

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7489658号
(P7489658)

(45)発行日 令和6年5月24日(2024.5.24)

(24)登録日 令和6年5月16日(2024.5.16)

(51)国際特許分類

F I

G 0 6 F 21/33 (2013.01)

G 0 6 F 21/32 (2013.01)

G 0 6 F 21/33

G 0 6 F 21/32

請求項の数 20 外国語出願 (全51頁)

(21)出願番号	特願2020-98960(P2020-98960)	(73)特許権者	520201123
(22)出願日	令和2年6月5日(2020.6.5)		モカ システム インコーポレイテッド
(65)公開番号	特開2020-201956(P2020-201956 A)		大韓民国、1 3 5 5 4、ギョングード、ソナムーシ、ブンダンーグ、ジョンジエイルー口、2 4 8、# 1 7 0 4
(43)公開日	令和2年12月17日(2020.12.17)	(74)代理人	110000877
審査請求日	令和4年6月1日(2022.6.1)		弁理士法人 R Y U K A 国際特許事務所
(31)優先権主張番号	10-2019-0066684	(72)発明者	リー、ジョン クン
(32)優先日	令和1年6月5日(2019.6.5)		大韓民国、1 3 5 5 4、ギョングード、ソナムーシ、ブンダンーグ、ジョンジエイルー口、2 4 8、# 1 7 0 4
(33)優先権主張国・地域又は機関	韓国(KR)	(72)発明者	モカ システム インコーポレイテッド内
			チョイ、ソン ビン
			大韓民国、1 3 5 5 4、ギョングード、ソナムーシ、ブンダンーグ、ジョンジ
			最終頁に続く

(54)【発明の名称】 アクセス制御デバイス、アクセス制御システム及びそれらを用いたアクセス制御方法

(57)【特許請求の範囲】

【請求項1】

ターゲットドアに対応するアクセス制御デバイスの周辺にある前記ターゲットドアに入るために、ユーザのアクセス認証を実行する前記ユーザの端末により実行されるアクセス制御方法であって、

前記ユーザの前記端末において、前記アクセス制御デバイスを検出する段階と、

前記検出されたアクセス制御デバイスと前記ユーザの前記端末との間に通信チャネルを確立する段階と、

前記通信チャネルを通じて、前記アクセス制御デバイスから識別情報を受信する段階と、

前記受信した識別情報に基づいて、前記ユーザの前記アクセス認証の前記ターゲットドアをチェックする段階と、

前記ユーザの前記端末に予め格納されたアクセス権情報に基づいて、前記ユーザが前記ターゲットドアにアクセスすることを認められているか否かを判定する段階とを備え、

前記アクセス権情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、及び、アクセススケジュール情報、のうちの少なくとも1つを含み、

有効期間が前記アクセス権情報に設定され、

前記有効期間が経過した場合、前記アクセス権情報が失効し、

前記アクセス制御方法は、前記アクセス権情報が失効した後で、前記アクセス権情報を管

理するサーバから前記アクセス権情報に関連する情報を取得する段階を、さらに備える、アクセス制御方法。

【請求項 2】

前記通信チャネルを通じて、前記ユーザの生体認証情報を受信する段階をさらに備え、前記ユーザの前記生体認証情報は、前記アクセス制御デバイスに対して前記ユーザから入力され、

前記アクセス権情報は、登録された生体認証情報をさらに含む、請求項 1 に記載のアクセス制御方法。

【請求項 3】

前記ユーザが前記ターゲットドアにアクセスすることを認められているか否かを前記判定する段階は、

前記ユーザの前記受信した生体認証情報を前記登録された生体認証情報と比較する段階と、

前記ユーザの生体認証情報が前記登録された生体認証情報のうちの 1 つに合致する場合、前記アクセス認証が成功したと判定する段階と

を含む、請求項 2 に記載のアクセス制御方法。

【請求項 4】

前記登録された生体認証情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、アクセススケジュール情報、及び、前記有効期間のうちの少なくとも 1 つに対応する、請求項 3 に記載のアクセス制御方法。

【請求項 5】

前記アクセス権情報は、前記登録された生体認証情報に対応する前記アクセススケジュール情報をさらに含む、

前記ユーザの生体認証情報が前記登録された生体認証情報のうちの 1 つに合致する場合、前記アクセス認証が成功したと前記判定する段階は、

前記アクセス権情報の前記ユーザの前記受信した生体認証情報に関連する前記アクセススケジュール情報と現在の時刻を比較する段階と、

前記現在の時刻がアクセススケジュールに含まれていない場合、前記アクセス認証が失敗したと判定する段階と

を含む、請求項 4 に記載のアクセス制御方法。

【請求項 6】

前記アクセス権情報は、前記登録された生体認証情報に対応する前記登録された端末識別情報をさらに含む、

前記ユーザの生体認証情報が前記登録された生体認証情報のうちの 1 つに合致する場合、前記アクセス認証が成功したと前記判定する段階は、

前記ユーザの生体認証情報が前記登録された生体認証情報のうちの 1 つに合致する場合、前記ユーザの前記端末の前記識別情報を、前記ユーザの前記受信した生体認証情報に合致した前記登録された生体認証情報に対応する前記登録された端末識別情報と比較する段階と、

前記ユーザの前記端末の前記識別情報が、前記ユーザの前記受信した生体認証情報に対応する前記登録された端末識別情報のうちの 1 つに合致しない場合、前記アクセス認証が失敗したと判定する段階と

を含む、請求項 4 に記載のアクセス制御方法。

【請求項 7】

前記アクセス権情報は、前記登録されたアクセス制御デバイス識別情報を含み、

前記ユーザが前記ターゲットドアにアクセスすることを認められているか否かを前記判定する段階は、

前記受信した識別情報を、前記アクセス権情報の前記登録されたアクセス制御デバイス識別情報と比較する段階と、

前記受信した識別情報が、前記登録されたアクセス制御デバイス識別情報のうちの 1 つ

10

20

30

40

50

に合致する場合、前記アクセス認証が成功したと判定する段階と
を含む、請求項 1 から 6 のいずれか一項に記載のアクセス制御方法。

【請求項 8】

前記登録されたアクセス制御デバイス識別情報は、前記登録されたユーザ識別情報、前記登録された端末識別情報、前記アクセススケジュール情報、及び、前記有効期間のうちの少なくとも 1 つに対応する、請求項 7 に記載のアクセス制御方法。

【請求項 9】

前記アクセス権情報は、前記登録されたアクセス制御デバイス識別情報に対応する前記アクセススケジュール情報をさらに含み、

前記受信した識別情報が前記登録されたアクセス制御デバイス識別情報のうちの 1 つに合致する場合、前記アクセス認証が成功したと前記判定する段階は、

前記アクセス権情報の前記受信した識別情報に関連する前記アクセススケジュール情報と現在の時刻を比較する段階と、

前記現在の時刻がアクセススケジュールに含まれていない場合、前記アクセス認証が失敗したと判定する段階と

を含む、請求項 8 に記載のアクセス制御方法。

【請求項 10】

前記アクセス権情報は、前記登録されたアクセス制御デバイス識別情報に対応する前記登録された端末識別情報をさらに含み、

前記受信した識別情報が前記登録されたアクセス制御デバイス識別情報のうちの 1 つに合致する場合、前記アクセス認証が成功したと前記判定する段階は、

前記ユーザの前記端末の前記識別情報を、前記受信した識別情報に関連する前記登録された端末識別情報と比較する段階と、

前記ユーザの前記端末の前記識別情報が、前記受信した識別情報に対応する前記登録された端末識別情報のうちの 1 つに合致しない場合、前記アクセス認証が失敗したと判定する段階と

を含む、請求項 8 に記載のアクセス制御方法。

【請求項 11】

前記アクセス権情報が失効した場合、前記ユーザが前記ターゲットドアにアクセスすることを認められているか否かを前記判定する前記段階が回避される、請求項 1 から 10 のいずれか一項に記載のアクセス制御方法。

【請求項 12】

前記アクセス認証が成功した場合、

ドア開放信号を生成する段階と、

前記ドア開放信号を前記アクセス制御デバイスに伝送する段階であって、前記ドア開放信号は、前記アクセス制御デバイスにドア開放動作を実行させる、段階と

をさらに備える、請求項 1 から 11 のいずれか一項に記載のアクセス制御方法。

【請求項 13】

前記アクセス権情報は、前記サーバから伝送される、請求項 1 から 12 のいずれか一項に記載のアクセス制御方法。

【請求項 14】

前記判定する前記段階が完了した場合、前記アクセス認証の結果情報を生成する段階をさらに備える、請求項 1 から 13 のいずれか一項に記載のアクセス制御方法。

【請求項 15】

複数のユーザに関連する前記アクセス認証の前記結果情報を管理する前記サーバに、前記アクセス認証の前記結果情報を伝送する段階をさらに備える、請求項 14 に記載のアクセス制御方法。

【請求項 16】

前記ターゲットドアは、前記検出されたアクセス制御デバイスと前記ユーザの前記端末との間の距離に基づいて選択される、請求項 1 から 15 のいずれか一項に記載のアクセス

10

20

30

40

50

制御方法。

【請求項 17】

前記ターゲットドアは、前記検出されたアクセス制御デバイスと前記ユーザの前記端末との間の、特定の距離より短い前記距離を有する前記検出されたアクセス制御が導入されたドアである、請求項 16 に記載のアクセス制御方法。

【請求項 18】

請求項 1 から 17 のいずれか一項に記載のアクセス制御方法を、プロセッサに実行させるためのプログラム。

【請求項 19】

アクセス制御デバイスに対応するターゲットドアの周辺にある前記アクセス制御デバイスであって、

前記アクセス制御デバイスとユーザの端末との間に通信チャネルを確立するように構成される通信ユニットと、

前記通信チャネルを通じて、前記ユーザの前記端末に対して、前記ターゲットドアに入るために前記ユーザの前記端末に予め格納されたアクセス権情報に基づいて、前記ユーザの前記端末により実行される前記ユーザのアクセス認証用の前記アクセス制御デバイスの識別情報を、前記通信ユニットを介して伝送するように構成される制御ユニットと

を備え、

前記アクセス権情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、及び、アクセススケジュール情報、のうちの少なくとも 1 つを含み、

有効期間が前記アクセス権情報に設定され、

前記有効期間が経過した場合、前記アクセス権情報が失効し、

前記端末は、前記アクセス権情報が失効した後で、前記アクセス権情報を管理するサーバから前記アクセス権情報に関連する情報を取得するように構成される、アクセス制御デバイス。

【請求項 20】

前記ユーザの生体認証情報を受信するための生体認証情報入力ユニットをさらに備え、

前記制御ユニットは、前記通信チャネルを通じて前記ユーザの前記端末に、前記ユーザの前記生体認証情報を、前記通信ユニットを介して伝送するように構成され、

前記ユーザの前記生体認証情報は、前記アクセス制御デバイスに対して前記ユーザから入力され、

前記アクセス権情報は、登録された生体認証情報をさらに含む、請求項 19 に記載のアクセス制御デバイス。

【発明の詳細な説明】

【技術分野】

【0001】

〔関連出願の相互参照〕

本願は、2019 年 6 月 5 日に出願された韓国特許出願第 10-2019-0066684 号の優先権及び利益を主張し、本開示は、その全体が参照により本明細書に組み込まれる。

【背景技術】

【0002】

1. 発明の分野

本開示は、アクセス制御デバイス、アクセス制御システム及びそれらを用いたアクセス制御方法に関する。

【0003】

2. 関連分野についての議論

アクセス制御システムは、ドアを通過する特定の空間にアクセスしようとする訪問者を認識及び管理するシステムである。アクセス制御システムは、典型的なオフィス及び住居

10

20

30

40

50

において、並びに、高いセキュリティを有するアクセスが制限される施設において広く用いられている。

【0004】

そのようなアクセス制御システムにおいて用いられる従来の認証方法は、磁気カード、スマートカード、非接触無線カードなどを用いた認証方法、及び、訪問者の指紋及び虹彩などの生体認証情報を用いた認証方法を含む。

【0005】

そのような従来の認証方法において、ドアの近くに設置された認証デバイスを通じて訪問者が認証を実行した後のみ、訪問者はドアにアクセスし得る。上述したように、認証は、別個の認証デバイスを通じて実行される必要がある。したがって、複数の訪問者がいる場合、認証を実行するのに長い時間がかかる。さらに、ユーザが、例えば、磁気カードなどの別個の認証手段を常に携帯する必要があるという点で不便であり、そのような認証手段が無くなった場合、別個の認証手段を盗んだ権限のない訪問者がドアにアクセスできてしまうという欠点もある。

【0006】

また、従来の認証方法では、ドアの近くに設置された認証デバイスをまとめて処理する制御サーバを用いることでしか、認証が実行されていない。したがって、制御サーバと、ドアの近くに設置された認証デバイスとの間の通信が接続されていない場合、又は、制御サーバが動作していない場合、ドアにアクセスできない。

【0007】

また、従来の認証方法では、アクセス認証のための情報が認証デバイスに格納されており、個人情報のセキュリティに関する課題が生じ得る。

【0008】

最近、これらの課題を解決すべく、ユーザの利便性を高め、また、アクセス制御システムのセキュリティを向上させる取り組みが行われている。

【発明の概要】

【0009】

本開示は、ユーザの利便性を向上させつつ、セキュリティを向上させることが可能なアクセス制御デバイス、アクセス制御システム及びそれらを用いたアクセス制御方法を提供することを対象とする。

【0010】

解決しようとする技術的課題は、上述の課題に限定されず、本明細書において説明されない他の技術的課題が、以下の説明及び添付の図面から当業者により明確に理解される。

【0011】

本開示の態様によれば、ターゲットドアに対応するアクセス制御デバイスの周辺にあるターゲットドアに入るために、ユーザのアクセス認証を実行するユーザの端末により実行されるアクセス制御方法が提供されてよく、当該方法は、ユーザの端末において、アクセス制御デバイスを検出する段階と、検出されたアクセス制御デバイスとユーザの端末との間に通信チャネルを確立する段階と、通信チャネルを通じて、アクセス制御デバイスから識別情報を受信する段階と、受信した識別情報に基づいて、ユーザのアクセス認証のターゲットドアをチェックする段階と、ユーザの端末に予め格納されたアクセス権情報に基づいて、ユーザがターゲットドアにアクセスすることを認められているか否かを判定する段階とを備え、アクセス権情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、アクセススケジュール情報、及び、アクセス権情報の有効期間情報のうちの少なくとも1つを含む。

【0012】

本開示の技術的な解決手段は、上述の解決手段に限定されず、以下の説明及び添付の図面から当業者により、本明細書において説明されない他の解決手段が明確に理解される。

【図面の簡単な説明】

【0013】

本開示の上記及び他の目的、特徴及び利点は、添付の図面に対する参照を用いて、それらの例示的な実施形態を詳細に説明することにより、当業者に対してより明らかになる。

【図 1】本開示の実施形態に係るアクセス制御システムのブロック図である。

【図 2】本開示の実施形態に係るサーバのブロック図である。

【図 3】本開示の実施形態に係る端末のブロック図である。

【図 4】本開示の実施形態に係るアクセス制御デバイスのブロック図である。

【図 5】本開示の実施形態に係るユーザの端末を用いて、アクセス制御デバイスを制御するための方法のフローチャートである。

【図 6】本開示の実施形態に係るユーザの端末においてアクセス認証を実行するための方法のフローチャートである。

【図 7】本開示の実施形態に係るアクセス権情報の例示的な図である。

【図 8】本開示の実施形態に係るアクセス権情報の例示的な図である。

【図 9】本開示の実施形態に係るアクセス制御方法に関する周辺図である。

【図 10】本開示の実施形態に係るアクセス認証結果を管理するための方法のフローチャートである。

【図 11】本開示の実施形態に係るドア開放を管理するための方法のフローチャートである。

【図 12】本開示の実施形態に係る、ドアにアクセスする際に、情報を通知するための方法のフローチャートである。

【図 13】本開示の実施形態に係る生体認証情報を用いてアクセス認証結果を管理するための方法のフローチャートである。

【図 14】本開示の実施形態に係る生体認証情報を用いてドア開放を管理するための方法のフローチャートである。

【図 15】本開示の実施形態に係るアクセス制御デバイスの設定を変更するための方法に関する周辺図である。

【図 16】本開示の実施形態に係るアクセス制御デバイスの設定を変更するための方法のフローチャートである。

【図 17】本開示の実施形態に係るアクセス制御デバイスにおいて、ユーザの端末により取得される生体認証情報を格納するための方法のフローチャートである。

【発明を実施するための形態】

【0014】

添付の図面と併せて行われる以下の詳細な説明から、本開示の上記の目的、特徴及び利点がより明らかになる。本開示は、様々に変更されてよく、いくつかの例示的な実施形態を有するので、具体的な実施形態は、添付の図面において示され、詳細に説明される。

【0015】

図では、わかりやすくするために層及び領域の厚みが誇張されている。また、要素又は層が別の要素又は層「上」にあることが言及される場合、当該要素又は層は、別の要素又は層に直接形成され得る、又は、第3の要素又は層がその間に介在され得る。本明細書にわたって、同様の参照符号は、同様の要素を指す。さらに、同様の参照符号は、実施形態の図面に示される同じ範囲内の同様の要素を指定するために用いられる。

【0016】

本開示の内容を不必要に曖昧にしないために、本開示と関連する周知の機能又は構成に関する詳細な説明が除外される。以下の説明では、序数（例えば、第1及び第2）が用いられるが、それらは、同様の要素を区別するためのみに用いられることも留意されたい。

【0017】

以下の説明で用いられる要素に対する接尾語「モジュール」及び「ユニット」は、本明細書の作成を容易にするためのみ区別なく与えられ又は用いられ、故に、特定の意味又は機能が割り当てられていないわけではない。

【0018】

本開示の態様によれば、ターゲットドアに対応するアクセス制御デバイスの周辺にある

10

20

30

40

50

ターゲットドアに入るために、ユーザのアクセス認証を実行するユーザの端末により実行されるアクセス制御方法が提供されてよく、当該方法は、ユーザの端末において、アクセス制御デバイスを検出する段階と、検出されたアクセス制御デバイスとユーザの端末との間に通信チャネルを確立する段階と、通信チャネルを通じて、アクセス制御デバイスから識別情報を受信する段階と、受信した識別情報に基づいて、ユーザのアクセス認証のターゲットドアをチェックする段階と、ユーザの端末に予め格納されたアクセス権情報に基づいて、ユーザがターゲットドアにアクセスすることを認められているか否かを判定する段階とを備え、アクセス権情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、アクセススケジュール情報、及び、アクセス権情報の有効期間情報のうちの少なくとも1つを含む。

10

【0019】

また、アクセス制御方法は、通信チャネルを通じて、ユーザの生体認証情報を受信する段階をさらに備えてよく、ユーザの生体認証情報は、アクセス制御デバイスに対してユーザから入力され、アクセス権情報は、登録された生体認証情報をさらに含む。

【0020】

また、ユーザがターゲットドアにアクセスすることを認められているか否かを判定する段階は、ユーザの受信した生体認証情報を登録された生体認証情報と比較する段階と、ユーザの生体認証情報が登録された生体認証情報のうちの1つに合致する場合、アクセス認証が成功したと判定する段階とを含んでよい。

【0021】

また、登録された生体認証情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、アクセススケジュール情報、及び、アクセス権情報の有効期間情報のうちの少なくとも1つに対応し得る。

20

【0022】

また、アクセス権情報は、登録された生体認証情報に対応するアクセススケジュール情報をさらに含んでよく、ユーザの生体認証情報が、登録された生体認証情報のうちの1つに合致する場合に、アクセス認証が成功したと判定する段階は、アクセス権情報のユーザの受信した生体認証情報に関連するアクセススケジュール情報と現在の時刻を比較する段階と、現在の時刻がアクセススケジュールに含まれていない場合、アクセス認証が失敗したと判定する段階とを含んでよい。

30

【0023】

また、アクセス権情報は、登録された生体認証情報に対応する登録された端末識別情報をさらに含んでよく、ユーザの生体認証情報が、登録された生体認証情報のうちの1つに合致する場合、アクセス認証が成功したと判定する段階は、ユーザの端末識別情報を、ユーザの受信した生体認証情報に関連する登録された端末識別情報と比較する段階と、ユーザの端末識別情報がユーザの受信した生体認証情報に対応する登録された端末識別情報のうちの1つに合致しない場合、アクセス認証が失敗したと判定する段階とを含んでよい。

