(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2010-55368
(P2010-55368A)
(43)公開日　平成22年3月11日(2010.3.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285
H04L 9/10	(2006.01)	H04L	9/00	621Z	5J104
H04L 9/32	(2006.01)	H04L	9/00	673D	

審査請求 未請求　請求項の数 6　ＯＬ　（全 19 頁）

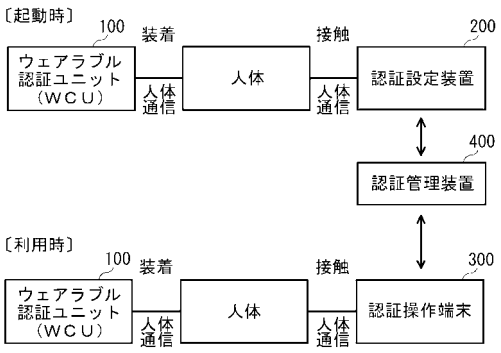
(21)出願番号　特願2008-219517 (P2008-219517)
(22)出願日　平成20年8月28日 (2008.8.28)

(71)出願人　000003621
株式会社竹中工務店
大阪府大阪市中央区本町４丁目１番１３号
(74)代理人　100107364
弁理士　斉藤　達也
(72)発明者　近藤　正芳
千葉県印西市大塚一丁目５番地１　株式会社竹中工務店技術研究所内
(72)発明者　高井　浩一郎
東京都江東区新砂一丁目１番１号　株式会社竹中工務店東京本店内

Ｆターム(参考)　5B285 AA01 BA00 CB12 CB42 CB53 CB89 DA10
5J104 AA07 AA16 EA03 EA08 EA16 KA01 NA05 NA36 NA41

(54)【発明の名称】認証システム及び携帯認証端末

(57)【要約】
【課題】高度な安全性を維持しつつ、認証の際の操作が簡易で利便性を向上することができる認証システム及び携帯型認証端末を提供すること。
【解決手段】認証システムは、被認証者に装着されるウェアラブル認証ユニット（ＷＣＵ）１００、認証操作を行う認証操作端末３００、及び認証管理を行う認証管理装置４００を備える。ＷＣＵ１００は、被認証者に対するＷＣＵ１００の装着有無を検知する装着検知手段と、ＷＣＵ１００又は被認証者を一意に識別するための識別情報を記憶する識別情報記憶手段と、被認証者によるＷＣＵ１００の装着が継続して行われていることを条件として、識別情報を、被認証者を媒体とした人体通信にて認証操作端末３００に送信する携帯認証端末側人体通信手段とを備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
被認証者に装着される携帯認証端末、被認証者の認証操作を行うための認証操作端末、及び前記認証操作端末に接続されるものであって認証管理を行う認証管理装置を備えた認証システムであって、
前記携帯認証端末は、
前記被認証者に対する当該携帯認証端末の装着有無を検知する装着検知手段と、
当該携帯認証端末又は当該携帯認証端末を装着している前記被認証者を一意に識別するための識別情報を記憶する識別情報記憶手段と、
前記装着検知手段の検知結果に基づいて、前記被認証者による当該携帯認証端末の装着が当該携帯認証端末の起動後に継続して行われているか否かを判定し、当該装着が当該起動後に継続して行なわれていることを条件として、前記識別情報記憶手段にて記憶されている前記識別情報を、当該被認証者を媒体とした人体通信にて前記認証操作端末に送信する携帯認証端末側人体通信手段とを備え、
前記認証操作端末は、
前記携帯認証端末側人体通信手段から人体通信にて送信された前記識別情報を受信する認証操作端末側人体通信手段と、
前記認証管理装置との間で前記識別情報を含む情報を通信する認証操作端末側通信手段とを備え、
前記認証管理装置は、
前記識別情報と、前記被認証者の認証可否を特定する認証可否情報とを、対応付けて記憶する認証可否情報記憶手段と、
前記認証操作端末との間で前記識別情報を含む情報を通信する認証管理装置側通信手段と、
前記認証管理装置側通信手段を介して前記認証操作端末から受信された前記識別情報に基づいて前記認証可否情報記憶手段を参照し、当該受信された識別情報に対応する前記認証可否情報を取得することにより、前記被認証者の認証可否を判定する認証可否手段とを備えたこと、
を特徴とする認証システム。
【請求項２】
前記認証管理装置に接続されるものであって前記被認証者の認証に必要な情報の設定を行う認証設定装置を備え、
前記認証設定装置は、
前記被認証者を一意に特定するための被認証者識別情報の入力を受け付ける被認証者識別情報入力手段と、
前記認証管理装置との間で前記被認証者識別情報を含む情報を通信する認証設定装置側通信手段と、
前記携帯認証端末を起動させるための起動信号を当該携帯認証端末に対して送信する起動信号送信手段と、
前記被認証者識別情報入力手段にて前記被認証者識別情報の入力が受け付けられた場合に、当該被認証者識別情報を前記認証設定装置側通信手段を介して前記認証管理装置に送信し、当該認証管理装置から前記携帯認証端末の起動を許可する旨の起動許可信号を受信した場合に、前記起動信号送信手段を介して前記起動信号を前記携帯認証端末に送信する認証設定手段とを備え、
前記認証管理装置は、
前記被認証者識別情報と、前記被認証者に装着された前記携帯認証端末の起動可否を特定する起動可否情報とを、対応付けて記憶する起動可否情報記憶手段を備え、
前記認証管理装置の前記認証可否手段は、前記認証管理装置側通信手段を介して前記認証設定装置から受信された前記被認証者識別情報に基づいて前記起動可否情報記憶手段を参照し、当該受信された被認証者識別情報に対応する前記起動可否情報を取得することに

より、前記被認証者に装着された前記携帯認証端末の起動可否を判定し、起動可である場合には前記起動許可信号を前記認証管理装置側通信手段を介して前記認証設定装置に送信し、

前記携帯認証端末は、前記認証設定装置から送信された前記起動信号を受信する携帯認証端末側通信手段を備え、

前記携帯認証端末の前記携帯認証端末側人体通信手段は、当該携帯認証端末が前記被認証者に装着されていることが前記装着検知手段にて検知されていること、及び、前記携帯認証端末側通信手段を介して前記起動信号が受信されたことを条件として、前記識別情報を送信すること、

を特徴とする請求項１に記載の認証システム。

【請求項３】

前記携帯認証端末の前記識別情報記憶手段は、前記識別情報として、当該携帯認証端末を一意に識別するための携帯認証端末識別情報を記憶し、

前記携帯認証端末の前記携帯認証端末側人体通信手段は、当該携帯認証端末が前記被認証者に装着されていることが前記装着検知手段にて検知されていること、及び、前記携帯認証端末側通信手段を介して前記起動信号が受信されたことを条件として、前記携帯認証端末識別情報を送信すること、

を特徴とする請求項２に記載の認証システム。

【請求項４】

前記携帯認証端末の前記識別情報記憶手段は、前記識別情報として、前記被認証者識別情報を記憶し、

前記携帯認証端末の前記携帯認証端末側人体通信手段は、当該携帯認証端末が前記被認証者に装着されていることが前記装着検知手段にて検知されていること、及び、前記携帯認証端末側通信手段を介して前記起動信号が受信されたことを条件として、前記被認証者識別情報を送信すること、

を特徴とする請求項２に記載の認証システム。

【請求項５】

前記認証設定装置の前記認証設定手段は、前記起動信号として、前記被認証者識別情報入力手段にて受け付けられた前記被認証者識別情報を前記起動信号送信手段を介して前記携帯認証端末に送信し、

前記携帯認証端末は、前記携帯認証端末側通信手段を介して受信された前記被認証者識別情報を前記識別情報記憶手段に記憶させること、

を特徴とする請求項４に記載の認証システム。

【請求項６】

被認証者に装着される携帯認証端末であって、

前記被認証者に対する当該携帯認証端末の装着状態を検知する装着検知手段と、

当該携帯認証端末又は当該携帯認証端末を装着している前記被認証者を一意に識別するための識別情報を記憶する識別情報記憶手段と、

前記装着検知手段の検知結果に基づいて、前記被認証者による当該携帯認証端末の装着が当該携帯認証端末の起動後に継続して行われているか否かを判定し、当該装着が当該起動後に継続して行なわれていることを条件として、前記識別情報記憶手段にて記憶されている前記識別情報を、当該被認証者を媒体とした人体通信にて前記認証操作端末に送信する携帯認証端末側人体通信手段と、

を備えたことを特徴とする携帯認証端末。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、被認証者に装着される端末を利用して当該被認証者の認証を行うための認証システム及び携帯型認証端末に関する。

