(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6860793号
(P6860793)
(45)発行日　令和3年4月21日(2021.4.21)　(24)登録日　令和3年3月31日(2021.3.31)

(51)Int.Cl.　　F I
G06F 21/45 (2013.01)　　G06F 21/45
G06F 21/31 (2013.01)　　G06F 21/31

請求項の数 8　(全 28 頁)

(21)出願番号　特願2019-115273(P2019-115273)
(22)出願日　令和1年6月21日(2019.6.21)
(62)分割の表示　特願2014-265860(P2014-265860)の分割
原出願日　平成26年12月26日(2014.12.26)
(65)公開番号　特開2019-194890(P2019-194890A)
(43)公開日　令和1年11月7日(2019.11.7)
審査請求日　令和1年7月22日(2019.7.22)

(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　592135203
キヤノンＩＴソリューションズ株式会社
東京都港区港南２丁目１６番６号
(74)代理人　100189751
弁理士　木村　友輔
(72)発明者　上野　和博
東京都品川区東品川２丁目４番１１号　キヤノンＩＴソリューションズ株式会社内
(72)発明者　相澤　敦
東京都品川区東品川２丁目４番１１号　キヤノンＩＴソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】認証システム、その制御方法、及びプログラム、並びに、認証サーバ、その制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
ウェブサービスサーバからウェブサービスの提供を受ける画像形成装置と、前記画像形成装置と前記ウェブサービスサーバとの認可処理を行う情報処理装置とを含む情報処理システムであって、
前記情報処理装置は、
前記画像形成装置の認証処理手段で用いられるユーザ識別情報に対応する前記ウェブサービスサーバへのアクセストークンに係る情報を記憶する記憶手段、
を備え、
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用いた認証処理を行う認証処理手段と、
前記認証処理で用いたユーザ識別情報に対応するアクセストークンが前記記憶手段に記憶されているかに基づき、前記ウェブサービスへアクセスするためのアイテムの表示を制御する表示制御手段と、
を備えたことを特徴とする情報処理システム。
【請求項２】
前記画像形成装置が、前記記憶手段に記憶されたアクセストークンを用いて、前記ウェブサービスサーバに対して前記ウェブサービスを要求するウェブサービス要求手段
を更に備え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】

前記ウェブサービス要求手段は、前記認証処理手段により認証されたユーザに対応するアクセストークンを用いて、前記ウェブサービスサーバに対して前記ウェブサービスを要求することを特徴とする請求項２に記載の情報処理システム。

【請求項４】

前記認証処理手段は、読取媒体の読み取りにより得られた前記ユーザ識別情報を用いて前記ユーザの認証を行い、

前記記憶手段は、前記アクセストークンと前記認証処理で用いられる読取媒体の前記ユーザ識別情報とが対応するように記憶することを特徴とする請求項１乃至３のいずれか１項に記載の情報処理システム。

【請求項５】

ウェブサービスサーバからウェブサービスの提供を受ける画像形成装置と、前記画像形成装置と前記ウェブサービスサーバとの認可処理を行う情報処理装置とを含む情報処理システムの制御方法であって、

前記情報処理装置は、

前記画像形成装置の認証処理手段で用いられるユーザ識別情報に対応する前記ウェブサービスサーバへのアクセストークンに係る情報を記憶する記憶ステップ、

を実行し、

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用いた認証処理を行う認証処理ステップと、

前記認証処理で用いたユーザ識別情報に対応するアクセストークンが前記記憶ステップにより記憶されているかに基づき、前記ウェブサービスへアクセスするためのアイテムの表示を制御する表示制御ステップと、

を実行することを特徴とする情報処理システムの制御方法。

【請求項６】

ウェブサービスサーバとの認可処理を行う情報処理装置と通信可能な、前記ウェブサービスサーバからウェブサービスの提供を受け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用いた認証処理を行う認証処理手段と、

前記認証処理で用いたユーザ識別情報に対応するアクセストークンが、前記ユーザ識別情報に対応する前記ウェブサービスサーバへのアクセストークンに係る情報を記憶する前記情報処理装置に記憶されているかに基づき、前記ウェブサービスへアクセスするためのアイテムの表示を制御する表示制御手段と、

を備えたことを特徴とする画像形成装置。

【請求項７】

ウェブサービスサーバとの認可処理を行う情報処理装置と通信可能な、前記ウェブサービスサーバからウェブサービスの提供を受ける画像形成装置の制御方法であって、

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用いた認証処理を行う認証処理ステップと、

前記認証処理で用いたユーザ識別情報に対応するアクセストークンが、前記ユーザ識別情報に対応する前記ウェブサービスサーバへのアクセストークンに係る情報を記憶する前記情報処理装置に記憶されているかに基づき、前記ウェブサービスへアクセスするためのアイテムの表示を制御する表示制御ステップと、

を実行することを特徴とする画像形成装置の制御方法。

【請求項８】

ウェブサービスサーバとの認可処理を行う情報処理装置と通信可能な、前記ウェブサービスサーバからウェブサービスの提供を受ける画像形成装置のコンピュータを、

ユーザを識別するためのユーザ識別情報を用いた認証処理を行う認証処理手段と、

前記認証処理で用いたユーザ識別情報に対応するアクセストークンが、前記ユーザ識別情報に対応する前記ウェブサービスサーバへのアクセストークンに係る情報を記憶する前記情報処理装置に記憶されているかに基づき、前記ウェブサービスへアクセスするためのアイテムの表示を制御する表示制御手段と、

して機能させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
ウェブサービスサーバから取得したトークン情報とユーザの認証情報を容易に紐づけることの可能な認証システム、その制御方法、及びプログラム、並びに、認証サーバ、その制御方法、及びプログラムに関する。
【背景技術】
【０００２】
プリンタ機能を有する複合機であるＭＦＰ（Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎａｌ　Ｐｅｒｉｐｈｅｒａｌ）などの画像形成装置を用いて、例えばクライアントＰＣから印刷指示を行い、資料を印刷するということが行われる。
【０００３】
ＭＦＰにＩＣカードなどを用いてログインすると、ユーザはＭＦＰの機能を利用することができる。
【０００４】
一方で、ユーザに対してＩＤを付与し、ユーザ毎にストレージを割り当ててサービスを提供するウェブサービスサーバが存在する。サービスとは、例えばストレージに保存された画像をウェブサービスサーバがアルバムのように閲覧できる画面を生成してクライアントＰＣに送信し、クライアントＰＣからブラウザ等を通して画像を閲覧できるものがある。
【０００５】
ウェブサービスサーバが提供するサービスは例えばユーザがストレージ上に保存するカレンダーであったり、上述したようなウェブ上のアルバムであったり多岐にわたる。
【０００６】
下記の特許文献１には、ユーザごとに使用するウェブサービスのＩＤとパスワードを記憶しておき、ユーザがＭＦＰに認証することで、ユーザに対応するウェブサービスのＩＤとパスワードを利用することで当該ウェブサービスの利用を行うことのできる仕組みが開示されている。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２００８－２８２２１６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
前述した仕組みでは、ユーザがＭＦＰに認証すると、ＭＦＰはウェブサービスのＩＤとパスワードそのものをウェブサービスサーバと通信し、対応するウェブサービスを提供することができる。しかし悪意のある第三者に通信を傍受されることで、ＩＤとパスワードが漏えいした場合に第三者は漏洩したＩＤとパスワードでウェブサービスにログインし、ウェブサービスを閲覧したり、パスワードを変更したりすることができてしまう。
【０００９】
第三者にパスワードが変更されてしまうと、本来のユーザはウェブサービスにログインすることができなくなってしまうという重大なセキュリティ上のリスクがある。
【００１０】
そこで、アクセストークンという仕組みがある。アクセストークンとはウェブサービスサーバに認証するための情報である。
【００１１】
アクセストークンは有効期限が設けられていたり、定期的に変更されたりするものであ

るので、ＩＤとパスワードに比べてセキュリティ上有用である。
【００１２】
そのため、ユーザがＭＦＰに認証するための認証情報と、アクセストークンを対応付けて記憶しておくことで、ユーザはＭＦＰに認証することにより当該ユーザに対応するウェブサービスをアクセストークンを使用してセキュリティを保ってＭＦＰ上で利用することができる。例えばウェブサービス上のアルバムの画像を出力したり、ウェブサービス上のカレンダーを出力したりすることができる。
【００１３】
しかし、ユーザがＭＦＰを利用するための認証情報と、ウェブサービスを利用するためのアクセストークンとを対応付けて記憶するためには、ユーザがＭＦＰの認証サーバにアクセストークンを対応付けて記憶させる必要があり、手間がかかる。
【００１４】
そこで本発明の目的は、ユーザがウェブサービスを安全かつ容易に利用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】
【００１５】
上記の目的を達成するために、ウェブサービスサーバからウェブサービスの提供を受ける画像形成装置と、前記画像形成装置と前記ウェブサービスサーバとの認可処理を行う情報処理装置とを含む情報処理システムであって、前記情報処理装置は、前記画像形成装置の認証処理手段で用いられるユーザ識別情報に対応する前記ウェブサービスサーバへのアクセストークンに係る情報を記憶する記憶手段、を備え、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用いた認証処理を行う認証処理手段と、前記認証処理で用いたユーザ識別情報に対応するアクセストークンが前記記憶手段に記憶されているかに基づき、前記ウェブサービスへアクセスするためのアイテムの表示を制御する表示制御手段と、を備えたことと特徴とする。
【発明の効果】
【００１６】
本発明によれば、ユーザがウェブサービスを安全かつ容易に利用することができる、という効果を奏する。
【図面の簡単な説明】
【００１７】
【図１】本発明の実施形態におけるシステム構成の一例を示す構成図である。
【図２】本発明の実施形態における認証サーバ１００、ウェブサービスサーバ２００のハードウェア構成の一例を示す図である。
【図３】本発明の実施形態における画像形成装置３００のハードウェア構成の一例を示す図である。
【図４】本発明の実施形態における携帯端末４００のハードウェア構成の一例を示す図である。
【図５】本発明の実施形態における認証サーバ１００、ウェブサービスサーバ２００、画像形成装置３００、携帯端末４００の機能構成の一例を示す図である。
【図６】本発明の実施形態における一連の流れを示すフローチャートである。
【図７】認証サーバ１００がトークン情報に対応するカード登録用パスワードを生成する処理を説明するフローチャートである。
【図８】図６に示すカード登録処理の詳細な処理の流れを説明するフローチャートである。
【図９】図６に示すウェブサービス情報表示処理の詳細な処理の流れを説明するフローチャートである。
【図１０】認証テーブル１０００の一例を示す図である。
【図１１】カードＩＤテーブル１１００の一例を示す図である。
【図１２】二次元バーコード表示画面１２００の一例を示す画面例である。