【0024】

また、アクセス権情報は、登録されたアクセス制御デバイス識別情報を含んでよく、ユーザがターゲットドアにアクセスすることを認められているか否かを判定する段階は、受信した識別情報をアクセス権情報の登録されたアクセス制御デバイス識別情報と比較する段階と、受信した識別情報が、登録されたアクセス制御デバイス識別情報のうちの1つに合致する場合、アクセス認証が成功したと判定する段階とを含んでよい。

40

【0025】

また、登録されたアクセス制御デバイス識別情報は、登録されたユーザ識別情報、登録された端末識別情報、アクセススケジュール情報、及び、アクセス権情報の有効期間情報のうちの少なくとも1つに対応してよい。

【0026】

また、アクセス権情報は、登録されたアクセス制御デバイス識別情報に対応するアクセススケジュール情報をさらに含んでよく、受信した識別情報が、登録されたアクセス制御

50

デバイス識別情報のうちの1つに合致する場合、アクセス認証が成功したと判定する段階は、アクセス権情報の受信した識別情報に関連するアクセススケジュール情報と現在の時刻を比較する段階と、現在の時刻が、アクセススケジュールに含まれていない場合、アクセス認証が失敗したと判定する段階とを含んでよい。

【0027】

また、アクセス権情報は、登録されたアクセス制御デバイス識別情報に対応する登録された端末識別情報をさらに含んでよく、受信した識別情報が、登録されたアクセス制御デバイス識別情報のうちの1つに合致する場合、アクセス認証が成功したと判定する段階は、ユーザの端末識別情報を、受信した識別情報に関連する登録された端末識別情報と比較する段階と、ユーザの端末識別情報が、受信した識別情報に対応する登録された端末識別情報のうちの1つに合致しない場合、アクセス認証が失敗したと判定する段階とを含んでよい。

10

【0028】

また、アクセス権情報は、アクセス権情報の有効期間情報を含んでよく、アクセス権情報が失効した場合、ユーザがターゲットドアにアクセスすることを認められるか否かを判定する段階が回避されてよい。

【0029】

また、アクセス制御方法は、アクセス認証が成功した場合、ドア開放信号を生成する段階と、ドア開放信号をアクセス制御デバイスに伝送する段階であって、ドア開放信号は、アクセス制御デバイスにドア開放動作を実行させる、段階とをさらに備えてよい。

20

【0030】

また、アクセス権情報は、複数のドアに関連するアクセス権情報を管理するサーバから伝送され得る。

【0031】

また、アクセス制御方法は、判定する段階が完了した場合、アクセス認証の結果情報を生成する段階をさらに備えてよい。

【0032】

また、アクセス制御方法は、複数のユーザに関連するアクセス認証の結果情報を管理するサーバに、アクセス認証の結果情報を伝送する段階をさらに備えてよい。

【0033】

また、ターゲットドアは、検出されたアクセス制御デバイスとユーザの端末との間の距離に基づいて選択され得る。

30

【0034】

また、ターゲットドアは、検出されたアクセス制御デバイスとユーザの端末との間の、特定の距離より短い距離を有する検出されたアクセス制御が導入されたドアであってよい。

【0035】

本開示の態様によれば、上記の方法を実行するために、プログラムを記録した非一時的なコンピュータ可読記録媒体が提供され得る。

【0036】

本開示の態様によれば、アクセス制御デバイスに対応するターゲットドアの周辺にあるアクセス制御デバイスが提供されてよく、当該デバイスは、アクセス制御デバイスとユーザの端末との間に通信チャネルを確立するように構成される通信ユニットと、通信チャネルを通じて、ユーザの端末に対して、ターゲットドアに入るためにユーザの端末に予め格納されたアクセス権情報に基づいて、ユーザの端末により実行されるユーザのアクセス認証用のアクセス制御デバイス識別情報を、通信ユニットを介して伝送するように構成される制御ユニットとを備え、アクセス権情報は、登録されたユーザ識別情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、アクセススケジュール情報、及び、アクセス権情報の有効期間情報のうちの少なくとも1つを含む。

40

【0037】

また、アクセス制御デバイスは、ユーザの生体認証情報を受信するための生体認証情報

50

入力ユニットをさらに備えてよく、制御ユニットは、通信チャネルを通じてユーザの端末に、ユーザの生体認証情報を、通信ユニットを介して伝送するように構成されてよく、ユーザの生体認証情報は、アクセス制御デバイスに対してユーザから入力され、アクセス権情報は、登録された生体認証情報をさらに含んでよい。

【0038】

本開示の態様によれば、アクセス制御デバイスがユーザからドア開放入力を受信して、アクセス認証要求信号をユーザ端末に伝送し、ユーザ端末が予め格納されたアクセス権情報に基づいて、ユーザに対してアクセス認証を実行するアクセスシステムのアクセス制御方法が提供されてよく、アクセス制御方法は、アクセス制御デバイスが、ユーザからドア開放入力を受信する段階と、アクセス制御デバイスが、入力に従って生成された入力信号に従うアクセス認証要求信号を生成する段階と、ユーザ端末が、アクセス制御デバイスからアクセス認証要求信号を受信する段階と、ユーザ端末が、現在の時刻とアクセス権情報とに基づいて、ユーザに対してアクセス認証を実行する段階であって、アクセス権情報は、アクセススケジュール情報を含む、段階とを含む。

10

【0039】

また、アクセス制御方法は、ユーザ端末がサーバと通信する段階と、アクセス認証要求信号を受信する段階の後に、サーバから指定されたメッセージを受信する段階とをさらに含んでよい。

【0040】

また、指定されたメッセージは、アドバイズメッセージ又は通知メッセージを含んでよい。

20

【0041】

また、指定されたメッセージは、複数のメッセージのうち、現在の時刻に従って指定されたメッセージであってよい。

【0042】

また、アクセス認証を実行する段階は、現在の時刻がアクセススケジュール情報に含まれているか否かをチェックする段階と、現在の時刻がアクセススケジュール情報に含まれている場合、アクセス認証が成功したと判定する段階とを含んでよい。

【0043】

また、アクセス制御方法は、ユーザ端末がアクセス制御デバイスから識別情報を取得する段階をさらに含んでよい。アクセス権情報は、登録されたアクセス制御デバイス識別情報をさらに含んでよく、登録されたアクセス制御デバイス識別情報はアクセススケジュール情報に対応し得る。アクセス認証を実行する段階は、アクセススケジュール情報に対応する登録されたアクセス制御デバイス識別情報に、取得された識別情報が含まれているか否かをチェックする段階と、登録されたアクセス制御デバイス識別情報に、取得された識別情報が含まれていない場合、アクセス認証が失敗したと判定する段階とを含んでよい。

30

【0044】

また、アクセス制御デバイス識別情報を取得する段階は、アクセス制御デバイス識別情報を含むアクセス認証要求信号を受信する段階を含んでよい。

【0045】

また、アクセス制御方法は、アクセス認証を実行する段階の後に、アクセス認証が成功した場合、ユーザ端末がドア開放信号を生成する段階をさらに含んでよく、ドア開放信号は、アクセス制御デバイスにドア開放動作を実行させ得る。

40

【0046】

また、アクセス制御方法は、ユーザ端末が、アクセス制御デバイスにドア開放信号を伝送する段階をさらに含んでよい。

【0047】

また、アクセス制御方法は、サーバからアクセス権情報を受信する段階をさらに含んでよい。

【0048】

50

また、アクセス制御方法は、サーバにより伝送されたアクセス権情報を受信する段階の前に、サーバにアクセス権情報を要求する段階をさらに含んでよい。

【0049】

また、ユーザ端末は、BLE、Bluetooth（登録商標）、NFC及びWiFi（登録商標）のうちの少なくとも1つを通じて、アクセス制御デバイスと通信してよい。

【0050】

本開示の態様によれば、上述の方法を実行するために、そこに記録されたプログラムを有する記録媒体が提供され得る。

【0051】

本開示の態様によれば、アクセス権情報に基づいてユーザアクセス認証を実行するユーザ端末に、ユーザアクセス認証用の識別情報を伝送するアクセス制御デバイスが提供されてよく、アクセス制御デバイスは、ユーザ端末と通信するように構成される通信ユニットと、通信ユニットを通じてユーザ端末から、通信を開始するための信号が受信された場合、ユーザ端末に、アクセス制御デバイス識別情報を伝送するよう通信ユニットを制御するように構成される制御ユニットとを含む。

10

【0052】

また、アクセス制御デバイスは、ユーザの生体認証情報を受信するように構成される生体認証情報入力ユニットをさらに含んでよく、制御ユニットは、生体認証情報入力ユニットにより受信されたユーザの生体認証情報をユーザ端末に伝送するよう通信ユニットを制御してよい。

20

【0053】

また、制御ユニットは、生体認証情報入力ユニットにより受信された生体認証情報を暗号化してよい。

【0054】

また、アクセス制御デバイスは、ドア開放動作に必要な電力を提供するように構成される電源ユニットをさらに含んでよく、ユーザ端末からドア開放信号が受信された場合、制御ユニットは、ドア開放動作を実行するよう電源ユニットを制御してよい。

【0055】

本開示の態様によれば、ユーザからドア開放入力を受信し、ユーザ端末にアクセス認証要求信号を伝送するアクセス制御デバイスが提供されてよく、アクセス制御デバイスは、ユーザからドア開放入力を受信するように構成される入力ユニットと、ユーザ端末と通信するように構成される通信ユニットと、アクセス認証要求信号を生成し、入力ユニットを通じて、ドア開放入力が受信された場合、ユーザ端末にアクセス認証要求信号を伝送するよう通信ユニットを制御するように構成される制御ユニットとを含む。

30

【0056】

また、アクセス制御デバイスは、ドア開放動作に必要な電力を提供するように構成される電源ユニットをさらに含んでよく、制御ユニットは、ユーザ端末からドア開放信号が受信された場合、ドア開放動作を実行するよう電源ユニットを制御してよい。

【0057】

また、制御ユニットは、通信ユニットを通じてユーザ端末に、アクセス制御デバイス識別情報を伝送してよい。

40

【0058】

また、アクセス認証要求信号は、アクセス制御デバイス識別情報を含む信号であってよい。

【0059】

本開示の態様によれば、ユーザから受信した管理者情報及び設定変更情報に基づいて、設定変更信号を生成し、アクセス制御デバイスが設定変更を実行できるように、生成された設定変更信号をアクセス制御デバイスに伝送するユーザ端末の設定変更方法が提供されてよく、設定変更方法は、アクセス制御デバイスを検出し、アクセス制御デバイスとの通信を確立する段階と、アクセス制御デバイスにより実行される設定変更のために、設定変

50

更情報を受信する段階と、アクセス制御デバイスに伝送される管理者情報を受信する段階であって、その結果、当該管理者情報がアクセス制御デバイスの予め格納された管理者情報と比較される、段階と、受信した設定変更情報に基づいて、設定変更信号を生成する段階と、無線通信を通じてアクセス制御デバイスに、設定変更情報及び管理者情報を伝送する段階とを含む。

【0060】

また、設定変更は、アクセス制御デバイスの通信インターフェース設定変更と、アクセス制御デバイスのPIN設定変更と、アクセス制御デバイスのディスプレイユニット及びアクセス制御デバイスの音声出力ユニットのうちの少なくとも一方に対する設定変更と、アクセス制御デバイスにより認識されるカードに対するフォーマット変更と、アクセス制御デバイスのファームウェア更新と、アクセス制御デバイスにおける生体認証情報のストレージとの中の少なくとも1つを含んでよい。

10

【0061】

また、設定変更は、アクセス制御デバイスにおける生体認証情報のストレージであってよく、設定変更方法は、アクセス制御デバイスに格納される生体認証情報を取得する段階をさらに含んでよい。

【0062】

また、生体認証情報は、指紋情報、虹彩情報、静脈情報、顔情報及び音声情報のうちの少なくとも1つを含んでよい。

【0063】

また、生体認証情報を取得する段階は、ユーザから生体認証情報を受信する段階を含んでよい。

20

【0064】

また、生体認証情報を取得する段階は、サーバから生体認証情報を受信する段階を含んでよい。

【0065】

また、設定変更方法は、アクセス制御デバイスに生体認証情報を伝送する段階をさらに含んでよい。

【0066】

また、アクセス制御デバイスに生体認証情報を伝送する段階は、生体認証情報を含む設定変更信号を伝送する段階を含んでよい。

30

【0067】

また、設定変更方法は、生体認証情報を暗号化する段階をさらに含んでよい。

【0068】

また、管理者情報は、管理者のパスワードを含んでよい。

【0069】

また、アクセス制御デバイスに管理者情報を伝送する段階は、管理者情報を含む設定変更信号を伝送する段階を含んでよい。

【0070】

また、無線通信は、BLE、Bluetooth（登録商標）、NFC及びWiFi（登録商標）のうちの1つを含んでよい。

40

【0071】

また、設定変更方法は、アクセス制御デバイスから設定変更に対する結果情報を受信する段階をさらに含んでよい。

【0072】

本開示の態様によれば、ユーザ端末から設定変更信号を受信し、設定変更を実行するアクセス制御デバイスの設定変更方法が提供されてよく、設定変更方法は、ユーザ端末との通信を確立する段階と、ユーザ端末により生成された設定変更信号と、ユーザ端末からユーザ端末により受信された管理者情報とを受信する段階と、受信した管理者情報が予め格納された管理者情報に合致するか否かを判定する段階と、受信した管理者情報が予め格納

50

された管理者情報に合致する場合、設定変更信号に従って設定変更を実行する段階とを含む。

【0073】

また、設定変更は、アクセス制御デバイスの通信インタフェース設定変更と、アクセス制御デバイスのPIN設定変更と、アクセス制御デバイスのディスプレイユニット及びアクセス制御デバイスの音声出力ユニットのうちの少なくとも一方に対する設定変更と、アクセス制御デバイスにより認識されるカードに対するフォーマット変更と、アクセス制御デバイスのファームウェア更新と、アクセス制御デバイスにおける生体認証情報のストレージのうちの少なくとも1つを含んでよい。

【0074】

また、設定変更は、アクセス制御デバイスにおける生体認証情報のストレージであってよく、設定変更方法は、ユーザ端末から生体認証情報を受信する段階をさらに含んでよい。

【0075】

また、ユーザ端末から生体認証情報を受信する段階は、生体認証情報を含む設定変更信号を受信する段階を含んでよい。

【0076】

また、設定変更方法は、生体認証情報が暗号化されている場合、生体認証情報を復号する段階をさらに含んでよい。

【0077】

また、管理者情報は、管理者のパスワードを含んでよい。

【0078】

また、受信した管理者情報を受信する段階は、受信した管理者情報を含む設定変更信号を受信する段階を含んでよい。

【0079】

また、無線通信は、BLE、Bluetooth（登録商標）、NFC及びWiFi（登録商標）のうちの1つを含んでよい。

【0080】

また、設定変更方法は、ユーザ端末に設定変更の結果情報を伝送する段階をさらに含んでよい。

【0081】

本開示の態様によれば、上述の方法を実行するために、そこに記録されたプログラムを有する記録媒体が提供され得る。

【0082】

本開示の態様によれば、ユーザ端末により生成された管理者情報及び設定変更信号をユーザ端末から受信し、かつ、受信した管理者情報が予め格納された管理者情報に合致する場合、設定変更を実行するアクセス制御デバイスが提供されてよく、アクセス制御デバイスは、ユーザ端末と通信するように構成される通信ユニットと、管理者情報を格納するように構成されるストレージユニットと、通信ユニットを通じてユーザ端末からユーザ端末により受信された設定変更信号及び管理者情報を受信し、受信した管理者情報が予め格納された管理者情報と合致するか否かをチェックし、受信した管理者情報が予め格納された管理者情報と合致した場合、設定変更信号に従って設定変更が実行されるような制御を実行するように構成される制御ユニットとを含む。

【0083】

また、設定変更は、アクセス制御デバイスの通信インタフェース設定変更と、アクセス制御デバイスのPIN設定変更と、アクセス制御デバイスのディスプレイユニット及びアクセス制御デバイスの音声出力ユニットのうちの少なくとも一方に対する設定変更と、アクセス制御デバイスにより認識されるカードに対するフォーマット変更と、アクセス制御デバイスのファームウェア更新と、アクセス制御デバイスにおける生体認証情報のストレージとのうちの少なくとも1つを含んでよい。

【0084】

また、設定変更は、アクセス制御デバイスにおける生体認証情報のストレージであってよく、制御ユニットは、通信ユニットを通じてユーザ端末から生体認証情報を受信してよく、生体認証情報がストレージユニットに格納されるような制御を実行してよい。

【0085】

また、ユーザ端末から生体認証情報を受信する段階は、生体認証情報を含む設定変更信号を受信する段階を含んでよい。

【0086】

また、通信ユニットを通じて受信した生体認証情報が暗号化されている場合、制御ユニットは、生体認証情報を復号してよい。

【0087】

また、管理者情報は、管理者のパスワードを含んでよい。

【0088】

また、受信した管理者情報を受信する段階は、受信した管理者情報を含む設定変更信号を受信する段階を含んでよい。

【0089】

また、通信ユニットは、BLE、Bluetooth（登録商標）、NFC及びWiFi（登録商標）のうちの1つである無線通信スキームを用いてよい。

【0090】

また、制御ユニットは、通信ユニットを通じてユーザ端末に設定変更に対する結果情報を伝送してよい。

【0091】

本開示の実施形態に係るアクセス制御システム10000が後述される。アクセス制御システムは、ユーザの端末2000を通じてアクセス認証に成功した人のみが通過でき、アクセス制御デバイスが導入される環境に、アクセス制御デバイスが導入されるゾーンを通過するためのアクセス権を有するようにアクセスを管理するシステムを指し得る。アクセス制御システムは、例えば、フィットネスセンタ、オフィス又は機関などの屋内環境において用いられてよい、又は、軍用基地などの制限された領域の外部にあるビルに存在する屋外環境において用いられてもよい。

【0092】

ドアは、あるゾーンを通過することをブロック又は許容し得る。ドアは、ドアフレーム及びドアリーフを含んでよい。ドアフレームは、通行がブロックされる又は許可されているゾーンを定義する固定要素であってよい。ドアリーフは、外力に起因して位置が変わる要素である。位置に応じて、通行がブロックされる又は許可される場所が変更され得る。ドアリーフの位置の変更は、回転運動並びにドアリーフ全体の動きを含む包括的な意味を有し得る。ドアは上述の例に限定されないことが理解される。

【0093】

1. システム構成

図1は、実施形態に係るアクセス制御システム10000のブロック図である。

【0094】

図1を参照すると、アクセス制御システム10000は、サーバ1000、端末2000及びアクセス制御デバイス3000を含んでよい。

【0095】

サーバ1000は、ユーザの端末2000と通信して、様々な情報を交換してよい。

【0096】

実施形態によれば、サーバ1000は、ユーザアクセス認証に対して必要な情報をユーザの端末2000に提供してよい。また、サーバ1000は、ユーザの端末2000からアクセス認証結果情報を取得してよい。

【0097】

ユーザの端末2000は、アクセス制御デバイス3000と通信して、様々な情報を交換してよい。

10

20

30

40

50

【0098】

例えば、ユーザの端末2000は、アクセス制御デバイス3000からアクセス認証に必要な情報を受信してよい。また、ユーザの端末2000は、ドア開放要求に必要なデータ及び／又は設定変更要求をアクセス制御デバイス3000に伝送してよい。

【0099】

また、ユーザの端末2000は、後述するいくつかの実施形態を実行するためのアプリケーションを提供し得る。

【0100】

また、ユーザの端末2000は、例えば、スマートフォン、タブレット、ノートブック、パーソナルデジタルアシスタント（PDA）、ウェアラブルデバイスなどで実装されてよい。代替的に、ユーザの端末2000は、スマートカード、集積回路（IC）カード、磁気カード、又は、無線周波数（RF）チップなどで実装されてよく、データを記録することが可能である。

