(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7163204号
(P7163204)

(45)発行日　令和4年10月31日(2022.10.31)

(24)登録日　令和4年10月21日(2022.10.21)

(51)国際特許分類

Ｂ４１Ｊ	*29/38*	*(2006.01)*	Ｂ４１Ｊ	29/38	２０３
Ｂ４１Ｊ	*29/00*	*(2006.01)*	Ｂ４１Ｊ	29/00	Ｚ
Ｂ４１Ｊ	*29/42*	*(2006.01)*	Ｂ４１Ｊ	29/42	Ｆ
Ｈ０４Ｎ	*1/00*	*(2006.01)*	Ｈ０４Ｎ	1/00	３５０
Ｇ０６Ｆ	*3/12*	*(2006.01)*	Ｇ０６Ｆ	3/12	３３８

ＦＩ

請求項の数　10　（全14頁）　最終頁に続く

(21)出願番号　特願2019-7007(P2019-7007)
(22)出願日　平成31年1月18日(2019.1.18)
(65)公開番号　特開2020-116740(P2020-116740A)
(43)公開日　令和2年8月6日(2020.8.6)
審査請求日　令和3年12月20日(2021.12.20)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部 琢磨
(74)代理人　100124442
弁理士　黒岩 創吾
(72)発明者　山田 哲也
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
審査官　加藤 昌伸

最終頁に続く

(54)【発明の名称】　画像形成装置、画像形成装置の制御方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

ＩＣカードを読み取る読取装置と接続することが可能であり、かつ前記読取装置により読み取られた前記ＩＣカードに記憶されている認証情報を取得しユーザーの認証を行う認証アプリを備える画像形成装置であって、

前記読取装置を制御するドライバーを動作させる管理手段と、

認証方式を指示するための画面を表示する表示手段とを有し、

前記画像形成装置にプレインストールされているシステム認証アプリのドライバーが動作中の場合、前記表示手段は前記ＩＣカードを用いた認証方式で認証する指示が行えるように前記画面を表示し、

前記ユーザーの指示により前記画像形成装置にインストールされた一般認証アプリのドライバーが動作中の場合、前記表示手段は前記ＩＣカードを用いた認証方式で認証する指示が行えないように前記画面を表示することを特徴とする画像形成装置。

【請求項２】

前記システム認証アプリのドライバーの登録を行う登録手段を有し、

前記表示手段は、前記登録手段により前記システム認証アプリのドライバーが登録されている場合に、前記ＩＣカードを用いた認証方式で認証する指示が行えるように前記画面を表示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】

前記表示手段は、前記登録手段により前記システム認証アプリのドライバーが登録され

ている場合に、前記ＩＣカードを用いた認証方式の詳細な設定が行えるように前記画面を表示することを特徴とする請求項２に記載の画像形成装置。
【請求項４】
前記表示手段は、前記システム認証アプリが動作中である場合に、前記ＩＣカードを用いた認証方式で認証する指示が行えるように前記画面を表示することを特徴とする請求項１乃至３の何れか１項に記載の画像形成装置。
【請求項５】
前記画面とは前記システム認証アプリの認証設定のための第１画面であり、前記一般認証アプリの認証設定のための第２画面とは異なることを特徴とする請求項１乃至４の何れか１項に記載の画像形成装置。
【請求項６】
前記画面には、前記ＩＣカードを用いた認証方式とキーボードを用いた認証方式の中からユーザーの認証を行うための認証方式を選択する項目が含まれており、動作中の前記ドライバーがユーザーの指示によって前記画像形成装置にインストールされた一般認証アプリのドライバーである場合、前記ＩＣカードを用いた認証方式を選択できるように表示しないことを特徴する請求項１乃至５の何れか１項に記載の画像形成装置。
【請求項７】
前記キーボードを用いた認証方式は、前記ＩＣカードを用いた認証方式を選択し前記ＩＣカードを用いた認証方式でユーザーの認証を行うことを指示していない場合、または前記ユーザーの指示により前記画像形成装置にインストールされた一般認証アプリのドライバーが動作中の場合には、自動的に選択された状態となり、前記キーボードを用いた認証方式が有効になることを特徴とする請求項６に記載の画像形成装置。
【請求項８】
前記システム認証アプリのドライバーと前記一般認証アプリのドライバーは、認証アプリの管理画面で認証アプリの切り替え指示が出される毎に一方のドライバーが停止し、もう一方のドライバーが動作することを特徴とする請求項１乃至７の何れか１項に記載の画像形成装置。
【請求項９】
ＩＣカードを読み取る読取装置と接続することが可能であり、かつ前記読取装置により読み取られた前記ＩＣカードに記憶されている認証情報を取得しユーザーの認証を行う認証アプリを備える画像形成装置の制御方法であって、
前記読取装置を制御するドライバーを動作させる管理ステップと、
認証方式を指示するための画面を表示する表示ステップとを含み、
前記画像形成装置にプレインストールされているシステム認証アプリのドライバーが動作中の場合、前記表示ステップでは前記ＩＣカードを用いた認証方式で認証する指示が行えるように前記画面を表示し、
前記ユーザーの指示により前記画像形成装置にインストールされた一般認証アプリのドライバーが動作中の場合、前記表示ステップでは前記ＩＣカードを用いた認証方式で認証する指示が行えないように前記画面を表示することを特徴とする制御方法。
【請求項１０】
ＩＣカードを読み取る読取装置と接続することが可能であり、かつ前記読取装置により読み取られた前記ＩＣカードに記憶されている認証情報を取得しユーザーの認証を行う認証アプリを備える画像形成装置のプログラムであって、
前記読取装置を制御するドライバーを動作させる管理ステップと、
認証方式を指示するための画面を表示させる表示ステップとを含み、
前記画像形成装置にプレインストールされているシステム認証アプリのドライバーが動作中の場合、前記表示ステップでは前記ＩＣカードを用いた認証方式で認証する指示が行えるように前記画面を表示させ、
前記ユーザーの指示により前記画像形成装置にインストールされた一般認証アプリのドライバーが動作中の場合、前記表示ステップでは前記ＩＣカードを用いた認証方式で認証

