、ユーザからのプリント開始命令によって、パーソナルコンピュータ１０１、１０９からプリントサーバ１０２に送信される。なお、プリント開始命令によってパーソナルコンピュータ１０１、１０９から出力される印刷対象の画像データを画像形成装置で処理するための画像形成コマンドには、送信元のパーソナルコンピュータ１０１、１０９、及び送信先、すなわち印刷処理を行う画像形成装置１０７、１０８、１１０のネットワーク上のアドレスを示すドメインアドレスがそれぞれ付加されている。

【００２７】

また、画像形成コマンドには、後に説明するＩＤ情報を含むようにしてもよい。プリン

トサーバ１０２は、画像データを受信した際、画像形成コマンドの内容をチェックして、ユーザの個人認証を行うためのＩＤ情報が付加されているか判別することができる。
また、画像データの生成元であるパーソナルコンピュータ１０１等は、画像形成装置側で画像データを出力する際、ＩＤ情報の認証結果に基づいて出力を制御する（例えば、画像データの出力禁止、部分的な印刷出力のみを許可する等）ための出力制限情報を、ユーザの設定に従い生成し、画像形成コマンドに含めてプリントサーバ１０２に送信することも可能である。

【００２８】

パーソナルコンピュータ１０１、１０９でドキュメントデータを生成する際にＩＤ情報の設定を行わなかった場合、ドキュメントデータは画像形成装置１０７、１０８、１１０のいずれからでも印刷処理を行うことが可能である。

【００２９】

通信プロトコルの１例として、ＨＴＴＰプロトコルを利用したネットワーク１１２上の情報授受について説明する。尚、本発明の趣旨は、この例に限定されるものではなく、勿論、他の通信プロトコルでも応用は可能である。ＨＴＴＰプロトコルを使用して、ユーザから操作部を介して指示された所望の画像データが保持されているサーバに対してコマンドを送信し、そのサーバからの返信に応じて、そのサーバに保持されている画像データを取得して画像形成できるようにしてもよい。その際、操作部で、希望する印刷出力先のプリンタを指定し、また、指定されたプリンタを使用して印刷したい画像データが保持されている場所（サーバ等）を指定するのに使用される。

【００３０】

次に、ＨＴＴＰプロトコルについて説明する。

【００３１】

ＨＴＴＰプロトコルは、ＨＴＭＬ（ハイパー・テキストマークアップ・ランゲージ）で記述されたデータや、画像データなどを転送するために用いられる、ＴＣＰ／ＩＰプロトコル上のサービスである。これは通常、データ転送要求を発行するクライアントコンピュータと、データを保持しているサーバとがネットワークによって接続されたシステムにおいて用いられる。

【００３２】

クライアントコンピュータ上では、ＨＴＴＰクライアントを動作させ、このＨＴＴＰクライアントにおいて、利用者が、サーバ上にあるデータの位置を、ＵＲＬと呼ばれる、データが保持されている位置を指定するための指示形式によって入力する。これによりＨＴＴＰクライアントは、その入力に応じて、サーバに対して情報転送要求を発行する。

【００３３】

また、ＨＴＴＰプロトコルには、データを要求するためのコマンドであるＧＥＴコマンドと、そのデータに関する関連情報を要求するためのコマンドであるＨＥＡＤコマンドがあり、このＨＥＡＤコマンドにより、取得するデータがどのようなデータであるのかを前もって判別し、その後ＧＥＴコマンドによって、そのデータを取得し、その取得したデータを基に処理を行うのが一般的である。

【００３４】

このＨＥＡＤコマンドにより取得可能な関連情報の中には、そのデータのサイズや更新日時などの情報とともに、そのデータのフォーマット情報がある。このデータのフォーマット情報は"Content-type"と呼ばれる。これによれば、例えば、ＨＴＭＬによって記述されたデータの場合は"text/html"、ＧＩＦ画像データの場合は"image/gif"、ＪＰＥＧ画像データの場合は"image/jpeg"などの拡張子が付されているので、この拡張子からどのようなデータであるかを判別することが可能である。同様にＰＤＬファイルを指定する場合は、"image/pdl"という拡張子が付されるので、この拡張子に従って、各属性のフォーマットを指定することができる。

【００３５】

例えば、プリントサーバ１０２のホスト名称が"host.co.jp"で、そのサーバ上の、取得

したいデータの位置が"/pub/image.GIF"である場合には、"http://host.co.jp/pub/image.GIF"というＵＲＬを入力することにより、ＨＴＴＰクライアントは、そのサーバ"host.co.jp"に対して、まず"/pub/image.GIF"に対するＨＥＡＤコマンドを発行する。

【００３６】

これを受信したサーバ１０２では、"/pub/image.GIF"のデータのフォーマット情報を、そのＨＥＡＤコマンドの返信としてＨＥＡＤコマンドを発行したＨＴＴＰクライアントに対して送信する。

【００３７】

このＨＥＡＤコマンドの返信を受けたＨＴＴＰクライアントは次に、そのサーバ"host.co.jp"に対して"/pub/image.GIF"に対するＧＥＴコマンドを発行する。

【００３８】

このＧＥＴコマンドを受信したサーバ１０２は、"/pub/image.GIF"のデータを、そのＧＥＴコマンドの返信としてＧＥＴコマンドを発行したＨＴＴＰクライアントに対して送信する。

【００３９】

こうしてＧＥＴコマンドの返信を受けたＨＴＴＰクライアントは、ＨＥＡＤコマンドに対する返信として受け取ったフォーマット情報"/pub/image.GIF"のデータを受け取ることができ、こうして受信したデータを処理することができる。

【００４０】

このようにしてＨＴＴＰクライアントは、操作部１７２から入力されたＵＲＬを基に、指定されたサーバ１０２に記憶されている、指定されたデータを、そのデータの関連情報と共に取得することができる。

【００４１】

この画像形成装置は操作部１７２（図９を参照）を有しており、この操作部１７２は操作入力のためのボタンや操作入力の結果等を示すための表示器などを備え、ユーザが画像形成装置１０７、１０８、１１０を操作するために使用される。この操作部１７２において、ユーザはＵＲＬによりプリントしたいデータが存在する場所を指定する。この入力がなされるまで画像形成装置は入力待ち状態となる。ＵＲＬが入力されると、その入力されたＵＲＬの構造を解析し、所望のデータを保持しているサーバのアドレスと、そのサーバ内の取得したいデータの位置とを特定する。本実施形態では、プリントサーバ１０２に取得したいデータが存在するものとする。

【００４２】

そこで、プリントサーバ１０２に対して、取得したいデータに対するＨＥＡＤコマンドを発行する。このＨＥＡＤコマンドは、外部インタフェース（Ｉ／Ｆ）処理部４、ネットワーク１１２を介してプリントサーバ１０２に伝送される。

【００４３】

このＨＥＡＤコマンドを受信したプリントサーバ１０２は、その指定されたデータに関する情報を基にＨＥＡＤコマンドに対するフォーマット情報を生成し、ネットワークインターフェイス３０１（図１０を参照）、ネットワーク１１２を介して、要求元の画像形成装置に送信する。これにより、画像形成装置は、プリントサーバ１０２からのフォーマット情報を受信すると、そのプリントサーバ１０２からのフォーマット情報の中から"Content-type"の情報を抽出して、画像メモリ３（図９）に記憶する。

【００４４】

次にプリントサーバ１０２に対して、その取得したいデータに対するＧＥＴコマンドを発行する。このＧＥＴコマンドは、外部インタフェース処理部４、ネットワーク１１２を介してプリントサーバ１０２に発行される。

【００４５】

これによりプリントサーバ１０２では、このＧＥＴコマンドによって指定されたデータをネットワークインターフェイス３０１、ネットワーク１１２を介して画像形成装置に送信する。

