

(19) 日本国特許庁 (JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2018-45682

(P2018-45682A)

(43) 公開日 平成30年3月22日 (2018.3.22)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/32 (2013.01)	G06F 21/32	5B043
G06T 7/00 (2017.01)	G06T 7/00 510F	
G06F 21/45 (2013.01)	G06F 21/45	
G06F 21/31 (2013.01)	G06F 21/31	

審査請求 未請求 請求項の数 12 O L (全 18 頁)

(21) 出願番号	特願2017-132121 (P2017-132121)	(71) 出願人	000006747
(22) 出願日	平成29年7月5日 (2017.7.5)		株式会社リコー
(31) 優先権主張番号	特願2016-174874 (P2016-174874)		東京都大田区中馬込 1 丁目 3 番 6 号
(32) 優先日	平成28年9月7日 (2016.9.7)	(74) 代理人	100089118
(33) 優先権主張国	日本国 (JP)		弁理士 酒井 宏明
		(72) 発明者	渡邊 元気
			東京都大田区中馬込 1 丁目 3 番 6 号 株式
			会社リコー内
		(72) 発明者	井口 悟
			東京都大田区中馬込 1 丁目 3 番 6 号 株式
			会社リコー内
		F ターム (参考)	5B043 AA05 AA09 BA04 CA10 DA05
			EA02 FA03 FA07 GA13 GA18

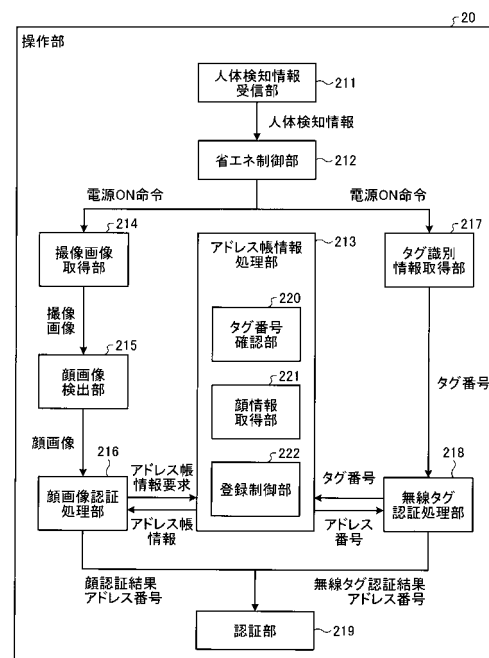
(54) 【発明の名称】 情報処理装置、情報処理システム、情報処理方法およびプログラム

(57) 【要約】

【課題】 顔認証に用いられる顔情報を登録する処理の効率を向上させる。

【解決手段】 本発明の情報処理装置は、記憶部とタグ識別情報取得部と顔情報取得部と登録制御部とを備える。記憶部は、無線タグを識別するタグ識別情報と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を記憶する。タグ識別情報取得部は、タグ識別情報を取得する。顔情報取得部は、アドレス帳情報を参照し、タグ識別情報取得部により取得されたタグ識別情報に対して、ユーザの顔情報が対応付けられていない場合は、タグ識別情報を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて顔情報を取得する。登録制御部は、顔情報取得部により取得された顔情報をタグ識別情報に対応付けてアドレス帳情報に登録する制御を行う。

【選択図】 図 5



【特許請求の範囲】

【請求項 1】

無線通信可能な媒体を示す無線タグを識別するタグ識別情報と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を記憶する記憶部と、

前記タグ識別情報を取得するタグ識別情報取得部と、

前記アドレス帳情報を参照し、前記タグ識別情報取得部により取得された前記タグ識別情報に対して、ユーザの顔情報が対応付けられていない場合は、前記タグ識別情報を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて前記顔情報を取得する顔情報取得部と、

前記顔情報取得部により取得された前記顔情報を前記タグ識別情報に対応付けて前記アドレス帳情報に登録する制御を行う登録制御部と、を備える、
情報処理装置。

10

【請求項 2】

前記撮像画像を取得する撮像画像取得部と、

前記撮像画像取得部により取得された前記撮像画像から顔画像を検出する顔画像検出部と、をさらに備え、

前記顔情報取得部は、前記顔画像検出部により検出された前記顔画像に基づいて前記顔情報を取得する、

請求項 1 に記載の情報処理装置。

【請求項 3】

20

前記顔画像検出部により検出された前記顔画像に対応する前記顔情報が前記アドレス帳情報に存在するか否かを判断する顔画像認証処理を行う顔画像認証処理部をさらに備える、

請求項 2 に記載の情報処理装置。

【請求項 4】

前記タグ識別情報取得部により取得された前記タグ識別情報が前記アドレス帳情報に存在するか否かを判断する無線タグ認証処理を行う無線タグ認証処理部をさらに備える、

請求項 3 に記載の情報処理装置。

【請求項 5】

30

前記顔画像認証処理の結果と前記無線タグ認証処理の結果とに基づき、前記タグ識別情報取得部により取得された前記タグ識別情報が前記アドレス帳情報に存在し、かつ、該タグ識別情報に対応付けられた前記顔情報が前記顔画像検出部により検出された前記顔画像に対応する前記顔情報と一致する場合は、前記無線タグを所持するユーザは、前記情報処理装置を使用する権限を有することを認める認証部をさらに備える、

請求項 4 に記載の情報処理装置。

【請求項 6】

前記情報処理装置は、操作を受け付ける操作部と、前記操作部で受け付けた前記操作に応じた動作を行う本体と、を備える画像処理装置であり、

前記操作部は、

前記タグ識別情報取得部と、前記顔情報取得部と、前記登録制御部と、を少なくとも有する、

40

請求項 1 乃至 5 のうちの何れか 1 項に記載の情報処理装置。

【請求項 7】

前記情報処理装置は、操作を受け付ける操作部と、前記操作部で受け付けた前記操作に応じた動作を行う本体と、を備える画像処理装置であり、

前記本体は、

第 1 のオペレーティングシステムと、

前記第 1 のオペレーティングシステム上で動作するアプリケーションにより制御され、スキャナまたはプリンタとして機能するエンジン部と、

前記記憶部と、

50

を備え、

前記操作部は、

第2のオペレーティングシステムと、

前記第2のオペレーティングシステム上で動作し、前記タグ識別情報取得部により取得された前記タグ識別情報と前記アドレス帳情報に含まれる前記タグ識別情報とを比較してタグ認証を行うタグ認証アプリケーションと、

前記第2のオペレーティングシステム上で動作し、前記顔情報取得部と前記登録制御部とを有する顔情報登録アプリケーションと、

を備える、

請求項1に記載の情報処理装置。

10

【請求項8】

前記操作部は、

前記第2のオペレーティングシステム上で動作し、前記撮像画像を取得する撮像画像取得部と、前記撮像画像取得部により取得された前記撮像画像から顔画像を検出する顔画像検出部と、前記顔画像検出部により検出された前記顔画像に対応する前記顔情報が前記アドレス帳情報に存在するか否かを判断する顔画像認証処理と、を有する顔認証アプリケーション、

を更に備え、

前記顔情報登録アプリケーションと前記顔認証アプリケーションとは1つのアプリケーションである、

20

請求項7に記載の情報処理装置。

【請求項9】

前記顔情報登録アプリケーションは、前記タグ認証後に、ユーザにより入力されたパスワードと、前記アドレス帳情報において前記タグ識別情報に対応付けられたパスワードとを比較してパスワード認証を行うパスワード認証部、を更に有し、