【図１３】認可要求画面１３００の一例を示す画面例である。
【図１４】認可画面１４００の一例を示す画面例である。
【図１５】ユーザ情報使用確認画面１５００の一例を示す画面例である。
【図１６】認可完了画面１６００の一例を示す画面例である。
【図１７】メニュー画面１７００の一例を示す画面例である。
【図１８】ユーザ情報管理画面１８００の一例を示す画面例である。
【図１９】正当アクセストークンテーブル１９００の一例を示す図である。
【図２０】ＩＣカード認証画面２０００の一例を示す図である。
【図２１】カレンダー画面２１００の一例を示す図である。
【発明を実施するための形態】
【００１８】
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。
【００１９】
図１は、本発明の画像形成装置３００、画像形成装置３００の備えるカードリーダ３１０、認証サーバ１００、ウェブサービスサーバ２００、携帯端末４００を含む認証システムの構成の一例を示すシステム構成図である。なお、認証サーバ１００は、画像形成装置３００内のサービスとして実行する構成であってもよい。
【００２０】
図１に示すように、本実施形態のシステムでは、画像形成装置３００、認証サーバ１００、ウェブサービスサーバ２００がローカルエリアネットワーク（ＬＡＮ）６００を介して接続される構成となっている。なお、ローカルネットワークに限らずインターネットを介した通信であってもよい。
【００２１】
画像形成装置３００は、カードリーダ３１０にかざされたＩＣカードのカードＩＤをもとに、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、紙に出力したり、ファクスを送信したりすることが可能な装置である。
【００２２】
なお、カードリーダ３１０のほか、画像形成装置３００上のタッチパネルで、ソフトキーボードを用いて、ユーザＩＤとパスワードを入力し、認証を実行可能な構成となっている。
【００２３】
認証サーバ１００は、ＩＣカード認証やキーボード認証による認証を実行するための認証テーブル１０００と図１１に示すカードＩＤテーブル１１００を記憶している装置である。
【００２４】
ウェブサービスサーバ２００は、ユーザ毎にストレージを与えてサービスを提供するサーバである。例えばストレージに保存された画像をウェブサービスサーバ２００がアルバムのように閲覧できる画面を生成してクライアントＰＣに送信し、クライアントＰＣからブラウザ等を通して画像を閲覧できるものがある。
【００２５】
なお、画像形成装置３００はＭＦＰの一例を示す装置である。
【００２６】
以下、図２を用いて、図１に示した認証サーバ１００、ウェブサービスサーバ２００に適用可能な情報処理装置のハードウェア構成について説明する。
【００２７】
図２において、２０１はＣＰＵで、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０３あるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　／　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或

いは各ＰＣの実行する機能を実現するために必要な各種プログラム等が記憶されている。
【００２８】
なお、認証サーバ１００の外部メモリ２１１には、認証テーブル１０００が記憶されている。認証テーブル１０００の一例は、図１０である。また、ウェブサービスサーバ２００の外部メモリ２１１には、ユーザに対してウェブサービスを提供可能なウェブアプリケーションが記憶されている。例えばユーザがＩＤとパスワードを用いてウェブサービスサーバ２００にクライアントＰＣでログインし、クライアントＰＣからウェブサービスの提供要求をウェブサービスサーバ２００に送信する。すると、ウェブサービスサーバ２００は、ユーザが使用可能なウェブサービスを提供するウェブアプリケーションを外部メモリ２１１から特定して、当該ウェブアプリケーションを動作させる。これによりウェブアプリケーションがウェブサービスとして様々な情報をクライアントＰＣに返す。
【００２９】
２０２はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０３あるいは外部メモリ２１１からＲＡＭ２０２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。
【００３０】
また、２０５は入力コントローラで、入力デバイス２０９や不図示のマウス等のポインティングデバイス等からの入力を制御する。２０６はビデオコントローラで、ディスプレイ（ＣＲＴ）２１０等の表示器への表示を制御する。なお、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。
【００３１】
２０７はメモリコントローラで、ブートプログラム，各種のアプリケーション，フォントデータ，ユーザファイル，編集ファイル，各種データ等を記憶するハードディスク（ＨＤ）や、フレキシブルディスク（ＦＤ）、或いはＰＣＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１１へのアクセスを制御する。
【００３２】
２０８は通信Ｉ／Ｆコントローラで、ネットワーク（例えば、図１に示したＬＡＮ６００）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。
【００３３】
なお、ＣＰＵ２０１は、例えばＲＡＭ２０２内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ディスプレイ２１０上での表示を可能としている。また、ＣＰＵ２０１は、ディスプレイ２１０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。
【００３４】
ハードウェア上で動作する各種プログラム（例えば、ブラウザ）は、外部メモリ２１１（記憶手段）に記録されており、必要に応じてＲＡＭ２０２にロードされることによりＣＰＵ２０１によって実行されるものである。
【００３５】
次に図３を用いて、本発明の画像形成装置としての画像形成装置３００のハードウェア構成について説明する。
【００３６】
図３は画像形成装置３００のハードウェア構成の一例を示すブロック図である。
【００３７】
図３において、コントローラユニット３０００は、画像入力デバイスとして機能するスキャナ３０１５や、画像出力デバイスとして機能するプリンタ３０１４と接続されるとともに、図１に示したＬＡＮ６００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。
【００３８】
図３に示すように、コントローラユニット３０００は、ＣＰＵ３００１、ＲＡＭ３００６、ＲＯＭ３００２、外部記憶装置（ハードディスクドライブ（ＨＤＤ））３００７、ネットワークインタフェース（Ｎｅｔｗｏｒｋ　Ｉ／Ｆ）３００３、モデム（Ｍｏｄｅｍ）３００４、操作部インタフェース（操作部Ｉ／Ｆ）３００５、外部インタフェース（外部Ｉ／Ｆ）３００９、イメージバスインタフェース（ＩＭＡＧＥ　ＢＵＳ　Ｉ／Ｆ）３００８、ラスタイメージプロセッサ（ＲＩＰ）３０１０、プリンタインタフェース（プリンタＩ／Ｆ）３０１１、スキャナインタフェース（スキャナＩ／Ｆ）３０１２、画像処理部３０１３等で構成される。
【００３９】
ＣＰＵ３００１は、システム全体を制御するプロセッサである。
【００４０】
ＲＡＭ３００６は、ＣＰＵ３００１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。
【００４１】
ＲＯＭ３００２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。
【００４２】
外部記憶装置（ハードディスクドライブＨＤＤ）３００７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。また、各種テーブルを記憶している。
【００４３】
操作部インタフェース（操作部Ｉ／Ｆ）３００５は、操作部（ＵＩ）３０１８とのインタフェース部であり、操作部３０１８に表示する画像データを操作部３０１８に対して出力する。
【００４４】
また、操作部Ｉ／Ｆ３００５は、操作部３０１８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ＣＰＵ３００１に伝える役割をする。なお、操作部３０１８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。
【００４５】
ネットワークインタフェース（Ｎｅｔｗｏｒｋ　Ｉ／Ｆ）３００３は、ネットワーク（ＬＡＮ）に接続し、データの入出力を行なう。
【００４６】
モデム（ＭＯＤＥＭ）３００４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。
【００４７】
外部インタフェース（外部Ｉ／Ｆ）３００９は、ＵＳＢ、ＩＥＥＥ１３９４、プリンタポート、ＲＳ－２３２Ｃ等の外部入力を受け付けるインタフェース部であり、本実施形態においては、認証で必要となるＩＣカード読み取り用のカードリーダ３１０が接続されている。
【００４８】
そして、ＣＰＵ３００１は、この外部Ｉ／Ｆ３００９を介してカードリーダ３１０によるＩＣカードからの情報読み取りを制御し、該ＩＣカードから読み取られた情報を取得可能である。尚、ＩＣカードに限らず、ユーザを特定することが可能な記憶媒体であればよい。この場合、記憶媒体には、ユーザを識別するための識別情報が記憶される。この識別情報は、記憶媒体の製造番号でも、ユーザが企業内で与えられるユーザコードであってもよい。以上のデバイスがシステムバス上に配置される。
【００４９】

