

(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2012-207452

(P2012-207452A)

(43) 公開日 平成24年10月25日(2012.10.25)

(51) Int.Cl.	F I	テーマコード (参考)
<b>E05B 49/00 (2006.01)</b>	E05B 49/00 F	2E250
<b>G06Q 50/10 (2012.01)</b>	E05B 49/00 J	
<b>G06Q 10/00 (2012.01)</b>	G06F 17/60 124	
	G06F 17/60 506	
	G06F 17/60 510	

審査請求 未請求 請求項の数 10 O L (全 21 頁)

(21) 出願番号 特願2011-74089 (P2011-74089)  
 (22) 出願日 平成23年3月30日 (2011.3.30)

(71) 出願人 000232254  
 日本電気通信システム株式会社  
 東京都港区三田1丁目4番28号  
 (74) 代理人 100093595  
 弁理士 松本 正夫  
 (72) 発明者 岩瀬 充明  
 東京都港区三田一丁目4番28号 日本電  
 気通信システム株式会社内  
 Fターム(参考) 2E250 AA19 BB08 BB09 BB29 BB46  
 BB65 CC16 CC27 DD06 EE02  
 FF28 GG06 GG13

(54) 【発明の名称】 鍵開閉システム、施錠管理装置、施錠管理方法、及び施錠管理プログラム

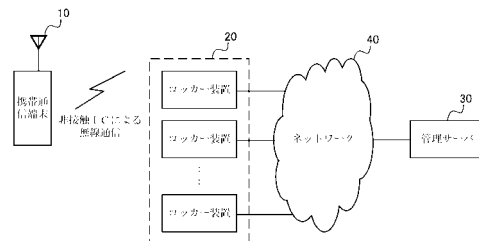
(57) 【要約】 (修正有)

【課題】 携帯通信端末に搭載される非接触ICを用いて施錠・解錠を行うロッカー装置の提供。

【解決手段】 鍵開閉システム100が、非接触ICを備える1つ以上の携帯通信端末10と、複数のロッカーを備えるロッカー装置20と、ロッカーの鍵の開閉を管理する施錠管理装置と、各ロッカーの所定の情報及びロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを管理する管理サーバ30とを備え、施錠管理装置が、非接触ICリーダ/ライタ手段と、ロッカーの施錠時に鍵情報ファイルを生成する鍵情報ファイル生成手段と、ロッカーの鍵の開閉を制御する鍵開閉制御手段とを含み、鍵情報ファイルが生成された場合鍵情報ファイルを携帯通信端末及び管理サーバへ送信し、携帯通信端末から鍵情報ファイルを受信した場合当該ロッカーに関する鍵情報ファイルを管理サーバから取得し、双方の解錠キー情報が同一である場合、ロッカーの解錠を行う。

【選択図】 図1

鍵開閉システム100



**【特許請求の範囲】****【請求項 1】**

非接触 IC を備える 1 つ以上の携帯通信端末と、  
複数のロッカーを備えるロッカー装置と、  
前記携帯通信端末による前記ロッカーの鍵の開閉を管理する施錠管理装置と、  
前記各ロッカーの所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを管理する管理サーバとを備え、  
前記施錠管理装置が、  
前記非接触 IC とデータの送受信を行う非接触 IC リード/ライター手段と、  
所定の前記ロッカーの施錠時に、当該ロッカーに関する前記鍵情報ファイルを生成する  
鍵情報ファイル生成手段と、  
前記ロッカーの鍵の開閉を制御する鍵開閉制御手段とを含み、  
前記鍵開閉制御手段が、  
前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報  
ファイルの前記携帯通信端末及び前記管理サーバへ送信し、  
所定の前記携帯通信端末から前記非接触 IC リード/ライター手段を介して前記鍵情報フ  
ァイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッ  
カーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの  
解錠キー情報が同一である場合、当該ロッカーの解錠を行う  
ことを特徴とする鍵開閉システム。 10

**【請求項 2】**

前記鍵情報ファイルが、  
前記ロッカーの情報として、少なくとも当該ロッカーを備える前記ロッカー装置の所在  
地及び当該ロッカーを識別するためのロッカー番号を含むことを特徴とする請求項 1 に記  
載の鍵開閉システム。

**【請求項 3】**

前記鍵開閉制御手段は、  
前記非接触 IC リード/ライター手段を介して、前記非接触 IC へ前記鍵情報ファイルを送  
信し、  
前記携帯通信端末は、  
受信した前記鍵情報ファイルを前記非接触 IC へ読み込ませる制御手段を備える  
ことを特徴とする請求項 1 又は請求項 2 に記載の鍵開閉システム。 30

**【請求項 4】**

前記携帯通信端末が、  
一時的にデータを保存するメモリを備え、  
前記制御手段が、  
前記非接触 IC を介して受信した前記鍵情報ファイルを前記メモリに保存し、前記メモ  
リに保存した鍵情報ファイルを前記非接触 IC に読み込ませ、その後、前記メモリに保存  
されている鍵情報ファイルを削除する  
ことを特徴とする請求項 3 に記載の鍵開閉システム。 40

**【請求項 5】**

前記携帯通信端末は、  
他の前記携帯通信端末から所定の鍵情報ファイルを受信すると、前記制御手段が、受信  
した前記鍵情報ファイルを、非接触 IC へ読み込ませることを特徴とする請求項 3 又は請  
求項 4 に記載の鍵開閉システム。

**【請求項 6】**

前記管理サーバが、  
前記鍵情報ファイルを格納する鍵情報ファイル格納手段と、  
前記施錠管理装置からの要求に応じて、所定の鍵情報ファイルを前記鍵情報ファイル格  
納手段から取得し、前記施錠管理装置へ送信する鍵情報ファイル管理手段と 50

を備えることを特徴とする請求項 1 から請求項 5 の何れか 1 項に記載の鍵開閉システム。

【請求項 7】

非接触 IC を備える 1 つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置であって、

前記非接触 IC とデータの送受信を行う非接触 IC リーダ/ライタ手段と、

所定の前記ロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む前記鍵情報ファイルを生成する鍵情報ファイル生成手段と、

前記ロッカーの鍵の開閉を制御する鍵開閉制御手段とを含み、

前記鍵開閉制御手段が、

前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報ファイルを、前記携帯通信端末及び前記鍵情報ファイルを管理する前記管理サーバへ送信し、

所定の前記携帯通信端末から前記非接触 IC リーダ/ライタ手段を介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う

ことを特徴とする施錠管理装置。

【請求項 8】

前記鍵情報ファイルが、

前記ロッカーの情報として、少なくとも当該ロッカーを備える前記ロッカー装置の所在地及び当該ロッカーを識別するためのロッカー番号を含むことを特徴とする請求項 7 に記載の施錠管理装置。

【請求項 9】

非接触 IC を備える 1 つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置による施錠管理方法であって、

所定の前記ロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む前記鍵情報ファイルを生成する鍵情報ファイル生成ステップと、

前記ロッカーの鍵の開閉を制御する鍵開閉制御ステップとを含み、

前記鍵開閉制御ステップで、

前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報ファイルを、前記携帯通信端末及び前記鍵情報ファイルを管理する前記管理サーバへ送信し、

所定の前記携帯通信端末から前記非接触 IC を介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う

ことを特徴とする施錠管理方法。

【請求項 10】

非接触 IC を備える 1 つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置上で動作する施錠管理プログラムであって、

前記施錠管理装置に、

所定の前記ロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む前記鍵情報ファイルを生成する鍵情報ファイル生成処理と、

前記ロッカーの鍵の開閉を制御する鍵開閉制御処理をと実行させ、

前記鍵開閉制御処理で、

前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報

10

20

30

40

50

報ファイルを、前記携帯通信端末及び前記鍵情報ファイルを管理する前記管理サーバへ送信し、

所定の前記携帯通信端末から前記非接触ＩＣを介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う

ことを特徴とする施錠管理プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コインロッカー等のロッカー装置の鍵管理技術に関し、特に、携帯通信端末に搭載される非接触ＩＣを用いてロッカー装置の施錠・解錠を行う技術に関する。

