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

特許第6411903号
(P6411903)

(45)発行日　平成30年10月24日(2018.10.24)　(24)登録日　平成30年10月5日(2018.10.5)

(51)Int.Cl.		F I		
G06F 21/35	(2013.01)	G06F	21/35	
H04L 9/32	(2006.01)	H04L	9/00	673B
E05B 49/00	(2006.01)	E05B	49/00	K

請求項の数 2　(全 12 頁)

(21)出願番号　特願2015-11568(P2015-11568)
(22)出願日　平成27年1月23日(2015.1.23)
(65)公開番号　特開2016-136352(P2016-136352A)
(43)公開日　平成28年7月28日(2016.7.28)
審査請求日　平成30年1月9日(2018.1.9)

(73)特許権者　390037028
美和ロック株式会社
東京都港区芝３丁目１番１２号
(74)代理人　100067323
弁理士　西村　教光
(74)代理人　100124268
弁理士　鈴木　典行
(72)発明者　関岡　利泰
東京都港区芝３丁目１番１２号　美和ロック株式会社内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】ゲート制御システム

(57)【特許請求の範囲】
【請求項１】
数ｍ～数十ｍの検知範囲による近距離無線通信を可能とし、管理エリア内に設置されるゲートを制御するゲート制御装置と、
前記検知範囲内に進入したときに前記ゲート制御装置との間で近距離無線通信により認証に必要な認証用ＩＤが送信可能なユーザが所持する携帯端末と、
を備え、
前記ゲート制御装置が前記携帯端末から受信した前記認証用ＩＤを正常認証したときに前記ゲートを制御するゲート制御システムにおいて、
前記認証用ＩＤと、前記認証用ＩＤを暗号化する暗号化用データと、前記暗号化用データを特定する識別データとを含む認証用データが前記携帯端末によって読取可能な形態を成す被読取体が付与された認証用データ取得媒体を用い、
前記携帯端末は、前記認証用データ取得媒体から前記認証用データを取得し、前記検知範囲内に進入したときに前記暗号化用データで暗号化した前記認証用ＩＤと前記識別データとを合わせて前記ゲート制御装置に送信し、
前記ゲート制御装置は、前記携帯端末から送信された前記識別データから前記暗号化用データを特定し、該特定した暗号化用データで前記暗号化された認証用ＩＤを復号化して前記認証用ＩＤが正当であると判断したときに前記ゲートの制御を行うことを特徴とするゲート制御システム。
【請求項２】

数ｍ～数十ｍの検知範囲による近距離無線通信を可能とし、管理エリア内に設置されるゲートを制御するゲート制御装置と、
前記検知範囲内に進入したときに前記ゲート制御装置との間で近距離無線通信により認証に必要な認証用ＩＤが送信可能なユーザが所持する携帯端末と、
を備え、
前記ゲート制御装置が前記携帯端末から受信した前記認証用ＩＤを正常認証したときに前記ゲートを制御するゲート制御システムにおいて、
前記認証用ＩＤと、前記携帯端末と前記ゲート制御装置との間で共有される署名鍵とを含む認証用データが前記携帯端末によって読取可能な形態を成す被読取体が付与された認証用データ取得媒体を用い、
前記携帯端末は、前記認証用データ取得媒体から前記認証用データを取得し、前記検知範囲内に進入したときに、前記認証用ＩＤと、前記署名鍵と前記認証用ＩＤとを基に作成する署名とを合わせて前記ゲート制御装置に送信し、
前記ゲート制御装置は、前記携帯端末から送信された前記署名を前記署名鍵を使って検証し、前記署名と前記認証用ＩＤとが正当であると判断したときに前記ゲートの制御を行うことを特徴とするゲート制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザの電気的操作により管理エリアに設置される各種ゲートを開閉可能な状態又は開扉／閉扉状態にするゲート制御システムに関するものである。
【背景技術】
【０００２】
例えば住宅（戸建、マンション等の集合住宅）や各種施設（ホテルや医療機関等の公共施設、オフィスビルやレンタルオフィス等の商業施設、各種研究を行う研究施設）における共用部又は専有部の出入口に設置される各種ゲートを開閉可能な状態又は開扉／閉扉状態とするため、通常の鍵穴挿入式の金属製鍵に代わり、例えばリモコンキーや非接触式ＩＣカード等のＩＤキーを使ったゲート制御システムが提案されている。
【０００３】
このゲート制御システムは、事前にリーダーに対してＩＤキーを登録し、このＩＤキーとゲートに対応するリーダーとの間で認証用ＩＤ（錠の施解錠やゲートの開閉制御に必要な認証用の情報であり、例えばゲートを特定するゲートＩＤやユーザ個人を特定するユーザＩＤ）の送受信を行い、認証用データの正否判断によってゲートを制御している（例えば、非特許文献１を参照）。
【先行技術文献】
【特許文献】
【０００４】
【非特許文献１】「ＶＥＲＳＡ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌｌｅｒ」、美和ロック株式会社、２０１３年６月版、ｐ．８－９
【発明の概要】
【発明が解決しようとする課題】
【０００５】
近年では、リモコンキーや非接触式ＩＣカード等のＩＤキーの代わりに、各種携帯端末（スマートフォン、フィーチャーフォン、ウェアラブルデバイス）を使い、ハンズフリーでゲートを制御するゲート制御システムが開発されている。このシステムでは、例えばＮＦＣ（Near Field Communication）のような数ｃｍ～数十ｃｍ程度の通信エリアを利用してゲート制御時に携帯端末をリーダーに直接翳してゲートを制御する、所謂「近接モード」と、例えばブルートゥース（登録商標）のような数ｍ～数十ｍ程度の短距離の通信エリアを利用してバッグ等に携帯した状態でリーダーの検知範囲に進入することでゲートの制御が可能な、所謂「ハンズフリーモード」を有している。

