(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-217524
(P2005-217524A)
(43)公開日　平成17年8月11日(2005.8.11)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04M 11/00	H04M 11/00	301	3E038
G07C 9/00	G07C 9/00	Z	5C087
G08B 25/00	G08B 25/00	510M	5K024
G08B 25/04	G08B 25/04	E	5K067
H04B 7/26	H04M 3/42	E	5K101

審査請求 未請求　請求項の数 13　OL　（全 39 頁）　最終頁に続く

(21)出願番号　特願2004-18679(P2004-18679)
(22)出願日　平成16年1月27日(2004.1.27)

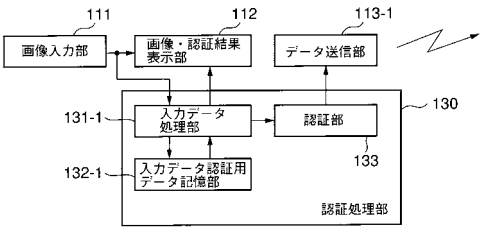
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103090
弁理士　岩壁　冬樹
(74)代理人　100114720
弁理士　須藤　浩
(72)発明者　渡辺　英樹
東京都港区芝五丁目７番１号　日本電気株式会社内

Fターム(参考)　3E038 AA01 AA11 BB05 CA06 HA07 JA01
5C087 BB03 DD05 DD06 EE07 EE14 FF01 FF02 FF23 GG02 GG10 GG18 GG20

最終頁に続く

(54)【発明の名称】セキュリティ管理システムおよびセキュリティ管理方法

(57)【要約】
【課題】　携帯電話機を用いたセキュリティ管理システムを構築する場合、携帯電話機において取得した画像等のデータをユーザ認証を行なうユーザ認証システム等に送信しなければならなかった。
【解決手段】　携帯電話機１００が備えた画像入力部１１１にユーザの顔の画像を入力し、ユーザの顔の画像データを生成する。入力データ処理部１３１－１は、予め入力データ認証用データ記憶部１３２－１が記憶している、登録された人物である許可者の顔の画像データとユーザの顔の画像データとを比較して、同一人物であると判定すると、パスワードの入力を要求し、ユーザが入力したパスワードと携帯電話機１００の電話番号との組み合わせをセキュリティ管理装置に送信する。セキュリティ管理装置では、受信したパスワードと電話番号とが、あらかじめ記憶しているパスワードと電話番号との組み合わせと合致すると、特定の場所に入退場するドアを開閉する。
【選択図】　図４



【特許請求の範囲】
【請求項１】
携帯電話機から受信した信号を用いてセキュリティ管理を行なうセキュリティ管理装置を備えたセキュリティ管理システムにおいて、
前記携帯電話機は、
所定の資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶する許可者固有データ記憶手段と、
携帯電話機の使用者の特徴を表すデータである使用者データを入力する使用者データ入力手段と、
前記使用者データと前記許可者固有データとを比較して、前記使用者と前記許可者とが同一人物であるか否か判断する判断手段と、
前記判断手段が、前記使用者と前記許可者とが同一人物であると判断すると、前記使用者と前記許可者とが同一人物であることを示す情報である認証情報を生成する認証手段と、
前記認証手段が生成した認証情報を前記セキュリティ管理装置に送信する認証情報送信手段とを含み、
前記セキュリティ管理装置は、
前記携帯電話機が送信した認証情報を受信する認証情報受信手段と、
前記許可者に関する情報である許可者情報を予め記憶する許可者情報記憶手段と、
前記認証情報受信手段が受信した前記認証情報と前記許可者情報記憶手段が記憶している許可者情報とが合致するか否か判断する認証結果処理手段とを含む
ことを特徴とするセキュリティ管理システム。
【請求項２】
携帯電話機から受信した信号を用いて、携帯電話機の使用者の特定の場所への入退場の管理を行なうセキュリティ管理システムであって、
セキュリティ管理装置は、認証結果処理手段が認証情報と許可者情報とが合致すると判断すると、携帯電話機の使用者に前記特定の場所への入場または前記特定の場所からの退場を許可する制御手段とを含む
請求項１記載のセキュリティ管理システム。
【請求項３】
携帯電話機は、
使用者がパスワードを入力する操作入力手段を含み、
認証手段が、使用者が前記操作入力手段に入力したパスワードと、携帯電話機の電話番号とを含む認証情報を生成する
請求項２記載のセキュリティ管理システム。
【請求項４】
制御手段は、特定の場所の出入り口のドアの開閉を制御する
請求項２または請求項３記載のセキュリティ管理システム。
【請求項５】
制御手段は、特定の場所の出入り口のドアの開錠と施錠と制御する
請求項２または請求項３記載のセキュリティ管理システム。
【請求項６】
携帯電話機からデータ処理装置へのアクセスの管理を行なう身元確認システムとを備えたセキュリティ管理システムにおいて、
前記携帯電話機は、
アクセス資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶する許可者固有データ記憶手段と、
携帯電話機の使用者の特徴を表すデータである使用者データを入力する使用者データ入力手段と、
前記使用者データと前記許可者固有データとを比較して、前記使用者と前記許可者とが

同一人物であるか否か判断する判断手段と、
前記判断手段が、前記使用者と前記許可者とが同一人物であると判断すると、前記使用者と前記許可者とが同一人物であることを示す情報である認証情報を生成する認証手段と、
前記認証手段が生成した認証情報を無線通信回線を介して前記身元確認システムに送信する認証情報送信手段とを含み、
前記身元確認システムは、
前記携帯電話機が送信した認証情報を受信する認証情報受信手段と、
前記許可者に関する情報である許可者情報を予め記憶する許可者情報記憶手段と、
前記認証情報受信手段が受信した前記認証情報と前記許可者情報記憶手段が記憶している許可者情報とが合致するか否か判断する認証結果処理手段と、
前記認証結果処理手段が、前記認証情報と前記許可者情報とが合致すると判断すると、前記携帯電話機に、前記データ処理装置へのアクセスを許可する制御手段とを含む
ことを特徴とするセキュリティ管理システム。
【請求項７】
許可者固有データ記憶手段は、許可者固有データとして、許可者の顔の画像のデータを記憶し、
使用者データ入力手段は、使用者データとして、撮影された使用者の顔の画像のデータを入力する
請求項１から請求項６のうちいずれか１項記載のセキュリティ管理システム。
【請求項８】
許可者固有データ記憶手段は、許可者固有データとして、許可者の音声のデータを記憶し、
使用者データ入力手段は、使用者データとして、使用者の音声のデータを入力する
請求項１から請求項７のうちいずれか１項記載のセキュリティ管理システム。
【請求項９】
許可者固有データ記憶手段は、許可者固有データとして、許可者の指紋の画像のデータを記憶し、
使用者データ入力手段は、使用者データとして、使用者の指紋の画像のデータを入力する
請求項１から請求項８のうちいずれか１項記載のセキュリティ管理システム。
【請求項１０】
携帯電話機とセキュリティ管理装置とが共働してセキュリティ管理を行なうセキュリティ管理方法において、
前記携帯電話機は、
所定の資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶し、
携帯電話機の使用者の特徴を表すデータである使用者データを入力し、
前記使用者データと前記許可者固有データとを比較して、前記使用者と前記許可者とが同一人物であるか否か判断し、
前記使用者と前記許可者とが同一人物であると判断した場合に、前記使用者と前記許可者とが同一人物であることを示す情報である認証情報を生成し、
生成した前記認証情報を前記セキュリティ管理装置に送信し、
前記セキュリティ管理装置は、
前記許可者に関する情報である許可者情報を予め記憶し、
前記携帯電話機が送信した認証情報を受信し、
受信した前記認証情報と記憶している許可者情報とが合致するか否か判断する
ことを特徴とするセキュリティ管理方法。
【請求項１１】
携帯電話機とセキュリティ管理装置とが共働して、携帯電話機の使用者の特定の場所へ

の入退場の管理を行なうセキュリティ管理方法であって、
セキュリティ管理装置は、認証情報と許可者情報とが合致すると判断すると、携帯電話機の使用者に前記特定の場所への入場または前記特定の場所からの退場を許可する
請求項１０記載のセキュリティ管理方法。
【請求項１２】
携帯電話機は、
パスワードを入力し、
入力したパスワードと携帯電話機の電話番号とを含む認証情報を生成する
請求項１０または請求項１１記載のセキュリティ管理方法。
【請求項１３】
携帯電話機と身元確認システムとが共働して、携帯電話機からデータ処理装置へのアクセスの管理を行なうセキュリティ管理方法であって、
アクセス資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶し、
携帯電話機の使用者の特徴を表すデータである使用者データを入力し、
前記使用者データと前記許可者固有データとを比較して、前記使用者と前記許可者とが同一人物であるか否か判断し、
前記使用者と前記許可者とが同一人物であると判断すると、前記使用者と前記許可者とが同一人物であることを示す情報である認証情報を生成し、
生成した前記認証情報を無線通信回線を介して前記身元確認システムに送信し、
前記身元確認システムは、
前記許可者に関する情報である許可者情報を予め記憶し、
前記携帯電話機が送信した認証情報を受信し、
受信した前記認証情報と記憶している許可者情報とが合致するか否か判断し、
前記認証情報と前記許可者情報とが合致すると判断した場合に、前記携帯電話機に、前記データ処理装置へのアクセスを許可する
ことを特徴とするセキュリティ管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、携帯電話機が取得した人物を特定する情報を用いて人物を認識するセキュリティ管理システムおよびセキュリティ管理方法に関する。
【背景技術】
【０００２】
携帯電話機を用いたセキュリティ管理システムを構築する場合、携帯電話機の使用者がセキュリティ管理システムに登録されている人物（携帯電話機の所有者）であるか否かを特定することは困難である。
【０００３】
携帯電話機を用いたセキュリティ管理システムとして、例えば、特許文献１に記載されている認証システムがある。その認証システムでは、携帯電話通信網等の通信回線網に接続された認証サーバを設置し、画像撮影機能付き携帯電話機で人物を特定する画像（例えば、顔の画像。）を撮影し、撮影した画像の画像データを通信回線網を介して認証サーバに送信する。そして、認証サーバが、予め記憶している画像データと受信した画像データとを比較して、携帯電話機のユーザに通信回線網に接続された他のシステムの操作を許可するか否かを決定する。
【０００４】
また、画像を利用したセキュリティ管理システムとして、例えば、特許文献２に記載されている入退室管理システムがある。その入退室管理システムでは、入退室の管理を行なう部屋の入退室口で入退室しようとしている人物の画像を撮影し、撮影した画像データと、予めデータベースが記憶している画像データとを警備員が比較して、警備員が入退室し

ようとしている人物を入退室させるか否かを判断する。
【０００５】
【特許文献１】特開２００１－３０６５１７号公報　（第４－６頁、第１図）
【特許文献２】特開平９－３１９８７７号公報　（第３－５頁、第１図）
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかし、特許文献１に記載されている認証システムでは、通信回線網に接続された認証サーバを設置する必要があるため、コストがかかる。また、携帯電話機は撮影した画像データを通信回線網を介して認証サーバに送信するが、画像データは一般にデータ量が大きく、携帯電話機および通信回線網に負荷がかかる。さらに、認証サーバは、予め記憶している画像データと受信した画像データとを比較する画像データ処理を行なうが、画像データ処理に時間がかかってしまう。
【０００７】
また、特許文献２に記載されている入退室管理システムでは、予め画像データを含むデータベースを記憶する制御端末を設置する必要があり、さらに、入退室しようとしている人物を入退室させるか否かを判断する警備員を常駐させる必要もあり、コストがかかる。
【０００８】
そこで、本発明は、予め画像データを記憶したり、予め記憶している画像データと携帯電話機が撮影した画像データとを比較したりするサーバや警備員等を用いずに、携帯電話機のユーザを特定して人物認証を行なうセキュリティ管理システムおよびセキュリティ管理方法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】
【０００９】
本発明によるセキュリティ管理システムは、携帯電話機から受信した信号を用いてセキュリティ管理を行なうセキュリティ管理装置を備えたセキュリティ管理システムであって、携帯電話機が、所定の資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶する許可者固有データ記憶手段と、携帯電話機の使用者の特徴を表すデータである使用者データを入力する使用者データ入力手段と、使用者データと許可者固有データとを比較して、使用者と許可者とが同一人物であるか否か判断する判断手段と、判断手段が、使用者と許可者とが同一人物であると判断すると、使用者と許可者とが同一人物であることを示す情報である認証情報を生成する認証手段と、認証手段が生成した認証情報をセキュリティ管理装置に送信する認証情報送信手段とを含み、セキュリティ管理装置が、携帯電話機が送信した認証情報を受信する認証情報受信手段と、許可者に関する情報である許可者情報を予め記憶する許可者情報記憶手段と、認証情報受信手段が受信した認証情報と許可者情報記憶手段が記憶している許可者情報とが合致するか否か判断する認証結果処理手段とを含むことを特徴とする。
【００１０】
セキュリティ管理システムは、携帯電話機から受信した信号を用いて、携帯電話機の使用者の特定の場所への入退場の管理を行なうセキュリティ管理システムであって、セキュリティ管理装置が、認証結果処理手段が認証情報と許可者情報とが合致すると判断すると、携帯電話機の使用者に特定の場所への入場または特定の場所からの退場を許可する制御手段とを含むように構成されていてもよい。
【００１１】
携帯電話機が、使用者がパスワードを入力する操作入力手段を含み、認証手段が、使用者が操作入力手段に入力したパスワードと携帯電話機の電話番号とを含む認証情報を生成するように構成されていてもよい。そのような構成によれば、より厳密にユーザ認証を行なうことができる。
【００１２】
制御手段は、特定の場所の出入り口のドアの開閉を制御してもよい。そのような構成に

よれば、特定の場所への入場および特定の場所からの退場をすることができる人物を、許可者に限定することができる。

【００１３】

制御手段は、特定の場所の出入り口のドアの開錠と施錠とを制御してもよい。そのような構成によれば、特定の場所の出入り口のドアが自動ドアでなくても、特定の場所への入場および特定の場所からの退場をすることができる人物を、許可者に限定することができる。

【００１４】

本発明による他の態様のセキュリティ管理システムは、携帯電話機からデータ処理装置へのアクセスの管理を行なう身元確認システムとを備えたセキュリティ管理システムであって、携帯電話機が、アクセス資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶する許可者固有データ記憶手段と、携帯電話機の使用者の特徴を表すデータである使用者データを入力する使用者データ入力手段と、使用者データと許可者固有データとを比較して、使用者と許可者とが同一人物であるか否か判断する判断手段と、判断手段が使用者と許可者とが同一人物であると判断すると、使用者と許可者とが同一人物であることを示す情報である認証情報を生成する認証手段と、認証手段が生成した認証情報を無線通信回線を介して身元確認システムに送信する認証情報送信手段とを含み、身元確認システムが、携帯電話機が送信した認証情報を受信する認証情報受信手段と、許可者に関する情報である許可者情報を予め記憶する許可者情報記憶手段と、認証情報受信手段が受信した認証情報と許可者情報記憶手段が記憶している許可者情報とが合致するか否か判断する認証結果処理手段と、認証結果処理手段が、認証情報と許可者情報とが合致すると判断すると、携帯電話機に、データ処理装置へのアクセスを許可する制御手段とを含むことを特徴とする。