【背景技術】

【０００２】

コインロッカー等のロッカーシステムは、これまで、磁気カードやキー操作によるものが種であったが、近年、ＩＣカード等を用いた方式が増えつつある。そのような背景技術によるロッカーシステムの例が、例えば特許文献１、特許文献２に開示されている。

【０００３】

特許文献１に記載のロッカーシステムについて、図１５を参照して説明する。

【０００４】

特許文献１に記載のロッカーシステムは、錠管理装置１０２０が、錠付き戸棚１０１０の格納庫ごとに付された格納庫の識別コードに対応して、該格納庫を施錠した非接触型ＩＣカード１０５０の識別コードを記憶する。

【０００５】

また、錠管理装置１０２０は、該識別コードに対応して、利用者の移動体通信端末装置１０３０に付けられた電話番号、電子メールアドレス、利用者の氏名、住所、暗証番号等の個人情報をテーブルとして記憶しておく。

【０００６】

錠管理装置１０２０は、施錠者からの依頼を受ける等により、施錠が行われて使用中の格納庫に対応して記憶している非接触型ＩＣカード１０５０の識別コードを別の非接触型ＩＣカード１０５０の識別コードに書き換えた場合に、前述のテーブルから、新たに指定された非接触型ＩＣカード１０５０に対応する電話番号又は電子メールアドレスを引き出し、該電話番号又は電子メールアドレスを有する移動体通信端末装置１０３０に、該格納庫の解錠を促す案内（音声によるアナウンス又は電子メール）を送信する。

【０００７】

該案内には、錠管理装置１０２０が解錠すべき錠付き戸棚１０１０の格納庫１０１１の位置や施錠者の情報等を含めてもよい。

【０００８】

また、錠管理装置１０２０と移動体通信端末装置１０３０との間の通信は、施錠者から錠管理装置１０２０への依頼の手段としても使用出来る。

【０００９】

例えば、施錠者が錠管理装置１０２０の音声応答にて、施錠して使用中の格納庫１０１１の解錠を依頼したい他の利用者の非接触型ＩＣカード５０の識別コード、または、移動体通信端末装置３０の電話番号、電子メールアドレスを知らせ、錠管理装置１０２０が該情報にもとづき該テーブルのデータを更新するようにしてもよい。また、施錠者が電子メールにて前記と同じデータを錠管理装置１０２０へ送信し前記のデータ更新を要求してもよい。

【先行技術文献】

【特許文献】

【００１０】

10

20

30

40

50

【特許文献1】特開2003-337979号公報

【特許文献2】特開2010-209527号公報

【特許文献3】特開2007-131434号公報

【特許文献4】特開2009-293317号公報

【発明の概要】

【発明が解決しようとする課題】

【0011】

上述したように、引用文献1等の背景技術による発明は、携帯電話の非接触ICを利用してコインロッカーの施錠・解錠をする方法において、コインロッカーの施錠者が他の人に解錠させたいと考えた時、施錠者が携帯電話機を操作して、コインロッカーを管理する鍵管理装置に対して、施錠した非接触ICカード情報の変更要求を行うことにより、他の人が持つ非接触IC搭載の携帯電話機で解錠を可能とするものであった。

10

【0012】

しかし、このような方法では、以下のような課題がある。

【0013】

第1の課題は、コインロッカーの鍵管理は従来発明にある鍵管理装置が行っているため、コインロッカー施錠者が鍵管理装置に対してコインロッカー施錠情報の更新を依頼することになり、コインロッカー施錠者の携帯電話操作が煩雑になる、ということである。

【0014】

第2の課題は、コインロッカー施錠者が鍵管理装置に対してコインロッカー施錠情報の更新を依頼した後は、コインロッカーの解錠は他者のみになるため、コインロッカー施錠者自身の携帯電話を使って解錠することが出来ない、ということである。

20

【0015】

第3の課題は、コインロッカーの鍵施錠者が他の人に鍵の解錠をさせる為には、鍵管理装置に鍵施錠者と解錠者の携帯電話の電話番号、電子メールアドレスを取得しておく必要があるため、鍵施錠者、鍵解錠者、それぞれのプライベート情報のセキュリティ上の問題があるということである。

【0016】

また、特許文献2では、鍵情報の生成において、暗証情報入力装置で暗証情報を入力しているため、セキュリティの面において改善の余地がある。

30

【0017】

また、特許文献2では、暗証情報に「解錠するべき装置」の所在を判断する情報が含まれておらず、解錠するべきロッカーの地域・場所・ロッカーNoなどがわからないという課題がある。

【0018】

また、特許文献2では、解錠は鍵装置と携帯端末の間での暗証情報のやりとりのみで、可能となっており、セキュリティの面から改善の余地がある。

【0019】

(発明の目的)

本発明の目的は、上述の課題を解決し、携帯通信端末に搭載される非接触ICを用いてロッカー装置の施錠・解錠を行う鍵開閉システム、施錠管理装置、施錠管理方法、及び施錠管理プログラムを提供することである。

40

【課題を解決するための手段】

【0020】

本発明の第1の鍵開閉システムは、非接触ICを備える1つ以上の携帯通信端末と、複数のロッカーを備えるロッカー装置と、携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置と、各ロッカーの所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを管理する管理サーバとを備え、施錠管理装置が、非接触ICとデータの送受信を行う非接触ICリーダ/ライタ手段と、所定のロッカーの施錠時に、当該ロッカーに関する鍵情報ファイルを生成する鍵情報ファイル生成手段と、ロッカ

50

一の鍵の開閉を制御する鍵開閉制御手段とを含み、鍵開閉制御手段が、鍵情報ファイル生成手段によって鍵情報ファイルが生成された場合、当該鍵情報ファイルを携帯通信端末及び管理サーバへ送信し、所定の携帯通信端末から非接触ＩＣリーダ／ライタ手段を介して鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応するロッカーを特定し、当該ロッカーに関する鍵情報ファイルを管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う。

【 0 0 2 1 】

本発明の第１の施錠管理装置は、非接触ＩＣを備える１つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置であって、非接触ＩＣとデータの送受信を行う非接触ＩＣリーダ／ライタ手段と、所定のロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを作成する鍵情報ファイル生成手段と、ロッカーの鍵の開閉を制御する鍵開閉制御手段とを含み、鍵開閉制御手段が、鍵情報ファイル生成手段によって鍵情報ファイルが生成された場合、当該鍵情報ファイルを、携帯通信端末及び鍵情報ファイルを管理する管理サーバへ送信し、所定の携帯通信端末から非接触ＩＣリーダ／ライタ手段を介して鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応するロッカーを特定し、当該ロッカーに関する鍵情報ファイルを管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う。

10

【 0 0 2 2 】

本発明の第１の施錠管理方法は、非接触ＩＣを備える１つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置による施錠管理方法であって、所定のロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを作成する鍵情報ファイル生成ステップと、ロッカーの鍵の開閉を制御する鍵開閉制御ステップとを含み、鍵開閉制御ステップで、鍵情報ファイル生成手段によって鍵情報ファイルが生成された場合、当該鍵情報ファイルを、携帯通信端末及び鍵情報ファイルを管理する管理サーバへ送信し、所定の携帯通信端末から非接触ＩＣを介して鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応するロッカーを特定し、当該ロッカーに関する鍵情報ファイルを管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う。

20

【 0 0 2 3 】

本発明の第１の施錠管理プログラムは、非接触ＩＣを備える１つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置上で動作する施錠管理プログラムであって、施錠管理装置に、所定のロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを作成する鍵情報ファイル生成処理と、ロッカーの鍵の開閉を制御する鍵開閉制御処理をと実行させ、鍵開閉制御処理で、鍵情報ファイル生成手段によって鍵情報ファイルが生成された場合、当該鍵情報ファイルを、携帯通信端末及び鍵情報ファイルを管理する管理サーバへ送信し、所定の携帯通信端末から非接触ＩＣを介して鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応するロッカーを特定し、当該ロッカーに関する鍵情報ファイルを管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う。

