

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5299787号
(P5299787)

(45) 発行日 平成25年9月25日 (2013. 9. 25)

(24) 登録日 平成25年6月28日 (2013. 6. 28)

(51) Int. Cl.

F I

G O 6 F 21/31 (2013. 01)

G O 6 F 21/20 1 3 1 A

G O 6 F 21/34 (2013. 01)

G O 6 F 21/20 1 3 4

請求項の数 15 (全 37 頁)

(21) 出願番号 特願2009-296423 (P2009-296423)
 (22) 出願日 平成21年12月25日 (2009. 12. 25)
 (65) 公開番号 特開2010-231765 (P2010-231765A)
 (43) 公開日 平成22年10月14日 (2010. 10. 14)
 審査請求日 平成23年8月1日 (2011. 8. 1)
 (31) 優先権主張番号 特願2009-83413 (P2009-83413)
 (32) 優先日 平成21年3月5日 (2009. 3. 5)
 (33) 優先権主張国 日本国 (JP)

(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】 情報処理システムと認証サーバと、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】

読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバと、前記読取対象物を読み取る読取手段を備える装置と、情報処理装置とが通信可能に接続される情報処理システムであって、

前記読取手段を備える装置は、

前記読取手段によって読み取られた読取対象物の読取対象物識別情報を前記認証サーバへ送信する読取対象物識別情報送信手段と、

前記読取対象物識別情報送信手段によって前記読取対象物識別情報を送信することで、当該読取対象物識別情報を前記ユーザ情報記憶手段に登録するための登録キー情報又は前記読取対象物識別情報を前記ユーザ情報記憶手段から削除するための当該読取対象物識別情報に対応する削除キー情報を、前記認証サーバから受信するキー情報受信手段と、

前記キー情報受信手段によって受信した前記登録キー情報又は削除キー情報を出力するキー情報出力手段と

を備え、

前記認証サーバは、

前記読取対象物識別情報送信手段によって送信された読取対象物識別情報を受信する読取対象物識別情報受信手段と、

前記読取対象物識別情報受信手段によって受信した読取対象物識別情報が、前記ユーザ

10

20

情報記憶手段に登録されているか否かを判定する登録判定手段と、

前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記登録キー情報を、前記読取手段を備える装置に送信し、前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記削除キー情報を、前記読取手段を備える装置に送信するキー情報送信手段と、

前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報とを取得する情報取得手段と、

前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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登録手段と、

前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除手段と、

を備えることを特徴とする情報処理システム。

【請求項 2】

前記削除手段は、前記読取対象物が前記読取手段に所定時間読み取られた場合に、前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報をユーザ情報記憶手段から削除することを特徴とする請求項 1 に記載の情報処理システム。

【請求項 3】

前記認証サーバは、

前記キー情報送信手段で送信したキー情報の有効期間の情報を用いて、前記情報取得手段によって取得した登録キー情報が有効であるか否かを判定する有効性判定手段とを更に備え、

前記登録手段は、前記有効性判定手段で、前記情報取得手段によって取得された前記登録キー情報が有効であると判定される場合に、前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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ことを特徴とする請求項 1 又は 2 に記載の情報処理システム。

【請求項 4】

前記認証サーバは、

前記有効性判定手段で、前記情報取得手段によって取得された登録キー情報が有効であると判定される場合に、登録成功を示す登録成功結果情報を送信し、前記情報取得手段によって取得された登録キー情報が有効でないとして判定される場合に、登録失敗を示す登録失敗結果情報を送信する登録結果情報送信手段とを更に備えることを特徴とする請求項 3 に記載の情報処理システム。

【請求項 5】

前記有効性判定手段は、更に前記情報取得手段によって取得された削除キー情報が有効であるか否かを判定し、

前記削除手段は、前記有効性判定手段で、前記情報取得手段によって取得された削除キー情報が有効であると判定される場合に、前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除することを特徴とする請求項 3 又は 4 に記載の情報処理システム。

【請求項 6】

前記認証サーバは、

前記有効性判定手段で、前記情報取得手段によって取得された削除キー情報が有効であると判定される場合に、削除成功を示す削除成功結果情報を送信し、前記情報取得手段によって取得された削除キー情報が有効でないとして判定される場合に、削除失敗を示す削除失敗結果情報を送信する削除結果情報送信手段とを更に備えることを特徴とする請求項 5 に記載の情報処理システム。

【請求項 7】

前記登録キー情報及び前記削除キー情報は、前記読取対象物識別情報受信手段で前記読取対象物識別情報を受信した場合に発行されるキー情報であって、

前記登録手段は、前記情報取得手段によって取得された前記キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別情報とを対応付けて前記ユーザ情報記憶手段に登録し、

前記削除手段は、前記情報取得手段によって取得された前記キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除することを特徴とする請求項1乃至6のいずれか1項に記載の情報処理システム。

【請求項8】

前記キー情報出力手段は、前記読取手段を備える装置の表示手段に前記登録キー情報又は削除キー情報を表示させるか、前記読取手段を備える装置の印刷手段によって前記登録キー情報又は削除キー情報を印刷することを特徴とする請求項1乃至7のいずれか1項に記載の情報処理システム。

【請求項9】

前記情報処理装置は、

前記キー情報出力手段によって出力された登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報の入力を受け付ける入力受付手段と、

前記入力受付手段によって入力を受け付けた登録キー情報又は削除キー情報とユーザ識別情報とを前記認証サーバに送信する情報送信手段と
を備えることを特徴とする請求項1乃至8のいずれか1項に記載の情報処理システム。

【請求項10】

前記情報送信手段は、前記入力受付手段で入力を受け付けたユーザ識別情報を、前記読取手段を備える装置を介して前記認証サーバに送信し、また、前記認証サーバに送信されたユーザ識別情報による認証が行われた場合に、前記登録キー情報又は削除キー情報を、前記読取手段を備える装置を介して前記認証サーバに送信することを特徴とする請求項9に記載の情報処理システム。

【請求項11】

読取対象物を読み取る読取手段を備える装置と、情報処理装置と通信可能に接続され、前記読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバであって、

前記読取手段を備える装置から送信された読取対象物識別情報を受信する読取対象物識別情報受信手段と、

前記読取対象物識別情報受信手段によって受信した読取対象物識別情報が、前記ユーザ情報記憶手段に登録されているか否かを判定する登録判定手段と、

前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記読取対象物識別情報を前記ユーザ情報記憶手段に登録するための当該読取対象物識別情報に対応する登録キー情報を前記読取手段を備える装置に送信し、前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記読取対象物識別情報を前記ユーザ情報記憶手段から削除するための削除キー情報を、前記読取手段を備える装置に送信するキー情報送信手段と、

前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報とを取得する情報取得手段と、

前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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登録手段と、

前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除手段と、

を備えることを特徴とする認証サーバ。

10

20

30

40

50

【請求項 1 2】

読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバと、前記読取対象物を読み取る読取手段を備える装置と、情報処理装置とが通信可能に接続される情報処理システムにおける処理方法であって、

前記読取手段を備える装置の送信手段が、前記読取手段によって読み取られた読取対象物の読取対象物識別情報を前記認証サーバへ送信する読取対象物識別情報送信ステップと

、
前記読取手段を備える装置のキー情報受信手段が、前記読取対象物識別情報送信ステップによって前記読取対象物識別情報を送信することで、当該読取対象物識別情報を前記ユーザ情報記憶手段に登録するための登録キー情報又は前記読取対象物識別情報を前記ユーザ情報記憶手段から削除するための当該読取対象物識別情報に対応する削除キー情報を、前記認証サーバから受信するキー情報受信ステップと、

前記読取手段を備える装置のキー情報出力手段が、前記キー情報受信ステップによって受信した前記登録キー情報又は削除キー情報を出力するキー情報出力ステップと、

前記認証サーバの読取対象物識別情報受信手段が、前記読取対象物識別情報送信ステップによって送信された読取対象物識別情報を受信する読取対象物識別情報受信ステップと

、
前記認証サーバの登録判定手段が、前記読取対象物識別情報受信ステップによって受信した読取対象物識別情報が、前記ユーザ情報記憶手段に登録されているか否かを判定する登録判定ステップと、

前記認証サーバのキー情報送信手段が、前記登録判定ステップによって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記登録キー情報を、前記読取手段を備える装置に送信し、前記登録判定ステップによって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記削除キー情報を、前記読取手段を備える装置に送信するキー情報送信ステップと、

前記認証サーバの情報取得手段が、前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報とを取得する情報取得ステップと、

前記認証サーバの登録手段が、前記情報取得ステップによって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得ステップによって取得されたユーザ識別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登録ステップと、

前記認証サーバの削除手段が、前記情報取得ステップによって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除ステップと、
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 3】

読取対象物を読み取る読取手段を備える装置と、情報処理装置と通信可能に接続され、前記読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバの処理方法であって、

読取対象物識別情報受信手段が、前記読取手段を備える装置から送信された読取対象物識別情報を受信する読取対象物識別情報受信ステップと、

登録判定手段が、前記読取対象物識別情報受信ステップによって受信した読取対象物識別情報が、前記ユーザ情報記憶手段に登録されているか否かを判定する登録判定ステップと、

キー情報送信手段が、前記登録判定ステップによって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記読取対象物識別情報を前記ユーザ情報記憶手段に登録するための当該読取対象物識別情報に対応する登録キー情報を前記読取手段を備える装置に送信し、前記登録判定ステップによって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記読取対象物

10

20

30

40

50

識別情報を前記ユーザ情報記憶手段から削除するための削除キー情報を、前記読取手段を備える装置に送信するキー情報送信ステップと、

情報取得手段が、前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報とを取得する情報取得ステップと、

登録手段が、前記情報取得ステップによって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得ステップによって取得されたユーザ識別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登録ステップと、

削除手段が、前記情報取得ステップによって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除ステップと、

を含むことを特徴とする認証サーバの処理方法。

【請求項 1 4】

読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバと、前記読取対象物を読み取る読取手段を備える装置と、情報処理装置とが通信可能に接続される情報処理システムで実行可能なプログラムであって、

前記読取手段を備える装置を、

前記読取手段によって読み取られた読取対象物の読取対象物識別情報を前記認証サーバへ送信する読取対象物識別情報送信手段と、

前記読取対象物識別情報送信手段によって前記読取対象物識別情報を送信することで、当該読取対象物識別情報を前記ユーザ情報記憶手段に登録するための登録キー情報又は前記読取対象物識別情報を前記ユーザ情報記憶手段から削除するための当該読取対象物識別情報に対応する削除キー情報を、前記認証サーバから受信するキー情報受信手段と、

前記キー情報受信手段によって受信した前記登録キー情報又は削除キー情報を出力するキー情報出力手段として機能させ、

前記認証サーバを、

前記読取対象物識別情報送信手段によって送信された読取対象物識別情報を受信する読取対象物識別情報受信手段と、

前記読取対象物識別情報受信手段によって受信した読取対象物識別情報が、前記ユーザ情報記憶手段に登録されているか否かを判定する登録判定手段と、

前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記登録キー情報を、前記読取手段を備える装置に送信し、前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記削除キー情報を、前記読取手段を備える装置に送信するキー情報送信手段と、

前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報とを取得する情報取得手段と、

前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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登録手段と、

前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除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 5】

読取対象物を読み取る読取手段を備える装置と、情報処理装置と通信可能に接続され、前記読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバで実行可能なプログラムであって、

前記認証サーバを、

前記読取手段を備える装置から送信された読取対象物識別情報を受信する読取対象物識

10

20

30

40

50

別情報受信手段と、

前記読取対象物識別情報受信手段によって受信した読取対象物識別情報が、前記ユーザ情報記憶手段に登録されているか否かを判定する登録判定手段と、

前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記読取対象物識別情報を前記ユーザ情報記憶手段に登録するための当該読取対象物識別情報に対応する登録キー情報を前記読取手段を備える装置に送信し、前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記読取対象物識別情報を前記ユーザ情報記憶手段から削除するための削除キー情報を、前記読取手段を備える装置に送信するキー情報送信手段と、

10

前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報とを取得する情報取得手段と、

前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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登録手段と、

前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除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】

20

【0001】

本発明は、ユーザ情報の入力が困難であり読取対象物から認証情報を読み取る機能を備える装置を用いて、認証サーバにおいて新規の読取対象物の識別情報を容易に登録、及び削除可能とする情報処理システムと認証サーバ、その処理方法およびプログラムに関する。

【背景技術】

【0002】

従来印刷を行う場合に、クライアント端末に備えるプリンタドライバを介して印刷データを印刷機器に出力すると、印刷装置で受信した印刷データをタイムリーに出力することが行われていた。

30

【0003】

しかしながら、出力された紙媒体が放置されることによって情報漏洩につながることから、近年においてはクライアント端末から出力された印刷データをサーバ上もしくは印刷装置内に一時蓄積し、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要求を行った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。