【００１５】

許可者固有データ記憶手段が、許可者固有データとして許可者の顔の画像のデータを記憶し、使用者データ入力手段が、使用者データとして、撮影された使用者の顔の画像のデータを入力するように構成されていてもよい。そのような構成によれば、ユーザの顔の画像のデータを用いて、ユーザが許可者であるか否かを判断することができる。

【００１６】

許可者固有データ記憶手段が、許可者固有データとして許可者の音声のデータを記憶し、使用者データ入力手段が、使用者データとして使用者の音声のデータを入力するように構成されていてもよい。そのような構成によれば、ユーザの音声のデータを用いて、ユーザが許可者であるか否かを判断することができる。

【００１７】

許可者固有データ記憶手段が、許可者固有データとして許可者の指紋の画像のデータを記憶し、使用者データ入力手段が、使用者データとして使用者の指紋の画像のデータを入力するように構成されていてもよい。そのような構成によれば、ユーザの指紋の画像のデータを用いて、ユーザが許可者であるか否かを判断することができる。

【００１８】

本発明によるセキュリティ管理方法は、携帯電話機とセキュリティ管理装置とが共働してセキュリティ管理を行なうセキュリティ管理方法であって、携帯電話機が、所定の資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶し、携帯電話機の使用者の特徴を表すデータである使用者データを入力し、使用者データと許可者固有データとを比較して使用者と許可者とが同一人物であるか否か判断し、使用者と許可者とが同一人物であると判断した場合に、使用者と許可者とが同一人物であることを示す情報である認証情報を生成し、生成した認証情報をセキュリティ管理装置に送信し、セキュリティ管理装置が、許可者に関する情報である許可者情報を予め記憶し、携帯電話機が送信した認証情報を受信し、受信した認証情報と記憶している許可者情報とが合致するか否か判断することを特徴とする。

【００１９】

セキュリティ管理方法は、携帯電話機とセキュリティ管理装置とが共働して、携帯電話機の使用者の特定の場所への入退場の管理を行なうセキュリティ管理方法であって、セキュリティ管理装置が、認証情報と許可者情報とが合致すると判断すると、携帯電話機の使用者に特定の場所への入場または特定の場所からの退場を許可するように構成されていてもよい。

【００２０】

携帯電話機が、パスワードを入力し、入力したパスワードと携帯電話機の電話番号とを含む認証情報を生成するように構成されていてもよい。そのような方法によれば、より厳密にユーザ認証を行なうことができる。

【００２１】

本発明による他の態様のセキュリティ管理方法は、携帯電話機と身元確認システムとが共働して、携帯電話機からデータ処理装置へのアクセスの管理を行なうセキュリティ管理方法であって、アクセス資格を有する人物である許可者に関する固有のデータである許可者固有データを記憶し、携帯電話機の使用者の特徴を表すデータである使用者データを入力し、使用者データと許可者固有データとを比較して使用者と許可者とが同一人物であるか否か判断し、使用者と許可者とが同一人物であると判断すると、使用者と許可者とが同一人物であることを示す情報である認証情報を生成し、生成した認証情報を無線通信回線を介して身元確認システムに送信し、身元確認システムが、許可者に関する情報である許可者情報を予め記憶し、携帯電話機が送信した認証情報を受信し、受信した認証情報と記憶している許可者情報とが合致するか否か判断し、認証情報と許可者情報とが合致すると判断した場合に、携帯電話機に、データ処理装置へのアクセスを許可することを特徴とする。

【発明の効果】

【００２２】

本発明によれば、携帯電話機の用いて携帯電話機のユーザを特定し、安価で簡易なセキュリティ管理システムを提供することができる。

【発明を実施するための最良の形態】

【００２３】

実施の形態１．

本発明の第１の実施の形態を図面を参照して説明する。図１は、本発明による携帯電話機１００の外観の一例を示す説明図である。なお、図１（ａ）は、携帯電話機１００を閉じた状態の外観を示す説明図であり、図１（ｂ）は携帯電話機１００を開いた状態を示す説明図である。

【００２４】

本発明による携帯電話機１００は、上部筐体部１０と下部筐体部２０とがヒンジによって接続されて構成され、上部筐体部１０は、情報を表示する第１の表示部１１、アナログの電気信号である音声出力信号を音声に変換して出力するスピーカ１２、情報を表示する第２の表示部１３、画像を撮影するカメラ１４、および電波を送受信するアンテナ１５を含み、下部筐体部２０は、携帯電話機１００のユーザが情報を入力する操作部２１、入力した音声をアナログの電気信号である音声入力信号に変換するマイクロフォン２２、および携帯電話機１００のユーザがカメラ１４を用いて画像を撮影する指示を入力するボタンであるシャッターボタン２３を含む。

【００２５】

第１の表示部１１および第２の表示部１３は、例えば、ＬＣＤ（液晶ディスプレイ）によって実現される。

【００２６】

図２は、本発明の第１の実施の形態によるセキュリティ管理システムの構成を示す説明図である。本発明の第１の実施の形態によるセキュリティ管理システムは、携帯電話機１００と、携帯電話機１００が送信した情報を受信する無線受信部５を含むセキュリティ管理装置と、セキュリティ管理装置の制御に応じて開閉または開錠・施錠するセキュリティ

管理ドア２００とを含む。なお、ここでは、セキュリティ管理システムとして、ドア内への入退場資格を有する利用者のみの入退場が許可されるシステムを例示するが、本発明によるセキュリティ管理システムの応用は、そのような場合に限られない。

【００２７】

図３は、本発明の第１の実施の形態による携帯電話機１００の構成を説明するブロック図である。本発明の第１の実施の形態による携帯電話機１００は、スピーカ１２、アンテナ１５、マイクロフォン２２、アンテナ１５が受信した無線周波数信号を入力して周波数変換し、さらに音声信号またはデータ信号に復調する無線通信部３０、無線通信部３０が出力した音声信号（デジタル信号）を音声出力信号（アナログ信号）に変換してスピーカ１２に出力し、マイクロフォン２２から入力した音声入力信号（アナログ信号）を音声信号に変換する音声処理回路３１－１、携帯電話機１００の全体の各部を制御する携帯電話機主制御部３２－１、特定の場所への入場および特定の場所からの退場を許可するべき人物である許可者の特徴の情報である許可者特徴情報と携帯電話機１００の電話番号とを予め記憶する記憶部３３－１、ブルートゥース（登録商標）規格にもとづいて無線信号を送受信し、ブルートゥース用アンテナ（図示せず）を含むブルートゥース回路３４、操作部２１とシャッターボタン２３とに入力された情報を携帯電話機主制御部３２－１に出力する操作入力部（操作入力手段）３５、携帯電話機主制御部３２－１の制御にもとづいて情報を表示する第１の表示部１１および第２の表示部を含む表示部３６、外部機器とデータを送受信するデータ入出力インタフェース３７、外部機器と接続する接続コネクタ３８、およびＣＣＤ（Ｃｈａｒｇｅ Ｃｏｕｐｌｅｄ Ｄｅｖｉｃｅ）カメラまたはＣＭＯＳ（Ｃｏｍｐｒｅｍｅｎｔａｒｙ Ｍｅｔａｌ Ｏｘｉｄｅ Ｓｅｍｉｃｏｎｄｕｃｔｏｒ）カメラであるカメラ１４と、カメラ１４が撮影した画像の画像入力信号（アナログ信号）を画像信号（デジタル信号）に変換して画像データを生成し携帯電話機主制御部３２－１に出力するカメラユニット３９を含む。

【００２８】

無線通信部３０は、音声処理回路３１－１から音声信号を入力し、携帯電話機主制御部３２－１からデータ信号を入力し、入力した各信号を変調して無線周波数信号に変換し、アンテナ１５に出力する。携帯電話機主制御部３２－１は、例えば、ＭＰＵ（Ｍｉｃｒｏ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）によって実現される。記憶部３３－１は、例えば、フラッシュＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）によって実現される。なお、本発明の第１の実施の形態による携帯電話機１００は、ブルートゥース回路３４を含んでいるが、本発明は、これに限定されるものではなく、セキュリティ管理装置と無線通信することができる回路であれば、ＩｒＤＡ回路（赤外線通信回路）や、その他の無線通信回路であってもよい。また、カメラユニット３９は、ＪＰＥＧ（Ｊｏｉｎｔ Ｐｈｏｔｏｇｒａｐｈｉｃ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）符号化機能や、ＭＰＥＧ（Ｍｏｔｉｏｎ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）符号化機能を含んでいてもよい。また、記憶部３３－１は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。

【００２９】

なお、ここでは、近距離通信によって携帯電話機からセキュリティ管理装置に所定の信号が送信される場合を例にして説明を行うが、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるようにセキュリティ管理システムが構成されていてもよい。

【００３０】

また、本発明の第１の実施の形態による携帯電話機１００の記憶部３３－１が記憶している許可者特徴情報は、許可者の顔の画像データである。そして、携帯電話機主制御部３２－１は、カメラユニット３９が生成した画像データと、記憶部３３－１が記憶している許可者の顔の画像データとをマッチングする認証処理を行ない、携帯電話機１００のユーザが許可者であるか否かを判定する。

【００３１】

次に、本発明の第１の実施の形態による携帯電話機１００において、本発明の第１の実

施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成について説明する。図４は、本発明の第１の実施の形態による携帯電話機１００において、本発明の第１の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【００３２】

本発明の第１の実施の形態による携帯電話機１００において、本発明の第１の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成は、ユーザの顔を撮影して撮影した画像の画像データを生成する画像入力部（使用者データを入力する使用者データ入力手段）１１１、画像および情報を表示する画像・認証結果表示部１１２、ユーザ認証を行ない、ユーザ（使用者）が許可者であるか否かを判定する認証処理部１３０と、認証処理部１３０が出力した情報をセキュリティ管理装置に送信するデータ送信部（認証情報送信手段）１１３－１とを含む。また、認証処理部１３０は、予め許可者の顔の画像データを記憶する入力データ認証用データ記憶部（許可者固有データ記憶手段）１３２－１と、画像入力部１１１が生成した画像データと入力データ認証用データ記憶部１３２－１が記憶している画像データとをマッチングする認証処理を行ない、ユーザと許可者とが同一人物であるか否かを判定し、同一人物であると判定すると、ユーザにパスワードの入力を要求するメッセージを画像・認証結果表示部１１２に表示させる入力データ処理部（判断手段、認証手段）１３１－１と、入力データ処理部１３１－１がユーザと許可者とが同一人物であると判定すると、記憶部３３－１が予め記憶している携帯電話機１００の電話番号と、ユーザと許可者とが同一人物であることを示す情報と、ユーザが入力したパスワードとを組み合わせた情報である認証情報をデータ送信部１１３－１に出力する認証部１３３とを含む。なお、画像入力部１１１が入力したユーザの顔の画像は、携帯電話機の使用者の特徴を表すデータである使用者データの一例である。

【００３３】

画像入力部１１１は、カメラユニット３９によって実現される。画像・認証結果表示部１１２は、表示部３６によって実現される。データ送信部１１３－１は、ブルートゥース回路３４によって実現される。入力データ認証用データ記憶部１３２－１は、記憶部３３－１によって実現される。入力データ処理部１３１－１と認証部１３３とは、携帯電話機主制御部３２－１によって実現される。なお、セキュリティ管理システムが、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成されている場合には、データ送信部１１３－１は、無線通信部３０およびアンテナ１５で実現される。また、その場合には、ブルートゥース回路３４は不要である。

【００３４】

図５は、本発明の第１の実施の形態によるセキュリティ管理装置の構成を説明するブロック図である。

【００３５】

本発明の第１の実施の形態によるセキュリティ管理装置は、ブルートゥース規格にもとづいて携帯電話機１００のブルートゥース回路３４と無線信号を送受信し、無線受信部５であるブルートゥース用アンテナを含むブルートゥース回路５１、セキュリティ管理装置全体を制御するセキュリティ管理装置主制御部４０、セキュリティ管理装置主制御部４０の制御にもとづいてセキュリティ管理ドア２００の開閉を制御するセキュリティ管理ドア制御部５２、および特定の場所の出入り口に設置されているセキュリティ管理ドア２００を含む。そして、セキュリティ管理装置主制御部４０は、セキュリティ管理装置を制御するプログラムを記憶するプログラム記憶部４２、予め許可者の情報を記憶するデータ記憶部４３、セキュリティ管理装置主制御部４０の全体を制御する中央処理装置４１、およびセキュリティ管理ドア制御部５２と情報の送受信を行なう入出力インタフェース４４を含む。

【００３６】

なお、本発明の第１の実施の形態によるセキュリティ管理装置は、ブルートゥース回路５１を含んでいるが、本発明は、これに限定されるものではなく、携帯電話機１００と無

線通信することができる回路であれば、ＩｒＤＡ回路（赤外線通信回路）や、その他の無線通信回路であってもよい。セキュリティ管理ドア制御部５２は、セキュリティ管理ドア２００を開閉させるモータを含んでもよいし、セキュリティ管理ドア２００が自動ドアでない場合は、セキュリティ管理ドア２００を施錠および開錠するためのアクチュエータ（例えばソレノイド）を含んでもよい。また、データ記憶部４３は、各許可者の携帯電話機の電話番号とパスワードとを予め対応付けて認証データとして記憶している。

【００３７】

また、セキュリティ管理システムが、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成されている場合には、ブルートゥース回路５１は不要である。そして、セキュリティ管理装置は、例えば、携帯電話通信網を含む公衆回線網またはＩＰ通信網を介して、携帯電話機から所定の信号を受信する。また、その場合には、一般に、セキュリティ管理ドア制御部５２およびセキュリティ管理ドア２００はセキュリティ管理装置から離れた場所に設置されるので、セキュリティ管理装置とセキュリティ管理ドア制御部５２とは、公衆電話網やＩＰ通信網で接続される。

【００３８】

本発明の第１の実施の形態によるセキュリティ管理装置において、本発明の第１の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成について説明する。図６は、本発明の第１の実施の形態によるセキュリティ管理装置において、本発明の第１の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成を示すブロック図である。

