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

特許第5375884号
(P5375884)

(45)発行日　平成25年12月25日(2013.12.25)　(24)登録日　平成25年10月4日(2013.10.4)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131A
H04L 9/32	(2006.01)	H04L	9/00	673A
G06F 3/12	(2006.01)	G06F	3/12	K
G06K 17/00	(2006.01)	G06K	17/00	L
H04N 1/00	(2006.01)	H04N	1/00	C

請求項の数 9　(全 25 頁)　最終頁に続く

(21)出願番号　特願2011-146318(P2011-146318)
(22)出願日　平成23年6月30日(2011.6.30)
(65)公開番号　特開2013-15887(P2013-15887A)
(43)公開日　平成25年1月24日(2013.1.24)
審査請求日　平成23年12月27日(2011.12.27)

(73)特許権者　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(73)特許権者　312000206
キヤノンＭＪアイティグループホールディングス株式会社
東京都品川区東品川２丁目４番１１号
(73)特許権者　301015956
キヤノンソフトウェア株式会社
東京都品川区東品川二丁目４番１１号
(74)代理人　100189751
弁理士　木村　友輔
(74)代理人　100188938
弁理士　榛葉　加奈子

最終頁に続く

(54)【発明の名称】認証装置、認証方法、及びコンピュータプログラム

(57)【特許請求の範囲】

【請求項１】

認証処理によって認証されたユーザによる使用を許可する画像形成装置であって、

ユーザ認証に用いるカード識別情報を取得する第１の取得手段と、

認証サーバに対して、前記第１の取得手段で取得したカード識別情報に対応するユーザの認証要求を行う認証要求手段と、

前記認証要求に応じて前記認証サーバによって行われる認証処理により認証されたユーザのユーザ識別情報と、前記カード識別情報とを含む情報をキャッシュ情報として記憶装置に記憶する記憶手段と、

前記認証サーバによる認証の結果を得られない場合に、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第１の判定手段と、

前記第１の判定手段により、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、ユーザの操作に従って入力されるユーザ識別情報を取得する第２の取得手段と、

前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第２の判定手段と、

前記第２の判定手段により、前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された場合は、前記カード識別情報に対応するユーザによる前記画像形成装置の使用を可能にすべく、前記第１の取

得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録する追加手段を備え、
前記追加手段は、前記第２の取得手段で取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていると判定された場合は、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録しないことを特徴とする画像形成装置。
【請求項２】
前記第２の判定手段により、前記第２の取得手段で取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、前記追加手段により新たに記憶装置に追加登録されるキャッシュ情報が示すユーザによる当該画像形成装置の使用を許可する使用許可手段をさらに備え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】
前記第１の判定手段により、前記カード識別情報が前記記憶装置に含まれていないと判定された後に、当該画像形成装置の使用を承認する承認ユーザとなり得る承認ユーザを、前記キャッシュ情報を用いて認証する承認ユーザ認証手段を更に備え、
前記使用許可手段は、前記承認ユーザ認証手段による認証処理が成功した後に、前記追加手段により新たに記憶装置に追加登録されるキャッシュ情報が示すユーザによる当該画像形成装置の使用を許可することを特徴とする請求項２に記載の画像形成装置。
【請求項４】
前記第１の判定手段により、前記第１の取得手段で取得したカード識別情報を含むキャッシュ情報が前記記憶装置に記憶されていないと判定された場合に、当該画像形成装置の使用を承認する承認ユーザとなり得るユーザのキャッシュ情報を表示部に表示する表示手段と、
前記表示手段により表示されたキャッシュ情報のうち、承認ユーザとするユーザのキャッシュ情報の選択を受け付ける選択受付手段と、
前記選択受付手段で受け付けた承認ユーザのカード識別情報を取得する第３の取得手段を更に備え、
前記承認ユーザ認証手段は、前記第３の取得手段で取得した承認ユーザのカード識別情報が、前記選択受付手段で選択を受けて付けたキャッシュ情報に含まれるか否かにより承認ユーザの認証処理を行うことを特徴とする請求項３に記載の画像形成装置。
【請求項５】
前記キャッシュ情報には、前記記憶手段により記憶されたキャッシュ情報であるか、または、前記追加手段により追加登録されたキャッシュ情報であるかを示す識別情報が含まれ、
前記表示手段は、前記記憶装置に記憶されているキャッシュ情報のうち、前記記憶手段により記憶されたことを示す識別情報を含むキャッシュ情報を、前記承認ユーザとなり得るユーザのキャッシュ情報として表示部に表示することを特徴とする請求項４に記載の画像形成装置。
【請求項６】
前記第１の判定手段で、前記カード識別情報を含むキャッシュ情報が前記記憶装置に記憶されていると判定される場合には、前記使用許可手段は、当該カード識別情報を含むキャッシュ情報が示すユーザによる当該画像形成装置の使用を許可することを特徴とする請求項２乃至５のいずれか１項に記載の画像形成装置。
【請求項７】
前記認証サーバから、前記カード識別情報に対応するユーザの認証に失敗した旨の結果を受信した後に、前記記憶装置に記憶されている当該カード識別情報を含むキャッシュ情報を削除する削除手段をさらに備えることを特徴とする請求項１乃至６のいずれか１項に記載の画像形成装置。
【請求項８】

認証処理によって認証されたユーザによる使用を許可する画像形成装置の制御方法であって、
前記画像形成装置が、
ユーザ認証に用いるカード識別情報を取得する第１の取得工程と、
認証サーバに対して、前記第１の取得工程で取得したカード識別情報に対応するユーザの認証要求を行う認証要求工程と、
前記認証要求に応じて前記認証サーバによって行われる認証処理により認証されたユーザのユーザ識別情報と、前記カード識別情報とを含む情報をキャッシュ情報として記憶装置に記憶する記憶工程と、
前記認証サーバによる認証の結果を得られない場合に、前記第１の取得工程で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第１の判定工程と、
前記第１の判定工程により、前記第１の取得工程で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、ユーザの操作に従って入力されるユーザ識別情報を取得する第２の取得工程と、
前記第２の取得工程により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第２の判定工程と、
前記第２の判定工程により、前記第２の取得工程により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された場合は、前記カード識別情報に対応するユーザによる前記画像形成装置の使用を可能にすべく、前記第１の取得工程で取得したカード識別情報及び第２の取得工程で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録する追加工程を実行することを特徴とし、
前記追加工程は、前記第２の取得工程で取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていると判定された場合は、前記第１の取得工程で取得したカード識別情報及び第２の取得工程で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録しないことを特徴とする画像形成装置の制御方法。
【請求項９】
認証処理によって認証されたユーザによる使用を許可する画像形成装置において実行可能なコンピュータプログラムであって、
前記画像形成装置を、
ユーザ認証に用いるカード識別情報を取得する第１の取得手段と、
認証サーバに対して、前記第１の取得手段で取得したカード識別情報に対応するユーザの認証要求を行う認証要求手段と、
前記認証要求に応じて前記認証サーバによって行われる認証処理により認証されたユーザのユーザ識別情報と、前記カード識別情報とを含む情報をキャッシュ情報として記憶装置に記憶する記憶手段と、
前記認証サーバによる認証の結果を得られない場合に、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第１の判定手段と、
前記第１の判定手段により、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、ユーザの操作に従って入力されるユーザ識別情報を取得する第２の取得手段と、
前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第２の判定手段と、
前記第２の判定手段により、前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された場合は、前記カード識別情報に対応するユーザによる前記画像形成装置の使用を可能にすべく、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録する追加手段として機能させることを特徴とし、
前記追加手段を、前記第２の取得手段で取得したユーザ識別情報が含まれるキャッシュ

情報が前記記憶装置に記憶されていると判定された場合は、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録しない手段として機能させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザが機器を使用する際のユーザ認証技術に関する。
【０００２】
近年、オフィスのセキュリティ意識の高まりとともに、情報のインプット／アウトプットを行う装置である複合機に対するセキュリティも要求されるようになってきた。
【０００３】
そこで、ユーザが所有するＩＣカードのカード情報とユーザ特定情報とが対応付けられた認証情報を認証サーバに記憶させておき、複合機を利用する際にユーザが所有するＩＣカードのカード情報を読み取り、そのカード情報を用いた認証処理が正常終了して初めて複合機を利用させることなどが行われるようになってきている。
【０００４】
しかし、通信エラーなど認証サーバとの通信が行えない等の理由により認証処理が出来ない場合には、複合機を使用することができず、作業が停止してしまうことになる。そこで、特許文献１ではキャッシュデータとして複合機にユーザ名、パスワードを保持し、認証サーバとの通信が行えない場合にも複合機に保持されたキャッシュデータを用いて、複合機にログインが可能なシステムが記載されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００９－６５２８８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、特許文献１に記載されたシステムは、キャッシュデータの有効期限が切れているユーザやキャッシュ数の上限値が超えたことによりキャッシュデータが削除されたユーザについては、認証をおこない複合機にログインすることができない。
【０００７】
このような問題に対処するために、例えば、複合機を使用するユーザのユーザ情報を取得し当該ユーザ情報が、複合機のキャッシュデータテーブルに含まれるか否かを判定し、含まれていないと判定された場合に、前記キャッシュデータテーブルに含まれるユーザから、前記複合機を使用するユーザによる複合機の使用を承認するユーザの選択を受け付け、選択された承認ユーザのユーザ情報が複合機のキャッシュデータテーブルに存在すれば、前記ユーザによる複合機の使用を許可することなども考えられる。
【０００８】
しかし、上記のような方法で複合機を使用できるようにする場合に、キャッシュデータテーブルにキャッシュデータが登録されていて、認証ができなかったＩＣカードを所有するユーザを、正常に認証可能なＩＣカードを所有するユーザ、つまりはキャッシュデータテーブルにキャッシュデータが保存されているユーザとしてログインすることを許可してしまうと、正常に認証可能なユーザに成りすまし、当該ユーザに関連付けられた印刷データの出力が不正に行われたりする危険性があり、セキュリティ上好ましくない。
【０００９】
そこで、本発明は、認証処理ができなかったＩＣカードを所有するユーザに複合機等の

