

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-40125

(P2017-40125A)

(43) 公開日 平成29年2月23日(2017.2.23)

(51) Int.Cl.
E05B 49/00 (2006.01)

F I
E O 5 B 49/00

テーマコード(参考)
2 E 2 5 0

審査請求 未請求 請求項の数 3 O L (全 20 頁)

(21) 出願番号 特願2015-163166 (P2015-163166)
(22) 出願日 平成27年8月20日 (2015.8.20)

(71) 出願人 399031827
エイディシーテクノロジー株式会社
愛知県名古屋市中区錦一丁目20番19号
名神ビル
(71) 出願人 505014672
インディゴ株式会社
東京都世田谷区三軒茶屋2丁目11番22号
サンタワーズセンタービル12階
(74) 代理人 110000578
名古屋国際特許業務法人
(72) 発明者 清水 芳貴
東京都千代田区神田司町2-19-4 K
S司町ビル4F エイディシーテクノロジー
株式会社内

最終頁に続く

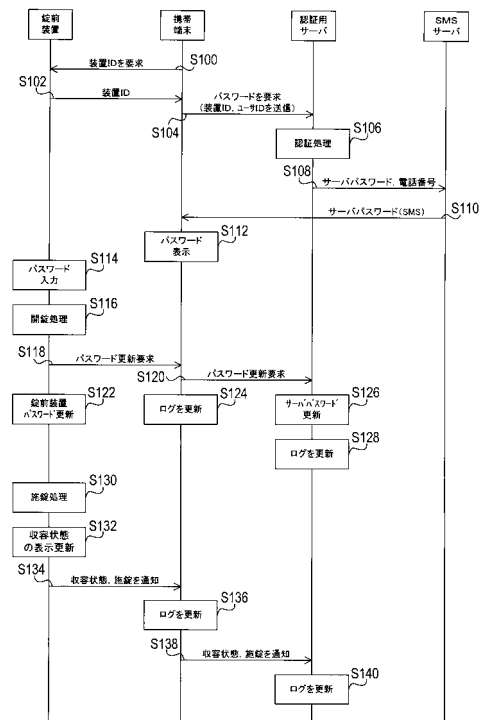
(54) 【発明の名称】 錠前装置

(57) 【要約】

【課題】錠前のセキュリティ性を向上させる。

【解決手段】錠前装置は、サーバからユーザに通知されるパスワードの入力を受け付けるパスワード受付部(S114)と、パスワード受付部が入力を受け付けたパスワードが、自装置にて記憶されている錠前装置パスワードに対応する場合には、錠前を開錠する開錠部(S116)と、を備える。サーバは、錠前装置を識別するための装置識別情報と、ユーザを識別するためのユーザ識別情報とを、無線通信を介してユーザの携帯端末から受信すると共に、これらの識別情報に基づき錠前の開錠を許可するか否かを決定し、該開錠を許可する場合には、当該サーバに記憶されている、錠前装置パスワードに対応するサーバパスワードを該ユーザに通知する。

【選択図】 図4



【特許請求の範囲】**【請求項 1】**

サーバからユーザに通知されるパスワードの入力を受け付けるパスワード受付部と、前記パスワード受付部が入力を受け付けた前記パスワードが、自装置にて記憶されている錠前装置パスワードに対応する場合には、錠前を開錠する開錠部と、を備えることを特徴とする錠前装置であって、

前記サーバは、前記錠前装置を識別するための装置識別情報と、前記ユーザを識別するためのユーザ識別情報とを、無線通信を介して前記ユーザの携帯端末から受信すると共に、これらの識別情報に基づき前記錠前の開錠を許可するか否かを決定し、該開錠を許可する場合には、当該サーバに記憶されている、前記錠前装置パスワードに対応するサーバパスワードを該ユーザに通知すること、

を特徴とする錠前装置。

【請求項 2】

請求項 1 に記載の錠前装置において、

前記錠前装置は、前記携帯端末に前記装置識別情報を提供する識別情報提供部をさらに備え、

前記携帯端末は、前記錠前装置から取得した前記装置識別情報を前記サーバに送信すること、

を特徴とする錠前装置。

【請求項 3】

請求項 1 又は請求項 2 に記載の錠前装置において、

前記サーバパスワードは、前記錠前の開錠を許可することを決定した前記サーバから前記携帯端末に無線通信を介して送信され、該携帯端末により前記ユーザに通知されること

、

を特徴とする錠前装置。

【発明の詳細な説明】**【技術分野】****【0001】**

本開示は、錠前の開錠を行う錠前装置に関する。

【背景技術】**【0002】**

無線通信により電子鍵から受信した識別情報と、予め保存されている識別情報とにより錠前に設けられた電子錠にて認証処理を行い、認証に成功した場合には錠前の開錠を許可するセキュリティ装置が知られている（特許文献 1 参照）。このようなセキュリティ装置によれば、扉等に設けられた錠前のセキュリティ性を高めることができる。

【先行技術文献】**【特許文献】****【0003】**

【特許文献 1】特開 2009 - 287251 号公報

【発明の概要】**【発明が解決しようとする課題】****【0004】**

しかしながら、電子鍵と電子錠との間の無線通信が傍受されて識別情報が漏えいする恐れがあると共に、電子錠にて認証処理が行われるため、電子錠が解析されて認証処理の内容が漏えいする恐れがある。

【0005】

本開示は、錠前のセキュリティ性を向上させることを目的とする。

【課題を解決するための手段】**【0006】**

本開示の一側面は、サーバからユーザに通知されるパスワードの入力を受け付けるパス

10

20

30

40

50

ワード受付部と、パスワード受付部が入力を受け付けたパスワードが、自装置にて記憶されている錠前装置パスワードに対応する場合には、錠前を開錠する開錠部と、を備えることを特徴とする錠前装置であって、サーバは、錠前装置を識別するための装置識別情報と、ユーザを識別するためのユーザ識別情報とを、無線通信を介してユーザの携帯端末から受信すると共に、これらの識別情報に基づき錠前の開錠を許可するか否かを決定し、該開錠を許可する場合には、当該サーバに記憶されている、錠前装置パスワードに対応するサーバパスワードを該ユーザに通知すること、を特徴とする錠前装置に関するものである。

【0007】

このような構成によれば、サーバにて、携帯端末から受信した装置識別情報とユーザ識別情報とに基づき錠前の開錠を許可するか否かが決定され、開錠が許可された場合には、錠前を開錠するためのパスワードがユーザに通知される。そして、ユーザが通知されたパスワードを錠前装置に入力することで、錠前が開錠される。

10

【0008】

このため、錠前装置や携帯端末を解析しても、ユーザの開錠を許可するか否かを決定する処理の内容を把握できない。また、ユーザが自ら錠前装置にパスワードを入力するため、錠前装置との間の通信が傍受されてパスワードが漏えいすることを未然に防ぐことができる。したがって、錠前のセキュリティ性を向上させることができる。

【0009】

また、上記構成において、錠前装置は、携帯端末に装置識別情報を提供する識別情報提供部をさらに備え、携帯端末は、錠前装置から取得した装置識別情報を前記サーバに送信する。

20

【0010】

このような構成によれば、装置識別情報を人目に晒すことなくサーバに送信することができ、装置識別情報が第三者に把握されるのを抑制できる。また、開錠の対象となる錠前に設けられた錠前装置の装置識別情報が、確実に携帯端末を介してサーバに提供されるため、サーバでは、開錠を許可するか否かを正確に判断できる。

【0011】

また、上記構成において、サーバパスワードは、錠前の開錠を許可することを決定したサーバから携帯端末に無線通信を介して送信され、該携帯端末によりユーザに通知される。

30

【0012】

このような構成によれば、錠前の開錠が許可された場合には、携帯端末を介してユーザに対し錠前装置に入力すべきパスワードが報知される。このため、使い勝手が向上すると共に、パスワードが第三者に把握されるのを抑制できる。

【図面の簡単な説明】

【0013】

【図1】図1Aは第1実施形態の開錠システムのブロック図であり、図1Bは第1実施形態の携帯端末のブロック図である。

【図2】図2Aは第1実施形態の錠前装置のブロック図であり、図2Bは第1実施形態の認証用サーバのブロック図である。

40

【図3】図3A、図3Bは、第1実施形態の錠前装置が設けられた箱型部材の一例である。

【図4】第1実施形態の開錠処理のフローチャートである。

【図5】第2実施形態の開錠処理のフローチャートである。

【図6】図6Aは第2実施形態の錠前装置パスワード更新処理のフローチャートであり、図6Bは第2実施形態のサーバパスワード更新処理のフローチャートである。

【発明を実施するための形態】

【0014】

以下、本開示の実施形態について図面を用いて説明する。なお、本開示の実施の形態は、下記の実施形態に何ら限定されることはなく、本開示の技術的範囲に属する限り種々の

50

形態を採りうる。

【 0 0 1 5 】

[第 1 実施形態]