一方、イメージバスインタフェース（ＩＭＡＧＥ　ＢＵＳ　Ｉ／Ｆ）３００８は、システムバス３０１６と画像データを高速で転送する画像バス３０１７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３０１７は、ＰＣＩバスまたはＩＥＥＥ１３９４で構成される。画像バス３０１７上には以下のデバイスが配置される。

【００５０】

ラスタイメージプロセッサ（ＲＩＰ）３０１０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。

【００５１】

プリンタインタフェース（プリンタＩ／Ｆ）３０１１は、プリンタ３０１４とコントローラユニット３０００を接続し、画像データの同期系／非同期系の変換を行う。

【００５２】

また、スキャナインタフェース（スキャナＩ／Ｆ）３０１２は、スキャナ３０１５とコントローラユニット３０００を接続し、画像データの同期系／非同期系の変換を行う。

【００５３】

画像処理部３０１３は、入力画像データに対し、補正、加工、編集をおこなったり、プリント出力画像データに対して、プリンタの補正、解像度変換等を行う。また、これに加えて、画像処理部３０１３は、画像データの回転や、多値画像データに対してはＪＰＥＧ、２値画像データはＪＢＩＧ、ＭＭＲ、ＭＨ等の圧縮伸張処理を行う。

【００５４】

スキャナＩ／Ｆ３０１２に接続されるスキャナ３０１５は、原稿となる紙上の画像を照明し、ＣＣＤラインセンサで走査することで、ラスタイメージデータとして電気信号に変換する。原稿用紙は原稿フィーダのトレイにセットし、装置使用者が操作部３０１８から読み取り起動指示することにより、ＣＰＵ３００１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。

【００５５】

プリンタＩ／Ｆ３０１１に接続されるプリンタ３０１４は、ラスタイメージデータを用紙上の画像に変換する部分であり、その方式は感光体ドラムや感光体ベルトを用いた電子写真方式、微小ノズルアレイからインクを吐出して用紙上に直接画像を印字するインクジェット方式等があるが、どの方式でも構わない。プリント動作の起動は、ＣＰＵ３００１からの指示によって開始する。尚、プリンタ３０１４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。

【００５６】

操作部Ｉ／Ｆ３００５に接続される操作部３０１８は、液晶ディスプレイ（ＬＣＤ）表示部を有する。ＬＣＤ上にはタッチパネルシートが貼られており、システムの操作画面を表示するとともに、表示してあるキーが押されると、その位置情報を操作部Ｉ／Ｆ３００５を介してＣＰＵ３００１に伝える。また、操作部３０１８は、各種操作キーとして、例えば、スタートキー、ストップキー、ＩＤキー、リセットキー等を備える。

【００５７】

ここで、操作部３０１８のスタートキーは、原稿画像の読み取り動作を開始する時などに用いる。スタートキーの中央部には、緑と赤の２色のＬＥＤがあり、その色によってスタートキーが使える状態であるか否かを示す。また、操作部３０１８のストップキーは、稼動中の動作を止める働きをする。また、操作部３０１８のＩＤキーは、使用者のユーザＩＤを入力する時に用いる。リセットキーは、操作部３０１８からの設定を初期化する時に用いる。

【００５８】

外部Ｉ／Ｆ３００９に接続されるカードリーダ３１０は、ＣＰＵ３００１からの制御により、ＩＣカード（例えば、ソニー社のＦｅｌｉＣａ（登録商標））内に記憶されている情報を読み取り、読み取った情報を外部Ｉ／Ｆ３００９を介してＣＰＵ３００１へ通知する。

【００５９】
なお、本実施形態では、認証テーブルを認証サーバ１００に記憶する構成としたが、画像形成装置３００内に記憶して、認証サーバと同様の動作を実現してもよい。
【００６０】
次に図４に示す図を用いて携帯端末４００のハードウェア構成の説明を行う。
【００６１】
図４は、携帯端末４００のハードウェア構成を示す図である。尚、図４に示すハードウェア構成はあくまで一例である。
【００６２】
携帯端末４００は、タッチパネルを備える装置である。本実施形態では、いわゆるスマートフォンやタブレット端末のような装置を想定して説明を行うが、特にこれに限らない。タッチパネルを備える装置であれば、パーソナルコンピュータであってもよい。
【００６３】
ＣＰＵ４０１は、システムバスを介してメモリやコントローラを統括的に制御する。ＲＯＭ４０２あるいはフラッシュメモリ４１４には、ＣＰＵ４０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　／　ＯｕｔｐｕｔＳｙｓｔｅｍ）やオペレーティングシステムが記憶されている。更には、携帯端末４００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。
【００６４】
ＲＡＭ４０３は、ＣＰＵ４０１の主メモリ、ワークエリア等として機能する。ＣＰＵ４０１は、処理の実行に際して必要なプログラム等をＲＡＭ４０３にロードして、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。
【００６５】
ディスプレイコントローラ４０４は、ディスプレイ４１０等の表示装置への表示を制御する。ディスプレイ４１０は例えば液晶ディスプレイである。また、ディスプレイ４１０の表面にはタッチパネル４１１が備えられている。タッチパネル４１１に対するタッチ操作の検知をタッチパネルコントローラ４０５が制御する。タッチパネルコントローラ４０５は、タッチパネル４１１に対する複数の箇所に対するタッチ操作（以下、マルチタッチという。）も検知することが可能である。
【００６６】
カメラコントローラ４０６は、カメラ４１２における撮影を制御する。カメラ４１２はデジタルカメラであり、カメラコントローラ４０６からの制御で撮像した画像を撮像素子でデジタルデータに変換する。カメラ４１２は静止画と動画を撮影することが可能である。
【００６７】
センサコントローラ４０７は、携帯端末４００が備える各種センサ４１３からの入力を制御する。携帯端末４００のセンサ４１３には様々なセンサが存在し、例えば方位センサ、加速度センサ等である。
【００６８】
ネットワークコントローラ４０８は、ネットワークを介して、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を用いたインターネット通信等が可能である。
【００６９】
フラッシュメモリコントローラ４０９は、ブートプログラム、ブラウザソフトウエア、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フラッシュメモリ４１４へのアクセスを制御する。本実施形態においては、フラッシュメモリとして説明を行うが、ハードディスクやフレキシブルディスク、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カード型メモリ等の記憶媒体であってもよい。
【００７０】

前述したＣＰＵ４０１、各メモリ、各コントローラは、１つのチップ４１５に統合されている。いわゆるＳｏＣ（Ｓｙｓｔｅｍ　ｏｎ　Ｃｈｉｐ）の形態で携帯端末４００の内部に備えられている。

【００７１】

尚、ＣＰＵ４０１は、例えばＲＡＭ４０３内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ディスプレイ４１０での表示を可能としている。

【００７２】

本発明の携帯端末４００が後述する各種処理を実行するために用いられる各種プログラム等はフラッシュメモリ４１４に記録されており、必要に応じてＲＡＭ４０３にロードされることによりＣＰＵ４０１によって実行されるものである。さらに、本発明に係わるプログラムが用いる定義ファイルや各種情報テーブルはフラッシュメモリ４１４に格納されている。以上が、本実施形態におけるハードウェア構成である。

【００７３】

次に図５に示す図を用いて認証サーバ１００、ウェブサービスサーバ２００、画像形成装置３００、携帯端末４００の機能構成を説明する、なお、図５の機能構成図は一例であって用途や目的に応じて様々な構成例がある。

【００７４】

認証サーバ１００は、通信部１５０、認証テーブル管理部１５１、パスワード生成部１５２を備える。

【００７５】

通信部１５０は、画像形成装置３００やウェブサービスサーバ２００、携帯端末４００との通信を行う機能部である。

【００７６】

認証テーブル管理部１５１は、認証テーブル１０００を管理する機能部である。

【００７７】

パスワード生成部１５２は、アクセストークンと対応付けられるパスワードを生成する機能部である。

【００７８】

ウェブサービスサーバ２００は、通信部２５０、データ管理部２５１、トークン管理部２５２、画面生成部２５３を備える。

【００７９】

通信部２５０は、認証サーバ１００、携帯端末４００、画像形成装置３００との通信を行う機能部である。

【００８０】

データ管理部２５１は、ウェブサービスとして提供するデータであるウェブサービス情報をユーザごとに管理する機能部である。

【００８１】

トークン管理部２５２は、リフレッシュトークンに対応するアクセストークンを生成したり、受け付けたアクセストークンが正当なものか否かを判定したりする機能部である。

【００８２】

画面生成部２５３は、携帯端末４００や画像形成装置３００へ送信する画面を生成する機能部である。

【００８３】

画像形成装置３００は、カードリーダ制御部３５０、認証サーバ通信部３５１、認証部３５２、表示制御部３５３、出力制御部３５４、アプリケーション部３５５、ウェブサービスサーバ通信部３５６を備える。

