(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7066380号
(P7066380)

(45)発行日　令和4年5月13日(2022.5.13)

(24)登録日　令和4年5月2日(2022.5.2)

(51)国際特許分類

H04L 9/32 (2006.01)	FI	H04L	9/32 200D
G06F 21/32 (2013.01)		H04L	9/32 100D
		H04L	9/32 200F
		G06F	21/32

請求項の数　14　（全34頁）

(21)出願番号　特願2017-222223(P2017-222223)
(22)出願日　平成29年11月17日(2017.11.17)
(65)公開番号　特開2019-96938(P2019-96938A)
(43)公開日　令和1年6月20日(2019.6.20)
審査請求日　令和2年11月2日(2020.11.2)

(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　100114775
弁理士　高岡 亮一
(74)代理人　100121511
弁理士　小田 直
(72)発明者　白河 祐貴
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　金沢 史明

最終頁に続く

(54)【発明の名称】　システム、システムにおける方法、情報処理装置、情報処理装置における方法、およびプログラム

(57)【特許請求の範囲】

【請求項１】

生体認証のための認証モジュール、該認証モジュールにより認証処理を行う際に必要なユーザの第１生体情報と該第１生体情報の登録の際に作成された第１秘密鍵とを格納するための耐タンパー性を備える記憶手段、ユーザの第１生体情報を読み取る生体情報センサ、およびディスプレイを有する情報処理装置と、

前記情報処理装置とネットワークを介して接続可能な、前記第１秘密鍵に対応する第１公開鍵を管理するためのサーバと、を含むシステムであって、

前記情報処理装置は、

前記ユーザの操作に従い所定の処理の実行を制御する実行手段と、

前記所定の処理の実行に際して、前記所定の処理に生体情報を関連付けることが指示された場合に、前記ユーザから前記生体情報センサを介して入力された、前記第１生体情報とは異なる第２生体情報を前記記憶手段に格納する格納手段と、

前記ユーザの該第２生体情報に対応する第２秘密鍵を前記記憶手段に格納したうえで、当該第２秘密鍵に対応する第２公開鍵を前記サーバに対して登録するための登録手段と、

前記サーバから認証要求を受信した場合に、前記ユーザから前記生体情報センサを介して入力された生体情報と前記記憶手段に登録された生体情報とを用いて、認証モジュールによる生体認証処理を実行する認証手段と、

前記生体認証処理で前記記憶手段に格納された前記第２生体情報についての認証に成功した場合に、前記第２秘密鍵と、前記認証要求に含まれるパラメータとを用いて、署名デー

タを作成する作成手段と、
前記作成された署名データを、前記サーバに送信する送信手段と、を有し、
前記サーバは、
前記認証要求に基づき前記情報処理装置から送信されてきた署名データの、前記サーバで管理している前記第２公開鍵を用いた検証を行う検証手段を、有し、
前記情報処理装置は、さらに、
前記サーバでの前記検証に成功した場合には、前記ディスプレイで、前記第２生体情報に関連付けられている前記所定の処理の実行に係る表示を行う表示手段と、を有することを特徴とするシステム。
【請求項２】
前記表示手段は、前記所定の処理の実行に係る表示として、前記第２生体情報の登録名称と、該所定の処理の内容を表示することを特徴とする請求項１に記載のシステム。
【請求項３】
前記表示手段は、前記所定の処理の実行に係る表示として、さらに、前記ユーザの他の生体情報の登録名称と、該他の生体情報に関連付けられている処理の内容とを表示することを特徴とする請求項２記載のシステム。
【請求項４】
前記表示手段は、前記所定の処理の実行に係る表示において、
該所定の処理がキャンセルされる場合には、ログアウトすることなく、別の表示に係る画面に遷移することを特徴とする請求項２または３に記載のシステム。
【請求項５】
前記情報処理装置は、さらに、
前記サーバでの前記検証に成功に応じて受信する通知に従い、前記第２生体情報に関連付けられている処理を特定する特定手段と、
前記サーバに対して、前記特定された処理のための要求を行う要求手段と、を有し、
前記表示手段は、前記所定の処理の実行に係る表示として、前記特定された処理の実行に係る表示を行うことを特徴とする請求項１乃至４のいずれか一項に記載のシステム。
【請求項６】
前記登録手段は、前記第２公開鍵を前記サーバに対して登録する際に、該第２公開鍵に対応する前記所定の処理の内容をさらに登録し、
前記サーバは、さらに、
前記署名データの検証に成功した場合に、前記第２公開鍵に対応する処理の内容を特定する特定手段と、
前記特定された処理の実行に係る表示を行うために必要となるデータを前記情報処理装置に対して送信する送信手段と、を有することを特徴とする請求項１乃至４のいずれか一項に記載のシステム。
【請求項７】
前記サーバは、前記情報処理装置からの登録の要求に応じて、前記第２公開鍵と、前記所定の処理の内容と、該情報処理装置の種別とを関連付けて管理する管理手段を有し、
前記管理手段は、さらに、前記登録された前記所定の処理の内容に対して、前記情報処理装置の種別とは異なる種別の情報処理装置に対応する処理の内容を管理し、
前記特定手段は、前記署名データの検証に成功した場合に、該署名データを送信した前記情報処理装置の種別に応じた処理の内容を特定することを特徴とする請求項６に記載のシステム。
【請求項８】
前記表示手段は、さらに、前記所定の処理に生体情報を関連付ける指示の際に、さらに、既に前記記憶手段に格納された生体情報とは異なる生体情報が格納されるよう、既に管理済みの生体情報の登録名称を識別できる表示を提供することを特徴とする請求項１乃至７のいずれか一項に記載のシステム。
【請求項９】

生体認証のための認証モジュール、該認証モジュールにより認証処理を行う際に必要なユーザの第１生体情報と該第１生体情報の登録の際に作成された第１秘密鍵とを格納するための耐タンパー性を備える記憶手段、ユーザの第１生体情報を読み取る生体情報センサ、およびディスプレイを有する情報処理装置と、
前記情報処理装置とネットワークを介して接続可能な、前記第１秘密鍵に対応する第１公開鍵を管理するためのサーバと、を含むシステムにおける方法であって、
前記情報処理装置が、
前記ユーザの操作に従い所定の処理の実行を制御する実行工程と、
前記所定の処理の実行に際して、前記所定の処理に生体情報を関連付けることが指示された場合に、前記ユーザから前記生体情報センサを介して入力された、前記第１生体情報とは異なる第２生体情報を前記記憶手段に格納する格納工程と、
前記ユーザの該第２生体情報に対応する第２秘密鍵を前記記憶手段に格納したうえで、当該第２秘密鍵に対応する第２公開鍵を前記サーバに対して登録するための登録工程と、
前記情報処理装置が、前記サーバから認証要求を受信した場合に、前記ユーザから前記生体情報センサを介して入力された生体情報と前記記憶手段に登録された生体情報とを用いて、認証モジュールによる生体認証処理を実行する認証工程と、
前記情報処理装置が、前記生体認証処理で前記記憶手段に格納された前記第２生体情報についての認証に成功した場合に、前記第２秘密鍵と、前記認証要求に含まれるパラメータとを用いて、署名データを作成する作成工程と、
前記情報処理装置が、前記作成された署名データを、前記サーバに送信する送信工程と、
前記サーバが、前記認証要求に基づき前記情報処理装置から送信されてきた署名データの、前記サーバで管理している前記第２公開鍵を用いた検証を行う検証工程と、
前記情報処理装置が、前記サーバでの前記検証に成功した場合には、前記ディスプレイで、前記第２生体情報に関連付けられている前記所定の処理の実行に係る表示を行う表示工程と、を有することを特徴とする方法。

【請求項１０】

生体認証のための認証モジュール、該認証モジュールにより認証処理を行う際に必要なユーザの生体情報を格納するための耐タンパー性を備える記憶手段、ユーザの生体情報を読み取る生体情報センサ、およびディスプレイを有する情報処理装置であって、
ユーザの認証に成功した後に提供されるべき第１処理の登録に関連して、前記生体情報センサを用いて読み取られる前記ユーザの第１生体情報を前記記憶手段に格納する格納手段と、
前記第１生体情報について作成され、前記記憶手段に格納されている第１秘密鍵に対応する第１公開鍵を登録するための要求をサーバに送信する送信手段と、を有し、
前記格納手段は、さらに、前記ユーザの認証に成功した後に提供されるべき第２処理の登録に関連して、前記生体情報センサを用いて読み取られる前記ユーザの第２生体情報を前記記憶手段に格納し、
前記送信手段は、さらに、前記第２生体情報について作成され、前記記憶手段に格納されている第２秘密鍵に対応する第２公開鍵を登録するための要求を前記サーバに送信し、
前記認証モジュールにより前記生体情報センサを用いて読み取られた前記第１生体情報を用いた生体認証が成功したことで前記第１秘密鍵を用いて生成された署名データが前記サーバで登録済みの前記第１公開鍵により検証できた場合に、前記ディスプレイに前記第１処理の内容に関する第１画面が表示され、
前記認証モジュールにより前記生体情報センサを用いて読み取られた前記第２生体情報を用いた生体認証が成功したことで前記第２秘密鍵を用いて生成された署名データが前記サーバで登録済みの前記第２公開鍵により検証できた場合に、前記ディスプレイに前記第２処理の内容に関する第２画面が表示されることを特徴とする情報処理装置。

【請求項１１】

第３処理の登録に関連して前記生体情報センサを用いて読み取った生体情報が該第３処理とは異なる他の処理と既に関連付けられている場合、その旨を示す通知を行う画面を前記

ディスプレイに表示する第１表示手段をさらに有することを特徴とする請求項１０に記載の情報処理装置。
【請求項１２】
認証時に、前記生体情報センサを用いて読み取った生体情報とは異なる、前記記憶手段に格納された生体情報の登録名称と、該異なる生体情報と関連付けられている処理とを確認するための確認画面を前記ディスプレイに表示する第２表示手段をさらに有することを特徴とする請求項１０または１１に記載の情報処理装置。
【請求項１３】
生体認証のための認証モジュール、該認証モジュールにより認証処理を行う際に必要なユーザの生体情報を格納するための耐タンパー性を備える記憶手段、ユーザの生体情報を読み取る生体情報センサ、およびディスプレイを有する情報処理装置における方法であって、
ユーザの認証に成功した後に提供されるべき第１処理の登録に関連して、前記生体情報センサを用いて読み取られる前記ユーザの第１生体情報を前記記憶手段に格納する第１格納工程と、
前記第１生体情報について作成され、前記記憶手段に格納されている第１秘密鍵に対応する第１公開鍵を登録するための要求をサーバに送信する第１送信工程と、
前記ユーザの認証に成功した後に提供されるべき第２処理の登録に関連して、前記生体情報センサを用いて読み取られる前記ユーザの第２生体情報を前記記憶手段に格納する第２格納工程と、
前記第２生体情報について作成され、前記記憶手段に格納されている第２秘密鍵に対応する第２公開鍵を登録するための要求を前記サーバに送信する第２送信工程と、
前記認証モジュールにより前記生体情報センサを用いて読み取られた前記第１生体情報を用いた生体認証が成功したことで前記第１秘密鍵を用いて生成された署名データが前記サーバで登録済みの前記第１公開鍵により検証された場合に、前記ディスプレイに前記第１処理の内容に関する第１画面を表示する第１表示工程と、
前記認証モジュールにより前記生体情報センサを用いて読み取られた前記第２生体情報を用いた生体認証が成功したことで前記第２秘密鍵を用いて生成された署名データが前記サーバで登録済みの前記第２公開鍵により検証された場合に、前記ディスプレイに前記第２処理の内容に関する第２画面を表示する第２表示工程と、を有することを特徴とする方法。
【請求項１４】
請求項１０乃至１２のいずれか一項に記載の各手段としてコンピュータを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】
本発明は、ネットワークサービスの利用時の操作性向上のためのシステムに関する。
【背景技術】
【０００２】
近年、生体認証を含む新たな認証システムとして、ＦＩＤＯ（Ｆａｓｔ　Ｉｄｅｎｔｉｔｙ　Ｏｎｌｉｎｅ）が注目されている。生体認証で用いられる指紋や静脈といった生体情報は、外部に情報が流出してしまった場合に、従来のＩＤ／パスワード認証におけるパスワードと異なり、情報を書き換えることができないため情報漏洩が致命的になる。
【０００３】
これに対して、ＦＩＤＯは予めユーザの手元のデバイスとＷｅｂサービスを提供するサーバとの間で登録処理を行っておく。登録処理では、デバイスにはユーザの生体情報と紐付いた秘密鍵が保存され、サーバ側にはその生体情報と紐付きデバイスに搭載された認証器の情報や秘密鍵のペアとなる公開鍵などの情報が登録される。そして、認証はインターネットを経由してサーバ上で行うのではなく、ユーザの手元のデバイス上で行い、ネットワーク上には秘密鍵で署名された認証結果が流れる。つまり、生体情報がネットワーク上を流れることがないため、情報漏洩のリスクが少ないと言える。

【０００４】
また、ＩＤ／パスワード認証とは異なり、生体認証を採用している認証システムでは、例えば、親指、人差指、中指、など複数の生体情報を登録できるシステムがある。特許文献１は、複数の指の指紋と、各指の指紋と特定の機能とをそれぞれ関連付けて登録しておき、認証時に認識された指紋が、登録された複数の指紋データのいずれかと一致する場合に、一致した指紋と関連付けられた機能を実行する携帯電話機を開示している。
【先行技術文献】
【特許文献】
【０００５】
【文献】特開２００５－２６８９５１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
例えば、ＭＦＰ（多機能周辺装置）等のデバイスをオフィスやコンビニに配置して、プリントサーバにあるデータをプリントするプルプリントシステムがある。プルプリントシステムを利用してプリント処理を実行するためには、（１）プリントサーバとの認証を行い、（２）プリントするドキュメントの選択や枚数、濃さなどの印刷設定を行い、（３）実行ボタンを押下する必要がある。
【０００７】
ステップ（２）のような設定は、定型的な操作であることが多く、プリント処理を実行する度に、ユーザが同じ操作を行うのは非効率的である。なお、プルプリントシステムに限らず、ＰＣやスマートフォンなどのデバイスからサーバとの通信を要するＷｅｂサービスを利用する場合においても同様に、該Ｗｅｂサービスにおいて定型的な操作を行う場合に都度ユーザが同じ操作を行うのは非効率的である。
【０００８】
しかしながら、特許文献１の技術では、デバイスにおける機能を利用するためのものであり、上述したようなＷｅｂサービスを利用する場合は考慮されていない。例えば、Ｗｅｂサービスを利用する場合、サービスを提供するサーバ側でユーザを認証する必要があり、デバイスにおける認証だけでは、即座にＷｅｂサービスの機能を実行することはできない。
【０００９】
本発明は、Ｗｅｂサービスを利用する際の操作性を向上させるシステ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】
【００１０】
本発明の一実施形態のシステムは、生体認証のための認証モジュール、該認証モジュールにより認証処理を行う際に必要なユーザの第１生体情報と該第１生体情報の登録の際に作成された第１秘密鍵とを格納するための耐タンパー性を備える記憶手段、ユーザの第１生体情報を読み取る生体情報センサ、およびディスプレイを有する情報処理装置と、前記情報処理装置とネットワークを介して接続可能な、前記第１秘密鍵に対応する第１公開鍵を管理するためのサーバと、を含むシステムであって、前記情報処理装置は、前記ユーザの操作に従い所定の処理の実行を制御する実行手段と、前記所定の処理の実行に際して、前記所定の処理に生体情報を関連付けることが指示された場合に、前記ユーザから前記生体情報センサを介して入力された、前記第１生体情報とは異なる第２生体情報を前記記憶手段に格納する格納手段と、前記ユーザの該第２生体情報に対応する第２秘密鍵を前記記憶手段に格納したうえで、当該第２秘密鍵に対応する第２公開鍵を前記サーバに対して登録するための登録手段と、前記サーバから認証要求を受信した場合に、前記ユーザから前記生体情報センサを介して入力された生体情報と前記記憶手段に登録された生体情報とを用いて、認証モジュールによる生体認証処理を実行する認証手段と、前記生体認証処理で前記記憶手段に格納された前記第２生体情報についての認証に成功した場合に、前記第２秘密鍵と、前記認証要求に含まれるパラメータとを用いて、署名データを作成する作成手段