機器を利用可能にする際に、認証が可能なユーザとして機器を利用させることを防止することを目的とする。

【課題を解決するための手段】

【００１０】

認証処理によって認証されたユーザによる使用を許可する画像形成装置であって、ユーザ認証に用いるカード識別情報を取得する第１の取得手段と、認証サーバに対して、前記第１の取得手段で取得したカード識別情報に対応するユーザの認証要求を行う認証要求手段と、前記認証要求に応じて前記認証サーバによって行われる認証処理により認証されたユーザのユーザ識別情報と、前記カード識別情報とを含む情報をキャッシュ情報として記憶装置に記憶する記憶手段と、前記認証サーバによる認証の結果を得られない場合に、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第１の判定手段と、前記第１の判定手段により、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、ユーザの操作に従って入力されるユーザ識別情報を取得する第２の取得手段と、前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第２の判定手段と、前記第２の判定手段により、前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された場合は、前記カード識別情報に対応するユーザによる前記画像形成装置の使用を可能にすべく、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録する追加手段を備え、前記追加手段は、前記第２の取得手段で取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていると判定された場合は、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録しないことを特徴とする。

【００１１】

また、本発明は、認証処理によって認証されたユーザによる使用を許可する画像形成装置の制御方法であって、前記画像形成装置が、ユーザ認証に用いるカード識別情報を取得する第１の取得工程と、認証サーバに対して、前記第１の取得手段で取得したカード識別情報に対応するユーザの認証要求を行う認証要求工程と、前記認証要求に応じて前記認証サーバによって行われる認証処理により認証されたユーザのユーザ識別情報と、前記カード識別情報とを含む情報をキャッシュ情報として記憶装置に記憶する記憶工程と、前記認証サーバによる認証の結果を得られない場合に、前記第１の取得工程で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第１の判定工程と、前記第１の判定工程により、前記第１の取得工程で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、ユーザの操作に従って入力されるユーザ識別情報を取得する第２の取得工程と、前記第２の取得工程により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第２の判定工程と、前記第２の判定工程により、前記第２の取得工程により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された場合は、前記カード識別情報に対応するユーザによる前記画像形成装置の使用を可能にすべく、前記第１の取得工程で取得したカード識別情報及び第２の取得工程で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録する追加工程を実行することを特徴とし、前記追加工程は、前記第２の取得工程で取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていると判定された場合は、前記第１の取得工程で取得したカード識別情報及び第２の取得工程で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録しないことを特徴とする。

【００１２】

また、本発明は、認証処理によって認証されたユーザによる使用を許可する画像形成装

置において実行可能なコンピュータプログラムであって、前記画像形成装置を、ユーザ認証に用いるカード識別情報を取得する第１の取得手段と、認証サーバに対して、前記第１の取得手段で取得したカード識別情報に対応するユーザの認証要求を行う認証要求手段と、前記認証要求に応じて前記認証サーバによって行われる認証処理により認証されたユーザのユーザ識別情報と、前記カード識別情報とを含む情報をキャッシュ情報として記憶装置に記憶する記憶手段と、前記認証サーバによる認証の結果を得られない場合に、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第１の判定手段と、前記第１の判定手段により、前記第１の取得手段で取得したカード識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された後に、ユーザの操作に従って入力されるユーザ識別情報を取得する第２の取得手段と、前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されているかを判定する第２の判定手段と、前記第２の判定手段により、前記第２の取得手段により取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていないと判定された場合は、前記カード識別情報に対応するユーザによる前記画像形成装置の使用を可能にすべく、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録する追加手段として機能させることを特徴とし、前記追加手段を、前記第２の取得手段で取得したユーザ識別情報が含まれるキャッシュ情報が前記記憶装置に記憶されていると判定された場合は、前記第１の取得手段で取得したカード識別情報及び第２の取得手段で取得したユーザ識別情報を含むキャッシュ情報を記憶装置に追加登録しない手段として機能させることを特徴とする。

【発明の効果】

【００１３】

本発明によれば、認証処理ができなかったＩＣカードを所有するユーザに複合機等の機器を利用可能にする際に、認証が可能なユーザとして機器を利用させることを防止することが可能となる。

【図面の簡単な説明】

【００１４】

【図１】本発明の実施形態におけるシステムの構成を示す図である。

【図２】本発明の実施形態のクライアントＰＣ１００、認証サーバ２００のハードウェア構成を示す図である。

【図３】本発明の実施形態の複合機３００のハードウェア構成を示す図である。

【図４】本発明の実施形態を構成するクライアントＰＣ１００、認証サーバ２００、複合機３００の機能ブロック図である。

【図５】本発明の実施形態におけるユーザ認証処理のフローを示す図である。

【図６】本発明の実施形態におけるキャッシュデータテーブル（図１１）の更新処理のフローを示す図である。

【図７】本発明の実施形態において、認証サーバ２００と複合機３００との通信がエラーとなった場合の処理のフローを示す図である。

【図８】本発明の実施形態における、キャッシュデータに登録されていないユーザのログインを承認する処理のフローを示す図である。

【図９】本発明の実施形態におけるバックアップファイルを作成する処理のフローを示す図である。

【図１０】本発明の実施形態における認証テーブルを示す図である。

【図１１】本発明の実施形態におけるキャッシュデータテーブルを示す図である。

【図１２】本発明の実施形態におけるバックアップファイルを示す図である。

【図１３】本発明の実施形態におけるキャッシュデータ管理設定ファイルを示す図である。

【図１４】本発明の実施形態においてユーザに対してＩＣカード認証を促す画面を示す図

である。
【図１５】本発明の実施形態における承認ユーザ一覧画面を示す図である。
【図１６】本発明の実施形態において承認ユーザに対してＩＣカード認証を促す画面を示す図である。
【図１７】本発明の実施形態において承認ユーザによりログインが承認されたユーザのユーザ名の入力を受け付ける画面を示す図である。
【発明を実施するための形態】
【００１５】
以下、図面を参照して、本発明の実施形態を詳細に説明する。
【００１６】
図１は本発明の複合機３００、および認証サーバ２００を用いたシステムの構成の一例を示すシステム構成図である。
【００１７】
図１に示すように、本実施形態のシステムは、１又は複数のクライアントＰＣ１００、複数の複合機（画像形成装置）３００、認証サーバ２００がローカルエリアネットワーク（ＬＡＮ）４００を介して接続され、それぞれ情報の送受信を行う構成となっている。
【００１８】
認証サーバ２００は、認証テーブル（図１０）を記憶しており、ユーザにより複合機３００のカードリーダ３１９へＩＣカードがかざされることによってなされる認証依頼に応じて、該認証テーブルを用いた認証処理を行う。
【００１９】
以下、図２を用いて、図１に示したクライアントＰＣ１００、認証サーバ２００に適用可能な情報処理装置のハードウェア構成について説明する。
【００２０】
図２は、図１に示したクライアントＰＣ１００、認証サーバ２００に適用可能な情報処理装置のハードウェア構成を示すブロック図である。
【００２１】
図２において、２０１はＣＰＵで、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０２あるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　／　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或いは各ＰＣの実行する機能を実現するために必要な後述する各種プログラム等が記憶されている。
【００２２】
２０３はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０２あるいは外部メモリ２１１からＲＡＭ２０３にロードして、該ロードしたプログラムを実行することで各種動作を実現するものである。
【００２３】
また、２０５は入力コントローラで、キーボード（ＫＢ）２０９や不図示のマウス等のポインティングデバイス等からの入力を制御する。２０６はビデオコントローラで、ＣＲＴディスプレイ（ＣＲＴ）２１０等の表示器への表示を制御する。なお、図２では、ＣＲＴ２１０と記載しているが、表示器はＣＲＴだけでなく、液晶ディスプレイ等の他の表示器であってもよい。これらは必要に応じて管理者が使用するものである。
【００２４】
２０７はメモリコントローラで、ブートプログラム，各種のアプリケーション，フォントデータ，ユーザファイル，編集ファイル，各種データ等を記憶するハードディスク（ＨＤ）や、フレキシブルディスク（ＦＤ）、或いはＰＣＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１１へのアクセスを制御する。

【００２５】
２０８は通信Ｉ／Ｆコントローラで、ネットワーク（例えば、図１に示したＬＡＮ４００）を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いた通信等が可能である。
【００２６】
なお、ＣＰＵ２０１は、例えばＲＡＭ２０３内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ＣＲＴ２１０上での表示を可能としている。また、ＣＰＵ２０１は、ＣＲＴ２１０上の不図示のマウスカーソル等でのユーザ指示を可能とする。
【００２７】
本発明を実現するための後述する各種プログラムは、外部メモリ２１１に記録されており、必要に応じてＲＡＭ２０３にロードされることによりＣＰＵ２０１によって実行されるものである。さらに、上記プログラムの実行時に用いられる定義ファイル及び各種情報テーブル等も、外部メモリ２１１に格納されており、これらについての詳細な説明も後述する。
【００２８】
次に、図３を用いて、図１に示した複合機３００のハードウェア構成について説明する。
【００２９】
図３は、図１に示した複合機３００のハードウェア構成の一例を示すブロック図である。
【００３０】
図３に示すように、コントローラユニット３００は、ＣＰＵ３０１、ＲＡＭ３０６、ＲＯＭ３０２、外部記憶装置（ハードディスクドライブ（ＨＤＤ））３０７、ネットワークインタフェース（Ｎｅｔｗｏｒｋ　Ｉ／Ｆ）３０３、モデム（Ｍｏｄｅｍ）３０４、操作部インタフェース（操作部Ｉ／Ｆ）３０５、外部インタフェース（外部Ｉ／Ｆ）３０９、イメージバスインタフェース（ＩＭＡＧＥ　ＢＵＳ　Ｉ／Ｆ）３０８、ラスタイメージプロセッサ（ＲＩＰ）３１０、プリンタインタフェース（プリンタＩ／Ｆ）３１１、スキャナインタフェース（スキャナＩ／Ｆ）３１２、画像処理部３１３等で構成される。
【００３１】
ＣＰＵ３０１は、システム全体を制御するプロセッサである。ＲＡＭ３０６は、ＣＰＵ３０１が動作するためのシステムワークメモリであり、プログラムを記録するためのプログラムメモリや、画像データを一時記憶するための画像メモリである。ＲＯＭ３０２は、システムのブートプログラムや各種制御プログラムが格納されている。
【００３２】
外部記憶装置（ハードディスクドライブＨＤＤ）３０７は、システムを制御するための各種プログラム、画像データ等を格納する。
【００３３】
操作部インタフェース（操作部Ｉ／Ｆ）３０５は、操作部（ＵＩ）３１８とのインタフェース部であり、操作部３１８に表示する画像データを操作部３１８に対して出力する。
【００３４】
また、操作部Ｉ／Ｆ３０５は、操作部３１８から本システム使用者が入力した情報（例えば、ユーザ情報等）をＣＰＵ３０１に伝える役割をする。なお、操作部３１８はタッチパネルを有する表示部を備え、該表示部に表示されたボタンを、ユーザが押下（指等でタッチ）することにより、各種指示を行うことができる。
【００３５】
ネットワークインタフェース（Ｎｅｔｗｏｒｋ　Ｉ／Ｆ）３０３は、ネットワーク（ＬＡＮ）に接続し、データの入出力を行なう。
【００３６】
モデム（ＭＯＤＥＭ）３０４は公衆回線に接続し、ＦＡＸの送受信等のデータの入出力