【００８４】

カードリーダ制御部３５０は、カードリーダ３１０にかざされたカードＩＤ（製造番号）を取得する機能部である。

【００８５】
認証サーバ通信部３５１は、認証サーバ１００と認証要求の送受信を行う機能部である。
【００８６】
認証部３５２は、認証システム全般の制御及び、認証に成功した際にはユーザ情報を用いて画像形成装置３００の利用を許可させるものとする。
【００８７】
表示制御部３５３は、画像形成装置３００の操作部３０１８に各種画面を表示させるための機能部である。
【００８８】
出力制御部３５４は、印刷データの出力を制御する機能部である。
【００８９】
アプリケーション部３５５は、画像形成装置３００のプリント・スキャン・ＵＳＢ機能等を実行するアプリケーションを制御するための機能部である。
【００９０】
ウェブサービスサーバ通信部は、ウェブサービスサーバ２００と通信を行う機能部である。
【００９１】
携帯端末４００は、撮影部４５０、通信部４５１、表示制御部４５２、アプリケーション部４５３を備える。
【００９２】
撮影部４５０は、画像形成装置３００の操作部３０１８に表示される二次元バーコードを撮影、読み取ることが可能な機能部である。
【００９３】
通信部４５１は、認証サーバ１００、ウェブサービスサーバ２００と通信することが可能な機能部である。
【００９４】
表示制御部４５２は、認証サーバ１００、ウェブサービスサーバ２００から送信される画面を表示する機能部である。
【００９５】
アプリケーション部４５３は、ウェブブラウザなどのアプリケーションの動作を制御する機能部である。
【００９６】
次に図６に示すフローチャートを用いて、本発明の実施形態を説明する。
【００９７】
ステップＳ６０１では、画像形成装置３００のＣＰＵ３００１が、ＩＣカードをかざして画像形成装置３００にログインする旨を表示した認証画面２０００を表示する。例えば図２０に示す認証画面２０００である。
【００９８】
ステップＳ６２５では、画像形成装置３００のＣＰＵ３００１が、認証画面２０００に配置されたユーザ情報管理ボタン２００１が押下されたか否かを判定する。ユーザ情報管理ボタン２００１が押下されたと判定した場合は処理をステップＳ６２６に進め、ユーザ情報管理ボタン２００１が押されないと判定した場合は処理をステップＳ６０２に進める。
【００９９】
ステップＳ６２６では、画像形成装置３００のＣＰＵ３００１が、画像形成装置３００に認証することでウェブサービスが利用できるようにユーザのＩＣカードとウェブサービスサーバ２００の生成したアクセストークンとを対応付けて記憶する処理であるカード登録処理を行う。カード登録処理の詳細は後の図８を用いて説明する。
【０１００】

ステップＳ６０２では、画像形成装置３００のＣＰＵ３００１が、ユーザによってカードリーダ３１０にＩＣカードがかざされたかを定期的に検知する処理を実行する。ＩＣカードがかざされた場合には、ステップＳ６０３へ処理を移す。

【０１０１】

ステップＳ６０３では、画像形成装置３００のＣＰＵ３００１が、ユーザによってかざされたＩＣカードのカードＩＤをカードリーダ３１０から取得する。

【０１０２】

ステップＳ６０４では、画像形成装置３００のＣＰＵ３００１が、ステップＳ６０３で取得したカードＩＤを認証サーバ１００に対して送信する。

【０１０３】

ステップＳ６０５では、認証サーバ１００のＣＰＵ２０１が、ステップＳ６０４で送信されたカードＩＤを受信する。

【０１０４】

ステップＳ６０６では、認証サーバ１００のＣＰＵ２０１が、カードＩＤを使用して認証を行う。より具体的には、認証サーバ１００に記憶されるカードＩＤテーブル１１００を照合し、カードＩＤテーブル１１００にカードＩＤが記憶されているか否かを判定する。カードＩＤテーブル１１００にはカードＩＤ１１０１（認証情報）とユーザ名１００１（認証情報）が対応付けて記憶されている。カードＩＤ１１０１はカードＩＤを示し、ユーザ名１００１はユーザを識別する名称が格納されている。

【０１０５】

更に図１０に示す認証テーブル１０００を参照する。認証テーブル１０００には、ユーザ名１００１とアクセストークン１００２とリフレッシュトークン１００３とカード登録用パスワード１００４とが対応付けて記憶されている。アクセストークン１００２は、ウェブサービスサーバ２００からユーザのウェブサービスの情報であるウェブサービス情報を取得するためのトークン情報である。リフレッシュトークン１００３はアクセストークン１００２を更新するためのキーである。ウェブサービスサーバ２００に対して認証サーバ１００がリフレッシュトークン１００３を送信すると、ウェブサービスサーバ２００はリフレッシュトークン１００３に対応するアクセストークン１００２を更新する。カード登録用パスワード１００４は、ＩＣカードとアクセストークン１００２とを対応付けて記憶するためのキーである。

【０１０６】

ステップＳ６０７では、認証サーバ１００のＣＰＵ２０１が、ステップＳ６０６の照合により認証結果を判定する。より具体的にはステップＳ６０２で検知したカードＩＤ１１０１に対応するユーザ名１００１が、認証テーブル１０００に格納されている場合認証を成功とし、認証テーブル１０００に格納されていない場合は認証を失敗と判断する。認証に成功した場合は、ステップＳ６０８へ処理を移す。認証に失敗した場合は、ステップＳ６０９へ処理を移す。

【０１０７】

ステップＳ６０８では、認証サーバ１００のＣＰＵ２０１が、認証サーバ１００に対して認証結果（認証失敗）を送信する。

【０１０８】

ステップＳ６０９では、認証サーバ１００のＣＰＵ２０１が、ウェブサービスサーバ２００に対して、ステップＳ６０６で照合したユーザ名１００１に対応するリフレッシュトークン１００３と、トークン取得要求を送信する。

【０１０９】

ステップＳ６１０では、ウェブサービスサーバ２００のＣＰＵ２０１が、リフレッシュトークン１００３と、トークン取得要求を受信する。

【０１１０】

ステップＳ６１１では、ウェブサービスサーバ２００のＣＰＵ２０１が、リフレッシュトークン１００３に対応するアクセストークンを再発行する（更新手段）。より具体的に

説明する。ウェブサービスサーバ２００の外部メモリ２１１には図１９に示す正当アクセストークンテーブル１９００が格納されている。正当アクセストークンテーブル１９００には正当アクセストークン１９０１とリフレッシュトークン１００３とＩＤ１９０２、パスワード１９０３が対応付けて記憶されている。正当アクセストークン１９０１は、ウェブサービスサーバ２００が管理する正当なアクセストークンであり、この正当アクセストークンであれば対応するユーザのウェブサービス情報を取得して、アクセストークンの送信元にユーザのウェブサービス情報を送信することができる。ＩＤ１９０２、パスワード１９０３はウェブサービスサーバ２００にログインするためのＩＤとパスワードである。

【０１１１】

リフレッシュトークン１００３を受け付けると、対応する正当アクセストークン１９０１を書き換え、再発行を行う。

【０１１２】

ステップＳ６１２では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ６１１で再発行した正当アクセストークン１９０１を認証サーバ１００に対して送信する。

【０１１３】

ステップＳ６１３では、認証サーバ１００のＣＰＵ２０１が、ウェブサービスサーバ２００で再発行された正当アクセストークン１９０１（トークン情報
）を受信する。（トークン情報取得手段）

【０１１４】

ステップＳ６１４では、認証サーバ１００のＣＰＵ２０１が、ステップＳ６１３で受信した正当アクセストークン１９０１をステップＳ６０９で送信したリフレッシュトークン１００３に対応するアクセストークン１００２に更新する。このようにリフレッシュトークンを用いてアクセストークンを更新することで、アクセストークンが通信を傍受されることなどにより漏洩したとしても、漏洩したアクセストークンを無効にすることができる。また、有効期限の切れていないアクセストークンを画像形成装置３００に提供することが可能となる。

【０１１５】

ステップＳ６１５では、認証サーバ１００のＣＰＵ２０１が、画像形成装置３００に対して認証結果（認証成功を示す情報、アクセストークンありを示す情報、ユーザ名１００１）を送信する

【０１１６】

ステップＳ６１６では、画像形成装置３００のＣＰＵ３００１が、認証サーバ１００から送信される認証結果を受信する（認証受付手段）。

【０１１７】

ステップＳ６１７では、画像形成装置３００のＣＰＵ３００１が、ステップＳ６１６で受信した認証結果を判定する。認証に成功した場合は、ステップＳ６１８へ処理を移す。認証に失敗した場合は、ステップＳ６２４へ処理を移す。

【０１１８】

ステップＳ６１８では、画像形成装置３００のＣＰＵ３００１が、ステップＳ６１６で受信した認証結果にトークンありを示す情報が存在するかを判定する。トークンありを示す情報が存在した場合は、ステップＳ６１９へ処理を移す。トークンありを示す情報が存在しない場合は、ステップＳ６２３へ処理を移す。

【０１１９】

ステップＳ６１９では、画像形成装置３００のＣＰＵ３００１が、ウェブサービスサーバ２００が提供するウェブサービスを使用するためのアクセス用アイコンを追加したメニュー画面１７００（ログイン後の画面）を操作部３０１８に表示する。例えば図１７に示すメニュー画面１７００である。メニュー画面１７００には、画像形成装置３００の利用することのできる機能を示すアイコンが表示されている。例えば、コピーアイコンを押下すると、コピー機能が利用可能な画面に遷移する。図１７にはウェブサービスにアクセスすることの可能なウェブサービスカレンダーアイコン１７０１が配置されている。ウェブ

サービスカレンダーアイコン１７０１の押下を受け付けると、ウェブサービスにアクセスし、アクセストークンを用いてウェブサービスが提供するカレンダーの情報を取得する。なお、ウェブサービスは一例であってカレンダーに限定されない。

【０１２０】

ステップＳ６２０では、画像形成装置３００のＣＰＵ３００１が、メニュー画面１７００のウェブサービスカレンダーアイコン１７０１が押下されたか否かを判定する。ウェブサービスカレンダーアイコン１７０１が押下されたと判定した場合は処理をステップＳ６２１に進め、ウェブサービスカレンダーアイコン１７０１が押下されないと判定した場合は処理をステップＳ６２２に進める。

