

明 細 書

発明の名称： アクセス制御装置、鍵装置および鍵ホルダ

技術分野

[0001] 本発明の実施形態は、アクセス制御装置、鍵装置および鍵ホルダに関する。

背景技術

[0002] 昨今、スマートキーの技術は広く知られ、実運用されている。従来のスマートキーには、電源が切れた時の対応のためにエマージェンシーキーが用意されているものがある。しかしながら、エマージェンシーキーは、本人確認機能を有しておらず、誰でも使えるというセキュリティ面の課題がある。

[0003] 一方、本人確認の技術としては、指紋などの生体情報を用いた生体認証がある。生体認証は、セキュリティが高いが、生体認証を行うデバイスを動作させるために電源が必要である。このため、スマートキーの電源が切れた状況で使用するエマージェンシーキーは、生体認証を用いて本人確認を行うのは難しい。

[0004] また、生体認証は、本人拒否率を0%にできない。本人拒否が発生した場合の回避策として、生体認証デバイスは、PINコードを用いて認証を行うものがある。しかしながら、従来のエマージェンシーキーなどに適用できる携帯可能な生体認証デバイスは、PINコードでの認証を行うための構成を設けるのが難しく、本人拒否が発生した場合の対応が困難であるという問題がある。

先行技術文献

特許文献

[0005] 特許文献1：日本国特許第4539246号

発明の概要

発明が解決しようとする課題

[0006] 上記の課題を解決するため、本願に係る発明は、セキュリティレベル低下

を抑えつつ、実用性を高めることができるアクセス制御装置、鍵装置および鍵ホルダ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

[0007] 実施形態によれば、アクセス制御装置は、第1通信インターフェースと第2通信インターフェースとプロセッサとを有する。第1通信インターフェースは、鍵識別情報を有する鍵装置と通信する。第2通信インターフェースは、予め登録されている確認装置と通信する。プロセッサは、第1通信インターフェースにより通信する鍵装置から鍵識別情報としての識別子と鍵装置の使用者がセキュリティ機器のアクセス権者であるかを生体情報で確認した生体認証結果とを取得し、鍵装置の鍵識別情報が正当な鍵の鍵識別情報と一致し、かつ、生体認証結果が認証失敗である場合、第2通信インターフェースを用いて鍵装置に対応づけられた確認装置にアクセス許可の確認を要求する確認要求信号を送信し、確認要求信号に対して確認装置からアクセスの許可を示す確認応答信号を受信すればセキュリティ機器へのアクセスを許可とする。

図面の簡単な説明

[0008] [図1]図1は、各実施形態に係る認証システムの構成例を概略的に説明するための図である。

[図2]図2は、第1実施形態に係る認証システムにおけるアクセス制御装置および鍵装置の構成例を示すブロック図である。

[図3]図3は、第1実施形態に係るアクセス制御装置におけるアクセス管理テーブルの構成例を示す図である。

[図4]図4は、第1実施形態に係る認証システムの動作例を説明するためのシーケンスである。

[図5]図5は、第1実施形態に係る認証システムの動作例を説明するためのシーケンスである。

[図6]図6は、第1実施形態に係るアクセス管理装置の動作例を説明するためのフローチャートである。

[図7]図7は、第2実施形態に係る認証システムにおけるアクセス制御装置および鍵装置の構成例を示すブロック図である。

[図8]図8は、第2実施形態に係る鍵装置の構成例を示す外観図である。

[図9]図9は、第2実施形態に係る鍵装置を鍵ホルダに収納した状態の例を示す図である。

[図10]図10は、第2実施形態に係る鍵装置を収納した鍵ホルダの例を示す図である。

[図11]図11は、第2実施形態に係る認証システムの動作例を説明するためのシーケンスである。

[図12]図12は、第2実施形態に係るアクセス管理装置の動作例を説明するためのフローチャートである。

[図13]図13は、第3実施形態に係る認証システムにおける各装置の構成例を示すブロック図である。

[図14]図14は、第3実施形態に係る鍵装置および鍵ホルダの構成例を示す図である。

[図15]図15は、第3実施形態に係る認証システムの動作例を説明するためのシーケンスである。

[図16]図16は、第4実施形態に係る認証システムにおける各装置の構成例を示すブロック図である。

[図17]図17は、第4実施形態に係る認証システムの動作例を説明するためのシーケンスである。

[図18]図18は、第4実施形態に係るアクセス管理装置の動作例を説明するためのフローチャートである。

実施形態

[0009] 以下、図面を参照して各実施形態について説明する。

なお、各図は各実施形態とその理解を促すための模式図であり、その形状や寸法、比などは適宜、設計変更することができる。

[0010] 図1は、各実施形態に係る認証システム1（1A、1B、1C、1D）の

全体構成を概略的に説明するための図である。

実施形態に係る認証システム１（１Ａ、１Ｂ、１Ｃ、１Ｄ）は、アクセス制御装置１０（１０Ａ、１０Ｂ、１０Ｃ、１０Ｄ）および鍵装置２０（２０Ａ、２０Ｂ、２０Ｃ、２０Ｄ）などで構成される。アクセス制御装置１０は、正当なユーザが操作する鍵装置２０によってアクセス可能とするようなアクセス制御を行う装置である。例えば、アクセス制御装置１０は、セキュリティ機器としての電子錠を含む錠前装置である。アクセス制御装置１０としての錠前装置は、自動車、家屋などの扉などに錠前（錠）として設けられ、鍵装置２０を用いて開錠される。

[0011] 鍵装置２０は、アクセス制御装置１０がアクセスを許可するための鍵情報と生体認証結果とをアクセス制御装置へ与える。鍵情報は、鍵装置２０を識別するための識別子（アクセス管理識別子）を含む情報であれば良い。鍵情報は、通信によって鍵装置２０からアクセス制御装置１０へ供給される。また、鍵情報は、鍵装置２０に設けた物理キーの形状などをアクセス制御装置１０が認識することにより取得するようにしても良い。また、鍵装置２０は、生体認証を行う機能を有し、生体認証による人物の認証結果を出力する。生体認証に用いる生体情報は、例えば、指紋画像である。この場合、鍵装置２０は、使用者の指紋画像と予め登録してある登録者（正当な使用者、アクセス権者）のテンプレート（指紋認証用の辞書データ）とを照合することにより正当な使用者であるか否かを判定する。

[0012] 確認装置３０は、正当な使用者ごとに設定される情報端末である。確認装置３０は、アクセス制御装置１０において鍵装置２０（又は鍵装置２０の登録者）ごとに確認要求の通知先として設定される。確認装置３０は、アクセス制御装置１０からの確認要求を受けた場合、所定期間においてユーザによるアクセス許可（開錠指示）の入力を受け付ける。確認装置３０は、ユーザによりアクセス許可（開錠指示）が入力されると、アクセス許可（開錠）を要求する確認信号をアクセス制御装置１０へ送信する。

[0013] （第１実施形態）

次に、第1実施形態に係る鍵装置20Aおよびアクセス制御装置10Aの構成について説明する。

図2は、第1実施形態に係るアクセス制御装置10Aおよび鍵装置20Aにおける構成例を示すブロック図である。

図2に示す構成例において、アクセス制御装置10Aは、プロセッサ11、ROM12、RAM13、データメモリ14、タイマ15、第1通信インターフェース16、第2通信インターフェース17、送電インターフェース18および電子錠（セキュリティ機器）19などを有する。

[0014] プロセッサ11は、各部の制御および各種の処理などを実行する。プロセッサ11は、例えば、CPU（central processing unit）である。プロセッサ11は、ROM11またはデータメモリ14に記憶されたプログラムを実行することにより各部の制御および各種の処理を実現する。

[0015] ROM12は、書き換え不可のデータを保存する不揮発性メモリである。ROM12は、プログラムまたは制御データなどを記憶する。RAM13は、データを一時的に記憶する揮発性メモリである。

データメモリ14は、書き換え可能な不揮発性のメモリである。データメモリ14は、HDD（ハードディスクドライブデータ）あるいはSSD（ソリッドステートドライブ）などで実現される。データメモリ14は、電子錠19を開錠するための鍵（アクセスを許可するための鍵）などの管理情報（設定情報）を記憶するアクセス管理テーブル14aを有する。

[0016] 図3は、アクセス管理テーブル14aの構成例を示す図である。

アクセス管理テーブル14aは、鍵装置20Aの識別子と確認先（確認要求信号の送信先）を示す情報とが対応づけて記憶される。アクセス管理テーブル14aに記憶する識別子は、当該アクセス制御装置10Aに対応づけた正当な鍵（鍵装置）を示す識別子（アクセス管理識別子）である。複数の鍵装置で開錠可能とする場合、アクセス管理テーブル14aには、複数の識別子を記憶して良い。確認先を示す情報は、鍵装置20Aに対応する確認装置（例えば、鍵装置20Aに生体情報を登録した登録者が所持者する確認装置

）３０を示す情報である。また、確認先を示す情報は、開錠（アクセス許可）の確認を要求する確認要求信号を送信する送信先を示す情報であっても良い。例えば、確認先を示す情報は、確認装置３０が受信可能な通知先（メールアドレス等）を示す情報であっても良い。

[0017] タイマ１５は、経過時間を計時する。タイマ１５は、プロセッサ１１により制御され、プロセッサ１１によりリセットされた時間から経過した時間を計時する。

第１通信インターフェース１６は、鍵装置２０Ａと通信するためのインターフェースである。第１通信インターフェース１６は、無線通信用のインターフェースであっても良いし、物理的かつ電氣的に接触して信号の送受信を行うインターフェースであっても良い。後者の場合、第１通信インターフェース１６は、鍵装置２０Ａに設けたコンタクト部と接触する構成を有するものとすればよい。