【0101】

アクセス制御デバイス3000は、ドアの開閉を制御し得る。

【0102】

例えば、アクセス制御デバイス3000は、ドアのロック又はロック解除を制御するために、ドアに設置されてよい。アクセス制御デバイス3000は、必ずしも、ドアに設置される必要はなく、選択に応じて、様々な形態において提供されてよい。例えば、アクセス制御デバイス3000は、ドアに又はドアから障害物を提供する又は引き出すために、ドアに隣接する壁に設置されてよい。また、ドアが自動ドアである場合、アクセス制御デバイス3000は、ドアリーフの位置を変えて、ドアを開閉してよい。

【0103】

しかしながら、図1に示されるブロック図は、説明の便宜上の単なる例であり、本開示は、それに限定されることない。いくつかの実施形態によれば、任意の要素が図1のブロック図に追加されてよく、図1に示される要素が除外され又は細分化されてよい。

【0104】

図2は、実施形態に係るサーバ1000のブロック図である。

【0105】

図2を参照すると、サーバ1000は、サーバ通信ユニット1100と、サーバ入力ユニット1200と、サーバストレージユニット1300と、サーバディスプレイユニット1400と、サーバ制御ユニット1500とを含んでよい。

【0106】

サーバ通信ユニット1100は、ユーザの端末2000と通信してよい。例えば、サーバ通信ユニット1100は、ユーザの端末2000からアクセス権情報の要求を受信してよい。また、サーバ通信ユニット1100は、アクセス権情報をユーザの端末2000に伝送してよい。また、サーバ通信ユニット1100は、ユーザの端末2000からユーザアクセス認証結果に関する情報を受信してよい。また、ユーザの端末2000がアクセス認証要求信号を受信した場合、サーバ通信ユニット1100は、ユーザの端末2000と通信して、予め設定されたメッセージをユーザの端末2000に伝送してよい。

【0107】

別の例として、サーバ通信ユニット1100は、アクセス制御デバイス3000に格納される生体認証情報をユーザの端末2000に伝送してよい。

【0108】

また、サーバ通信ユニット1100は、Bluetooth（登録商標） Low energy（BLE）、Bluetooth（登録商標）、無線ローカルエリアネットワーク（WLAN）、ワイヤレスフィデリティ（WiFi（登録商標））、WiFi（登録商標）ダイレクト、近距離無線通信（NFC）、赤外線データ協会（IrDA）、超広帯域（UWB）、Zigbee（登録商標）、3G、4G及び5G、及び、様々な通信規格を通じてデータを伝送できる他の有線又は無線ユニットなどのモバイル通信ユニットを含ん

でよい。

【0109】

サーバ入力ユニット1200は、ユーザ入力に対応する電気信号を取得してよい。サーバ入力ユニット1200は、キーパッド、キーボード、スイッチ、ボタン及びタッチスクリーンを含んでよい。

【0110】

サーバストレージユニット1300は、様々な種類のデータを格納してよい。

【0111】

例えば、サーバストレージユニット1300は、アクセス権情報を格納してよい。また、サーバストレージユニット1300は、ユーザの端末2000から取得したユーザアクセス認証結果情報を格納してよい。また、ユーザの端末2000がアクセス認証要求信号を受信した場合、サーバストレージユニット1300は、伝送対象の指定されたメッセージをユーザの端末2000に格納してよい。また、サーバストレージユニット1300は、サーバ1000の動作に必要なプログラムを格納してよい。また、サーバストレージユニット1300は、ユーザの端末2000を通じて、アクセス制御デバイス3000に格納対象の生体認証情報を格納してよい。

【0112】

サーバストレージユニット1300は、フラッシュメモリタイプのメモリ、ハードディスクタイプのメモリ、マルチメディアカードマイクロタイプのメモリ、カードタイプのメモリ（例えば、SD又はXDメモリ）、ランダムアクセスメモリ（RAM）、スタティックランダムアクセスメモリ（SRAM）、リードオンリメモリ（ROM）、電氣的消去可能プログラマブルリードオンリメモリ（EEPROM）、プログラマブルリードオンリメモリ（PROM）、磁気メモリ、磁気ディスク、及び、光学ディスクの中から選択される少なくとも1つのタイプの記憶媒体を含んでよい。また、メモリは、一時的に、永久的に、又は、半永久的に情報を格納してよい、又は、ビルトインタイプ又はリムーバブルタイプのメモリとして提供されてよい。

【0113】

サーバディスプレイユニット1400は、視覚情報を出力してよい。

【0114】

例えば、サーバディスプレイユニット1400は、液晶ディスプレイ（LCD）、有機発光ダイオード（OLED）ディスプレイ、アクティブマトリクス式有機発光ダイオード（AMOLED）デバイスなどであってよい。

【0115】

サーバ制御ユニット1500は、サーバ1000の各要素を制御してよい、又は、様々な種類の情報を処理及び計算してよい。例えば、サーバ制御ユニット1500は、サーバ通信ユニット1100を通じて、アクセス権情報をユーザの端末2000に伝送してよい。また、ユーザの端末2000がアクセス認証要求信号を受信した場合、サーバ制御ユニット1500は、ユーザの端末2000と通信して、サーバ通信ユニット1100を通じて、予め設定されたメッセージをユーザの端末2000に伝送してよい。また、サーバ制御ユニット1500は、サーバ通信ユニット1100を通じて、アクセス制御デバイス3000に格納される生体認証情報をユーザの端末2000に伝送してよい。

【0116】

また、以下の方法で説明される段階のうち、サーバ制御ユニット1500は、サーバ1000により実行されるいくつかの段階を実行するための動作を制御してよい、又は、当該段階を実行するために必要とされる計算を実行してよい。

【0117】

サーバ制御ユニット1500は、ソフトウェア、ハードウェア、又は、それらの組み合わせで実装されてよい。例えば、ハードウェアにおいて、サーバ制御ユニット1500は、フィールドプログラマブルゲートアレイ（FPGA）、特定用途向け集積回路（ASIC）、半導体チップ、及び、様々な他のタイプの電子回路で実装されてよい。別の例とし

10

20

30

40

50

て、ソフトウェアにおいて、サーバ制御ユニット１５００は、上述したハードウェアに従って実行される論理プログラム又は様々な種類のコンピュータ言語で実装されてよい。

【０１１８】

サーバ１０００は、必ずしも上述の要素のすべてを含んでいる必要はなく、選択に応じて要素のいくつかが除外されてよい。例えば、サーバ１０００が、直接的な視覚情報を提供していない場合、サーバディスプレイユニット１４００がサーバ１０００から除外され得る。また、選択に応じて、追加の機能又は操作を実行するための要素は、サーバ１０００に選択的に提供されてよい。

【０１１９】

図３は、実施形態に係る端末２０００のブロック図である。

10

【０１２０】

図３を参照すると、端末２０００は、端末通信ユニット２１００と、端末ディスプレイユニット２２００と、端末入力ユニット２３００と、端末位置情報計算ユニット２４００と、端末ストレージユニット２５００と、端末制御ユニット２６００と、端末生体認証情報入力ユニット２７００とを含んでよい。

【０１２１】

端末通信ユニット２１００は、サーバ１０００と通信してよい。

【０１２２】

例えば、端末通信ユニット２１００は、サーバ１０００からアクセス権情報を要求してよい。また、端末通信ユニット２１００は、サーバ１０００からアクセス権情報を受信してよい。また、端末通信ユニット２１００は、ユーザアクセス認証結果に関する情報をサーバ１０００に伝送してよい。また、端末通信ユニット２１００がアクセス認証要求信号を受信した場合、端末通信ユニット２１００は、ユーザの端末２０００と通信して、サーバ１０００から予め設定されたメッセージを受信してよい。

20

【０１２３】

別の例として、端末通信ユニット２１００は、サーバ１０００からアクセス制御デバイス３０００に格納される生体認証情報を受信してよい。

【０１２４】

また、端末通信ユニット２１００は、アクセス制御デバイス３０００と通信してよい。

【０１２５】

例えば、端末通信ユニット２１００は、アクセス制御デバイス３０００から生体認証情報を受信してよい。また、端末通信ユニット２１００は、アクセス制御デバイス３０００からアクセス制御デバイス３０００の識別情報を受信してよい。また、端末通信ユニット２１００は、アクセス制御デバイス３０００からアクセス認証要求信号を受信してよい。また、端末通信ユニット２１００は、アクセス制御デバイス３０００にドア開放信号を伝送してよい。

30

【０１２６】

別の例として、端末通信ユニット２１００は、アクセス制御デバイス３０００に設定変更信号を伝送してよい。また、端末通信ユニット２１００は、アクセス制御デバイス３０００から設定変更結果情報を受信してよい。

40

【０１２７】

端末通信ユニット２１００は、BLE、Bluetooth（登録商標）、WLAN、Wi-Fi（登録商標）、Wi-Fi（登録商標）ダイレクト、NFC、IRDA、UWB、Zigbee（登録商標）、3G、4G及び5G、及び、様々な通信規格を通じてデータを伝送できる他の有線又は無線ユニットなどのモバイル通信ユニットを含んでよい。

【０１２８】

端末ディスプレイユニット２２００は、様々な視覚情報を出力してよい。

【０１２９】

例えば、端末ディスプレイユニット２２００は、通信が確立された場合、アクセス制御デバイス３０００が情報を出力し得ることを検出してよい。また、端末ディスプレイユニ

50

ット2200は、ユーザアクセス認証結果を視覚的に出力してよい。また、端末ディスプレイユニット2200は、サーバ1000から受信したメッセージを視覚的に出力してよい。また、端末ディスプレイユニット2200は、アクセス制御デバイス3000の設定を変更すべく、設定変更情報を入力するためのスクリーンを視覚的に出力してよい。

【0130】

端末ディスプレイユニット2200は、LCDディスプレイ、OLEDディスプレイ又はAMOLEDディスプレイなどであってよい。端末ディスプレイユニット2200がタッチスクリーンとして提供される場合、端末ディスプレイユニット2200は、端末入力ユニット2300として機能し得る。この場合、選択に応じて、別個の端末入力ユニット2300が提供されてなくてよく、例えば、電圧調整機能、電源ボタン機能、ホームボタン機能などの制限された機能を実行するように構成される端末入力ユニット2300が提供されてよい。

10

【0131】

端末入力ユニット2300は、ユーザ入力に対応する信号を取得してよい。

【0132】

例えば、端末入力ユニット2300は、サーバ1000から、アクセス権情報を要求するための入力を受信してよい。また、端末入力ユニット2300は、アクセス制御デバイス3000から、識別情報又は生体認証情報を要求するための入力を受信してよい。

【0133】

別の例として、端末入力ユニット2300は、設定変更情報を受信して、アクセス制御デバイス3000の設定を変更してよい。また、端末入力ユニット2300は、管理者情報が、アクセス制御デバイス3000に予め格納された管理者情報と合致するか否かがチェックされる管理者情報を受信してよい。

20

【0134】

端末入力ユニット2300は、例えば、キーボード、キーパッド、ボタン、ジョグダイヤル又はホイールで実装されてよい。また、ユーザ入力は、例えば、ボタン押し、タッチ又はドラッグであってよい。端末ディスプレイユニット2200が、タッチスクリーンで実装されている場合、端末ディスプレイユニット2200は、端末入力ユニット2300として機能し得る。

【0135】

端末位置情報計算ユニット2400は、端末2000の位置情報を取得して、その位置を判定してよい。例えば、端末位置情報計算ユニット2400は、位置判定を実行するための座標情報を取得するように構成される、GPSユニットなどのユニットであってよい。

30

【0136】

端末ストレージユニット2500は、様々な種類のデータを格納してよい。

【0137】

例えば、端末ストレージユニット2500は、端末2000の動作に必要なデータを格納してよい。また、端末ストレージユニット2500は、アクセス権情報を格納してよい。

【0138】

端末ストレージユニット2500は、フラッシュメモリタイプのメモリ、ハードディスクタイプのメモリ、マルチメディアカードマイクロタイプのメモリ、カードタイプのメモリ（例えば、SD又はXDメモリ）、RAM、SRAM、ROM、EEPROM、PROM、磁気メモリ、磁気ディスク、及び、光学ディスクの中から選択される少なくとも1つのタイプの記憶媒体を含んでよい。また、メモリは、一時的に、永久的に、又は、半永久的に情報を格納してよく、ビルトインタイプ又はリムーバブルタイプのメモリとして提供されてよい。

40

【0139】

端末制御ユニット2600は、端末2000の各要素を制御してよい、又は、様々な種類の情報を処理及び計算してよい。また、端末制御ユニット2600は、ユーザの端末2000に含まれるいくつかの要素から信号を取得してよい。また、以下の方法で説明され

50

る段階のうち、端末制御ユニット２６００は、ユーザの端末２０００により実行されるいくつかの段階を実行するための動作を制御してよい、又は、段階を実行するのに必要な計算を実行してよい。

【０１４０】

端末制御ユニット２６００は、ソフトウェア、ハードウェア又はそれらの組み合わせで実装されてよい。例えば、ハードウェアにおいて、端末制御ユニット２６００は、ＦＰＧＡ、ＡＳＩＣ、半導体チップ及び様々な他のタイプの電子回路で実装されてよい。別の例として、ソフトウェアにおいて、端末制御ユニット２６００は、上述したハードウェアに従って実行される論理プログラム又は様々な種類のコンピュータ言語で実装されてよい。

【０１４１】

端末生体認証情報入力ユニット２７００は、ユーザの生体認証情報を受信し得る。生体認証情報は、ユーザの音声情報、指紋情報、虹彩情報、顔情報及び静脈情報のうちの少なくとも１つを指し得る。端末生体認証情報入力ユニット２７００は、ユーザの音声情報が入力されるマイク、ユーザの指紋情報が入力されるスクリーンキャナ、及び、ユーザの虹彩情報、顔情報及び静脈情報が入力されるカメラのうちの少なくとも１つを用いて実装され得る。

【０１４２】

図４は、実施形態に係るアクセス制御デバイス３０００のブロック図である。

【０１４３】

図４を参照すると、アクセス制御デバイス３０００は、通信ユニット３１００と、ディスプレイユニット３２００と、音声出力ユニット３３００と、センサユニット３４００と、ストレージユニット３５００と、電源ユニット３６００と、制御ユニット３７００と、生体認証情報入力ユニット３８００と、入力ユニット３９００とを含んでよい。

【０１４４】

通信ユニット３１００は、ユーザの端末２０００と通信してよい。

【０１４５】

例えば、通信ユニット３１００は、アクセス制御デバイス３０００の識別情報をユーザの端末２０００に伝送してよい。また、通信ユニット３１００は、アクセス制御デバイス３０００により受信した生体認証情報をユーザの端末２０００に伝送してよい。また、通信ユニット３１００は、ドアを開けるためのユーザの入力に対応する入力信号に従って生成されたアクセス認証要求信号をユーザの端末２０００に伝送してよい。

【０１４６】

別の例として、通信ユニット３１００は、ユーザの端末２０００から設定変更信号を受信してよい。また、通信ユニット３１００は、設定変更を実行することにより取得された結果情報をユーザの端末２０００に伝送してよい。

【０１４７】

通信ユニット３１００は、無線通信規格に従って通信を主に行ってよいが、ＢＬＥ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＷＬＡＮ、ＷｉＦｉ（登録商標）、ＷｉＦｉ（登録商標）ダイレクト、ＮＦＣ、ＩＲＤＡ、ＵＷＢ、Ｚｉｇｂｅｅ（登録商標）、３Ｇ、４Ｇ及び５Ｇ、及び、様々な通信規格を通じてデータを伝送できる他の有線又は無線ユニットなどのモバイル通信ユニットを含んでよい。

【０１４８】

ディスプレイユニット３２００は、ユーザに視覚的に提供される情報を出力してよい。

【０１４９】

例えば、ドア開放信号が受信された場合、ディスプレイユニット３２００は、受信を示す情報を視覚情報として出力してよい。また、設定変更信号が受信された場合、ディスプレイユニット３２００は、受信を示す情報を視覚情報として出力してよい。

【０１５０】

ディスプレイユニット３２００は、ＬＣＤディスプレイ、ＯＬＥＤディスプレイ、又は、ＡＭＯＬＥＤディスプレイなどであってよい。ディスプレイユニット３２００がタッチ

10

20

30

40

50

パネルを含む場合、ディスプレイユニット 3 2 0 0 は、タッチ入力ベースの入力デバイスとして動作してよい。

【0 1 5 1】

音声出力ユニット 3 3 0 0 は、ユーザに聴覚的に提供される情報を出力してよい。

【0 1 5 2】

例えば、ドア開放信号が受信される場合、ディスプレイユニット 3 2 0 0 は、受信を示す情報を聴覚情報として出力してよい。また、設定変更信号が受信された場合、ディスプレイユニット 3 2 0 0 は、受信を示す情報を聴覚情報として出力してよい。

【0 1 5 3】

音声出力ユニット 3 3 0 0 は、音を出力するスピーカ又はブザーなどであってよい。

10

【0 1 5 4】

センサユニット 3 4 0 0 は、アクセス制御デバイス 3 0 0 0 が必要とする外部環境信号を取得してよい。例えば、センサユニット 3 4 0 0 は、ユーザ又はオブジェクトなどからの距離に関する信号を取得してよい。別の例として、センサユニット 3 4 0 0 は、ドアリーフの位置を判定するのに必要な信号を取得してよい。

【0 1 5 5】

様々な種類の情報がストレージユニット 3 5 0 0 に格納され得る。

【0 1 5 6】

例えば、ストレージユニット 3 5 0 0 は、制御ユニット 3 7 0 0 の制御動作を実行するためのプログラムを格納してよく、外部から受信されるデータ、制御ユニット 3 7 0 0 により生成されるデータなどを格納してよい。また、ストレージユニット 3 5 0 0 は、管理者情報が、ユーザの端末 2 0 0 0 により受信された管理者情報と合致するか否かチェックされる管理者情報を格納してよい。また、ストレージユニット 3 5 0 0 は、ユーザの端末 2 0 0 0 から受信した生体認証情報を格納してよい。

20

【0 1 5 7】

ストレージユニット 3 5 0 0 は、フラッシュメモリタイプのメモリ、ハードディスクタイプのメモリ、マルチメディアカードマイクロタイプのメモリ、カードタイプのメモリ（例えば、SD 又は XD メモリ）、RAM、SRAM、ROM、EEPROM、PROM、磁気メモリ、磁気ディスク及び光学ディスクの中から選択される少なくとも 1 つのタイプの記憶媒体を含んでよい。また、メモリは、一時的に、永久的に、又は、半永久的に情報を格納してよく、ビルトインタイプ又はリムーバブルタイプのメモリとして提供されてよい。

30

【0 1 5 8】

電源ユニット 3 6 0 0 は、ドアリーフをロック又はロック解除するのに必要な電力を提供してよい。また、ドアが自動ドアとして実装される場合、電源ユニット 3 6 0 0 は、ドアリーフを開閉するのに必要な電力を提供してよい。

【0 1 5 9】

電源ユニット 3 6 0 0 は、モータ、ソレノイド又はアクチュエータとして提供されてよい。

【0 1 6 0】

40

電源ユニット 3 6 0 0 が、ドアリーフをロック又はロック解除するのに必要な電力を提供する場合、電源ユニット 3 6 0 0 は、ロックユニットが維持され、及び／又は、これがロック状態からロック解除状態に変更されるように電力を提供してよい。ロックユニットは、例えば、デッドボルト、ラッチボルト又はそれらの組み合わせとして提供されてよい。また、ロックユニットは、例として説明されたデッドボルト及びラッチボルトに限定されず、典型的なロックユニットが利用されてよい。

【0 1 6 1】

制御ユニット 3 7 0 0 は、アクセス制御デバイス 3 0 0 0 の各要素を制御してよい、又は、様々な種類の情報を処理及び計算してよい。また、制御ユニット 3 7 0 0 は、アクセス制御デバイス 3 0 0 0 に含まれるいくつかの要素から信号を取得してよい。また、以下

50

の方法で説明される段階のうち、制御ユニット 3700 は、アクセス制御デバイス 3000 により実行されるいくつかの段階を実行するための動作を制御してよい、又は、段階を実行するのに必要な計算を実行してよい。

【0162】

制御ユニット 3700 は、ソフトウェア、ハードウェア又はそれらの組み合わせで実装され得る。例えば、ハードウェアにおいて、制御ユニット 3700 は、FPGA、ASIC、半導体チップ及び様々な他のタイプの電子回路で実装されてよい。別の例として、ソフトウェアにおいて、制御ユニット 3700 は、上述したハードウェアに従って実行される論理プログラム又は様々な種類のコンピュータ言語で実装されてよい。