【０００６】
また、この種のシステムでは、ＣＰＵのリバースエンジニアリングを防止するため、耐タンパ性を有する部品が使用し、さらに独自の暗号化方式によりＩＤキーとリーダーとの間の通信を保護しているため、通信の傍受による認証用データが漏洩することがなく、安心してシステムを利用することができる。
【０００７】
ところで、ＩＤキーの代わりにユーザが所持する携帯端末を鍵として利用する場合、携帯端末には耐タンパ性が無くリバースエンジニアリングが容易であることから、制御対象となるゲートに対応するリーダーとの間でペアリング操作が必要となる。しかしながら、例えば世帯数が数百となる大規模は集合住宅においてシステムを採用する場合、各世帯のユーザが所持する携帯端末をペアリング操作しなければならずシステム提供者がペアリング処理を実施することは現実的ではない。
【０００８】
そのため、ユーザ個々の携帯端末を認証キーとして利用する場合、ユーザが各自で使用するゲートのリーダーとペアリング操作を行う必要があるが、携帯端末の操作に関する知識の乏しいユーザがいる場合も考えられるため、全てのユーザが容易にペアリング操作可能なシステムの導入が望まれている。
【０００９】
そこで、本発明は上記問題点に鑑みてなされたものであり、制御対象となるゲートを制御するゲート制御装置とユーザが所持する携帯端末とのペアリング操作を行わずとも高いセキュリティ性を保った状態で近距離無線通信によるゲートの制御を可能とするゲート制御システムを提供することを目的とするものである。
【課題を解決するための手段】
【００１０】
上記した目的を達成するために、請求項１記載のゲート制御システムは、数ｍ～数十ｍの検知範囲による近距離無線通信を可能とし、管理エリア内に設置されるゲートを制御するゲート制御装置と、
前記検知範囲内に進入したときに前記ゲート制御装置との間で近距離無線通信により認証に必要な認証用ＩＤが送信可能なユーザが所持する携帯端末と、
を備え、
前記ゲート制御装置が前記携帯端末から受信した前記認証用ＩＤを正常認証したときに前記ゲートを制御するゲート制御システムにおいて、
前記認証用ＩＤと、前記認証用ＩＤを暗号化する暗号化用データと、前記暗号化用データを特定する識別データとを含む認証用データが前記携帯端末によって読取可能な形態を成す被読取体が付与された認証用データ取得媒体を用い、
前記携帯端末は、前記認証用データ取得媒体から前記認証用データを取得し、前記検知範囲内に進入したときに前記暗号化用データで暗号化した前記認証用ＩＤと前記識別データとを合わせて前記ゲート制御装置に送信し、
前記ゲート制御装置は、前記携帯端末から送信された前記識別データから前記暗号化用データを特定し、該特定した暗号化用データで前記暗号化された認証用ＩＤを復号化して前記認証用ＩＤが正当であると判断したときに前記ゲートの制御を行うことを特徴とする。
【００１１】
請求項２記載のゲート制御システムは、数ｍ～数十ｍの検知範囲による近距離無線通信を可能とし、管理エリア内に設置されるゲートを制御するゲート制御装置と、
前記検知範囲内に進入したときに前記ゲート制御装置との間で近距離無線通信により認証に必要な認証用ＩＤが送信可能なユーザが所持する携帯端末と、
を備え、
前記ゲート制御装置が前記携帯端末から受信した前記認証用ＩＤを正常認証したときに前記ゲートを制御するゲート制御システムにおいて、