30

40

【 発明の効果 】

【 0 0 2 4 】

本発明によれば、携帯通信端末に搭載される非接触ＩＣを用いてロッカー装置の施錠・解錠を行うことができる。

【 図面の簡単な説明 】

【 0 0 2 5 】

【 図 1 】本発明の第１の実施の形態による鍵開閉システムの構成を示すブロック図である。

【 図 2 】第１の実施の形態による携帯通信端末の構成を示すブロック図である。

50

【図 3】第 1 の実施の形態によるロッカー装置の構成を示すブロック図である。

【図 4】第 1 の実施の形態による施錠管理装置の構成を示すブロック図である。

【図 5】第 1 の実施の形態による携帯通信端末間の鍵情報ファイルの送受信の構成を示す図である。

【図 6】第 1 の実施の形態による鍵情報ファイルの構成例を示す図である。

【図 7】第 1 の実施の形態によるロッカー施錠時の動作を示すシーケンス図である。

【図 8】第 1 の実施の形態によるロッカー解錠時の動作を示すシーケンス図である。

【図 9】第 1 の実施の形態による管理サーバの構成を示すブロック図である。

【図 10】第 1 の実施の形態による鍵情報ファイルの転送の動作を示すシーケンス図である。

【図 11】本発明の鍵開閉システムの最小限の構成を示すブロック図である。

【図 12】本発明の第 1 の実施の形態による鍵開閉システムの特徴を示す図である。

【図 13】本発明の施錠管理装置のハードウェア構成例を示すブロック図である。

【図 14】本発明の携帯通信端末のハードウェア構成例を示すブロック図である。

【図 15】背景技術によるロッカーシステムの構成を示すブロック図である。

【発明を実施するための形態】

【0026】

本発明の上記及び他の目的、特徴及び利点を明確にすべく、添付した図面を参照しながら、本発明の実施形態を以下に詳述する。なお、上述の本願発明の目的のほか、他の技術的課題、その技術的課題を解決する手段及びその作用効果についても、以下の実施形態による開示によって明らかとなるものである。

【0027】

なお、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。

【0028】

(第 1 の実施の形態)

図 1 は、本発明の第 1 の実施の形態による鍵開閉システム 100 の構成を示すブロック図である。

【0029】

図 1 を参照すると、鍵開閉システム 100 は、携帯電話機等の携帯電話端末 10 と、1 つ以上のロッカー装置 20 (20-1 ~ 20-n) と、管理サーバ 30 とから構成される。

【0030】

ロッカー装置 20 と管理サーバ 30 とは、ネットワーク 40 を介しての通信を可能とする。また、携帯通信端末 10 とロッカー装置 20 とは、非接触 IC による無線通信を可能とする。なお、ロッカー装置 20 は、コインロッカー等を想定するが、これに限定はされない。

【0031】

ロッカー装置 20-1 ~ 20-n は、それぞれ、物理的に所定の地域に拡散配置されていてもよく、同一地域であってもよい。

【0032】

ここで、図 2 を参照すると、図 2 は、携帯通信端末 10 の構成を示すブロック図である。なお、本発明の本質的な特徴でない、一般的な携帯電話機の有する機能については、図示を省略する。

【0033】

図 2 を参照すると、携帯通信端末 10 は、制御手段 11 と、メモリ 12 と、非接触 IC 13 と、表示手段 14 とを備える。

【0034】

非接触 IC 13 は、一般に Felica (登録商標) などと呼ばれるものと同様に、非接触 IC のリーダ/ライタとの間で、データの通信を行う装置である。

10

20

30

40

50

## 【 0 0 3 5 】

非接触 IC 13 は、ロッカー装置 20 の施錠時に、後述するロッカー装置 20 の非接触 IC リーダ/ライタ手段 21 から、鍵情報ファイル 60 を受信する。

## 【 0 0 3 6 】

また、非接触 IC 13 は、ロッカー装置 20 の解錠時に、鍵情報ファイル 60 を、ロッカー装置 20 の非接触 IC リーダ/ライタ手段 21 に送信する。

## 【 0 0 3 7 】

制御手段 11 は、所定の鍵管理用プログラムを実行し、該鍵管理用プログラムを介して、非接触 IC 13 へ鍵情報ファイル 60 を読み込ませる。

## 【 0 0 3 8 】

また、制御手段 11 は、所定の鍵管理用プログラムを実行し、該鍵管理用プログラムを介して、非接触 IC 13 に取り込んである鍵情報ファイル 60 を再生成し、メモリ 12 へ一時保存する。

## 【 0 0 3 9 】

ここで、鍵管理用プログラムとは、非接触 IC 13 の鍵情報ファイル 60 へアクセスできるプログラムをいう。非接触 IC 13 内のデータ保存領域はセキュアな領域であるため、該鍵管理用プログラムを用いることで非接触 IC 13 の鍵情報ファイル 60 へアクセスできる。同様に、非接触 IC 13 へ鍵情報ファイル 60 を読み込ませる処理も、該鍵管理用プログラムを用いて行う。

## 【 0 0 4 0 】

図 3 は、ロッカー装置 20 の構成を示すブロック図である。なお、図 3 には、ロッカー装置 20 の接続状態を説明するために、ネットワーク 40 と管理サーバ 30 についても、便宜上図示している。

## 【 0 0 4 1 】

ロッカー装置 20 は、1 つ以上のロッカー 21 ( 21 - 1 ~ 21 - m ) と、施錠管理装置 22 とを備える。

## 【 0 0 4 2 】

ロッカー 21 は、鍵がかけられる戸棚等である。

## 【 0 0 4 3 】

施錠管理装置 22 は、ロッカー 21 の施錠・解錠を管理する装置である。

## 【 0 0 4 4 】

ここで、施錠管理装置 22 の構成を図 4 に示す。図 4 を参照すると、施錠管理装置 22 は、非接触 IC リーダ/ライタ手段 221 と、鍵情報ファイル 60 を生成する鍵情報ファイル生成手段 222 と、ネットワーク 40 を介して管理サーバ 30 と通信を行う通信手段 223 と、ロッカー 21 の鍵の開閉を行う鍵開閉制御手段 224 とを備える。

## 【 0 0 4 5 】

非接触 IC リーダ/ライタ手段 221 は、一般に Felica ( 登録商標 ) などと呼ばれる非接触 IC のリーダー/ライタの役割を行う機能を有する。

## 【 0 0 4 6 】

非接触 IC リーダ/ライタ手段 221 は、非接触 IC 13 との間で鍵情報ファイルの送受信を行う。

## 【 0 0 4 7 】

ここで、鍵情報ファイル 60 の構成例を図 6 に示す。鍵情報ファイル 60 は、ヘッダ部 61 と、テキスト部 62 と、鍵情報部 63 とから構成される。

## 【 0 0 4 8 】

ヘッダ部 61 は、ファイルのバージョン、形式などの規定情報を含む。

## 【 0 0 4 9 】

テキスト部 62 は、ロッカー装置 20 の所在地を示す情報を含む。所在地を含む情報は、例えば該所在地を示す地図情報の URL 等である。

## 【 0 0 5 0 】

10

20

30

40

50

鍵情報部 6 3 は、ロッカー装置 2 0 の所在地と、ロッカー 2 1 - m のロッカー番号と、解錠キー情報とを含む。

【 0 0 5 1 】

なお、ヘッダ部 6 1、テキスト部 6 2、鍵情報部 6 3 の記述フォーマットなどは、任意のものが可能であるものとする。図 6 においては、現在一般に普及されているトルカ ( T o r u c a ) ( 登録商標 ) を参考に記載したものである。また、鍵情報部 6 3 については、情報漏えいの観点から、暗号化してもよいものとする。

【 0 0 5 2 】

ここで、管理サーバ 3 0 の構成を、図 9 のブロック図に示す。図 9 を参照すると、管理サーバ 3 0 は、と、鍵情報ファイル 6 0 の管理を行う鍵情報ファイル管理手段 3 1 と、下記情報ファイル 6 0 を格納する鍵情報ファイル格納手段 3 2 と、施錠管理装置 2 2 と通信を行う通信手段 3 3 を備える。

10

【 0 0 5 3 】

次に、本実施の形態における、携帯通信端末間の鍵情報ファイルの送受信の構成を、図 5 に示す。

【 0 0 5 4 】

図 5 において、携帯通信端末 1 0 a が、ロッカー装置 2 0 の所定のロッカー 2 1 - m を施錠したものである。携帯通信端末 1 0 a は、非接触 I C 1 3 を搭載している。