【背景技術】

【０００２】
従来から、入退出管理等における認証方法として、入退出が許可された被認証者に、当該被認証者を一意に識別するためのＩＤが記憶されたＩＤカード等の認証デバイスを所持させて、入退出の際にそのＩＤカードに記憶されたＩＤを、カード情報読み取り装置等にて読み取り、当該読み取ったＩＤを予め登録されたＩＤと照合することが行われている。
【０００３】
しかしながら、このようなＩＤカードを用いた認証方法では、入退出を許可されていない第三者がＩＤカードを何らかの不正手段によって入手してしまうと、当該第三者がＩＤカードの正当な被認証者になりすまして入退室を行うことが可能となる危険性がある。
【０００４】
このため、このような問題を回避するために、ＩＤカードのＩＤ情報に代えて、被認証者自身の人体の特徴である生体情報を用いて本人認証を行う生体認証の技術も実用化されている。この生体認証としては、指紋を生体情報として用いる指紋認証、静脈を生体情報として用いる静脈認証、あるいは、顔画像を撮像してその顔画像の特徴量を生体情報として用いる顔認証等がある。このような生体認証の技術では、不正な第三者による正当な者へのなりすましを防止することができる（例えば特許文献１参照）。
【０００５】
【特許文献１】特開２００８－１２３３１２
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、このような生体認証の技術では、被認証者の生体情報を認証に使用するので、クリーンルームや実験室等への入退室等で被認証者が手袋を着用している場合には指紋認証を行うことができなかったり、マスクやサングラス等を着用している場合には顔認証を行うことができない。このため、このような場合には、被認証者は、認証を行う毎に手袋やサングラス等の着用物を着脱しなければならず、認証作業が煩雑になるという問題がある。特に、半導体製造工場の如き高清浄度のクリーンルーム内で認証が必要になる場合には、手袋やサングラス等を取り外すことが好ましくない場合があり、生体情報による認証自体が困難になる。
【０００７】
本発明は、上記に鑑みてなされたものであって、高度な安全性を維持しつつ、認証の際の操作が簡易で利便性を向上することができる認証システム及び携帯型認証端末を提供することを目的とする。
【課題を解決するための手段】
【０００８】
上述した課題を解決し、目的を達成するために、請求項１に記載の認証システムは、被認証者に装着される携帯認証端末、被認証者の認証操作を行うための認証操作端末、及び前記認証操作端末に接続されるものであって認証管理を行う認証管理装置を備えた認証システムであって、前記携帯認証端末は、前記被認証者に対する当該携帯認証端末の装着有無を検知する装着検知手段と、当該携帯認証端末又は当該携帯認証端末を装着している前記被認証者を一意に識別するための識別情報を記憶する識別情報記憶手段と、　前記装着検知手段の検知結果に基づいて、前記被認証者による当該携帯認証端末の装着が当該携帯認証端末の起動後に継続して行われているか否かを判定し、当該装着が当該起動後に継続して行なわれていることを条件として、前記識別情報記憶手段にて記憶されている前記識別情報を、当該被認証者を媒体とした人体通信にて前記認証操作端末に送信する携帯認証端末側人体通信手段とを備え、前記認証操作端末は、前記携帯認証端末側人体通信手段から人体通信にて送信された前記識別情報を受信する認証操作端末側人体通信手段と、前記認証管理装置との間で前記識別情報を含む情報を通信する認証操作端末側通信手段とを備え、前記認証管理装置は、前記識別情報と、前記被認証者の認証可否を特定する認証可否情報とを、対応付けて記憶する認証可否情報記憶手段と、前記認証操作端末との間で前記

識別情報を含む情報を通信する認証管理装置側通信手段と、前記認証管理装置側通信手段を介して前記認証操作端末から受信された前記識別情報に基づいて前記認証可否情報記憶手段を参照し、当該受信された識別情報に対応する前記認証可否情報を取得することにより、前記被認証者の認証可否を判定する認証可否手段とを備えたことを特徴とする。

【０００９】

請求項２に記載の認証システムは、請求項１に記載の認証システムにおいて、前記認証管理装置に接続されるものであって前記被認証者の認証に必要な情報の設定を行う認証設定装置を備え、前記認証設定装置は、前記被認証者を一意に特定するための被認証者識別情報の入力を受け付ける被認証者識別情報入力手段と、前記認証管理装置との間で前記被認証者識別情報を含む情報を通信する認証設定装置側通信手段と、前記携帯認証端末を起動させるための起動信号を当該携帯認証端末に対して送信する起動信号送信手段と、前記被認証者識別情報入力手段にて前記被認証者識別情報の入力が受け付けられた場合に、当該被認証者識別情報を前記認証設定装置側通信手段を介して前記認証管理装置に送信し、当該認証管理装置から前記携帯認証端末の起動を許可する旨の起動許可信号を受信した場合に、前記起動信号送信手段を介して前記起動信号を前記携帯認証端末に送信する認証設定手段とを備え、前記認証管理装置は、前記被認証者識別情報と、前記被認証者に装着された前記携帯認証端末の起動可否を特定する起動可否情報とを、対応付けて記憶する起動可否情報記憶手段を備え、前記認証管理装置の前記認証可否手段は、前記認証管理装置側通信手段を介して前記認証設定装置から受信された前記被認証者識別情報に基づいて前記起動可否情報記憶手段を参照し、当該受信された被認証者識別情報に対応する前記起動可否情報を取得することにより、前記被認証者に装着された前記携帯認証端末の起動可否を判定し、起動可である場合には前記起動許可信号を前記認証管理装置側通信手段を介して前記認証設定装置に送信し、前記携帯認証端末は、前記認証設定装置から送信された前記起動信号を受信する携帯認証端末側通信手段を備え、前記携帯認証端末の前記携帯認証端末側人体通信手段は、当該携帯認証端末が前記被認証者に装着されていることが前記装着検知手段にて検知されていること、及び、前記携帯認証端末側通信手段を介して前記起動信号が受信されたことを条件として、前記識別情報を送信することを特徴とする。

【００１０】

請求項３に記載の認証システムは、請求項２に記載の認証システムにおいて、前記携帯認証端末の前記識別情報記憶手段は、前記識別情報として、当該携帯認証端末を一意に識別するための携帯認証端末識別情報を記憶し、前記携帯認証端末の前記携帯認証端末側人体通信手段は、当該携帯認証端末が前記被認証者に装着されていることが前記装着検知手段にて検知されていること、及び、前記携帯認証端末側通信手段を介して前記起動信号が受信されたことを条件として、前記携帯認証端末識別情報を送信することを特徴とする。

【００１１】

請求項４に記載の認証システムは、請求項２に記載の認証システムにおいて、前記携帯認証端末の前記識別情報記憶手段は、前記識別情報として、前記被認証者識別情報を記憶し、前記携帯認証端末の前記携帯認証端末側人体通信手段は、当該携帯認証端末が前記被認証者に装着されていることが前記装着検知手段にて検知されていること、及び、前記携帯認証端末側通信手段を介して前記起動信号が受信されたことを条件として、前記被認証者識別情報を送信することを特徴とする。

【００１２】

請求項５に記載の認証システムは、請求項４に記載の認証システムにおいて、前記認証設定装置の前記認証設定手段は、前記起動信号として、前記被認証者識別情報入力手段にて受け付けられた前記被認証者識別情報を前記起動信号送信手段を介して前記携帯認証端末に送信し、前記携帯認証端末は、前記携帯認証端末側通信手段を介して受信された前記被認証者識別情報を前記識別情報記憶手段に記憶させることを特徴とする。

【００１３】

請求項６に記載の携帯認証端末は、被認証者に装着される携帯認証端末であって、前記被認証者に対する当該携帯認証端末の装着状態を検知する装着検知手段と、当該携帯認証

端末又は当該携帯認証端末を装着している前記被認証者を一意に識別するための識別情報を記憶する識別情報記憶手段と、前記装着検知手段の検知結果に基づいて、前記被認証者による当該携帯認証端末の装着が当該携帯認証端末の起動後に継続して行われているか否かを判定し、当該装着が当該起動後に継続して行なわれていることを条件として、前記識別情報記憶手段にて記憶されている前記識別情報を、当該被認証者を媒体とした人体通信にて前記認証操作端末に送信する携帯認証端末側人体通信手段とを備えたことを特徴とする。

【発明の効果】

【００１４】

請求項１に記載の認証システム又は請求項６に記載の携帯認証端末によれば、被認証者による携帯認証端末の装着が当該携帯認証端末の起動後に継続して行われていることを条件として、携帯認証端末から識別情報が送信され、この識別情報に基づいて被認証者の認証が行われるので、正当な被認証者以外の第三者が被認証者から携帯認証端末を取り外して認証を行った場合には、認証情報が送信されないために認証をパスしないため、第三者によるなりすましを防止することができ、認証の確実性を向上させることができる。

また、携帯認証端末から送信された識別情報に基づいて被認証者の認証が行われるので、マスクや手袋を装着した状態のままで認証作業を行うことができ、認証作業を簡素化することができる。さらに、被認証者が認証操作端末に触れることによる自然な動作で認証が行なわれるので、被認証者の作業や思考を中断することなく認証を行うことが可能となる。

