(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2007-168154
(P2007-168154A)
(43)公開日　平成19年7月5日(2007.7.5)

(51)Int.Cl.		F I			テーマコード（参考）
B41J 29/38	(2006.01)	B41J	29/38	Z	2C061
H04N 1/00	(2006.01)	H04N	1/00	107Z	5B021
B41J 29/00	(2006.01)	B41J	29/00	Z	5C062
G06F 3/12	(2006.01)	G06F	3/12	K	

審査請求 未請求　請求項の数 10　ＯＬ　（全 15 頁）

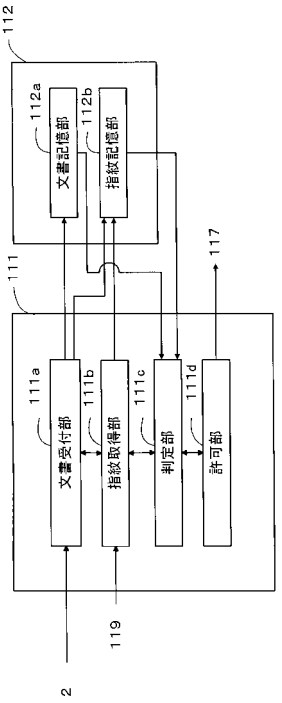
(21)出願番号　特願2005-366000 (P2005-366000)
(22)出願日　平成17年12月20日 (2005.12.20)

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(74)代理人　100080182
弁理士　渡辺　三彦
(72)発明者　宮崎　仁一
京都市伏見区竹田向代町１３６番地　村田機械株式会社内

Ｆターム(参考)　2C061 AP01 AP07 CL10 HK11 HN15 HQ12
5B021 AA01
5C062 AA29 AB17 AB22 AB38 AB42 AC02 AC04 AC22 AC24 AC58 BA00

(54)【発明の名称】画像形成装置、クライアント端末装置、及び、画像処理システム

(57)【要約】
【課題】利便性が良好で、且つ、セキュリティの確保可能なプリンタを実現する。
【解決手段】ネットワークプリンタ１のＣＰＵ１１１は、クライアント端末装置２から、指紋情報が付与された文書情報である第１形式の文書情報を受け付ける文書受付部１１１ａと、文書受付部１１１ａによって第１形式の文書情報が受け付けられた場合に、外部から指紋情報を取得する指紋取得部１１１ｂと、文書受付部１１１ａによって受け付けられた指紋情報と、指紋取得部１１１ｂによって取得された指紋情報とが、同一の個体を示す情報であるか否かを判定する判定部１１１ｃと、判定部１１１ｃによって同一の個体を示す情報であると判定された場合に、文書受付部１１１ａによって受け付けられた第１形式の文書情報のプリント処理を許可する許可部１１１ｄとを備えている。
【選択図】図３



【特許請求の範囲】
【請求項１】
クライアント端末装置と通信可能に接続され、プリント処理を実行可能に構成された画像形成装置であって、
前記クライアント端末装置から、個体認証情報が付与された文書情報である第１形式の文書情報を受け付ける文書受付手段と、
外部から個体認証情報を取得する認証取得手段と、
前記文書受付手段によって受け付けられた個体認証情報と、前記認証取得手段によって取得された個体認証情報とが、同一の個体を示す情報であるか否かを判定する判定手段と、
前記判定手段によって２つの個体認証情報が同一の個体を示す情報であると判定された場合に、前記文書受付手段によって受け付けられた第１形式の文書情報のプリント処理を許可する許可手段とを備えることを特徴とする画像形成装置。
【請求項２】
前記個体認証情報は、指紋情報であることを特徴とする請求項１に記載の画像形成装置。
【請求項３】
前記文書受付手段は、個体認証情報が付与されていない文書情報である第２形式の文書情報を受け付け、
前記許可手段は、前記文書受付手段によって受け付けられた第２形式の文書情報のプリント処理を許可することを特徴とする請求項１又は２に記載の画像形成装置。
【請求項４】
プリント処理を実行可能に構成された画像形成装置と通信可能に接続されたクライアント端末装置であって、
個体認証情報を格納する認証記憶手段と、
所定の文書情報に、前記認証記憶手段から読み出した個体認証情報を付与して第１形式の文書情報を生成する文書生成手段と、
前記文書生成手段によって生成された第１形式の文書情報をプリント処理するべく前記画像形成装置へ送信する文書送信手段とを備えることを特徴とするクライアント端末装置。
【請求項５】
外部から個体認証情報を取得して、前記認証記憶手段に格納する認証取得手段を備え、
前記認証取得手段は、前記画像形成装置のドライバをインストールする際に、個体認証情報を取得することを特徴とする請求項４に記載のクライアント端末装置。
【請求項６】
前記文書生成手段は、前記個体認証情報を、前記文書情報と同一の様式に変換して前記文書情報に付与することを特徴とする請求項４又は５に記載のクライアント端末装置。
【請求項７】
前記同一の様式は、ＰＤＬ（Ｐａｇｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｌａｎｇｕａｇｅ）であることを特徴とする請求項６に記載のクライアント端末装置。
【請求項８】
前記文書生成手段は、前記個体認証情報を、前記文書情報の前のページに付与することを特徴とする請求項７に記載のクライアント端末装置。
【請求項９】
前記文書生成手段は、前記文書情報と前記個体認証情報とを判別可能とするＰＪＬ（Ｐｒｉｎｔ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）コマンドを付与することを特徴とする請求項７又は８に記載のクライアント端末装置。
【請求項１０】
外部からの操作入力を受け付けるクライアント端末装置と、このクライアント端末装置と通信可能に接続され、プリント処理を実行可能に構成された画像形成装置とを有する画

