(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4498199号
(P4498199)

(45)発行日　平成22年7月7日(2010.7.7)　(24)登録日　平成22年4月23日(2010.4.23)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 15/00 330C
G09C 1/00 (2006.01)　G09C 1/00 640E

請求項の数 12　(全 17 頁)

(21)出願番号　特願2005-115907(P2005-115907)
(22)出願日　平成17年4月13日(2005.4.13)
(65)公開番号　特開2006-293831(P2006-293831A)
(43)公開日　平成18年10月26日(2006.10.26)
審査請求日　平成18年6月8日(2006.6.8)

(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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　福水　誠
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

最終頁に続く

(54)【発明の名称】認証装置及び認証システム並びに認証方法

(57)【特許請求の範囲】
【請求項１】
サーバ装置とネットワークを介して接続された複合機であって、
ユーザの認証手続の過程において前記複合機の電話番号を表示する表示手段と、
前記表示手段によって表示した電話番号への発呼に対する着信信号から発信者の電話番号を取得する取得手段と、
前記取得手段で取得した電話番号を前記サーバ装置に送信する送信手段と、
前記サーバ装置による、前記取得した電話番号を登録しているか否かについての判定結果を、前記サーバ装置から受信する受信手段と、
前記判定結果が前記取得した電話番号を登録していることを示す場合に、前記ユーザの認証に成功したことを表示する認証結果表示手段と、
を備えることを特徴とする複合機。
【請求項２】
前記ユーザのユーザ名を取得するユーザ情報取得手段を更に備え、
更に、前記送信手段は、前記ユーザ情報取得手段で取得した前記ユーザ名を前記サーバ装置へ送信し、前記サーバ装置が該ユーザ名を登録しているか否かを判定することを特徴とする請求項１に記載の複合機。
【請求項３】
更に、前記受信手段は、前記サーバ装置による前記ユーザ名を登録しているか否かについての判定の結果を受信し、前記判定結果が、前記取得したユーザ名を登録していること

を示す場合に、前記表示手段が前記複合機の電話番号を表示することを特徴とする請求項２に記載の複合機。
【請求項４】
前記複合機の電話回線を使用中であっても他の着信を受信可能な割り込み着信機能を有し、前記電話回線が使用中であっても該割り込み着信機能により前記取得手段による電話番号の取得を可能とすることを特徴とする請求項１に記載の複合機。
【請求項５】
前記ユーザの認証に成功した後に、予め定められたタイミングで前記表示手段と前記取得手段と前記受信手段とを機能させて認証状態の継続を確認する確認手段を更に備えることを特徴とする請求項１に記載の複合機。
【請求項６】
前記認証手続の開始から、前記表示手段による前記電話番号の表示を含む予め決められた期間内において、該表示手段により表示される電話番号に対応する回線をオフフック状態へ移行させる移行手段を更に備えることを特徴とする請求項１に記載の複合機。
【請求項７】
前記移行手段は、前記予め決められた期間内においてユーザによる予め定められた操作入力があった場合は、前記回線をオンフック状態へ移行させることを特徴とする請求項６に記載の複合機。
【請求項８】
前記移行手段は、オフフック状態への移行を実行しようとした際に、既に当該装置が回線を使用中であった場合、前記ユーザの電話番号を入力させるインターフェースを提供し、
回線が空いたならば前記インターフェースで入力された電話番号へ発呼する手段を更に備えることを特徴とする請求項６に記載の複合機。
【請求項９】
前記取得手段において、前記着信信号が番号非表示発信によるものであった場合、番号通知状態で再度電話をかけなおすよう指示する手段を有することを特徴とする請求項１に記載の複合機。
【請求項１０】
サーバ装置とネットワークを介して接続された複合機の制御方法であって、
表示手段が、ユーザの認証手続の過程において前記複合機の電話番号を表示する表示工程と、
取得手段が、前記表示工程によって表示された電話番号への発呼に対する着信信号から発信者の電話番号を取得する取得工程と、
送信手段が、前記取得工程で取得した電話番号を前記サーバ装置に送信する送信工程と、
受信手段が、前記サーバ装置による、前記取得した電話番号を登録しているか否かについての判定結果を、前記サーバ装置から受信する受信工程と、
認証結果表示手段が、前記判定結果が前記取得した電話番号を登録していることを示す場合に、前記ユーザの認証に成功したことを表示する認証結果表示工程と
を備えることを特徴とする方法。
【請求項１１】
請求項１０に記載の制御方法をコンピュータに実行させるための制御プログラム。
【請求項１２】
請求項１０に記載の制御方法をコンピュータに実行させるための制御プログラムを格納した記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバ等の情報処理装置へのログイン等に好適な認証処理技術に関するもの

である。

【背景技術】

【０００２】

遠隔の装置に対して認証を行う構成に関しては種々の提案がなされている。特許文献１には、携帯電話などの携帯端末からネットワークに接続する際、ユーザ名やパスワードを用いて利用者の確認を行う構成（ＰＡＰ認証方式）や、利用者が所有する認証ＩＣカードを接続することで本人か否かを認証を行う構成（ＩＣカードセキュリティ方式）における課題が記載されている。

【０００３】

特許文献１によると、ＰＡＰ認証方式では、ユーザが所有する端末を選ばない。そのため、ユーザ名やパスワードが漏洩したり、他人に盗まれたりした場合には、本人以外でもどのような端末からでも簡単にアクセスできてしまう。従って、ＰＡＰ認証方式では、不正な接続を有効に防止できないという課題を有することが記載されている。

【０００４】

そこで、特許文献１では、このようなセキュリティ上の課題を解決するために、発信者番号通知サービスを認証に利用することが開示されている。

【０００５】

発信者番号通知サービスとは、通信回線を提供する通信事業者がユーザに対して提供するサービスである。このサービスでは、携帯電話などの携帯端末から任意の電話番号に対して電話をかけた場合、携帯端末通信基地局に携帯端末固有のコードと発信者電話番号通知要求が自動的に送信される。これらの情報を受信した基地局や電話交換網は、もともと保持している電話番号データベースから携帯端末固有のコードに関連付けられた発信者電話番号を割り出す。また、接続先の電話番号につながるように回線接続交換を行って、電話回線網を着信対象の電話機に接続する。そして、着信対象の電話機に発信者電話番号を送信することで、着信対象の電話機に携帯端末の電話番号を表示させる。この発信者番号通知サービスの提供を受けるには、着信対象の電話機にサービスを受ける設定がされていることが前提となる。

【０００６】

特許文献１では、ユーザが保有しているＰＣをネットワークに接続してデータ通信を行う場合に、ＰＣに接続された携帯端末を利用する。また、予めユーザのＩＤ名、パスワード、ユーザの電話番号を認証データとして通信装置に登録しておく。ネットワークに接続する場合、まず、携帯端末を介して接続先に電話をかける。携帯端末中継基地を介して携帯端末固有コードを含むアクセス情報を受けた電話交換網は、通信事業者が有する電話番号データベースにアクセスする。そして、携帯端末固有コードに基づいて、携帯端末の電話番号を割り出す。その後、割り出した携帯端末の電話番号を電話回線網を介して着信基地局に送信する。発信者番号通知サービスを設定している着信基地局の通信装置は携帯端末の電話番号を取得することができる。その後、携帯端末からはユーザＩＤとパスワードが送信されてくる。

【０００７】

通信装置は、事前に登録されたユーザＩＤ、パスワード、ユーザの電話番号と、携帯端末から通知された電話番号、ユーザＩＤ、パスワードを比較する。そして、これら全てが一致した場合に、通信装置がネットワーク接続を開始する。