[0018] また、第１通信インターフェース１６は、無線通信用のインターフェースとして、近距離無線通信または非接触通信に対応したインターフェースであっても良い。例えば、近距離無線通信を行う場合、第１通信インターフェース１６は、ブルートゥース（Bluetooth（登録商標））などの近距離無線の規格に適合した無線通信を行う近距離無線インターフェースで構成される。

[0019] また、非接触通信を行う場合、第１通信インターフェース１６は、例えば、ＮＦＣ（Near Field Communication）などの非接触通信の規格に適合した構成を有する非接触通信インターフェースとする。ＮＦＣ（Near Field Communication）などの非接触通信は、非接触で電力の供給を行いながら非接触通信を行う。このため、非接触通信を行う場合、第１通信インターフェース１６および送電インターフェース１８が非接触通信インターフェースで構成されるものとして良い。

[0020] 第２通信インターフェース１７は、確認装置３０と通信するためのインターフェースである。第２通信インターフェース１７は、確認要求の送信先として設定される通知先に確認要求を送信できるものであれば良い。例えば、

第2通信インターフェース17は、無線又は有線で確認装置30と通信接続するものであっても良いし、クラウドを介して確認装置30へ情報を送信するものであっても良い。例えば、第2通信インターフェース17は、Ethernet（登録商標）、Wi-Fi（登録商標）、Bluetooth、LTE（Long Term Evolution）（登録商標）などの様々な通信規格に準拠した有線または無線のインターフェースを採用することができる。また、それらの組み合わせで第2通信インターフェース17を実現することもできる。

[0021] 送電インターフェース（電力供給器）18は、鍵装置20Aへ電力を要求するためのデバイスである。また、送電インターフェース18は、鍵装置20Aが動作するための電源供給を供給するだけでなく、動作用のクロック、リセット制御信号などを供給するものであっても良い。送電インターフェース18は、鍵装置20Aにおける動作用の電力の受電方式に応じたインターフェースにより構成される。例えば、非接触で鍵装置20Aへ電力を供給するデバイスとする場合、送電インターフェース18は、給電用の電波を放射するアンテナおよびアンテナから電波を放射させる回路などにより構成される。

[0022] 電子錠19は、アクセス制御の対象となるセキュリティ機器である。プロセッサ11は、鍵装置20Aからの情報に応じて電子錠19を制御する。例えば、電子錠19は、プロセッサ11からの開錠信号を受けて錠前機構を開錠する。ただし、電子錠19は、セキュリティ機器の一例であり、セキュリティ機器は、電子錠に限定されるものではない。電子錠19として例示するセキュリティ機器は、鍵装置20Aの鍵情報と鍵装置20Aの利用者に対する生体認証結果とに応じてアクセスが制御されるものであれば良い。

[0023] 次に、第1実施形態に係る鍵装置20Aの構成について説明する。

図2に示す構成例において、鍵装置20Aは、プロセッサ21、ROM22、RAM23、データメモリ24、通信インターフェース25、生体センサ（指紋センサ）27、および、受電インターフェース28などを有する。

[0024] プロセッサ21は、データバスなどを介してROM22、RAM23、デ

ータメモリ 24、通信インターフェース 25 および生体センサ 27 に接続する。また、受電インターフェース 28 は、各部に電力を供給するように接続される。

[0025] プロセッサ 21 は、鍵装置 20 A 全体の制御を司る制御部として機能する。プロセッサ 21 は、例えば、CPU である。プロセッサ 21 は、プログラムを実行することにより各部の制御及び情報処理を実現するものであればよい。すなわち、プロセッサ 21 は、ROM 22 またはデータメモリ 24 に記憶される制御プログラム及び制御データに基づいて種々の処理を行う。

なお、後述するようなプロセッサ 21 がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであっても良い。

[0026] ROM 22 は、予め制御用のプログラム及び制御データなどを記憶する不揮発性のメモリである。ROM 22 は、製造段階で制御プログラム及び制御データなどを記憶した状態で鍵装置 20 A に組み込まれる。

[0027] RAM 23 は、揮発性のメモリである。RAM 23 は、プロセッサ 21 の処理中のデータなどを一時的に格納する。例えば、RAM 23 は、計算用バッファ、受信用バッファ及び送信用バッファとして機能する。計算用バッファとしては、プロセッサ 21 が実行する種々の演算処理の結果などを一時的に保持する。受信用バッファとしては、通信インターフェース 25 を介してアクセス制御装置 10 A から受信するコマンドデータなどを保持する。送信用バッファとしては、通信インターフェース 25 を介してアクセス制御装置 10 A へ送信するメッセージ（レスポンスデータ）などを保持する。

[0028] データメモリ 24 は、フラッシュROMなどのデータの書き込み及び書換えが可能な不揮発性のメモリにより構成される。データメモリ 24 は、運用用途に応じてインストールされる制御プログラム、アプリケーション及び種々のデータを格納する。

[0029] また、データメモリ 24 は、生体（指紋）認証の辞書データとして用いる登録者（アクセス権者）の生体情報を含む認証データを記憶する認証データ

ベース（DB）24aを有する。認証DB24aは、例えば、登録者の生体情報から生成される特徴点情報などの特徴量を登録者の認証データとして記憶する。登録者が複数である場合、認証DB24aには、各登録者の認証データが記憶される。鍵装置20Aは、特定の1人の登録者に対する認証データを認証DB24aに登録するものであっても良いし、複数の登録者に対応する複数の認証データを認証DB24aに登録するようにしても良い。

[0030] また、データメモリ24は、当該鍵装置20Aを特定する鍵識別情報としての識別子（アクセス管理識別子）を記憶する。識別子は、鍵識別情報としてアクセス制御装置10Aへ供給される。アクセス制御装置10Aでは、鍵装置20Aから取得する識別子によってアクセスが許可される正当な鍵であるかを判定する。

[0031] 通信インターフェース25は、アクセス制御装置10Aと通信するためのインターフェースである。通信インターフェース25は、アクセス制御装置10Aの第1通信インターフェース16と通信接続し、データの送受信を行う。通信インターフェース25は、第1通信インターフェース16に対応した通信方式のインターフェースである。

[0032] 例えば、アクセス制御装置10Aと鍵装置20AとがNFC（Near Field Communication）などの非接触通信で通信する場合、通信インターフェース25および第1通信インターフェース16は、非接触通信用のインターフェースで構成される。また、アクセス制御装置10Aと鍵装置20AとがBluetooth（登録商標）などの近距離無線で通信する場合、通信インターフェース25および第1通信インターフェース16は、近距離無線通信用のインターフェースで構成される。また、通信インターフェース25および第1通信インターフェース16は、物理的かつ電氣的に接触して信号の送受信を行うインターフェースであっても良い。

[0033] 生体センサ27は、鍵装置20Aの使用者の生体情報を取得する。生体センサ27は、例えば、指紋センサである。生体センサ27としての指紋センサは、使用者の指から指紋画像を取得する。生体センサ27としての指紋セ

ンサは、CCDセンサなどを備える。また、指紋センサ27は、電気容量の変化を検出するセンサなどを備えるものであってもよい。指紋センサ27は、指紋画像をプロセッサ21に供給する。

[0034] プロセッサ21は、生体センサ27が検知する生体情報を処理し、生体認証などを実行する。例えば、プロセッサ21は、指紋センサ27からの指紋画像を処理する。プロセッサ21は、指紋センサ27からの指紋画像から特徴点情報（特徴点の座標及び特徴量など示す情報）を抽出する。

[0035] プロセッサ21は、指紋センサ27で取得する指紋画像と登録されている指紋画像との照合処理を行う。プロセッサ21は、指紋センサ27で取得した指紋画像と登録されている指紋画像と類似度を算出する。ここでは、類似度は、高いほど指紋画像同士の類似性が高いことを示す指標である。例えば、プロセッサ21は、指紋センサ27で取得した指紋画像の特徴点情報を抽出する。プロセッサ21は、所定のアルゴリズムに従って、指紋画像同士の類似度として、抽出した特徴点情報と登録されている指紋画像の特徴点情報との類似度を算出する。

[0036] また、プロセッサ21は、照合処理（認証処理）として、算出した類似度と認証用の閾値とを比較することにより生体認証の成否を判定する。例えば、プロセッサ21は、算出した類似度が認証用の閾値以上であれば同一人物である（認証成功）とし、類似度が認証用の閾値未満であれば同一人物と認めない（認証失敗）とすることにより認証処理の結果を得るようにしてもよい。

[0037] 受電インターフェース28は、電力を受電するインターフェースである。受電インターフェース28は、送電インターフェース18に対応し、送電インターフェース18から送電される電力を受電するものであれば良い。例えば、受電インターフェース28および送電インターフェース18は、非接触電力伝送を実現する構成であっても良い。受電インターフェース28および送電インターフェース18は、コンタクト部を介して接触して電力伝送を行うものであっても良い。また、受電インターフェース28は、通信インター

フェース 25 と一体であっても良いし、通信インターフェース 25 に含まれる構成としても良い。

[0038] また、受電インターフェース 28 は、アクセス制御装置 10A 以外の外部装置からの電力を受電するようにしても良い。例えば、受電インターフェース 28 は、電力供給装置が非接触で伝送する電力を受電するようにしても良い。受電インターフェース 28 が外部装置から電力を受電するシステム構成とした場合、アクセス制御装置 10A は送電インターフェース 18 を省略して良い。