像処理システムであって、
前記クライアント端末装置は、
個体認証情報を格納する認証記憶手段と、
所定の文書情報に、前記認証記憶手段から読み出した個体認証情報を付与して第１形式の文書情報を生成する文書生成手段と、
前記文書生成手段によって生成された第１形式の文書情報をプリント処理するべく前記画像形成装置へ送信する文書送信手段とを備え、
前記画像形成装置は、
前記クライアント端末装置から、前記第１形式の文書情報を受け付ける文書受付手段と、
外部から個体認証情報を取得する認証取得手段と、
前記文書受付手段によって受け付けられた個体認証情報と、前記認証取得手段によって取得された個体認証情報とが、同一の個体を示す情報であるか否かを判定する判定手段と、
前記判定手段によって２つの個体認証情報が同一の個体を示す情報であると判定された場合に、前記文書受付手段によって受け付けられた第１形式の文書情報のプリント処理を許可する許可手段とを備えることを特徴とする画像処理システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プリント処理を実行可能に構成された画像形成装置、クライアント端末装置及び画像処理システムに関するものであり、より詳しくは、個体認証情報を用いてプリント処理におけるセキュリティを確保する画像形成装置、クライアント端末装置及び画像処理システムに関するものである。
【背景技術】
【０００２】
従来、パーソナルコンピュータ等のクライアント端末装置にＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等を介して通信可能に接続されたプリンタ（いわゆる、ネットワークプリンタ）では、例えば、クライアント端末装置においてアプリケーションソフトウェアを介して作成された文書情報がプリントデータとして受信されて印刷される。ところが、プリントデータをプリンタへ送信したクライアント端末装置のユーザがプリンタから排出されたプリント済みの記録紙を取りに行くまでの間、プリントされた情報は誰もが容易に視認し、また持ち去ることも可能な状態に放置される。従って、企業、役所等において機密性が高い書類のセキュリティを確保できないという問題があった。
【０００３】
このような問題を解消するべく、いわゆる「親展印刷モード」という機能を有するプリンタ及びプリントシステム（特許文献１参照）が提案されている。この特許文献１に開示された発明においては、プリンタが受け取ったプリントデータに認証情報（例えばユーザＩＤ及びパスワード）が含まれている場合には、プリンタが親展印刷モードで印刷すべき書類であると判断する。この場合、プリンタはプリントデータを受信しても直ちに印刷することはせず、受信したプリントデータに含まれている認証情報が入力されたときに、入力された認証情報に対応するプリントデータに含まれている文書情報のプリントを実行する。
【０００４】
このようなプリンタを用いる場合、ユーザはプリンタへプリントデータを送信した後、プリンタの直近へ移動して、例えばプリンタの操作部の操作により認証情報を入力することによって、プリンタに印刷開始命令を与えれば、プリンタへ送信しておいたプリントデータに含まれる文書情報をその時点で印刷させることができる。したがって、ユーザはプリント済みの書類を他人に見られないようにしてプリント処理を実行させることが可能となるため、セキュリティの確保が可能となる。

【特許文献１】特開平５－１４３２５３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、パスワード等をプリンタに入力することが煩雑である場合があり、また、パスワード等が漏洩することによりセキュリティの確保が困難となる場合もある。更に、ユーザがパスワードを忘れてしまった場合には、プリンタへ送信しておいたプリントデータに含まれる文書情報をプリントできない場合もあり、利便性が充分であるとは言えなかった。
【０００６】
本発明は、かかる課題に鑑みてなされたものであり、利便性が良好で、且つ、セキュリティの確保が可能なプリンタ等の画像形成装置、クライアント端末装置及び画像処理システムを提供することを目的とするものである。
【課題を解決するための手段】
【０００７】
上記目的を達成するために、請求項１記載の画像形成装置は、クライアント端末装置と通信可能に接続され、プリント処理を実行可能に構成された画像形成装置であって、前記クライアント端末装置から、個体認証情報が付与された文書情報である第１形式の文書情報を受け付ける文書受付手段と、外部から個体認証情報を取得する認証取得手段と、前記文書受付手段によって受け付けられた個体認証情報と、前記認証取得手段によって取得された個体認証情報とが、同一の個体を示す情報であるか否かを判定する判定手段と、前記判定手段によって２つの個体認証情報が同一の個体を示す情報であると判定された場合に、前記文書受付手段によって受け付けられた第１形式の文書情報のプリント処理を許可する許可手段とを備えることを特徴としている。
【０００８】
この構成によれば、文書受付手段によって、通信可能に接続されたクライアント端末装置から、個体認証情報が付与された文書情報である第１形式の文書情報が受け付けられる。そして、認証取得手段によって、外部から個体認証情報が取得される。更に、判定手段によって、文書受付手段により受け付けられた個体認証情報と、認証取得手段により取得された個体認証情報とが、同一の個体を示す情報であるか否かが判定される。そして、許可手段によって、判定手段により２つの個体認証情報が同一の個体を示す情報であると判定された場合に、文書受付手段により受け付けられた第１形式の文書情報のプリント処理が許可される。
【０００９】
従って、クライアント端末装置から受け付けられ文書情報に付与された個体認証情報と、外部から取得された個体認証情報とが、同一の個体を示す情報であると判定された場合に、クライアント端末装置から受け付けられた文書情報のプリント処理が許可されるため、利便性が良好で、且つ、セキュリティの確保が可能となる。
【００１０】
請求項２記載の画像形成装置は、請求項１記載の画像形成装置において、前記個体認証情報が、指紋情報であることを特徴としている。
【００１１】
この構成によれば、個体認証情報が指紋情報であるため、認証取得手段によって個体認証情報が簡単に且つ短時間で取得されると共に、判定手段による判定が容易に且つ短時間で行われる。従って、認証取得手段及び判定手段が簡単な構成で実現される。
【００１２】
請求項３記載の画像形成装置は、請求項１又は２に記載の画像形成装置において、前記文書受付手段が、個体認証情報が付与されていない文書情報である第２形式の文書情報を受け付け、前記許可手段が、前記文書受付手段によって受け付けられた第２形式の文書情報のプリント処理を許可することを特徴としている。