【００４６】
こうしてプリントサーバ１０２からの返信を画像形成装置が受信すると、そのプリントサーバ１０２から受信したデータを基に、画像メモリ３（図９）に画像データを格納する。
【００４７】
次に、画像メモリ３で記憶した"Content-type"がＪＰＥＧ画像である場合、ＣＰＵ１７１は、全体的な制御により画像処理回路１７０に対してＪＰＥＧ画像用の画像処理の設定を行う。不図示のＵＣＲ回路では、ＵＣＲ８０％の設定とし、不図示のパルス幅変調（以下、「ＰＷＭ」と呼ぶ。）回路には画素クロックの１／２の周波数で感光ドラムへのレーザ露光制御を行い、ドット形成を行うように設定する。ＪＰＥＧ画像はＵＣＲ８０％で黒成分が抽出されるため、黒から他の色に遷移するような画像の階調性のつながりに優れた画像を生成することが可能になると共に、１／２周波数でＰＷＭを行うため画像の階調性に優れた画像を生成することができる。
【００４８】
ＪＰＥＧフォーマットでない時、ＣＰＵ１７１は、全体的な制御により画像処理回路１７０に対してＧＩＦ画像用の設定を行う。即ち、不図示のＵＣＲ回路にはＵＣＲ１００％の設定を行い、不図示のＰＷＭ回路には不図示のクロック信号そのままの周波数でＰＷＭを行うように設定する。
【００４９】
このようにＧＩＦ画像に関しては、ＵＣＲ１００％で黒成分が抽出されるため、淡い灰色の画像は黒色トナーのみで画像形成され、Ｃ，Ｍ，Ｙ，Ｋの合成により生成される画像において問題となる、灰色が純黒色による灰色でなくなってしまうという事態を回避することができる。
【００５０】
またＰＷＭは、供給される不図示のクロック信号と同一周波数であるためジャギーが目立たない高解像度の画像を形成できる。
【００５１】
画像の階調補正データは、ＰＷＭ変調用補正データとして階調再現性を優先したＪＰＥＧ用ルックアップテーブル（以下、「ＬＵＴ」と呼ぶ。）を不図示の不揮発性メモリに格納しておく。解像度を優先するＧＩＦ画像の場合は、階調再現性を優先したＪＰＥＧ用ＬＵＴに格納しておき、ＪＰＥＧの場合と異なる階調補正データに切り替えるようにするのが効果的である。
【００５２】
（ＩＤ情報を付加して印刷を行う場合）
次に、パーソナルコンピュータ１０１にて作成したドキュメントデータに、ＩＤ情報を付加して印刷を行う場合の説明を行う。
【００５３】
図４は、パーソナルコンピュータ１０１におけるＩＤ情報を付加するための構成を説明する図であり、図５はパーソナルコンピュータ１０１において、ＩＤ情報を付加するシーケンスを説明する図である。
まず、パーソナルコンピュータ１０１は画像データの出力要求（Ｓ１０１）があった場合（Ｓ１０１－ＹＥＳ）に、ＩＤ情報の付加をユーザに問う（Ｓ１０２）。この際に、ユーザがＩＤ情報の付加を要求しなかった場合は（Ｓ１０２－ＮＯ）、処理をステップＳ１０６に進め、出力装置（画像形成装置）を選択して、プリントサーバ１０２へ画像データの出力を行う。
【００５４】
一方、ステップＳ１０２において、ユーザがＩＤ情報の付加を要求した場合は（Ｓ１０２－ＹＥＳ）、指紋読取装置１２１においてＩＤ情報（ここでは、指紋）の入力を行う（Ｓ１０３）。
【００５５】

ＩＤ情報が入力されたら（Ｓ１０４－ＹＥＳ）、指紋読取装置１２１より、外部Ｉ／Ｆ２０５を経由してパーソナルコンピュータ１０１に、指紋の特徴量データとしてＩＤ情報が取り込まれる（Ｓ１０４）。

【００５６】

取り込まれたＩＤ情報は、パーソナルコンピュータ１０１内のＩＤ情報付加部２０２によって、画像データ格納部２０４から取り出された出力画像（画像データ）に付加される（Ｓ１０５）。ＩＤ情報は、例えば、プリント開始命令によってパーソナルコンピュータ１０１、１０９から出力される印刷対象の画像データを、画像形成装置で処理するための画像形成コマンドに含めることが可能である。

【００５７】

この後、ステップＳ１０６において、出力装置としての画像形成装置を選択（ネットワーク上のアドレスを示すドメインアドレスを指定）し、ネットワークＩ／Ｆ２０１を経由して画像データ及び画像形成コマンドがプリントサーバ１０２へと出力される（Ｓ１０７）。

【００５８】

（プリントサーバ１０２におけるＩＤ情報判別）

次に、プリントサーバ１０２におけるＩＤ情報の判別に関して説明を行う。

【００５９】

図６はプリントサーバ１０２におけるＩＤ情報を判別する構成を説明する図であり、図７はプリントサーバ１０２におけるＩＤ情報を判別するシーケンスを示す図である。

まず、プリントサーバ１０２はパーソナルコンピュータ１０１から画像データをネットワークＩ／Ｆ３０１を経由して受信する（Ｓ２０１）。受信された画像データは、ＩＤ情報判別部３０２に送信され、ＩＤ情報が画像データに付加されているか否かの判別が行われる（Ｓ２０２）。送信された画像データにＩＤ情報が付加されてなければ（Ｓ２０３－ＮＯ）、処理をステップＳ２０５に進め、ＩＤ情報が付加されていない旨が制御部３０３に通知され、制御部３０３は画像データを一旦画像データ格納部３０４に格納した後、出力先アドレス判別部３０５によって判別されたドメインアドレスにて指定されている出力先の画像形成装置に画像データの転送を行う（Ｓ２０３、Ｓ２０５）。

【００６０】

一方、画像データにＩＤ情報が付加されている場合は（Ｓ２０３－ＹＥＳ）、処理をステップＳ２０４に進め、ＩＤ情報が付加されている旨が制御部３０３に通知され、出力先アドレス判別部３０５によって判別されたドメインアドレスにて指定されている出力先のセキュリティ認証レベル（ＩＤ情報を認証するためのＩＤ情報入力装置を備えており、ＩＤ情報の認証が可能か否か）を制御部３０３が判定する。出力先として選択された画像形成装置が、指紋読取装置１２１等を有する場合、画像データは一旦画像データ格納部３０４に格納された後、出力先アドレス判別部３０５によって判別されたドメインアドレスにて指定されている出力先の画像形成装置に画像データ（画像形成コマンドにＩＤ情報、出力制限情報が含まれる場合は、これらの情報を含む）は送信される（Ｓ２０４、Ｓ２０５）。

【００６１】

一方、画像形成装置側からプリントサーバ１０２のデータを指定して印刷を行う場合は、以下の手順に従うものとする。まず、プリントサーバ１０２上にあるデータの位置を、ＵＲＬと呼ばれる、データが保持されている位置を指定するための指示形式によって指定する。これによりＨＴＴＰクライアントは、その入力に応じて、プリントサーバ１０２に対して情報転送要求を発行する。

【００６２】

プリントサーバ１０２のホスト名称が"host.co.jp"で、そのプリントサーバ上の、取得したいデータの位置が"/pub/image.GIF"である場合には、"http://host.co.jp/pub/image.GIF"というＵＲＬをプリントサーバ１０２に送信することにより、ＨＴＴＰクライアントは、そのサーバ"host.co.jp"に対して、まず"/pub/image.GIF"に対するＨＥＡＤコマン