を行う。

【００３７】

外部インタフェース（外部Ｉ／Ｆ）３０９は、ＵＳＢ、ＩＥＥＥ１３９４、プリンタポート、ＲＳ－２３２Ｃ等の外部入力を受け付けるインタフェース部であり、本実施形態においては、認証で必要となるＩＣカード読み取り用のカードリーダ３１９が接続されている。

【００３８】

そして、ＣＰＵ３０１は、この外部Ｉ／Ｆ３０９を介してカードリーダ３１９によるＩＣカードからの情報読み取りを制御し、該ＩＣカードから読み取られた情報を取得可能である。尚、ＩＣカードに限らず、ユーザを特定することが可能な記憶媒体であればよい。この場合、記憶媒体には、ユーザを識別するための識別情報が記憶される。この識別情報は、記憶媒体の製造番号でも、ユーザが企業内で与えられるユーザコードであってもよい。以上のデバイスがシステムバス上に配置される。

【００３９】

一方、イメージバスインタフェース（ＩＭＡＧＥ　ＢＵＳ　Ｉ／Ｆ）３０８は、システムバス３１６と画像データを高速で転送する画像バス３１７とを接続し、データ構造を変換するバスブリッジである。

【００４０】

画像バス３１７は、ＰＣＩバスまたはＩＥＥＥ１３９４で構成される。画像バス３１７上には以下のデバイスが配置される。

【００４１】

ラスタイメージプロセッサ（ＲＩＰ）３１０は、例えば、ＰＤＬコード等のベクトルデータをビットマップイメージに展開する。

【００４２】

プリンタインタフェース（プリンタＩ／Ｆ）３１１は、プリンタ３１４とコントローラユニット３００を接続し、画像データの同期系／非同期系の変換を行う。

【００４３】

また、スキャナインタフェース（スキャナＩ／Ｆ）３１２は、スキャナ３１５とコントローラユニット３００を接続し、画像データの同期系／非同期系の変換を行う。

【００４４】

画像処理部３１３は、入力画像データに対し、補正、加工、編集をおこなったり、プリント出力画像データに対して、プリンタの補正、解像度変換等を行う。また、これに加えて、画像処理部３１３は、画像データの回転や、多値画像データに対してはＪＰＥＧ、２値画像データはＪＢＩＧ、ＭＭＲ、ＭＨ等の圧縮伸張処理を行う。

【００４５】

スキャナＩ／Ｆ３１２に接続されるスキャナ３１５は、原稿となる紙上の画像を照明し、ＣＣＤラインセンサで走査することで、ラスタイメージデータとして電気信号に変換する。原稿用紙は原稿フィーダのトレイにセットし、装置使用者が操作部３１８から読み取り起動指示することにより、ＣＰＵ３０１がスキャナに指示を与え、フィーダは原稿用紙を１枚ずつフィードし、原稿画像の読み取り動作を行う。

【００４６】

プリンタＩ／Ｆ３１１に接続されるプリンタ３１４は、ラスタイメージデータを用紙上の画像に変換する部分であり、その方式は感光体ドラムや感光体ベルトを用いた電子写真方式、微小ノズルアレイからインクを吐出して用紙上に直接画像を印字するインクジェット方式等があるが、どの方式でも構わない。プリント動作の起動は、ＣＰＵ３０１からの指示によって開始する。尚、プリンタ部３１４には、異なる用紙サイズまたは異なる用紙向きを選択できるように複数の給紙段を持ち、それに対応した用紙カセットがある。

【００４７】

操作部Ｉ／Ｆ３０５に接続される操作部３１８は、液晶ディスプレイ（ＬＣＤ）表示部を有する。ＬＣＤ上にはタッチパネルシートが貼られており、システムの操作画面を表示

するとともに、表示してあるキーが押されると、その位置情報を操作部Ｉ／Ｆ３０５を介してＣＰＵ３０１に伝える。また、操操作部３１８は、各種操作キーとして、例えば、スタートキー、ストップキー、ＩＤキー、リセットキー等を備える。

【００４８】

ここで、操操作部３１８のスタートキーは、原稿画像の読み取り動作を開始する時などに用いる。スタートキーの中央部には、緑と赤の２色のＬＥＤがあり、その色によってスタートキーが使える状態であるか否かを示す。また、操操作部３１８のストップキーは、稼動中の動作を止める働きをする。また、操操作部３１８のＩＤキーは、使用者のユーザＩＤを入力する時に用いる。リセットキーは、操操作部３１８からの設定を初期化する時に用いる。

【００４９】

外部Ｉ／Ｆ３０９に接続されるカードリーダ３１９は、ＣＰＵ３０１からの制御により、ＩＣカード（例えば、ソニー社のＦｅｌｉＣａ（登録商標））内に記憶されている情報を読み取り、読み取った情報を外部Ｉ／Ｆ３０９を介してＣＰＵ３０１へ通知する。

【００５０】

以上のような構成によって、複合機３００は、スキャナ３１５から読み込んだ画像データをＬＡＮ４００上に送信したり、ＬＡＮ４００から受信した印刷データをプリンタ部３１４により印刷出力することができる。

【００５１】

また、スキャナ３１５から読み込んだ画像データをモデム３０４により、公衆回線上にＦＡＸ送信したり、公衆回線からＦＡＸ受信した画像データをプリンタ部３１４により出力することできる。

【００５２】

次に、図４を用いて本発明のクライアントＰＣ１００、認証サーバ２００、複合機３００の機能について説明する。図４は、クライアントＰＣ１００、認証サーバ２００、複合機３００の機能の一例を示す機能ブロック図である。

【００５３】

＜クライアントＰＣ１００＞

クライアントＰＣ１００上のＷｅｂブラウザ１５０は、複合機３００内のＷｅｂサービス部３５５にアクセスし、キャッシュデータ管理設定ファイル（図１３）を書き換えることにより、キャッシュデータの有効期限やバックアップ処理時間などの設定を変更する機能を有する。

【００５４】

＜認証サーバ２００＞

認証サーバ２００は図４に示すとおり、データ通信部２５０、認証部２５１が機能構成として含まれている。

【００５５】

データ通信部２５０は、複合機３００の認証サーバ通信部３５１からの認証要求を受信し、認証サーバ通信部３５１へ認証結果を送信する。

【００５６】

認証サーバ２００上の認証部２５１は、複合機３００の認証サーバ通信部３５１からの認証要求を受けると、認証サーバ２００上で管理される認証テーブル（図１０）にアクセスし、認証要求されたカード番号に紐付いたユーザ名を検索し、認証要求を発信した複合機３００上の認証サーバ通信部３５１へ認証結果を返信する。

【００５７】

＜複合機３００＞

複合機３００は図４で示すように、カードリーダ制御部３５０、認証サーバ通信部３５１、認証処理部３５２、キャッシュ処理部３５３、バックアップ部３５４、Ｗｅｂサービス部３５５が機能構成として含まれている。

【００５８】

複合機３００上のカードリーダ制御部３５０は、カードリーダ３１９にかざされたカードのカード情報（製造番号等）を取得する。

【００５９】

認証サーバ通信部３５１は、カードリーダ制御部３５０が取得したカード番号を用いて認証要求を認証サーバ２００の認証部２５１へ送信し、認証サーバ２００より返される認証結果、または認証サーバ２００より発行されたアクセスキーを受信する機能を有する。

【００６０】

キャッシュ処理部３５３は、キャッシュデータテーブル（図１１）を保持しており、認証サーバ２００と通信可能な場合は、キャッシュデータテーブルに認証サーバ２００から返されたユーザ情報をキャッシュする。そして、認証サーバ２００と通信できない場合にはキャッシュデータを使用し、カードリーダ３１９にかざされたカード番号に紐付いたユーザ名を検索し認証を行う。また、キャッシュデータにないユーザ（以下、未登録ユーザ）のカードがかざされた場合、認証サーバ２００と通信しキャッシュされたユーザ（以下、承認ユーザ）の一覧（図１５）を表示する。そして、選択された承認ユーザのカードがカードリーダにかざされることにより、未登録ユーザの情報をキャッシュする。

【００６１】

なお、複合機３００の起動時には、キャッシュデータテーブルは消去されていることから、キャッシュ処理部３５３は、複合機３００の起動時に図１２に示すバックアップファイルを記憶領域から取得し、取得したバックアップファイルのユーザ情報をキャッシュデータテーブルに登録する。このとき登録フラグには“１”を設定する。バックアップファイルの作成処理については、図９に示すフローチャートを用いて後述する。

【００６２】

ちなみに、キャッシュデータテーブルには図１１で示すようにカード情報１１０１、ユーザ名１１０２、認証日時１１０３、登録フラグ１１０４、承認カード情報１１０５を保持している。カード情報１１０１には、カードリーダ３１９にかざされたカードのカード情報が登録される。また、ユーザ名１１０２には認証サーバ２００と通信可能な場合に、認証サーバ２００から取得したユーザ名が登録され、通信できない場合に未登録ユーザがキャッシュされた場合は、ユーザ名登録画面（図１７）から入力されたユーザ名がキャッシュされる。認証日時１１０３には、ユーザがログインをした際に、その都度、新しい認証日時が上書きされる。登録フラグ１１０４には、認証サーバ２００から返された認証結果が成功だった場合には“１”がキャッシュされ、認証サーバ２００と通信できず、未登録ユーザが、承認ユーザのカードをかざしてもらうことでキャッシュされた場合には“０”がキャッシュされる。認証カード情報１１０５には、未登録ユーザを登録する際（未登録ユーザをログインさせる際）に承認ユーザがかざしたカード情報がキャッシュされる。