【００１３】
この構成によれば、文書受付手段によって、個体認証情報が付与されていない文書情報である第２形式の文書情報が受け付けられ、許可手段によって、文書受付手段により受け付けられた第２形式の文書情報のプリント処理が許可される。
【００１４】
従って、個体認証情報が付与されていない文書情報である第２形式の文書情報が受け付けられ、プリント処理が許可されるため、個体認証情報が付与された文書情報である第１形式の文書情報に加えて、個体認証情報が付与されていない文書情報である第２形式の文書情報をプリント処理することが可能となる。
【００１５】
請求項４記載のクライアント端末装置は、プリント処理を実行可能に構成された画像形成装置と通信可能に接続されたクライアント端末装置であって、個体認証情報を格納する認証記憶手段と、所定の文書情報に、前記認証記憶手段から読み出した個体認証情報を付与して第１形式の文書情報を生成する文書生成手段と、前記文書生成手段によって生成された第１形式の文書情報をプリント処理するべく前記画像形成装置へ送信する文書送信手段とを備えることを特徴としている。
【００１６】
この構成によれば、認証記憶手段に、個体認証情報が格納されており、文書生成手段によって、所定の文書情報に、認証記憶手段から読み出した個体認証情報が付与されて第１形式の文書情報が生成される。そして、文書送信手段によって、文書生成手段により生成された第１形式の文書情報がプリント処理するべく画像形成装置へ送信される。
【００１７】
そこで、文書情報に個体認証情報が付与された第１形式の文書情報が画像形成装置へ送信されるため、画像形成装置で個体認証をすることにより、文書情報のプリント処理を許可するか否かの判定が可能となる。従って、文書情報のプリント処理において、利便性が良好で、且つ、セキュリティの確保が可能となる。
【００１８】
請求項５記載のクライアント端末装置は、請求項４に記載のクライアント端末装置において、外部から個体認証情報を取得して、前記認証記憶手段に格納する認証取得手段を備え、前記認証取得手段が、前記画像形成装置のドライバをインストールする際に、個体認証情報を取得することを特徴としている。
【００１９】
この構成によれば、認証取得手段によって、画像形成装置のドライバをインストールする際に、外部から個体認証情報が取得されて、認証記憶手段に格納されるため、個体認証情報を確実に取得することが可能となる。
【００２０】
請求項６記載のクライアント端末装置は、請求項４又は５に記載のクライアント端末装置において、前記文書生成手段が、前記個体認証情報を、前記文書情報と同一の様式に変換して前記文書情報に付与することを特徴としている。
【００２１】
この構成によれば、文書生成手段によって、個体認証情報が、文書情報と同一の様式に変換して文書情報に付与されるため、画像形成装置側の処理が簡略化される。
【００２２】
請求項７記載のクライアント端末装置は、請求項６に記載のクライアント端末装置において、前記同一の様式が、ＰＤＬ（Ｐａｇｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｌａｎｇｕａｇｅ）であることを特徴としている。
【００２３】
この構成によれば、個体認証情報及び文書情報の様式が、ＰＤＬであるため、画像形成装置側の処理が更に簡略化される。
【００２４】

請求項８記載のクライアント端末装置は、請求項７に記載のクライアント端末装置において、前記文書生成手段が、前記個体認証情報を、前記文書情報の前のページに付与することを特徴としている。

【００２５】

この構成によれば、文書生成手段によって、個体認証情報が文書情報の前のページに付与されるため、画像形成装置側での個体認証情報の判定処理が速やかに行われると共に、個体認証情報が付与された文書であるか否かの識別処理（第１形式の文書情報であるか第２形式の文書情報であるかの識別処理）が、速やかに行われる。

【００２６】

請求項９記載のクライアント端末装置は、請求項８に記載のクライアント端末装置において、前記文書生成手段が、前記文書情報と前記個体認証情報とを判別可能とするＰＪＬ（Ｐｒｉｎｔ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）コマンドを付与することを特徴としている。

【００２７】

この構成によれば、文書生成手段によって、文書情報と個体認証情報とを判別可能とするＰＪＬコマンドが付与されるため、画像形成装置側ではＰＪＬコマンドに基づいて文書情報と個体認証情報とを容易に判別することが可能となる。

【００２８】

請求項１０記載の画像処理システムは、外部からの操作入力を受け付けるクライアント端末装置と、このクライアント端末装置と通信可能に接続され、プリント処理を実行可能に構成された画像形成装置とを有する画像処理システムであって、前記クライアント端末装置が、個体認証情報を格納する認証記憶手段と、所定の文書情報に、前記認証記憶手段から読み出した個体認証情報を付与して第１形式の文書情報を生成する文書生成手段と、前記文書生成手段によって生成された第１形式の文書情報をプリント処理するべく前記画像形成装置へ送信する文書送信手段とを備え、前記画像形成装置が、前記クライアント端末装置から、前記第１形式の文書情報を受け付ける文書受付手段と、外部から個体認証情報を取得する認証取得手段と、前記文書受付手段によって受け付けられた個体認証情報と、前記認証取得手段によって取得された個体認証情報とが、同一の個体を示す情報であるか否かを判定する判定手段と、前記判定手段によって２つの個体認証情報が同一の個体を示す情報であると判定された場合に、前記文書受付手段によって受け付けられた第１形式の文書情報のプリント処理を許可する許可手段とを備えることを特徴としている。

【００２９】

この構成によれば、クライアント端末装置において、認証記憶手段に、個体認証情報が格納されており、文書生成手段によって、所定の文書情報に、認証記憶手段から読み出した個体認証情報が付与されて第１形式の文書情報が生成される。そして、文書送信手段によって、文書生成手段により生成された第１形式の文書情報がプリント処理するべく画像形成装置へ送信される。

【００３０】

また、画像形成装置において、文書受付手段によって、クライアント端末装置から、個体認証情報が付与された文書情報である第１形式の文書情報が受け付けられる。そして、認証取得手段によって、外部から個体認証情報が取得され、判定手段によって、文書受付手段により受け付けられた個体認証情報と、認証取得手段により取得された個体認証情報とが、同一の個体を示す情報であるか否かが判定される。更に、許可手段によって、判定手段により２つの個体認証情報が同一の個体を示す情報であると判定された場合に、文書受付手段により受け付けられた第１形式の文書情報のプリント処理が許可される。

【００３１】

従って、画像形成装置において、クライアント端末装置から受け付けられ文書情報に付与された個体認証情報と、外部から取得された個体認証情報とが、同一の個体を示す情報であると判定された場合に、クライアント端末装置から受け付けられた文書情報のプリント処理が許可されるため、利便性が良好で、且つ、セキュリティの確保が可能となる。

