

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4958118号
(P4958118)

(45) 発行日 平成24年6月20日(2012.6.20)

(24) 登録日 平成24年3月30日(2012.3.30)

| | | |
|-----------------------------|------------|-------|
| (51) Int.Cl. | F I | |
| G06F 21/20 (2006.01) | G06F 21/20 | 1 3 4 |
| G06F 3/12 (2006.01) | G06F 21/20 | 1 4 5 |
| G06K 17/00 (2006.01) | G06F 3/12 | K |
| H04L 9/32 (2006.01) | G06K 17/00 | F |
| H04N 1/00 (2006.01) | G06K 17/00 | L |
| 請求項の数 13 (全 31 頁) 最終頁に続く | | |

(21) 出願番号 特願2008-281196 (P2008-281196)
 (22) 出願日 平成20年10月31日(2008.10.31)
 (65) 公開番号 特開2010-108348 (P2010-108348A)
 (43) 公開日 平成22年5月13日(2010.5.13)
 審査請求日 平成21年6月29日(2009.6.29)

(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
 (74) 代理人 100096091
 弁理士 井上 誠一
 (72) 発明者 醍醐 敦
 東京都港区三田3丁目11番28号 キヤ
 ノンITソリューションズ株式会社内
 審査官 田中 慎太郎

(56) 参考文献 特開2008-181491 (JP, A)
)
 特開2008-097207 (JP, A)
)

最終頁に続く

(54) 【発明の名称】 画像形成装置、情報処理システムと、その処理方法およびプログラム

(57) 【特許請求の範囲】

【請求項1】

ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段と通信する、記憶媒体を読み取る読取手段を備える画像形成装置であって、

ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、

前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、

前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する第1の記憶媒体識別情報登録要求手段と、
 を備えることを特徴とする画像形成装置。

【請求項2】

前記第 1 の記憶媒体識別情報登録要求手段は、前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていないと判定される場合に、前記削除要求手段で削除要求を出力することなく、前記登録要求を出力す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】

ユーザに一時的に付与される記憶媒体の記憶媒体識別情報の一覧を記憶する記憶媒体識別情報一覧記憶手段と、

前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報が前記記憶媒体識別情報一覧にあるか否かによって、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報に対応する記憶媒体がユーザに一時的に付与される記憶媒体かを判定する記憶媒体判定手段と

を更に備えることを特徴とする請求項 1 または 2 に記載の画像形成装置。

【請求項 4】

前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体として判定されない場合、ユーザが通常利用する記憶媒体として、前記記憶媒体識別情報を前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを出力する第 2 の記憶媒体識別情報登録要求手段

を更に備えることを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の画像形成装置。

【請求項 5】

ユーザに一時的に付与される記憶媒体でログインする場合に、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報に対応して設定された使用できる機能を制限するための機能制限情報を取得する機能制限情報取得手段と、

前記機能制限情報取得手段で取得した機能制限情報に従って、機能制限してログインさせるログイン手段と

を更に備えることを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の画像形成装置。

【請求項 6】

前記機能制限情報は、前記ユーザに一時的に付与される記憶媒体がかざされた時に付与される権限情報と、前記通常利用される記憶媒体がかざされた時に付与される権限情報を用いて生成されることを特徴とする請求項 5 に記載の画像形成装置。

【請求項 7】

前記ユーザ情報記憶手段は、認証サーバ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】

ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段を備える認証サーバと、前記認証サーバと通信可能な、記憶媒体を読み取る読取手段を備える画像形成装置とを含む情報処理システムであって、

前記画像形成装置は、

ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、

前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、

前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別

10

20

30

40

50

情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する記憶媒体識別情報登録要求手段とを備え、

前記認証サーバは、

前記画像形成装置の出力により、前記他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求と、前記記憶媒体識別情報とユーザ識別情報とを含む登録要求を受信する要求受信手段と、

前記要求受信手段で受信した削除要求に従って、他のユーザのユーザ識別情報に対応して記憶されている、前記記憶媒体識別情報取得手段で取得されたユーザに一時的に付与された記憶媒体の記憶媒体識別情報を前記ユーザ情報記憶手段から削除する記憶媒体識別情報削除手段と、

10

前記要求受信手段で受信した登録要求に含まれる記憶媒体識別情報を、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報として、前記ユーザ識別情報と前記記憶媒体情報とを対応付けて前記ユーザ情報記憶手段に登録する記憶媒体識別情報登録手段とを備えることを特徴とする情報処理システム。

【請求項 9】

前記画像形成装置の前記記憶媒体識別情報登録要求手段は、前記認証サーバで、前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体に対応する記憶媒体識別情報であると判定される場合、前記登録要求を送信し、

前記認証サーバは、

ユーザに一時的に付与される記憶媒体の記憶媒体識別情報の一覧を記憶する記憶媒体識別情報一覧記憶手段と、

20

前記記憶媒体識別情報の一覧に従って、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報がユーザに一時的に付与される記憶媒体に対応する記憶媒体識別情報であるか否かを判定する記憶媒体判定手段と

を更に備えることを特徴とする請求項 8 に記載の情報処理システム。

【請求項 10】

ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段と通信する、記憶媒体を読み取る読取手段を備える画像形成装置における処理方法であって、

前記画像形成装置が、

ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付工程と、

前記ユーザ識別情報受付工程で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得工程と、

30

前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求工程と、

40

前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する第 1 の記憶媒体識別情報登録要求工程と

を含むことを特徴とする画像形成装置における処理方法。

【請求項 11】

ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段を備える認証サーバと、前記認証サーバと通信可能な、記憶媒体を読み取る読取手段を備える画像形成装置とを含む情報処理システムにおける処理方法であって、

前記画像形成装置が、

50

ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付工程と、
前記ユーザ識別情報受付工程で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得工程と、

前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求工程と、

10

前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する記憶媒体識別情報登録要求工程と

を含み、

前記認証サーバが、

前記画像形成装置の出力により、前記他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求と、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を受信する要求受信工程と、

前記要求受信工程で受信した削除要求に従って、他のユーザのユーザ識別情報に対応して記憶されている、前記記憶媒体識別情報取得工程で取得されたユーザに一時的に付与された記憶媒体の記憶媒体識別情報を前記ユーザ情報記憶手段から削除する記憶媒体識別情報削除工程と、

20

前記要求受信工程で受信した登録要求に含まれる記憶媒体識別情報を、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報として、前記ユーザ識別情報と前記記憶媒体情報とを対応付けて前記ユーザ情報記憶手段に登録する記憶媒体識別情報登録工程とを含むことを特徴とする情報処理システムにおける処理方法。

【請求項 1 2】

ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段と通信する、記憶媒体を読み取る読取手段を備える画像形成装置で実行可能なプログラムであって、

30

前記画像形成装置を、

ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、

前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、

前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、

40

前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する第 1 の記憶媒体識別情報登録要求手段

として機能させることを特徴とするプログラム。

【請求項 1 3】

ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段を備える認証サーバと、前記認証サーバと通信可能な、記憶媒体を読み取る読取手段を備える画像形成装置とを含む情報処理システムで実行可能なプログラムであって、

50

前記画像形成装置を、
 ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、
 前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、
前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、

10

前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する記憶媒体識別情報登録要求手段として機能させ、

前記認証サーバを、
 前記画像形成装置の出力により、前記他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求と、前記記憶媒体識別情報とユーザ識別情報とを含む登録要求を受信する要求受信手段と、

前記要求受信手段で受信した削除要求に従って、他のユーザのユーザ識別情報に対応して記憶されている、前記記憶媒体識別情報取得手段で取得されたユーザに一時的に付与された記憶媒体の記憶媒体識別情報を前記ユーザ情報記憶手段から削除する記憶媒体識別情報削除手段と、

20

前記要求受信手段で受信した登録要求に含まれる記憶媒体識別情報を、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報として、前記ユーザ識別情報と前記記憶媒体情報とを対応付けて前記ユーザ情報記憶手段に登録する記憶媒体識別情報登録手段として機能させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

30

【0001】

本発明は、記憶媒体用いた画像形成装置の認証において、ユーザに一時的に付与される記憶媒体による認証を可能にする画像形成装置、情報処理システムと、その処理方法およびプログラムに関する。

【背景技術】

【0002】

従来から、ユーザは、サーバ上に一時蓄積された印刷データに対して、印刷装置から印刷要求を行うことで、印刷装置から印刷データを出力する、所謂「ブルプリント（蓄積印刷）」の印刷システムが知られている。これにより、ユーザはアプリケーションから印刷時に特定の印刷装置への出力ではなく、所望の印刷装置からの印刷データ出力を可能としている（例えば、特許文献1）。

40

【0003】

このような印刷システムにおける印刷手順の一例は、以下の通りである。

ユーザが、印刷装置に接続されたICカードリーダーにICカードをかざすと、ICカードリーダーがICカードのUID（ユニークなID）を検知する。そして、印刷装置は、使用可能なユーザが否かを判断するため、認証サーバに格納された、UIDに基づくログインの可否が設定された認証テーブルを参照し、ユーザの認証処理を実行する。

そして、認証処理の結果、ログインできれば、印刷装置は、サーバ上に一時蓄積された当該ユーザの印刷データを取得し印刷する。

このような仕組みにおいて、新たに印刷装置を利用する者や利用しなくなった者等が発

50

生じた場合、管理者にU I Dの登録依頼やU I Dの削除依頼をし、管理者がそれらの処理を行うため、管理者の手間を要してしまうという問題が生じる。

【 0 0 0 4 】

そこで、特許文献2には、I Cカード認証時にU I Dが登録されていなければ、I CカードのU I Dを認証テーブルに登録する仕組みが開示されている。

【特許文献1】特開2006-99714号公報

【特許文献2】特開2008-181491号公報

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 5 】

上記特許文献2のシステムは、新規に発行されたI Cカードがかざされ、I Cカード認証が実行された場合に、かざされたI Cカードのカード情報(U I D)が認証サーバの認証テーブルに登録されていなければ、I Cカードのカード情報の登録を行なうシステムである。

一方、I Cカード運用を行なっている企業において、I Cカード紛失もしくはI Cカードを忘れた場合、一時的な貸出カード(テンポラリカード)を利用するというケースが多々ある。テンポラリカードは、日々異なるユーザに貸与されるため、上記特許文献2のシステムを利用した場合、最初に登録されたユーザにテンポラリカード情報が紐付いてしまい、次に貸し出されたユーザは当該カードを登録することができないという問題が生じる。また、そのままカードをかざせば、前ユーザでログインしてしまうという問題も孕んでおり、実質的にテンポラリカード運用は不可能なシステムとなっている。

【 0 0 0 6 】

そこで本発明の目的は、ユーザに一時的に付与される記憶媒体の記憶媒体識別情報を、他のユーザから削除させ、現在利用するユーザと対応付けて登録させることで、ユーザに一時的に付与される記憶媒体においても適切に認証を得ることを可能にする仕組みを提供することである。

【課題を解決するための手段】

【 0 0 0 7 】

前述した目的を達成するための第1の発明は、ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段と通信する、記憶媒体を読み取る読取手段を備える画像形成装置であって、ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する第1の記憶媒体識別情報登録要求手段と、を備えることを特徴とする。