前記登録制御部は、前記パスワード認証の成功時に、前記顔情報を前記タグ識別情報に対応付けて前記アドレス帳情報に登録する制御を許可する、

請求項8に記載の情報処理装置。

【請求項10】

無線通信可能な媒体を示す無線タグを識別するタグ識別情報と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を記憶する記憶部と、

30

前記タグ識別情報を取得するタグ識別情報取得部と、

前記アドレス帳情報を参照し、前記タグ識別情報取得部により取得された前記タグ識別情報に対して、ユーザの顔情報が対応付けられていない場合、前記タグ識別情報を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて前記顔情報を取得する顔情報取得部と、

前記顔情報取得部により取得された前記顔情報を前記タグ識別情報に対応付けて前記アドレス帳情報に登録する制御を行う登録制御部と、を備える、

情報処理システム。

【請求項11】

40

無線通信可能な媒体を示す無線タグを識別するタグ識別情報を取得するタグ識別情報取得ステップと、

前記タグ識別情報と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を参照し、前記タグ識別情報取得ステップにより取得された前記タグ識別情報に対して、ユーザの顔情報が対応付けられていない場合、前記タグ識別情報を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて前記顔情報を取得する顔情報取得ステップと、

前記顔情報取得ステップにより取得された前記顔情報を前記タグ識別情報に対応付けて前記アドレス帳情報に登録する制御を行う登録制御ステップと、を含む、

情報処理方法。

50

【請求項 12】

コンピュータに、

無線通信可能な媒体を示す無線タグを識別するタグ識別情報を取得するタグ識別情報取得ステップと、

前記タグ識別情報と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を参照し、前記タグ識別情報取得ステップにより取得された前記タグ識別情報に対して、ユーザの顔情報が対応付けられていない場合、前記タグ識別情報を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて前記顔情報を取得する顔情報取得ステップと、

前記顔情報取得ステップにより取得された前記顔情報を前記タグ識別情報に対応付けて前記アドレス帳情報に登録する制御を行う登録制御ステップと、を実行させるためのプログラム。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置、情報処理システム、情報処理方法およびプログラムに関する。

【背景技術】

【0002】

従来、顔認証技術を利用して、MFPを使用するユーザの認証を行う技術が知られている。例えば特許文献1には、顔などの生体情報を取得して認証を行う認証方式と、タグ内の情報を無線により読み取ることにより認証を行う認証方式とを組み合わせた複合認証方式が開示されている。

20

【発明の概要】

【発明が解決しようとする課題】

【0003】

しかしながら、従来の顔認証方式を利用したシステムでは、例えばMFPなどの機器（認証を条件に使用できる機器）の管理者が、予めユーザごとの個人情報（氏名、住所、メールアドレス等）の登録作業に加えて、顔認証に用いられる顔情報の元となる顔画像を撮影し、その撮影により得られた画像に基づく顔情報と個人情報とを紐付けて登録する作業が必要になっていた。つまり、顔認証に用いられる顔情報を登録する処理の効率が悪いという問題がある。

30

【0004】

本発明は、上記に鑑みてなされたものであって、顔認証に用いられる顔情報を登録する処理の効率を向上させることが可能な情報処理装置、情報処理システム、情報処理方法およびプログラムを提供することを目的とする。

【課題を解決するための手段】

【0005】

上述した課題を解決し、目的を達成するために、本発明は、無線通信可能な媒体を示す無線タグを識別するタグ識別情報と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を記憶する記憶部と、前記タグ識別情報を取得するタグ識別情報取得部と、前記アドレス帳情報を参照し、前記タグ識別情報取得部により取得された前記タグ識別情報に対して、ユーザの顔情報が対応付けられていない場合は、前記タグ識別情報を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて前記顔情報を取得する顔情報取得部と、前記顔情報取得部により取得された前記顔情報を前記タグ識別情報に対応付けて前記アドレス帳情報に登録する制御を行う登録制御部と、を備える情報処理装置である。

40

【発明の効果】

【0006】

本発明によれば、顔認証に用いられる顔情報を登録する処理の効率を向上させることが

50

できる。

【図面の簡単な説明】

【0007】

【図1】図1は、第1の実施形態に係る情報処理システムの構成の一例を示す図である。

【図2】図2は、第1の実施形態に係る情報処理システムにおいて無線タグを所持するユーザがタグリーダに無線タグを翳すときの様子を説明するための図である。

【図3】図3は、第1の実施形態に係るMFPのハードウェア構成例を示す図である。

【図4】図4は、第1の実施形態に係るMFPのソフトウェア構成例を示す図である。

【図5】図5は、第1の実施形態に係るMFPが有する機能の一例を示す図である。

【図6】図6は、第1の実施形態に係るデフォルトのアドレス帳情報の一例を示す図である。

10

【図7】図7は、第1の実施形態に係る特徴点情報が登録された後のアドレス帳情報の一例を示す図である。

【図8】図8は、第1の実施形態に係るPCの動作例を示すフローチャートである。

【図9】図9は、第1の実施形態に係るMFPの動作例を示すフローチャートである。

【図10】図10は、第2の実施形態に係る操作部のアプリ層の構成例を示す図である。

【図11】図11は、第2の実施形態に係る操作部が有する機能とアプリケーションとの関係例を示す図である。

【図12】図12は、第2の実施形態に係るMFPの動作例を示すフローチャートである。

20

【発明を実施するための形態】

【0008】

（第1の実施形態）

以下、添付図面を参照しながら、本発明に係る情報処理装置、情報処理システム、情報処理方法およびプログラムの実施形態を詳細に説明する。以下では、本発明に係る情報処理装置として、画像処理装置の一つである複合機（MFP：Multifunction Peripheral）を例に挙げて説明するが、これに限定されるものではない。例えば情報処理装置としては、カメラ、プロジェクタ、インタラクティブホワイトボード（電子黒板）、テレビ会議／Web会議システムの専用端末、デジタルサイネージ、プロダクションプリンタ、3Dプリンタ、ファクシミリなどが挙げられる。要するに、情報処理装置は認証を条件として使用が許可される装置であればよく、その種類は任意である。なお、複合機とは、コピー機能、スキャナ機能、プリンタ機能、ファクシミリ機能などの複数の異なる機能を有する装置である。

30

【0009】

図1は、本実施形態の情報処理システム100の構成の一例を示す図である。図1に示すように、情報処理システム100は、MFP1と、外部ツールとして機能するPC（Personal Computer）2とを備え、これらはインターネットなどのネットワーク8を介して相互に接続可能である。後述するように、PC2は、MFP1の管理者の操作に応じて、ユーザの個人情報（氏名、住所、メールアドレスなど）や、無線通信可能な媒体を示す無線タグを識別するタグ番号（タグ識別情報の一例）を後述のアドレス帳情報に登録する処理を行う。

40

【0010】

この例では、MFP1を使用する1以上のユーザごとに、タグ番号が記憶された無線タグ114が予め配布されている。そして、図2に示すように、無線タグ114を所持するユーザが、MFP1に設置されたタグリーダ113に無線タグ114をかざすと、無線タグ114とタグリーダ113との間で近距離無線通信が行われ、無線タグ114に記憶されたタグ番号がタグリーダ113によって読み取られる。また、この例では、タグ番号を取得可能な範囲に対応する撮像範囲を撮像するためのカメラ112（言い換えれば、タグリーダ113に対して無線タグ114をかざすユーザを撮像するためのカメラ112）がMFP1に接続されている。このカメラ112による撮像で得られた撮像画像から、無線

50

タグ 114 をかざすユーザの顔画像を検出することができ、検出された顔画像を用いて、ユーザの認証が行われる。具体的な内容については後述する。なお、撮像とは、レンズなどの光学系により結像された被写体の像を、電気信号に変換することを指す。