【0004】

ブルプリントシステムの多くは、ユーザ自身が出力した印刷データに対して印刷要求を行うようにするために、ユーザを特定するＩＣカードを用いた認証を行っている。

【0005】

40

ＩＣカードを用いることにより、ユーザは簡易に自身が出力した印刷データをブルプリントすることが可能になったが、一方でＩＣカードやユーザ情報を管理する管理者は、新規入社した社員などに対して付与したＩＣカードのカード情報（例えば、製造番号）をＩＣカードを用いてユーザ認証する認証サーバを都度更新しなければならず、管理上の負荷が多かった。

【0006】

このような負荷を軽減するために、認証サーバに登録されていないＩＣカードがかざされた場合、印刷装置からＩＣカードのカード情報（例えば、製造番号）を新規に認証サーバに登録する技術が公開されている（特許文献１）。

【先行技術文献】

50

【特許文献】

【0007】

【特許文献1】特開2008-181491号公報

【発明の概要】

【発明が解決しようとする課題】

【0008】

しかしながら、特許文献1ではカード情報登録時に、登録ユーザを特定するため、複合機の操作部（ユーザインタフェース）より当該ICカードを用いるユーザのユーザ情報（ユーザ名、パスワード等）を入力する必要があった。

【0009】

そのため、複合機のようにタッチパネルやテンキーを用いてユーザ情報の入力可能な操作部（ユーザインタフェース）を持たないプリンタではユーザ情報の入力できないため、カード情報を認証サーバに登録することができなかった。

【0010】

特に、ブルブリントシステムなどと連携する場合、社員番号などのユーザ名（ネットワークへのログイン名）を用いて、自分の出力した印刷データを取得するため、カード情報からユーザ名を特定する必要があるため、ユーザ名とカード情報を対応付けて管理する必要がある。

【0011】

ここで、各ユーザが使用しているクライアント端末にカードリーダを接続し、認証サーバに対して登録要求を送信するという仕組みも考えられるがカードリーダの管理を考えると、現実的な運用には向かなかった。

【0012】

そこで、本発明の目的は、ユーザ情報の入力が困難であり読取対象物から認証情報を読み取る機能を備える装置を用いて、認証サーバにおいて新規の認証情報（例えば、ICカードなどのカード番号）とユーザ情報（例えば、ユーザ名）とを対応付けて登録させ、また、既に登録済の認証情報の削除をすることで管理者の負担を軽減することができ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】

【0013】

前述した目的を達成するために、本発明の情報処理システムは、読取対象物を識別するための読取対象物識別情報と、当該読取対象物を所有するユーザのユーザ識別情報とを対応付けて記憶するユーザ情報記憶手段を備える認証サーバと、前記読取対象物を読み取る読取手段を備える装置と、情報処理装置とが通信可能に接続される情報処理システムであって、前記読取手段を備える装置は、前記読取手段によって読み取られた読取対象物の読取対象物識別情報を前記認証サーバへ送信する読取対象物識別情報送信手段と、前記読取対象物識別情報送信手段によって前記読取対象物識別情報を送信することで、当該読取対象物識別情報を前記ユーザ情報記憶手段に登録するための登録キー情報又は前記読取対象物識別情報を前記ユーザ情報記憶手段から削除するための当該読取対象物識別情報に対応する削除キー情報を、前記認証サーバから受信するキー情報受信手段と、前記キー情報受信手段によって受信した前記登録キー情報又は削除キー情報を出力するキー情報出力手段とを備え、前記認証サーバは、前記読取対象物識別情報送信手段によって送信された読取対象物識別情報を受信する読取対象物識別情報受信手段と、前記読取対象物識別情報受信手段によって受信した読取対象物識別情報が、前記ユーザ情報記憶手段に登録されているか否かを判定する登録判定手段と、前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていないと判定された場合に、前記登録キー情報を、前記読取手段を備える装置に送信し、前記登録判定手段によって前記ユーザ情報記憶手段に前記読取対象物識別情報が登録されていると判定された場合に、前記削除キー情報を、前記読取手段を備える装置に送信するキー情報送信手段と、前記情報処理装置から入力された前記登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識

10

20

30

40

50

別情報とを取得する情報取得手段と、前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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登録手段と、前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除する削除手段と、を備えることを特徴とする。

【0014】

また、前記削除手段は、前記読取対象物が前記読取手段に所定時間読み取られた場合に、前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報をユーザ情報記憶手段から削除することを特徴とする。

【0015】

また、前記認証サーバは、前記キー情報送信手段で送信したキー情報の有効期間の情報を用いて、前記情報取得手段によって取得した登録キー情報が有効であるか否かを判定する有効性判定手段とを更に備え、前記登録手段は、前記有効性判定手段で、前記情報取得手段によって取得された前記登録キー情報が有効であると判定される場合に、前記情報取得手段によって取得された登録キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別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ことを特徴とする。

【0016】

また、前記認証サーバは、前記有効性判定手段で、前記情報取得手段によって取得された登録キー情報が有効であると判定される場合に、登録成功を示す登録成功結果情報を送信し、前記情報取得手段によって取得された登録キー情報が有効でないと判定される場合に、登録失敗を示す登録失敗結果情報を送信する登録結果情報送信手段とを更に備えることを特徴とする。

【0017】

また、前記有効性判定手段は、更に前記情報取得手段によって取得された削除キー情報が有効であるか否かを判定し、前記削除手段は、前記有効性判定手段で、前記情報取得手段によって取得された削除キー情報が有効であると判定される場合に、前記情報取得手段によって取得された削除キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除することを特徴とする。

【0018】

また、前記認証サーバは、前記有効性判定手段で、前記情報取得手段によって取得された削除キー情報が有効であると判定される場合に、削除成功を示す削除成功結果情報を送信し、前記情報取得手段によって取得された削除キー情報が有効でないと判定される場合に、削除失敗を示す削除失敗結果情報を送信する削除結果情報送信手段とを更に備えることを特徴とする。

【0019】

また、前記登録キー情報及び前記削除キー情報は、前記読取対象物識別情報受信手段で前記読取対象物識別情報を受信した場合に発行されるキー情報であって、前記登録手段は、前記情報取得手段によって取得された前記キー情報に対応する読取対象物識別情報と、前記情報取得手段によって取得されたユーザ識別情報とを対応付けて前記ユーザ情報記憶手段に登録し、前記削除手段は、前記情報取得手段によって取得された前記キー情報に対応する読取対象物識別情報を前記ユーザ情報記憶手段から削除することを特徴とする。

【0020】

また、前記キー情報出力手段は、前記読取手段を備える装置の表示手段に前記登録キー情報又は削除キー情報を表示させるか、前記読取手段を備える装置の印刷手段によって前記登録キー情報又は削除キー情報を印刷することを特徴とし、更に、前記情報処理装置は、前記キー情報出力手段によって出力された登録キー情報又は削除キー情報と、前記読取対象物を所有するユーザのユーザ識別情報の入力を受け付ける入力受付手段と、前記入力受付手段によって入力を受け付けた登録キー情報又は削除キー情報とユーザ識別情報とを前記認証サーバに送信する情報送信手段とを備えることを特徴とする。

10

20

30

40

50

【 0 0 2 1 】

また、前記情報送信手段は、前記入力受付手段で入力を受け付けたユーザ識別情報を、前記読取手段を備える装置を介して前記認証サーバに送信し、また、前記認証サーバに送信されたユーザ識別情報による認証が行われた場合に、前記登録キー情報又は削除キー情報を、前記読取手段を備える装置を介して前記認証サーバに送信することを特徴とする。

【 発明の効果 】

【 0 0 2 2 】

本発明によれば、ユーザ情報の入力が困難であり読取対象物から認証情報を読み取る機能を備える装置を用いて、認証サーバにおいて新規の認証情報（例えば、ＩＣカードなどのカード番号）とユーザ情報（例えば、ユーザ名）とを対応付けて登録させ、また、既に登録済の認証情報の削除をすることで管理者の負担を軽減することができる。

【 図面の簡単な説明 】

【 0 0 2 3 】

【図 1】本発明の実施形態にかかるシステムの構成の一例を示すシステム構成図である。

【図 2】本発明の実施形態にかかるクライアントＰＣ１００と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を示すブロック図である。

【図 3】本発明の実施形態にかかるプリンタ３００のハードウェア構成の一例を示すブロック図である。

【図 4】本発明の実施形態にかかるプリンタ３００に備えるＮＩＣ６００のハードウェア構成の一例を示すブロック図である。

【図 5】本発明の実施形態にかかるクライアントＰＣ１００、ＩＣカード認証サーバ２００、プリンタ３００の機能を示すブロック図である。

【図 6】本発明の実施形態にかかる情報処理システムのカード情報認証処理の一例を示すフローチャートである。

【図 7】本発明の実施形態にかかる情報処理システムのカード情報登録処理の一例を示すフローチャートである。

【図 8】本発明の実施形態にかかる情報処理システムのカード情報登録処理の一例を示すフローチャートである。

【図 9】本発明の実施形態にかかる情報処理システムのカード情報登録処理の一例を示すフローチャートである。

【図 10】本発明の実施形態にかかる情報処理システムのアクセスキーリスト削除処理の一例を示すフローチャートである。

【図 11】ＩＣカード認証サーバ２００の外部メモリ２０１１にて管理される登録モード設定ファイルの一例を示す図である。

【図 12】ＩＣカード認証サーバ２００の外部メモリ２０１１管理されるアクセスキーリストの一例を示す図である。

【図 13】ＩＣカード認証サーバ２００の外部メモリ２０１１にて管理される認証に用いられるユーザテーブルの一例を示す図である。

【図 14】クライアントＰＣ１００のＣＲＴ２０１０で表示する認証ページの一例を示す図である。

【図 15】クライアントＰＣ１００のＣＲＴ２０１０で表示する認証エラーページの一例を示す図である。

【図 16】クライアントＰＣ１００のＣＲＴ２０１０で表示するアクセスキー入力ページの一例を示す図である。

【図 17】クライアントＰＣ１００のＣＲＴ２０１０で表示する登録成功ページの一例を示す図である。

【図 18】クライアントＰＣ１００のＣＲＴ２０１０で表示する登録失敗ページの一例を示す図である。

【図 19】本発明の実施形態２にかかる情報処理システムのカード情報削除処理の一例を示すフローチャートである。

10

20

30

40

50

【図 2 0】本発明の実施形態 2 にかかる情報処理システムのカード情報削除処理の一例を示すフローチャートである。

【図 2 1】本発明の実施形態 2 にかかる情報処理システムのカード情報削除処理の一例を示すフローチャートである。

【図 2 2】IC カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 にて管理される削除モード設定ファイルの一例を示す図である。

【図 2 3】IC カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 管理されるアクセスキーリストの一例を示す図である。

【図 2 4】クライアント PC 1 0 0 の CRT 2 0 1 0 で表示するアクセスキー入力ページの一例を示す図である。

10

【発明を実施するための形態】

【 0 0 2 4 】

〔実施形態 1〕

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。

【 0 0 2 5 】

図 1 は本発明のプリンタ 3 0 0、カードリーダー 4 0 0、クライアント PC 1 0 0 および IC カード認証サーバ 2 0 0 を用いたセキュアプリントシステムの構成の一例を示すシステム構成図である。

【 0 0 2 6 】

なお、不図示ではあるが、本システムに印刷ジョブを格納するサーバや、プリンタ自体に印刷ジョブを格納するマストレージを装着することにより、様々なタイプのセキュアプリントシステム（蓄積印刷）が利用可能となる。

20

【 0 0 2 7 】

プリンタ 3 0 0（画像形成装置）、カードリーダー 4 0 0（読取装置）、クライアント PC 1 0 0（情報処理装置）および IC カード認証サーバ 2 0 0 は LAN（Local Area Network）5 0 0 を介して通信可能に接続されている。なお、クライアント PC 1 0 0 やプリンタ 3 0 0 は 1 又は複数の LAN 5 0 0 上に接続する構成になっている。

【 0 0 2 8 】

クライアント PC 1 0 0 は、クライアント PC に記憶されている Web ブラウザから IC カードのカード情報を登録可能な情報処理装置である。また、プリンタドライバを記憶しており、不図示のプリントサーバやマストレージに印刷データを蓄積させることが可能な情報処理装置である。

30

【 0 0 2 9 】

IC カード認証サーバ 2 0 0 は、ユーザの使用する IC カード番号（カード情報）とユーザ名などの認証するために用いられるユーザ情報を保持し、IC カード番号からユーザ名を検索することが可能な情報処理装置である。

【 0 0 3 0 】

プリンタ 3 0 0 は NIC 6 0 0 を備えており、また NIC 6 0 0 はカードリーダー 4 0 0 と接続されている。プリンタ 3 0 0 は、カードリーダー 4 0 0 で読み取った IC カード番号を IC カード認証サーバ 2 0 0 に問い合わせを行い、認証を行わせることができる装置である。また、IC カード認証サーバ 2 0 0 で認証されたことを受けて、不図示のプリントサーバやマストレージから、認証されたユーザに対応する印刷データを受信し、紙出力することが可能な装置である。