前記認証用ＩＤと、前記携帯端末と前記ゲート制御装置との間で共有される署名鍵とを含む認証用データが前記携帯端末によって読取可能な形態を成す被読取体が付与された認証用データ取得媒体を用い、

前記携帯端末は、前記認証用データ取得媒体から前記認証用データを取得し、前記検知範囲内に進入したときに、前記認証用ＩＤと、前記署名鍵と前記認証用ＩＤとを基に作成する署名とを合わせて前記ゲート制御装置に送信し、

前記ゲート制御装置は、前記携帯端末から送信された前記署名を前記署名鍵を使って検証し、前記署名と前記認証用ＩＤとが正当であると判断したときに前記ゲートの制御を行うことを特徴とする。

【発明の効果】

【００１２】

本発明の発明によれば、ユーザが所持する携帯端末を認証キーとして利用し、携帯端末と管理エリア内に設置された各ゲートに対応するゲート制御装置との間でペアリング操作を行わずとも、ユーザは認証用データ取得媒体から認証用データを取得するだけで、携帯端末とゲート制御装置をペアリング操作した状態と同様のセキュリティ性を確保した状態でゲート制御に必要な各種データの通信を行うことができる。

【図面の簡単な説明】

【００１３】

【図１】本発明に係るゲート制御システムの構成を示す概略ブロック図である。

【図２】本発明に係るゲート制御システムの他の構成例を示す概略ブロック図である。

【発明を実施するための形態】

【００１４】

以下、本発明を実施するための形態について、添付した図面を参照しながら詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではなく、この形態に基づいて当業者等によりなされる実施可能な他の形態、実施例及び運用技術等は全て本発明の範疇に含まれる。

【００１５】

［システム構成について］

まず、本発明に係るゲート制御システムの構成について説明する。

図１に示すように、ゲート制御システム１は、ゲートの制御時に認証キーとして使用されるユーザが所持する携帯端末１０と、管理対象となる管理エリア内における共用部や専有部のゲート４０又はゲート４０近傍に設けられるゲート制御装置２０と、携帯端末１０がゲート制御装置２０との間で通信される認証用ＩＤ（例えばユーザを特定するユーザＩＤやゲートを特定するゲートＩＤ）を含む認証用データを取得するための認証用データデータ取得媒体３０とで概略構成される。

【００１６】

本発明のゲート制御システム１における「管理エリア」とは、例えば住宅（戸建、マンション等の集合住宅）や各種施設（ホテルや医療機関等の公共施設、オフィスビルやレンタルオフィス等の商業施設、各種研究を行う研究施設）を含む建物、この種の建物内で分割されたエリア（階数によるエリア分割や同フロア内における分割は問わない）、複数棟からなる建物群、建物とその周辺施設を含むエリアのような、管理業者（管理形態は単独の管理業者による管理、分割された各エリアに応じて複数の管理業者が混在する場合も含む）が管理対象とするエリアである。

【００１７】

また、図１に示すように、管理エリア内には、ユーザが所持する携帯端末１０の電気的操作によって制御対象であるゲート４０（ユーザ自身が操作する開き戸、引き戸、折り戸等の一般的な扉の他、ユーザの移動や操作に伴って連動する自動ドア、回転ドア、自動改札機や入退出管理ゲートのような開閉体も含む）を開閉可能な状態若しくは開扉／閉扉するゲート制御装置２０が複数箇所に設置される。

【００１８】

なお、本例のゲート制御システム１の運用モードとして、例えばＮＦＣ（Near Field Communication）のような通信範囲が数ｃｍ～数十ｃｍ程度の極短距離の通信エリアを利用し、ゲート制御時に携帯端末１０をゲート制御装置２０の情報通信部２１に翳す（近接させる）ことでゲートを制御する「近接モード」と、例えばブルートゥース（登録商標）のような数ｍ～数十ｍ程度の短距離の通信エリアを利用してユーザが所持するバッグ等に携帯端末１０を携帯した状態でゲート制御装置２０の検知範囲内に進入することでゲートの制御を行う「ハンズフリーモード」を有する。また、各モードは、ユーザ各自が利便性を考慮して選択可能となっている。

【００１９】

＜携帯端末について＞

携帯端末１０は、ユーザが所持する各種携帯型通信端末（例えば携帯電話、スマートフォン、ウェアラブルデバイス等）であり、近距離無線通信部１１と、キー制御部１２と、キー記憶部１３と、表示部１４と、入力操作部１５と、データ取得部１６とを備えている。