【００３９】

本発明の第１の実施の形態によるセキュリティ管理装置において、本発明の第１の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成は、携帯電話機１００から情報を受信するデータ受信部（認証情報受信手段）２１３と、データ受信部２１３が受信した情報にもとづいてセキュリティ管理ドア２００を開閉または開錠・施錠する認証結果処理部２３０とを含む。認証結果処理部２３０は、許可者の携帯電話機の電話番号の情報と、パスワードとを予め対応付けて認証データとして記憶している受信データ認証用データ記憶部（許可者情報記憶手段）２３１と、データ受信部２１３が受信した情報と、受信データ認証用データ記憶部２３１が記憶している認証データとが合致するか否かを判断する受信データ処理部（認証結果処理手段）２３２と、受信データ処理部２３２が、データ受信部２１３が受信した情報と、受信データ認証用データ記憶部２３１が記憶している認証データとが合致すると判断すると、セキュリティ管理ドア２００を開閉または開錠・施錠する制御部（制御手段）２３３とを含む。

【００４０】

データ受信部２１３は、ブルートゥース回路５１によって実現される。受信データ認証用データ記憶部２３１は、データ記憶部４３によって実現される。制御部２３３は、中央処理装置４１と入出力インタフェース４４とセキュリティドア制御部５２とによって実現される。セキュリティ管理システムが、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成されている場合には、データ受信部２１３として、公衆電話網やＩＰ通信網を接続するためのインタフェースが用いられる。

【００４１】

次に、本発明の第１の実施の形態の動作について図面を参照して説明する。まず、本発明の第１の実施の形態における携帯電話機１００の動作について説明する。図７は、本発明の第１の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【００４２】

まず、携帯電話機１００の画像入力部１１１が、ユーザの顔を撮影して画像データを生成し、生成した画像データを画像・認証結果表示部１１２と入力データ処理部１３１－１とに出力する（ステップＳ１０１）。画像・認証結果表示部１１２は、入力された画像データの画像を表示する。

【００４３】
入力データ処理部１３１－１は、入力されたユーザの顔の画像データと、入力データ認証用データ記憶部１３２－１が記憶している許可者の顔の画像データとをマッチングする認証処理を行ない（ステップＳ１０２）、携帯電話機１００のユーザが許可者であるか否かを判定する。マッチングする方法は、例えば、テンプレートマッチング等の既知のマッチング方法を用いる。なお、許可者の顔の画像データは、携帯電話機の契約時等に予め入力データ認証用データ記憶部１３２－１に記憶させておく。例えば、画像入力部１１１が許可者の顔を撮影して、許可者の顔の画像データを生成し、入力データ処理部１３１－１が入力データ認証用データ記憶部１３２－１に、画像入力部１１１が生成した画像データを記憶させてもよいし、接続コネクタ３８に接続された警備保障会社の外部機器から、接続コネクタ３８とデータ入出力インタフェース３７とを介して許可者の顔の画像データを入力データ処理部１３１－１に入力し、入力データ処理部１３１－１が入力データ認証用データ記憶部１３２－１に、入力された画像データを記憶させてもよい。また、同様の方法で、入力データ認証用データ記憶部１３２－１が記憶する画像データを変更してもよい。また、許可者は複数であってもよい。従って、入力データ認証用データ記憶部１３２－１が記憶する許可者の顔の画像データは、複数の許可者のそれぞれの顔の画像データであってもよい。

【００４４】
入力データ処理部１３１－１は、認証処理の結果、携帯電話機１００のユーザが許可者であるか否かを画像・認証結果表示部１１２に表示させる（ステップＳ１０３）。入力データ処理部１３１－１は、ユーザが許可者であると判定すると（ステップＳ１０４）、ユーザにパスワードの入力を要求する画面を画像・認証結果表示部１１２に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－１に出力する。なお、入力データ処理部１３１－１は、記憶部３３－１が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－１は、携帯電話機１００の電話番号を示す情報と、ユーザが許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を認証部１３３に入力し、認証部１３３は、入力された認証情報をデータ送信部１１３－１に出力し、データ送信部１１３－１に、データ受信部２１３へ認証情報を送信させる（ステップＳ１０５）。

【００４５】
入力データ処理部１３１－１は、ユーザが許可者でないと判定すると（ステップＳ１０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ１０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【００４６】
次に、本発明の第１の実施の形態におけるセキュリティ管理装置の動作について説明する。図８は、本発明の第１の実施の形態におけるセキュリティ管理装置の動作を説明するフローチャートである。

【００４７】
データ受信部２１３が認証情報を受信すると（ステップＳ１１０）、受信した認証情報を認証結果処理部２３０の受信データ処理部２３２に出力する。受信データ処理部２３２は、受信した認証情報に含まれている電話番号の情報とパスワードとの組み合わせが、受信データ認証用データ記憶部２３１が予め対応付けて記憶している電話番号の情報とパスワードとである認証データに含まれているか否かを判定する（ステップＳ１１１）。

【００４８】
受信データ処理部２３２は、受信した認証情報に含まれている電話番号の情報とパスワードとの組み合わせが、受信データ認証用データ記憶部２３１が予め対応付けて記憶している電話番号の情報とパスワードとである認証データに含まれていると判定すると、ユーザに特定の場所への入場および特定の場所からの退場を許可し（ステップＳ１１２）、制御部２３３を介して、セキュリティ管理ドア２００を開ける、またはセキュリティ管理ド

アを開錠する。すると、ユーザは、特定の場所への入場および特定の場所からの退場をすることができる。なお、制御部２３３は、所定の時間経過後、セキュリティ管理ドア２００を閉じる、または施錠する。受信データ処理部２３２は、受信した認証情報に含まれている電話番号の情報とパスワードとの組み合わせが、受信データ認証用データ記憶部２３１が予め対応付けて記憶している電話番号の情報とパスワードとである認証データに含まれていないと判定すると、ユーザに特定の場所への入場および特定の場所からの退場を許可しない（ステップＳ１１３）。従って、セキュリティ管理ドア２００を開けない、またはセキュリティ管理ドア２００を開錠しない。すると、ユーザは、特定の場所への入場および特定の場所からの退場をすることができない。

【００４９】

以上、述べたように、この実施の形態によれば、ユーザの顔の画像データをセキュリティ管理装置に送信することなく、特定の場所への入場および特定の場所からの退場を許可するべき人物に、特定の場所への入場および特定の場所からの退場を許可することができる。従って、ユーザが認証のための操作を開始してから短時間でセキュリティ管理ドア２００を開けることができる。

【００５０】

また、セキュリティ管理システムが、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成されている場合には、セキュリティ管理ドア２００等のセキュリティ管理対象物から離れた場所に認証結果処理部２３０を設置することができる。従って、多数箇所に存在する多数のセキュリティ管理対象物を１つの認証結果処理部２３０で制御できる。

【００５１】

実施の形態２．

次に、本発明の第２の実施の形態を説明する。第２の実施の形態のセキュリティ管理システムの構成は、第１の実施の形態の構成と同様である。そのため、第１の実施の形態と同様の装置等については図２と同じ符号を付し、説明を省略する。

【００５２】

本発明による第２の実施の形態の携帯電話機１００の構成は、カメラユニット３９を含まない点が第１の実施の形態と異なり、その他の構成は第１の実施の形態と同様である。ただし、音声処理回路３１－２、携帯電話機主制御部３２－２および記憶部３３－２の動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等については図３と同じ符号を付し、説明を省略する。なお、第１の実施の形態の場合と同様に、セキュリティ管理システムを、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成してもよい。

【００５３】

図９は、本発明の第２の実施の形態による携帯電話機１００の構成を説明するブロック図である。音声処理回路３１－２は、無線通信部３０が出力した音声信号を音声出力信号に変換してスピーカ１２に出力し、マイクロフォン２２が入力した音声入力信号を音声信号に変換して音声データを生成し、携帯電話機主制御部３２－２に出力する。記憶部３３－２が予め記憶している許可者特徴情報は、許可者の音声のデータである許可者音声データである。例えば、このとき記憶部３３－２が記憶している音声のデータは、予め決められた特定の言葉の音声のデータであってよい。また、記憶部３３－２は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。そして、携帯電話機主制御部３２－２は、携帯電話機１００の全体の各部を制御し、音声処理回路３１－２に入力された携帯電話機１００のユーザの音声のデータと、記憶部３３－２が記憶している許可者音声データとをマッチングする認証処理を行ない、携帯電話機１００のユーザが許可者であるか否かを判定する。

【００５４】

次に、本発明の第２の実施の形態による携帯電話機１００において、本発明の第２の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成について説明

する。本発明の第２の実施の形態による携帯電話機１００において、本発明の第２の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成は、画像入力部１１１を音声入力部（使用者データ入力手段）１１４に置き換え、画像・認証結果表示部１１２を認証結果表示部１１５に置き換えたものであり、その他の構成は第１の実施の形態と同様である。ただし、入力データ処理部（判断手段、認証手段）１３１－２と入力データ認証用データ記憶部（許可者固有データ記憶手段）１３２－２との動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等については図４と同じ符号を付し、説明を省略する。

【００５５】

図１０は、本発明の第２の実施の形態による携帯電話機１００において、本発明の第２の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【００５６】

音声入力部１１４は、ユーザの音声を入力すると、入力した音声の音声データを生成する。認証結果表示部１１５は、入力データ処理部１３１－２が出力した情報を表示する。また、入力データ認証用データ記憶部１３２－２は、許可者の音声のデータである許可者音声データを予め記憶している。このとき入力データ認証用データ記憶部１３２－２が記憶している許可者音声データは、予め決められた特定の言葉の音声のデータであってよい。入力データ処理部１３１－２は、音声入力部１１４が生成した音声データと入力データ認証用データ記憶部１３２－２が記憶している許可者音声データとをマッチングする認証処理を行ない、ユーザが許可者であるか否かを判定し、ユーザが許可者であると判定すると、ユーザにパスワードの入力を要求するメッセージを認証結果表示部１１５に表示させる

【００５７】

音声入力部１１４は、マイクロフォン２２と音声処理回路３１－２とによって実現される。認証結果表示部１１５は、表示部３６によって実現される。入力データ認証用データ記憶部１３２－２は、記憶部３３－２によって実現される。入力データ処理部１３１－２は、携帯電話機主制御部３２－２によって実現される。

【００５８】

本発明の第２の実施の形態によるセキュリティ管理装置の構成は、第１の実施の形態におけるセキュリティ管理装置の構成と同様なため、図５と同じ符号を付し、説明を省略する。

【００５９】

本発明の第２の実施の形態によるセキュリティ管理装置において、本発明の第２の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成は、本発明の第１の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成と同様なため、図６と同じ符号を付し、説明を省略する。

【００６０】

次に、本発明の第２の実施の形態の動作について図面を参照して説明する。本発明の第２の実施の形態における携帯電話機１００の動作について説明する。図１１は、本発明の第２の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【００６１】

まず、音声入力部１１４は、ユーザの音声が入力されると、入力された音声の音声データを生成して入力データ処理部１３１－２に出力する（ステップＳ２０１）。例えば、このとき音声入力部１１４に入力する音声は、予め決められた特定の言葉の音声である。

【００６２】

入力データ処理部１３１－２は、入力されたユーザの音声データと、入力データ認証用データ記憶部１３２－２が記憶している許可者音声データとをマッチングする認証処理を行ない（ステップＳ２０２）、携帯電話機１００のユーザが許可者であるか否かを判定する。マッチングする方法は、例えば、テンプレートマッチング等の既知のマッチング方法

を用いる。なお、許可者音声データは、携帯電話機の契約時等に予め記憶部３３－２に記憶させておく。例えば、音声入力部１１４に許可者の音声を入力して許可者音声データを生成し、生成した許可者音声データを入力データ処理部１３１－２に出力する。入力データ処理部１３１－２は、入力データ認証用データ記憶部１３２－２に、入力された許可者音声データを記憶させる。また、接続コネクタ３８に接続された警備保障会社の外部機器から、接続コネクタ３８とデータ入出力インタフェース３７とを介して許可者音声データを入力データ処理部１３１－２に入力し、入力データ処理部１３１－２が入力データ認証用データ記憶部１３２－２に、入力された許可者音声データを記憶させてもよい。同様の方法で、入力データ認証用データ記憶部１３２－２に記憶させる許可者音声データを変更してもよい。また、許可者は複数であってもよい。従って、入力データ認証用データ記憶部１３２－２が記憶する許可者音声データは、複数の許可者のそれぞれの音声データであってもよい。

【００６３】

入力データ処理部１３１－２は、認証処理の結果、携帯電話機１００のユーザが許可者であるか否かを認証結果表示部１１５に表示させる（ステップＳ２０３）。入力データ処理部１３１－２は、ユーザが許可者であると判定すると（ステップＳ２０４）、ユーザにパスワードの入力を要求する画面を認証結果表示部１１５に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－２に出力する。なお、入力データ処理部１３１－２は、記憶部３３－２が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－２は、携帯電話機１００の電話番号を示す情報と、ユーザが許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を認証部１３３に入力し、認証部１３３は、入力された認証情報をデータ送信部１１３－１に出力し、データ送信部１１３－１に、セキュリティ管理装置のデータ受信部２１３へ認証情報を送信させる（ステップＳ２０５）。

【００６４】

入力データ処理部１３１－２は、ユーザが許可者でないと判定すると（ステップＳ２０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ２０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【００６５】

本発明の第２の実施の形態におけるセキュリティ管理装置の動作は、本発明の第１の実施の形態におけるセキュリティ管理装置の動作と同様なため説明を省略する。

【００６６】

以上、述べたように、この実施の形態によれば、画像データ処理という携帯電話機１００に負荷のかかる処理を行なうことなく、特定の場所への入場および特定の場所からの退場を許可するべき人物に、特定の場所への入場および特定の場所からの退場を許可することができる。

【００６７】

実施の形態３．

次に、本発明の第３の実施の形態を説明する。第３の実施の形態のセキュリティ管理システムの構成は、第１の実施の形態の構成と同様である。そのため、第１の実施の形態と同様の装置等については図２と同じ符号を付し、説明を省略する。なお、第１の実施の形態の場合と同様に、セキュリティ管理システムを、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成してもよい。

【００６８】

本発明による第３の実施の形態の携帯電話機１００の構成は、カメラユニット３９を指紋入力部６０に置き換えた点が第１の実施の形態と異なり、その他の構成は第１の実施の形態と同様である。ただし、携帯電話機主制御部３２－３および記憶部３３－３の動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等