【0011】

図 3 は、第 1 の実施形態の複合機（MFP：Multifunction Peripheral）1 のハードウェア構成図である。MFP 1 は、操作を受け付ける操作部 20 と、操作部 20 で受け付けた操作に応じた動作を行う本体 10 と、を備える画像処理装置である。この例では、本体 10 は、例えばコピー機能、スキャナ機能、ファクシミリ機能、プリンタ機能等の各種の機能を備える。

【0012】

図 3 の例では、本体 10 と操作部 20 は、専用の通信路 30 を介して相互に通信可能に接続されている。通信路 30 は、例えば USB（Universal Serial Bus）規格のものをを用いることもできるが、有線か無線かを問わず任意の規格のものであってよい。また、本体 10 は、コピー機能、スキャナ機能、ファクシミリ機能、プリンタ機能等の画像生成機能のうち、一つの機能を有していてもよいし又は複数の機能を有していてもよい。

【0013】

操作部 20 としては、単独で完結した情報処理を実行可能な電子機器を用いることができる。一例として、操作部 20 としては、スマートフォン又はタブレット型端末等の情報処理端末を用いることができる。この場合、操作部 20 として用いられる情報処理端末は、MFP 1 の操作部として機能する。

【0014】

より詳しくは、操作部 20 として用いられる情報処理端末は、従来、MFP 1 専用の操作部として固定され設置されていた操作パネルの代わりに、MFP 1 に装着及び取り外し可能に接続される。すなわち、操作部 20 として用いられる情報処理端末は、例えば MFP 1 の操作パネルが配置される位置等の所定の位置に取り外し可能（分離可能）ながらも、MFP 1 と一体的に設置される。従って、操作部 20 として用いられる情報処理端末及び MFP 1 は、一台の装置として把握されてもよい。操作部 20 である情報処理端末は、MFP 1 から取り外されると、MFP 1 との間で、例えば Bluetooth（登録商標）又は赤外線通信等の無線通信を行い、MFP 1 の操作部として機能する。

【0015】

（本体のハードウェア構成）

次に、本体 10 のハードウェア構成について説明する。図 3 に示すように、本体 10 は、CPU 11 と、ROM 12 と、RAM 13 と、HDD（ハードディスクドライブ）14 と、人体検知センサ 15 と、エンジン部 16 と、接続 I/F 17 と、通信 I/F 18 と、を備える。以上の各部 11～18 は、システムバス 19 を介して相互に接続されている。

【0016】

CPU 11 は、本体 10 の動作を統括的に制御する。CPU 11 は、RAM 13 をワークエリア（作業領域）として ROM 12 又は HDD 14 等に格納されたプログラムを実行することで、本体 10 全体の動作を制御し、上述したコピー機能、スキャナ機能、ファクシミリ機能、プリンタ機能などの各種機能を実現する。

【0017】

人体検知センサ 15 は、検知範囲内の人体の有無を検知するセンサである。ここでは、検知範囲はカメラ 112 の撮像範囲を少なくとも含む範囲である。人体検知センサ 15 としては、例えば焦電センサなどが用いられる。

【0018】

エンジン部 16 は、コピー機能、スキャナ機能、ファクシミリ機能及びプリンタ機能等を実現させるための、汎用的な情報処理及び通信以外の処理を行うハードウェアである。エンジン部 16 は、例えば原稿の画像をスキャンして読み取るスキャナ、用紙等のシート材への印刷を行うプロッタ、ファクシミリ通信を行うファクシミリ通信部等を備えている。さらに、印刷済みシート材を仕分けるフィニッシャ及び原稿を自動給送する ADF（自

10

20

30

40

50

動原稿給送装置)のような特定のオプションを備えることもできる。

【0019】

接続 I / F 17 は、通信路 30 を介して操作部 20 と通信するためのインタフェースである。なお、図 3 において、通信路 30 は、有線的に図示されているが、上述のように操作部 20 は、MFP 1 の本体 10 に対して装着及び取り外しが可能となっている。このため、操作部 20 を MFP 1 に装着しているときには、通信路 30 は有線通信路として機能し、操作部 20 を MFP 1 から取り外したときには、通信路 30 は無線通信路として機能する。通信 I / F 18 は、ネットワーク 8 上の PC 2 等の外部装置と通信するためのインタフェースである。

【0020】

(操作部のハードウェア構成)

次に、操作部 20 のハードウェア構成について説明する。図 3 に示すように、操作部 20 は、CPU 21 と、ROM 22 と、RAM 23 と、フラッシュメモリ 24 と、通信 I / F 25 と、カメラ I / F 26 と、タグリーダ I / F 27 と、接続 I / F 28 と、操作パネル 29 と、を備え、これらがシステムバス 40 を介して相互に接続されている。

【0021】

CPU 21 は、操作部 20 の動作を統括的に制御する。CPU 21 は、RAM 23 をワークエリア(作業領域)として ROM 22 またはフラッシュメモリ 24 に格納されたプログラムを実行することで操作部 20 全体の動作を制御する。通信 I / F 25 は、例えばネットワーク 8 上の PC 2 等の外部装置と通信するためのインタフェースである。

【0022】

カメラ I / F 26 は、所定の撮像範囲を撮像するカメラ 112 と接続するためのインタフェースである。タグリーダ I / F 27 は、タグリーダ 113 と接続するためのインタフェースである。タグリーダ 113 は、検知範囲内の無線タグ 114 との間で近距離無線通信を行い、無線タグ 114 に記憶されたタグ番号を読み取る(受信する)装置である。無線タグ 114 とタグリーダ 113 との間の通信方式としては、無線タグ 114 から電波を発信する Active タイプと、タグリーダ 113 から電波を発信し、それを受けた無線タグ 114 が応答を返す Passive タイプとが存在する。なお、ここでは、カメラ 112 の撮像範囲は、タグリーダ 113 がタグ番号を受信可能(取得可能)な範囲に対応している。要するに、カメラ 112 の撮像範囲は、タグリーダ 113 に対して無線タグ 114 をかざすユーザを撮像できる範囲に設定される。

【0023】

なお、この例では、カメラ 112 と操作部 20、または、タグリーダ 113 と操作部 20 は、物理的に異なる装置同士が、USB ケーブル等を介して接続されていることとして説明をする。しかし、操作部 20 にカメラ 112 やタグリーダ 113 が内蔵されていてもよい。すなわち、操作部 20 とカメラ 112、または、操作部 20 とタグリーダ 113 が一体的に形成されていてもよい(一つの装置として形成されていてもよい)。

【0024】

接続 I / F 28 は、通信路 30 を介して本体 10 と通信するためのインタフェースである。操作パネル 29 は、タッチセンサを備えた液晶表示装置(LCD)で構成される。操作パネル 29 は、ユーザの操作に応じた各種の入力を受け付けると共に、例えば受け付けた入力に応じた情報、MFP 1 の動作状況を示す情報、設定状態を示す情報等の各種の情報を表示する。なお、操作パネル 29 は、タッチセンサを備えた有機 EL 表示装置で構成してもよい。さらに、これに加えて又はこれに代えて、ハードウェアキー等の操作部又は発光部等の表示部を設けてもよい。

【0025】

(MFP のソフトウェア構成)

図 4 に、MFP 1 のソフトウェア構成の一例を示す。図 4 に示すように、本体 10 は、アプリ層 101 と、サービス層 102 と、OS 層 103 (第 1 のオペレーティングシステム)とを有する。アプリ層 101、サービス層 102 及び OS 層 103 の実体は、ROM