ドを発行する。
【００６３】
これを受信したプリントサーバ１０２では、"/pub/image.GIF"のデータのフォーマット情報とともに、ＩＤ情報や出力制限情報を、そのＨＥＡＤコマンドの返信としてＨＥＡＤコマンドを発行したＨＴＴＰクライアントに対して送信する。
【００６４】
このＨＥＡＤコマンドの返信を受けたＨＴＴＰクライアントは次に、
そのサーバ"host.co.jp"に対して"/pub/image.GIF"に対するＧＥＴコマンドを発行する。
【００６５】
このＧＥＴコマンドを受信したプリントサーバ１０２は、"/pub/image.GIF"のデータを、そのＧＥＴコマンドの返信としてＧＥＴコマンドを発行したＨＴＴＰクライアントに対して送信する。
【００６６】
こうしてＧＥＴコマンドの返信を受けたＨＴＴＰクライアントは、ＨＥＡＤコマンドに対する返信として受け取ったフォーマット情報"/pub/image.GIF"と出力制限情報のデータを受け取ることができ、こうして受信したデータを処理することができる。
【００６７】
このようにしてＨＴＴＰクライアントは、操作部１７２から入力されたＵＲＬを基に、指定されたプリントサーバ１０２に記憶されている、指定されたデータを、そのデータの関連情報と共に取得することができる。
【００６８】
プリントサーバ１０２は当該文書に付随したフォーマット情報と、出力制限情報を返信している為、例えば、画像形成装置１１０は、出力制限情報に基づいて、印刷を許可するかどうかをＣＰＵ１７１で判断する。指定された画像形成装置が、ＩＤ情報の認証部等、セキュリティ設定を保持する手段を持たない場合は、この画像データは画像形成装置に送信されずエラー処理となって画像データは送信されない（Ｓ２０６）。
【００６９】
（画像形成装置における指紋認証）
（画像形成装置の構成）
次に、画像形成装置１１０におけるＩＤ情報の認証及び画像形成処理に関して説明する。図８は、本発明の実施形態にかかる画像形成装置１１０の断面図である。図８において画像形成装置１１０には、画像データ入力部２００が物理的に一体化されて配置されている例を示しているが、これは一例であり、分離されて配置されてもよいものとする。
【００７０】
画像データ入力部２００において、２０１は原稿積載台としてのプラテンガラスであり、２０２はスキャナであり、不図示の原稿照明ランプ、走査ミラー等で構成される。画像取り込み処理が開始されると、２０２が所定方向に往復走査されて、原稿の反射光は走査ミラー２０４～２０６経由でレンズ２０７に導光され、イメージセンサ部２０８内のＣＣＤセンサはレンズ２０７を透過した光を結像する。なお、画像データ入力部２００には、更に、ＡＤＦ（自動原稿送り器）もしくは圧板カバーを装着（不図示）することも可能である。
【００７１】
画像形成部１００は、トナー像を形成する４つのステーション（１６ａ、１６ｂ、１６ｃ、１６ｄが並設されており、その構成は同一である。）、記録媒体を供給する給紙ユニット２０、トナー像を記録媒体に転写する中間転写ユニット３０、記録媒体上に転写されたトナー像を加熱・加圧して定着させる定着ユニット４０及び画像形成装置における認証処理及び画像形成処理の全体的な制御を司る制御ユニット２５から構成される。
【００７２】
尚、図８の構成では、トナー像を構成するユニットとして、４つのステーションが設けられている例を示したが、本発明の趣旨はこれに限定されるものではなく、例えば、１つ

の感光ドラムから構成されるものでも、本発明を適用することは可能である。

【００７３】

次に、個々のユニットについて詳しく説明する。画像形成部１００における各ステーション１６ａ，１６ｂ，１６ｃ，１６ｄには、像担持体としての感光ドラム１１a、１１b、１１c、１１dがその中心で回転が可能な状態に支持しれており、矢印方向に回転駆動される。感光ドラム１１a～１１dの外周面に対向してその回転方向に一次帯電器１２a、１２b、１２c、１２d、光学系１３a、１３b、１３c、１３d、現像装置１４a、１４b、１４c、１４dが配置されている。一次帯電器１２a～１２dにおいて感光ドラム１１a～１１dの表面に均一な帯電量の電荷を与える。次いで光学系１３a～１３dにより、記録画像信号に応じて変調した、例えば、レーザービームなどの光線を感光ドラム１１a～１１d上に露光させることによって、静電潜像を形成する。さらに、イエロー、シアン、マゼンタ、ブラックといった４色の現像剤（トナー）をそれぞれ収納した現像装置１４a～１４dによって静電潜像をトナー像として顕像化する。顕像化された可視画像を中間転写体に転写する画像転写領域Ta、Tb、Tc、Tdの下流側では、クリーニング装置１５a、１５b、１５c、１５dにより転写材に転写されずに感光ドラム１１a～１１d上に残されたトナーを掻き落としてドラム表面の清掃を行う。以上に示したプロセスにより、各トナーによる画像形成が順次行われる。

【００７４】

給紙ユニット２０は，記録材Ｐを収納するためのカセット２１a・bおよび手差しトレイ２７、カセット内もしくは手差しトレイより記録媒体（記録材）Ｐを一枚ずつ送り出すためのピックアップローラ２２a・bおよび２６、各ピックアップローラから送り出された記録材Ｐをレジストローラまで搬送するための給紙ローラ対２３及び給紙ガイド２４、そして画像形成部の画像形成タイミングに合わせて記録材Ｐを二次転写領域Teへ送り出すためのレジストローラ２５a、２５bから成る。

【００７５】

次に、中間転写ユニット３０について詳細に説明する。中間転写ベルト３１(その材料として例えば、ＰＥＴ[ﾎﾟﾘｴﾁﾚﾝﾃﾚﾌﾀﾚｰﾄ]やＰＶｄｆ[ﾎﾟﾘﾌｯ化ﾋﾞﾆﾘﾃﾞﾝ]などが用いられる)は、中間転写ベルト３１に駆動を伝達する駆動ローラ３２、ばね（不図示）の付勢によって中間転写ベルト３１に適度な張力を与えるテンションローラ３３、ベルトを挟んで二次転写領域Teに対向する従動ローラ３４に巻回させる。これらのうち駆動ローラ３２とテンションローラ３３の間に一次転写平面が形成される。駆動ローラ３２は金属ローラの表面に数ｍｍ厚のゴム（ウレタンまたはクロロプレン）をコーティングしてベルトとのスリップを防いでいる。駆動ローラ３２はパルスモータ（不図示）によって回転駆動される。各感光ドラム１１a～１１dと中間転写ベルト３１が対向する一次転写領域Ta～Tdには、中間転写ベルト３１の裏に一次転写ブレード３５a～３５dが配置されている。従動ローラ３４に対向して二次転写ローラ３６が配置され、中間転写ベルト３１とのニップによって二次転写領域Teを形成する。二次転写ローラ３６は中間転写体に対して適度な圧力で加圧されている。また、中間転写ベルト３１上、二次転写領域Teの下流には中間転写ベルト３１の画像形成面をクリーニングするためのクリーニング装置(不図示)が配され、前記クリーニング装置は、クリーナーブレード（不図示：材質としては、ポリウレタンゴムなどが用いられる）および廃トナーを収納する廃トナーボックス（不図示)から成る。

【００７６】

制御ユニット２５は、各ユニット内の機構の動作を制御するための制御基板（不図示）や、モータドライブ基板（不図示）などから成る。

【００７７】

定着ユニット４０は、二次転写領域Teにて転写された画像を載せた記録材Ｐを加熱・加圧することで画像を定着させる。

【００７８】

その他の画像形成装置１０７，１０８も同様の構成となっている。

【００７９】
（画像形成装置の制御ブロック）
図９は、画像形成装置１１０の制御ブロック図であり、図１２は画像形成装置１１０における処理の流れを概略的に説明するフローチャートである。１７１は画像形成装置１１０の基本制御を行うＣＰＵであり、ＲＯＭ１７４、ＲＡＭ１７５及び入出力ポート（Ｉ／Ｏ）１７３がアドレスバス、データバスにより接続されている。入出力ポート１７３には、画像形成装置１１０を制御する、モータ、クラッチ等の各種負荷出力（不図示）や、記録材の位置を検知するセンサ出力等が入力されている。
【００８０】
ＣＰＵ１７１はＲＯＭ１７４の内容に従って入出力ポート１７３を介して順次入出力の制御を行い画像形成動作を実行する。画像形成装置の装置全体の動作を制御するＣＰＵ１７１と各ユニット間とは、ＣＰＵ１７１のシステムバスやシリアルバスなどを介して相互に接続され、各種データの送受信を行っている。
【００８１】
ネットワーク１１２は、インターネットやＬＡＮなどを含み、各画像形成装置とプリントサーバ１０２とを互いに接続し、これら装置間で各種データを双方向に送受信するための電気通信回線である。ＲＯＭ１７４、ＲＡＭ１７５は、ＣＰＵ１７１により実行されるプログラムを格納し、ＣＰＵ１７１の動作時、各種データ等を一時的に記憶するためのワークエリアとしても使用される。勿論、不図示のハードディスク（以下、「ＨＤＤ」と呼ぶ。）など他の記憶ユニットにプログラムの少なくとも一部を格納することも可能であり、ＨＤＤに画像データ等を格納するようにしてもよい。
【００８２】
ＣＰＵ１７１には操作部１７２が接続されており、ＣＰＵ１７１は、操作部１７２上の表示ユニット（不図示）に種々のデータや画像形成装置の状態を表示するための表示制御、操作部１７２のキー入力部（不図示）から入力された操作入力に基づく動作の制御を司る。操作者はキー入力部を介して、画像形成動作モードや、表示の切り替えをＣＰＵ１７１に指示し、ＣＰＵ１７１は画像形成装置１１０の状態や、キー入力による動作モードの設定に関する表示を表示ユニットに表示する。
【００８３】
ＣＰＵ１７１には、イメージセンサ部２０８で電気信号に変換された信号を、処理する画像処理部１７０と、処理された画像を蓄積する画像メモリ部３が接続されている。
【００８４】
画像メモリ部３には画像データ入力部２００と外部I/F処理部４と画像形成部１００が接続される。
【００８５】
画像データ入力部２００で読み込まれた原稿画像は、所定の画像処理が行われた後、画像メモリ部３に送られ、蓄積される。ネットワーク１１２を介して外部Ｉ／Ｆ処理部４に入力される。また、コンピュータ１０１などで生成された画像データに関しては、コンピュータ１０１で既に画像処理が施されているので、そのまま画像メモリ部３に送られる。画像データ入力部２００と外部Ｉ／Ｆ処理部４から画像メモリ部３に送られた画像データは画像形成部１００に送られ、画像形成部１００は、記録材Ｐ上に画像データに基づいた画像形成を行う。
【００８６】
外部I/F処理部４は、ネットワーク１１２を介して、このネットワーク１１２に接続されている他の装置との間での通信を制御している。プリントサーバ１０２より送られた画像データは、外部Ｉ／Ｆ処理部４を経由して画像形成装置１１０に取り込まれ、ＣＰＵ１７１の制御の下、画像処理部１７０にてＩＤ情報が画像データに付加されているか否か判別される。ＩＤ情報が付加されていない場合は（Ｓ１２１０－ＮＯ）、そのまま、画像形成処理に移行する。
【００８７】