【 0 0 5 5 】

携帯通信端末 1 0 a は、ロッカー装置 2 0 の所定のロッカー 2 1 - m を施錠した際に施錠管理装置 2 2 から取得した鍵情報ファイル 6 0 を、電子メールに添付して携帯通信端末 1 0 b へ送信する。該電子メールは、基地局 5 0 a、ネットワーク 4 0、基地局 5 0 b を経由して、携帯通信端末 1 0 b へ到着する。

20

【 0 0 5 6 】

電子メールを受け取った携帯通信端末 1 0 b は、該電子メールに添付されている鍵情報ファイルを取得し、自装置の非接触 I C 1 3 に取り込む。

【 0 0 5 7 】

なお、電子メールで所定の情報やファイルを添付して送受信する方法については、一般的に実現されている事項なので詳述しない。

【 0 0 5 8 】

( 第 1 の実施の形態の動作の説明 )

次に、本実施の形態による鍵開閉システム 1 0 0 の動作について、図面を参照して詳細に説明する。

30

【 0 0 5 9 】

( ロッカーの施錠時の動作の説明 )

まず、携帯通信端末 1 0 が、所定のロッカー 2 1 - m を施錠する動作について説明する。図 7 は、本実施の形態によるロッカー施錠時の動作を示すシーケンス図である。なお、ここでは、携帯通信端末 1 0 a が、所定のロッカー 2 1 - m を施錠する動作を例として説明を行う。

【 0 0 6 0 】

図 7 を参照すると、まず、携帯通信端末 1 0 a のユーザが、ロッカー 2 1 - m に荷物などを入れる ( ステップ S 7 0 1 ) 。

40

【 0 0 6 1 】

次いで、該ユーザが、ロッカー 2 1 m の番号などの情報を施錠管理装置 2 2 にて入力した後、携帯通信端末 1 0 a を施錠管理装置 2 2 に近づける ( ステップ S 7 0 2 ) 。

【 0 0 6 2 】

次いで、施錠管理装置 2 2 の非接触 I C リーダ / ライタ手段 2 2 1 が、携帯通信端末 1 0 a の非接触 I C 1 3 と通信を開始する ( ステップ S 7 0 3 ) 。

【 0 0 6 3 】

ここで、非接触 I C ( 一般に F e l i c a ( 登録商標 ) などと呼ばれるものを含む ) と

50

非接触ＩＣリーダー／ライタの無線通信は、非接触ＩＣリーダー／ライタの発生する電磁誘導により、非接触ＩＣに対して電力を発生させる事により、両者間の通信が可能となる。両者間の通信確立方法については、周知の事項なので詳述しない。

【００６４】

次いで、施錠管理装置２２の鍵情報ファイル生成手段２２２が、ロッカー２１－ｍの鍵情報ファイル６０を生成し（ステップＳ７０４）、非接触ＩＣリーダー／ライタ手段２２１が、該鍵情報ファイル６０を、非接触ＩＣ１３へ送信する（ステップＳ７０５）。

【００６５】

携帯通信端末１０ａの非接触ＩＣ１３は、受信した鍵情報ファイル６０を、メモリ１２に格納し、次いで、制御手段１２が、該鍵情報ファイル６０を非接触ＩＣ１３に読み込ませる（ステップＳ７０６）。

10

【００６６】

次いで、制御手段１１が、非接触ＩＣ１３を介して、鍵情報ファイル６０を受信した旨を示す「鍵情報ファイル取得通知」を施錠管理装置２２に送信する（ステップＳ７０７）。

【００６７】

非接触ＩＣリーダー／ライタ手段２２１が「鍵情報ファイル取得通知」を受信すると、鍵開閉制御手段２２４が、ロッカー２１－ｍの施錠を行う（ステップＳ７０８）。

【００６８】

次いで、鍵開閉制御手段２２４が、非接触ＩＣリーダー／ライタ手段２２１を介して、施錠した旨を示す「施錠確認通知」を送信する（ステップＳ７０９）。

20

【００６９】

非接触ＩＣ１３が「施錠確認通知」を受信すると、制御手段１１が、該鍵情報ファイル６０に含まれる鍵情報部６３の内容（ロッカー２１－ｍの所在地とロッカー番号）を、表示手段１３へ表示する（ステップＳ７１０）。

【００７０】

次いで、制御手段１１は、非接触ＩＣ１３を介して、ロッカーが施錠された事を確認した旨を示す「施錠確認通知」を送信する（ステップＳ７１１）。

【００７１】

また、制御手段１１は、メモリ１２に格納されている鍵情報ファイル６０を破棄する（ステップＳ７１２）。これにより、鍵情報ファイル６０の情報は非接触ＩＣ１３にだけ存在することとなる。

30

【００７２】

次いで、非接触ＩＣリーダー／ライタ手段２２１が「施錠確認通知」を受信すると、施錠管理装置２２は、その旨を所定の表示部へ表示する（ステップＳ７１３）。該表示部及び表示の方法は本発明の本質的な特徴ではないので、詳細は省略する。

【００７３】

次いで、施錠管理装置２２は、ロッカー２１－ｍの鍵情報ファイル６０を、管理サーバ３０へ送信する（ステップＳ７１４）。

【００７４】

管理サーバ３０は、通信手段３１が該鍵情報ファイル６０を受信すると、鍵情報ファイル管理手段３１が、該鍵情報ファイル６０を鍵情報ファイル格納手段３２へ格納する（ステップＳ７１５）。

40

【００７５】

（鍵情報ファイルの転送の動作の説明）

次に、ロッカー２１－ｍの鍵情報ファイル６０の転送の動作について説明する。

【００７６】

図１０は、本実施の形態による鍵情報ファイルの転送の動作を示すシーケンス図である。

【００７７】

50

図10を参照すると、まず、携帯通信端末10aが、鍵情報ファイル60を添付した電子メールを携帯通信端末10bへ送信する(ステップS1001)。

【0078】

この時、携帯通信端末10aは、ユーザの操作による指示により、制御手段11が鍵管理用プログラムを実行し、該鍵管理用プログラムを介して非接触IC13に取り込んである鍵情報ファイルを再生成し、メモリ12に一時保存する。そして、メモリ12に一時保存された鍵情報ファイル60を、電子メールに添付して送信する。一時保存された鍵情報ファイル60は、電子メール送信後、破棄される。

【0079】

携帯通信端末10bが該電子メールを受信すると、制御手段12が、受信した鍵情報ファイル60を、メモリ12に格納する(ステップS1002)。

10

【0080】

次いで、制御手段12が、鍵管理用プログラムを実行し、該鍵管理用プログラムを介して、メモリ12に格納されている該鍵情報ファイル60を非接触IC13に読み込ませ(ステップS1003)、さらに、該鍵情報ファイル60に含まれる鍵情報部63の情報であるロッカー21-mの所在地とロッカー番号を、表示手段13へ表示する(ステップS1004)。

【0081】

次いで、制御手段12が、メモリ12の鍵情報ファイル60を削除する(ステップS1005)。

20

【0082】

なお、電子メールによるデータの送受信する方法については、既存技術で実現されている事項なので詳述しない。また、鍵情報ファイル60の送付先は、複数であっても良い。

【0083】

(他の携帯通信端末によるロッカー解錠の動作の説明)

次に、ロッカー21-mを施錠した携帯通信端末10aからロッカー21-mの鍵情報ファイル60を受信して自端末の非接触ICに読み込ませた携帯通信端末10bが、ロッカー21-mを解錠する動作について説明する。

【0084】

図8は、本実施の形態によるロッカー解錠時の動作を示すシーケンス図である。

30

【0085】

図8を参照すると、まず、携帯通信端末10bのユーザが、携帯通信端末10bを施錠管理装置22にかざす(ステップS901)。

【0086】

次いで、施錠管理装置22の非接触ICリーダ/ライタ手段221が、携帯通信端末10bの非接触IC13と通信を開始する(ステップS802)。

【0087】

次いで、施錠管理装置22の鍵開閉制御手段224が、非接触ICリーダ/ライタ手段221を介して、鍵情報ファイルの要求を示す「鍵情報要求通知」を非接触IC13へ送信する(ステップS803)。