[構成の説明]

第 1 実施形態の開錠システム 1 は、錠前の開錠や施錠を行うためのシステムであり、1 又は複数の携帯端末 1 0 , 1 又は複数の錠前装置 2 0 , 認証用サーバ 3 0 を有する (図 1 A) 。なお、携帯端末 1 0 と錠前装置 2 0 とは、無線通信が可能となっている。また、携帯端末 1 0 は、インターネット 2 を介して認証用サーバ 3 0 と通信を行うと共に、認証用サーバ 3 0 は、インターネット 2 を介して S M S サーバ 4 0 と通信を行う。

【 0 0 1 6 】

携帯端末 1 0 は、携帯電話機能を有し、インターネットにアクセス可能な携帯型の装置 (例えば、携帯電話やスマートフォン等) として構成されている。携帯端末 1 0 は、錠前装置 2 0 により制御される錠前を開錠するためのパスワードを認証用サーバ 3 0 から取得し、ユーザに報知する。携帯端末 1 0 は、近距離通信部 1 1 , 電話通信部 1 2 , 記憶部 1 3 , 制御部 1 4 , 表示部 1 5 , 操作部 1 6 等を有する (図 1 B) 。

【 0 0 1 7 】

近距離通信部 1 1 は、ブルートゥース (登録商標) により近距離の無線通信を行う部位であり、錠前装置 2 0 と無線通信を行う。また、近距離通信部 1 1 は、自装置の付近に設けられた中継機と無線通信を行い、インターネット 2 にアクセスしても良い。無論、ブルートゥースに替えて、例えば、無線 L A N 等の規格に従い近距離の無線通信を行っても良い。

【 0 0 1 8 】

電話通信部 1 2 は、携帯電話回線を利用して通話やインターネット 2 へのアクセスを行う部位であり、無線通信を介して認証用サーバ 3 0 と通信を行う。また、電話通信部 1 2 は、ショートメッセージサービスを利用してテキストデータの送受信を行う。

【 0 0 1 9 】

記憶部 1 3 は、フラッシュメモリや H D D 等の不揮発性の記憶装置から構成されており、各種データが保存されている。また、記憶部 1 3 には、ユーザ I D (特許請求の範囲におけるユーザ識別情報の一例に相当) やユーザによる錠前の開錠や施錠を記録したログ情報が記憶されている。

【 0 0 2 0 】

なお、ユーザ I D とは、自装置のユーザに割り当てられた識別情報であり、錠前を開錠するか否かを決定するための認証処理 (詳細は後述する) において、当該ユーザと他のユーザとを見分けるために用いられる。ユーザ I D は、例えば、文字データや数値データ等から構成されていても良いし、画像データとして構成されていても良い。また、ユーザ I D に替えて、当該ユーザに固有に割り当てられた認証用データを用いても良い。

【 0 0 2 1 】

制御部 1 4 は、 C P U , R O M , R A M , I / O 及びこれらを接続するバスライン等からなる周知のコンピュータを中心に構成されており、記憶部 1 3 等から読み出され、 R A M にロードされたプログラム等に従い動作する。

【 0 0 2 2 】

表示部 1 5 は、液晶ディスプレイ等として構成され、各種情報を表示する。

操作部 1 6 は、タッチパネル等として構成され、各種操作を受け付ける。

また、携帯端末 1 0 には、錠前の開錠等を行うための端末用アプリがインストールされており、記憶部 1 3 には、端末用アプリとして動作するプログラムが保存されている。なお、端末用アプリは、例えば、記憶媒体 1 7 に記憶された状態で提供されても良いし、インターネット 2 を介して提供されても良い。

【 0 0 2 3 】

また、携帯端末 1 0 には、現在の年月日時を特定する時計アプリがインストールされている。

10

20

30

40

50

錠前装置 20 は、正しいパスワードが入力されると、キーボックス等の箱型部材を開閉する蓋部に設けられた錠前を開錠する。無論、これに限らず、錠前装置 20 は、様々な錠前を開錠する構成とすることができ、例えば、ロッカーや建物の戸や窓等に設けられた錠前を開錠しても良いし、建物の戸等に設けられた錠前に後から取り付けられ、該錠前を開錠する構成となっても良い。また、錠前装置 20 は、予め定められた条件が充足されると、自装置に記憶されているパスワード（錠前装置パスワード）を更新する（詳細は後述する）。

【0024】

錠前装置 20 は、近距離通信部 21，記憶部 22，表示部 23，操作部 24，制御部 25，錠前制御部 26，錠前 27，収容状態センサ 28等を有する（図 2A）。

10

近距離通信部 21 は、ブルートゥースにより近距離の無線通信を行う部位であり、携帯端末 10 と無線通信を行う。無論、ブルートゥースに替えて、例えば、無線 LAN 等の規格に従い近距離の無線通信を行っても良い。

【0025】

記憶部 22 は、フラッシュメモリや HDD 等の不揮発性の記憶装置から構成されており、各種データが保存されている。また、記憶部 22 には、装置 ID（特許請求の範囲における装置識別情報の一例に相当）や錠前装置パスワードが記憶されている。

【0026】

なお、装置 ID とは、自装置に割り当てられた識別情報であり、錠前の開錠を許可するか否かを決定するための認証処理（詳細は後述する）において、自装置と他の錠前装置 20 とを見分けるために用いられる。装置 ID は、例えば、文字データや数値データ等から構成されていても良いし、画像データとして構成されていても良い。また、自装置に固有に割り当てられたアドレス（例えば、ブルートゥースデバイスに固有に割り当てられたアドレスや、物理アドレス等）等を、装置 ID として用いても良い。また、装置 ID に替えて、錠前装置 20 に固有に割り当てられた認証用データを用いても良い。

20

【0027】

また、錠前装置パスワードとは、錠前を開錠することが許可されたユーザを確認するために記憶部 22 に記憶されているパスワード（符号）である。

表示部 23 は、LED や液晶ディスプレイ等から構成され、各種情報を表示する。

【0028】

操作部 24 は、各種ボタン等から構成され、開錠のためのパスワードの入力操作等といった各種操作を受け付ける。

30

制御部 25 は、CPU，ROM，RAM，I/O 及びこれらを接続するバスライン等からなる周知のコンピュータを中心に構成されており、ROM に記憶されているプログラム等に従い動作する。また、制御部 25 は、現在の年月日時を特定する時計機能を有している。

【0029】

錠前制御部 26 は、モータ等のアクチュエータを駆動することで、錠前 27 の施錠及び開錠を行う。

錠前 27 は、箱型部材を開閉する蓋部に設けられており、施錠されると蓋部が開放できない状態にする。

40

【0030】

収容状態センサ 28 は、箱型部材に保全対象物（例えば、ドアの鍵等の物品）が収容されていることを検出するセンサである。

認証用サーバ 30 は、錠前装置 20 に錠前を開錠させるためのパスワードをユーザに通知すると共に、錠前装置 20 と同様のタイミング及び更新方法で、自装置に記憶されているパスワード（サーバパスワード）を更新する（詳細は後述する）。

【0031】

サーバパスワードとは、各錠前装置 20 により開錠がなされる錠前に対応して設けられており、対応する錠前を開錠することが許可されたユーザを確認するために用いられるパ

50

スワード（符号）である。

【0032】

また、認証用サーバ30は、PC等として構成されており、通信部31，記憶部32，制御部33，表示部34，操作部35等を備える（図2B参照）。

通信部31は、インターネット2や携帯電話回線へのアクセスを行う部位であり、無線通信を介して携帯端末10と通信を行う。

【0033】

記憶部32は、HDD等の不揮発性の記憶装置から構成されており、各種データが保存されている。また、記憶部32には、後述する開錠のための認証処理に用いられる認証データや、開錠システム1を利用する各ユーザ（携帯端末10のユーザ）の個人情報（例えば、携帯端末10の電話番号等）や、各ユーザによる錠前の開錠や施錠等を記録したログ情報が記憶されている。

10

【0034】

制御部33は、CPU，ROM，RAM，I/O及びこれらを接続するバスライン等からなる周知のコンピュータを中心に構成されており、記憶部32等から読み出され、RAMにロードされたプログラム等に従い動作する。