【０００８】

つまり、特許文献１に開示の技術は、ユーザ所有の携帯端末の電話番号は基本的に重複することが無いことに着目し、認証キーとして電話番号を利用するものである。すなわち、特許文献１は、電話回線に接続されたサーバに対して携帯端末にて電話回線経由でサーバに接続し、ログインの認証にユーザ名、パスワードに加え、携帯電話の電話番号を使用する構成を記載している。

【０００９】

また、特許文献２には、ユーザ名とパスワードの入力においてキーボードの有無を判定

し、キーボード有りの場合はキーボードから、無しの場合は磁気カード等から認証情報を入力する構成が記載されている。すなわち、キーボードの有無に応じて物理的認証システムを使い分ける構成が示されている。例えば、ユーザＩＤとパスワードを予め保持した認証サーバと、ＰＣ、プリンタとがネットワークに接続されている環境において、ＰＣにおいてのユーザ認証はユーザＩＤおよびパスワードをキーボードより入力することによってなされる。また、ＰＣと同一のネットワークに接続されたプリンタにおいてもユーザ認証が必要とされている場合には、プリンタに磁気カードを挿入することでその実行者のユーザ認証がなされるというものである。

【特許文献１】特開平１１－０２７７５０号公報

【特許文献２】特開２００２－１７１２５２号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

認証情報としてユーザ名とパスワードを入力する場合、即ち、特許文献１に記載のＰＡＰ認証方式の場合は、単純な認証のためなりすましを防止することが困難である。一方、特許文献２のように磁気カード等を用いて認証を行う場合は、専用磁気カード等が必要となり利便性に不満が残る。また、磁気カード自体にプロテクトがかけられないため、やはりなりすましを防止することが困難である。

これに対して、特許文献１に記載されているように電話機の番号通知サービスを認証に利用することは、その普及度や番号通知に関するセキュリティの高さから有効な方法である。

【００１１】

しかしながら、上記特許文献１では、ユーザがどこでログインを行ったかについては何等考慮されていない。携帯電話の電話番号だけではどこの場所からログインしたかを証明する本人確認と認証を同時に保証することは出来ない。すなわち、特許文献１は、公共の場に据え付けられた情報端末をユーザが操作してログインするような場合に、実際にユーザがその情報端末を操作していることまでを保証することは考慮されていない。

【００１２】

特許文献１に記載されている環境は、携帯端末とＰＣとがセットであることが前提となっている。例えば、ユーザが携帯端末とＰＣとを持って外出し、外出先から社内のネットワークに接続するという使用方法である。

【００１３】

しかし、公共の場における情報端末をユーザが利用する場合では、ユーザは自分の携帯端末のみを所持しているだけに過ぎない。例えば、コンビニエンスストアに設置されたプリンタを介して、ユーザがサーバにあるドキュメントを印刷する場合を考える。この場合に印刷物のセキュリティを確保するためには、ユーザがプリンタの存在する場所にいることを特定する必要がある。

【００１４】

本発明は、電話機の番号通知サービスを利用するとともに、認証操作を行うユーザの位置に関する保証を可能とし、認証処理の信頼性を向上することを目的とする。

【課題を解決するための手段】

【００１５】

上記の目的を達成するための本発明の一態様による複合機は以下の構成を備える。即ち、サーバ装置とネットワークを介して接続された複合機は、ユーザの認証手続の過程において前記複合機の電話番号を表示する表示手段と、前記表示手段によって表示した電話番号への発呼に対する着信信号から発信者の電話番号を取得する取得手段と、前記取得手段で取得した電話番号を前記サーバ装置に送信する送信手段と、前記サーバ装置による、前記取得した電話番号を登録しているか否かについての判定結果を、前記サーバ装置から受信する受信手段と、前記判定結果が前記取得した電話番号を登録していることを示す場合に、前記ユーザの認証に成功したことを表示する認証結果表示手段とを備える。

【００１６】
また、上記の目的を達成するための本発明の更なる態様による複合機は以下の構成を備える。即ち、前記ユーザのユーザ名を取得するユーザ情報取得手段を更に備え、更に、前記送信手段は、前記ユーザ情報取得手段で取得した前記ユーザ名を前記サーバ装置へ送信し、前記サーバ装置が該ユーザ名を登録しているか否かを判定し、更に、前記受信手段は、前記サーバ装置による前記ユーザ名を登録しているか否かについての判定の結果を受信し、前記判定結果が、前記取得したユーザ名を登録していることを示す場合に、前記表示手段が前記複合機の電話番号を表示する。
【発明の効果】
【００１７】
本発明によれば、電話機の番号通知サービスを利用するとともに、認証操作を行うユーザの位置に関する保証が得られ、認証処理の信頼性が向上する。
【発明を実施するための最良の形態】
【００１８】
以下、添付の図面を参照して本発明の好適な実施形態を説明する。
【００１９】
図１は、本実施形態による端末装置１００の内部構成を示すブロック図である。図１において、端末装置１００は、画像読取機能及び記録機能を具備した複合機（ＭＦＰ）である。通信部１０１は、外部装置との通信を行うためのインターフェースを提供する。通信部１０１は、電話回線１３０と接続するためのインターフェース、ＬＡＮ或いはインターネット等のコンピュータネットワーク１２０に接続するためのインターフェースを備える。なお、本例では、通信部１０１はＬＡＮ経由でインターネットに接続し、インターネット上の所定のサーバ（情報処理装置）との間で認証処理を行う。また、通信部１０１は該サーバとの間で画像データ及びその他のデータの送受信を行う。電話番号取得部１０２は、電話回線１３０を介して通信部１０１にて着信した信号から電話番号を取得する。本実施形態では、発信者番号通知サービスを利用し、このサービスにより通知された電話番号が取得される。
【００２０】
画像読取部１０３は、原稿の送信又は原稿のコピーのために、原稿を光学的に読み取り、画像データを生成する。印刷記録部１０４は、コピーやプリント画像を記録媒体に上に印刷する。表示部１０５は、各種操作状況及び操作ガイド及びステータス状況を表示する。操作部１０６は、各種の操作キーを具備する。利用者が各種キーを操作することにより、例えば、印刷記録部１０４によるコピー枚数の設定や、画像読取部１０３による原稿の読取方法の設定や、上記サーバ装置による認証のための文字入力等を行うことができる。なお、表示部１０５と操作部１０６の一部或いは全てをタッチパネルにより実現するようにしてもよい。
【００２１】
ＲＯＭ１０７には制御部１１０によって実行される各種プログラムが記憶されている。フローチャートを参照して説明される端末装置１００の各処理は、ＲＯＭ１０７に格納された制御プログラムを制御部１１０が実行することにより実現される。ＲＡＭ１０８は、ＲＯＭ１０７から転送された各種プログラムや記憶部１０９から転送されたデータを記憶する。また、ＲＡＭ１０８の一部は制御部１１０が各種プログラムを実行する際のワークエリアとして確保されている。記憶部１０９は例えばハードディスクを具備し、大容量のデータを記憶可能である。制御部１１０は、ＣＰＵを具備し、各種制御や各種信号処理を行う。
【００２２】
コンピュータネットワーク１２０はＬＡＮ及びインターネットを構成している（以下、インターネット１２０とも称する）。電話回線１３０は、公衆回線であり、携帯電話等からの着信を受ける。
【００２３】

