(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7309379号
(P7309379)

(45)発行日　令和5年7月18日(2023.7.18)

(24)登録日　令和5年7月7日(2023.7.7)

(51)国際特許分類		FI		
H04N 1/00 (2006.01)		H04N	1/00	912
H04L 67/02 (2022.01)		H04N	1/00	350
G06F 3/01 (2006.01)		H04L	67/02	
		G06F	3/01	510

請求項の数　11　（全19頁）

(21)出願番号　特願2019-28395(P2019-28395)
(22)出願日　平成31年2月20日(2019.2.20)
(65)公開番号　特開2020-136919(P2020-136919A)
(43)公開日　令和2年8月31日(2020.8.31)
審査請求日　令和4年1月31日(2022.1.31)

(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　佐藤 鉄也
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　野口 俊明

最終頁に続く

(54)【発明の名称】　周辺装置、方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

情報媒体から電子データを生成する機能を備える周辺装置であって、

ユーザーの認証が行われたウェアラブル端末と通信することで、当該ウェアラブル端末の識別情報と、該ユーザーの識別情報と、該ユーザーに対応する宛先と、を対応付けて登録する登録手段と、

所定の範囲内のウェアラブル端末から、認証状態に係る情報を含むデータを取得する取得手段と、

前記取得されたデータが認証済みであることを示す情報を含む場合に、前記周辺装置で検出された情報媒体から得られる情報に基づく前記機能を用いた電子データの生成と、前記ウェアラブル端末の識別情報で特定されるユーザーに対応付けて登録されている宛先に対する該生成された電子データの送信と、を含む処理を開始する実行手段と、

を有することを特徴とする周辺装置。

【請求項２】

前記実行手段により前記処理が開始される場合に、当該処理に対する割り込み処理を指示することができる画面の表示を制御する表示制御手段を、更に有することを特徴とする請求項１に記載の周辺装置。

【請求項３】

前記割り込み処理は、前記実行手段により開始された前記処理のキャンセルを含むことを特徴とする請求項２に記載の周辺装置。

【請求項４】
前記実行手段により実行された前記処理が完了したあとに、完了したことを示す通知、及び、前記情報媒体の取り忘れに係る通知の少なくともいずれかを、前記ウェアラブル端末に対して行う通知手段を、更に有することを特徴とする請求項１乃至３のいずれか１項に記載の周辺装置。
【請求項５】
前記周辺装置は、原稿をスキャンすることで、前記電子データとして画像データを生成することを特徴とする請求項１乃至４のいずれか１項に記載の周辺装置。
【請求項６】
前記周辺装置は、スキャナを備える画像処理装置、デジタルカメラ、デジタル健康器具、またはデジタル楽器であることを特徴とする請求項１乃至４のいずれか１項に記載の周辺装置。
【請求項７】
前記周辺装置はユーザーにより入力されるパスワードを用いた認証機能を備え、前記ウェアラブル端末はユーザーの生体情報を用いた認証機能を備えることを特徴とする請求項１乃至６のいずれか１項に記載の周辺装置。
【請求項８】
情報媒体から電子データを生成する機能を備える周辺装置における方法であって、
ユーザーの認証が行われたウェアラブル端末と通信することで、当該ウェアラブル端末の識別情報と、該ユーザーの識別情報と、該ユーザーに対応する宛先と、を対応付けて登録する登録ステップと、
所定の範囲内のウェアラブル端末から、認証状態に係る情報を含むデータを取得する取得ステップと、
前記取得されたデータが認証済みであることを示す情報を含む場合に、前記周辺装置で検出された情報媒体から得られる情報に基づく前記機能を用いた電子データの生成と、前記ウェアラブル端末の識別情報で特定されるユーザーに対応付けて登録されている宛先に対する該生成された電子データの送信と、を含む処理を開始する実行ステップと、
を有することを特徴とする方法。
【請求項９】
前記処理が開始される場合に、当該処理に対する割り込み処理を指示することができる画面の表示を制御する表示制御ステップを、更に有することを特徴とする請求項８に記載の方法。
【請求項１０】
実行された前記処理が完了したあとに、完了したことを示す通知、及び、前記情報媒体の取り忘れに係る通知の少なくともいずれかを、前記ウェアラブル端末に対して行う通知ステップを、更に有することを特徴とする請求項８または９に記載の方法。
【請求項１１】
情報媒体から電子データを生成する周辺装置の機能を用いた方法を実現するためのプログラムであって、
ユーザーの認証が行われたウェアラブル端末と通信することで、当該ウェアラブル端末の識別情報と、該ユーザーの識別情報と、該ユーザーに対応する宛先と、を対応付けて登録する登録ステップと、
所定の範囲内のウェアラブル端末から、認証状態に係る情報を含むデータを取得する取得ステップと、
前記取得されたデータが認証済みであることを示す情報を含む場合に、前記周辺装置で検出された情報媒体から得られる情報に基づく前記機能を用いた電子データの生成と、前記ウェアラブル端末の識別情報で特定されるユーザーに対応付けて登録されている宛先に対する該生成された電子データの送信と、を含む処理を開始する実行ステップと、
を有することを特徴とする方法を実現するためのプログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、所定の認証方式を利用するユーザーの周辺装置の利用の利便性を向上させるための技術に関する。
【背景技術】
【０００２】
従来から、画像処理装置、ＭＦＰ（多機能周辺装置）などの周辺装置では、ユーザー入力によるパスワードの認証や、カードリーダーにカードをかざす認証を採用していることが多い。画像処理装置では、その認証完了後に、予め登録してある自分のメールアドレスを宛先として、スキャンした画像データを送信するボタンを提供している（例えば、特許文献１）。
【０００３】
また、指紋認証など、生体情報を用いてユーザー認証を行う周辺装置も存在する。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２００９－１７１３０９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
上述した周辺装置では、ユーザー入力による認証作業のあと、ユーザーのキー操作などに応じて、スキャナへ配置した原稿のスキャンによる画像データの生成とその送信を実行していた。
【０００６】
周辺装置が複数のユーザーに共有される場合には、認証作業やキー入力などの周辺装置に対する操作によってユーザーを拘束してしまう時間を最小化したい。例えば、周辺装置を利用したユーザーが、予め登録してある自分のメールアドレスを宛先に対してスキャンにより得られた画像データを送信したい場合には、従来のようなユーザー操作を省略できるような仕組みが望まれる。
【０００７】
そこで、本発明は、所定の認証方式を利用するユーザーについては、従来に比べて、周辺装置の特定の機能の利用を素早く開始できるための仕組み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】
【０００８】
本発明は、情報媒体から電子データを生成する機能を備える周辺装置であって、ユーザーの認証が行われたウェアラブル端末と通信することで、当該ウェアラブル端末の識別情報と、該ユーザーの識別情報と、該ユーザーに対応する宛先と、を対応付けて登録する登録手段と、所定の範囲内のウェアラブル端末から、認証状態に係る情報を含むデータを取得する取得手段と、前記取得されたデータが認証済みであることを示す情報を含む場合に、前記周辺装置で検出された情報媒体から得られる情報に基づく前記機能を用いた電子データの生成と、前記ウェアラブル端末の識別情報で特定されるユーザーに対応付けて登録されている宛先に対する該生成された電子データの送信と、を含む処理を開始する実行手段と、を有することを特徴とする。
【発明の効果】
【０００９】
本発明は、所定の認証方式を利用するユーザーについては、従来に比べて、周辺装置の特定の機能の利用を素早く開始できるための仕組みを提供することを目的とする。
【図面の簡単な説明】
【００１０】
【図１】システムの全体構成を示す模式図