【００１５】

請求項２に記載の認証システムによれば、携帯認証端末は、当該携帯認証端末が被認証者に装着されており、かつ、認証設定装置から起動信号が受信されたことを条件として、識別情報を送信するので、被認証者に装着されていない状態で当該携帯認証端末が起動されて識別情報が送信されることを防止でき、認証の確実性を一層向上させることができる。

【００１６】

請求項３に記載の認証システムによれば、携帯認証端末には携帯認証端末識別情報が記憶され、被認証者識別情報が記憶されないので、携帯認証端末が盗難等にあっても、この携帯認証端末から、個人情報である被認証者識別情報が漏洩することを確実に防止できる。さらに、従来のＩＣカードのように被認証者識別情報が記録されていた場合には、各被認証者に１枚のＩＣカードを支給する必要があったが、この認証システムでは、同時に認証を行う必要がない複数の被認証者の相互間で同一の携帯認証端末を共有できるので、携帯認証端末の総数を低減でき、コストを低減できる。

【００１７】

請求項４に記載の認証システムによれば、携帯認証端末から認証管理装置に被認証者識別情報が送信されるので、携帯認証端末識別情報が送信される場合と異なり、認証管理装置においては、携帯認証端末識別情報に基づいて被認証者識別情報を取得するための構成や処理が不要となり、認証管理装置の構成や処理を簡易化できる。さらに、従来のＩＣカードのように被認証者識別情報が記録されていた場合には、各被認証者に１枚のＩＣカードを支給する必要があったが、この認証システムでは、同時に認証を行う必要がない複数の被認証者の相互間で同一の携帯認証端末を共有できるので、携帯認証端末の総数を低減でき、コストを低減できる。

【００１８】

請求項５に記載の認証システムによれば、起動信号として被認証者識別情報を携帯認証端末に送信するので、被認証者識別情報によって起動信号を兼用化でき、携帯認証端末の起動処理を簡易化できる。

【発明を実施するための最良の形態】

【００１９】

以下に添付図面を参照して、この発明に係る認証システム及び携帯認証端末の各実施の

形態を詳細に説明する。まず、各実施の形態の構成及び処理内容について説明し、各実施の形態に対する変形例について説明する。ただし、各実施の形態によって本発明が限定されるものではない。

【００２０】

〔実施の形態１〕

まず実施の形態１について説明する。この形態は、携帯認証端末の識別情報記憶手段に携帯認証端末識別情報を記憶させる形態である。

【００２１】

図１は、実施の形態１に係る認証システムの構成と、認証処理の概要を説明するためのブロック図である。認証システムは、図１に示すように、携帯認証端末であるウェアラブル認証ユニット（Ｗｅａｒａｂｌｅ　Ｃｅｒｔｉｆｉｃａｔｅ　Ｕｎｉｔ，以下「ＷＣＵ」）１００、認証設定装置２００、認証操作端末３００、及び認証管理装置（データベースサーバ）４００を備えて構成されている。

【００２２】

（概要）

まず、これら各装置の構成及び機能の概要を説明する。ＷＣＵ１００は、被認証者に着脱自在に装着されて、当該ＷＣＵ１００を一意に識別するためのユニットＩＤを当該被認証者を媒体とした人体通信により定期的に送信するものであって、特許請求の範囲における携帯認証端末に対応する。認証設定装置２００は、被認証者から入力された当該被認証者の生体情報（以下「人体ＩＤ」と称する）に基づいて当該被認証者の本人認証を行うものであって、特許請求の範囲における認証設定装置に対応する。認証操作端末３００は、ＷＣＵ１００から送信されたユニットＩＤを人体通信により受信し、当該ユニットＩＤに基づいて、当該ＷＣＵ１００を装着している被認証者の認証を行うものであって、特許請求の範囲における認証操作端末に対応する。認証管理装置４００は、認証設定装置２００及び認証操作端末３００に接続されて認証管理を行うものであり、特許請求の範囲における認証管理装置に対応する。

【００２３】

このように構成されたＷＣＵ１００と認証設定装置２００の相互間、あるいは、ＷＣＵ１００と認証操作端末３００の相互間では、当該ＷＣＵ１００を装着した被認証者を媒体とした人体通信を行う。人体通信とは、人体が微弱な電流を流す性質を応用して当該人体を通信媒体の代わりとして使い、近距離のデータ通信を行う技術である。具体的には、人体の体内電流の変化を利用したり、送信側の機器から、人体に無害な程度の電流を流すことで体内電流を変化させ、受信側の機器で変化を読みとることで、通信を実現する。

【００２４】

この他、ＷＣＵ１００と認証設定装置２００は、無線通信によっても通信を行うことができる。また、認証設定装置２００と認証管理装置４００の相互間、あるいは、認証操作端末３００と認証管理装置４００の相互間は、無線または有線（例えばインターネットやＬＡＮ：Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ等のネットワークを含む）によって通信を行うことができる。なお、無線通信としては、光通信、電波通信、あるいは音波通信を含む任意の無線通信を行うことができる。

【００２５】

図１の上方にはＷＣＵ１００の起動時の認証処理の概要、下方にはＷＣＵ１００の利用時の認証処理の概要をそれぞれ示す。ＷＣＵ１００の起動時には、当該ＷＣＵ１００を装着した被認証者が認証設定装置２００に自己の人体ＩＤ（生体情報）を入力し、認証設定装置２００はこの人体ＩＤ（生体情報）に基づいて被認証者の認証を行う。認証をクリアした場合、認証設定装置２００からの起動信号によってＷＣＵ１００を起動させる。「ＷＣＵ１００を起動させる」とは、ＷＣＵ１００をユニットＩＤの送信が可能となる状態にすることを意味する。すなわち、ＷＣＵ１００に記憶されたユニットＩＤを人体通信によって認証設定装置２００に送信する。認証設定装置２００は、受信したユニットＩＤを認証管理装置４００に送信し、認証管理装置４００はユニットＩＤ等の登録を行う。

【００２６】
ＷＣＵ１００の利用時には、当該ＷＣＵ１００を装着した被認証者が、管理エリアの入り口等に設置された認証操作端末３００に対して、当該ＷＣＵ１００を所定の通信距離内に位置させること又は接触させることにより、人体通信によりユニットＩＤを認証操作端末３００に送信する。認証操作端末３００は受信したユニットＩＤを認証管理装置４００に送信し、認証管理装置４００が当該ユニットＩＤに基づいて被認証者の認証を行い、この認証結果を認証操作端末３００に送信する。認証操作端末３００は、認証管理装置４００からの認証結果に基づいて、入り口の扉を自動開錠する等の所定の処理を行う。
【００２７】
（構成－ＷＣＵ）
次に、本実施の形態の認証システムの詳細について説明する。最初に、ＷＣＵ１００の構成について説明する。図２は、ＷＣＵ１００の構成を機能概念的に示すブロック図である。ＷＣＵ１００は、接触センサ１０１、人体通信部１０２、通信部１０３、制御部１０４、入力部１０５、出力部１０６、及びＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０７を備えて構成されている。
【００２８】
接触センサ１０１は、被認証者に対するＷＣＵ１００の装着有無を検知するもので、特許請求の範囲における装着検知手段に対応する。この接触センサ１０１は、例えば、温度センサ及び脈拍センサを組み合わせて構成されており、温度センサにて所定範囲の体温が検出されている場合であって、脈拍センサにて所定範囲の脈拍が検出されている場合に、被認証者に対してＷＣＵ１００が装着されているものと検知する。この接触センサ１０１には、被認証者に対するＷＣＵ１００の装着が継続的に行われているか否かを検知する機能が付加されており、例えば、温度センサによる体温検出や脈拍センサによる脈拍検出が所定時間以上途絶した場合には、被認証者からＷＣＵ１００が取り外されたものと判定する。あるいは、接触センサ１０１は、ＷＣＵ１００を被認証者に手首に装着するためのリストバンドの状態を監視しており、リストバンドのロック機構が解除された場合や、リストバンドの引き出し長さが被認証者の手首の外周長さを超えて手を通過可能な所定長さ以上となった場合には、被認証者からＷＣＵ１００が取り外されたものと判定する。接触センサ１０１は、これらの検知結果及び判定結果を含んだ信号を制御部１０４に出力する。
【００２９】
人体通信部１０２は、人体通信を行う通信モジュールである。この人体通信部１０２は、接触センサ１０１の検知結果に基づいて、被認証者によるＷＣＵ１００の装着が当該ＷＣＵ１００の起動後に継続して行われているか否かを判定し、当該装着が当該起動後に継続して行なわれていることを条件として、ＲＯＭ１０７にて記憶されているユニットＩＤを、当該被認証者を媒体とした人体通信にて認証設定装置２００に送信するもので、特許請求の範囲における携帯認証端末側人体通信手段に対応する。
【００３０】
通信部１０３は、認証設定装置２００から起動信号を受信したり、その他の各種の情報を認証設定装置２００との間で送受信する無線通信モジュールである。
【００３１】
制御部１０４は、ＷＣＵ１００の全体を制御する制御手段であり、例えばＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）及び当該ＣＰＵ上で解釈実行されるプログラムから構成される。
【００３２】
入力部１０５は、当該ＷＣＵ１００に対して任意の情報を入力するための入力手段であり、例えば、操作ボタン等の公知の入力デバイスとして構成される。
【００３３】
出力部１０６は、当該ＷＣＵ１００の外部に対して任意の情報を出力するための出力手段であり、例えば、液晶ディスプレイ等の公知の出力デバイスとして構成される。
【００３４】