【００２０】

携帯端末１０は、一般的な携帯型通信端末の機能（例えば、電話機能、メール機能、各種コンピュータネットワークを用いた通信機能、カメラ機能）を有する他、キー記憶部１３に記憶されるゲート制御用のアプリケーションプログラム（ゲート制御アプリ）が起動することで携帯端末１０がゲート制御用の認証キーとして機能する。

【００２１】

近距離無線通信部１１は、ゲート制御装置２０との間で通信状態が確立すると、近距離無線通信（Near Field Communication：ＮＦＣ）を用いてゲート制御に必要な各種データの通信を行う。そのため、例えばＭｉＦａｒｅ（ＩＳＯ／ＩＥＣ　１４４４３）やＦｅｌｉＣａ（ＩＳＯ／ＩＥＣ　１５４０８）等の電磁界や電波を用いて数ｃｍ程度の距離で無線通信可能とするＲＦＩＤタグ（Radio Frequency Identification Tag）や、ブルートゥース（登録商標）等の数ｍ～数十ｍの距離で無線通信可能とするモジュール等の各種近距離無線デバイスで構成されている。

【００２２】

なお、近距離無線デバイスとして機能するＲＦＩＤタグには、複数の電子素子が乗った回路基板で構成されるものに加え、近年実用化されている小さなワンチップのＩＣ（集積回路）で構成されたＩＣタグも含まれる。また、近距離無線通信の仕様としては、パッシブタイプ（受動タイプ）、アクティブタイプ（能動タイプ）、パッシブタイプ及びアクティブタイプの双方を組み合わせたセミアクティブタイプ（起動型能動タイプ）を問わない。

【００２３】

キー制御部１２は、例えばＣＰＵ（Central Processing Unit ）やＲＯＭ（Read Only Memory），ＲＡＭ（Random Access Memory）又はこれらの機能を具備するＭＰＵ（Micro-Processing Unit ）等のプロセッサで構成され、通常の携帯型通信端末として機能するようにキー記憶部１３に記憶される各種駆動制御プログラムを実行するとともに、キー記憶部１３に記憶されるゲート制御アプリの処理シーケンスに従って、携帯端末１０を認証キーとして機能させるように携帯端末１０を構成する各部の駆動制御を行う。

【００２４】

ゲート制御アプリの起動によるキー制御部１２の処理内容としては、ゲート制御装置２０との間で近距離無線通信が行えるようにゲート制御装置２０からの呼び掛け信号に対する応答信号を送信してゲート制御装置２０との間で通信状態を確立する処理、通信状態確立後にゲート制御装置２０から送信されたデータ要求信号に対する応答として認証用データ取得媒体３０から取得した認証用データに含まれる暗号化用データを用いて認証用ＩＤとゲート制御装置２０からデータ要求信号とともに送信される後述する不正防止データとを暗号化する処理、暗号化した認証用ＩＤ及び不正防止データと暗号化データを特定する識別データとを認証制御データとしてゲート制御装置２０に送信する処理がある。