40

【 0 0 3 1 】

以下、図 2 を用いて、図 1 に示したクライアント PC 1 0 0、IC カード認証サーバ 2 0 0 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。

【 0 0 3 2 】

図 2 において、2 0 0 1 は CPU で、システムバス 2 0 0 4 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、ROM 2 0 0 3 あるいは外部メモリ 2 0 1 1 に

50

は、CPU 2001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各種プログラム等が記憶されている。

【0033】

2002はRAMで、CPU 2001の主メモリ、ワークエリア等として機能する。CPU 2001は、処理の実行に際して必要なプログラム等をROM 2003あるいは外部メモリ 2011からRAM 2002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。

【0034】

また、2005は入力コントローラで、キーボード (KB) 2009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。2006はビデオコントローラで、CRTディスプレイ (CRT) 2010等の表示器への表示を制御する。なお、図2では、CRT 2010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ユーザが使用するものである。

【0035】

2007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 2011へのアクセスを制御する。

【0036】

2008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LAN 500) 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。

【0037】

なお、CPU 2001は、例えばRAM 2002内の表示情報用領域へアウトラインフォントの展開 (ラスターライズ) 処理を実行することにより、CRT 2010上での表示を可能としている。また、CPU 2001は、CRT 2010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。

【0038】

ハードウェア上で動作する各種プログラムは、外部メモリ 2011に記録されており、必要に応じてRAM 2002にロードされることによりCPU 2001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 2011に格納されている。

【0039】

以下、図3を用いて、図1に示したプリンタ300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。

【0040】

入力部3000は、本プリンタ300とNIC 600を接続するものであり、NIC 600とのデータ通信を司るものである。

【0041】

CPU 3001は、本プリンタ300の全体的な制御を司るもので、印刷処理部3003の印刷制御や表示部3007での表示制御を行う。

【0042】

操作部3002は、本印刷装置に直接ユーザが触れる際のI/Fを提供するもので、電源のON/OFFや、カーソルキーなどのユーザが操作可能なハードキーなどがある。

【0043】

印刷処理部3003は、入力部3000で受信したコマンドの解析、および印刷ジョブ (PDL) の解析等を行うものである。

10

20

30

40

50

【 0 0 4 4 】

記憶部 3 0 0 4 は、本印刷装置を動作させるための不図示の R O M (R e a d O n l y M e m o r y)、不図示の R A M (R a m d o m A c c e s s M e m o r y)、不図示の二次記憶装置等からなる。R A M は使用制限のないデータ記憶領域であり、入力部 3 0 0 0 の受信バッファ、或いは印刷処理部 3 0 0 3 でのデータ展開等に使用される領域である。

【 0 0 4 5 】

出力部 3 0 0 5 は、入力部 3 0 0 0 を介して受信した印刷ジョブを、印刷処理部 3 0 0 3 で印刷可能なイメージ情報に展開されたものを紙に転写するものである。用紙カセット 3 0 0 6 は出力部 3 0 0 5 の処理に合わせて適切な用紙を供給する。

10

【 0 0 4 6 】

表示部 3 0 0 7 は、プリンタ 3 0 0 でのエラーメッセージや、印刷時の印刷ジョブ名などを表示する液晶ディスプレイである。この表示部は複合機とは異なり、最低限の情報を表示可能な表示部となっている。

【 0 0 4 7 】

N I C 6 0 0 は、ネットワークインタフェースカードであり、L A N 5 0 0 を介して他の機器から受信したデータを、N I C 6 0 0 が窓口となって受け取り、その後、不図示の N I C 内部のプログラムに渡したり、プリンタ 3 0 0 の入力部 3 0 0 0 に渡したりすることができ、N I C O S 9 0 0 が受信データの受け渡し制御を行うことが可能である。

【 0 0 4 8 】

以下、図 4 を用いて、図 3 に示した N I C 6 0 0 に適用可能なネットワークインタフェース装置のハードウェア構成について説明する。

20

【 0 0 4 9 】

図 4 において、C P U 4 0 0 1 は N I C の制御を司るものであり、内部で接続されている装置の制御を行う。また、R O M 4 0 0 7 あるいは内部メモリ 4 0 0 5 に記憶するプログラムを読み出し、実行する。或いは他の装置との通信などの制御を行っている。

【 0 0 5 0 】

R A M 4 0 0 2 は、C P U 4 0 0 1 の主メモリ、ワークエリア等として機能する。C P U 4 0 0 1 は、処理の実行に際して必要なプログラム等を R O M 4 0 0 7 あるいは内部メモリ 4 0 0 5 から R A M 4 0 0 2 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。

30

【 0 0 5 1 】

通信 I / F コントローラ 4 0 0 3 は、ネットワーク（例えば、図 1 に示した L A N 5 0 0 ）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、T C P / I P や U D P などの通信プロトコルを用いた通信が可能である。

【 0 0 5 2 】

U S B I / F コントローラ 4 0 0 4 は、カードリーダー 4 0 0 などの U S B 機器と N I C 6 0 0 を接続・通信するものであり、U S B の通信制御処理を実行する。

【 0 0 5 3 】

内部メモリ 4 0 0 5 は、N I C 6 0 0 を制御するプログラム（O S ）が搭載されており、また該 O S 上で動作する、アプリケーションプログラム、およびその設定情報を記憶する領域である。

40

【 0 0 5 4 】

4 0 0 6 はメモリコントローラで、各種のアプリケーション、各種データ等を記憶する内部メモリ 4 0 0 5 へのアクセスを制御する。

【 0 0 5 5 】

R O M 4 0 0 7 は、読み出し専用の半導体メモリであり、電源を切っても内容が消えないことから、ブートプログラムが格納される。

【 0 0 5 6 】

50

機器 I / F コントローラ 4 0 0 8 は、N I C 6 0 0 とプリンタ 3 0 0 を接続・通信するものである。

【 0 0 5 7 】

尚、N I C 6 0 0 に適用可能なネットワークインタフェース装置は C P U 4 0 0 1 や R A M 4 0 0 2 等を用いて演算処理するため、情報処理装置（コンピュータ）としても動作する。

【 0 0 5 8 】

次に、本実施形態に係るカード情報登録システムの機能構成について説明する。図 5 は、本実施形態に係るカード情報登録システムの機能構成を示すブロック図である。

【 0 0 5 9 】

本発明の実施形態に係るシステムは、I C カード認証サーバ 2 0 0 とクライアント P C 1 0 0 とプリンタ 3 0 0 に接続された N I C 6 0 0 とが、双方向通信可能な所定の L A N 5 0 0 （通信媒体）を介して接続した構成となっている。また、N I C 6 0 0 には U S B 通信可能な所定の L A N 5 0 0 を介して、カードリーダー 4 0 0 が接続した構成となっている。

【 0 0 6 0 】

それぞれの機能間の動作フローに関しては後述するため、ここでは各種端末内に記載されている機能ブロック図の説明を記載する。

【 0 0 6 1 】

まず、クライアント P C 1 0 0 の機能構成について説明する。クライアント P C 1 0 0 は、アクセスキー入力部 1 5 0 とユーザ情報入力部 1 5 1 と登録部 1 5 2 を備えている。

【 0 0 6 2 】

アクセスキー入力部 1 5 0 は、クライアント P C 1 0 0 が備える W e b ブラウザを介してユーザが入力するプリンタ 3 0 0 で発行されたアクセスキーを受け付ける機能部である。

【 0 0 6 3 】

ユーザ情報入力部 1 5 1 は、クライアント P C 1 0 0 が備える W e b ブラウザを介してユーザが入力するユーザ名とパスワードを受け付ける機能部である。

【 0 0 6 4 】

登録部 1 5 2 は、ユーザ情報入力部 1 5 1 とアクセスキー入力部 1 5 0 で受け付けたユーザ名とアクセスキーをプリンタ 3 0 0 に送信することで I C カード認証サーバ 2 0 0 へカード情報を登録することができる機能部である。

【 0 0 6 5 】

次に、I C カード認証サーバ 2 0 0 の機能構成について説明する。I C カード認証サーバ 2 0 0 は、プリンタ通信部 2 5 0 と認証部 2 5 1 とユーザ情報管理部 2 5 2 を備えている。

【 0 0 6 6 】

I C カード認証サーバ上の認証部 2 5 1 は、プリンタ 3 0 0 の認証サーバ通信部 3 5 1 から認証要求を受け、I C カード認証サーバで管理されるユーザテーブル（図 1 3 ）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プリンタ 3 0 0 の認証サーバ通信部 3 5 1 へ返信する機能部である。

【 0 0 6 7 】

また、ユーザ情報管理部 2 5 2 は、認証要求を受けたカード情報（製造番号）が、認証サーバ上で管理されるユーザテーブル（図 1 3 ）に存在しない場合、一時的に当該カード番号に紐づいたアクセスキーを発行し、認証サーバ通信部 3 5 1 が認証要求を発信したプリンタ 3 0 0 の認証サーバ通信部 3 5 1 へ返信する機能部である。

【 0 0 6 8 】

なおアクセスキーは、I C カード認証サーバ 2 0 0 内で管理されるユニークなランダムキーであり、キー発行時間とともに I C カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 で

10

20

30

40

50

記憶管理される（図１２）。

【００６９】

次に、プリンタ３００の機能構成について説明する。プリンタ３００では、カードリーダー制御部３５０と認証サーバ通信部３５１と本体通信部３５２とＷｅｂ制御部３５３とＵＳＢ制御部３５４と印刷制御部３５５とを備えている。

【００７０】

プリンタ３００のカードリーダー４００制御部３５０は、カードリーダー４００にかざされたカード情報（製造番号）を取得する機能部である。

【００７１】

認証サーバ通信部３５１は、当該カード番号を用いて認証要求をＩＣカード認証サーバ２００へ送信し、ＩＣカード認証サーバ２００より返される認証結果、またはＩＣカード認証サーバ２００より発行されたアクセスキーを受信する機能部である。

10

【００７２】

また、Ｗｅｂ制御部３５３はクライアントＰＣ１００に送信する画面情報（ＨＴＭＬ等の形式）を管理し、クライアントＰＣ１００のＷｅｂブラウザからの要求に応じて、画面情報から送信する画面を生成し、生成された画面（図１４～図１８）を送信する機能部である。

【００７３】

また、本体通信部３５２は、プリンタ３００の表示部へアクセスキーを表示させたり、エラーメッセージを表示させる機能部である。またＵＳＢＩ／Ｆコントローラに対し、

20

ＵＳＢデバイスへの命令の送受信を行なう機能部である。

【００７４】

ＵＳＢ制御部３５４は、ＮＩＣ６００上のＵＳＢＩ／Ｆコントローラ４００４を経由して接続されたＮＩＣ６００に接続されたＵＳＢ機器との通信を行ない、ＵＳＢ機器の制御を行なう機能部である。本実施では、カードリーダー４００の制御を行なう。

【００７５】

印刷制御部３５５は、不図示のプリントサーバやマスメモリから印刷ジョブ受信する機能部であり、受信した印刷ジョブを印刷処理部に出力する機能部である。

【００７６】

次に、図６を用いて、本発明の実施形態における、カード情報登録処理について説明する。

30

【００７７】

なお、図６はカード情報認証処理の一例を示すフローチャートである。

【００７８】

まず、ステップＳ１００では、ＮＩＣ６００上の内部メモリ４００５に格納されたアプリケーションプログラムがＲＡＭ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。ＮＩＣ６００上のＣＰＵ４００１は、カードリーダー制御部３５０により、ＮＩＣＯＳ上のＵＳＢ制御部３５４に対してカード読み取り開始コマンドを送信する。

【００７９】

ＵＳＢ制御部３５４はこのコマンドをカードリーダー４００に送信する。すなわち、カードリーダー制御部３５０はカードリーダー４００に対してポーリング開始処理の指示コマンドを送る。

40

【００８０】

ステップＳ１０１では、ステップＳ１００でのポーリング開始処理の指示に従って、カードリーダー４００がポーリングを開始し、カード読み取り状態になる。

【００８１】

ステップＳ１０２では、カードリーダー４００は、ユーザによってユーザが所有するＩＣカード（読取対象物）がかざされたことを検知し、プリンタ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。

【００８２】

50

ステップS 1 0 3では、N I C 6 0 0上のC P U 4 0 0 1は、カードリーダー制御部3 5 0により、カード検知イベントを受信する。

【0083】

ステップS 1 0 4では、N I C 6 0 0上のC P U 4 0 0 1は、カードリーダー制御部3 5 0により、ステップS 1 0 3にて取得したカード検知イベントに含まれるI Cカードのカード情報（読取対象物識別情報）（例えば、カードの製造番号等）を取得する。