【０１２１】

ステップＳ６２１では、画像形成装置３００のＣＰＵ３００１が、ウェブサービス情報を取得し、操作部３０１８に表示する処理であるウェブサービス情報表示処理を行う。詳細な処理の流れは、図９に示すフローチャートで後述する。

【０１２２】

ステップＳ６２２では、画像形成装置３００のＣＰＵ３００１が、メニュー画面１７００に表示されているアイコンが押下され、押下されたアイコンに対応する処理を実行する。

【０１２３】

ステップＳ６２３では、画像形成装置３００のＣＰＵ３００１が、メニュー画面１７００を表示する。ステップＳ６２３で表示するメニュー画面１７００には、ウェブサービスカレンダーアイコン１７０１は配置されていない。

【０１２４】

ステップＳ６２４では、画像形成装置３００のＣＰＵ３００１が、アクセストークンとユーザを対応付けて記憶するために認証サーバ１００がパスワードを生成する為のＵＲＬが埋め込まれた二次元バーコードを操作部に表示する。二次元バーコードは事前にＨＤＤ３００７に記憶されているものを表示する。例えば図１２に示すような二次元バーコード表示画面１２００である。二次元バーコード表示画面１２００には二次元バーコード１２０１が表示され、ユーザはこのバーコードを読みとることで、二次元バーコードに含まれるＵＲＬにアクセスすることが可能になる。

【０１２５】

以上、本発明の実施形態における一連の処理の流れを説明した。

【０１２６】

次に、図７に示すフローチャートを用いて認証サーバ１００がアクセストークンに対応するパスワードを生成する処理を詳細に説明する。

【０１２７】

ステップＳ７０１では、携帯端末４００のＣＰＵ４０１が、撮影部４５０により画像形成装置３００の操作部３０１８に表示されたカード登録を行う為のＵＲＬ情報が埋め込まれた二次元バーコードの読み取りを行う。

【０１２８】

ステップＳ７０２では、携帯端末４００のＣＰＵ４０１が、ステップＳ７０１で読み取った二次元バーコードに埋め込まれているＵＲＬにアクセスを行う。（認証サーバ１００に対して、認可要求画面１３００の要求を行う。）

【０１２９】

ステップＳ７０３では、認証サーバ１００のＣＰＵ２０１が、認可要求画面１３００の要求を受信する。

【０１３０】

ステップＳ７０４では、認証サーバ１００のＣＰＵ２０１が、認可要求画面１３００を携帯端末４００に送信する。認可要求画面１３００は外部メモリ２１１に記憶されているものとする。

【０１３１】

ステップＳ７０５では、携帯端末４００のＣＰＵ４０１が、ステップＳ７０４で送信された認可要求画面１３００をディスプレイ４１０に表示する。認可要求画面１３００は図１３に示す認可要求画面１３００である。認可要求画面１３００にはスタートボタン１３０１が配置されており、スタートボタン１３０１の押下を受け付けることでウェブサービスサーバ２００への認可要求が行われる。

【０１３２】

ステップＳ７０６では、携帯端末４００のＣＰＵ４０１が、スタートボタン１３０１の押下を受け付け、認可要求を認証サーバ１００に送信する。

【０１３３】

ステップＳ７０７では、認証サーバ１００のＣＰＵ２０１が、認可要求を受信する。ステップＳ７０６でウェブサービスサーバ２００に対して直接認可要求を送信せずに認証サーバ１００に対して認可要求を送信することで、ステップＳ７１７でウェブサービスサーバ２００が送信するトークン情報の送信先を認証サーバ１００にすることができる。トークン情報とはアクセストークンとリフレッシュトークンを示す。

【０１３４】

ステップＳ７０８では、認証サーバ１００のＣＰＵ２０１が、ウェブサービスサーバ２００に対してトークン情報の送信先を付して認可要求を送信する。

【０１３５】

ステップＳ７０９では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ７０８で送信された認可要求を受信する。

【０１３６】

ステップＳ７１０では、ウェブサービスサーバ２００のＣＰＵ２０１が、携帯端末４００に認可画面１４００を送信する。図１４に示す認可画面１４００には、ＩＤ入力欄１４０１とパスワード入力欄１４０２とログインボタン１４０３とが配置されている。ＩＤ入力欄１４０１とパスワード入力欄１４０２はそれぞれユーザがウェブサービスサーバ２００にログインするためのＩＤ１９０２とパスワード１９０３を入力するための入力欄である。ログインボタン１４０３の押下を受け付けると、ＩＤ入力欄１４０１とパスワード入力欄１４０２に入力されたＩＤ１９０２とパスワード１９０３をウェブサービスサーバ２００に対して送信してログインを行う。

【０１３７】

ステップＳ７１１では、携帯端末４００のＣＰＵ４０１が、ウェブサービスサーバ２００が送信した認可画面１４００を受信し、認可画面１４００をディスプレイ４１０に表示する。

【０１３８】

ステップＳ７１２では、携帯端末４００のＣＰＵ４０１が、ログインボタン１４０３の押下を受け付けることでウェブサービスサーバ２００に対して認可画面１４００のＩＤ入力欄１４０１とパスワード入力欄１４０２に入力されたＩＤとパスワード（認可情報）を送信する。

【０１３９】

ステップＳ７１３では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ７１２で送信されたＩＤとパスワード（認可情報）を受信する。

【０１４０】

ステップＳ７１４では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ７１３で受信した認可情報の確認を行う。より具体的には、ステップＳ７１３で受信したＩＤとパスワードの組と、ウェブサービスサーバ２００の外部メモリ２１１に記憶されているＩＤ１９０２とパスワード１９０３の組とが一致するか否かによって確認を行う。

【０１４１】

ステップＳ７１５では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ７１３で受信した認可情報に基づいて認可が成功したか否かを判定する。具体的には外部メモリ２１１に記憶されるＩＤ１９０２とパスワード１９０３の組と、ステップＳ７１３で

受信したＩＤとパスワードの組とが一致する場合、認可が成功したと判定し、一致しない場合、認可が失敗したと判定する。認可が成功した場合処理をステップＳ７１８に進める。認可が失敗した場合処理をステップＳ７１６に進める。

【０１４２】

ステップＳ７１６では、ウェブサービスサーバ２００のＣＰＵ２０１が、ウェブサービスサーバ２００は携帯端末４００に対して認可失敗画面を送信する。

【０１４３】

ステップＳ７１７では、携帯端末４００のＣＰＵ４０１が、ウェブサービスサーバ２００から受信した認可失敗画面を操作部３０１８に表示する。認可失敗画面を表示したあと、処理を終了する。

【０１４４】

ステップＳ７１８では、ウェブサービスサーバ２００のＣＰＵ２０１が、携帯端末４００に対してウェブサービスを利用する際に使用するユーザ情報の許諾を確認するための画面であるユーザ情報使用確認画面１５００を送信する。図１５に示すユーザ情報使用確認画面１５００にはウェブサービスが使用するユーザ情報１５０１と承諾ボタン１５０２とキャンセルボタン１５０３が配置されている。ユーザはウェブサービスが使用するユーザ情報１５０１を確認し、問題がなければ承諾ボタン１５０２を押下する。

【０１４５】

ステップＳ７１９では、携帯端末４００のＣＰＵ４０１が、ユーザ情報使用確認画面１５００を受信し、ディスプレイ４１０に表示する。

【０１４６】

ステップＳ７２０では、携帯端末４００のＣＰＵ４０１が、表示されたユーザ情報使用確認画面１５００の承諾ボタン１５０２またはキャンセルボタン１５０３のいずれかが押下されたか否かを判定する。承諾ボタン１５０２が押下されたと判定した場合処理をステップＳ７１６に進め、キャンセルボタン１５０３が押下されたと判定した場合、処理をステップＳ７２１に進める。

【０１４７】

ステップＳ７２１では、ウェブサービスサーバ２００のＣＰＵ２０１が、キャンセルボタン１５０３が押下された情報を受信する。

【０１４８】

ステップＳ７２２では、ウェブサービスサーバ２００のＣＰＵ２０１が、認証サーバ１００に対して、承認キャンセルした旨を表す結果を送信する。

【０１４９】

ステップＳ７２３では、認証サーバ１００のＣＰＵ２０１が、承認キャンセルした旨を表す結果を受信する。

【０１５０】

ステップＳ７２４では、認証サーバ１００のＣＰＵ２０１が、携帯端末４００に対して認可キャンセル画面を送信する。

【０１５１】

ステップＳ７２５では、携帯端末４００のＣＰＵ４０１が、認証サーバ１００から受信した認可キャンセル画面をディスプレイ４１０に表示する。

【０１５２】

ステップＳ７２６では、ウェブサービスサーバ２００のＣＰＵ２０１が、承認の要求を受信する。

【０１５３】

ステップＳ７３３では、ウェブサービスサーバ２００のＣＰＵ２０１が、ＩＤ１９０２に対応する正当アクセストークン１９０１とリフレッシュトークン１００３を生成する。生成した正当アクセストークン１９０１とリフレッシュトークン１００３はＩＤ１９０２と対応付けて正当アクセストークンテーブル１９００に格納する。

【０１５４】

ステップＳ７２７では、ウェブサービスサーバ２００のＣＰＵ２０１が、認証サーバ１００に対して承認した旨を表す結果とＩＤ１９０２に紐づく正当アクセストークン１９０１とリフレッシュトークン１００３とを送信する。

【０１５５】

ステップＳ７２８では、認証サーバ１００のＣＰＵ２０１が、承認した旨を表す結果とＩＤ１９０２に紐づく正当アクセストークン１９０１とリフレッシュトークン１００３とを受信する（トークン情報取得手段）。