10

20

30

40

50

12又はHDD14等に格納されている各種ソフトウェアである。CPU11が、これらのソフトウェアを実行することにより、各種の機能が提供される。

【0026】

アプリ層101のソフトウェアは、ハードウェア資源を動作させて所定の機能を提供するためのアプリケーションソフトウェア（以下の説明では、単に「アプリ」と称する場合がある）である。例えばアプリとしては、コピー機能を提供するためのコピーアプリ、スキャナ機能を提供するためのスキャナアプリ、ファクシミリ機能を提供するためのファクシミリアプリ、プリンタ機能を提供するためのプリンタアプリ等が挙げられる。

【0027】

サービス層102のソフトウェアは、アプリ層101とOS層103との間に介在し、アプリに対し、本体10が備えるハードウェア資源を利用するためのインタフェースを提供するソフトウェアである。具体的には、ハードウェア資源に対する動作要求の受け付け、動作要求の調停を行う機能を提供するためのソフトウェアである。サービス層102が受け付ける動作要求としては、スキャナによる読み取りやプロッタによる印刷等の要求がある。

【0028】

なお、サービス層102によるインタフェースの機能は、本体10のアプリ層101だけではなく、操作部20のアプリ層201に対しても提供される。すなわち、操作部20のアプリ層201（アプリ）も、サービス層102のインタフェース機能を介して、本体10のハードウェア資源（例えばエンジン部16）を利用した機能を実現することができる。

【0029】

OS層103のソフトウェアは、本体10が備えるハードウェアを制御する基本機能を提供するための基本ソフトウェア（オペレーティングシステム）である。サービス層102のソフトウェアは、各種アプリからのハードウェア資源の利用要求を、OS層103が解釈可能なコマンドに変換してOS層103に渡す。そして、OS層103のソフトウェアによりコマンドが実行されることで、ハードウェア資源は、アプリの要求に従った動作を行う。

【0030】

同様に、操作部20は、アプリ層201と、サービス層202と、OS層203（第2のオペレーティングシステム）とを有する。操作部20が備えるアプリ層201、サービス層202及びOS層203も、階層構造については本体10側と同様である。ただし、アプリ層201のアプリにより提供される機能及びサービス層202が受け付け可能な動作要求の種類は、本体10側とは異なる。アプリ層201のアプリは、操作部20が備えるハードウェア資源を動作させて所定の機能を提供するためのソフトウェアである。主には、本体10が備える機能（コピー機能、スキャナ機能、ファクシミリ機能、プリンタ機能）に関する操作及び表示を行うためのUI（ユーザインタフェース）の機能を提供するためのソフトウェアである。

【0031】

なお、実施形態の例では、機能の独立性を保つために、本体10側のOS層103のソフトウェアと操作部20側のOS層203のソフトウェアが互いに異なる。つまり、本体10と操作部20は、別々のオペレーティングシステムで互いに独立して動作する。例えば、本体10側のOS層103のソフトウェアとしてLinux（登録商標）を用い、操作部20側のOS層203のソフトウェアとしてAndroid（登録商標）を用いることも可能である。

【0032】

本体10及び操作部20を、別々のオペレーティングシステムで動作させることで、本体10と操作部20との間の通信は、共通の装置内のプロセス間通信ではなく、異なる装置間の通信として行われる。操作部20が受け付けた入力（ユーザからの指示内容）を本体10へ伝達する動作（コマンド通信）及び本体10が操作部20へイベントを通知する

10

20

30

40

50

動作などがこれに該当する。ここでは、操作部 20 が本体 10 へコマンド通信を行うことにより、本体 10 の機能を使用することができる。また、本体 10 から操作部 20 に通知するイベントには、本体 10 における動作の実行状況、本体 10 側で設定された内容等が挙げられる。

【0033】

また、実施形態の例では、操作部 20 に対する電力供給は、本体 10 から通信路 30 を経由して行われているので、操作部 20 の電源制御を、本体 10 の電源制御とは別に（独立して）行うことができる。

【0034】

なお、この例では、本体 10 と操作部 20 は、通信路 30 を介して電気的かつ物理的に接続されているが、上述のように本体 10 から操作部 20 を取り外すこともできる。この場合、本体 10 及び操作部 20 に、例えば赤外線通信部、RF 通信部、Bluetooth（登録商標）通信部等の近距離無線通信部を設ける。RF は、「Radio Frequency」の略記である。又は、本体 10 及び操作部 20 に、Wi-Fi（登録商標）等の無線 LAN 通信機能を設け、図 4 に示すように無線 LAN アクセスポイント（無線 LAN AP）41 及びネットワーク 8 を介して相互に通信可能としてもよい。LAN は、「Local Area Network」の略記である。本体 10 から操作部 20 を取り外し可能である場合、操作部 20 は、通信路 30 を介して本体 10 から供給された電力を二次電池に蓄電しておき、本体 10 から取り外されたときに、二次電池に蓄電された電力で動作して本体 10 と通信を行う。

【0035】

次に、MFP 1 が有する機能について説明する。図 5 は、MFP 1 の操作部 20 が有する機能の一例を示す図である。図 5 に示すように、操作部 20 は、人体検知情報受信部 211 と、省エネ制御部 212 と、アドレス帳情報処理部 213 と、撮像画像取得部 214 と、顔画像検出部 215 と、顔画像認証処理部 216 と、タグ識別情報取得部 217 と、無線タグ認証処理部 218 と、認証部 219 とを有する。説明の便宜上、図 5 においては、本発明に関する機能を主に例示しているが、操作部 20 が有する機能は、これらに限られるものではない。例えば上述の機能の一部が本体 10 側に搭載される形態であってもよい。

【0036】

人体検知情報受信部 211 は、人体検知センサ 15 から、検知範囲内の人体の有無を示す人体検知情報を受信（取得）する。人体検知情報受信部 211 は、人体検知センサ 15 から受信した人体検知情報を省エネ制御部 212 へ渡す。

【0037】

省エネ制御部 212 は、操作部 20 が動作可能な通常状態よりも消費電力が小さい状態を示す省エネ状態で、人体検知情報受信部 211 から、検知範囲内に人体が存在することを示す人体検知情報を受信した場合、撮像画像取得部 214 およびタグ識別情報取得部 217 の各々を動作可能な状態に復帰させる（電源 ON 命令を送信する）。

【0038】

アドレス帳情報処理部 213 は、後述の顔画像認証処理部 216 および無線タグ認証処理部 218 の各々に対して、無線タグ 114 を識別するタグ番号（タグ識別情報の一例）と、ユーザの個人情報とを少なくとも対応付けたアドレス帳情報を提供する。アドレス帳情報は、例えば操作部 20 内のフラッシュメモリ 24 に記憶される形態であってもよいし、本体 10 内の HDD 14 に記憶される形態であってもよいし、外部サーバに記憶される形態であってもよい。つまり、フラッシュメモリ 24、HDD 14 および外部サーバのうちの何れかが「記憶部」として機能する。

【0039】

本実施形態におけるアドレス帳情報は、ユーザ情報と、タグ番号と、ユーザの顔情報とが対応付けられた情報である。この例では、顔情報は、ユーザの顔画像に含まれる特徴点を示す特徴点情報であるが、これに限られるものではなく、例えば顔画像であってもよい。