40

【0088】

「鍵情報要求通知」を非接触IC13が受信すると、制御手段11が、鍵管理用プログラムを実行し、該鍵管理用プログラムを介して、非接触IC13内の鍵情報ファイル60を再生成してメモリ12に一時保存し(ステップS804)、非接触IC13を介して該鍵情報ファイル60を非接触ICリーダ/ライタ手段221へ送信する(ステップS805)。なお、メモリ12に一時保存された鍵情報ファイル60は、その後破棄される。

【0089】

非接触ICリーダ/ライタ手段221が鍵情報ファイル60を受信すると、鍵開閉制御手段224が、鍵情報ファイル60から解錠対象のロッカー21(以下、ロッカー21-mとする)を特定し、管理サーバ30に対し、該ロッカー21-mの鍵情報ファイル60

50

を要求する（ステップ S 8 0 6）。

【 0 0 9 0 】

該要求を受けた管理サーバ 3 0 は、鍵情報ファイル管理手段 3 1 が、鍵情報ファイル格納手段 3 2 から、ロッカー 2 1 - m の鍵情報ファイル 6 0 を取得し、該鍵情報ファイル 6 0 を施錠管理装置 2 2 へ送信する（ステップ S 8 0 7）。

【 0 0 9 1 】

次いで、施錠管理装置 2 2 の鍵開閉制御手段 2 2 4 は、携帯通信端末 1 0 b から取得した鍵情報ファイル 6 0 と、管理サーバ 3 0 から取得した鍵情報ファイル 6 0 との解錠キー情報が同一であるか否かを確認し（ステップ S 8 0 8）、同一である場合、ロッカー 2 1 - m を解錠する（ステップ S 8 0 9）。

10

【 0 0 9 2 】

なお、鍵情報ファイル 6 0 が同一でない場合は、当然ながら解錠は行わず、エラーとして処理が終了する。

【 0 0 9 3 】

次いで、鍵開閉制御手段 2 2 4 は、非接触 IC リーダ/ライタ手段 2 2 1 を介して、ロッカー 2 1 - m の解錠を行った旨を携帯通信端末 1 0 b へ送信するとともに（ステップ S 8 1 0）、その旨を施錠管理装置 2 2 の所定の表示部へ表示する（ステップ S 8 1 1）。

【 0 0 9 4 】

携帯通信端末 1 0 b は、非接触 IC 1 3 が施錠管理装置 2 2 から解錠の旨を受信すると、制御手段 1 1 が、その旨を表示手段 1 3 へ表示する（ステップ S 8 1 2）。

20

【 0 0 9 5 】

次いで、携帯通信端末 1 0 b は、制御手段 1 1 が、非接触 IC 1 3 に格納されている鍵情報ファイル 6 0 を破棄するとともに（ステップ S 8 1 3）、ロッカー 2 1 - m の解錠を確認した旨を施錠管理装置 2 2 へ送信する（ステップ S 8 1 4）。

【 0 0 9 6 】

次いで、施錠管理装置 2 2 の鍵開閉制御手段 2 2 4 が、管理サーバ 3 0 に対し、ロッカー 2 1 - m の鍵情報ファイル 6 0 を削除する旨の要求を、通信手段 2 2 3 を介して行う（ステップ S 8 1 5）。

【 0 0 9 7 】

次いで、管理サーバ 3 0 の鍵情報ファイル管理手段 3 1 が、鍵情報ファイル格納手段 3 2 から、ロッカー 2 1 - m の鍵情報ファイル 6 0 を削除する（ステップ S 8 1 6）。

30

携帯電話機 1 0 b のユーザは、解錠されたコインロッカー 2 1 - m から手動にて荷物を取り出す（ステップ S 8 1 7）。

【 0 0 9 8 】

（第 1 の実施の形態による効果）

【 0 0 9 9 】

本実施の形態によれば、以下の効果を奏する。

【 0 1 0 0 】

第 1 の効果は、ロッカー 2 1 の鍵情報ファイル 6 0 を電子メールで他の非接触 IC 1 3 搭載の携帯通信端末 1 0 に送信するので、管理サーバ 3 0 への鍵情報変更手続きの煩わしさを削減できることである。

40

【 0 1 0 1 】

第 2 の効果は、ロッカー 2 1 の施錠者自身の携帯通信端末 1 0 にも、非接触 IC 1 3 内部に鍵情報ファイル 6 0 を保存しているので、鍵情報ファイル 6 0 を他の携帯通信端末 1 0 に送信した後でも、施錠者の携帯通信端末 1 0 でコインロッカーの解錠ができることである。

【 0 1 0 2 】

第 3 の効果は、管理サーバ 3 0 には、鍵施錠者と解錠者の電話番号、電子メールアドレス等を登録しておく必要がないので、ロッカー 2 1 の鍵施錠者、鍵解錠者それぞれのプライベート情報のセキュリティが保たれることである。

50

## 【0103】

なお、本発明の課題を解決できる最小限の構成を図11に示す。施錠管理装置22が、非接触IC13を備える1つ以上の携帯通信端末10によるロッカー21の鍵の開閉を管理する施錠管理装置22であって、非接触IC13とデータの送受信を行う非接触ICリーダー/ライター手段221と、所定のロッカー21の施錠時に、当該ロッカー21に関する所定の情報及び当該ロッカー21の鍵を解錠するための解錠キー情報を含む鍵情報ファイル60を生成する鍵情報ファイル生成手段222と、ロッカーの鍵の開閉を制御する鍵開閉制御手段224とを含み、鍵開閉制御手段224が、鍵情報ファイル生成手段222によって鍵情報ファイル60が生成された場合、当該鍵情報ファイル60を、携帯通信端末10及び鍵情報ファイル60を管理する管理サーバ30へ送信し、所定の携帯通信端末10から非接触ICリーダー/ライター手段221を介して鍵情報ファイル60を受信した場合、当該鍵情報ファイル60に対応するロッカー21を特定し、当該ロッカー21に関する鍵情報ファイル60を管理サーバ30から取得し、双方の鍵情報ファイル60の解錠キー情報が同一である場合、当該ロッカー21の解錠を行うことで、上述した本発明の課題を解決することができる。

10

## 【0104】

(第2の実施の形態)

次に、本発明の第2の実施の形態について説明する。なお、鍵開閉システム100構成は第1の実施の形態と同様であるため、図示は省略する。

## 【0105】

第1の実施例では、鍵施錠者の携帯通信端末10aから、他の携帯通信端末10bへ鍵情報ファイルを送信することで、該携帯通信端末10bでもロッカー21の解錠を可能としている。

20

## 【0106】

これに対し、本実施の形態では、鍵情報ファイルを受信した携帯通信端末10が、さらに他の携帯通信端末10へ該鍵情報ファイルを電子メールにて送信する。該送信の機能は、第1の実施の形態で説明した携帯通信端末10aの機能により実現できるため、説明は省略する。

## 【0107】

ここで、本実施の特徴を、図12に示す。このような特徴を有することにより、本実施の形態では、ねずみ算的に鍵情報ファイルを配信することができる。

30

## 【0108】

なお、第1の実施の形態で述べたように、何れかの携帯通信端末10がロッカー21-mの解錠を行うと、ロッカー21-mに係る鍵情報ファイル60が管理サーバ30から削除されるため、その後、他の携帯通信端末10はロッカー21-mの解錠を行うことは出来ない。

## 【0109】

(第2の実施の形態による効果)

本実施の形態によれば、鍵情報ファイルの配布先に自由度を持たせているので、不特定多数(現実的には“コインロッカーを開けて欲しい相手の数”)に鍵情報ファイルを配布ができる。

40

## 【0110】

次に、本発明の施錠管理装置22のハードウェア構成例について、図13を参照して説明する。図13は、本発明の施錠管理装置22のハードウェア構成例を示すブロック図である。