また、前記第1の記憶媒体識別情報登録要求手段は、前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていないと判定される場合に、前記削除要求手段で削除要求を出力することなく、前記登録要求を出力することを特徴とする。

10

20

30

40

50

【 0 0 0 8 】

また、ユーザに一時的に付与される記憶媒体の記憶媒体識別情報の一覧を記憶する記憶媒体識別情報一覧記憶手段と、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報が前記記憶媒体識別情報一覧にあるか否かによって、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報に対応する記憶媒体がユーザに一時的に付与される記憶媒体かを判定する記憶媒体判定手段とを更に備えることを特徴とする。

【 0 0 0 9 】

また、前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体として判定されない場合、ユーザが通常利用する記憶媒体として、前記記憶媒体識別情報を前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを出力する第2の記憶媒体識別情報登録要求手段を更に備えることを特徴とする。

10

【 0 0 1 0 】

また、前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体として判定されない場合、ユーザが通常利用する記憶媒体として、前記記憶媒体識別情報を前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを出力する第2の記憶媒体識別情報登録要求手段を更に備えることを特徴とする。

20

【 0 0 1 1 】

また、ユーザに一時的に付与される記憶媒体でログインする場合に、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報に対応して設定された使用できる機能を制限するための機能制限情報を取得する機能制限情報取得手段と、前記機能制限情報取得手段で取得した機能制限情報に従って、機能制限してログインさせるログイン手段とを更に備えることを特徴とする。

また、前記機能制限情報は、前記ユーザに一時的に付与される記憶媒体がかざされた時に付与される権限情報と、前記通常利用される記憶媒体がかざされた時に付与される権限情報を用いて生成されることを特徴とする。

30

また、前記ユーザ情報記憶手段は、認証サーバに備えることを特徴とする。

【 0 0 1 2 】

第2の発明は、ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段を備える認証サーバと、前記認証サーバと通信可能な、記憶媒体を読み取る読取手段を備える画像形成装置とを含む情報処理システムであって、前記画像形成装置は、ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する記憶媒体識別情報登録要求手段とを備え、前記認証サーバは、前記画像形成装置の出力により、前記他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記

40

50

憶媒体識別情報の削除要求と、前記記憶媒体識別情報とユーザ識別情報とを含む登録要求を受信する要求受信手段と、前記要求受信手段で受信した削除要求に従って、他のユーザのユーザ識別情報に対応して記憶されている、前記記憶媒体識別情報取得手段で取得されたユーザに一時的に付与された記憶媒体の記憶媒体識別情報を前記ユーザ情報記憶手段から削除する記憶媒体識別情報削除手段と、前記要求受信手段で受信した登録要求に含まれる記憶媒体識別情報を、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報として、前記ユーザ識別情報と前記記憶媒体情報とを対応付けて前記ユーザ情報記憶手段に登録する記憶媒体識別情報登録手段とを備えることを特徴とする。

また、前記画像形成装置の前記記憶媒体識別情報登録要求手段は、前記認証サーバで、前記記憶媒体識別情報がユーザに一時的に付与される記憶媒体に対応する記憶媒体識別情報であると判定される場合、前記登録要求を送信し、前記認証サーバは、ユーザに一時的に付与される記憶媒体の記憶媒体識別情報の一覧を記憶する記憶媒体識別情報一覧記憶手段と、前記記憶媒体識別情報の一覧に従って、前記記憶媒体識別情報取得手段で取得した記憶媒体識別情報がユーザに一時的に付与される記憶媒体に対応する記憶媒体識別情報であるか否かを判定する記憶媒体判定手段とを更に備えることを特徴とする。

【0013】

第3の発明は、ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段と通信する、記憶媒体を読み取る読取手段を備える画像形成装置における処理方法であって、前記画像形成装置が、ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付工程と、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得工程と、前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求工程と、前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する第1の記憶媒体識別情報登録要求工程とを含むことを特徴とする。

【0014】

第4の発明は、ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段を備える認証サーバと、前記認証サーバと通信可能な、記憶媒体を読み取る読取手段を備える画像形成装置とを含む情報処理システムにおける処理方法であって、前記画像形成装置が、ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付工程と、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得工程と、前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求工程と、前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付工程で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する記憶媒体識別情報登録要求工程とを含み、前記認証サーバが、前記画像形成装置の出力により

、前記他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求と、前記記憶媒体識別情報をと前記ユーザ識別情報と含む登録要求を受信する要求受信工程と、前記要求受信工程で受信した削除要求に従って、他のユーザのユーザ識別情報に対応して記憶されている、前記記憶媒体識別情報取得工程で取得されたユーザに一時的に付与された記憶媒体の記憶媒体識別情報を前記ユーザ情報記憶手段から削除する記憶媒体識別情報削除工程と、前記要求受信工程で受信した登録要求に含まれる記憶媒体識別情報を、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報として、前記ユーザ識別情報と前記記憶媒体情報を対応付けて前記ユーザ情報記憶手段に登録する記憶媒体識別情報登録工程とを含むことを特徴とする。

10

【0015】

第5の発明は、ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段と通信する、記憶媒体を読み取る読取手段を備える画像形成装置で実行可能なプログラムであって、前記画像形成装置を、ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより
当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する第1の記憶媒体識別情報登録要求手段として機能させることを特徴とする。

20

第6の発明は、ユーザを識別するためのユーザ識別情報を記憶するユーザ情報記憶手段を備える認証サーバと、前記認証サーバと通信可能な、記憶媒体を読み取る読取手段を備える画像形成装置とを含む情報処理システムで実行可能なプログラムであって、前記画像形成装置を、ユーザを識別するためのユーザ識別情報を受け付けるユーザ識別情報受付手段と、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報を用いて認証された後、記憶媒体の登録指示を受け付けた場合に、前記読取手段によって記憶媒体を読み取ることによって得られる記憶媒体識別情報を取得する記憶媒体識別情報取得手段と、前記記憶媒体識別情報が、繰り返し利用されるユーザに一時的に付与される記憶媒体として判定され、当該記憶媒体識別情報が前記ユーザ情報記憶手段で他のユーザのユーザ識別情報に対応して既に記憶されていると判定される場合に、前記他のユーザにより当該記憶媒体を用いた認証が成功しないように、当該他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求を出力する削除要求手段と、前記記憶媒体識別情報をユーザに一時的に付与された記憶媒体として、前記ユーザ識別情報受付手段で受け付けたユーザ識別情報に対応して前記ユーザ情報記憶手段に記憶するように、前記記憶媒体識別情報と前記ユーザ識別情報とを含む登録要求を出力する記憶媒体識別情報登録要求手段として機能させ、前記認証サーバを、前記画像形成装置の出力により、前記他のユーザのユーザ識別情報に対応して記憶されている、ユーザに一時的に付与された記憶媒体の記憶媒体識別情報の削除要求と、前記記憶媒体識別情報とユーザ識別情報とを含む登録要求を受信する要求受信手段と、前記要求受信手段で受信した削除要求に従って、他のユーザのユーザ識別情報に対応して記憶されている、前記記憶媒体識別情報取得手段で取得されたユーザに一時的に付与された記憶媒体の記憶媒体識別情報を前記ユーザ情報記憶手段から削除する記憶媒体識別情報削除手段と、前記要求受信手段で受信した登録要求に含まれる記憶媒体識別情報を、ユーザに一時的に付与された記憶

30

40

50

媒体の記憶媒体識別情報として、前記ユーザ識別情報と前記記憶媒体情報とを対応付けて前記ユーザ情報記憶手段に登録する記憶媒体識別情報登録手段として機能させることを特徴とする。

【発明の効果】

【0016】

本発明によれば、ユーザに一時的に付与される記憶媒体の記憶媒体識別情報を、他のユーザから削除させ、現在利用するユーザと対応付けて登録させることで、ユーザに一時的に付与される記憶媒体においても適切に認証処理を可能とする画像形成装置、情報処理システムと、その処理方法およびプログラムを提供することが可能になる。

10

【発明を実施するための最良の形態】

【0017】

以下、図面を参照しながら、本発明に係る画面形成システムの好適な実施形態について詳細に説明する。

図1は、本実施形態の画像形成システム（情報処理システム）の一例を示すシステム構成図である。

図1に示すように、画像形成システム（情報処理システム）は、例えば、1又は複数の複合機300、1又は2台のICカード認証サーバ200、1又は複数のクライアントPC100がローカルエリアネットワーク（LAN）400（通信媒体）を介して接続された構成をとる。

20

【0018】

複合機300は、後述するカードリーダー319にかざされたカードから読み取られたカード番号を認証依頼としてICカード認証サーバ200に送信するとともに、これも後述する複合機の操作部308で入力されたユーザ名とパスワードをICカード認証サーバ200に認証依頼として送信する。

【0019】

ICカード認証サーバ200は、後述するICカード認証用テーブル（図9）を格納しており、複合機300からのICカードによる認証依頼、または、ユーザ名とパスワードによる認証依頼に応じて、ICカード認証用テーブルを用いて認証処理を行う。

尚、ICカード認証サーバ200を、例えば、ディレクトリサーバ（不図示）と通信可能に構成し、ユーザ名とパスワードによる認証依頼があった場合には、ディレクトリサーバに問い合わせ、ユーザ名がディレクトリサーバ内に記憶されていれば認証成功と判断し、認証結果をICカード認証サーバ200から複合機300へ送信することも可能である。つまり、ICカード認証サーバ200はディレクトリサーバの機能を備える装置である。

30

また、クライアントPC100は、複合機300への印刷設定等を行なう。

【0020】

次に、図2を用いて、図1に示したクライアントPC100、ICカード認証サーバ200のハードウェア構成について説明する。

図2は、クライアントPC100、ICカード認証サーバ200に適用可能な情報処理装置のハードウェア構成例を示すブロック図である。

40

【0021】

図2に示すように、クライアントPC100、ICカード認証サーバ200は、システムバス204を介してCPU（Central Processing Unit）201、RAM（Random Access Memory）203、ROM（Read Only Memory）202、入力コントローラ205、ビデオコントローラ206、メモリコントローラ207、通信I/Fコントローラ208等が接続された構成を採る。

【0022】

CPU201は、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

50

に制御する。

また、ROM 202あるいは外部メモリ 211には、CPU 201の制御プログラムであるBIOS (Basic Input/Output System)やOS (Operating Systems)や、各サーバあるいは各PCが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。

RAM 203は、CPU 201の主メモリ、ワークエリア等として機能する。CPU 201は、処理の実行に際して必要なプログラム等をROM 202あるいは外部メモリ 211からRAM 203にロードし、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。

【0023】

また、入力コントローラ 205は、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。

ビデオコントローラ 206は、CRTディスプレイ (Cathode Ray Tube) 210等の表示器への表示を制御する。尚、図2ではCRT 210と記載しているが、表示器はCRTに限らず、液晶ディスプレイ等の他の表示器でもよい。これらは、必要に応じて管理者が使用する。

【0024】

メモリコントローラ 207は、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外部記憶装置 (ハードディスク (HD)) や、フレキシブルディスク (FD)、あるいは、PCMCIA (Personal Computer Memory Card International Association) 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。

通信I/Fコントローラ 208は、ネットワーク (例えば、図1に示したLAN 400) を介して外部機器と接続・通信し、ネットワークでの通信制御処理を実行する。例えば、TCP/IP (Transmission Control Protocol/Internet Protocol) を用いた通信等が可能である。