一方、ＩＤ情報が画像データに付加されている場合（Ｓ１２１０－ＹＥＳ）、ＣＰＵ１７１は、ＩＤ情報の認証が必要である旨をユーザに促す（Ｓ１２２０）。ユーザの認証がＣＰＵ１７１により許可されない限り、この画像データは出力されない。

【００８８】

例えば、パーソナルコンピュータ１０１に接続する指紋読取装置１２１からＩＤ情報を取り込んで、画像データにＩＤ情報を付加した場合を想定する。

【００８９】

画像データに付加されたＩＤ情報は、個人情報記憶部１８２に記憶され、画像形成装置１１０に接続する指紋読取装置１２１から取り込まれたＩＤ情報と、個人情報記憶部１８２に格納されているＩＤ情報とが一致しないと、ＣＰＵ１７１が判定した場合（Ｓ１２３０-（不一致））、この画像データが画像処理装置１１０で処理されないように、ＣＰＵ１７１は画像形成装置１１０を制御し（Ｓ１２５０）、ＩＤ情報が一致した場合のみ（Ｓ１２３０-（一致））、画像データが画像形成装置１１０で処理されて出力されるようにＣＰＵ１７１は画像形成装置１１０を制御する（Ｓ１２４０）。

【００９０】

認証により、ＣＰＵ１７１はユーザが該当する文書を印刷することが許可されていると判別すると、ＣＰＵ１７１は、操作部１７２を制御して、「認証結果はＯＫです。印字可能です」等のメッセージを操作部１７２の表示画面に表示させることができる。

【００９１】

（出力制限情報に基づく制御）

個人情報記憶部１８２に格納されているＩＤ情報と、画像形成装置１１０に接続する指紋読取装置１２１から入力されたＩＤ情報とが一致すると、ＣＰＵ１７１が判定する場合、ＣＰＵ１７１は、画像データの処理を実行するように画像形成装置を制御する。この際、プリントサーバ１０２から取得した画像データの出力制限情報に基づいて、画像形成装置１１０のプリント動作モード（印刷機能）を制限するようにＣＰＵ１７１は画像形成装置１７１を制御することができるものとする。

【００９２】

例えば、プリントサーバ１０２から取得した出力制限情報の内容が白黒印刷のみを許可する設定がなされているとすると、ＣＰＵ１７１は、画像データの処理において、白黒プリントモードでの印刷動作を許可し、カラーモードでの印刷動作を禁止するように制御する。

【００９３】

（オリジナルの原稿画像の情報をプリントサーバ１０２から取得する印刷）

原稿画像データを画像データ入力部２００から読み込ませて、オリジナルの原稿画像データをプリントサーバ１０２から取得して印刷する場合を説明する。この印刷によれば、例えば、一旦、画像形成装置１１０等により処理された原稿データを再び、画像データ入力部２００から読み込み複製印刷する場合、複製によりセキュリティ情報が画像形成に反映されなくなることを防止するものである。

【００９４】

出力制限情報の内容が、プリントサーバ１０２に格納されたオリジナル原稿画像データを取得して印刷するモードを設定するものである場合、ＣＰＵ１７１は、プリントサーバ１０２に対して、画像データの送信を要求し、当該する画像データを取得して、印刷動作を行うように画像形成装置１１０を制御することができる。その場合、画像データのオリジナルをプリントサーバ１０２に要求するために、ＣＰＵ１７１は、プリントサーバ１０２に対してＨＥＡＤコマンドを発行し、原稿画像データが格納されているＵＲＬアドレスを指定して、ＨＥＡＤコマンドをプリントサーバ１０２に送信する。ＵＲＬアドレスは、オリジナルの原稿画像データを取得するために、例えば、最初に操作部１７２から入力されたＵＲＬを画像メモリ３内に保持してき、再度、プリントサーバ１０２に原稿画像データの送信を要求する際に利用することができるものとする。

【００９５】

画像形成装置１１０はオリジナルのデータとして原稿画像データを受信し（このデータは、画像データ入力部２００で入力された原稿画像のオリジナル画像データに対応する）、画像メモリ部３に原稿画像データを格納する。この際、ＣＰＵ１７１は、画像データ入力部２００から読み取った原稿画像に代わり、今回、新たにプリントサーバ１０２から送られて、メモリ部３に格納された原稿画像データに基づいて画像形成を行うように画像形成装置１１０を制御することができる。

【００９６】

この際、ＣＰＵ１７１は、原稿画像データを処理するために、個人情報記憶部１８２に予め格納されているユーザのＩＤ情報と新たに照合を行うために、画像形成装置１１０に接続する指紋読取装置１２１から、再度、ユーザのＩＤ情報の取得を行い、ＩＤ情報が一致した場合、ＣＰＵ１７１は、画像形成部１００を制御して、新たにプリントサーバ１０２から送られて、メモリ部３に格納された原稿画像データに基づく画像形成処理を実行する。

【００９７】

以上の処理によれば、一旦、画像形成装置１１０等により処理された原稿データを再び、画像データ入力部２００から読み込み複製印刷する場合、オリジナルの原稿画像データをＵＲＬアドレスより取得して、データ自体をオリジナルの原稿画像データから取得するとともに、ユーザのＩＤ情報の認証を再度行うようにする、データ面の照合とユーザの個人情報の認証を連動させることにより、複製の際、ＩＤ情報等セキュリティ情報が画像形成に反映されなくなることを防止するが可能になる。

【００９８】

この際、指紋読取装置１２１が読み取ったＩＤ情報が一致した場合のみ、ＣＰＵ１７１は、プリントサーバ１０２へのアクセスを許可するように制御することも可能である。

【００９９】

また、ＣＰＵ１７１は、ＩＤ情報が一致するものであっても、出力制限情報の内容によっては、記録材Ｐに画像形成すること禁止される場合、画像形成装置１１０の操作部１７２に設けられている表示部などを利用して、画像データを表示することも可能である。

【０１００】

また、予め暗号化された画像データを画像メモリ３に格納しておき、ＩＤ情報が一致した場合に、ＣＰＵ１７１は、暗号化された画像データを、出力制限情報に基づいて復号化することを許可し、ＩＤ情報が一致ない場合は復号化を禁止するように画像形成装置１１０を制御することも可能である。

【０１０１】

また、ＩＤ情報が一致した場合に、ＣＰＵ１７１は、プリントサーバ１０２におけるオリジナル原稿画像データの内容を変更、印刷サイズや解像度などの付帯条件の変更を許可し、ＩＤ情報が一致しない場合は、付帯条件の変更を禁止することも可能である。また、ＩＤ情報が一致しない場合は、かかる変更を許可しないようにして、プリントサーバ１０２から取得する画像データが意図的あるいは不用意に変更されるのを防止することができる。

【０１０２】

本実施形態によれば、ユーザの個人認証を行うためのＩＤ情報と、画像データの出力を制御する出力制限情報とに基づいて、出力先のセキュリティ環境に応じた画像形成が可能になる。

