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

特許第3897041号

(P3897041)

(45)発行日　平成19年3月22日(2007.3.22)　(24)登録日　平成19年1月5日(2007.1.5)

(51)Int.Cl.		F I		
G06F 3/12	(2006.01)	G06F	3/12	K
B41J 29/38	(2006.01)	B41J	29/38	Z
H04N 1/00	(2006.01)	H04N	1/00	C
		H04N	1/00	106C

請求項の数 11　(全 18 頁)

(21)出願番号　特願2004-334851 (P2004-334851)
(22)出願日　平成16年11月18日 (2004.11.18)
(65)公開番号　特開2006-146508 (P2006-146508A)
(43)公開日　平成18年6月8日 (2006.6.8)
審査請求日　平成16年11月18日 (2004.11.18)

(73)特許権者　303000372
コニカミノルタビジネステクノロジーズ株式会社
東京都千代田区丸の内一丁目６番１号
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100098316
弁理士　野田　久登

最終頁に続く

(54)【発明の名称】画像形成システムおよび画像形成装置

(57)【特許請求の範囲】

【請求項１】

端末装置、画像形成装置およびサーバ装置を備えた画像形成システムであって、

前記端末装置は、

ユーザ識別情報を入力する入力手段と、

前記ユーザ識別情報を含むプリントジョブを前記画像形成装置に送信する送信手段とを備え、

前記画像形成装置は、

前記ユーザ識別情報を含むプリントジョブを受信する受信手段と、

前記ユーザ識別情報が、自装置の使用を許可されたユーザからのものであるか否かの認証を前記サーバ装置に要求する要求手段と、

前記サーバ装置の発行する自装置の使用を許可されたユーザである旨を示す証明書を受信した場合に、前記プリントジョブに基づいて画像を形成する画像形成手段と、

前記証明書を証明書の有効期間内、保持する保持手段と、

前記受信したユーザ識別情報が、前記保持手段により証明書が保持されているユーザからのものであるか否かを判断する簡易認証手段とを備え、

前記画像形成手段は、前記簡易認証手段により証明書が存在すると判断された場合に、前記要求手段による要求を行なうことなく、画像形成処理を行ない、

前記サーバ装置は、

前記要求手段により要求のあったユーザ識別情報に基づいて、前記画像形成装置の使用

を許可されたユーザであるか否かを認証する認証手段と、
前記認証手段により前記画像形成装置の使用を許可されたユーザである旨を示す証明書を発行し、前記画像形成装置に送信する発行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２】
前記画像形成装置は、前記証明書の有効期間を設定する設定手段をさらに備えた、請求項１に記載の画像形成システム。
【請求項３】
前記端末装置は、
前記証明書の有効期間を設定する設定手段と、
前記設定手段により設定された有効期間を前記画像形成装置に通知する通知手段とをさらに備えたことを特徴とする、請求項１または２に記載の画像形成システム。
【請求項４】
前記サーバ装置は、
前記証明書の有効期間を設定する設定手段と、
前記設定手段により設定された有効期間を前記画像形成装置に通知する通知手段とをさらに備えたことを特徴とする、請求項１～３のいずれかに記載の画像形成システム。
【請求項５】
前記有効期間は、ユーザ毎に設定されることを特徴とする、請求項１～４のいずれかに記載の画像形成システム。
【請求項６】
前記画像形成装置は、有効期間の過ぎた証明書を削除する削除手段をさらに備えたことを特徴とする、請求項１～５のいずれかに記載の画像形成システム。
【請求項７】
ユーザ識別情報を含むプリントジョブを受信する受信手段と、
前記ユーザ識別情報が、自装置の使用を許可されたユーザからのものであるか否かの認証を外部認証装置に要求する要求手段と、
前記外部認証装置の発行する自装置の使用を許可されたユーザである旨を示す証明書を受信した場合に、前記プリントジョブに基づいて画像を形成する画像形成手段と、
前記証明書を証明書の有効期間内、保持する保持手段と、
前記受信したユーザ識別情報が、前記保持手段により証明書が保持されているユーザからのものであるか否かを判断する簡易認証手段とを備え、
前記画像形成手段は、前記簡易認証手段により証明書が存在すると判断された場合に、前記要求手段による要求を行なうことなく、画像形成処理を行なうことを特徴とする、画像形成装置。
【請求項８】
前記証明書の有効期間を設定する設定手段をさらに備えた、請求項７に記載の画像形成装置。
【請求項９】
前記有効期間はユーザ毎に設定されることを特徴とする、請求項７または８記載の画像形成装置。
【請求項１０】
有効期間の過ぎた証明書を削除する削除手段をさらに備えたことを特徴とする、請求項７～９のいずれかに記載の画像形成装置。
【請求項１１】
端末装置、画像形成装置およびサーバ装置を備えた画像形成システムであって、
前記端末装置は、
ユーザ識別情報を入力する入力手段と、
前記ユーザ識別情報が、前記画像形成装置の使用を許可されたユーザのユーザ識別情報であるか否かの認証を前記サーバ装置に要求する要求手段と、

前記サーバ装置の発行する前記画像形成装置の使用を許可されたユーザである旨を示す証明書をプリントジョブと共に前記画像形成装置に送信する送信手段と、
前記証明書を証明書の有効期間内、保持する保持手段と、
前記受信したユーザ識別情報が、前記保持手段により証明書が保持されているユーザからのものであるか否かを判断する簡易認証手段とを備え、
前記簡易認証手段により証明書が存在すると判断された場合に、前記要求手段による要求を行なうことなく、前記送信手段は、前記画像形成装置にプリントジョブを送信し、
前記サーバ装置は、
前記要求手段により要求のあったユーザ識別情報に基づいて、前記画像形成装置の使用を許可されたユーザであるか否かを認証する認証手段と、
前記認証手段により前記画像形成装置の使用を許可されたユーザである旨を示す証明書を発行し、前記端末装置に送信する発行手段とを備え、
前記画像形成装置は、
前記証明書を含むプリントジョブを受信する受信手段と、
前記プリントジョブに基づいて画像を形成する画像形成手段とを備え、
前記画像形成手段は、前記端末装置から前記証明書を受信した場合に、画像形成処理を行なうことを特徴とする、画像形成システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、画像形成システムおよび画像形成装置に関し、特に、認証機能を有した画像形成システムおよび画像形成装置に関する。

【背景技術】

【０００２】

画像形成装置の一種であるＭＦＰ（Multi Function Peripherals）やＰＣ（Personal Computer）をネットワークに接続し、ＰＣからＭＦＰへデータを送信し、プリントを実行させる技術が知られている。

【０００３】

近年、セキュリティの観点から、ＭＦＰの使用時にはユーザの認証が必要になってきている。一般的にＭＦＰの前でコピージョブを行なう場合は、一度ユーザ認証を行えば、認証状態を解除するまで連続して複数のコピージョブを実行することが可能である。

【０００４】

下記の特許文献１には、ＰＣよりデータをプリンタでプリントする際に、印刷することを許可されたユーザであるか否かを外部サーバに問い合わせた上で、許可されたユーザである場合は、外部サーバから受け取ったチケットをプリンタに送信することでプリントを行なう技術が開示されている。

【０００５】

特許文献２には、プリンタドライバをインストールする際に認証を行ない、認められたユーザのみにプリンタドライバのインストールを認める管理システムが開示されている。

【０００６】

特許文献３には、複数の装置を有するシステムにおいて、第１の装置での認証により装置の作動が許可されている場合において、第２の装置で同一ユーザからの認証要求を受けたときには、使用を禁止あるいは使用機能を制限する技術が開示されている。