【図２】各装置の内部構成の例を示すブロック図
【図３】各装置の機能構成の例を示すブロック図
【図４】ウェアラブル端末をＭＦＰに登録する処理を示したフローチャート
【図５】ＭＦＰで提供される画面の例
【図６】自分への送信処理の例を示したフローチャート
【図７】自分への送信処理に関するＭＦＰで提供される画面の例
【図８】送信完了後のＭＦＰの処理の例を示したフローチャート
【発明を実施するための形態】
【００１１】
以下、具体的な実施例について図面を用いて説明する。
【００１２】
＜システム構成＞
図１は、本実施例におけるシステムの全体構成を示す模式図である。
【００１３】
本システムは、周辺装置の一例であるＭＦＰ１０１と、ウェアラブル端末１０２から主に構成される。ウェアラブル端末１０２を装着するユーザーが保有するスマートフォンやタブレットなどである情報処理装置１０４があっても良い。ウェアラブル端末１０２及び情報処理装置１０４は、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの無線通信で互いに通信できる。情報処理装置１０４は、指紋や顔画像などの生体情報を検出するセンサーと、該センサーで検出したデータを用いた認証機能を備えている。
【００１４】
ＭＦＰ１０１と、ウェアラブル端末１０２は、ネットワーク１０３で接続される。ネットワーク１０３は、本実施例では主に無線による近接通信であり、ＢＬＥ（Ｂｌｕｅｔｏｏｔｈ Ｌｏｗ Ｅｎｅｒｇｙ）やＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）である。
【００１５】
ウェアラブル端末は、生体情報などを用いた認証機能や、該端末を装着中のユーザーに係る外部認証の状態を管理する機能を搭載したものがある。例えば、心電図認証機能を搭載したバンド型のウェアラブル端末がある。このバンド型のウェアラブル端末では、バンドの留め金に着脱を検知するセンサーを搭載しており、一度、心電図を用いた認証を行うと、バンドの留め金を外すまで認証された状態を保つことができる。本発明に適用可能なウェアラブル端末には、心電図認証機能をもつバンド型のウェアラブル端末以外にも、虹彩認証を行う眼鏡型のウェアラブル端末など、周辺装置と通信する機能、認証機能、装着状態を検出できる機構などをもつ様々なウェアラブル端末がある。
【００１６】
本実施例では、ウェアラブル端末１０２を装着したユーザーのＭＦＰ１０１へのログインのための生体情報を用いた認証をウェアラブル端末１０２で実施する例を説明する。そして、認証が成功した状態のウェアラブル端末１０２をユーザーがＭＦＰ１０１に近接するなどして無線で通信が行われた場合には、ＭＦＰ１０１は、その通信で特定されるログインユーザーの情報を用いて特定の機能を実行する。
【００１７】
具体例としては、ＭＦＰ１０１が、ウェアラブル端末１０２の近接で特定されるログインユーザーのアドレス情報などの宛先に対して、スキャンで得られた画像データの自動送信を開始する例について説明する。
【００１８】
＜周辺装置の内部構成＞
図２（Ａ）は、周辺装置の一例であるＭＦＰ１０１の内部構成を示す図である。
【００１９】
ＭＦＰ１０１はコントローラユニット２００を含み、コントローラユニット２００には、画像入力デバイスであるスキャナ２１５や画像出力デバイスであるプリンタ２１６が接

続されるとともに、操作部２０９が接続される。コントローラユニット２００は、スキャナ２１５で読み取られた画像データをネットワークＩ／Ｆ２０４により送信する送信機能を実現するための制御を行う。

【００２０】

コントローラユニット２００は、プロセッサであるＣＰＵ２０１を有し、ＣＰＵ２０１は、ＲＯＭ２０６に格納されているブートプログラムによりオペレーションシステム（ＯＳ）を立ち上げる。ＣＰＵ２０１は、このＯＳ上で、ＲＯＭ２０６やＨＤＤ（ハードディスクドライブ）２０７に格納されているプログラムを実行し、これによって各種処理を実行する。このＣＰＵ２０１の作業領域としてはＲＡＭ２０２が用いられる。ＲＡＭ２０２は、作業領域を提供するとともに、画像データを一時記憶するための画像メモリー領域を提供する。ＨＤＤ２０７は、上記プログラムや画像データを格納する。ＣＰＵ２０１には、システムバス２１０を介して、ＲＯＭ２０６およびＲＡＭ２０２、操作部Ｉ／Ｆ（操作部インターフェース）２０３が接続される。さらにＣＰＵ２０１には、ネットワークＩ／Ｆ（ネットワークインターフェース）２０４、画像バスＩ／Ｆ（画像バスインターフェース）２０８が接続される。

【００２１】

操作部Ｉ／Ｆ２０３は、タッチパネルを有する操作部２０９とのインターフェースであり、操作部２０９に表示すべきＵＩを操作部２０９に対して出力する。また、操作部Ｉ／Ｆ２０３は、操作部２０９においてユーザーにより入力された情報をＣＰＵ２０１に送出する。ネットワークＩ／Ｆ２０４は、ＭＦＰ１０１をＬＡＮに接続するためのインターフェースである。ネットワークＩ／Ｆ２０４によるネットワークへの接続は、有線でも無線でもよい。近接通信Ｉ／Ｆ２０５は、ＢＬＥなどの近接通信用の通信方式に対応したインターフェースであり、ＭＦＰ１０１とウェアラブル端末１０２などの外部の装置とを接続する。

【００２２】

画像バスＩ／Ｆ２０８は、システムバス２１０と、画像データを高速で転送する画像バス２１１とを接続し、データ形式を変換するためのバスブリッジである。画像バス２１１は、ＰＣＩバスまたはＩＥＥＥ１３９４等によって構成される。画像バス２１１上には、デバイスＩ／Ｆ２１２、スキャナ画像処理部２１３、プリンタ画像処理部２１４が設けられる。デバイスＩ／Ｆ２１２には、スキャナ２１５およびプリンタ２１６が接続され、デバイスＩ／Ｆ２１２は、画像データの同期系／非同期系の変換を行う。スキャナ画像処理部２１３は、入力画像データに対し補正、加工、編集を行う。プリンタ画像処理部２１４は、プリント出力画像データに対してプリンタ２１６に応じた補正、解像度変換などを行う。スキャナ２１５は、原稿の読み取り、原稿の有無の検知などを行う。

【００２３】

＜ウェアラブル端末の内部構成＞

図２（Ｂ）は、ウェアラブル端末１０２の内部構成を示す図である。

【００２４】

システムバス２４１は、２４２～２５２の各部を相互に接続する。ＣＰＵ２４２は、ＲＯＭ２４４や記憶装置２４５に格納されているＯＳ（オペレーティングシステム）などのプログラム（後述する各処理を実現するプログラムも含む）を読み出して各種制御処理を実行する。ＲＡＭ２４３は、ＣＰＵ２４２のメモリーやワークエリアとして機能する。ネットワークＩ／Ｆ２４７は、ＷｉＦｉなどを用いた、外部のネットワーク機器と片方向または双方向にデータをやり取りする。ＣＰＵ２４２は、ＲＡＭ２４３やＲＯＭ２４４と共にプログラムの実行処理を行うとともに、記録装置２４５等の記録媒体にデータを記録する処理を行う。

【００２５】

Ｔａｍｐｅｒ　Ｍｏｄｕｌｅ（ＴＰＭ）２４６は、機密情報を処理したり格納したりする目的で、格納したデータを外部から読み取られることを防ぐ耐タンパー性を備えた記憶領域である。本発明では、生体認証に用いる生体情報自体、またはその生体情報の特徴量

や、その生体情報に対応する秘密鍵などが格納される。生体情報自体、またはその生体情報の特徴量など生体認証処理に必要で、ＴＰＭ２４６に格納されるデータを生体情報と呼ぶ。生体情報センサー２４８は、ユーザーの生体情報を読取るセンサーであり、例えばユーザーの心電図の情報を読み取り信号に変換する。なお、ＴＰＭ２４６に代えて、耐タンパー性を備えるような特別な記憶領域に、生体情報や秘密鍵といった情報を管理する仕組みであってもよい。