【０１０３】

（第２実施形態）

本発明の第２実施形態について説明する。本実施形態は、オリジナル原稿として用いられるデータの一部（例えば、１ページ内の一部分や、複数ページのうちの一部分）等、特定のページや領域に対して、その内容の開示範囲を出力制限情報により管理する内容に関するものである。

【０１０４】

画像形成装置１１０には指紋読取装置１２１が接続されているために、画像形成処理を実行するに際し、第１実施形態の場合と同様にＩＤ情報の認証をユーザに促し、ＩＤ情報が一致したと判別される場合、ＣＰＵ１７１は、部分的な画像形成を実行して少なくとも一部の画像データは出力されないように画像形成装置を制御することができる。この場合、通常の複写動作の少なくとも一部のみを許可するようにし、また、オリジナルの原稿画像の印字をサーバ１０２から取得する際も少なくとも一部分だけ取得できるように制限するようにしてもよい。
この場合、部分的な制限は、出力制限情報で特定されている内容に従い、ＣＰＵ１７１は、ページや特定の領域に対して指定されている内容を制限して、文書毎にその内容の開示範囲を管理する。

【０１０５】
例えば、ポストスクリプト言語やテキストなどで記述された文書や画像と文字の混在した文書などから構成される文書データのうちの一部分（例えば、テキストデータの部分のみ）を開示するように、開示範囲を任意に設定することができる。
画像データ（文書データ）の例として、企業内のプロジェクト計画の概要を記述した機密性の高い文書を印刷する場合など、画像形成により開示される範囲をユーザ個人のアクセス権限に応じて設定することも可能である。この場合、プリントサーバ１０２に格納されているオリジナルの画像データ（文書データ）に対して、各ページや特定の領域ごとにセキュリティレベルを設定しておき、例えば、機密性の高い文書のページＰ１からページＰ３は中レベルのランクＢ、ページ４はそれより高いレベルのランクＡ等と設定しておき、画像データ（文書データ）を画像メモリ３に格納する際、出力制限情報として、セキュリティレベルに関する情報を画像データ（文書データ）と合わせて、メモリ３に格納しておく。

【０１０６】
画像データを出力する際には、ＩＤ情報によりユーザの認証をＣＰＵ１７１が行い、Ａランクのデータを参照可能なセキュリティレベルのユーザの場合、例えば、ＣＰＵ１７１は、上述のＡランク及びＢランクのページの文書（序呪術のＰ１～Ｐ４）を出力するようにする。また、Ｂランクのセキュリティレベルのユーザの場合、ＣＰＵ１７１は、Ｂランクに設定されているページのみ（Ｐ１～Ｐ３）を出力するように画像形成装置を制御する。

【０１０７】
セキュリティレベルの設定は、ユーザ個人のアクセス権限に対応したレベルの設定に限らず、例えば、上述の例で説明したように、テキストデータのみなど、データの属性を限定するものや、印刷範囲（ページＰ１～Ｐ３）のみを出力、暗号された画像データの復号化範囲などについて、開示範囲を指定することができるものとする。

【０１０８】
また、画像データ（文書データ）の属性として、例えば、ＪＰＥＧフォーマットによる写真などの画像データと、テキストデータなど、複数のファーマット形式で構成されるＨＴＭＬ文書の場合、ＣＰＵ１７１はＩＤ情報が一致しないと判別した場合、文書部分のテキストデータのみ印刷可能とし、ＪＰＥＧフォーマットによる写真の画像データ部分は出力しないようにし、ＩＤ情報が一致した場合、ＣＰＵ１７１は、ＪＰＥＧフォーマットの画像データ部分も出力するように、画像形成装置を制御することも可能である。

【０１０９】
ＣＰＵ１７１は、同一ページ中の一部分、特定の領域のみを表示しないようにするため、網掛け処理を行ったり、黒のトナーで塗りつぶして目視できないようにしたり、画像データそのものを白地データに置き換えるマスキング処理などをするなど、一部分の画像処理をその他の開示許可領域と変更するようなことも可能である。また、ＣＰＵ１７１は、ＪＰＥＧフォーマットの画像データ部分の解像度を極めて粗い低解像度に落として、印刷を行うように画像形成装置を制御することも可能である。

【０１１０】

尚、開示範囲の設定は、１つの画像データ（文書データ）の一部分に限らず、改訂した新しいバージョンの画像データ（文書データ）に関して、新旧の画像データ（文書データ）を指定して、開示範囲をそれぞれ設定することも可能である。

【０１１１】

例えば、出力制限情報により、複数回改訂された画像データ（文書データ）群のうち、所定の改訂分のみを開示許可するように開示範囲を設定することも可能である。旧版の画像データ（文書データ）については、セキュリティレベルを最低レベルに落として、個人認証も不要でオリジナルの画像データ（文書データ）をプリントサーバ１０２から取得できるものとし、所定の改訂版以降からは、所定のセキュリティレベルに応じて、オリジナルの画像データ（文書データ）をプリントサーバ１０２から取得して、印刷するように設定することも可能である。

【０１１２】

また、訂正書き換え中の文書等が印刷されることを禁止するために、最新の改訂バージョンのオリジナル画像データ（文書データ）に関しては、表示のみを許可し、印刷や内容変更を禁止するなどの制限を、出力制限情報により設定することも可能である。
この場合、例えば、ユーザの個人認証をＩＤ情報に基づいて行い、そのユーザ個人に認められているセキュリティ設定のレベルに応じて、開示範囲（表示が許可される範囲）が制限されるようにしてもよく、ＩＤ情報が一致しない場合には、表示を禁止することも可能である。

【０１１３】

本実施形態の画像形成装置によれば、ＩＤ情報の認証と出力制限情報の開示範囲の設定に基づき、ユーザのセキュリティ設定レベルに応じて画像データの特定のページや領域など、開示範囲を制御して画像形成を行うことができる。

【０１１４】

（第３実施形態）

次に、本発明の第３実施形態について説明する。本実施形態は、印刷回数や、プリントサーバ１０２から取得するオリジナルの画像データの取得回数を出力制限情報に従い制限する内容に関するものである。

【０１１５】

ネットワーク１１２に接続する画像形成装置１１０等の構成は、第１及び第２実施形態の場合と同様とし、画像データを生成するパーソナルコンピュータ１０１等、オリジナルの画像データを画像データ格納部３０４に格納するプリントサーバ１０２、ＩＤ情報及び出力制限情報に基づいて画像データの印刷を行う画像形成装置１０７（操作部からパスワード等を入力することによりユーザを認証する）、１１０（指紋読取装置１２１が接続しており、画像形成装置１０７に比べてセキュリティ保護のレベルが高い）等が接続しているものとする。

【０１１６】

プリントサーバ１０２は、パーソナルコンピュータ１０１等から送信されてきた画像データにＩＤ情報が付加されているか否かを判別する。プリントサーバ１０２のＩＤ情報判別部３０２は、ＩＤ情報が付加されている画像データの場合は、セキュリティを保護する画像形成装置１０７または、１１０を画像データの出力先として選択する。セキュリティ保護に関する手段を有さない画像形成装置１０８は選択されない。

【０１１７】

ここで、プリントサーバ１０２が画像形成装置１０７を出力先として選択した場合、図４に示すパーソナルコンピュータ１０１において、指紋読取装置１２１より入力した指紋の特徴量データを用いたＩＤ情報を画像データに付加しても、操作部からのキー入力（指紋の特徴量データではなく、パスワードなどの情報）による認証しか行えない、セキュリティレベル保護のレベルが画像形成装置１１０より低い、画像形成装置１０７にも画像データが送付されてしまうケースも生じる。

【０１１８】

図１０は、本発明の実施形態にかかるプリントサーバ１０２’の構成を示す図である。図１０におけるプリントサーバ１０２’には、ＩＤ情報識別部３０６が追加されている点で、図６のプリントサーバ１０２と相違する（構成の共通する部分は説明を省略する）。このＩＤ情報識別部３０６は、画像データに付加されてきたＩＤ情報の内容（指紋の特徴量データに基づくＩＤ情報か、操作部から入力されたパスワードに関する暗号化データに基づくＩＤ情報）を識別する手段として機能する。具体的には、ＩＤ情報識別部３０６は、画像データに付加されているＩＤ情報の情報量に基づいて、ＩＤ情報の内容を識別する。ＩＤ情報の情報量として、操作部からキー入力により入力された暗号データは、指紋の特徴量データから作成されたＩＤ情報に比べて情報量が少ないという相違点（情報量の差）に基づいて、ＩＤ情報識別部３０６は、ＩＤ情報として画像データに付加されているデータが、指紋の特徴量データに基づくＩＤ情報か、操作部から入力されたパスワードに関する暗号化データに基づくＩＤ情報かを識別する（セキュリティレベルの識別を行う）。