については図３と同じ符号を付し、説明を省略する。

【００６９】

図１２は、本発明の第３の実施の形態による携帯電話機１００の構成を説明するブロック図である。指紋入力部６０は、ユーザに指先を接触させて指紋の形状を入力し、入力された指紋の形状を画像のデータに変換してユーザの指紋の画像のデータであるユーザ指紋画像データを生成し、生成したユーザ指紋画像データを携帯電話機主制御部３２－３に入力する。記憶部３３－３が予め記憶している許可者特徴情報は、許可者の指紋の画像のデータである許可者指紋画像データである。また、記憶部３３－３は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。そして、携帯電話機主制御部３２－３は、携帯電話機１００の全体の各部を制御し、指紋入力部６０が生成したユーザ指紋画像データと、記憶部３３－３が記憶している許可者指紋画像データとをマッチングする認証処理を行ない、携帯電話機１００のユーザが許可者であるか否かを判定する。

【００７０】

指紋入力部６０は、例えば、指紋の山部（凸部）と谷部（凹部）との電荷蓄積の差を検出し、画像データに変換を行なう静電容量式半導体センサー方式の指紋認識装置によって実現される。

【００７１】

次に、本発明の第３の実施の形態による携帯電話機１００において、本発明の第３の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成について説明する。本発明の第３の実施の形態による携帯電話機１００において、本発明の第３の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成は、画像入力部１１１を指紋形状入力部（使用者データ入力手段）１１６に置き換えたものであり、その他の構成は第１の実施の形態と同様である。ただし、入力データ処理部（判断手段、認証手段）１３１－３と入力データ認証用データ記憶部（許可者固有データ記憶手段）１３２－３との動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等については図４と同じ符号を付し、説明を省略する。

【００７２】

図１３は、本発明の第３の実施の形態による携帯電話機１００において、本発明の第３の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【００７３】

指紋形状入力部１１６は、ユーザに指先を接触させて指紋の形状を入力し、入力された指紋の形状を画像のデータに変換してユーザ指紋画像データを生成し、生成したユーザ指紋画像データを入力データ処理部１３１－３に入力する。入力データ認証用データ記憶部１３２－３は、予め許可者の指紋の画像のデータである許可者指紋画像データを記憶している。入力データ処理部１３１－３は、指紋形状入力部１１６が生成したユーザ指紋画像データと、入力データ認証用データ記憶部１３２－３が記憶している許可者指紋画像データとをマッチングする認証処理を行ない、携帯電話機１００のユーザが許可者であるか否かを判定する。

【００７４】

本発明の第３の実施の形態によるセキュリティ管理装置の構成は、第１の実施の形態におけるセキュリティ管理装置の構成と同様なため、図５と同じ符号を付し、説明を省略する。

【００７５】

本発明の第３の実施の形態によるセキュリティ管理装置において、本発明の第３の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成は、本発明の第１の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成と同様なため、図６と同じ符号を付し、説明を省略する。

【００７６】

次に、本発明の第３の実施の形態の動作について図面を参照して説明する。本発明の第

３の実施の形態における携帯電話機１００の動作について説明する。図１４は、本発明の第３の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【００７７】

ユーザに指先を指紋形状入力部１１６に接触させ、指紋形状入力部１１６に指紋の形状を入力すると（ステップＳ３０１）、指紋形状入力部１１６は、入力された指紋の形状を画像データに変換してユーザ指紋画像データを生成し、生成したユーザ指紋画像データを画像・認証結果表示部１１２と入力データ処理部１３１－３とに出力する。画像・認証結果表示部１１２は、入力されたユーザ指紋画像データの画像を表示する。

【００７８】

入力データ処理部１３１－３は、入力されたユーザ指紋画像データと、入力データ認証用データ記憶部１３２－３が記憶している許可者指紋画像データとをマッチングする認証処理を行ない（ステップＳ３０２）、携帯電話機１００のユーザが許可者であるか否かを判定する。マッチングする方法は、例えば、テンプレートマッチング等の既知のマッチング方法を用いる。なお、許可者指紋画像データは、携帯電話機の契約時等に予め入力データ認証用データ記憶部１３２－３に記憶させておく。例えば、許可者が指先を指紋形状入力部１１６に接触させ、指紋形状入力部１１６に指紋の形状を入力し、指紋形状入力部１１６は、入力された指紋の形状を指紋の画像のデータに変換して許可者指紋画像データを生成し、生成した許可者指紋画像データを入力データ処理部１３１－３に出力し、入力データ処理部１３１－３は、入力された許可者指紋画像データを入力データ認証用データ記憶部１３２－３に記憶させてもよいし、接続コネクタ３８に接続された警備保障会社の外部機器から、接続コネクタ３８とデータ入出力インタフェース３７とを介して許可者指紋画像データを入力データ処理部１３１－３に入力し、入力データ処理部１３１－３が入力データ認証用データ記憶部１３２－３に、入力された許可者指紋画像データを記憶させてもよい。同様の方法で、入力データ認証用データ記憶部１３２－３に記憶させる許可者指紋画像データを変更してもよい。また、許可者は複数であってもよい。従って、入力データ認証用データ記憶部１３２－３が記憶する許可者指紋画像データは、複数の許可者のそれぞれの指紋の画像データであってもよい。

【００７９】

入力データ処理部１３１－３は、認証処理の結果、携帯電話機１００のユーザが許可者であるか否かを画像・認証結果表示部１１２に表示させる（ステップＳ３０３）。入力データ処理部１３１－３は、ユーザが許可者であると判定すると（ステップＳ３０４）、ユーザにパスワードの入力を要求する画面を画像・認証結果表示部１１２に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－３に出力する。なお、入力データ処理部１３１－３は、記憶部３３－３が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－３は、携帯電話機１００の電話番号と、ユーザが許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を、認証部１３３に入力し、認証部１３３は入力された認証情報をデータ送信部１１３－１に出力し、データ送信部１１３－１に、データ受信部２１３へ、認証情報を送信させる（ステップＳ３０５）。

【００８０】

入力データ処理部１３１－３は、ユーザが許可者でないと判定すると（ステップＳ３０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ３０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【００８１】

本発明の第３の実施の形態におけるセキュリティ管理装置の動作は、本発明の第１の実施の形態におけるセキュリティ管理装置の動作と同様なため説明を省略する。

【００８２】

以上、述べたように、この実施の形態によれば、ユーザの指紋の画像データを用いて、ユーザが特定の場所への入場および特定の場所からの退場を許可するべき人物であるか否

かを判定しているため、厳密なユーザ認証を行なうことができる。

【００８３】

実施の形態４.

次に、本発明の第４の実施の形態を説明する。第４の実施の形態のセキュリティ管理システムの構成は、第１の実施の形態の構成と同様である。そのため、第１の実施の形態と同様の装置等については図２と同じ符号を付し、説明を省略する。なお、第１の実施の形態の場合と同様に、セキュリティ管理システムを、携帯電話通信網を介して携帯電話機からセキュリティ管理装置に所定の信号が送信されるように構成してもよい。

【００８４】

本発明による第４の実施の形態の携帯電話機１００の構成は、指紋入力部６０を含む点が第１の実施の形態と異なり、その他の構成は第１の実施の形態と同様である。ただし、音声処理回路３１－２の動作は、第２の実施の形態における動作と同様であり、指紋入力部６０の動作は第３の実施の形態における動作と同様である。また、携帯電話機主制御部３２－４および記憶部３３－４の動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態、第２の実施の形態および第３の実施の形態と同様の回路等についてはそれぞれ図３、図９および図１２と同じ符号を付し、説明を省略する。

【００８５】

図１５は、本発明の第４の実施の形態による携帯電話機１００の構成を説明するブロック図である。記憶部３３－４が予め記憶している許可者特徴情報は、許可者の顔の画像データと、許可者の音声のデータである許可者音声データと、許可者の指紋の画像のデータである許可者指紋画像データとである。ここで、許可者音声データは、許可者が予め決められた言葉を発声した音声のデータであってよい。記憶部３３－４は、これらの各データを予め対応付けて記憶している。また、記憶部３３－４は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。携帯電話機主制御部３２－４は、カメラユニット３９が入力したユーザの顔の画像データと記憶部３３－４が記憶している許可者の顔の画像データとをマッチングする処理と、音声処理回路３１－２が入力したユーザの音声データと記憶部３３－４が記憶している許可者音声データとをマッチングする処理と、指紋入力部６０が入力したユーザ指紋画像データと記憶部３３－４が記憶している許可者指紋画像データとをマッチングする処理とである認証処理を行ない、携帯電話機１００のユーザが許可者であるか否かを判定する。

【００８６】

次に、本発明の第４の実施の形態による携帯電話機１００において、本発明の第４の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成について説明する。本発明の第４の実施の形態による携帯電話機１００において、本発明の第４の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成は、音声入力部１１４と、指紋形状入力部１１６とを加えたものであり、その他の構成は第１の実施の形態と同様である。ただし、音声入力部１１４の動作は、第２の実施の形態における動作と同様であり、指紋形状入力部１１６の動作は第３の実施の形態における動作と同様である。また、入力データ処理部（判断手段、認証手段）１３１－４と入力データ認証用データ記憶部（許可者固有データ記憶手段）１３２－４との動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態、第２の実施の形態および第３の実施の形態と同様の回路等についてはそれぞれ図４、図１０および図１３と同じ符号を付し、説明を省略する。

【００８７】

図１６は、本発明の第４の実施の形態による携帯電話機１００において、本発明の第４の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【００８８】

入力データ認証用データ記憶部１３２－４が予め記憶している許可者特徴情報は、許可者の顔の画像データと、許可者の音声のデータである許可者音声データと、許可者の指紋

の画像のデータである許可者指紋画像データとである。入力データ認証用データ記憶部１３２－４は、これらの各データを予め対応付けて記憶している。入力データ処理部１３１－４は、画像入力部１１１が入力したユーザの顔の画像データと入力データ認証用データ記憶部１３２－４が記憶している許可者の顔の画像データとをマッチングする処理と、音声入力部１１４が入力したユーザの音声データと入力データ認証用データ記憶部１３２－４が記憶している許可者音声データとをマッチングする処理と、指紋形状入力部１１６が入力したユーザ指紋画像データと入力データ認証用データ記憶部１３２－４が記憶している許可者指紋画像データとをマッチングする処理とである認証処理を行ない、携帯電話機１００のユーザが許可者であるか否かを判定する。

【００８９】

本発明の第４の実施の形態によるセキュリティ管理装置の構成は、第１の実施の形態におけるセキュリティ管理装置の構成と同様なため、図４と同じ符号を付し、説明を省略する。

【００９０】

本発明の第４の実施の形態によるセキュリティ管理装置において、本発明の第４の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成は、本発明の第１の実施の形態による携帯電話機１００から受信した情報を処理する部分の構成と同様なため、図６と同じ符号を付し、説明を省略する。

【００９１】

次に、本発明の第４の実施の形態の動作について図面を参照して説明する。本発明の第４の実施の形態における携帯電話機１００の動作について説明する。図１７は、本発明の第４の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【００９２】

まず、画像入力部１１１が、ユーザの顔を撮影してユーザの顔の画像データを生成し、生成した画像データを画像・認証結果表示部１１２と入力データ処理部１３１－４とに出力する（ステップＳ４０１）。画像・認証結果表示部１１２は、入力された画像データの画像を表示する。そして、音声入力部１１４にユーザの音声が入力されると（ステップＳ４０２）、音声データを生成し、入力データ処理部１３１－４に出力する。例えば、このとき音声入力部１１４に入力する音声は、予め決められた特定の言葉の音声である。また、ユーザが指先を指紋形状入力部１１６に接触させ、指紋形状入力部１１６に指紋の形状を入力すると（ステップＳ４０３）、指紋形状入力部１１６は、入力された指紋の形状を指紋の画像のデータに変換してユーザ指紋画像データを生成し、生成したユーザ指紋画像データを画像・認証結果表示部１１２と入力データ処理部１３１－４に出力する。画像・認証結果表示部１１２は、入力されたユーザ指紋画像データの画像を表示する。

【００９３】

入力データ処理部１３１－４は、画像入力部が入力したユーザの顔の画像データと入力データ認証用データ記憶部１３２－４が記憶している許可者の顔の画像データとをマッチングする処理と、音声入力部１１４が入力したユーザの音声データと入力データ認証用データ記憶部１３２－４が記憶している許可者音声データとをマッチングする処理と、指紋形状入力部１１６が入力したユーザ指紋画像データと入力データ認証用データ記憶部１３２－４が記憶している許可者指紋画像データとをマッチングする処理とである認証処理を行ない（ステップＳ４０４）、携帯電話機１００のユーザが許可者であるか否かを判定する。なお、入力データ処理部１３１－４は、各マッチング処理のそれぞれの全てにおいて合致した場合に携帯電話機１００のユーザが許可者であると判定する。

【００９４】

入力データ処理部１３１－４は、認証処理の結果、携帯電話機１００のユーザが許可者であるか否かを画像・認証結果表示部１１２に表示させる（ステップＳ４０５）。入力データ処理部１３１－４は、ユーザが許可者であると判定すると（ステップＳ４０６）、ユーザにパスワードの入力を要求する画面を画像・認証結果表示部１１２に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワ

ードを入力データ処理部１３１－４に出力する。なお、入力データ処理部１３１－４は、記憶部３３－４が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－４は、携帯電話機１００の電話番号を示す情報と、ユーザが許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を、認証部１３３に入力し、認証部１３３は入力された認証情報をデータ送信部１１３－１に出力し、データ送信部１１３－１に、データ受信部２１３へ、認証情報を送信させる（ステップＳ４０７）。

【００９５】

入力データ処理部１３１－４は、ユーザが許可者でないと判定すると（ステップＳ１０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ１０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【００９６】

本発明の第４の実施の形態におけるセキュリティ管理装置の動作は、本発明の第１の実施の形態におけるセキュリティ管理装置の動作と同様なため説明を省略する。

【００９７】

以上、述べたように、この実施の形態によれば、ユーザの、顔の画像データと音声データと指紋の画像データとを用いて、ユーザが特定の場所への入場および特定の場所からの退場を許可するべき人物であるか否かを判定しているため、より厳密なユーザ認証を行なうことができる。

【００９８】

実施の形態５．

次に、本発明の第５の実施の形態を説明する。図１８は、本発明の第５の実施の形態によるセキュリティ管理システムの構成を示す説明図である。本発明の第５の実施の形態によるセキュリティ管理システムは、携帯電話機１００と、携帯電話機１００と情報を送受信する基地局３００～３０ｎ、各基地局と専用デジタル回線やＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等で接続され、各基地局から受信したデータの出力を制御する交換機能を有する制御局４００、携帯電話機１００のユーザの身元を認証する身元確認システム５００、銀行の業務を遂行する銀行システム６００および制御局４００と身元確認システム５００と銀行システム６００とを接続する通信ネットワーク７００とを含む。