【００６３】

バックアップ処理部３５４は、既定の時間ごとに、キャッシュデータテーブルの登録フラグ１１０４が“１”で、有効期限を経過していないユーザ情報をバックアップファイル（図１２）に登録する。

【００６４】

ＷｅｂサービスＷｅｂ部３５５はクライアントＰＣ１００のＷＥＢブラウザ１５０からの要求に応じて、該当するＷｅｂページを返す仕組みを提供する。

【００６５】

次に図５のフローチャートを用いて、ユーザ認証処理について説明する。

【００６６】

なお、本フローチャートのステップＳ５０１、ステップＳ５０３～ステップＳ５０５、ステップＳ５１１については、複合機３００のＣＰＵ３０１が所定の制御プログラムを読み出して実行することでなされる処理である。

【００６７】

また、ステップＳ５０２については、カードリーダ３１９が実行する処理である。

【００６８】

また、ステップＳ５０６～ステップＳ５１０の処理については、認証サーバ２００のＣＰＵ２０１が所定の制御プログラムを読み出して実行することでなされる処理である。

【００６９】

ステップＳ５０１では、複合機３００の認証処理部３５２は、操作部３１８に認証画面（図１４）を表示し、ユーザに対してカードリーダ３１９へＩＣカードをかざすよう促す。

【００７０】

ステップＳ５０２では、カードリーダ３１９がユーザによりかざされたＩＣカードからカード製造番号などのカード情報を取得し、複合機３００の認証処理部３５２へ当該取得したカード情報を送信する。

【００７１】

ステップＳ５０３では、複合機３００の認証処理部３５２は、ステップＳ５０２でカードリーダ３１９が取得したカード情報をカードリーダ３１９から受信する。

【００７２】

ステップＳ５０４では、複合機３００の認証サーバ通信部３５１は、ステップＳ５０３で認証処理部３５２が取得したカード情報を認証要求として認証サーバ２００のデータ通信部２５０へ送信する。

【００７３】

ステップＳ５０５では、複合機３００の認証サーバ通信部３５１は、認証サーバ２００との通信が成功したか否かを判断する。

【００７４】

認証サーバ２００への通信に失敗した場合（ステップＳ５０５：ＹＥＳ）は、処理を図７のフローチャートで示す処理へ移行する。

【００７５】

認証サーバ２００への通信が成功した場合（ステップＳ５０５：ＮＯ）は、処理をステップＳ５０６へ移行する。

【００７６】

ステップＳ５０６では、認証サーバ２００のデータ通信部２５０は、ステップＳ５０５で複合機３００の認証サーバ通信部３５１から送信されたカード情報を含む認証要求を受信する。

【００７７】

ステップＳ５０７では、認証サーバ２００の認証部２５１は、ステップＳ５０５で受け取ったカード情報の認証結果を判定する。具体的には、受信したカード情報が図１０に示す認証テーブルに存在するか否かを判定し、存在すれば認証成功として処理をステップＳ５０８に移行する（ステップＳ５０７：ＹＥＳ）。

【００７８】

他方、受信したカード情報が認証テーブル（図１０）に存在しない場合は（ステップＳ５０７：ＮＯ）、認証失敗として処理をステップＳ５１０に移行する。

【００７９】

ステップＳ５１０では、認証サーバ２００のデータ通信部２５０は、複合機３００の認証処理部３５２に認証が失敗した旨の結果を送信する。

【００８０】

ステップＳ５０８では、認証サーバ２００の認証部２５１は、認証に成功したユーザのユーザ情報（カード情報１００１、ユーザ名１００２、パスワード１００３、日時１００４）を認証テーブル（図１０）から取得する。

【００８１】

ステップＳ５０９では、認証サーバ２００のデータ通信部２５０は、複合機３００の認証処理部３５２に認証が成功した旨の結果と、認証テーブル（図１０）から取得したユーザ情報とを送信する。

【００８２】

ステップＳ５１１では、複合機３００の認証処理部３５２は、ステップＳ５０９またはステップＳ５１０で認証サーバ２００のデータ通信部２５０から送信された認証結果を受信する。

【００８３】

認証結果を受信すると、処理を図６のフローチャートで示す処理へ移行する。

【００８４】

次に図６を用いて、複合機３００に記憶されたキャッシュデータテーブル（図１１）の更新処理について説明する。

【００８５】

なお、図６のフローチャートで示す処理は、複合機３００のＣＰＵ３０１が所定の制御プログラムを読み出して実行することでなされる処理である。

【００８６】

ステップＳ６０１では、複合機３００の認証処理部３５２は、認証サーバ２００のデータ通信部２５０から送信された認証結果が、認証に成功した旨の結果なのか、認証に失敗した旨の結果なのかを判断する。

【００８７】

認証に失敗した旨の結果である場合（ステップＳ６０１：ＮＯ）、処理をステップＳ６０２に移行する。

【００８８】

認証に成功した旨の結果である場合（ステップＳ６０１：ＹＥＳ）、処理をステップＳ６０５に移行する。

【００８９】

ステップＳ６０２では、複合機３００のキャッシュ処理部３５３は、図５のステップＳ５０３で取得したカード情報がキャッシュデータテーブル（図１１）に存在するか否かを判断する。

【００９０】

存在すると判断された場合は（ステップＳ６０２：ＹＥＳ）処理をステップＳ６０３に移行し、存在しないと判断された場合は（ステップＳ６０２：ＮＯ）処理をステップＳ６０４に移行する。

【００９１】

ステップＳ６０３では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）に残っている当該ユーザの情報を削除する。

【００９２】

このステップＳ６０３の削除処理により、認証サーバ２００にユーザ情報が存在しないユーザの情報がキャッシュデータテーブル（図１１）に存在しているという状態を回避することが可能となる。

【００９３】

ステップＳ６０４では、認証に失敗した旨を通知するエラー画面（不図示）を、操作部３１８に表示する。

【００９４】

ステップＳ６０５では、複合機３００のキャッシュ処理部３５３は、認証を行った日時を取得する。

【００９５】

ステップＳ６０６では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）にステップＳ５０３で取得したカード情報が登録されているか否かを確認する。

【００９６】

登録されていると判断された場合は（ステップＳ６０６：ＹＥＳ）、処理をステップＳ６０７に移行する。登録されていないと判断された場合は（ステップＳ６０６：ＮＯ）、処理をステップＳ６０８に移行する。

【００９７】
ステップＳ６０７では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）の当該ユーザ（ステップＳ５０３で取得したカード情報に対応するユーザ）のユーザ情報を、ステップＳ５１１で認証サーバ２００から受信したユーザ情報により上書きする。なお、上書きする具体的なデータは、ステップＳ５１１で受信したユーザ名１１０２、ステップＳ６０５で取得した認証日時１１０３であり、また登録フラグ１１０４には“１”を設定し、承認カード情報１１０５には“ＮＵＬＬ”を設定する。
【００９８】
ステップＳ６０７でキャッシュデータテーブル（図１１）の更新処理が行われると、処理をステップＳ６１１に移行する。
【００９９】
ステップＳ６０８では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）のデータ数が上限値に達しているか否かを判断する。上限値に達している場合（ステップＳ６０８：ＹＥＳ）は処理をステップＳ６０９に移行し、上限値に達していない場合（ステップＳ６０８：ＮＯ）は処理をステップＳ６１０に移行する。
【０１００】
なお、キャッシュのデータ数が上限値に達しているか否かについては、キャッシュデータ管理設定ファイル（図１３）のキャッシュ上限数１３０４に従い判断する。
【０１０１】
ステップＳ６０９では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブルに登録されているユーザ情報のうち、認証日時１１０３が最も古いユーザ情報を削除する。
【０１０２】
ステップＳ６１０では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）にステップＳ５０３で取得したカード情報１１０１、ステップＳ５１１で受信したユーザ名１１０２、ステップＳ６０５で取得した認証日時１１０３を設定し、登録フラグには“１”を設定する。承認カード情報１１０５には“ＮＵＬＬ”を設定する。
【０１０３】
ステップＳ６１０でキャッシュデータテーブル（図１１）の更新処理が行われると、処理をステップＳ６１１に移行する。
【０１０４】
ステップＳ６１１では、複合機３００の認証処理部３５２は、ステップＳ５１１で受信したユーザ情報にてログインを受け付ける。
【０１０５】
次に、図７を用いて、ステップＳ５０５で通信がエラーであると判断された場合の処理について説明する
【０１０６】
なお、図７のフローチャートで示す処理は、複合機３００のＣＰＵ３０１が所定の制御プログラムを読み出して実行することでなされる処理である。
【０１０７】
ステップＳ７０１では、複合機３００のキャッシュ処理部３５３は、ＨＤＤ３０７などの記憶領域に記憶されたキャッシュデータテーブル（図１１）を取得する。
【０１０８】
ステップＳ７０２では、複合機３００のキャッシュ処理部３５３は、ステップＳ７０１で取得したキャッシュデータテーブルに、ステップＳ５０３で取得したカード情報が登録されているか否かを判断する。
【０１０９】
登録されていると判断された場合は（ステップＳ７０２：ＹＥＳ）、処理をステップＳ７０３に移行し、登録されていないと判断された場合は（ステップＳ７０２：ＮＯ）。処

理をステップＳ７０８に移行する。

【０１１０】

ステップＳ７０３では、複合機３００のキャッシュ処理部３５３は、ステップＳ５０３で取得したカード情報と一致するカード情報を有するユーザ情報が有効期限内か否かを確認する。具体的には、図１３に示すキャッシュデータ管理設定ファイルのフラグ”０”ユーザ有効期限１３０１またはフラグ“１”ユーザ有効期限１３０２に設定された値と、キャッシュデータテーブルの認証日時１１０３の値とを用いて判断する。

【０１１１】

ユーザ情報の登録フラグが“０”のユーザについては、フラグ０ユーザ有効期限１３０１に設定された日数をユーザ情報の認証日時１１０３に加算することで算出された日時が有効期限となる。