【０１５６】

ステップＳ７２９では、認証サーバ１００のＣＰＵ２０１が、カード登録用パスワード１００４を生成する（パスワード生成手段）。

【０１５７】

ステップＳ７３０では、認証サーバ１００のＣＰＵ２０１が、ステップＳ７２８で受信した正当アクセストークン１９０１とリフレッシュトークン１００３と、ステップＳ７２９で生成したカード登録用パスワード１００４を認証テーブル１０００に格納する。ユーザ名１００１は空欄で登録する。

【０１５８】

ステップＳ７３１では、認証サーバ１００のＣＰＵ２０１が、認可完了画面１６００を生成し、携帯端末４００に送信する。図１６に示す認可完了画面１６００には、カード登録用パスワード１００４を表示するパスワード表示欄１６０１が設けられている。

【０１５９】

ステップＳ７３２では、携帯端末４００のＣＰＵ４０１が、ステップＳ７３１で送信された認可完了画面１６００をディスプレイ４１０に表示する。これによりユーザはカード登録用パスワード１００４を確認することができる。

【０１６０】

以上により、図７に示すフローチャートの説明を終了する。

【０１６１】

次に図８に示すフローチャートを用いて、図６に示すカード登録処理の詳細な処理の流れを説明する。

【０１６２】

ステップＳ８０１では、画像形成装置３００のＣＰＵ３００１は、操作部３０１８にユーザ情報管理画面１８００を表示する。図１８に示すユーザ情報管理画面１８００にはユーザ名入力欄１８０１とカード登録用パスワード入力欄１８０２とカード検知ボタン１８０３とが配置されている。ユーザ名入力欄１８０１はユーザ名１００１を入力するための入力欄である。カード登録用パスワード入力欄１８０２は、カード登録用パスワードを入力する為の入力欄である。カード検知ボタン１８０３は押下されるとカードリーダ３１０でＩＣカードのカードＩＤ１１０１を読み取る。

【０１６３】

ステップＳ８０２では、画像形成装置３００のＣＰＵ３００１は、ユーザ名入力欄１８０１とカード登録用パスワード入力欄１８０２への入力を受け付ける。（パスワード受付手段・認証情報取得手段）

【０１６４】

ステップＳ８１２では、画像形成装置３００のＣＰＵ３００１は、カード検知ボタン１８０３が押下されたか否かを判定する。カード検知ボタン１８０３が押下された場合処理をステップＳ８１３に進める。カード検知ボタン１８０３が押下されるまで待機する。

【０１６５】

ステップＳ８１３では、画像形成装置３００のＣＰＵ３００１は、カードリーダ３１０でＩＣカードのカードＩＤ１１０１を読み取る。（認証情報取得手段）

【０１６６】

ステップＳ８０３では、画像形成装置３００のＣＰＵ３００１は、認証サーバ１００に対してステップＳ８０２で入力されたユーザ名１００１、カード登録用パスワード１００

４、カードＩＤ１１０１を送信する。
【０１６７】
ステップＳ８０４では、認証サーバ１００のＣＰＵ２０１は、ユーザ名１００１、カード登録用パスワード１００４、カードＩＤ１１０１を受信する。
【０１６８】
ステップＳ８０５では、認証サーバ１００のＣＰＵ２０１は、ステップＳ８０４で受信したカード登録用パスワード１００４が認証テーブル１０００にすでに登録されているかを照合する。
【０１６９】
ステップＳ８０６では、認証サーバ１００のＣＰＵ２０１は、ステップＳ８０５で行った照合処理の判定を行う。カード登録用パスワード１００４が認証テーブル１０００に登録されていた場合は、ステップＳ８０９へ処理を移す。登録されていなかった場合は、ステップＳ８０７へ処理を移す。
【０１７０】
ステップＳ８０７では、認証サーバ１００のＣＰＵ２０１は、画像形成装置３００に対してカード登録用パスワード照合失敗画面を送信する。
【０１７１】
ステップＳ８０８では、画像形成装置３００のＣＰＵ３００１は、認証サーバ１００から受信したカード登録用パスワード照合失敗画面を操作部に表示する。
【０１７２】
ステップＳ８０９では、認証サーバ１００のＣＰＵ２０１は、カード登録用パスワード１００４に対応するユーザ名１００１にステップＳ８０４で受信したユーザ名１００１を登録することで認証テーブル１０００を更新する。更にステップＳ８０４で受信したカードＩＤとユーザＩＤをカードＩＤテーブル１１００に登録する（保存手段）。登録が完了したら、登録が行われたレコードのカード登録用パスワード１００４を削除する。こうすることで、他のユーザからの登録要求により偶然パスワードが一致し、ユーザ情報が上書きされてしまうことを防止する。
【０１７３】
このように、認証サーバ１００が生成した登録用パスワードを用いることで、画像形成装置３００に認証を行うためのカードＩＤ１１０１、ユーザ名１００１、アクセストークン１００２、リフレッシュトークン１００３を対応付けて記憶することができる。これにより、ユーザは画像形成装置３００に認証することで、ウェブサービスサーバ２００のウェブサービス情報を取得し、画像形成装置３００でウェブサービス情報を利用することができる。
【０１７４】
ステップＳ８１０では、認証サーバ１００のＣＰＵ２０１は、画像形成装置３００に対してカードＩＤ登録成功画面を送信する。
【０１７５】
ステップＳ８０９では、画像形成装置３００のＣＰＵ３００１は、認証サーバ１００から受信したカードＩＤ登録成功画面を操作部３０１８に表示する。
【０１７６】
以上で図８に示すフローチャートの説明を終了する。
【０１７７】
次に図９に示すフローチャートを用いて図６に示すウェブサービス情報表示処理の詳細な処理の流れを説明する。
【０１７８】
ステップＳ９０１では、画像形成装置３００のＣＰＵ３００１が、アクセストークン取得要求を認証サーバ１００に対して送信する。
【０１７９】
ステップＳ９０２では、認証サーバ１００のＣＰＵ２０１が、アクセストークン取得要

求を受信する。
【０１８０】
ステップＳ９０３では、認証サーバ１００のＣＰＵ２０１が、ステップＳ６０４で送信したカードＩＤ１１０１に対応するアクセストークン１００２を取得する。
【０１８１】
ステップＳ９０４では、認証サーバ１００のＣＰＵ２０１が、ステップＳ９０３で取得したアクセストークン１００２を画像形成装置３００に対して送信する。
【０１８２】
ステップＳ９０５では、画像形成装置３００のＣＰＵ３００１が、アクセストークン１００２を受信する。
【０１８３】
ステップＳ９０６では、画像形成装置３００のＣＰＵ３００１が、ウェブサービスサーバ２００に対してウェブサービスであるカレンダーのカレンダーデータの送信要求を、ステップＳ９０５で受信したアクセストークン１００２と併せて送信する。
【０１８４】
ステップＳ９０７では、ウェブサービスサーバ２００のＣＰＵ２０１が、カレンダーデータの送信要求とアクセストークン１００２とを受信する。
【０１８５】
ステップＳ９０８では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ９０７で受信したアクセストークン１００２が正当であるか否かを判定する。具体的には、ウェブサービスサーバ２００に外部メモリ２１１に記憶される正当アクセストークンテーブル１９００に基づいて判定する。正当アクセストークンテーブル１９００の正当アクセストークン１９０１にステップＳ９０７で受信したアクセストークン１００２が存在するか否かを判定し、存在すると判定した場合には正当であると判断する。存在しないと判定した場合は正当でないと判断する。ステップＳ９０７で受信したアクセストークン１００２が正当であると判定した場合には処理をステップＳ９１２に進め、ステップＳ９０７で受信したアクセストークン１００２が正当でないと判定した場合は、処理をステップＳ９０９に進める。
【０１８６】
ステップＳ９０９では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ９０７で受信したアクセストークン１００２が正当でなかった旨を伝えるエラー画面を画像形成装置３００に対して送信する。
【０１８７】
ステップＳ９１０では、画像形成装置３００のＣＰＵ３００１が、ウェブサービスサーバ２００から送信されたエラー画面を受信する。
【０１８８】
ステップＳ９１１では、画像形成装置３００のＣＰＵ３００１が、ステップＳ９１０で受信したエラー画面を操作部３０１８に表示する。
【０１８９】
ステップＳ９１２では、ウェブサービスサーバ２００のＣＰＵ２０１が、正当であると判定したアクセストークン１００２に基づいて、ユーザのカレンダーデータを取得する（情報取得手段）。
【０１９０】
ステップＳ９１３では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ９１２で取得したカレンダーデータに基づいてカレンダー画面２１００を生成する。例えば図２１に示すカレンダー画面２１００である。
【０１９１】
ステップＳ９１４では、ウェブサービスサーバ２００のＣＰＵ２０１が、ステップＳ９１３で生成したカレンダー画面２１００を画像形成装置３００に送信する。
【０１９２】

ステップＳ９１５では、画像形成装置３００のＣＰＵ３００１が、ステップＳ９１４で送信されたカレンダー画面２１００を受信する。

【０１９３】

ステップＳ９１６では、画像形成装置３００のＣＰＵ３００１が、ステップＳ９１５で受信したカレンダー画面２１００を操作部３０１８に表示する。

【０１９４】

以上で図９に示すフローチャートの説明を終了する。

【０１９５】

以上のように、ユーザは画像形成装置３００に認証するだけでウェブサービスサーバ２００が提供するウェブサービスのウェブサービス情報を画像形成装置３００で利用することが可能になる。