【0084】

なお、本実施例ではカードを用いた構成とするが、カードの代わりにユーザの生体情報（指紋、指静脈など）を用いた構成をとることも可能である。

【0085】

ステップS 1 0 5では、N I C 6 0 0上のC P U 4 0 0 1は、認証サーバ通信部3 5 1により、I Cカード認証サーバに対して認証要求コマンドを送信する（読取対象物識別情報送信）。認証要求コマンドにはステップS 1 0 4で取得したカード情報（読取対象物識別情報）が含まれる。

【0086】

ステップS 1 0 6では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、プリンタ通信部2 5 0により、プリンタ3 0 0から送られた認証要求コマンドを受信する（読取対象物識別情報受信）。

【0087】

ステップS 1 0 7では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、認証部2 5 1により、ステップS 1 0 6で取得した認証要求に含まれるカード情報（製造番号）が、I Cカード認証サーバ上で管理するユーザテーブル（図1 3）に存在するかを検索する。

【0088】

ステップS 1 0 8では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、認証部2 5 1により、ステップS 1 0 7の検索（認証）の結果を判断する。カード情報がユーザテーブル（図1 3）に存在する場合（認証が成功した場合）、すなわち当該I Cカードに対応するユーザがI Cカード認証サーバ2 0 0のユーザテーブル（図1 3）に登録されている場合はステップS 1 0 9へ進み、カード情報がユーザテーブル（図1 3）に存在しない場合（認証が失敗した場合）は、ステップS 1 1 0に進む。

【0089】

ステップS 1 0 9では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、認証部2 5 1によりステップS 1 0 7で検索されたカード情報に対応するユーザ名1 3 0 1を取得する。

【0090】

なお、本実施形態ではユーザ名1 3 0 1を取得するように構成したが、メールアドレスなども取得するように構成してもよい。

【0091】

ステップS 1 1 0では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、ユーザ情報管理部2 5 2により、I Cカード認証サーバの外部メモリ2 0 1 1に記憶する登録モード設定ファイル（図1 1）から設定情報を読み出す。

【0092】

ステップS 1 1 1では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、ユーザ情報管理部2 5 2により、ステップS 1 1 0で読み出された設定情報のうち、プリンタからのカード登録1 1 0 1を参照し、プリンタからのカード登録モードのO N / O F Fを判定する。登録モードがO Nである場合、ステップS 1 1 2に進み、O F Fである場合はステップS 1 1 5に進む。

【0093】

ステップS 1 1 2では、I Cカード認証サーバ2 0 0のC P U 2 0 0 1は、ユーザ情報管理部2 5 2により、I Cカード認証サーバの外部メモリ2 0 1 1に記憶する内アクセスキーリスト（図1 2）を読み出す。

10

20

30

40

50

【 0 0 9 4 】

ステップ S 1 1 3 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ランダムな値であり、かつアクセスキーリスト内に存在しない一意のアクセスキーを生成する。なお、カード情報がカードの製造番号などである場合には、カードの製造番号をアクセスキーとして用いることや、カードの製造番号からハッシュ値を取得し、このハッシュ値をアクセスキーとして用いてもよい。

【 0 0 9 5 】

また、ステップ S 1 1 3 で生成されたアクセスキーは、一意のアクセスキーを複数用意しており、アクセスキーリストで利用していないアクセスキーを前述の複数のアクセスキーから決定するような構成であってもよい。

10

【 0 0 9 6 】

つまり、アクセスキーとはカード情報をユーザ名（ユーザ識別情報）と対応付けて登録するために、登録するカード情報を特定するための登録キーである。

【 0 0 9 7 】

ステップ S 1 1 4 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 1 1 3 で生成したアクセスキー、ステップ S 1 0 6 で取得したカード情報（製造番号）、アクセスキーを生成した時の時間であるアクセスキー発行日時をアクセスキーリスト（図 1 2 ）のカード情報 1 2 0 1 ，アクセスキー 1 2 0 2 ，キー発行時間 1 2 0 3 に追加登録する（生成時間管理）。

20

【 0 0 9 8 】

ステップ S 1 1 5 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、プリンタ通信部 2 5 0 により、プリンタへ認証結果コマンドを送信する（認証結果送信）。認証が成功した場合には、認証結果コマンドに認証成功フラグ、及びステップ S 1 0 9 で取得したユーザ名が含まれ、認証が失敗した場合且つアクセスキーが生成された場合には、認証結果コマンドに認証失敗フラグ、及びステップ S 1 1 3 で生成されたアクセスキーが含まれる。

【 0 0 9 9 】

なお、ステップ S 1 1 1 で N O の場合（カード登録モード O F F の場合）には、アクセスキーが生成されないため認証結果コマンドにアクセスキーは含まず、認証失敗フラグが含まれる。

30

【 0 1 0 0 】

ステップ S 1 1 6 では、N I C 6 0 0 上の C P U 4 0 0 1 は、認証サーバ通信部 3 5 1 により、認証サーバから返された認証結果コマンドを受信する（認証結果受信）。

【 0 1 0 1 】

ステップ S 1 1 7 では、N I C 6 0 0 上の C P U 4 0 0 1 は、認証サーバ通信部 3 5 1 により、ステップ 1 1 6 で受信した認証結果コマンドを解析し認証成功フラグがある場合には、認証成功と判断し、プリンタ 3 0 0 の印刷機能を実行するためにプリンタ 3 0 0 へのログインを行う。ログインしたのち、ステップ S 1 1 8 に進む。認証失敗フラグがある場合には、認証失敗と判断し、ステップ S 1 1 9 に進む。

40

【 0 1 0 2 】

この認証結果コマンドの解析は、認証成功フラグある場合には有効なユーザ名が取得され、認証失敗フラグがある場合には有効なユーザ名が取得されないようになっている。つまり、認証結果によって有効なユーザであると判定される場合に、ステップ S 1 1 8 へ処理を移し、有効なユーザでないと判定される場合にステップ S 1 1 9 に処理を移す。

【 0 1 0 3 】

ステップ S 1 1 8 では、N I C 6 0 0 上の C P U 4 0 0 1 は、不図示のプリントサーバ通信部により、ステップ 1 1 7 で取得した認証結果コマンドに含まれるユーザ名を取得し、不図示のプリントサーバに対して当該ユーザ名に対応する印刷ジョブの印刷要求コマンドを送信する。

【 0 1 0 4 】

50

プリントサーバは印刷要求コマンドを受信し、当該ユーザ名に対応する印刷ジョブが存在する場合は、印刷要求のあったプリンタ300に対してLPR印刷を行う。そして、NIC600のCPU4001は、印刷制御部355で印刷ジョブを受け取り、印刷処理部3003へ印刷ジョブを出力する。

【0105】

ここで、不図示のプリントサーバはクライアントPC100からの印刷要求を受け付ける機能を保持する。クライアントPC100から印刷要求を受信した場合、印刷ジョブをプリントサーバのハードディスクに格納する。また、印刷ジョブ内部データを解析し、印刷を行ったユーザ名、ドキュメント名、印刷ジョブを特定する印刷ジョブ特定情報（例えばファイルパス）などの書誌情報データを管理する。

10

【0106】

プリンタ300からの印刷要求受信時に、この書誌情報データをユーザ名で検索し、当該ユーザ名が一致した印刷ジョブの印刷ジョブ特定情報を取得し、印刷ジョブ特定情報から印刷ジョブを取得してプリンタ300に対してLPR印刷を行う。

【0107】

ステップS119では、NIC600上のCPU4001は、認証サーバ通信部351により、ステップS117で取得した認証結果コマンドを解析し、コマンドにアクセスキー（読取対象物識別情報登録キー）が含まれるか否かを判断する。アクセスキーが含まれる場合、すなわち認証サーバがカード登録モードで動作している場合はステップS120に進み、アクセスキーが含まれない場合、すなわち認証サーバがカード登録モードで動作していない場合はステップS121に進む。

20

【0108】

ステップS120では、NIC600上のCPU4001は、本体通信部352により、プリンタ本体に対してアクセスキーの文字列を含む表示コマンドを発行する。プリンタ本体はこの表示コマンドを受け、プリンタの表示部にアクセスキー文字列を表示する。ここでは、表示部にステップS119で取得したアクセスキーを表示させる。

【0109】

本実施形態では、アクセスキーをユーザに通知するために表示部にアクセスキーを表示するという方法を用いたが、他の実施形態としてアクセスキー記載した紙を出力する仕組みを用いてもよい。この場合、ICカード認証サーバ200内でアクセスキーを含む印刷データを生成し、ICカード認証サーバ200に備えるプリンタドライバを介して、プリンタ300に印刷ジョブを送信する。そして、送信された印刷ジョブをプリンタ300は受信して、プリンタ300の出力部3005でアクセスキーが印字された紙を出力する。

30

【0110】

つまり、アクセスキーを出力することでユーザにアクセスキーを示すような構成であればよい。

【0111】

ステップS121では、NIC600上のCPU4001は、本体通信部352により、プリンタ本体に対して表示コマンドを発行する。プリンタ本体はこの表示コマンドを受け、プリンタの表示部に文字を表示する。ここでは、表示部に「ニンショウエラー」と表示させる。

40

【0112】

次に、図7～9を用いて、本発明の実施形態における、カード情報登録処理について説明する。

【0113】

なお、図7～9はカード情報登録処理の一例を示すフローチャートである。

【0114】

図7のステップS200では、クライアントPC100のCPU2001は、Webブラウザにより、プリンタ300のNIC600のWeb制御部353にHTTP通信を用いてアクセス要求を行う。

50

【 0 1 1 5 】

ステップ S 2 0 1 では、N I C 6 0 0 上の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、クライアント P C 1 0 0 からのアクセス要求を受信する。

【 0 1 1 6 】

ステップ S 2 0 2 では、N I C 6 0 0 の C P U 4 0 0 1 は、W e b 制御部 3 5 3 より、認証ページ (図 1 4) を生成する。

【 0 1 1 7 】

ステップ S 2 0 3 では、N I C 6 0 0 上の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、クライアント P C 1 0 0 に対してステップ 2 0 2 で生成した認証ページ (図 1 4) を送信する。

10

【 0 1 1 8 】

ステップ S 2 0 4 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、通信 I / F コン트롤ー 2 0 0 8 を介して、プリンタ 3 0 0 より送信された認証ページを受信する。

【 0 1 1 9 】

ステップ S 2 0 5 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、W e b ブラウザにより、ステップ S 2 0 4 で受信した認証ページ (図 1 4) を表示する。この認証ページを表示させユーザからのユーザ名とパスワードとを含むユーザ情報の入力を受け付ける。

【 0 1 2 0 】

ステップ S 2 0 6 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、W e b ブラウザにより、認証ページ上の認証ボタン 1 0 0 0 が押されるのを待機する。認証ボタン 1 0 0 0 が押されたことを検知した場合、ステップ S 2 0 7 に進む。

20

【 0 1 2 1 】

ステップ S 2 0 7 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、ユーザによって認証ボタン 1 0 0 0 が押下されることで、ユーザ情報入力部 1 5 1 により W e b ブラウザで入力されたユーザ名とパスワードとを含むユーザ情報の入力を受け付ける。そして、プリンタ 3 0 0 に認証要求コマンドと、ユーザ名とパスワードとを含むユーザ情報の H T T P リクエストを送信する。

【 0 1 2 2 】

ステップ S 2 0 8 では、N I C 6 0 0 の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、クライアント P C 1 0 0 からの H T T P リクエストコマンドを受信する。

30

【 0 1 2 3 】

ステップ S 2 0 9 では、N I C 6 0 0 の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、ステップ S 2 0 8 で受信 H T T P リクエストコマンドからユーザ名、パスワードを取得する。

【 0 1 2 4 】

ステップ S 2 1 0 では、N I C 6 0 0 の C P U 4 0 0 1 は、認証サーバ通信部 3 5 1 により、I C カード認証サーバ 2 0 0 に対して認証要求コマンドを送信する。認証要求コマンドにはステップ S 2 0 9 で取得したユーザ名、パスワードが含まれる。

【 0 1 2 5 】

ステップ S 2 1 1 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、プリンタ通信部 2 5 0 により、プリンタから送られたユーザ名、パスワードを含む認証要求コマンドを受信する。

40

【 0 1 2 6 】

ステップ S 2 1 2 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、認証部 2 5 1 により、ステップ S 2 1 1 で取得した認証要求に含まれるユーザ名が、I C カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 に記憶、管理するユーザテーブル (図 1 3) に存在し、且つステップ S 2 1 1 で取得したパスワードが当該ユーザテーブルのパスワードと合致するかを検索する。

【 0 1 2 7 】

ステップ S 2 1 3 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、認証部 2 5

50

1により、ステップS 2 1 2の認証結果を判断する。ステップS 2 1 2での検索の結果、認証要求に含まれるユーザ名とパスワードがユーザテーブル(図13)に存在する場合、すなわち当該ユーザがサーバに登録されている場合はステップS 2 1 4へ進み、ユーザ名とパスワードがユーザテーブルに存在しない場合はステップS 2 1 6に進む。