【発明の効果】

【００３２】
請求項１に記載の画像形成装置によれば、クライアント端末装置から受け付けられ文書情報に付与された個体認証情報と、外部から取得された個体認証情報とが、同一の個体を示す情報であると判定された場合に、クライアント端末装置から受け付けられた文書情報のプリント処理が許可されるため、利便性を良好としつつ、セキュリティを確保することができる。
【００３３】
請求項２に記載の画像形成装置によれば、個体認証情報が指紋情報であるため、認証取得手段によって個体認証情報が簡単に且つ短時間で取得されると共に、判定手段による判定が容易に且つ短時間で行われるので、認証取得手段及び判定手段を簡単な構成で実現できる。
【００３４】
請求項３に記載の画像形成装置によれば、個体認証情報が付与されていない文書情報である第２形式の文書情報が受け付けられ、プリント処理が許可されるため、個体認証情報が付与された文書情報である第１形式の文書情報に加えて、個体認証情報が付与されていない文書情報である第２形式の文書情報をプリント処理することができる。
【００３５】
請求項４に記載のクライアント端末装置によれば、文書情報に個体認証情報が付与された第１形式の文書情報が画像形成装置へ送信されるため、画像形成装置で個体認証をすることにより、文書情報のプリント処理を許可するか否かの判定が可能となるので、文書情報のプリント処理において、利便性を良好とし、且つ、セキュリティを確保することができる。
【００３６】
請求項５に記載のクライアント端末装置によれば、画像形成装置のドライバをインストールする際に、外部から個体認証情報が取得されて、認証記憶手段に格納されるため、個体認証情報を確実に取得することができる。
【００３７】
請求項６に記載のクライアント端末装置によれば、個体認証情報が、文書情報と同一の様式に変換して文書情報に付与されるため、画像形成装置側の処理を簡略化することができる。
【００３８】
請求項７に記載のクライアント端末装置によれば、個体認証情報及び文書情報の様式が、ＰＤＬであるため、画像形成装置側の処理を更に簡略化することができる。
【００３９】
請求項８に記載のクライアント端末装置によれば、文書生成手段によって、個体認証情報が文書情報の前のページに付与されるため、画像形成装置側での個体認証情報の判定処理を速やかに行うことができると共に、個体認証情報が付与された文書であるか否かの識別処理（第１形式の文書情報であるか第２形式の文書情報であるかの識別処理）を、速やかに行うことができる。
【００４０】
請求項９に記載のクライアント端末装置によれば、文書情報と個体認証情報とを判別可能とするＰＪＬコマンドが付与されるため、画像形成装置側ではＰＪＬコマンドに基づいて文書情報と個体認証情報とを容易に判別することができる。
【００４１】
請求項１０に記載の画像処理システムによれば、画像形成装置において、クライアント端末装置から受け付けられ文書情報に付与された個体認証情報と、外部から取得された個体認証情報とが、同一の個体を示す情報であると判定された場合に、クライアント端末装置から受け付けられた文書情報のプリント処理が許可されるため、利便性を良好としつつ、セキュリティを確保することができる。
【発明を実施するための最良の形態】

【００４２】
以下、本発明に係る画像処理システムについて図面に基づき説明する。図１は、本発明に係る画像処理システムの一例を示す構成図である。すなわち、画像処理システムは、ネットワークプリンタ１（本発明に係る画像形成装置の実施形態の一例）とクライアント端末装置２とを備えている。画像形成装置としては、画像データをクライアント端末装置２から受信すると共に、受信した画像データをプリントするプリント機能を有するネットワークプリンタを例に挙げて説明するが、これ以外のファクシミリ送信処理及びインターネットファクシミリ送信処理の少なくとも１の処理を実行可能に構成された複合機であっても本発明を適用することは可能である。
【００４３】
ネットワークプリンタ１は、ＣＰＵ（中央処理装置）１１１、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１１２、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１１３、画像メモリ１１４、コーデック（ＣＯＤＥＣ：Ｃｏｄｅｒ ａｎｄ Ｄｅｃｏｄｅｒ）１１５、読取部１１６、記録部１１７、操作部１１８、指紋読取部１１９、表示部１２０、及び、ＬＡＮインターフェース１２１を備えたものであって、各部１１１～１２１は、バス１２２を介して通信可能に接続されている。
【００４４】
ＣＰＵ１１１は、ＲＯＭ１１３に格納された制御プログラムに従って、このネットワークプリンタ１を構成する各部１１２～１２１を制御する制御手段として機能する。ＲＡＭ１１２は、ＣＰＵ１１１のワークエリア等として機能する。ＲＯＭ１１３は、前記制御プログラムを格納するものである。画像メモリ１１４は、受信した画像データ、読取部１１６で読み取った画像データ等を蓄積するものである。
【００４５】
コーデック１１５は、画像データの符号化及び復号を行うものである。すなわち、読取部１１６により読み取った原稿の画像データを送信のためにＭＨ、ＭＲ方式等により符号化し、外部から受信した画像データを復号するものである。
【００４６】
読取部１１６は、原稿の画像データを読み取るものであり、例えば、ＣＣＤカラーラインセンサ、Ａ／Ｄコンバータ、画像処理回路等で構成されている。記録部１１７は、受信した画像データ等を記録紙上に画像形成処理（プリント処理）を行うものである。例えば電子写真方式のものが適用される。操作部１１８は、ユーザが情報を入力する入力キー、タッチパネル等から構成され、ユーザによる各種の入力操作は、この操作部１１８を介して行われる。なお、記録部１１７は、図３を用いて後述する許可部１１１ｄによってプリント処理が許可された文書情報に限って、プリント処理を実行するものである。
【００４７】
指紋読取部１１９は、例えば、ＣＣＤカメラ等からなる撮像手段を備え、ＣＣＤカメラを介してユーザの指紋を撮像することにより生成された指紋情報（＝指紋の画像データ）から個人認証に必要な特徴点データを抽出するものである。表示部１２０は、例えば操作部１１８に並設されたＬＣＤ（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）等からなり、各種の画面情報を表示する表示手段として機能する。ＬＡＮインターフェース１２１は、ネットワークプリンタ１とＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）２１とを通信可能に接続するものである。ＬＡＮ２１には、例えば、ユーザからの操作入力を受け付けるクライアント端末装置２が接続される。
【００４８】
クライアント端末装置２は、例えば、パーソナルコンピュータ等からなり、マウス、キーボード等を介してユーザからの操作入力を受け付けて、ＬＡＮ２１を介してネットワークプリンタ１への操作入力を伝送すると共に、ネットワークプリンタ１からＬＡＮ２１を介して画像データ等の種々の情報を受信して、モニタに表示するものである。
【００４９】
上記した構成を備えるネットワークプリンタ１は、ＬＡＮ２１を介してクライアント端