と、前記作成された署名データを、前記サーバに送信する送信手段と、を有し、前記サーバは、前記認証要求に基づき前記情報処理装置から送信されてきた署名データの、前記サーバで管理している前記第２公開鍵を用いた検証を行う検証手段を、有し、前記情報処理装置は、さらに、前記サーバでの前記検証に成功した場合には、前記ディスプレイで、前記第２生体情報に関連付けられている前記所定の処理の実行に係る表示を行う表示手段と、を有する。

【発明の効果】

【００１１】

本発明のシステムによれば、Ｗｅｂサービスを利用する際の操作性を向上させることが可能となる。

【図面の簡単な説明】

【００１２】

【図１】システムのネットワーク構成を示す図である。

【図２】サーバおよびＰＣのハードウェア構成例を示す図である。

【図３】画像形成装置のハードウェア構成例を示す図である。

【図４】携帯端末のハードウェア構成例を示す図である。

【図５】各装置のソフトウェア構成例を示す図である。

【図６】オーセンティケータをサービスに登録する処理のシーケンスを示す図である。

【図７】オーセンティケータの登録時に使用するパラメータの一例を示す図である。

【図８】オーセンティケータの登録時に表示されるＵＩの一例を示す図である。

【図９】認証時の処理のシーケンスを示す図である。

【図１０】認証時に使用するパラメータの一例を示す図である。

【図１１】認証時に表示されるＵＩの一例を示す図である。

【図１２】第２実施形態における認証時に表示されるＵＩの一例を示す図である。

【図１３】第３実施形態における登録時に表示されるＵＩの一例を示す図である。

【図１４】第３実施形態における登録時のＭＦＰの処理を示す図である。

【図１５】第４実施形態における認証時に表示されるＵＩの一例を示す図である。

【発明を実施するための形態】

【００１３】

以下、本発明を実施するための形態について図面などを参照して説明する。

なお、本発明はＷｅｂ上のサービスがユーザを認証するために、ユーザの手元にある情報処理装置上で生体認証を行い、その結果を以ってサービスがユーザを認証する仕組みに関するものである。これは、Ｗｅｂ上のサービスにユーザの手元にある情報処理装置での生体認証に紐付く情報、例えば、認証識別情報、公開鍵などを予め登録しておくことで実現することができる。このような仕組みの一例としてＦＩＤＯを挙げたが、本発明はＦＩＤＯに限定したものではないことを予め断っておく。

【００１４】

［第１実施形態］

＜システム構成＞

図１は、本システムのネットワーク構成例を示す図である。

本システムは、ＭＦＰ１０１、携帯端末１０２、サーバ１０３、およびクライアントＰＣ１０４を備える。

【００１５】

サーバ１０３は、ネットワーク１０５や１０６を介し、ＭＦＰ１０１や携帯端末１０２、クライアントＰＣ１０４等の情報処理装置に接続可能であり、これら各デバイスにサービスを提供する外部システムである。サーバ１０３は、ＭＦＰ１０１や携帯端末１０２、クライアントＰＣ１０４から各種要求を受け付けるＷｅｂサーバを含み、１台のサーバ装置から構成されていてもよく、複数台の装置により構成されていてもよい。また、サーバ１０３は、一部または全部を仮想マシンやストレージなどのリソースを用いて構築してもよい。

【００１６】
本実施形態では、サーバ１０３が提供するサービスの一例として、プリントサービスがある。プリントサービスは、ネットワーク１０５や１０６を介して受信した文書データや画像データ等の各種データを保持し、ネットワーク１０５や１０６に接続するＭＦＰ１０１に保持したデータを提供して印刷させるクラウドプリントサービスを提供する。また、本実施形態では、ＭＦＰ１０１は、ユーザの手元にある生体認証を行う情報処理装置の一例である。なお、本発明は、ＭＦＰ１０１に限らず、その他の情報処理装置、例えば、携帯端末１０２やクライアントＰＣ１０４においても適用しうる。
【００１７】
ＭＦＰ１０１、携帯端末１０２、サーバ１０３、およびクライアントＰＣ１０４は、ネットワーク１０５を介して互いに接続される。ネットワーク１０５は、例えば、インターネット等のＬＡＮ、ＷＡＮ、電話回線、専用デジタル回線、ＡＴＭやフレームリレー回線、ケーブルテレビ回線、データ放送用無線回線等のいずれである。また、ネットワーク１０５は、これらの組み合わせにより実現される、いわゆる通信ネットワークである。ネットワーク１０５は、データの送受信が可能であればよい。
【００１８】
ＭＦＰ１０１と携帯端末１０２とは、ネットワーク１０６を介して接続される。ネットワーク１０６は、ＬＡＮなどの上述のネットワーク回線に加え、例えば、ＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）やＢｌｕｅＴｏｏｔｈ（登録商標）等の近距離通信なども含む。
【００１９】
＜サーバおよびＰＣのハードウェア構成＞
図２は、サーバ１０３およびクライアントＰＣ１０４のハードウェア構成例を示す図である。
ＣＰＵ２０１は、ＲＡＭ２０２をワークメモリとして、ＲＯＭ２０３および記憶装置２１０に格納されたプログラムを実行し、内部バス２１１を介して後述する各構成を総括的に制御する。キーボードコントローラ２０４は、キーボード２０８や不図示のポインティングデバイス（マウス、タッチパッド、タッチパネル、トラックボールなど）からの操作入力を制御する。
【００２０】
ディスプレイコントローラ２０５は、ディスプレイ２０９の表示を制御する。ディスクコントローラ２０６は、各種データを記憶するハードディスク（ＨＤ）、フレキシブルディスク（ＦＤ）等の記憶装置２１０へのデータアクセスを制御する。ネットワークインタフェース２０７は、ＬＡＮなどのネットワークに接続されて、ネットワークに接続された他の機器との通信を制御する。ハードウェアを構成する各部２０１～２０７は、内部バス２１１を介して接続されている。
【００２１】
＜ＭＦＰのハードウェア構成＞
図３は、ＭＦＰ１０１のハードウェア構成例を示す図である。ＭＦＰ１０１は画像形成装置の一例である。画像形成装置は、ＭＦＰ１０１に限られるものではなく、例えば、レーザービームプリンタ、インクジェットプリンタなどであってもよい。ＣＰＵ２２１は、ＲＡＭ２２２をワークメモリとして、ＲＯＭ２２３および記憶装置２２４に格納されたプログラムを実行し、内部バス２３３を介して後述する各構成を総括的に制御する。
【００２２】
ＲＡＭ２２２は、ＣＰＵ２２１の主メモリであり、ワークエリア等として機能する。記憶装置２２４は、各種データを格納する。ＲＯＭ２２３や記憶装置２２４には、例えば、後述する各処理を実現するプログラムが格納される。ネットワークＩ／Ｆ２２５は、他の情報処理装置と片方向または双方向にデータをやりとりする。生体情報センサ２２６は、ユーザの生体情報を読み取るセンサであり、例えば、ユーザの指紋、虹彩、静脈、声紋、顔画像などの生体情報を読み取り信号に変換する。なお、生体情報は、これらに限られるも

のではない。
【００２３】
Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ（ＴＰＭ）２２７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手段である。ＴＰＭ２２７は、生体情報センサ２２６で入力した生体情報やＭＦＰ１０１内で生成した秘密鍵を記憶すると共に、記憶している生体情報と入力された生体情報とを検証する機能を有する。なお、携帯端末１０２や、クライアントＰＣ１０４がＴＰＭ２２７を有していてもよい。
【００２４】
近接通信Ｉ／Ｆ２２８は、ＮＦＣやＢｌｕｅＴｏｏｔｈ（登録商標）などの近接通信用の通信方式に対応したネットワークＩ／Ｆであり、携帯端末１０２等と通信し、データのやりとりを行う。例えば、携帯端末１０２等からＭＦＰ１０１に対してプリント指示を行うことも可能である。デバイス制御部２２９は、ＭＦＰ１０１に備えられたプリント部２３０を制御し、電子写真技術やインクジェット技術などの印刷技術を利用して実際の用紙にプリントする。
【００２５】
入出力Ｉ／Ｆ２３１は、ＭＦＰ１０１に備えられた複数の入出力装置２３２を制御する。具体的には、入出力Ｉ／Ｆ２３１は、ボタンやタッチパネルなどの入出力装置２３２からの入力を受け付け、該入力に対応する信号を各処理部へ伝える。また、入出力Ｉ／Ｆ２３１は、液晶ディスプレイやタッチパネルなどの表示装置（ディスプレイ）への表示を制御する。また、ＭＦＰ１０１は、入出力装置２３２としてスキャナを備えていてもよい。スキャナは、紙原稿や写真を読み取り、電子データに変換する。この場合、入出力Ｉ／Ｆ２３１は、スキャナを制御する。
【００２６】
＜携帯端末のハードウェア構成＞
図４は、携帯端末１０２のハードウェア構成例を示す図である。
携帯端末１０２は、サーバ１０３やクライアントＰＣ１０４を構成する基本的なハードウェアに加え、無線通信機能をさらに備える。内部バス２４１、ＣＰＵ２４２、ＲＡＭ２４３、ＲＯＭ２４４は、図２に示した内部バス２１１、ＣＰＵ２０１、ＲＡＭ２０２、ＲＯＭ２０３と同様の機能を有する。
【００２７】
記憶装置２４５は、ソリッドステートドライブ（ＳＳＤ）やＳＤメモリカードなどの記憶装置であり、記憶装置２１０と同様に各種データを記憶する。ＴＰＭ２４６は、図３に示したＴＰＭ２２７と同様の機能を有する。ネットワークＩ／Ｆ２４７は、ネットワークに接続された他の情報処理装置との通信の制御に加え、無線通信機能を備える。生体情報センサ２４８は、図３に示した生体情報センサ２２６と同様の機能を有する。
【００２８】
タッチパネル２４９は、ディスプレイ機能とポインティング機能の両方を備えた装置であり、ディスプレイに表示されたオブジェクトをユーザが指やタッチペンなどで操作することができる。なお、タッチパネル２４９は、一部ないしは全面が指紋や静脈などの生体情報センサになっているようなタッチパネルでもよく、その場合、タッチパネル２４９に生体情報センサ２４８が備わっている構成となる。近接通信Ｉ／Ｆ２５０は、図３に示した近接通信Ｉ／Ｆ２２８と同様の機能を有する。
【００２９】
＜携帯端末およびクライアントＰＣのソフトウェア構成＞
図５（Ａ）は、携帯端末１０２およびクライアントＰＣ１０４の本発明で利用するソフトウェアの構成の一例を示す図である。
アプリケーション３１１は、サーバ１０３と連携してプリントサービスをユーザに提供するためのアプリケーションである。
【００３０】

具体的には、アプリケーション３１１を利用することにより、サーバ１０３のＭＦＰサービス３４１からサービス、例えば、プリントデータを取得したり、プリントデータをＭＦＰ１０１に送信してプリントしたりする機能が提供される。また、例えば、ユーザがプリントサービスにアクセスするための認証情報をＭＦＰサービス３４１に登録する機能が提供される。また、例えば、アプリケーション３１１を介して、ＭＦＰサービス３４１がユーザを認証し、ユーザが個人のＷｅｂページを閲覧する機能が提供される。

【００３１】

アプリケーション３１１は、表示部（ＵＩ）３１２および通信部３１３から構成される。アプリケーション３１１は、Ｗｅｂブラウザや、携帯端末１０２にインストールされた文書作成や画像閲覧などを行うためのネイティブアプリケーションである。ユーザが表示部３１２を操作し、通信部３１３がサーバ１０３と通信を行うことで上述した各種サービスをユーザに提供する。

【００３２】

＜ＭＦＰのソフトウェア構成＞

図５（Ｂ）は、ＭＦＰ１０１の本発明で利用するソフトウェアの構成の一例を示す図である。

ＭＦＰ１０１は、ＭＦＰアプリケーション３２１およびオーセンティケータ（認証モジュール）３３１から構成される。

【００３３】

ＭＦＰアプリケーション３２１は、ＭＦＰ１０１にインストールされたアプリケーションであり、プリントやスキャン、コピーなどの機能を提供する。ＭＦＰアプリケーション３２１は、機能ごとに分かれて実装されていてもよく、また複数の機能を統合して実装されていてもよい。表示部３２２は、入出力装置２３２であるタッチパネルを介してユーザにユーザインタフェース（ＵＩ）を提供する。

【００３４】

プリント実行部３２３は、プリントデータのプリントを実行する。スキャン実行部３２４は、入出力装置２３２であるスキャナを用いて紙原稿や写真などを読み取り電子データに変換する。コピー実行部３２５は、スキャナを用いて紙原稿や写真などを読み取り、プリント部２３０を用いてコピーした結果を出力する。通信部３２６は、ネットワークＩ／Ｆ２２５を介してネットワークに接続されたサーバ１０３などの他の情報処理装置と通信する。

【００３５】

オーセンティケータ登録制御部３２７は、オーセンティケータ３３１に対して後述するクレデンシャルの作成要求を行う。また、オーセンティケータ登録制御部３２７は、オーセンティケータ３３１をＭＦＰサービス３４１に登録する際に、ＭＦＰサービス３４１に対して送信する各種要求を生成する。

【００３６】

なお、本実施形態では、オーセンティケータ登録制御部３２７は、ＭＦＰアプリケーション３２１に含まれるが、これに限られるものではない。例えば、オーセンティケータ登録制御部３２７を、ＭＦＰアプリケーション３２１とは独立して構成し、ＭＦＰアプリケーション３２１が、独立したオーセンティケータ登録制御部３２７を呼び出すようにしてもよい。