【0163】

生体認証情報入力ユニット 3800 は、ユーザの生体認証情報を受信してよい。

【0164】

例えば、生体認証情報入力ユニット 3800 は、ユーザの音声情報、指紋情報、虹彩情報、顔情報及び静脈情報のうちの少なくとも 1 つを受信してよい。

【0165】

生体認証情報入力ユニット 3800 は、ユーザの音声情報が入力されるマイク、ユーザの指紋情報が入力されるスクリーンキャナ、ユーザの虹彩情報、顔情報及び静脈情報が入力されるカメラのうちの少なくとも 1 つを用いて実装され得る。

【0166】

入力ユニット 3900 は、様々な入力を受信し得る。

【0167】

例えば、入力ユニット 3900 は、ユーザからドア開放入力を受信してよく、電源ユニット 3600 を駆動させて、ドアを開いてよい。また、入力ユニット 3900 は、ユーザからドア開放入力を受信してよく、次に、アクセス制御デバイス 3000 がアクセス認証要求信号をユーザの端末 2000 に伝送することを可能にし得る。

【0168】

例えば、入力ユニット 3900 は、キーボード、キーパッド、ボタン、スイッチ、ジョグダイヤル、又は、ホイールとして実装されてよい。また、ユーザ入力は、例えば、スイッチ押し、ボタン押し、タッチ、又は、ドラッグであってよい。ディスプレイユニット 3200 が、タッチスクリーンで実装される場合、ディスプレイユニット 3200 は、入力ユニット 3900 として機能し得る。

【0169】

本開示の実施形態に係るアクセス制御デバイス 3000 は、必ずしも上記の要素のすべてを含んでいる必要はなく、要素のいくつかが、選択に応じて除外されてよい。

【0170】

本開示の実施形態に係るアクセス制御システム 10000 は、少なくとも 1 つのアクセス制御デバイス 3000 を含む形態で実装されてよい。例として、アクセス制御システム 10000 は、通信ユニット 3100 及び制御ユニット 3700 を含む 1 つのアクセス制御デバイス 3000 を含んでよい。具体例として、アクセス制御デバイス 3000 は、読み取り機として機能する通信ユニット 3100 を通じて端末 2000 から取得した情報を受信してよく、コントローラとして機能する制御ユニット 3700 を通じて取得した情報を分析してよく、ドアロックデバイスをロック解除するための信号を伝送する機能を実行してよい。また、アクセス制御デバイス 3000 は、ドアロックデバイスをロック解除するための信号を伝送する機能に加えて、ドアアクセス制御、時間及び出席管理及びシステムモード変更などの動作を制御する機能を実行してよい。

【0171】

別の例として、アクセス制御システム 10000 は、少なくとも通信ユニット 3100 を含む第 1 のアクセス制御デバイス 3000 と、少なくとも制御ユニット 3700 を含む第 2 のアクセス制御デバイス 3000 とを含んでよい。具体例として、第 1 のアクセス制御デバイス 3000 は、読み取り機として機能する通信ユニット 3100 を通じて端末 2

10

20

30

40

50

000から取得される情報を受信してよく、有線又は無線通信方式で第2のアクセス制御デバイス3000に接続される通信ユニット3100を通じて第2のアクセス制御デバイス3000に、取得した情報を伝送してよい。この場合、第2のアクセス制御デバイス3000が第1のアクセス制御デバイス3000から情報を受信した場合、第2のアクセス制御デバイス3000は、コントローラとして機能する制御ユニット3700を通じて受信した情報に基づいて、ドアロックデバイスをロック解除するための信号を伝送する機能を実行してよい。また、第2のアクセス制御デバイス3000は、ドアロックデバイスをロック解除するための信号を伝送する機能に加えて、ドアアクセス制御、時間及び出席管理及びシステムモード変更などの動作を制御する機能を実行してよい。また、選択に応じて、追加の機能又は操作を実行するための要素がアクセス制御デバイス3000に提供されてよい。

10

【0172】

様々な実施形態に関連するアクセス制御システム10000、及び、アクセス制御システム10000に含まれる要素、操作及び用語などが上述されてきた。上述のアクセス制御システム10000、及び、アクセス制御システム10000に含まれる要素、操作及び用語などは、後述する様々な方法及び実施形態に適用され得る。しかしながら、以下のアクセス制御システム10000は、必ずしも、上述の要素及び機能を有するように構成されなければならないわけではなく、上述のアクセス制御システム10000とは異なる構成を有するアクセス制御システムにさらに適用されてよいことを留意されたい。

【0173】

2. ユーザの端末を用いたアクセス制御デバイスの制御

図5は、本開示の実施形態に係るユーザの端末2000を用いてアクセス制御デバイス3000を制御するための方法のフローチャートである。

20

【0174】

図5を参照すると、ユーザの端末2000を用いてアクセス制御デバイス3000を制御するための方法は、ユーザの端末2000に、アクセス制御デバイス3000を制御するための制御信号を生成させる段階(S100)と、ユーザの端末2000に、制御信号をアクセス制御デバイス3000に伝送させる段階(S110)とを含んでよい。

【0175】

いくつかの実施形態によれば、ユーザの端末2000がアクセス制御デバイス3000を制御するための制御信号を生成する段階(S100)が実行されてよい。

30

【0176】

ユーザの端末2000は、アクセス制御デバイス3000を制御すべく、様々な操作を実行してよく、アクセス制御デバイス3000に伝送される制御信号を生成してよい。制御信号は、ドアを開けるためのものであってよい、又は、アクセス制御デバイス3000の設定を変更するためのものであってよい。

【0177】

例えば、ユーザの端末2000は、アクセス制御デバイス3000を制御して、ドアを開けるべく、ユーザアクセス認証を実行してよい。アクセス認証が成功した場合、ユーザの端末2000は、アクセス制御デバイス3000に伝送されるドア開放信号を生成してよい。アクセス制御デバイス3000は、ドア開放信号を受信し、ドア開放信号に従ってドアを開けてよい。

40

【0178】

別の例として、アクセス制御デバイス3000を制御して設定を変更すべく、ユーザの端末2000は、アクセス制御デバイス3000に対する設定変更情報を受信し、設定変更情報に基づいて、アクセス制御デバイス3000に対する設定変更信号を生成してよい。アクセス制御デバイス3000は、設定変更信号を受信し、設定変更信号に従って設定を変更してよい。

【0179】

いくつかの実施形態によれば、ユーザの端末2000が制御信号をアクセス制御デバイ

50

ス 3 0 0 0 に伝送する段階（S 1 1 0）が実行されてよい。

【0 1 8 0】

アクセス制御デバイス 3 0 0 0 を制御すべく、ユーザの端末 2 0 0 0 は、制御信号をアクセス制御デバイス 3 0 0 0 に伝送してよい。例えば、ユーザの端末 2 0 0 0 は、ドアを開けるべく、ドア開放信号をアクセス制御デバイス 3 0 0 0 に伝送してよい。ドア開放信号が受信された場合、アクセス制御デバイス 3 0 0 0 は、ドアを開けてよい。別の例として、ユーザの端末 2 0 0 0 は、アクセス制御デバイス 3 0 0 0 の設定を変更すべく、設定変更信号をアクセス制御デバイス 3 0 0 0 に伝送してよい。設定変更信号が受信された場合、アクセス制御デバイス 3 0 0 0 は設定変更を実行してよい。

【0 1 8 1】

上述したユーザの端末 2 0 0 0 を用いたアクセス制御デバイス 3 0 0 0 の制御は、説明の便宜上の単なる例である。したがって、本開示は、それに限定されず、ユーザの端末 2 0 0 0 を用いたアクセス制御デバイス 3 0 0 0 の典型的な制御が利用され得る。

【0 1 8 2】

3. アクセス制御方法

従来のアクセス制御システムは、アクセス制御用の認証サーバ及びアクセス制御デバイスを含む。ユーザがアクセスのための許可を要求した場合、アクセス制御用の認証サーバ及びアクセス制御デバイスは、アクセスを許可するか否かを判定するために、互いに体系的に関連する。

【0 1 8 3】

そのような従来のシステムでは、アクセス制御用の認証サーバ及びアクセス制御デバイスが通信可能なままであり、それぞれの役割も果たしている場合のみアクセスを許可するか否かが判定され得る。したがって、アクセス制御認証サーバが無効である場合、又は、アクセス制御用の認証サーバと、アクセス制御デバイスとの間の通信における課題がある場合、ユーザのアクセスが許可されることはない。また、従来のシステムは、アクセス認証情報がアクセス制御デバイスに格納され得るので、セキュリティの脅威に対して脆弱である。

【0 1 8 4】

ユーザの端末 2 0 0 0 においてアクセス認証を実行する方法が、図 6、図 7 及び図 8 を参照して後述される。

【0 1 8 5】

図 6 は、本開示の実施形態に係るユーザの端末 2 0 0 0 においてアクセス認証を実行するための方法のフローチャートである。

【0 1 8 6】

ユーザの端末 2 0 0 0 がアクセス認証を実行する方法は、アクセス認証情報を取得する段階（S 2 0 0）と、アクセス認証を実行する段階（S 2 1 0）とを含んでよい。

【0 1 8 7】

ユーザの端末 2 0 0 0 は、情報を取得してユーザアクセス認証を実行してよい（S 2 0 0）。

【0 1 8 8】

ユーザの端末 2 0 0 0 は、サーバ 1 0 0 0 及びアクセス制御デバイス 3 0 0 0 から、ユーザアクセス認証を実行するための情報を取得してよい。例えば、ユーザの端末 2 0 0 0 は、サーバ 1 0 0 0 からアクセス権情報を取得してよい。また、ユーザの端末 2 0 0 0 は、アクセス制御デバイス 3 0 0 0 の識別情報と、ユーザから受信した生体認証情報とをアクセス制御デバイス 3 0 0 0 から取得してよい。

【0 1 8 9】

ユーザの端末 2 0 0 0 は、ユーザに対してアクセス認証を実行してよい（S 2 1 0）。

【0 1 9 0】

アクセス認証は、ユーザがアクセス権を有するか否かを判定するためのものであってよい。したがって、アクセス認証の成功は、ユーザがアクセス権を有するとの判定であって

10

20

30

40

50

よく、アクセス認証の失敗は、ユーザがアクセス権を有していないとの判定であってよい。

【0191】

ユーザの端末2000は、予め格納されたアクセス権情報に基づいて、様々な方法でユーザアクセス認証を実行してよい。

【0192】

識別情報は、複数のデバイスのうちの特定のデバイスを識別するための情報であってよい。例えば、識別情報は、デバイスID、ユニバーサルユニーク識別子(UUID)、ユニーク識別子(UID)、IPアドレス、MACアドレス、CPU(MCU)シリアル番号又はHDDシリアル番号、及び、端末の通信番号のうちの少なくとも1つを含んでよい。

【0193】

アクセス権情報は、ユーザがアクセス権を有するか否かに従ってユーザアクセス認証を実行するために、ユーザの端末2000によって用いられる情報である。アクセス権情報は、互いに対応し得る登録されたユーザ識別情報、登録された生体認証情報、登録された端末識別情報、登録されたアクセス制御デバイス識別情報、アクセススケジュール情報及び有効期間情報のうちの少なくとも1つを含んでよい。アクセス権情報は、サーバ1000に登録され、管理者によって管理されてよい。ユーザの端末2000は、アクセス認証を実行する前に、サーバ1000からアクセス権情報を取得し、取得したアクセス権情報を格納してよい。また、アクセス権情報は、ユーザの端末2000に格納されてよい。しかしながら、アクセス権情報が失効している、又は、格納されていない場合、ユーザの端末2000は、サーバ1000からアクセス権情報を受信してよい。

【0194】

図7及び図8を参照して、ユーザアクセス認証を実行する方法が後述される。

【0195】

図7及び図8は、本開示の実施形態に係るアクセス権情報の例示的な図である。しかしながら、図7及び図8は、説明の便宜上の単なる例であり、アクセス権情報は、それに限定されない。選択に応じて、いくつかの情報がそこから除外されてよい、又は、様々な追加の情報がそれに追加されてよい。

【0196】

ユーザの端末2000は、アクセス制御デバイス3000から受信した識別情報に基づいて、ユーザのアクセス認証のターゲットドアをチェックしてよい。

【0197】

ユーザの端末2000は、アクセス権情報をアクセス制御デバイス3000の識別情報と比較することにより、ユーザアクセス認証を実行してよい。

【0198】

詳細には、アクセス権情報は、登録されたアクセス制御デバイス識別情報を含む。ユーザの端末2000は、アクセス制御デバイス3000から取得した識別情報がアクセス権情報に含まれているか否かをチェックしてよく、アクセス制御デバイス3000の識別情報がアクセス権情報に含まれている場合、アクセス認証が成功したと判定してよい。また、ユーザの端末2000は、アクセス制御デバイス3000から取得した識別情報がアクセス権情報に含まれているか否かをチェックしてよく、アクセス制御デバイス3000の識別情報がアクセス権情報に含まれていない場合、アクセス認証が失敗したと判定してよい。

【0199】

また、アクセス権情報内の他の情報に対応する登録されたアクセス制御デバイス識別情報にアクセス制御デバイス3000の識別情報が含まれている場合、ユーザの端末2000は、ユーザアクセス認証が成功したと判定してよい。アクセス権情報内の他の情報に対応する登録されたアクセス制御デバイス識別情報にアクセス制御デバイス3000の識別情報が含まれていない場合、ユーザの端末2000は、ユーザアクセス認証が失敗したと判定してよい。

【0200】

例えば、図 7 において、ユーザの端末 2000 が「a」であり、かつ、対応するアクセス制御デバイス 3000 が「第 1 のドア」である場合、アクセス権情報に登録され、かつ、「a」がアクセス権を有しているアクセス制御デバイス識別情報に「第 1 のドア」の識別情報が含まれているので、ユーザの端末 2000 は、アクセス認証が成功したと判定してよい。別の例として、図 7 において、ユーザの端末 2000 が「a」であり、かつ、対応するアクセス制御デバイス 3000 が「第 4 のドア」である場合、アクセス権情報に登録されており、かつ、「a」がアクセス権を有しているアクセス制御デバイス識別情報に「第 4 のドア」の識別情報が含まれていないので、ユーザの端末 2000 は、アクセス認証が失敗したと判定してよい。

【0201】

また、ユーザの端末 2000 は、アクセス権情報をユーザの端末 2000 の識別情報と比較することにより、ユーザアクセス認証を実行してよい。

【0202】

詳細には、アクセス権情報が、登録された端末識別情報に対応する登録されたアクセス制御デバイス識別情報を有する場合、ユーザの端末 2000 は、アクセス制御デバイス 3000 から取得した識別情報に対応する登録された端末識別情報にユーザの端末 2000 の識別情報が含まれているか否かをチェックしてよく、ユーザの端末 2000 の識別情報が登録された端末識別情報に含まれている場合、アクセス認証が成功したと判定してよい。また、登録された端末識別情報に対応する登録されたアクセス制御デバイス識別情報をアクセス権情報が有する場合、ユーザの端末 2000 は、アクセス制御デバイス 3000 から取得した識別情報に対応する登録された端末識別情報にユーザの端末 2000 の識別情報が含まれているか否かをチェックしてよく、登録された端末識別情報にユーザの端末 2000 の識別情報が含まれていない場合、アクセス認証が失敗したと判定してよい。

【0203】

例えば、図 8 において、ユーザの端末 2000 が「b」であり、かつ、対応するアクセス制御デバイス 3000 が「第 1 のドア」である場合、アクセス権情報内にありかつ、「第 1 のドア」に対するアクセス権が割り当てられている登録された端末識別情報に「b」の識別情報が含まれているので、ユーザの端末 2000 は、アクセス認証が成功したと判定してよい。別の例として、図 8 において、ユーザの端末 2000 が「b」であり、かつ、対応するアクセス制御デバイス 3000 が「第 2 のドア」である場合、アクセス権情報に登録されており、かつ、「第 2 のドア」に対するアクセス権が割り当てられている端末識別情報に「b」の識別情報が含まれていないので、ユーザの端末 2000 は、アクセス認証が失敗したと判定してよい。

【0204】

また、ユーザの端末 2000 は、アクセス権情報をユーザから取得した生体認証情報と比較することにより、ユーザアクセス認証を実行してよい。

【0205】

詳細には、アクセス権情報は、登録された生体認証情報を含む。ユーザの端末 2000 は、ユーザから取得した生体認証情報がアクセス権情報に含まれているか否かをチェックしてよく、ユーザから取得した生体認証情報がアクセス権情報に含まれている場合、アクセス認証が成功したと判定してよい。また、アクセス権情報は、登録された生体認証情報を含む。ユーザの端末 2000 は、ユーザから取得した生体認証情報がアクセス権情報に含まれているか否かをチェックしてよく、ユーザから取得した生体認証情報がアクセス権情報に含まれていない場合、アクセス認証が失敗したと判定してよい。

【0206】

また、ユーザから受信した生体認証情報が、アクセス権情報内の他の情報に対応する登録された生体認証情報に含まれている場合、ユーザの端末 2000 は、ユーザアクセス認証が成功したと判定してよい。ユーザから受信した生体認証情報が、アクセス権情報内の他の情報に対応する登録された生体認証情報に含まれていない場合、ユーザの端末 2000 は、ユーザアクセス認証が失敗したと判定してよい。

10

20

30

40

50

【0207】

例えば、図7において、ユーザの生体認証情報が「a'」であり、かつ、対応するアクセス制御デバイス3000が「第1のドア」である場合、アクセス権情報に登録されており、かつ、「a'」がアクセス権を有しているアクセス制御デバイス識別情報に「第1のドア」の識別情報が含まれているので、ユーザの端末2000は、アクセス認証が成功したと判定してよい。別の例として、図7において、ユーザの生体認証情報が「a'」であり、かつ、対応するアクセス制御デバイス3000が「第4のドア」である場合、アクセス権情報に登録されており、かつ、「a'」がアクセス権を有しているアクセス制御デバイス識別情報に「第4のドア」の識別情報が含まれていないので、ユーザの端末2000は、アクセス認証が失敗したと判定してよい。

10

【0208】

また、ユーザの端末2000は、アクセス権情報を現在の時刻と比較することにより、ユーザアクセス認証を実行してよい。

【0209】

詳細には、ユーザの端末2000は、現在の時刻がアクセススケジュール情報に含まれているか否かをチェックしてよく、現在の時刻がアクセススケジュール情報に含まれている場合、アクセス認証が成功したと判定してよい。また、ユーザの端末2000は、現在の時刻がアクセススケジュール情報に含まれているか否かをチェックしてよく、現在の時刻がアクセススケジュール情報に含まれていない場合、アクセス認証が失敗したと判定してよい。

20

【0210】

また、ユーザの端末2000は、アクセス権情報に対応する情報に含まれているアクセス制御デバイス3000の識別情報に対応するアクセススケジュール情報に、現在の時刻が含まれているか否かをチェックしてよく、アクセス制御デバイス3000の識別情報に対応するアクセススケジュール情報に現在の時刻が含まれていない場合、アクセス認証が失敗したと判定してよい。

【0211】

また、ユーザの端末2000は、アクセス権情報に対応する情報に含まれているユーザの端末2000の識別情報に対応するアクセススケジュール情報に現在の時刻が含まれているか否かをチェックしてよく、ユーザの端末2000の識別情報に対応するアクセススケジュール情報に現在の時刻が含まれていない場合、アクセス認証が失敗したと判定してよい。

30

【0212】

また、ユーザの端末2000は、アクセス権情報に対応する情報に含まれている取得した生体認証情報に対応するアクセススケジュール情報に現在の時刻が含まれているか否かをチェックしてよく、取得した生体認証情報に対応するアクセススケジュール情報に現在の時刻が含まれていない場合、アクセス認証が失敗したと判定してよい。