する指示が行えないように前記画面を表示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】
【０００１】
本発明は、外部接続された読取装置を利用してユーザー認証する画像形成装置、画像形成装置の制御方法、及びプログラムに関する。
【背景技術】
【０００２】
画像読み取りユニット、印刷ユニット、通信ユニットを備え、コピー、プリント、スキャンした画像の送信等の画像処理アプリケーションを持つＭＦＰ（Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）が知られている。ＭＦＰに限らずスマートフォンなどの情報機器は、ユーザーが本体購入後に、一般アプリケーションを別途インストール仕組みを持つ。ＭＦＰ、スマートフォンのＯＳの提供者は、第３者が一般アプリケーションを開発するためのＳＤＫ（Ｓｏｆｔｗａｒｅ Ｄｅｖｅｌｏｐｍｅｎｔ Ｋｉｔ）を提供し、本体内には一般アプリケーションが本体機能を利用するためのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）を実装する。
【０００３】
複数のユーザーにより利用され、認証されたユーザーごとに利用機能制限、パーソナライズを行なうために、ユーザー認証機能を備えるＭＦＰが存在する。ユーザー名とパスワードを操作パネルのソフトキーボードが入力させるキーボード認証が標準機能として搭載されることが多い。社員証として個人に配布されているＩＣカードをかざすことで認証するＩＣカード認証、指静脈など生体情報を読み取らせて認証する生体認証も提供される。これらの認証には、ＵＳＢで接続される読取装置がＭＦＰとは別途必要となることもあり、オプション商品として提供されることが多い（特許文献１参照）。
【０００４】
ＵＳＢでは、接続装置の機能によりデバイス・クラスという仕様群にグループ化され（例えば、ＵＳＢメモリはマスストレージ・クラスというクラスに属する）、クラス・ドライバーと呼ばれる共通のデバイスドライバ・アプリケーションで制御することが可能である。しかし、前記読取装置は装置固有の制御が必要なため、専用のドライバーがセットで必要となる。
【先行技術文献】
【特許文献】
【０００５】
【文献】特開２０１１－０７３３４３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ＩＣカードを読み取る読取装置を用いて複数の認証方式を提供可能なＭＦＰにおいて、認証方式を選択させる設定画面が提供されるが、装着されるオプションまたは認証方式を考慮せずに一律同じ設定画面を表示するとユーザーにとって不都合となる虞がある。具体的には、ユーザーが希望する認証アプリケーションをＭＦＰにインストールしたにも関わらず、希望しない認証アプリケーションに関するＩＣカード認証の設定ができることはユーザーに不都合である。
【０００７】
本発明は、この課題を解決するため、希望しない認証アプリケーションに関するＩＣカード認証の設定ができないように制御することを目的とする。
【課題を解決するための手段】
【０００８】
本発明の一実施形態に係る画像形成装置は、ＩＣカードを読み取る読取装置と接続することが可能であり、かつ前記読取装置により読み取られた前記ＩＣカードに記憶されてい

る認証情報を取得しユーザーの認証を行う認証アプリを備える画像形成装置であって、前記読取装置を制御するドライバーを動作させる管理手段と、認証方式を指示するための画面を表示する表示手段とを有し、前記画像形成装置にプレインストールされているシステム認証アプリのドライバーが動作中の場合、前記表示手段は前記ＩＣカードを用いた認証方式で認証する指示が行えるように前記画面を表示し、前記ユーザーの指示により前記画像形成装置にインストールされた一般認証アプリのドライバーが動作中の場合、前記表示手段は前記ＩＣカードを用いた認証方式で認証する指示が行えないように前記画面を表示することを特徴とする。

【発明の効果】

【０００９】

希望しない認証アプリケーションに関するＩＣカード認証の設定ができないようになる。

【図面の簡単な説明】

【００１０】

【図１】ＭＦＰ１０１に関連するシステム構成図

【図２】ＭＦＰ１０１のハードウェアの構成を示すブロック図

【図３】ＭＦＰ１０１のソフトウェアの構成を示すブロック図とＩＣカード認証部３４４動作時のソフトウェアの構成を示すブロック図と一般認証アプリケーション動作時のソフトウェアの構成を示すブロック図