[0039] なお、鍵装置 20A は、図 2 が示すような構成の他に必要に応じた構成を具備したり、特定の構成が除外されたりしてもよい。例えば、鍵装置 20A は、種々の情報を表示する表示部を具備するものであっても良い。表示部は、プロセッサ 21 からの制御に従って情報を表示するものであれば良い。表示部の具体例としては、プロセッサ 21 からの制御に従って点灯するライト（例えば、LED（Light Emitting Diode））などであっても良いし、プロセッサ 21 が指示される画像（情報）を表示するディスプレイであっても良い。

[0040] 次に、第 1 実施形態に係る認証システム 1A の動作について説明する。

図 4 および図 5 は、鍵装置 20A における生体認証が失敗した場合における認証システム 1A の動作例を説明するためのシーケンスである。図 4 は、生体認証が失敗した後の確認要求信号に対して確認装置 30 でアクセス許可が指示された場合のタイミングチャートであり、図 5 は、生体認証が失敗した後の確認要求信号に対する確認応答信号がなかった場合のタイミングチャートである。

[0041] 図 4 に示すように、アクセス制御装置 10A は、鍵装置 20A に対して動作の電力を供給する（ST10）。例えば、アクセス制御装置 10A は、送電インターフェース 18 から鍵装置 20A の受電インターフェース 28 が受電可能な電力を出力する。

[0042] 鍵装置 20A は、アクセス制御装置 10A から供給される電力によって起

動する。起動した鍵装置20Aのプロセッサ21は、通信インターフェース25によるアクセス制御装置10Aとの通信状態を確立する。アクセス制御装置10Aとの通信状態が確立すると、プロセッサ21は、データメモリ24に記録されている当該鍵装置の識別情報としての識別子を読み出す(ST11)。

[0043] また、プロセッサ21は、生体センサ27により使用者の生体情報を取得し、生体認証を実行する(ST12)。例えば、プロセッサ21は、生体センサ27としての指紋センサが取得する使用者の指紋画像とデータメモリ24に記憶している登録者の認証データに含まれる指紋画像の特徴点情報とを照合することにより生体認証を実行する。ここでは、プロセッサ21は、使用者と登録者とが同一人物であると認証できず、生体認証に失敗した(生体認証がNGであった)ものとする。

[0044] 鍵装置20Aのプロセッサ21は、データメモリ24から読み出した識別子と生体認証結果(ここでは、生体認証が失敗したことを示す情報)とを通信インターフェース25によりアクセス制御装置10Aへ送信する(ST13)。

[0045] アクセス制御装置10Aは、第1通信インターフェース16によって鍵装置20Aから識別子と生体認証結果とを受信する。鍵装置20Aの識別子を受信すると、アクセス制御装置10Aのプロセッサ11は、アクセス管理テーブル14aを参照して当該鍵装置20Aが正当な鍵であるか否かを判定する。プロセッサ11は、受信した鍵装置20Aの識別子がアクセス管理テーブル14aに登録されている識別子と一致するか否かにより、正当な鍵であるか否かを判定する。図4に示す例では、プロセッサ11は、鍵装置20Aが正当な鍵であると判定するものとする。

[0046] また、プロセッサ11は、鍵装置20Aが正当な鍵である場合、鍵装置20Aにおける生体認証結果を確認する。ここで、生体認証が成功である場合、つまり、鍵装置20Aが正当な鍵で、かつ、鍵装置20Aの使用者が登録者(正当な利用者)である場合、プロセッサ11は、電子錠19を開錠(ア

クセスを許可)する制御を行う。

- [0047] また、生体認証が失敗である場合、つまり、鍵装置20Aが正当な鍵で、かつ、鍵装置20Aの使用者が登録者(正当な利用者)であることが生体認証で確認できなかった場合、プロセッサ11は、当該識別子に対応する確認先に確認要求信号を送信する(ST14)。すなわち、プロセッサ11は、アクセス管理テーブル14aを参照し、当該識別子に対応する確認先を特定する。確認先(確認要求信号の送信先)を特定すると、プロセッサ11は、第2通信インターフェース17を介して特定した確認先へ確認要求信号を送信する。
- [0048] また、確認要求信号を送信する場合、プロセッサ11は、当該確認要求信号に対する確認装置30からの確認応答信号を有効とする期間(許容時間)を設定し、タイマによる時間監視を開始する。時間監視を開始した後、プロセッサ11は、設定した許容時間内であれば、確認装置30からの確認応答信号を受け付ける。なお、許容時間を設けずに、確認装置30からの確認応答信号を受け付けるようにしてもよい。
- [0049] 確認装置30は、アクセス制御装置10Aからの確認要求信号を受信した場合、ユーザによるアクセス制御装置10Aの電子錠19を開錠させる指示を受け付ける。例えば、確認装置30は、確認要求信号を受けると、図示しない表示部にアクセス制御装置10Aの電子錠を開錠するか否かの確認画面を表示する。
- [0050] 確認装置30は、表示部に確認画面を表示した状態において、図示しない操作部を用いてユーザが入力する電子錠の開錠指示を受け付ける(ST16)。確認装置30は、操作部に電子錠の開錠指示が入力されると、アクセス制御装置10Aに対して電子錠19の開錠を要求する確認応答信号を送信する(ST17)。また、確認装置30にメモリと生体認証センサを付設して、予めメモリに登録しておいた指紋や指静脈像などの生体特徴情報とセンサで得られる生体情報との照合により、本人確認した結果を確認応答信号として、アクセス制御装置10Aに送信してもよい。

[0051] アクセス制御装置 10A のプロセッサ 11 は、確認要求信号を送信した後、許容時間内において確認応答信号を受け付ける。プロセッサ 11 は、許容時間内に確認装置 30 からの確認応答信号を受信すると、アクセスを許可する処理として電子錠 19 を開錠する制御を行う (ST18)。例えば、プロセッサ 11 は、錠を開錠させる制御信号を電子錠 19 へ供給し、電子錠 19 は、プロセッサ 11 からの制御信号に応じて錠を開錠する。

[0052] また、図 5 に示すように、アクセス制御装置 10A のプロセッサ 11 は、確認要求信号を送信してから許容時間内に確認応答信号の受信がなければ、アクセスを不可として電子錠 19 を開錠しないようにする。この場合、アクセス制御装置 10A のプロセッサ 11 は、許容時間内に確認応答信号の受信がなければ、アクセス不可となった旨の通知などをアラームなどで報知するようにしても良いし、確認装置 30 へ通知するようにしても良い。また、プロセッサ 11 は、アクセスを不可とした場合に鍵装置 20A から取得した識別子などの情報をクリアするようにしても良い。

[0053] 次に、第 1 実施形態に係るアクセス制御装置 10A の動作について説明する。

図 6 は、第 1 実施形態に係るアクセス制御装置 10A の動作例を説明するためのフローチャートである。

まず、アクセス制御装置 10A のプロセッサ 11 は、送電インターフェース 18 により鍵装置 20A へ動作用の電力を供給する。プロセッサ 11 は、送電インターフェース 18 から送電する電力によって起動する鍵装置 20A と第 1 通信インターフェース 16 を介して通信する。プロセッサ 11 は、第 1 通信インターフェース 16 により鍵装置 20A の識別子と鍵装置 20A における生体認証の結果とを取得する (ST30)。

[0054] 第 1 通信インターフェース 16 により鍵装置 20A の識別子を受信すると、プロセッサ 11 は、受信した識別子がアクセス管理テーブル 14a に登録済みの識別子と一致するか否かにより鍵装置 20A が正当な鍵であるか否かを判定する (ST31)。

- [0055] 鍵装置20Aが正当な鍵でないと判定した場合(ST31、NO)、プロセッサ11は、当該鍵装置20Aによるアクセスを不可とする(ST38)。例えば、アクセスを不可とする場合、プロセッサ11は、鍵装置20Aを用いた電子錠19の開錠を拒否する。この場合、プロセッサ11は、アクセス不可を示すアラームを鳴らしたり、アクセス不可を示す情報を表示装置により表示したりしても良い。
- [0056] 鍵装置20Aが正当な鍵であると判定した場合(ST31、YES)、プロセッサ11は、さらに、鍵装置20Aから取得する生体認証の結果に基づいて鍵装置20Aの使用者が登録者であると認証されたか否かを判定する(ST32)。生体認証により使用者が登録者であることが確認された場合、つまり、生体認証が成功であった場合(ST32、YES)、プロセッサ11は、当該鍵装置20Aによるアクセスを許可する(ST33)。例えば、プロセッサ11は、電子錠19を開錠させる制御信号を出力することにより電子錠19を開錠させる。
- [0057] また、生体認証により使用者が登録者であることが確認できなかった場合、つまり、生体認証が失敗であった場合(ST32、NO)、プロセッサ11は、第2通信インターフェース17を用いて、アクセス管理テーブル14aにおいて当該識別子に対応づけられている確認先としての確認装置30へ確認応答信号を送信する(ST33)。確認応答信号を送信した場合、プロセッサ11は、タイマ15による時間の計時を開始する(ST35)。
- [0058] タイマ15による計時を開始した後、プロセッサ11は、第2通信インターフェース17により確認装置30からの確認応答信号を受信したかを監視する(ST36)。確認応答信号は、確認装置30においてアクセス制御装置10Aに対してアクセスの許可が指示されたことを示す信号である。確認応答信号を受信した場合(ST36、YES)、プロセッサ11は、アクセスを許可し(ST33)、電子錠19を開錠させる制御を行う。
- [0059] 確認応答信号が受信できない場合(ST36、NO)、プロセッサ11は、タイマ15が計時する時間によって所定の許容時間が経過したかチェック