図２は、本実施形態による端末装置１００とサーバの接続状態を説明する図である。図２に示されるように、情報端末１００はインターネット（１２０）を介してサーバ３００と接続可能である。サーバ３００にはプルプリントの対象となる画像データが登録されている。なお、プルプリントとは、プリントを行う端末装置１００から、サーバに保存されている画像データやドキュメントデータを取得して印刷を行う印刷形態のことである。但し、本発明はプルプリントのみに制限されるものではなく、サーバから端末装置１００に対してデータを送信する印刷形態であってもよい。端末装置１００がプルプリントを行う際には、端末装置１００はインターネットを経由してサーバ３００から所望の画像を取得し、これをプリントアウトする。なお、プルプリントを行うべく端末装置１００がサーバ３００にログインする際には、操作部１０６からのキー入力と携帯電話２００からの発信による番号通知が用いられる。

【００２４】

以下、本実施形態の認証動作例として、コンビニエンスストア等に設置した端末装置（複合機）１００（パブリック環境の端末装置１００）を用いてプルプリントを行う場合を説明する。図３Ａ及び図３Ｂは本実施形態の端末装置１００による認証動作を説明するフローチャートである。図４は回線使用中の割り込み着信を可能とする割り込み着信設定がなされていない場合に、端末装置１００における回線確保動作を説明するフローチャートである。図５は、回線確保動作における状態遷移を示す図である。図６は本実施形態の端末装置１００における表示部１０５の各段階における表示例を示す図である。また、図９はサーバ３００における認証処理に関わる動作を示すフローチャートである。

【００２５】

まず、事前処理について説明する。なお、この事前処理における手順や手法などは如何なるものであってもよい。

事前処理として、ユーザはパーソナルコンピュータ等を用いてサーバ３００にユーザ登録を行っておく。ユーザ登録により、サーバ３００には当該ユーザのユーザ名と携帯電話の電話番号が登録される。この登録情報は例えば図２の登録テーブル３００ａの形態でサーバ３００に保持される。また、本サーバや別のサーバに、端末装置で出力を所望するデータなどを保存しておく。

【００２６】

さて、端末装置１００の操作部１０６を操作して「プルプリント」を選択すると図６の画面６０１が表示部１０５に表示される。なお、本実施形態において表示部１０５はタッチパネルで構成されており、画面６０１上のキー入力ボタン６０１ａ或いは携帯電話ボタン６０１ｂを指で触れることでボタン操作ができる。携帯電話ボタン６０１ｂを選択することにより、ログインパスワードに携帯電話の電話番号を用いる認証モードが選択される。この認証モードが選択されると、処理はステップＳ３０１からステップＳ３０２へ進む。ステップＳ３０２では、端末装置１００が電話回線１３０からの着信に対して割り込み着信設定がなされているかを判定する。割り込み着信設定がなされていない場合は、当該端末装置１００への回線を確保するためにステップＳ３２０へ進み、オフフック処理を行う。すなわち、強制的に端末装置１００をオフフックの状態として、他の機器からの着信を防止する。なお、オフフックとは、電話回線と接続された状態とすることを示す表現であるが、その手法はどのようなものであってもよい。

【００２７】

続いて、ステップＳ３０３へ進み、画面６０２を表示してユーザにユーザ名を入力させる。このユーザ名は、事前処理においてサーバ３００に登録されたユーザ名に相当するものである。ユーザ名は例えばアルファベットと数字の組み合わせで構成される。ユーザは操作部１０６に設けられたテンキーを用いてユーザ名を入力する。入力されたユーザ名はユーザ名表示領域６０２ａに表示される。なお、テンキーを表示部１０５に表示してタッチパネルによりユーザ名を入力できるようにしてもよい。ユーザ名が入力されて確認ボタン６０２ｂが押されると、ステップＳ３０４へ進み、端末装置１００は入力されたユーザ名をインターネット１２０を介してサーバ３００へ送信し、照会を要求する。なお、所定

時間内にユーザ名の入力がなかった場合は本処理を終了して画面を初期状態へ戻すものとする。

【００２８】

一方、サーバ３００は、図９に示すように端末装置１００からの要求受信を待機している（ステップＳ９０１）。そして、上記ステップＳ３０４による照会要求が受信されると、ステップＳ９０２を経てステップＳ９０４へ処理を進め、入力されたユーザ名と登録テーブル３００ａにより照会を行う。より具体的には、サーバ３００は送信されたユーザ名が登録テーブル３００ａに登録されているか否かを判定する。そしてステップＳ９０５において、その判定結果を端末装置１００に通知する。

【００２９】

サーバ３００より登録されているユーザ名である旨の通知を受けた場合は、処理はステップＳ３０５からステップＳ３０６へ進む。ステップＳ３０６では、画面６０３のような表示６０３ａにより、当該端末装置１００の電話番号を提示して携帯電話により当該端末装置１００へ電話をかけるようにユーザを促す。続いて、ステップＳ３０７では、確認キー６０３ｂが押されるのを待つ。確認キー６０３ｂが押されると、再び割り込み着信設定がなされているかどうかに従って処理を分岐する。割り込み着信設定がなされている場合はステップＳ３１０へ進み、着信検出タイマ（フェイルセーフタイマ）をスタートして携帯電話の電話番号による認証処理を開始する。一方、割り込み着信設定がなされていない場合は、上記ステップＳ３２０においてオフフック状態となっている。従ってステップＳ３０９へ進み、端末装置１００の通信部１０１をオンフック状態に戻し、上記のステップＳ３１０へ進む。なお、確認ボタン６０３ｂの押下を待たずに、画面６０３を表示した後、直ちにステップＳ３０８の処理を行うようにしてもよい。ステップＳ３１０で着信検出タイマをスタートするとステップＳ３３０へ進む。

【００３０】

以上のように、確認ボタン６０３ｂとステップＳ３０７を設けたことにより、画面６０３の表示を見てからユーザは携帯電話２００を準備し、携帯電話のダイヤル準備完了の合図として複合機の確認キー６０３ｂを押下することができる。なお、画面６０３の表示後、所定時間が経過するまで確認ボタン６０３ｂが押下されなかった場合は、当該認証処理を強制終了する。以上のように、目の前の端末装置１００（複合機）の操作と電話番号認証は、その場に居ないと成り立たないため、ユーザの位置の特定が可能となる。つまり、確実にユーザは端末装置１００の前で認証操作を行っているということが判断可能である。

【００３１】

ステップＳ３３０で、端末装置１００は上記ステップＳ３０６で表示した電話番号への着信を待つ。通信部１０１によって着信が検出されると、ステップＳ３３１へ進む。ステップＳ３３１では、電話番号取得部１０２が発信者通知信号（例えばＦＳＫ：周波数変調）を解析し、電話番号を取得する。もちろん、発信者の電話番号の取得手法はこれに限らない。

【００３２】

電話番号が取得された場合は、ステップＳ３３２からステップＳ３３３へ進み、取得した電話番号をサーバ３００へ送信し、ログインを要求する。サーバ３００は登録テーブル３００ａを参照して、先に送信されたユーザ名と、ステップＳ３３３で送信された電話番号により認証、ユーザログイン処理を行う。即ち、図９に示されるように、サーバ３００においては、ログイン要求を受信するとステップＳ９０１、Ｓ９０２、Ｓ９０３を経てステップＳ９０６へ処理が進む。ステップＳ９０６では、電話番号とユーザ名を登録テーブル３００ａの登録内容と比較することによりログインを試みる。そして、ステップＳ９０７においてログインの成否を端末装置１００に通知する。この時点では、装置がログイン中ではないのでステップＳ９０８においてＮＯに分岐する。ステップＳ３３４ではサーバにより認証が得られたかどうかを判定する。すなわち、この時点において、認証が得られるか否かは、取得した電話番号が登録された番号か否かであることと等しい。