【００９９】

銀行システム６００は、例えば、サーバ等のデータ処理装置によって実現される。通信ネットワーク７００は、例えば、公衆回線網や、ＩＰ電話網、インターネット等である。

【０１００】

本発明による第５の実施の形態の携帯電話機１００の構成は、ブルートゥース回路３４を含まない点が第１の実施の形態と異なり、その他の構成は第１の実施の形態における携帯電話機１００の構成と同様である。ただし、記憶部３３－５および携帯電話機主制御部３２－５の動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等については図３と同じ符号を付し、説明を省略する。

【０１０１】

図１９は、本発明の第５の実施の形態による携帯電話機１００の構成を説明するブロック図である。記憶部３３－５は、銀行システム６００へのアクセスを許可された人物であるアクセス許可者の顔の画像データを予め記憶している。また、記憶部３３－５は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。携帯電話機主制御部３２－５は、携帯電話機１００の全体の各部の制御と、カメラユニット３９が撮影して生成したユーザの顔の画像データと、記憶部３３－５が記憶しているアクセス許可者の顔の画像データとをマッチングする認証処理とを行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報とユーザが入力したパスワードとを組み合わせた情報である認証情報を、無線通信部３０に、アンテナ１５と各基地局のいずれかと制御局４００と通信ネットワーク７００とを介して身元確認システム５０

０へ送信させる。

【０１０２】

次に、本発明の第５の実施の形態による携帯電話機１００において、本発明の第５の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成について説明する。本発明の第５の実施の形態による携帯電話機１００において、本発明の第５の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成は、第１の実施の形態と同様である。ただし、入力データ処理部１３１－５と入力データ認証用データ記憶部１３２－５とデータ送信部１１３－２の動作は第１の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等については図４と同じ符号を付し、説明を省略する。なお、データ送信部１１３－２は、無線通信部３０によって実現される。

【０１０３】

図２０は、本発明の第５の実施の形態による携帯電話機１００において、本発明の第５の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成を示すブロック図である。

【０１０４】

入力データ認証用データ記憶部１３２－５は、銀行システム６００へのアクセスを許可された人物であるアクセス許可者の顔の画像データを予め記憶している。入力データ処理部１３１－５は、画像入力部１１１が撮影して生成したユーザの顔の画像データと、入力データ認証用データ記憶部１３２－５が記憶しているアクセス許可者の顔の画像データとをマッチングする認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報とユーザが入力したパスワードとを組み合わせた情報である認証情報を、認証部１３３に出力する。データ送信部１１３－２は、認証部１３３が出力した認証情報を、基地局３００と制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信する。

【０１０５】

図２１は、本発明の第５の実施の形態の身元確認システム５００の構成を示すブロック図である。本発明の第５の実施の形態の身元確認システム５００は、制御局４００および銀行システム６００と通信ネットワーク７００を介して情報を送受信する通信部（認証情報受信手段）５０１、身元確認システム全体を制御する身元確認システム制御部（認証結果処理手段、制御手段）５０２および銀行システム６００へのアクセスを許可するユーザの携帯電話機の電話番号とパスワードとを予め対応付けて認証データとして記憶している身元確認システム記憶部（許可者情報記憶手段）５０３を含む。なお、身元確認システムは、例えば、サーバ等によって実現される。

【０１０６】

次に、本発明の第５の実施の形態の動作について図面を参照して説明する。まず、本発明の第５の実施の形態における携帯電話機１００の動作について説明する。図２２は、本発明の第５の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【０１０７】

まず、画像入力部１１１が、ユーザの顔を撮影して画像データを生成し、生成した画像データを画像・認証結果表示部１１２と入力データ処理部１３１－５とに出力する（ステップＳ５０１）。画像・認証結果表示部１１２は、入力された画像データの画像を表示する。

【０１０８】

入力データ処理部１３１－５は、入力されたユーザの顔の画像データと、入力データ認証用データ記憶部１３２－５が記憶しているアクセス許可者の顔の画像データとをマッチングする認証処理を行ない（ステップＳ５０２）、携帯電話機１００のユーザがアクセス許可者であるか否かを判定する。マッチングする方法は、例えば、テンプレートマッチン

グ等の既知のマッチング方法を用いる。なお、アクセス許可者の顔の画像データは、携帯電話機の契約時等に予め入力データ認証用データ記憶部１３２－５に記憶させておく。例えば、画像入力部１１１がアクセス許可者の顔を撮影して、アクセス許可者の顔の画像データを生成し、入力データ処理部１３１－５が入力データ認証用データ記憶部１３２－５に、画像入力部１１１が生成した画像データを記憶させてもよいし、接続コネクタ３８に接続された警備保障会社の外部機器から、接続コネクタ３８とデータ入出力インタフェース３７とを介してアクセス許可者の顔の画像データを入力データ処理部１３１－５に入力し、入力データ処理部１３１－５が入力データ認証用データ記憶部１３２－５に、入力されたアクセス許可者の顔の画像データを記憶させてもよい。同様の方法で、入力データ認証用データ記憶部１３２－５に記憶させる画像データを変更してもよい。また、アクセス許可者は複数であってもよい。従って、入力データ認証用データ記憶部１３２－５が記憶するアクセス許可者の顔の画像データは、複数のアクセス許可者のそれぞれの顔の画像データであってもよい。

【０１０９】

入力データ処理部１３１－５は、認証処理の結果、携帯電話機１００のユーザがアクセス許可者であるか否かを画像・認証結果表示部１１２に表示させる（ステップＳ５０３）。入力データ処理部１３１－５は、ユーザがアクセス許可者であると判定すると（ステップＳ５０４）、ユーザにパスワードの入力を要求する画面を画像・認証結果表示部１１２に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－５に出力する。なお、入力データ処理部１３１－１は、記憶部３３－１が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－５は、携帯電話機１００の電話番号と、ユーザがアクセス許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を、認証部１３３に入力し、認証部１３３は入力された認証情報をデータ送信部１１３－２に出力し、データ送信部１１３－２に、各基地局のいずれかと制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信させる（ステップＳ５０５）。

【０１１０】

入力データ処理部１３１－５は、ユーザがアクセス許可者でないと判定すると（ステップＳ５０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ５０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【０１１１】

次に、本発明の第５の実施の形態における身元確認システム５００の動作について説明する。図２３は、本発明の第５の実施の形態における身元確認システム５００の動作を説明するフローチャートである。

【０１１２】

身元確認システム５００において、通信部５０１が認証情報を受信すると（ステップＳ５１０）、受信した認証情報を身元確認システム制御部５０２に出力する。身元確認システム制御部５０２は、受信した認証情報に含まれている電話番号とパスワードとの組み合わせが、身元確認システム記憶部５０３が予め対応付けて記憶している電話番号とパスワードとである認証データに含まれているか否かを判定する（ステップＳ５１１）。

【０１１３】

身元確認システム制御部５０２は、受信した認証情報に含まれている電話番号の情報とパスワードとの組み合わせが、身元確認システム記憶部５０３が予め対応付けて記憶している電話番号とパスワードとである認証データに含まれていると判定すると、ユーザに携帯電話機１００、各基地局、制御局４００および通信ネットワーク７００を介した銀行システム６００へのアクセスを許可する（ステップＳ５１２）。身元確認システム制御部５０２は、受信した認証情報に含まれている電話番号の情報とパスワードとが、身元確認システム記憶部５０３が予め対応付けて記憶している電話番号の情報とパスワードとである認証データに合致しないと判定すると、銀行システム６００へのアクセスを許可しない（

ステップＳ５１３）。

【０１１４】

身元確認システム５００が、ユーザに銀行システム６００へのアクセスを許可した場合、例えば、ユーザが携帯電話機１００を介して残高照会をするとき、ユーザは、携帯電話機１００の操作入力部３５を操作して、口座番号を特定する情報と残高照会を指示する情報とを入力する。操作入力部３５は入力された口座番号を特定する情報と残高照会を指示する情報とを入力データ処理部１３１－５に出力する。入力データ処理部１３１－５は、認証部１３３を介してデータ送信部１１３－２に、口座番号を特定する情報と残高照会を指示する情報とを、各基地局、制御局４００および通信ネットワーク７００を介して身元確認システム６００に送信させる。以上が本発明の第５の実施の形態による携帯電話機１００において、本発明の第５の実施の形態による身元確認システム５００に送信する情報を処理する部分の動作である。

【０１１５】

そして、身元確認システム５００において、通信部５０１が口座番号を特定する情報と残高照会を指示する情報とを受信すると、通信部５０１は、口座番号を特定する情報と残高照会を指示する情報とを通信ネットワーク７００を介して銀行システム６００に送信する。銀行システムは、口座番号を特定する情報にもとづいて特定された口座番号の口座の残高照会を行ない、口座番号を特定する情報の口座番号の口座の残高金額を特定する情報を身元確認システム５００に送信する。身元確認システム５００において、通信部５０１が残高金額を特定する情報を受信すると、通信部５０１は、受信した残高金額を特定する情報を、通信ネットワーク７００、制御局４００および各基地局を介して携帯電話機１００に送信する。携帯電話機１００において、無線通信部３０が残高金額を特定する情報を受信すると、携帯電話主制御部３２－５に入力する。携帯電話主制御部３２－５は入力された残高金額を特定する情報にもとづいて、残高金額を表示部３６に表示させる。

【０１１６】

以上、述べたように、この実施の形態によれば、ユーザの顔の画像データを身元確認システム５００に送信することなく、銀行システム６００へのアクセスを許可するべき人物に、銀行システム６００へのアクセスを許可することができる。

【０１１７】

実施の形態６．

次に、本発明の第６の実施の形態を説明する。第６の実施の形態のセキュリティ管理システムの構成は、第５の実施の形態の構成と同様である。そのため、第５の実施の形態と同様のシステム等については図１８と同じ符号を付し、説明を省略する。

【０１１８】

本発明による第６の実施の形態の携帯電話機１００の構成は、ブルートゥース回路３４を含まない点が第２の実施の形態と異なり、その他の構成は第２の実施の形態と同様である。ただし、携帯電話機主制御部３２－６および記憶部３３－６の動作は第２の実施の形態における動作とは異なる。そのため、第２の実施の形態と同様の回路等については図９と同じ符号を付し、説明を省略する。

【０１１９】

図２４は、本発明の第６の実施の形態による携帯電話機１００の構成を説明するブロック図である。記憶部３３－６は、銀行システム６００へのアクセスを許可された人物であるアクセス許可者の音声のデータである許可者音声データを予め記憶している。例えば、このとき記憶部３３－６が記憶している音声のデータは、予め決められた特定の言葉の音声のデータである。また、記憶部３３－６は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。そして、携帯電話機主制御部３２－６は、携帯電話機１００の全体の各部を制御し、音声処理回路３１－２に入力された音声のデータと、記憶部３３－６が記憶している許可者音声データとをマッチングする認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報

とユーザが入力したパスワードとを組み合わせた情報である認証情報を、無線通信部３０に、アンテナ１５と各基地局のいずれかと制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信させる。

【０１２０】

次に、本発明の第６の実施の形態による携帯電話機１００において、本発明の第６の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成について説明する。本発明の第６の実施の形態による携帯電話機１００において、本発明の第６の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成は、第２の実施の形態と同様である。ただし、入力データ処理部１３１－６と入力データ認証用データ記憶部１３２－６とデータ送信部１１３－２の動作は第２の実施の形態における動作とは異なる。そのため、第２の実施の形態と同様の回路等については図１０と同じ符号を付し、説明を省略する。なお、データ送信部１１３－２は、無線通信部３０によって実現される。

【０１２１】

図２５は、本発明の第６の実施の形態による携帯電話機１００において、本発明の第６の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成を示すブロック図である。

【０１２２】

入力データ認証用データ記憶部１３２－６は、銀行システム６００へのアクセスを許可された人物であるアクセス許可者の音声のデータである許可者音声データを予め記憶している。例えば、このとき入力データ認証用データ記憶部１３２－６が記憶している音声のデータは、予め決められた特定の言葉の音声のデータである。そして、入力データ処理部１３１－６は、音声入力部１１４に入力された音声のデータと、入力データ認証用データ記憶部１３２－６が記憶している許可者音声データとをマッチングする認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報とユーザが入力したパスワードとを組み合わせた情報である認証情報を、認証部１３３に出力する。データ送信部１１３－２は、認証部１３３が出力した認証情報を、基地局３００と制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信する。

【０１２３】

本発明の第６の実施の形態による身元確認システム５００の構成は、第５の実施の形態における身元確認システム５００の構成と同様なため、図２１と同じ符号を付し、説明を省略する。

【０１２４】

次に、本発明の第６の実施の形態の動作について図面を参照して説明する。本発明の第６の実施の形態における携帯電話機１００の動作について説明する。図２６は、本発明の第６の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【０１２５】

まず、携帯電話機１００の音声入力部１１４にユーザの音声が入力されると、入力した音声の音声データを生成して入力データ処理部１３１－６に出力する（ステップＳ６０１）。例えば、音声入力部１１４に入力する音声は、予め決められた特定の言葉である。

【０１２６】

入力データ処理部１３１－６は、入力されたユーザの音声データと、入力データ認証用データ記憶部１３２－６が記憶しているアクセス許可者音声のデータとをマッチングする認証処理を行ない（ステップＳ６０２）、携帯電話機１００のユーザがアクセス許可者であるか否かを判定する。マッチングする方法は、例えば、テンプレートマッチング等の既知のマッチング方法を用いる。なお、アクセス許可者の音声のデータは、携帯電話機の契約時等に予め入力データ認証用データ記憶部１３２－６に記憶させておく。例えば、音声入力部１１４にアクセス許可者の音声を入力し、許可者音声データを生成して、入力デー

タ処理部１３１－６に出力する。入力データ処理部１３１－６は、入力データ認証用データ記憶部１３２－６に、入力された許可者音声データを記憶させる。また、接続コネクタ３８に接続された警備保障会社の外部機器から、接続コネクタ３８とデータ入出力インタフェース３７とを介して許可者音声データを入力データ処理部１３１－６に入力し、入力データ処理部１３１－６が入力データ認証用データ記憶部１３２－６に、入力された許可者音声データを記憶させてもよい。同様の方法で、入力データ認証用データ記憶部１３２－６に記憶させる許可者音声データを変更してもよい。また、アクセス許可者は複数であってもよい。従って、入力データ認証用データ記憶部１３２－６が記憶する許可者音声データは、複数のアクセス許可者のそれぞれの音声データであってもよい。

【０１２７】

入力データ処理部１３１－６は、認証処理の結果、携帯電話機１００のユーザがアクセス許可者であるか否かを認証結果表示部１１５に表示させる（ステップＳ６０３）。入力データ処理部１３１－６は、ユーザがアクセス許可者であると判定すると（ステップＳ６０４）、ユーザにパスワードの入力を要求する画面を認証結果表示部１１５に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－６に出力する。なお、入力データ処理部１３１－６は、記憶部３３－６が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－６は、携帯電話機１００の電話番号と、ユーザがアクセス許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を、認証部１３３に入力し、認証部１３３は入力された認証情報をデータ送信部１１３－２に出力し、データ送信部１１３－２に、各基地局のいずれかと制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信させる（ステップＳ６０５）。