【０１１２】

ユーザ情報の登録フラグが“１”のユーザについては、フラグ１ユーザ有効期限１３０２に設定された日数をユーザ情報の認証日時１１０３に加算することで算出された日時が有効期限となる。

【０１１３】

このようにして求められた有効期限を過ぎていないと判断された場合（ステップＳ７０３：ＹＥＳ）は、処理をステップＳ７０６に移行し、有効期限が過ぎていると判断された場合（ステップＳ７０３：ＮＯ）は、処理をステップＳ７０４に移行する。

【０１１４】

ステップＳ７０４では、複合機３００のキャッシュ処理部３５３は、ステップＳ７０３で有効期限が過ぎていると判断されたユーザ情報をキャッシュデータテーブルから削除する。

【０１１５】

ステップＳ７０５では、複合機３００は、認証に失敗した旨を示すエラー画面（不図示）を表示し、処理を図８のフローチャートで示す処理へ移行する。

【０１１６】

ステップＳ７０６では、複合機３００のキャッシュ処理部３５３は、現在日時を取得する。そして、ステップＳ７０７で、複合機３００のキャッシュ処理部３５３は、ステップＳ７０６で取得した現在日時を、ステップＳ５０３で取得したカード情報に対応するユーザのユーザ情報に上書きする。

【０１１７】

そして、処理を図６のステップＳ６１１に移行し、ステップＳ７０７で上書きしたユーザ情報を用いてログインする。

【０１１８】

ステップＳ７０８では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）のデータのうち、登録フラグが“１”であり、有効期限内のユーザ情報を取得する。有効期限内か否かの判断については、ステップＳ７０３での判断と同様である。

【０１１９】

すなわち、承認ユーザとなり得るユーザのユーザ情報をキャッシュデータテーブルから取得する。なお、登録フラグが“１”であるユーザは、認証サーバ２００の認証テーブルを用いた認証処理に成功したユーザである。

【０１２０】

ステップＳ７０９では、複合機３００のキャッシュ処理部３５３は、ステップＳ７０８で取得したユーザ情報の一覧を操作部３１８に表示する（一覧表示画面の一例として図１５）。

【０１２１】

ステップＳ７１０では、複合機３００のキャッシュ処理部３５３は、ステップＳ７０９で表示した承認ユーザ情報一覧から、承認ユーザの選択を受け付ける。

【０１２２】
ステップＳ７１１では、複合機３００のキャッシュ承認部３５３は、ユーザから承認ユーザが選択され、一覧画面上の認証ボタン１５０２が押下されたか否かを判断する。
【０１２３】
認証ボタン１５０２が押下されたと判断した場合（ステップＳ７１１：ＹＥＳ）は、処理を図８のフローチャートのステップＳ８０１へ移行する。
【０１２４】
認証ボタンが押下されていない場合（ステップＳ７１１：ＮＯ）は、処理をステップＳ７１１へ移行し、戻るボタン１５０１が押下されたか否かを判断する。戻るボタン１５０１が押下された場合（ステップＳ７１２：ＹＥＳ）は、処理を図５のステップＳ５０１へ移行し、再度ユーザ認証画面（図１４）を表示する。認証ボタン１５０２、戻るボタン１５０１のどちらも押下されていない場合（ステップＳ７１２：ＮＯ）は、引き続き待機状態を維持する。なお、一定時間、ユーザからの操作が行われない場合は、処理を図５のステップＳ５０１に移行するよう構成しても良い。
【０１２５】
次に、図８に示すフローチャートを用いて、承認ユーザのカードがカードリーダ３１９にかざされることでキャッシュデータテーブルにユーザ情報が登録されていないユーザ（未登録ユーザ）のログインを承認する処理について説明する
【０１２６】
なお、図８のフローチャートのステップＳ８０１、ステップＳ８０２、ステップＳ８０４～ステップＳ８１２に示す処理は、複合機３００のＣＰＵ３０１が所定の制御プログラムを読み出して実行することでなされる処理である。
【０１２７】
また、ステップＳ８０３は、カードリーダ３１９が実行する処理である。
【０１２８】
ステップＳ８０１では、複合機３００のキャッシュ処理部３５３は、ステップＳ７１０でユーザにより選択された承認ユーザの認証を促すための承認ユーザ認証ダイアログ（図１６）を操作部３１８に表示する。
【０１２９】
ステップＳ８０２では、複合機３００のキャッシュ処理部３５３は、ユーザにより、承認ユーザ認証ダイアログの戻るボタン１６０１が押下されたか否かを判断する。戻るボタン１６０１がユーザにより押下された場合は、処理を図７のステップＳ７０９に移行し、再度承認ユーザ一覧画面（図１５）を表示し、承認ユーザの選択を受け付ける。
【０１３０】
戻るボタン１６０１が押下されない場合は（ステップＳ８０２：ＮＯ）、処理をステップＳ８０３に移行する。
【０１３１】
ステップＳ８０３では、カードリーダ３１９は、ステップＳ７１０で選択された承認ユーザのＩＣカードを検知し、検知したＩＣカードのカード情報を取得する。
【０１３２】
ステップＳ８０４では、複合機３００のキャッシュ処理部３５３は、ステップＳ８０３でカードリーダ３１９が取得したカード情報を受け取る。
【０１３３】
ステップＳ８０５では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブルに保存されている、ステップＳ７１０で選択された承認ユーザのカード情報と、ステップＳ８０４でカードリーダ３１９から受け取ったカード情報とが一致するかを確認する。
【０１３４】
一致する場合（ステップＳ８０４：ＹＥＳ）は、処理をステップＳ８０７に移行し、一致しない場合（ステップＳ８０５：ＮＯ）は、処理をステップＳ８０６に移行する。

【０１３５】
ステップＳ８０６では、複合機３００のキャッシュ処理部３５３は、認証に失敗した旨を示す認証エラー画面（不図示）を表示する。そして、処理をステップＳ７０９に移行し、再度承認ユーザ一覧画面を表示し、承認ユーザの選択を受け付ける。
【０１３６】
ステップＳ８０７では、複合機３００のキャッシュ処理部３５３は、ユーザ名の登録を受け付けるユーザ名登録画面（図１７）を表示する。
【０１３７】
ステップＳ８０８では、複合機３００のキャッシュ処理部３５３は、ユーザからのユーザ名の入力を受け付ける。なお、ステップＳ８０８の処理は、ログインを承認されるユーザのユーザ情報（ユーザ名）をキャッシュデータテーブルに設定するための処理である。
【０１３８】
ステップＳ８０９では、複合機３００のキャッシュ処理部３５３は、ユーザ名登録画面上のＯＫボタンがユーザにより押下されたか否かを判断する。
【０１３９】
押下されたと判断した場合（ステップＳ８０９：ＹＥＳ）は、処理をステップＳ８１１に移行し、押下されていない場合（ステップＳ８０９：ＮＯ）は処理をステップＳ８１０へ移行する。
【０１４０】
ステップＳ８１０では、ユーザによりキャンセルボタンが押下されたか否かを判断する。キャンセルボタンが押下された場合は、処理をステップＳ５０１に移行する。
【０１４１】
ステップＳ８１１では、ステップＳ８０８で入力を受け付けたユーザ名がキャッシュデータテーブルに登録されているいずれかのキャッシュデータに設定されているかを判定する。ＣＰＵ２０１がこの判定処理でＮＯと判定した場合には、処理をステップＳ８１２に進め、複合機３００のキャッシュ処理部３５３は、現在日時（認証日時）を取得する。

【０１４２】
ステップＳ８１３では、複合機３００のキャッシュ処理部３５３は、キャッシュデータテーブル（図１１）にステップＳ５０３で取得したカード情報、ステップＳ８０８で受け付けたユーザ名、ステップＳ８１１で取得した現在日時を設定し、登録フラグに“０”を設定する。そして、ステップＳ８０３で取得した承認ユーザのカード情報を承認カード情報１１０５に設定する。
【０１４３】
そして、複合機３００のキャッシュ処理部３５３は、処理をステップＳ６１１に移行し、ステップＳ８１３で設定した情報を用いて、ログインを行う。
【０１４４】
本発明では、ユーザから入力を受け付けたユーザ名が既にキャッシュデータテーブルに含まれるいずれかのキャッシュデータのユーザ名に設定されていないと判定した場合に、認証処理が出来なかったＩＣカードの情報と入力されたユーザ名とを対応付けられたキャッシュデータを新たにキャッシュデータテーブルに登録する。これにより、キャッシュデータを用いた認証が可能なＩＣカード情報と対応付けられているユーザ名を、認証処理が出来なかったＩＣカードの情報と対応付けて登録することを防ぐことが可能となり、不正な成りすましを好適に防止することが可能となる。
【０１４５】
なお、本実施形態においては、承認ユーザのカードを検知し、その後ログインの承認を受けるユーザのユーザ情報の入力を受け付けているが、処理の順序としては、ログインの承認を受けるユーザのユーザ情報の入力を受け付けた後に承認ユーザのカードを検知するという構成であっても良い。
【０１４６】

次に、図９を用いて、バックアップファイル（図１２）の作成処理について説明する。なお、図９のフローチャートに示す処理は、複合機３００内のバックアップ部３５４の機能により、ＣＰＵ３０１が所定の制御プログラムを読み出して実行することでなされる処理である。

【０１４７】

ステップＳ９０１は、複合機３００のバックアップ部３５４は、バックアップ処理時刻が到来したか否かを判断する。バックアップ処理時刻が到来していると判断された場合（ステップＳ９０１：ＹＥＳ）は、処理をステップＳ９０２へ移行する。バックアップ処理時刻が到来していないと判断された場合（ステップＳ９０１：ＮＯ）は、本フローチャートの処理を終了する。

【０１４８】

バックアップ処理時刻については、あらかじめ記憶されたキャッシュデータ管理設定ファイルのバックアップ処理時刻１３０３に従う。

【０１４９】

ステップＳ９０２では、複合機３００のバックアップ部３５４は、キャッシュデータテーブル（図１１）を取得する。

【０１５０】

ステップＳ９０３では、複合機３００のバックアップ部３５４は、キャッシュデータテーブルに設定されているユーザ情報を１件読み取る。

【０１５１】

ステップＳ９０４では、複合機３００のバックアップ部３５４は、ステップＳ９０３でユーザ情報を読み取れたか否かを判断する。

【０１５２】

読み取れた場合（ステップＳ９０４：ＹＥＳ）は、処理をステップＳ９０５に移行し、読み取れなかった場合（ステップＳ９０４：ＮＯ）は、本フローチャートの処理を終了する。