【００３７】

また、オーセンティケータ登録制御部３２７は、ＯＳに標準搭載されていてもよい。このように、オーセンティケータ登録制御部３２７をＭＦＰアプリケーション３２１から独立させることで、ＭＦＰアプリケーション３２１だけでなく、他のアプリケーションがオーセンティケータ登録制御部３２７を呼び出せるような構成にすることができる。

【００３８】

オーセンティケータ認証制御部３２８は、オーセンティケータ３３１に対して認証処理を要求したり、認証時にＭＦＰサービス３４１に対して送信する要求を生成したりする。オ

ーセンティケータ認証制御部３２８が行う具体的な処理に関しては後述する。なお、オーセンティケータ認証制御部３２８に関してもオーセンティケータ登録制御部３２７と同様に、ＭＦＰアプリケーション３２１から独立して構成してもよい。

【００３９】

ショートカット管理部３２９は、生体情報と操作の紐付けを管理する。本実施形態では、予め所定の操作を生体情報と紐付けて登録しておくことで、認証後直ちに操作を実行できる状態にする。登録済みの操作をショートカット操作と呼ぶことにする。ショートカット管理部３２９が行う具体的な処理に関しては後述する。

【００４０】

オーセンティケータ３３１は、生体情報センサ２２６により読み取った生体情報を用いた生体認証のための認証モジュールである。オーセンティケータ登録処理部３３２は、ＭＦＰアプリケーション３２１のオーセンティケータ登録制御部３２７などからクレデンシャルの作成要求を受け付け、ペアの鍵（秘密鍵および公開鍵）の作成やクレデンシャルの作成を行う。

【００４１】

生体認証処理部３３３は、ＭＦＰアプリケーション３２１のオーセンティケータ認証制御部３２８などから生体認証要求を受け付けて、生体情報センサ２２６により読み取った生体情報を用いた生体認証を行う。認証情報格納部３３４は、認証情報などをＴＰＭ２２７に対して格納する。認証情報は、例えば、後述する表Ａや表Ｂに示す情報である。生体情報の入力を受け付けるためのＵＩを、タッチパネル２４９を介してユーザに提供するソフトウェアモジュールである。生体情報要求部３３５は、生体情報の入力を受け付けるためのＵＩを、タッチパネルなどの入出力装置２３２を介してユーザに提供する。

【００４２】

＜ＭＦＰ１０１が管理するテーブルの例＞

【表１】

表Ａ　認証情報管理テーブル

認証情報 ID	サービス ID	ユーザ ID	秘密鍵	生体情報 ID
407c-8841-79d	mfpservice.com	user001	1faea2da-a269-4fa7-812a-509470d9a0cb	d493a744
4c04-428b-a7a2	mfpservice.com	user001	d7ae30c8-3775-4706-8597-aaf681bc30f5	dcc97daa
92b2-498d-bea6	mfpservice.com	user001	36ae5eed-732b-4b05-aa7b-4dddb4be3267	51caacaa
・・・	・・・	・・・	・・・	・・・

【００４３】

表Ａの認証情報管理テーブルは、１つのレコードが１つの認証情報のエントリを示す。表Ａのレコードは、オーセンティケータ３３１をＭＦＰサービス３４１などのサービスに登録する際に作成され、表Ａに追加される。認証情報ＩＤ列には、各認証情報には、各認証情報を一意に識別するためのＩＤを格納する。

【００４４】

サービスＩＤ列には、ＭＦＰサービス３４１など、オーセンティケータの登録対象となるサービスを一意に識別するためのＩＤを格納する。本実施形態では、サービスＩＤとしてサービスのドメイン名を使用する。表Ａでは、サービスＩＤとしてＭＦＰサービス３４１のドメイン名が格納されている。ユーザＩＤ列には、レガシー認証等で使用する、ＭＦＰサービス３４１がユーザを一意に識別するためのＩＤを格納する。なお、本実施形態では、生体認証と区別するために、ユーザＩＤとパスワードの一致を検証する認証をレガシー認証と記載する。

【００４５】
秘密鍵列には、オーセンティケータ登録処理部３３２が作成したペアの鍵のうち、秘密鍵の識別子を格納する。秘密鍵に対応する（ペアとなる）公開鍵は、サービスＩＤ列に示されるサービスに登録される。生体情報ＩＤ列には、生体情報の特徴量に対応するＩＤを格納する。認証情報管理テーブルの各列に対応する情報を格納する手順、および公開鍵をＭＦＰサービス３４１に送信、格納する手順については後述する。
【００４６】
【表２】

表Ｂ　ショートカット管理テーブル

認証情報 ID	サービス ID	生体情報	操作
407c-8841-79d	mfpservice.com	右手親指	{"disp": "ホーム画面へ", "func": null, "param": null }
4c04-428b-a7a2	mfpservice.com	右手人差し指	{"disp": "全てプリント", "func": "print", "param": { "color": "auto", "print_target": "all" } , … }
92b2-498d-bea6	mfpservice.com	右手中指	{"disp": "スキャンして送信", "func": "scan", "param": { "color": "auto", "dist": "user001@xxx.com"}, … }
・・・	・・・	・・・	・・・

【００４７】
表Ｂのショートカット管理テーブルは、生体認証によるショートカット操作の登録と実行を実現するために必要となるテーブルである。１つのレコードが生体情報とそれに紐付けられたショートカット操作の組み合わせを示す。表Ｂのレコードは、生体認証によるショートカット操作を登録する際に作成され、表Ｂに追加される。認証情報ＩＤおよびサービスＩＤの各列は、表Ａの各列と同様である。
【００４８】
生体情報列には、オーセンティケータ３３１の登録処理の際に、ショートカット操作と紐付けて登録する生体情報の種別を示す登録名称を格納する。この登録名称は、ＭＦＰアプリケーション３２１が予め定めたものでもよく、また、ユーザがカスタマイズしたものでもよい。また、表Ｂでは生体情報の登録名称として指紋を用いる場合を例に命名しているが、登録名称はこれに限られるものではない。操作列には、生体情報と紐付けられた操作に関する情報を格納する。ショートカット操作の登録および実行に関する手順については後述する。
【００４９】
＜サーバのソフトウェア構成＞
図５（Ｃ）は、サーバ１０３のソフトウェア構成の一例を示す図である。
ＭＦＰサービス３４１は、プルプリントやスキャン送信などのプリントサービスをＨＴＴＰなどの通信プロトコルを利用して提供するＷｅｂサービスである。ＭＦＰサービス３４１は、ＣＰＵ２０１が、ＲＯＭ２０３に格納されたプログラムをＲＡＭ２０２に読み出して実行することで実現される。
【００５０】
レガシー認証処理部３４２は、通信部３５２が受信したレガシー認証要求に含まれるユーザＩＤとパスワードとが、ユーザ情報格納部３４６に格納されているユーザＩＤとパスワードと一致するかを検証するソフトウェアモジュールである。なお、本実施形態では、生体認証と区別するために、ユーザＩＤとパスワードの一致を検証する認証をレガシー認証

と記載する。
【００５１】
オーセンティケータ情報処理部３４３は、通信部３５２が受信したクレデンシャルを用いて、オーセンティケータ３３１に関する情報を、オーセンティケータ情報格納部３４７に格納するソフトウェアモジュールである。また、オーセンティケータ情報処理部３４３は、通信部３５２が受信した後述するアサーション情報（Ａｓｓｅｒｔｉｏｎ）を検証する。
【００５２】
プリントデータ処理部３４４は、通信部３５２が受信した各種要求に応じた処理を実行するソフトウェアモジュールである。例えば、プリントデータ処理部は、通信部が受信したプリントデータの登録要求に応じてプリントデータ格納部３４８に該プリントデータを登録する。また、例えば、プリントデータ処理部は、通信部が受信したプリントデータの取得要求に応じて、プリントデータ格納部３４８から該プリントデータを取得する。
【００５３】
スキャンデータ処理部３４５は、通信部３５２が受信したスキャンデータを、メールサーバなどを介して外部に送信したり、スキャンデータ格納部３４９に該スキャンデータを登録したりするソフトウェアモジュールである。ユーザ情報格納部３４６は、表Ｃを用いて後述するユーザ情報を、記憶装置２２４や外部のストレージシステム（不図示）に格納するソフトウェアモジュールである。
【００５４】
オーセンティケータ情報格納部３４７は、表Ｅを用いて後述するオーセンティケータ３３１に関する情報（オーセンティケータ情報）を記憶装置２２４や外部のストレージシステムに格納するソフトウェアモジュールである。プリントデータ格納部３４８は、携帯端末１０２やクライアントＰＣ１０４から送信されたプリントデータを記憶装置２２４や外部のストレージシステムに格納するソフトウェアモジュールである。
【００５５】
スキャンデータ格納部３４９は、ＭＦＰ１０１がスキャンし、通信部３５２が受信したスキャンデータを記憶装置２２４や外部のストレージシステムに格納するソフトウェアモジュールである。なお、ＭＦＰ１０１がスキャンしたスキャンデータは、サーバ１０３に格納されてもよく、また、ＭＦＰ１０１に格納されてもよく、その両方に格納されてもよい。
【００５６】
プレゼンテーション部３５０は、通信部３５２が受信したオーセンティケータの登録を行うための画面の取得要求などに応じて、ＨＴＭＬやＣＳＳ、ＪａｖａＳｃｒｉｐｔ（登録商標）などを作成するソフトウェアモジュールである。トークン管理部３５１は、表Ｆを用いて後述するトークンの発行や検証を行うソフトウェアモジュールである。通信部３５２は、ネットワークＩ／Ｆ２２５を介して、ＭＦＰ１０１や携帯端末１０２、クライアントＰＣ１０４などの外部の危機と通信するためのソフトウェアモジュールである。
【００５７】
＜サーバ１０３が管理するテーブルの例＞
【表３】

表Ｃ　ユーザ情報管理テーブル

ユーザ ID	パスワード	メールアドレス
user001	******	user001@xxx.co.jp
user002	******	user002@xxx.co.jp
・・・	・・・	・・・

【００５８】
表Ｃのユーザ情報管理テーブルは、ＭＦＰサービス３４１のユーザ情報格納部３４６が管理するテーブルである。ユーザ情報管理テーブルは、１つのレコードが１つのユーザ情報を示す。ユーザＩＤ列には、ＭＦＰサービス３４１のユーザを一意に識別するためのＩＤを格納する。パスワード列には、ユーザを認証するためのパスワードを格納する。このパ

スワードは、レガシー認証で使用するパスワードである。メールアドレス列には、ユーザのメールアドレスを格納する。なお、ユーザ情報管理テーブルには、メールアドレス以外にもユーザの住所など、ユーザに関する属性情報を格納してもよい。

【００５９】

【表４】

表Ｄ　ａｔｔｅｓｔａｔｉｏｎチャレンジ管理テーブル

attestation チャレンジ	ユーザ ID	有効期限
65C9B063-9C33	user001	2017-05-02T12:00:34Z
7317EFBA-4E63	user002	2017-05-02T12:03:12Z
・・・	・・・	・・・

【００６０】

表Ｄのａｔｔｅｓｔａｔｉｏｎチャレンジ管理テーブルは、ＭＦＰサービス３４１のユーザ情報格納部３４６が管理するテーブルである。ａｔｔｅｓｔａｔｉｏｎチャレンジ管理テーブルは、１つのレコードが１つのａｔｔｅｓｔａｔｉｏｎチャレンジの情報を示す。ａｔｔｅｓｔａｔｉｏｎチャレンジは、チャレンジレスポンス認証を行うための検証用データとして利用するパラメータであり、ユーザごとに発行される。

【００６１】

ａｔｔｅｓｔａｔｉｏｎチャレンジの発行処理については後述する。ａｔｔｅｓｔａｔｉｏｎチャレンジ列には、ａｔｔｅｓｔａｔｉｏｎチャレンジの値を格納する。ユーザＩＤ列にはａｔｔｅｓｔａｔｉｏｎチャレンジを発行したユーザのユーザＩＤを格納する。有効期限列には、ａｔｔｅｓｔａｔｉｏｎチャレンジの有効期限を格納する。

【００６２】

【表５】

表Ｅ　オーセンティケータ情報管理テーブル

認証情報 ID	公開鍵	ユーザ ID
407c-8841-79d	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	user001
4c04-428b-a7a2	8143CA9F-35C9-4333-948F-BFCE66A74310	uesr001
・・・	・・・	・・・

【００６３】

表Ｅのオーセンティケータ情報管理テーブルは、ＭＦＰサービス３４１のオーセンティケータ情報格納部３４７が管理するテーブルである。オーセンティケータ情報管理テーブルは、１つのレコードが１つのオーセンティケータ情報を示す。オーセンティケータ３３１の登録を行うと、オーセンティケータ情報管理テーブルにレコードが追加される。証情情報ＩＤ列には、登録されたオーセンティケータ３３１が認証情報管理テーブル（表Ａ）にて管理する認証情報の認証情報ＩＤ列の値が格納される。

【００６４】

公開鍵列には、オーセンティケータ３３１が作成し、認証情報管理テーブル（表Ａ）にて管理する秘密鍵に対応する（ペアになる）公開鍵を格納する。すなわち、認証情報管理テーブル（表Ａ）とオーセンティケータ情報管理テーブル（表Ｅ）において認証情報ＩＤの値が同一の秘密鍵と公開鍵では、表Ａの秘密鍵で暗号化されたデータは、表Ｅの公開鍵で復号化できるということである。ユーザＩＤ列には、ＭＦＰサービス３４１がユーザを一意に識別するためのＩＤを格納する。

【００６５】

【表６】

表Ｆ　トークン管理テーブル

トークン	ユーザ ID	有効期限
3FD4FA-AA4-56DC-B45F-45BCD65AC45D	user001	2017-05-02T13:14:31Z
EC51DC-36C4-4BC3-54CF-31ECE6CACBF0	user002	2017-05-02T13:31:32Z
・・・	・・・	・・・