【０００７】

特許文献４には、携帯端末のメールアドレスをサーバに予め登録しておき、携帯端末からサーバにアクセスするとき、アクセスを受けたサーバから携帯端末に鍵付きのＵＲＬをメールで送信する事項が記載されている。そのメールを受け取った携帯端末は、送られてきた鍵付きのＵＲＬにアクセスする。サーバは、鍵付きのＵＲＬを携帯端末に送信してから、携帯端末から鍵付きのＵＲＬにアクセスがあるまでの時間が所定時間内かどうかを判定する。その結果に基づき、ＵＲＬへのアクセスの許可／禁止を決定する。

【特許文献１】特開２００１－１１７７３７号公報
【特許文献２】特開２００２－１６９６７３号公報
【特許文献３】特開２００３－２８８３２３号公報
【特許文献４】特開２００３－２６４５５１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００８】
ＰＣからデータを送信して外部機器でプリントを行なう場合は、ジョブ毎に認証処理を行なうこととなる。この認証処理を外部サーバで行なう場合は、ネットワーク環境に依存した通信時間の問題や、外部サーバへの処理の集中などによって認証処理に時間を要する場合があるという問題点が存在した。たとえば、ＰＣからプリントを行なう際に、外部のサーバに認証要求を行なう場合、最悪の場合、一回の認証に数分間かかることがあり、著しく生産性を落としてしまうという問題があった。
【０００９】
また、プリンタドライバのインストール時のみ認証を行なう技術を採用すると、共有で使用しているＰＣではセキュリティが保たれているとは言えない。個人で使用しているＰＣに対しても、そのＰＣを不正に使用された場合にセキュリティ上の問題が生じることとなる。
【００１０】
本発明は、上述の問題点を解決するためになされたものであり、認証の負荷を軽減させつつ、セキュリティを保つことができる画像形成システムおよび画像形成装置を提供することを目的としている。
【課題を解決するための手段】
【００１１】
上記問題点を解決するため、この発明のある局面に従うと、端末装置、画像形成装置およびサーバ装置を備えた画像形成システムにおいて、端末装置は、ユーザ識別情報を入力する入力手段と、ユーザ識別情報を含むプリントジョブを画像形成装置に送信する送信手段とを備え、画像形成装置は、ユーザ識別情報を含むプリントジョブを受信する受信手段と、ユーザ識別情報が、自装置の使用を許可されたユーザからのものであるか否かの認証をサーバ装置に要求する要求手段と、サーバ装置の発行する自装置の使用を許可されたユーザである旨を示す証明書を受信した場合に、プリントジョブに基づいて画像を形成する画像形成手段と、証明書を証明書の有効期間内、保持する保持手段と、受信したユーザ識別情報が、保持手段により証明書が保持されているユーザからのものであるか否かを判断する簡易認証手段とを備え、画像形成手段は、簡易認証手段により証明書が存在すると判断された場合に、要求手段による要求を行なうことなく、画像形成処理を行ない、サーバ装置は、要求手段により要求のあったユーザ識別情報に基づいて、画像形成装置の使用を許可されたユーザであるか否かを認証する認証手段と、認証手段により画像形成装置の使用を許可されたユーザである旨を示す証明書を発行し、画像形成装置に送信する発行手段とを備えることを特徴とする。
【００１２】
好ましくは画像形成装置は、証明書の有効期間を設定する設定手段をさらに備える。
【００１３】
好ましくは端末装置は、証明書の有効期間を設定する設定手段と、設定手段により設定された有効期間を画像形成装置に通知する通知手段とをさらに備えたことを特徴とする。
【００１４】
好ましくはサーバ装置は、証明書の有効期間を設定する設定手段と、設定手段により設定された有効期間を画像形成装置に通知する通知手段とをさらに備えたことを特徴とする。
【００１５】
好ましくは有効期間は、ユーザ毎に設定されることを特徴とする。

【００１６】
好ましくは画像形成装置は、有効期間の過ぎた証明書を削除する削除手段をさらに備えたことを特徴とする。
【００１７】
この発明の他の局面に従うと、画像形成装置は、ユーザ識別情報を含むプリントジョブを受信する受信手段と、ユーザ識別情報が、自装置の使用を許可されたユーザからのものであるか否かの認証を外部認証装置に要求する要求手段と、外部認証装置の発行する自装置の使用を許可されたユーザである旨を示す証明書を受信した場合に、プリントジョブに基づいて画像を形成する画像形成手段と、証明書を証明書の有効期間内、保持する保持手段と、受信したユーザ識別情報が、保持手段により証明書が保持されているユーザからのものであるか否かを判断する簡易認証手段とを備え、画像形成手段は、簡易認証手段により証明書が存在すると判断された場合に、要求手段による要求を行なうことなく、画像形成処理を行なうことを特徴とする。
【００１８】
好ましくは画像形成装置は、証明書の有効期間を設定する設定手段をさらに備える。
【００１９】
好ましくは、有効期間はユーザ毎に設定されることを特徴とする。
【００２０】
好ましくは画像形成装置は、有効期間の過ぎた証明書を削除する削除手段をさらに備えたことを特徴とする。
【００２１】
この発明のさらに他の局面に従うと、端末装置、画像形成装置およびサーバ装置を備えた画像形成システムにおいて、端末装置は、ユーザ識別情報を入力する入力手段と、ユーザ識別情報が、画像形成装置の使用を許可されたユーザのユーザ識別情報であるか否かの認証をサーバ装置に要求する要求手段と、サーバ装置の発行する画像形成装置の使用を許可されたユーザである旨を示す証明書をプリントジョブと共に画像形成装置に送信する送信手段と、証明書を証明書の有効期間内、保持する保持手段と、受信したユーザ識別情報が、保持手段により証明書が保持されているユーザからのものであるか否かを判断する簡易認証手段とを備え、簡易認証手段により証明書が存在すると判断された場合に、要求手段による要求を行なうことなく、送信手段は、画像形成装置にプリントジョブを送信し、サーバ装置は、要求手段により要求のあったユーザ識別情報に基づいて、画像形成装置の使用を許可されたユーザであるか否かを認証する認証手段と、認証手段により画像形成装置の使用を許可されたユーザである旨を示す証明書を発行し、端末装置に送信する発行手段とを備え、画像形成装置は、証明書を含むプリントジョブを受信する受信手段と、プリントジョブに基づいて画像を形成する画像形成手段とを備え、画像形成手段は、端末装置から証明書を受信した場合に、画像形成処理を行なうことを特徴とする。
【発明の効果】
【００２７】
本発明によると、証明書を用いることにより、認証の負荷を軽減させつつ、セキュリティを保つことができる画像形成システムおよび画像形成装置を提供することが可能である。
【発明を実施するための最良の形態】
【００２９】
以下、本発明の実施の形態について説明する。
【００３０】
本実施の形態において、画像形成システムは、基本的にはＰＣと、画像形成装置と、認証サーバとから構成される。ＰＣからデータを画像形成装置に送り、プリントを行なう際に、外部の認証サーバにて認証処理が行なわれる。認証結果には有効期間が設けられる。有効期間内であれば、画像形成装置は外部のサーバに対する認証処理を省くことを認める。