【０１５３】

ステップＳ９０５では、複合機３００のバックアップ部３５４は、ステップＳ９０３で読み取ったユーザ情報の登録フラグ１１０４が“１”であるか否かを判断する。登録フラグ１１０４が“１”であった場合（ステップＳ９０５：ＹＥＳ）は、処理をステップＳ９０６に移行し、登録フラグ１１０４が“１”ではない場合（ステップＳ９０５：ＮＯ）は、本フローチャートの処理を終了する。

【０１５４】

なお、登録フラグが“１”であるユーザとは、認証サーバ２００と通信を行い、認証テーブル（図１０）を用いた認証処理に成功したユーザである。

【０１５５】

ステップＳ９０６では、複合機３００のバックアップ部３５４は、ユーザ情報の有効期限が期限内か否かを判断する。なお、具体的な判断方法については、ステップＳ７０３の処理と同様である。

【０１５６】

有効期限内であると判断された場合（ステップＳ９０６：ＹＥＳ）は、処理をステップＳ９０７に移行し、有効期限を過ぎていると判断された場合（ステップＳ９０６：ＮＯ）は、本フローチャートの処理を終了する。

【０１５７】

ステップＳ９０７では、複合機３００のバックアップ部３５４は、登録フラグ１１０４が“１”であり、有効期限内のユーザ情報（カード情報、ユーザ名、認証日時）をバックアップファイル（図１２）に保存する。

【０１５８】

なお、本フローチャートのステップＳ９０３～ステップＳ９０７の処理については、キャッシュデータテーブルに保存されているユーザ情報の全てについて読み込み処理が実行

されるまで繰り返される。

【０１５９】

本フローチャートの処理により登録フラグが“１”であるユーザ（承認ユーザとなり得るユーザ）のユーザ情報がバックアップされることで、複合機３００の起動時に当該バックアップファイルがキャッシュデータテーブルのデータとして用いることが可能となり、キャッシュデータテーブルが消去されている複合機３００の起動時等であっても承認ユーザによるログインの承認が可能となる。

【０１６０】

すなわち、複合機３００の起動時などキャッシュデータテーブルが消去されている状態であっても、バックアップファイルを用いることで、キャッシュデータが複合機に保持されていないユーザでも、承認ユーザによるログインの承認を得ることができるようになる。

【０１６１】

以上の処理により、キャッシュデータが複合機に保持されていないユーザでも、キャッシュデータが複合機に保持されているユーザから承認を得ることにより、複合機にログインすることが可能となる

【０１６２】

なお、上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【０１６３】

本発明は、例えば、システム、装置、方法、プログラムもしくは記録媒体等としての実施態様を採ることが可能であり、具体的には、複数の機器から構成されるシステムに適用しても良いし、また、ひとつの機器からなる装置に適用しても良い。

【０１６４】

また、本発明におけるプログラムは、図５～図９の処理方法をコンピュータが実行可能なプログラムであり、本発明の記憶媒体には、図５～図９の処理方法をコンピュータで実行可能なプログラムが記憶されている。なお、本発明におけるプログラムは図５～図９の各装置の処理方法ごとのプログラムであってもよい。

【０１６５】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、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）が記録媒体に格納されたプログラムを読み出し、実行することによっても本発明の目的が達成されることは言うまでもない。

【０１６６】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記録した記録媒体は本発明を構成することになる。

【０１６７】

プログラムを供給するための記録媒体としては、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、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク等を用いることが出来る。

【０１６８】

また、コンピュータが読み出したプログラム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）等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。

【０１６９】

さらに、記録媒体から読み出されたプログラムが、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等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。

【０１７０】

また、本発明は、複数の機器から構成されるシステムに適用しても、ひとつの機器から成る装置に適用しても良い。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１７１】

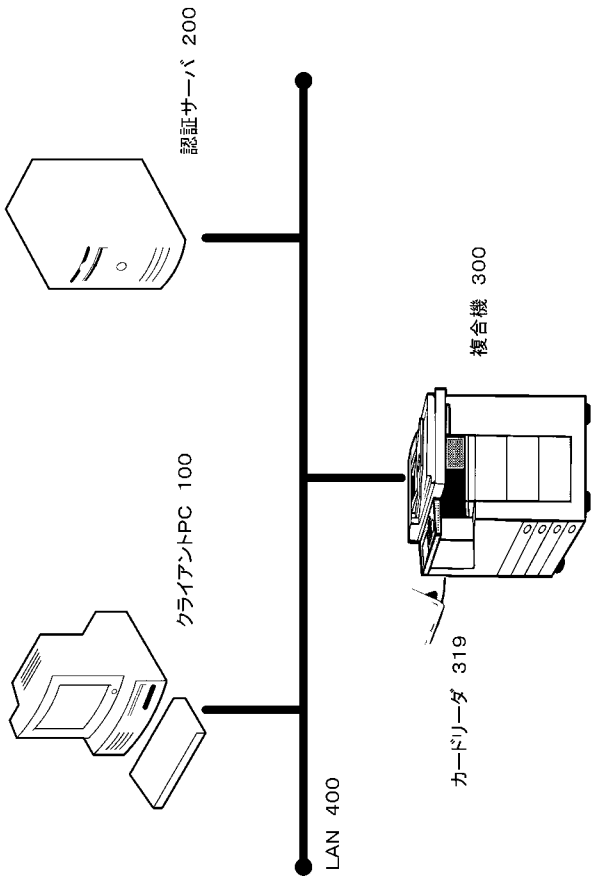
さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