ＲＯＭ１０７は、ＷＣＵ１００を一意に識別するための識別情報（認証端末識別情報）であるユニットＩＤを記憶するもので、特許請求の範囲における識別情報記憶手段に対応する。ただし、ユニットＩＤを記憶する記憶媒体は任意であり、ＲＯＭに代えてフレッシュメモリ等を用いることもできるが、ユニットＩＤが不正に書換え等されることがない記憶媒体や記憶形式を採用することが好ましく、例えばユニットＩＤを暗号化してＲＯＭ１０７に記憶させてもよい。

【００３５】

（構成－認証設定装置）

次に、認証設定装置２００の構成について説明する。図３は、認証設定装置２００の構成を機能概念的に示すブロック図である。認証設定装置２００は、通信部２０１、認証部２０２、生体情報入力部２０３、登録部２０４、及び読み取り装置２１０を備えて構成されている。

【００３６】

通信部２０１は、認証管理装置４００との間でユニットＩＤや人体ＩＤ（生体情報）を含む情報を通信するもので、特許請求の範囲における認証設定装置側通信手段に対応する。また、通信部２０１は、ＷＣＵ１００を起動させるための起動信号を当該ＷＣＵ１００に対して送信するもので、特許請求の範囲における起動信号送信手段に対応する。

【００３７】

認証部２０２は、生体情報入力部２０３にて人体ＩＤ（生体情報）の入力が受け付けられた場合に、当該人体ＩＤ（生体情報）を通信部２０１を介して認証管理装置４００に送信し、当該認証管理装置４００からＷＣＵ１００の起動を許可する旨の起動許可信号を受信した場合に、通信部２０１を介して起動信号をＷＣＵ１００に送信するもので、特許請求の範囲における認証設定手段に対応する。

【００３８】

生体情報入力部２０３は、被認証者を一意に特定するための被認証者識別情報の入力を受け付けるもので、特許請求の範囲における被認証者識別情報入力手段に対応する。ここでは、被認証者識別情報は被認証者の人体ＩＤ（生体情報）であり、生体情報入力部２０３は、人体ＩＤ（生体情報）としての指紋情報をスキャンするスキャナや、人体ＩＤ（生体情報）としての顔画像を撮像するカメラ等である。

【００３９】

登録部２０４は、認証管理装置４００に、人体ＩＤやユニットＩＤを登録する登録手段である。

【００４０】

読み取り装置２１０は、ＷＣＵ１００からユニットＩＤを読み取る読取り手段であり、人体通信部２１１を備える。この人体通信部２１１は、ＷＣＵ１００の人体通信部１０２から人体通信にて送信されたユニットＩＤを人体通信により受信する人体通信手段である。

【００４１】

（構成－認証操作端末）

次に、認証操作端末３００の構成について説明する。図４は、認証操作端末３００の構成を機能概念的に示すブロック図である。認証操作端末３００は、通信部３０１、登録部３０２、制御部３０３、表示部３０４、ＲＯＭ３０５、及び読み取り装置３１０を備えて構成されている。

【００４２】

通信部３０１は、認証管理装置４００との間でユニットＩＤを含む情報を通信するもので、特許請求の範囲における認証操作端末側通信手段に対応する。また、通信部３０１は、ＷＣＵ１００との無線通信による送受信を行う通信モジュールである。

【００４３】

登録部３０２は、認証管理装置４００に、ユニットＩＤや機器ＩＤを登録する登録手段である。

【００４４】
制御部３０３は、認証管理装置４００から受信した制御信号や表示情報に基づいて所定の制御処理や表示処理を実行する。このような処理として例えば、入室許可／不許可に基づく入り口のドアの開閉制御や入室許可の表示部３０４への表示あるいは入室不許可の旨の表示部３０４への表示を制御する。
【００４５】
表示部３０４は、被認証者に各種情報を表示するものであり、例えば、液晶ディスプレイ等が該当する。
【００４６】
ＲＯＭ３０５は、認証操作端末３００を一意に識別するための機器ＩＤを記憶した記憶媒体である。ただし、機器ＩＤを記憶する記憶媒体は任意であり、ＲＯＭに代えてフレッシュメモリ等を用いることもできるが、機器ＩＤが不正に書換え等されることがない記憶媒体や記憶形式を採用することが好ましく、例えば機器ＩＤを暗号化してＲＯＭ３０５に記憶させてもよい。
【００４７】
読み取り装置３１０は、ＷＣＵ１００からユニットＩＤを読み取るものであり、具体的には、人体通信部３１１を備えている。この人体通信部３１１は、ＷＣＵ１００から被認証者を媒体とした人体通信によりユニットＩＤを受信するもので、特許請求の範囲における認証操作端末側人体通信手段に対応する。
【００４８】
この認証操作端末３００は、被認証者の認証のみを行う認証専用装置として構成することもできるが、被認証者によって操作される公知の機器に、被認証者の認証を行う機能を付加することで構成してもよい。例えば、認証操作端末３００は、管理エリアへの入退室用の扉を制御する扉制御装置であり、この場合、被認証者が当該認証操作端末３００に触れることにより、制御部３０３が人体ＩＤに基づく制御信号に従って扉の開閉制御を行う。また、認証操作端末３００は、例えば、製造工場に用いられる情報端末（例えば、各種の情報をモニタに表示する端末であり、キオスク端末と称されるものを含む）であり、この場合には、被認証者が当該認証操作端末３００に触れることにより、制御部３０３が被認証者ＩＤに応じたメニュー画面を表示部３０４に表示する。また、認証操作端末３００は、製造工場におけるハンディターミナルであり、被認証者が当該認証操作端末３００に触れることにより、人体ＩＤに基づく表示情報を表示部３０４に表示したり、作業の継続指示等の出力を行う。また、認証操作端末３００は、例えば、情報伝達を行うための情報端末であり、この場合、制御部３０３は、人体ＩＤに基づく制御信号と表示情報に従って、電子メールの送信や、電話による通話を行えるように制御する。なお、認証操作端末３００の例は、これらに限定されるものではなく、任意の処理制御を行うように構成することができる。以下の実施の形態では、主として、認証操作端末３００が扉制御装置である場合について説明する。
【００４９】
（構成－認証管理装置）
次に、認証管理装置４００の構成について説明する。図５は、認証管理装置４００の構成を機能概念的に示すブロック図である。認証管理装置４００は、通信部４０１、ＤＢ管理部４０２、認証データベース（以下「認証ＤＢ」）４１０、登録データベース（以下「登録ＤＢ」）４２０、コンテンツデータベース（「コンテンツＤＢ」）４３０、及び利用データベース（「利用ＤＢ」）４４０を備えて構成されている。
【００５０】
通信部４０１は、認証設定装置２００や認証操作端末３００との間で各種情報の送受信を行う通信モジュールであり、特許請求の範囲における認証管理装置側通信手段に対応する。本実施の形態では、通信部４０１は、認証設定装置２００から人体ＩＤを受信し、当該人体ＩＤが認証ＤＢ４１０に登録されているか否かの認証結果を認証設定装置２００に送信する。また、通信部４０１は、認証操作端末３００からユニットＩＤや機器ＩＤを受

信し、表示情報や利用可否情報を認証操作端末３００に送信する。

【００５１】

ＤＢ管理部４０２は、認証ＤＢ４１０、登録ＤＢ４２０、コンテンツＤＢ４３０、利用ＤＢ４４０に対するデータの参照や登録を行うもので、特許請求の範囲における認証可否手段に対応する。

【００５２】

認証ＤＢ４１０は、被認証者の認証を行うための認証情報を格納するもので、特許請求の範囲における認証可否情報記憶手段に対応する。この認証情報の構成例を図６（ａ）に示す。認証情報は、被認証者を一意に識別するための識別情報である人体ＩＤ（生体情報）、及びＷＣＵ１００の起動可否（認証情報の認証可否）を示す起動可否情報を相互に対応付けて構成されている。