【0025】

尚、CPU 201は、例えばRAM 203内の表示情報用領域へアウトラインフォントの展開 (ラスライズ) 処理を実行することにより、CRT 210上に表示することが可能である。また、CPU 201は、CRT 210上のマウスカーソル (図示しない) 等によるユーザ指示を可能とする。

【0026】

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RAM 203にロードされることによりCPU 201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についても後述する。

【0027】

次に、図3を用いて、本発明の情報処理装置としての複合機 300を制御するコントローラユニットのハードウェア構成について説明する。

図3は、複合機 300のコントローラユニット 316のハードウェア構成例を示すブロック図である。

【0028】

図3において、コントローラユニット 316は、画像入力デバイスとして機能するスキャナ 314や、画像出力デバイスとして機能するプリンタ 312と接続されるとともに、図1に示したLAN 400のようなローカルエリアネットワークや、例えばPSTNまたはISDN等の公衆回線 (WAN) と接続することで、画像データやデバイス情報の入出力を行なう。

【0029】

10

20

30

40

50

図3に示すように、コントローラユニット316は、CPU301、RAM302、ROM303、外部記憶装置（ハードディスクドライブ（HDD））304、ネットワークインタフェース（Network I/F）305、モデム（Modem）306、操作部インタフェース（操作部I/F）307、外部インタフェース（外部I/F）318、イメージバスインタフェース（IMAGE BUS I/F）320、ラスト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）313、画像処理部317等で構成される。

【0030】

CPU301は、システム全体を制御するプロセッサである。

RAM302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。

10

ROM303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。

外部記憶装置（ハードディスクドライブHDD）304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。

【0031】

操作部インタフェース（操作部I/F）307は、操作部（UI）308とのインタフェース部であり、操作部308に表示する画像データを操作部308に対して出力する。また、操作部I/F307は、操作部308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308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。

20

【0032】

ネットワークインタフェース（Network I/F）305は、ネットワーク（LAN）に接続し、データの入出力を行なう。

モデム（MODEM）306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。

【0033】

外部インタフェース（外部I/F）318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、認証が必要となるICカード読み取り用のカードリーダー319が接続されている。

30

そして、CPU301は、この外部I/F318を介してカードリーダー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309上に配置される。

40

【0034】

一方、イメージバスインタフェース（IMAGE BUS I/F）320は、システムバス309と画像データを高速で転送する画像バス315とを接続し、データ構造を変換するバスブリッジである。

画像バス315は、PCIバスまたはIEEE1394で構成される。画像バス315上には以下のデバイスが配置される。

【0035】

ラスト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。

プリンタインタフェース（プリンタI/F）311は、プリンタ312とコントローラ

50

ユニット 3 1 6 を接続し、画像データの同期系 / 非同期系の変換を行う。

また、スキャナインタフェース (スキャナ I / F) 3 1 3 は、スキャナ 3 1 4 とコントローラユニット 3 1 6 を接続し、画像データの同期系 / 非同期系の変換を行う。

【 0 0 3 6 】

画像処理部 3 1 7 は、入力画像データに対し、補正、加工、編集を行ったり、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 3 1 7 は、画像データの回転や、多値画像データに対しては J P E G、2 値画像データは J B I G、M M R、M H 等の圧縮伸張処理を行う。

【 0 0 3 7 】

スキャナ I / F 3 1 3 に接続されるスキャナ 3 1 4 は、原稿となる紙上の画像を照明し、C C D ラインセンサで走査することで、ラスティ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 3 0 8 から読み取り起動指示することにより、C P U 3 0 1 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。

10

【 0 0 3 8 】

プリンタ I / F 3 1 1 に接続されるプリンタ 3 1 2 は、ラスティ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、C P U 3 0 1 からの指示によって開始する。尚、プリンタ部 3 1 2 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。

20

【 0 0 3 9 】

操作部 I / F 3 0 7 に接続される操作部 3 0 8 は、液晶ディスプレイ (L C D) 表示部を有する。L C D 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 / F 3 0 7 を介して C P U 3 0 1 に伝える。また、操作部 3 0 8 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、I D キー、リセットキー等を備える。

ここで、操作部 3 0 8 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 L E D 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、操作部 3 0 8 のストップキーは、稼働中の動作を止める働きをする。また、操作部 3 0 8 の I D キーは、使用者のユーザ I D を入力する時に用いる。リセットキーは、操作部 3 0 8 からの設定を初期化する時に用いる。

30

【 0 0 4 0 】

外部 I / F 3 1 8 に接続されるカードリーダー 3 1 9 は、C P U 3 0 1 からの制御により、I C カード (例えば、ソニー社の F e l i c a (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 / F 3 1 8 を介して C P U 3 0 1 へ通知する。

【 0 0 4 1 】

次に、図 4 を用いて、本発明のクライアント P C 1 0 0、認証サーバ 2 0 0、情報処理装置としての複合機 3 0 0 の機能について説明する。

40

図 4 は、クライアント P C 1 0 0、認証サーバ 2 0 0、複合機 3 0 0 の機能の一例を示す機能ブロック図である。

尚、各機能の処理の詳細については、後述の図 5 ~ 図 1 0 のフローチャートに沿って説明する。

【 0 0 4 2 】

クライアント P C 1 0 0 は W e b ブラウザ 1 5 0 等の機能を備える。

W e b ブラウザ 1 5 0 は、不図示の複合機 3 0 0 のウェブサービスへのアクセスに用いる。ウェブサービス上で、後述する図 1 1 に示すテンポラリカードリストを作成することが可能になる。

作成方法は、ブラウザ上に表示されるリストにカード情報を入力しても、また、クライ

50

アントPC100上で作成したテンポラリカードリストをアップロードしてもよく、本発明は、テンポラリカードリストの作成方法には依存しない。

【0043】

認証サーバ200は、複合機通信部250、認証部251、ユーザ情報管理部252、使用制限管理部253等の機能を備える。

複合機通信部250は、複合機300内の認証サービス通信部351からの認証要求・カード情報登録要求等を受信し、また、認証結果を認証サービス通信部351に返信する。

認証部251は、複合機通信部250が受信した認証要求に従って、認証サーバ200内で保持する後述の図13に示すICカード認証用テーブルから、カード情報と一致するユーザ情報を取得する。認証結果は複合機通信部250が送信する。

ユーザ情報管理部252は、複合機通信部250が受信したカード情報登録要求等のユーザ情報管理に関する要求に従って、図13に示すICカード認証用テーブルを書き換える。

使用制限管理部253は、図14に示す使用制限情報を比較し、制限情報をマージする。本発明内の処理では、テンポラリカード(テンポラリICカード)ログイン時に当該ユーザの使用制限情報と、テンポラリカードログイン時の指定された使用制限情報を比較し、権限の低い使用制限情報を採用する。

【0044】

複合機300は、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、カード情報登録部353、テンポラリカード番号管理部354等の機能を備える。

カードリーダ制御部350は、複合機300に接続されたICカードリーダ319との通信を行い、カードリーダ319のカード読み取り状態の制御を行う。また、カードリーダにICカードがかざされた場合は、ICカード内に保持されているカード情報を取得する。

認証サーバ通信部351は、認証サーバ200内の複合機通信部250との通信を行い、認証要求・カード情報登録要求等を送受信する。

認証処理部352は、認証サーバ通信部351が認証サーバ200より受信した認証結果に応じて、複合機300にログインする。

カード情報登録部353は、カード情報登録に関する処理を管理し、各処理に応じた画面の遷移等を制御する。

テンポラリカード番号管理部354は、かざされたICカードのカード情報が後述する図11に示すテンポラリカードリスト内に存在するか否かを確認する。

【0045】

以下、図5～図10を用いて、本実施形態の画像形成システム(情報処理システム)1による管理者を介さないテンポラリカードの認証情報管理処理の流れを説明する。

図5～図8は、本発明における複合機300のカード登録の処理の流れを示すフローチャートである。

【0046】

まず、複合機300のCPU301は、カード登録処理を実行するアプリケーションプログラムの起動処理を実行する。すなわち、複合機300上のHDD304に格納されたアプリケーションプログラムがRAM302上にロードされ、アプリケーションプログラムが実行される(ステップ101)。

アプリケーションプログラム300は、図4に示した各種機能、すなわち、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、カード情報登録部353、テンポラリカード管理部354を備える。

【0047】

次に、CPU301は、複合機300上のカードリーダ制御部350により、接続されたカードリーダ319を読み取り開始状態にする(ステップ102)。これにより、カード検知あるいはカード外し等のカードリーダ319からのイベントを取得可能になる。ま

10

20

30

40

50

た、本イベント内にはカードから読み取られたカード情報（製造番号）が含まれる。

【0048】

次に、CPU301は、複合機300上の認証処理部352により、図15に示すICカード認証画面を表示する（ステップ200）。

次に、CPU301は、複合機300上のカード情報登録部353により、図15のICカード認証画面上のユーザ情報管理ボタン1000が押下されたことを検知する（ステップ201）。これにより、ユーザ管理モードになり、カード情報登録ボタン1002が押下されることでテンポラリカードの登録が可能になる。なお、ステップ201では、カードリーダー319に対してカード読み取り停止コマンドを送信する。すなわち、カードリーダー319に対してポーリング停止のコマンドを送り、カードリーダーにICカードがかざされてもカード情報を読み取られないようにする。

10

次に、CPU301は、複合機300上のカード情報登録部353により、図16のユーザ情報確認画面を表示する（ステップ202）。

【0049】

そして、CPU301は、カード情報登録部353により、図16のユーザ情報確認画面のユーザ確認ボタン1001が押下されたことを検知し（ステップ203）、図16のユーザ情報確認画面に入力されたユーザ名、パスワード、ユーザ確認先（認証サーバ200で管理されるドメイン情報）の欄に入力された情報を取得する（ステップ204）。

次に、CPU301は、複合機300上の認証サーバ通信部351により、認証サーバ200に対し、ステップ208で取得したユーザ名、パスワード、ユーザ確認先（認証サーバ200で管理されるドメイン情報）を用いて、ユーザ情報確認要求（認証要求）を送信する（ステップ205）。

20

【0050】

認証サーバ200のCPU201は、認証サーバ200上の複合機通信部250により、複合機300上の認証サーバ通信部351からのユーザ情報確認要求（認証要求）を受信し（ステップ206）、認証サーバ200上の認証部251により、複合機300からのユーザ情報確認要求（認証要求）に従い、認証サーバ200内に保持するICカード認証用テーブル（図13）から当該ユーザを検索し、ユーザ名、メールアドレス、使用制限情報等で構成される当該ユーザのユーザ情報を取得する（ステップ207）。

30

【0051】

図13は、認証サーバ200に記憶されているユーザ情報の一例であり、ユーザ名（ユーザ識別情報）、パスワード、カード情報（記憶媒体識別情報）、メールアドレス、所属グループ等が対応してユーザ情報が記憶されている。また、カード情報（記憶識別情報）として、現在使用しているICカード情報（製造番号）（記憶媒体識別情報）と、現在使用しているカードがテンポラリカードか否かを示すテンポラリカードフラグがユーザ名（ユーザ識別情報）を含むユーザ情報に対応して記憶される。また、所属グループは、グループ名とロール名が紐付いて記憶されており、後述する図14に示すような構造を持つ権限情報と紐付いている。