【図４】アプリケーション管理部３１０が提供する管理ＵＩの例

【図５】操作部ＵＩ管理部３２０の制御する画面遷移の例

【図６】操作部ＵＩ管理部３２０の提供するアプリケーション選択画面の例

【図７】ＭＦＰ１０１起動時の一般アプリケーションによる操作部ＵＩ管理部３２０への登録処理

【図８】Ｗｅｂサーバー３２１が提供するポータル画面の例

【図９】システム認証アプリ３４０が提供する認証画面の例

【図１０】システム認証アプリ３４０動作時のＩＣカード認証実現のシーケンス

【図１１】一般認証アプリケーション動作時のＩＣカード認証実現のシーケンス

【図１２】認証設定部３４１による認証設定ＵＩの表示制御のフローチャート

【図１３】認証設定ＵＩの例

【発明を実施するための形態】

【００１１】

以下、図面を参照して本発明の実施の形態を詳しく説明する。尚、以下の実施の形態は特許請求の範囲に係る発明を限定するものでなく、また実施の形態で説明されている特徴の組み合わせの全てが発明の解決手段に必須のものとは限らない。

【００１２】

〔第１の実施形態〕

本発明に係る第１の実施形態について説明する。

【００１３】

＜＜システム構成＞＞

図１は、画像形成装置であるＭＦＰ１０１と関連するシステムの全体図である。ＬＡＮ１００に後述する装置が接続されている。ＰＣ１０２ではＭＦＰ１０１に対してプリントジョブの送信、ＷｅｂブラウザーでＭＦＰ１０１の提供するＷｅｂＵＩの表示・操作などを行う。認証サーバー１０３では、ＭＦＰ１０１を利用可能なユーザーの管理を行い、ＭＦＰ１０１からの照会を受けつけてユーザーの認証・照合を行う。

【００１４】

＜＜ハードウェア構成＞＞

図２は、ＭＦＰ１０１の構成を示すハードウェアブロック図である。ＣＰＵ２０１を含む制御部２００は、ＭＦＰ１０１全体の動作を制御する。ＣＰＵ２０１は、ＲＯＭ２０２に記憶された制御プログラムを読み出して読取や送信などの各種制御を行う。ＲＡＭ２０３は、ＣＰＵ２０１の主メモリ、ワークエリア等の一時記憶領域として用いられる。

【００１５】
ＨＤＤ２０４は、画像データや各種プログラムを記憶する。操作部Ｉ／Ｆ２０５は、操作部２０９と制御部２００とを接続する。プリンタＩ／Ｆ２０６は、プリンタ２１０と制御部２００とを接続する。印刷対象の画像データはプリンタＩ／Ｆ２０６を介して制御部２００から転送され、プリンタ２１０において記録媒体上に印刷される。スキャナＩ／Ｆ２０７は、スキャナ２１１と制御部２００とを接続する。スキャナ２１１は、原稿上の画像を読み取って画像データを生成し、スキャナＩ／Ｆ２０７を介して制御部２００に入力する。
【００１６】
ネットワークＩ／Ｆ２０８は、制御部２００（ＭＦＰ１０１）をＬＡＮ１００に接続する。ネットワークＩ／Ｆ２０８は、ＬＡＮ１００上の外部装置との間で各種情報の送受信（例えば、ＰＣ１０２からのプリントジョブの受信）を行なう。ＵＳＢ　Ｉ／Ｆ２１２は、ＵＳＢデバイスと制御部２００とを接続する。ＵＳＢデバイスは、ＭＦＰ１０１を購入する顧客が付加的な機能を希望する場合にオプションとして購入されるものである。本発明に関わるユーザー認証機能に利用されるものとして、ＩＣカードＲ／Ｗ２１３、生体認証装置２１４などが接続されるが、本実施例ではＩＣカードＲ／Ｗ２１３が接続されるケースをベースに説明する。無論生体認証装置２１４であってもよい。
【００１７】
＜＜ソフトウェア構成＞＞
図３は、ＭＦＰ１０１において本発明に関連するソフトウェア構成について示したブロック図である。プリント制御部３３１は、アプリケーションからの指示を受けてプリントＩ／Ｆ２０６を介してプリンタ２１０の制御を行う。スキャン制御部３３２は、アプリケーションからの指示を受けてスキャンＩ／Ｆ２０７を介してスキャナ２１１の制御を行う。
【００１８】
ＭＦＰ１０１のファームウェアの一部として出荷時にいくつかのアプリケーションがインストールされている。このようなアプリケーションをシステムアプリケーション」と呼ぶ。また、出荷後にユーザーがアプリケーションをＭＦＰ１０１にインストールすることが可能である。ユーザーがインストールアプリケーションを「一般アプリケーション」と呼ぶ。またアプリケーションの中には「認証アプリケーション」がある。操作部ＵＩ管理部３２０は、起動している認証アプリケーションが提供する認証画面を操作部２０９に表示し、認証がＯＫとなるまではＭＦＰ１０１の機能をユーザーが使えないように制御する。そのため、ＭＦＰ１０１が動作時には常に１つの認証アプリケーションが動作するように制御を行う。
【００１９】
ＭＦＰ１０１にはシステムアプリケーションがインストールされている。システムアプリケーションとしては、コピーアプリ３３３、プリントアプリ３３４、スキャンアプリ３３５が存在する。コピーアプリ３３３は、プリント制御部３３１及びスキャン制御部３３２を利用して所謂コピーの機能を提供する。プリントアプリ３３４は、ＰＣ１０２から投入されたプリントジョブを溜め置いて、ログインしたユーザーの投入したジョブのリストを表示し、ユーザーに内容を確認させて、プリント制御部３３１を利用して印刷するアプリケーションである。スキャン制御部３３２を利用してスキャンされた画像をメールなどで外部に送信するアプリケーションである。システム認証アプリ３４０もシステムアプリケーションと同様にプレインストール形式の認証アプリケーションであり、システムアプリケーションおよびシステム認証アプリ３４０はユーザーの指示で追加されるアプリケーションではなくＭＦＰ１０１にインストール済みのアプリケーションである。
【００２０】
アプリケーション管理部３１０は、一般アプリケーション、認証アプリケーションの情報、状態の管理、及びインストール・アンインストールのためのＵＩをＷｅｂＵＩとして提供する。図４はアプリケーションを管理するための管理画面の表示例である。一般アプリケーションは、「アプリケーションＡ」、「アプリケーションＢ」の２つがインストー