【００５３】

図５の登録ＤＢ４２０は、被認証者が利用する機器に関する登録情報を格納する格納手段である。この登録情報の構成例を図６（ｂ）に示す。登録情報は、人体ＩＤ、ユニットＩＤ、及び認証操作端末３００を一意に識別するための機器ＩＤを相互に対応付けて構成されている。

【００５４】

図５のコンテンツＤＢ４３０は、ＷＣＵ１００や認証操作端末３００に出力するコンテンツ情報を格納する格納手段である。このコンテンツ情報の構成例を図６（ｃ）に示す。コンテンツ情報は、人体ＩＤ、機器ＩＤ、及び被認証者に対して表示すべき表示情報を相互に対応付けて構成されている。

【００５５】

図５の利用ＤＢ４４０は、被認証者による各認証操作端末３００の利用可否を特定するための利用情報を格納するもので、特許請求の範囲における認証可否情報記憶手段に対応する。この利用情報の構成例を図６（ｄ）に示す。利用情報は、人体ＩＤ、機器ＩＤ、及び各認証操作端末３００の利用可否を示す利用可否情報を相互に対応付けて構成されている。

【００５６】

（処理－起動処理）

次に、以上のように構成された認証システムによる認証処理について説明する。まず、ＷＣＵ１００の起動処理について説明する。図７は、ＷＣＵ１００の起動処理のフローチャートである。なお、この処理の前提として、認証管理装置４００の認証ＤＢ４１０には図６（ａ）に示す情報、コンテンツＤＢ４３０には図６（ｃ）に示す情報、及び利用ＤＢ４４０には図６（ｄ）に示す情報が、予め任意の方法で格納されているものとする。

【００５７】

被認証者は、認証ステーションにおいてＷＣＵ１００の装着及び起動処理を行う。認証ステーションとは、被認証者の認証作業を行うエリアであり、例えばクリーンルームの前室が該当し、被認証者が入室する他、当該被認証者がＷＣＵ１００の装着を行った事実を目視等にて監視する監視員が配置される。この認証ステーションにおいて、監視員の監視下、被認証者はＷＣＵ１００を装着する。このＷＣＵ１００の電源ＯＮ後、接触センサ１０１は、被認証者とＷＣＵ１００との接触検知の有無の継続的な監視を開始し（ステップＳＡ－１）、この接触を検知した場合には（ステップＳＡ－１，Ｙｅｓ）、制御部１０４に接触検知信号を出力する。この接触検知信号の出力を受けた制御部１０４は、当該ＷＣＵ１００を、認証設定装置２００からの起動信号の受信待ち状態とする（ステップＳＡ－２）。

【００５８】

また、認証ステーションには認証設定装置２００が設置されており、被認証者が、ＷＣＵ１００を装着した状態のまま、自己の人体ＩＤ（生体情報）を生体情報入力部２０３を介して入力すると（ステップＳＡ－３，Ｙｅｓ）、認証部２０２は、入力された人体ＩＤ（生体情報）を認証管理装置４００に送信する（ステップＳＡ－４）。この人体ＩＤ（生

体情報）を受信した認証管理装置４００のＤＢ管理部４０２は（ステップＳＡ－５，Ｙｅｓ）、認証部２０２から送信された人体ＩＤ（生体情報）に対応して予め設定されている起動可否情報を認証ＤＢ４１０から取得し、この起動可否情報を含んだ起動可否信号を認証設定装置２００に送信する（ステップＳＡ－６）。

【００５９】

認証設定装置２００は、認証管理装置４００から受信した起動可否信号に含まれる起動可否情報に基づいて、ＷＣＵ１００の起動が許可されているか否かを判定し（ステップＳＡ－７)、許可されていない場合には（ステップＳＡ－７，Ｎｏ）、ステップＳＡ－３に戻り、許可されている場合には（ステップＳＡ－７，Ｙｅｓ）、通信部２０１を介してＷＣＵ１００に所定の起動信号を無線送信する（ステップＳＡ－８）。

【００６０】

この起動信号を通信部１０３を介して受信したＷＣＵ１００の制御部１０４は（ステップＳＡ－２，Ｙｅｓ）、当該ＷＣＵ１００を起動状態とし、自己のＲＯＭ１０７に記憶されているユニットＩＤを人体通信部１０２による人体通信にて送信可能な人体通信待ち状態とする（ステップＳＡ－９）。その後、被認証者が、ＷＣＵ１００を装着した状態のまま、認証設定装置２００の読み取り装置２１０に接触すると、ＷＣＵ１００の人体通信部１０２と認証設定装置２００の人体通信部２１１との間で被認証者を媒体とした人体通信が行われ（ステップＳＡ－９，Ｙｅｓ）、ユニットＩＤが人体通信部１０２から人体通信部２１１に送信される（ステップＳＡ－１０）（ステップＳＡ－１１，Ｙｅｓ）。認証設定装置２００の登録部２０４は、このように送信されたユニットＩＤと、ステップＳＡ－３で受信した人体ＩＤ（生体情報）とを対応付けて、認証管理装置４００に送信する（ステップＳＡ－１２）。認証管理装置４００のＤＢ管理部４０２は、認証設定装置２００から送信されたユニットＩＤと人体ＩＤとを対応付けて登録ＤＢ４２０に登録する（ステップＳＡ－１３，Ｙｅｓ）（ステップＳＡ－１４）。これにてＷＣＵ１００の起動処理が終了する。

【００６１】

なお、ステップＳＡ－１において接触が検知された以降、被認証者に対するＷＣＵ１００の装着状態は接触センサ１０１にて継続的に監視されており（ステップＳＡ－１５）、当該装着が継続的に行われている限りにおいて、ユニットＩＤの送信可能状態を継続するが、当該装着が継続的に行われていないこと（被認証者からＷＣＵ１００が少なくとも一次的に取り外されたこと）が接触センサ１０１にて検知された場合（ステップＳＡ－１５，Ｙｅｓ）、ユニットＩＤの送信可能状態がリセットされて当該ユニットＩＤの送信が停止される（ステップＳＡ－１６）。この場合には、再びステップＳＡ－１に戻り、監視員の監視下で被認証者がＷＣＵ１００を再び装着しない限り、ステップＳＡ－９のように人体通信を行っても、ユニットＩＤが認証設定装置２００に送信されないため、ユニットＩＤを登録ＤＢ４２０に登録することができなくなる。また、後述する利用処理においてもＷＣＵ１００からのユニットＩＤの送信が不可となる。従って、ＷＣＵ１００を起動状態とした後、被認証者がＷＣＵ１００を不正に第三者に受け渡した場合でも、この第三者によるなりすましを防止できる。

【００６２】

（処理－利用処理）

次に、このようにして起動されたＷＣＵ１００の利用処理について説明する。図８は、ＷＣＵ１００の利用処理のフローチャートである。被認証者が、ＷＣＵ１００を装着した状態のままで、入り口等に設置された認証操作端末３００の前に立ち、この認証操作端末３００の読み取り装置３１０に接触すると、ＷＣＵ１００の人体通信部１０２と認証操作端末３００の人体通信部３１１との間で被認証者を媒体とした人体通信が行われ、ユニットＩＤが人体通信部１０２から人体通信部３１１に送信される（ステップＳＢ－１，Ｙｅｓ）（ステップＳＢ－２）。

【００６３】

ここで、認証操作端末３００に対する接触は、必ずしも認証を意図した特別な作業とし

て行う必要はなく、例えば、認証操作端末３００の人体通信部３１１を、被認証者が認証作業以外の通常作業時に触れる位置（例えば入り口扉のドアノブや床面）に配置することで、被認証者が認証作業を意識しない自然な動作の中でユニットＩＤの送信を行うことができる。

【００６４】

なお、上述のように、被認証者からＷＣＵ１００が取り外された場合には（ステップＳＢ－３，Ｙｅｓ）、ユニットＩＤの送信が停止されることから（ステップＳＢ－４）、ステップＳＢ－２のようにユニットＩＤが人体通信部１０２から人体通信部３１１へ送信された場合には、当該事実をもって、被認証者からＷＣＵ１００が取り外されていないことが確認でき、監視員の監視下で最初にＷＣＵ１００が装着された被認証者（すなわち正当な被認証者）が認証操作端末３００に対する操作を行ったことを正確に確認できる。また、各ＷＣＵ１００のＲＯＭ１０７に記憶させるユニットＩＤは定期的に変更することで、セキュリティを一層向上させてもよい。

【００６５】

次いで、認証操作端末３００の制御部３０３は、ＷＣＵ１００からユニットＩＤを受信した場合には（ステップＳＢ－５，Ｙｅｓ）、このユニットＩＤと自己のＲＯＭ３０５に記憶された機器ＩＤを対応付けて、通信部３０１を介して認証管理装置４００に送信する（ステップＳＢ－６）。