する（ST37）。確認応答信号が受信したタイミングが許容時間内であれば（ST37、NO）、プロセッサ11は、確認応答信号の受信待ちとする。許容時間を超えた場合（ST37、YES）、プロセッサ11は、鍵装置20Aによるアクセスを不可とする（ST38）。

[0060] 上記のように、第1実施形態に係るアクセス制御装置は、識別子により鍵（鍵装置）の正当性と生体認証による本人認証結果とに応じてアクセスの可否を制御する。アクセス制御装置は、鍵が正当で、生体認証が失敗した場合、当該鍵に対応づけた確認先にアクセスの可否を問い合わせる。アクセス制御装置は、確認先からアクセスの許可を指示する信号を所定の許容時間内に受信できればアクセスを許可する。

[0061] これにより、生体認証が失敗した場合でも予め登録した確認先でのアクセス許可によってアクセス制御装置でのアクセスを許可とすることができる。すなわち、鍵装置による生体認証で本人拒否が発生した場合であっても、予め設定した確認装置でのアクセス確認による2要素認証でアクセスコントロールことができ、セキュリティレベル低下を抑えつつ、実用性の高い認証システムを提供できる。また、確認装置30にメモリと生体認証センサを付設して、予めメモリに登録しておいた指紋や指静脈像などの生体特徴情報とセンサで得られる生体情報との照合により、本人確認した結果を確認応答信号として、アクセス制御装置10Aに送信する構成をならば、確認装置を他人が悪用することも回避でき、正当な本人のみが開錠可能であることを担保できる。

[0062] （第2実施形態）

次に、第2実施形態について説明する。

図7は、第2実施形態に係る認証システム1Bにおけるアクセス制御装置10Bおよび鍵装置20Bにおける構成例を示すブロック図である。

図7に示す第2実施形態に係る認証システム1Bは、鍵装置20Bが物理キーKを有し、アクセス制御装置10Bがキー識別部51および挿入部51aを有する点で図2などに示す第1実施形態に係る認証システム1Aと構成

が異なる。図 7 に示す構成例において、図 2 に示す構成と同様なものについては同一箇所に同一符号を付して詳細な説明を省略する。また、第 1 実施形態の構成から導かれる効果についても同様にここでは詳細な説明を省略する。

[0063] 図 7 に示す構成例において、アクセス制御装置 10B は、プロセッサ 11、ROM 12、RAM 13、データメモリ 14、タイマ 15、第 1 通信インターフェース 16、第 2 通信インターフェース 17、送電インターフェース 18 および電子錠（セキュリティ機器） 19 およびキー識別部（キー識別器） 51 を有する。

[0064] キー識別部 51 は、セットされた物理キー K を識別する。例えば、キー識別部 51 は、物理キーが挿入される挿入部 51a を有し、挿入部 51a に挿入（セット）された物理キーの形状が所定の形状（正当な鍵の形状）であるかを判別する。キー識別部 51 は、挿入部 51a に挿入された物理キーが正当な鍵である場合に正当な鍵であることを示す信号をプロセッサ 11 へ供給する。なお、キー識別部 51 は、挿入部 51a に挿入（セット）された物理キーを光学的にスキャンすることにより正当な鍵であるか否かを判別するものであっても良い。

[0065] また、キー識別部 51 の挿入部 51a は、送電インターフェース 18 に含まれる構成としても良い。送電インターフェース 18 は、挿入部 51a に挿入された物理キー K を備える鍵装置 20B に対して電力を供給するように構成すれば良く、キー識別部 51 と一体的に構成しても良い。例えば、送電インターフェース 18 は、挿入部 51a に挿入された物理キーに物理的に接触するコンタクト部を設け、コンタクト部から物理キーを通じて鍵装置 20B へ電力を供給するようにしても良い。

[0066] また、鍵装置 20B は、図 7 に示す構成例において、プロセッサ 21、ROM 22、RAM 23、データメモリ 24、通信インターフェース 25、生体センサ（指紋センサ） 27、受電インターフェース 28、および、物理キー K を有する。プロセッサ 21、ROM 22、RAM 23、データメモリ 2

4、通信インターフェース25、生体センサ（指紋センサ）27および受電インターフェース28は、図2と同等の機能を有するもので実現できる。

[0067] 物理キーKは、アクセス制御装置10Bにおけるキー識別部51の挿入部51aにセットされる。物理キーKは、キー識別部51が正当な鍵であるか否かを識別可能なものであれば良い。例えば、物理キーKは、キー識別部51で識別可能な形状を有し、形状によって正当な鍵であるか否かが判別される。また、図7に示す例において、物理キーKは、受電インターフェース28に電氣的に接続される。

[0068] 図8は、第2実施形態に係る鍵装置20Bの構成例を示す図である。

図8に示す構成例において、鍵装置20Bは、本体Caに物理キーKを取り付けたものとなっている。本体Caは、プロセッサ21、ROM22、RAM23、データメモリ24、通信インターフェース25、生体センサ（指紋センサ）27、および、受電インターフェース28などを有する。本体Caの表面には、生体センサとしての指紋センサ27が設けられ、本体Ca内には、プロセッサ21、ROM22、RAM23、データメモリ24、通信インターフェース25、および、受電インターフェース28などが内蔵される。

[0069] 物理キーKは、鍵としての固有の鍵識別情報を有する。例えば、物理キーKは、鍵としての固有の形状で形成される。物理キーKの形状は、鍵と特定する鍵識別情報として、キー識別部51で認識される。この場合、物理キーKは、識別情報としての形状が変形しないような金属などの材料が形成される。物理キーKは、識別情報とする形状が設けられた部位がアクセス制御装置10Bにおける挿入部51aに挿入できるように本体Caに取り付けられる。

[0070] なお、物理キーKは、金属などの導電性の材料で形成し、挿入部51aに挿入された状態において送電インターフェース18から電力が供給されるようにしても良い。この場合、物理キーKは、送電インターフェース18からの電力を受電インターフェース28へ伝送するように構成すれば良い。これ

により、アクセス制御装置 10B は、送電インターフェース 18 から挿入部 51a にセットされた物理キー K を通じて鍵装置 20B の受電インターフェースに電力を送電できる構成となる。

[0071] 図 9 および図 10 は、第 2 実施形態に係る鍵装置 20B の構成例を示す図である。

図 9 および図 10 に示す構成例において、鍵装置 20B は、スマートキー本体としての鍵ホルダ 60 に収納される構成を有する。鍵装置 20B は、鍵ホルダ 60 に着脱可能な形状を有する。図 9 に示す構成例において、鍵装置 20B は、鍵ホルダ 60 から取り出した状態で使用する。

[0072] 鍵ホルダ 60 は、例えば、鍵装置 20B を挿入した状態でスマートキーとして使用される。スマートキーとしての鍵ホルダ 60 は、図 10 に示すように、筐体の表面に操作キー 61 (61a、61b、61c) を有し、操作キー 61 の操作によってアクセス制御装置 10B の電子錠 19 を操作する携帯型の電子装置である。この場合、鍵ホルダ 60 は、一次電池または二次電池などの電池を有し、電池からの電力によって動作する。スマートキーとしての鍵ホルダ 60 は、電池からの電力によって動作可能な状態において、アクセス制御装置 10B と無線通信によって通信し、操作キー 61 への入力に応じて電子錠 19 を開錠させる。

[0073] 鍵ホルダ 60 は、電源としての電池から供給可能な電力が低下すると、スマートキーとしては動作不能 (電池切れ) となる。また、鍵ホルダ 60 は、故障などの不具合によってもスマートキーとしては動作不能となる。鍵ホルダ 60 に収納される鍵装置 20B は、電池で駆動するスマートキーとしての鍵ホルダ 60 に対して、エマージェンシーキーとして機能する。鍵装置 20B は、鍵ホルダ 60 から取り出した状態において物理キー K がアクセス制御装置 10B のキー識別部 51 の挿入部 51a にセットされ、電子錠 19 を開錠させるための鍵として利用される。

[0074] 次に、第 2 実施形態に係る認証システム 1B の動作について説明する。

図 11 は、第 2 実施形態に係る鍵装置 20B における生体認証が失敗した

場合における認証システム 1 B の動作例を説明するためのシーケンスである。図 1 1 は、生体認証が失敗した後の確認要求信号に対して確認装置でアクセス許可が指示された場合の動作例を示す。なお、図 1 1 に示す動作例において、確認要求信号を送信した後の動作は、図 4 に示す動作例と同様であるため、詳細な説明を省略するものとする。

[0075] 図 1 1 に示すように、鍵装置 2 0 B を用いてアクセス制御装置 1 0 B の電子錠を開錠する場合、使用者は、鍵装置 2 0 B の物理キー K をアクセス制御装置 1 0 B におけるキー識別部 5 1 の挿入部 5 1 a に挿入する (S T 4 0)。

[0076] アクセス制御装置 1 0 B のキー識別部 5 1 は、挿入部 5 1 a にセットされた物理キー K を識別することにより挿入部 5 1 a に挿入された鍵が正当な鍵であるか否かを判別する。キー識別部 5 1 は、正当な鍵が挿入されたであると判別した場合、プロセッサ 1 1 に正当な鍵が挿入部 5 1 a に挿入されたことを示す信号を供給する (S T 4 1)。