【００２５】
なお、本例のシステムにおいて、ゲート制御アプリは、ゲート制御装置２０から送信された呼び掛け信号の受信をトリガとして起動する構成とするが、バックグラウンドで常時起動する構成やユーザが使用の都度起動する構成としてもよい。
【００２６】
キー記憶部１３は、例えばＥＥＰＲＯＭやフラッシュメモリ等の不揮発性メモリやＤＲＡＭやＳＤＲＡＭ等の揮発性メモリを含む各種半導体メモリで構成され、携帯端末１０を通常の携帯型通信端末としての機能させるために必要な各種駆動制プログラムを記憶している。
【００２７】
また、キー記憶部１３には、携帯端末１０に具備されるキー制御部１２（コンピュータ）に対し、ゲート制御システム１を使用する上で必要なゲート制御処理シーケンスを実行させるためのゲート制御アプリが記憶（インストール）されている。
【００２８】
表示部１４は、例えば液晶ディスプレイ（Liquid Crystal Display：ＬＣＤ）やＥＬディスプレイ（electroluminescence display ：ＥＬＤ）や等の表示領域を有するディスプレイ装置で構成され、キー制御部１２の制御により、ゲート制御アプリの駆動に伴って連動表示される表示内容の他、携帯端末１０の駆動に必要な各種表示内容を表示領域上に表示している。
【００２９】
入力操作部１５は、例えばテンキーや選択ボタン等の操作キー、表示部１４の表示画面上のソフトキーからなるタッチパネル等のＵＩ（User Interface）等の各種入力機器で構成され、例えば認証用データ取得媒体３０から認証用データを取得するときや運用モードの選択設定するとき等に所定操作されると、この操作内容に応じた操作情報をキー制御部１２に出力している。
【００３０】
データ取得部１６は、例えば携帯端末１０に搭載されるカメラ機能や非接触通信機能を利用して認証用データ取得媒体３０に付与される被読取体３０ａから認証用データを取得する。つまり、データ取得部１６は、認証用データ取得媒体３０に付与される被読取体３０ａの形態に応じて携帯端末１０の機能を適宜選択されることになる。例えば被読取体３０ａがＱＲコード（登録商標）のような情報識別子である場合は携帯端末１０に搭載されるカメラを識別子読取手段として機能させ、被読取体３０ａが非接触型ＩＣチップであれば、近距離無線通信部１１の非接触通信機能（ＮＦＣによる通信機能）を非接触通信手段として機能させる。
【００３１】
＜ゲート制御装置について＞
ゲート制御装置２０は、図１に示すように、情報通信部２１と、ゲート側制御部２２と、ゲート側記憶部２３と、ゲート駆動機構２４と、電源部２５とを備えている。ゲート制御装置２０は、管理エリア内においてユーザが出入する各種ゲート４０に設けられた駆動対象となるゲート４０の開閉に係る制御を行う装置である。
なお、ゲート制御装置２０の設置数は、単数又は複数の何れでもよく、また装置形態としては、スタンドアロン型又は不図示の管理装置との間で通信可能（接続方法は有線・無線を問わない）に接続され管理されるネットワーク接続型の何れでもよい。
【００３２】
情報通信部２１は、各種近距離無線通信（ＮＦＣ、ブルートゥース（登録商標）等）を利用して携帯端末１０との間で各種情報の送受信が可能なリーダーとして機能する各種通信機器で構成され、制御対象となる対応する各ゲート４０の近傍又はゲート４０の所定箇所に設置される。情報通信部２１は、携帯端末１０との間で通信状態を確立させるため、一定周期で所定の通信範囲内に近接する携帯端末１０に対してポーリングを行っており、携帯端末１０が通信範囲内に近接した際にゲート制御アプリを起動させる呼び掛け（呼び

掛け信号の送信）を行っている。

【００３３】

また、情報通信部２１は、携帯端末１０との間で通信状態が確立すると、リプレイ攻撃による不正を防止するため、ゲート側制御部２２で作成した不正防止データ（例えばｎｏｎｃｅのような使い捨てのランダム値、通し番号、日時情報）をデータ要求信号とセットにして携帯端末１０に送信する。さらに、情報通信部２１は、送信したデータ要求信号に対する応答として認証制御データ（暗号化された認証用ＩＤ＋暗号化された不正防止データ＋識別データ）を受け取ると、この受け取った認証制御データをゲート側制御部２２に出力する。

【００３４】

なお、情報通信部２１は、携帯端末１０との間の通信を行う方法として上記のような所定周期でポーリングを行う方法の他、省電力化を図る目的として通信の意思を確認するため、ゲート制御装置２０の所定箇所に設けた不図示の操作ボタンが操作されたときにのみ通信を行う構成とすることもできる。

【００３５】

ゲート側制御部２２は、例えばＣＰＵ（Central Processing Unit ）やＲＯＭ（Read Only Memory），ＲＡＭ（Random Access Memory）又はこれらの機能を具備するＭＰＵ（Micro-Processing Unit ）等のプロセッサで構成され、ゲート制御装置２０を構成する各部の駆動制御や電源供給制御を行っている。

【００３６】

ゲート側制御部２２が実施するゲート制御処理としては、情報通信部２１の検知範囲内に進入した携帯端末１０に対して通信を確立させるために呼び掛け信号を送信する処理と、データ要求信号とセットで送信する不正防止データを作成する処理と、呼び掛け信号を送信した携帯端末１０からの応答信号を確認したときにデータ要求信号と作成した不正防止データとをセットで携帯端末１０に送信する処理と、認証制御データに含まれる識別データとゲート側記憶部２３に記憶されるデータ特定情報とを照合して暗号化用データを特定する処理と、携帯端末１０から受け取った認証制御データに含まれる暗号化された識別用ＩＤ及び不正防止データを前記処理で特定した暗号化用データで復号化する処理と、復号化した不正防止データが過去に送信した不正防止データと一致するか否かを判断する処理と、不正防止データが過去のものと一致したときにゲート制御データが不正であると判断してゲート制御を終了する処理と、不正防止データが過去のものと異なるときは識別用ＩＤとゲート側記憶部２３に記憶される識別用ＩＤとを照合し、識別用ＩＤが正常に認証された場合にのみ、現在の錠前やゲート４０の状態に応じたゲート制御信号をゲート駆動機構２４に送信する処理を適宜行っている。なお、上記処理に関する一連の処理手順については、後述する処理動作の項において説明する。