【0035】

表示部34は、液晶ディスプレイ等として構成され、各種情報を表示する。

操作部35は、キーボードやマウス等として構成され、各種操作を受け付ける。

また、認証用サーバ30には、錠前27を開錠するためのパスワードをユーザに通知するサーバ用アプリがインストールされており、記憶部32には、サーバ用アプリとして動作するプログラムが保存されている。なお、サーバ用アプリは、例えば、記憶媒体36に記憶された状態で提供されても良いし、インターネット2を介して提供されても良い。

20

【0036】

また、認証用サーバ30には、現在の年月日時を特定する時計アプリがインストールされている。

ここで、錠前装置20が設けられた箱型部材の一例について説明する。箱型部材50は、錠前装置20が搭載されており、内部に保全対象物を収納可能であると共に、南京錠として構成されている（図3A，3B）。

【0037】

箱型部材50は、略直方体形状の筐体51を有しており、筐体51は、正面側の主面を含む前側部分51aと、背面側の主面を含む後側部分51bとに分離可能に構成されている。そして、前側部分51aと後側部分51bとを結合した状態で固定する図示しない錠前機構（錠前27に相当）が設けられている。また、筐体51の内部には、物品を収容するためのスペースが形成されている。

30

【0038】

また、箱型部材50は、テンキー52，LED53，U字型部材54等を備える。

テンキー52は、前側部分51aにおける正面側の主面に配されており、錠前装置20の操作部24に相当する。

【0039】

LED53は、正面側の主面におけるテンキー52の上方に配されており、錠前装置20の表示部23に相当する。LED53は、内部に収納された保全対象物の有無や、施錠の状態を表示する。

40

【0040】

U字型部材54は、U字状に湾曲した金属製の棒状部材であり、筐体51の上面に設けられている。U字型部材54は、錠前27に相当する部位であり、開錠された状態では、上下方向に変位可能に構成されており、上方向に変位させると、U字型部材54の一端が孔部51cの外部に位置する状態になる。

【0041】

錠前装置20の錠前制御部26は、錠前機構とU字型部材54の施錠及び開錠を同時に

50

行う。錠前機構が開錠された状態になると、前側部分 5 1 と後側部分 5 2 とが分離可能になる。また、U字型部材 5 4 が開錠された状態になると、U字型部材 5 4 は上下方向に変位可能となり、U字型部材 5 4 が上方向に変位すると、U字型部材 5 4 の一端が、後側部分 5 1 b の上部に形成された孔部 5 1 c の外部に位置した状態になる。

【 0 0 4 2 】

そして、前側部分 5 1 と後側部分 5 2 とを結合させると共に、U字型部材 5 4 を下端まで変位させると、錠前機構とU字型部材 5 4 を施錠可能な状態になる。この時、これらを施錠すると、前側部分 5 1 と後側部分 5 2 とが結合し、且つ、U字型部材 5 4 の一端が孔部 5 1 c に挿入された状態で固定される。

【 0 0 4 3 】

[動作の説明]

次に、第 1 実施形態の開錠システム 1 の動作について説明する。

開錠システム 1 は、錠前 2 7 の開錠が許可されているユーザに対し、該錠前 2 7 を開錠するパスワードを通知する。具体的には、該ユーザのユーザ ID と錠前 2 7 に設けられた錠前装置 2 0 の装置 ID が、携帯端末 1 0 から認証用サーバ 3 0 に送信され、これらの ID により認証処理が行われる。認証処理により、該ユーザによる該錠前 2 7 の開錠を許可するか否かが決定され、許可された場合、携帯端末 1 0 を介して該ユーザにパスワード（認証用サーバ 3 0 に記憶されているサーバパスワード）が通知される。通知されるパスワードは、錠前装置 2 0 に記憶されている錠前装置パスワードに対応しており（一例として、これらのパスワードが一致しており）、ユーザが通知されたパスワードを錠前装置 2 0 に入力すると、該錠前 2 7 が開錠される。

【 0 0 4 4 】

また、第 1 実施形態では、開錠に用いるパスワードはワンタイムパスワードとして構成されており、開錠が行われると、錠前装置 2 0 と認証用サーバ 3 0 では、それぞれ、対応する更新アルゴリズムにより自装置にて記憶されているパスワードが更新される。無論、更新後における各装置のパスワードが、更新前と同様の対応関係を有しているのは、言うまでも無い。

【 0 0 4 5 】

以下では、錠前 2 7 の開錠を行う際に携帯端末 1 0 と錠前装置 2 0 と認証用サーバ 3 0 とにより行われる開錠処理について詳しく説明する（図 4）。なお、開錠処理では、携帯端末 1 0 での処理は、携帯用アプリに従い動作する制御部 1 4 により実行されると共に、認証用サーバ 3 0 での処理は、サーバ用アプリに従い動作する制御部 3 3 により実行される。また、錠前装置 2 0 での処理は、制御部 2 5 により実行される。

【 0 0 4 6 】

S 1 0 0 では、携帯端末 1 0 は、開錠を行うユーザ（対象ユーザとも記載）からの操作に応じて近距離通信部 1 1 を介して錠前装置 2 0 と無線通信を行い、開錠を行う錠前 2 7（対象錠前とも記載）に設けられた錠前装置 2 0 に装置 ID を要求するコマンドを送信する。なお、携帯端末 1 0 は、錠前装置 2 0 に接近した際に錠前装置 2 0 から電波を受信すると、表示部 1 5 等を介して錠前装置 2 0 の存在をユーザに報知し、装置 ID の取得を促しても良い。また、携帯端末 1 0 は、該電波の受信に応じて錠前装置 2 0 に装置 ID を要求するコマンドを送信しても良い。

【 0 0 4 7 】

錠前装置 2 0 は、近距離通信部 2 1 を介して行われる携帯端末 1 0 との間の無線通信により上記コマンドを受信すると、無線通信により、携帯端末 1 0 に対し、自装置の装置 ID を送信する（S 1 0 2）。

【 0 0 4 8 】

無論、無線通信に限らず、例えば、錠前装置 2 0 と携帯端末 1 0 を有線通信路により一時的に接続し、有線通信路を介して錠前装置 2 0 から携帯端末 1 0 に装置 ID を送信しても良い。また、例えば、RFID により錠前装置 2 0 から携帯端末 1 0 に装置 ID を送信しても良いし、錠前装置 2 0 のディスプレイに表示されたバーコード情報や、錠前装置 2

10

20

30

40

50

0 本体やその周辺等に描かれたバーコード情報等を携帯端末 10 にて読み取ることで、携帯端末 10 にて装置 ID を取得しても良い。また、対象ユーザが錠前装置 20 の表示部 23 等から装置 ID を読み取り、操作部 16 を介して携帯端末 10 に装置 ID を入力する構成としても良い。

【0049】

S104では、錠前装置 20 から装置 ID を受信した携帯端末 10 は、電話通信部 12 により携帯電話回線やインターネット 2 を介して認証用サーバ 30 と通信を行う。そして、認証用サーバ 30 に対し、装置 ID と、自装置の記憶部 13 に記憶されている対象ユーザのユーザ ID を送信することで、対象錠前を開錠するパスワードを要求する。

【0050】

S106では、通信部 31 を介して装置 ID 及びユーザ ID を受信した認証用サーバ 30 は、これらの ID に基づき認証処理を行い、対象ユーザによる対象錠前の開錠を許可するか否かを決定する。

【0051】

ここで、認証処理は、記憶部 32 に記憶されている認証データに基づき行われる。認証データは、各ユーザのユーザ ID と該ユーザが施錠を許可されている錠前 27 に設けられた錠前装置 20 の装置 ID との対応関係を示している。受信した装置 ID とユーザ ID が対応していることを認証データが示している場合には、対象ユーザによる対象錠前の開錠することを許可する。一方、そうでない場合には、対象ユーザによる対象錠前の開錠を許可しない。

【0052】

開錠を許可すると、認証用サーバ 30 は、記憶部 32 から、対象錠前を開錠するサーバパスワードと、対象ユーザの携帯端末 10 の電話番号を読み出す。そして、通信部 31 を介して SMS サーバと通信を行い、ショートメッセージサービスにより対象ユーザの携帯端末 10 にサーバパスワードを送信する (S108, S110)。

【0053】

S112では、携帯端末 10 は、ショートメッセージサービスにより受信したサーバパスワードを表示部 15 に表示することで、該サーバパスワードをユーザに報知する。無論、これに限らず、例えば、音声によりサーバパスワードを報知しても良い。