## 【0111】

図13を参照すると、本発明の施錠管理装置22は、一般的なコンピュータ装置と同様のハードウェア構成であり、CPU(Central Processing Unit)801、RAM(Random Access Memory)等のメモリからなる、データの作業領域やデータの一時退避領域に用いられる主記憶部802、ネットワークを

50

介してデータの送受信を行う通信部 803、入力装置 805 や出力装置 806 及び記憶装置 807 と接続してデータの送受信を行う入出力インタフェース部 804、上記各構成要素を相互に接続するシステムバス 808 を備えている。記憶装置 807 は、例えば、ROM (Read Only Memory)、磁気ディスク、半導体メモリ等の不揮発性メモリから構成されるハードディスク装置等で実現される。

【0112】

本発明の施錠管理装置 22 の各機能は、プログラムを組み込んだ、LSI (Large Scale Integration) 等のハードウェア部品である回路部品を実装することにより、その動作をハードウェア的に実現することは勿論として、その機能を提供するプログラムを、記憶装置 807 に格納し、そのプログラムを主記憶部 802 にロードして CPU 801 で実行することにより、ソフトウェア的に実現することも可能である。

10

【0113】

また、管理サーバ 30 も、上記のようなハードウェア構成を有し、管理サーバ 30 が有する各機能をハードウェア的又はソフトウェア的に実現する。

【0114】

次に、本発明の携帯通信端末 10 のハードウェア構成例について、図 14 を参照して説明する。図 14 は、本発明の携帯通信端末 10 のハードウェア構成例を示すブロック図である。

【0115】

図 14 を参照すると、本発明の携帯通信端末 10 は、一般的な携帯電話機等と同様のハードウェア構成であり、CPU (Central Processing Unit) 901、RAM (Random Access Memory) 等のメモリからなる、データの作業領域やデータの一時退避領域に用いられる主記憶部 902、無線通信によりデータの送受信を行う無線通信部 903、入力部 905 や表示部 906 及び記憶装置 907 と接続してデータの送受信を行う入出力インタフェース部 904、上記各構成要素を相互に接続するシステムバス 908 を備えている。

20

【0116】

本発明の携帯通信端末 10 22 の各機能は、プログラムを組み込んだ、LSI (Large Scale Integration) 等のハードウェア部品である回路部品を実装することにより、その動作をハードウェア的に実現することは勿論として、その機能を提供するプログラムを、記憶装置 907 に格納し、そのプログラムを主記憶部 902 にロードして CPU 801 で実行することにより、ソフトウェア的に実現することも可能である。

30

【0117】

以上、好ましい実施の形態をあげて本発明を説明したが、本発明は必ずしも、上記実施の形態に限定されるものでなく、その技術的思想の範囲内において様々に変形して実施することができる。

【0118】

なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

40

【0119】

また、本発明の各種の構成要素は、必ずしも個々に独立した存在である必要はなく、複数の構成要素が一個の部材として形成されていること、一つの構成要素が複数の部材で形成されていること、ある構成要素が他の構成要素の一部であること、ある構成要素の一部と他の構成要素の一部とが重複していること、等でもよい。

【0120】

また、本発明の方法およびコンピュータプログラムには複数の手順を順番に記載してあるが、その記載の順番は複数の手順を実行する順番を限定するものではない。このため、本発明の方法およびコンピュータプログラムを実施する時には、その複数の手順の順番は

50

内容的に支障しない範囲で変更することができる。

【0121】

また、本発明の方法およびコンピュータプログラムの複数の手順は個々に相違するタイミングで実行されることに限定されない。このため、ある手順の実行中に他の手順が発生すること、ある手順の実行タイミングと他の手順の実行タイミングとの一部ないし全部が重複していること、等でもよい。

【0122】

さらに、上記実施形態の一部又は全部は、以下の付記のようにも記載されうるが、これに限定されない。

【0123】

(付記1)

非接触ICを備える1つ以上の携帯通信端末と、  
複数のロッカーを備えるロッカー装置と、  
前記携帯通信端末による前記ロッカーの鍵の開閉を管理する施錠管理装置と、  
前記各ロッカーの所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む鍵情報ファイルを管理する管理サーバとを備え、  
前記施錠管理装置が、  
前記非接触ICとデータの送受信を行う非接触ICリーダ/ライタ手段と、  
所定の前記ロッカーの施錠時に、当該ロッカーに関する前記鍵情報ファイルを生成する鍵情報ファイル生成手段と、  
前記ロッカーの鍵の開閉を制御する鍵開閉制御手段とを含み、  
前記鍵開閉制御手段が、  
前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報ファイルを前記携帯通信端末及び前記管理サーバへ送信し、  
所定の前記携帯通信端末から前記非接触ICリーダ/ライタ手段を介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う  
ことを特徴とする鍵開閉システム。

10

20

30

【0124】

(付記2)

前記鍵情報ファイルが、  
前記ロッカーの情報として、少なくとも当該ロッカーを備える前記ロッカー装置の所在地及び当該ロッカーを識別するためのロッカー番号を含むことを特徴とする付記1に記載の鍵開閉システム。

【0125】

(付記3)

前記鍵開閉制御手段は、  
前記非接触ICリーダ/ライタ手段を介して、前記非接触ICへ前記鍵情報ファイルを送信し、  
前記携帯通信端末は、  
受信した前記鍵情報ファイルを前記非接触ICへ読み込ませる制御手段を備える  
ことを特徴とする付記1又は付記2に記載の鍵開閉システム。

40

【0126】

(付記4)

前記携帯通信端末が、  
一時的にデータを保存するメモリを備え、  
前記制御手段が、  
前記非接触ICを介して受信した前記鍵情報ファイルを前記メモリに保存し、前記メモリに保存した鍵情報ファイルを前記非接触ICに読み込ませ、その後、前記メモリに保存

50

されている鍵情報ファイルを削除する

ことを特徴とする付記 3 に記載の鍵開閉システム。

【 0 1 2 7 】

( 付記 5 )

前記携帯通信端末は、

他の前記携帯通信端末から所定の鍵情報ファイルを受信すると、前記制御手段が、受信した前記鍵情報ファイルを、非接触 IC へ読み込ませることを特徴とする付記 3 又は付記 4 に記載の鍵開閉システム。

【 0 1 2 8 】

( 付記 6 )

前記管理サーバが、

前記鍵情報ファイルを格納する鍵情報ファイル格納手段と、

前記施錠管理装置からの要求に応じて、所定の鍵情報ファイルを前記鍵情報ファイル格納手段から取得し、前記施錠管理装置へ送信する鍵情報ファイル管理手段と

を備えることを特徴とする付記 1 から付記 5 の何れか 1 項に記載の鍵開閉システム。

【 0 1 2 9 】

( 付記 7 )

非接触 IC を備える 1 つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置であって、

前記非接触 IC とデータの送受信を行う非接触 IC リーダ/ライタ手段と、

所定の前記ロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む前記鍵情報ファイルを生成する鍵情報ファイル生成手段と、

前記ロッカーの鍵の開閉を制御する鍵開閉制御手段とを含み、

前記鍵開閉制御手段が、

前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報ファイルを、前記携帯通信端末及び前記鍵情報ファイルを管理する前記管理サーバへ送信し、

所定の前記携帯通信端末から前記非接触 IC リーダ/ライタ手段を介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う

ことを特徴とする施錠管理装置。

【 0 1 3 0 】

( 付記 8 )

前記鍵情報ファイルが、

前記ロッカーの情報として、少なくとも当該ロッカーを備える前記ロッカー装置の所在地及び当該ロッカーを識別するためのロッカー番号を含むことを特徴とする付記 7 に記載の施錠管理装置。

【 0 1 3 1 】

( 付記 9 )

前記鍵開閉制御手段は、

前記非接触 IC リーダ/ライタ手段を介して、前記非接触 IC へ前記鍵情報ファイルを送信する

ことを特徴とする付記 7 又は付記 8 に記載の施錠管理装置。

【 0 1 3 2 】

( 付記 1 0 )

非接触 IC を備える 1 つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置による施錠管理方法であって、