。アドレス帳情報に含まれる情報のうち、ユーザ情報とタグ番号については、MFP1の管理者が、PC2を操作して予め登録する作業を行う。この管理者による登録作業が完了した初期状態のアドレス帳情報（以下、「デフォルトのアドレス帳情報」と称する場合がある）は、図6に示すような形態となり、特徴点情報は未入力の状態（「null」）となる。なお、この例では、1つのユーザ情報と、1つのタグ番号と、1つの特徴点情報との組（1行分の情報群）ごとに、該組を識別するための番号（以下、「アドレス番号」と称する場合がある）が割り当てられる。

【0040】

図5に戻って説明を続ける。図5に示すように、アドレス帳情報処理部213は、タグ番号確認部220と、顔情報取得部221と、登録制御部222と、を含む。タグ番号確認部220は、後述のタグ識別情報取得部217によりタグ番号が取得されるたびに、その取得されたタグ番号を後述の無線タグ認証処理部218から受け取る。そして、タグ番号確認部220は、タグ識別情報取得部217により取得されたタグ番号（無線タグ認証処理部218から受け取ったタグ番号）がアドレス帳情報に存在するか否かを確認し、アドレス帳情報に存在する場合は、該当するアドレス番号を無線タグ認証処理部218へ送信し、アドレス帳情報に存在しない場合はエラーを送信する。また、タグ番号確認部220は、タグ識別情報取得部217により取得されたタグ番号（無線タグ認証処理部218から受け取ったタグ番号）がアドレス帳情報に存在する場合、そのタグ番号を顔情報取得部221へ通知する。

【0041】

顔情報取得部221は、アドレス帳情報を参照し、後述のタグ識別情報取得部217により取得されたタグ番号に対して、ユーザの顔情報が対応付けられていない場合は、タグ番号を取得可能な範囲に対応する撮像範囲を撮像して得られる撮像画像に基づいて顔情報を取得する。本実施形態では、顔情報取得部221は、後述の顔画像検出部215により検出された顔画像に基づいて顔情報を取得する。より具体的には、顔情報取得部221は、アドレス帳情報を参照し、タグ番号確認部220から通知されたタグ番号に対して特徴点情報（顔情報の一例）が対応付けられていない場合は、後述の顔画像検出部215に対して、顔画像を要求する顔画像要求を送信し、その応答として顔画像を取得する。そして、顔画像に含まれる特徴点を抽出して特徴点情報を取得（生成）する。そして、登録制御部222に対して、上記のようにして取得した特徴点情報と、タグ番号確認部220から通知されたタグ番号と、を通知する。

【0042】

登録制御部222は、顔情報取得部221により取得された特徴点情報をタグ番号に対応付けてアドレス帳情報に登録する制御を行う。この例では、登録制御部222は、顔情報取得部221から通知された特徴点情報とタグ番号とを対応付けてアドレス帳情報に登録する制御を行う。図7は、登録制御部222による特徴点情報の登録が行われた後のアドレス帳情報の一例を示す図である。

【0043】

図5の説明を続ける。撮像画像取得部214は、カメラ112の撮像により得られた撮像画像をカメラ112から取得する。この例では、検知範囲内に人物が侵入すると、撮像画像取得部214は動作を開始し、カメラ112から撮像画像を取得する。撮像画像取得部214は、カメラ112から取得した撮像画像を顔画像検出部215へ送信する。

【0044】

顔画像検出部215は、撮像画像取得部214により取得された撮像画像から顔画像を検出する。そして、所定期間の間、上述の顔画像要求の受信を待ち、顔画像要求を受信した場合は、検出した顔画像を、顔情報取得部221および顔画像認証処理部216の各々へ送信し、顔画像要求を受信しなかった場合は、検出した顔画像を顔画像認証処理部216のみへ送信する。ここでは、顔情報取得部221および顔画像認証処理部216の各々へ顔画像が送信される場合は、同一の顔画像が送信されることになる（自動的に後述の顔画像認証処理は成功することになる）。

【0045】

顔画像の検出方法としては公知の様々な技術を利用することができるが、例えば、<http://www.vision.cs.chubu.ac.jp/cvtutorial/pdf/03objection.pdf>のP6-P26に開示されているような「Haar-like特徴による顔検出」を利用してもよい。以下、「Haar-like特徴による顔検出」の概略を説明する。探索領域中で計算対象である矩形中の黒色の領域のピクセル値の和の値から白色の領域のピクセル値の和の値を引いた値をHaar-Like特徴量と呼ぶ。この矩形の配置場所は探索領域内のどこにどう配置しても良いので、探索領域中に数万通りの配置場所の可能性があることになる。これらに対して、Boostingにより探索領域内の各弱識別器を事前学習で重みづけし、重要度が上位の数十個の弱識別器のみを選択して強識別器を作成する。そして、この強識別器によって（人の顔らしさを示す白黒矩形数パターンによって）その領域が人の顔領域かどうかを判断する。

10

【0046】

顔画像認証処理部216は、顔画像検出部215により検出された顔画像に対応する顔情報がアドレス帳情報に存在するか否かを判断する顔画像認証（顔認証）処理を行う。この例では、顔画像認証処理部216は、顔画像検出部215から顔画像を受け取ると、アドレス帳情報処理部213に対して、アドレス帳情報を要求するアドレス帳情報要求を送信し、その応答としてアドレス帳情報を受信する。そして、顔画像検出部215から受け取った顔画像に含まれる特徴点を抽出して特徴点情報を生成し、その生成した特徴点情報（顔画像に対応する顔情報の一例）が、アドレス帳情報処理部213から受け取ったアドレス帳情報に存在するか否かを判断する。要するに、アドレス帳情報に登録されているユーザの数だけ、特徴点情報のマッチングを行う。また、顔情報として、特徴点情報の代わりに顔画像が採用されている場合は、顔画像認証処理部216は、顔画像検出部215から受け取った顔画像が、アドレス帳情報処理部213から受け取ったアドレス帳情報に存在するか否かを判断する。この場合、例えば顔画像1枚当たりの各ピクセルの輝度値を1本のベクトルとし、パターン認識でマッチングを行う手法などがある。例として、<http://www.cvlab.cs.tsukuba.ac.jp/~kfukui/papers/ssii2007.pdf>に開示されているような部分空間法を用いた顔画像認証などが挙げられる。そして、顔画像認証処理部216は、顔画像認証処理の結果を示す顔認証結果を認証部219へ送信する。この例では、顔画像認証処理部216は、顔画像認証処理の結果が肯定の場合、該当するアドレス番号を併せて認証部219へ送信する。

20

30

【0047】

タグ識別情報取得部217は、タグリーダー113によるタグ番号の読み取りが行われるたびに、その読み取られたタグ番号をタグリーダー113から取得する。タグ識別情報取得部217は、タグリーダー113から取得したタグ番号を無線タグ認証処理部218へ送信する。

【0048】

無線タグ認証処理部218は、タグ識別情報取得部217により取得されたタグ番号がアドレス帳情報に存在するか否かを判断する無線タグ認証処理を行う。この例では、無線タグ認証処理部218は、アドレス帳情報処理部213に対して、タグ識別情報取得部217から受け取ったタグ番号を送信し、該タグ番号がアドレス帳情報に存在するか否かの判断をアドレス帳情報処理部213に行わせる。上述したように、アドレス帳情報処理部213（タグ番号確認部220）は、無線タグ認証処理部218から受け取ったタグ番号がアドレス帳情報に存在する場合は、該当するアドレス番号を無線タグ認証処理部218へ送信し、アドレス帳情報に存在しない場合はエラーを通知する。無線タグ認証処理部218は、アドレス帳情報処理部213からアドレス番号を受け取った場合は、無線タグ認証処理の結果が肯定であると判断し、エラーを受け取った場合は、無線タグ認証処理の結果は否定であると判断することができる。そして、無線タグ認証処理部218は、無線タグ認証処理の結果を示す無線タグ認証結果を認証部219へ送信する。この例では、無線タグ認証処理部218は、無線タグ認証処理の結果が肯定の場合、該当するアドレス番号を併せて認証部219へ送信する。