【０１９６】

以上、本発明の実施形態によれば、ウェブサービスサーバから取得したトークン情報とユーザの認証情報を容易に紐づけることの可能な仕組みを提供することが可能となる。

【０１９７】

本発明は、例えば、システム、装置、方法、プログラム若しくは記憶媒体等としての実施形態も可能であり、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よいし、また、１つの機器からなる装置に適用してもよい。

【０１９８】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムを、システム或いは装置に直接、或いは遠隔から供給するものを含む。そして、そのシステム或いは装置のコンピュータが前記供給されたプログラムコードを読み出して実行することによっても達成される場合も本発明に含まれる。

【０１９９】

したがって、本発明の機能処理をコンピュータで実現するために、前記コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明は、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。

【０２００】

その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等の形態であってもよい。

【０２０１】

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、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷなどがある。また、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などもある。

【０２０２】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続する。そして、前記ホームページから本発明のコンピュータプログラムそのもの、若しくは圧縮され自動インストール機能を含むファイルをハードディスク等の記録媒体にダウンロードすることによっても供給できる。

【０２０３】

また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明に含まれるものである。

【０２０４】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせる。そして、ダウンロードした鍵情報を使用す

ることにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【０２０５】

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って、前述した実施形態の機能が実現される。その他、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部又は全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【０２０６】

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る。その後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部又は全部を行い、その処理によっても前述した実施形態の機能が実現される。

【０２０７】

なお、前述した実施形態は、本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。即ち、本発明はその技術思想、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

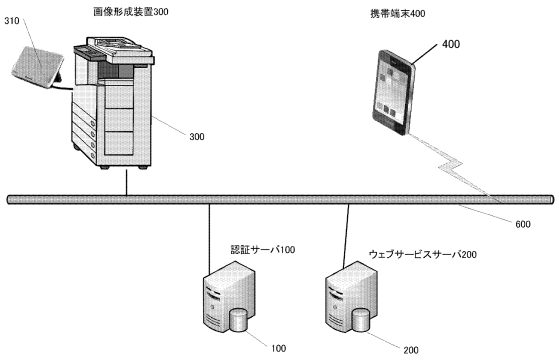
【符号の説明】

【０２０８】

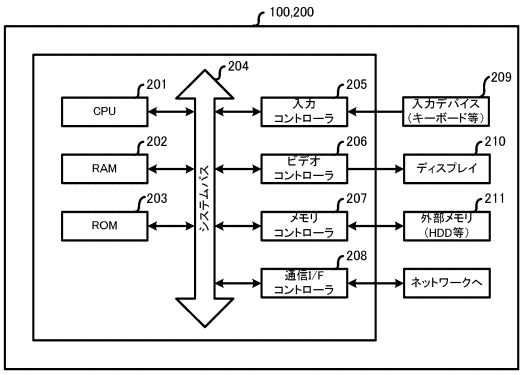
１００　認証サーバ
２００　ウェブサービスサーバ
３００　画像形成装置
３１０　ＩＣカードリーダ
６００　ＬＡＮ
２０１　ＣＰＵ
２０２　ＲＡＭ
２０３　ＲＯＭ
２０４　システムバス
２０５　入力コントローラ
２０６　ビデオコントローラ
２０７　メモリコントローラ
２０８　通信Ｉ／Ｆコントローラ
２０９　キーボード
２１０　ＣＲＴディスプレイ
２１１　外部メモリ
３００１　ＣＰＵ
３００２　ＲＯＭ
３００３　ネットワークインタフェース
３００４　モデム
３００５　操作部Ｉ／Ｆ
３００６　ＲＡＭ
３００７　外部記憶装置
３００８　イメージバスＩ／Ｆ
３００９　外部Ｉ／Ｆ
３０１０　ラスタイメージプロセッサ
３０１１　プリンタＩ／Ｆ
３０１２　スキャナＩ／Ｆ
３０１３　画像処理部
３０１４　プリンタ

３０１５　スキャナ
４０１　ＣＰＵ
４０２　ＲＯＭ
４０３　ＲＡＭ
４０４　ディスプレイコントローラ
４０５　タッチパネルコントローラ
４０６　カメラコントローラ
４０７　センサコントローラ
４０８　ネットワークコントローラ
４０９　フラッシュメモリコントローラ
４１０　ディスプレイ
４１１　タッチパネル
４１２　カメラ
４１３　センサ
４１４　フラッシュメモリ

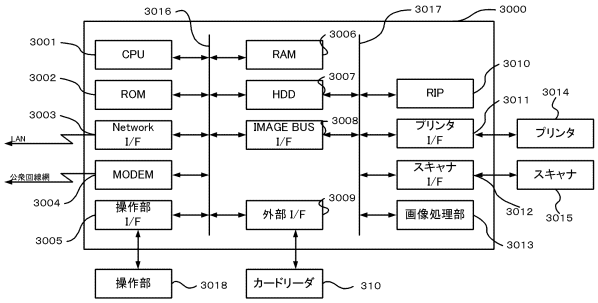
【図１】



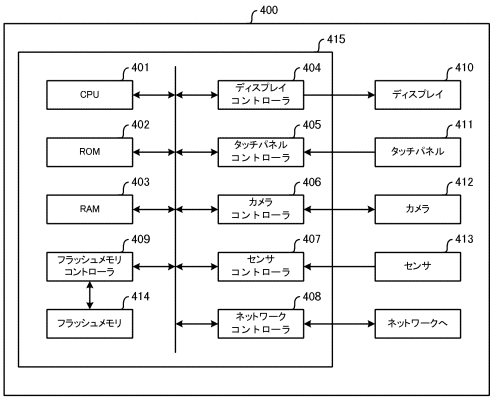
【図２】



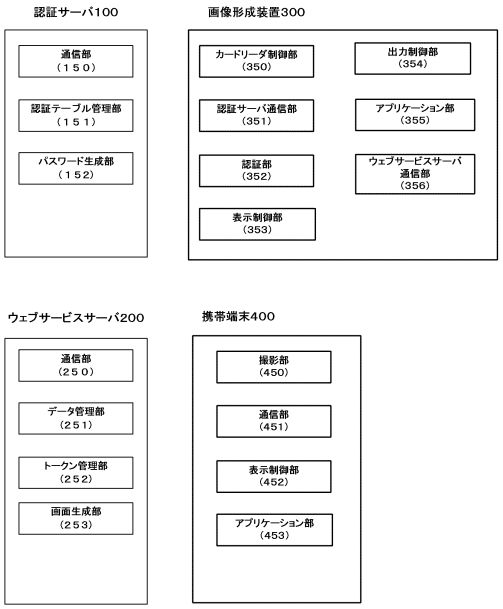
【図３】


3016
3017
3000
3001
CPU
RAM
3006
3002
ROM
HDD
3007
RIP
3010
3003
Network I/F
IMAGE BUS I/F
3008
プリンタ I/F
3011
3014
プリンタ
LAN
公衆回線網
MODEM
スキャナ I/F
スキャナ
3004
操作部 I/F
外部 I/F
3009
画像処理部
3012
3015
3005
3013
操作部
3018
カードリーダ
310

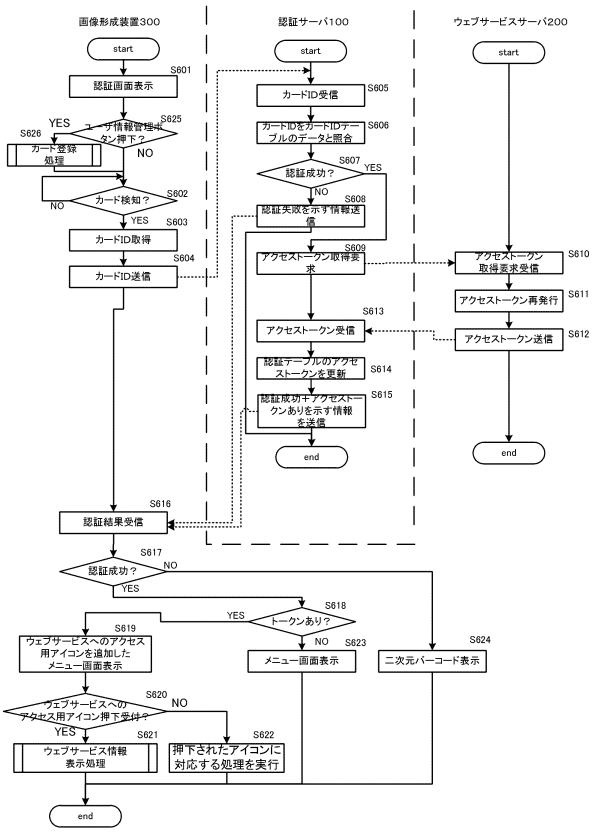
【図４】


400
415
401
CPU
404
ディスプレイコントローラ
410
ディスプレイ
402
ROM
405
タッチパネルコントローラ
411
タッチパネル
403
RAM
406
カメラコントローラ
412
カメラ
409
フラッシュメモリコントローラ
407
センサコントローラ
413
センサ
414
フラッシュメモリ
408
ネットワークコントローラ
ネットワークへ