【００２６】

タッチパネル２４９は、表示と入力の２つの機能を備えており、ユーザーに伝える情報を表示したりするとともに、ユーザーが画面に手などで圧力を加えることにより、触れられた画面位置情報を外部へ情報信号として出力する。出力された信号情報をアプリケーションが利用することで、ユーザーはタッチパネル２４９を通じてアプリケーションを操作することができる。

【００２７】

近接通信Ｉ／Ｆ２５０は、ＮＦＣやＢｌｕｅｔｏｏｔｈなどの近接通信用の通信方式に対応したインターフェースである。本実施例においては、ＭＦＰ１０１とこのインターフェースを介して通信を行う。

【００２８】

留め金センサー２５１は、ウェアラブル端末１０２がユーザーに装着されているかを検知するためのセンサーである。ウェアラブル端末１０２がユーザーに装着された状態で一度認証が行われると、留め金センサー２５１が、ユーザーからウェアラブル端末１０２が取り外されたことを検知するまで認証された状態となる。

【００２９】

振動モーター２５２は、ウェアラブル端末１０２を振動させる。この振動により、ユーザーへの通知を行う。

【００３０】

ウェアラブル端末１０２は、マイク（不図示）なども備え、タッチパネル２４９に代えてユーザー入力を音声で受け付けることも可能である。

【００３１】

情報処理装置１０４は、少なくとも、ウェアラブル端末１０２のＣＰＵ２４２、ＲＯＭ２４４、記憶装置２４５、ＲＡＭ２４３、ＴＰＭ２４６、生体情報センサー２４８、近接通信Ｉ／Ｆ２５０などと同様の構成を備える。なお、情報処理装置１０４の記憶装置は、ウェアラブル端末１０２と連携するためのアプリケーションプログラムが格納され、ＣＰＵにより実行される。

【００３２】

ここで、情報処理装置１０４は、該アプリケーションの機能により、ウェアラブル端末１０２の代わりに、ペアリングしたウェアラブル端末１０２を装着するユーザーの生体認証を行うことができる。認証に成功した場合には、その認証状態をウェアラブル端末１０２に通知することができる。つまり、ウェアラブル端末１０２自体に認証機能が無くても、装着者の認証状態と、認証により特定されたユーザーの識別情報を、情報処理装置１０４から得られることになる。

【００３３】

＜ＭＦＰの機能構成＞

図３（Ａ）は、ＭＦＰ１０１の機能構成の一例を示すブロック図である。

【００３４】

ＭＦＰ１０１では、表示制御部３０１、機能実行部３０２、通信部３０３、認証部３０４、認証制御部３０５、ユーザー情報格納部３０６が動作する。ＭＦＰ１０１の各部は、ＲＯＭ２０４やＨＤＤ２０７に記憶されている１以上のプログラムを、ＣＰＵ２０１がＲＡＭ２０２に読み出して実行することによって実現する。

【００３５】

表示制御部３０１は、後述するログイン画面や、ウェアラブル端末の登録指示を受け付

けるためのＵＩを操作部２０９に表示するためのソフトウェアモジュールである。機能実行部３０２は、スキャナ２１５を用いた原稿のスキャン、ネットワークＩ／Ｆ２０４を用いた画像データの送信、プリンタ２１６を用いた画像データの印刷などの機能を実行するソフトウェアモジュールである。機能ごとにモジュールが用意されても良い。通信部３０３は、ウェアラブル端末１０２などの外部の装置と通信するためのソフトウェアモジュールである。

【００３６】

認証部３０４は、ＩＣカードなどを用いた認証情報（パスワードなど）の入力によるユーザー認証を行うためのソフトウェアモジュールである。認証部３０４による認証の結果に従い、機能実行部３０２による各機能の制限制御や、画像データの送信先となる認証ユーザーのアドレス情報の取得などが行われることになる。

【００３７】

認証制御部３０５は、ウェアラブル端末１０２で提供される認証に係る機能を利用するためのソフトウェアモジュールである。例えば、ウェアラブル端末１０２を提供する企業からＳＤＫ（Ｓｏｆｔｗａｒｅ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｋｉｔ）のような形で提供されることが考えられる。認証制御部３０５は、認証部３０４と連携し、ウェアラブル端末１０２で認証成功しているユーザーについては、認証部３０４での更なる認証処理の実行を省略するといった制御を実現する。

【００３８】

ユーザー情報格納部３０６は、表Ａを用いて後述するユーザー情報管理テーブルや、表Ｂを用いて後述する端末管理テーブルをＨＤＤ２０７などの記憶装置に格納して管理するソフトウェアモジュールである。

【００３９】

＜ウェアラブル端末の機能構成＞

図３（Ｂ）は、ウェアラブル端末の機能構成の一例を示すブロック図である。

【００４０】

ウェアラブル端末１０２では、入力受付部３４１、通信部３４２、通知部３４３、認証処理部３４４、生体情報格納部３４５、認証管理部３４６が動作する。ウェアラブル端末１０２の各部は、ＲＯＭ２４４や記憶装置２４５に記憶されている１以上のプログラムを、ＣＰＵ２４２がＲＡＭ２４３に読み出して実行することによって実現する。

【００４１】

入力受付部３４１は、ユーザーによる入力を、タッチパネル２４９やマイク（不図示）を介して受け付けるためのソフトウェアモジュールである。通信部３４２は、ウェアラブル端末１０２などの外部の装置と通信するためのソフトウェアモジュールであり、ＢＬＥなどの近接通信でウェアラブル端末１０２と通信する。通知部３４３は、タッチパネル２４９にユーザーに伝える情報を表示したり、振動モーター２５２を振動させたりすることで、ユーザーに通知するソフトウェアモジュールである。

【００４２】

認証処理部３４４は、生体情報を読み取り生体認証を行うソフトウェアモジュールである。また、認証処理部３４４は、留め金センサー２５１がユーザーからウェアラブル端末１０２が取り外されたことを検知したときに、その信号を受けて認証状態を未認証の状態に変更する。さらに認証処理部３４４は、ＭＦＰ１０１などからの認証状態の確認の依頼を受けた時に認証状態を返却する。なお、情報処理装置１０４で認証処理を代行させるウェアラブル端末であっても、認証状態を管理し、ＭＦＰ１０１に対してその状態を返却するための認証処理部３４４を有する。

【００４３】

生体情報格納部３４５は、耐タンパー性を備えるような特別な記憶領域で、表Ｃを用いて後述する生体情報テーブルや表Ｄを用いて後述する認証情報テーブルを管理するソフトウェアモジュールである。

【００４４】

＜ＭＦＰが管理するテーブル＞

表Ａと表Ｂは、ＭＦＰ１０１のユーザー情報格納部３０６が管理するテーブルの例である。

【００４５】

【表１】

表A

ユーザーID	パスワード	メールアドレス
user001	**********	user001@co.jp
user004	**********	user004@co.jp
・・・	・・・	・・・

【００４６】

表Ａは、ユーザー情報管理テーブルである。１つのレコードが１つのユーザー情報を示している。ユーザーＩＤ列は、ＭＦＰ１０１のユーザーを一意に識別するための識別情報（ユーザーＩＤ）である。パスワード列は、認証部３０４がユーザーを認証するためのパスワードを格納する。メールアドレス列は、ユーザーの連絡先であるメールアドレスを格納する。メールアドレス以外にもユーザーのホームフォルダのファイルパスや、ユーザーの住所など、ユーザーに関する属性情報を本テーブルに格納するようにしてもよい。

【００４７】

【表２】

表B

認証情報ID	公開鍵	ユーザーID
407c-8841-79d	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	user001
4c04-428b-a7a2	8143CA9F-35C9-4333-948F-BFCE66A74310	user002
・・・	・・・	・・・