【0054】

そして、S114では、錠前装置 20 は、操作部 24 を介してユーザからパスワードの入力を受け付ける。入力されたパスワードが、錠前装置 20 にて記憶されている錠前装置パスワードに対応する場合 (一例として、これらが一致する場合)、錠前装置 20 は、錠前制御部 26 により錠前 27 (対象錠前) を開錠する。

【0055】

S118では、錠前装置 20 は、携帯端末 10 に対し、サーバパスワードの更新を要求するパスワード更新要求を送信する。パスワード更新要求を受信した携帯端末 10 は、パスワード更新要求を認証用サーバ 30 に送信する (S120)。

【0056】

S122では、錠前装置 20 は、予め定められた更新アルゴリズムに従い、記憶部 22 に記憶されている錠前装置パスワードを更新する。

S124では、携帯端末 10 は、時計アプリにより現在の年月日時を特定し、ログ情報に、現在の年月日時と、対象錠前の開錠の記録と、対象錠前に設けられた錠前装置 20 の装置 ID 等を追加する。

【0057】

S126では、認証用サーバ 30 は、錠前装置 20 に対応する更新アルゴリズムに従い、記憶部 32 に記憶されているサーバパスワードを更新する。

S128では、認証用サーバ 30 は、時計アプリにより現在の年月日時を特定し、ログ情報に、現在の年月日時と、対象錠前の開錠の記録と、対象ユーザのユーザ ID と、対象錠前に設けられた錠前装置 20 の装置 ID 等を追加する。

10

20

30

40

50

【 0 0 5 8 】

S 1 3 0では、対象錠前が施錠される。具体的には、例えば、ユーザが箱型部材を閉鎖したり、錠前27に対し操作を行うことで施錠を行っても良い。また、例えば、携帯端末10を操作し、錠前装置20に施錠を指示するコマンドを送信し、錠前装置20が該コマンドに応じて錠前27を制御し、施錠を行っても良い。

【 0 0 5 9 】

S 1 3 2では、錠前装置20は、収容状態センサ28からの信号に基づき、箱型部材の内部に保全対象物が収容されているか否か（収容状態）を判定し、表示部23にて判定結果を表示する（以後、表示部23は、判定結果の表示を継続する）。

【 0 0 6 0 】

S 1 3 4では、錠前装置20は、携帯端末10に対し、収容状態と施錠がなされた旨の情報を送信する。

S 1 3 6では、携帯端末10は、収容状態と施錠がなされた旨の情報を受信すると、時計アプリにより現在の年月日時を特定する。そして、ログ情報に、現在の年月日時と、収容状態と、対象錠前の施錠の記録と、対象錠前に設けられた錠前装置20の装置ID等を追加する。

【 0 0 6 1 】

S 1 3 8では、携帯端末10は、認証用サーバ30に対し、収容状態と対象錠前の施錠がなされた旨の情報を送信する。

S 1 4 0では、認証用サーバ30は、収容状態と施錠がなされた旨の情報を受信すると、時計アプリにより現在の年月日時を特定する。そして、ログ情報に、現在の年月日時と、収容状態と、対象錠前の施錠の記録と、対象ユーザのユーザIDと、対象錠前に設けられた錠前装置20の装置ID等を追加する。

【 0 0 6 2 】

〔 第 2 実施形態 〕

次に、第2実施形態の開錠システム1について説明する。第2実施形態の開錠システム1は、第1実施形態と同様の構成を有しているが、錠前装置パスワードやサーバパスワードの更新タイミングが異なっている。具体的には、第1実施形態では、開錠後に錠前装置パスワード及びサーバパスワードが更新される。これに対し、第2実施形態では、予め定められた更新時期が到来するとこれらのパスワードが更新される。具体的には、例えば、所定時間が経過する度にこれらのパスワードを更新しても良いし、予め定められた年月日時が到来した際にこれらのパスワードを更新しても良い。そして、開錠処理では、錠前装置20にて特定される時刻を認証用サーバ30にて特定される時刻に合わせる時刻合わせが行われる。以下では、第1実施形態との相違点を中心に説明する。

【 0 0 6 3 】

(1) 開錠処理について

まず、第2実施形態の開錠処理について詳しく説明する（図5）。

S 2 0 0 ~ S 2 0 4は、第1実施形態の開錠処理のS 1 0 0 ~ S 1 0 4と同様であるため、説明を省略する。

【 0 0 6 4 】

S 2 0 6では、認証用サーバ30は、時計アプリにより現在の年月日時を特定し、現在の年月日時を示す日時情報を携帯端末10に送信する。

S 2 0 8では、日時情報を受信した携帯端末10は、錠前装置20に日時情報を送信する。

【 0 0 6 5 】

S 2 1 0では、日時情報を受信した錠前装置20は、制御部25の時計機能の時刻合わせを行う。具体的には、該時計機能により特定される年月日時を、受信した日時情報が示す年月日時に一致させる。

【 0 0 6 6 】

S 2 1 2 ~ S 2 2 2は、第1実施形態の開錠処理のS 1 0 6 ~ S 1 1 6と同様であるた

10

20

30

40

50

め、説明を省略する。

S 2 2 4では、錠前装置 2 0は、携帯端末 1 0に対し、対象錠前を開錠した旨を示す開錠通知を送信する。

【 0 0 6 7 】

S 2 2 6では、開錠通知を受信した携帯端末 1 0は、認証用サーバ 3 0に対し、開錠通知を送信する。

S 2 2 8 , S 2 3 0は、第 1 実施形態の開錠処理の S 1 2 4 , S 1 2 8と同様であり、S 2 3 2 ~ S 2 4 2は、第 1 実施形態の開錠処理の S 1 3 0 ~ S 1 4 0と同様であるため、説明を省略する。

【 0 0 6 8 】

(2) 錠前装置パスワード更新処理について

次に、予め定められた更新時期が到来すると、錠前装置 2 0に記憶されている錠前装置パスワードを更新する錠前装置パスワード更新処理について説明する(図 6 A)。なお、本処理は、錠前装置 2 0にて周期的なタイミングで実行される。

【 0 0 6 9 】

S 3 0 0では、錠前装置 2 0の制御部 2 5は、時計機能により特定される年月日時に基づき(換言すれば、自装置で計測された時間に基づき)、予め定められた更新時期が到来したか否かを判定する。そして、肯定判定が得られた場合には(S 3 0 0 : Y e s)、S 3 0 5に移行し、否定判定が得られた場合には(S 3 0 0 : N o)、本処理を終了する。

【 0 0 7 0 】

S 3 0 5では、制御部 2 5は、第 1 実施形態の開錠処理の S 1 2 2と同様にして、錠前装置パスワードを更新し、本処理を終了する。

(3) サーバパスワード更新処理について

次に、予め定められた更新時期が到来すると、認証用サーバ 3 0に記憶されているサーバパスワードを更新するサーバパスワード更新処理について説明する(図 6 B)。なお、本処理は、認証用サーバ 3 0にて周期的なタイミングで実行される。

【 0 0 7 1 】

S 4 0 0では、認証用サーバ 3 0の制御部 3 3は、時計アプリにより特定される年月日時に基づき(換言すれば、自装置で計測された時間に基づき)、予め定められた更新時期が到来したか否かを判定する。そして、肯定判定が得られた場合には(S 4 0 0 : Y e s)、S 4 0 5に移行し、否定判定が得られた場合には(S 4 0 0 : N o)、本処理を終了する。

【 0 0 7 2 】

S 4 0 5では、制御部 3 3は、第 1 実施形態の開錠処理の S 1 2 6と同様にして、サーバパスワードを更新し、本処理を終了する。

[他の実施形態]

(1) 第 1 , 第 2 実施形態では、ショートメッセージサービスを利用して認証用サーバ 3 0からユーザにパスワードが通知される。しかしながら、パスワードの通知方法はこれに限定されることは無く、例えば、電子メールによりパスワードを通知しても良いし、携帯端末 1 0から認証用サーバ 3 0に設けられたウェブサイトにアクセスすることで、パスワードを通知しても良い。また、認証用サーバ 3 0から携帯端末 1 0における携帯用アプリにパスワードを送信しても良いし、認証用サーバ 3 0の表示部 3 4にパスワードを表示すると共に、オペレータが携帯端末 1 0に電話をかけ、表示されたパスワードをユーザに知らせても良い。