【0213】

例えば、図7において、ユーザの端末2000が「a」であり、ユーザの生体認証情報が「a'」であり、かつ、対応するアクセス制御デバイス3000が「第1のドア」である場合、ユーザの端末2000は、アクセス認証が成功したと判定する。しかしながら、たとえこの場合であっても、現在の時刻が午前8時である場合、「第1のドア」に対応するアクセススケジュール情報に現在の時刻が含まれていないので、ユーザの端末2000は、アクセス認証が失敗したと判定してよい。別の例として、図7において、ユーザの端末2000が「a」であり、ユーザの生体認証情報が「a'」であり、かつ、対応するアクセス制御デバイス3000が「第1のドア」である場合、ユーザの端末2000は、アクセス認証が成功したと判定する。しかしながら、たとえこの場合であっても、現在の時刻が午前8時である場合、「a」及び／又は「a'」に対応するアクセススケジュール情報に現在の時刻が含まれていないので、ユーザの端末2000は、アクセス認証が失敗したと判定してよい。

40

50

【0214】

また、アクセス権情報が失効したか否かに従って、ユーザの端末2000は、ユーザアクセス認証情報を実行してよい。

【0215】

詳細には、ユーザの端末2000は、アクセス権情報が失効したか否かをチェックしてよく、アクセス権情報が失効した場合、アクセス認証が失敗したと判定してよい。

【0216】

アクセス認証が成功したとユーザの端末2000が判定したにもかかわらず、アクセス権情報が失効した場合、ユーザの端末2000は、アクセス認証が失敗したと判定してよい。代替的に、アクセス権情報が失効した場合、ユーザの端末2000は、アクセス認証が失敗したとすぐに判定してよい。

10

【0217】

例えば、図7において、ユーザの端末2000が「a」であり、ユーザの生体認証情報が「a'」であり、かつ、対応するアクセス制御デバイス3000が「第1のドア」である場合、ユーザの端末2000は、アクセス認証が成功したと判定する。しかしながら、この場合であっても、アクセス権情報の有効期間を示す5時間が経過し、それにより、アクセス権情報が失効した場合、ユーザの端末2000は、アクセス認証が失敗したと判定し得る。また、図7において、アクセス権情報の有効期間を示す5時間が経過し、それにより、アクセス権情報が失効した場合、ユーザの端末2000は、アクセス認証が失敗したと判定し得る。

20

【0218】

ユーザの端末2000は、アクセス権情報の登録されたアクセス制御デバイス識別情報と、受信した識別情報を比較し、受信した識別情報が、登録されたアクセス制御デバイス識別情報のうちの1つに合致する場合、アクセス認証が成功したと判定してよい。

【0219】

また、ユーザの端末2000は、アクセス権情報の受信した識別情報に関連するアクセススケジュール情報と現在の時刻を比較し、現在の時刻がアクセススケジュールに含まれていない場合、アクセス認証が失敗したと判定してよい。

【0220】

また、ユーザの端末2000は、ユーザの端末2000の識別情報を、受信した識別情報に関連する登録された端末識別情報と比較し、ユーザの端末2000の識別情報が、受信した識別情報に対応する登録された端末識別情報のうちの1つに合致していない場合、アクセス認証が失敗したと判定してよい。

30

【0221】

また、ユーザの端末2000は、アクセス権情報が失効した場合、ユーザがターゲットドアにアクセスすることを認められているか否かを判定する段階を回避してよい。

【0222】

また、ユーザの端末2000は、ユーザの受信した生体認証情報を登録された生体認証情報と比較し、ユーザの生体認証情報が、登録された生体認証情報のうちの1つに合致する場合、アクセス認証が成功したと判定してよい。

40

【0223】

また、ユーザの端末2000は、アクセス権情報のユーザの受信した生体認証情報に関連するアクセススケジュール情報と現在の時刻を比較し、現在の時刻がアクセススケジュールに含まれていない場合、アクセス認証が失敗したと判定してよい。

【0224】

また、ユーザの端末2000は、ユーザの受信した生体認証情報に関連する登録された端末識別情報と、ユーザの端末2000の識別情報を比較し、ユーザの端末2000の識別情報が、ユーザの受信した生体認証情報に対応する登録された端末識別情報のうちの1つに合致していない場合、アクセス認証が失敗したと判定してよい。

【0225】

50

アクセス認証方法は、上述の方法に限定されず、上述の方法の組み合わせでさらに提供され得る。

【0226】

図9は、本開示の実施形態に係るアクセス制御方法の周辺図である。

【0227】

例として、図9に示されるように、実施形態に係るアクセス制御方法によれば、ユーザの端末2000は、アクセス制御デバイス3000から識別情報及び／又は生体認証情報を受信してよく、ユーザの端末2000は、アクセス認証情報に基づいて、ユーザアクセス認証を実行してよい。ユーザアクセス認証が成功した場合、ユーザは、対応するドアにアクセスし得る。

【0228】

図10、図11及び図12を参照して、ユーザの端末2000がアクセス認証を実行するアクセス制御システム10000のアクセス制御方法が後述される。

【0229】

図10は、本開示の実施形態に係るアクセス認証結果を管理するための方法のフローチャートである。ユーザの端末2000は、アクセス制御デバイス3000に近づき、アクセス認証を実行し、その結果をサーバ1000に伝送する。したがって、アクセス認証結果は、サーバ1000により管理され得る。したがって、アクセス制御システム10000は、作業者などの時間及び出席管理用に利用され得る。

【0230】

図10を参照すると、アクセス認証結果を管理するための方法は、ユーザの端末2000が、サーバ1000からアクセス権情報を要求する段階(S300)と、サーバ1000が、アクセス権情報をユーザの端末2000に伝送する段階(S310)と、ユーザの端末2000とアクセス制御デバイス3000との間に通信を確立する段階(S320)と、アクセス制御デバイス3000が、識別情報をユーザの端末2000に伝送する段階(S330)と、ユーザの端末2000が、アクセス認証を実行する段階(S340)と、ユーザの端末2000が、アクセス認証結果情報を生成する段階(S350)と、ユーザの端末2000が、アクセス認証結果情報をサーバ1000に伝送する段階(S360)とを含んでよい。

【0231】

本開示のいくつかの実施形態によれば、ユーザの端末2000がサーバ1000からアクセス権情報を要求する段階(S300)が実行されてよい。

【0232】

ユーザの端末2000は、そこに予め格納されたアクセス権情報を有してよい、又は、サーバ1000からアクセス権情報を要求してよい。

【0233】

例えば、アクセス権情報が格納されていない場合、ユーザの端末2000は、サーバ1000からアクセス権情報を自動的に要求してよい。また、アクセス権情報が失効した場合、ユーザの端末2000は、サーバ1000からアクセス権情報を自動的に要求してよい。

【0234】

代替的に、ユーザ要求が入力された場合に、ユーザの端末2000は、サーバ1000からアクセス権情報を要求してよい。例えば、アクセス権情報がユーザの端末2000に格納されているけれども、ユーザが、アクセス権情報を更新したいかもしれない、又は、アクセス権情報が格納されていることを知らないかもしれない。この場合、ユーザは、ユーザの端末2000に要求を入力してよく、ユーザの端末2000は、サーバ1000からアクセス権情報を要求してよい。

【0235】

段階S300は、必ずしも必要ではなく、いくつかの実施形態に従って省略されてよい。

【0236】

10

20

30

40

50

また、本開示のいくつかの実施形態によれば、サーバ１０００がアクセス権情報をユーザの端末２０００に伝送する段階（Ｓ３１０）が実行され得る。

【０２３７】

ユーザの端末２０００からアクセス権情報要求が受信された場合、サーバ１０００は、アクセス権情報をユーザの端末２０００に伝送してよい。例えば、アクセス権情報がユーザの端末２０００に格納されていないので、又は、アクセス権情報が失効したので、ユーザがサーバ１０００へのアクセス権情報の要求を入力した場合、サーバ１０００は、アクセス権情報をユーザの端末２０００に伝送してよい。

【０２３８】

代替的に、ユーザの端末２０００からアクセス権情報要求が受信され場合であっても、サーバ１０００は、アクセス権情報をユーザの端末２０００に伝送してよい。例えば、サーバ１０００は、ユーザの端末２０００との周期的な通信を通じて、アクセス権情報がユーザの端末２０００に格納されているか否かをチェックしてよく、アクセス権情報が格納されていない場合、アクセス権情報をユーザの端末２０００に自動的に伝送してよい。

【０２３９】

サーバ１０００が、アクセス権情報をユーザの端末２０００に伝送した場合、ユーザの端末２０００は、アクセス権情報を受信し、受信したアクセス権情報を端末ストレージユニット２５００に格納してよい。

【０２４０】

段階Ｓ３１０は、必ずしも必要ではなく、いくつかの実施形態に従って省略され得る。

【０２４１】

本開示のいくつかの実施形態によれば、ユーザの端末２０００とアクセス制御デバイス３０００との間に通信を確立する段階（Ｓ３２０）が実行され得る。

【０２４２】

ユーザの端末２０００がアクセス制御デバイス３０００に近づいた場合、ユーザの端末２０００は、アクセス制御デバイス３０００を検出し、アクセス制御デバイス３０００との通信チャネルを確立してよい。この場合、通信チャネルが確立された場合、ユーザの端末２０００又はアクセス制御デバイス３０００は、外部に通知を出力してよい。

【０２４３】

ＢＬＥ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＮＦＣ及びＷｉ－Ｆｉ（登録商標）などの近距離通信規格に従って、ユーザの端末２０００とアクセス制御デバイス３０００との間の通信が実行されてよい。

【０２４４】

本開示のいくつかの実施形態によれば、アクセス制御デバイス３０００が識別情報をユーザの端末２０００に伝送する段階（Ｓ３３０）が実行され得る。

【０２４５】

ユーザの端末２０００との通信チャネルが確立された場合、アクセス制御デバイス３０００は、アクセス制御デバイス３０００の識別情報をユーザの端末２０００に自動的に伝送してよい。代替的に、ユーザの端末２０００から識別情報の要求が受信された場合、アクセス制御デバイス３０００は、識別情報をユーザの端末２０００に伝送してよい。また、アクセス制御デバイス３０００が、識別情報をユーザの端末２０００に伝送する段階、及び、ユーザの端末２０００とアクセス制御デバイス３０００との間に通信チャネルを確立する段階が同時に実行されてよい。

【０２４６】

本開示のいくつかの実施形態によれば、ユーザの端末２０００がアクセス認証を実行する段階（Ｓ３４０）が実行され得る。

【０２４７】

ユーザの端末２０００は、端末ストレージユニット２５００に予め格納されたアクセス権情報に基づいて説明されたアクセス認証方法（Ｓ２１０）のうちの少なくとも１つにより、ユーザアクセス認証を実行してよい。

10

20

30

40

50

【0248】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス認証結果情報を生成する段階(S350)が実行され得る。

【0249】

ユーザの端末2000は、アクセス認証を実行してよく、アクセス認証が成功した場合、アクセス認証が成功したことを示す結果情報を生成してよい。代替的に、ユーザの端末2000は、アクセス認証を実行してよく、アクセス認証が失敗した場合、アクセス認証が失敗したことを示す結果情報を生成してよい。この場合、ユーザの端末2000は、端末ディスプレイユニット2200を通じて、認証結果を示す視覚的な通知を出力してよい、又は、別個の出力ユニットを通じて、認証結果を示す音声通知メッセージを出力してよい。

10

【0250】

本開示のいくつかの実施形態によれば、ユーザの端末2000がサーバ1000にアクセス認証結果情報を伝送する段階(S360)が実行され得る。

【0251】

ユーザの端末2000は、生成されたアクセス認証結果情報をサーバ1000に伝送してよい。サーバ1000は、アクセス認証結果情報を受信して、これをサーバストレージユニット1300に格納してよい。

【0252】

図11は、本開示の実施形態に係るドア開放を管理するための方法のフローチャートである。ユーザの端末2000は、アクセス制御デバイス3000に近づき、アクセス認証を実行し、ドア開放信号をアクセス制御デバイス3000に伝送することにより、ドアの開閉操作を制御してよい。したがって、アクセス制御システム10000は、ドアにアクセスする手段として、ユーザの端末2000を利用してよい。

20

【0253】

図11を参照すると、ドア開放を管理するための方法は、ユーザの端末2000が、サーバ1000からアクセス権情報を要求する段階(S400)と、サーバ1000が、アクセス権情報をユーザの端末2000に伝送する段階(S410)と、ユーザの端末2000とアクセス制御デバイス3000との間に通信を確立する段階(S420)と、アクセス制御デバイス3000が、識別情報をユーザの端末2000に伝送する段階(S430)と、ユーザの端末2000が、アクセス認証を実行する段階(S440)と、ユーザの端末2000が、ドア開放信号を生成する段階(S450)と、ユーザの端末2000が、ドア開放信号をアクセス制御デバイス3000に伝送する段階(S460)と、アクセス制御デバイス3000が、ドア開放動作を実行する段階(S470)とを含んでよい。

30

【0254】

本開示のいくつかの実施形態によれば、ユーザの端末2000がサーバ1000からアクセス権情報を要求する段階(S400)が実行され得る。

【0255】

段階S400は、上述した段階S300と同様に実行され、したがって、それらの詳細な説明が省略される。

40

【0256】

段階S400は、必ずしも必要ではなく、いくつかの実施形態に従って省略されてよい。

【0257】

また、本開示のいくつかの実施形態によれば、サーバ1000が、アクセス権情報をユーザの端末2000に伝送する段階(S410)が実行され得る。

【0258】

段階S410は、上述した段階S310と同様に実行され、したがって、それらの詳細な説明が省略される。

【0259】

段階S410は、必ずしも必要ではなく、いくつかの実施形態に従って省略されてよい。

50

【0260】

本開示のいくつかの実施形態によれば、ユーザの端末2000とアクセス制御デバイス3000との間に、通信チャネルを確立する段階（S420）が実行され得る。

【0261】

段階S420は、上述した段階S320と同様に実行され、したがって、それらの詳細な説明が省略される。

【0262】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000が、ユーザの端末2000に識別情報を伝送する段階（S430）が実行され得る。

【0263】

段階S430は、上述した段階S330と同様に実行され、したがって、それらの詳細な説明が省略される。

【0264】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス認証を実行する段階（S440）が実行され得る。

【0265】

段階S440は、上述した段階S340と同様に実行され、したがって、それらの詳細な説明が省略される。

【0266】

本開示のいくつかの実施形態によれば、ユーザの端末2000がドア開放信号を生成する段階（S450）が実行され得る。

【0267】

また、ユーザがアクセス認証に成功した場合、ユーザの端末2000は、アクセス制御デバイス3000に伝送されるドア開放信号を生成してよい。ドア開放信号は、アクセス制御デバイス3000に、ドア開放動作を実行させ得る。つまり、ユーザの端末2000からアクセス制御デバイス3000にドア開放信号が伝送された場合、制御ユニット3700は、電源ユニット3600を通じて、アクセス制御デバイス3000をドア開放状態に変更し得る。しかしながら、ユーザアクセス認証が失敗した場合、ユーザの端末2000は、ドア開放信号を生成しなくてよい。

【0268】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス制御デバイス3000にドア開放信号を伝送する段階（S460）が実行され得る。

【0269】

ユーザの端末2000は、ドア開放信号をアクセス制御デバイス3000に伝送してよい。例えば、ユーザの端末2000は、BLE、Bluetooth（登録商標）、WLAN、Wi-Fi（登録商標）、Wi-Fi（登録商標）ダイレクト、NFC、IRDA、UWB及びZigbee（登録商標）などの無線通信を通じて、ドア開放信号をアクセス制御デバイス3000に伝送してよい。

【0270】

また、望まれていないドアが開くことを防止すべく、ユーザの端末2000とアクセス制御デバイス3000との間の距離が特定の距離より短い又はそれに等しい場合、ユーザの端末2000は、ドア開放信号をアクセス制御デバイス3000に伝送してよい。

【0271】

この場合、ユーザの端末2000は、ドア開放信号をアクセス制御デバイス3000に伝送してよく、アクセス制御デバイス3000は、ドア開放信号の受信に成功した場合、肯定応答信号（ACK）をユーザの端末2000に伝送してよい。また、ユーザの端末2000は、ドア開放信号をアクセス制御デバイス3000に伝送してよく、アクセス制御デバイス3000は、ドア開放信号の受信に成功しなかった場合、否定応答信号（NACK）を伝送してよい。この場合、ユーザの端末2000がアクセス制御デバイス3000から肯定応答信号を受信した場合、アクセス制御デバイス3000は、ドアが開けられる

10

20

30

40

50

ことを示す情報をサーバ1000に伝送してよい。逆に、ユーザの端末2000がアクセス制御デバイス3000から否定応答信号を受信した場合、アクセス制御デバイス3000は、ドアが開けられないことを示す情報をサーバ1000に伝送してよい。

【0272】

また、いくつかの実施形態によれば、アクセス制御デバイス3000がドア開放動作を実行する段階（S470）が実行され得る。

【0273】

アクセス制御デバイス3000がユーザの端末2000からドア開放信号を受信した場合、アクセス制御デバイス3000は、ドアリーフがロック解除状態になり得るように、電源ユニット3600を通じて電力を提供してよい。また、ドアが自動ドアである場合、アクセス制御デバイス3000は、ドアリーフが開いた状態になり得るように、電源ユニット3600を通じて電力を提供してよい。

【0274】

ドアリーフがロック解除された後、アクセス制御デバイス3000は、ドアリーフがロック条件に基づいてロックされるように、電源ユニット3600を通じて電力を提供してよい。アクセス制御デバイス3000は、センサユニット3400から取得された信号に基づいて、ドアリーフが再び閉められたか否かを判定してよい。ドアリーフが再び閉められた場合、アクセス制御デバイス3000は、ドアリーフがロックされ得るように、電源ユニット3600を通じて電力を提供してよい。また、アクセス制御デバイス3000は、ドアリーフが再び閉められても、ロックスタンバイ時間の後にドアリーフがロックされ得るように、ロックスタンバイ時間をさらに考慮して、電源ユニット3600を通じて電力を提供してよい。また、ディスプレイユニット3200、音声出力ユニット3300及び／又は別個の出力ユニットを通じて、聴覚情報、視覚情報及び振動のうちの少なくとも1つを出力することにより、アクセス制御デバイス3000は、ドアが開くことを通知してよい。

【0275】

上述のドア開放管理方法では、図示されていないが、ユーザの端末2000がアクセス認証を実行する段階（S440）の後に、ユーザの端末2000がアクセス認証結果情報を生成する段階（S350）及びユーザの端末2000がアクセス認証結果情報をサーバ1000に伝送する段階（S360）も実行されてよい。

【0276】

図12は、本開示の実施形態に係る、ドアにアクセスすると情報を通知するための方法のフローチャートである。ドアは、スイッチを押してドアを開けることにより、ドア開放入力を要求する自動ドアなどで実施されるものと仮定する。ユーザがアクセス制御デバイス3000に近づいて、入力ユニット3900を通じてドア開放入力を入力して、ドアを開ける場合、ユーザの端末2000は、アクセス制御デバイス3000からアクセス認証要求信号を受信し、サーバ1000と通信するサーバ1000から予め設定されたメッセージ取得してよい。したがって、アクセス制御システム10000は、アドバタイズメントのための手段、又は、ドアにアクセスする場合の情報通知として、ユーザの端末2000を利用してよい。

【0277】

図12を参照すると、ドアにアクセスすると、情報を通知するための方法は、ユーザの端末2000が、サーバ1000からアクセス権情報を要求する段階（S500）と、サーバ1000が、アクセス権情報をユーザの端末2000に伝送する段階（S505）と、アクセス制御デバイス3000が、ドア開放入力を受信する段階（S510）と、アクセス制御デバイス3000が、アクセス認証要求信号を生成する段階（S515）と、アクセス制御デバイス3000が、アクセス認証要求信号をユーザの端末2000に伝送する段階（S520）と、ユーザの端末2000が、サーバ1000と通信する段階（S525）と、サーバ1000が、メッセージをユーザの端末2000に伝送する段階（S530）と、ユーザの端末2000が、アクセス認証を実行する段階（S535）と、ユー

ザの端末 2000 が、ドア開放信号を生成する段階（S540）と、ユーザの端末 2000 が、ドア開放信号をアクセス制御デバイス 3000 に伝送する段階（S545）と、アクセス制御デバイス 3000 が、ドア開放動作を実行する段階（S550）とを含んでよい。