[0077] プロセッサ 1 1 は、正当な鍵が挿入部 5 1 a に挿入されたことを示す信号を受けると、送電インターフェース 1 8 により鍵装置 2 0 B への電力を供給する (S T 4 2)。送電インターフェース 1 8 は、挿入部 5 1 a に挿入された物理キー K を通じて鍵装置 2 0 B の受電インターフェース 2 8 が受電可能な電力を出力する。また、送電インターフェース 1 8 は、非接触で受電インターフェース 2 8 に電力を供給するものであっても良く、その場合には送電インターフェース 1 8 は非接触で受電インターフェース 2 8 が受電可能な電力を送電する。

[0078] 鍵装置 2 0 B は、受電インターフェース 2 8 により物理キー K を挿入部 5 1 a に挿入したアクセス制御装置 1 0 B からの電力を受電する。受電インターフェース 2 8 が電力を受電すると、鍵装置 2 0 B のプロセッサ 2 1 は、各部を起動させて生体認証を実行する (S T 4 3)。例えば、プロセッサ 2 1 は、生体センサ 2 7 を起動させ、生体センサ 2 7 が取得する使用者の生体情報と登録者の認証データに含まれる生体情報の特徴点情報 (登録者の生体情

報の特徴量)とを照合することにより生体認証を実行する。

[0079] ここで、プロセッサ21は、生体認証の結果として、使用者と登録者とが同一人物であると認証できず、生体認証に失敗した(生体認証がNGであった)ものとする。この場合、鍵装置20Bのプロセッサ21は、認証結果として、生体認証が失敗したことを示す情報)を通信インターフェース25によりアクセス制御装置10Bへ送信する(ST44)。

[0080] アクセス制御装置10Bは、第1通信インターフェース16によって鍵装置20Bから生体認証結果を受信する。鍵装置20Bから生体認証結果を受信すると、プロセッサ11は、受信した生体認証結果に基づいて使用者が登録者であることが確認できたか否かを判定する。ここで、鍵装置20Bの使用者が登録者(正当な利用者)であることが生体認証で確認できた場合、つまり、生体認証が成功である場合、プロセッサ11は、電子錠19を開錠(アクセスを許可)する制御を行う。

[0081] また、鍵装置20Bの使用者が登録者(正当な利用者)であることが生体認証で確認できなかった場合、つまり、生体認証が失敗である場合、プロセッサ11は、挿入部51aに挿入された物理キーを有する鍵装置20Bに対応づけて設定されている確認先に確認要求信号を送信する(ST46)。すなわち、プロセッサ11は、アクセス管理テーブル14aを参照し、キー識別部51が正当と判定する鍵に対応して設定されている確認先を特定する。確認先(確認要求信号の送信先)を特定すると、プロセッサ11は、第2通信インターフェース17を介して特定した確認先へ確認要求信号を送信する。

[0082] また、確認要求信号を送信する場合、プロセッサ11は、当該確認要求信号に対する確認装置30からの確認応答信号を有効とする期間(許容時間)を設定し、タイマ15による時間監視を開始する。時間監視を開始した後、プロセッサ11は、設定した許容時間内であれば、確認装置30からの確認応答信号を受け付ける。

[0083] 確認装置30は、アクセス制御装置10Bからの確認要求信号を受信した

場合、ユーザによるアクセス制御装置 10B の電子錠 19 を開錠させる指示を受け付ける。例えば、確認装置 30 は、確認要求信号を受けると、図示しない表示部にアクセス制御装置 10B の電子錠を開錠するか否かの確認画面を表示する。確認装置 30 は、表示部に確認画面を表示した状態において、図示しない操作部を用いてユーザが入力する電子錠の開錠指示を受け付ける（ST47）。確認装置 30 は、ユーザにより電子錠の開錠指示（アクセス許可の指示）が入力されると、アクセス制御装置 10B に対して電子錠 19 の開錠を要求する確認応答信号を送信する（ST48）。

[0084] アクセス制御装置 10B のプロセッサ 11 は、確認要求信号を送信した後、許容時間内において確認応答信号を受け付ける。プロセッサ 11 は、許容時間内に確認装置 30 からの確認応答信号を受信すると、アクセスを許可する処理として電子錠 19 を開錠する制御を行う（ST49）。例えば、プロセッサ 11 は、錠を開錠させる制御信号を電子錠 19 へ供給し、電子錠 19 は、プロセッサ 11 からの制御信号に応じて錠を開錠する。

[0085] また、アクセス制御装置 10B のプロセッサ 11 は、確認要求信号を送信してから許容時間内に確認応答信号の受信がなければ、図 5 と同様に、アクセスを不可として電子錠 19 を開錠しないようにする。

[0086] 次に、第 2 実施形態に係るアクセス制御装置 10B の動作について説明する。

図 12 は、第 2 実施形態に係るアクセス制御装置 10B の動作例を説明するためのフローチャートである。

アクセス制御装置 10B のキー識別部 51 は、挿入部 51a に物理キー K が挿入された場合、挿入された物理キー K が正当な鍵であるか否かを判別する（ST51）。キー識別部 51 は、挿入された物理キー K が正当な鍵であれば、正当な鍵が挿入部 51a に挿入されたことを示す信号をプロセッサ 11 へ供給する。

[0087] プロセッサ 11 は、キー識別部 51 からの信号に応じて挿入部 51a に正当な鍵が挿入されたことを検知する（ST52）。プロセッサ 11 は、正当

な鍵が挿入されたことを示す信号が無ければ（ST52、NO）、ST51へ戻り、キー識別部51からの信号待ちとなる。なお、キー識別部51から正当な鍵ではない物理キーが挿入されたことを示す信号を受けた場合、プロセッサ11は、ST60へ進み、アクセス不可とする処理を実行するようにしても良い。

[0088] 正当な鍵が挿入部51aに挿入されたことを示す信号を受けると、プロセッサ11は、送電インターフェース18により鍵装置20Bへの電力を供給させる（ST53）。プロセッサ11は、送電インターフェース18へ送電を指示し、送電インターフェース18は、プロセッサ11からの指示に応じて鍵装置20Bへの給電を開始する。例えば、送電インターフェース18は、挿入部51aに挿入された物理キーKを通じて鍵装置20Bの受電インターフェース28が受電可能な電力を出力する。また、送電インターフェース18は、非接触電力伝送によって受電インターフェース28が受電可能な電力を送電しても良い。

[0089] 鍵装置20Bは、受電インターフェース28により物理キーKを挿入部51aに挿入したアクセス制御装置10Bからの電力を受電する。鍵装置20Bは、受電インターフェース28が受電する電力によって起動して生体認証を実行する。鍵装置20Bは、生体認証結果を含む情報を通信インターフェース25によりアクセス制御装置10Bへ送信する。

[0090] アクセス制御装置10Bのプロセッサ11は、送電インターフェース18から送電する電力によって起動する鍵装置20Bと第1通信インターフェース16を介して通信する。プロセッサ11は、第1通信インターフェース16により鍵装置20Bにおける生体認証結果を取得する。

[0091] 鍵装置20Bから生体認証結果を受信すると、プロセッサ11は、取得した生体認証結果に基づいて鍵装置20Bの使用者が登録者であると認証されたか否かを判定する（ST54）。生体認証により使用者が登録者であることが確認された場合、つまり、生体認証が成功であった場合（ST54、YES）、プロセッサ11は、当該鍵装置20Bによるアクセスを許可する（

ST55)。例えば、プロセッサ11は、電子錠19を開錠させる制御信号を出力することにより電子錠19を開錠させる。

[0092] また、生体認証により使用者が登録者であることが確認できなかった場合、つまり、生体認証が失敗であった場合(ST54、NO)、プロセッサ11は、第2通信インターフェース17を用いて、アクセス管理テーブル14aを参照して挿入された鍵に対応づけて登録されている確認先を特定する。確認先を特定すると、プロセッサ11は、特定した確認先へ確認応答信号を送信する(ST56)。確認応答信号を送信した場合、プロセッサ11は、タイマ15による時間の計時を開始する(ST57)。

[0093] タイマ15による計時を開始した後、プロセッサ11は、第2通信インターフェース17により確認装置30からの確認応答信号を受信したかを監視する(ST58)。確認応答信号は、確認装置30においてアクセス制御装置10Bに対してアクセスの許可が指示されたことを示す信号である。確認応答信号を受信した場合(ST58、YES)、プロセッサ11は、アクセスを許可し(ST55)、電子錠19を開錠させる制御を行う。

[0094] 確認応答信号が受信できない場合(ST58、NO)、プロセッサ11は、タイマ15が計時する時間によって所定の許容時間が経過したかチェックする(ST59)。確認応答信号が受信したタイミングが許容時間内であれば(ST59、NO)、プロセッサ11は、確認応答信号の受信待ちとする。許容時間を超えた場合(ST59、YES)、プロセッサ11は、鍵装置20Bによるアクセスを不可とする(ST60)。例えば、アクセスを不可とする場合、プロセッサ11は、鍵装置20Bを用いた電子錠19の開錠を拒否する。この場合、プロセッサ11は、アクセス不可を示すアラームを鳴らしたり、アクセス不可を示す情報を表示装置により表示したりしても良い。