【 0 0 7 3 】

また、オペレータによる電話連絡や、専用のアプリケーションを利用してワンタイムパスワードをユーザに連絡するシステムが存在するが、このような既存のシステムと第 1 , 第 2 実施形態の開錠システム 1 とを組み合わせ使用しても良い。すなわち、既存のシステムに用いられているサーバを認証用サーバ 3 0として構成し、携帯端末 1 0から認証用サーバ 3 0に装置 I Dとユーザ I Dを送信しても良い。そして、認証用サーバ 3 0にてサ

10

20

30

40

50

ーバパスワードを特定すると共に、既存のシステムと同様の手段でユーザにサーバパスワードを通知しても良い。

【0074】

このような構成を有する場合であっても、同様の効果を得ることができる。

(2) 第1実施形態の開錠処理では、錠前27の開錠が行われた後の段階で、錠前装置パスワードとサーバパスワードが更新される。しかしながら、これに限らず、認証処理にて開錠が決定された後に、携帯端末10を介して錠前装置20と認証用サーバ30との間で通信を行い、錠前装置パスワードとサーバパスワードを更新しても良い。そして、更新を行った後に、認証用サーバ30からユーザに対しサーバパスワードを通知し、錠前装置20に正しいパスワードが入力された際には、錠前27を開錠しても良い。このような構成を有する場合であっても、同様の効果を得ることができる。

10

【0075】

(3) 第2実施形態の開錠処理では、錠前装置20にパスワードが入力される前の段階で、認証用サーバ30から錠前装置20に日時情報が送信され、錠前装置20の時刻合せが行われる。

【0076】

しかしながら、これに限らず、パスワードの入力がなされた後の段階で、同様にして錠前装置20の時刻合せを行っても良い。

また、第2実施形態の時刻合せでは、錠前装置20にて特定される年月日時が、認証用サーバ30にて特定される年月日時に合わせられる。

20

【0077】

しかしながら、これに限らず、錠前装置20にて生成された日時情報を、携帯端末10を介して認証用サーバ30に送信し、認証用サーバ30にて特定される年月日時を、錠前装置20にて特定される年月日時に合わせても良い。また、携帯端末10にて生成された日時情報を錠前装置20と認証用サーバ30に送信し、錠前装置20にて特定される年月日時と、認証用サーバ30にて特定される年月日時を、該日時情報が示す年月日時に合わせることで、時刻合せを行っても良い。

【0078】

このような構成を有する場合であっても、同様の効果を得ることができる。

(4) 上記実施形態における1つの構成要素が有する機能を複数の構成要素として分散させたり、複数の構成要素が有する機能を1つの構成要素に統合させたりしてもよい。また、上記実施形態の構成の少なくとも一部を、同様の機能を有する公知の構成に置き換えてもよい。また、上記実施形態の構成の一部を省略してもよい。また、上記実施形態の構成の少なくとも一部を、他の上記実施形態の構成に対して付加又は置換してもよい。なお、特許請求の範囲に記載した文言のみによって特定される技術思想に含まれるあらゆる態様が本開示の実施形態である。

30

【0079】

(5) 上述した開錠システム1の他、携帯端末10、錠前装置20、認証用サーバ30、SMSサーバ40等、種々の形態で本開示を実現することもできる。この他にも、携帯端末10、錠前装置20、認証用サーバ30、SMSサーバ40等としてコンピュータを機能させるためのプログラム、このプログラムを記録した媒体、携帯端末10、錠前装置20、認証用サーバ30、SMSサーバ40等により実行される処理に相当する方法等、種々の形態で本開示を実現することもできる。

40

【0080】

[効果]

第1、第2実施形態によれば、以下の効果が得られる。

(1) ユーザが錠前27の開錠を行う際には、装置IDとユーザIDが認証用サーバ30に送信され、認証用サーバ30での認証処理にて開錠を許可するか否かが決定される。そして、開錠を許可する場合には、認証用サーバ30にて記憶されているサーバパスワードがショートメッセージサービスを利用してユーザに通知され、通知されたサーバパスワ

50

ードを錠前装置 20 に入力することで、錠前 27 が開錠される。

【0081】

このため、携帯端末 10 や錠前装置 20 を解析しても、ユーザ ID や認証処理の内容を把握できず、また、携帯端末 10 を解析しても、錠前装置 20 に入力すべきパスワードを把握できない。また、ユーザが自ら錠前装置 20 にパスワードを入力するため、錠前装置 20 と携帯端末 10 との間の通信が傍受されてもパスワードが漏えいしない。したがって、錠前のセキュリティ性を向上させることができる。

【0082】

また、携帯端末 10 の処理負荷を抑えることができ、スマートフォン等のような高性能な携帯端末 10 を用いなくても開錠システム 1 を利用することができる。

(2) また、高度なセキュリティを要する認証処理は、処理負荷が大きく、高性能のハードウェアが必要になると共に、処理が複雑であるため不具合が混入する可能性が高い。このため、仮に認証処理を錠前装置 20 で行うとなると、錠前装置 20 のコストが増加する。これに対し、開錠システム 1 では、複数の錠前 27 の開錠に対応する認証処理が認証用サーバ 30 にて一括して行われており、各錠前装置 20 の処理が簡略化されている。

【0083】

このため、数多く存在する錠前装置 20 のコストを抑えることができ、これにより、開錠システム 1 全体のコストを大幅に抑制できる。

(3) また、錠前装置 20 に不具合が混入した場合、数多くの錠前装置 20 を個別に修正する必要があり、多大なコストが必要となるが、認証用サーバ 30 の不具合に対処する場合には、認証用サーバ 30 に対し 1 回の修正を行うのみで対処できる。これに対し、開錠システム 1 のように、複雑な認証処理を認証用サーバ 30 で行うことで、錠前装置 20 への不具合の混入を抑えることができる。さらに、認証処理のバージョンアップを行いたい場合にも、認証用サーバ 30 に対し 1 回の修正を行うのみで対処できる。このため、不具合への対処やメンテナンスが容易になる。

【0084】

(4) また、ブルートゥース等の規格の近距離無線通信により錠前装置 20 から携帯端末 10 に装置 ID を送信する構成とすることで、錠前装置 20 に近づかないと装置 ID を取得できなくなる。このため、必要以上に装置 ID が携帯端末 10 に送信されるのを抑制でき、これにより、セキュリティ性を向上させることができる。

【0085】

(5) また、錠前装置 20 では、箱型部材の内部に保全対象物が収容されているか否かの収容状態が判定され、収容状態が表示されるため、利便性が向上する。さらに、収容状態が携帯端末 10 や認証用サーバ 30 に送信され、ログ情報に記録される。これにより、保全対象物の紛失等のトラブルが生じた場合に、ログ情報を参照することで、トラブルの原因等を把握したり推測したりすることが可能となる。また、このような記録を残すことで、保全対象物の盗難等を抑止できる。

【0086】

(6) さらに、第 1, 第 2 実施形態、及び、他の実施形態は、以下の発明 (a) ~ (n) として次のような構成を有している。

(a) 錠前 (27) を開錠する錠前装置 (20) と、携帯端末 (10) と、無線通信を介して前記携帯端末と通信を行うサーバ (30) とを有する開錠システム (1) において、前記錠前装置は、パスワードの入力を受け付けるパスワード受付部 (S114, S220) と、前記パスワード受付部が入力を受け付けた前記パスワードが、自装置にて記憶されている錠前装置パスワードに対応する場合には、前記錠前を開錠する開錠部 (S116, S222) と、を備え、前記携帯端末は、前記錠前装置を識別するための装置識別情報を取得する識別情報取得部 (S102, S202) と、前記装置識別情報と、ユーザを識別するためのユーザ識別情報とを前記サーバに送信する識別情報送信部 (S104, S204) と、を備え、前記サーバは、前記装置識別情報及び前記ユーザ識別情報を、前記携帯端末から受信する識別情報受信部 (S104, S204) と、前記識別情報受信部が受

10

20

30

40

50

信した前記装置識別情報及び前記ユーザ識別情報に基づき、前記錠前の開錠を許可するかどうかを決定する開錠決定部（S106，S212）と、前記錠前の開錠を許可する場合には、自装置にて記憶されているパスワードであって、前記錠前装置パスワードに対応するパスワードであるサーバパスワードを前記ユーザに通知するための処理を行うパスワード通知部（S108，S214）と、を備えること、を特徴とする開錠システム（1）。