【０１１９】

図１１は、プリントサーバ１０２’におけるＩＤ情報を識別する処理の流れを説明するフローチャートである。

【０１２０】

まず、プリントサーバ１０２’は、パーソナルコンピュータ１０１等から送信された画像データをネットワークＩ／Ｆ３０１を経由して受信する。

受信された画像データは、ＩＤ情報判別部３０２に送信され、画像データにＩＤ情報が付加されているか否かについてＩＤ情報の判別が行われる（Ｓ２０２）。

送付された画像データにＩＤ情報が付加されていなければ（Ｓ２０３－ＮＯ）、処理をステップＳ２０５に進め、ＩＤ情報判別部３０２は、ＩＤ情報が画像データに付加されていない旨を制御部３０３に通知する。そして、制御部３０３は、画像データを一旦画像データ格納部３０４に格納した後、出力先アドレス判別部３０５によって判別されたドメインアドレスにて指定されている出力先の画像形成装置に画像データの転送を行う（Ｓ２０３、Ｓ２０５）。

【０１２１】

一方、送信された画像データにＩＤ情報が付加されている場合は（Ｓ２０３－ＹＥＳ）、処理をステップＳ２１１に進め、ＩＤ情報判別部３０２は、ＩＤ情報が画像データに付加されている旨を制御部３０３に通知する。そして、ＩＤ情報判別部３０２は、画像データをＩＤ情報識別部３０６に送信する。ＩＤ情報識別部３０６は、画像データに付加されているＩＤ情報の情報量に従い、ＩＤ情報の内容を識別し、情報量が多い（指紋の特徴量データに基づくＩＤ情報）と識別した場合（Ｓ２１２－ＹＥＳ）、処理をステップＳ２１３に進め、ＩＤ情報の内容は指紋の特徴量データに基づくＩＤ情報である旨を制御部３０３に通知する。この場合、画像データの出力先が、ＩＤ情報として指紋読取装置１２１により指紋の認証が可能な画像形成装置１１０と指定されている場合のみ（Ｓ２１３－ＹＥＳ）、出力先アドレス判別部３０５は、画像データを画像形成装置１１０に送信する（Ｓ２０５）。

【０１２２】

一方、ステップＳ２１３において、出力先として画像形成装置１１０が指定されていない場合（Ｓ２１３－ＮＯ）、エラー処理として画像データは送信されない（Ｓ２０６）。

【０１２３】

また、ステップＳ２１２において、ＩＤ情報の情報量が少ない（操作部から入力されたパスワードに関する暗号化データに基づくＩＤ情報）と識別された場合は（Ｓ２１２－ＮＯ）、ＩＤ情報識別部３０６は、その旨を制御部３０３に通知し、画像データの出力先の指定が１０７の画像形成装置と指定されていた時のみ、出力先アドレス判別部３０５は、画像データを画像形成装置１０７に送信する（Ｓ２０５）。その他の出力先が指定されている場合は（Ｓ214－ＮＯ）、エラー処理となり、画像データは送付されない（Ｓ２０６）。

【０１２４】

以上のように、ＩＤ情報の情報量に基づいて、出力先の画像形成装置におけるセキュリティの認証に関する装置のレベルが、画像データに付加されているＩＤ情報の情報量に対応したものでなければ、画像データを画像形成装置に送信しないことで、更に、セキュリティレベルの高い画像形成システムの構築が可能となる。

【０１２５】

様々な数学的暗号化手法が考案されているが、機密文書の配布に際しては、データの秘匿性を確保するために、解読困難な暗号化処理を行って機密文書データを配信するようにしてもよい。その場合、暗号化された機密文書データに内包される認証情報を正確に取り出すことで、簡単な構成で秘匿性の向上を図ることができる。

【０１２６】

例えば、暗号化した機密文書データを記録装置で紙面に印刷して配布し、受け取ったユーザは、画像データ入力部２００によって、暗号化された機密文書データを読み取り、画像データに変換する。この際、画像データ入力部２００で読み取られた機密文書データは特徴抽出処理が行われ、認証情報が抽出される。この処理は、ＣＰＵ１７１の全体的な制御の下、画像処理部１７０が実行する。更に、ＣＰＵ１７１及び画像処理部１７０は、指紋情報などのＩＤ情報量の有無やＩＤ情報の情報量などに基づき、機密文書データを復号化処理するかどうかを決定する。

【０１２７】

例えば、オリジナル原稿画像データにＩＤ情報を付与して暗号化されて印刷出力された印刷出力紙を原稿画像として、再度、画像形成装置により複写しようとした場合、印刷出力紙（暗号化原稿画像）をプラテンガラス上に置き、画像データ入力部２００で暗号化原稿画像を読み取って、画像データに変換する場合を想定する。

【０１２８】

この場合、暗号化原稿画像であっても、十分にＩＤ情報を読み取ることができるが、画像データ入力部２００の読み取り用センサの読み取り解像度と、画像形成装置の印字解像度は、設計値に対し僅かな誤差が含まれる。従って、暗号化原稿画像の複写を複数回繰り返していくうちに、読み取りセンサの解像度やセンサ光学系の若干収差などや、画像形成装置の印刷時の画像ドットのばらつきや、印刷倍率誤差などが累積し、ある程度、複写を繰り返すうちに、暗号化した画像自体の暗号情報が欠落し、情報が変化してしまうことになる。

【０１２９】

従って、暗号化原稿画像の複写を所定の回数以上繰り返すと、記録した情報が劣化して、復号化したときの誤り率が高くなってしまうことになる。この場合、復号化後の再生画像の品位は極端に落ちてしまう。場合によっては、文字情報が別の文字情報にランダムに化けてしまうという問題が発生する。

【０１３０】

このような場合、出力制限情報として、オリジナルの原稿画像、あるいは暗号化原稿画像を取得、複製する回数を一定回数に限定することで、文字化けが生じるようなご認識の問題を解消することが可能になる。

【０１３１】

画像形成システムは、システム立上げ時に各画像形成装置１０７、１０８、１１０より、各画像形成装置のセキュリティレベルがプリントサーバ１０２に通知され、プリントサーバ１０２は各画像形成装置のセキュリティレベルを把握しているものとする。

【０１３２】

出力制限情報において、オリジナル画像情報の取得を回数規定しておき、プリントサーバ１０２は、文書ごとに、どのユーザがどの文書を何回、プリントサーバ１０２から取得したかという情報取得回数を各オリジナル文書ごとに格納しておくことも可能である。

【０１３３】

例えば、出力制限情報の内容として、最大１０回までのオリジナル情報の取得を規定した場合、ユーザは、オリジナル画像データをプリントサーバ１０２から取得する毎に、オ

リジナル文書を格納しているプリントサーバ１０２は、ユーザがオリジナル画像データの取得を行った回数を累積して記憶して、累積データを参照可能な状態で、例えば、画像データ格納部３０４等に格納する。オリジナル原稿画像データの出力制限情報に最大データ取得可能回数＝１０回と規定され、画像データ格納部３０４には、ユーザにおける累積データ取得回数＝８回と格納されている場合、あと、２回までデータの再取得が可能であることが判別できる。

【０１３４】

例えば、画像形成装置における操作部１７２の表示部に「オリジナル画像のＵＲＬ、ファイル名、オリジナル画像の最大取得数＝１０回、現在の取得回数＝８、残り取得回数＝１回」を表示するようにしてもよい。

【０１３５】

このように、プリントサーバ１０２内のオリジナル原稿画像データに出力制限情報として、ユーザのデータ取得回数を関連つけて格納しておくことにより、秘匿性の高い情報のアクセス回数、データ取得回数、データアクセスしたユーザを把握できるようになり、例えば、同一人物が複数回データ取得を繰り返しているとかで、データの活用率の試算やデータ漏洩防止の為の情報提供が可能になる。

【０１３６】

本実施形態の画像形成システムによれば、ＩＤ情報の情報量に基づいて、出力先の画像形成装置におけるセキュリティの認証に関する装置のレベルが、画像データに付加されているＩＤ情報の情報量に対応したものでなければ、画像データを画像形成装置に送信しないことで、更に、セキュリティレベルの高い画像形成システムの構築が可能となる。
あるいは、ＩＤ情報の認証と出力制限情報における取得回数制限の設定に基づき、オリジナルのを制御して画像形成を行うことが可能になる。