【００３１】
このような構成により、同一のユーザがＰＣからジョブデータを送信してプリントを行なう際に、連続してプリントを行なう場合は、１つ目のジョブの認証処理の結果を採用することができ、連続した複数回の認証処理を行なわずに済む。
【００３２】
これにより、生産性を落とすことなく、かつセキュリティを保つことができる画像形成システムを提供することが可能となる。
【００３３】
［第１の実施の形態］
図１は、本発明の第１の実施の形態における画像形成システムの構成を示す図である。
【００３４】
図を参照して、画像形成システムは、ＭＦＰなどである画像形成装置１と、端末装置であるクライアントＰＣ２ａ，２ｂ，・・・と、認証サーバ６とから構成される。画像形成装置１、クライアントＰＣ２ａ，２ｂ，・・・、および認証サーバ６は、ネットワークを介して接続されている。
【００３５】
画像形成装置１は、走査した原稿画像、およびクライアントＰＣ２ａ，２ｂ，・・・から送信されたプリントデータから生成した画像の複写画像を用紙上に形成する装置である。
【００３６】
図２は、図１の画像形成装置１のハードウェア構成を示すブロック図である。
【００３７】
図を参照して、画像形成装置１は、装置全体を制御する制御部１０６と、原稿から画像データを読取るイメージリーダ部１０１と、用紙上に画像を印刷するプリンタ部１０２と、近距離の無線通信を行なったり、印刷装置をネットワークや電話回線に接続するための通信部１０３と、ジョブデータなどを記憶するための記憶部１０４と、ユーザとのインターフェースである操作パネル１０５と、消耗品の残量などを検出するセンサ部１０７とを含む。
【００３８】
図３は、図１のクライアントＰＣ１台のハードウェア構成を示すブロック図である。
【００３９】
図を参照して、クライアントＰＣは、装置全体の制御を行なうＣＰＵ６０１と、ディスプレイ６０５と、ネットワークに接続したり外部と通信を行なうためのＬＡＮ（ローカルエリアネットワーク）カード６０７（またはモデムカード）と、キーボードやマウスなどにより構成される入力装置６０９と、フレキシブルディスクドライブ６１１と、ＣＤ－ＲＯＭドライブ６１３と、ハードディスクドライブ６１５と、ＲＡＭ６１７と、ＲＯＭ６１９とを備えている。
【００４０】
フレキシブルディスクドライブ６１１により、フレキシブルディスクＦに記録されたプログラムなどのデータを読取ることが可能であり、ＣＤ－ＲＯＭドライブ６１３により、ＣＤ－ＲＯＭ６１３ａに記録されたプログラムなどのデータを読取ることが可能である。
【００４１】
図４は、第１の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。
【００４２】
ステップＳ１００において、ユーザは、画像形成装置に、ユーザ認証処理により取得する証明書の有効期間を設定する。設定の方法は、画像形成装置上の操作パネル１０５からの入力に基づいた設定でもよく、外部のＰＣなどからリモートで設定する方法でも良い。
【００４３】
また、画像形成装置内のＲＯＭに有効期間として固定値を入れておく構成でもよい。有

効期間は、画像形成装置での画像形成処理が終了するまでの時間でも良い。

【００４４】

ステップＳ１０１において、ユーザは、クライアントＰＣ上で、ユーザ名、およびユーザを識別するＩＤもしくはパスワード（ユーザ情報）を入力する。ユーザによりプリント要求が行われた際に、画像形成装置に、ユーザ情報を付加した状態でプリントデータが送信される。

【００４５】

ステップＳ１０２において、クライアントＰＣより受信したユーザ情報と、画像形成装置内に記録されている、証明書管理テーブル内の証明書のユーザ情報とを比較する。証明書管理テーブルのユーザ情報は、ステップＳ１００で画像形成装置内に設定された有効期間の間管理される。

【００４６】

ユーザ情報が一致する証明書が存在しなかった場合（Ｓ１０２でＮＯ）は、画像形成装置は、認証サーバに対して、ユーザ認証の要求を行なう。ユーザ情報が一致する証明書が存在した場合（Ｓ１０２でＹＥＳ）は、ユーザ認証処理の要求を行わずに、ステップＳ１０６で画像形成処理を開始する。

【００４７】

ステップＳ１０３において、認証サーバは、画像形成装置より受信したユーザ情報よりユーザ認証処理を行なう。認証ＯＫ／ＮＧの結果は画像形成装置に送信される。また、認証ＯＫの場合は、証明書を要求のあった画像形成装置に通知する。

【００４８】

ステップＳ１０４において、ユーザ認証処理の結果、認証ＯＫであった場合（Ｓ１０４でＹＥＳ）は、画像形成装置は、証明書を証明書管理テーブルに追加し、管理を開始する（Ｓ１０５）。認証ＮＧの場合（Ｓ１０４でＮＯ）は、画像形成装置は、クライアントＰＣに対して、ユーザ情報が誤っていることを通知する。この通知を受けて、ステップＳ１０８で、クライアントＰＣには入力されたユーザＩＤではプリントできない旨が表示される。

【００４９】

ステップＳ１０６において、画像形成装置は、プリントデータを画像データに変換するとともに、該画像データに基づいて画像イメージを形成して記録紙に複写する画像形成処理を開始する。

【００５０】

また、ステップＳ１０７において、画像形成装置は、ステップＳ１０５で証明書管理テーブルでの管理を開始した証明書が、ステップＳ１００で設定された有効期間に達した際に、該当する証明書を管理テーブルから削除する。

【００５１】

図５は、画像形成装置で管理される証明書管理テーブルの構成を示す図である。

【００５２】

図を参照して、証明書管理テーブルには、ユーザ名、パスワード（ＩＤ）、証明書ＩＤ、証明書登録時間、および証明書有効期間が証明書として含まれている。

【００５３】

一旦証明書が発行されると、所定の有効期間の間、そのユーザに対する画像形成装置の使用が認められる。従って、その期間内であれば、認証サーバへの認証要求なしにユーザは画像形成装置を使用できるため、装置の使い勝手が向上する。

【００５４】

図６は、図４のステップＳ１０３で行なわれる認証処理を示すフローチャートである。

【００５５】

図を参照して、ステップＳ１００１で、認証の対象となるユーザのユーザ名の検索が行なわれる。ステップＳ１００３で、ユーザ名が登録されていたかが判断され、ＹＥＳであればそのユーザ名に対応するパスワードが、入力されたものと一致するかが判定される。

【００５６】
ステップＳ１００５でＹＥＳであれば、ステップＳ１００７で認証結果ＯＫと判断し、ステップＳ１００３またはＳ１００５でのいずれかでＮＯであれば、ステップＳ１００９で認証結果ＮＧと判断する。
【００５７】
なお、図６と同じ処理が、証明書管理テーブル内のデータとユーザ情報とを比較する処理においても行なわれる。
【００５８】
なお、クライアントＰＣ上で、ユーザ認証処理により取得される証明書の有効期間を設定することとしてもよい。その際に、ジョブ毎に有効期間を設定可能としてもよく、一度設定した内容が全てのジョブに反映される構成でもよい。また、ユーザによる設定を認めずプリンタドライバインストール時に固定値が設定される構成でもよい。
【００５９】
クライアントＰＣ上で設定された証明書の有効期間は、ユーザ情報と共にプリントデータに付加されることで、画像形成装置に通知される。設定された有効期間の通知タイミングは、特に限定されるものではない。これらの事項は、以降の実施の形態でも同様である。
【００６０】
さらに、認証サーバ上で、ユーザ認証処理により取得される証明書の有効期間を設定することとしてもよい。その際に、ユーザ毎に有効期間の設定を可能としてもよく、画像形成装置ごとに設定する構成でも良い。
【００６１】
認証サーバ上で設定された証明書の有効期間は、ユーザ認証処理の結果とともに、画像形成装置に通知される。設定された有効期間の通知タイミングは、特に限定されるものではない。これらの事項は、以降の実施の形態でも同様である。
【００６２】
［第２の実施の形態］
第２の実施の形態における画像形成システムのハードウェア構成は、図１～３に示されるものと同じであるため、ここでの説明を繰返さない。
【００６３】
第２の実施の形態においては、証明書管理テーブルをクライアントＰＣに記録し、クライアントＰＣで証明書を管理することを特徴としている。
【００６４】
図７は、第２の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。
【００６５】
図を参照して、ステップＳ２００およびＳ２０１での処理は、図４のステップＳ１００およびＳ１０１での処理と同一であるため、ここでの説明を繰返さない。
【００６６】
ステップＳ２０２において、ユーザによりプリント要求が行われた際に、クライアントＰＣ内に記録された証明書管理テーブルに、証明書が存在するか否かが判定される。管理されている証明書が存在する場合は、ステップＳ２０１で入力したユーザ情報と一致する証明書が存在するか否かを判断する（Ｓ２０２）。ステップＳ２０１で入力したユーザ情報と一致する証明書が存在しない場合（Ｓ２０２でＮＯ）は、認証サーバに対してユーザ認証の要求を行なう。証明書が存在した場合（Ｓ２０２でＹＥＳ）は、ユーザ認証処理を行わずに画像形成装置に、証明書を付加した状態でプリントデータを送信する。
【００６７】
ステップＳ２０３において、認証サーバは、クライアントＰＣより受信したユーザ情報よりユーザ認証処理を行なう。認証ＯＫ／ＮＧの結果がクライアントＰＣに送られ、認証ＯＫの場合は、証明書を要求のあったクライアントＰＣに通知する。