【０１２８】

入力データ処理部１３１－６は、ユーザがアクセス許可者でないと判定すると（ステップＳ６０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ６０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【０１２９】

本発明の第６の実施の形態における身元確認システム５００の動作は、本発明の第５の実施の形態における身元確認システム５００の動作と同様なため説明を省略する。

【０１３０】

以上、述べたように、この実施の形態によれば、画像データ処理という携帯電話機１００に負荷のかかる処理を行なうことなく、銀行システム６００へのアクセスを許可するべき人物に、銀行システム６００へのアクセスを許可することができる。

【０１３１】

実施の形態７．

次に、本発明の第７の実施の形態を説明する。本発明による第７の実施の形態のセキュリティ管理システムの構成は、第５の実施の形態の構成と同様である。そのため、第５の実施の形態と同様のシステム等については図１８と同じ符号を付し、説明を省略する。

【０１３２】

本発明による第７の実施の形態の携帯電話機１００の構成は、ブルートゥース回路３４を含まない点が第３の実施の形態と異なり、その他の構成は第３の実施の形態と同様である。ただし、携帯電話機主制御部３２－７および記憶部３３－７の動作は第３の実施の形態における動作とは異なる。そのため、第３の実施の形態と同様の回路等については図１２と同じ符号を付し、説明を省略する。

【０１３３】

図２７は、本発明の第７の実施の形態による携帯電話機１００の構成を説明するブロック図である。記憶部３３－７は、アクセス許可者の指紋の画像のデータである許可者指紋画像データを予め記憶している。また、記憶部３３－７は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。そして、携帯電話機主制御部３２－７は、携帯電話

機１００の全体の各部を制御し、指紋入力部６０が生成したユーザの指紋の画像データであるユーザ指紋画像データと、記憶部３３－７が記憶している許可者指紋画像データとをマッチングする認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報とユーザが入力したパスワードとを組み合わせた情報である認証情報を、無線通信部３０に、アンテナ１５といずれかの基地局と制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信させる。

【０１３４】

次に、本発明の第７の実施の形態による携帯電話機１００において、本発明の第７の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成について説明する。本発明の第７の実施の形態による携帯電話機１００において、本発明の第７の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成は、第３の実施の形態と同様である。ただし、入力データ処理部１３１－７と入力データ認証用データ記憶部１３２－７とデータ送信部１１３－２の動作は第３の実施の形態における動作とは異なる。そのため、第３の実施の形態と同様の回路等については図１３と同じ符号を付し、説明を省略する。なお、データ送信部１１３－２は、無線通信部３０によって実現される。

【０１３５】

図２８は、本発明の第７の実施の形態による携帯電話機１００において、本発明の第７の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成を示すブロック図である。

【０１３６】

入力データ認証用データ記憶部１３２－７は、アクセス許可者の指紋の画像のデータである許可者指紋画像データを予め記憶している。入力データ処理部１３１－７は、指紋形状入力部１１６が生成したユーザ指紋画像データと、入力データ認証用データ記憶部１３２－７が記憶している許可者指紋画像データとをマッチングする認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報とユーザが入力したパスワードとを組み合わせた情報である認証情報を、認証部１３３に出力する。データ送信部１１３－２は、認証部１３３が出力した認証情報を、基地局３００と制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信する。

【０１３７】

本発明の第７の実施の形態による身元確認システム５００の構成は、第５の実施の形態における身元確認システム５００の構成と同様なため、図２１と同じ符号を付し、説明を省略する。

【０１３８】

次に、本発明の第７の実施の形態の動作について図面を参照して説明する。本発明の第７の実施の形態における携帯電話機１００の動作について説明する。図２９は、本発明の第７の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【０１３９】

ユーザに指先を指紋形状入力部１１６に接触させ、指紋形状入力部１１６に指紋の形状を入力すると（ステップＳ７０１）、指紋形状入力部１１６は、入力された指紋の形状を画像のデータに変換してユーザの指紋の画像データであるユーザ指紋画像データを生成し、生成したユーザ指紋画像データを画像・認証結果表示部１１２と入力データ処理部１３１－７とに出力する。画像・認証結果表示部１１２は、入力されたユーザ指紋画像データの画像を表示する。

【０１４０】

入力データ処理部１３１－７は、入力されたユーザ指紋画像データと、入力データ認証

用データ記憶部１３２－７が記憶している許可者指紋画像データとをマッチングする認証処理を行ない（ステップＳ７０２）、携帯電話機１００のユーザがアクセス許可者であるか否かを判定する。マッチングする方法は、例えば、テンプレートマッチング等の既知のマッチング方法を用いる。なお、許可者指紋画像データは、携帯電話機の契約時等に予め入力データ認証用データ記憶部１３２－７に記憶させておく。例えば、アクセス許可者が指先を指紋形状入力部１１６に接触させ、指紋形状入力部１１６に指紋の形状を入力し、指紋形状入力部１１６は、入力された指紋の形状を画像のデータに変換して許可者指紋画像データを生成し、生成した許可者指紋画像データを入力データ処理部１３１－７に出力し、入力データ処理部１３１－７は、入力された許可者指紋画像データを入力データ認証用データ記憶部１３２－７に記憶させてもよいし、接続コネクタ３８に接続された警備保障会社の外部機器から、接続コネクタ３８とデータ入出力インタフェース３７とを介して許可者指紋画像データを入力データ処理部１３１－７に入力し、入力データ処理部１３１－７が入力データ認証用データ記憶部１３２－７に、入力された許可者指紋画像データを記憶させてもよい。同様の方法で、入力データ認証用データ記憶部１３２－７に記憶させる許可者指紋画像データを変更してもよい。また、アクセス許可者は複数であってもよい。従って、入力データ認証用データ記憶部１３２－７が記憶する許可者指紋画像データは、複数のアクセス許可者のそれぞれの指紋の画像データであってもよい。

【０１４１】

入力データ処理部１３１－７は、認証処理の結果、携帯電話機１００のユーザがアクセス許可者であるか否かを画像・認証結果表示部１１２に表示させる（ステップＳ７０３）。入力データ処理部１３１－７は、ユーザがアクセス許可者であると判定すると（ステップＳ７０４）、ユーザにパスワードの入力を要求する画面を画像・認証結果表示部１１２に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－７に出力する。なお、入力データ処理部１３１－７は、記憶部３３－７が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－７は、携帯電話機１００の電話番号と、ユーザがアクセス許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を、認証部１３３に入力し、認証部１３３は入力された認証情報をデータ送信部１１３－２に出力し、データ送信部１１３－２に、各基地局のいずれかと制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信させる（ステップＳ７０５）。

【０１４２】

入力データ処理部１３１－７は、ユーザがアクセス許可者でないと判定すると（ステップＳ７０４）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ７０６）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【０１４３】

本発明の第７の実施の形態における身元確認システム５００の動作は、本発明の第５の実施の形態における身元確認システム５００の動作と同様なため説明を省略する。

【０１４４】

以上、述べたように、この実施の形態によれば、ユーザの指紋の画像データを用いて、ユーザが銀行システム６００へのアクセスを許可するべき人物であるか否かを判定しているため、厳密なユーザ認証を行なうことができる。

【０１４５】

実施の形態８．

次に、本発明の第８の実施の形態を説明する。本発明による第８の実施の形態のセキュリティ管理システムの構成は、第５の実施の形態の構成と同様である。そのため、第５の実施の形態と同様のシステム等については図１８と同じ符号を付し、説明を省略する。

【０１４６】

本発明による第８の実施の形態の携帯電話機１００の構成は、ブルートゥース回路３４を含まない点が第４の実施の形態と異なり、その他の構成は第４の実施の形態と同様であ

る。ただし、携帯電話機主制御部３２－８および記憶部３３－８の動作は第４の実施の形態における動作とは異なる。そのため、第４の実施の形態と同様の回路等については図１５と同じ符号を付し、説明を省略する。

【０１４７】

図３０は、本発明の第８の実施の形態による携帯電話機１００の構成を説明するブロック図である。記憶部３３－８が予め記憶している許可者特徴情報は、アクセス許可者の顔の画像データと、アクセス許可者の音声のデータである許可者音声データと、アクセス許可者の指紋の画像のデータである許可者指紋画像データとである。記憶部３３－８は、これらの各データを予め対応付けて記憶している。また、記憶部３３－８は、予め携帯電話機１００の固有のパスワードを記憶していてもよい。携帯電話機主制御部３２－８は、カメラユニット３９が入力したユーザの顔の画像データと記憶部３３－８が記憶しているアクセス許可者の顔の画像データとをマッチングする処理と、音声処理回路３１－２が入力したユーザの音声データと記憶部３３－８が記憶しているアクセス許可者の音声のデータとをマッチングする処理と、指紋入力部６０が入力したユーザ指紋画像データと記憶部３３－８が記憶している許可者指紋画像データとをマッチングする処理とである認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定する。

【０１４８】

次に、本発明の第８の実施の形態による携帯電話機１００において、本発明の第８の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成について説明する。本発明の第８の実施の形態による携帯電話機１００において、本発明の第８の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成は、第４の実施の形態と同様である。ただし、入力データ処理部１３１－８と入力データ認証用データ記憶部１３２－８とデータ送信部１１３－２の動作は第４の実施の形態における動作とは異なる。そのため、第１の実施の形態と同様の回路等については図１６と同じ符号を付し、説明を省略する。なお、データ送信部１１３－２は、無線通信部３０によって実現される。

【０１４９】

図３１は、本発明の第８の実施の形態による携帯電話機１００において、本発明の第８の実施の形態による身元確認システム５００に送信する情報を処理する部分の構成を示すブロック図である。

【０１５０】

入力データ認証用データ記憶部１３２－８が予め記憶しているアクセス許可者特徴情報は、アクセス許可者の顔の画像データと、アクセス許可者の音声のデータである許可者音声データと、アクセス許可者の指紋の画像のデータである許可者指紋画像データとである。入力データ認証用データ記憶部１３２－８は、これらの各データを予め対応付けて記憶している。入力データ処理部１３１－８は、画像入力部１１１が入力したユーザの顔の画像データと入力データ認証用データ記憶部１３２－４が記憶しているアクセス許可者の顔の画像データとをマッチングする処理と、音声入力部１１４が入力したユーザの音声データと入力データ認証用データ記憶部１３２－８が記憶しているアクセス許可者の音声のデータとをマッチングする処理と、指紋形状入力部１１６が入力したユーザ指紋画像データと入力データ認証用データ記憶部１３２－８が記憶している許可者指紋画像データとをマッチングする処理とである認証処理を行ない、携帯電話機１００のユーザがアクセス許可者であるか否かを判定し、ユーザがアクセス許可者であると判定すると、携帯電話機１００の電話番号とユーザがアクセス許可者であることを示す情報とユーザが入力したパスワードとを組み合わせた情報である認証情報を、認証部１３３に出力する。データ送信部１１３－２は、認証部１３３が出力した認証情報を、基地局３００と制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信する。

【０１５１】

本発明の第８の実施の形態による身元確認システム５００の構成は、第５の実施の形態における身元確認システム５００の構成と同様なため、図２１と同じ符号を付し、説明を

省略する。

【０１５２】

次に、本発明の第８の実施の形態の動作について図面を参照して説明する。本発明の第８の実施の形態における携帯電話機１００の動作について説明する。図３２は、本発明の第８の実施の形態における携帯電話機１００の動作を説明するフローチャートである。

【０１５３】

まず、画像入力部１１１が、ユーザの顔を撮影して画像データを生成し、生成した画像データを画像・認証結果表示部１１２と入力データ処理部１３１－８とに出力する（ステップＳ８０１）。画像・認証結果表示部１１２は、入力された画像データの画像を表示する。そして、音声入力部１１４にユーザの音声が入力されると、ユーザ音声データを生成して入力データ処理部１３１－８に出力する（ステップＳ８０２）。例えば、このとき音声入力部１１４に入力する音声は、予め決められた特定の言葉である。また、ユーザに指先を指紋形状入力部１１６に接触させ、指紋形状入力部１１６に指紋の形状を入力すると（ステップＳ８０３）、指紋形状入力部１１６は、入力された指紋の形状を画像のデータに変換してユーザ指紋画像データを生成し、生成したユーザ指紋画像データを画像・認証結果表示部１１２と入力データ処理部１３１－８とに出力する。画像・認証結果表示部１１２は、入力されたユーザ指紋画像データの画像を表示する。

【０１５４】

入力データ処理部１３１－８は、画像入力部１１１が入力したユーザの顔の画像データと入力データ認証用データ記憶部１３２－８が記憶しているアクセス許可者の顔の画像データとをマッチングする処理と、音声入力部１１４が入力したユーザ音声データと入力データ認証用データ記憶部１３２－８が記憶している許可者音声データとをマッチングする処理と、指紋形状入力部１１６が入力したユーザ指紋画像データと、入力データ認証用データ記憶部１３２－８が記憶している許可者指紋画像データとをマッチングする処理とである認証処理を行ない（ステップＳ８０４）、携帯電話機１００のユーザがアクセス許可者であるか否かを判定する。なお、入力データ処理部１３１－８は、各マッチング処理のそれぞれの全てにおいて合致した場合に携帯電話機１００のユーザがアクセス許可者であると判定する。

【０１５５】

入力データ処理部１３１－８は、認証処理の結果、携帯電話機１００のユーザがアクセス許可者であるか否かを画像・認証結果表示部１１２に表示させる（ステップＳ８０５）。入力データ処理部１３１－８は、ユーザがアクセス許可者であると判定すると（ステップＳ８０６）、ユーザにパスワードの入力を要求する画面を画像・認証結果表示部１１２に表示させる。ユーザが、操作入力部３５にパスワードを入力すると、操作入力部３５は入力されたパスワードを入力データ処理部１３１－８に出力する。なお、入力データ処理部１３１－８は、記憶部３３－８が予め記憶しているパスワードを読みだしてもよい。入力データ処理部１３１－８は、携帯電話機１００の電話番号と、ユーザがアクセス許可者であることを示す情報と、パスワードとを組み合わせた情報である認証情報を、認証部１３３に入力し、認証部１３３は入力された認証情報をデータ送信部１１３－２に出力し、データ送信部１１３－２に、各基地局のいずれかと制御局４００と通信ネットワーク７００とを介して身元確認システム５００へ送信させる（ステップＳ８０７）。

【０１５６】

入力データ処理部１３１－８は、ユーザがアクセス許可者でないと判定すると（ステップＳ８０６）、ユーザが利用することができる携帯電話機１００の機能を制限する（ステップＳ８０８）。具体的には、電話機能、電子メール送受信機能、ウェブ閲覧機能等の使用を制限する。