【００６６】
表Ｆのトークン管理テーブルは、ＭＦＰサービス３４１のトークン管理部３５１が管理するテーブルである。トークンは、本実施形態において、レガシー認証や生体認証等による各種認証処理が成功した結果、ＭＦＰサービス３４１のトークン管理部３５１が発行する。ＭＦＰアプリケーション３２１は、ＭＦＰサービス３４１を利用する際に、発行されたトークンを付与して要求を送信することで、ＭＦＰサービス３４１が提供するサービスを利用できる。
【００６７】
トークン管理テーブルは、１つのレコードが１つのトークンの情報を示す。トークン列には、トークンを格納する。ユーザＩＤ列には、ＭＦＰサービス３４１のユーザを一意に識別するためのＩＤを格納する。有効期限列には、トークンの有効期限を格納する。ＭＦＰサービス３４１は、ユーザからの要求に付与されたトークンが、トークン管理テーブルのトークン列に存在し、有効期限列の有効期限を過ぎていない場合に、該要求を受け付ける。
【００６８】
＜オーセンティケータ登録処理＞
次に、図６～図８を用いて、デバイスのオーセンティケータ３３１を登録する処理について説明する。
以下、デバイスがＭＦＰ１０１の場合について説明するが、デバイスが携帯端末１０２やクライアントＰＣ１０４であっても同様である。
【００６９】
なお、オーセンティケータ３３１の情報をＭＦＰサービス３４１に登録することを、単にオーセンティケータの登録と呼ぶ。また、本実施形態では、ショートカット操作を登録する際にオーセンティケータの登録が行われる。サービスの利用を開始するための、何らかの操作とは紐付いていない通常のオーセンティケータの登録は既に登録済みか、または本実施形態ではレガシー認証で代用可能であるものとする。
【００７０】
図６は、ＭＦＰサービス３４１にオーセンティケータ３３１を登録するまでの処理シーケンスを示す図である。また、図７は、オーセンティケータ３３１の登録処理において、ＭＦＰ１０１とサーバ１０３との通信に含まれるパラメータの一例を示す図である。また、図８は、オーセンティケータ３３１の登録処理において、ＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩ（ユーザインタフェース）の一例を示す図である。
【００７１】
まず、図６のステップＳ４１１において、ＭＦＰ１０１のユーザ４０１が、ＭＦＰアプリケーション３２１からサーバ１０３のＭＦＰサービス３４１に対して、ショートカット操作の登録を要求する。図８（Ａ）～図８（Ｅ）は、ステップＳ４１１にてショートカット操作の登録要求がなされるまでのＵＩの一例を示す図である。
【００７２】
図８（Ａ）の画面６１１は、認証画面である。ボタン６１２は、指紋などの生体情報の読み取りを行うためのボタンであり、生体情報センサ２２６を備える。ユーザ４０１は、ボタン６１２に指紋を押し当てることで認証が行われる。なお、画面６１１では、認証方法として指紋認証を用いる場合を例に説明したが、オーセンティケータ３３１の登録に用いる認証方法は指紋認証に限定されない。

【００７３】
例えば、指紋の登録が１つもなされていない場合は、レガシー認証で認証することも可能である。また、例えば、サービスの利用開示時に、ＭＦＰサービス３４１に対して、何らかの操作とは紐付いていない生体情報を用いて、オーセンティケータの登録を実行し、該生体情報を用いた生体認証で認証することも可能である。
【００７４】
図８（Ｂ）の画面６２１は、ＭＦＰ１０１の機能を選択する画面である。ボタン６２２を押下すると、コピーを実行するための設定画面に遷移する。ボタン６２３を押下すると、プリントを実行するための設定画面に遷移する。ボタン６２４を押下すると、スキャンを実行するための設定画面に遷移する。ここでは、ボタン６２３が押下された場合について説明する。
【００７５】
図８（Ｃ）の画面６３１は、ボタン６２３が押下された場合に表示されるプリントを実行するための設定画面である。選択欄６３２には、図８（Ａ）の画面６１１にて認証されたユーザ４０１がプリント可能なリントデータの一覧が表示される。プリントデータの一覧は、ＭＦＰサービス３４１のプリントデータ格納部３４８から取得される。ユーザ４０１は、プリントしたいプリントデータを選択欄６３２のチェックボックスで選択する。
【００７６】
ボタン６３３を押下すると、プリントに関する詳細な設定を行う設定画面に遷移し、枚数や濃さなどのパラメータを設定することができる。ボタン６３４を押下すると、プリントが実行される。図８（Ｄ）の画面６４１は、ショートカット操作の登録要求を行うかをユーザに問合わせるための画面である。ボタン６３４が押下され、プリントが実行されると、画面６４１に遷移する。
【００７７】
なお、図８（Ｄ）に示す例では、画面６４１において、ショートカット操作の登録要求を行うかを問合わせるための表示とともに、プリントが実行中であることが示される。ここでは、画面６２１や画面６３１で選択された操作や、ボタン６３３が押下されることにより表示される印刷設定（不図示）などのパラメータが記憶されている。
【００７８】
これら操作およびパラメータを今後も利用するために、ショートカット操作として生体情報と紐付けて登録する場合、ボタン６４２を押下する。また、これら操作およびパラメータをショートカット操作として登録しない場合、ボタン６４３を押下する。ボタン６４２を押下すると、これら操作およびパラメータを引き継ぎながら図８（Ｅ）に示す画面６５１が表示される。一方、ボタン６４３を押下すると、ショートカット操作の登録を行わずに、処理を終了し、ホーム画面等の他の画面に遷移する。
【００７９】
図８（Ｅ）の画面６５１は、ショートカット操作の登録を行うための画面である。画面６５１では、画面６２１および画面６３１から引き継がれた操作およびパラメータと紐付けて登録する生体情報の種別を選択する。一覧６５２には、現在登録されているショートカット操作と該ショートカット操作に紐付けられている生体情報との組み合わせが表示される。また、一覧６５２において、これからショートカット操作として登録する操作およびパラメータと紐付ける指紋情報を選択する。
【００８０】
操作およびパラメータと紐付けたい指紋情報の種別（行）を選択すると、ショートカット操作の登録要求がサーバ１０３に送信（ステップＳ４１１）されるとともに、図８（Ｆ）の画面６６１に遷移する。図６（Ｅ）に示す例では、ショートカット操作が未登録の「右手人差指」の行が選択されたものとする。
【００８１】
なお、上述した図８（Ａ）～図８（Ｅ）は、ショートカット操作の登録要求を行うためのＵＩの一例であり、ショートカット操作を行うまでの手順およびＵＩは、これに限られる

ものではない。例えば、本実施形態では、実際にプリントを行う操作を行った後に、該操作とパラメータを引き継ぐことによりショートカット操作の登録要求を行った。しかし、このように、コピーや、プリント、スキャンなどの実際の操作を行わずに、ユーザがショートカット操作の登録を予め行うように操作とパラメータを設定させてもよい。

【００８２】

図６の説明に戻る。ステップＳ４１２では、ＭＦＰアプリケーション３２１のオーセンティケータ登録制御部３２７が、ＭＦＰサービス３４１に対して、オーセンティケータ３３１の登録を要求する。本実施形態では、ショートカット操作の登録に伴い、ＭＦＰサービス３４１へのオーセンティケータ３３１の登録が必要となる。ステップＳ４１３では、ＭＦＰサービス３４１のオーセンティケータ情報処理部３４３が、登録パラメータを作成する。登録パラメータは、サーバ１０３がオーセンティケータ３３１の登録処理を実行する際に使用するデータである。

【００８３】

ＭＦＰアプリケーション３２１を介してオーセンティケータ３３１が該登録パラメータを受け取り、登録パラメータに含まれるデータを用いてクレデンシャルを作成する。そして、サーバ１０３は、ＭＦＰアプリケーション３２１を介してクレデンシャルを受け取り、該クレデンシャルに基づき、ＭＦＰアプリケーション３２１からの登録要求が不正な要求でないことを検証する。以下、登録パラメータについて説明する。

【００８４】

図７（Ａ）は、登録パラメータの一例を示す図である。登録パラメータ５１０は、アカウント情報５１１、暗号化パラメータ５１２、ａｔｔｅｓｔａｔｉｏｎチャレンジ５１３から構成される。アカウント情報５１１には、ＭＦＰサービス３４１における、図８（Ａ）の認証において特定したユーザＩＤや、該ユーザＩＤと紐付くメールアドレスなどユーザに関する属性情報が格納される。

【００８５】

暗号化パラメータ５１２には、ＭＦＰサービス３４１がサポートしている暗号化アルゴリズムなど、登録する認証情報に関する属性情報が格納される。ａｔｔｅｓｔａｔｉｏｎチャレンジ５１３には、チャレンジレスポンス認証を行うために利用する検証用データが格納される。検証用データすなわちａｔｔｅｓｔａｔｉｏｎチャレンジ５１３は、ステップＳ４１３にて登録パラメータを作成する際に作成され、ａｔｔｅｓｔａｔｉｏｎチャレンジ管理テーブル（表Ｄ）にユーザＩＤや有効期限などと紐付けて格納される。

【００８６】

なお、図７（Ａ）に示す登録パラメータは一例であり、これに限られるものではない。例えば、図７（Ａ）に示したほかに、登録パラメータ５１０は、拡張領域として、ＭＦＰサービス３４１がオーセンティケータ３３１等の動作を制御するために利用する、ＭＦＰサービス３４１が指定可能な拡張パラメータを格納する領域を有していてもよい。

【００８７】

ステップＳ４１４では、ＭＦＰサービス３４１の通信部４５２が、ステップＳ４１３で作成した登録パラメータ５１０を返却（応答）する。なお、ステップＳ４１４にて返却されるデータには、登録パラメータ５１０の他に、例えば、プレゼンテーション部３５０が作成したオーセンティケータの登録画面や、該登録画面を表示するための各種プログラムやデータ等を含んでいてもよい。

【００８８】

また、ステップＳ４１４にて返却されるデータには、図８（Ａ）の認証において発行されたトークンを含めてもよい。図８（Ｆ）の画面６６１は、登録画面の一例である。ボタン６６２は、指紋などの生体情報の読み取りを行うためのボタンであり、生体情報センサ２２６を備える。

【００８９】

ステップＳ４１５では、ＭＦＰアプリケーション３２１のオーセンティケータ登録制御部３２７が、オーセンティケータ３３１に対して、クレデンシャルの作成要求を行う。作成

要求は、ＭＦＰアプリケーション３２１の表示部３２２が、オーセンティケータの登録画面（図８（Ｆ））を読み込んだ際に実行される。例えば、オーセンティケータ３３１の登録画面を読み込んだ時に発生するｏｎｌｏａｄイベントでステップＳ４１５の処理を実行する。クレデンシャルの作成要求には、登録要求パラメータを含める。以下、登録要求パラメータについて説明する。

【００９０】

図７（Ｂ）は、登録要求パラメータ５２０の一例を示す図である。登録要求パラメータ５２０は、登録パラメータ５１０、サービスＩＤ５２１と、およびＷｅｂＯｒｉｇｉｎ５２２から構成される。登録パラメータ５１０は、ＭＦＰサービス３４１からステップＳ４１４にて受信した登録パラメータ５１０である。

【００９１】

サービスＩＤ５２１は、表Ａや表Ｂで説明した、オーセンティケータの登録対象のサービスを一意に識別するためのＩＤである。ＷｅｂＯｒｉｇｉｎ５２２は、プロトコルとホスト名とポートの組み合わせであり、本実施形態ではＭＦＰサービス３４１のＯｒｉｇｉｎが格納される。

【００９２】

図６の説明に戻る。ステップＳ４１６では、オーセンティケータ３３１の生体情報要求部３３５が、ユーザ４０１に対して、登録するショートカット操作を実行する際に用いる生体情報を要求する。このとき、図８（Ｆ）に示す画面６１１が表示される。なお、画面６１１では、生体情報として指紋を要求しているが、生体情報は、指紋に限られるものではない。例えば、生体情報として、静脈、虹彩、声紋、顔画像などの情報を利用でき、いずれかに限定するものではない。

【００９３】

ここでは、生体情報のいずれか、または任意の複数の生体情報の組み合わせを、生体認証に用いる生体情報として入力するようにＭＦＰ１０１を構成する。画面６１１のボタン６１２は、指紋などの生体情報の読み取りを行うためのボタンであり、生体情報センサ２２６を備える。ユーザ４０１は、ボタン６６２に指紋を押し当てることにより、生体情報センサ２２６を介して生体情報を入力する。

【００９４】

ステップＳ４１８では、オーセンティケータ３３１のオーセンティケータ登録処理部３３２が、読み取った生体情報の特徴量と生体情報を一意に識別するための生体情報ＩＤを作成する。ステップＳ４１９では、オーセンティケータ登録処理部３３２が、秘密鍵および公開鍵のペアを作成する。そしてオーセンティケータ登録処理部３３２は、認証情報格納部３３４を介してＴＰＭ２２７に格納されている認証情報管理テーブル（表Ａ）に、以下の情報を格納する。

【００９５】

すなわち、ステップＳ４１８で作成した生体情報ＩＤと、ステップＳ４１９で作成した鍵ペアのうち秘密鍵と、クレデンシャルの作成要求に含まれる登録要求パラメータ５２０のサービスＩＤおよびユーザＩＤと紐付けて認証情報として格納する。また、格納された認証情報には、各認証情報を一意に識別するためのＩＤが作成され、認証情報管理テーブル（表Ａ）に格納される。ステップＳ４２０では、オーセンティケータ登録処理部３３２が、クレデンシャルを作成する。以下、クレデンシャルについて説明する。

【００９６】

図７（Ｃ）は、クレデンシャルの一例を示す図である。クレデンシャル５３０は、認証情報ＩＤ５３１、アルゴリズム５３２、公開鍵５３３、ａｔｔｅｓｔａｔｉｏｎ５３４、およびオーセンティケータ名５３５から構成される。認証情報ＩＤ５３１は、ステップＳ４１９で認証情報管理テーブル（表Ａ）に格納した認証情報ＩＤであり、公開鍵５３３は、ステップＳ４１９で作成された鍵ペアの公開鍵である。

【００９７】

アルゴリズム５３２には、ステップＳ４１９において鍵ペアを作成する際に利用したアル

ゴリズムを格納する。また、ａｔｔｅｓｔａｔｉｏｎ５３４は、クレデンシャルの作成要求に含まれる登録要求パラメータに含まれるａｔｔｅｓｔａｔｉｏｎチャレンジ５１３をステップＳ４１９にて作成された秘密鍵を用いて暗号化したデータである。オーセンティケータ名５３５は、オーセンティケータ３３１の名称であり、オーセンティケータ３３１が作成する。

【００９８】

ステップＳ４２１では、オーセンティケータ登録処理部３３２が、ＭＦＰアプリケーション３２１に対して、ステップＳ４２０で作成したクレデンシャル５３０を応答する。ステップＳ４２２では、ＭＦＰアプリケーション３２１の通信部３２６が、ＭＦＰサービス３４１に対して、ステップＳ４２１で受信したクレデンシャル５３０を送信する。

【００９９】

ステップＳ４２３では、ＭＦＰサービス３４１のオーセンティケータ情報処理部３４３が、受信したクレデンシャル５３０を用いて、オーセンティケータの登録処理を行う。以下、オーセンティケータ情報処理部３４３が実行するクレデンシャルの登録処理について説明する。

【０１００】

オーセンティケータ情報処理部３４３は、クレデンシャル５３０に含まれるａｔｔｅｓｔａｔｉｏｎ５３４を、同じクレデンシャル５３０に含まれる公開鍵５３３で復号し、不正な登録要求でないことを検証する。さらに、オーセンティケータ情報処理部３４３は、ａｔｔｅｓｔａｔｉｏｎチャレンジ管理テーブル（表Ｄ）において、ａｔｔｅｓｔａｔｉｏｎ５３４を公開鍵５３３で復号した値と同一の値をａｔｔｅｓｔａｔｉｏｎチャレンジ列に持つレコードを特定する。

【０１０１】

そして、オーセンティケータ情報処理部３４３は、特定したレコードのユーザＩＤをクレデンシャル５３０と紐付けるユーザＩＤとする。そして、オーセンティケータ情報処理部３４３は、クレデンシャル５３０に含まれる認証情報ＩＤ５３１および公開鍵５３３と、クレデンシャル５３０と紐付けるユーザＩＤとをオーセンティケータ情報管理テーブル（表Ｅ）に格納（登録）する。