【００４８】

表Ｂは、ＭＦＰに登録されたウェアラブル端末に関する情報を管理する端末管理テーブルである。１つのレコードが１つのウェアラブル端末の情報を表している。認証情報ＩＤ列は、ＭＦＰ１０１のユーザーと紐づけられているウェアラブル端末を一意に識別するためのＩＤである。尚、図４を用いて後述するが認証情報ＩＤはＭＦＰ１０１の登録要求を受けて、ウェアラブル端末１０２が発行する。公開鍵列はウェアラブル端末１０２が発行した秘密鍵とペアになる公開鍵の情報である。秘密鍵はウェアラブル端末１０２で保存、管理される。ユーザーＩＤ列はウェアラブル端末と紐づいているＭＦＰ１０１のユーザーＩＤを格納する。さらに、各レコードに対応するウェアラブル端末の識別情報である端末ＩＤを、各レコードに含ませて管理してもよい。

【００４９】

＜ウェアラブル端末が管理するテーブル＞

表Ｃと表Ｄは、ウェアラブル端末１０２の生体情報格納部３４５が管理するテーブルの例である。

【００５０】

【表３】

表C

生体情報ID	認証状態
d493a744	認証済

【００５１】
表Ｃは、生体情報テーブルである。１つのレコードが１つの生体情報を示している。生体情報ＩＤ列は生体情報の特徴量に対応する識別情報（生体情報ＩＤ）を格納する。認証状態列は、認証状態を表している。認証されている場合は、“認証済”であり、認証されていない場合は、“未認証”となる。認証状態は、認証処理部３４４が生体情報を用いて認証処理を実行した場合や、ユーザーからウェアラブル端末１０２が取り外された場合に更新される。
【００５２】
【表４】

表D

認証情報ID	アプリケーション名	秘密鍵
407c-8841-79d	mfp_app	1faea2da-a269-4fa7-812a-509470d9a0cb
4c04-428b-a7a2	pos_app	d7ae30c8-3775-4706-8597-aaf681bc30f5
92b2-498d-bea6	med-svc	36ae5eed-732b-4b05-aa7b-4dddb4be3267
・・・	・・・	・・・

【００５３】
表Ｄは、認証情報テーブルである。１つのレコードが１つの認証情報を表している。認証情報ＩＤ列は、各認証情報に対して一意な識別情報（認証情報ＩＤ）である。アプリケーション名は、アプリケーションを一意に識別する名前である。認証情報ＩＤはアプリケーションごとに発行される。秘密鍵列は、各認証情報に対応付けて生成された秘密鍵を格納する。秘密鍵とペアとなる公開鍵は、秘密鍵の生成時に一緒に生成され、前記アプリケーション名で示されるアプリケーションで管理、参照される。
【００５４】
表Ｄに対応する情報を格納する手順については図４を用いて後述する。
【００５５】
＜ウェアラブル端末の登録＞
ＭＦＰ１０１からのウェアラブル端末１０２の登録について図４、及び、図５を用いて説明する。
【００５６】
図５（Ａ）は、ＭＦＰ１０１のログイン画面の一例である。ログイン画面５００は、テキストボックス５０１、テキストボックス５０２、ボタン５０３で構成される。テキストボックス５０１は、ユーザーＩＤの入力を受け付けるためのテキストボックスである。テキストボックス５０２はパスワードの入力を受け付けるためのテキストボックスである。ボタン５０３は、各テキストボックスに入力されたユーザーＩＤとパスワードでログインを受け付けるためのボタンである。図４で示すフローチャートは、例えば、ボタン５０３への操作を検知する、ログイン用のＩＣカードをカードリーダーにタッチすることで開始される処理の一例を説明するものである。
【００５７】

ＭＦＰ１０１の認証部３０４は、入力されたユーザーＩＤとパスワードでログイン処理を行う。ここでは、テキストボックス５０１、５０２に入力された情報が利用される。認証部３０４は、表Ａのユーザー情報管理テーブルに保存されている情報にテキストボックス５０１、５０２に入力されたユーザーＩＤとパスワードが格納されているかを確認することでログイン可否を判断する。ログインできなかった場合にはログイン画面５００にその旨を通知（不図示）して再入力を求める。

【００５８】

表示制御部３０１は、ログイン後、ログインしたユーザーのためのトップ画面を表示する。ここで、図５（Ｂ）を用いてトップ画面について説明する。

【００５９】

図５（Ｂ）は、ＭＦＰ１０１のトップ画面の一例である。トップ画面５２０は、ＭＦＰ１０１が提供する機能を実行するためのボタンを配置する。ボタン５２１はウェアラブル端末の登録を受け付けるためのボタンである。

【００６０】

図４は、ウェアラブル端末１０２の登録に関する、ＭＦＰ１０１とウェアラブル端末１０２のそれぞれの処理を示したフローチャートである。本処理は、ＭＦＰ１０１が、トップ画面５２０のボタン５２１へのユーザー操作を検知したことに応じて、開始される。

【００６１】

なお、Ｓ４０４からＳ４１０がＭＦＰ１０１の処理である。Ｓ４５１からＳ４５６がウェアラブル端末１０２の処理である。図４で示す処理は、ＭＦＰ１０１とウェアラブル端末１０２のそれぞれのフローチャートに記載の各ステップに係るプログラムが実行されることで、実現されることになる。

【００６２】

Ｓ４０４で、認証制御部３０５は、登録モードになっているウェアラブル端末の検出処理を実行し、Ｓ４０５に遷移する。

【００６３】

Ｓ４０５で、認証制御部３０５は、ウェアラブル端末を検出できたかを確認する。後述するがウェアラブル端末１０２は、登録モードに状態を変更することが可能で、Ｓ４０４では登録モードになっているウェアラブル端末だけが検出される。ウェアラブル端末が検出できた場合はＳ４０６に遷移する。検出できないまま、所定時間、経過してしまった場合には、表示制御部３０１が検出できなかった旨を表示し、本処理を終了する。本処理が終了する場合には、図５（Ｂ）で示すＭＦＰ１０１のトップ画面に戻ることになる。

【００６４】

Ｓ４０６で、表示制御部３０１は、登録するウェアラブル端末を確認するための画面を表示し、Ｓ４０７に遷移する。

【００６５】

図５（Ｃ）は、Ｓ４０６で表示制御部３０１が表示する確認画面の一例である。確認画面５５０は、テキスト表示領域５５１と、ボタン５５２、５５３から成る。テキスト表示領域５５１は、Ｓ４０４で検出したウェアラブル端末を表示する。ボタン５５２は、テキスト表示領域５５１で表示しているウェアラブル端末の登録処理の実行を受け付けるためのボタンである。ボタン５５３は、ウェアラブル端末の登録のキャンセルを受け付けるためのボタンである。尚、確認画面５５０の例では、１つだけが検出された例について記載しているが、登録モードのウェアラブル端末が複数検出された場合は、選択するためのＵＩを表示してもよい。

【００６６】

Ｓ４０７で、表示制御部３０１は、確認画面５５０への操作があるまで監視を続ける。ここで、ボタン５５２への操作が検知された場合はＳ４０８に遷移する。ボタン５５３への操作が検知された場合は本処理を終了する。