【００３３】
なお、ステップＳ３３３においては電話番号のみをサーバ３００へ送信してもよいし、ユーザ名と電話番号のペアをサーバ３００へ送信してもよい。電話番号のみが送信される場合には、その直前でその端末装置から照会要求とともに受信したユーザ名を、当該端末装置のＩＤに対応付けてサーバ３００が保持する。そして、サーバ３００は、その後電話番号のみを含むログイン要求を受信した際には、当該ログイン要求の送信元の端末装置のＩＤに対応して保持されているユーザ名を取得する。
【００３４】
認証に成功した場合、すなわち取得した電話番号がユーザ名に対応付けられて登録された番号であった場合は、ステップＳ３３４からステップＳ３３５に進む。ステップＳ３３５では、画面６０４を表示し、本人確認に成功したことを通知し、プルプリント操作が可能な環境へ移行する。例えば、サーバ３００に保持されたデータを指定して、印刷実行可能な表示画面をユーザに提供するなどである。
【００３５】
一方、ステップＳ３０５でユーザ名がサーバ３００において未登録であった場合は、処理はステップＳ３０５からステップＳ３２１へ進む。ステップＳ３２１においてはユーザ名の照合が失敗に終わった回数、すなわち不一致回数をカウントする。そして、ステップＳ３２２において不一致回数が所定回数以内であれば、ステップＳ３０３へ戻り、例えば画面６１１を表示して再びユーザ名の入力を促す。ユーザはこの画面からユーザ名を再度入力して確認ボタン６０２ｂを押すことで、ステップＳ３０４の照会処理が再度実行される。ステップ３２２で不一致回数が所定回数を超えた場合は、ステップＳ３４１へ進み、認証に失敗したことを示す画面６２１を表示する。確認ボタン６２１ａが押されると当該認証処理が終了する。
【００３６】
また、端末装置１００において着信した際に、携帯電話２００が番号非通知に設定されていること等により、ステップＳ３３１で電話番号を取得できない場合がある。そのような場合、処理はステップＳ３３２からステップＳ３５０へ進む。ステップＳ３５０では、表示部１０５に画面６１３のごとき表示を行い、電話番号が取得できない旨を通知し、番号通知状態にして再度電話をかけなおすことを指示する。確認ボタン６１３ａが押されるとステップＳ３５２へ進み、不一致回数のカウント値が１つ増加される。そして、ステップＳ３５３において不一致回数が所定回数を超えたか否かを判定する。不一致回数が所定回数以内であればステップＳ３０６へ戻り、画面６０３を表示して、再度端末装置１００へ電話をかけさせる。不一致回数が所定回数を超えた場合は、ステップＳ３５３からステップＳ３４１へ進み、画面６２１を表示して認証に失敗したことをユーザに通知する。
【００３７】
また、端末装置１００において取得した電話番号をサーバ３００で照会（ステップＳ３３３）した結果、当該電話番号が未登録であった場合（ログインに失敗した場合）は、ステップＳ３３４からステップＳ３５１へ進む。ステップＳ３５１では、例えば画面６２１を表示部１０５に表示して、電話番号が違う旨を通知する。確認ボタン６１２ａが押されるとステップＳ３５２へ進み、不一致回数のカウント値が１つ増加される。そして、ステップＳ３５３において不一致回数が所定回数を超えたか否かを判定する。不一致回数が所定回数以内であればステップＳ３０６へ戻り、画面６０３を表示して、再度端末装置１００へ電話をかけさせる。不一致回数が所定回数を超えた場合は、ステップＳ３５３からステップＳ３４１へ進み、画面６２１を表示して認証に失敗したことをユーザに通知する。
【００３８】
なお、ステップＳ３４１では、ユーザ名の不一致回数オーバー（Ｓ３２２）、着信検出タイマのタイムアウト（Ｓ３４０）、電話番号が取得できないことや取得した電話番号が未登録であることによる不一致回数オーバー（Ｓ３５３）により認証に失敗した旨が表示される。従って、画面６２１においては、どの理由で認証に失敗したかを示すようにしてもよい。たとえば、ステップＳ３５３からの分岐によりステップＳ３４１が実行された場

合には、画面６２１において、『着信検出タイマのタイムアウトにより認証に失敗しました。もう一度はじめからやり直してください』というように表示される。

【００３９】

また、画面６２１のような通知を所定時間行った後に、表示部１０５の表示内容を自動的に初期画面に戻すようにしてもよい。このようにすれば、確認ボタン６２１ａを押し忘れても、画面は初期画面へ戻るので、次の使用者に違和感が生じない。

【００４０】

さて、本実施形態では、ログイン後も、更にセキュリティを高めるために所定のタイミングで（たとえば、所定枚数のプリント出力毎に）携帯電話による認証が行われる。すなわち、図３Ｂのステップ３３６において、セキュリティを高めるために、再認証を行う必要があるか否かを判断し、必要があると判断された場合はステップＳ３０６に処理を戻す。この結果、図６の画面６０３が表示され、携帯電話を用いて端末装置１００に電話をかけるようユーザを促す。そして、新たな認証に成功するまで、プルプリント処理を中断状態にする。また、認証に失敗すれば、その時点でプルプリント処理を中止することになる。また、ログアウトが指示されると、ステップＳ３３７からステップＳ３３８へ進み、プルプリントを終了し、サーバ３００からログアウトして本処理を終了する。このとき、サーバ装置３００では、処理がステップＳ９０８においてＹＥＳへ分岐し、ステップＳ９０９において、当該端末装置１００によるログイン状態が解除される。

【００４１】

なお、上記処理において、サーバ３００との通信に適宜暗号化を用いてセキュリティの強化を図るようにしてもよいことは明らかである。

【００４２】

次に図４及び図５を用いてステップＳ３２０におけるオフフック処理を説明する。オフフック処理は、回線使用中の割込み着信設定がなされていない回線において認証処理時に効率的に回線を確保することを目的とする。ステップＳ５０１において、通信部１０１において回線が使用中か否かを判断する。使用中の場合は、回線が空くまで認証が出来ない。従って、処理はステップＳ５０２に進み、回線が空くまでの間ユーザを待たせるための表示を表示部１０５により行う。たとえば、「暫くお待ちください」を表示する。回線が空いていた、或いは回線が空き状態に移行したならば、処理はステップＳ５０３へ進む。ステップＳ５０３では、認証操作中に他の着信を受信しないように、通信部１０１を強制的にオフフック状態とする。

【００４３】

ステップＳ５０３により、図５の５０１に示されるように、端末装置１００において強制オフフック（図５の５５１）が実行される。これは、上述のように携帯電話番号による認証を行うために、早期に端末装置１００の電話回線を確保し、他の着信を拒否させるために行われる。その後、サーバ３００に登録されたユーザ名が入力されると、図６の画面６０３により、端末装置１００へ電話をかけるようユーザを促す。ユーザは携帯電話を準備しダイヤル準備ができたところで、ダイヤル準備完了の合図として確認ボタン６０３ａを押す。この確認ボタン６０３ａの押下により、オフフック解除（図５の５５２）が行われ、オンフック状態へ移行する（ステップＳ３０９）。ユーザは携帯電話２００から端末装置１００にダイヤルする（図５の５５３）。端末装置１００は着信（図５の５５４）した信号から電話番号を取得し、これを用いて認証を実行する。