[0095] 以上のような第2実施形態に係る認証システムによれば、鍵装置に備えた物理キーによる鍵の確認と鍵装置における使用者に対する生体認証の結果に応じて電子錠の開錠などのアクセス制御が可能となる。例えば、鍵装置をス

マートキーに対するエマージェンシーキーとする場合、スマートキー本体としての鍵ホルダに不具合や電池切れが生じて、エマージェンシーキーとしての鍵装置が生体認証で使用者を確認することができ、セキュリティを確保できる。また、生体認証で本人拒否が発生した場合であっても、予め設定した確認装置でのアクセス確認によって2要素認証でアクセスコントロールすることができ、セキュリティレベル低下を抑えつつ、実用性が高い認証システムを提供できる。

[0096] (第3実施形態)

次に、第3実施形態について説明する。

図13は、第3実施形態に係る認証システム1Cにおける各装置の構成例を示すブロック図である。図13に示す第3実施形態に係る認証システム1Cは、アクセス制御装置(錠前装置)10C、鍵装置20C、確認装置30および鍵ホルダ70を有する。また、図14は、第3実施形態に係る鍵装置20Cおよび鍵ホルダ70の構成例を示す図である。

[0097] 第3実施形態に係る認証システム1Cは、鍵装置20Cが鍵ホルダ70に収納された状態で生体認証を行う点が第2実施形態で説明した認証システム1Bとは異なる。なお、図13及び図14に示す構成例において、図2、図7又は図18に示す構成と同様なものについては同一箇所同一符号を付して詳細な説明を省略する。また、第1または第2実施形態の構成から導かれる効果についても同様にここでは詳細な説明を省略する。

[0098] 図13に示す構成例において、アクセス制御装置10Cは、プロセッサ11、ROM12、RAM13、データメモリ14、タイマ15、第1通信インターフェース16、第2通信インターフェース17および電子錠(セキュリティ機器)19およびキー識別部(キー識別器)51を有する。

図13に示すアクセス制御装置10Cは、図7に示す第2実施形態のアクセス制御装置10Bの構成から送電インターフェース18を省略した構成となっている。また、アクセス制御装置10Cは、第1通信インターフェース16が鍵ホルダ70の通信インターフェース74と通信する構成となってい

る点が第2実施形態とは異なっている。

[0099] 図13に示す構成例において、鍵装置20Cは、プロセッサ21、ROM22、RAM23、データメモリ24、通信インターフェース25、生体センサ（指紋センサ）27、受電インターフェース28、および、物理キーKを有する。

[0100] 鍵装置20Cにおいて、鍵ホルダ70に収納された状態において、受電インターフェース28が鍵ホルダ70に設けた電池75から電力を受電できるように接続され、プロセッサ21が鍵ホルダ70のプロセッサ71と情報通信ができるように接続される。

なお、物理キーKは、第2実施形態で説明したものと同様に、鍵としての固有の情報を有する。物理キーKは、キー識別部51によって正当な鍵であるか否かが判別されるように構成されるものとする。

[0101] 図13に示す構成例において、鍵ホルダ70は、鍵装置20Cの少なくとも一部を収納する筐体70aを有する。鍵ホルダ70は、筐体70a内において、プロセッサ71、ROM72、RAM73、通信インターフェース74および電池75を有する。また、プロセッサ71は、データバスなどを介してROM22、RAM23、通信インターフェース74などに接続する。また、プロセッサ71は、コンタクト部71aを介して筐体70aに収納された鍵装置20Cのプロセッサ21にも接続される。また、電池75は、筐体70a内の各部にも電力を供給するように接続される。また、電池75は、コンタクト部75aを介して筐体70aに収納された鍵装置20Cの受電インターフェース28に電力を供給するように接続される。

[0102] プロセッサ71は、鍵ホルダ70の制御を司る制御部として機能する。プロセッサ71は、例えば、CPUである。プロセッサ71は、プログラムを実行することにより各部の制御及び情報処理を実現するものであればよい。すなわち、プロセッサ71は、ROM72などに記憶される制御プログラム及び制御データに基づいて種々の処理を行う。また、図13に示す構成例において、プロセッサ71は、当該鍵ホルダ70に鍵装置20Cを収納した状

態において鍵装置２０Ｃのプロセッサ２１と通信可能なように接続される。
なお、後述するようなプロセッサ２１がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであっても良い。

[0103] ROM ７２は、予め制御用のプログラム及び制御データなどを記憶する不揮発性のメモリである。ROM ７２は、製造段階で制御プログラム及び制御データなどを記憶した状態で鍵装置２０Ｃに組み込まれる。

[0104] RAM ７３は、揮発性のメモリである。RAM ７３は、プロセッサ７１の処理中のデータなどを一時的に格納する。例えば、RAM ７３は、計算用バッファ、受信用バッファ及び送信用バッファとして機能する。計算用バッファとしては、プロセッサ７１が実行する種々の演算処理の結果などを一時的に保持する。受信用バッファとしては、通信インターフェース７４を介してアクセス制御装置１０Ｃから受信するコマンドデータなどを保持する。送信用バッファとしては、通信インターフェース７４を介してアクセス制御装置１０Ｃへ送信するメッセージ（レスポンスデータ）などを保持する。

[0105] 通信インターフェース７４は、アクセス制御装置１０Ｃと通信するためのインターフェースである。通信インターフェース７４は、図２に示す通信インターフェース２５と同様に、アクセス制御装置１０Ｃの第１通信インターフェース１６と通信接続し、データの送受信を行う。通信インターフェース７４は、第１通信インターフェース１６に対応した通信方式のインターフェースであれば良い。

[0106] 電池７５は、鍵ホルダ７０および鍵装置２０Ｃの電源として用いる。電池７５は、乾電池などの一次電池または充電電池などの二次電池である。図１３に示す構成例において、電池７５は、鍵装置２０Ｃを収納した状態において鍵装置２０Ｃの受電インターフェース２８に接続するものとする。

[0107] また、図１４に示す構成例において、鍵装置２０Ｃは、物理キーＫなどの一部が鍵ホルダ７０内に収納される筐体７０ａを有する。鍵装置２０Ｃは、鍵ホルダ７０に着脱可能な形状を有する。鍵装置２０Ｃは、鍵ホルダ７０に

収納された状態で生体センサ２７が取得する生体情報に対する生体認証ができるように構成される。また、鍵装置２０Ｃは、生体センサ２７が生体情報を取得できる状態で鍵ホルダ７０に収納され、鍵ホルダ７０と電氣的にも接続する。図１３に示すように、鍵装置２０Ｃは、鍵ホルダ７０内に設けた電池７５から動作用の電力を受電でき、鍵ホルダ７０内のプロセッサ７１と情報の送受信ができるように接続される。

[0108] すなわち、鍵装置２０Ｃは、鍵ホルダ７０に収納した状態において、鍵ホルダ７０からの電力を受けて動作し、使用者から取得する生体情報に対する生体認証が実行できる。また、鍵ホルダ７０は、アクセス制御装置１０Ｃと通信する通信インターフェース７４を有する。このため、鍵装置２０Ｃは、鍵ホルダ７０に収納した状態において、鍵ホルダ７０を介してアクセス制御装置１０Ｃと通信できるように構成される。

[0109] 次に、第３実施形態に係る認証システム１Ｃの動作について説明する。

図１５は、第３実施形態に係る鍵装置２０Ｃにおける生体認証が失敗した場合における認証システム１Ｃの動作例を説明するためのシーケンスである。図１５は、生体認証が失敗した後の確認要求信号に対して確認装置３０でアクセス許可が指示された場合の動作例を示す。なお、図１５に示す動作例において、確認要求信号を送信した後の動作は、図４に示す動作例と同様であるため、詳細な説明を省略するものとする。

[0110] 図１５に示すように、鍵ホルダ７０は、収納している鍵装置２０Ｃに対して動作用の電力を供給する（ＳＴ７０）。例えば、鍵装置２０Ｃが鍵ホルダ７０に収納された状態において、鍵ホルダ７０の電池７５は、鍵装置２０Ｃの受電インターフェースに接続される。鍵装置２０Ｃの受電インターフェース２８は、鍵ホルダ７０の電池７５から動作用の電力を取得し、当該鍵装置２０Ｃ内の各部に供給する。また、鍵ホルダ７０のプロセッサ７１は、図示しない操作キーなどへの入力に応じて電池７５から動作用の電力を供給するように制御しても良い。

[0111] 鍵装置２０Ｃのプロセッサ２１は、鍵ホルダ７０の電池７５からの電力に

よって起動する。起動した鍵装置20Cのプロセッサ21は、データメモリ24に記録されている当該鍵装置の識別情報としての識別子を読み出す(ST71)。また、プロセッサ21は、生体センサ27により使用者の生体情報を取得し、取得した生体情報に対する生体認証を実行する(ST72)。例えば、プロセッサ21は、生体センサ27としての指紋センサが取得する使用者の指紋画像とデータメモリ24に記憶している登録者の認証データに含まれる生体情報の特徴点情報(生体情報の特徴量)とを照合することにより生体認証を実行する。図15では、プロセッサ21は、使用者と登録者とが同一人物であると認証できず、生体認証に失敗した(生体認証がNGであった)ものとする。

[0112] 鍵装置20Cのプロセッサ21は、データメモリ24から読み出した識別子と生体認証結果(ここでは、生体認証が失敗したことを示す情報)とを鍵ホルダ70へ通知する(ST73)。ここで、プロセッサ21は、当該鍵装置20Cの識別子と使用者に対する生体認証結果とをアクセス制御装置10Cへの転送用のデータとして鍵ホルダ70のプロセッサ71へ通知するようにしても良い。