所定の前記ロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの

10

20

30

40

50

鍵を解錠するための解錠キー情報を含む前記鍵情報ファイルを作成する鍵情報ファイル生成ステップと、

前記ロッカーの鍵の開閉を制御する鍵開閉制御ステップとを含み、

前記鍵開閉制御ステップで、

前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報ファイルを、前記携帯通信端末及び前記鍵情報ファイルを管理する前記管理サーバへ送信し、

所定の前記携帯通信端末から前記非接触ＩＣを介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う

10

ことを特徴とする施錠管理方法。

【 0 1 3 3 】

( 付 記 1 1 )

前記鍵情報ファイルが、

前記ロッカーの情報として、少なくとも当該ロッカーを備える前記ロッカー装置の所在地及び当該ロッカーを識別するためのロッカー番号を含むことを特徴とする付記 1 0 に記載の施錠管理方法。

【 0 1 3 4 】

( 付 記 1 2 )

前記鍵開閉制御ステップで、

非接触ＩＣリーダ/ライタ手段によって、前記非接触ＩＣへ前記鍵情報ファイルを送信する

20

ことを特徴とする付記 1 0 又は付記 1 1 に記載の施錠管理方法。

【 0 1 3 5 】

( 付 記 1 3 )

非接触ＩＣを備える 1 つ以上の携帯通信端末によるロッカーの鍵の開閉を管理する施錠管理装置上で動作する施錠管理プログラムであって、

前記施錠管理装置に、

所定の前記ロッカーの施錠時に、当該ロッカーに関する所定の情報及び当該ロッカーの鍵を解錠するための解錠キー情報を含む前記鍵情報ファイルを作成する鍵情報ファイル生成処理と、

30

前記ロッカーの鍵の開閉を制御する鍵開閉制御処理をと実行させ、

前記鍵開閉制御処理で、

前記鍵情報ファイル生成手段によって前記鍵情報ファイルが生成された場合、当該鍵情報ファイルを、前記携帯通信端末及び前記鍵情報ファイルを管理する前記管理サーバへ送信し、

所定の前記携帯通信端末から前記非接触ＩＣを介して前記鍵情報ファイルを受信した場合、当該鍵情報ファイルに対応する前記ロッカーを特定し、当該ロッカーに関する前記鍵情報ファイルを前記管理サーバから取得し、双方の鍵情報ファイルの解錠キー情報が同一である場合、当該ロッカーの解錠を行う

40

ことを特徴とする施錠管理プログラム。

【 0 1 3 6 】

( 付 記 1 4 )

前記鍵情報ファイルが、

前記ロッカーの情報として、少なくとも当該ロッカーを備える前記ロッカー装置の所在地及び当該ロッカーを識別するためのロッカー番号を含むことを特徴とする付記 1 3 に記載の施錠管理プログラム。

【 0 1 3 7 】

( 付 記 1 5 )

50

前記鍵開閉制御処理で、  
非接触ＩＣリーダ／ライタ手段によって、前記非接触ＩＣへ前記鍵情報ファイルを送信する

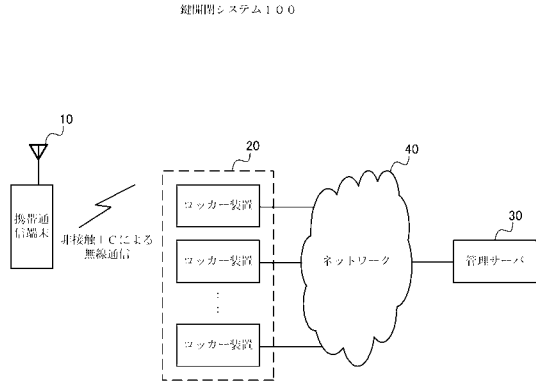
ことを特徴とする付記１３又は付記１４に記載の施錠管理プログラム。

【符号の説明】

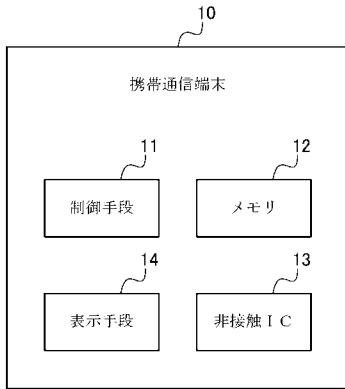
【０１３８】

１００	： 鍵開閉システム	
１０	： 携帯通信端末	
１１	： 制御手段	
１２	： メモリ	10
１３	： 非接触ＩＣ	
１４	： 表示手段	
２０	： ロッカー装置	
２１	( ロッカー ２１ - １ ~ ２１ - m )	： ロッカー
２２	： 施錠管理装置	
２２１	： 非接触ＩＣリーダ／ライタ手段	
２２２	： 鍵情報ファイル生成手段	
２２３	： 通信手段	
２２４	： 鍵開閉制御手段	
３０	： 管理サーバ	20
３１	： 鍵情報ファイル管理手段	
３２	： 鍵情報ファイル格納手段	
３３	： 通信手段	
４０	： ネットワーク	
５０	： 基地局	
６０	： 鍵情報ファイル	
６１	： ヘッダ部	
６２	： テキスト部	
６３	： 鍵情報部	
８０１	： ＣＰＵ	30
８０２	： 主記憶部	
８０３	： 通信部	
８０４	： 入出力インタフェース部	
８０５	： 入力装置	
８０６	： 出力装置	
８０７	： 記憶装置	
８０８	： システムバス	
９０１	： ＣＰＵ	
９０２	： 主記憶部	
９０３	： 無線通信部	40
９０４	： 入出力インタフェース部	
９０５	： 入力部	
９０６	： 出力部	
９０７	： 記憶装置	
９０８	： システムバス	