【００６８】
ステップＳ２０４において、ユーザ認証処理の結果、認証ＯＫの場合（Ｓ２０４でＹＥＳ）は、クライアントＰＣは、画像形成装置に証明書を付加した状態でプリントデータを送信する。認証ＮＧの場合（Ｓ２０４でＮＯ）は、ユーザに対して入力されたユーザ情報が誤っている旨を通知する（Ｓ２０９）。
【００６９】
ステップＳ２０５において、プリントデータを受信した画像形成装置は、プリントデータに証明書が付加されているか否かを判断する。その結果、証明書が付加されているのが確認できれば（Ｓ２０５でＹＥＳ）、ステップＳ２０６で画像形成処理を開始する。また、当該証明書の有効期限をクライアントＰＣに通知する。証明書が付加されていない場合（Ｓ２０５でＮＯ）は、クライアントＰＣに対してプリントできない旨を通知する。
【００７０】
ステップＳ２０７において、クライアントＰＣは、画像形成装置から受信した証明書の有効期限を基に、証明書管理テーブルでの証明書の管理を開始する。
【００７１】
ステップＳ２０８において、クライアントＰＣは、ステップＳ２０７で証明書管理テーブルでの管理を開始した証明書が、ステップＳ２００で設定された有効期間に達した際に、該当する証明書を管理テーブルから削除する。
【００７２】
［第３の実施の形態］
第３の実施の形態における画像形成システムのハードウェア構成は、図１～３に示されるものと同じであるため、ここでの説明を繰返さない。
【００７３】
第３の実施の形態においては、証明書管理テーブルにユーザ登録がなされていない時に、認証サーバによる認証を通じてクライアントＰＣが証明書を得て、クライアントＰＣが証明書を添付してプリントデータを再送信することを特徴としている。
【００７４】
図８は、第３の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。
【００７５】
図を参照して、ステップＳ３００およびＳ３０１での処理は、図４のステップＳ１００およびＳ１０１での処理と同一であるため、ここでの説明を繰返さない。
【００７６】
ステップＳ３０２において、クライアントＰＣより受信したユーザ情報と、画像形成装置内に記録された証明書管理テーブル内の証明書のユーザ情報とを比較する。ステップＳ３００で、設定された有効期間の間管理されているユーザ情報が一致する証明書が存在しなかった場合（Ｓ３０２でＮＯ）は、クライアントＰＣに対して、証明書の要求を行なう。ユーザ情報が一致する証明書が存在した場合（Ｓ３０２でＹＥＳ）は、ステップＳ３０６において画像形成処理を開始する。画像形成装置から証明書の要求がクライアントＰＣに対してあった場合は、クライアントＰＣは、認証サーバに対してユーザ認証の要求を行なう。
【００７７】
ステップＳ３０４～Ｓ３０５、Ｓ３０８での処理は、図７のステップＳ２０３～Ｓ２０５、Ｓ２０９での処理と同様であるため、ここでの説明を繰返さない。
【００７８】
また、ステップＳ３０９、Ｓ３１５、Ｓ３０６、Ｓ３０７での処理は、図４のステップＳ１０８、Ｓ１０５、Ｓ１０６、Ｓ１０７での処理と同様であるため、ここでの説明を繰返さない。
【００７９】
［第４の実施の形態］

第４の実施の形態における画像形成システムのハードウェア構成は、図１～３に示されるものと同じであるため、ここでの説明を繰返さない。

【００８０】

第４の実施の形態においては、証明書管理テーブルをクライアントＰＣに記録し、画像形成装置が認証サーバから証明書を得て、それをクライアントＰＣに送信することを特徴としている。

【００８１】

図９は、第４の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【００８２】

図を参照して、ステップＳ４００およびＳ４０１での処理は、図４のステップＳ１００およびＳ１０１での処理と同一であるため、ここでの説明を繰返さない。

【００８３】

ステップＳ４０２において、ユーザによりプリント要求が行われた際に、クライアントＰＣ内の証明書管理テーブルに証明書が存在するか否かが判定される。管理されている証明書が存在する場合は、ステップＳ４０１で入力したユーザ情報と一致する証明書が存在するか否かを判断する。その結果、ステップＳ４０１で入力したユーザ情報と一致する証明書が存在しない場合（Ｓ４０２でＮＯ）は、画像形成装置にユーザ情報を付加した状態でプリントデータを送信する。証明書が存在した場合（Ｓ４０２でＹＥＳ）は、画像形成装置に証明書を付加した状態でプリントデータを送信する。

【００８４】

ステップＳ４０３において、クライアントＰＣより受信したプリントデータに証明書が付加されているか否かを画像形成装置で判断する。証明書が付加されていた場合（Ｓ４０３でＹＥＳ）は、ステップＳ４０６において画像形成処理を開始する。証明書が付加されていなかった場合（Ｓ４０３でＮＯ）は、プリントデータに付加されてきたユーザ情報に対して、認証サーバにユーザ認証の要求を行なう。これを受けて認証サーバは認証処理を行なう（Ｓ４０４）。

【００８５】

ステップＳ４０５において、ユーザ認証処理の結果、認証ＯＫの場合（Ｓ４０５でＹＥＳ）は、画像形成装置は、クライアントＰＣに対して、証明書と証明書の有効期間を通知する。認証ＮＧの場合（Ｓ４０５でＮＯ）は、クライアントＰＣに対して入力されたユーザ情報が誤っている旨を通知する。これを受けてクライアントＰＣは、プリント不可である旨を表示する（Ｓ４０９）。

【００８６】

ステップＳ４０６～Ｓ４０８での処理は、図７のステップＳ２０６～Ｓ２０８での処理と同じであるため、ここでの説明を繰返さない。

【００８７】

［画像形成装置の動作１］

図１０は、第１の実施の形態における画像形成システムに採用される画像形成装置の動作を示すフローチャートである。

【００８８】

図を参照して、ステップＳ５００でプリントデータを受信したかが判定される。ＹＥＳであれば、ステップＳ５０１でプリントデータと共に受信したユーザ情報が、証明書管理テーブルの証明書の中に存在するかが判定される。ここでＹＥＳであれば、ステップＳ５０６でプリントデータに基づいて画像のイメージを生成し、ステップＳ５０７で画像形成処理を行なう。

【００８９】

ステップＳ５０１でＮＯであれば、ステップＳ５０２で、外部サーバに対して認証を要求し、ステップＳ５０３でその結果を受信する。認証が成功（認証ＯＫ）であれば（Ｓ５０４でＹＥＳ）、ステップＳ５０５で認証結果と共に受信した証明書を証明書管理テーブ