ルされている。４０２の列で状態を表示し、アプリケーションＡが開始状態である一方、アプリケーションＢは停止状態であることがわかる。「アプリケーションＡ」、「アプリケーションＢ」はユーザーのインストール指示によりインストールされたアプリケーションであり、システムアプリケーションとは異なる。４０３の列のボタンを押下することで、開始状態と停止状態を変更することができる。また、４０４の列の「アンインストール」ボタンを押下してアンインストールすることができる。４０５の行で、ファイルパスを入力して「インストール」ボタンを押下することでアプリケーションをインストールすることができる。

【００２１】

認証アプリケーションは、「一般認証アプリＡ」がユーザーによりインストールされているが、プレインストールの「システム認証アプリ」が開始状態にあることが４１２に示す状態の表示で分かる。４１３の列の「切替」ボタンを押下することで、その行の認証アプリケーションを開始状態に変更することができるが、開始状態の認証アプリケーションの「切替」ボタンはグレイアウトして押下できないように制御する。結果、すべての認証アプリケーションが停止状態にならない。４１５の行で、ファイルパスを入力して「インストール」ボタンを押下することでアプリケーションをインストールすることができる。なお、認証アプリは何れか１つが起動している状態とするので、システム認証アプリもしくは一般認証アプリのどちらか一方は必ず開始状態となっている。

【００２２】

操作部ＵＩ管理部３２０は、操作部２０９に表示するアプリケーションを管理する。例えば、図５に示す画面フローのような制御を行う。起動時にＳ５０１で認証アプリケーションに制御権を渡すことで、認証画面を表示する。操作部ＵＩ管理部３２０は、認証が成功したことで表示権限が返却されると、Ｓ５０２でアプリケーション選択画面を表示する。

【００２３】

図６はアプリケーション選択画面の表示例である。Ｓ５０３で、「コピー」ボタン６０１が押下されるとコピーアプリ３３３、「プリント」ボタン６０２が押下されるとプリントアプリ３３４、「スキャンして送信」ボタン６０３が押下されるとスキャンアプリ３３５に制御権を渡す。「設定」ボタン６０４が押下されると、すべてのシステムアプリケーションを含むＭＦＰ１０１に関わる設定メニューを提供する。

【００２４】

ＭＦＰ１０１の起動時に図７に示すような処理が行われることで、操作部ＵＩ管理部３２０はどのアプリケーションが管理対象を把握する。開始状態にある認証アプリケーションは、アプリケーションの起動時に、自らが動作する認証アプリケーションである旨を操作部ＵＩ管理部３２０に登録されるよう要求を行う。次に、システムアプリケーション・一般アプリケーションのうち操作部２０９でのＵＩ操作を提供するアプリケーションが操作部ＵＩ管理部３２０に登録されるよう要求を行う。図６のアプリケーション選択画面には、登録要求を行ったアプリケーションが表示される。

【００２５】

Ｗｅｂサーバー３２１は、ＰＣ１０２からのＷｅｂＵＩ提供要求を受信し、要求されたアプリケーションにＷｅｂＵＩ提供要求を行う。ＷｅｂＵＩを提供するアプリケーションは、起動時にその旨をＷｅｂサーバー３２１に登録する処理を行う。図８は、Ｗｅｂサーバー３２１が提供するポータル画面の表示例である。８０１の領域にＭＦＰ１０１の状態を表示している。「設定／登録」ボタン８１１が押下されると、システムアプリケーションを含むＭＦＰ１０１に関わる設定のＷｅｂＵＩに遷移する。設定のＷｅｂＵＩは入口のＵＩをメニュー画面として、そこから各種設定に遷移するような複数画面から構成される。「アドレス帳」ボタン８１２が押下されると、スキャンアプリ３３５で利用される送信先の設定ためのＷｅｂＵＩに遷移する。８２１～８２３のボタンは、前述したＷｅｂサーバー３２１に登録を行ったアプリケーションの提供するＷｅｂＵＩに遷移する。一般アプリケーションに関わる設定は、遷移先の各一般アプリケーションが提供するＷｅｂＵＩの中で提供される。