末装置２から画像データを受信すると共に、受信した画像データを、記録部１１７を介して記録紙上にプリントするものである。

【００５０】

図２は、本発明に係るクライアント端末装置２の一例を示す構成図である。すなわち、クライアント端末装置２は、ＣＰＵ（中央処理装置）２１１、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２１２、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２１３、操作部２１４、指紋読取部２１５、表示部２１６、及び、ＬＡＮインターフェース２１７を備えたものであって、各部２１１～２１７は、バス２１８を介して通信可能に接続されている。

【００５１】

ＣＰＵ２１１は、ＲＯＭ２１３に格納された制御プログラムに従って、このクライアント端末装置２を構成する各部２１２～２１７を制御する制御手段として機能する。ＲＡＭ２１２は、ＣＰＵ２１１のワークエリア等として機能する。ＲＯＭ２１３は、前記制御プログラムを格納するものである。

【００５２】

操作部２１４は、ユーザが情報を入力するマウス、キーボード等から構成され、ユーザによる各種の入力操作は、この操作部２１４を介して行われる。指紋読取部２１５は、例えばＣＣＤカメラ等からなる撮像手段を備え、ＣＣＤカメラを介してユーザの指紋を撮像することにより生成された指紋情報（指紋画像データ）から個人認証に必要な特徴点データを抽出するものである。表示部２１６は、例えばＬＣＤ等からなり、各種の画面情報を表示するものである。ＬＡＮインターフェース２１７は、クライアント端末装置２とＬＡＮ２１とを通信可能に接続するものである。

【００５３】

図３は、本発明に係るネットワークプリンタ１の主要部の一例を示す機能構成図である。ネットワークプリンタ１のＣＰＵ１１１は、機能的に、文書受付部１１１ａ（文書受付手段に相当する）と、指紋取得部１１１ｂ（認証取得手段に相当する）と、判定部１１１ｃ（判定手段に相当する）と、許可部１１１ｄ（許可手段に相当する）とを備えている。また、ネットワークプリンタ１のＲＡＭ１１２は、機能的に、文書記憶部１１２ａと、指紋記憶部１１２ｂとを備えている。

【００５４】

ここでは、ＣＰＵ１１１が、ＲＯＭ１１３等に予め格納された制御プログラムを読み出して実行することにより、文書受付部１１１ａ、指紋取得部１１１ｂ、判定部１１１ｃ、及び、許可部１１１ｄを含む機能部として機能すると共に、ＲＡＭ１１２を、文書記憶部１１２ａ、及び、指紋記憶部１１２ｂを含む機能部として機能させるものである。

【００５５】

次に、ネットワークプリンタ１の各機能部について説明する。文書受付部１１１ａは、クライアント端末装置２から、個体認証情報（ここでは、指紋情報）が付与された文書情報である第１形式の文書情報を受け付けると共に、個体認証情報が付与されていない文書情報である第２形式の文書情報を受け付けるものである。また、文書受付部１１１ａは、クライアント端末装置２から受け付けた第１形式の文書情報及び第２形式の文書情報を文書記憶部１１２ａに格納するものである。

【００５６】

指紋取得部１１１ｂは、文書受付部１１１ａによって第１形式の文書情報が受け付けられた場合に、図１に示す指紋読取部１１９を介して、外部から個体認証情報（ここでは、指紋情報）を取得し、取得した指紋情報を指紋記憶部１１２ｂに格納するものである。より具体的には、指紋取得部１１１ｂは、まず、指紋読取部１１９に配設されたＣＣＤカメラの撮像範囲内にユーザの指（通常、人差し指）が載置されたことを検出し、次に、その指を撮像して画像データを取得し、そして、その画像データから指紋情報（＝特徴点データ）を抽出するものである。

【００５７】

判定部１１１ｃは、文書受付部１１１ａによって受け付けられた指紋情報と、指紋取得部１１１ｂによって取得された指紋情報とが、同一の個体（＝ユーザ）を示す情報であるか否かを判定するものである。すなわち、判定部１１１ｃは、第１形式の文書情報に含まれる指紋情報と指紋取得部１１１ｂにより取得された指紋情報との指紋認証処理を行うことにより、いわゆる個体認証処理を行うものである。

【００５８】

許可部１１１ｄは、判定部１１１ｃによって２つの指紋情報（第１形式の文書情報に含まれる指紋情報、及び、指紋取得部１１１ｂにより取得された指紋情報）が同一の個体を示す情報であると判定された場合に、文書受付部１１１ａによって受け付けられた第１形式の文書情報のプリント処理を許可すると共に、同一の個体を示す情報ではないと判定された場合に、表示部１２０のＬＣＤにエラーメッセージを表示するものである。また、許可部１１１ｄは、文書受付部１１１ａによって受け付けられた第２形式の文書情報のプリント処理を許可するものである。換言すれば、許可部１１１ｄは、文書受付部１１１ａによって第１形式の文書情報が受け付けられた場合には、判定部１１１ｃによって個体認証が成立した場合に限ってプリント処理を許可し、文書受付部１１１ａによって第２形式の文書情報が受け付けられた場合には、無条件にプリント処理を許可するものである。なお、図１に示す記録部１１７は、許可部１１１ｄによって、プリント処理が許可された文書情報に限って、プリント処理を実行するものである。

【００５９】

文書記憶部１１２ａは、文書受付部１１１ａによって受け付けられた第１形式の文書情報及び第２形式の文書情報を格納するものである。指紋記憶部１１２ｂは、指紋取得部１１１ｂによって取得された指紋情報を格納するものである。

【００６０】

図４は、本発明に係るクライアント端末装置２の主要部の一例を示す機能構成図である。クライアント端末装置２のＣＰＵ２１１は、機能的に、指紋取得部２１１ａ（認証取得手段に相当する）と、文書生成部２１１ｂ（文書生成手段に相当する）と、文書送信部２１１ｃ（文書送信手段に相当する）とを備えている。また、クライアント端末装置２のＲＡＭ２１２は、機能的に、指紋記憶部２１２ａ（認証記憶手段に相当する）を備えている。