【００６７】

Ｓ４０８で、認証制御部３０５は、通信部３０３を介してウェアラブル端末１０２に登

録依頼を送信してＳ４０９に遷移する。登録依頼にはアプリケーション名を含める。
【００６８】
Ｓ４０９で、通信部３０３は、Ｓ４０９で送信した登録依頼の応答があったかを監視する。応答があった場合は、Ｓ４１０に遷移する。応答がない場合は監視を続ける。
【００６９】
Ｓ４１０で、認証部３０４は、認証制御部３０５を介して受け取った応答に含まれる認証情報ＩＤと公開鍵と、Ｓ４０１でログインしたユーザーのユーザーＩＤとを、表Ｂの端末管理テーブルに保存して終了する。以上により、ＭＦＰ１０１での登録処理が終了する。
【００７０】
次に、ウェアラブル端末１０２の登録処理について説明する。
【００７１】
ウェアラブル端末の入力受付部３４１が、登録モード変更するためのユーザー操作を受け付けると、Ｓ４５１の処理が開始される。登録モードに変更するための操作とは、例えば、ウェアラブル端末の１０２のタッチパネル２４８を一定回数タップすることなどである。
【００７２】
Ｓ４５１で、認証処理部３４４は、登録依頼を受け付けるための登録モードに状態を変更して、Ｓ４５２に遷移する。Ｓ４５２で、認証処理部３４４は、ＭＦＰ１０１などの他の装置からの通信を監視し、登録依頼があったかをチェックする。登録依頼があった場合はＳ４５４に遷移する。登録依頼がない場合はＳ４５３に遷移する。
【００７３】
Ｓ４５３で、認証処理部３４４は、登録モードに変更してから一定期間経ったかを確認する。一定期間経っていた場合はタイムアウトして、登録モードを解除して処理を終了する。一定期間経っていない場合はＳ４５２に遷移して、通信の監視を続ける。
【００７４】
Ｓ４５４で、認証処理部３４４は、認証情報ＩＤと、秘密鍵、公開鍵の鍵ペアを作成して、Ｓ４５５に遷移する。Ｓ４５５で、生体情報格納部３４５は、表Ｄの認証情報テーブルに、Ｓ４５４で作成した認証情報ＩＤと秘密鍵、Ｓ４５２で受信した登録依頼に含まれるアプリケーション名を保存し、Ｓ４５６に遷移する。なお、認証情報ＩＤと、秘密鍵、公開鍵の鍵ペアは、生体情報を用いて認証処理に成功したタイミングで、事前に作成され、保存されていてもよい。
【００７５】
Ｓ４５６で、通信部３４２は、Ｓ４５４で作成した認証情報ＩＤと公開鍵をＭＦＰ１０１に送信して、処理を終了する。
【００７６】
以上のようにウェアラブル端末の登録処理を行うことで、ＭＦＰ１０１のユーザーとウェアラブル端末を紐づけることができる。
【００７７】
＜自分の連絡先への送信＞
次に、ＭＦＰ１０１でスキャンした画像データを、ログインユーザーの連絡先に送信する処理について、図６から図８を用いて説明する。
【００７８】
本実施例では、ウェアラブル端末１０２を装着したユーザーがＭＦＰ１０１のスキャナ２１５にスキャンしたい原稿を置くことで、処理が開始できる。
【００７９】
具体的には、原稿がＭＦＰ１０１のスキャナ２１５に置かれた場合に、認証制御部３０５は、通信部３０３を介して、ウェアラブル端末が、所定の距離範囲（認証状態を確認可能な範囲）内に存在するかの存在確認を行う。その範囲に、ウェアラブル端末の存在が確認された場合に、図６で示す処理が開始される。なお、スキャナ２１５に原稿が置かれているのにもかかわらず、その範囲にウェアラブル端末の存在が確認されない場合には、表

示制御部３０１が、図７（Ａ）に示すような、エラーメッセージを含むログイン画面５００を表示してもよい。

【００８０】

図６は、スキャンした画像データをログインユーザーの連絡先に送信するときの、ＭＦＰ１０１とウェアラブル端末１０２の処理を示したフローチャートである。Ｓ６０４からＳ６１７までがＭＦＰ１０１の処理である。Ｓ６３１からＳ６３５までがウェアラブル端末１０２の処理である。図６に示す処理は、ＭＦＰ１０１とウェアラブル端末１０２のそれぞれのフローチャートに記載の各ステップに係るプログラムが実行されることで、実現されることになる。

【００８１】

Ｓ６０４で、認証制御部３０５は、所定の距離範囲内に、ウェアラブル端末１０２の存在を確認する。Ｓ６０５で、認証制御部３０５は、ウェアラブル端末１０２に認証状態の確認依頼を送信してＳ６０６に遷移する。この確認依頼には、認証情報ＩＤなどを、該ＩＤに対応する登録済みの公開鍵で暗号化したものを含めて送信する。本例では、登録済のウェアラブル端末が存在した場合に認証状態の確認をしている。しかし、認証状態を確認可能な範囲が広い場合や、複数存在した場合のために、ウェアラブル端末を動かすジェスチャーやタッチパネル２４８へのタップなどの操作により、ユーザーの認証の意志を確認してからウェアラブル端末に認証状態の確認をしてもよい。

【００８２】

Ｓ６０６で、通信部３０３は、ウェアラブル端末１０２から認証状態が返却されたかを監視する。ウェアラブル端末１０２からのデータの返却により、認証状態が取得できた場合はＳ６０７に遷移する。認証状態が返却されていない場合は、監視を続ける。ウェアラブル端末１０２から返却されるデータは登録済みの公開鍵により復号できる。また、ウェアラブル端末１０２から返却されるデータには、認証状態に加えて、ウェアラブル端末１０２の識別情報が含まれる。そのほかにも、ウェアラブル端末１０２から返却されるデータに、認証情報ＩＤや装着者のユーザーＩＤといった識別情報を含めることも可能である。

【００８３】

Ｓ６０７で、認証部３０４は、返却された認証状態を確認し、認証済である場合にはＳ６０８に遷移する。認証状態が未認証である場合にはＳ６１８に遷移する。Ｓ６１８では、表示制御部３０１が、前述した図７（Ａ）に示すようなエラーメッセージを含むログイン画面５００を表示する。そして、本処理を終了する。

【００８４】

Ｓ６０８で、表示制御部３０１は、ＭＦＰ１０１の操作部２０９に対して送信実行中画面の表示を制御する。なお、表示制御部３０１は、ウェアラブル端末１０２に対して、送信実行中を示す情報と、後述の割り込み処理の指示を受け付けるための情報とを提供することで、ウェアラブル端末１０２のタッチパネルに対する表示を制御してもよい。さらに、Ｓ６０９で機能実行部３０２は、原稿のスキャン制御、ならびに、スキャンデータの送信制御を開始する。ここでは、表Ｂを参照することで、Ｓ６０４で存在が確認されたウェアラブル端末１０２に紐付けて登録されるユーザーＩＤが特定される。そして、表Ａのユーザー情報管理テーブルを参照して、そのユーザーＩＤに対応する宛先情報（メールアドレス）が特定できる。特定された宛先情報が、スキャンデータの送信先に自動で設定される。また、ウェアラブル端末１０２から返却されたデータに含まれる識別情報（端末ＩＤ、認証情報ＩＤやユーザーＩＤ）を用いて、対応する宛先情報を特定しても良い。

【００８５】

また、宛先以外のスキャン、送信の設定（解像度、ファイルフォーマットなど）は、予めＭＦＰ１０１で管理しているデフォルト設定が利用される。なお、この設定については、ユーザーＩＤに紐付けて、ユーザー毎のお気に入りの設定がＭＦＰ１０１またはネットワーク上の認証サーバーなどに登録されていて、それが利用されても良い。その場合には、ユーザーＩＤに対応する宛先情報と一緒に、お気に入りの設定が読み出されることになる。