【0128】

ステップS 2 1 4では、ICカード認証サーバ200のCPU2001は、認証部251によりステップS 2 1 3で一致したユーザのユーザ名1301を取得する。なお、本実施形態ではユーザ名1301を取得するように構成したが、メールアドレスなども取得するように構成してもよい。

【0129】

ステップS 2 1 5では、ICカード認証サーバ200のCPU2001は、プリンタ通信部250により、プリンタ300へ認証結果コマンドを送信する。認証結果コマンドには認証成功を示す認証結果フラグ、ステップS 2 1 4で取得した少なくともユーザ名を含むユーザ情報が含まれる。

【0130】

ステップS 2 1 6では、ICカード認証サーバ200のCPU2001は、プリンタ通信部250により、プリンタへ認証結果コマンドを送信する。認証結果コマンドには認証失敗を示す認証結果フラグが含まれる。

【0131】

ステップS 2 1 7では、NIC600上のCPU4001は、認証サーバ通信部351により、ICカード認証サーバ200から返された認証結果コマンドを受信する。

【0132】

図8のステップS 2 1 8では、NIC600上のCPU4001は、認証サーバ通信部351により、ステップS 2 1 7で受信した認証結果コマンドを解析する。認証結果コマンドに認証成功を示すフラグを含む場合には、認証に成功したと判定しステップS 2 2 4に進み、認証結果コマンドに認証失敗を示すフラグを含む場合には認証に失敗した場合はステップS 2 1 9に進む。

【0133】

ステップS 2 1 9では、NIC600上のCPU4001は、Web制御部353により、認証エラーページ(図15)を生成する。

【0134】

ステップS 2 2 0では、NIC600上のCPU4001は、Web制御部353により、クライアントPC100に対してステップS 2 1 9で生成した認証エラーページ(図15)を送信する。

【0135】

ステップS 2 2 1では、クライアントPC100のCPU2001は、通信I/Fコントローラ2008を介してプリンタ300より返されたHTTP通信によって、認証エラーページ(図15)レスポンスコマンドを受信する。

【0136】

ステップS 2 2 2では、クライアントPC100のCPU2001は、クライアントPC100に備えるWebブラウザにより、ステップS 2 2 1で受信した認証エラーページ(図15)を表示する。

【0137】

ステップS 2 2 3では、戻るボタン1004がユーザによって押下されたか否かを検知して、ユーザによって押下された場合には再認証すると判定し、ステップS 2 0 5へ処理を移し、ステップS 2 0 4で受信した認証ページを表示させる。また、終了ボタン1005が押下されたことを検知した場合には、処理を終了とする。本実施形態では、認証エラーページを表示すると処理を終了する構成としたが、

【0138】

ステップS 2 2 4では、NIC600上のCPU4001は、Web制御部353によ

10

20

30

40

50

り、アクセスキー入力ページ（図16）を生成する。

【0139】

ステップS225では、NIC600上のCPU4001は、Web制御部353により、クライアントPC100に対してステップS223で生成したHTTP通信によって、アクセスキー入力ページ（図16）を送信する。

【0140】

ステップS226では、クライアントPC100のCPU2001は、通信I/Fコントローラ2008を介して、プリンタ300よりHTTP通信によって、アクセスキー入力ページを受信する。

【0141】

ステップS227では、クライアントPC100のCPU2001は、クライアントPC100に備えるWebブラウザにより、ステップS225で受信したアクセスキー入力ページ（図16）をCRT2010に表示する。

【0142】

ステップS228では、クライアントPC100のCPU2001は、Webブラウザにより、アクセスキー入力ページ上の登録ボタン1002が押されるのを待機する。登録ボタン1002が押されたことを検知した場合、ステップS229に進む。

【0143】

ステップS229では、クライアントPC100のCPU2001は、ユーザによって登録ボタン1002が押下されることで、アクセスキー入力部150によりWebブラウザで入力されたアクセスキーの入力を受け付ける。にそして、登録部152により、受け付けたアクセスキーを含むHTTPリクエストコマンドをプリンタ300へ送信する。

【0144】

ステップS230では、NIC600上のCPU4001は、Web制御部により、クライアントPC100からのアクセスキーを含むHTTPリクエストコマンドを受信する。

【0145】

ステップS231では、NIC600上のCPU4001は、Web制御部353により、ステップS230で取得したHTTPリクエストコマンドを解析し、アクセスキーを取得する。

【0146】

ステップS232では、NIC600上のCPU4001は、認証サーバ通信部351により、ICカード認証サーバ200に対してカード情報登録要求コマンドを送信する。カード情報登録認証要求コマンドにはステップ231で取得したアクセスキーが含まれる。

【0147】

ステップS233では、ICカード認証サーバ200のCPU2001は、プリンタ通信部250により、プリンタから送られたアクセスキーを含むカード情報登録要求コマンドを受信する。

【0148】

ステップS234では、ICカード認証サーバ200のCPU2001は、ユーザ情報管理部252により、ステップ233で取得したカード情報登録要求に含まれるアクセスキーを取得する。また、ステップ214で取得した当該ユーザのユーザ名を取得する（登録情報取得）。

【0149】

なお、本実施形態では、ステップS214で取得したユーザ名をRAM2002に保持しておき、このユーザ名による通信を継続することによって、ステップS234でユーザ名を取得するように構成したが、ステップS232で、アクセスキーとステップS217で受信したユーザ名を含むカード情報登録認証要求コマンドを送信して、このカード情報登録認証要求コマンドに含まれるユーザ名を取得するように構成することも可能である。

10

20

30

40

50

【 0 1 5 0 】

ステップ S 2 3 5 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、 I C カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 内で保持するアクセスキーリスト (図 1 2) を取得する。

【 0 1 5 1 】

図 9 のステップ S 2 3 6 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 5 で取得したアクセスキーリスト (図 1 2) 内に、ステップ S 2 3 4 で取得したアクセスキーが含まれているか検索する。アクセスキーが含まれている場合はステップ S 2 3 7 に進み、含まれていない場合はステップ S 2 4 6 へ進む。

10

【 0 1 5 2 】

ステップ S 2 3 7 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 でアクセスキー 1 2 0 2 を検索し、ステップ S 2 3 4 で取得したアクセスキーと一致したアクセスキーに対応しての該当アクセスキーリストに記憶されているに含まれるキー発行時間 1 2 0 3 を取得する。

【 0 1 5 3 】

ステップ S 2 3 8 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、 I C カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 に保持する登録モード設定ファイル (図 1 1) を読み出す。

【 0 1 5 4 】

20

ステップ S 2 3 9 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 8 で読み出した登録モード設定ファイル内に記載されたアクセスキー有効期間 1 1 0 2 (所定時間) を取得する。

【 0 1 5 5 】

ステップ S 2 4 0 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 7 取得したキー発行時間と I C カード認証サーバ 2 0 0 で管理しているシステムの現在時刻 (年月日時分秒) と比較し、時間差異がステップ S 2 3 9 で取得したアクセスキー有効期間内 (所定時間内) であればステップ S 2 4 1 に進み、期間外 (期間を超えている) であればステップ S 2 4 5 に進む。 (時間判定)

【 0 1 5 6 】

30

ステップ S 2 4 1 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 で取得したアクセスキーに紐づいたカード情報 1 2 0 1 (例えば、製造番号) を取得する。

【 0 1 5 7 】

ステップ S 2 4 2 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ユーザテーブル (図 1 3) のステップ S 2 1 4 (または、ステップ S 2 3 4) で取得したユーザ名に対応するカード情報 1 3 0 2 にステップ S 2 4 1 で取得したカード情報 (製造番号) を登録する。

【 0 1 5 8 】

ステップ S 2 4 3 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザテーブル (図 1 3) にカード情報の登録が完了したため、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 で取得したアクセスキーのレコードをアクセスキーリスト (図 1 2) から削除する。

40

【 0 1 5 9 】

ステップ S 2 4 4 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、プリンタ通信部 2 5 0 により、プリンタへ登録結果コマンドを送信する (登録成功結果情報送信) 。登録結果コマンドには登録成功を示す登録結果フラグ (O K) (登録成功結果情報) が含まれる。

【 0 1 6 0 】

ステップ S 2 4 5 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、期限を超え

50

てしまった情報であるため、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 で取得したアクセスキーのレコードをアクセスキーリスト (図 1 2) から削除する。

【 0 1 6 1 】

ステップ S 2 4 6 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、プリンタ通信部 2 5 0 により、プリンタへ登録できなかった旨のエラー表示するための登録結果コマンドを送信する (登録失敗結果情報送信)。登録結果コマンドには登録失敗を示す登録結果フラグ (N G) (登録失敗結果情報) が含まれる。

【 0 1 6 2 】

ステップ S 2 4 7 では、N I C 6 0 0 上の C P U 4 0 0 1 は、認証サーバ通信部 3 5 1 により、I C カード認証サーバ 2 0 0 から返された登録結果コマンドを受信する。

10

【 0 1 6 3 】

ステップ S 2 4 8 では、N I C 6 0 0 上の C P U 4 0 0 1 は、認証サーバ通信部 3 5 1 により、ステップ 2 4 7 で受信した登録結果コマンドを解析する。登録に成功した場合はステップ S 2 4 9 に進み、認証に失敗した場合はステップ S 2 5 3 に進む。

【 0 1 6 4 】

ステップ S 2 4 9 では、N I C 6 0 0 上の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、登録成功ページ (図 1 7) を生成する。

【 0 1 6 5 】

ステップ S 2 5 0 では、N I C 6 0 0 上の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、クライアント P C 1 0 0 に対してステップ S 2 4 9 で生成した登録成功ページ (図 1 7) を H T T P 通信によって送信する。

20

【 0 1 6 6 】

ステップ S 2 5 1 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、登録部 1 5 2 より、プリンタ 3 0 0 より返された登録成功ページを含む H T T P レスポンスコマンドを受信する。

【 0 1 6 7 】

ステップ S 2 5 2 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、W e b ブラウザにより、ステップ S 2 5 1 で受信した登録成功ページ (図 1 7) を C R T 2 0 1 0 に表示する。

【 0 1 6 8 】

30

ステップ S 2 5 3 では、N I C 6 0 0 上の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、登録失敗ページ (図 1 8) を生成する。

【 0 1 6 9 】

ステップ S 2 5 4 では、N I C 6 0 0 上の C P U 4 0 0 1 は、W e b 制御部 3 5 3 により、クライアント P C 1 0 0 に対してステップ S 2 4 9 で生成した登録失敗ページ (図 1 8) を含む H T T P レスポンスコマンドを送信する。

【 0 1 7 0 】

ステップ S 2 5 5 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、登録部 1 5 2 により、プリンタ 3 0 0 より返された登録失敗ページを含む H T T P レスポンスコマンドを受信する。

40

【 0 1 7 1 】

ステップ S 2 5 5 では、クライアント P C 1 0 0 の C P U 2 0 0 1 は、W e b ブラウザにより、ステップ S 2 5 1 で受信した登録失敗ページ (図 1 8) を C R T 2 0 1 0 に表示する。

【 0 1 7 2 】

なお本実施形態でのカード情報登録処理では、登録処理にかかる要求をクライアント P C 1 0 0 からプリンタ 3 0 0 に要求し、プリンタ 3 0 0 から I C カード認証サーバ 2 0 0 へ要求を行うことでカード情報の登録を可能な構成としたが、クライアント P C 1 0 0 から I C カード認証サーバ 2 0 0 へ要求を行うことで実現することも可能である。

【 0 1 7 3 】

50

例えば、ステップS 2 0 0 , ステップS 2 0 7 , ステップS 2 2 9 の送信を、I C カード認証サーバ2 0 0 に送信する。この場合、当該各ステップに対応する処理をプリンタ3 0 0 ではなく、I C カード認証サーバ2 0 0 に実行させるように構成する。

【0 1 7 4】

次に、図1 0 を用いて、本発明の実施形態における、カード情報登録処理について説明する。

【0 1 7 5】

なお、図1 0 は本発明の実施形態における、アクセスキーリストの削除処理を示すフローチャートである。また、本フローチャートは所定の時間になった時（例えば、1 日1 回 P M 1 0 : 0 0 ）に行う定時処理である。

10

【0 1 7 6】

ステップS 3 0 0 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、I C カード認証サーバ2 0 0 の外部メモリ2 0 1 1 に保持する登録モード設定ファイル（図1 1 ）を読み出す。

【0 1 7 7】

ステップS 3 0 1 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、ステップS 3 0 0 で読み出された登録モード設定ファイル内に記載されたアクセスキー有効期間1 1 0 2 を取得する。

【0 1 7 8】

ステップS 3 0 2 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、I C カード認証サーバ2 0 0 の外部メモリ2 0 1 1 に保持するアクセスキーリスト（図1 2 ）を取得する。