鍵ホルダ70のプロセッサ71は、鍵装置20Cの識別子と使用者に対する生体認証結果とを鍵装置20Cから受けると、受信した識別子及び生体認証結果を含む情報を通信インターフェース74によりアクセス制御装置10Cへ送信する(ST74)。

[0113] アクセス制御装置10Cは、第1通信インターフェース16によって鍵装置20Cからの識別子と生体認証結果とを受信する。鍵装置20Cの識別子を受信すると、アクセス制御装置10Cのプロセッサ11は、アクセス管理テーブル14aを参照して当該鍵装置20Aが正当な鍵であるか否かを判定する。例えば、プロセッサ11は、受信した鍵装置20Aの識別子がアクセス管理テーブル14aに登録されている識別子と一致するか否かにより、正当な鍵である否かを判定する。図15に示す例では、プロセッサ11は、受信した識別子が示す鍵装置20Cが正当な鍵であると判定するものとする。

- [0114] また、プロセッサ 11 は、鍵装置 20C が正当な鍵である場合、鍵装置 20A における生体認証結果を確認する。鍵装置 20C が正当な鍵で、かつ、鍵装置 20C の使用者が登録者（正当な利用者）である場合、つまり、生体認証が成功（OK）である場合、プロセッサ 11 は、電子錠 19 を開錠（アクセスを許可）する制御を行う。
- [0115] 鍵装置 20A が正当な鍵で、かつ、鍵装置 20A の使用者が登録者（正当な利用者）であることが生体認証で確認できなかった場合、つまり、生体認証が失敗（NG）である場合（ST75）、プロセッサ 11 は、当該識別子に対応する確認先に確認要求信号を送信する（ST76）。例えば、プロセッサ 11 は、アクセス管理テーブル 14a を参照し、当該識別子に対応する確認先を特定する。確認先（確認要求信号の送信先）を特定すると、プロセッサ 11 は、第 2 通信インターフェース 17 を介して特定した確認先へ確認要求信号を送信する。
- [0116] また、確認要求信号を送信する際、プロセッサ 11 は、当該確認要求信号に対する確認装置 30 からの確認応答信号を有効とする期間（許容時間）を設定し、タイマ 15 による時間監視を開始する。時間監視を開始した後、プロセッサ 11 は、設定した許容時間内であれば、確認装置 30 からの確認応答信号を受け付ける。
- [0117] 確認装置 30 は、アクセス制御装置 10C からの確認要求信号を受信した場合、ユーザによるアクセス制御装置 10C の電子錠 19 を開錠させる指示を受け付ける。例えば、確認装置 30 は、確認要求信号を受けると、図示しない表示部にアクセス制御装置 10A の電子錠を開錠するか否かの確認画面を表示する。
- ここで、確認装置 30 では、ユーザが図示しない操作部を用いて電子錠の開錠指示したものとする。確認装置 30 は、ユーザが指示した電子錠の開示指示を受け付けると（ST77）、アクセス制御装置 10C に対して電子錠 19 の開錠を要求する確認応答信号を送信する（ST78）。
- [0118] アクセス制御装置 10C のプロセッサ 11 は、確認要求信号を送信した後

、許容時間内において確認応答信号を受け付ける。プロセッサ 11 は、許容時間内に確認装置 30 からの確認応答信号を受信すると、アクセスを許可する処理として電子錠 19 を開錠する制御を行う（ST79）。例えば、プロセッサ 11 は、錠を開錠させる制御信号を電子錠 19 へ供給し、電子錠 19 は、プロセッサ 11 からの制御信号に応じて錠を開錠する。

[0119] また、アクセス制御装置 10C のプロセッサ 11 は、確認要求信号を送信してから許容時間内に確認応答信号の受信がなければ、アクセスを不可として電子錠 19 を開錠しないようにする。

[0120] 上述したように、第 3 実施形態に係るアクセス制御装置 10C は、鍵装置 20C へ電力供給がなく、識別子および生体認証結果を鍵ホルダ 70 を介して受信する以外の動作は、図 6 に示すフローチャートのような第 1 実施形態と同様な動作で実現できる。このため、第 3 実施形態に係るアクセス制御装置 10C の動作例を詳細に説明することを省略するものとする。

[0121] なお、認証システムとしては、確認装置 30 が生体センサを有するものであっても良い。この場合、確認装置 30 は、アクセス許可を示す確認応答信号を受信すると、生体センサを用いてユーザに対する生体認証を実行し、その認証結果によってセキュリティ機器へのアクセスを許可するようにしても良い。

[0122] 以上のような第 3 実施形態に係る認証システムによれば、鍵装置を鍵ホルダに収納した状態において、鍵装置が鍵ホルダからの電力によって生体認証を実行し、鍵の識別子と生体認証結果とを鍵ホルダを介してアクセス制御装置へ提示できる。

[0123] これにより、電池などの電源や通信機能を持たない鍵装置であっても、鍵ホルダに装着することによって、鍵の確認と使用者に対する生体認証結果とに応じた電子錠の開錠などのアクセス制御が可能となる。また、生体認証で本人拒否が発生した場合であっても、予め設定した確認装置でのアクセス確認によって 2 要素認証でアクセスコントロールでき、セキュリティレベル低下を抑えつつ、実用性が高い認証システムを提供できる。

[0124] (第4実施形態)

次に、第4実施形態について説明する。

図16は、第4実施形態に係る認証システム1Dにおける各装置の構成例を示すブロック図である。

図16に示す第4実施形態に係る認証システム1Dは、アクセス制御装置(錠前装置)10D、鍵装置20Dおよび確認装置30を有する。アクセス制御装置10Dの構成は、図2に示すアクセス制御装置10Aの構成に加えて生体センサ82を具備する点が第1実施形態と異なる。また、鍵装置20Dの構成は、第1実施形態で説明した図2に示すアクセス制御装置10Aの生体センサ27が省略された点が第1実施形態と異なる。

[0125] なお、図16に示す構成例において、図2に示す構成と同様なものについては同一箇所に同一符号を付して詳細な説明を省略する。また、第1実施形態の構成から導かれる効果についても同様にここでは詳細な説明を省略する。

[0126] 図16に示す構成例において、アクセス制御装置10Dは、プロセッサ11、ROM12、RAM13、データメモリ14、タイマ15、第1通信インターフェース16、第2通信インターフェース17、電子錠(セキュリティ機器)19および生体センサ82を有する。

[0127] 図16に示すアクセス制御装置10Dは、図2に示す第1実施形態のアクセス制御装置10Aの構成に生体センサ82を具備した構成となっている。アクセス制御装置10Dにおいて、プロセッサ11は、生体センサ82が取得する生体情報に対して生体認証を実行する機能を有する。生体センサ82は、例えば、第1実施形態で説明した図2に示す鍵装置20Aが具備する生体センサ27と同様なもので実現できる。

[0128] ただし、生体センサ82は、生体情報として指紋情報を取得するものに限定されない。生体センサ82は、アクセス制御装置10Dにおいて実施できる生体認証に対応する生体情報を取得するものであれば良い。例えば、生体センサ82は、生体情報として顔情報を取得するものであっても良い。

[0129] また、アクセス制御装置１０Ｄは、生体センサ８２を用いて生体認証を実行するため、登録者の認証データ（生体情報の辞書データ）を格納する認証ＤＢ１４ｂをデータメモリ１４に設ける。認証ＤＢ１４ｂは、図２に示す第１実施形態で説明した認証ＤＢ２４ａと同様に、登録者の認証データとして登録者の生体情報の特徴点情報などの特徴量を記憶する。また、認証ＤＢ１４ｂは、複数の登録者の認証データを格納するようにしても良い。認証ＤＢ１４ｂは、鍵装置２０Ｃの鍵識別情報に対応づけて鍵識別情報が示す鍵に対応する登録者（アクセス権者）の生体情報の特徴点情報を含む認証データを記憶する。ただし、認証ＤＢ１４ｂは、データメモリ１４におけるセキュアなメモリ領域に確保される。

[0130] また、図１６に示す構成例において、鍵装置２０Ｄは、プロセッサ２１、ＲＯＭ２２、ＲＡＭ２３、データメモリ２４、通信インターフェース２５および受電インターフェース２８を有する。鍵装置２０Ｄは、第１実施形態で説明した図２に示す鍵装置２０Ａにおいて生体センサ２７を省略したもので実現できる。

[0131] 次に、第４実施形態に係る認証システム１Ｄの動作について説明する。

図１７は、第４実施形態に係る鍵装置２０Ｄにおける生体認証が失敗した場合における認証システム１Ｄの動作例を説明するためのシーケンスである。図１７は、生体認証が失敗した後の確認要求信号に対して確認装置３０でアクセス許可が指示された場合の動作例を示す。なお、図１７に示す動作例において、確認要求信号を送信した後の動作は、図４に示す動作例と同様であるため、詳細な説明を省略するものとする。

[0132] 図１７に示すように、アクセス制御装置１０Ｄは、鍵装置２０Ｄに対して動作の電力を供給する（ＳＴ８０）。例えば、アクセス制御装置１０Ｄは、送電インターフェース１８から鍵装置２０Ｄの受電インターフェース２８が受電可能な電力を出力する。