【００８６】
図７（Ｂ）は、Ｓ６０８で表示する送信実行中画面の一例である。送信実行中画面７５０は、ボタン７５１からボタン７５３で構成される。ボタン７５１は、自分の連絡先への送信をキャンセルする指示を受けつけるためのボタンである。ボタン７５２は、他の人に送信するための設定ＵＩを表示するためのボタンである。ボタン７５３は、スキャンデータの送信ではなく、コピー処理に切り替えるために、コピー処理の設定ＵＩを表示するためのボタンである。
【００８７】
送信実行中画面７５０を介して、いずれかのボタンが操作されると、割り込み処理となり、Ｓ６１５の処理が実行される。送信実行中画面７５０に対していずれのボタンへも操作がなく、送信処理が完了すると、割り込み処理は発生しない。割り込みが発生した場合には、送信処理は開始されない、または、実行中であれば停止（一時中断）される。
【００８８】
Ｓ６１１で、表示制御部３０１は、Ｓ６０９の送信処理が完了したかを監視する。処理が完了した場合は、Ｓ６１２に遷移する。処理が完了していない場合は、Ｓ６１４に遷移する。
【００８９】
Ｓ６１２で、図８（Ａ）を用いて後述する送信完了処理を実行し、Ｓ６１３に遷移する。
【００９０】
Ｓ６１３で、図８（Ｂ）を用いて後述する原稿取り忘れ確認処理を実行して、本処理を終了する。
【００９１】
Ｓ６１４で、表示制御部３０１は、送信実行中画面７５０で、いずれかのボタンが操作されて割り込みが発生したかを監視する。割り込みが発生した場合にはＳ６１５に遷移する。割り込みが発生していない場合は、Ｓ６１１に遷移し送信処理が完了したかの監視を続ける。ここで、表示制御部３０１が処理するＳ６０８の送信実行中画面の表示と、機能実行部３０２が処理するＳ６０９の処理は、別スレッドで行われる。そのため、Ｓ６１４の割り込みの有無の判断は、Ｓ６０９での処理開始から、送信処理の完了までの間に、非同期で実行されることになる。
【００９２】
Ｓ６１５で、表示制御部３０１は、送信実行中画面７５０から指示された割り込み処理の内容を確認する。処理内容が、ボタン７５１による処理のキャンセルであった場合にはＳ６１６に遷移する。そのほかのボタン７５２やボタン７５３への操作であった場合にはＳ６１７に遷移する。
【００９３】
Ｓ６１６で、機能実行部３０２は、実行中の処理をキャンセルして処理を終了する。送信処理が中断されている場合には、送信済みのデータをサーバーから削除するなどして、送信処理をキャンセルする。
【００９４】
Ｓ６１７で、表示制御部３０１は、指定された処理内容に対応する機能を実行するためのＵＩ（設定画面）を表示する。ボタン７５２が押下された場合は、他の人に送信するための設定を行うＵＩを表示する。ボタン７５３が操作されていた場合にはコピー用のＵＩ（設定画面）を表示する。設定完了後、スキャンデータを用いた送信処理、またはコピー処理が実行され、処理が完了した場合にはＳ６１３に遷移する。
【００９５】
続いて、ウェアラブル端末１０２の処理についても説明する。
【００９６】
Ｓ６３１で、通信部３４２は、ＭＦＰ１０１からの通信を監視し、その内容が認証状態の確認依頼があったかをチェックする。認証状態の確認依頼があった場合はＳ６３２に遷移する。認証状態の確認依頼がなかった場合は、通信内容の監視を続ける。確認依頼を含

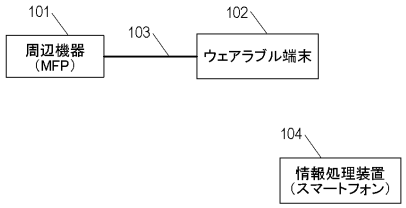
むデータは、秘密鍵を用いて復号できる。
【００９７】
Ｓ６３２で、認証処理部３４４は、生体情報格納部３４５を介して、Ｓ６３１で受信した認証状態の確認依頼に含まれる認証情報ＩＤが、前述した表Ｄで示すテーブルに登録され、管理されているかを確認する。認証情報ＩＤの登録がある場合はＳ６３３に遷移する。認証情報ＩＤがない場合には、図４で説明した登録処理がなされていないと判断して、Ｓ６３５に遷移する。
【００９８】
Ｓ６３３で、認証処理部３４４は、生体情報格納部３４５を介して、表Ｃの生体情報テーブルの認証状態を取得し、Ｓ６３４に遷移する。Ｓ６３４で、通信部３４２は、ＭＦＰ１０１に認証状態を含むデータを送信して、処理を終了する。認証状態を含むデータは、秘密鍵で暗号化してもよい。また、該データには、前述した通り、自身の端末ＩＤ、認証情報ＩＤなどの識別情報を含めても良い。
【００９９】
Ｓ６３５で、認証処理部３４４は、認証状態を未認証としてＳ６３４に遷移する。この場合には、通信部３４２は、ＭＦＰ１０１に未認証を示す認証状態を送信して、処理を終了する。
【０１００】
図８（Ａ）は、Ｓ６１２で実行する送信完了処理の詳細である。図８（Ａ）では、ＭＦＰ１０１の処理のみならず、それに付随して発生する、ウェアラブル端末１０２が実行する処理についても説明する。
【０１０１】
Ｓ８０１で、ＭＦＰ１０１の通信部３０３は、Ｓ６０９で実行されたログインユーザーに対応する宛先情報を用いた送信処理の完了を示す結果を通知する。
【０１０２】
Ｓ８２１で、ウェアラブル端末１０２の通信部３４２は、ＭＦＰ１０１からの通信を監視し、送信処理の結果を受信したかをチェックする。送信処理の結果を受信した場合は、Ｓ８２２に遷移する。送信処理の結果を受信していない場合は通信内容の監視を続ける。
【０１０３】
Ｓ８２２で、通知部３４３は、送信処理の結果をユーザーに通知する。ユーザーへの通知は、タッチパネル２４９に、伝えるべきメッセージを表示したり、振動モーター２５２を振動させたりすることで行う。このようにウェアラブル端末１０２で送信完了を確認できるようにすることで、ＭＦＰ１０１の操作部２０９を見ていない場合やＭＦＰ１０１と少し離れた場所にいる場合でもユーザーが送信処理の結果を確認できる。
【０１０４】
図８（Ｂ）は、Ｓ６１３で実行する原稿取り忘れ確認処理の詳細である。図８（Ｂ）では、ＭＦＰ１０１の処理以外にも、関連するウェアラブル端末１０２が実行する処理についても説明する。
【０１０５】
Ｓ８５１で、ＭＦＰ１０１の機能実行部３０２は、原稿が取り除かれたことを監視する。スキャナ２１５から原稿が取り除かれると、スキャナ２１５がそれを検知して、機能実行部３０２に信号が送られる。原稿が取り除かれたことを検知した場合は、処理を終了する。原稿が取り除かれたことを検知しない場合は、Ｓ８５２に遷移する。Ｓ８５２で、ＭＦＰ１０１の機能実行部３０２は、通知条件を満たしているかを判断する。通知条件は、例えば、スキャナ２１５から原稿が取り除かれることなく、一定時間が経過した場合やウェアラブル端末１０２とＭＦＰ１０１が一定以上遠くなった場合などである。通知条件を満たしている場合はＳ８５３に遷移する。通知条件を満たしていない場合は、Ｓ８５１に遷移する。
【０１０６】
Ｓ８５３で、ＭＦＰ１０１の通信部３０３は、ウェアラブル端末１０２に、原稿が取り