【００６６】

認証管理装置４００のＤＢ管理部４０２は、ユニットＩＤと機器ＩＤを通信部４０１を介して受信すると（ステップＳＢ－７，Ｙｅｓ)、これらユニットＩＤ及び機器ＩＤを、登録ＤＢ４２０において当該ユニットＩＤに対応付けて登録されている人体ＩＤに対応付けて、登録ＤＢ４２０に登録する（ステップＳＢ－８）。

【００６７】

また、認証管理装置４００のＤＢ管理部４０２は、認証操作端末３００から受信したユニットＩＤに対応する人体ＩＤを登録ＤＢ４２０から取得することにより、当該ユニットＩＤを人体ＩＤに変換し（ステップＳＢ－９）、この人体ＩＤと認証操作端末３００から受信した機器ＩＤとに対応する表示情報及び利用可否情報をコンテンツＤＢ４３０及び利用ＤＢ４４０から取得して、通信部４０１を介して認証操作端末３００に送信する（ステップＳＢ－１０）。

【００６８】

認証操作端末３００は、認証管理装置４００から通信部３０１を介して利用可否情報を受信すると、制御部３０３が利用可否情報に応じた制御処理を行う（ステップＳＢ－１１，Ｙｅｓ）（ステップＳＢ－１２）。例えば、利用可否情報によって利用許可が示されている場合には、扉の電子錠を自動開錠することで、被認証者の管理エリア内への入室を許可する。

【００６９】

あるいは、認証操作端末３００の制御部３０３は、認証管理装置４００から受信した表示情報に応じた表示処理を行う（ステップＳＢ－１１，Ｙｅｓ）（ステップＳＢ－１２）。例えば、表示処理としては、表示情報に含まれるメッセージを表示部３０４に表示する。あるいは、表示情報に含まれるメッセージを通信部３０１を介してＷＣＵ１００に送信し、当該メッセージを当該ＷＣＵ１００の出力部１０６に表示させる。このような表示処理を行うことで、被認証者や認証操作端末３００に応じたメッセージ等の表示を行うことができ、被認証者に様々な情報（例えば、認証操作端末３００の操作ガイダンス、被認証者への業務連絡等）を提示することが可能となる。なお、必ずしも「表示」に限定されず、例えばＷＣＵ１００にバイブレーション機能を設け、当該バイブレーション機能を表示情報に基づいて作動させることで、被認証者の呼び出しを行い、被認証者に構内電話等にて所定の連絡先に連絡させること等もできる。

【００７０】

この他、認証操作端末３００が情報端末、工程端末、管理端末等として構成された場合

には、当該表示情報に応じて認証操作端末３００の表示部３０４に表示される初期操作画面を変更するようにしてもよい。例えば、認証操作端末３００の図示しない記憶部には、表示情報と初期操作画面との対応関係が予め設定されており、表示情報に応じた初期操作画面を呼び出して表示することで、認証操作端末３００のパーソナライズ化を図ることが可能となる。

【００７１】

また、利用処理における被認証者の認証履歴を認証管理装置４００等に格納し、被認証者の行動内容を監視してもよい。例えば、管理エリアの入り口扉の前後両方に認証操作端末３００の人体通信部３１１を設置し、当該入り口扉に対する出入りのいずれの時点でも認証を行わせることで、所定の動線に反して被認証者が行動した事実を把握したり、このような動線に反する行動を禁止したり、被認証者の現在位置や退出確認等を行うことができる。

【００７２】

（効果）

このように実施の形態１の認証システムでは、ＷＣＵ１００からユニットＩＤが送信され、このユニットＩＤに基づいて被認証者の認証が行われるので、正当な被認証者以外の第三者が被認証者からＷＣＵ１００を取り外して認証を行った場合には、認証情報が送信されないために認証をパスしないため、第三者によるなりすましを防止することができ、認証の確実性を向上させることができる。

【００７３】

また、ＷＣＵ１００から人体通信にて送信されたユニットＩＤに基づいて被認証者の認証が行われるので、マスクや手袋を装着した状態のままで認証作業を行うことができ、認証作業を簡素化することができる。

【００７４】

さらに、被認証者が認証操作端末３００に触れることによる自然な動作で認証が行なわれるので、被認証者の作業や思考を中断することなく認証を行うことが可能となる。

【００７５】

また、ＷＣＵ１００は、当該ＷＣＵ１００が被認証者に装着されており、かつ、認証設定装置２００から起動信号が受信されたことを条件として、ユニットＩＤを送信するので、被認証者に装着されていない状態で当該ＷＣＵ１００が起動されてユニットＩＤが送信されることを防止でき、認証の確実性を一層向上させることができる。

【００７６】

また、ＷＣＵ１００にはユニットＩＤが記憶され、人体ＩＤ（生体情報）が直接記憶されないので、ＷＣＵ１００が盗難等にあっても、このＷＣＵ１００から、個人情報である人体ＩＤ（生体情報）が漏洩することを確実に防止できる。

【００７７】

さらに、従来のＩＣカードのように人体ＩＤ（生体情報）が記録されていた場合には、各被認証者に１枚のＩＣカードを支給する必要があったが、この認証システムでは、同時に認証を行う必要がない複数の被認証者の相互間で同一のＷＣＵ１００を共有できるので、ＷＣＵ１００の総数を低減でき、コストを低減できる。

【００７８】

〔実施の形態２〕

次に、実施の形態２について説明する。この形態は、携帯認証端末の識別情報記憶手段に被認証者識別情報を記憶させる形態である。なお、実施の形態２の構成は、特記する場合を除いて実施の形態１の構成と略同一であり、実施の形態１の構成と略同一の構成についてはこの実施の形態１で用いたのと同一の符号又は名称を必要に応じて付して、その説明を省略する。

【００７９】

（構成－ＷＣＵ）

図９は、実施の形態２に係るＷＣＵの構成を機能概念的に示すブロック図である。ＷＣ

Ｕ１０００は、接触センサ１０１、人体通信部１０２、通信部１０３、制御部１０４、入力部１０５、出力部１０６、ＲＯＭ１０７、及びＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１０８を備えて構成されている。ＲＡＭ１０８は、認証設定装置２００から受信した人体ＩＤを記憶するもので、特許請求の範囲における被認証者識別情報に対応する。

【００８０】

なお、他の構成は実施の形態１と同様であるが、認証管理装置４００の登録ＤＢ４２０には、ユニットＩＤを除いた情報が格納される。

【００８１】

（処理－起動処理）

次に、以上のように構成された認証システムによる認証処理について説明する。まず、ＷＣＵ１０００の起動処理について説明する。図１０は、実施の形態２におけるＷＣＵ１０００の起動処理のフローチャートである。ただし、ステップＳＣ－１、ステップＳＣ－３からＳＣ－７、及びステップＳＣ－９からＳＣ－１５は、図７のステップＳＡ－１、ステップＳＡ－３からＳＡ－７、及びステップＳＡ－９からＳＡ－１５に対して、ユニットＩＤに代えて人体ＩＤを用いた点を除いてそれぞれ同じであるため、その説明を省略する。

【００８２】

認証設定装置２００は、認証管理装置４００から受信した起動可否信号に含まれる起動可否情報に基づいて、ＷＣＵ１０００の起動が許可されているか否かを判定した後（ステップＳＣ－７)、許可されている場合には（ステップＳＣ－７，Ｙｅｓ）、通信部２０１を介してＷＣＵ１０００に起動信号を無線送信する（ステップＳＣ－８）。ここで、起動信号としては、実施の形態１と異なり、ステップＳＣ－３において認証設定装置２００の生体情報入力部２０３に入力された被認証者の人体ＩＤ（生体情報）を送信する。

【００８３】

この人体ＩＤ（生体情報）を受信したＷＣＵ１０００は（ステップＳＣ－２，Ｙｅｓ）、当該受信した人体ＩＤ（生体情報）をＲＡＭ１０８に保存する（ステップＳＣ－２ａ）。その後は、当該ＲＡＭ１０８に保存した人体ＩＤ（生体情報）を、実施の形態１におけるユニットＩＤに代えて用いて、認証設定装置２００への登録等を行う。これにてＷＣＵ１０００の起動処理が完了する。

【００８４】

なお、ステップＳＣ－１において接触が検知された以降、被認証者に対するＷＣＵ１０００の装着状態は接触センサ１０１にて継続的に監視されており（ステップＳＣ－１５）、当該装着が継続的に行われていないこと（被認証者からＷＣＵ１０００が少なくとも一次的に取り外されたこと）が接触センサ１０１にて検知された場合（ステップＳＣ－１５，Ｙｅｓ）、人体ＩＤ（生体情報）の送信可能状態がリセットされて当該人体ＩＤ（生体情報）の送信が停止される（ステップＳＣ－１６）。さらにこの際、ＷＣＵ１０００が取り外されることで、ＲＡＭ１０８に保存されていた人体ＩＤ（生体情報）が自動的に消去されるので、ＷＣＵ１０００の不正使用を一層確実に防止できると共に、個人情報である人体ＩＤ（生体情報）が外部に漏洩することを防止できる。