【０１３７】

（他の実施形態）

なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。

【０１３８】

この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【０１３９】

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、フレキシブルディスク，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。

【０１４０】

また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

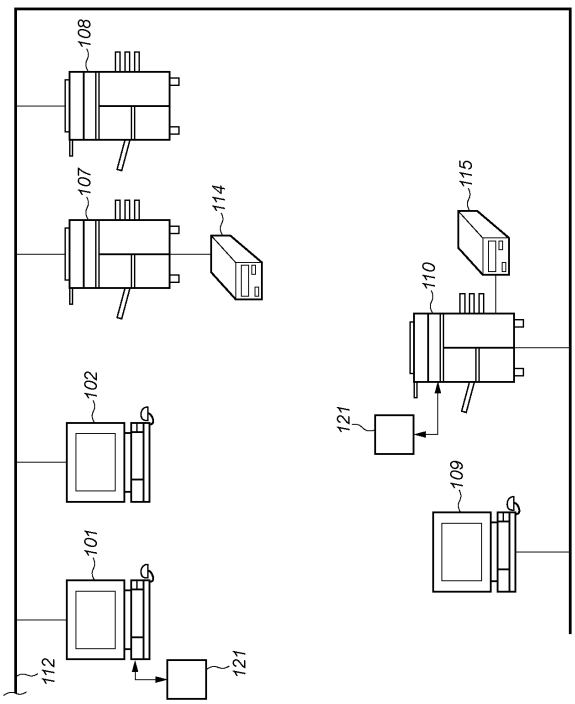
【０１４１】

さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

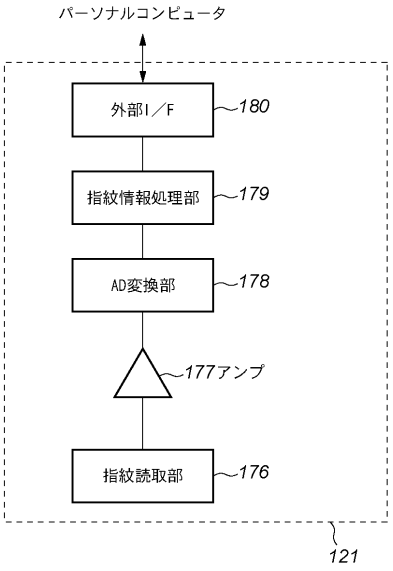
【図面の簡単な説明】

【０１４２】
【図１】本発明の第１実施形態にかかる画像形成システムの構成を示す図である。
【図２】指紋読取装置１２１の構成を説明する図である。
【図３】指紋読取部１７６の詳細を説明する図である。
【図４】パーソナルコンピュータ１０１におけるＩＤ情報を付加するための構成を説明する図である。
【図５】パーソナルコンピュータ１０１において、ＩＤ情報を付加するシーケンスを説明する図である。
【図６】プリントサーバ１０２におけるＩＤ情報を判別する構成を説明する図である。
【図７】プリントサーバ１０２におけるＩＤ情報を判別するシーケンスを示す図である。
【図８】画像形成装置の具体的な構成を説明する断面図である。
【図９】画像形成装置の制御ブロック図である。
【図１０】本発明の第３実施形態にかかるプリントサーバ１０２’の構成を示す図である。
【図１１】プリントサーバ１０２’におけるＩＤ情報を識別する処理の流れを説明するフローチャートである。
【図１２】画像形成装置における処理の流れを概略的に説明するフローチャートである。

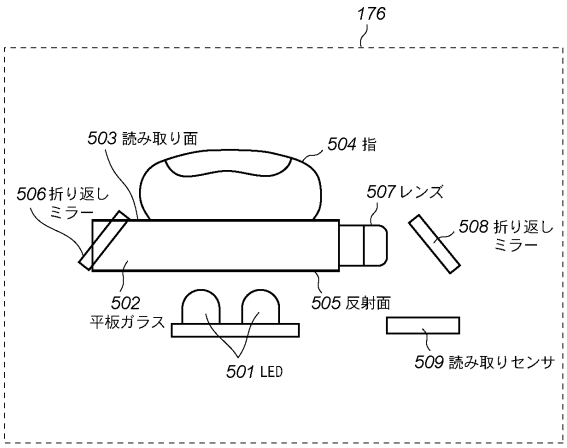
【図１】



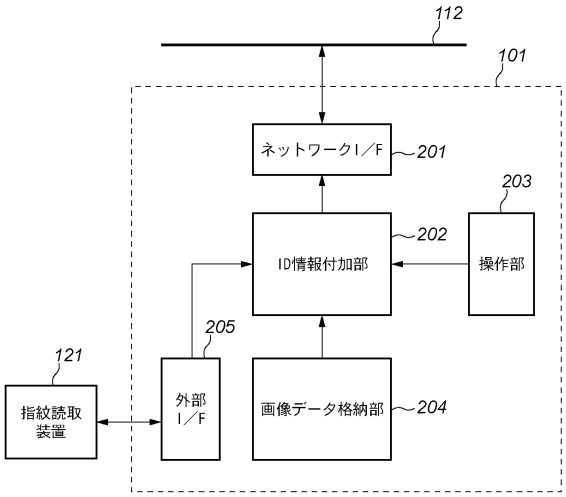
【図２】



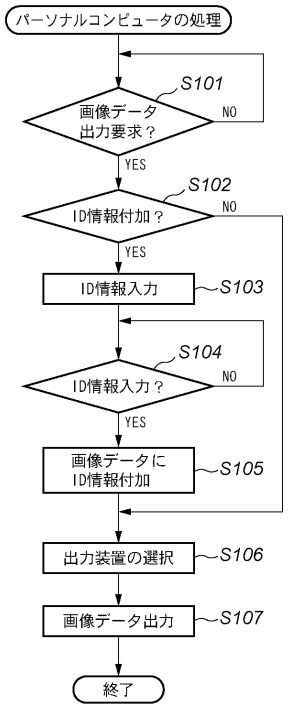
【図３】


176
503 読み取り面
504 指
506 折り返し
ミラー
507 レンズ
508 折り返し
ミラー
502
平板ガラス
505 反射面
501 LED
509 読み取りセンサ

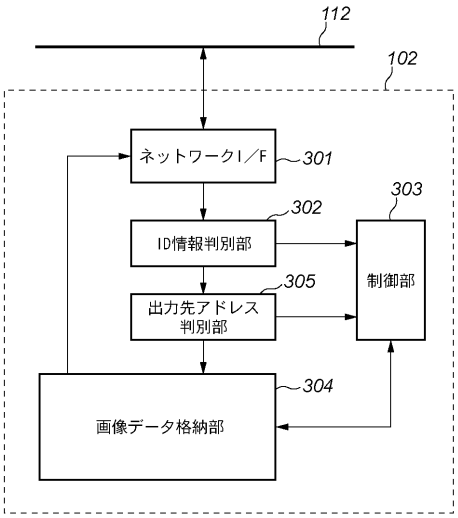
【図４】


112
101
ネットワークI／F
201
203
ID情報付加部
202
操作部
205
121
指紋読取
装置
外部
I／F
画像データ格納部
204

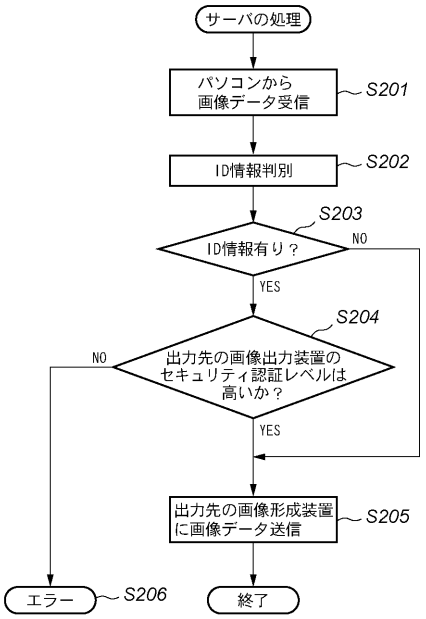
【図５】


パーソナルコンピュータの処理
S101
画像データ
出力要求？
NO
YES
S102
ID情報付加？
NO
YES
ID情報入力
S103
S104
ID情報入力？
NO
YES
画像データに
ID情報付加
S105
出力装置の選択
S106
画像データ出力
S107
終了