忘れられていることを通知する。
【０１０７】
Ｓ８７１で、ウェアラブル端末１０２の通信部３４２は、ＭＦＰ１０１からの通信を監視し、原稿が取り忘れられていることの通知を受信したかチェックする。原稿の取り忘れを示す通知をＭＦＰ１０１から受信した場合にはＳ８７２に遷移する。該通知を受信していない場合は、通信の監視を続ける。
【０１０８】
Ｓ８７２で、通知部３４３は、原稿の取り忘れが発生しているかもしれないことをユーザーに通知する。ユーザーへの通知は、タッチパネル２４９に原稿の取り忘れが発生している可能性を示すメッセージを表示したり、振動モーター２５２を振動させたりすることで行う。このようにウェアラブル端末１０２でユーザーへの通知を行うことで、ユーザーは原稿の取り忘れに気づくことができる。
【０１０９】
以上、本実施例によれば、ＭＦＰ１０１への端末登録後は、予め認証済みのウェアラブル端末１０２を装着したユーザーが、ＭＦＰ１０１のスキャナに原稿をセットするだけで、他の操作なしに、自分の連絡先にスキャンした画像データを送信することができる。
【０１１０】
また、本実施例に依れば、ＭＦＰ１０１では生体情報を用いた認証処理は実行されない。つまり、複数ユーザーに共有されるような周辺装置に対して、各個人の生体情報を登録する必要が無いので、共有装置の利用のために生体情報を自分の所有物以外に登録することへの抵抗感を抑えることが可能である。
【０１１１】
（応用例１）
前述した実施例では、ＭＦＰ１０１のスキャナに原稿をセットするだけで、他の操作なしに、自分の連絡先にスキャンした画像データを送信することができた。また、スキャン開始後から、送信開始後までの間に、ＭＦＰ１０１の操作部２０９に対する操作により、割り込み処理が可能であった。
【０１１２】
この割り込み処理の指示に関しては、ＭＦＰ１０１に備えられたマイク（不図示）、ウェアラブル端末１０２のタッチパネル２４９やマイク（不図示）に対する音声入力により、実現されても良い。予め、入力ワードとして、“キャンセル”や“コピー”などが登録されており、音声解析によって、割り込み処理が可能となる。
【０１１３】
（応用例２）
前述した実施例では、ＭＦＰ１０１のスキャナを例に説明した。本発明は、それ以外にも、電子データ以外の情報媒体から情報を抽出して電子データに変換する機能を提供する周辺装置でも適用可能である。その場合には、変換後の電子データは、前述した実施例と同様にウェアラブル端末の装着者に対応する宛先へ自動で送信されることになる。ＭＦＰ１０１以外の例としては、被写体を情報媒体としたデジタルカメラなどがある。
【０１１４】
他にも、周辺装置のＭＦＰ１０１以外の具体例としては、デジタル健康器具が挙げられる。具体的には、周辺装置は、ウェアラブル端末の装着者の健康情報（血圧、体重、水分量、栄養状態など）を測定して、電子データに変換する。また、周辺装置のＭＦＰ１０１以外の具体例としては、デジタル楽器などが挙げられる。その場合には、周辺装置は、ウェアラブル端末の装着者の発声した音声、演奏した音楽をデジタルデータに変換する。これらの例では、情報媒体は、ウェアラブル端末の装着者自身、またはウェアラブル端末の装着者の動作となる。本応用例では、前述したＳ６１３の処理が省略される。
【０１１５】
（他の実施例）
本発明は、上述した実施形態を適宜組み合わせることにより構成された装置あるいはシ

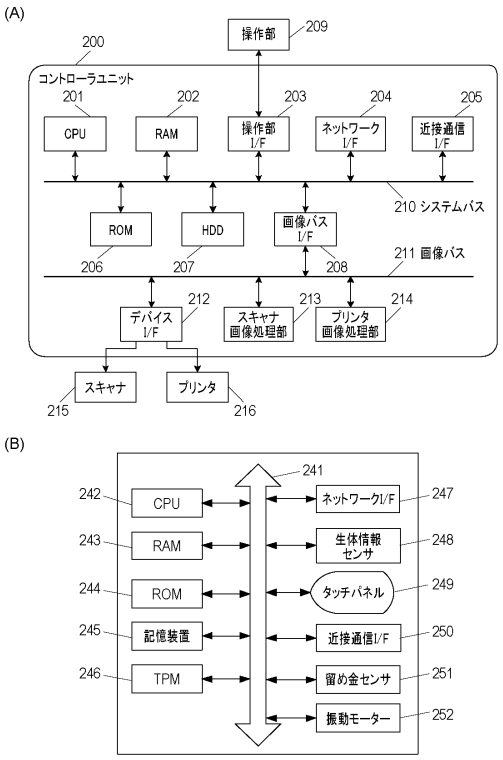
ステムやその方法も含まれるものとする。
【０１１６】
　ここで、本発明は、上述した実施形態の機能を実現する１以上のソフトウェア（プログラム）を実行する主体となる装置あるいはシステムである。また、その装置あるいはシステムで実行される上述した実施形態を実現するための方法も本発明の一つである。また、そのプログラムは、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給され、そのシステム或いは装置の１以上のコンピュータ（ＣＰＵやＭＰＵ等）によりそのプログラムが１以上のメモリーに読み出され、実行される。つまり、本発明の一つとして、さらにそのプログラム自体、あるいは該プログラムを格納したコンピューターにより読み取り可能な各種記憶媒体も含むものとする。また、上述した実施形態の機能を実現する回路（例えば、ＡＳＩＣ）によっても、本発明は実現可能である。
【符号の説明】
【０１１７】
　１０１　ＭＦＰ
　１０２　ウェアラブル端末１０２

【図面】

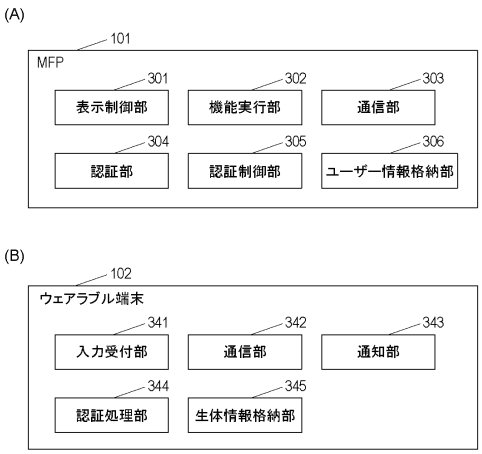
【図１】


101
周辺機器
（MFP）
103
102
ウェアラブル端末
104
情報処理装置
（スマートフォン）

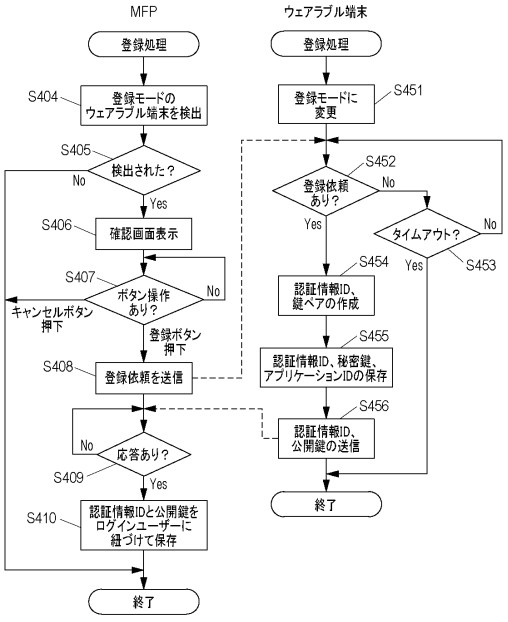
【図２】


(A)
操作部
209
200
コントローラユニット
201
CPU
202
RAM
203
操作部
I/F
204
ネットワーク
I/F
205
近接通信
I/F
210 システムバス
ROM
206
HDD
207
画像バス
I/F
208
211 画像バス
デバイス
I/F
212
スキャナ
画像処理部
213
プリンタ
画像処理部
214
スキャナ
215
プリンタ
216
(B)
241
242
CPU
243
RAM
244
ROM
245
記憶装置
246
TPM
ネットワークI/F
247
生体情報
センサ
248
タッチパネル
249
近接通信I/F
250
留め金センサ
251
振動モーター
252