【００８５】

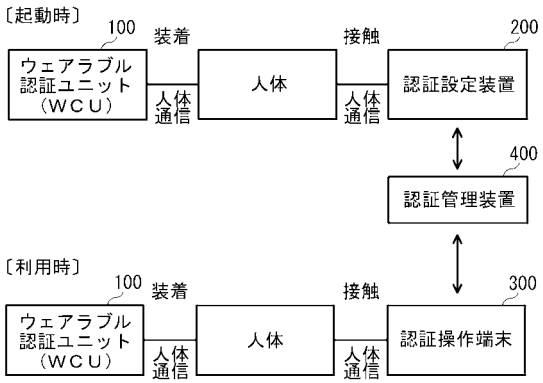
（処理－利用処理）

次に、ＷＣＵ１０００の利用処理について説明する。図１１は、実施の形態２におけるＷＣＵ１０００の利用処理のフローチャートである。ただし、この利用処理では、ＷＣＵ１０００のＲＡＭ１０８に保存した人体ＩＤ（生体情報）を、実施の形態１におけるユニットＩＤに代えて用いる点を除いて、実施の形態１の利用処理と同様であるため、その説明を省略する。なお、この利用処理では、図８のステップＳＢ－９で行っていたユニットＩＤから人体ＩＤ（生体情報）への変換が不要となり、また、ステップＳＤ－４では、人体ＩＤ（生体情報）の送信が停止されると共に、ＲＡＭ１０８に保存されていた人体ＩＤ（生体情報）が自動的に消去される。

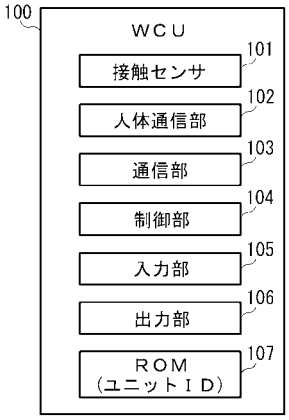
【００８６】
（効果）
　このように実施の形態２の認証システムでは、実施の形態１と同様の効果に加えて、ユニットＩＤから人体ＩＤ（生体情報）を取得するための構成や処理が不要となり、認証操作端末３００の構成や処理を簡易化できる。
【００８７】
〔各実施の形態に対する変形例〕
　以上、本発明に係る各実施の形態について説明したが、本発明の具体的な構成及び手段は、特許請求の範囲に記載した各発明の技術的思想の範囲内において、任意に改変及び改良することができる。
【００８８】
　例えば、上記実施の形態１及び２では、被認証者が認証設定装置２００に生体情報を入力して認証を行っていたが、パスワード等の人体ＩＤ（生体情報）を認証設定装置２００に入力して認証を行うように構成してもよい。
【００８９】
　また、実施の形態１では、人体の体内電流の変化を利用した人体通信を行っていたが、人体を媒体として通信を行えるものであればいずれの方式を用いても良い。
【００９０】
（解決しようとする課題や発明の効果について）
　まず、発明が解決しようとする課題や発明の効果は、前記した内容に限定されるものではなく、本発明によって、前記に記載されていない課題を解決したり、前記に記載されていない効果を奏することもでき、また、記載されている課題の一部のみを解決したり、記載されている効果の一部のみを奏することがある。
【図面の簡単な説明】
【００９１】
【図１】本発明の実施の形態１に係る認証システムの構成と、認証処理の概要を説明するためのブロック図である。
【図２】実施の形態１のＷＣＵの構成を機能概念的に示すブロック図である。
【図３】認証設定装置の構成を機能概念的に示すブロック図である。
【図４】認証操作端末の構成を機能概念的に示すブロック図である。
【図５】認証管理装置の構成を機能概念的に示すブロック図である。
【図６】認証管理装置に格納される情報の構成例を示す図であり、（ａ）は認証情報の構成例、（ｂ）は登録情報の構成例、（ｃ）はコンテンツ情報の構成例、（ｄ）は利用情報の構成例を示す図である。
【図７】実施の形態１におけるＷＣＵの起動処理のフローチャートである。
【図８】実施の形態１におけるＷＣＵの利用処理のフローチャートである。
【図９】実施の形態２に係るＷＣＵの構成を機能概念的に示すブロック図である。
【図１０】実施の形態２におけるＷＣＵの起動処理のフローチャートである。
【図１１】実施の形態２におけるＷＣＵの利用処理のフローチャートである。
【符号の説明】
【００９２】
１００、１０００　ウェアラブル認証ユニット（ＷＣＵ）
１０１　接触センサ
１０２、２１１、３１１　人体通信部
１０３、２０１、３０１、４０１　通信部
１０４、３０３　制御部
１０５　入力部
１０６　出力部
１０７、３０５　ＲＯＭ
１０８　ＲＡＭ

２００　認証設定装置
２０２　認証部
２０３　生体情報入力部
２０４、３０２　登録部
２１０、３１０　読み取り装置
３００　認証操作端末
３０４　表示部
４００　認証管理装置
４０２　ＤＢ管理部
４１０　認証データベース
４２０　登録データベース
４３０　コンテンツデータベース
４４０　利用データベース