【００３７】

ゲート側記憶部２３は、例えばＥＥＰＲＯＭやフラッシュメモリ等の不揮発性メモリやＤＲＡＭやＳＤＲＡＭ等の揮発性メモリを含む各種半導体メモリ、ＨＤＤ等の各種記憶装置で構成される。

【００３８】

ゲート側記憶部２３は、認証用ＩＤ及び不正防止データを暗号化するための暗号化用データと、各暗号化データを特定する識別データと、認証用ＩＤとが関連付けされた状態でテーブル化されたデータ特定情報の他、ゲート制御装置２０を構成する各部の駆動制御プログラムを記憶している。またゲート側記憶部２３は、リプレイ攻撃による不正アクセスを防止するため、携帯端末１０に送信した過去の不正防止データを記憶している。

【００３９】

なお、ゲート側記憶部２３は、必要に応じて、モニタ情報としての状態信号（ゲート４０の開閉状態信号や錠前の施解錠状態信号、施解錠操作履歴）等の各種データを記憶するようにしてもよい。

【００４０】

ゲート駆動機構２４は、ゲート側制御部２２からのゲート制御信号に応じて、制御対象となるゲート４０の制御盤４１に駆動信号を出力してゲート４０を開扉状態又は閉扉状態としたりゲート４０を開扉又は閉扉可能な状態にしたりする機構である。

【００４１】

ゲート駆動機構２４の具体的な形態例としては、ゲート４０に設けられたモータやソレノイド等の駆動装置と錠前で構成し扉枠の係止穴に対してデッドボルトを突出（施錠時）又は引き込む（解錠時）ことで錠前を施錠又は解錠してゲート４０を開扉又は閉扉可能な状態とする形態、ゲート４０の開閉時に操作されるハンドルやノブをロック状態から開扉操作可能な状態とする形態、扉枠の電気式ストライクを駆動制御してゲート４０を開閉可能な状態とする形態、既存のメカ式サムターンを電気的に回動させる後付け式の錠装置においてサムターンを施錠／解錠操作方向に回動して錠前を施解錠することでゲート４０を開扉又は閉扉可能な状態とする形態、電動サムターンを施錠／解錠操作方向に回動して錠前の施解錠を行うことでゲート４０を開扉又は閉扉状態とする形態等がある。

【００４２】

電源部２５は、一般的な商用電源ユニット、ボタン電池や乾電池（一次電池、二次電池を問わず）等の各種電池が着脱交換可能な電源ユニット若しくは光起電力効果を利用して太陽光や照明光等の光エネルギーを直接電力に変換する光電池モジュールの何れかで構成され、ゲート制御装置２０を構成する各部の駆動電源を適宜供給している。

【００４３】

＜認証用データ取得媒体について＞

認証用データ取得媒体３０は、ゲート制御システム１を運用する管理業者からユーザに対して譲渡されるカード状媒体や紙であり、携帯端末１０に取得される認証用データが読取可能な形態を成す被読取体３０ａが付与されている。この認証用データには、暗号化データと、この暗号化データを特定する識別データと、認証用ＩＤとが含まれている。

【００４４】

被読取体３０ａの形態としては、例えば一次元コード（バーコード）や二次元コード（ＱＲコード（登録商標））、カラードットのような情報識別子、ＲＦＩＤチップ等があり、形態に応じて媒体自体に印刷したり、シール体として媒体表面に貼着したり、チップとして媒体に内蔵して付与されている。

【００４５】

［処理動作について］

次に、上述したゲート制御システム１における一連の処理動作について説明する。

ここでは、管理エリアをマンションとし、ハンズフリーモードによって携帯端末１０が保持するゲートＩＤで共用エントランスのゲート４０を制御する際の処理動作である。

【００４６】

まず、ユーザは、携帯端末１０を所定操作して管理業者から譲渡された認証用データ取得媒体３０の被読取体３０ａから認証用データを取得する。これにより、携帯端末１０に認証用データが保存される。

【００４７】

次に、ユーザは、携帯端末１０を所持した状態でゲート制御装置２０の通信範囲内に進入すると、携帯端末１０がゲート制御装置２０からの呼び掛け信号を受信する。この呼び掛け信号への応答として応答信号をゲート制御装置２０に送信し、携帯端末１０とゲート制御装置２０との間で近距離無線通信が確立する。

【００４８】

次に、ゲート制御装置２０は、呼び掛け信号を送信した携帯端末１０からの応答信号を確認すると、この携帯端末１０に対して認証用データを要求するデータ要求信号を不正防止データとセットで送信する。次に、携帯端末１０は、ゲート制御装置２０からのデータ要求信号に対する応答としてゲート制御装置２０に認証制御データを送信する。