ルに追加する。その後、ステップＳ５０６からの処理を行なう。

【００９０】

ステップＳ５０４でＮＯであれば、ステップＳ５０８でプリントデータを破棄する。

【００９１】

ステップＳ５００でＮＯであれば、ステップＳ５０９で、証明書管理テーブルに証明書が存在するかが判定され、ＹＥＳであれば、ステップＳ５１０で管理されている証明書は有効期限が切れているかを判定する。ここでＹＥＳであれば、ステップＳ５１１で証明書管理テーブルから該当する証明書を削除する。

【００９２】

［画像形成装置の動作２］

図１１は、第３の実施の形態における画像形成システムに採用される画像形成装置の動作を示すフローチャートである。

【００９３】

図を参照して、ステップＳ６００でプリントデータを受信したかが判定される。ＹＥＳであれば、ステップＳ６０１で受信したプリントデータに証明書が存在するかが判定される。

【００９４】

ステップＳ６０１でＹＥＳであれば、ステップＳ６０２で、受信した証明書を証明書管理テーブルに追加する。その後、ステップＳ６０３でプリントデータに基づいて画像のイメージを生成し、ステップＳ６０４で画像形成処理を行なう。

【００９５】

ステップＳ６０１でＮＯであれば、ステップＳ６０５において、受信したユーザ情報が証明書管理テーブルに存在するかが判定され、ＹＥＳであればステップＳ６０３へ移行し、ＮＯであれば、ステップＳ６０６でプリントデータを破棄した後、ステップＳ６０７で証明書が付加されたプリントデータを要求する。

【００９６】

ステップＳ６００でＮＯであれば、ステップＳ６０８で、証明書管理テーブルに証明書が存在するかが判定され、ＹＥＳであれば、ステップＳ６０９で管理されている証明書は有効期限が切れているかを判定する。ここでＹＥＳであれば、ステップＳ６１０で証明書管理テーブルから該当する証明書を削除する。

【００９７】

［第５の実施の形態］

第５の実施の形態における画像形成システムのハードウェア構成は、図１～３に示されるものと同じであるため、ここでの説明を繰返さない。

【００９８】

本実施の形態における画像形成装置では、他のジョブの画像形成処理を行っている間に受信したプリントデータはまとめて認証要求を行なうこととしている。

【００９９】

図１２は、第５の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【０１００】

ステップＳ７０１において、ユーザは、クライアントＰＣ上で、ユーザ名、およびユーザを識別するＩＤもしくはパスワード（ユーザ情報）を入力する。ユーザによりプリント要求が行われた際に、画像形成装置にユーザ情報を付加した状態で１つのジョブのプリントデータが送信される。ステップＳ７０２においても同様に、１つのジョブのプリントデータが送信される。

【０１０１】

画像形成装置は、これら複数のプリントデータを受信したものをまとめて、認証サーバにユーザ認証要求を行なう。ステップＳ７０３において、認証サーバにおいてユーザ認証処理が行なわれる。

【０１０２】
認証ＯＫ／ＮＧの結果は画像形成装置に送信される。また、認証ＯＫの場合は、証明書を要求のあった画像形成装置に送信する。
【０１０３】
ステップＳ７０４において、ユーザ認証処理の結果、認証ＯＫであった場合（Ｓ７０４でＹＥＳ）は、ステップＳ７０５において、画像形成装置は、プリントデータを画像データに変換するとともに、該画像データに基づいて画像イメージを形成して記録紙に複写する画像形成処理を開始する。
【０１０４】
認証ＮＧの場合（Ｓ７０４でＮＯ）は、画像形成装置は、クライアントＰＣに対して、ユーザ情報が誤っていることを通知する。この通知を受けて、ステップＳ７０６で、クライアントＰＣには入力されたユーザＩＤではプリントできない旨が表示される。
【０１０５】
［第６の実施の形態］
第６の実施の形態における画像形成システムのハードウェア構成は、図１～３に示されるものと同じであるため、ここでの説明を繰返さない。
【０１０６】
本実施の形態における画像形成装置では、クライアントＰＣがまとめて認証要求を行なうこととしている。
【０１０７】
図１３は、第６の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。
【０１０８】
ステップＳ８００において、ユーザにより、クライアントＰＣ上で、ユーザ名、およびユーザを識別するＩＤもしくはパスワード（ユーザ情報）が入力され、プリント要求が行われる。ステップＳ８００で要求のあったプリント要求から所定時間分のプリント要求（Ｓ８０１）に対して、まとめて認証サーバに認証要求が行なわれる。
【０１０９】
ステップＳ８０２において、認証サーバにおいてユーザ認証処理が行なわれる。
【０１１０】
認証ＯＫ／ＮＧの結果はクライアントＰＣに送信される。また、認証ＯＫの場合は、証明書を要求のあったクライアントＰＣに送信する。
【０１１１】
ステップＳ８０３において、ユーザ認証処理の結果、認証ＯＫであった場合（Ｓ８０３でＹＥＳ）は、クライアントＰＣは、証明書を添付して、ステップＳ８００、Ｓ８０１でプリントの対象とされたそれぞれのプリントデータを画像形成装置に送信する。これを受けて画像形成装置は、プリントデータを画像データに変換するとともに、該画像データに基づいて画像イメージを形成して記録紙に複写する画像形成処理を開始する（Ｓ８０４）。
【０１１２】
認証ＮＧの場合（Ｓ８０３でＮＯ）は、ステップＳ８０５で、クライアントＰＣには入力されたユーザＩＤではプリントできない旨が表示される。
【０１１３】
［画像形成装置の動作３］
図１４は、第５の実施の形態における画像形成システムに採用される画像形成装置の動作を示すフローチャートである。
【０１１４】
図を参照して、ステップＳ９００で初期化処理が行なわれる。ステップＳ９０１で、プリントデータを受信したかが判定される。ＹＥＳであれば、ステップＳ９０２で他のジョブが画像形成処理実行中であるかが判定される。