【0052】

40

このとき、ユーザ情報を検索できた場合、認証成功とし、ユーザ名を含めた認証結果情報を生成する。一方、ユーザ情報を検索できなかった場合、認証不成功とし、認証不成功情報を含めた認証結果を生成する。

そして、認証サーバ200のCPU201は、認証サーバ200上の複合機通信部250により、複合機300に対し、ステップ207で取得した認証結果（確認結果）を送信する（ステップ208）。

【0053】

複合機300のCPU301は、認証サービス通信部351により認証結果（確認結果）を受信する（ステップ209）。

尚、本実施の形態では、ステップ201でユーザ情報管理ボタン1000が押下された

50

場合にステップ202～ステップ209のユーザ情報確認処理を実行するように構成したが、この処理はこのタイミングに限らず、後述する図6のステップ223でYES（ボタン押下後）の場合に実行するように構成してもよい。すなわち、認証サーバ200がカード情報を登録する前であれば、いずれのタイミングでユーザ情報確認処理を実行してもよい。

【0054】

次に、複合機300のCPU301は、カード情報登録部353により、ステップ209で受信した確認結果内容を解析する（ステップ210）。認証成功（ステップ210のYES）であればステップ211に、認証不成功（ステップ210のNO）であればステップ220に進む。

10

【0055】

前述のステップ210においてユーザ情報確認が認証不成功（ステップ210のNO）の場合、CPU301は、カード情報登録部353により、図18に示すユーザ情報確認エラー画面を表示する（ステップ220）。

そして、CPU301は、カード情報登録部353により、図18のユーザ情報確認エラー画面上のOKボタン1003の押下を検知する（ステップ221）。

ステップ221で押下が検知されたら（ステップ221のYES）、続いてこの図18のユーザ情報確認エラー画面を削除し、ステップ200へ戻る。

【0056】

一方、ステップ210で認証成功と判断された場合（ステップ210のYES）、複合機300のCPU301は、カード情報登録部353により、図17に示すユーザ情報管理メニュー画面を表示し（ステップ211）、カード情報登録ボタン1002が押下されたことを検知する（ステップ212）。

20

ステップ212でカード情報登録ボタン1002の押下が検出された場合（ステップ212のYES）、複合機300のCPU301は、カード情報登録部353により、図19に示すカード情報登録画面を表示し（ステップ213）、カードリーダー319に対してカード読み取り開始コマンドを送信する（図6のステップ214）。すなわち、カードリーダー319に対してポーリング開始の指示コマンドを送る。

【0057】

上記のステップ214の処理により、カードリーダー319がポーリングを開始し、カード読み取り状態になる（ステップ215）。

30

カードリーダー319は、カードがかざされたことを検知し、複合機300にカード情報の含まれたカード検知イベントを発行する（ステップ216）。

【0058】

複合機300のCPU301は、カードリーダー制御部350により、カード検知イベントを受信し（ステップ217）、カードリーダーにかざされたICカードのカード情報（製造番号等）を取得する（ステップ218）。尚、ICカードのカード情報は、カード検知イベントに含まれている。

次に、複合機300のCPU301は、カード情報登録部353により、ステップ218で取得したカード情報を、図20に示すように、ステップ213で表示したカード情報登録画面上に表示する（ステップ219）。

40

【0059】

次に、複合機300のCPU301は、カード情報登録部353により、図20のカード情報表示画面上のボタンが押下されたことを検知し（ステップ223）、OKボタン1004が押下された場合はステップ224に進み、戻るボタン1005が押された場合には図5のステップ211に戻り、ユーザ情報管理メニュー画面を表示する。

【0060】

一方、ステップ223でOKボタン1004が押下された場合、複合機300のCPU301は、テンポラリカード番号管理部354により、図11に示すテンポラリカードリスト（一時的に付与される記憶媒体識別情報一覧）が存在するか否か、すなわち、テンポ

50

ラリカード運用を行うか否かを確認する（ステップ224）。テンポラリカードリストが存在しない場合、テンポラリカード運用をしないと判断し（ステップ224のNO）、図8のステップ251に進み、テンポラリカードリストが存在し、テンポラリカード運用を行う場合（ステップ224のYES）は、ステップ225へ進む。

ここで、図11は、テンポラリカードリストの一例であり、一時的にユーザに貸し出されるテンポラリカードのカード情報（製造番号）がリストとして記憶される。本実施の形態では、複合機300の外部メモリ211内にテンポラリカードリストを保持する。

【0061】

テンポラリ運用を行わない場合（ステップ224のNO）、図8のステップ251に進むが、この場合、後述するステップ227～ステップ250の処理が行われず、自ユーザのICカード認証用テーブルへの追加登録処理が行われる。

テンポラリカード運用を行う場合（ステップ224のYES）は、CPU301は、テンポラリカード番号管理部354により、図11に示すテンポラリカードリストを取得し（ステップ225）、ステップ218で取得したカードリーダー319にかざされたカードのカード情報が、テンポラリカードリスト（ユーザに一時的に付与される記憶媒体の記憶媒体識別情報の一覧）内に存在するか否かを判断する（ステップ226）。言い換えると、ステップ226の処理は、ステップ218で取得した記憶媒体識別情報と一致する前記憶媒体識別情報が存在するか否かを判定する記憶媒体判定処理である。

テンポラリカードリスト内にカード情報が存在した場合、当該カード情報のカードがテンポラリカードであると判断し（ステップ226のYES）、ステップ227に進み、存在しない場合は、当該カードはテンポラリカードでないと判断し（ステップ226のNO）、図7のステップ238へ進む、自ユーザのICカード認証用テーブルへの上書き登録処理が行われる。

【0062】

以上のステップ224～ステップ226の説明では、テンポラリカードリストは複合機300の外部メモリ211内に保持するように構成したが、テンポラリカードリストを認証サーバ200内に保持する構成にしてもよい。この場合、ステップ218で取得したカード情報を認証サーバ200に送信し、認証サーバ200で当該カード情報のカードがテンポラリカードであるか否かを判定すればよい。

【0063】

次に、複合機300のCPU301は、認証サービス通信部351により、当該テンポラリカードが既に図13に示すICカード認証用テーブルに登録されているか否かを判定し、登録されている場合には削除する処理を行う（ステップ227～ステップ237）。

すなわち、当該テンポラリカードが以前他のユーザによって使用されていた場合には、当該テンポラリカードがICカード認証用テーブルに他のユーザのカードとして登録されており、これを削除する処理を行う。

【0064】

まず、CPU301は、認証サービス通信部351により、認証サーバ200に対してステップ218で取得したカード情報のカード情報取得要求を送信する（ステップ227）。カード情報取得要求にはICカード情報（製造番号）が含まれる。

次に、認証サーバ200のCPU201は、複合機通信部250により、複合機300の認証サーバ通信部351により送られたカード情報取得要求を受信したうえ（ステップ228）、認証サーバ200のユーザ情報管理部252により、複合機300から送られたカード情報取得要求に従い、認証サーバ200内に保持しているICカード認証用テーブル（図13）から、ステップ218で取得したICカード情報（製造番号）に紐づくユーザを検索し、当該ユーザ情報（ユーザ名）を取得する（ステップ229）。

このとき、当該テンポラリカードが以前に登録されているものであればカード情報が得られ、未登録であればカード情報は得られない。

そして、認証サーバ200のCPU201は、複合機通信部250により、複合機300に対し、ステップ229の検索結果として得られたユーザ情報（ユーザ名）をカード情

10

20

30

40

50

報として送信する（ステップ230）。

【0065】

次に、複合機300のCPU301は、認証サーバ通信部351が、ステップ229で取得したユーザ名を含むカード情報を受信し（ステップ231）、カード情報を解析する（ステップ232）。

すなわち、ステップ231でカード情報（ユーザ情報）が取得できた場合、当該テンポラリカードは登録済みであり、登録を削除するためにステップ233に進み、カード情報が取得できなかった場合、当該テンポラリカードは未登録であり、登録処理を行うためにステップ239に進む。

尚、ステップ231で取得したカード情報がステップ204で取得したユーザに登録されている場合、すなわち、当該テンポラリカードが以前に同じユーザによって既に正しく登録されている場合には、既に登録済みである旨を画面に表示させて処理を終了させてもよい。この場合、ステップ231で取得したカード情報がステップ204で取得したユーザ以外に登録されている場合にステップ233に進み、登録を削除する処理を行うことになる。

10

【0066】

ステップ232で当該テンポラリカードが登録済みであった場合には、複合機300のCPU301は、認証サーバ通信部351により、ステップ231で取得したカード情報から、当該カードの削除要求コマンドを作成し、認証サーバ200に送信する（ステップ233）。

20

削除要求コマンドには、ユーザ名、ICカード情報（製造番号）等が含まれる。

これは、同一のテンポラリカードが複数ユーザに使用されることを防ぐため、テンポラリカードが別のユーザに登録されていた場合に、認証サーバ200に保持されているICカード認証用テーブルの当該ユーザ情報からテンポラリカード情報を削除する処理である。

【0067】

認証サーバ200のCPU201は、複合機通信部251により、認証サーバ通信部351から送られたカード情報削除要求を受信し（ステップ234）、ユーザ情報管理部252により、複合機300からのカード情報削除要求に含まれるユーザ名、ICカード情報を取得し、図13に示すICカード認証用テーブルから、当該ユーザ名を検索し、当該ユーザ名に紐付いた当該ICカード情報を削除する（ステップ235）。ここで、削除されるデータは、ICカード認証用テーブル（図13）のうちのカード番号テーブルである。

30

そして、認証サーバ200のCPU201は、複合機通信部251により、複合機300に対し、ステップ235の削除結果を送信する（ステップ236）。削除結果は削除成功か失敗かを示す情報である。

【0068】

複合機300のCPU301は、認証サーバ通信部351により削除結果を受信し（ステップ237）、カード情報登録部353により、ステップ237で受信した削除結果を解析する（ステップ238）。削除が成功していれば（ステップ238のYES）、当該テンポラリカード情報を登録するためにステップ239に進み、削除が失敗していた場合には（ステップ238のNO）、エラー情報を表示するために後述する図8のステップ260に進む。

40

【0069】

ステップ238でカード情報の削除が成功していた場合（ステップ238のYES）、および、前述した図6のステップ226でカードリーダ319にかざされたカードがテンポラリカードでなかった場合（ステップ226のNO）、ステップ239～ステップ249の処理で、認証サーバ200に保持されているICカード認証用テーブルの自分のユーザ情報に既に何らかのICカード情報が登録されているかを調べ、登録されている場合に当該ICカード情報を削除する処理を実行する。

50

これは、1ユーザ1ICカードの運用を行うためであり、ステップ245～ステップ249の処理により既に登録されているICカード情報を削除することにより、テンポラリカード返却後にテンポラリカード情報の削除処理をし忘れた場合でも、自分のICカード情報を新たに登録することによりテンポラリカード情報が削除され、なりすましによる悪用を防ぐことが可能になる。

【0070】

まず、複合機300のCPU301は、認証サーバ通信部351により、認証サーバ200に対して、自ユーザのカード情報取得要求を送信する(ステップ239)。送信されるデータにはユーザ名が含まれる。