【００４９】

次に、ゲート制御装置２０は、認証制御データに含まれる暗号化された認証用ＩＤを復

号化するため、受け取った認証制御データに含まれる識別データとゲート側記憶部２３に記憶されるデータ特定情報とを照合して暗号化用データを特定する。そして、認証制御データに含まれる暗号化された認証用ＩＤと不正防止データを復号化し、この不正防止データがゲート側記憶部２３に記憶される過去の不正防止データと一致するか否かを判断する。

【００５０】

このとき、不正防止データが一致する場合は、認証制御データが傍受され不正アクセスされていると判断して処理を終了する。

一方、不正防止データが異なる場合は、認証制御データは正常に送信されたものと判断し、認証用ＩＤとゲート側記憶部２３に記憶されるデータ特定情報とを照合し、受け取った認証用ＩＤが正常に認証された場合にのみ、現在の錠前やゲート４０の状態に応じたゲート制御信号をゲート駆動機構２４に送信する。

【００５１】

そして、ゲート駆動機構２４は、入力したゲート制御信号に従って制御対象とするゲート４０の制御盤４１に駆動信号を出力してゲート４０の駆動を制御する。

【００５２】

以上説明したように、上述したゲート制御システム１は、携帯端末１０が認証用データ取得媒体３０から認証用データを取得し、この認証用データに含まれる暗号化用データを用いて認証用ＩＤとゲート制御装置２０から送信される不正防止データとを暗号化し、これらを認証制御データとしてゲート制御装置２０に送信する。ゲート制御装置２０は、受信した認証制御データに含まれる識別データから暗号化に使用した暗号化用データを特定する。

次に、特定した暗号化用データで暗号化された認証用ＩＤと不正防止データを復号化し、認証用ＩＤの正当性及び不正防止データの確認を行い、認証用ＩＤ及び不正防止データが共に正常であると判断したときに、ゲート駆動機構２４を駆動制御して制御対象であるゲート４０を所定の状態に制御している。

【００５３】

これにより、管理業者から譲渡された認証用データ取得媒体３０に付与される被読取体３０ａから携帯端末１０に認証用データを保存させるという作業のみで携帯端末１０とゲート制御装置２０との間で共有する暗号化用データを用いて暗号化の対象となるデータ（認証用ＩＤや不正防止データ）を暗号化した状態で通信することができるので、ペアリングと同等のセキュリティ性を確保することができる。

【００５４】

また、携帯端末１０とゲート制御装置２０との間で通信状態が確立したときに、データ要求信号とともに不正防止データをゲート制御装置２０から携帯端末１０に送信し、ゲート制御データにこの不正防止データを暗号化した状態でゲート制御装置２０に返信することで、傍受されたゲート制御データによるリプレイ攻撃を防止することができる。

【００５５】

［その他の実施形態について］

なお、本発明は上記各実施形態に限定されるものではなく、例えば以下に示すように使用環境などに応じて適宜変更して実施することもできる。また、以下の変更例を本発明の要旨を逸脱しない範囲の中で任意に組み合わせて実施することもできる。

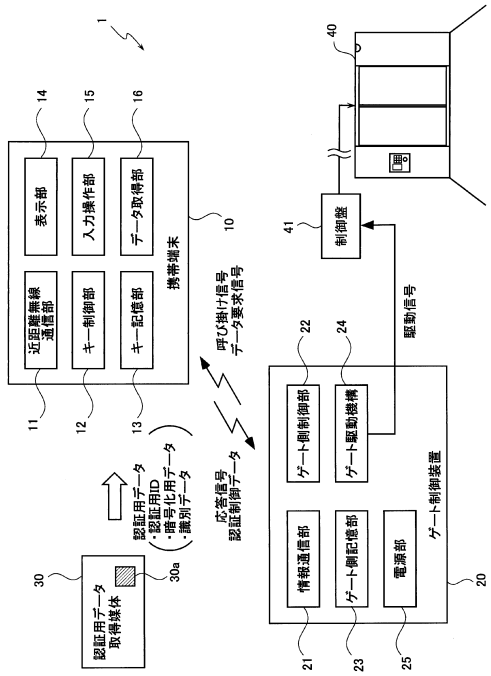
【００５６】

上述した形態では、認証用データ取得媒体３０から認証用ＩＤと暗号化用データと識別データを取得して認証用ＩＤと不正防止データとを暗号化したものに識別データを付与したものを認証制御データとしてゲート制御装置２０に送信する構成で説明したが、これに限定されることはない。つまり、本システムの目的である携帯端末１０とゲート制御装置２０との間でセキュリティ性が保たれリバースエンジニアリングによって暗号化用データなどの漏洩を防止することができればよいため、例えば下記に示すようなシステム構成とすることができる。