【０１１５】
ステップＳ９０２でＮＯであれば、ステップＳ９０４において、認証待ちジョブフラグを“Ｆａｌｓｅ”とする。ステップＳ９０５において、認証待ちのジョブを含めて、外部サーバにユーザ認証を要求する。ステップＳ９０６において、外部サーバから認証結果を受信する。
【０１１６】
ステップＳ９０７において、認証がＯＫであったかを判定し、ＹＥＳであれば、ステップＳ９０９において画像イメージを作成し、ステップＳ９１０で画像形成処理を行ない、ステップＳ９０１へ戻る。
【０１１７】
ステップＳ９０７においてＮＯであれば、ステップＳ９０８でプリントデータを破棄し、ステップＳ９０１へ戻る。
【０１１８】
ステップＳ９０２でＹＥＳであれば、ステップＳ９０３で認証待ちジョブフラグを“Ｔｒｕｅ”としてステップＳ９０１へ戻る。
【０１１９】
ステップＳ９０１においてＮＯであれば、ステップＳ９１１で他のジョブが画像形成処理実行中であるか判断し、ＹＥＳであればステップＳ９０１へ戻り、ＮＯであればステップＳ９１２で認証待ちフラグが“Ｔｒｕｅ”であるかが判定される。ステップＳ９１２でＹＥＳであれば、ステップＳ９０４へ進み、ＮＯであれば、ステップＳ９０１へ戻る。
【０１２０】
本実施の形態においては、他のジョブの画像形成処理が行なわれている間にプリントデータが受信されると、そのジョブを認証待ち（認証待ちフラグ“Ｔｒｕｅ”）とする。画像形成処理実行中に蓄積した認証待ちのジョブについて、画像形成処理が実行中でなくなったときにまとめて認証が行なわれる。
【０１２１】
このような処理を行なうことにより、外部のサーバに対する認証処理の負荷を軽減させることができ、かつセキュリティを保つことが可能となる。
【０１２２】
なお、１つ目のプリントデータを受信してから所定時間経過した後に外部認証サーバに認証要求を行なうようにし、所定時間が経過する間に受信したプリントデータをまとめて認証要求するようにしても良い。
【０１２３】
［実施の形態における効果］
以上のように、ＰＣからプリントを行う際に、外部のサーバにて認証処理を行う画像形成システムおよび画像形成装置において、認証結果に有効期間を設け、有効期間内であれば時間の要する外部のサーバに対する認証処理を省くことで、セキュリティを保ちつつ、画像形成の生産性を確保することが可能となる。
【０１２４】
また、複数のジョブに対してまとめて外部のサーバに認証処理を要求することでも同様に、外部のサーバに対する認証処理の負荷を軽減させることができ、セキュリティを保ちつつ、画像形成の生産性を確保することが可能となる。
【０１２５】
なお、上述の実施の形態におけるフローチャートの処理を実行するプログラムを提供することもできるし、そのプログラムをＣＤ－ＲＯＭ、フレキシブルディスク、ハードディスク、ＲＯＭ、ＲＡＭ、メモリカードなどの記録媒体に記録してユーザに提供することにしてもよい。また、プログラムはインターネットなどの通信回線を介して装置にダウンロードするようにしてもよい。
【０１２６】
また、上述の実施の形態では、画像形成装置としてＭＦＰを例示したが、本発明の画像

形成装置はＭＦＰ以外の装置であってもよい。例えば、ネットワーク機能を有したプリンタによっても画像形成装置を構成することができる。

【０１２７】

尚、今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【０１２８】

【図１】本発明の第１の実施の形態における画像形成システムの構成を示す図である。

【図２】図１の画像形成装置１のハードウェア構成を示すブロック図である。

【図３】図１のクライアントＰＣ１台のハードウェア構成を示すブロック図である。

【図４】第１の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【図５】画像形成装置で管理される証明書管理テーブルの構成を示す図である。

【図６】図４のステップＳ１０３で行なわれる認証処理を示すフローチャートである。

【図７】第２の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【図８】第３の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【図９】第４の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【図１０】第１の実施の形態における画像形成システムに採用される画像形成装置の動作を示すフローチャートである。

【図１１】第３の実施の形態における画像形成システムに採用される画像形成装置の動作を示すフローチャートである。

【図１２】第５の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

【図１３】第６の実施の形態における画像形成システムで行なわれる処理を示すフローチャートである。

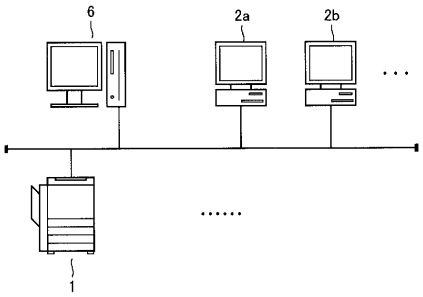
【図１４】第５の実施の形態における画像形成システムに採用される画像形成装置の動作を示すフローチャートである。

【符号の説明】

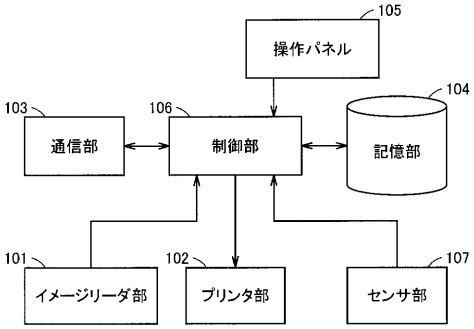
【０１２９】

１　画像形成装置、２ａ，２ｂ　クライアントＰＣ、６　認証サーバ、１０６　制御部、１０２　プリンタ部、１０３　通信部、１０４　記憶部、１０５　操作パネル、６０１　ＣＰＵ。

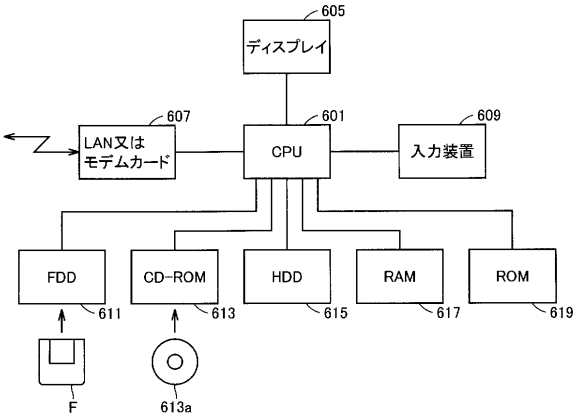
【図１】



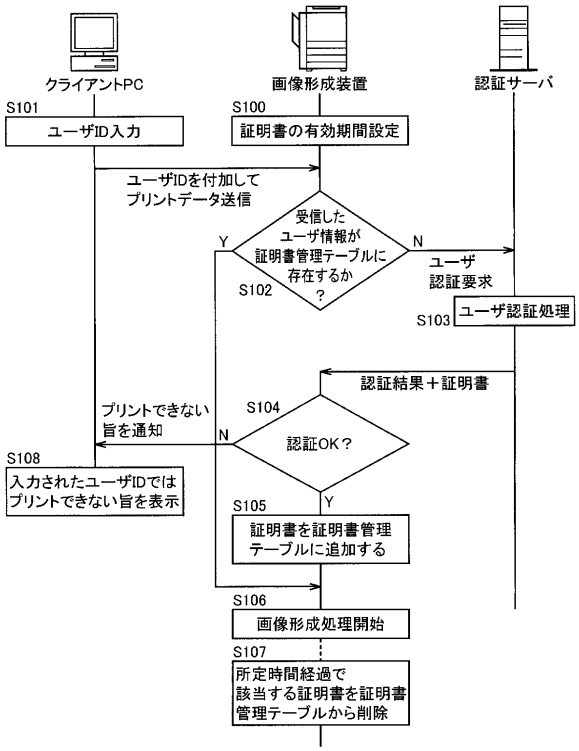
【図２】



【図３】



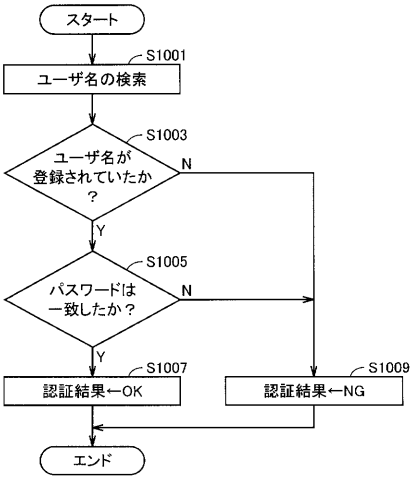
【図４】



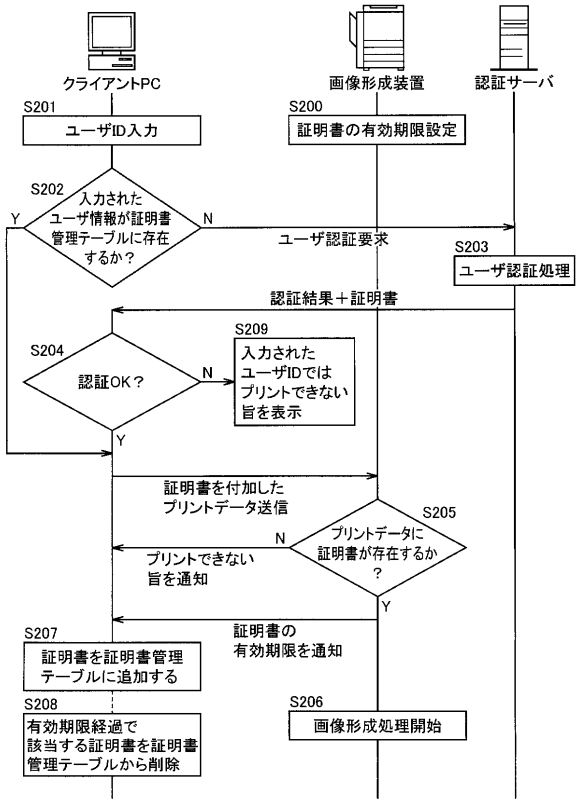
【図５】

証明書管理テーブル				
ユーザ名	パスワード	証明書ID	登録時間	有効期間
sato	12qwaszx	mfp1_1112	0403031330	3
suzuki	34erdfcv	mfp1_1113	0403031331	2