[0133] 鍵装置２０Ｄは、アクセス制御装置１０Ｄから供給される電力によって起動する。起動した鍵装置２０Ｄのプロセッサ２１は、通信インターフェース

25によるアクセス制御装置10Dとの通信状態を確立する。アクセス制御装置10Aとの通信状態が確立すると、プロセッサ21は、データメモリ24に記録されている当該鍵装置の鍵識別情報としての識別子を読み出す(ST81)。識別子を読み出すと、鍵装置20Dのプロセッサ21は、データメモリ24から読み出した識別子を通信インターフェース25によりアクセス制御装置10Dへ送信する(ST82)。

[0134] アクセス制御装置10Dは、第1通信インターフェース16によって鍵装置20Dからの識別子を受信する。鍵装置20Dの識別子を受信すると、アクセス制御装置10Aのプロセッサ11は、アクセス管理テーブル14aを参照して当該鍵装置20Aが正当な鍵であるか否かを判定する(ST83)。プロセッサ11は、受信した鍵装置20Aの識別子がアクセス管理テーブル14aに登録されている識別子と一致するか否かにより、正当な鍵であるか否かを判定する。図4に示す例では、プロセッサ11は、鍵装置20Aが正当な鍵であると判定するものとする。

[0135] また、プロセッサ11は、鍵装置20Dが正当な鍵である場合、生体センサ82により使用者の生体情報を取得し、取得した使用者の生体情報に対する生体認証を実行する(ST84)。例えば、プロセッサ11は、データメモリ24の認証DB14bに記憶している当該識別子に対応する登録者の認証データを特定する。プロセッサ11は、登録者の認証データを特定すると、生体センサ27が取得する使用者の生体情報と登録者の認証データに含まれる生体情報の特徴点情報とを照合することにより生体認証を実行する。生体認証が成功である場合、つまり、鍵装置20Aが正当な鍵で、かつ、鍵装置20Aの使用者が登録者(正当な利用者)である場合、プロセッサ11は、電子錠19を開錠(アクセスを許可)する制御を行う。

[0136] なお、プロセッサ11が実行する生体認証は、生体センサ82が取得する生体情報に応じた認証処理である。例えば、生体センサ82が指紋センサである場合、プロセッサ11は、指紋による生体認証を実行する。また、生体センサ82がカメラなどの顔画像を取得するものである場合、プロセッサ1

1 は、顔画像による生体認証を実行する。

[0137] ここでは、プロセッサ 11 は、使用者が識別子に対応する登録者と同一人物であると認証できず、生体認証に失敗した（生体認証がNGであった）ものとする（ST85）。生体認証が失敗である場合、つまり、鍵装置 20A が正当な鍵で、かつ、鍵装置 20A の使用者が登録者（正当な利用者）であることが生体認証で確認できなかった場合、プロセッサ 11 は、当該識別子に対応する確認先に確認要求信号を送信する（ST86）。プロセッサ 11 は、アクセス管理テーブル 14a を参照し、当該識別子に対応する確認先を特定し、第 2 通信インターフェース 17 により特定した確認先へ確認要求信号を送信する。

[0138] また、確認要求信号を送信する場合、プロセッサ 11 は、当該確認要求信号に対する確認装置 30 からの確認応答信号を有効とする期間（許容時間）を設定し、タイマによる時間監視を開始する。時間監視を開始した後、プロセッサ 11 は、設定した許容時間内であれば、確認装置 30 からの確認応答信号を受け付ける。

[0139] 確認装置 30 は、アクセス制御装置 10D からの確認要求信号を受信した場合、ユーザによるアクセス制御装置 10D の電子錠 19 を開錠させる指示を受け付ける。確認装置 30 は、ユーザにより電子錠の開錠指示（アクセス許可の指示）が入力されると（ST87）、アクセス制御装置 10D に対して電子錠 19 の開錠を要求する確認応答信号を送信する（ST88）。

[0140] アクセス制御装置 10D のプロセッサ 11 は、確認要求信号を送信した後、許容時間内において確認応答信号を受け付ける。プロセッサ 11 は、許容時間内に確認装置 30 からの確認応答信号を受信すると、アクセスを許可する処理として電子錠 19 を開錠する制御を行う（ST89）。例えば、プロセッサ 11 は、錠を開錠させる制御信号を電子錠 19 へ供給し、電子錠 19 は、プロセッサ 11 からの制御信号に応じて錠を開錠する。

[0141] また、確認要求信号を送信してから許容時間内に確認応答信号の受信がなければ、アクセス制御装置 10D のプロセッサ 11 は、アクセスを不可とし

て電子錠 19 を開錠しないようにする。この場合、アクセス制御装置 10A のプロセッサ 11 は、アクセス不可となった旨をアラームなどで報知するようにしても良いし、確認装置 30 へ通知するようにしても良い。

[0142] 次に、第 4 実施形態に係るアクセス制御装置 10D の動作について説明する。

図 18 は、第 4 実施形態に係るアクセス制御装置 10D の動作例を説明するためのフローチャートである。

まず、アクセス制御装置 10D のプロセッサ 11 は、送電インターフェース 18 により鍵装置 20A へ動作用の電力を供給する。プロセッサ 11 は、送電インターフェース 18 から送電する電力によって起動する鍵装置 20D と第 1 通信インターフェース 16 を介して通信する。プロセッサ 11 は、第 1 通信インターフェース 16 により鍵装置 20D の識別子を取得する (ST90)。

[0143] 第 1 通信インターフェース 16 により鍵装置 20D の識別子を受信すると、プロセッサ 11 は、受信した識別子がアクセス管理テーブル 14a に登録済みの識別子と一致するか否かにより鍵装置 20D が正当な鍵であるか否かを判定する (ST91)。

[0144] 鍵装置 20D が正当な鍵でないと判定した場合 (ST91、NO)、プロセッサ 11 は、当該鍵装置 20D によるアクセスを不可とする (ST99)。例えば、アクセスを不可とする場合、プロセッサ 11 は、鍵装置 20D を用いた電子錠 19 の開錠を拒否する。この場合、プロセッサ 11 は、アクセス不可を示すアラームを鳴らしたり、アクセス不可を示す情報を表示装置により表示したりしても良い。

[0145] 鍵装置 20D が正当な鍵であると判定した場合 (ST91、YES)、プロセッサ 11 は、生体認証を実行する (ST92)。プロセッサ 11 は、生体センサ 82 が取得する使用者の生体情報と当該鍵装置 20D に対応づけられた登録者の認証データに含まれる生体情報の特徴点情報とを照合する。プロセッサ 11 は、使用者の生体情報と登録者の生体情報の特徴点情報との類

似度によって使用者が登録者であるか否かを判定し、その判定結果を生体認証結果とする。

[0146] 生体認証が完了すると、プロセッサ11は、生体認証結果に基づいて使用者が当該鍵装置に対応づけられた登録者であることが認証されたか否かを判定する(ST93)。生体認証により使用者が登録者であることが確認された場合、つまり、生体認証が成功であった場合(ST93、YES)、プロセッサ11は、当該鍵装置20Dによるアクセスを許可する(ST94)。例えば、プロセッサ11は、電子錠19を開錠させる制御信号を出力することにより電子錠19を開錠させる。

[0147] また、生体認証により使用者が登録者であることが確認できなかった場合、つまり、生体認証が失敗であった場合(ST93、NO)、プロセッサ11は、アクセス管理テーブル14aにおいて当該識別子に対応づけられている確認先を特定し、第2通信インターフェース17を用いて特定した確認先へ確認応答信号を送信する(ST95)。確認応答信号を送信した際、プロセッサ11は、タイマ15による時間の計時を開始する(ST96)。

[0148] タイマ15による計時を開始した後、プロセッサ11は、第2通信インターフェース17により確認装置30からの確認応答信号を受信したかを監視する(ST97)。確認応答信号は、確認装置30においてアクセス制御装置10Aに対してアクセスの許可が指示されたことを示す信号である。確認応答信号を所定の許容時間に受信した場合(ST97、YES)、プロセッサ11は、アクセスを許可し(ST94)、電子錠19を開錠させる制御を行う。

[0149] 確認応答信号が受信できない場合(ST97、NO)、プロセッサ11は、タイマ15が計時する時間によって所定の許容時間が経過したかチェックする(ST98)。タイマ15が計時する時間が許容時間内であれば(ST98、NO)、プロセッサ11は、再び確認応答信号の受信待ちとする。タイマ15が計時する時間が許容時間を超えた場合(ST98、YES)、プロセッサ11は、鍵装置20Dによるアクセスを不可とする(ST94)。

- [0150] 上記のように、第4実施形態に係るアクセス制御装置は、鍵装置から取得する識別子が正当な鍵（鍵装置）の識別子であれば、生体認証を実行する。アクセス制御装置は、使用者と当該鍵の登録者との生体認証が成功すればアクセスを許可するが、生体認証が失敗した場合には当該鍵に対応づけた確認先（確認装置）にアクセスの可否を問い合わせる。アクセス制御装置は、確認先からアクセスの許可を指示する信号を所定の許容時間内に受信できればアクセスを許可する。
- [0151] これにより、鍵装置で生体認証を実行しなくても、鍵の識別子と生体認証の結果とによるアクセス制御ができ、さらに、生体認証が失敗した場合でも予め登録した確認先でのアクセス確認によって電子錠の開錠などのアクセス許可を行うことができる。すなわち、アクセス制御装置での生体認証による本人拒否が発生した場合であっても、予め設定した確認装置でのアクセス確認による2要素認証でアクセスコントロールすることができ、セキュリティレベル低下を抑えつつ、実用性の高い認証システムを提供できる。
- [0152] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。