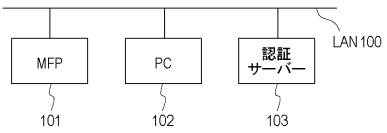
【００２６】
ＳＤＫ　Ｉ／Ｆ３５０は、一般アプリケーションがＭＦＰ１０１の機能を利用したり、連携したりするためのＡＰＩである。例えば、デバイス制御ＡＰＩ３５１を利用することでプリント制御部３３１、スキャン制御部３３２などを介して、プリンタ２１０、スキャナ２１１を制御することができる。
【００２７】
システム認証アプリ３４０は、キーボード認証とＩＣカード認証の２つの認証方式を提供する認証アプリケーションである。図９－ａは、認証方式としてキーボード認証のみが有効時の認証画面の表示例である。図９－ｂは、ＩＣカード認証のみが有効時の認証画面の表示例である。図９－ｃは、キーボード認証とＩＣカード認証の両方が有効時の認証画面の表示例である。キーボード認証の画面上にＩＣカードを翳すことで認証が可能な文言を表示している。
【００２８】
認証設定部３４１は、認証方式の選択、認証方式手段ごとの詳細設定などを管理し、設定するためのＵＩを提供する。ＵＩは、図３のアプリケーション選択画面の「設定」ボタン６０４、図８のＷｅｂＵＩのポータル画面の「設定／登録」ボタン８１１といったＭＦＰ１０１自体の設定の入口から表示することができる。
【００２９】
ユーザー管理部３４２では、ＭＦＰ１０１を利用可能なユーザーを管理する。キーボード認証部３４３は、認証情報としてユーザー名／パスワードを入力する認証画面を提供し、入力された認証情報を認証設定部３４１で指定された認証先で照合する制御を行う。
【００３０】
ＩＣカード認証部３４４は、ＩＣカードＲ／Ｗ２１３が読み取ったＩＣカード内の読取情報を認証情報として認証処理を行う。ＩＣカードＲ／Ｗ２１３はＭＦＰ１０１のオプションとして導入されるので、ＩＣカードＲ／Ｗ２１３を制御するドライバーソフトは一般アプリケーションとしてインストールされることになる。図３に示すように、操作部ＵＩ管理部３２０に動作する認証アプリケーションとして登録されたシステム認証アプリ３４０とインストールされたドライバー（システム認証アプリ用Ｒ／Ｗドライバー３６１とする）が連携し、ＩＣカード認証のカードＲ／Ｗの機能を実現する。具体的なシーケンスを図１０を用いて説明する。
【００３１】
システム認証アプリ用Ｒ／Ｗドライバー３６１はＭＦＰ１０１の起動時にＳ１００１でＩＣ認証ＡＰＩ３５３に対して、自らをＩＣカード認証用のＲ／Ｗのドライバーとして登録するように要求する。そして、ＩＣ認証ＡＰＩ３５３はＳ１００２でＩＣカード認証部３４４に登録要求を転送する。ＩＣカード認証部３４４はＳ１００３でドライバーの登録処理を行い、起動時の処理は終了する。
【００３２】
ＩＣカード認証部３４４は操作部ＵＩ管理部３２０からＳ１０１０で認証画面表示要求を受けると、Ｓ１０１１で認証画面を表示し、Ｓ１０１２でＩＣ認証ＡＰＩ３５３に、ＩＣカードＲ／Ｗがカードの読取処理を開始するように要求する。ＩＣ認証ＡＰＩ３５３はＳ１０１３で要求をシステム認証アプリ用Ｒ／Ｗドライバー３６１に転送する。システム認証アプリ用Ｒ／Ｗドライバー３６１は要求を受信すると、Ｓ１０１４でＵＳＢ制御ＡＰＩ３５２を介して数１０ｍｓｅｃおきにＩＣカードＲ／Ｗに電波を発してカードを検知するよう指示する。
【００３３】
Ｓ１０１５でＩＣカードを検知するとＩＣカード内の認証情報を読み取り、Ｓ１０１６で読み取った認証情報をＩＣ認証ＡＰＩ３５３に通知する。ＩＣ認証ＡＰＩ３５３はＳ１０１７でＩＣカード認証部３４４に認証情報を転送する。ＩＣカード認証部３４４はＳ１０１８で受信した認証情報を元に認証処理を行い、認証が成功すれば認証処理が終了した旨を操作部ＵＩ管理部３２０に通知する。その通知を受け付けた操作部ＵＩ管理部３２０