【００４４】

携帯電話２００の受話器から呼び出し音が聞こえれば、端末装置１００に着信している。従って、ユーザは呼び出し音を確認して携帯電話をオンフック（図５の５５５）する。

【００４５】

以上、本実施形態による認証処理を詳述した。

【００４６】

なお、ステップＳ５０１において回線使用中であった場合は、ステップＳ５０２で『暫くお待ちください』というメッセージを表示部１０５に表示したが、これに限られるもの

ではない。例えば、ステップＳ５０１で電話回線が使用中と判定された場合は、回線が使用中であることを表示するとともに、回線が空きしだい優先的に使用できるように予約する機能を設けてもよい。このような予約の処理について図７と図８を用いて以下に説明する。

【００４７】

図７は、予約処理を含むオフフック処理を説明するフローチャートである。図７の処理は、図４に示したオフフック処理に代わるものである。図８は予約処理時における画面の遷移例を示す図である。図３Ａで説明したように、図８の画面６０１において携帯電話ボタン６０１ｂが押され、当該端末装置１００において割り込み着信設定がなされていない場合は、ステップＳ３２０のオフフック処理（図７）が起動する。

【００４８】

図７において、ステップＳ５０１で回線が使用中であると判定された場合は、ステップＳ５２１へ進む。ステップＳ５２１では、表示部１０５を用いてユーザ名と携帯電話の番号を入力させるインターフェース（画面８０１）を提示する。ユーザは画面８０１の電話番号入力欄８０１ａに電話番号を、ユーザ名入力欄８０１ｂにユーザ名を入力し、確認ボタン８０１ｃを押す。確認ボタン８０１ｃが押されると、ステップＳ５２２において、ステップＳ３０４と同様にユーザ名入力欄８０１ｂに入力されたユーザ名を、インターネット１２０を介してサーバ３００に通知し、照会を行う。サーバ３００から照会の結果を受けて、未登録のユーザ名であった場合はステップＳ５２７へ進み、例えば画面８２１を表示して予約を拒否する。

【００４９】

一方、登録されたユーザであると確認された場合は、ステップＳ５２４へ進み、表示部１０５に画面８１１を表示させるとともに予約を受け付ける。画面８２１、画面８１１を表示した後は所定の時間の経過を待って表示部１０５の表示をスタンバイ状態へ戻す。そして、回線が空きしだい携帯電話に端末装置１００の通信部１０１が電話をかけ（発呼し）、ステップＳ３０３以降の処理を実行する（ステップＳ５２５，Ｓ５２６）。即ち、電話番号入力欄８０１ａに入力された電話番号へ発呼を行うことで、回線を確保した旨をユーザに通知する。例えば、所定回数着信を発生させて、回線を切り、そのままステップＳ５０３へ進んで、強制オフフック状態とする。このとき、当該発呼に対してユーザが携帯電話をオフフック状態とした場合に、回線が空いた旨を通知するアナウンスを流すようにしてもよい。そして、ステップＳ３０３へ処理を進めて、上述したログイン操作を可能とする。従って、認証再開時は通常のログインと同じ操作でログインが可能である。

【００５０】

また、端末装置１００において認証が正常終了または異常終了した時点で、内部メモリから認証のためにユーザが入力した情報や取得した電話番号は消去するように構成することが好ましい。

【００５１】

上記実施形態によれば、ログイン操作時にユーザ名を入力した結果、端末装置１００に電話をかけることを促すメッセージが出され、このメッセージに応じて電話をかけることが要求される。例えば、端末装置１００に入力されたユーザ名がサーバ３００に送信され、サーバ３００に登録されたユーザ名であると判定された場合に、携帯電話から電話をかけるように要求される。このように、一連の認証手続の所定のタイミングでユーザに電話をかけることが要求されるので、ユーザがその場に居合わせなければならないという状況が効果的に提供される。このように、端末装置１００の操作と電話番号認証は、その場（端末装置１００のある場所）に居ないと成り立たないため、不特定多数のユーザが使用する情報端末１００による認証処理において、本人位置特定と認証を短時間で簡単に行うことが可能である。また、認証に使用する電話番号は電話局から送付されてくるため、改ざんやなりすましの余地が無く、簡易な構成で高い信頼性を持った認証を実現できる。

【００５２】

また、通信部１０１を割り込み着信許可機能に対応させれば、ログイン時に回線が使用

中の場合でも番号通知の確認を行える。従って、他の装置からの着信によって回線が使用中となっていることに起因する待ち時間がなくなる。また、割り込み着信許可機能に対応していない場合は、端末装置の所定操作に連動して、回線未使用状態から強制的にオフフック状態とし、他者からの着信をブロックするようにした。こうして、認証が成立するまでは、ＦＡＸ受信等の認証に差し支える受信の可能性を低減することが可能となる。すなわち、他からの着信により端末装置１００の回線が占有される可能性が極力減らされるので、ログインを短時間で行えるようになる。なお、上記実施形態では、オンフックへの復帰は、表示部１０５／操作部１０６へのユーザからの所定の操作入力に従ってなされる。このため、ユーザは、携帯電話からダイヤルする準備できた時点でオンフックへ復帰させることができ、強制的なオフフックの状態を適切に継続させることができる。

【００５３】

また、上記実施形態では、ログイン後も不定期に携帯電話から電話をかけることを促し、着信から取得された電話番号を用いた認証を行っている。このように、その情報端末の前でしか対応できない操作の要求と認証を繰り返すことにより、不正使用を効果的に防止し、信頼性を一段と高めることができる。

【００５４】

また、上記実施形態では、端末装置１００からサーバ装置３００へのログインにおける認証処理を説明したが、端末装置１００自身へのユーザからのログインのための認証にも上記認証処理を利用できる。この場合、端末装置１００がサーバ３００で行った照会処理やログイン処理を行うことになる。また、コンピュータネットワーク１２０によるサーバ３００への認証情報（ユーザ名や電話番号）の通知は不要となる。また、端末装置１００もＭＦＰに限られるものではなく、あらゆる情報処理装置を適用することができる。

【００５５】

また、上記実施形態では、予めサーバ３００にユーザ名と電話番号を登録していたが、更にユーザ名と電話番号に対応するパスワードを登録することも可能である。

【００５６】

この場合、ユーザが図３ＡのステップＳ３０３で端末装置１００に対してユーザ名とともにパスワードを入力する。サーバ３００は入力されたユーザ名とパスワードを用いて、予め登録されているユーザであるかどうかを判定する。このように構成することで、更にセキュリティを確保することが可能である。

【００５７】

また、上記実施形態では、認証情報を保持するサーバ３００と端末装置１００との関係を用いて本発明の一例を説明したが、本発明の構成はこれに限るものではない。例えば、サーバとして認証用のサーバと、ドキュメントデータを保持するサーバとを別々に設けてもよい。また、本実施形態におけるサーバ３００を端末装置内部に認証部として設けるよう構成してもよい。この場合、端末装置内部の認証部では上記のサーバ３００と同等の情報を有することで実現可能である。

【００５８】

なお、上記実施形態では、端末装置１００が入力されたユーザ名をサーバ３００に問い合わせ、その問い合わせを受けたサーバ３００が登録情報を用いて登録されたユーザ名と等しいか否かを判定する。そして、等しい場合には、サーバ３００は合致した旨の情報、即ち、その後の処理（端末装置１００固有の電話番号の表示）を行うための情報を端末装置１００に対して送出している。