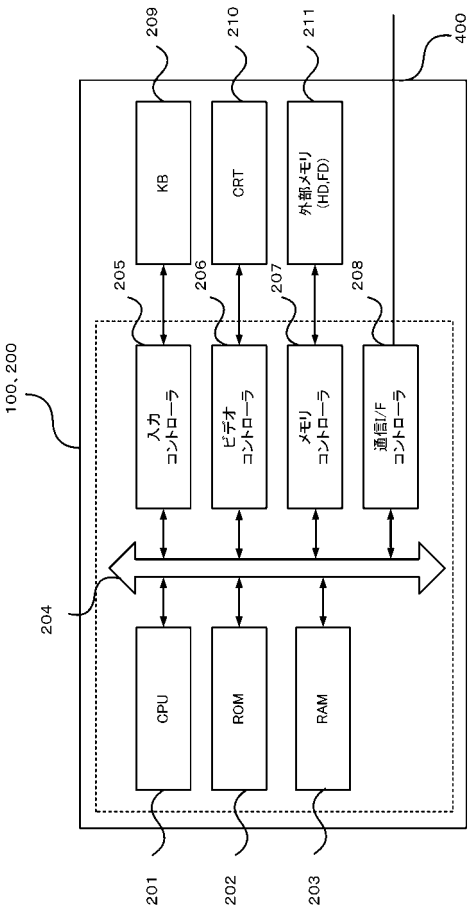
【０１７２】

１００　クライアントＰＣ
２００　認証サーバ
３００　複合機
３１９　カードリーダ
４００　ＬＡＮ

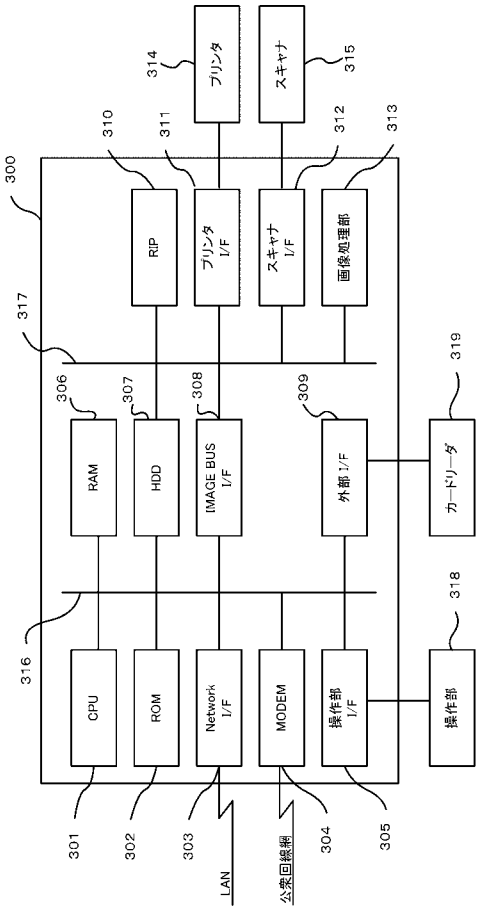
【図１】



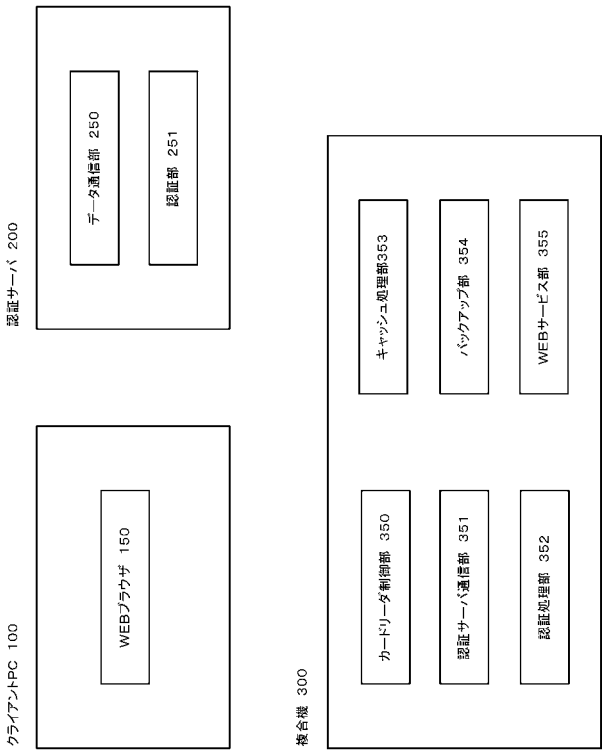
【図２】



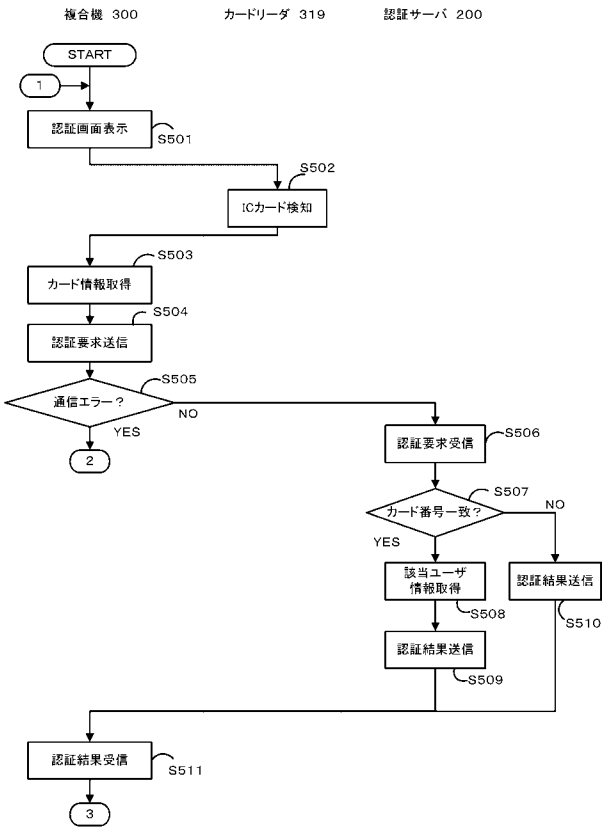
【図３】


プリンタ
スキャナ
314
315
310
311
312
313
300
RIP
プリンタ I/F
スキャナ I/F
画像処理部
317
319
306
307
308
309
RAM
HDD
IMAGE BUS I/F
外部 I/F
カードリーダ
318
316
CPU
ROM
Network I/F
MODEM
操作部 I/F
操作部
301
302
303
304
305
LAN
公衆回線網

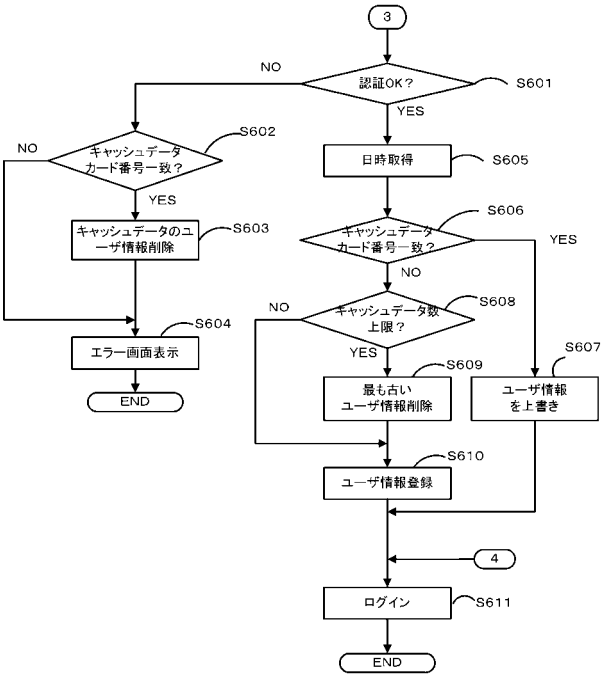
【図４】


認証サーバ 200
データ通信部 250
認証部 251
クライアントPC 100
WEBブラウザ 150
複合機 300
キャッシュ処理部353
バックアップ部 354
WEBサービス部 355
カードリーダ制御部 350
認証サーバ通信部 351
認証処理部 352

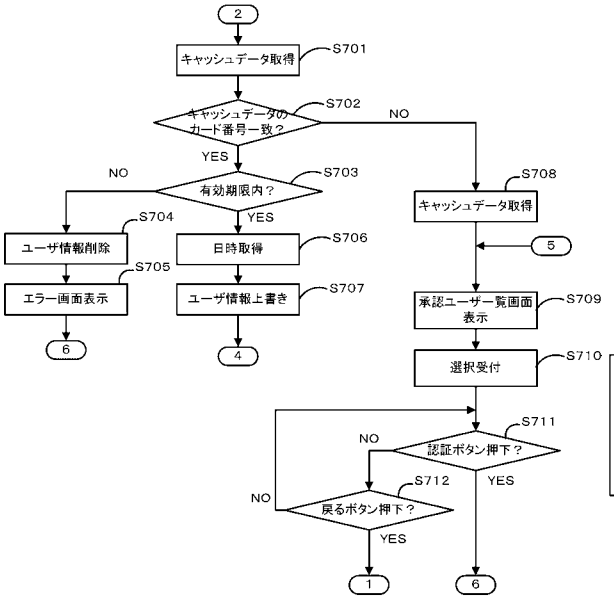
【図５】


複合機 300
カードリーダ 319
認証サーバ 200
START
1
認証画面表示
S501
S502
ICカード検知
S503
カード情報取得
S504
認証要求送信
S505
通信エラー？
NO
YES
2
S506
認証要求受信
S507
カード番号一致？
NO
YES
該当ユーザ情報取得
S508
認証結果送信
S509
S510
認証結果受信
S511
3

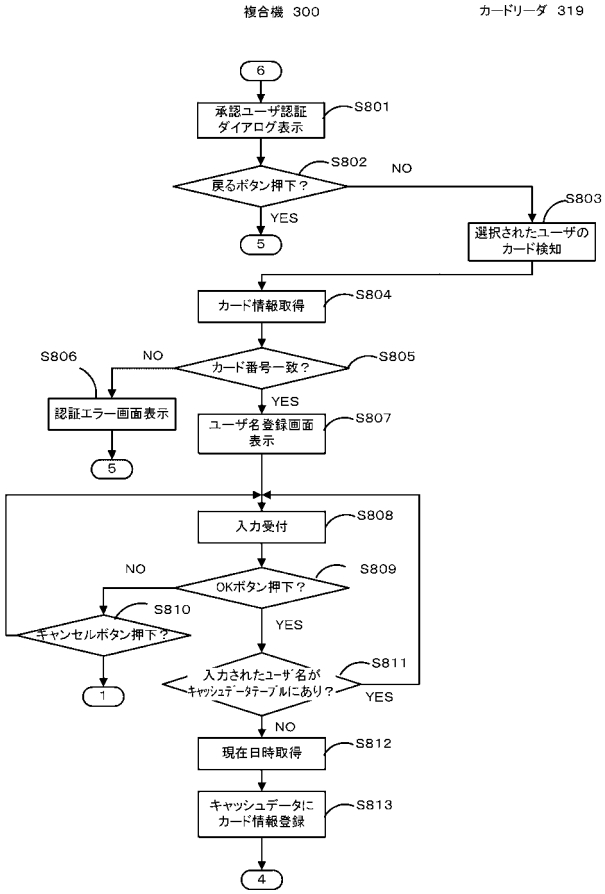
【図６】


3
認証OK？
S601
NO
YES
キャッシュデータ カード番号一致？
S602
NO
YES
キャッシュデータのユーザ情報削除
S603
エラー画面表示
S604
END
日時取得
S605
キャッシュデータ カード番号一致？
S606
YES
NO
キャッシュデータ数上限？
S608
NO
YES
S607
最も古いユーザ情報削除
S609
ユーザ情報を上書き
S610
ユーザ情報登録
4
ログイン
S611
END

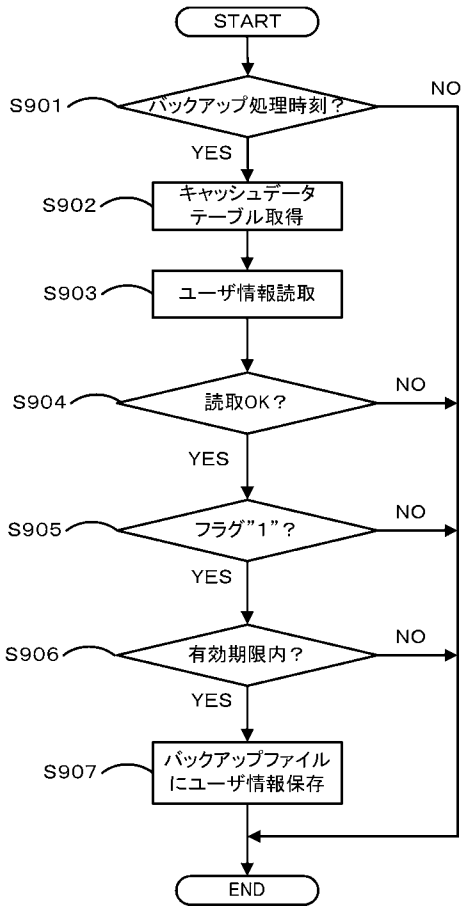
【図７】


2
キャッシュデータ取得
S701
キャッシュデータのカード番号一致？
S702
NO
YES
有効期限内？
S703
NO
YES
ユーザ情報削除
S704
日時取得
S706
エラー画面表示
S705
ユーザ情報上書き
S707
6
4
S708
キャッシュデータ取得
5
承認ユーザー一覧画面表示
S709
選択受付
S710
S711
認証ボタン押下？
NO
YES
S712
戻るボタン押下？
NO
YES
1
6

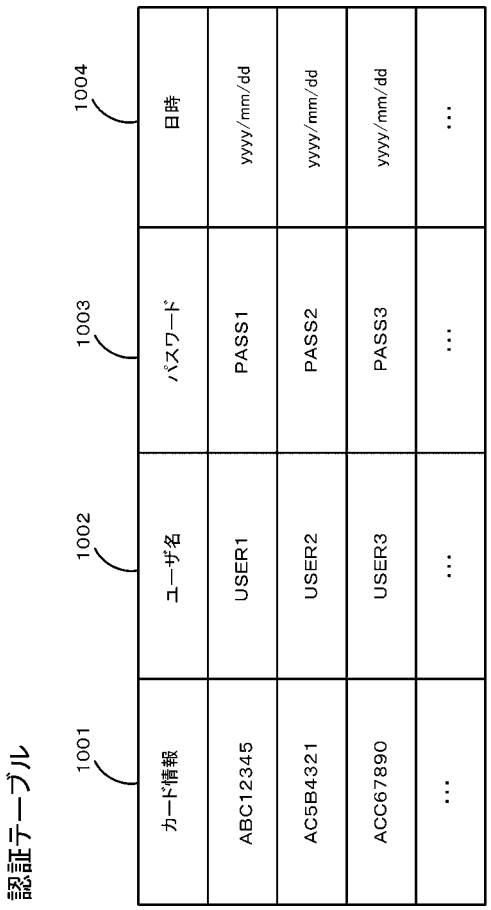
【図８】


複合機 300
カードリーダ 319
6
承認ユーザ認証ダイアログ表示
S801
S802
戻るボタン押下？
NO
YES
S803
選択されたユーザのカード検知
5
カード情報取得
S804
S806
NO
カード番号一致？
S805
YES
認証エラー画面表示
ユーザ名登録画面表示
S807
5
入力受付
S808
NO
S809
OKボタン押下？
S810
キャンセルボタン押下？
YES
S811
入力されたユーザ名がキャッシュデータテーブルにあり？
YES
NO
1
現在日時取得
S812
キャッシュデータにカード情報登録
S813
4