20

【0 1 7 9】

ステップS 3 0 3 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、ステップS 3 0 2 で取得したアクセスキーリストのアクセスキー1 2 0 2 内で、後述するステップS 3 0 4 ~ ステップS 3 0 7 の処理が未実行であるアクセスキーが存在するかを判断する。未実行のアクセスキーが存在する場合はステップS 3 0 4 へ進み、存在しない場合は処理を終了する。

【0 1 8 0】

ステップS 3 0 4 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、ステップS 3 0 3 で未実行と判断されたアクセスキーをアクセスキー1 2 0 2 から取得し、取得したアクセスキーに対応するアクセスキー発行時間をキー発行時間1 2 0 3 から取得する。

30

【0 1 8 1】

ステップS 3 0 5 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、I C カード認証サーバ2 0 0 で管理しているシステムの現在時刻（年月日時分秒）を取得する。

【0 1 8 2】

ステップS 3 0 6 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、ステップS 3 0 4 で取得したキー発行時間と、I C 認証サーバのシステムの現在時刻（年月日時分秒）とを比較し、時間差異がステップS 3 0 1 で取得したアクセスキー有効期間1 1 0 2 内であればステップS 3 0 3 に進み、期間外（期間を超えている）であればステップS 3 0 7 に進む。

40

【0 1 8 3】

ステップS 3 0 6 では、I C カード認証サーバ2 0 0 のC P U 2 0 0 1 は、ユーザ情報管理部2 5 2 により、ステップS 3 0 3 で取得したアクセスキー（期限を超えたアクセスキー）のレコードをアクセスキーリスト（図1 2 ）から削除する。

【0 1 8 4】

次に、図1 1 を用いて、本発明の実施形態における、登録モード設定ファイルについて説明する。

50

【 0 1 8 5 】

登録モード設定ファイルは、ＩＣカード認証サーバ２００の外部メモリ２０１１に記憶されており、ＣＰＵ２００１によって読みだされる。

【 0 1 8 6 】

登録モード設定ファイルには、プリンタからのカード登録１１０１とアクセスキー有効期間１１０２が記述されており、プリンタからのカード登録１１０１には、プリンタからカード登録可能にするか否かを判定させるためのフラグ（値）が設定されている。プリンタからのカード登録１１０１に「ＯＮ」が設定されている場合にはプリンタからのカード登録可能とすることができる。また、プリンタからのカード登録１１０１に「ＯＦＦ」が設定されている場合にはプリンタからのカード登録不可能とすることができる。

10

【 0 1 8 7 】

アクセスキー有効期間１１０２には、ＩＣカード認証サーバ２００で生成され、後述する図１２に記憶したアクセスキーが生成されてから有効である時間が設定されている。この設定された時間に従って、アクセスキーを削除させることができる。

【 0 1 8 8 】

なお、プリンタからのカード登録１１０１の「ＯＮ／ＯＦＦ」、アクセスキー有効期間１１０２に設定する有効時間はＩＣカード認証サーバ２００を管理するユーザによって任意に設定することができる。

【 0 1 8 9 】

次に、図１２を用いて、本発明の実施形態における、アクセスキーリストについて説明する。

20

【 0 1 9 0 】

アクセスキーリストは、ＩＣカード認証サーバ２００の外部メモリ２０１１に記憶されており、ＣＰＵ２００１によって検索、登録することが可能なテーブル（或いはデータベース）である。

【 0 1 9 1 】

アクセスキーリストは、カード情報１２０１，アクセスキー１２０２，キー発行時間１２０３で構成されており、カード情報１２０１には、プリンタ３００から受信したカード情報（例えば、カードの製造番号）が、アクセスキー１２０２にはＩＣカード認証サーバ２００で一意的値となるべく生成され、プリンタ３００に送信されたアクセスキーが、キー発行時間１２０３には、アクセスキーが発行された際の時間（年月日時分秒）が記憶されている。

30

【 0 1 9 2 】

次に、図１３を用いて、本発明の実施形態における、ユーザテーブルについて説明する。

【 0 1 9 3 】

ユーザテーブルは、ＩＣカード認証サーバ２００の外部メモリ２０１１に記憶されており、ＣＰＵ２００１によって検索（認証）、登録することが可能なテーブル（或いはデータベース）である。

【 0 1 9 4 】

ユーザテーブルは、ユーザ名１３０１，パスワード１３０３，カード情報１３０２，メールアドレス１３０４で構成されており、ユーザ名１３０１とパスワード１３０３は、クライアントＰＣ１００からの認証の際に用いられる情報で、企業においてはネットワークにログインするためのログインＩＤ（社員番号）と任意に設定されたパスワードが記憶される。

40

【 0 1 9 5 】

また、カード情報１３０２は、有効期間内にクライアントＰＣ１００からアクセスキーが入力された場合に登録される情報で、ＩＣカードから読み出された識別番号が記憶される。

【 0 1 9 6 】

50

さらに、メールアドレス 1304 は、ユーザ名 1301 に対応して利用されるメールアドレスが記憶されている。

【0197】

本実施形態では、ユーザテーブルを IC カード認証サーバ 200 の外部メモリ 2011 に記憶するように構成したが、例えば LDAP サーバ (Lightweight Directory Access Protocol サーバ) などに記憶させるように構成してもよい。

【0198】

また、パスワードを機密に管理するために、ユーザ名とパスワードを LDAP サーバに、ユーザ名とカード情報とメールアドレスとを IC カード認証サーバ 200 に記憶するように構成し、IC 認証サーバと LDAP サーバを別筐体とすることも可能である。

10

【0199】

本実施形態によれば、ユーザ情報の入力が困難なプリンタ (画像形成装置) においても、例えば IC カードなどのカード番号 (認証情報) とユーザ情報 (ユーザ名とパスワード等) と対応付けて登録させることで、管理者の管理負担を軽減することができる。

【0200】

特に、クライアント PC 100 から出力した印刷データを蓄積し、IC カードによる認証が成功した場合に蓄積した印刷データを受け取り、印刷を実行する蓄積型のセキュリティ印刷システムにおいて、リッチな表示を行うことができないプリンタが設置されている場合でも容易に IC カードを登録することができる。

20

【0201】

〔実施形態 2〕

実施形態 1 では、IC カード認証サーバ 200 に登録されていない IC カードをカードリーダー 400 にかざすことによって、IC カード認証サーバ 200 上で一時的に生成されるカード番号を特定するための識別番号であるアクセスキーを生成し、このアクセスキーを Web ブラウザ上で入力することで、ユーザ情報の入力が困難なプリンタ (画像形成装置) においても、IC カード認証サーバ 200 に当該ユーザのカード情報を登録することが可能とした。

【0202】

しかし、実施形態 1 では管理者の手を介さずに IC カード認証サーバに当該ユーザのカード情報登録が可能となったものの、当該ユーザが自分で認証サーバ上のカード情報を削除することができない。

30

【0203】

そこで、実施形態 2 では、上記 IC カード認証サーバ 200 に登録された当該ユーザのカード情報を削除する仕組みを提供する。

【0204】

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。

【0205】

まず、図 19 ~ 24 を用いて、本発明の実施形態 2 における、カード情報削除処理について説明する。

40

【0206】

なお、実施形態 2 は、実施形態 1 の図 12 を図 23 に置き換え、図 6 を図 19 と図 20 に置き換え、図 9 を図 21 に置き換えることで実現可能である。

【0207】

その他の図面に関しては、実施形態 1 と実施形態 2 では同等のものとし、説明は省略する。

【0208】

まず、図 19 を用い、本発明の実施形態における、カード情報削除処理について説明する。なお、実施形態 1 と同じ処理については同じステップを付し、説明を省略する。

【0209】

50

ステップS 5 0 0では、カードリーダ4 0 0は、ユーザによってユーザが所有するICカード（読取対象物）がかざされたこと、もしくは外されたことを検知する。

【0 2 1 0】

ステップS 5 0 1では、カードリーダ4 0 0がステップS 5 0 0で発生したイベントを判断する。カードがかざされた場合はステップS 5 0 2に進み、カードが外された場合はステップS 5 0 3へ進む。

【0 2 1 1】

ステップS 5 0 2では、カードリーダ4 0 0がかざされたカードのカード情報を取得する。

【0 2 1 2】

ステップS 5 0 3では、カードリーダ4 0 0は、プリンタ3 0 0にカードイベント情報を発行する。なお、カードイベントの種類がカードかざしであった場合、取得したカード情報も併せてプリンタ3 0 0に発行する。

【0 2 1 3】

ステップS 5 0 4では、NIC 6 0 0上のCPU 4 0 0 1は、カードリーダ制御部3 5 0により、カード検知イベントを受信する。また、合わせてイベント受信時間についても取得するものとする。なお、イベント受信時間はプリンタ3 0 0内で管理するシステム時間を用いるものとする。

【0 2 1 4】

ステップS 5 0 5では、NIC 6 0 0上のCPU 4 0 0 1は、ステップS 5 0 4で取得したカードイベントの種類を判断する。カード外しイベントだった場合はステップS 5 0 7へ進み、カードかざしイベントだった場合はステップS 5 0 6へ進む。

【0 2 1 5】

ステップS 5 0 6では、NIC 6 0 0上のCPU 4 0 0 1は、ステップS 5 0 4にて取得したカード検知イベントに含まれるICカードのカード情報（読取対象物識別情報）（例えば、カードの製造番号等）を取得し、RAM 4 0 0 2に記憶させる。そして、カード外しイベントを受け付けるまで待機する。また、カード検知イベント取得時のイベント取得時間をRAM 4 0 0 2に記憶する。

【0 2 1 6】

ステップS 5 0 7では、NIC 6 0 0上のCPU 4 0 0 1は、認証サーバ通信部3 5 1により、ICカード認証サーバに対して認証要求コマンドを送信する（読取対象物識別情報送信）。すなわち、実施形態2ではカード検知時に認証要求が発行されるのではなく、カード外し時に認証要求が発行される仕組みとなる。なお、認証要求コマンドにはステップS 5 0 6で取得しRAM 4 0 0 1に記憶したカード情報（読取対象物識別情報）及び、ステップS 5 0 4で取得したカード検知イベント取得時の時間及びカード外しイベント取得時の時間が含まれる。

【0 2 1 7】

ステップS 1 0 6～ステップS 1 0 8は実施形態1と同じ処理のため説明を省略する。

【0 2 1 8】

ステップS 5 0 8では、カード情報がユーザテーブル（図1 3）に存在しない場合（認証が失敗した場合）の処理である。具体的にはステップS 1 1 0～1 1 4の処理が該当するため、説明は省略する。

【0 2 1 9】

ステップS 5 0 9では、ICカード認証サーバ2 0 0のCPU 2 0 0 1は、ユーザ情報管理部2 5 2により、ICカード認証サーバの外部メモリ2 0 1 1に記憶する削除モード設定ファイル（図2 2）から設定情報を読み出す。

【0 2 2 0】

ステップS 5 1 0では、ICカード認証サーバ2 0 0のCPU 2 0 0 1は、ユーザ情報管理部2 5 2により、ステップS 5 0 9で読み出された設定情報のうち、プリンタからのカード削除5 0 0 0を参照し、

10

20

30

40

50

プリンタからのカード削除モードのON/OFFを判定する。削除モードがONである場合、ステップS511に進み、OFFである場合はステップS109に進む。

【0221】

ステップS511では、ICカード認証サーバ200のCPU2001は、ユーザ情報管理部252により、ステップS509で読み出された設定情報のうち、削除モード移行時間閾値5001を参照し、ステップS106で取得した認証要求に含まれるカード検知イベント取得時の時間と、カード外しイベント取得時の時間の差分とを比較する。すなわち、カードかざし時間が閾値よりも長い場合はステップS512へ進み、閾値以下である場合はステップS109へ進む。

【0222】

ステップS512では、ICカード認証サーバ200のCPU2001は、ユーザ情報管理部252により、ICカード認証サーバの外部メモリ2011に記憶するアクセスキーリスト(図23)を読み出す。

【0223】

ステップS513では、ICカード認証サーバ200のCPU2001は、ユーザ情報管理部252により、ランダムな値であり、かつアクセスキーリスト内に存在しない一意のアクセスキーを生成する。なお、カード情報がカードの製造番号などである場合には、カードの製造番号をアクセスキーとして用いることや、カードの製造番号からハッシュ値を取得し、このハッシュ値をアクセスキーとして用いてもよい。

【0224】

また、ステップS513で生成されたアクセスキーは、一意のアクセスキーを複数用意しており、アクセスキーリストで利用していないアクセスキーを前述の複数のアクセスキーから決定するような構成であってもよい。

【0225】

つまり、アクセスキーはカード情報と対応付けて管理する、ユーザのカード情報を特定するための登録・削除キーである。また、ステップS513で生成されるアクセスキーはかざされたICカードを削除する(利用できないようにする)ためのアクセスキーである。ステップS508で生成されるアクセスキーは、ICカードを登録する(利用できないようにする)ためのアクセスキーである。