次に、認証サーバ200のCPU201は、複合機通信部250により、認証サーバ通信部351から送られたカード情報取得要求を受信し(ステップ240)、ユーザ情報管理部252により、複合機300からのカード情報取得要求に従いカード情報一覧を取得する(ステップ241)。すなわち、図13に示すICカード認証用テーブルから、ステップ240で取得した当該ユーザ名を検索し、当該ユーザ名に紐付いたICカード情報をすべて取得する。

そして、認証サーバ200のCPU201は、複合機通信部250により、複合機300に対し、ステップ241で取得した当該ユーザに登録されたICカード情報のリストであるカード情報一覧を送信する(ステップ242)。

【0071】

複合機300のCPU301は、認証サーバ通信部351により、カード情報一覧を受信し(ステップ243)、カード情報登録部353により、ステップ243で取得したカード情報一覧を解析する(ステップ244)。カード情報が取得された場合(ステップ244のYES)、すなわち、カード情報が登録されていた場合には、登録されていたICカード情報を削除するため、ステップ245に進み、カード情報が取得されなかった場合(ステップ244のNO)、すなわち、カード情報が登録されていなかった場合には、テンポラリカードのカード情報を登録するために、後述する図8のステップ251に進む。

【0072】

ステップ244でカード情報が登録されていた場合(ステップ244のYES)、登録されているカード情報を削除する処理(ステップ245～ステップ249)を実行する。

すなわち、複合機300のCPU301は、認証サーバ通信部351により、認証サーバ200に対し、ステップ243で取得したカード情報一覧のカード情報削除要求を送信する(ステップ245)。送信データには、ユーザ名およびICカード情報(製造番号)のリストが含まれる。

【0073】

認証サーバ200のCPU201は、複合機通信部250により、認証サーバ通信部351から送られたカード情報削除要求を受信し(ステップ246)、ユーザ情報管理部252により、複合機300からのカード情報削除要求に従い、図13に示すICカード認証用テーブルから当該カード情報を削除する(ステップ247)。

すなわち、ICカード認証用テーブル(図13)から、ステップ245で取得した当該ユーザ名を検索し、当該ユーザ名に紐付いたICカード情報をすべて削除する。ここで、当該ユーザ情報は削除しない。

そして、認証サーバ200のCPU201は、複合機通信部250により、複合機300に対し、ステップ247で実施したカード情報削除の削除結果を送信する(ステップ248)。削除結果は、削除結果を示す結果フラグ(成功又は失敗)である。

【0074】

複合機300のCPU301は、認証サーバ通信部351により、削除結果を受信し(ステップ249)、カード情報登録部353により、ステップ249で受信したカード削除結果を解析する(ステップ250)。削除成功ならば(ステップ250のYES)、テンポラリカードのカード情報を登録するために、ステップ251に進み、削除失敗ならば

10

20

30

40

50

(ステップ250のNO)、エラー情報を表示するために後述する図8のステップ260に進む。

【0075】

ステップ250で削除成功と判断された場合(ステップ250のYES)、または、前述の図6ステップ224で複合機300にテンポラリカード設定がなかった場合(ステップ224のNO)、または、前述の図7ステップ244で当該ユーザのICカード認証用テーブルに登録済みのカード情報がなかった場合(ステップ244のNO)、ステップ251~ステップ255の処理によりICカード認証用テーブルへカードリーダ319に実際にかざされたカードのカード情報(製造番号)を登録するカードの登録処理を行う。

ステップ239~ステップ249による処理を行った場合には、すでに自分のユーザ情報におけるICカード情報は削除されているため、上書き登録を行うことになる。

10

【0076】

まず、複合機300のCPU301は、認証サーバ通信部351により、認証サーバ200に対して、ステップ218で取得したICカードのカード情報のカード情報登録要求を送信する(ステップ251)。このカード情報登録要求には、ユーザ名、ICカード情報、テンポラリカードフラグが含まれる。

ここで、テンポラリカードフラグは、当該カードがテンポラリカードであることを示すもので、前述の図6のステップ226において、当該カードが図11に示したテンポラリカードリストにあり、テンポラリカードであると判断されていた場合(ステップ226のYES)に、テンポラリカード登録要求のテンポラリカードフラグに「True」の値を入れる。一方、ステップ226において、テンポラリカードでないと判断されていた場合(ステップ226のNO)、および、図6のステップ224において複合機300にテンポラリカード運用の設定がなかった場合(ステップ224のNO)、テンポラリカード登録要求のテンポラリカードフラグに「False」の値を入れる。

20

【0077】

次に、認証サーバ200のCPU201は、複合機通信部250により、認証サーバ通信部351から送られたカード情報登録要求(ユーザ名、ICカード情報、テンポラリカードフラグ)を受信し(ステップ252)、ユーザ情報管理部252により、複合機300からのカード情報登録要求に従い、ICカード認証用テーブル(図13)に当該カード情報を追加する(ステップ253)。すなわち、ICカード認証用テーブル(図13)から、ステップ252で取得した当該ユーザ名を検索し、当該ユーザ情報に、ステップ252で取得したICカード情報およびテンポラリカードフラグを登録する。

30

そして、認証サーバ200のCPU201は、複合機通信部250により、複合機300に対し、ステップ253の登録結果(登録の成功または失敗)を送信する(ステップ254)。

【0078】

複合機300のCPU301は、認証サーバ通信部351により、登録結果を受信し(ステップ255)、カード情報登録部353により、ステップ255で受信したカード登録結果を解析する(ステップ256)。登録が成功していれば(ステップ256のYES)登録が成功した旨を表示するためにステップ257に進み、登録が失敗していれば(ステップ256のNO)エラー情報を表示するためにステップ260に進む。

40

【0079】

登録が成功した場合(ステップ256のYES)、複合機300のCPU301は、カード情報登録部353により、図21に示すカード登録成功画面を表示し(ステップ257)、カード登録成功画面上のOKボタン1006の押下を検知し(ステップ258)、図21のカード登録成功画面を削除してから(ステップ259)、図5のステップ200へ戻る。

【0080】

一方、登録が失敗した場合(ステップ256のNO)、または、ステップ250でICカード認証用テーブルから当該ユーザについて登録されていたカード情報を削除できな

50

った場合（ステップ250のNO）、または、図7のステップ238で前回テンポラリカードを使用したユーザのカード情報をICカード認証用テーブルから削除できなかった場合（ステップ238のNO）、複合機300のCPU301は、カード情報登録部353により、図22に示すようなカード登録処理エラー画面を表示する（ステップ260）。カード登録処理エラー画面に表示する文言はエラー内容に応じて変更可能とする。

そして、カード登録処理エラー画面上のOKボタン1007の押下を検知し（ステップ261）、図22のカード登録処理エラー画面を削除してから（ステップ262）、図5のステップ200へ戻る。

【0081】

以上の処理により、ユーザが使用する通常のICカードあるいはテンポラリカードのICカード認証用テーブルへの登録が完了する。

これによって、図13に示すICカード認証用テーブルの当該ユーザの情報として、ユーザ名およびパスワード、メールアドレス、所属グループ等に加えて、カード情報が登録される。カード情報は、カード番号（ICカードの製造番号）およびテンポラリカードフラグであり、使用するカードがテンポラリカードの場合はテンポラリカードフラグが「True」、通常の自分のカードの場合はテンポラリカードフラグが「False」となる。

【0082】

以上に説明した図5～図8のフローチャートによるカード情報登録処理では、1ユーザ1ICカードの運用を前提とし、ICカード認証用テーブルに他のICカードが登録されている場合、または、以前に使用されたテンポラリカードの情報がICカード認証用テーブルに登録されている場合は、まず、それらのICカード情報を削除してから登録を行う（上書き登録）。

【0083】

上述のように図13のICカード認証用テーブルを用いて上書き登録する他に、例えば、図25のICカード認証用テーブルを用いて、自分のカード用（通常使用するICカード）の認証テーブル（2501）と、テンポラリカード用の認証テーブル（2502）を別に設ける方法も採ることが可能である。ステップ226で通常使用するICカードのカード番号と判定される場合（ステップ226でNO）は、ステップ253で通常使用するICカードのカード番号が2501に登録され、ステップ226でテンポラリカードのカード番号と判定される場合（ステップ226でYES）は、ステップ253でテンポラリカードのカード番号が2502に登録される。この形態は、例えば、通常は、通常使用するICカードを使用し、通常使用するカードを忘れた際にテンポラリカードを借り、テンポラリカードのカード番号を登録した場合に特に有効に適用可能である。テンポラリカードが付与された次の日に、通常使用するカードを用いた認証を行った場合には、通常使用するカードのカード番号は削除されておらず、再度通常使用するカードの登録を行うことなくログインすることが可能となる。

【0084】

また、テンポラリカードのカード番号を登録後、通常使用するICカードで認証を行うと、通常使用するICカードのカード番号が2501に登録されているため、後述するステップ306ではユーザ有と判定される。ユーザ有と判定されると（ステップ306でNO）、テンポラリカード番号が2502に登録されているか否かを判定し、テンポラリカード番号が登録されている場合、2502からテンポラリカード番号を削除するように構成する。

【0085】

次に、図9、図10を用いて、本実施の形態のカード認証処理を説明する。

図9および図10は、カード認証処理の流れを示すフローチャートである。

【0086】

複合機300に接続されたICカードリーダー319が、ICカードがかざされたことを検知する（ステップ300）。ICカードリーダー319は、ICカードが検知されると、

10

20

30

40

50

ＩＣカード情報（製造番号）を取得し、取得したＩＣカード情報（製造番号）とともに、複合機３００にカード検知イベントを送信する（ステップ３０１）。

【００８７】

複合機３００のＣＰＵ３０１は、カードリーダ制御部３５０により、カード検知イベントを受信し、かざされたＩＣカードのＩＣカード情報（製造番号）を取得する（ステップ３０２）。

次に、複合機３００のＣＰＵ３０１は、認証サーバ通信部３５１が、認証サーバ２００に対してステップ３０２で取得したＩＣカード情報を含む認証要求を送信する（ステップ３０３）。

【００８８】

認証サーバ２００のＣＰＵ２０１は、複合機通信部２５０が、認証サーバ通信部３５１から送られたＩＣカード情報を含む認証要求を受信し（ステップ３０４）、認証部２５１により、複合機３００からの認証要求に従い、認証サーバ内に保持しているＩＣカード認証用テーブル（図１３）から、ステップ３０４で取得したＩＣカード情報を検索する（ステップ３０５）。

すなわち、図１３に示すＩＣカード認証用テーブルを検索して、当該ＩＣカード情報が存在するか否かを検索する。ＩＣカードが登録されている場合には、ＩＣカード認証用テーブル内にＩＣカード情報とユーザ情報が紐付いて格納されているので、ＩＣカード情報がＩＣカード認証用テーブル内に存在すればユーザ情報が登録されており、認証成功となる。