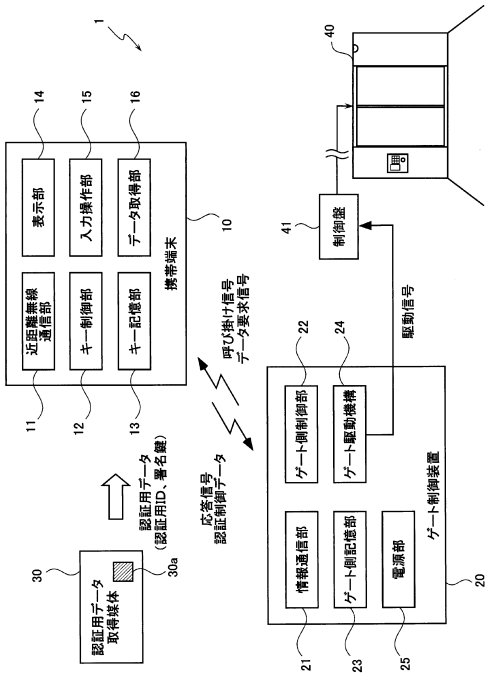
【００５７】
ここで、本例のゲート制御システムにおける他の構成例について図２を参照しながら説明する。なお、ここでは、上述したシステム構成を同様の構成についてはその説明を省略し、図２に示す形態において特徴となる構成要件及び処理内容についてのみ説明する。
【００５８】
本システムの他の形態例としては、携帯端末１０が認証用データ取得媒体３０から認証用ＩＤと署名の作成に用いる署名鍵を取得し、ゲート制御装置２０は、事前に署名鍵と認証用ＩＤとをペアで記憶する。つまり、携帯端末１０とゲート制御装置２０との間で署名鍵が共有化されていることが前提となる。
【００５９】
携帯端末１０は、認証用ＩＤと不正防止データと署名鍵とを用いて署名を作成（なお、署名を作成するにあたり、少なくとも認証用ＩＤと署名鍵を用いて署名を作成すればよい）し、認証用ＩＤと不正防止データと署名を合わせてゲート制御装置２０に送信する。
【００６０】
ゲート制御装置２０は、受信した署名を共有する署名鍵を用いて検証し、署名の正当性を確認すると、受信したデータ（認証用ＩＤや不正防止データ）が正当性を有する場合にのみゲートを所定の状態に制御する。また、データ要求信号を送信する際に、リプレイ攻撃を防止するための不正防止データも携帯端末１０に送信する。
【００６１】
このシステム構成による処理手順としては、まず携帯端末１０とゲート制御装置２０との間で通信を確立させ、携帯端末１０に対してゲート制御装置２０からデータ要求信号と不正防止データを送信する。携帯端末１０は、認証用データ取得媒体３０から取得した認証用ＩＤと不正防止データと秘密鍵とから署名を作成し、この作成した署名と、認証用ＩＤと、不正防止データとを合わせて認証制御データとしてゲート制御装置２０に送信する。
【００６２】
ゲート制御装置２０は、自身が記憶する署名鍵を用いて受信した認証制御データに付与される署名の検証を行い、検証した結果、受信した署名と検証時に作成した署名とが一致したときに正常なデータであると確認して認証用ＩＤの正当性や不正防止データの正当性の有無を判断してゲートの制御を行う。
【００６３】
以上のように、携帯端末１０とゲート制御装置２０との間で署名鍵を共有しておくことで署名の作成と検証が行えるため、ゲート制御装置２０の記憶領域が少なく上述した形態のようにデータ特定情報を記憶する容量が確保できないような場合であっても、通信のセキュリティ性を確保してリバースエンジニアリングによる情報漏洩を防止することができる。
【符号の説明】
【００６４】
１…ゲート制御システム
１０…携帯端末
１１…近距離無線通信部
１２…キー制御部
１３…キー記憶部
２０…ゲート制御装置
２１…情報通信部
２２…ゲート側制御部
２３…ゲート側記憶部
２４…ゲート駆動機構
２５…電源部
３０…認証用データ取得媒体（３０ａ…被読取体）

４０…ゲート
４１…制御盤

【図１】



【図２】



フロントページの続き

(56)参考文献 特開２００４－２７２５６８（ＪＰ，Ａ）
特開２００６－２５７８１５（ＪＰ，Ａ）
国際公開第２００５／０５７４４７（WO，Ａ１）
特開２００５－３５０９２６（ＪＰ，Ａ）
特開２００６－００９３３３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３５
Ｅ０５Ｂ　４９／００
Ｈ０４Ｌ　９／３２