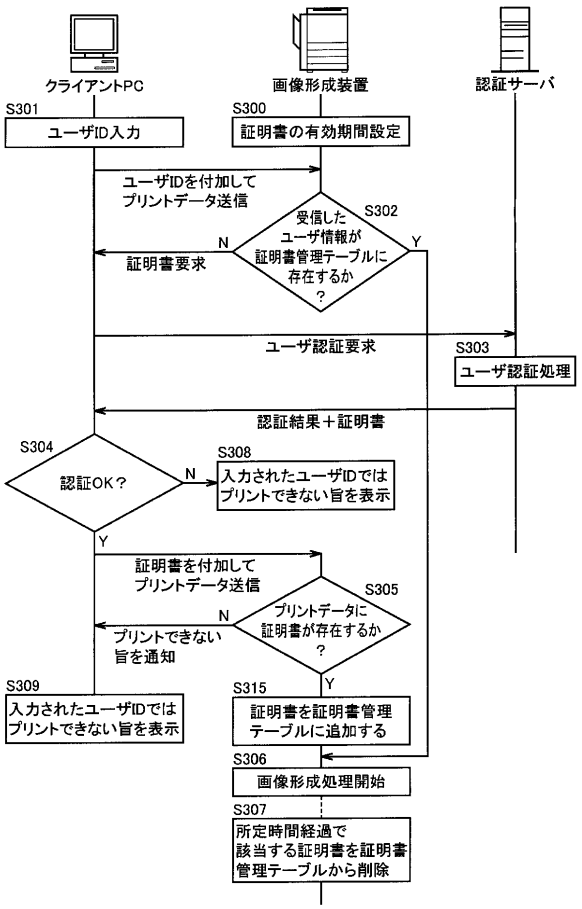
【図６】



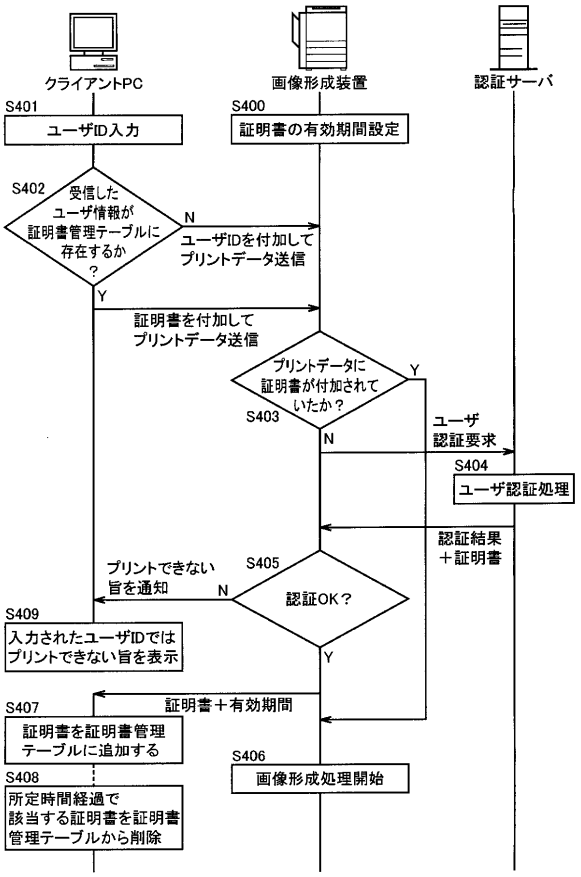
【図７】


クライアントPC
画像形成装置
認証サーバ
S201
ユーザID入力
S200
証明書の有効期限設定
S202
入力された
ユーザ情報が証明書
管理テーブルに存在
するか？
Y
N
ユーザ認証要求
S203
ユーザ認証処理
認証結果＋証明書
S204
認証OK？
N
S209
入力された
ユーザIDでは
プリントできない
旨を表示
Y
証明書を付加した
プリントデータ送信
S205
プリントデータに
証明書が存在するか
？
N
プリントできない
旨を通知
Y
証明書の
有効期限を通知
S207
証明書を証明書管理
テーブルに追加する
S208
有効期限経過で
該当する証明書を証明書
管理テーブルから削除
S206
画像形成処理開始

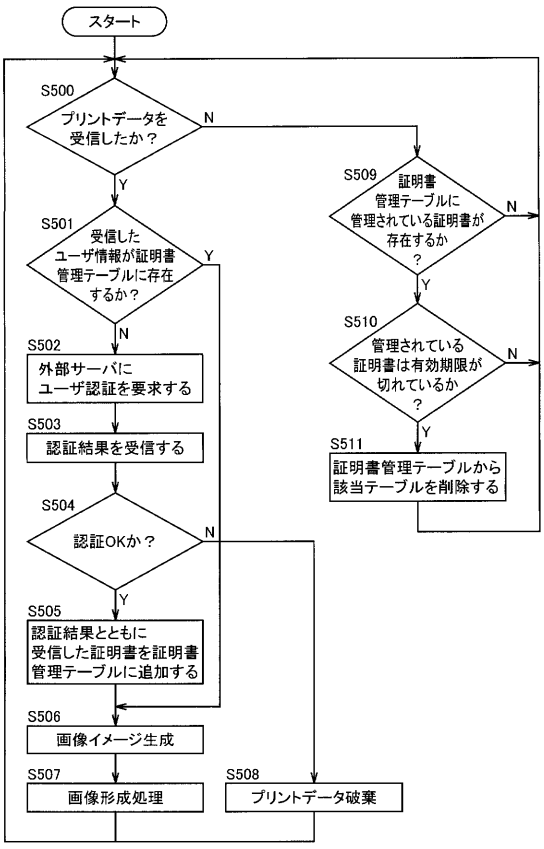
【図８】


クライアントPC
画像形成装置
認証サーバ
S301
ユーザID入力
S300
証明書の有効期間設定
ユーザIDを付加して
プリントデータ送信
S302
受信した
ユーザ情報が
証明書管理テーブルに
存在するか
？
N
Y
証明書要求
ユーザ認証要求
S303
ユーザ認証処理
認証結果＋証明書
S304
認証OK？
N
S308
入力されたユーザIDでは
プリントできない旨を表示
Y
証明書を付加して
プリントデータ送信
S305
プリントデータに
証明書が存在するか
？
N
プリントできない
旨を通知
Y
S309
入力されたユーザIDでは
プリントできない旨を表示
S315
証明書を証明書管理
テーブルに追加する
S306
画像形成処理開始
S307
所定時間経過で
該当する証明書を証明書
管理テーブルから削除