【0087】

このような構成によれば、ユーザが錠前の開錠を行う際には、錠前装置識別情報とユーザ識別情報がサーバに送信され、サーバにて該ユーザによる開錠を許可するかが決定される。そして、開錠を許可する場合には、サーバにて記憶されているサーバパスワードが該ユーザに通知され、通知されたサーバパスワードが錠前装置に入力されると錠前が開錠される。

10

【0088】

このため、錠前装置を解析しても、ユーザの開錠を許可するかどうかを決定する処理の内容を把握できない。また、ユーザが自ら錠前装置にパスワードを入力するため、錠前装置との間の通信が傍受されてパスワードが漏えいすることを未然に防ぐことができる。したがって、錠前のセキュリティ性を向上させることができる。

【0089】

（b）また、（a）において、前記錠前装置は、前記携帯端末に前記装置識別情報を提供する識別情報提供部（S102，S202）をさらに備え、前記識別情報取得部は、前記錠前装置から提供された前記装置識別情報を取得すること、を特徴とする開錠システム。

20

【0090】

このような構成によれば、装置識別情報を人目に晒すことなくサーバに送信することができ、装置識別情報が第三者に把握されるのを抑制できる。また、開錠の対象となる錠前に設けられた錠前装置の装置識別情報が確実に携帯端末に提供されるため、サーバでは、開錠を許可するかどうかを正確に判断できる。

【0091】

（c）また、（a）又は（b）において、前記パスワード通知部は、前記携帯端末に前記サーバパスワードを送信し、前記携帯端末は、前記サーバから前記サーバパスワードを受信するパスワード受信部（S110，S216）と、受信した前記サーバパスワードを前記ユーザに報知する報知部（S112，S218）と、をさらに備えることを特徴とする開錠システム。

30

【0092】

このような構成によれば、錠前の開錠が許可された場合には、携帯端末を介してユーザに対し錠前装置に入力すべきパスワードが報知される。このため、使い勝手が向上すると共に、パスワードが第三者に把握されるのを抑制できる。

【0093】

（d）また、（c）において、前記携帯端末は、携帯電話機能を有しており、前記パスワード通知部は、前記携帯電話機能による通話の際に利用される携帯電話回線を介して行われるショートメッセージサービスにより、前記携帯端末に前記サーバパスワードを送信し、前記パスワード受信部は、前記ショートメッセージサービスにより、前記サーバから前記サーバパスワードを受信すること、を特徴とする開錠システム。

40

【0094】

携帯電話番号は、メールアドレス等と比べると入手が困難であり、個人を特定する上で有用な情報であると考えられるが、このような構成によれば、開錠システムを利用するためには携帯端末の携帯電話番号の登録が必要となる。このため、開錠システムのユーザの特定が容易になり、ユーザによる不適切な行為（例えば、開錠システムの悪用や、錠前や錠前装置の破壊や、錠前により保全されている物の盗難や破壊等）を抑制できる。

【0095】

（e）また、（a）から（d）のいずれかにおいて、前記錠前装置は、前記開錠部が前

50

記錠前を開錠するのに伴い、予め定められた更新方法に従い、前記錠前装置パスワードを更新する錠前装置更新部（S 1 2 2）をさらに備え、前記サーバは、前記開錠決定部が前記錠前の開錠を許可するか否かを決定するのに伴い、前記更新方法に従い前記サーバパスワードを更新することで、前記サーバパスワードを前記錠前装置パスワードに対応させるサーバ更新部（S 1 2 6）をさらに備えること、を特徴とする開錠システム。

【0096】

このような構成によれば、錠前が開錠される度に錠前装置パスワードとサーバパスワードが更新されるため、セキュリティ性が向上する。

また、錠前装置による錠前装置パスワードの更新タイミングとサーバによるサーバパスワードの更新タイミングを確実に同期させることができる。このため、一方のパスワードのみが更新された結果、錠前装置パスワードとサーバパスワードが異なってしまい、サーバから通知されたサーバパスワードを錠前装置に入力したにも関わらず、錠前を開錠できないという事態の発生を抑制できる。

10

【0097】

（f）また、（a）から（d）のいずれかにおいて、前記錠前装置は、時間を計測した結果に基づき予め定められた更新時期が到来したか否かを判定し、肯定判定が得られた場合には、予め定められた更新方法に従い、前記錠前装置パスワードを更新する錠前装置更新部（S 3 0 0，S 3 0 5）をさらに備え、前記サーバは、時間を計測した結果に基づき前記更新時期が到来したか否かを判定し、肯定判定が得られた場合には、前記更新方法に従い前記サーバパスワードを更新することで、前記サーバパスワードを前記錠前装置パスワードに対応させるサーバ更新部（S 4 0 0，S 4 0 5）をさらに備えること、を特徴とする開錠システム。

20

【0098】

このような構成によれば、錠前装置パスワードとサーバパスワードを予め定められた頻度で更新できるため、セキュリティ性が向上する。

また、錠前装置による錠前装置パスワードの更新タイミングとサーバによるサーバパスワードの更新タイミングを同期させることができ、一方のパスワードのみが更新された結果、錠前装置パスワードとサーバパスワードが異なってしまうという事態の発生を抑制できる。

30

【0099】

（g）また、（f）において、前記サーバは、前記携帯端末に対し、前記サーバ更新部で計測される時間を示す時間情報を送信する時間情報送信部（S 2 0 6）をさらに備え、前記携帯端末は、前記サーバから前記時間情報を受信すると共に、該時間情報を前記錠前装置に送信する時間情報中継部（S 2 0 6，S 2 0 8）をさらに備え、前記錠前装置は、前記携帯端末から前記時間情報を受信すると共に、該時間情報に基づき、前記錠前装置更新部にて計測される時間を、前記サーバ更新部にて計測される時間と一致するように調整する時間調整部（S 2 0 8，S 2 1 0）をさらに備えること、を特徴とする開錠システム。

【0100】

このような構成によれば、錠前装置による錠前装置パスワードの更新タイミングとサーバによるサーバパスワードの更新タイミングを、より精度良く同期させることができる。

40

（h）また、（a）から（g）において、前記錠前装置は、前記開錠部が前記錠前を開錠すると、前記携帯端末に対し、前記錠前の開錠を示す開錠通知を送信する開錠通知部（S 1 1 8，S 2 2 4）をさらに備え、前記携帯端末は、前記錠前装置から前記開錠通知を受信すると、現在の日時と、前記錠前の開錠を記録する携帯端末記録部（S 1 1 8，S 1 2 4，S 2 2 4，S 2 2 8）をさらに備えること、を特徴とする開錠システム。

【0101】

このような構成によれば、錠前により保全されている物の紛失や破壊等といったトラブルが生じた場合に記録を参照することで、トラブルの原因等を把握したり推測したりすることが可能となる。また、このようなトラブルが生じた場合には、ユーザは、自分の携帯

50

端末に残っている記録に基づき自分に非が無いことを証明できる。

【0102】

(i) また、(a) から (g) において、前記錠前装置は、前記開錠部が前記錠前を開錠すると、前記携帯端末に対し、前記錠前の開錠を示す開錠通知を送信する開錠通知部 (S118, S224) をさらに備え、前記携帯端末は、前記錠前装置から前記開錠通知を受信すると、該開錠通知を前記サーバに送信する開錠通知中継部 (S118, S120, S224, S226) をさらに備え、前記サーバは、前記携帯端末から前記開錠通知を受信すると、現在の日時と、前記錠前の開錠を記録するサーバ記録部 (S120, S128, S226, S230) をさらに備えること、を特徴とする開錠システム。

【0103】

このような構成によれば、錠前により保全されている物の紛失や破壊等といったトラブルが生じた場合に記録を参照することで、トラブルの原因等を把握したり推測したりすることが可能となる。また、このような記録を残すことで、ユーザによる不適切な行為 (例えば、錠前により保全されている物の盗難や破壊等) を抑止できる。

【0104】

(j) 錠前 (27) を開錠する錠前装置 (20) を識別するための装置識別情報を取得する識別情報取得部 (S102, S202) と、ユーザによる前記錠前の開錠を許可するか否かをサーバ (30) に決定させると共に、該開錠を許可する場合には、該ユーザに前記錠前装置に入力するパスワードを該サーバに通知させるため、該ユーザを識別するためのユーザ識別情報と、前記識別情報取得部が取得した前記装置識別情報とを、無線通信を介して該サーバに送信する識別情報送信部 (S104, S204) と、を備えることを特徴とする携帯端末 (10)。

【0105】

このような構成によれば、ユーザによる錠前の開錠を許可するか否かをサーバにおいて決定することができる。これにより、錠前装置や携帯端末を解析しても、ユーザの開錠を許可するか否かを決定する処理の内容を把握できなくなるため、錠前のセキュリティ性を向上させることができる。