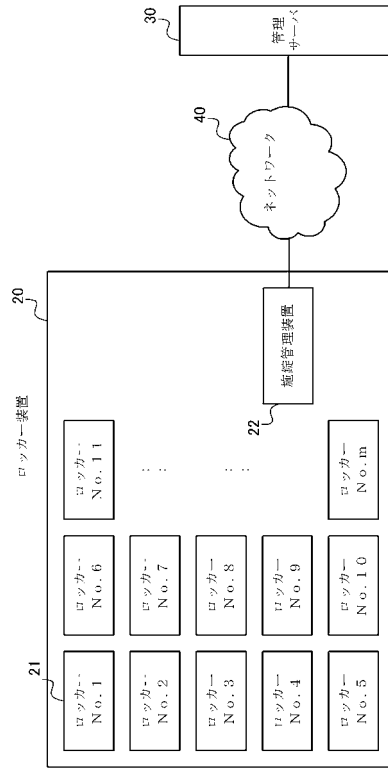
【図1】



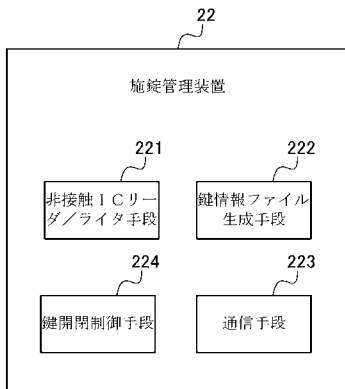
【図2】



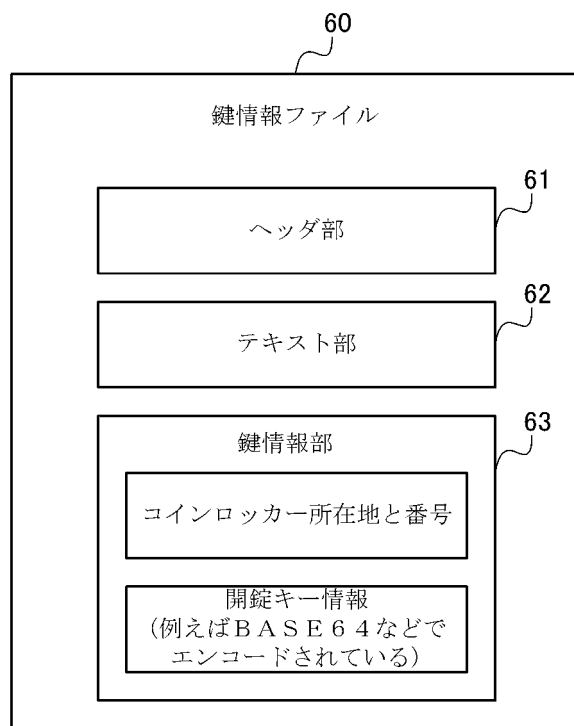
【図3】



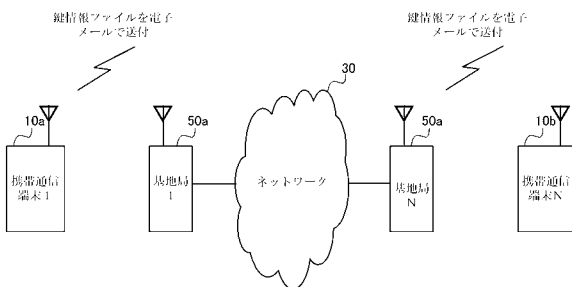
【図4】



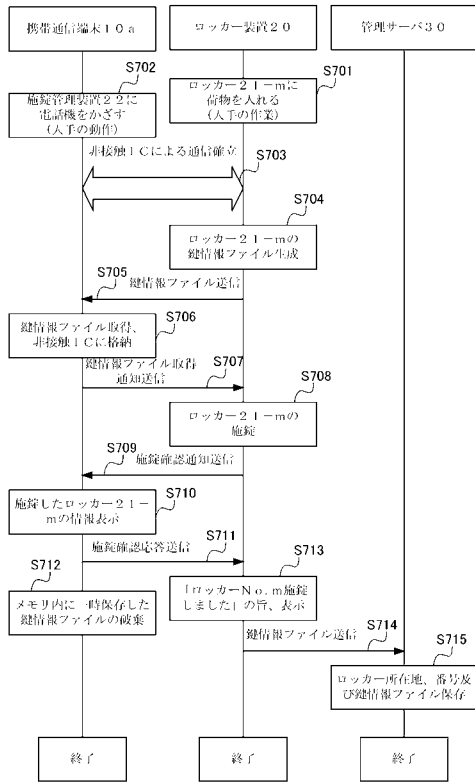
【図6】



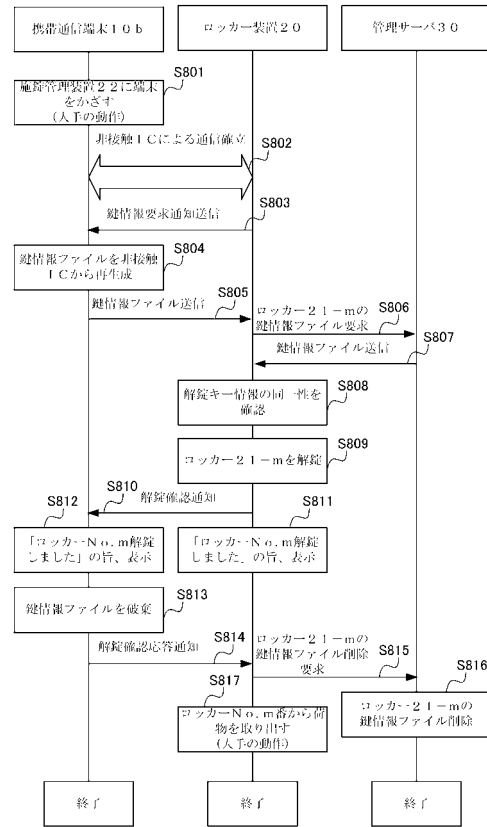
【図5】



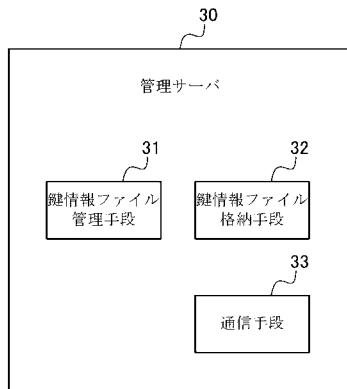
【図 7】



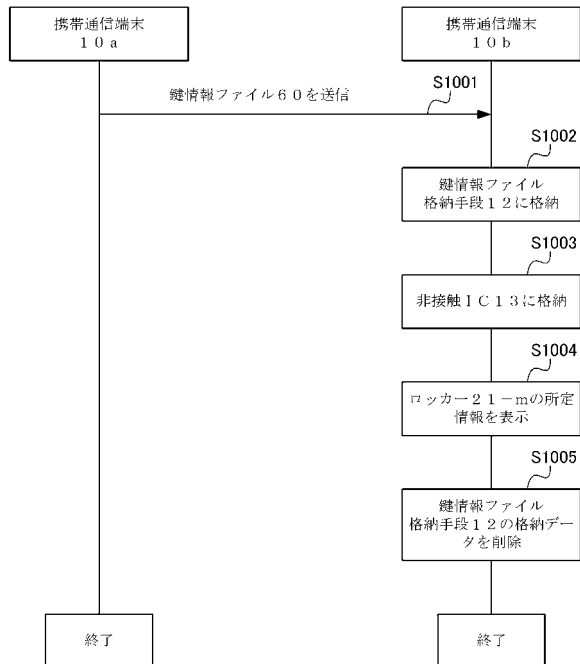
【図 8】



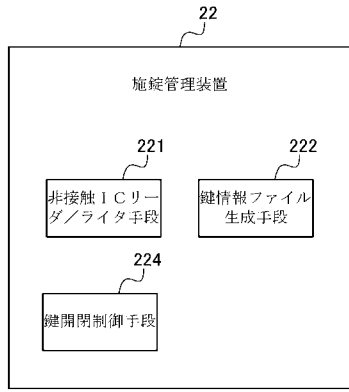
【図 9】



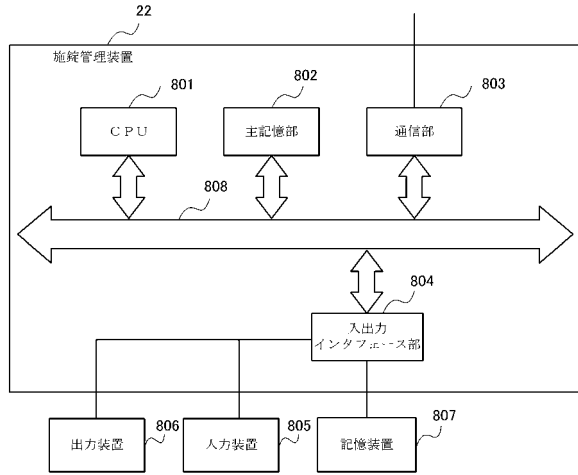
【図 10】



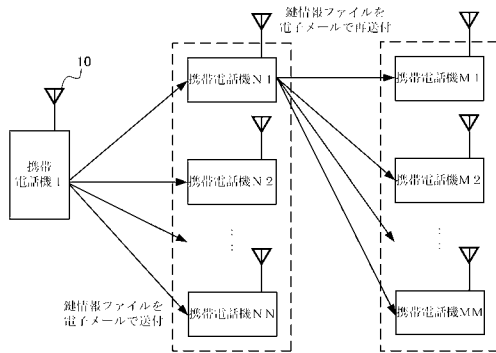
【図 1 1】



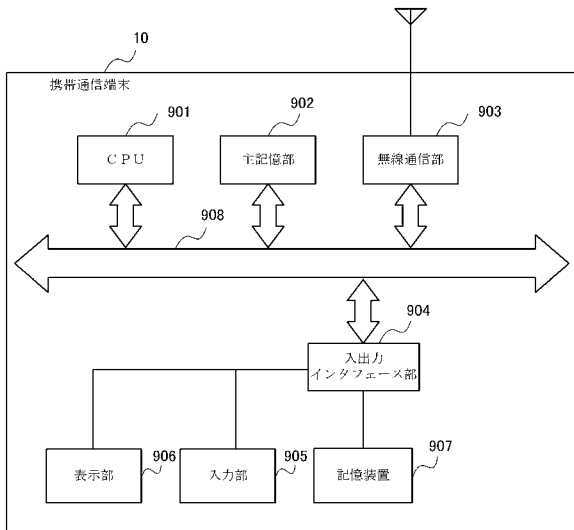
【図 1 3】



【図 1 2】



【図 1 4】



【図 1 5】