【0226】

ステップS514では、ICカード認証サーバ200のCPU2001は、ユーザ情報管理部252により、ステップS513で生成したアクセスキー、ステップS106で取得したカード情報(製造番号)、アクセスキーを生成した時の時間であるアクセスキー発行日時をアクセスキーリスト(図23)のカード情報1201、アクセスキー1202、キー発行時間1203に追加登録する(生成時間管理)。また、キーステータスは削除キーであることを意味する“DELETE”を登録する。

【0227】

ステップS515では、ICカード認証サーバ200のCPU2001は、プリンタ通信部250により、プリンタ300へ認証結果コマンドを送信する(認証結果送信)。認証が成功した場合(ステップS108でYES)且つステップS109ユーザ名を取得した場合には、認証結果コマンドに認証成功フラグ、及びステップS109で取得したユーザ名を含める。また、認証が成功した場合(ステップS108でYES)且つステップS513でアクセスキーが生成された場合には、認証結果コマンドに認証失敗フラグ、及びステップS513で生成されたアクセスキーを含める。さらに、認証が失敗した場合(ステップS108でNO)には、認証結果コマンドに認証失敗フラグ及びステップS508で生成されたアクセスキーを含める。

【0228】

なお、ステップS116～ステップS121の処理は、実施形態1と同じ処理のため説明を省略する。

【0229】

10

20

30

40

50

次に、図 2 1 を用い、本発明の実施形態における、カード情報削除処理について説明する。なお、前述の通り図 2 1 は実施形態 1 の図 8 に続く処理として記載している。

【 0 2 3 0 】

ステップ S 6 0 0 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 でアクセスキー 1 2 0 2 を検索し、ステップ S 2 3 4 で取得したアクセスキーと一致したアクセスキーに対応しての該当アクセスキーリストに記憶されているに含まれるキーステータス 1 2 0 4 を取得し、ステータスが “ D E L E T E ” であるかを判断する。“ D E L E T E ” である場合はステップ S 6 0 2 へ進み、“ D E L E T E ” 以外、すなわち “ A D D ” である場合はステップ S 6 0 1 へ進む。

【 0 2 3 1 】

つまり、前述のステップ S 5 1 3 で生成されたアクセスキーが、クライアント P C 1 0 0 の C R T 2 0 1 0 で表示される図 2 4 のアクセスキー入力ページを介して入力された場合は、I C カードを削除する（利用不可にする）ために、ステップ S 6 0 2 へ進む。また、ステップ S 5 0 8 で生成されたアクセスキーが、クライアント P C 1 0 0 の C R T 2 0 1 0 で表示される図 2 4 のアクセスキー入力ページを介して入力された場合は、I C カードを登録する（利用可能にする）ために、ステップ S 6 0 1 へ進む。

【 0 2 3 2 】

ステップ S 6 0 1 では、カード情報登録に関する制御であり、具体的にはステップ S 2 3 7 ~ 2 4 4 の処理が該当するため、説明は省略する。

【 0 2 3 3 】

ステップ S 6 0 2 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 でアクセスキー 1 2 0 2 を検索し、ステップ S 2 3 4 で取得したアクセスキーと一致したアクセスキーに対応しての該当アクセスキーリストに記憶されているに含まれるキー発行時間 1 2 0 3 を取得する。

【 0 2 3 4 】

ステップ S 6 0 3 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、I C カード認証サーバ 2 0 0 の外部メモリ 2 0 1 1 に保持する削除モード設定ファイル（図 2 2 ）を読み出す。

【 0 2 3 5 】

ステップ S 6 0 4 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 6 0 3 で読み出した削除モード設定ファイル内に記載されたアクセスキー有効期間 5 0 0 2 （所定時間）を取得する。

【 0 2 3 6 】

ステップ S 6 0 5 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 6 0 2 で取得したキー発行時間と I C カード認証サーバ 2 0 0 で管理しているシステムの現在時刻（年月日時分秒）と比較し、時間差異がステップ S 6 0 4 で取得したアクセスキー有効期間内（所定時間内）であればステップ S 6 0 6 に進み、期間外（期間を超えている）であればステップ S 2 4 5 に進む。（時間判定）

【 0 2 3 7 】

ステップ S 6 0 6 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 で取得したアクセスキーに紐づいたカード情報 1 2 0 1 （例えば、製造番号）を取得する。

【 0 2 3 8 】

ステップ S 6 0 7 では、I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ユーザ情報管理部 2 5 2 により、ユーザテーブル（図 1 3 ）からステップ S 2 1 4 （または、ステップ S 2 3 4 ）で取得したユーザ名に対応するカード情報 1 3 0 2 を削除する。なお、アクセスキーに対応するカード情報を図 2 3 のアクセスキーリストから特定し、この特定したカード情報と一致するカード情報 1 3 0 2 を検索し、検索されたカード情報を削除するようにしてもよい。つまり、削除するカード情報を特定する方法は、カード情報を特定できればどのような方法を用いてもよい。

10

20

30

40

50

【 0 2 3 9 】

ステップ S 6 0 8 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ステップ S 6 0 7 で実施したユーザテーブル (図 1 3) からのカード削除結果を判断する。削除が成功した場合はステップ S 6 0 9 へ進み、削除が失敗した場合 (カードが登録されていなかった場合等) はステップ S 2 4 6 へ進む。

【 0 2 4 0 】

ステップ S 6 0 9 では、 I C カード認証サーバ 2 0 0 の C P U 2 0 0 1 は、ステップ S 6 0 7 で実施したユーザテーブル (図 1 3) からのカード削除が成功したため、ユーザ情報管理部 2 5 2 により、ステップ S 2 3 6 で取得したアクセスキーのレコードをアクセスキーリスト (図 2 3) から削除する。

10

【 0 2 4 1 】

ステップ S 6 1 0 では、カード情報が削除されたことを示す登録結果をプリンタ 3 0 0 に送信する。なお、ステップ S 6 1 0 でカード情報が削除されたことを示す登録結果を送信した場合には、ステップ S 2 4 8 で Y E S、ステップ S 2 4 9 に推移し、ステップ S 2 4 9 では、削除成功ページが作成され、クライアント P C 1 0 0 へ送信されるように構成する。

【 0 2 4 2 】

その他、ステップ S 2 4 5 以降の処理については実施形態 1 と同じ処理であるため、説明は省略する。

【 0 2 4 3 】

20

以上の処理により、 I C カードを認証サーバに設定された閾値以上の長さかざす処理を実施するだけで、カード削除要求のアクセスキーが生成される。ユーザはこのアクセスキーをブラウザ上より入力することで、ユーザは管理者の手を煩わせることなく、任意のタイミングで任意のカード情報を削除することが可能となる。

【 0 2 4 4 】

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。

【 0 2 4 5 】

以上、一実施形態について示したが、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と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、一つの機器からなる装置に適用しても良い。

30

【 0 2 4 6 】

また、本発明におけるプログラムは、図 6 ~ 図 1 0、図 1 9 ~ 図 2 1 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、本発明の記憶媒体は図 6 ~ 図 1 0、図 1 9 ~ 図 2 1 の処理方法をコンピュータが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 6 ~ 図 1 0、図 1 9 ~ 図 2 1 の各装置の処理方法ごとのプログラムであってもよい。

【 0 2 4 7 】

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 C P U や M P U) 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。

40

【 0 2 4 8 】

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憶した記録媒体は本発明を構成することになる。

【 0 2 4 9 】

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、 C D - R O M、 C D - R、 D V D - R O M、磁気テープ、不揮発性のメモ리카ード、 R O M、 E E P R O M、シリコンディスク等を用

50

いることができる。

【0250】

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。

【0251】

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。

【0252】

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、1つの機器からなる装置に適用してもよい。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用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。

【0253】

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。

【0254】

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。

【0255】

また上記のソフトウェアで実現する各処理を、ファームウェアやハードウェア構成にして、各処理を各手段として実現することも可能であり、本発明の技術的範囲はこのようなファームウェアやハードウェア構成による実現も含むものである。

【符号の説明】

【0256】

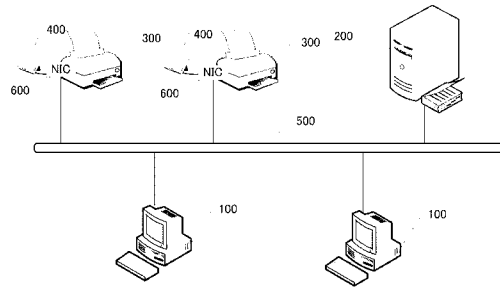
- 100 クライアントPC
- 200 IC認証サーバ
- 300 プリンタ
- 400 カードリーダー
- 500 LAN
- 600 NIC