【0106】

(k) 錠前装置パスワードが入力されると錠前 (27) を開錠する錠前装置 (20) を識別するための装置識別情報、及び、該錠前を開錠するユーザを識別するためのユーザ識別情報を、無線通信を介して携帯端末 (10) から受信する識別情報受信部 (S104, S204) と、前記識別情報受信部が受信した前記装置識別情報及び前記ユーザ識別情報に基づき、前記錠前の開錠を許可するか否かを決定する開錠決定部 (S106, S212) と、前記錠前の開錠を許可する場合には、自装置にて記憶されているパスワードであって、前記錠前装置パスワードに対応するパスワードであるサーバパスワードを前記ユーザに通知するための処理を行うパスワード通知部 (S108, S214) と、を備えることを特徴とするサーバ (30)。

【0107】

このような構成によれば、サーバにて、携帯端末から受信した装置識別情報とユーザ識別情報とに基づき錠前の開錠を許可するか否かが決定され、開錠が許可された場合には、錠前を開錠するためのパスワードがユーザに通知される。これにより、錠前装置や携帯端末を解析しても、ユーザの開錠を許可するか否かを決定する処理の内容を把握できなくなるため、錠前のセキュリティ性を向上させることができる。

【0108】

(l) 錠前 (27) を開錠する錠前装置 (20) を識別するための装置識別情報を取得する識別情報取得部 (S102, S202) と、前記錠前の開錠のために前記錠前装置に入力するパスワードをサーバ (30) からユーザに通知させるため、該ユーザを識別するためのユーザ識別情報と、前記識別情報取得部が取得した前記装置識別情報とを、無線通信を介して該サーバに送信する識別情報送信部 (S104, S204) として、携帯端末を制御するコンピュータを動作させること、を備えることを特徴とする携帯端末用プログ

10

20

30

40

50

ラム。

【0109】

このような構成によれば、ユーザによる錠前の開錠を許可するか否かをサーバにおいて決定することができる。これにより、錠前装置や携帯端末を解析しても、ユーザの開錠を許可するか否かを決定する処理の内容を把握できなくなるため、錠前のセキュリティ性を向上させることができる。

【0110】

(m) 錠前装置パスワードが入力されると錠前(27)を開錠する錠前装置(20)を識別するための装置識別情報、及び、該錠前を開錠するユーザを識別するためのユーザ識別情報を、無線通信を介して携帯端末(10)から受信する識別情報受信部(S104, S204)と、前記識別情報受信部が受信した前記装置識別情報及び前記ユーザ識別情報に基づき、前記錠前の開錠を許可するか否かを決定する開錠決定部(S106, S212)と、前記錠前の開錠を許可する場合には、自装置にて記憶されているパスワードであって、前記錠前装置パスワードに対応するパスワードであるサーバパスワードを前記ユーザに通知するための処理を行うパスワード通知部(S108, S214)として、コンピュータを動作させること、を特徴とするサーバ用プログラム。

10

【0111】

このような構成によれば、サーバにて、携帯端末から受信した装置識別情報とユーザ識別情報とに基づき錠前の開錠を許可するか否かが決定され、開錠が許可された場合には、錠前を開錠するためのパスワードがユーザに通知される。これにより、錠前装置や携帯端末を解析しても、ユーザの開錠を許可するか否かを決定する処理の内容を把握できなくなるため、錠前のセキュリティ性を向上させることができる。

20

【0112】

(n) 錠前(27)を開錠する錠前装置(20)を識別するための装置識別情報と、該錠前を開錠するユーザを識別するためのユーザ識別情報とをサーバに送信する識別情報送信手順(S104)と、前記サーバにて、前記識別情報送信手順で該サーバに送信された前記装置識別情報と前記ユーザ識別情報とに基づき、前記錠前の開錠を許可するか否かを決定する開錠決定手順(S104, S204)と、前記開錠決定手順にて前記錠前の開錠を許可すると決定された場合には、前記サーバに記憶されている該開錠を行うためのパスワードを、前記ユーザに通知するパスワード通知手順(S108~S112, S214~S218)と、前記ユーザが、前記パスワード通知手順にて通知された前記パスワードを、前記錠前装置に入力するパスワード入力手順(S114, S220)と、前記パスワード入力手順にて入力された前記パスワードが、前記錠前装置に記憶されている錠前装置パスワードに対応する場合には、前記錠前の開錠する開錠手順(S116, S222)と、を備えることを特徴とする開錠方法。

30

【0113】

このような開錠方法によれば、ユーザが錠前の開錠を行う際には、錠前装置識別情報とユーザ識別情報がサーバに送信され、サーバにて該ユーザによる開錠を許可するか否かが決定される。そして、開錠を許可する場合には、サーバにて記憶されているサーバパスワードが該ユーザに通知され、通知されたサーバパスワードが錠前装置に入力されると錠前が開錠される。

40

【0114】

このため、錠前装置を解析しても、ユーザの開錠を許可するか否かを決定する処理の内容を把握できない。また、ユーザが自ら錠前装置にパスワードを入力するため、錠前装置との間の通信が傍受されてパスワードが漏えいすることを未然に防ぐことができる。したがって、錠前のセキュリティ性を向上させることができる。

【0115】

なお、上記実施形態の説明で用いた用語と、発明(a)~(n)の記載に用いた用語との対応を示す。

第1, 第2実施形態における認証用サーバ30がサーバの一例に相当し、装置IDが装

50

置識別情報の一例に、ユーザIDがユーザ識別情報の一例に相当する。

【0116】

また、端末用アプリが携帯端末用プログラムの一例に相当し、サーバ用アプリがサーバ用プログラムの一例に相当する。また、開錠処理により実現される方法が、開錠方法の一例に相当する。

【0117】

また、第1実施形態の開錠処理のS102が識別情報提供部，識別情報取得部の一例に、S104が識別情報送信部，識別情報受信部，識別情報送信手順の一例に、S106が開錠決定部，開錠決定手順の一例に相当する。

【0118】

また、S108がパスワード通知部の一例に、S108～S112がパスワード通知手順の一例に、S110がパスワード受信部の一例に、S112が報知部の一例に、S114がパスワード受付部，パスワード入力手順の一例に、S116が開錠部，開錠手順の一例に相当する。

【0119】

また、S118が開錠通知部，携帯端末記録部，開錠通知中継部の一例に、S120が開錠通知中継部，サーバ記録部の一例に、S122が錠前装置更新部の一例に、S124が携帯端末記録部の一例に、S126がサーバ更新部の一例に、S128がサーバ記録部の一例に相当する。

【0120】

また、第2実施形態の開錠処理のS202が識別情報取得部，識別情報提供部の一例に、S204が識別情報送信部，識別情報受信部，識別情報送信手順の一例に、S206が時間情報送信部，時間情報中継部の一例に、S208が時間情報中継部，時間調整部の一例に相当する。

【0121】

また、S210が時間調整部の一例に、S212が開錠決定部，開錠決定手順の一例に、S214がパスワード通知部の一例に、S214～S218がパスワード通知手順の一例に、S216がパスワード受信部の一例に、S218が報知部の一例に相当する。

【0122】

また、S220がパスワード受付部，パスワード入力手順の一例に、S222が開錠部，開錠手順の一例に、S224が開錠通知部，携帯端末記録部，開錠通知中継部の一例に、S226が開錠通知中継部，サーバ記録部の一例に、S228が携帯端末記録部の一例に、S230がサーバ記録部の一例に相当する。

【0123】

また、錠前装置パスワード更新処理のS300，S305が錠前装置更新部の一例に、サーバパスワード更新処理のS400，S405がサーバ側更新部の一例に相当する。

[特許請求の範囲との対応]

上記実施形態の説明で用いた用語と、特許請求の範囲の記載に用いた用語との対応を示す。

【0124】

第1，第2実施形態における認証用サーバ30がサーバの一例に相当し、装置IDが装置識別情報の一例に、ユーザIDがユーザ識別情報の一例に相当する。

また、第1実施形態の開錠処理のS102が識別情報提供部，識別情報取得部の一例に、S104が識別情報送信部，識別情報受信部の一例に、S106が開錠決定部の一例に、S108がパスワード通知部の一例に、S110がパスワード受信部の一例に、S112が報知部の一例に、S114がパスワード受付部の一例に、S116が開錠部の一例に相当する。