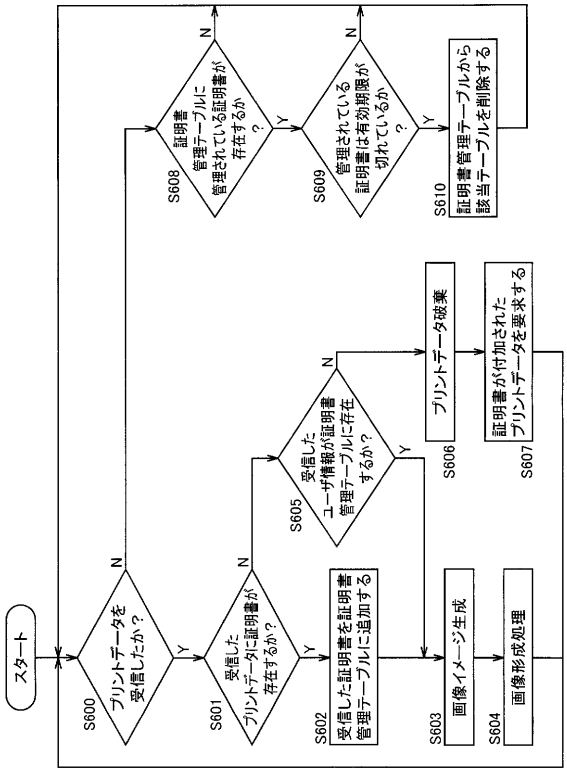
【図９】


クライアントPC
画像形成装置
認証サーバ
S401
ユーザID入力
S400
証明書の有効期間設定
S402
受信した
ユーザ情報が
証明書管理テーブルに
存在するか
？
N
ユーザIDを付加して
プリントデータ送信
Y
証明書を付加して
プリントデータ送信
プリントデータに
証明書が付加されて
いたか？
Y
S403
N
ユーザ
認証要求
S404
ユーザ認証処理
認証結果
＋証明書
プリントできない
旨を通知
S405
認証OK？
N
Y
S409
入力されたユーザIDでは
プリントできない旨を表示
S407
証明書＋有効期間
証明書を証明書管理
テーブルに追加する
S406
画像形成処理開始
S408
所定時間経過で
該当する証明書を証明書
管理テーブルから削除

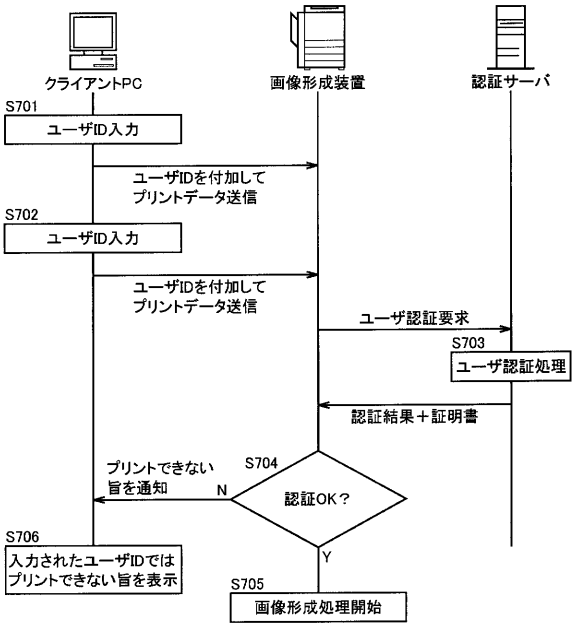
【図１０】


スタート
S500
プリントデータを
受信したか？
N
Y
S501
受信した
ユーザ情報が証明書
管理テーブルに存在
するか？
Y
N
S502
外部サーバに
ユーザ認証を要求する
S503
認証結果を受信する
S504
認証OKか？
N
Y
S505
認証結果とともに
受信した証明書を証明書
管理テーブルに追加する
S506
画像イメージ生成
S507
画像形成処理
S508
プリントデータ破棄
S509
証明書
管理テーブルに
管理されている証明書が
存在するか
？
N
Y
S510
管理されている
証明書は有効期限が
切れているか
？
N
Y
S511
証明書管理テーブルから
該当テーブルを削除する

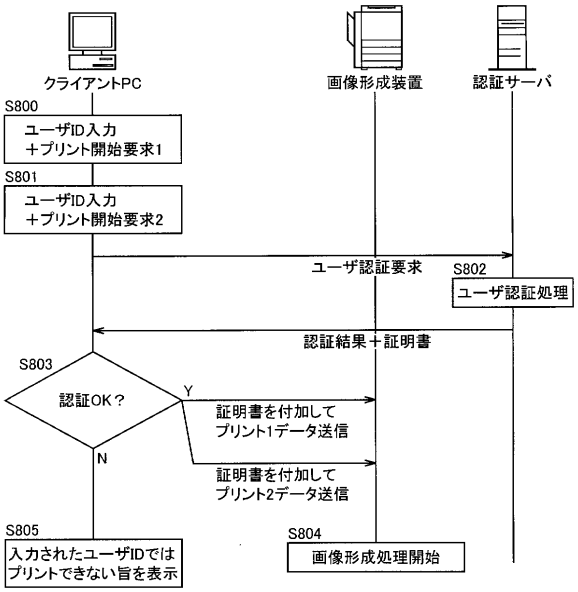
【図１１】



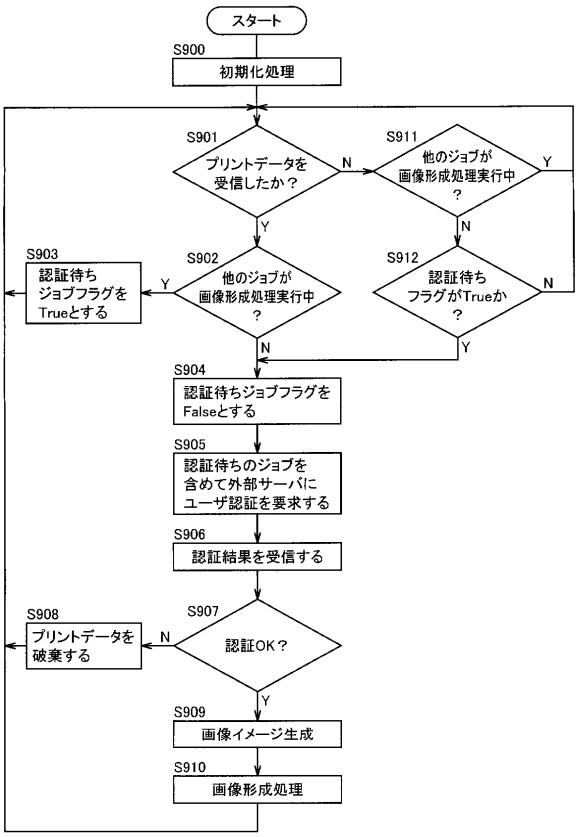
【図１２】



【図１３】



【図１４】



フロントページの続き

(74)代理人　100109162
　　弁理士　酒井　將行
(72)発明者　杉浦　博
　　東京都千代田区丸の内一丁目６番１号　コニカミノルタビジネステクノロジーズ株式会社内
(72)発明者　冨田　篤
　　東京都千代田区丸の内一丁目６番１号　コニカミノルタビジネステクノロジーズ株式会社内

審査官　田中　友章

(56)参考文献　特開２００１－３１２３７７（ＪＰ，Ａ）
　　特開２００３－２３３７２５（ＪＰ，Ａ）
　　特開２００３－３４８２８１（ＪＰ，Ａ）
　　特開２００３－２７１３５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｇ０６Ｆ　　３／１２
　　Ｂ４１Ｊ　２９／３８
　　Ｈ０４Ｎ　　１／００