【００８９】

認証サーバ２００のＣＰＵ２０１は、認証部２５１により、ステップ３０５の認証結果を判断する（ステップ３０６）。すなわち、ＩＣカード情報がＩＣカード認証用テーブル内に存在する場合、ユーザ情報が登録されており、認証成功とし（ステップ３０６のＹＥＳ）、当該ユーザの複合機３００の使用権限を決定するためにステップ３０７に進む。一方、ＩＣカード情報がＩＣカード認証用テーブル内に存在しない場合、ユーザ情報は登録されておらず、認証失敗とし（ステップ３０６のＮＯ）、認証処理を失敗で終了するためにステップ３１２に進む。

【００９０】

ステップ３０６でユーザ情報が登録されていた場合（ステップ３０６のＹＥＳ）、認証サーバ２００のＣＰＵ２０１は、認証部２５１により、ステップ３０５で検索したＩＣカード情報のカードのＩＣカード認証用テーブル内のテンポラリカードフラグの「Ｔｒｕｅ」、「Ｆａｌｓｅ」の別を判定する（ステップ３０７）。テンポラリカードフラグが「Ｔｒｕｅ」の場合、当該ＩＣカードはテンポラリカードであり（ステップ３０７のＴｒｕｅ）、自ユーザ権限とテンポラリカード権限をマージするためステップ３０８に進む。一方、テンポラリカードフラグが「Ｆａｌｓｅ」の場合、当該ＩＣカードはテンポラリカードではなく、自分のカードと判断され、ステップ３１２に進む。自分のカードの場合は、自分のユーザ権限がそのまま使用されることになる。

【００９１】

ステップ３０７が「Ｔｒｕｅ」でテンポラリカードと判断された場合、認証サーバ２００のＣＰＵ２０１は、使用制限管理部２５３により、ステップ３０５で取得したユーザに関する使用制限情報を、ＩＣカード認証用テーブル（図１３）を取得する（ステップ３０８）。

すなわち、ＩＣカード認証用テーブル（図１３）から、ステップ３０５で取得した当該ユーザ名を検索し、当該ユーザ情報に紐付いたグループ名を取得し、さらに、当該グループに紐付いたロール名を取得し、そのロール名に紐付いた使用制限情報を取得する。ここで、ユーザ・グループ・ロールと紐付いているのは、ユーザの使用制限管理を容易にするためである。ユーザは必ず１以上のグループに所属するものとする。また、グループには１以上のロールが設定されているものとする。このような構成を採ることにより、ユーザは必ず１以上のロールに紐付いていることになる。ユーザが１以上のロールに紐付いてい

10

20

30

40

50

る場合は、図 1 4 に示すような使用制限情報のそれぞれの項目を比較し、権限の強い方（制限の弱い方）を自ユーザの使用制限情報として取得する。この使用制限情報は、複合機 3 0 0 の機能を制限するための機能制限情報となる。

図 1 4 は、認証サーバ 2 0 0 に記憶されている権限情報構造の一例であり、複合機 3 0 0 で使用可能な機能の制限を定義する。

【 0 0 9 2 】

次に、認証サーバ 2 0 0 の CPU 2 0 1 は、使用制限管理部 2 5 3 により、認証サーバ 2 0 0 内に保持されてるテンポラリロール（図 1 2 ）に指定されたロールの使用制限情報を取得する（ステップ 3 0 9 ）。

図 1 2 は、認証サーバ 2 0 0 に記憶されているテンポラリカードのロール（権限）を決定するための設定ファイルの一例であり、図 1 1 のテンポラリカードリストに記憶されているカード番号に対する権限を示すロール名が記載されている。

すなわち、使用制限管理部 2 5 3 により、図 1 2 に示すテンポラリロールに指定されたロール名を取得し、そのロール名に紐付いた使用制限情報を取得する。

【 0 0 9 3 】

次に、認証サーバ 2 0 0 の CPU 2 0 1 は、使用制限管理部 2 5 3 により、ステップ 3 0 8 で取得した自ユーザの使用制限情報と、ステップ 3 0 9 で取得したテンポラリロールに指定されたロールの使用制限情報を比較し、権限の低い方（制限の強い方）を当該使用制限情報として取得する（ステップ 3 1 0 ）。

例えば、ユーザに設定されたロールの使用制限のなかで、カラーコピーが「制限なし」になっていたとする。一方、テンポラリロールに指定されたロールの使用制限のなかで、カラーコピーが「モノクロコピーのみ可能」になっていたとする。この場合、当該テンポラリカードのマージ済みの使用制限としては、権限の低い「モノクロコピーのみ可能」が反映される。

ステップ 3 0 8 では、ユーザに複数のロールが紐付いていた場合に、権限の強い方が適用されたが、テンポラリロールとのマージ処理では、権限の弱い方が適用される。

【 0 0 9 4 】

次に、ステップ認証サーバ 2 0 0 の CPU 2 0 1 は、使用制限管理部 2 5 3 により、ステップ 3 0 5 で取得したユーザ情報（ユーザ名、メールアドレス、テンポラリカードフラグ）と、ステップ 3 1 0 で取得した使用制限情報を含む認証に必要なユーザ情報（ユーザ名、メールアドレス、テンポラリカードフラグ、使用制限情報）を作成する（ステップ 3 1 1 ）。

【 0 0 9 5 】

ステップ 3 1 1 の後、および、ステップ 3 0 6 でユーザ情報が存在しなかった場合（ステップ 3 0 6 の N O ））、および、ステップ 3 0 7 でテンポラリカードフラグが「 F a l s e 」だった場合（ステップ 3 0 7 の F a l s e ）、ステップ認証サーバ 2 0 0 の CPU 2 0 1 は、複合機通信部 2 5 0 により、複合機 3 0 0 に対し、認証結果、または認証結果および使用制限情報を含むユーザ情報を送信する（ステップ 3 1 2 ）。

このとき、ステップ 3 0 6 でユーザ情報が存在しなかった場合（ステップ 3 0 6 の N O ））は、認証結果として、当該 IC カードが登録されていなかった（認証不成功）の情報を複合機 3 0 0 に送る。

また、ステップ 3 0 7 でテンポラリカードが「 F a l s e 」だった場合（ステップ 3 0 7 の F a l s e ）は、図示していないが、ステップ 3 0 5 のユーザ検索で得られたユーザ名に紐付いた使用制限情報を取得し、ユーザ情報として複合機 3 0 0 に送る。この場合およびステップ 3 1 1 後の認証結果は、当該 IC カードが登録されているので認証成功である。

【 0 0 9 6 】

複合機 3 0 0 の CPU 3 0 1 は、認証サーバ通信部 3 5 1 により、認証結果を受信し（ステップ 3 1 3 ）、認証処理部 3 5 2 により、ステップ 3 1 3 で取得した認証結果を解析する（ステップ 3 1 4 ）。

10

20

30

40

50

認証結果が成功ならば（ステップ314のYES）ログイン処理を行うためにステップ315に進み、失敗ならば（ステップ314のNO）エラー画面を表示するためにステップ320に進む。すなわち、CPU301は、認証処理部352により、図24に示すような認証エラー画面を表示し（ステップ320）、認証エラー画面上のOKボタン1009の押下を検出し（ステップ321）、検出後、認証エラー画面を削除し（ステップ322）、図9のステップ300に戻り、新たなICカードがかざされるのを待機する。

【0097】

ステップ314で認証結果が成功だった場合（ステップ314のYES）、複合機300のCPU301は、認証処理部352により、ステップ313で取得したユーザ情報のうちのテンポラリカードフラグを確認する（ステップ315）。

10

テンポラリカードフラグが「True」の場合（ステップ315のYES）、当該ICカードはテンポラリカードであり、テンポラリカード認証ダイアログ画面を表示するためにステップ316に進み、「False」の場合（ステップ315のNO）、当該ICカードは自分のICカードであり、そのままログインするためにステップ319に進む。

【0098】

ステップ315でICカードがテンポラリカードであった場合（ステップ315のYES）、複合機300のCPU301は、認証処理部352により、図23に示すようなテンポラリカード認証画面を表示し（ステップ316）、テンポラリカード認証画面のOKボタン1008の押下を検出し（ステップ317）、検出後、図23に示すテンポラリカード認証画面を削除する（ステップ318）。

20

【0099】

ステップ318の後、および、ステップ315でテンポラリカードでなかった場合（ステップ315のNO）、複合機300のCPU300は、認証処理部352により、ステップ313で取得したユーザ情報を用いて複合機300にログインする。

尚、複合機300にログインすると、ステップ313で受信した認証結果に含まれる権限情報（機能制限情報）に従って、複合機300で使用できない機能が制限され、操作部308の表示が制御される。テンポラリカードの場合は、テンポラリカード用の権限と自カードの権限の弱い方の権限が適用され、自カードの場合には自カードの権限が適用される。自カードに複数のルールが存在する場合には、複数のルールのなかで権限の強い方の権限が適用される。

30

【0100】

以上に説明したように、本発明に係る画像形成システム（情報処理システム）では、自ユーザのICカードが何らかの理由で使用できない場合に、安全性を保持してテンポラリカードを運用できる管理者不要の画像形成システム（情報処理システム）を構築することが可能になる。

すなわち、テンポラリカードリストを複合機300が保持することにより、使用されるカードがテンポラリカードであることを識別可能とし、テンポラリカードである場合に、当該カードが既に他のユーザに登録されている場合、強制的に他ユーザの登録を削除し、自ユーザに当該テンポラリカードを登録することができる。

また、自ユーザに既に何らかのカード情報が登録されている場合、それらのカード情報を削除して、テンポラリカードを登録する。テンポラリカードが通常の自カードかを判断するためにテンポラリカードフラグが設定されている。

40

【0101】

また、認証サーバは、テンポラリカードによるログインか否かを判定し、テンポラリカードでログインする場合には、テンポラリカード用に登録された権限情報と、既に認証されているユーザの権限情報をマージし、権限の低い方を優先にした権限情報を含む認証情報を構築することができる。すなわち、テンポラリカードを使用する場合には、通常の自己のカードを使用する場合に比べて、複合機300の使用権限を低く設定することが可能になる。

【0102】

50

以上、添付図面を参照しながら本発明に係る画像生成システムおよび画像形成装置、認証サーバ等の好適な実施形態について説明したが、前述した実施の携帯に限定されるものではない。

例えば、本実施の形態は、予めテンポラリカードリストを複合機300に登録しておく構成を採ったが、このリストを認証サーバ側で保持する構成にしてもよい。また、テンポラリカードリストを複合機300から登録する際、ユーザインタフェース上で指定できるようにしてもよい。

また、本実施の形態では、認証サーバのICカード認証用テーブルに登録可能なICカードをカードの種類(テンポラリカードまたは通常のカード)によらず1枚としたが、上書きを行うのはテンポラリカードのみとし、通常カードの登録情報は削除しないようにする構成にしてもよい。この場合、通常カードでログインすると、認証サーバは通常カードを認証するとともに、登録されているテンポラリカードの情報を削除するように構成すればよい。