【０１５７】

本発明の第８の実施の形態における身元確認システム５００の動作は、本発明の第５の実施の形態における身元確認システム５００の動作と同様なため説明を省略する。

【０１５８】

以上、述べたように、この実施の形態によれば、ユーザの、顔の画像データと音声データと指紋の画像データとを用いて、ユーザが銀行システム６００へのアクセスを許可を許可するべき人物であるか否かを判定しているため、より厳密なユーザ認証を行なうことができる。

【０１５９】

なお、第５の実施の形態から第８の実施の形態では、銀行システム６００へのアクセスのユーザ認証について述べたが、本発明はこれに限定されるものではなく、厳密なユーザ認証を必要とする多様なシステムへ適用することができる。

【０１６０】

また、上記の各実施の形態では、ユーザが入退場資格を有する者でない、またはアクセス資格を有する者でないと判定された場合には、ユーザが利用することができる携帯電話機１００の機能を制限するようにしたが、そのように制御しなくてもよい。例えば、入退場を許可しなかったり、アクセスを許可しないようにするだけであってもよい。

【産業上の利用可能性】

【０１６１】

本発明は、厳密なセキュリティ管理を必要とする特定の場所への入退場や、銀行システム等へのアクセス等に利用することができる。

【図面の簡単な説明】

【０１６２】

【図１】本発明による携帯電話機の外観の一例を示す説明図である。

【図２】本発明の第１の実施の形態によるセキュリティ管理システムの構成を示す説明図である。

【図３】本発明の第１の実施の形態による携帯電話機の構成を説明するブロック図である。

【図４】本発明の第１の実施の形態による携帯電話機において、本発明の第１の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【図５】本発明の第１の実施の形態によるセキュリティ管理装置の構成を説明するブロック図である。

【図６】本発明の第１の実施の形態によるセキュリティ管理装置において、本発明の第１の実施の形態による携帯電話機から受信した情報を処理する部分の構成を示すブロック図である。

【図７】本発明の第１の実施の形態における携帯電話機の動作を説明するフローチャートである。

【図８】本発明の第１の実施の形態におけるセキュリティ管理装置の動作を説明するフローチャートである。

【図９】本発明の第２の実施の形態による携帯電話機の構成を説明するブロック図である。

【図１０】本発明の第２の実施の形態による携帯電話機において、本発明の第２の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【図１１】本発明の第２の実施の形態における携帯電話機の動作を説明するフローチャートである。

【図１２】本発明の第３の実施の形態による携帯電話機の構成を説明するブロック図である。

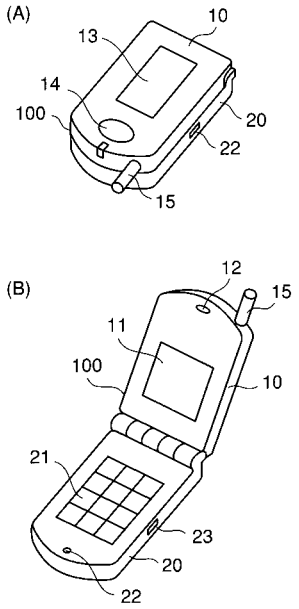
【図１３】本発明の第３の実施の形態による携帯電話機において、本発明の第３の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。

【図１４】本発明の第３の実施の形態における携帯電話機の動作を説明するフローチャートである。

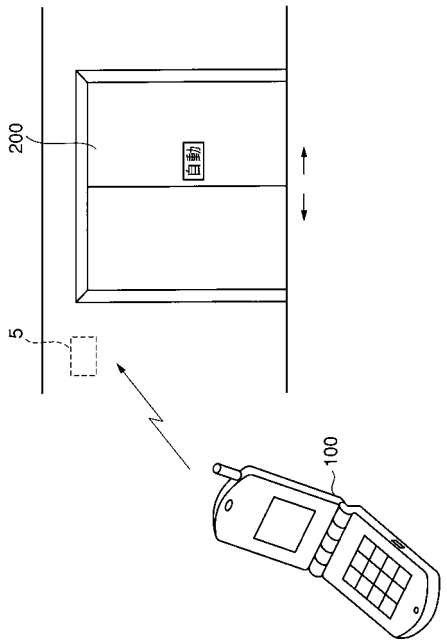
【図１５】本発明の第４の実施の形態による携帯電話機の構成を説明するブロック図である。
【図１６】本発明の第４の実施の形態による携帯電話機において、本発明の第４の実施の形態によるセキュリティ管理装置に送信する情報を処理する部分の構成を示すブロック図である。
【図１７】本発明の第４の実施の形態における携帯電話機の動作を説明するフローチャートである。
【図１８】本発明の第５の実施の形態によるセキュリティ管理システムの構成を示す説明図である。
【図１９】本発明の第５の実施の形態による携帯電話機の構成を説明するブロック図である。
【図２０】本発明の第５の実施の形態による携帯電話機において、本発明の第５の実施の形態による身元確認システムに送信する情報を処理する部分の構成を示すブロック図である。
【図２１】本発明の第５の実施の形態の身元確認システムの構成を示すブロック図である。
【図２２】本発明の第５の実施の形態における携帯電話機の動作を説明するフローチャートである。
【図２３】本発明の第５の実施の形態における身元確認システムの動作を説明するフローチャートである。
【図２４】本発明の第６の実施の形態による携帯電話機の構成を説明するブロック図である。
【図２５】本発明の第６の実施の形態による携帯電話機において、本発明の第６の実施の形態による身元確認システムに送信する情報を処理する部分の構成を示すブロック図である。
【図２６】本発明の第６の実施の形態における携帯電話機の動作を説明するフローチャートである。
【図２７】本発明の第７の実施の形態による携帯電話機の構成を説明するブロック図である。
【図２８】本発明の第７の実施の形態による携帯電話機において、本発明の第７の実施の形態による身元確認システムに送信する情報を処理する部分の構成を示すブロック図である。
【図２９】本発明の第７の実施の形態における携帯電話機の動作を説明するフローチャートである。
【図３０】本発明の第８の実施の形態による携帯電話機の構成を説明するブロック図である。
【図３１】本発明の第８の実施の形態による携帯電話機において、本発明の第８の実施の形態による身元確認システムに送信する情報を処理する部分の構成を示すブロック図である。
【図３２】本発明の第８の実施の形態における携帯電話機の動作を説明するフローチャートである。
【符号の説明】
【０１６３】
１０　上部筐体部
１１　第１の表示部
１２　スピーカ
１３　第２の表示部
１４　カメラ
１５　アンテナ
２１　操作部

２２　マイクロフォン
２３　シャッターボタン
３０　無線通信部
３１－１、３１－２　音声処理回路
３２－１、３２－２、３２－３、３２－４、３２－５、３２－６、３２－７、３２－８
携帯電話機主制御部
３３－１、３３－２、３３－３、３３－４、３３－５、３３－６、３３－７、３３－８
記憶部
３４　ブルートゥース回路
３５　操作入力部
３６　表示部
３７　データ入出力インタフェース
３８　接続コネクタ
３９　カメラユニット
４０　セキュリティ管理装置主制御部
４１　中央処理装置
４２　プログラム記憶部
４３　データ記憶部
４４　入出力インタフェース
５１　ブルートゥース回路
５２　セキュリティ管理ドア制御部
６０　指紋入力部
１００　携帯電話機
１１１　画像入力部
１１２　画像・認証結果表示部
１１３－１、１１３－２　データ送信部
１１４　音声入力部
１１５　認証結果表示部
１１６　指紋形状入力部
１３０　認証処理部
１３１－１、１３１－２、１３１－３、１３１－４、１３１－５、１３１－６、１３１－７、１３１－８　入力データ処理部
１３２－１、１３２－２、１３２－３、１３２－４、１３２－５、１３２－６、１３２－７、１３２－８　入力データ認証用データ記憶部
１３３　認証部
２００　セキュリティ管理ドア
２１３　データ受信部
２３０　認証結果処理部
２３１　受信データ認証用データ記憶部
２３２　受信データ処理部
２３３　制御部
３００、３０１、３０ｎ　基地局
４００　制御局
５００　身元確認システム
５０１　通信部
５０２　身元確認システム制御部
５０３　身元確認システム記憶部
６００　銀行システム
７００　通信ネットワーク

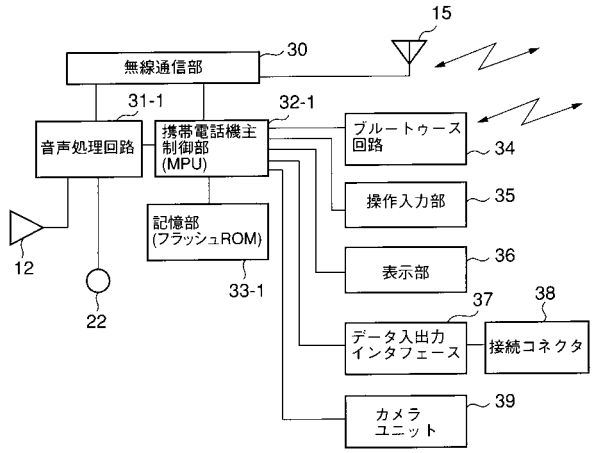
【図１】


(A)
10
13
14
100
20
22
15
(B)
12
15
11
100
10
21
23
20
22

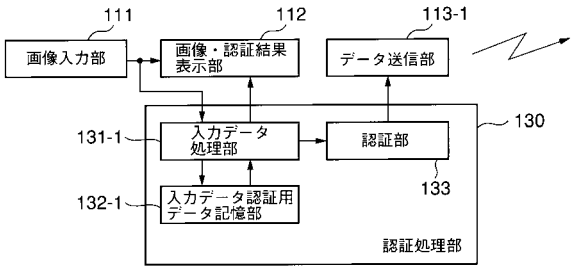
【図２】


200
自動
5
100

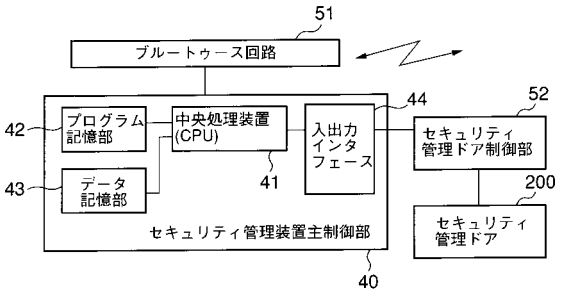
【図３】


15
無線通信部
30
31-1
32-1
音声処理回路
携帯電話機主制御部(MPU)
ブルートゥース回路
34
操作入力部
35
記憶部(フラッシュROM)
33-1
表示部
36
12
22
37
38
データ入出力インタフェース
接続コネクタ
カメラユニット
39

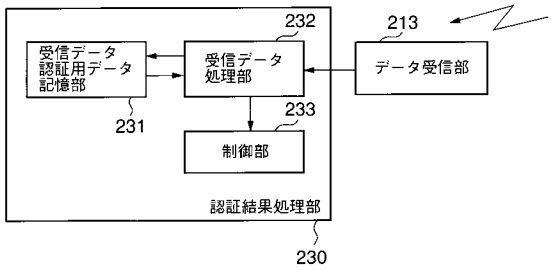
【図４】


111
112
113-1
画像入力部
画像・認証結果表示部
データ送信部
131-1
入力データ処理部
認証部
130
132-1
入力データ認証用データ記憶部
133
認証処理部

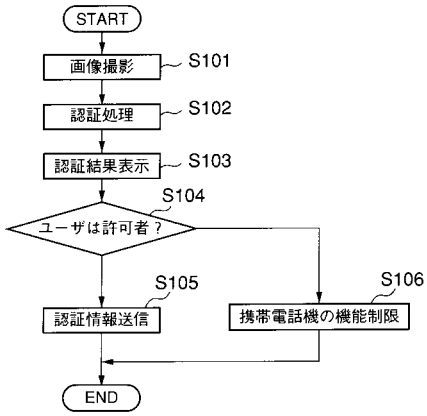
【図５】


51
ブルートゥース回路
44
52
42
プログラム記憶部
中央処理装置(CPU)
入出力インタフェース
セキュリティ管理ドア制御部
43
データ記憶部
41
200
セキュリティ管理ドア
セキュリティ管理装置主制御部
40