はＳ１０２０でアプリケーション選択画面を表示する。
【００３４】
＜＜一般認証アプリケーション＞＞
後からインストールされた一般認証アプリケーションが動作している場合は、図３－ｂに示すように一般認証アプリＡ３６３と一般認証アプリＡ用Ｒ／Ｗドライバー３６２がインストールされている構成となる。具体的なシーケンスを図１１を用いて説明する。
【００３５】
起動時に、一般認証アプリＡ３６３は操作部ＵＩ管理部３２０に対して、動作する認証アプリとしての登録を要求する。操作部ＵＩ管理部３２０は、一般認証アプリＡ３６３に対してＳ１１１０で認証画面表示要求を行い、一般認証アプリＡ３６３は、Ｓ１１１１で認証画面を表示する。一般認証アプリＡ用Ｒ／Ｗドライバー３６２がＳ１１１２でＵＳＢ制御ＡＰＩ３５２を介してＩＣカードＲ／Ｗを制御してＩＣカードの情報を読み取り、一般認証アプリＡ３６３は読取情報を取得しＳ１１１４で認証処理を行う。
【００３６】
ここで認証処理Ｓ１１１４の前にＳ１１１３で行われる一般認証アプリＡ用Ｒ／Ｗドライバー３６２と一般認証アプリＡ３６３のやりとりは、ＭＦＰ１０１のＳＤＫ　Ｉ／Ｆ３５０とは関係なく独自の処理方法で行われて構わない。Ｓ１１１５で一般認証アプリＡ３６３認証処理が終了した旨を操作部ＵＩ管理部３２０に通知すると、操作部ＵＩ管理部３２０はＳ１１１６でアプリケーション選択画面を表示する。このように、ＩＣ認証ＡＰＩ３５３、ＩＣカード認証部３４４での処理が発生することなくＩＣカード認証が実施される。
【００３７】
＜＜認証設定ＵＩ表示＞＞
前述のとおり図３の「設定」ボタン６０４が押下されると図８の設定メニューを表示する。また、図８の「設定／登録」ボタン８１１が押下されても設定メニューを表示する。両者はＵＩが異なるだけで設定できる内容は同じである。設定メニューの中で認証に関するメニュー（非図示）が選択された場合は、認証設定部３４１が、システム認証アプリ３４０に関する設定ＵＩを提供する。その制御を、ここではＵＩがＷｅｂＵＩであるとして図１２のフローチャートを用いて説明する。
【００３８】
ユーザー操作により、Ｓ１２０１で認証設定ＵＩの表示の要求が行われると、Ｓ１２０２でアプリケーション管理部３１０の認証アプリケーション管理（図４参照）でシステム認証アプリ３４０が動作中であるかを確認する。動作していない（すなわち、一般アプリケーションの「一般認証アプリＡ」が動作している）場合は、前述のとおり、図８の「認証アプリＡ」の認証設定のための設定ＵＩを表示するためのボタンが表示される。「認証アプリＡ」の認証設定はその設定ＵＩで認証設定は行われるため、特に制御を行わず終了する。
【００３９】
動作中の場合は、Ｓ１２０３でシステム認証アプリ用Ｒ／Ｗドライバー３６１が動作しているかを判定する。判定方法の具体例の１つとしては、アプリケーション管理部３１０においてシステム認証アプリ用Ｒ／Ｗドライバー３６１が開始状態であることである。他の方法としては、ＩＣカード認証部３４４が図１０で示したシーケンスのＳ１００３の登録処理を行ったことである。判定の結果、システム認証アプリ用Ｒ／Ｗドライバー３６１が動作していると判断した場合は、Ｓ１２０４で図１３－ａで示すような認証設定ＵＩを、動作していないと判断した場合は、Ｓ１２０５で図１３－ｂに示すような設定ＵＩを表示する。また、システム認証アプリ用Ｒ／Ｗドライバー３６１が開始状態であり、かつ登録処理が行われていることを条件にシステム認証アプリ用Ｒ／Ｗドライバー３６１が動作していると判断する形態もある。なお、システム認証アプリ用Ｒ／Ｗドライバー３６１が動作中であることを必須条件とする実施例であるが、例えば、一般認証アプリＡが動作しているか否かのみを判定条件としても良い。