40

50

【0049】

認証部219は、顔画像認証処理の結果と無線タグ認証処理の結果とに基づき、タグ識別情報取得部217により取得されたタグ番号がアドレス帳情報に存在し、かつ、該タグ番号に対応付けられた顔情報（この例では特徴点情報）が顔画像検出部215により検出された顔画像に対応する顔情報と一致する場合は、タグ識別情報取得部217により取得されたタグ番号が記憶された無線タグ114を所持するユーザは、MF P1を使用する権限を有することを認める（無線タグ114を所持するユーザを認証する）。この例では、認証部219は、顔画像認証処理部216から、顔画像認証処理の結果が肯定であることを示す顔認証結果を受け取り、無線タグ認証処理部218から、無線タグ認証処理の結果が肯定であることを示す無線タグ認証結果を受け取り、かつ、顔認証結果と併せて通知されたアドレス番号と、無線タグ認証結果と併せて通知されたアドレス番号とが一致する場合にユーザを認証し、MF P1を使用可能な状態に制御する。

10

【0050】

図8は、MF P1の管理者がデフォルトのアドレス帳情報を登録する際のPC2の動作例を示すフローチャートである。管理者はPC2を操作して、アドレス帳情報を登録するための画面（登録画面）を表示させ、未登録のユーザの個人情報を登録するための操作を行う。この操作を受け付けたPC2は、個人情報を登録する処理を行う（ステップS1）。次に、管理者は、ステップS1で個人情報を登録したユーザに対して配布予定の無線タグ114のタグ番号を登録するための操作を行う。この操作を受け付けたPC2は、ステップS1で登録した個人情報に対応付けてタグ番号を登録する処理を行う（ステップS2）。そして、PC2は、デフォルトのアドレス情報を更新する処理（記憶部内のアドレス情報を更新する処理）を行う（ステップS3）。

20

【0051】

図9は、無線タグ114を所持するユーザが、タグリーダ113に対して、自身の所持する無線タグ114を翳した場合のMF P1の動作例を示すフローチャートである。各ステップの具体的な内容は上述したとおりであるので、詳細な説明については適宜に省略する。図9に示すように、タグ識別情報取得部217は、タグリーダ113からタグ番号を取得する（ステップS101）。次に、タグ番号確認部220は、ステップS101で取得されたタグ番号がアドレス帳情報に存在するか否かを判断する（ステップS102）。ステップS102の結果が否定の場合（ステップS102：No）、結果として認証されないことになる（ここでは処理終了と記載）。ステップS102の結果が肯定の場合（ステップS102：Yes）、顔情報取得部221は、アドレス帳情報を参照し、ステップS101で取得されたタグ番号に対して、特徴点情報に対応付けられているか否かを確認する（ステップS103）。また、ステップS102の結果が肯定の場合（ステップS102：Yes）、タグ番号確認部220は、該当するアドレス番号を無線タグ認証処理部218へ送信する。上述したように、無線タグ認証処理部218は、アドレス帳情報処理部213（タグ番号確認部220）からアドレス番号を受け取った場合は、無線タグ認証処理の結果が肯定であると判断することができ、無線タグ認証処理の結果を示す無線タグ認証結果を認証部219へ送信する。

30

【0052】

ステップS103の結果が否定の場合（ステップS103：No）、顔情報取得部221は顔画像検出部215から顔画像を取得し（ステップS104）、その取得した顔画像に含まれる特徴点を抽出して特徴点情報を取得（生成）する（ステップS105）。その後、顔情報取得部221は顔画像検出部215から取得した顔画像を破棄する（ステップS106）。そして、登録制御部222は、ステップS105で取得された特徴点情報と、ステップS101で取得されたタグ番号とを対応付けてアドレス帳情報に登録する制御を行う（ステップS107）。そして、処理はステップS108に移行する。

40

【0053】

ステップS103の結果が肯定の場合（ステップS103：Yes）、または、ステップS107の後、顔画像認証処理部216による顔画像認証処理が行われ（ステップS1

50

08)、顔画像認証処理の結果を示す顔画像認証結果が認証部219へ送信される。そして、認証部219は、顔画像認証処理の結果と無線タグ認証処理の結果とに基づき、認証が成功したか否かを判断する(ステップS109)。ステップS109の結果が肯定の場合(ステップS109:Yes)、認証部219はMF P1を使用可能な状態に制御する(ステップS110)。ステップS109の結果が否定の場合(ステップS109:No)、処理は終了する。

【0054】

以上に説明したように、本実施形態では、タグリーダ113へ向けて翳された無線タグ114に記憶されたタグ番号(タグ識別情報取得部217により取得されたタグ番号)に対して、予め特徴点情報が対応付けられていない場合は、タグ番号を取得可能な範囲(タグリーダ113と無線タグ114とが無線通信可能な範囲)に対応する撮像範囲を撮像して得られる撮像画像に基づいて特徴点情報を取得し、その取得した特徴点情報をタグ番号に対応付けてアドレス帳情報に登録する制御を行う。これにより、MF P1の管理者による作業負担を軽減することができ、顔認証に用いられる顔情報(この例では特徴点情報)に登録する処理の効率を向上させることができる。

【0055】

例えば任意の企業において、該企業に導入されているMF Pに、上述のアドレス帳情報を登録する場合、社員ごとの社員証用の撮影写真などを用いて特徴点情報を抽出して登録することが想定される。しかし、社員証用の写真の撮影を行わない企業や、写真の解像度が粗く特徴点情報を得ることができないような場合には、アドレス帳情報を作成することができず、適切に顔認証を行うことができない。そこで、機器の管理者が写真撮影や、該写真撮影で得られた画像(写真)から抽出された特徴点情報とタグ番号とを対応付けた登録作業などを行うことにすると、管理者の作業負担が高くなってしまう。これに対して、以上に説明した本実施形態によれば、管理者の作業負担を軽減しつつ適切に顔認証を行うことができる。

【0056】

以上、本発明に係る実施形態について説明したが、本発明は、上述の実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上述の実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、上述の実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。

【0057】

また、上述の実施形態では、本体10と操作部20は、別々のオペレーティングシステム(OS)で互いに独立して動作しているが、これに限らず、例えば本体10と操作部20が同じオペレーティングシステムで動作する形態であってもよい。

【0058】

また、上述した実施形態のMF P1で実行されるプログラムは、インストール可能な形式または実行可能な形式のファイルでCD-ROM、フレキシブルディスク(FD)、CD-R、DVD(Digital Versatile Disk)、USB(Universal Serial Bus)等のコンピュータで読み取り可能な記録媒体に記録して提供するように構成してもよいし、インターネット等のネットワーク経由で提供または配布するように構成してもよい。また、各種プログラムを、ROM等の不揮発性の記録媒体に予め組み込んで提供するように構成してもよい。

【0059】

以下に、他の実施形態について図面を参照して説明するが、第1の実施形態と同一又は同様の作用効果を奏する箇所については同一の符号を付してその説明を省略する。

【0060】

(第2の実施形態)