【０１０２】

ステップＳ４２４では、オーセンティケータ情報処理部３４３が、通信部３５２を介して、ＭＦＰアプリケーション３２１に対して正常にオーセンティケータ３３１の登録処理が完了した旨を通知する。ステップＳ４２５にて、ＭＦＰアプリケーション３２１の表示部３２２は、ＭＦＰサービス３４１から登録処理が完了した旨の通知を受信すると、ユーザ４０１に登録が完了したことを示す画面を表示する。

【０１０３】

図８（Ｇ）の画面６７１は、登録が完了したことを示す画面の一例である。ボタン６７２を押下すると、ホーム画面である画面６２１に遷移する。ボタン６７３を押下すると、ログアウトする。また、ステップＳ４２５では、ＭＦＰアプリケーション３２１のショートカット管理部３２９が、認証情報ＩＤ、サービスＩＤ、ショートカット操作、および生体情報の登録名称を紐付けてショートカット管理テーブル（表Ｂ）に格納（登録）する。

【０１０４】

＜認証及びショートカット操作の実行＞

図９～図１１を用いて、デバイスが認証および登録済みのショートカット操作を実行する処理について説明する。なお、以下、デバイスがＭＦＰ１０１の場合について説明するが、デバイスが携帯端末１０２やクライアントＰＣ１０４であっても同様である。本実施形態では、ＭＦＰ１０１がＭＦＰサービス３４１を利用する際に、ＭＦＰ１０１にて生体認証を行うと、登録済みのショートカット操作をすぐに実行できる状態になる。

【０１０５】

図９は、登録済みのショートカット操作を実行するまでの処理シーケンスを示す図である。また、図１０は、登録済みのショートカット操作の実行において行われる認証処理で使

用するパラメータの一例を示す図である。また、図１１は、登録済みのショートカット操作の実行において、ＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例を示す図である。

【０１０６】

まず、図９のステップＳ７１１において、ユーザ４０１が、入出力装置２３２であるボタンやタッチパネルなどを介して、ＭＦＰアプリケーション３２１を起動する。ステップＳ７１２では、ＭＦＰアプリケーション３２１のオーセンティケータ認証制御部３２８が、ＭＦＰサービス３４１に対してサービスの利用開始を要求する。

【０１０７】

ステップＳ７１３では、ＭＦＰサービス３４１のオーセンティケータ情報処理部３４３が、認証パラメータを作成する。認証パラメータは、ＭＦＰサービス３４１が該サービスを利用するユーザ４０１の認証を行う際に使用するデータである。以下、認証パラメータについて説明する。

【０１０８】

図１０（Ａ）は、認証パラメータの一例を示す図である。認証パラメータ８１０は、Ａｓｓｅｒｔｉｏｎチャレンジ８１１およびＡｓｓｅｒｔｉｏｎ拡張領域８１２から構成される。Ａｓｓｅｒｔｉｏｎチャレンジ８１１には、チャレンジレスポンス認証を行うために利用する検証用データが格納される。Ａｓｓｅｒｔｉｏｎ拡張領域８１２には、ＭＦＰサービス３４１がオーセンティケータ３３１等の動作を制御するために利用する、ＭＦＰサービス３４１が指定可能な拡張パラメータが格納される。

【０１０９】

図９の説明に戻る。ステップＳ７１４では、ＭＦＰサービス３４１のオーセンティケータ情報処理部３４３が、通信部３５２を介してステップＳ７１３で作成した認証パラメータ８１０をＭＦＰアプリケーション３２１に返却する。ステップＳ７１５では、ＭＦＰアプリケーション３２１のオーセンティケータ認証制御部３２８が、オーセンティケータ３３１の生体認証処理部３３３に対して認証要求パラメータを渡し、認証要求を行う。認証要求には、認証要求パラメータを含める。以下、認証要求パラメータについて説明する。

【０１１０】

図１０（Ｂ）は、認証要求パラメータの一例を示す図である。認証要求パラメータ８２０は、認証パラメータ８１０、サービスＩＤ８２１、およびＷｅｂＯｒｉｇｉｎ８２２から構成される。認証パラメータ８１０は、ＭＦＰサービス３４１からステップＳ７１４にて受信した認証パラメータ８１０である。サービスＩＤ８２１およびＷｅｂＯｒｉｇｉｎ８２２は、図７（Ｂ）の登録要求パラメータのサービスＩＤおよびＷｅｂＯｒｉｇｉｎと同様である。

【０１１１】

図９の説明に戻る。ステップＳ７１６では、オーセンティケータ３３１の生体情報要求部３３５は、ユーザ４０１に対して生体認証の要求を行う。生体認証の要求では、ユーザ４０１に生体情報の入力を求める画面が表示される。

【０１１２】

図１１（Ａ）の画面９１１は、オーセンティケータ３３１が生体認証を行う際にＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例である。画面９１１のボタン９１２は、指紋などの生体情報の読み取りを行うためのボタンであり、生体情報センサ２２６を備える。

【０１１３】

ステップＳ７１７では、ユーザ４０１が、画面９１１（図１１（Ａ））のボタン９１２に指紋を押し当てることにより、生体情報センサ２２６を介して生体情報を入力する。なお、ここでは、ユーザ４０１が生体情報として、「右手人差指」の指紋情報を入力したとして説明を進める。また、画面９１１では、生体情報として指紋を要求しているが、生体情報は、指紋に限られるものではない。例えば、生体情報として、静脈、虹彩、声紋、顔画像などの情報を利用でき、いずれかに限定するものではない。

【０１１４】
ステップＳ７１８では、オーセンティケータ３３１の生体認証処理部３３３が、ユーザ４０１により入力された生体情報を取得する。そして、生体認証処理部３３３は、アサーション情報を作成する。アサーション情報は、ＭＦＰサービス３４１において、サービスの利用開始の要求を行ったユーザ４０１が不正な要求を行っていないことの検証に用いられるデータである。以下、アサーション情報について説明する。
【０１１５】
図１１（Ｃ）は、アサーション情報の一例を示す図である。アサーション情報８３０は、認証情報ＩＤ８３１および署名８３２から構成される。以下、生体認証処理部３３３が、アサーション情報８３０を構成する認証情報ＩＤ８３１および署名８３２を取得し、アサーション情報８３０を作成する手順を説明する。
【０１１６】
ステップＳ７１７において、オーセンティケータ３３１の生体認証処理部３３３が画面９１１（図１１（Ａ））を介して取得した生体情報と、ＴＰＭ２２７に格納された生体情報との照合を行う。照合アルゴリズムは、特徴点抽出法やパターンマッチング法などが用いられるが、本発明では照合アルゴリズムを特に限定するものではない。
【０１１７】
具体的には、生体認証処理部３３３は、取得した生体情報を基に、認証情報格納部３３４が管理する認証情報管理テーブル（表Ａ）からレコードを特定する。取得した生体情報を示す生体情報ＩＤが特定されることから、認証情報管理テーブル（表Ａ）において、該生体情報に対応する認証情報ＩＤ８３１および秘密鍵が特定される。すなわち、オーセンティケータ３３１が生体認証を実行し、認証成功であれば、秘密鍵が取り出される。
【０１１８】
そして、生体認証処理部３３３は、認証パラメータ８１０に含まれるＡｓｓｅｒｔｉｏｎチャレンジ８１１を、特定した秘密鍵を用いて署名８３２（署名データ）を作成する。また、生体認証処理部３３３は、特定した認証情報ＩＤ８３１、作成した署名８３２を含むアサーション情報８３０を作成する。
【０１１９】
ステップＳ７１９では、生体認証処理部３３３が、ステップＳ７１８で作成したアサーション情報８３０を、ＭＦＰアプリケーション３２１に返却する。ステップＳ７２０では、ＭＦＰアプリケーション３２１のオーセンティケータ認証制御部３２８が、通信部３２６を介して受信したアサーション情報８３０をＭＦＰサービス３４１に送信する。
【０１２０】
ステップＳ７２１では、ＭＦＰサービス３４１のオーセンティケータ情報処理部３４３が、受信したアサーション情報８３０の検証を行う。具体的には、オーセンティケータ情報処理部３４３は、アサーション情報８３０に含まれる署名８３２を、アサーション情報８３０に含まれる認証情報ＩＤ８３１で特定できる公開鍵を用いて復号化する。そして、復号化した値が、ステップＳ７１３で作成した認証パラメータ８１０に含まれるＡｓｓｅｒｔｉｏｎチャレンジ８１１と一致するかの検証を行う。
【０１２１】
なお、公開鍵の特定には、オーセンティケータ情報管理テーブル（表Ｅ）を用いる。ステップＳ７２２では、ＭＦＰサービス３４１のトークン管理部３５１が、トークンを発行し、該トークンに関する情報をトークン管理テーブル（表Ｆ）に格納する。ステップＳ７２３では、トークン管理部３５１が、通信部３５２を介してステップＳ７２２で発行したトークンをＭＦＰアプリケーション３２１に返却する。
【０１２２】
ステップＳ７２４では、ＭＦＰアプリケーション３２１のショートカット管理部３２９が、ステップＳ７１７でユーザ４０１により入力された生体情報を基に、該生体情報と紐付く操作を特定する。具体的には、ショートカット管理部３２９は、入力された生体情報を基に、認証情報格納部３３４が管理する認証情報管理テーブル（表Ａ）からレコードを特

定する。
【０１２３】
すなわち、入力された生体情報を示す生体情報ＩＤが表Ａにおいて特定されることから、表Ａにおいて、該生体情報に対応する認証情報ＩＤ８３１が特定される。そして、ショートカット管理部３２９は、認証情報格納部３３４が管理するショートカット管理テーブル（表Ｂ）において、特定された認証情報と紐付く操作を特定する。
【０１２４】
ステップＳ７２５では、ショートカット管理部３２９が、ＭＦＰサービス３４１に対してプリントデータの取得要求を送信する。ステップＳ７２６では、ＭＦＰサービス３４１のプリントデータ処理部３４４が、要求を受けたユーザ４０１に関するプリントデータを、プリントデータ格納部３４８から取得し、ＭＦＰアプリケーション３２１に返却する。このとき、必要があれば、ＭＦＰサービス３４１のプレゼンテーション部３５０から、ＭＦＰアプリケーション３２１の表示部３２２が画面を表示するためのデータを合わせて取得してもよい。
【０１２５】
図１１（Ｂ）の画面９２１は、ステップＳ７２６にてプリントデータが取得された後に、ＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例である。選択欄９２２には、取得されたプリントデータの一覧が表示される。ボタン９２３を押下すると、選択欄９２２のチェックボックスで選択されたプリントデータがプリントされる。画面９２１には、サービスを利用する際の認証時に、図１１（Ａ）の画面９１１において、「右手人差指」の指紋情報を入力したことで、該指紋情報（生体情報）と紐付くショートカット操作として登録された操作やパラメータの内容が表示される。
【０１２６】
上述したように、「右手人差指」には、図８（Ｃ）の画面６２１や画面６３１で選択された操作やパラメータが紐付いている。このため、画面９２１には、プリントに関する設定画面であって、プリントデータの一覧を全て印刷するように、選択欄９２２のチェックボックスにおいて全ての印刷可能なデータが選択された状態の設定画面が表示される。
【０１２７】
ボタン９２４を押下すると、プリントに関する詳細な設定を行う設定画面に遷移し、枚数や濃さなどのパラメータを設定することができる。ボタン９２５を押下すると、プリントは実行されずログアウトする。ここでは、ボタン９２３が押下された場合について説明する。ボタン９２３が押下されると、図９において、処理はステップＳ７２７に進む。
【０１２８】
ステップＳ７２７では、プリントが実行される。具体的には、ＭＦＰアプリケーション３２１のプリント実行部３２３がプリント処理を実行する。そして、図１１（Ｂ）の画面９２１から、図１１（Ｃ）の画面９３１に遷移する。画面９３１は、プリントが実行中であることが示される。そして、図９において、処理はステップＳ７２７に進む。
【０１２９】
なお、本実施形態において、図８や図１１で説明した画面遷移を実現する処理は、ＦＩＤＯのような認証方式を用いないシステムにおいても適用可能である。ＦＩＤＯのような認証方式を用いない場合とは、例えば生体認証を用いる場合であって、Ｗｅｂ上のサービスにユーザの手元にある情報処理装置での生体認証に紐付く情報、例えば、認証識別情報、公開鍵などを予め登録しておくような認証方式でない場合である。このような場合であっても、生体認証を用いるシステムにおいて、上述した画面遷移を実現することにより、サービス利用時の操作性を向上することができる。
【０１３０】
以上のように、本実施形態によれば、Ｗｅｂサービスを利用する際の操作性を向上させることが可能となる。例えば、ショートカット操作と生体情報を関連付けて登録しておくことで、生体認証の後、すぐに目的の操作を実行することができる。また、ショートカット操作を登録する際に、実際に実行した操作の後で登録作業を実行できるため、登録作業の

負荷を軽減できる。
【０１３１】
［第２実施形態］
第１実施形態では、生体認証の際にユーザが入力した生体情報を基に、該生体情報と紐付くショートカット操作が呼び出される場合について説明した。具体的には、図１１（Ａ）の画面９１１においてユーザが入力した生体情報を認証した後に、呼び出されたショートカット操作が図１１（Ｂ）の画面９２１に表示された。しかし、生体情報とショートカット操作の紐付けは複数登録することが可能である。
【０１３２】
例えば、本実施形態では、図８（Ｅ）に示したように、複数の指紋情報に対してそれぞれショートカット操作が紐付いている。このような場合、ユーザは、どの生体情報にどのショートカット操作を紐付けたか忘れてしまう可能性がある。したがって、図１１（Ａ）にて生体情報を入力した後、ユーザが意図したものではない操作が呼び出される可能性がある。このとき、例えば、図１１（Ｂ）において、ボタン９２５を押下する等してログアウトを行い、再度他の生体情報を入力し直して意図するショートカット操作を呼び出すのは不便である。
【０１３３】
そこで、本実施形態では、ユーザが、自身の意図しないショートカット操作と紐付いた生体情報を入力した場合であっても、ユーザに手間をかけることなく意図するショートカット操作を実行することを可能にする。なお、第１実施形態と共通の部分については、その説明を省略し、ここでは第１実施形態との差異のみ説明する。
【０１３４】
図１２は、ＭＦＰ１０１がＭＦＰサービス３４１を利用する際にＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例を示す図である。
図１２（Ａ）の画面１０１１は、図１１（Ａ）の画面９１１と同様に、オーセンティケータ３３１が生体認証を行う際にＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例である。
【０１３５】
また、図１２（Ｂ）の画面１０２１は、図１１（Ｂ）の画面９２１と同様に、生体認証が成功し、ステップＳ７２６にてプリントデータが取得された後に、ＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例である。ボタン１０２２を押下すると、サービスを利用する際の認証時に、図１２（Ａ）の画面１０１１において入力された生体情報と紐付く操作が実行される。図１２（Ｂ）に示す例では、「右手人差指」の指紋情報が入力されたことにより、該指紋情報と紐付く操作として、サーバ１０３から送信されたプリントジョブが全て実行される。
【０１３６】
ボタン１０２３を押下すると、図８の画面６２１のようなホーム画面に遷移する。なお、サービスを利用する際の認証時（画面１０１１）に、トークンを取得しているため、ホーム画面に戻って、他の操作を実行する際に別途認証を行う必要はない。認証時に入力した生体情報と紐付くショートカット操作をキャンセルする場合であっても、ログアウトや再度ログインする必要はなく、他の操作を実行することができる。
【０１３７】
操作一覧１０２４には、ショートカット操作として登録されている操作と、該操作を呼び出すための生体情報の一覧が表示される。操作一覧１０２４は、ショートカット管理テーブル（表Ｂ）を基に表示される。操作一覧１０２４に表示されたショートカット操作を選択することで、サービスを利用する際の認証時に、図１２（Ａ）の画面１０１１において入力された生体情報と紐付くショートカット操作とは異なる他のショートカット操作を実行することができる。
【０１３８】
なお、サービスを利用する際の認証時に、サーバ１０３からトークンを取得しているため