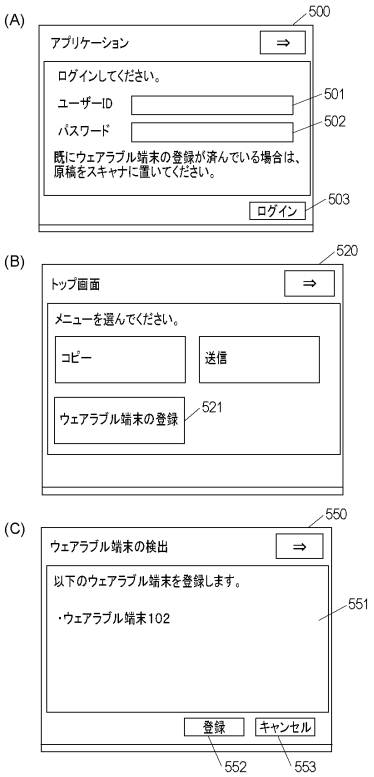
【図３】


(A)
101
MFP
301
表示制御部
302
機能実行部
303
通信部
304
認証部
305
認証制御部
306
ユーザー情報格納部
(B)
102
ウェアラブル端末
341
入力受付部
342
通信部
343
通知部
344
認証処理部
345
生体情報格納部

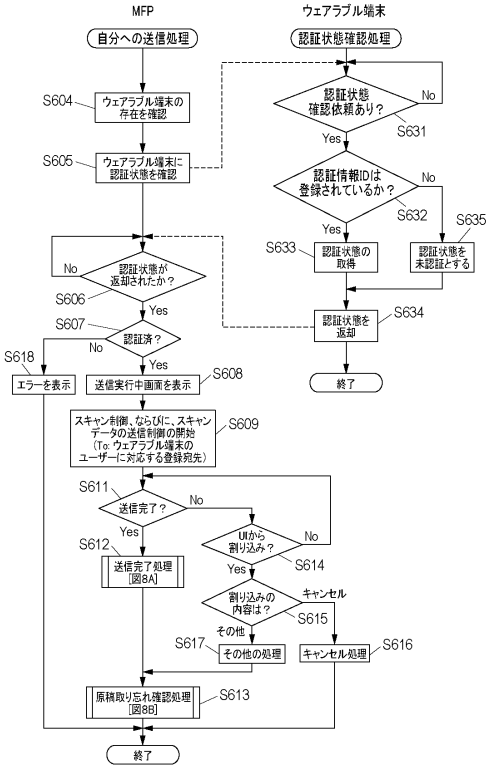
【図４】


MFP
ウェアラブル端末
登録処理
登録処理
S404
登録モードの
ウェアラブル端末を検出
S451
登録モードに
変更
S405
検出された？
No
Yes
S452
登録依頼
あり？
No
Yes
S406
確認画面表示
タイムアウト？
No
Yes
S453
S407
ボタン操作
あり？
No
キャンセルボタン
押下
S454
認証情報ID、
鍵ペアの作成
登録ボタン
押下
S455
認証情報ID、秘密鍵、
アプリケーションIDの保存
S408
登録依頼を送信
S456
認証情報ID、
公開鍵の送信
No
応答あり？
S409
Yes
終了
S410
認証情報IDと公開鍵を
ログインユーザーに
紐づけて保存
終了

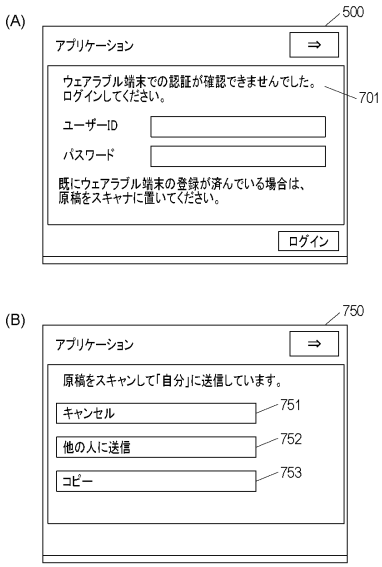
【図５】


(A)
500
アプリケーション
⇒
ログインしてください。
ユーザーID
501
パスワード
502
既にウェアラブル端末の登録が済んでいる場合は、
原稿をスキャナに置いてください。
ログイン
503
(B)
520
トップ画面
⇒
メニューを選んでください。
コピー
送信
ウェアラブル端末の登録
521
(C)
550
ウェアラブル端末の検出
⇒
以下のウェアラブル端末を登録します。
・ウェアラブル端末102
551
登録
キャンセル
552
553

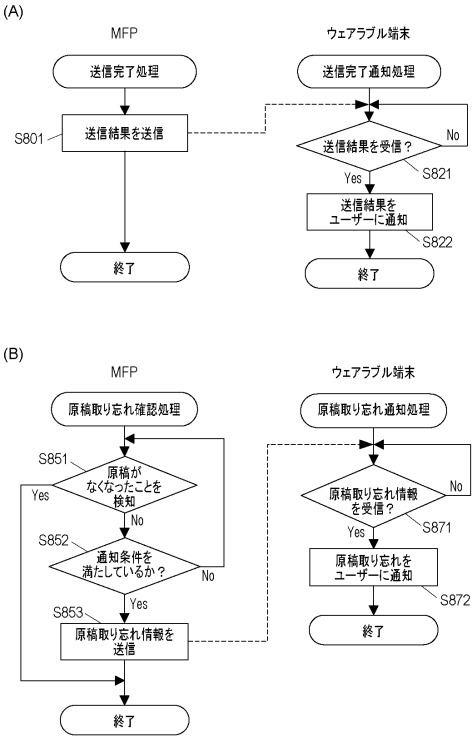
【図６】


MFP
ウェアラブル端末
自分への送信処理
認証状態確認処理
S604
ウェアラブル端末の存在を確認
S605
ウェアラブル端末に認証状態を確認
S606
認証状態が返却されたか？
No
Yes
S607
認証済？
No
Yes
S618
エラーを表示
送信実行中画面を表示
S608
スキャン制御、ならびに、スキャンデータの送信制御の開始
(To: ウェアラブル端末のユーザーに対応する登録宛先)
S609
S611
送信完了？
No
Yes
S612
送信完了処理
[図8A]
UIから割り込み？
No
Yes
S614
割り込みの内容は？
キャンセル
S615
その他
S617
その他の処理
キャンセル処理
S616
原稿取り忘れ確認処理
[図8B]
S613
終了
認証状態確認依頼あり？
No
Yes
S631
認証情報IDは登録されているか？
No
Yes
S632
S633
認証状態の取得
S635
認証状態を未認証とする
認証状態を返却
S634
終了

【図７】


(A)
500
アプリケーション
⇒
ウェアラブル端末での認証が確認できませんでした。
ログインしてください。
701
ユーザーID
パスワード
既にウェアラブル端末の登録が済んでいる場合は、
原稿をスキャナに置いてください。
ログイン
(B)
750
アプリケーション
⇒
原稿をスキャンして「自分」に送信しています。
キャンセル
751
他の人に送信
752
コピー
753

【図８】


(A)
MFP
ウェアラブル端末
送信完了処理
送信完了通知処理
S801
送信結果を送信
送信結果を受信？
No
Yes
S821
送信結果をユーザーに通知
S822
終了
終了
(B)
MFP
ウェアラブル端末
原稿取り忘れ確認処理
原稿取り忘れ通知処理
S851
原稿がなくなったことを検知
Yes
No
S852
通知条件を満たしているか？
No
Yes
S853
原稿取り忘れ情報を送信
原稿取り忘れ情報を受信？
No
Yes
S871
原稿取り忘れをユーザーに通知
S872
終了
終了

フロントページの続き

(56)参考文献 特開２０１７－１１１７３０（ＪＰ，Ａ）
特開２０１５－０７０３５３（ＪＰ，Ａ）
特開２０１８－１２１０９８（ＪＰ，Ａ）
特開２０１７－１０８３１６（ＪＰ，Ａ）
特開２０１７－０３７３６１（ＪＰ，Ａ）
特開２０１８－０６３７０２（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　１／００
Ｈ０４Ｌ　６７／０２
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　３／０１