【0125】

また、第2実施形態の開錠処理のS202が識別情報取得部，識別情報提供部の一例に、S204が識別情報送信部，識別情報受信部の一例に、S212が開錠決定部の一例に

10

20

30

40

50

、 S 2 1 4 がパスワード通知部の一例に、 S 2 1 6 がパスワード受信部の一例に、 S 2 1 8 が報知部の一例に、 S 2 2 0 がパスワード受付部の一例に、 S 2 2 2 が開錠部の一例に相当する。

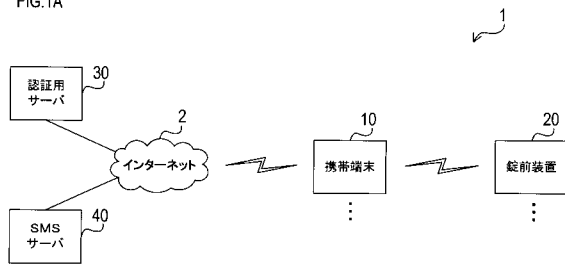
【符号の説明】

【 0 1 2 6 】

1 ... 開錠システム、 2 ... インターネット、 10 ... 携帯端末、 11 ... 近距離通信部、 12 ... 電話通信部、 13 ... 記憶部、 14 ... 制御部、 15 ... 表示部、 16 ... 操作部、 20 ... 錠前装置、 21 ... 近距離通信部、 22 ... 記憶部、 23 ... 表示部、 24 ... 操作部、 25 ... 制御部、 26 ... 錠前制御部、 27 ... 錠前、 28 ... 収容状態センサ、 30 ... 認証用サーバ、 31 ... 通信部、 32 ... 記憶部、 33 ... 制御部、 34 ... 表示部、 35 ... 操作部。

【 図 1 】

FIG.1A



【 図 2 】

FIG.2A

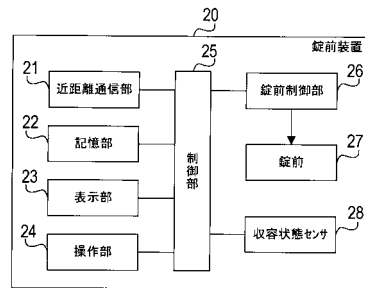


FIG.1B

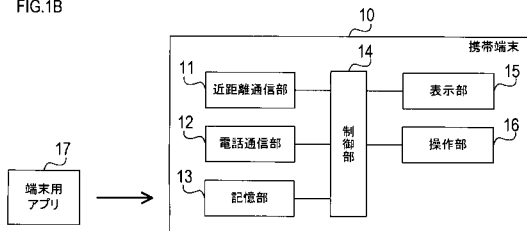
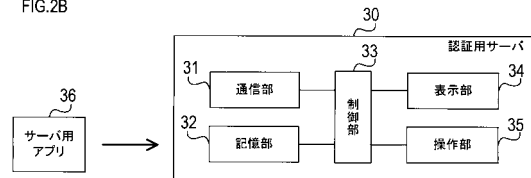


FIG.2B



【 図 3 】

FIG.3A

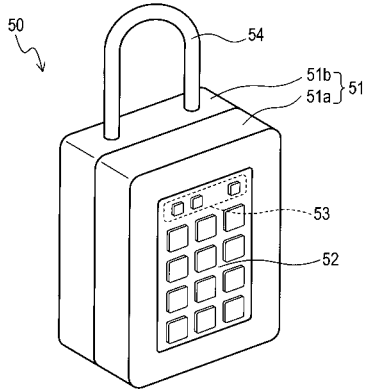
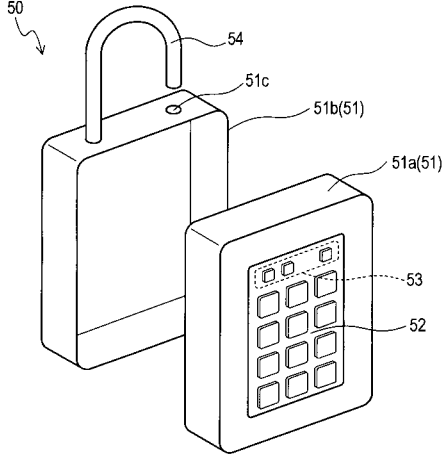
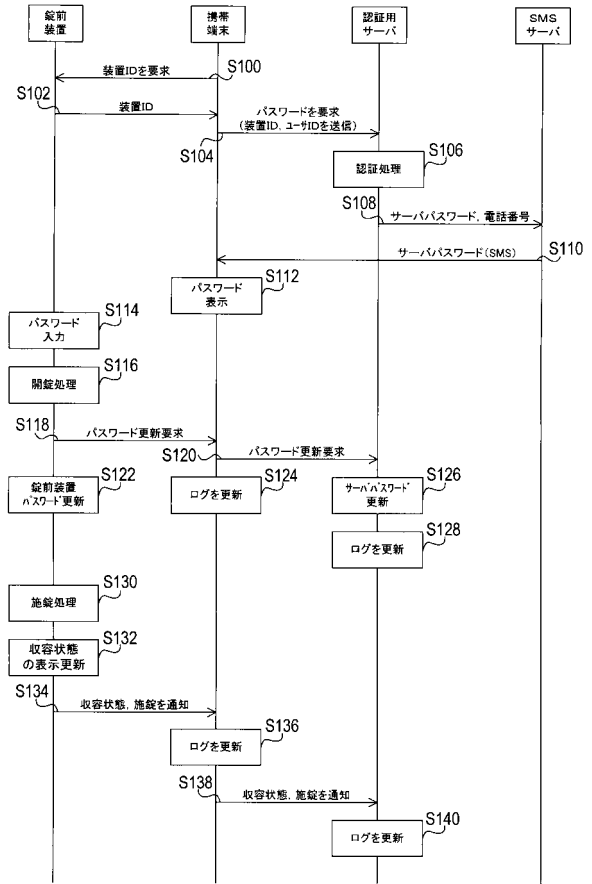


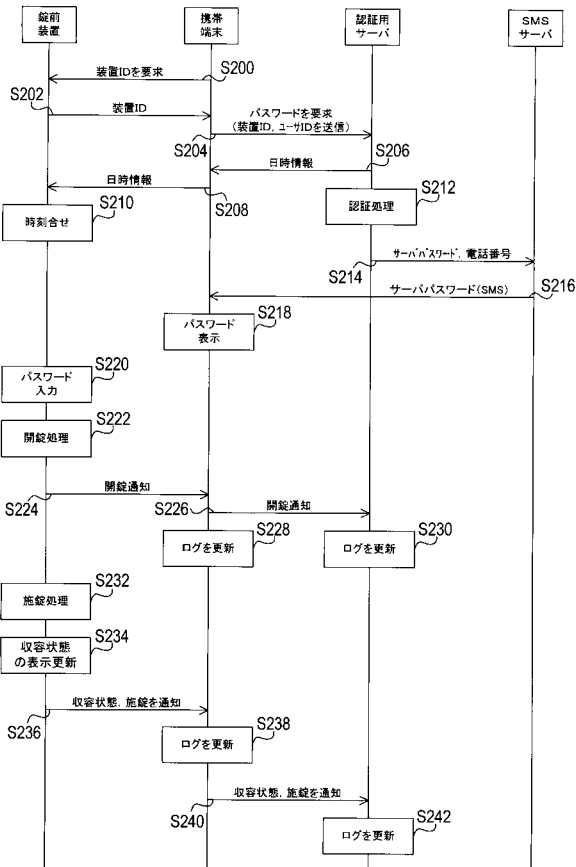
FIG.3B



【 図 4 】



【 図 5 】



【 図 6 】

FIG.6A

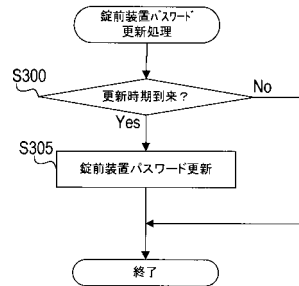
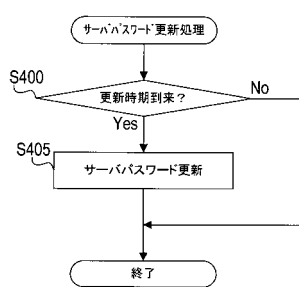


FIG.6B



フロントページの続き

(72)発明者 田中 優成

東京都世田谷区三軒茶屋2丁目1番2号 サンタワーズセンタービル12階 インディゴ株式会社内

Fターム(参考) 2E250 AA02 AA03 AA06 BB08 BB47 DD02 FF06 FF35