、他のショートカット操作を実行する際に別途認証を行う必要はない。スクロールバー１０２５を操作することで、ショートカット操作として登録されている操作を探索することができる。

【０１３９】

このように、本実施形態によれば、ユーザが、自身の意図しないショートカット操作と紐付いた生体情報を入力した場合であっても、ユーザに手間をかけることなく意図するショートカット操作を実行することが可能となる。

【０１４０】

［第３実施形態］

第１実施形態では、生体情報とショートカット操作とを紐付ける場合について説明した。しかし、入力する生体情報を間違えて登録してしまい、ショートカット操作を誤った生体情報と紐付けてしまう場合がある。例えば、図８（Ｅ）および図８（Ｆ）で示した画面において、未登録の「右手人差指」にショートカット操作を紐付ける際に、誤って実際には「右手中指」を登録してしまう場合がある。

【０１４１】

このように、既に他のショートカット操作と紐付けて登録されている「右手中指」の生体情報に対して、２つのショートカット操作が紐付けられてしまうことがある。そこで、本実施形態では、既に登録されている生体情報を二重に登録しようとした場合に、その旨をユーザに通知し、ユーザが誤ってショートカット操作を登録することを抑制する。なお、第１実施形態と共通の部分については、その説明を省略し、ここでは第１実施形態との差異のみ説明する。

【０１４２】

図１３は、本実施形態において、オーセンティケータ３３１の登録処理において、ＭＦＰアプリケーション３２１の表示部３２２が表示するＵＩの一例を示す図である。

図１３（Ａ）の画面１１１１は、図８（Ｅ）の画面６５１と同様に、ショートカット操作の登録を行うための画面である。一覧１１１２には、一覧６５２と同様に、現在登録されているショートカット操作と該ショートカット操作に紐付けられている生体情報との組み合わせが表示される。

【０１４３】

一覧１１１２の中から、ショートカット操作と紐付けたい指紋情報の種別（行）を選択すると、ショートカット操作の登録要求がサーバ１０３に送信（ステップＳ４１１）されるとともに、図１３（Ｂ）の画面１１２１に遷移する。画面１１２１は、ショートカット操作を登録する画面である。ボタン１１２２は、指紋などの生体情報の読み取りを行うためのボタンであり、生体情報センサ２２６を備える。

【０１４４】

図１３（Ｃ）の画面１１３１は、生体情報と該生体情報に紐付くショートカット操作の登録が正常に完了したことを示す画面の一例である。ボタン１１３２を押下すると、ホーム画面である画面６２１に遷移する。ボタン１１３３を押下すると、ログアウトする。一方、画面１１２１（図１３（Ｂ））において入力された生体情報が既に他のショートカット操作と紐付けて登録されている場合、図１３（Ｄ）の画面１１４１が表示され、ユーザにその旨通知する。

【０１４５】

画面１１４１は、画面１１２１において、既に他のショートカット操作と紐付けて登録されている生体情報が検出された場合に表示される。ボタン１１４２を押下すると、画面１１１１（図１３（Ａ））に遷移し、ショートカット操作の登録をやり直す。ボタン１１４３を押下すると、既に他のショートカット操作と紐付けて登録されている生体情報を、これから登録しようとしているショートカット操作と新たに紐付けて登録を上書きする。

【０１４６】

例えば、図１３（Ａ）の画面１１１１において、一覧１１１２から「右手人差指」を選択したにも関わらず、図１３（Ｂ）の画面１１２１において「右手中指」の指紋情報を入力

したとする。この場合、画面１１１１に示すように、「右手中指」は、既に他のショートカット操作と紐付けて登録されているため、画面１１４１が表示される。ここで、ボタン１１４３を登録すると、これから登録しようとしているショートカット操作は、既に登録されている「右手中指」に紐付く操作として登録が上書きされる。

【０１４７】

図１４は、本実施形態において、ＭＦＰ１０１が実行する、生体情報とショートカット操作とを紐付ける処理を説明するためのフローチャートである。

なお、図１４の処理は、本実施形態において、第１実施形態のステップＳ４１６～Ｓ４１８に対応する処理として実行される。

【０１４８】

ステップＳ１２１１では、オーセンティケータ３３１の生体情報要求部３３５が、ユーザに対して、登録するショートカット操作を実行する際に用いる生体情報を要求する。このとき、図１３（Ａ）に示す画面１１２１が表示される。なお、第１実施形態と同様に、画面１１２１では、生体情報として指紋を要求しているが、生体情報は、指紋に限られるものではない。例えば、生体情報として、静脈、虹彩、声紋、顔画像などの情報を利用でき、いずれかに限定するものではない。

【０１４９】

ステップＳ１２１２では、生体情報要求部３３５が、生体情報センサ２２６を介してユーザから指紋情報を取得する。ステップＳ１２１３では、生体認証処理部３３３が、取得した生体情報報と、ＴＰＭ２２７に格納された生体情報との照合を行う。ステップＳ１２１４では、生体認証処理部３３３が、ＴＰＭ２２７に格納された登録済みの生体情報の特徴量のうち、取得した生体情報の特徴量と一致するものが存在するか判断する。

【０１５０】

具体的には、認証情報管理テーブル（表Ａ）において、取得した生体情報の特徴量と一致するレコードが、生体情報ＩＤ列に存在するか確認する。取得した生体情報の特徴量と一致する生体情報が存在する場合、処理はステップＳ１２１５に進み、取得した生体情報の特徴量と一致する生体情報が存在しない場合、処理はステップＳ１２１６に進む。

【０１５１】

ステップＳ１２１５では、取得した生体情報を示す生体情報ＩＤが特定されることから、認証情報管理テーブル（表Ａ）において、該生体情報に対応する認証情報ＩＤ８３１が特定される。そして、ＭＦＰアプリケーション３２１のショートカット管理部３２９が、特定した認証情報ＩＤを用いてショートカット管理テーブル（表Ｂ）から取得した生体情報に対応するレコードを特定する。

【０１５２】

このとき、図１３（Ｄ）に示す画面１１４１が表示される。生体情報と紐付くショートカット操作を上書きして登録する場合、ユーザは、ボタン１１４３を押下し、処理はステップＳ１２１６に進む。一方、ショートカット操作の登録をやり直す場合、ユーザは、ボタン１１４２を押下し、処理はステップＳ１２１１に戻る。すなわち、生体情報の入力からやり直す。

【０１５３】

ステップＳ１２１６では、オーセンティケータ３３１のオーセンティケータ登録処理部３３２が、取得した生体情報の登録を行う。この処理は、図６に示すステップＳ４１８と同様である。以降の処理は、第１実施形態の場合と同様であり、ステップＳ４２５において、ＭＦＰアプリケーション３２１のショートカット管理部３２９が、生体情報とショートカット操作の組み合わせをショートカット管理テーブル（表Ｂ）に格納（登録）する。

【０１５４】

なお、上述した生体情報と紐付くショートカット操作を上書きして登録する場合、オーセンティケータ３３１はサーバ１０３において登録済みのため、ステップＳ４１９以降の処理は行われない。

【０１５５】

［第４実施形態］
第１実施形態では、ＭＦＰアプリケーション３２１のショートカット管理部３２９がショートカット管理テーブル（表Ｂ）を有し、生体情報とショートカット操作を紐付けて管理する。しかし、これらのデータは必ずしもＭＦＰアプリケーション３２１が管理する必要はない。そこで、本実施形態では、ＭＦＰサービス３４１が、生体情報とショートカット操作を紐付けて管理する場合について説明する。なお、第１実施形態やその他の実施形態と共通の部分については、その説明を省略し、ここでは差異のみ説明する。
【０１５６】
＜ソフトウェア構成の差異＞
本実施形態では、第１実施形態で説明したショートカット管理テーブル（表Ｂ）がＭＦＰアプリケーション３２１上に存在せず、後述する表Ｇおよび表ＨがＭＦＰサービス３４１上に存在する。
【０１５７】
＜オーセンティケータ登録処理の差異＞
本実施形態では、オーセンティケータ３３１をＭＦＰサービス３４１に登録する処理（図６）において、以下の点が第１実施形態と異なる。ステップＳ４２２では、ＭＦＰアプリケーション３２１の通信部３２６が、クレデンシャルを返却する際に、表Ｈを用いて後述する生体情報とショートカット操作の紐付け情報をクレデンシャルに付与して送信する。また、ステップＳ４２５は、実行されない。すなわち、ＭＦＰアプリケーション３２１においてショートカット操作の登録が行われない。
【０１５８】
＜認証時の差異＞
本実施形態では、登録済みのショートカット操作を実行するまでの処理（図９）において、以下の点が第１実施形態と異なる。ステップＳ７２４にて、ＭＦＰアプリケーション３２１がショートカット操作の特定は行わない。そして、ステップＳ７２４にて、登録されたショートカット操作を実行するにために必要となるデータの要求も行わない。
【０１５９】
本実施形態では、ステップＳ７２２の実行時、または実行後にＭＦＰサービス３４１のオーセンティケータ情報処理部３４３が、後述する表Ｇおよび表Ｈを用いてショートカット操作を特定し、ＭＦＰアプリケーション３２１に必要なデータを返却する。必要なデータは、例えば、ＭＦＰ１０１の表示部３２２が表示する表示画面のデータや、プリントデータ、操作実行スクリプトなどである。以下、本実施形態において、サーバ１０３が管理するテーブルについて説明する。
【０１６０】
【表７】

表Ｇ　オーセンティケータ情報・生体情報管理テーブル

認証情報 ID	ユーザ ID	公開鍵	端末種別	生体情報
407c-8841-79d	user001	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	printer	右手親指
4c04-428b-a7a2	user001	8143CA9F-35C9-4333-948F-BFCE66A74310	printer	右手人差指
92b2-498d-bea6	user001	4EA2107F-4027-41D0-B779-A8A30F845266	printer	右手中指
646b-3cb6-8704	user001	46E80B62-A72D-47C9-BC2A-B052DCAF53FE	tablet	右手親指
fe35-2cc5-92a1	user001	87DE5A4D-9784-4C15-A2FE-D00A51FA1860	tablet	右手人差指
89ae-4f85-a3c1	user001	9C5B5B95-1B7F-4B7E-B199-489B1BE8B267	tablet	右手中指
・・・	・・・	・・・	・・・	・・・

【０１６１】
表Ｇのオーセンティケータ情報および生体情報管理テーブルは、ＭＦＰサービス３４１が管理するテーブルである。表Ｇは、第１実施形態のオーセンティケータ情報管理テーブル（表Ｅ）を拡張したテーブルである。認証情報ＩＤ列、ユーザＩＤ列、および公開鍵列は、表Ｅと同様である。端末種別列には、ユーザがオーセンティケータ３３１をＭＦＰサービス３４１に登録した時に使用したデバイスの種別が格納される。端末種別は、デバイス

から送信されるＵｓｅｒＡｇｅｎｔ等から取得可能である。生体情報列は、表Ｂの生体情報列と同様である。

【０１６２】

【表８】

表Ｈ　ショートカット操作紐付けテーブル

生体情報	操作
右手親指	locate_home
右手人差指	device_type == ″printer″ ? print_all_jobs : get_all_print_jobs
右手中指	device_type == ″printer″ ? scan_and_send : take_picture_and_send
・・・	・・・

【０１６３】

表Ｈのショートカット操作紐付けテーブルは、ＭＦＰサービス３４１が管理するテーブルである。表Ｈは、第１実施形態において、ＭＦＰアプリケーション３２１が管理するショートカット管理テーブル（表Ｂ）に相当するテーブルである。生体情報列は、表Ｇと表Ｈを関連付けるための外部キーである。

【０１６４】

操作列には、生体情報と紐付けられた操作を実行するための命令が格納されている。ＭＦＰアプリケーション３２１からの要求に応じて、オーセンティケータ情報処理部３４３がステップＳ７２２の実行時や実行後にこれらの命令を実行する。これにより、オーセンティケータ情報処理部３４３が、表示画面のデータや、プリントデータ、操作実行スクリプトなど該要求に応じたデータをプリントデータ格納部３４８やプレゼンテーション部３５０等から取得する。取得したデータは、ＭＦＰアプリケーション３２１に返却される。

【０１６５】

このように、本実施形態によれば、第１実施形態と同様に、ショートカット操作の登録および実行を実現することができる。以下では、本実施形態の応用例として、表Ｇおよび表ＨのようなテーブルをＭＦＰサービス３４１側が有することで実現可能な機能について説明する。

【０１６６】

＜ショートカット操作の引き継ぎ＞

上述したように、本実施形態では、ＭＦＰサービス３４１が、生体情報とショートカット操作の紐付け情報を管理する。このため、同じユーザＩＤを使用することにより、ショートカット操作の登録を要求したデバイスとは異なるデバイスへ、紐付け情報を引き継ぎ、該異なるデバイスにおいても同様のショートカット操作を行うことが可能となる。

【０１６７】

オーセンティケータ情報および生体情報管理テーブル（表Ｇ）の１～３行目は、ＭＦＰ１０１において、オーセンティケータの登録処理を行った場合に格納されたオーセンティケータ情報である。また、４～６行目は、スマートフォンやタブレットなどの携帯端末１０２において、オーセンティケータの登録処理を行った場合に格納されたオーセンティケータ情報である。

【０１６８】

ここで、例えば、最初にＭＦＰ１０１において、「右手親指」、「右手人差指」、「右手中指」の３つの生体情報にそれぞれショートカット操作を登録している状態であるとする。そして、携帯端末１０２において、同一のユーザＩＤを使用して上述した３つの生体情報にそれぞれ同じショートカット操作を登録する場合について考える。このとき、ＭＦＰサービス３４１は、表Ｇおよび表Ｈのテーブルを有するため、登録済みの生体情報とショートカット操作の紐付けを携帯端末１０２に知らせることが可能である。