【００６１】

ここでは、ＣＰＵ２１１が、ＲＯＭ２１３等に予め格納された制御プログラムを読み出して実行することにより、指紋取得部２１１ａ、文書生成部２１１ｂ、及び、文書送信部２１１ｃを含む機能部として機能すると共に、ＲＡＭ２１２を、指紋記憶部２１２ａを含む機能部として機能させるものである。

【００６２】

次に、クライアント端末装置２の各機能部について説明する。指紋取得部２１１ａは、図２に示す指紋読取部２１５を介して、ネットワークプリンタ１のドライバをインストールする際に、外部から個体認証情報（ここでは、指紋情報）を取得し、指紋記憶部２１２ａに格納するものである。より具体的には、指紋取得部２１１ａは、まず、指紋読取部２１５に配設されたＣＣＤカメラの撮像範囲内にユーザの指（通常、人差し指）が載置されたことを検出し、次に、その指を撮像して画像データを取得し、そして、その画像データから指紋情報（＝特徴点データ）を抽出するものである。

【００６３】

文書生成部２１１ｂは、所定の文書情報に、指紋記憶部２１２ａから読み出した指紋情報を付与して第１形式の文書情報を生成するものである。また、文書生成部２１１ｂは、指紋情報を付与しない第２形式の文書情報をも生成するものである。ここで、所定の文書情報は、例えば、クライアント端末装置２にインストールされているワープロソフトを介して、クライアント端末装置２で生成されたものでも良いし、ＬＡＮ２１（又は、図略のインターネット）を介して他の端末装置（又は、サーバ装置）から取得されたものでもよい。

【００６４】
また、文書生成部２１１ｂは、指紋情報を、文書情報と同一の様式（ここでは、ＰＤＬ（Ｐａｇｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｌａｎｇｕａｇｅ））に変換して、ＰＤＬに変換された指紋情報を文書情報の前のページに付与して、第１形式の文書情報を生成するものである。更に、文書生成部２１１ｂは、文書情報と指紋情報とを判別可能とするＰＪＬ（Ｐｒｉｎｔ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）コマンドを付与して、第１形式の文書情報を生成するものである。
【００６５】
文書送信部２１１ｃは、文書生成部２１１ｂによって生成された第１形式の文書情報、及び、第２形式の文書情報をプリント処理するべく、ネットワークプリンタ１へＬＡＮ２１を介して送信するものである。また、指紋記憶部２１２ａは、指紋取得部２１１ａによって取得された指紋情報を格納するものである。
【００６６】
図５は、クライアント端末装置２の動作の一例を説明するフローチャートである。なお、便宜上、予め指紋取得部２１１ａによって指紋記憶部２１２ａに指紋情報が格納されているものとする。まず、文書生成部２１１ｂによって、指紋情報を付与するか否か（第１形式の文書情報を生成するか否か）の判定が行われる（Ｓ１０１）。指紋情報を付与しないと判定された場合（Ｓ１０１でＮＯ）には、文書生成部２１１ｂによって、文書情報が取得（または生成）され（Ｓ１０９）、第２形式の文書情報が生成され（Ｓ１１１）、処理がステップＳ１１３に進められる。
【００６７】
指紋情報を付与すると判定された場合（Ｓ１０１でＹＥＳ）には、文書生成部２１１ｂによって、文書情報が取得（または生成）され（Ｓ１０３）、文書生成部２１１ｂによって、指紋記憶部２１２ａから指紋情報が読み出される（Ｓ１０５）。そして、文書生成部２１１ｂによって、ステップＳ１０３で取得（又は生成）された文書情報に、ステップＳ１０５で読み出された指紋情報が付与されて第１形式の文書情報が生成される（Ｓ１０７）。ステップＳ１０７の処理、又は、ステップＳ１１１の処理が終了した場合には、文書送信部２１１ｃによって、生成された第１形式の文書情報（又は第２形式の文書情報）が、ネットワークプリンタ１へ送信され（Ｓ１１３）、処理が終了される。
【００６８】
図６は、ネットワークプリンタ１の動作の一例を説明するフローチャートである。まず、文書受付部１１１ａによって、クライアント端末装置２から文書情報が受け付けられたか否かの判定が行われる（Ｓ２０１）。文書情報が受け付けられていないと判定された場合（Ｓ２０１でＮＯ）には、処理が待機状態とされる。文書情報が受け付けられたと判定された場合（Ｓ２０１でＹＥＳ）には、判定部１１１ｃによって、文書受付部１１１ａによって受け付けられた文書情報が、第１形式の文書情報であるか否かの判定が行われる（Ｓ２０３）。第１形式の文書情報ではない（すなわち、第２形式の文書情報である）と判定された場合（Ｓ２０３でＮＯ）には、処理がステップＳ２１１に進められる。
【００６９】
判定部１１１ｃによって、第１形式の文書情報であると判定された場合（Ｓ２０３でＹＥＳ）には、判定部１１１ｃによって、受け付けられた第１形式の文書情報の中から、指紋情報と文書情報とが判別されて、指紋情報が抽出され（Ｓ２０５）、指紋取得部１１１ｂによって、指紋読取部１１９を介して指紋情報が取得される（Ｓ２０７）。そして、判定部１１１ｃによって、ステップＳ２０５で抽出された指紋情報と、ステップＳ２０７で取得された指紋情報とが同一の個体の指紋情報であるか否か（ここでは、簡単のため、「一致するか否か」と表記する）の判定が行われる（Ｓ２０９）。
【００７０】
一致すると判定された場合（Ｓ２０９でＹＥＳ）、又は、ステップＳ２０３でＮＯの場合には、許可部１１１ｄによって、文書情報のプリントが許可され（Ｓ２１１）、処理が終了される。一致しないと判定された場合（Ｓ２０９でＮＯ）には、許可部１１１ｄによ

って、例えば、「個人認証が成立しません！」等のエラーメッセージが表示部１２０のＬＣＤに表示され（Ｓ２１３）、処理が終了される。

【００７１】

このようにして、ネットワークプリンタ１において、クライアント端末装置２から受け付けられ文書情報に付与された指紋情報と、外部から取得された指紋情報とが、同一の個体を示す情報であると判定された場合に、クライアント端末装置２から受け付けられた文書情報のプリント処理が許可されるため、利便性が良好で、且つ、セキュリティの確保が可能となる。