【0278】

本開示のいくつかの実施形態によれば、ユーザの端末 2000 がサーバ 1000 からアクセス権情報を要求する段階（S500）が実行され得る。

【0279】

段階 S500 は、上述した段階 S300 と同様に実行され、したがって、それらの詳細な説明が省略される。

【0280】

段階 S500 は、必ずしも必要ではなく、いくつかの実施形態に従って省略されてよい。

【0281】

また、本開示のいくつかの実施形態によれば、サーバ 1000 がアクセス権情報をユーザの端末 2000 に伝送する段階（S505）が実行され得る。

【0282】

段階 S505 は、上述した段階 S310 と同様に実行され、したがって、それらの詳細な説明が省略される。

【0283】

段階 S505 は、必ずしも必要ではなく、いくつかの実施形態に従って省略され得る。

【0284】

本開示のいくつかの実施形態によれば、アクセス制御デバイス 3000 がドア開放入力を受信する段階（S510）が実行され得る。

【0285】

例えば、ドアが、ドア開放入力を提供するためにスイッチが押された場合のみ開く自動ドアで実装されると仮定する。ドア開放入力が受信された場合、アクセス制御デバイス 3000 は、ドアを開けるための入力信号を生成し得る。

【0286】

本開示のいくつかの実施形態によれば、アクセス制御デバイス 3000 がアクセス認証要求信号を生成する段階（S515）が実行され得る。

【0287】

例えば、アクセス制御デバイス 3000 は、ドア開放入力により生成された入力信号に従って、アクセス認証要求信号を生成してよい。この場合、アクセス認証要求信号は、アクセス制御デバイス 3000 の識別情報を含む信号であってよい。

【0288】

本開示のいくつかの実施形態によれば、アクセス制御デバイス 3000 がアクセス認証要求信号をユーザの端末 2000 に伝送する段階（S520）が実行され得る。

【0289】

アクセス制御デバイス 3000 は、アクセス認証要求信号をユーザの端末 2000 に伝送してよい。アクセス認証要求信号が受信された場合、ユーザの端末 2000 は、ユーザアクセス認証を実行してよい。また、アクセス認証要求信号は、アクセス制御デバイス 3000 の識別情報を含む信号を含んでよい。また、アクセス制御デバイス 3000 は、アクセス認証要求信号の伝送とは別に、アクセス制御デバイス 3000 の識別情報をユーザの端末 2000 に伝送してよい。

【0290】

例えば、アクセス制御デバイス 3000 とユーザの端末 2000 との間の通信が、BLE を通じて実行される場合、アクセス認証要求信号の伝送は、アクセス制御デバイス 3000 が、アドバタイズ信号をユーザの端末 2000 に伝送することを意味し得る。

【0291】

本開示のいくつかの実施形態によれば、ユーザの端末 2000 がサーバ 1000 と通信

10

20

30

40

50

する段階（Ｓ５２５）が実行され得る。

【０２９２】

アクセス制御デバイス３０００から、アクセス認証要求信号が受信された場合、ユーザの端末２０００は、サーバ１０００と通信してよい。例えば、アクセス制御デバイス３０００から、アクセス認証要求信号が受信された場合、ユーザの端末２０００は、予め設定されたメッセージを要求するための信号をサーバ１０００に自動的に伝送してよい。

【０２９３】

本開示のいくつかの実施形態によれば、サーバ１０００がメッセージをユーザの端末２０００に伝送する段階（Ｓ５３０）が実行され得る。

【０２９４】

サーバ１０００は、予め設定されたメッセージをユーザの端末２０００に伝送してよい。例えば、アドバタイズメントメッセージが指定されている場合、サーバ１０００は、アドバタイズメントメッセージをユーザの端末２０００に伝送してよい。また、通知メッセージが指定されている場合、サーバ１０００は、通知メッセージをユーザの端末２０００に伝送してよい。この場合、複数のメッセージが指定されてよく、異なるメッセージが、サーバ１０００に格納される複数のメッセージの中から、現在の時刻に従って指定されてよい。

【０２９５】

本開示のいくつかの実施形態によれば、ユーザの端末２０００がアクセス認証を実行する段階（Ｓ５３５）が実行され得る。

【０２９６】

段階Ｓ５３５は、上述した段階Ｓ３４０と同様に実行され、したがって、それらの詳細な説明が省略される。

【０２９７】

本開示のいくつかの実施形態によれば、ユーザの端末２０００がドア開放信号を生成する段階（Ｓ５４０）が実行され得る。

【０２９８】

段階Ｓ５４０は、上述した段階Ｓ４５０と同様に実行され、したがって、それらの詳細な説明が省略される。

【０２９９】

本開示のいくつかの実施形態によれば、ユーザの端末２０００がドア開放信号をアクセス制御デバイス３０００に伝送する段階（Ｓ５４５）が実行され得る。

【０３００】

段階Ｓ５４５は、上述した段階Ｓ４６０と同様に実行され、したがって、それらの詳細な説明が省略される。

【０３０１】

また、いくつかの実施形態によれば、アクセス制御デバイス３０００がドア開放動作を実行する段階（Ｓ５５０）が実行され得る。

【０３０２】

段階Ｓ５５０は、上述した段階Ｓ４７０と同様に実行され、したがって、それらの詳細な説明が省略される。

【０３０３】

ドア開放すると上述した情報通知方法において、図示されていないが、ユーザの端末２０００がアクセス認証結果情報を生成（Ｓ３５０）する段階と、ユーザの端末２０００が、アクセス認証結果情報をサーバ１０００に伝送する段階（Ｓ３６０）とは、また、ユーザの端末２０００がアクセス認証を実行する段階（Ｓ５３５）の後に実行され得る。

【０３０４】

ユーザの端末２０００がアクセス認証を実行するアクセス制御システム１００００において、ユーザの生体認証情報を用いるアクセス制御方法は、図１３及び図１４を参照して後述される。

10

20

30

40

50

【0305】

図13は、本開示の実施形態に係る生体認証情報を用いて、アクセス認証結果を管理するための方法のフローチャートである。ユーザの端末2000は、アクセス制御デバイス3000に近づいて、アクセス認証を実行し、その結果をサーバ1000に伝送する。したがって、アクセス認証結果は、サーバ1000により管理され得る。この場合、セキュリティが強化されたアクセス認証は、アクセス制御デバイス3000から受信したユーザの生体認証情報を用いて実行され得る。したがって、アクセス制御システム10000は、作業者の時間及び出席管理などに利用され得る。

【0306】

図13を参照すると、生体認証情報を用いてアクセス認証結果を管理するための方法は、ユーザの端末2000が、サーバ1000からアクセス権情報を要求する段階(S600)と、サーバ1000が、アクセス権情報をユーザの端末2000に伝送する段階(S610)と、ユーザの端末2000とアクセス制御デバイス3000との間に通信を確立する段階(S620)と、アクセス制御デバイス3000が生体認証情報を受信する段階(S630)と、アクセス制御デバイス3000が、生体認証情報をユーザの端末2000に伝送する段階(S640)と、ユーザの端末2000が、アクセス認証を実行する段階(S650)と、ユーザの端末2000が、アクセス認証結果情報を生成する段階(S660)と、ユーザの端末2000が、アクセス認証結果情報をサーバ1000に伝送する段階(S670)とを含んでよい。

【0307】

本開示のいくつかの実施形態によれば、ユーザの端末2000がサーバ1000からアクセス権情報を要求する段階(S600)が実行され得る。

【0308】

段階S600は、上述した段階S300と同様に実行され、したがって、それらの詳細な説明が省略される。

【0309】

段階S600は、必ずしも必要ではなく、いくつかの実施形態に従って省略され得る。

【0310】

また、本開示のいくつかの実施形態によれば、サーバ1000がアクセス権情報をユーザの端末2000に伝送する段階(S610)が実行され得る。

【0311】

段階S610は、上述した段階S310と同様に実行され、したがって、それらの詳細な説明が省略される。

【0312】

段階S610は、必ずしも必要ではなく、いくつかの実施形態に従って省略され得る。

【0313】

本開示のいくつかの実施形態によれば、ユーザの端末2000とアクセス制御デバイス3000との間に通信を確立する段階(S620)が実行され得る。

【0314】

段階S620は、上述した段階S320と同様に実行され、したがって、それらの詳細な説明が省略される。

【0315】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000が生体認証情報を受信する段階(S630)が実行され得る。

【0316】

アクセス制御デバイス3000は、生体認証情報入力ユニット3800を通じてユーザから生体認証情報を受信してよく、ユーザの生体認証情報を取得してよい。

【0317】

ユーザの生体認証情報は、ユーザの指紋情報、虹彩情報、顔情報、静脈情報及び音声情報のうちの1つを指し得る。例えば、生体認証情報入力ユニット3800がユーザの指紋

10

20

30

40

50

情報を取得するためのスクリーンキャナである場合、アクセス制御デバイス3000は、ユーザの指紋情報を受信及び取得してよい。また、生体認証情報入力ユニット3800がユーザの音声情報を取得するためのマイクである場合、アクセス制御デバイス3000は、ユーザの音声情報を受信及び取得してよい。また、生体認証情報入力ユニット3800がユーザの虹彩情報を取得するためのカメラである場合、アクセス制御デバイス3000は、ユーザの虹彩情報を受信及び取得してよい。

【0318】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000が、生体認証情報をユーザの端末2000に伝送する段階（S640）が実行され得る。

【0319】

ユーザから生体認証情報が取得された場合、アクセス制御デバイス3000は、取得した生体認証情報をユーザの端末2000に自動的に伝送してよい。代替的に、ユーザの端末2000からの生体認証情報の要求が受信された場合、アクセス制御デバイス3000は、取得した生体認証情報をユーザの端末2000に伝送してよい。

【0320】

この場合、セキュリティの目的として、アクセス制御デバイス3000は、取得した生体認証情報を暗号化し、暗号化された生体認証情報をユーザの端末2000に伝送してよい。例えば、アクセス制御デバイス3000は、アクセス制御デバイス3000のパブリックキーを用いて、取得した生体認証情報を暗号化してよい。

【0321】

また、アクセス制御デバイス3000は、生体認証情報に加えて、アクセス制御デバイス3000の識別情報をユーザの端末2000に伝送してよい。代替的に、アクセス制御デバイス3000は、生体認証情報に加えて、アクセス制御デバイス3000の識別情報をユーザの端末2000に伝送してよい。

【0322】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス認証を実行する段階（S650）が実行され得る。

【0323】

ユーザの端末2000は、アクセス制御デバイス3000から受信した生体認証情報を用いて、アクセス認証を実行してよい。この場合、アクセス制御デバイス3000により、生体認証情報が暗号化されている場合、ユーザの端末2000は、暗号化された生体認証情報を復号し、アクセス認証を実行してよい。例えば、アクセス制御デバイス3000から取得した生体認証情報が、アクセス制御デバイス3000のパブリックキーで暗号化されている場合、ユーザの端末2000は、アクセス制御デバイス3000のプライベートキーを用いて、暗号化された生体認証情報を復号し、次に、アクセス認証を実行してよい。

【0324】

段階S650は、上述した段階S340と同様に実行され、したがって、それらの詳細な説明が省略される。

【0325】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス認証結果情報を生成する段階（S660）が実行され得る。

【0326】

段階S660は、上述した段階S350と同様に実行され、したがって、それらの詳細な説明が省略される。

【0327】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス認証結果情報をサーバ1000に伝送する段階（S670）が実行され得る。

【0328】

段階S670は、上述した段階S360と同様に実行され、したがって、それらの詳細

10

20

30

40

50

な説明が省略される。

【0329】

生体認証情報を用いる上述のアクセス認証結果管理方法は、図示されていないが、ユーザアクセス認証を実行すべく、ユーザの端末2000がユーザの生体認証情報を取得することは、ユーザの端末2000が、アクセス制御デバイス3000が生体認証情報を受信する段階(S630)、及び、アクセス制御デバイス3000が生体認証情報をユーザの端末2000に伝送する段階(S640)を用いることなく、ユーザから生体認証情報を受信及び取得することを意味し得る。ユーザの生体認証情報は、ユーザの指紋情報、虹彩情報、顔情報、静脈情報及び音声情報のうちの1つを指し得る。例えば、端末生体認証情報入力ユニット2700が、ユーザの指紋情報を取得ためのスクリーンキャナである場合、ユーザの端末2000は、ユーザの指紋情報を受信及び取得してよい。また、端末生体認証情報入力ユニット2700が、ユーザの音声情報を取得するためのマイクである場合、ユーザの端末2000は、ユーザの音声情報を受信及び取得してよい。また、端末生体認証情報入力ユニット2700が、ユーザの虹彩情報を取得するためのカメラである場合、ユーザの端末2000は、ユーザの虹彩情報を受信及び取得してよい。

10

【0330】

図14は、本開示の実施形態に係る生体認証情報を用いて、ドア開放を管理するための方法のフローチャートである。ユーザの端末2000は、アクセス制御デバイス3000に近づいて、アクセス認証を実行し、ドア開放信号をアクセス制御デバイス3000に伝送する。したがって、ユーザの端末2000は、ドアの開閉操作を制御し得る。この場合、ユーザの端末2000は、ユーザの生体認証情報を用いて、セキュリティが強化されたアクセス認証を実行してよい。したがって、アクセス制御システム10000は、ドアにアクセスする手段として、ユーザの端末2000を利用してよい。

20

【0331】

図14を参照すると、生体認証情報を用いてドア開放を管理するための方法は、ユーザの端末2000が、サーバ1000からアクセス権情報を要求する段階(S700)と、サーバ1000が、アクセス権情報をユーザの端末2000に伝送する段階(S710)と、ユーザの端末2000とアクセス制御デバイス3000との間に通信を確立する段階(S720)と、アクセス制御デバイス3000が、生体認証情報を受信する段階(S730)と、アクセス制御デバイス3000が、生体認証情報をユーザの端末2000に伝送する段階(S740)と、ユーザの端末2000が、アクセス認証を実行する段階(S750)と、ユーザの端末2000が、ドア開放信号を生成する段階(S760)と、ユーザの端末2000が、ドア開放信号をアクセス制御デバイス3000に伝送する段階(S770)と、アクセス制御デバイス3000が、ドア開放動作を実行する段階(S780)とを含んでよい。

30

【0332】

本開示のいくつかの実施形態によれば、ユーザの端末2000がサーバ1000からアクセス権情報を要求する段階(S700)が実行され得る。

【0333】

段階S700は、上述した段階S300と同様に実行され、したがって、それらの詳細な説明が省略される。

40

【0334】

段階S700は、必ずしも必要ではなく、いくつかの実施形態に従って省略され得る。

【0335】

また、本開示のいくつかの実施形態によれば、サーバ1000がアクセス権情報をユーザの端末2000に伝送する段階(S710)が実行され得る。

【0336】

段階S710は、上述した段階S310と同様に実行され、したがって、それらの詳細な説明が省略される。

【0337】

50

段階 S 7 1 0 は、必ずしも必要ではなく、いくつかの実施形態に従って省略され得る。

【 0 3 3 8 】

本開示のいくつかの実施形態によれば、ユーザの端末 2 0 0 0 とアクセス制御デバイス 3 0 0 0 との間に通信を確立する段階（ S 7 2 0 ）が実行され得る。

【 0 3 3 9 】

段階 S 7 2 0 は、上述した段階 S 3 2 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

【 0 3 4 0 】

本開示のいくつかの実施形態によれば、アクセス制御デバイス 3 0 0 0 が生体認証情報を受信する段階（ S 7 3 0 ）が実行され得る。

10

【 0 3 4 1 】

段階 S 7 3 0 は、上述した段階 S 6 3 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

【 0 3 4 2 】

本開示のいくつかの実施形態によれば、アクセス制御デバイス 3 0 0 0 が生体認証情報をユーザの端末 2 0 0 0 に伝送する段階（ S 7 4 0 ）が実行され得る。

【 0 3 4 3 】

段階 S 7 4 0 は、上述した段階 S 6 4 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

【 0 3 4 4 】

20

本開示のいくつかの実施形態によれば、ユーザの端末 2 0 0 0 がアクセス認証を実行する段階（ S 7 5 0 ）が実行され得る。

【 0 3 4 5 】

段階 S 7 5 0 は、上述した段階 S 6 5 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

【 0 3 4 6 】

本開示のいくつかの実施形態によれば、ユーザの端末 2 0 0 0 がドア開放信号を生成する段階（ S 7 6 0 ）が実行され得る。

【 0 3 4 7 】

段階 S 7 6 0 は、上述した段階 S 4 5 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

30

【 0 3 4 8 】

本開示のいくつかの実施形態によれば、ユーザの端末 2 0 0 0 がドア開放信号をアクセス制御デバイス 3 0 0 0 （ S 7 7 0 ）に伝送する段階が実行され得る。

【 0 3 4 9 】

段階 S 7 7 0 は、上述した段階 S 4 6 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

【 0 3 5 0 】

また、いくつかの実施形態によれば、アクセス制御デバイス 3 0 0 0 がドア開放動作を実行する段階（ S 7 8 0 ）が実行され得る。

40

【 0 3 5 1 】

段階 S 7 8 0 は、上述した段階 S 4 7 0 と同様に実行され、したがって、それらの詳細な説明が省略される。

【 0 3 5 2 】

生体認証情報を用いた上述のアクセス認証結果管理方法において、図示されていないが、ユーザの端末 2 0 0 0 は、ユーザアクセス認証を実行すべく、ユーザの生体認証情報を取得する段階は、アクセス制御デバイス 3 0 0 0 が生体認証情報を受信する段階（ S 7 3 0 ）、及びアクセス制御デバイス 3 0 0 0 がユーザの端末 2 0 0 0 に生体認証情報を伝送する段階（ S 7 4 0 ）を用いることなく、ユーザの端末 2 0 0 0 がユーザから生体認証情報を受信及び取得することを意味し得る。ユーザの端末 2 0 0 0 は、端末生体認証情報入力

50

ユニット２７００を通じてユーザから生体認証情報を受信してよく、ユーザの生体認証情報を取得してよい。ユーザの生体認証情報は、ユーザの指紋情報、虹彩情報、顔情報、静脈情報及び音声情報のうちの１つを指し得る。例えば、端末生体認証情報入力ユニット２７００がユーザの指紋情報を取得するためのスクリーンスキャナである場合、ユーザの端末２０００は、ユーザの指紋情報を受信及び取得し得る。また、端末生体認証情報入力ユニット２７００が、ユーザの音声情報を取得するためのマイクである場合、ユーザの端末２０００は、ユーザの音声情報を受信及び取得してよい。また、端末生体認証情報入力ユニット２７００が、ユーザの虹彩情報を取得するためのカメラである場合、ユーザの端末２０００は、ユーザの虹彩情報を受信及び取得してよい。

【０３５３】

上述のドア開放管理方法は、図示されていないが、ユーザの端末２０００がアクセス認証結果情報を生成する段階（Ｓ３５０）と、ユーザの端末２０００がアクセス認証結果情報をサーバ１０００に伝送する段階（Ｓ３６０）とが、ユーザの端末２０００がアクセス認証を実行する段階（Ｓ７５０）の後にも実行されてもよい。

【０３５４】

４．アクセス制御デバイスのための設定変更方法

従来のアクセス制御システムでは、アクセス制御デバイスの設定を変更すべく、アクセス制御デバイスと管理サーバとの間のネットワークを確立することを通じて、アクセス制御デバイスの設定を変更する手順が必要であった。結果として、アクセス制御デバイスと管理サーバとの間にネットワークを確立する配線作業に対して、多くの費用及び努力が必要という点で課題が挙げられる。

【０３５５】

図１５は、本開示の実施形態に係るアクセス制御デバイス３０００の設定を変更するための方法に関する周辺図である。

【０３５６】

図１５に示されるように、実施形態に係るアクセス制御デバイス３０００の設定を変更するための方法において、ユーザの端末２０００は、設定変更情報を入力して設定変更信号を生成し、ユーザの端末２０００のユーザがアクセス制御デバイス３０００の設定を変更できるように、無線通信方式でアクセス制御デバイス３０００に設定変更信号を送送する。

【０３５７】

実施形態に係るアクセス制御デバイス３０００のための設定変更方法において、管理サーバは、ユーザの端末２０００が入力を実行して、アクセス制御デバイス３０００の設定を変更し、設定変更信号を生成し、アクセス制御デバイス３０００に設定変更信号を送送するという一連の処理に関与しなくてよい。