【０１６９】

例えば、携帯端末１０２において、ユーザがショートカット操作を登録する際に、ユーザに対して、ＭＦＰ１０１にて既に登録済みの生体情報とショートカット操作の紐付けの、

引き継ぎを行うようにリコメンド等行うことができる。これにより、ユーザは、ＭＦＰ１０１にて使用していた生体情報とショートカット操作の紐付けを他のデバイスにおいても引き継ぐことが可能となる。ただし、紐付け情報の引き継ぎは可能であるが、引継ぎ先のデバイスにおいて、オーセンティケータの登録処理は、デバイスごとに別途必要である。

【０１７０】

＜デバイスごとに異なる操作＞

上述したように、本実施形態では、ユーザが生体情報とショートカット操作の紐付けを、登録したデバイスとは異なる他のデバイスに引き継ぐことができる。しかし、デバイスごとに有する機能は異なるため、引き継ぎ先のデバイスにおいて実行できない操作もある。

【０１７１】

例えば、ＭＦＰサービス３４１により提供されるＭＦＰ１０１はプリント機能を備えているが、携帯端末１０２はプリント機能を備えていない。また、ＭＦＰ１０１はスキャン機能を備えているが、携帯端末１０２はスキャン機能を備えていないが、カメラ機能を有するため、画像の入力手段は備えている。すなわち、同じサービスを利用する場合であっても、デバイスの種別に応じて実行できる操作が異なる。

【０１７２】

そこで、このような場合には、引き継いだ操作を引き継ぎ先のデバイスに対応するように、ＭＦＰサービス３４１が管理するショートカット操作紐付けテーブル（表Ｈ）に格納する値を制御する。ここでは、ショートカット操作紐付けテーブル（表Ｈ）の２行目の操作を例に説明する。

【０１７３】

ショートカット操作紐付けテーブル（表Ｈ）の２行目は、生体情報として「右手人差指」を用いて認証が行われた場合に、プリントに関するショートカット操作が実行されることを示す。具体的には、ＭＦＰサービス３４１は、端末種別が“ｐｒｉｎｔｅｒ”であれば、“ｐｒｉｎｔ＿ａｌｌ＿ｊｏｂｓ”を実行し、端末種別が“ｐｒｉｎｔｅｒ”以外であれば、“ｇｅｔ＿ａｌｌ＿ｐｒｉｎｔ＿ｊｏｂｓ”を実行する。

【０１７４】

ＭＦＰサービス３４１が、“ｐｒｉｎｔ＿ａｌｌ＿ｊｏｂｓ”を実行すると、デバイスに対してプリントデータおよびデバイスにプリント処理を実行させるために必要なデータを返却する。ＭＦＰサービス３４１が、“ｇｅｔ＿ａｌｌ＿ｐｒｉｎｔ＿ｊｏｂｓ”を実行すると、デバイスに対してプリントジョブの一覧のみを返却する。

【０１７５】

これにより、プリント機能を備えた端末種別が“ｐｒｉｎｔｅｒ”のデバイスにおいて、「右手人差指」を用いて認証が行われると、プリントを実行することができる。一方、プリント機能を備えていない端末種別が“ｔａｂｌｅｔ”のデバイスにおいて、「右手人差指」を用いて認証が行われると、プリントを実行することができないため、プリントデータ格納部３４８に格納されたプリントジョブの一覧を取得することができる。

【０１７６】

このように、デバイスの端末種別に応じて、ＭＦＰサービス３４１が実行する命令を制御することで、端末種別に備わった機能に応じたサービスを提供することができる。なお、他の実施形態と同様に、本実施形態においても、生体情報は、指紋に限られるものではなく、静脈、虹彩、声紋、顔画像などの情報を利用でき、いずれかに限定するものではない。

【０１７７】

［第５実施形態］

第１実施形態～第４実施形態では、ショートカット操作の登録や実行を行うデバイスがＭＦＰ１０１である場合について説明したが、これに限られるものではない。本実施形態では、その他のデバイスの例として、スマートフォンやタブレットなどの携帯端末１０２においてショートカット操作を実行する場合について説明する。

【０１７８】

なお、本実施形態では、本実施形態に係る携帯端末１０２のハードウェア構成は、図４に

示した第１実施形態における携帯端末１０２のハードウェア構成と同様である。また、携帯端末１０２のソフトウェア構成は、図５（Ａ）に示した第１実施形態における携帯端末１０２のソフトウェア構成に、以下の構成を加えたものである。

【０１７９】

すなわち、本実施形態に係る携帯端末１０２は、図５（Ｂ）のＭＦＰ１０１が有するオーセンティケータ登録制御部３２７、オーセンティケータ認証制御部３２８、ショートカット管理部３２９、およびオーセンティケータ３３１をさらに有する。第１実施形態において説明した、オーセンティケータの登録処理や、認証処理のシーケンス図、各種パラメータの構成、各装置が有する各種テーブル等は、第１実施形態と同様であるため、その説明を省略する。

【０１８０】

図１５は、携帯端末１０２において登録済みのショートカット操作の実行する際に、携帯端末１０２の表示部３１２が表示するＵＩの一例を示す図である。

本実施形態では、携帯端末１０２のアプリケーション３１１が、第１実施形態におけるＭＦＰアプリケーション３２１に対応する、Ｗｅｂサービスを利用するアプリケーションとする。

【０１８１】

また、本実施形態では、アプリケーション３１１は、Ｗｅｂサービスとして通信販売サービスを提供する「買い物アプリ」である場合を例に説明する。「買い物アプリ」では、頻繁に購入する商品をショートカット操作として登録することができる。本実施形態では、既にショートカット操作の登録と、それに伴うサービスへのオーセンティケータの登録は済んでいるものとする。

【０１８２】

なお、本実施形態は、インターネット上の通信販売サービスにおける商品の購入に限らず、任意の電子商取引システムにおける取引内容に適用できる。例えば、インターネットバンキングにおいて、残高や明細の照会や、所定の相手への振り込みの実行など、各種サービスの利用においても、ショートカット操作として登録し、実行することができる。

【０１８３】

図１５（Ａ）は、アプリケーション３１１を起動した際のＵＩを示す図である。ボタン１３０１は、指紋などの生体情報の読み取りを行うためのボタンであり、生体情報センサ２４８を備える。なお、本実施形態においても、生体情報として指紋を利用する場合について説明するが、これに限られるものではなく、生体情報として、例えば、静脈、虹彩、声紋、顔画像などの情報を利用できる。

【０１８４】

ダイアログ１３１１は、アプリケーション３１１を起動した際に表示される。アプリケーション３１１は、ダイアログ１３１１を表示する間、ユーザからの生体情報の入力を受け付ける。そして、アプリケーション３１１は、予め登録しているショートカット操作と紐付けられた生体情報が入力されると、図１５（Ｂ）に示す画面に遷移する。

【０１８５】

ボタン１３１２を押下すると、生体情報の入力を待たずにダイアログ１３１１を閉じる。つまり、ユーザがショートカット操作を利用しない場合、ボタン１３１２を押下することにより、ホーム画面などの表示が行われる。ダイアログ１３１１が閉じられた場合であっても、再度アプリケーション３１１を起動すると、ダイアログ１３１１が表示され、アプリケーション３１１は、生体情報の受け付けを行う。

【０１８６】

ボタン１３１３を押下すると、生体情報の入力を待たずにダイアログ１３１１を閉じ、再度アプリケーション３１１を起動してもダイアログ１３１１が表示されないようになる。なお、ボタン１３１３を押下した場合であっても、アプリケーション３１１の設定（不図示）において、再度ダイアログ１３１１を表示させるように変更することも可能である。

【０１８７】

図１５（Ｂ）は、図１５（Ａ）の画面においてショートカット操作と紐付けられた生体情報が入力されると表示される画面である。ここでは、一例として既にショートカット操作の登録がなされた「右手人差指」の指紋情報が入力され、該指紋情報と紐付けられた操作が表示された場合について説明する。「右下人差指」には、「〇〇洗剤（１ケース）の購入」が紐付けられている。

【０１８８】

そこで、ボタン１３２１を押下すると、「〇〇洗剤（１ケース）の購入」が実行される。また、ボタン１３２２を押下すると、ショートカット操作を実行することなく、ホーム画面の表示が行われる。一覧１３２３には、現在登録されているショートカット操作とショートカット操作に紐付けられている生体情報との組み合わせが表示される。一覧１３２３にある行を押下すると、他のショートカット操作を呼び出すことができる。

【０１８９】

図１５（Ｃ）は、図１５（Ｂ）の画面において、ボタン１３２１を押下した後に表示される画面である。ボタン１３２１を押下したことにより、アプリケーション３１１は、購入処理に進み、図１５（Ｃ）の画面において該処理が完了した旨を通知する。

【０１９０】

このように、本実施形態によれば、第１実施形態～第３実施形態とは異なるデバイスにおいても、ショートカット操作を利用することができる。また、上述したような認証方式に対応するアプリケーションであれば、ＭＦＰアプリケーション３２１や、アプリケーション３１１に限らず、本発明は適用可能である。

【０１９１】

［その他の実施形態］

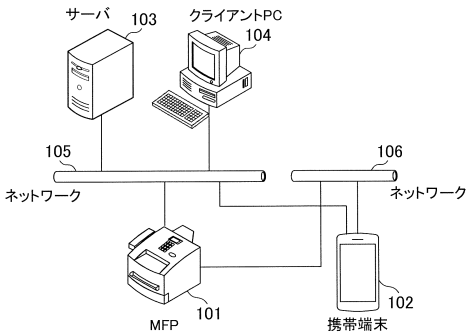
本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能である。

【０１９２】

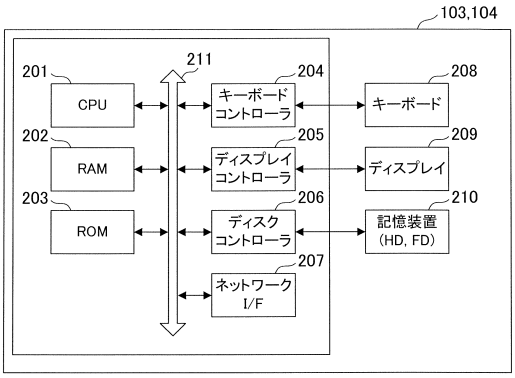
以上、本発明の好ましい実施形態について説明したが、本発明は、これらの実施形態に限定されず、その要旨の範囲内で種々の変形および変更が可能である。

【図面】

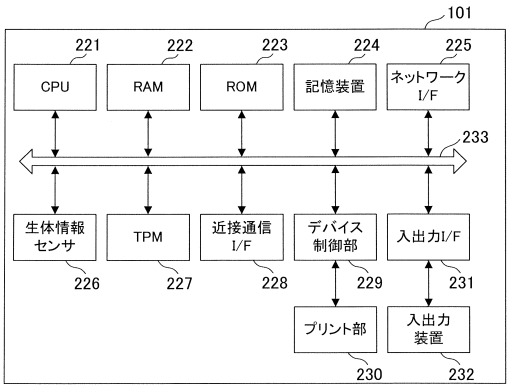
【図１】


サーバ
103
クライアントPC
104
105
106
ネットワーク
ネットワーク
MFP
101
携帯端末
102

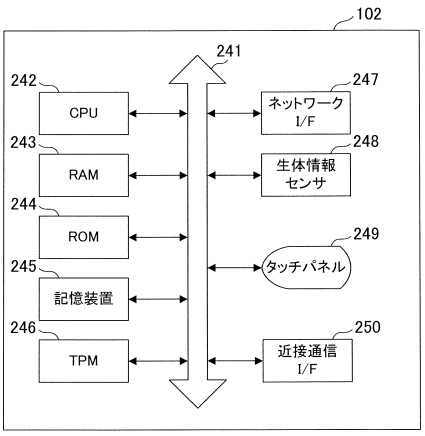
【図２】


103,104
211
201
CPU
202
RAM
203
ROM
204
キーボード
コントローラ
205
ディスプレイ
コントローラ
206
ディスク
コントローラ
207
ネットワーク
I/F
208
キーボード
209
ディスプレイ
210
記憶装置
(HD, FD)

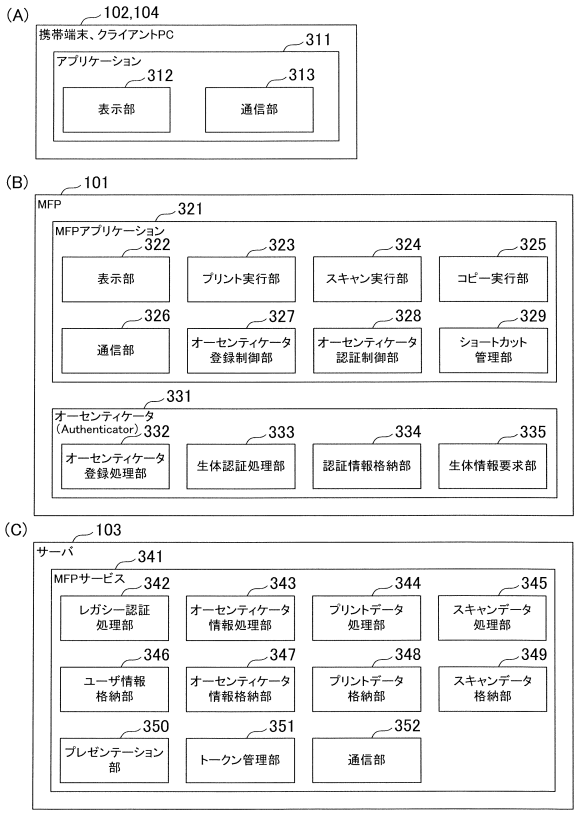
【図３】


101
221
222
223
224
225
CPU
RAM
ROM
記憶装置
ネットワーク
I/F
233
生体情報
センサ
TPM
近接通信
I/F
デバイス
制御部
入出力I/F
226
227
228
229
231
プリント部
入出力
装置
230
232

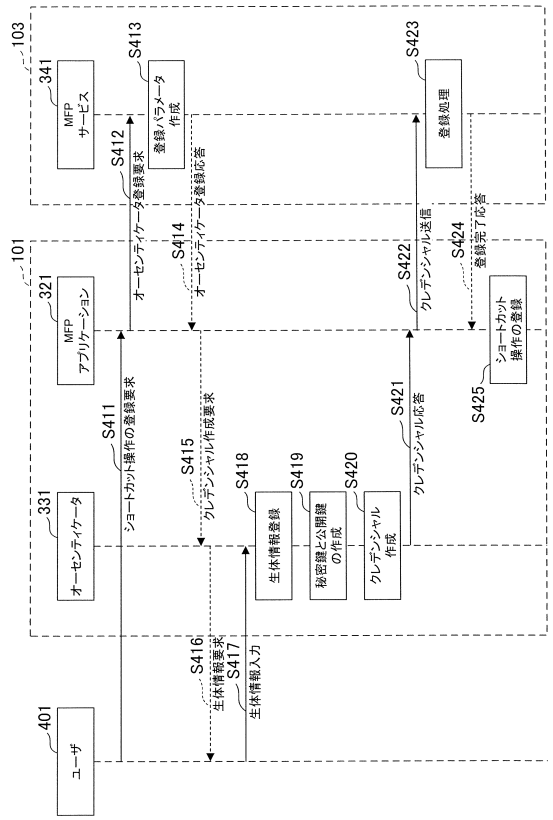
【図４】


102
241
242
CPU
243
RAM
244
ROM
245
記憶装置
246
TPM
247
ネットワーク
I/F
248
生体情報
センサ
249
タッチパネル
250
近接通信
I/F