【００７２】

また、個体認証情報が指紋情報であるため、指紋取得部１１１ｂによって個体認証情報が簡単に且つ短時間で取得されると共に、判定部１１１ｃによる判定が容易に且つ短時間で行われる。従って、指紋取得部１１１ｂ及び判定部１１１ｃが簡単な構成で実現される。

【００７３】

更に、個体認証情報が付与されていない文書情報である第２形式の文書情報が受け付けられ、プリント処理が許可されるため、個体認証情報が付与された文書情報である第１形式の文書情報に加えて、個体認証情報が付与されていない文書情報である第２形式の文書情報をプリント処理することが可能となる。

【００７４】

加えて、文書情報に個体認証情報が付与された第１形式の文書情報がネットワークプリンタ１へ送信されるため、ネットワークプリンタ１で個体認証（ここでは、指紋認証）をすることにより、文書情報のプリント処理を許可するか否かの判定が可能となる。従って、文書情報のプリント処理において、利便性が良好で、且つ、セキュリティの確保が可能となる。

【００７５】

また、ネットワークプリンタ１のドライバをインストールする際に、外部から個体認証情報（ここでは、指紋情報）が取得されて、指紋記憶部２１２ａに格納されるため、指紋情報を確実に取得することが可能となる。

【００７６】

更に、個体認証情報が、文書情報と同一の様式に変換して文書情報に付与されるため、ネットワークプリンタ１側の処理が簡略化される。

【００７７】

加えて、指紋情報が文書情報の前のページに付与されるため、ネットワークプリンタ１側での個体認証情報の判定処理が速やかに行われると共に、個体認証情報が付与された文書であるか否かの識別処理（第１形式の文書情報であるか第２形式の文書情報であるかの識別処理）が、速やかに行われる。

【００７８】

また、文書情報と個体認証情報とを判別可能とするＰＪＬコマンドが付与されるため、ネットワークプリンタ１側ではＰＪＬコマンドに基づいて文書情報と指紋情報とを容易に判別することが可能となる。

【００７９】

なお、本発明は、上記実施形態に限定されるものではなく、以下の形態でもよい。

（Ａ）本実施形態においては、個人認証情報が指紋情報である場合について説明したが、これに限らず、例えば、網膜、虹彩、声紋等の生体情報であってもよい。個人認証情報の種類によって、セキュリティのレベルが変化するため、適当な個人認証情報を選択すれば所望するセキュリティレベルを実現できる。

【００８０】

（Ｂ）本実施形態においては、画像形成装置がネットワークプリンタ１である場合について説明したが、プリント機能を有する複合機であってもよい。

【００８１】

（Ｃ）本実施形態においては、クライアント端末装置２が、ネットワークプリンタ１のドライバをインストールする際に、指紋情報を取得し、指紋記憶部２１２ａに格納する場合について説明したが、その他のタイミングで指紋情報を取得し、指紋記憶部２１２ａに格納する形態でもよい。例えば、クライアント端末装置２が、所定のユーザに割り当てられた際に指紋情報を取得し、指紋記憶部２１２ａに格納する形態でもよい。この場合には、クライアント端末装置２が所定のユーザに割り当てられた際に指紋読取部２１５を接続し、指紋情報が指紋記憶部２１２ａに格納された後は、指紋読取部２１５が不要となるため、クライアント端末装置２が簡略化される。

【００８２】

（Ｄ）本実施形態においては、クライアント端末装置２が、指紋読取部２１５を備える場合について説明したが、指紋情報が予め他の装置（例えば、ネットワークプリンタ１）で読み取られて、ＣＤ等の記録媒体に格納されており、所定のタイミングで指紋記憶部２１２ａに格納する形態でもよい。この場合には、クライアント端末装置２が、指紋読取部２１５を備える必要がないため、クライアント端末装置２が簡略化される。