図10は、第2の実施形態に係るアプリ層201の構成例を示す図である。本実施形態に係るアプリ層201は、タグ認証アプリ301(タグ認証アプリケーション)、顔情報

10

20

30

40

50

登録アプリ 3 1 1（顔情報登録アプリケーション）および顔認証アプリ 3 1 2（顔認証アプリケーション）を含む。タグ認証アプリ 3 0 1、顔情報登録アプリ 3 1 1 および顔認証アプリ 3 1 2 は、OS 層 2 0 3（第 2 のオペレーティングシステム）上で動作する。顔情報登録アプリ 3 1 1 と顔認証アプリ 3 1 2 とは 1 つのアプリケーション（統合アプリ 3 2 1）であってもよい。

【0061】

なお、ここではタグ認証アプリ 3 0 1、顔情報登録アプリ 3 1 1 および顔認証アプリ 3 1 2 の全てがアプリ層 2 0 1 に含まれる構成を例示しているが、本実施形態に係るソフトウェア構成はこれに限られるものではない。例えば、タグ認証アプリ 3 0 1、顔情報登録アプリ 3 1 1 および顔認証アプリ 3 1 2 のうちの少なくとも一部がサービス層 2 0 2 に含まれてもよい。

10

【0062】

図 1 1 は、第 2 の実施形態に係る操作部 5 0 の機能とアプリケーションとの関係例を示す図である。タグ認証アプリ 3 0 1 は、タグ識別情報取得部 2 1 7 および無線タグ認証処理部 2 1 8 を含む。タグ認証アプリ 3 0 1 は、タグ識別情報取得部 2 1 7 により取得されたタグ番号（タグ識別情報）と、アドレス帳情報に含まれるタグ番号とを比較してタグ認証を行う。

【0063】

顔情報登録アプリ 3 1 1 は、顔情報取得部 2 2 1、登録制御部 2 2 2 およびパスワード認証部 3 5 1 を含む。パスワード認証部 3 5 1 は、タグ認証アプリ 3 0 1 によるタグ認証後であって、ユーザの顔画像の撮影時に、ユーザにより入力されたパスワードとアドレス帳情報においてタグ番号に対応付けられたパスワードとを比較してパスワード認証を行う。登録制御部 2 2 2 は、パスワード認証の成功時に、顔情報をタグ番号に対応付けてアドレス帳情報に登録する制御を許可する。

20

【0064】

顔認証アプリ 3 1 2 は、撮像画像取得部 2 1 4、顔画像検出部 2 1 5 および顔画像認証処理部 2 1 6 を含む。顔認証アプリ 3 1 2 は、撮像画像から顔画像を検出し、検出された顔画像に対応する顔情報がアドレス帳情報に存在するか否かを判断する。

【0065】

図 1 2 は、第 2 の実施形態に係る M F P 1 の動作例を示すフローチャートである。本実施形態に係るフローチャートは、図 9 に示す第 1 の実施形態に係るフローチャートと、ステップ S 1 0 2 とステップ S 1 0 3 との間にステップ S 2 0 1 が挿入されている点で相違する。ステップ S 1 0 2 の結果が肯定の場合（ステップ S 1 0 2：Y e s）、すなわちタグ番号確認部 2 2 0 が、ステップ S 1 0 1 で取得されたタグ番号がアドレス帳情報に存在すると判断した場合、パスワード認証部 3 5 1 は、タグ認証後にユーザにより入力されたパスワードと、ステップ S 1 0 1 で取得されたタグ番号に対応付けられたパスワードとを比較し、パスワード認証が成功したか否かを判断する（S 2 0 1）。ステップ S 2 0 1 の結果が肯定の場合（ステップ S 2 0 1：Y e s）、すなわちユーザにより入力されたパスワードと取得されたタグ番号に対応付けられたパスワードとが一致する場合、ステップ S 1 0 3 の処理（顔情報取得部 2 2 1 によるタグ番号に対して特徴点情報が対応付けられているか否かを確認する処理）が行われる。ステップ S 2 0 1 の結果が否定の場合（S 2 0 1：N o）、すなわちユーザにより入力されたパスワードと取得されたタグ番号に対応付けられたパスワードとが一致しない場合、結果として認証されないことになる。

30

40

【0066】

本実施形態によれば、認証に関する処理（タグ情報を用いたタグ認証、ユーザの顔情報の取得・登録、顔情報を用いた顔認証等）が、操作部 5 0 の OS 層 2 0 3（第 2 のオペレーティングシステム）上で動作するアプリケーション（タグ認証アプリ 3 0 1、顔情報登録アプリ 3 1 1、顔認証アプリ 3 1 2 等）により行われる。操作部 5 0 の OS 層 2 0 3 は、本体 1 0 の OS 層 1 0 3（第 1 のオペレーティングシステム）とは独立して動作する。そのため、認証に関する処理を本体 1 0 とは独立して行うことが可能となり、認証に関す

50

る設定、メンテナンス等の作業性を向上させることが可能となる。また、本実施形態によれば、パスワード認証部 351 によりタグ認証後にパスワード認証が行われ、パスワード認証の成功時に顔情報が登録されるため、セキュリティ性を第 1 の実施形態よりも向上させることが可能となる。

【0067】

以上、本発明の実施形態を説明したが、上記実施形態は例として提示したものであり、発明の範囲を限定することを意図するものではない。この新規な実施形態はその他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で種々の省略、置き換え、変更、及び組み合わせを行うことができる。この実施形態及びその変形は発明の範囲及び要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

10

【符号の説明】

【0068】

1 MFP
2 PC
8 ネットワーク
10 本体
20, 50 操作部
100 情報処理システム
112 カメラ
113 タグリーダ
114 無線タグ
211 人体検知情報受信部
212 省エネ制御部
213 アドレス帳情報処理部
214 撮像画像取得部
215 顔画像検出部
216 顔画像認証処理部
217 タグ識別情報取得部
218 無線タグ認証処理部
219 認証部
220 タグ番号確認部
221 顔情報取得部
222 登録制御部
301 タグ認証アプリ
311 顔情報登録アプリ
312 顔認証アプリ
321 統合アプリ
351 パスワード認証部