10

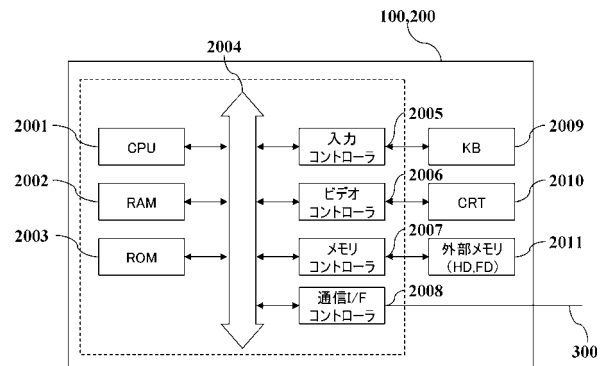
20

30

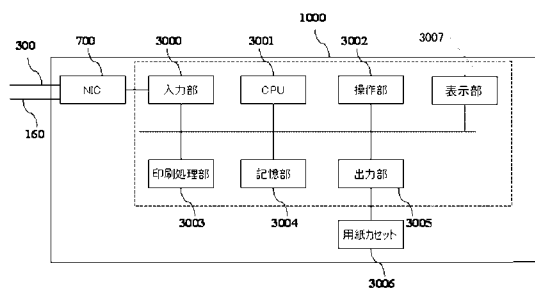
【図 1】



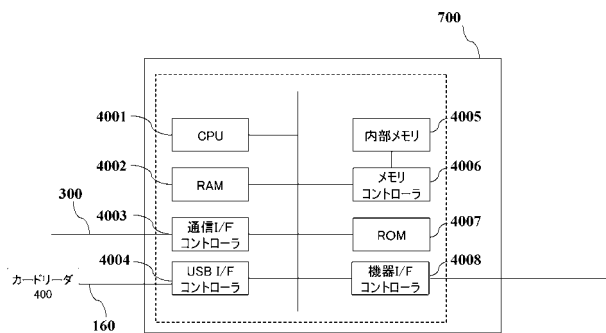
【図 2】



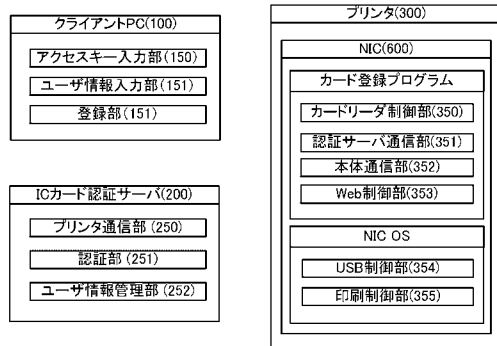
【図 3】



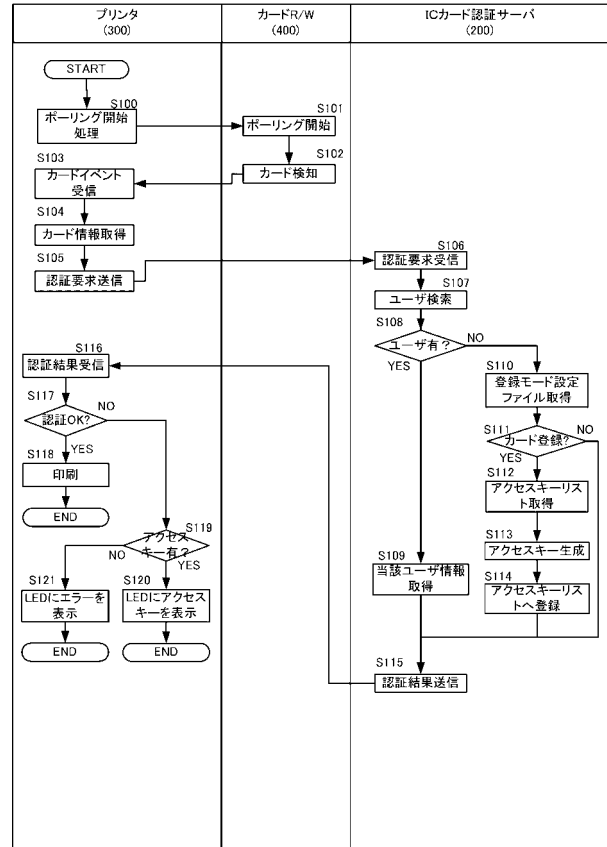
【図 4】



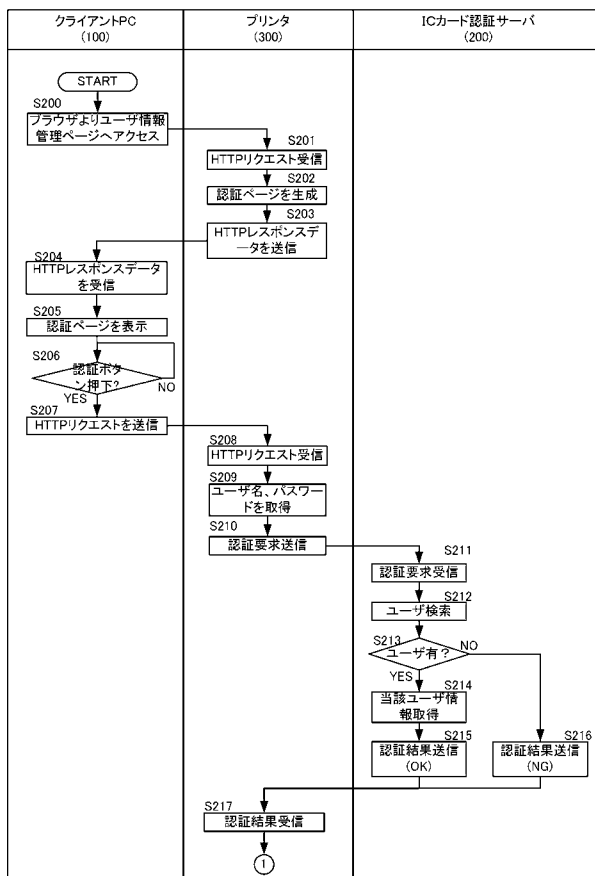
【図 5】



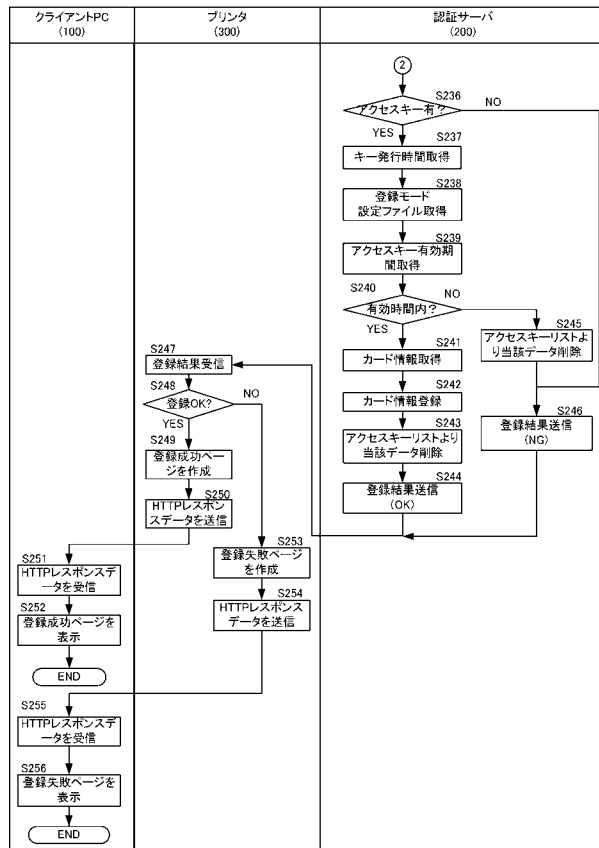
【図 6】



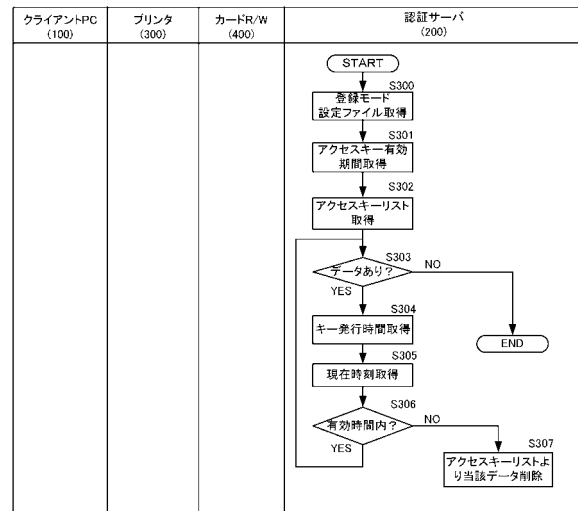
【図 7】



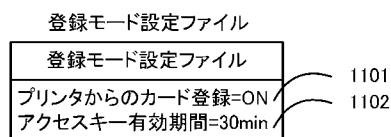
【図 9】



【図 10】



【図 11】

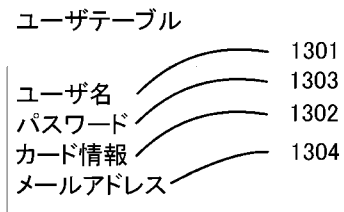


【図 12】

アクセスキーリスト

カード情報	アクセスキー	キー発行時間
1111111111	ABJE6A875A	200901201512
2222222222	56AR5ADFL0	200901201514
3333333333	7E4365ADG4N	200901201515
4444444444	PL46AERADF	200901201515
...	...	...

【図 1 3】



【図 1 4】

ユーザ名、パスワードを入力し、
“認証”ボタンを押してください。

ユーザ名:

パスワード:

1000

【図 1 5】

入力されたユーザ名、パスワードが違います。

ユーザ名、パスワードを入力し、
“認証”ボタンを押してください。

ユーザ名:

パスワード:

1001

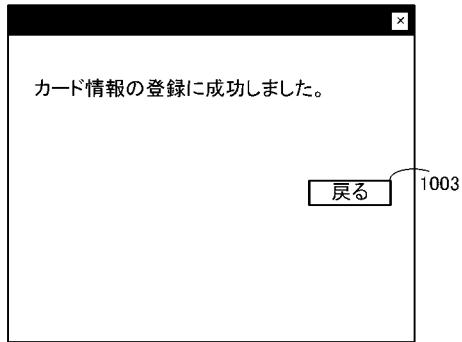
【図 1 6】

アクセスキーを入力し、
“登録”ボタンを押してください。

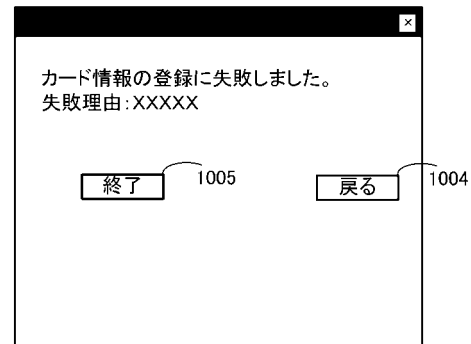
アクセスキー:

1002

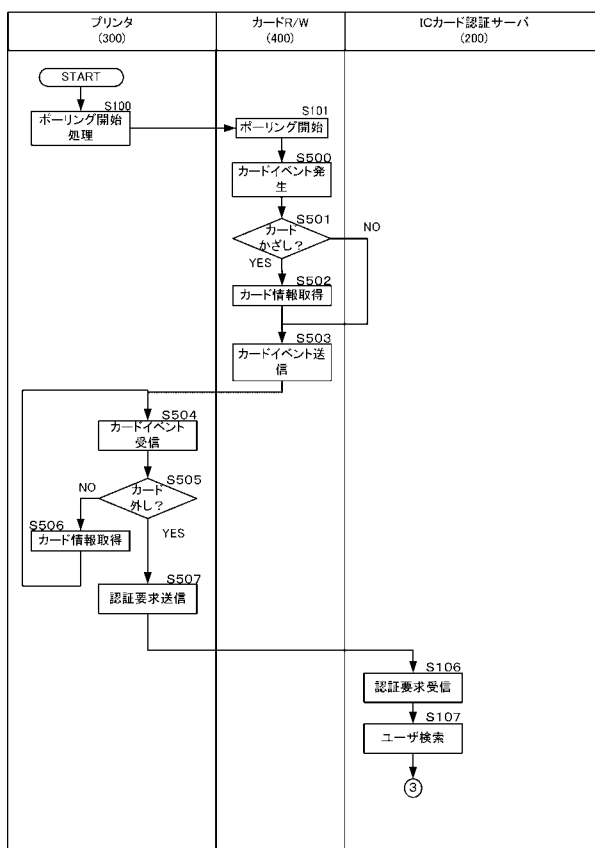
【図 17】



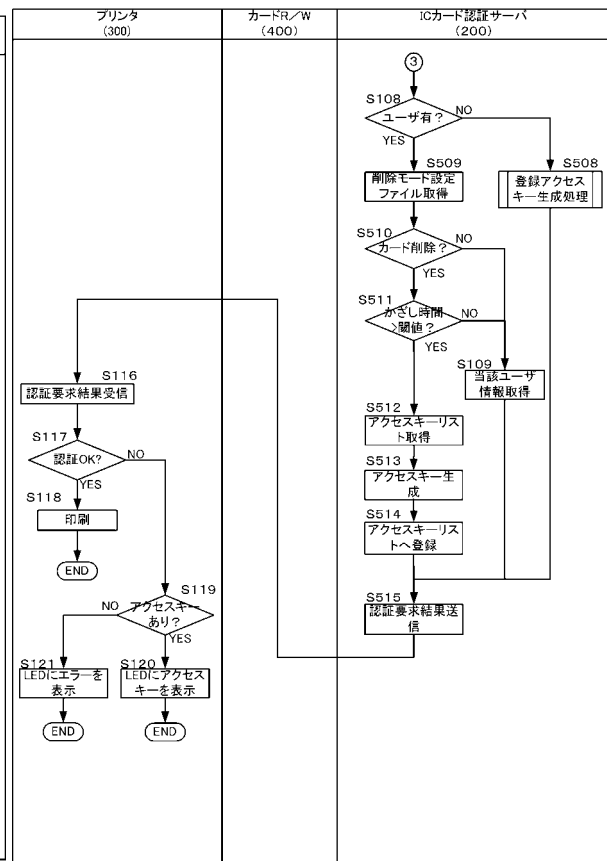
【図 18】



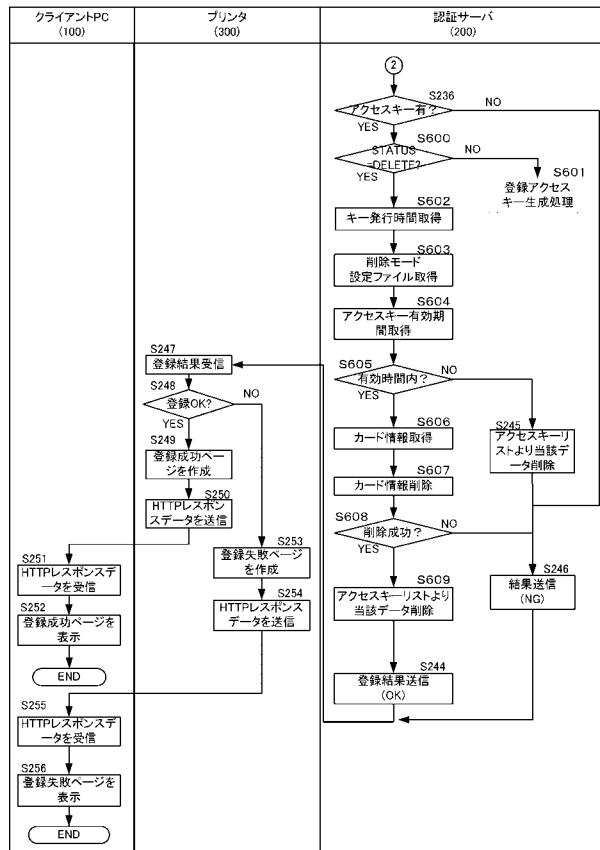
【図 19】



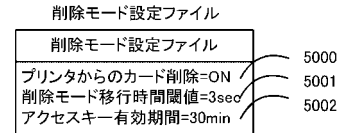
【図 20】



【図 2 1】



【図 2 2】



【図 2 3】

アクセスキーリスト

カード情報	アクセスキー	キー発行時間	キーステータス
1111111111	ABJE6A875A	200901201512	ADD
2222222222	56AR5ADFL0	200901201514	DELETE
3333333333	7E4365ADG4N	200901201515	ADD
4444444444	PL46AERADF	200901201515	ADD
...	...	...	...

【図 2 4】

アクセスキーを入力し、
“入力”ボタンを押してください。

アクセスキー:

フロントページの続き

(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 久慈 渉

(56)参考文献 特開2008-003743(JP,A)

特開2008-181491(JP,A)

特開平09-161033(JP,A)

特開2007-004372(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/31

G06F 21/34