【図９】


START
S901
バックアップ処理時刻？
NO
YES
S902
キャッシュデータテーブル取得
S903
ユーザ情報読取
S904
読取OK？
NO
YES
S905
フラグ”1”？
NO
YES
S906
有効期限内？
NO
YES
S907
バックアップファイルにユーザ情報保存
END

【図１０】


認証テーブル
1001
カード情報
ABC12345
ACSB4321
ACC67890
…
1002
ユーザ名
USER1
USER2
USER3
…
1003
パスワード
PASS1
PASS2
PASS3
…
1004
日時
yyyy/mm/dd
yyyy/mm/dd
yyyy/mm/dd
…

【図１１】

キャッシュデータテーブル

1101 カード情報	1102 ユーザ名	1103 認証日時	1104 登録フラグ	1105 承認カード情報
ABC12345	USER1	yyyy/mm/dd	1	
AC5B4321	USER2	yyyy/mm/dd	1	
ACC67890	USER3	yyyy/mm/dd	0	ABC12345
…	…	…	…	…

【図１２】

バックアップファイル

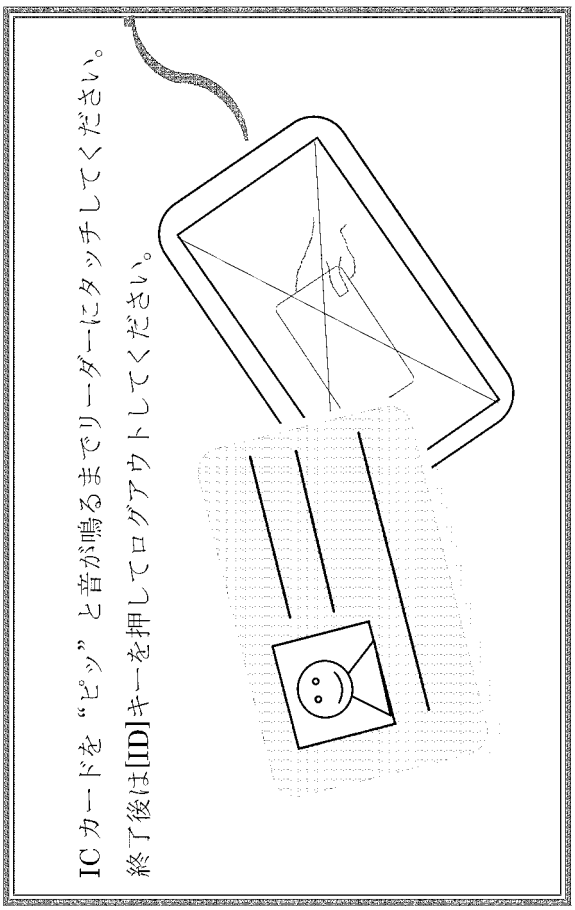
1201 カード情報	1202 ユーザ名	1203 認証日時
ABC12345	USER1	yyyy/mm/dd
AC5B4321	USER2	yyyy/mm/dd
…	…	…

【図１３】

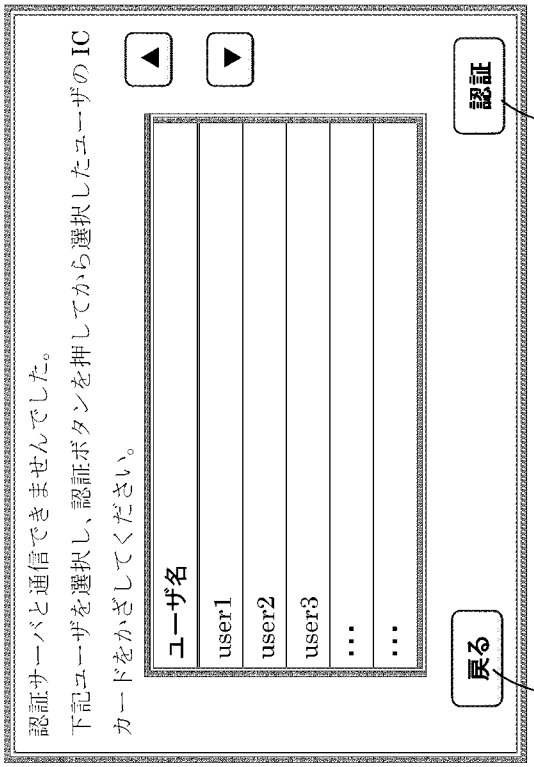
キャッシュデータ管理設定ファイル

1301 フラグ"0"ユーザ有効期限	1302 フラグ"1"ユーザ有効期限	1303 バックアップ処理時刻	1304 キャッシュ上限数
○日間	△日間	□時	×人

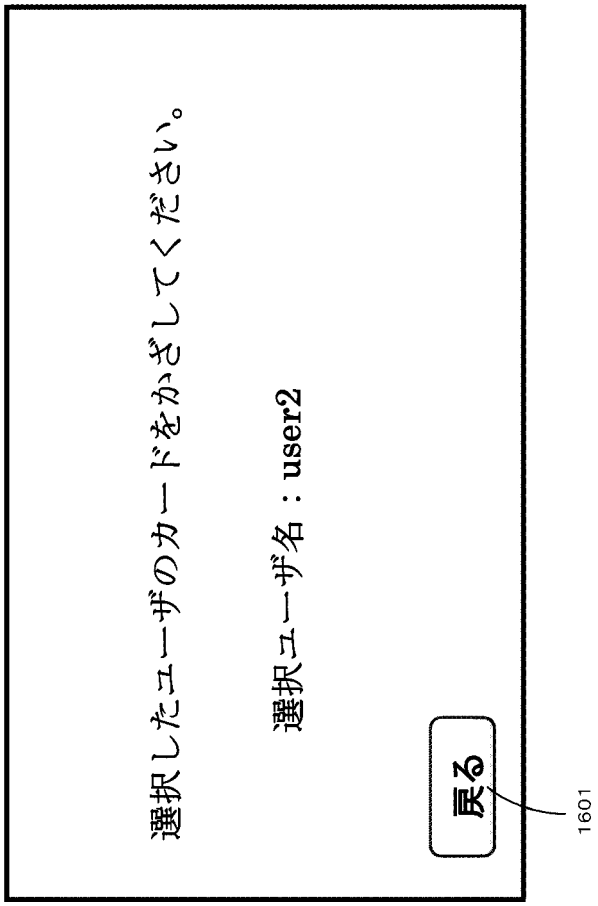
【図１４】



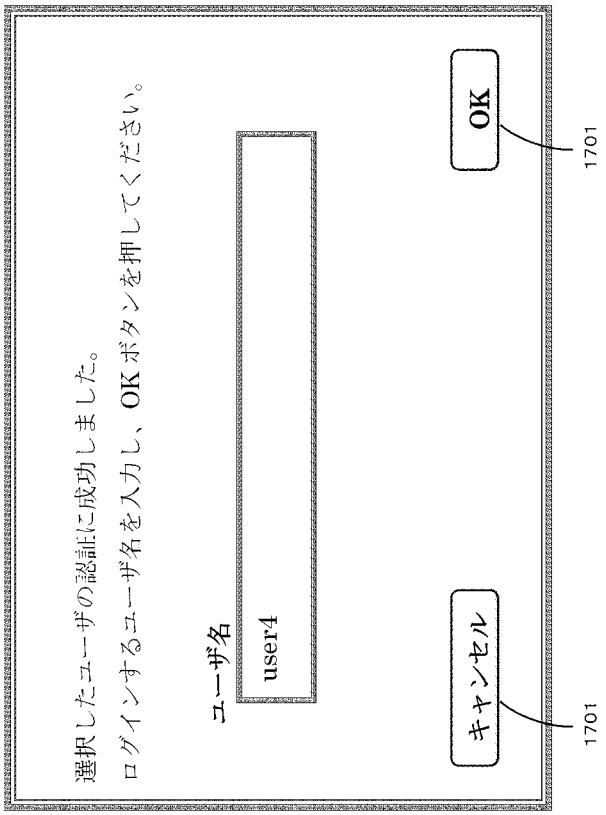
【図１５】


認証サーバと通信できませんでした。
下記ユーザを選択し、認証ボタンを押してから選択したユーザのIC
カードをかざしてください。
ユーザ名
user1
user2
user3
...
...
戻る
認証
1501
1502

【図１６】


選択したユーザのカードをかざしてください。
選択ユーザ名：user2
戻る
1601

【図１７】


選択したユーザの認証に成功しました。
ログインするユーザ名を入力し、OKボタンを押してください。
ユーザ名
user4
OK
キャンセル
1701
1701

フロントページの続き

(51)Int.Cl.　　ＦＩ
　　Ｈ０４Ｎ　1/00　　１０７Ｚ

(72)発明者　石坂　麻美
　　東京都港区三田３丁目９番６号　キヤノンソフトウェア株式会社内

審査官　久慈　渉

(56)参考文献　特開２０１１－１０７８４３（ＪＰ，Ａ）
　　特開２００８－２５０８４３（ＪＰ，Ａ）
　　特開２０１１－０９５７９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｇ０６Ｆ　２１／３１
　　Ｇ０６Ｆ　　３／１２
　　Ｇ０６Ｋ　１７／００
　　Ｈ０４Ｌ　　９／３２
　　Ｈ０４Ｎ　　１／００