【００５９】

しかしながら、ユーザ名と端末装置１００から送信されたユーザ名とがサーバ３００で合致した場合、サーバ３００が端末装置１００に対して登録されているユーザ名に対応する電話番号を端末装置１００に送信してもよい。

【００６０】

この場合、電話番号をサーバ３００から受け取った端末装置１００はその番号を所定の記憶領域に記憶しておく。その後、上記実施形態と同様に、端末装置１００の電話番号を

ユーザに表示し、当該電話番号に着信されたユーザの携帯電話番号を取得する。その後、取得した携帯電話番号とサーバ３００から送信され、記憶されていた登録電話番号とが一致するか否かを判定する。

【００６１】

判定の結果、記憶されていた登録電話番号と着信した電話番号が合致すれば、端末装置１００内においてユーザの認証に成功したと判断する。端末装置１００は認証が成功した旨をサーバ３００に通知することで、サーバ３００はこのユーザのログインを許可する。

【００６２】

本構成によれば、端末装置１００からサーバ３００へ着信した電話番号を通知し、サーバ３００で認証処理を行う必要がなくなるため、よりスムースかつ迅速にユーザの認証処理を実行できるようになる。

【００６３】

上記実施形態では、端末装置１００固有の電話番号をステップＳ３０６で表示し、ユーザはその電話番号に対して発呼する構成を採用した。しかしながら、端末装置１００が表示する電話番号をサーバ３００が有する電話番号とすることも可能である。

【００６４】

以下、その手順を示す。

【００６５】

まず、図３Ａのステップ３０１からＳ３０５までは上記実施形態と同等である。ステップＳ３０６において、表示する電話番号をサーバ３００固有の電話番号とする。なお、サーバ３００には公衆回線を利用した電話機能があることを前提とする。サーバ３００の電話番号は、予め端末装置１００に保持させているか、端末装置１００からユーザ名の照会が行われた際、サーバ３００から端末装置１００にサーバ３００の電話番号を送信してもよい。

【００６６】

続いて、ユーザは、Ｓ３０７において、画面の確認ボタンを押下し、端末装置１００の画面に表示されたサーバ３００の電話番号に発信する。端末装置１００は確認ボタンの押下を受け、サーバ１００に対して、ユーザが確認ボタンを押下した旨を通知する。通知を受けたサーバ１００はステップＳ３０８、Ｓ３０９、Ｓ３１０と同等の処理を実行する。

【００６７】

次に、サーバ３００は図３Ｂに示したステップＳ３３０において、着信したか否かを判定する。着信した場合はステップＳ３３１において電話番号を取得する。続いて、サーバ３００は、ステップＳ３３１で取得した電話番号と、予め登録され、ユーザ名と関連付けられていた電話番号が合致するか否かをステップＳ３３４で判定する。なお、ステップＳ３３３は本構成では省略される。

【００６８】

ステップＳ３３４において、合致したと判定された場合、サーバ３００は端末装置１００に対して、認証処理が成功した旨を通知するとともに、ユーザのログインを許可する。

【００６９】

その後、ステップＳ３３５では、上記実施形態と同様にユーザがサーバ３００に保持されたドキュメントなどを印刷出力する処理を可能とする。

【００７０】

以上、端末装置１００に表示させる電話番号をサーバ３００の電話番号とすることで、上記実施形態よりも認証処理に関する通信を簡略化でき、スムースかつ迅速にユーザの認証を行うことができる。

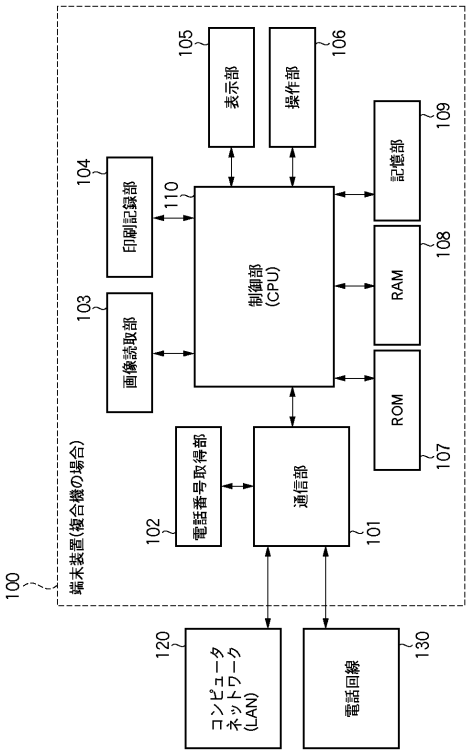
【００７１】

この変形例の特徴は、端末装置の表示部に、認証を行うサーバの電話番号を表示することにある。サーバの電話番号を表示するためには、ユーザが端末装置においてユーザ名を入力する必要がある。そのため、サーバはユーザが確実に端末装置の近傍に存在していることが判定できる。

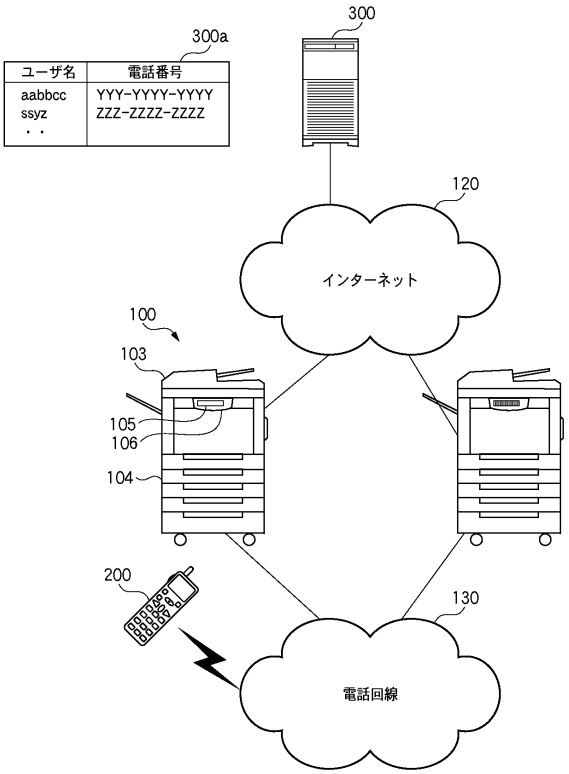
【００７２】
尚、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラム（実施形態では図に示すフローチャートに対応したプログラム）を、システムあるいは装置に直接あるいは遠隔から供給し、そのシステムあるいは装置のコンピュータが該供給されたプログラムコードを読み出して実行することによっても達成される場合を含む。
【００７３】
従って、本発明の機能処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明は、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。
【００７４】
その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等の形態であっても良い。
【００７５】
プログラムを供給するための記録媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などがある。
【００７６】
その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページから本発明のコンピュータプログラムそのもの、もしくは圧縮され自動インストール機能を含むファイルをハードディスク等の記録媒体にダウンロードすることによっても供給できる。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明に含まれるものである。
【００７７】
また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせ、その鍵情報を使用することにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。
【００７８】
また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される他、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現され得る。
【００７９】
さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現される。
【図面の簡単な説明】
【００８０】
【図１】実施形態による端末装置１００の内部構成例を示すブロック図である。
【図２】実施形態による端末装置、携帯電話、サーバの接続関係を概念的に説明する図である。
【図３Ａ】実施形態による認証処理を説明するフローチャートである。
【図３Ｂ】実施形態による認証処理を説明するフローチャートである。
【図４】実施形態によるオフフック処理を説明するフローチャートである。