【図面の簡単な説明】

【００８３】

【図１】本発明に係るネットワークプリンタの一例を示す構成図である。

【図２】本発明に係るクライアント端末装置の一例を示す構成図である。

【図３】本発明に係るネットワークプリンタの主要部の一例を示す機能構成図である。

【図４】本発明に係るクライアント端末装置の主要部の一例を示す機能構成図である。

【図５】クライアント端末装置の動作の一例を説明するフローチャートである。

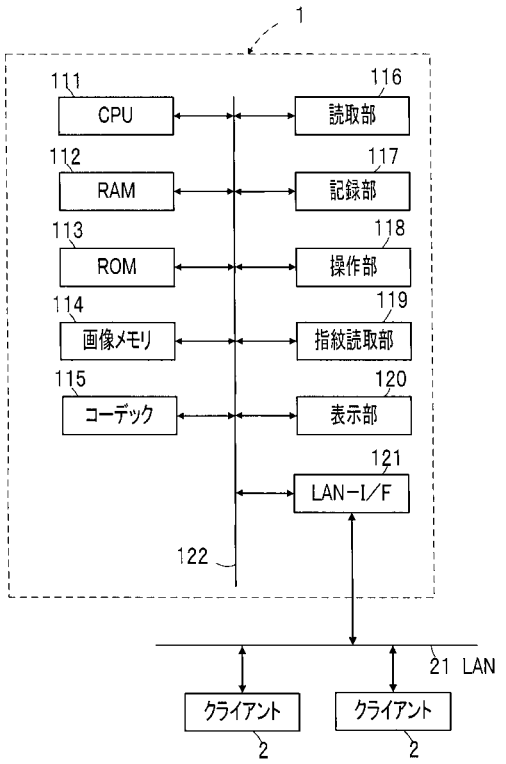
【図６】ネットワークプリンタの動作の一例を説明するフローチャートである。

【符号の説明】

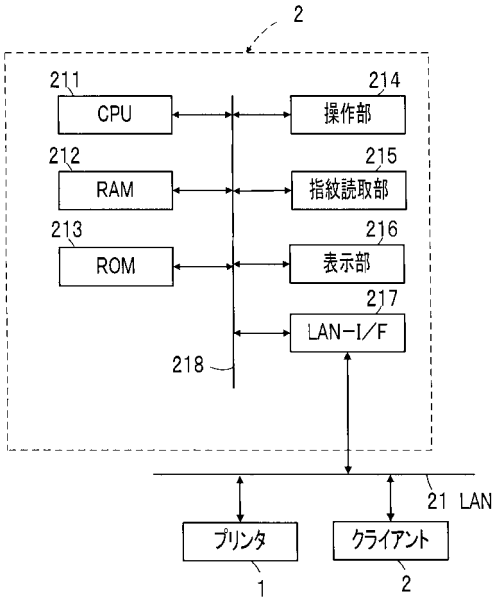
【００８４】

１　ネットワークプリンタ（画像形成装置）
１１１　ＣＰＵ
１１１ａ　文書受付部（文書受付手段）
１１１ｂ　指紋取得部（認証取得手段）
１１１ｃ　判定部（判定手段）
１１１ｄ　許可部（許可手段）
１１２　ＲＡＭ
１１２ａ　文書記憶部
１１２ｂ　指紋記憶部
２　クライアント端末装置
２１１　ＣＰＵ
２１１ａ　指紋取得部（認証取得手段）
２１１ｂ　文書生成部（文書生成手段）
２１１ｃ　文書送信部（文書送信手段）
２１２　ＲＡＭ
２１２ａ　指紋記憶部（認証記憶手段）

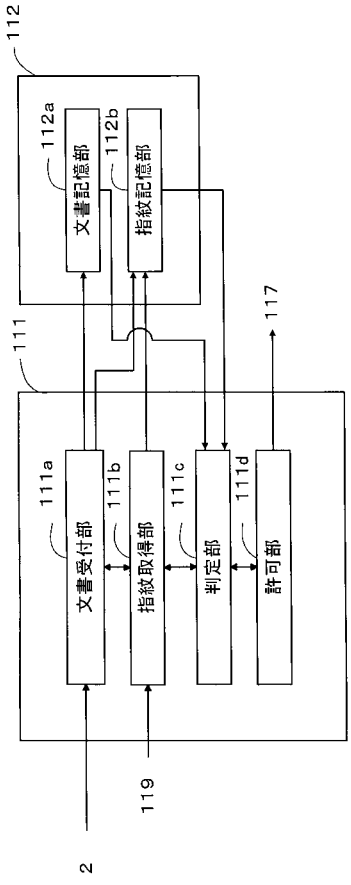
【図１】


1
111
CPU
116
読取部
112
RAM
117
記録部
113
ROM
118
操作部
114
画像メモリ
119
指紋読取部
115
コーデック
120
表示部
121
LAN−I/F
122
21 LAN
クライアント
2
クライアント
2

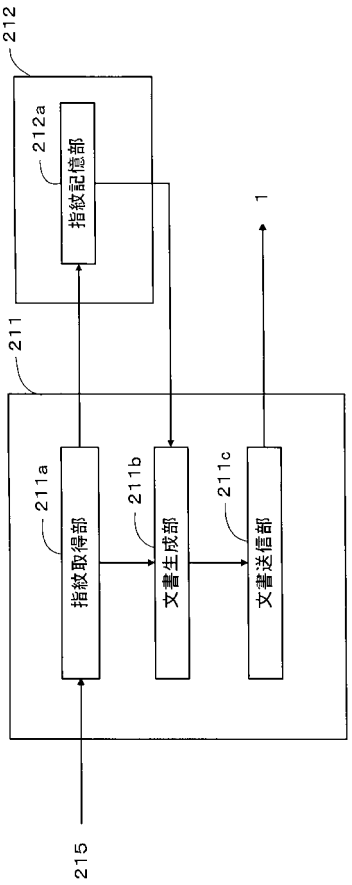
【図２】


2
211
CPU
214
操作部
212
RAM
215
指紋読取部
213
ROM
216
表示部
217
LAN−I/F
218
21 LAN
プリンタ
1
クライアント
2

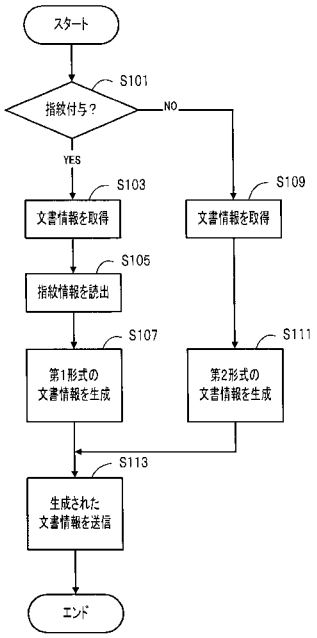
【図３】


112
112a
文書記憶部
112b
指紋記憶部
111
117
111a
文書受付部
111b
指紋取得部
111c
判定部
111d
許可部
119
2

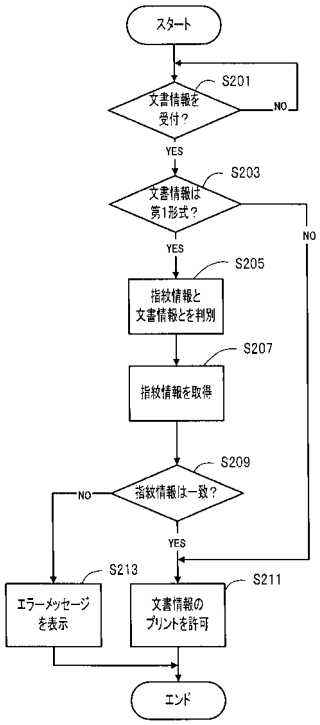
【図４】


212
212a
指紋記憶部
1
211
211a
指紋取得部
211b
文書生成部
211c
文書送信部
215

【図５】


スタート
S101
指紋付与？
NO
YES
S103
文書情報を取得
S105
指紋情報を読出
S107
第1形式の
文書情報を生成
S109
文書情報を取得
S111
第2形式の
文書情報を生成
S113
生成された
文書情報を送信
エンド

【図６】


スタート
S201
文書情報を
受付？
NO
YES
S203
文書情報は
第1形式？
NO
YES
S205
指紋情報と
文書情報とを判別
S207
指紋情報を取得
S209
指紋情報は一致？
NO
YES
S213
エラーメッセージ
を表示
S211
文書情報の
プリントを許可
エンド