【０３５８】

したがって、従来のアクセス制御システムとは異なり、実施形態に係るアクセス制御デバイス３０００のための設定変更方法は、たとえアクセス制御デバイス３０００とネットワーク接続される管理サーバがなかったとしても、ユーザが端末を有する場合、何も問題なく、アクセス制御デバイス３０００の設定を変更できる。

【０３５９】

実施形態に係るアクセス制御デバイス３０００のための設定変更方法の基本的な概念は、以下の様々な実施形態に適用され得る。

【０３６０】

図１６は、本開示の実施形態に係るアクセス制御デバイス３０００の設定を変更するための方法のフローチャートである。ユーザの端末２０００は、アクセス制御デバイス３０００の設定を変更することについての入力を受信し、アクセス制御デバイス３０００に近づき、設定変更信号をアクセス制御デバイス３０００に伝送することにより、アクセス制御デバイス３０００の設定を変更してよい。

【０３６１】

図16を参照すると、アクセス制御デバイス3000の設定を変更するための方法は、ユーザの端末2000が、アクセス制御デバイス3000との通信を確立する段階(S800)と、ユーザの端末2000が、設定変更情報を受信する段階(S810)と、ユーザの端末2000が、管理者情報を受信する段階(S820)と、ユーザの端末2000が、設定変更信号を生成する段階(S830)と、ユーザの端末2000が、設定変更信号をアクセス制御デバイス3000に伝送する段階(S840)と、アクセス制御デバイス3000が、管理者情報をチェックする段階(S850)と、アクセス制御デバイス3000の設定を変更する段階(S860)とを含んでよい。

【0362】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス制御デバイス3000を検出して通信を確立する段階(S800)が実行され得る。

【0363】

ユーザの端末2000は、近くのアクセス制御デバイス3000を検出してよい。例えば、ユーザの端末2000とアクセス制御デバイス3000との間の通信が、BLE通信を通じて実行される場合、ユーザの端末2000は、アクセス制御デバイス3000からアドバタイズ信号を受信し、アクセス制御デバイス3000を検出してよい。ユーザの端末2000が、アクセス制御デバイス3000を検出した後に、ユーザの端末2000は、アクセス制御デバイス3000との通信チャネルを確立してよい。この場合、通信チャネルが確立されると、ユーザの端末2000又はアクセス制御デバイス3000は、外部に通知を出力してよい。

【0364】

この場合、ユーザの端末2000は、最近の接続記録と、アクセス制御デバイス3000からの距離とを収集してよい。

【0365】

ユーザの端末2000とアクセス制御デバイス3000との間の通信は、BLE、Bluetooth(登録商標)、NFC及びWi-Fi(登録商標)などの近距離通信規格に従って実行されてよい。

【0366】

本開示のいくつかの実施形態によれば、ユーザの端末2000が設定変更情報を受信する段階(S810)が実行され得る。

【0367】

ユーザの端末2000は、端末ディスプレイユニット2200を通じて設定変更情報を受信するためのスクリーンを出力してよく、アクセス制御デバイス3000により実行される設定変更のための情報(以下では、設定変更情報と称する)を受信してよい。この場合、ユーザの端末2000は、設定がスクリーン上で変更され得るデバイスのリストを表示してよい。設定が変更されるデバイスが、デバイスのリストから選択された場合、変更される設定項目を含むスクリーンが端末ディスプレイユニット2200上に表示されてよい。

【0368】

ユーザの端末2000は、アクセス制御デバイス3000の通信インタフェース設定を変更するための情報を受信してよい。例えば、アクセス制御デバイス3000は、RS-485規格を用いる場合、ユーザの端末2000は、通信速度などの値を変更するための情報を受信してよい。別の例として、アクセス制御デバイス3000がWiEgand規格を用いる場合、ユーザの端末2000は、例えば、26ビットフォーマットから34ビットフォーマットへWiEgandフォーマットを変更するための情報を受信してよい。

【0369】

また、ユーザの端末2000は、アクセス制御デバイス3000のPIN設定を変更するための情報を受信してよい。例えば、ユーザの端末2000は、PINの桁数を変更するための情報を受信してよい。

【0370】

10

20

30

40

50

また、ユーザの端末 2000 は、ディスプレイユニット 3200 の設定を変更するための情報、又は、アクセス制御デバイス 3000 の音声出力ユニット 3300 を受信してよい。例えば、ユーザの端末 2000 は、アクセス制御デバイス 3000 の LED が、様々な状況に応じて異なる光の色を出力できるように設定を変更するための情報を受信してよい。別の例として、ユーザの端末 2000 は、アクセス制御デバイス 3000 のブザーが様々な状況に応じて異なる音を出力できるように、設定を変更するための情報を受信してよい。

【0371】

また、ユーザの端末 2000 は、アクセス制御デバイス 3000 により認識可能なカードタイプを変更するための情報を受信してよい。例えば、ユーザの端末 2000 は、Wi e g a n d フォーマットからスマートカードフォーマットへ、アクセス制御デバイス 3000 により認識可能なカードタイプを変更するための情報を受信してよい。

10

【0372】

また、ユーザの端末 2000 は、アクセス制御デバイス 3000 において、ユーザアクセス認証に必要な情報を受信してよい。例えば、ユーザの端末 2000 は、アクセス認証に必要であり、かつ、アクセス制御デバイス 3000 に格納される情報を受信してよい。

【0373】

また、ユーザの端末 2000 は、アクセス制御デバイス 3000 のファームウェアを更新するための情報を受信してよい。例えば、ユーザの端末 2000 は、アクセス制御デバイス 3000 に組み込まれるファームウェアを更新するための情報を受信してよい。

20

【0374】

上述したアクセス制御デバイス 3000 の設定変更情報の入力、説明の便宜上の単なる例である。したがって本開示は、それに限定されず、アクセス制御デバイス 3000 の典型的な入力タイプの設定変更情報が利用され得る。

【0375】

本開示のいくつかの実施形態によれば、ユーザの端末 2000 が管理者情報を受信する段階 (S820) が実行され得る。

【0376】

ユーザの端末 2000 は、設定変更権を有するユーザのみが、アクセス制御デバイス 3000 の設定を変更できるように、管理者情報を受信してよい。例えば、管理者情報は、管理者のパスワードであってよく、ユーザの端末 2000 は、6桁のパスワードを受信してよい。

30

【0377】

本開示のいくつかの実施形態によれば、ユーザの端末 2000 が設定変更信号を生成する段階 (S830) が実行され得る。

【0378】

ユーザの端末 2000 は、受信した設定変更情報に基づいて、設定変更信号を生成してよい。設定変更信号がアクセス制御デバイス 3000 に伝送された場合、アクセス制御デバイス 3000 は、設定変更を実行することが認められる。設定変更信号は、アクセス制御デバイス 3000 が設定変更を実行するのに必要なデータを含み得る。また、ユーザの端末 2000 は、受信した管理者情報を含む設定変更信号を生成してよい。

40

【0379】

本開示のいくつかの実施形態によれば、ユーザの端末 2000 が設定変更信号をアクセス制御デバイス 3000 に伝送する段階 (S840) が実行され得る。

【0380】

ユーザの端末 2000 は、設定変更情報に従ってアクセス制御デバイス 3000 の設定を変更するために、管理者情報及び設定変更信号をアクセス制御デバイス 3000 に伝送してよい。

【0381】

例えば、ユーザの端末 2000 とアクセス制御デバイス 3000 との間の通信は、BL

50

E、Bluetooth（登録商標）、NFC及びWi-Fi（登録商標）などの近距離通信規格に従って実行され得る。

【0382】

また、ユーザの端末2000は、受信した管理者情報をアクセス制御デバイス3000に別個に伝送しなくてよいが、受信した管理者情報を含む設定変更信号をアクセス制御デバイス3000に伝送してよい。

【0383】

また、ユーザの端末2000とアクセス制御デバイス3000との間の距離が特定の距離より短い又はそれに等しい場合、ユーザの端末2000は、設定変更信号及び／又は管理者情報をアクセス制御デバイス3000に伝送してよい。また、ユーザの端末2000は、設定変更信号をアクセス制御デバイス3000に伝送してよく、設定変更信号の受信に成功した場合、アクセス制御デバイス3000は、肯定応答信号（ACK）をユーザの端末2000に伝送してよい。また、ユーザの端末2000は、設定変更信号をアクセス制御デバイス3000に伝送してよく、設定変更信号の受信に成功しなかった場合、アクセス制御デバイス3000は、否定応答信号（NACK）を伝送してよい。

【0384】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000が管理者情報をチェックする段階（S850）が実行され得る。

【0385】

アクセス制御デバイス3000は、ユーザの端末2000により受信された管理者情報を受信し、当該管理者情報を、ストレージユニット3500に予め格納された管理者情報と比較して、受信した管理者情報と予め格納された管理者情報とが合致するか否かを判定してよい。例えば、アクセス制御デバイス3000は、ユーザの端末2000により受信された管理者のパスワードを受信し、当該管理者のパスワードをストレージユニット3500に予め格納された管理者のパスワードと比較して、受信した管理者のパスワードと予め格納された管理者のパスワードとが合致するか否かを判定してよい。ユーザの端末2000により受信された管理者情報が、ストレージユニット3500に予め格納された管理者情報と合致しない場合、アクセス制御デバイス3000は、設定変更信号に従って設定を変更しなくてよい。この場合、アクセス制御デバイス3000は、管理者情報がユーザの端末2000と不一致である示す通知メッセージを伝送してよい、又は、外部にアラームを出力してよい。ユーザの端末2000により受信された管理者情報と、ストレージユニット3500に予め格納された管理者情報とが互いに合致する場合、アクセス制御デバイス3000は、設定変更信号に従って設定を変更してよい。この場合、アクセス制御デバイス3000は、管理者情報が合致したことを示す通知メッセージをユーザの端末2000に伝送してよい、又は、外部にアラームを出力してよい。

【0386】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000が設定変更を実行する段階（S860）が実行され得る。

【0387】

ユーザの端末2000により受信された管理者情報と、ストレージユニット3500に予め格納された管理者情報とが互いに合致する場合、アクセス制御デバイス3000は、設定変更信号に従って設定変更を実行してよい。例えば、アクセス制御デバイス3000は、制御ユニット3700を通じて、設定変更情報に対応する設定変更を実行してよい。また、アクセス制御デバイス3000は、設定変更信号に含まれる情報を、制御ユニット3700を通じてストレージユニット3500に格納してよい。

【0388】

図17は、本開示の実施形態に係るアクセス制御デバイス3000において、ユーザの端末2000により取得した生体認証情報を格納するための方法のフローチャートである。ユーザの端末3000は、ユーザの生体認証情報を受信し、アクセス制御デバイス3000に近づき、受信した生体認証情報をアクセス制御デバイス3000に格納してよい。

10

20

30

40

50

【0389】

図17を参照すると、アクセス制御デバイス3000において、ユーザの端末2000により取得した生体認証情報を格納するための方法は、ユーザの端末2000が、アクセス制御デバイス3000との通信を確立する段階(S900)と、ユーザの端末2000が、生体認証情報を取得する段階(S910)と、ユーザの端末2000が、設定変更情報を受信する段階(S920)と、ユーザの端末2000が、管理者情報を受信する段階(S930)と、ユーザの端末2000が、設定変更信号を生成する段階(S940)と、ユーザの端末2000が、設定変更信号をアクセス制御デバイス3000に伝送する段階(S950)と、アクセス制御デバイス3000が、管理者情報をチェックする段階(S960)と、生体認証情報をアクセス制御デバイス3000に格納する段階(S970)とを含んでよい。

10

【0390】

本開示のいくつかの実施形態によれば、ユーザの端末2000がアクセス制御デバイス3000との通信を確立する段階(S900)が実行され得る。

【0391】

段階S900は、上述した段階S800と同様に実行され、したがって、それらの詳細な説明が省略される。

【0392】

本開示のいくつかの実施形態によれば、ユーザの端末2000が生体認証情報を取得する段階(S910)が実行され得る。

20

【0393】

例えば、ユーザの端末2000は、端末生体認証情報入力ユニット2700を通じて、ユーザから生体認証情報を受信することにより、アクセス制御デバイス3000に格納される生体認証情報を取得してよい。端末生体認証情報入力ユニット2700が、ユーザの指紋情報を取得するためのスクリーンキャナである場合、ユーザの端末2000は、ユーザの指紋情報を受信及び取得してよい。また、端末生体認証情報入力ユニット2700が、ユーザの音声情報を取得するためのマイクである場合、ユーザの端末2000は、ユーザの音声情報を受信及び取得してよい。また、端末生体認証情報入力ユニット2700が、ユーザの虹彩情報を取得するためのカメラである場合、ユーザの端末2000は、ユーザの虹彩情報を受信及び取得してよい。

30

【0394】

別の例として、ユーザの端末2000は、サーバ1000から、アクセス制御デバイス3000に格納される生体認証情報を受信及び取得してよい。

【0395】

また、ユーザの端末2000は、取得した生体認証情報を暗号化してよい。例えば、ユーザの端末2000は、アクセス制御デバイス3000のパブリックキーを用いて取得した生体認証情報を暗号化してよい。

【0396】

本開示のいくつかの実施形態によれば、ユーザの端末2000が設定変更情報を受信する段階(S920)が実行され得る。

40

【0397】

また、ユーザの端末2000は、必要な情報を受信して、アクセス制御デバイス3000に生体認証情報を格納してよい。例えば、ユーザの端末2000は、取得した生体認証情報の中から、どの生体認証情報の一部がアクセス制御デバイス3000に格納されるかを判定するのに必要な情報を受信してよい。

【0398】

本開示のいくつかの実施形態によれば、ユーザの端末2000が管理者情報を受信する段階(S930)が実行され得る。

【0399】

段階S930は、上述した段階S820と同様に実行され、したがって、それらの詳細

50

な説明が省略される。

【0400】

本開示のいくつかの実施形態によれば、ユーザの端末2000が設定変更信号を生成する段階(S940)が実行され得る。

【0401】

ユーザの端末2000は、取得した生体認証情報に基づいて、生体認証情報をアクセス制御デバイス3000に格納するために、設定変更信号を生成してよい。また、ユーザの端末2000は、受信した管理者情報及び取得した生体認証情報のうちの少なくとも一方を含む設定変更信号を生成してよい。

【0402】

本開示のいくつかの実施形態によれば、ユーザの端末2000が設定変更信号をアクセス制御デバイス3000に伝送する段階(S950)が実行され得る。

【0403】

ユーザの端末2000は、設定変更情報に従ってアクセス制御デバイス3000の設定を変更するために、管理者情報及び設定変更信号をアクセス制御デバイス3000に伝送してよい。また、ユーザの端末2000は、取得した生体認証情報をアクセス制御デバイス3000に別個に伝送してよい。例えば、ユーザの端末2000とアクセス制御デバイス3000との間の通信は、BLE、Bluetooth（登録商標）、NFC及びWi-Fi（登録商標）などの近距離通信規格に従って実行されてよい。

【0404】

また、ユーザの端末2000は、設定変更信号とは別に、受信した管理者情報及び取得した生体認証情報を伝送しなくてよいが、受信した管理者情報及び取得した生体認証情報のうちの少なくとも一方を含む設定変更信号をアクセス制御デバイス3000に伝送してよい。

【0405】

また、ユーザの端末2000とアクセス制御デバイス3000との間の距離が特定の距離より短い又はそれに等しい場合、ユーザの端末2000は、設定変更信号、管理者情報、及び／又は、生体認証情報をアクセス制御デバイス3000に伝送してよい。

【0406】

また、ユーザの端末2000は、設定変更信号をアクセス制御デバイス3000に伝送してよく、設定変更信号の受信に成功した場合、アクセス制御デバイス3000は、肯定応答信号(ACK)をユーザの端末2000に伝送してよい。また、ユーザの端末2000は、設定変更信号をアクセス制御デバイス3000に伝送してよく、設定変更信号の受信に成功しなかった場合、アクセス制御デバイス3000は、否定応答信号(NACK)を伝送してよい。

【0407】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000が管理者情報をチェックする段階(S960)が実行され得る。

【0408】

段階S960は、上述した段階S850と同様に実行され、したがって、それらの詳細な説明が省略される。

【0409】

本開示のいくつかの実施形態によれば、アクセス制御デバイス3000に生体認証情報を格納する段階(S970)が実行され得る。

【0410】

ユーザの端末2000により受信された管理者情報と、ストレージユニット3500に予め格納された管理者情報とが互いに合致する場合、アクセス制御デバイス3000は、ユーザの端末2000から受信した生体認証情報をストレージユニット3500に格納してよい。

【0411】

この場合、受信した生体認証情報が暗号化されている場合、アクセス制御デバイス 3000 は、暗号化された生体認証情報を復号し、復号した生体認証情報をストレージユニット 3500 に格納してよい。例えば、アクセス制御デバイス 3000 のパブリックキーで暗号化された生体認証情報を含む設定変更信号が、ユーザの端末 2000 から受信された場合、アクセス制御デバイス 3000 は、アクセス制御デバイス 3000 のプライベートキーで生体認証情報を復号し、当該生体認証情報をストレージユニット 3500 に格納してよい。

【0412】

実施形態に係る方法は、様々なコンピュータ手段により実行可能なプログラム命令の形態で実装されてよく、コンピュータ可読媒体に記録されてよい。コンピュータ可読媒体は、プログラム命令、データファイル及びデータ構造などを単独で又は組み合わせで含んでよい。媒体に記録されるプログラム命令は、実施形態に関して、具体的に設計及び構成されてよく、又は、コンピュータソフトウェアの分野における当業者により公知であり、利用可能であってよい。コンピュータ可読記録媒体の例は、ハードディスク、フロッピーディスク及び磁気テープなどの磁気媒体、例えば、コンパクトディスクリードオンリメモリ（CD-ROM）、デジタル多目的ディスク（DVD）などの光媒体、フロッピーディスクなどの磁気-光媒体、及び、特に、プログラム命令を格納及び実行するように構成される、例えば、リードオンリメモリ（ROM）、ランダムアクセスメモリ（RAM）、フラッシュメモリなどのハードウェアデバイスを含む。コンピュータ命令の例は、コンパイラにより生成された機械語コードだけでなく、インタープリタなどを用いてコンピュータにより実行可能な高水準言語コードも含む。ハードウェアデバイスは、実施形態の段階を実行すべく、1又は複数のソフトウェアユニットとして動作するように構成されてよく、逆もまたしかりである。

【0413】

本開示の実施形態によれば、ユーザがアクセス権を有するか否かがユーザの端末を通じて判定されるので、ユーザが別個の認証手段を持ち運ぶ必要がなく、したがって、ユーザの利便性を向上させることが可能である。

【0414】

また、本開示の実施形態によれば、アクセス認証を実行するための情報は、アクセス制御デバイスのストレージユニットに格納されている必要がなく、ユーザの端末又はサーバに格納されてよく、したがって、アクセス制御システムのセキュリティを向上させることが可能である。

【0415】

また、本開示の実施形態によれば、ドアにアクセスされているか否かに関する情報が、ユーザの端末によりサーバに伝送されるので、アクセス制御デバイスとサーバとの間のネットワークングを必要とせず、したがって、関連する費用及び努力を減らすことが可能である。

【0416】

また、本開示の実施形態によれば、配線作業に起因して、アクセス制御デバイスとサーバとの間のネットワークングを通じて、アクセス制御デバイスの設定を変更する手順が必要ではなく、ユーザの端末は、アクセス制御デバイスの設定を直接変更しており、したがって、関連する費用及び努力を減らすことが可能である。

【0417】

また、本開示の実施形態によれば、ユーザがスイッチを押して、ドアにアクセスする場合などにおいて、開放スイッチを押すことにより、ドアを開くことが可能な場合、アクセス認証要求が受信され得る。この場合、ユーザの端末は、アクセス認証を実行し、サーバから定義されたメッセージを受信してよい。したがって、アドバタイズメント又は情報通知をユーザに効果的に提供することが可能である。

【0418】

本発明の有利な効果は、上述した効果に限定されず、本明細書において説明されない他

10

20

30

40

50

の有利な効果が、以下の説明及び添付の図面から当業者により明確に理解される。

【0419】

本開示は、具体的な実施形態及び図面を参照して記載されているが、様々な変更形態及び変更が、当業者による開示から行われ得ることが理解される。例えば、適切な結果が実現され得るが、記載された技術は、上述した順序とは異なって実行され、及び／又は、システム、構造、デバイス又は回路などの記載されたコンポーネントが、上述した及び／又は他のコンポーネント又はそれらの均等物により、置換又は補足されたものとは異なる方式で組み合わせられる。