10

当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【図面の簡単な説明】

【0103】

【図1】本発明の実施の形態に係る画像形成システムの構成を示す図

【図2】認証サーバ200およびクライアントPC100のハードウェア構成を示す図

20

【図3】複合機300のハードウェア構成を示す図

【図4】本実施形態に係る画像形成システムの機能構成を示す図

【図5】ICカード登録処理の流れを示すフローチャート

【図6】ICカード登録処理の流れを示すフローチャート

【図7】ICカード登録処理の流れを示すフローチャート

【図8】ICカード登録処理の流れを示すフローチャート

【図9】カード認証処理の流れを示すフローチャート

【図10】カード認証処理の流れを示すフローチャート

【図11】複合機300内で管理されるテンポラリカードリストの一例を示す図

【図12】認証サーバ200内で管理されるテンポラリカードの権限設定用のファイルの一例を示す図

30

【図13】認証サーバ200内で管理されるICカード認証用テーブルの一例を示す図

【図14】認証サーバ200内で管理されるICカード認証用テーブル内のルール情報である使用制限情報の一例を示す図

【図15】ICカード認証画面例

【図16】ユーザ情報管理画面例

【図17】ユーザ情報管理メニュー画面例

【図18】ユーザ情報確認エラー画面例

【図19】カード情報登録画面例

【図20】カード情報登録画面例(カード情報表示)

40

【図21】カード情報登録画面例(登録成功表示)

【図22】カード情報登録画面例(登録処理エラー)

【図23】テンポラリカード認証画面例

【図24】認証エラー表示画面例

【図25】認証サーバ200内で管理されるICカード認証用テーブルの一例を示す図

【符号の説明】

【0104】

100 クライアントPC

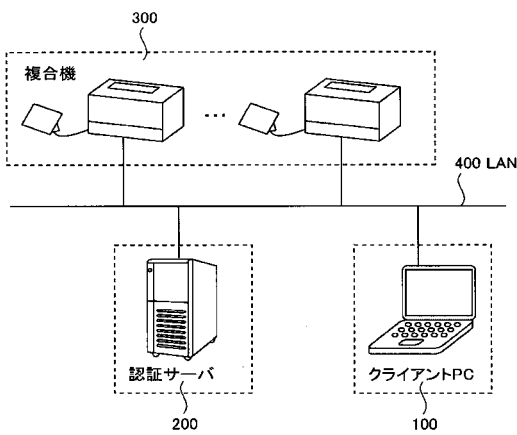
150 Webブラウザ

200 認証サーバ

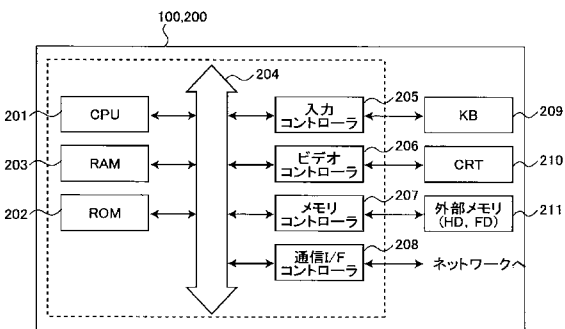
50

- 2 5 0 複合機通信部
- 2 5 1 認証部
- 2 5 2 ユーザ情報管理部
- 2 5 3 使用制限管理部
- 3 0 0 複合機
- 3 1 9 カードリーダー
- 3 5 0 カードリーダー制御部
- 3 5 1 認証サーバ通信部
- 3 5 2 認証処理部
- 3 5 3 カード情報登録部
- 3 5 4 テンポラリカード番号管理部