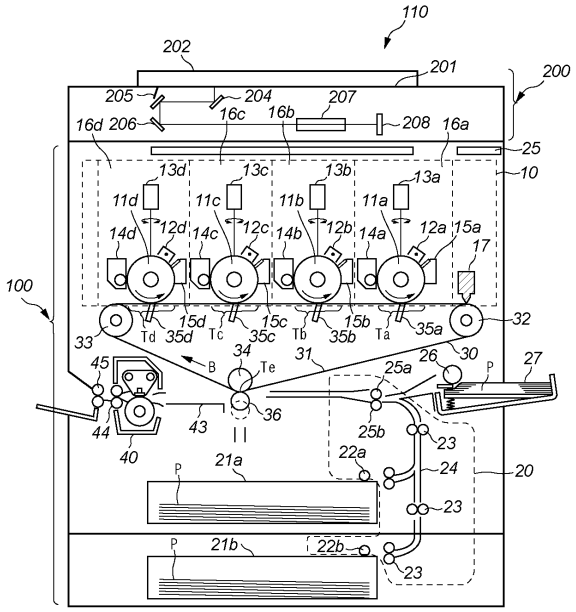
【図６】


112
102
ネットワークI／F
301
303
ID情報判別部
302
制御部
出力先アドレス
判別部
305
304
画像データ格納部

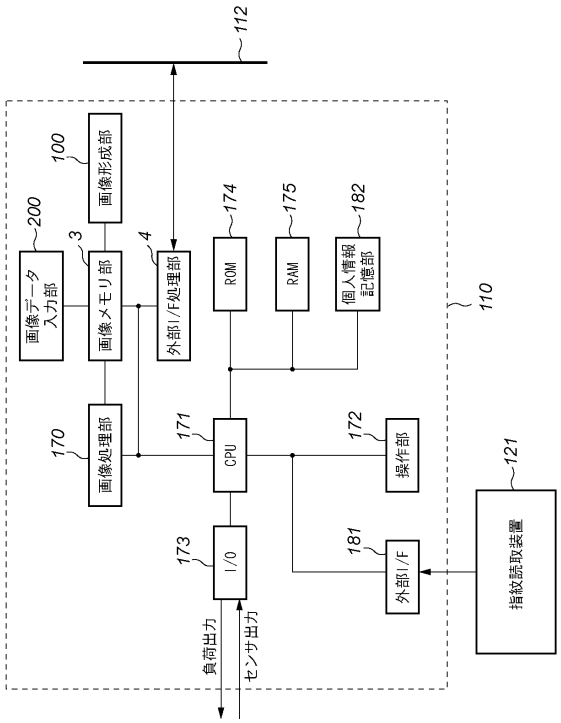
【図７】


サーバの処理
パソコンから
画像データ受信
S201
ID情報判別
S202
S203
ID情報有り？
NO
YES
S204
出力先の画像出力装置の
セキュリティ認証レベルは
高いか？
NO
YES
出力先の画像形成装置
に画像データ送信
S205
エラー
S206
終了

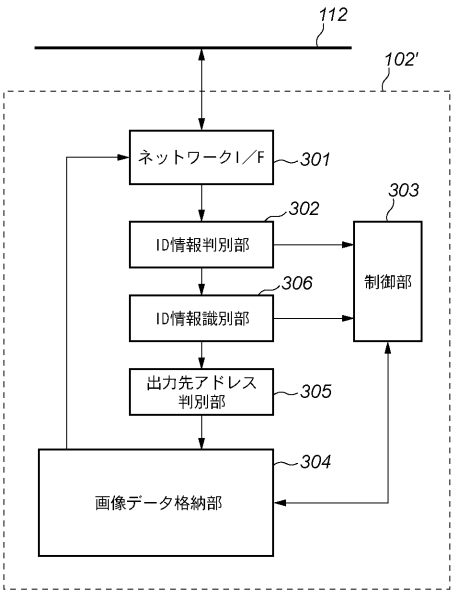
【図８】


110
202
201
200
205
204
207
16d 206
16c
16b
208
16a
25
10
13d
13c
13b
13a
11d
11c
11b
11a
14d
12d
14c
12c
14b
12b
14a
12a
15a
17
100
Td
35d
Tc
35c
Tb
35b
Ta
35a
32
33
45
B
34
Te
31
25a
26
30
P
27
44
43
36
25b
23
40
22a
24
20
P
21a
23
P
21b
22b
23

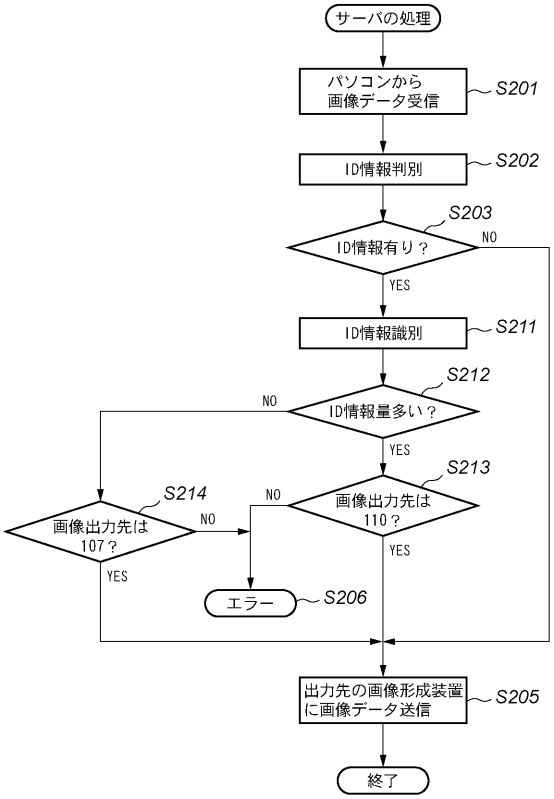
【図９】


112
100
画像形成部
200
画像データ
入力部
3
画像メモリ部
4
外部I/F処理部
ROM
174
RAM
175
個人情報
記憶部
182
110
170
画像処理部
171
CPU
172
操作部
121
指紋読取装置
173
I/O
181
外部I/F
負荷出力
センサ出力

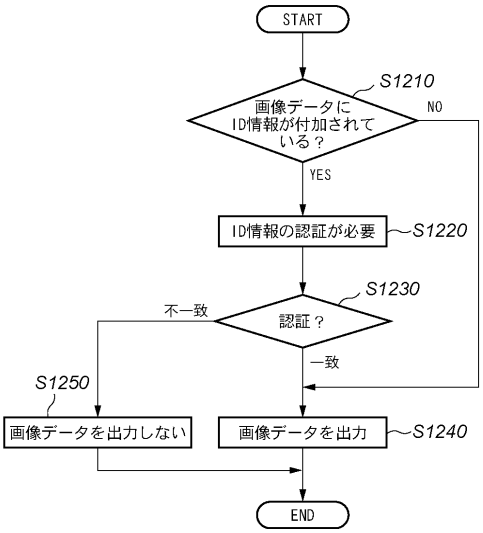
【図１０】


112
102'
ネットワークI／F
301
302
ID情報判別部
303
制御部
306
ID情報識別部
出力先アドレス
判別部
305
304
画像データ格納部

【図１１】


サーバの処理
パソコンから画像データ受信
S201
ID情報判別
S202
S203
ID情報有り？
NO
YES
ID情報識別
S211
S212
ID情報量多い？
NO
YES
S213
画像出力先は110？
NO
YES
S214
画像出力先は107？
NO
YES
エラー
S206
出力先の画像形成装置に画像データ送信
S205
終了

【図１２】


START
S1210
画像データにID情報が付加されている？
NO
YES
ID情報の認証が必要
S1220
S1230
認証？
不一致
一致
S1250
画像データを出力しない
画像データを出力
S1240
END

フロントページの続き

(72)発明者　小松　俊一
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
(72)発明者　増田　道晴
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
(72)発明者　長利　嘉人
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
(72)発明者　本保　綱男
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　田中　友章

(56)参考文献　特開２００１－３１２３８０（ＪＰ，Ａ）
特開２００１－０５１９１５（ＪＰ，Ａ）
特開２００３－０８７４５４（ＪＰ，Ａ）
特開２００１－０３６２７３（ＪＰ，Ａ）
特開２００４－２８７８２２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　３／１２
Ｂ４１Ｊ　２９／３８
Ｈ０４Ｎ　　１／２１