【図５】回線確保の例の状態遷移図である。
【図６】実施形態の認証処理における画面表示例を示す図である。
【図７】予約処理を説明するフローチャートである。
【図８】予約処理における画面表示例を示す図である。
【図９】サーバ装置における認証処理を説明するフローチャートである。

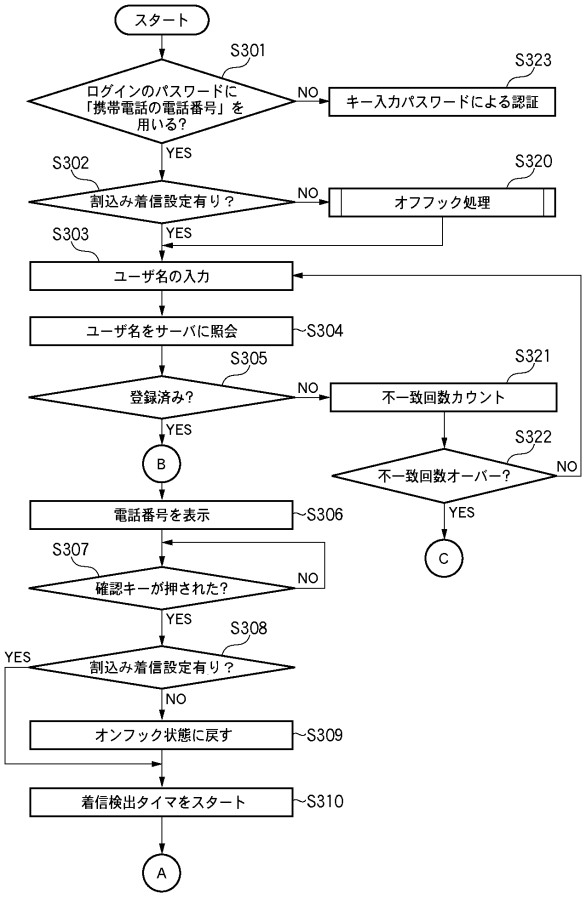
【図１】



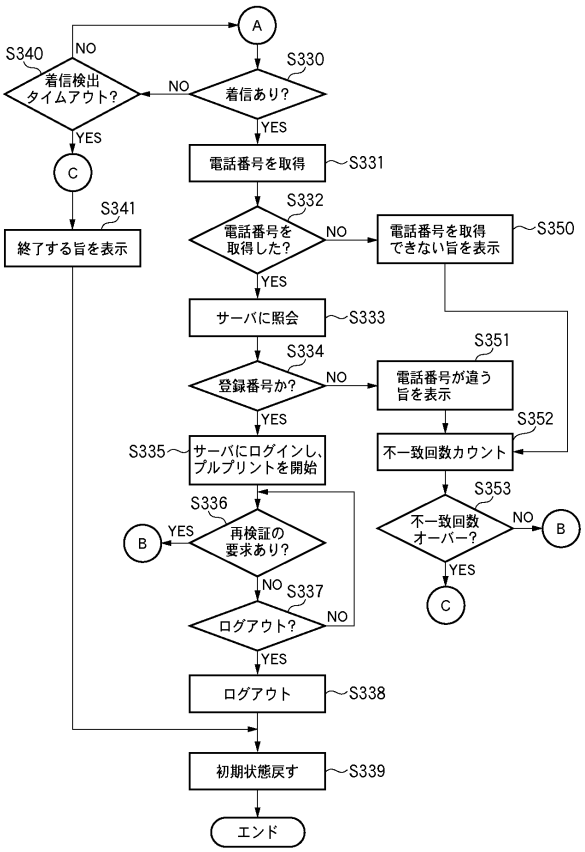
【図２】



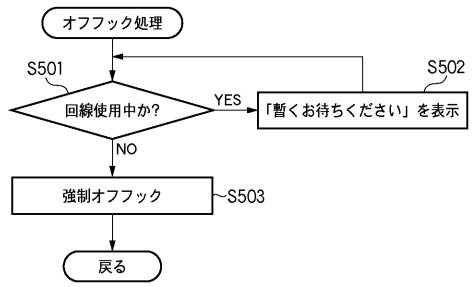
【図３Ａ】


スタート
S301
ログインのパスワードに「携帯電話の電話番号」を用いる?
NO
S323
キー入力パスワードによる認証
YES
S302
割込み着信設定有り？
NO
S320
オフフック処理
YES
S303
ユーザ名の入力
ユーザ名をサーバに照会
S304
S305
登録済み?
NO
S321
不一致回数カウント
YES
B
S322
不一致回数オーバー?
NO
YES
C
電話番号を表示
S306
S307
確認キーが押された?
NO
YES
S308
割込み着信設定有り？
YES
NO
オンフック状態に戻す
S309
着信検出タイマをスタート
S310
A

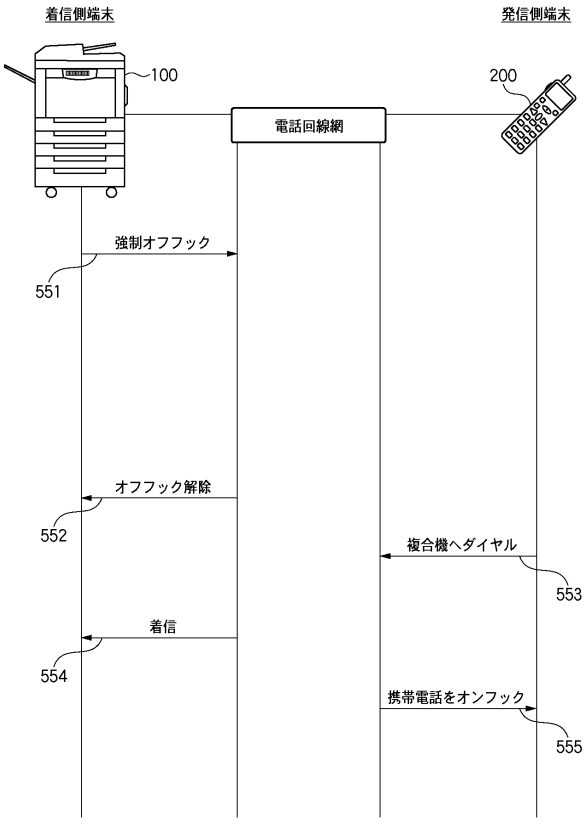
【図３Ｂ】


A
S340
NO
着信検出タイムアウト?
NO
S330
着信あり?
YES
YES
C
電話番号を取得
S331
S341
終了する旨を表示
S332
電話番号を取得した?
NO
電話番号を取得できない旨を表示
S350
YES
サーバに照会
S333
S334
登録番号か?
NO
S351
電話番号が違う旨を表示
YES
S335
サーバにログインし、プルプリントを開始
S352
不一致回数カウント
S336
B
YES
再検証の要求あり?
S353
不一致回数オーバー?
NO
B
NO
S337
ログアウト?
NO
YES
YES
C
ログアウト
S338
初期状態戻す
S339
エンド