【0420】

したがって、他の実装、実施形態及び均等物は、以下の特許請求の範囲の範囲内にある。

10

20

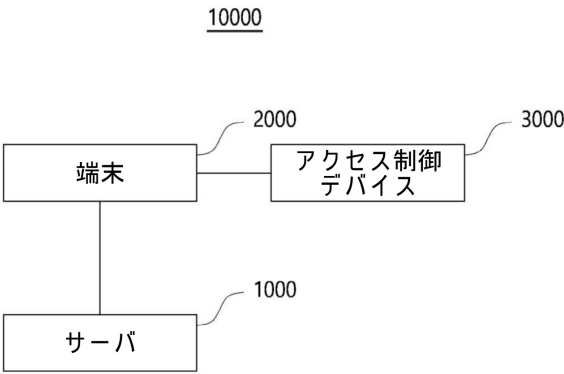
30

40

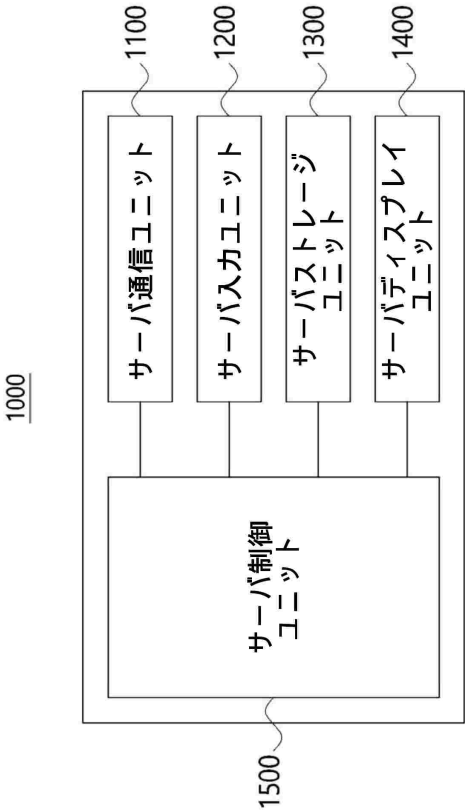
50

【図面】

【図 1】



【図 2】



10

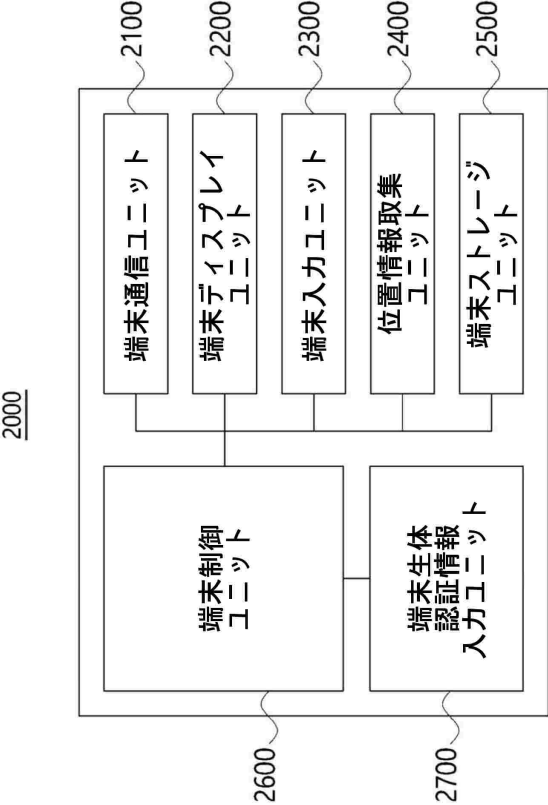
20

30

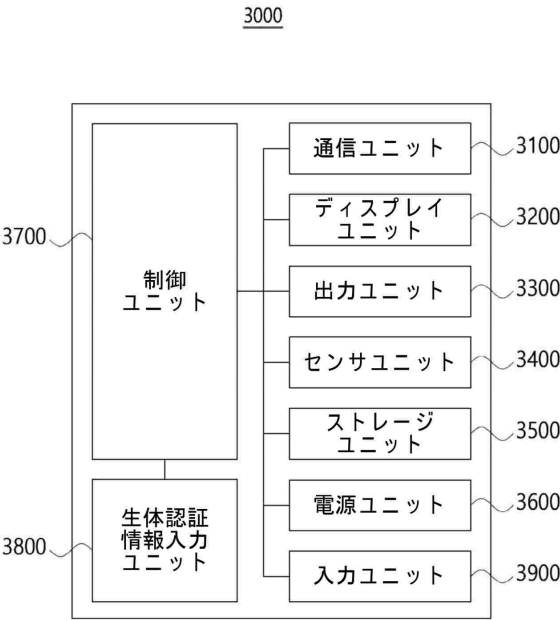
40

50

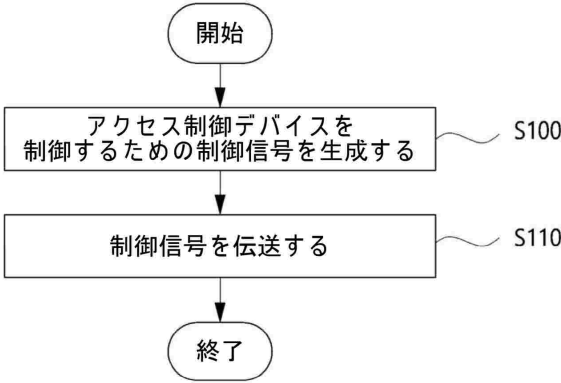
【図 3】



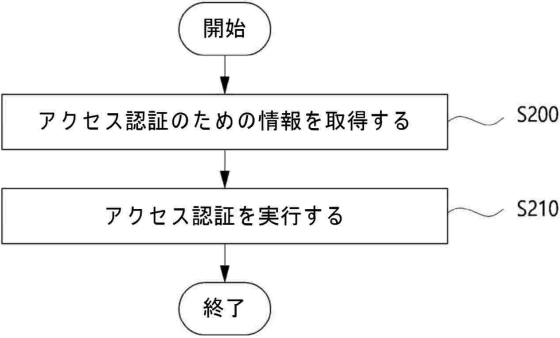
【図 4】



【図 5】



【図 6】



10

20

30

40

50

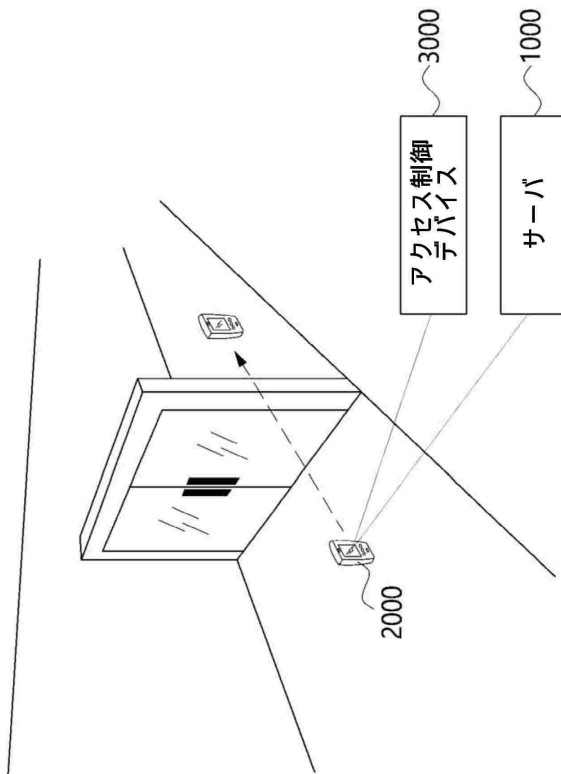
【図 7】

有効期間		
5時間		
ユーザ	A	アクセス スケジュール
端末	a	
生体認証情報	a'	
アクセス権を有する アクセス制御デバイス	1階	09:00~16:00
	2階	00:00~24:00
	4階	09:00~18:00

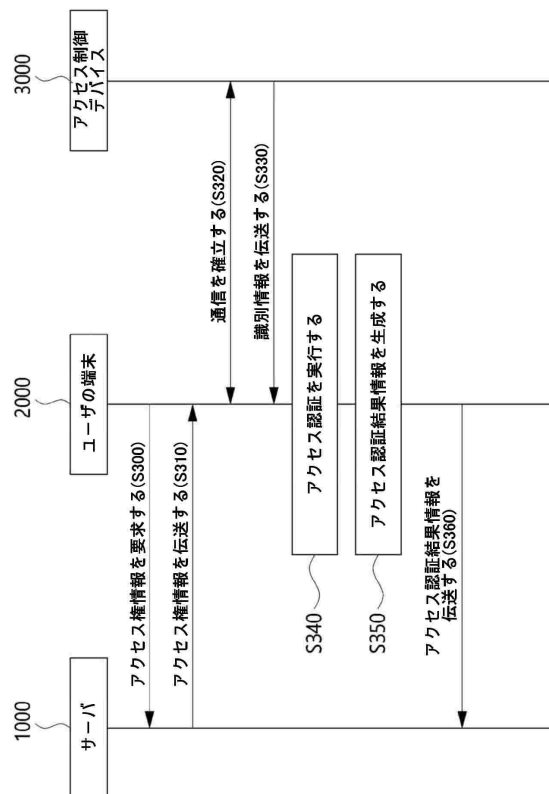
【圖 8】

有効期間							
5時間							
1階				2階			
ユーザ	端末	生体 認証情報	アクセス スケジュール	ユーザ	端末	生体 認証情報	アクセス スケジュール
A	a	a`	09:00-16:00	A	a	a`	00:00-24:00
B	b	b`	09:00-14:00	C	c	c`	09:00-18:00
C	c	c`	08:00-18:00	D	d	d`	08:00-19:00
D	d	d`	12:00-17:00	E	e	e`	17:00-20:00

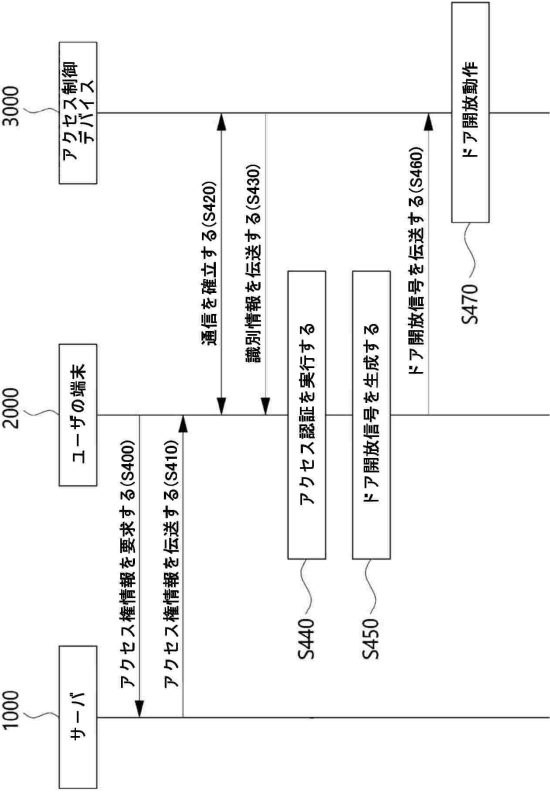
【図 9】



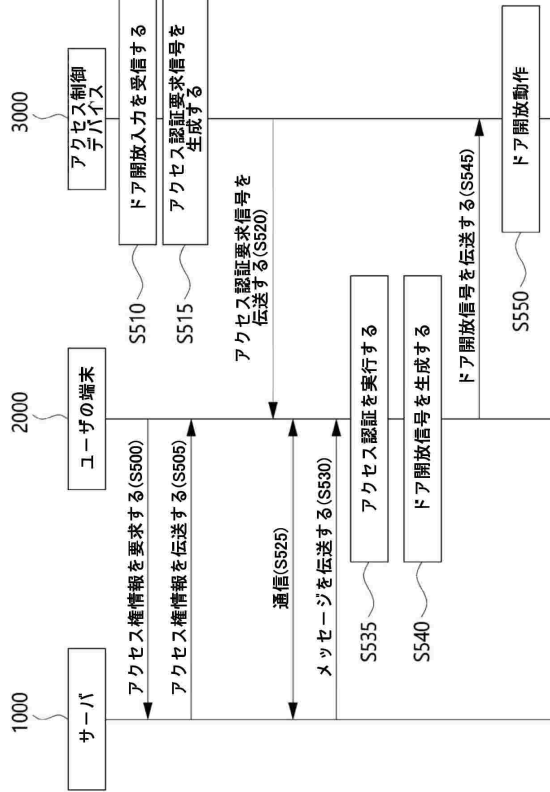
【図 10】



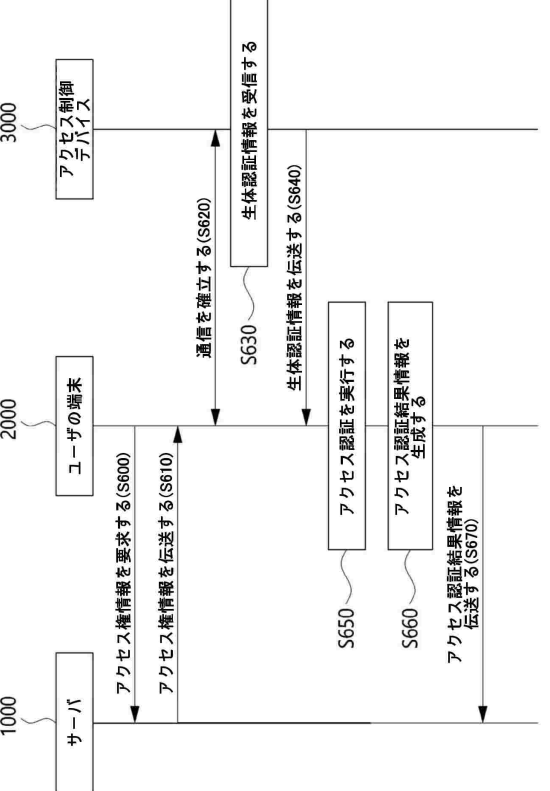
【図 1 1】



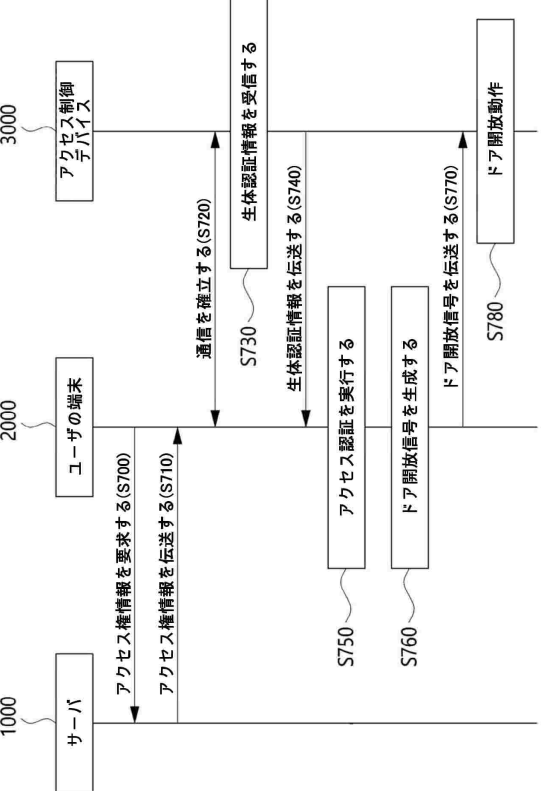
【図 1 2】



【図 1 3】



【図 1 4】



10

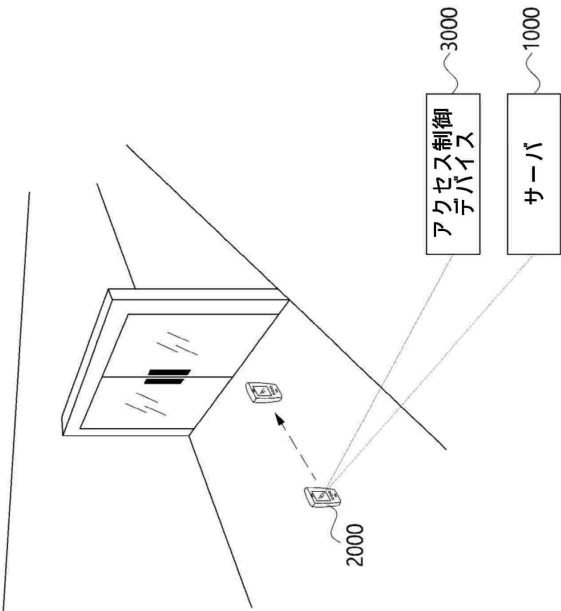
20

30

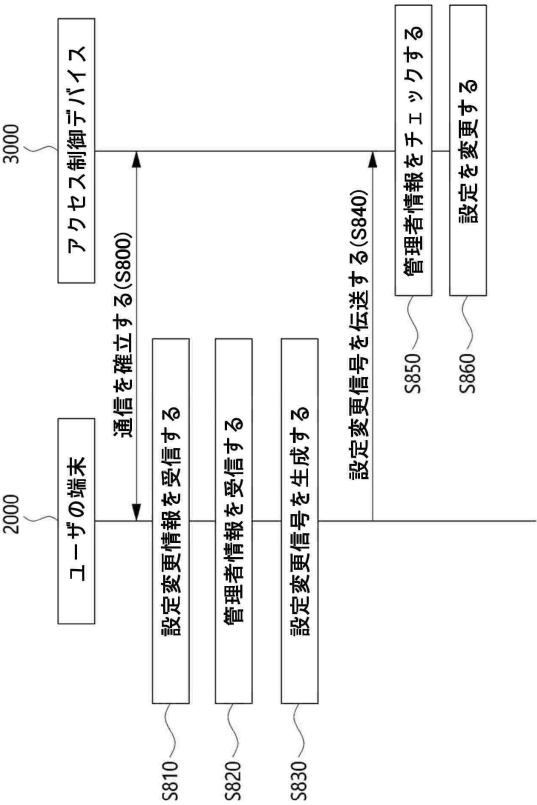
40

50

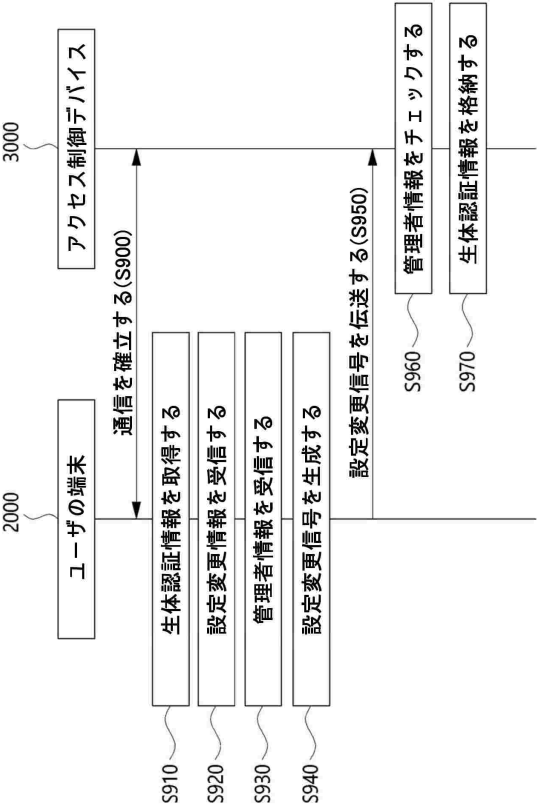
【図 15】



【図 16】



【図 17】



10

20

30

40

50

フロントページの続き

エイルー口、248、#1704 モカ システム インコーポレイテッド内

審査官 上島 拓也

- (56)参考文献 特開2017-106296 (JP, A)
特開2016-079645 (JP, A)
特表2019-508912 (JP, A)
国際公開第2015/146178 (WO, A1)
特開2011-107779 (JP, A)
特開2004-236166 (JP, A)
特開2014-190122 (JP, A)
特開2016-135972 (JP, A)
特開2003-196686 (JP, A)
米国特許出願公開第2016/0260271 (US, A1)
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/33
G06F 21/32