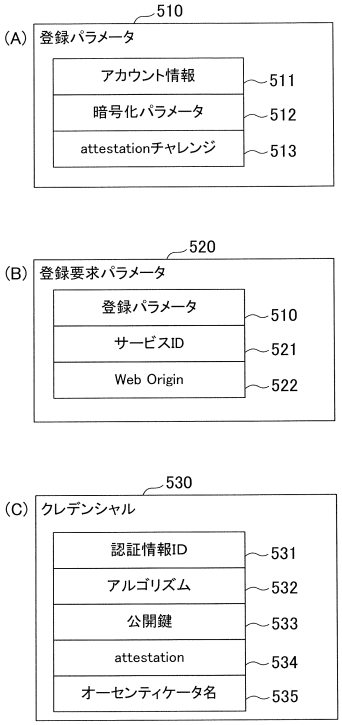
【図５】


(A)
102,104
携帯端末、クライアントPC
311
アプリケーション
312
表示部
313
通信部
(B)
101
MFP
321
MFPアプリケーション
322
表示部
323
プリント実行部
324
スキャン実行部
325
コピー実行部
326
通信部
327
オーセンティケータ登録制御部
328
オーセンティケータ認証制御部
329
ショートカット管理部
331
オーセンティケータ (Authenticator)
332
オーセンティケータ登録処理部
333
生体認証処理部
334
認証情報格納部
335
生体情報要求部
(C)
103
サーバ
341
MFPサービス
342
レガシー認証処理部
343
オーセンティケータ情報処理部
344
プリントデータ処理部
345
スキャンデータ処理部
346
ユーザ情報格納部
347
オーセンティケータ情報格納部
348
プリントデータ格納部
349
スキャンデータ格納部
350
プレゼンテーション部
351
トークン管理部
352
通信部

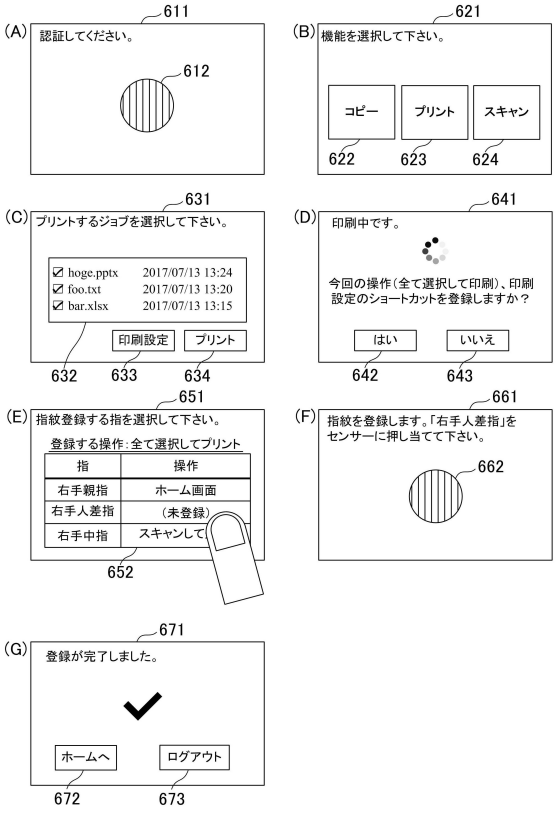
【図６】


103
341
MFPサービス
S412
登録要求
S413
登録パラメータ作成
S414
オーセンティケータ登録応答
S423
登録処理
S424
登録完了応答
101
321
MFPアプリケーション
S411
ショートカット操作の登録要求
S415
クレデンシャル作成要求
S418
生体情報登録
S419
秘密鍵と公開鍵の作成
S420
クレデンシャル作成
S421
クレデンシャル応答
S422
クレデンシャル送信
S425
ショートカット操作の登録
331
オーセンティケータ
S416
生体情報要求
S417
生体情報入力
401
ユーザ

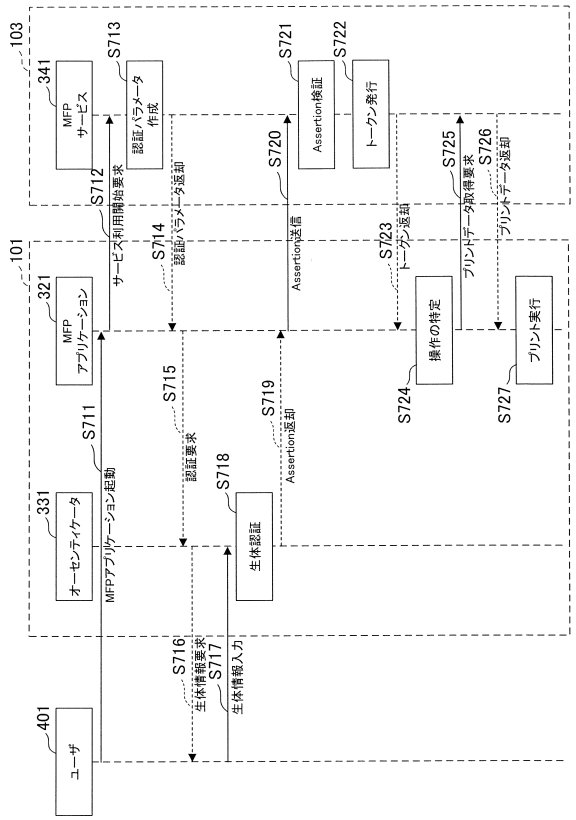
【図７】


510
(A) 登録パラメータ
アカウント情報
511
暗号化パラメータ
512
attestationチャレンジ
513
520
(B) 登録要求パラメータ
登録パラメータ
510
サービスID
521
Web Origin
522
530
(C) クレデンシャル
認証情報ID
531
アルゴリズム
532
公開鍵
533
attestation
534
オーセンティケータ名
535

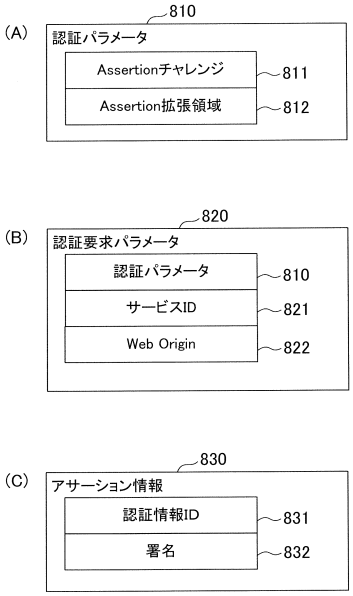
【図８】


(A)
611
認証してください。
612
(B)
621
機能を選択して下さい。
コピー
プリント
スキャン
622
623
624
(C)
631
プリントするジョブを選択して下さい。
hoge.pptx 2017/07/13 13:24
foo.txt 2017/07/13 13:20
bar.xlsx 2017/07/13 13:15
印刷設定
プリント
632
633
634
(D)
641
印刷中です。
今回の操作(全て選択して印刷)、印刷設定のショートカットを登録しますか？
はい
いいえ
642
643
(E)
651
指紋登録する指を選択して下さい。
登録する操作:全て選択してプリント
指
操作
右手親指
ホーム画面
右手人差指
(未登録)
右手中指
スキャンして
652
(F)
661
指紋を登録します。「右手人差指」をセンサーに押し当てて下さい。
662
(G)
671
登録が完了しました。
ホームへ
ログアウト
672
673

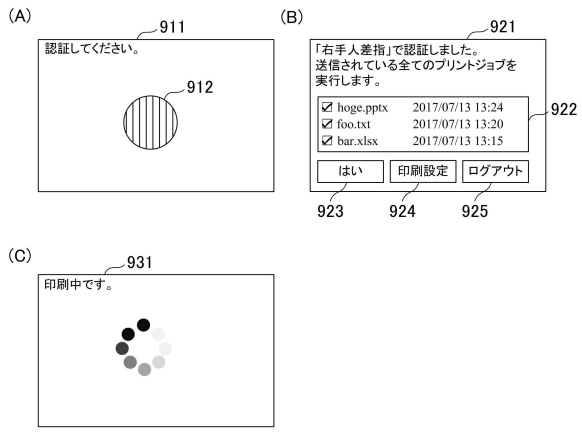
【図９】



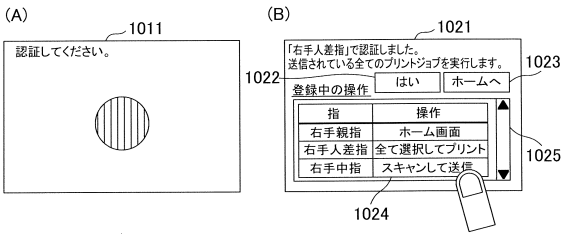
【図１０】



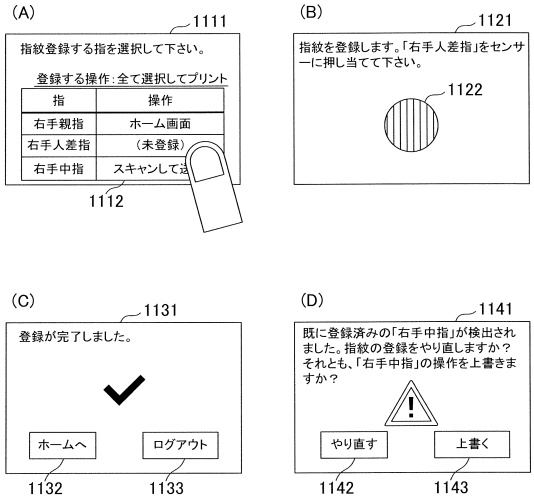
【図１１】



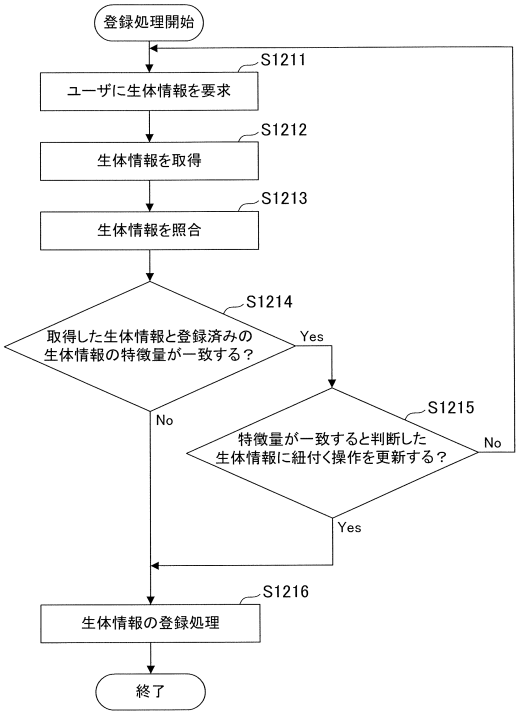
【図１２】



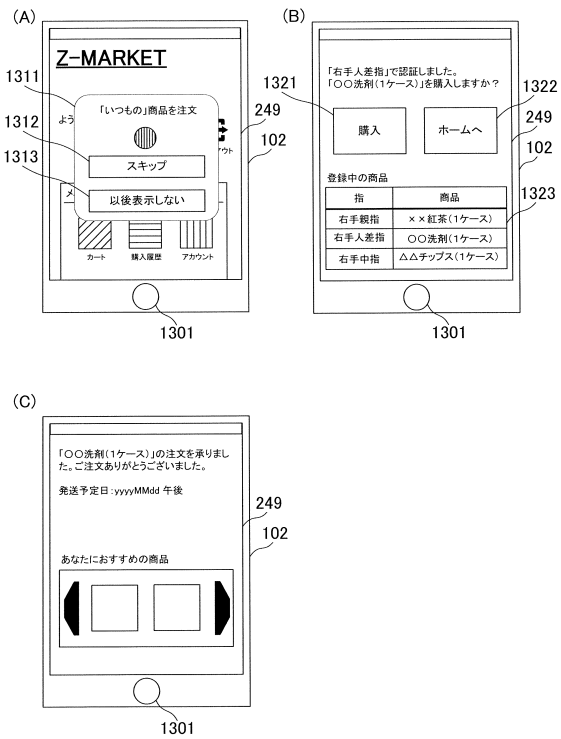
【図１３】


(A)
1111
指紋登録する指を選択して下さい。
登録する操作：全て選択してプリント
指
操作
右手親指
ホーム画面
右手人差指
（未登録）
右手中指
スキャンして送
1112
(B)
1121
指紋を登録します。「右手人差指」をセンサーに押し当てて下さい。
1122
(C)
1131
登録が完了しました。
ホームへ
ログアウト
1132
1133
(D)
1141
既に登録済みの「右手中指」が検出されました。指紋の登録をやり直しますか？
それとも、「右手中指」の操作を上書きますか？
やり直す
上書く
1142
1143

【図１４】


登録処理開始
S1211
ユーザに生体情報を要求
S1212
生体情報を取得
S1213
生体情報を照合
S1214
取得した生体情報と登録済みの生体情報の特徴量が一致する？
Yes
No
S1215
特徴量が一致すると判断した生体情報に紐付く操作を更新する？
No
Yes
S1216
生体情報の登録処理
終了

【図１５】


(A)
Z-MARKET
1311
「いつもの」商品を注文
1312
スキップ
1313
以後表示しない
カート
購入履歴
アカウント
249
102
1301
(B)
1321
「右手人差指」で認証しました。
「○○洗剤（1ケース）」を購入しますか？
購入
ホームへ
1322
249
102
登録中の商品
指
商品
右手親指
××紅茶（1ケース）
右手人差指
○○洗剤（1ケース）
右手中指
△△チップス（1ケース）
1323
1301
(C)
「○○洗剤（1ケース）」の注文を承りました。ご注文ありがとうございました。
発送予定日：yyyyMMdd 午後
249
102
あなたにおすすめの商品
1301

フロントページの続き

(56)参考文献 特開２０１４－１１９８６５（ＪＰ，Ａ）
米国特許出願公開第２００７／０１０６８９５（ＵＳ，Ａ１）
井澤秀益，五味秀仁，次世代認証技術を金融機関が導入する際の留意点 －ＦＩＤＯを中心に－，日本銀行金融研究所ディスカッション・ペーパー・シリーズ，日本銀行金融研究所，2016年02月29日，Ｎｏ．２０１６－Ｊ－３，ｐｐ．１－３２，［２０１７年3月１２日検索］，インターネット，＜URL：http://www.imes.boj.or.jp/research/papers/japanese/16-J-03.pdf＞

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３０－２１／４６