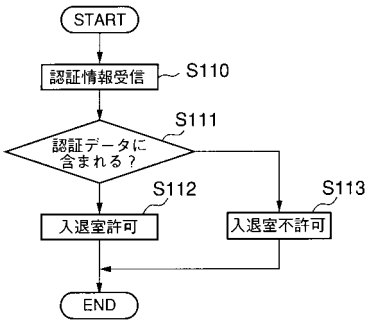
【図６】



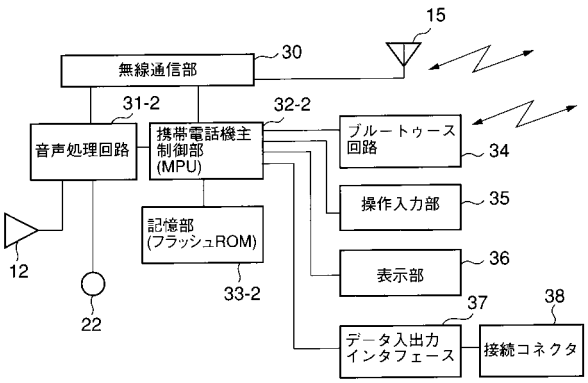
【図７】



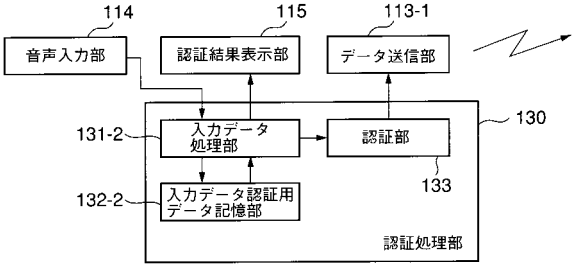
【図８】



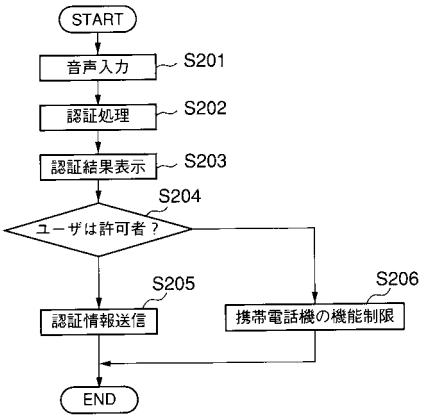
【図９】



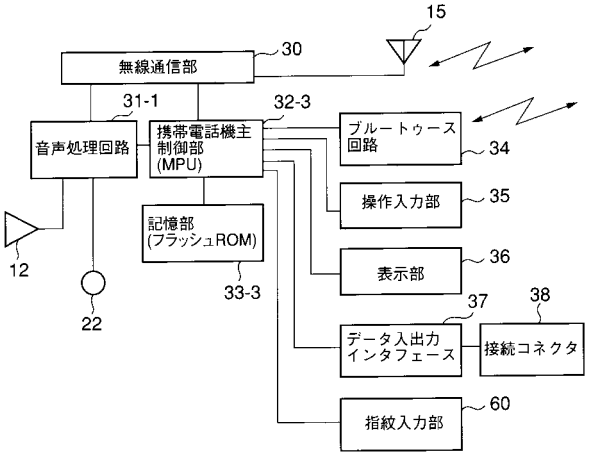
【図１０】



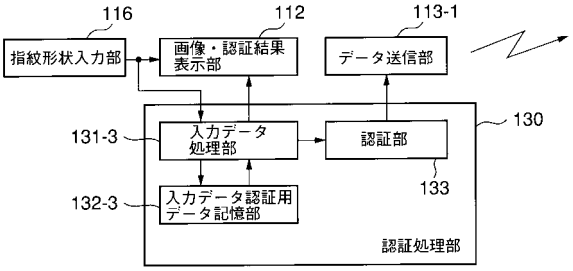
【図１１】



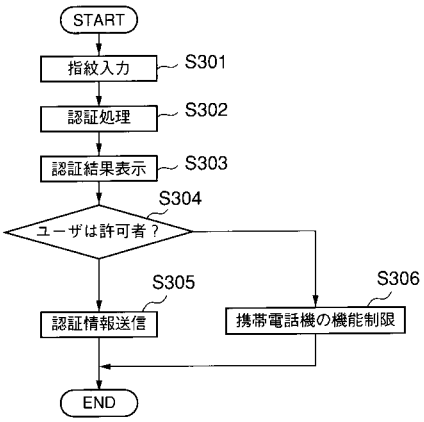
【図１２】



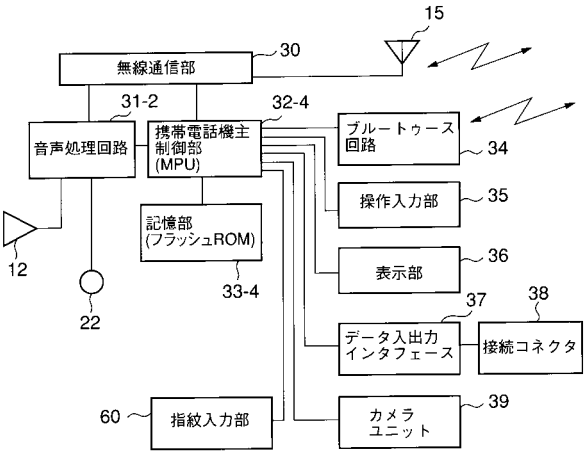
【図１３】



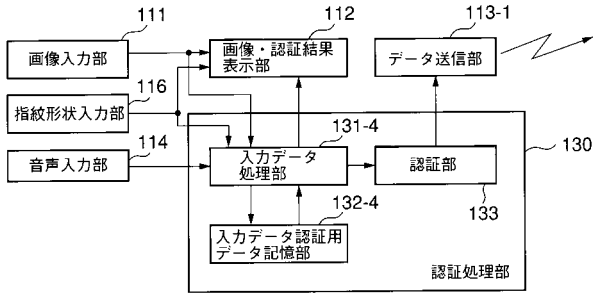
【図１４】



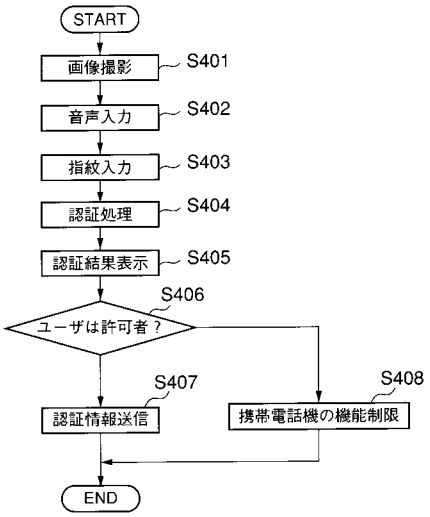
【図１５】



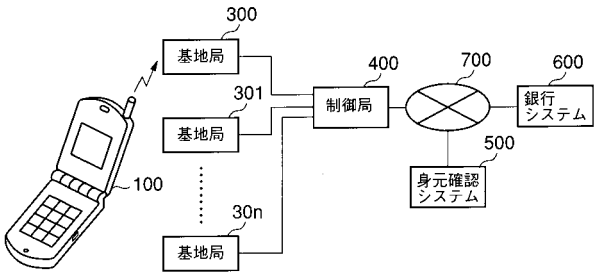
【図１６】



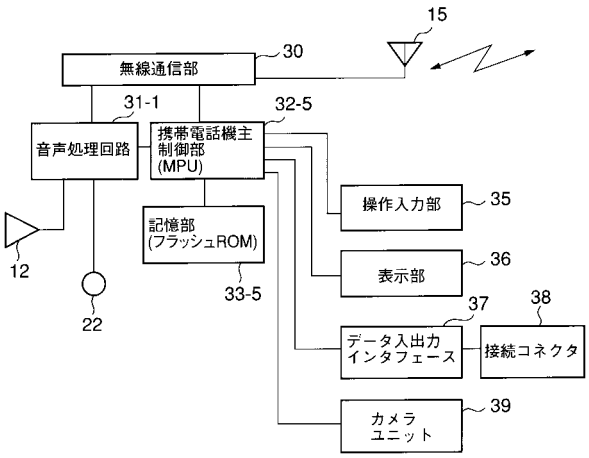
【図１７】



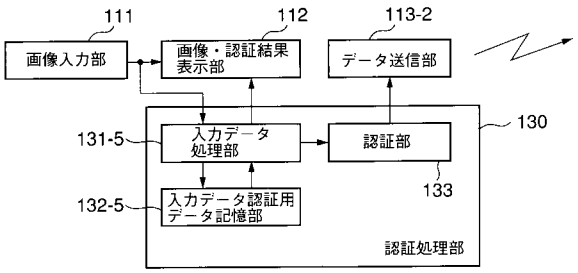
【図１８】



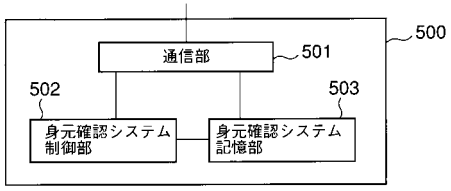
【図１９】



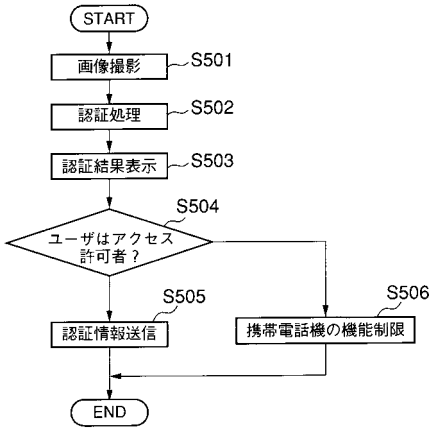
【図２０】



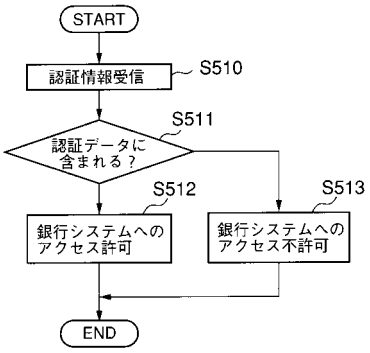
【図２１】



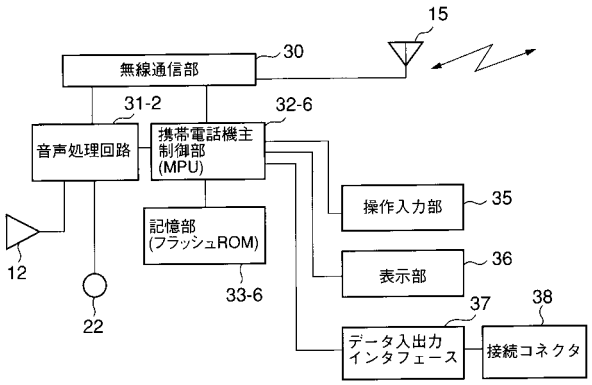
【図２２】



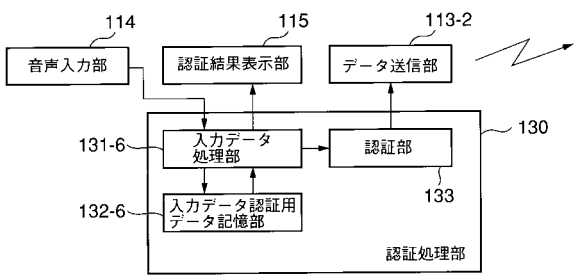
【図２３】



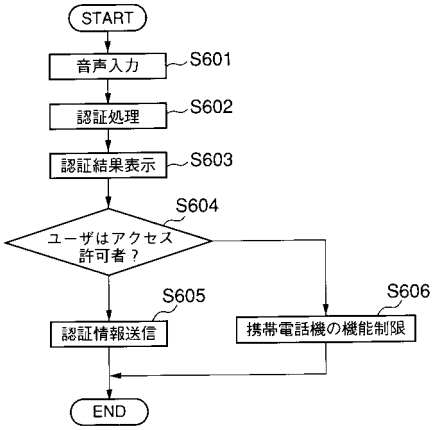
【図２４】



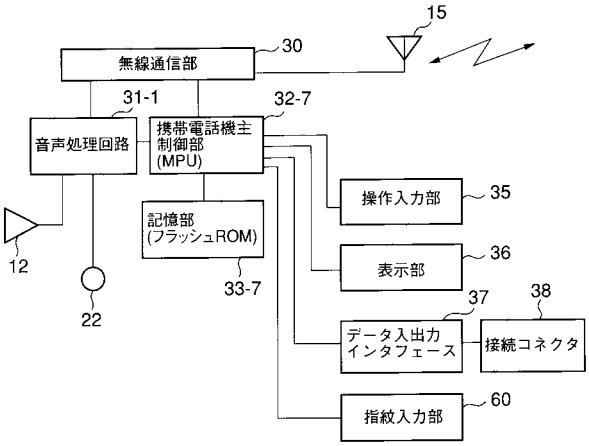
【図２５】



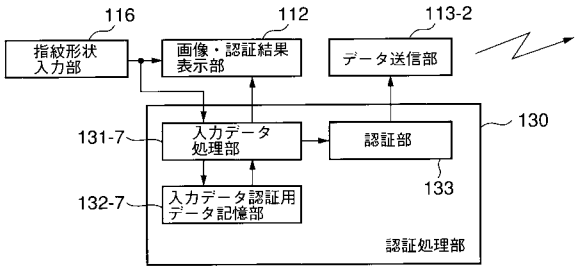
【図２６】



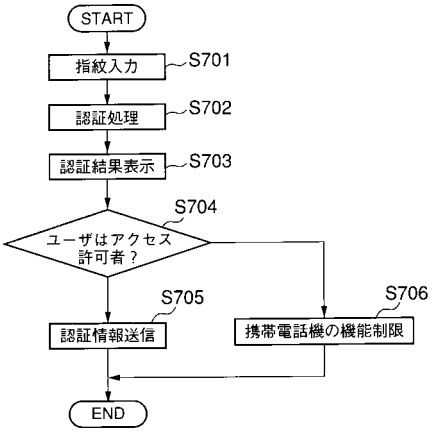
【図２７】



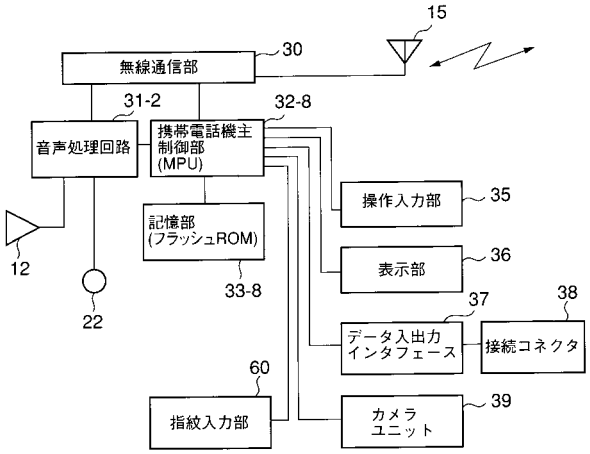
【図２８】



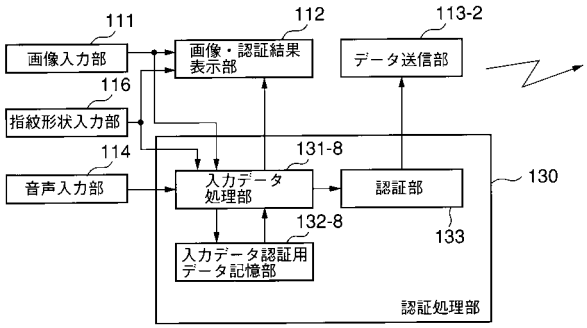
【図２９】



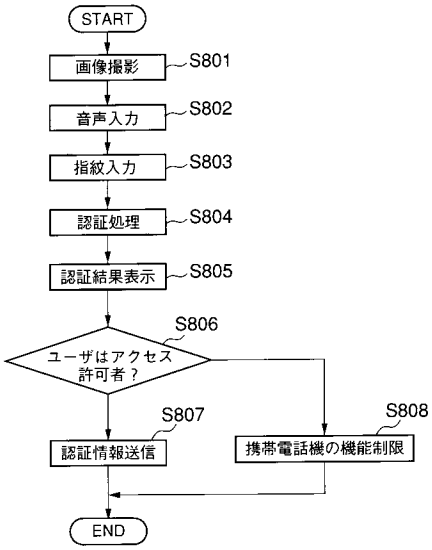
【図３０】



【図３１】



【図３２】


START
画像撮影
S801
音声入力
S802
指紋入力
S803
認証処理
S804
認証結果表示
S805
S806
ユーザはアクセス許可者？
S807
認証情報送信
S808
携帯電話機の機能制限
END

フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
Ｈ０４Ｍ 3/42	Ｈ０４Ｂ 7/26 Ｍ	

Ｆターム(参考) 5K024 AA62 AA79 CC11 GG01 GG05 GG08
5K067 AA41 BB04 BB21 EE02 EE12 EE35 GG01 GG11 HH22 HH23
5K101 KK13 LL12 NN06 NN21 PP03