20

30

【先行技術文献】

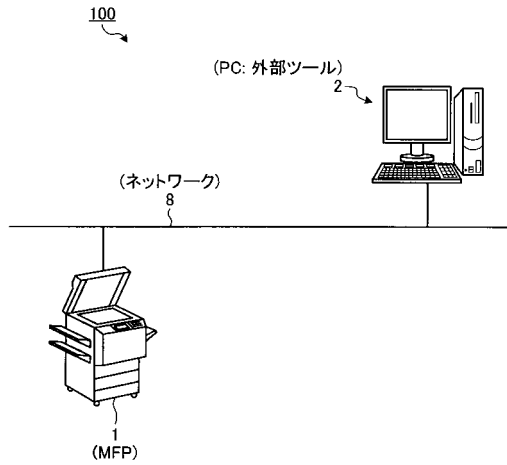
40

【特許文献】

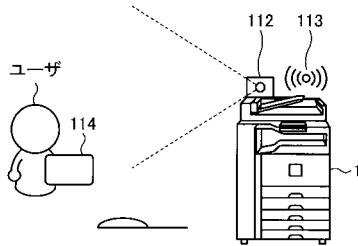
【0069】

【特許文献 1】特開 2012-88835 号公報

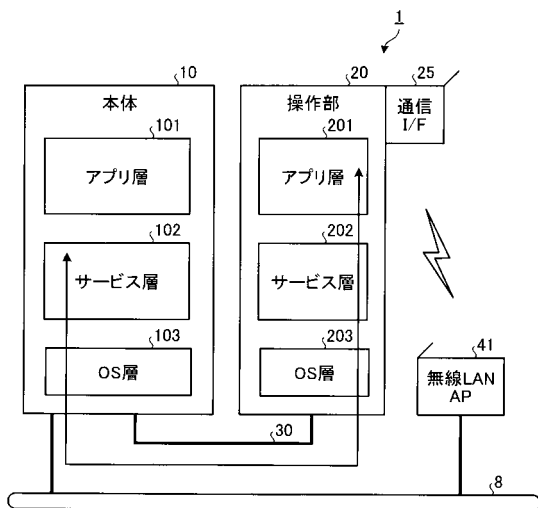
【図 1】



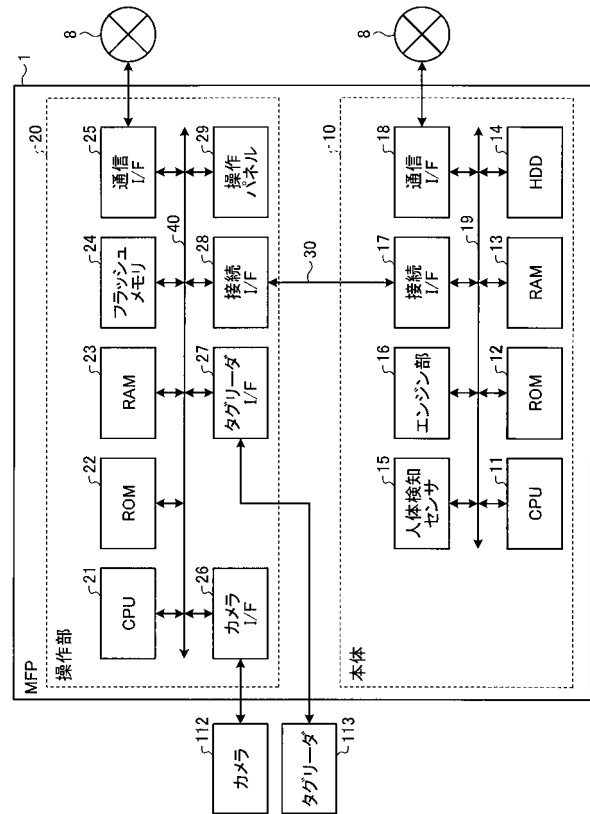
【図 2】



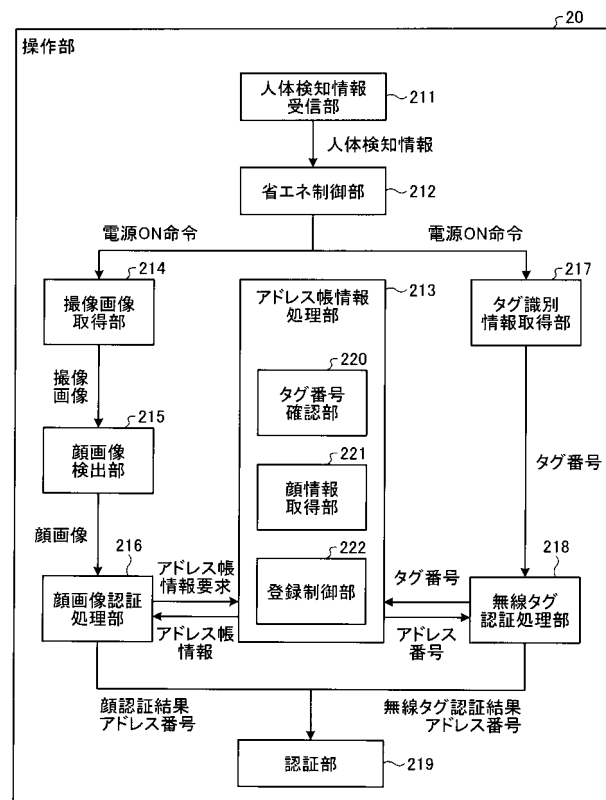
【図 4】



【図 3】



【図 5】



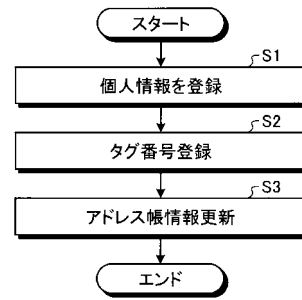
【図 6】

ユーザ情報	タグ番号	特徴点情報
氏名: 山田太郎 E-mail: aaa@xxx.jp ...	eee912sa000...	null

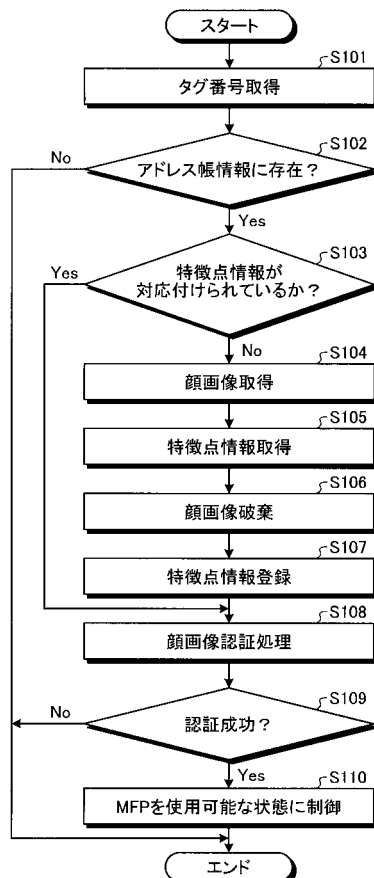
【図 7】

ユーザ情報	タグ番号	特徴点情報
氏名: 山田太郎 E-mail: aaa@xxx.jp ...	eee912sa000...	14149179904108341974 90801480180180810480 ...

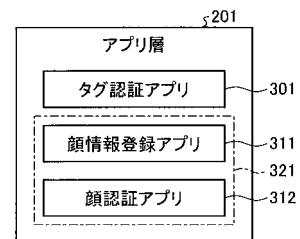
【図 8】



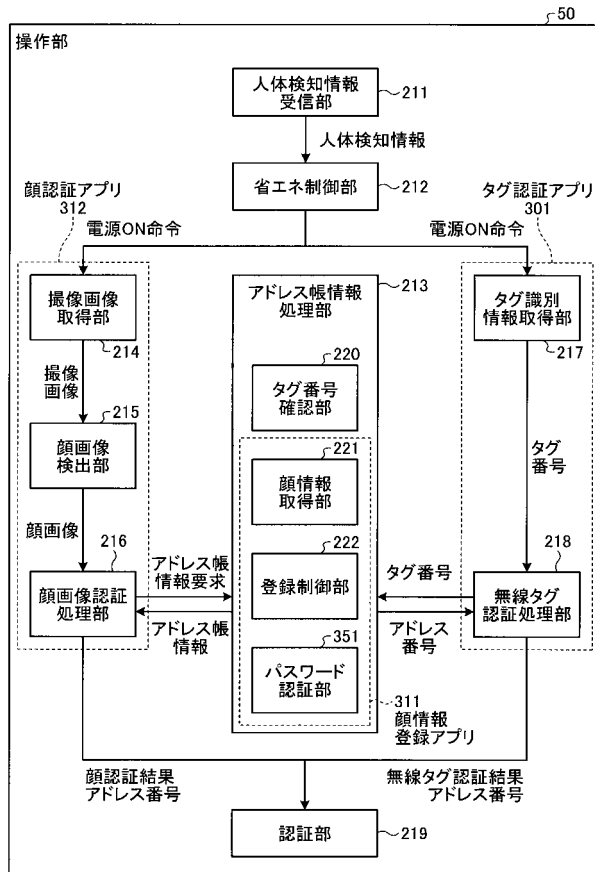
【図 9】



【図 10】



【図 1 1】



【図 1 2】