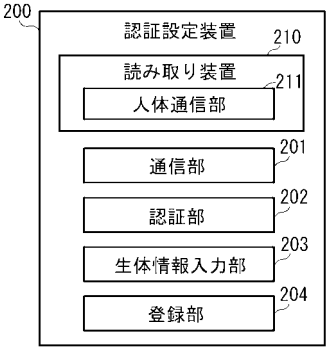
【図１】



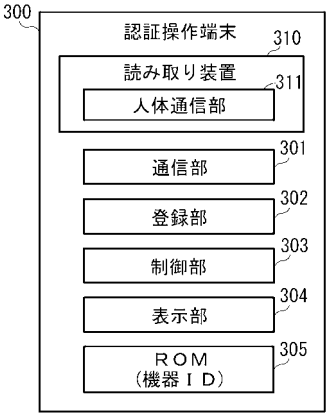
【図２】



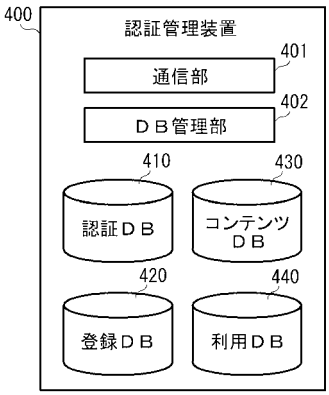
【図３】



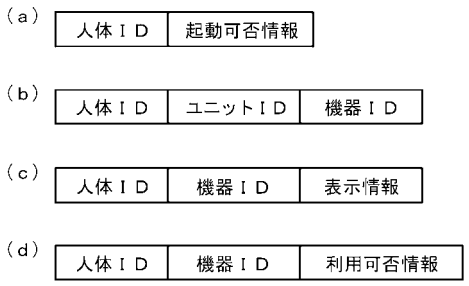
【図４】



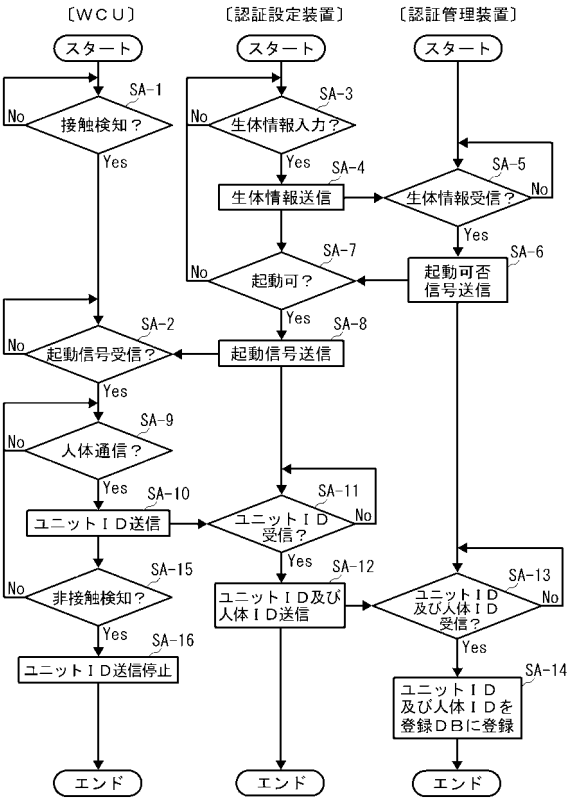
【図５】


400
認証管理装置
401
通信部
402
ＤＢ管理部
410
認証ＤＢ
430
コンテンツＤＢ
420
登録ＤＢ
440
利用ＤＢ

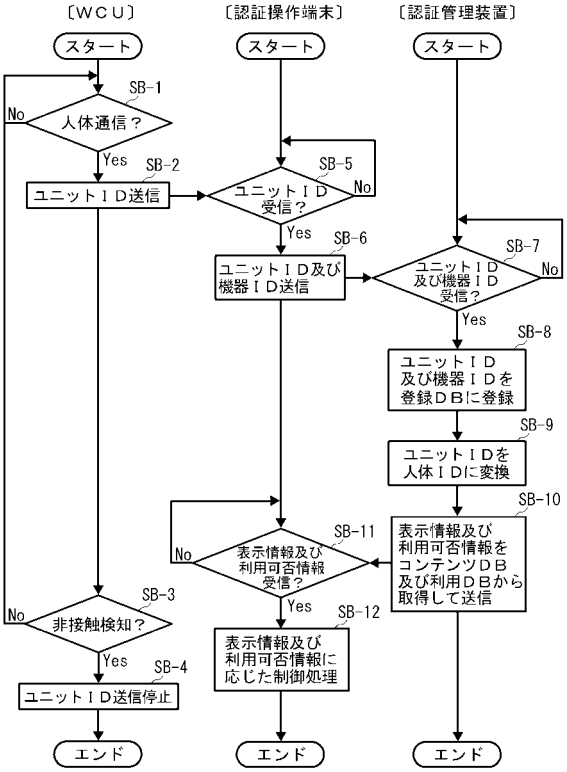
【図６】


（ａ）
人体ＩＤ
起動可否情報
（ｂ）
人体ＩＤ
ユニットＩＤ
機器ＩＤ
（ｃ）
人体ＩＤ
機器ＩＤ
表示情報
（ｄ）
人体ＩＤ
機器ＩＤ
利用可否情報

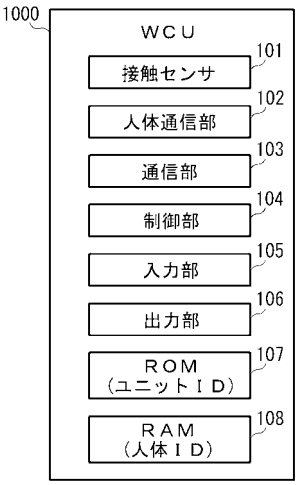
【図７】


〔ＷＣＵ〕
〔認証設定装置〕
〔認証管理装置〕
スタート
SA-1
接触検知？
No
Yes
SA-2
起動信号受信？
SA-3
生体情報入力？
SA-4
生体情報送信
SA-5
生体情報受信？
SA-6
起動可否信号送信
SA-7
起動可？
SA-8
起動信号送信
SA-9
人体通信？
SA-10
ユニットＩＤ送信
SA-11
ユニットＩＤ受信？
SA-12
ユニットＩＤ及び人体ＩＤ送信
SA-13
ユニットＩＤ及び人体ＩＤ受信？
SA-14
ユニットＩＤ及び人体ＩＤを登録ＤＢに登録
SA-15
非接触検知？
SA-16
ユニットＩＤ送信停止
エンド

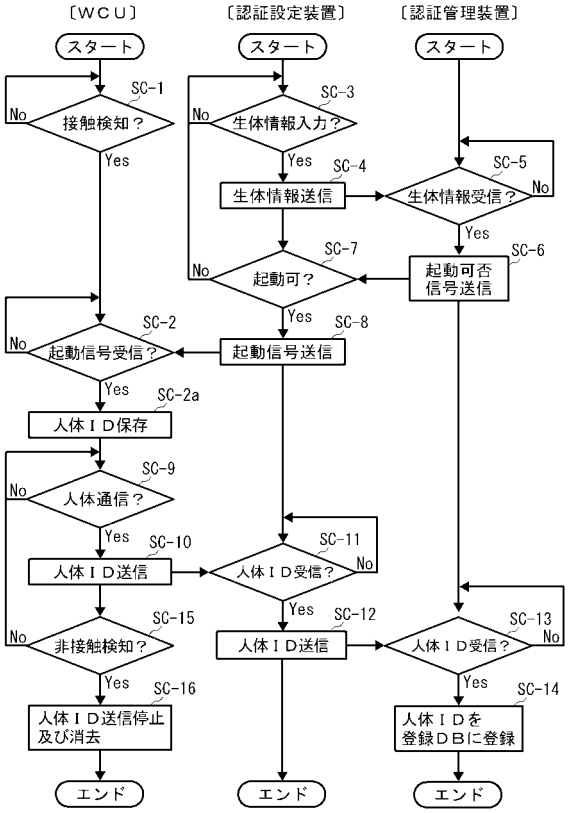
【図８】


〔ＷＣＵ〕
〔認証操作端末〕
〔認証管理装置〕
スタート
SB-1
人体通信？
SB-2
ユニットＩＤ送信
SB-3
非接触検知？
SB-4
ユニットＩＤ送信停止
SB-5
ユニットＩＤ受信？
SB-6
ユニットＩＤ及び機器ＩＤ送信
SB-7
ユニットＩＤ及び機器ＩＤ受信？
SB-8
ユニットＩＤ及び機器ＩＤを登録ＤＢに登録
SB-9
ユニットＩＤを人体ＩＤに変換
SB-10
表示情報及び利用可否情報をコンテンツＤＢ及び利用ＤＢから取得して送信
SB-11
表示情報及び利用可否情報受信？
SB-12
表示情報及び利用可否情報に応じた制御処理
エンド

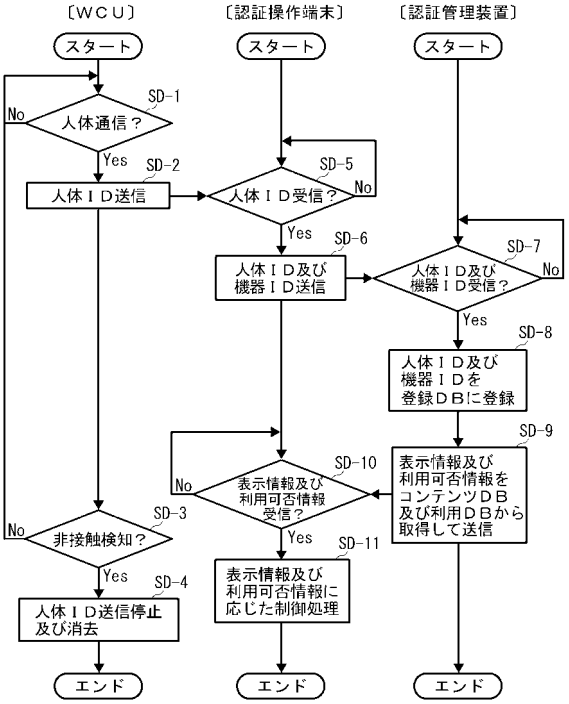
【図９】


1000
ＷＣＵ
101
接触センサ
102
人体通信部
103
通信部
104
制御部
105
入力部
106
出力部
107
ＲＯＭ（ユニットＩＤ）
108
ＲＡＭ（人体ＩＤ）

【図１０】


〔ＷＣＵ〕
〔認証設定装置〕
〔認証管理装置〕
スタート
スタート
スタート
SC-1
接触検知？
No
Yes
SC-3
生体情報入力？
No
Yes
SC-4
生体情報送信
SC-5
生体情報受信？
No
Yes
SC-7
起動可？
No
Yes
SC-6
起動可否
信号送信
SC-2
起動信号受信？
No
Yes
SC-8
起動信号送信
SC-2a
人体ＩＤ保存
SC-9
人体通信？
No
Yes
SC-10
人体ＩＤ送信
SC-11
人体ＩＤ受信？
No
Yes
SC-15
非接触検知？
No
Yes
SC-12
人体ＩＤ送信
SC-13
人体ＩＤ受信？
No
Yes
SC-16
人体ＩＤ送信停止
及び消去
SC-14
人体ＩＤを
登録ＤＢに登録
エンド
エンド
エンド

【図１１】


〔ＷＣＵ〕
〔認証操作端末〕
〔認証管理装置〕
スタート
スタート
スタート
SD-1
人体通信？
No
Yes
SD-2
人体ＩＤ送信
SD-5
人体ＩＤ受信？
No
Yes
SD-6
人体ＩＤ及び
機器ＩＤ送信
SD-7
人体ＩＤ及び
機器ＩＤ受信？
No
Yes
SD-8
人体ＩＤ及び
機器ＩＤを
登録ＤＢに登録
SD-9
表示情報及び
利用可否情報を
コンテンツＤＢ
及び利用ＤＢから
取得して送信
SD-10
表示情報及び
利用可否情報
受信？
No
Yes
SD-3
非接触検知？
No
Yes
SD-11
表示情報及び
利用可否情報に
応じた制御処理
SD-4
人体ＩＤ送信停止
及び消去
エンド
エンド
エンド