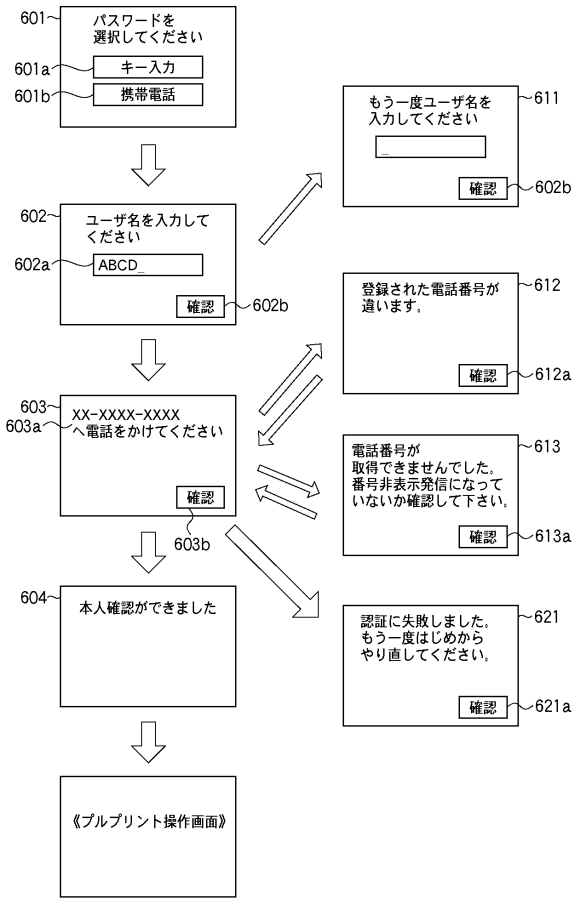
【図４】


オフフック処理
S501
回線使用中か?
YES
S502
「暫くお待ちください」を表示
NO
強制オフフック
S503
戻る

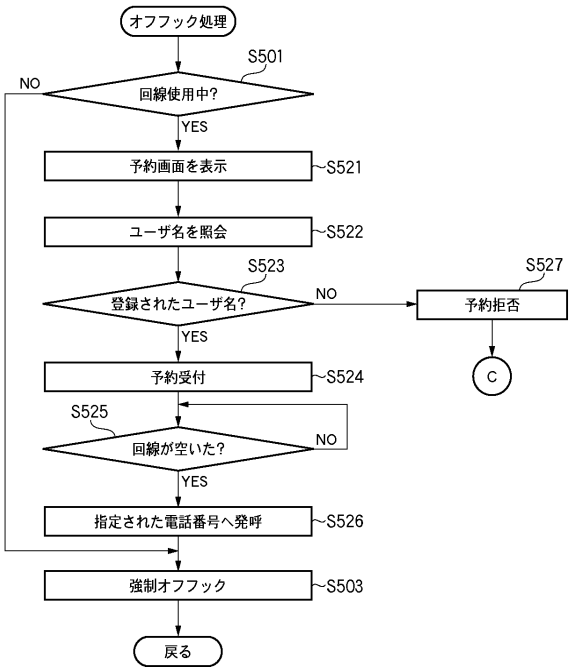
【図５】


着信側端末
発信側端末
100
200
電話回線網
強制オフフック
551
オフフック解除
552
複合機へダイヤル
553
着信
554
携帯電話をオンフック
555

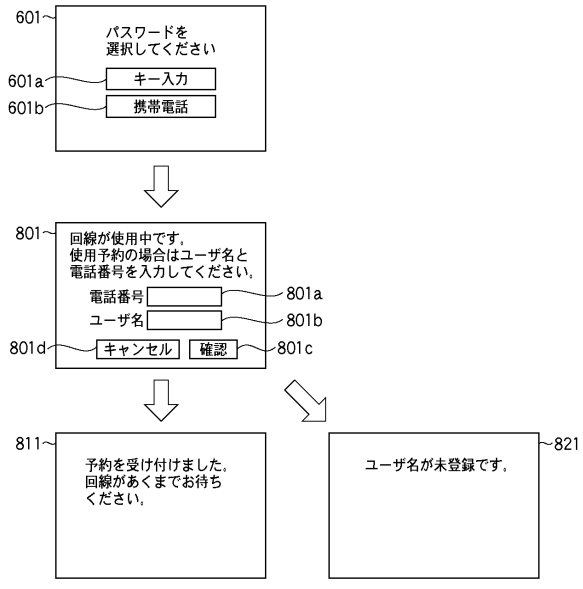
【図６】


601
パスワードを
選択してください
601a
キー入力
601b
携帯電話
602
ユーザ名を入力して
ください
602a
ABCD_
確認
602b
603
603a
XX-XXXX-XXXX
へ電話をかけてください
確認
603b
604
本人確認ができました
《プルプリント操作画面》
611
もう一度ユーザ名を
入力してください
確認
602b
612
登録された電話番号が
違います。
確認
612a
613
電話番号が
取得できませんでした。
番号非表示発信になって
いないか確認して下さい。
確認
613a
621
認証に失敗しました。
もう一度はじめから
やり直してください。
確認
621a

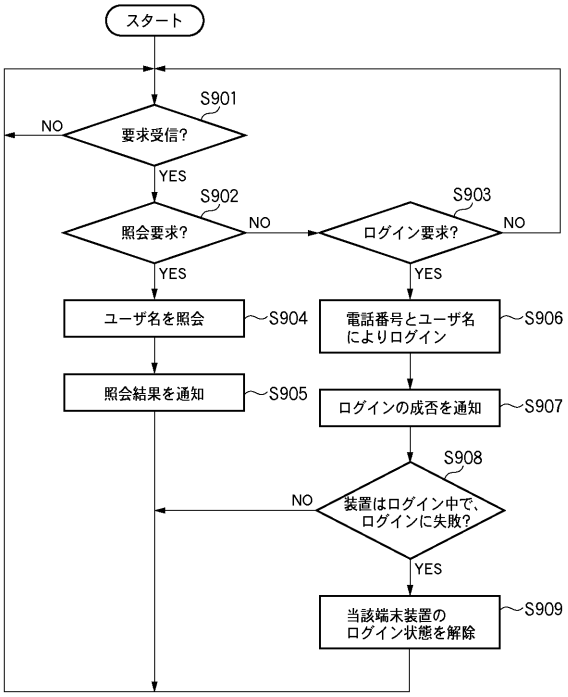
【図７】


オフフック処理
S501
回線使用中?
NO
YES
予約画面を表示
S521
ユーザ名を照会
S522
S523
登録されたユーザ名?
NO
S527
予約拒否
C
YES
予約受付
S524
S525
回線が空いた?
NO
YES
指定された電話番号へ発呼
S526
強制オフフック
S503
戻る

【図８】


601
パスワードを
選択してください
601a
キー入力
601b
携帯電話
801
回線が使用中です。
使用予約の場合はユーザ名と
電話番号を入力してください。
電話番号
801a
ユーザ名
801b
801d
キャンセル
確認
801c
811
予約を受け付けました。
回線があくまでお待ち
ください。
ユーザ名が未登録です。
821

【図９】


スタート
S901
要求受信?
NO
YES
S902
照会要求?
NO
YES
S903
ログイン要求?
NO
YES
ユーザ名を照会
S904
照会結果を通知
S905
電話番号とユーザ名
によりログイン
S906
ログインの成否を通知
S907
S908
装置はログイン中で、
ログインに失敗?
NO
YES
当該端末装置の
ログイン状態を解除
S909

フロントページの続き

審査官　平井　誠

(56)参考文献　特開２００２－０５５９５５（ＪＰ，Ａ）
特開２００５－０３８３０７（ＪＰ，Ａ）
特開２００３－２４８７８５（ＪＰ，Ａ）
特開２００５－０５６２９９（ＪＰ，Ａ）
特開２００１－２６８１６９（ＪＰ，Ａ）
特開２００５－００４４７２（ＪＰ，Ａ）
国際公開第０２／０３７３５８（WO，Ａ１）
米国特許出願公開第２００２／００５７７８０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０