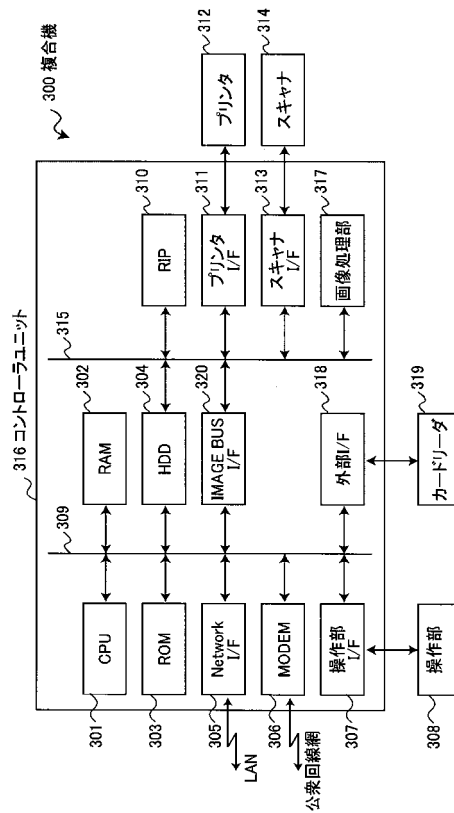
【図1】



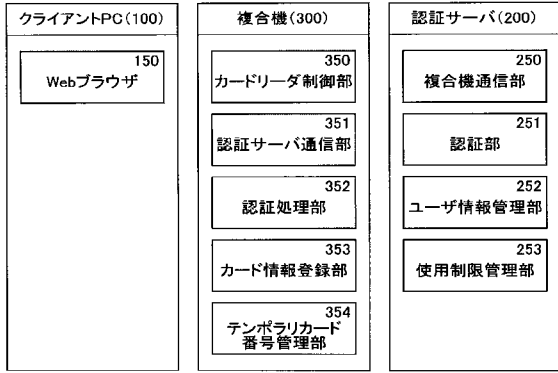
【図2】



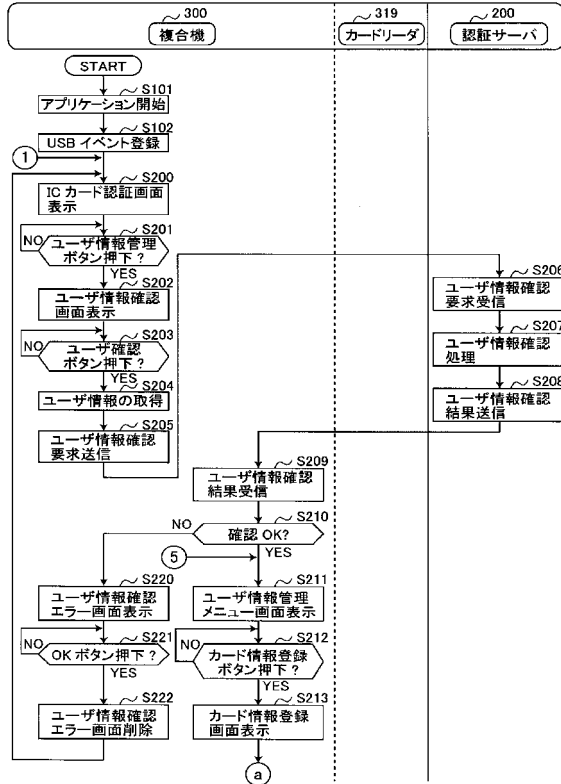
【図3】



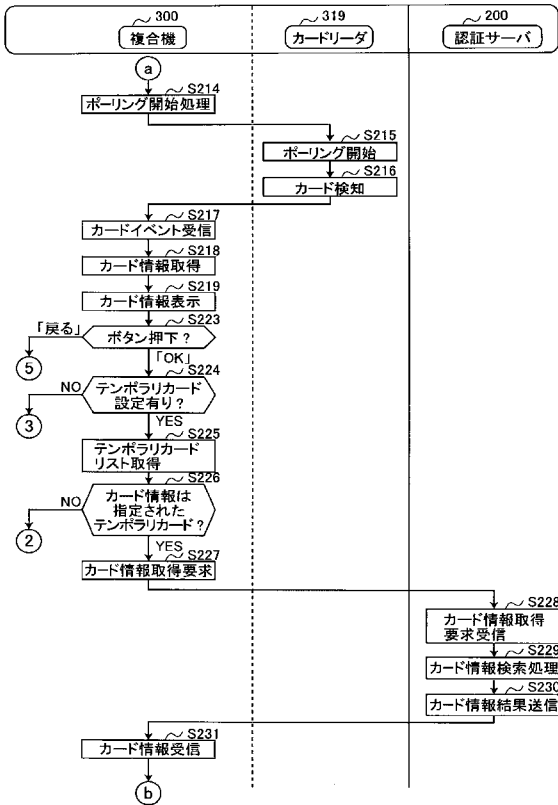
【図4】



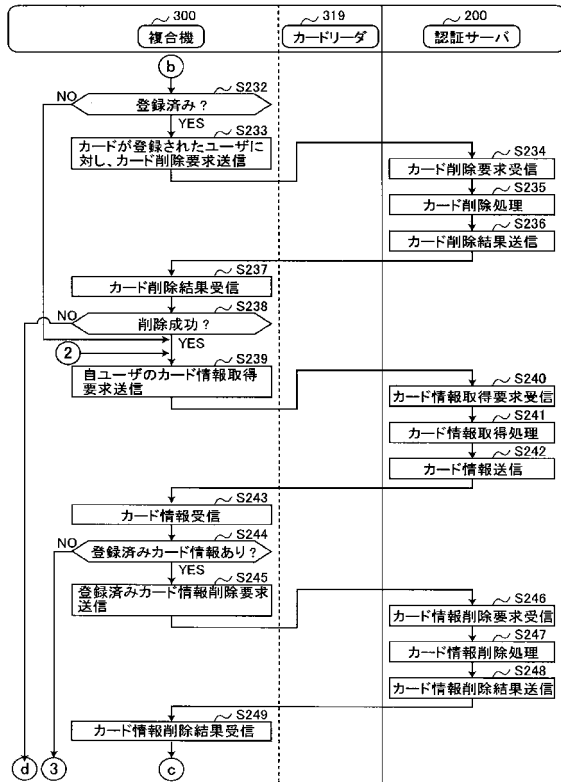
【図5】



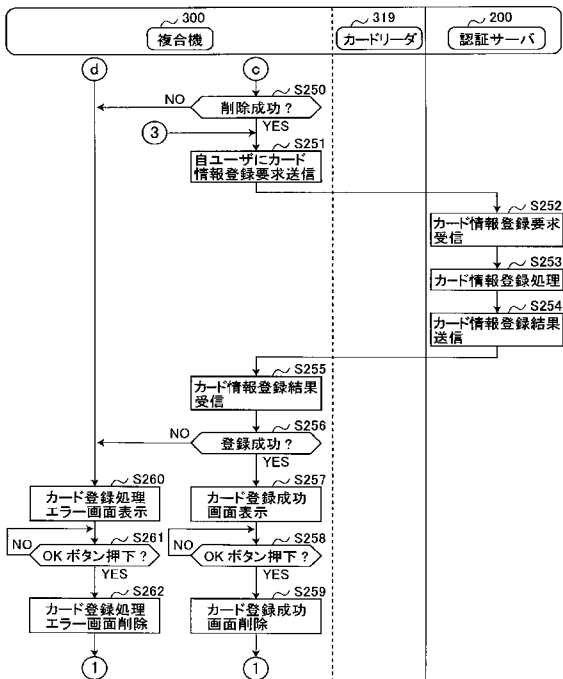
【図6】



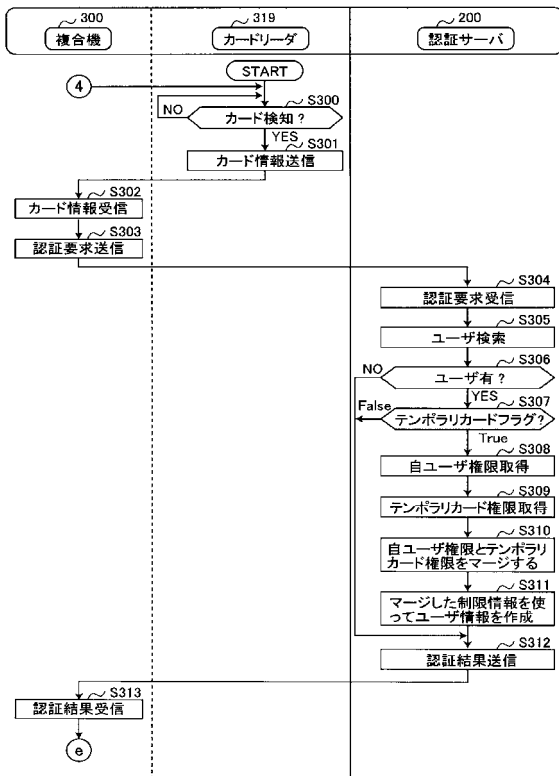
【図7】



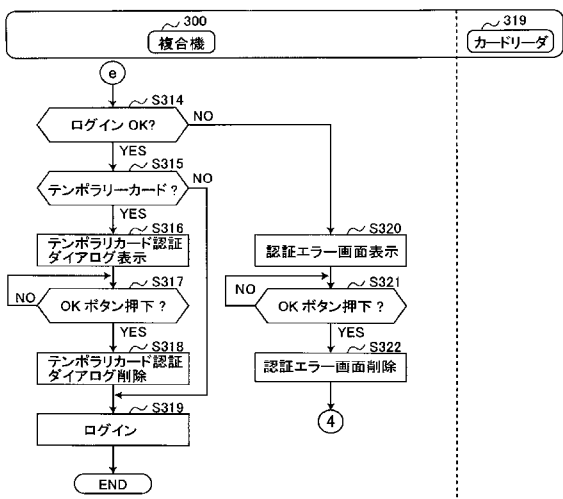
【図 8】



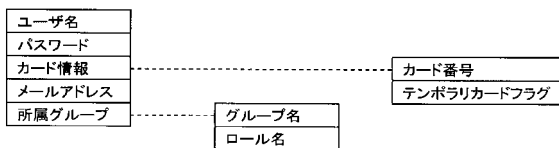
【図 9】



【図 10】



【図 13】



【図 14】

| ユーザー制限情報 | デバイス機能 | 制御機能 | 制御機能 |
|------------------------------|---------------------------|---------------|---------------|
| デバイス機能 (ApplicationCategory) | 印刷 (PrintCategory) | 許可する (Permit) | 許可する (Permit) |
| | コピー (CopyCategory) | 許可しない (Deny) | 許可しない (Deny) |
| | 送信 (SendCategory) | 許可しない (Deny) | 許可しない (Deny) |
| | ボックス (BoxCategory) | 許可しない (Deny) | 許可しない (Deny) |
| | ウェブブラウザ (BrowseCategory) | 許可しない (Deny) | 許可しない (Deny) |
| コピー機能 (Copy) | ユーティリティ (UtilityCategory) | 許可する (Permit) | 許可する (Permit) |
| | その他 (DefaultCategory) | 許可しない (Deny) | 許可しない (Deny) |
| | カラーコピー (ColorCopy) | 許可しない (Deny) | 許可しない (Deny) |
| | コピー方法 (Simplex) | 許可しない (Deny) | 許可しない (Deny) |
| | ページレイアウト (Nup) | 許可しない (Deny) | 許可しない (Deny) |
| スキャン機能 (Scan) | カラーレスキャン (ColorScan) | 許可しない (Deny) | 許可しない (Deny) |
| | 印刷 (PdfPrintFlag) | 許可する (Permit) | 許可する (Permit) |
| | カラー印刷 (ColorPrint) | 許可する (Permit) | 許可する (Permit) |
| | 印刷方法 (Simplex) | 許可する (Permit) | 許可する (Permit) |
| | ページレイアウト (Nup) | 許可しない (Deny) | 許可しない (Deny) |

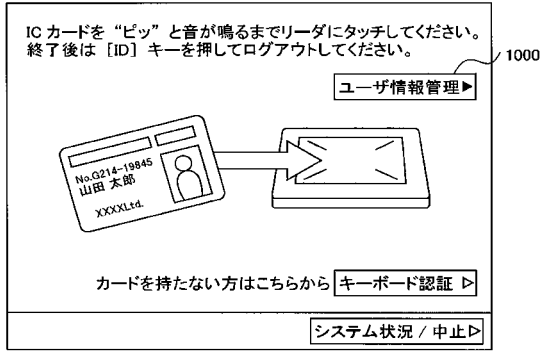
【図 11】

| |
|----------|
| 0000001 |
| 0000002 |
| 0000003 |
| ... |
| ABCDEFGH |

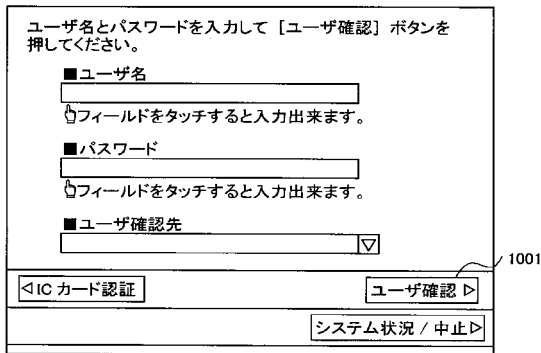
【図 12】

| | |
|----------|------|
| テンポラリロール | ロール名 |
|----------|------|

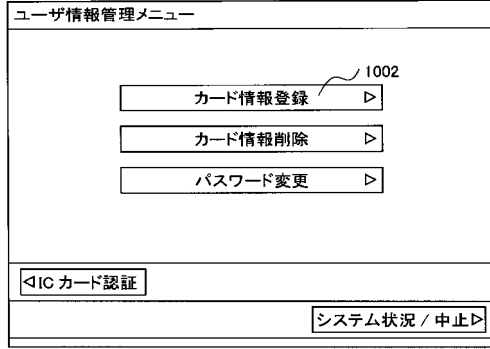
【図 15】



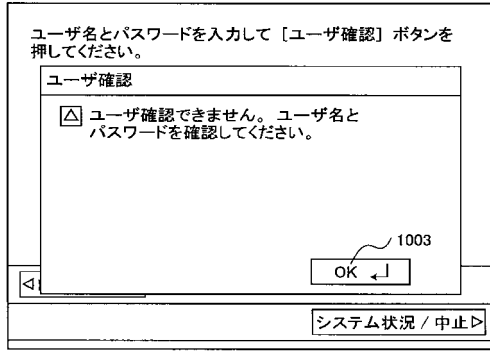
【図 16】



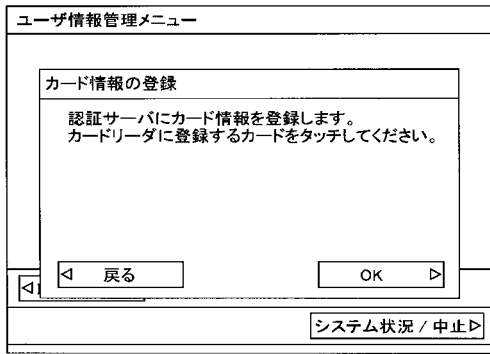
【図 17】



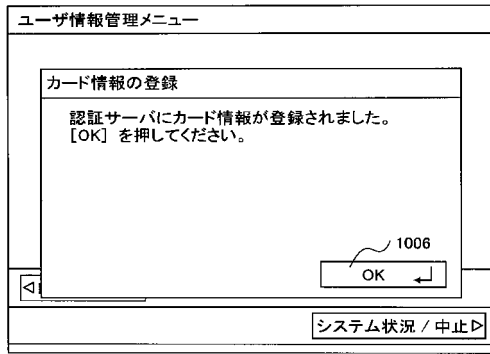
【図 18】



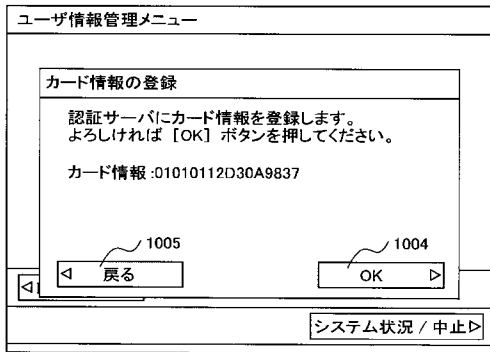
【図 19】



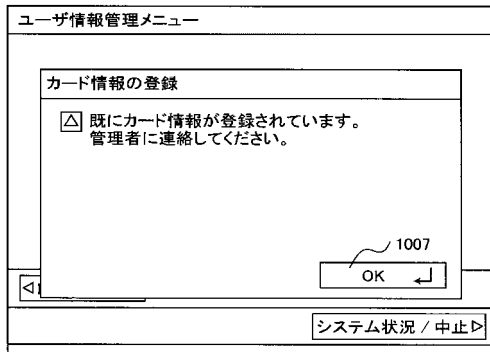
【図 21】



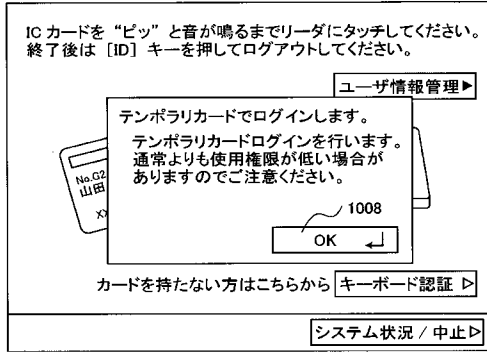
【図 20】



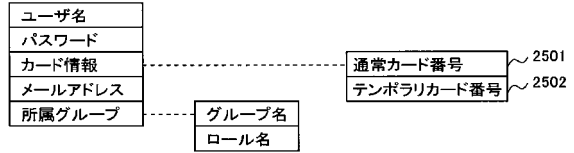
【図 22】



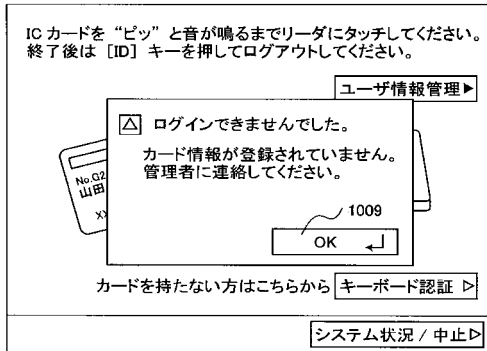
【図 2 3】



【図 2 5】



【図 2 4】



フロントページの続き

(51)Int.Cl.

B 4 1 J 29/00 (2006.01)

B 4 1 J 29/38 (2006.01)

F I

H 0 4 L 9/00 6 7 3 E

H 0 4 N 1/00 1 0 7 Z

B 4 1 J 29/00 Z

B 4 1 J 29/38 Z

(58)調査した分野(Int.Cl., DB名)

G 0 6 F 2 1 / 2 0

B 4 1 J 2 9 / 0 0

B 4 1 J 2 9 / 3 8

G 0 6 F 3 / 1 2

G 0 6 K 1 7 / 0 0

H 0 4 L 9 / 3 2

H 0 4 N 1 / 0 0