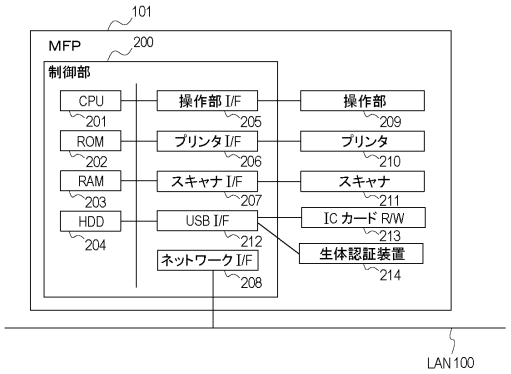
【００４０】
システム認証アプリの設定ＵＩは、１３０１の認証方式を選択させる部分、各認証方式の詳細設定（キーボード認証は１３１０、ＩＣカード認証は１３２０）から構成される。システム認証アプリ用Ｒ／Ｗドライバー３６１が動作している場合に表示される図１３－ａでは、１３０１でＩＣカード認証を認証方式として選択可能とするＵＩを提供するが、図１３－ｂでは提供しない。
【００４１】
また、１３２０のＩＣカード認証に関する詳細設定を図１３－ａでは提供するが、図１３－ｂでは提供しない。図１３－ｂでは、ＩＣカード認証に関わる設定を非表示としているが、表示したまま編集不可とする制御を行ってもよい。
【００４２】
さらに、何か一つの認証方式が有効になっている必要であるため、図１３－ａでは、１３０１でＩＣカード認証が選択されていない状態では、自動的にキーボード認証を有効状態のままで編集不可とするように制御する。また、図１３－ｂにおいても自動的に１３０１をグレイアウトして編集不可する。これにより、利用する認証方式が存在しなくなることを防ぐことができる。
【００４３】
以上、希望しない認証アプリケーションに関するＩＣカード認証の設定ができないように制御することが可能になることを説明した。
【００４４】
〔その他の実施例〕
本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施例の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。
【符号の説明】
【００４５】
１０１　ＭＦＰ
１０２　ＰＣ
１０３　認証サーバー
３４０　システム認証アプリ
３６１　システム認証アプリ用Ｒ／Ｗドライバー
３６２　一般認証アプリＡ用Ｒ／Ｗドライバー
３６３　一般認証アプリＡ

【図面】

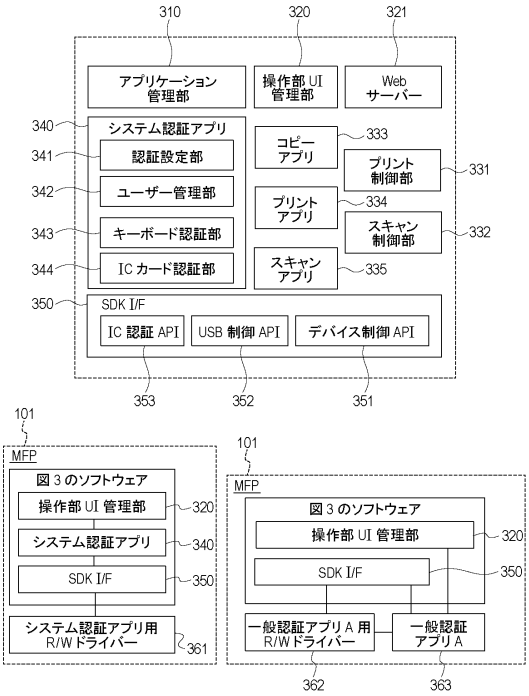
【図１】


LAN 100
MFP
PC
認証
サーバー
101
102
103

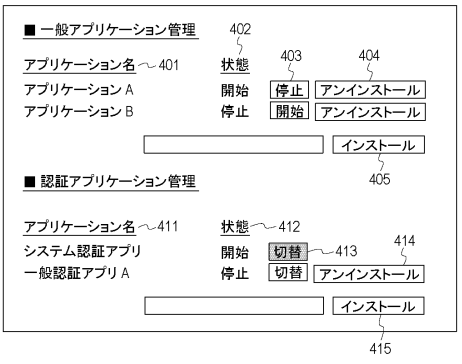
【図２】


101
MFP
200
制御部
CPU
201
ROM
202
RAM
203
HDD
204
操作部 I/F
205
プリンタ I/F
206
スキャナ I/F
207
USB I/F
212
ネットワーク I/F
208
操作部
209
プリンタ
210
スキャナ
211
IC カード R/W
213
生体認証装置
214
LAN 100

【図３】


310
320
321
アプリケーション
管理部
操作部 UI
管理部
Web
サーバー
340
システム認証アプリ
341
認証設定部
342
ユーザー管理部
343
キーボード認証部
344
IC カード認証部
333
コピー
アプリ
331
プリント
制御部
334
プリント
アプリ
332
スキャン
制御部
335
スキャン
アプリ
350
SDK I/F
IC 認証 API
USB 制御 API
デバイス制御 API
353
352
351
101
MFP
図 3 のソフトウェア
操作部 UI 管理部
320
システム認証アプリ
340
SDK I/F
350
システム認証アプリ用
R/W ドライバー
361
101
MFP
図 3 のソフトウェア
操作部 UI 管理部
320
SDK I/F
350
一般認証アプリ A 用
R/W ドライバー
一般認証
アプリ A
362
363

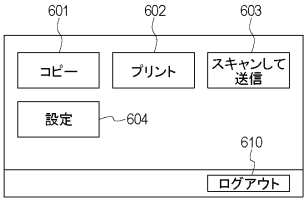
【図４】


■ 一般アプリケーション管理
402
アプリケーション名
401
状態
403
404
アプリケーション A
開始
停止
アンインストール
アプリケーション B
停止
開始
アンインストール
インストール
405
■ 認証アプリケーション管理
アプリケーション名
411
状態
412
414
システム認証アプリ
開始
切替
413
一般認証アプリ A
停止
切替
アンインストール
インストール
415