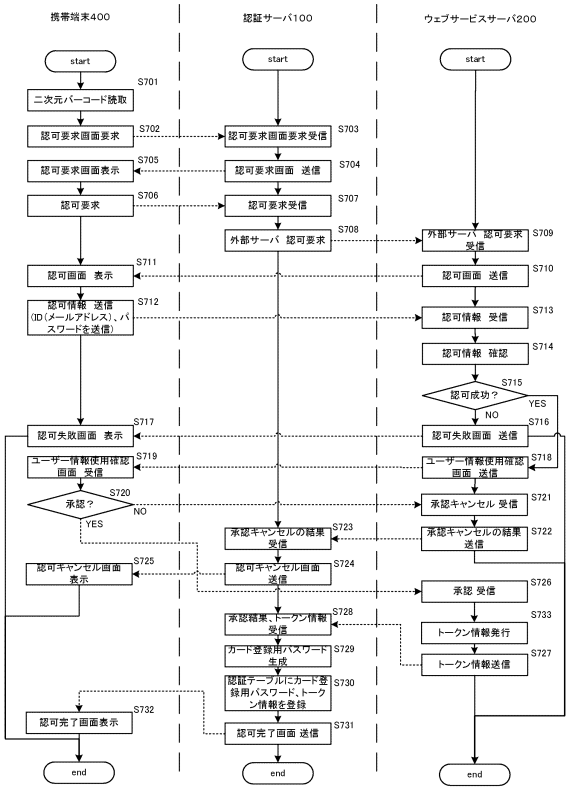
【図５】


認証サーバ100
通信部（１５０）
認証テーブル管理部（１５１）
パスワード生成部（１５２）
画像形成装置300
カードリーダ制御部（350）
出力制御部（354）
認証サーバ通信部（351）
アプリケーション部（355）
認証部（352）
ウェブサービスサーバ通信部（356）
表示制御部（353）
ウェブサービスサーバ200
通信部（２５０）
データ管理部（２５１）
トークン管理部（２５２）
画面生成部（２５３）
携帯端末400
撮影部（450）
通信部（451）
表示制御部（452）
アプリケーション部（453）

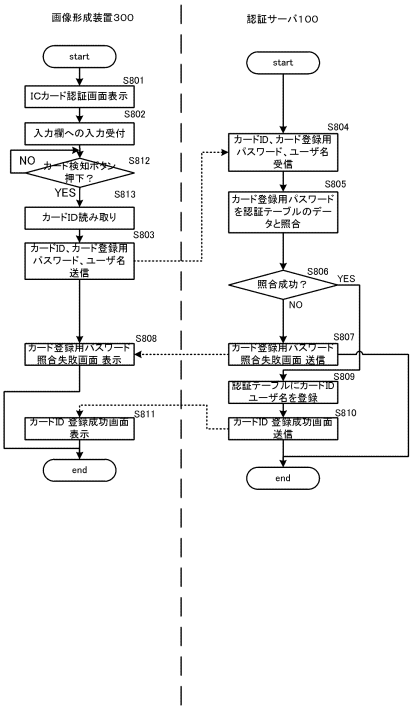
【図６】


画像形成装置300
認証サーバ100
ウェブサービスサーバ200
start
S601
認証画面表示
S625
ユーザ情報管理ボタン押下？
YES
NO
S626
カード登録処理
S602
カード検知？
NO
YES
S603
カードID取得
S604
カードID送信
S605
カードID受信
S606
カードIDをカードIDテーブルのデータと照合
S607
認証成功？
YES
NO
S608
認証失敗を示す情報送信
S609
アクセストークン取得要求
S610
アクセストークン取得要求受信
S611
アクセストークン再発行
S612
アクセストークン送信
S613
アクセストークン受信
S614
認証テーブルのアクセストークンを更新
S615
認証成功＋アクセストークンありを示す情報を送信
end
S616
認証結果受信
S617
認証成功？
NO
YES
S618
トークンあり？
YES
NO
S619
ウェブサービスへのアクセス用アイコンを追加したメニュー画面表示
S623
メニュー画面表示
S624
二次元バーコード表示
S620
ウェブサービスへのアクセス用アイコン押下受付？
NO
YES
S621
ウェブサービス情報表示処理
S622
押下されたアイコンに対応する処理を実行
end

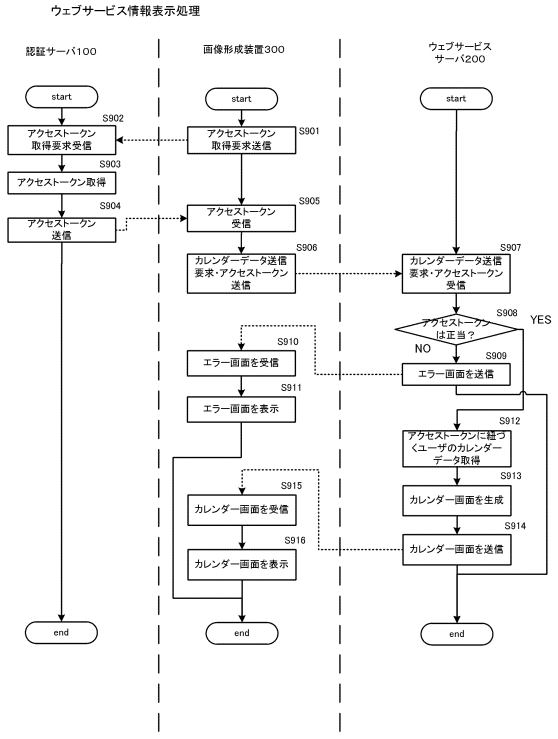
【図７】



【図８】



【図９】



【図１０】

認証テーブル1000

1001 ユーザ名	1002 アクセストークン	1003 リフレッシュトークン	1004 カード登録用パスワード
user01	C1Z21A	12KIU8	1234
user02	GX39AB	HD8J71	9876
user03	GZA19YZ	O8H3B5	5678

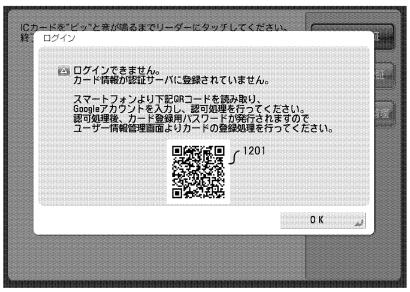
【図１１】

カードIDテーブル1100

カードID (1101)	ユーザ名 (1001)
sid00001	user01
sid00002	user02
sid00003	user03

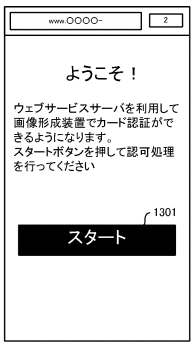
【図１２】

二次元バーコード表示画面1200



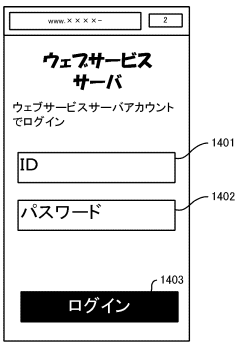
【図１３】

認可要求画面1300

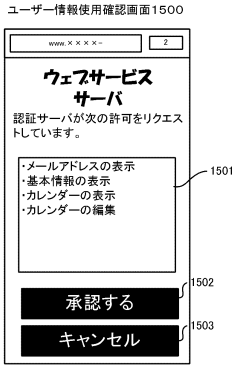


【図１４】

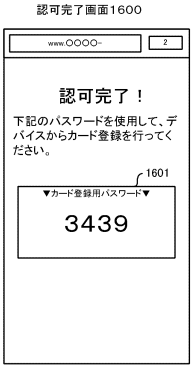
認可画面1400



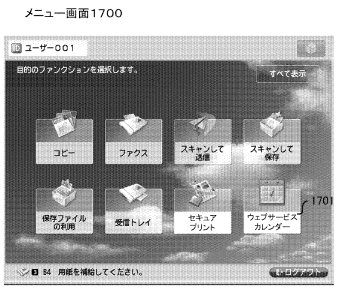
【図１５】



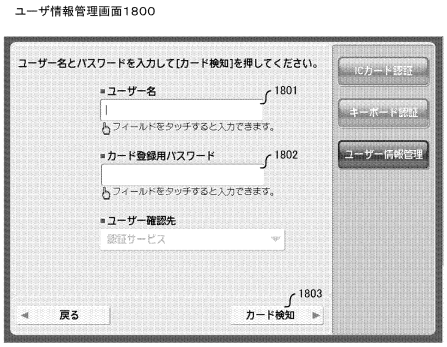
【図１６】



【図１７】



【図１８】

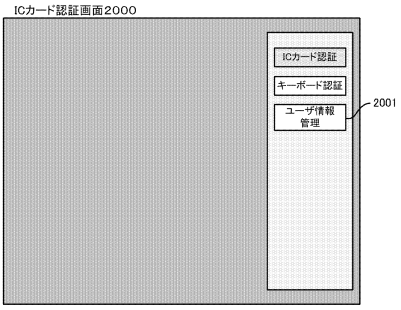


【図１９】

正当アクセストークンテーブル1900

1901 正当アクセストークン	1003 リフレッシュトークン	1902 ID	1903 パスワード
C1Z21A	12KIU8	ID1	pass
GX39AB	HD8J71	ID2	pass

【図２０】



【図２１】

カレンダー画面2100

2014年12月

月曜日	火曜日	水曜日	木曜日	金曜日	土曜日	日曜日
12月1日	2	3	4	5	6	7
	予定あり					
8	9	10	11	12	13	14
			予定あり			
15	16	17	18	19	20	21
		予定あり				
22	23	24	25	26	27	28
	予定あり			出願日		
29	30	31	1月1日	2	3	4

フロントページの続き

審査官　平井　誠

(56)参考文献　特開２００８－０７１３１８（ＪＰ，Ａ）
特開２０１４－０１０７６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－８８