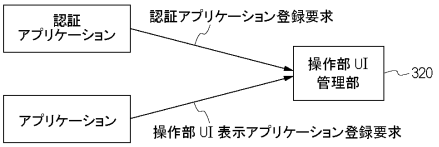
【図５】


S501
S502
S503
認証画面
アプリケーション選択画面
アプリケーション画面

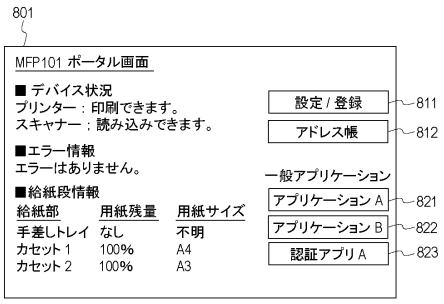
【図６】


601
602
603
コピー
プリント
スキャンして送信
設定
604
610
ログアウト

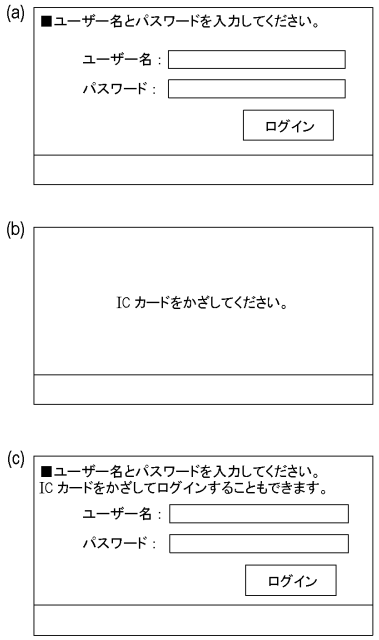
【図７】


認証アプリケーション
認証アプリケーション登録要求
操作部 UI 管理部
320
アプリケーション
操作部 UI 表示アプリケーション登録要求

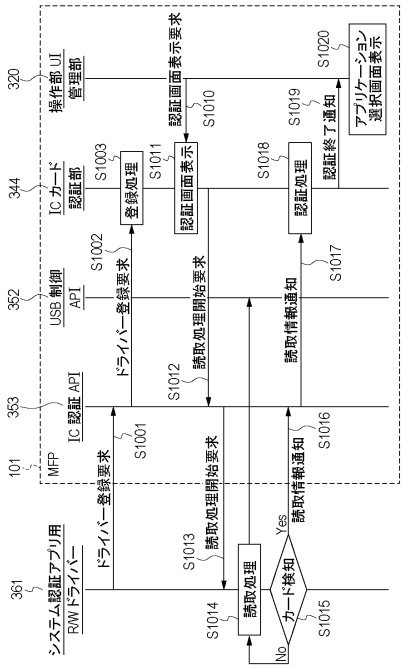
【図８】


801
MFP101 ポータル画面
■ デバイス状況
プリンター：印刷できます。
スキャナー：読み込みできます。
■エラー情報
エラーはありません。
■給紙段情報
給紙部 用紙残量 用紙サイズ
手差しトレイ なし 不明
カセット 1 100% A4
カセット 2 100% A3
設定 / 登録
811
アドレス帳
812
一般アプリケーション
アプリケーション A
821
アプリケーション B
822
認証アプリ A
823

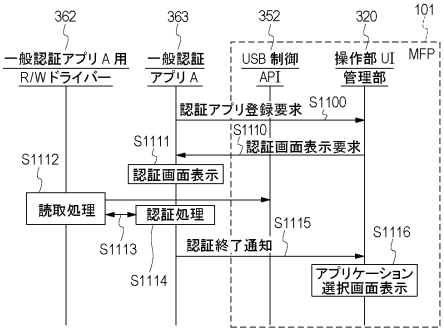
【図９】



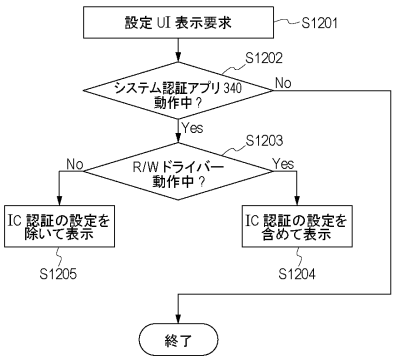
【図１０】



【図１１】



【図１２】



【図１３】


(a)
1301
認証方式
■ キーボード認証
□ IC カード認証
1310
キーボード認証
認証先
■ このデバイス
□ サーバー
1320
IC カード認証
認証先
■ このデバイス
□ サーバー
(b)
1301
認証方式
■ キーボード認証
1310
キーボード認証
認証先
■ このデバイス
□ サーバー

フロントページの続き

(51)国際特許分類　　ＦＩ
Ｇ０６Ｆ　3/12　３２２
Ｇ０６Ｆ　3/12　３２５

(56)参考文献　特開２０１８－００７０３６（ＪＰ，Ａ）
特開２０１８－０２６８４２（ＪＰ，Ａ）
特開２０１１－０７３３４３（ＪＰ，Ａ）
米国特許出願公開第２０１１／０２８６０２８（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｂ４１Ｊ　２９／００　－　２９／７０
Ｈ０４Ｎ　１／００
Ｇ０６Ｆ　３／０９　－　３／１２