(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2004-232277
(P2004-232277A)
(43)公開日　平成16年8月19日(2004.8.19)

(51)Int.Cl.[7]	F I		テーマコード（参考）
E05B 49/00	E05B 49/00	K	2E250

審査請求 未請求　請求項の数 7　OL　（全 14 頁）

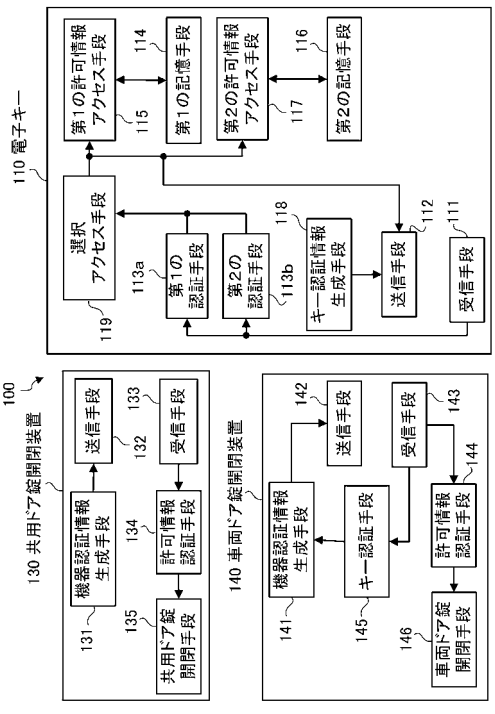
(21)出願番号　特願2003-20524(P2003-20524)
(22)出願日　平成15年1月29日(2003.1.29)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100072604
弁理士　有我　軍一郎
(72)発明者　湯原　雅裕
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考)　2E250 AA00 AA04 AA12 AA21 BB08 BB43 BB46 BB65 CC12 CC16 DD06 EE02 EE10 EE11 FF23 FF27 FF28 FF36 GG07 HH02 JJ03 KK03 LL01

(54)【発明の名称】電子キー及び電子キーシステム

(57)【要約】
【課題】複数の電子機器の作動を許可することができる電子キーを提供すること。
【解決手段】電子キー１１０は、共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０の作動の許可に使用される許可情報を記憶する第１の記憶手段１１４及び第２の記憶手段１１６と、第１の記憶手段１１４又は第２の記憶手段１１６のみに許可情報のアクセスを行う第１の許可情報アクセス手段１１５及び第２の許可情報アクセス手段１１７と、機器認証情報に基づいて共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０を認証する第１の機器認証手段１１３ａ及び第２の機器認証手段１１３ｂと、第１の機器認証手段１１３ａ又は第２の機器認証手段１１３ｂによる認証結果に応じた第１の許可情報アクセス手段１１５又は第２の許可情報アクセス手段１１７を選択し共用ドア錠開閉装置１３０又は車両ドア錠開閉装置１４０にアクセスを行わせる選択アクセス手段１１９とを備える。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電子機器の作動の許可に使用される許可情報を記憶する複数の記憶手段と、前記複数の記憶手段のうちの所定の記憶手段のみに前記許可情報のアクセスを行う複数の許可情報アクセス手段と、前記電子機器から送信されて前記電子機器の認証に使用される機器認証情報に基づいて前記電子機器を認証する機器認証手段と、前記機器認証手段による認証結果に応じた前記許可情報アクセス手段を前記複数の許可情報アクセス手段の中から選択し前記電子機器にアクセスを行わせる選択アクセス手段とを備えたことを特徴とする電子キー。
【請求項２】
前記記憶手段は、前記複数の記憶手段のうちの他の少なくとも１つの記憶手段と物理的に独立したことを特徴とする請求項１に記載の電子キー。
【請求項３】
前記許可情報アクセス手段は、前記複数の許可情報アクセス手段のうちの他の少なくとも１つの許可情報アクセス手段と異なる方法で前記記憶手段にアクセスを行うことを特徴とする請求項１又は請求項２に記載の電子キー。
【請求項４】
前記機器認証手段は、前記電子機器に応じた方法で前記電子機器を認証することを特徴とする請求項１から請求項３までの何れかに記載の電子キー。
【請求項５】
前記機器認証手段は、前記許可情報の前記記憶手段からの読み出しが前記電子機器によって要求されたときと、前記許可情報の前記記憶手段への書き込みが前記電子機器によって要求されたときとで前記電子機器を認証する方法を変更することを特徴とする請求項１から請求項４までの何れかに記載の電子キー。
【請求項６】
非接触ＩＣカード型運転免許証であることを特徴とする請求項１から請求項５までの何れかに記載の電子キー。
【請求項７】
請求項１から請求項６までの何れかに記載の電子キーと、複数の電子機器とを備え、
前記電子機器は、前記機器認証情報を前記電子キーに送信する機器認証情報送信手段と、前記電子キーの前記許可情報アクセス手段にアクセスを行うキーアクセス手段とを有したことを特徴とする電子キーシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子機器の作動の許可に使用される許可情報を電子機器に送信する電子キー及び電子キーシステムに関する。
【０００２】
【従来の技術】
従来、電子機器の作動の許可に使用される許可情報を電子機器に送信する電子キー及び電子キーシステムとして、所定の周波数の無線信号を発振する発振器と、使用者によって押下されることで、発振器に無線信号を発振させる押下スイッチと、発振器によって発振された無線信号を許可情報として電子機器に送信するアンテナとを備えた電子キー及び電子キーシステムが知られている（例えば、特許文献１参照。）。
【０００３】
【特許文献１】
特開平０６－２４０９３９号公報（第２－３頁、第３図）
【０００４】
【発明が解決しようとする課題】
しかしながら、上述した従来の電子キー及び電子キーシステムにおいては、所定の１つの電子機器の作動を許可することしかできないという問題があった。

【０００５】
そこで、本発明は、複数の電子機器の作動を許可することができる電子キーを提供することを目的とする。
【０００６】
【課題を解決するための手段】
上述した課題を解決するために、本発明の電子キーは、電子機器の作動の許可に使用される許可情報を記憶する複数の記憶手段と、前記複数の記憶手段のうちの所定の記憶手段のみに前記許可情報のアクセスを行う複数の許可情報アクセス手段と、前記電子機器から送信されて前記電子機器の認証に使用される機器認証情報に基づいて前記電子機器を認証する機器認証手段と、前記機器認証手段による認証結果に応じた前記許可情報アクセス手段を前記複数の許可情報アクセス手段の中から選択し前記電子機器にアクセスを行わせる選択アクセス手段とを備えた構成を有している。
【０００７】
この構成により、本発明の電子キーは、複数の記憶手段が複数の許可情報を記憶し、許可情報アクセス手段が所定の記憶手段のみに許可情報のアクセスを行い、電子機器にアクセスを行わせる許可情報アクセス手段を機器認証手段による認証結果に応じて選択アクセス手段が選択するので、複数の電子機器の作動を許可することができる。
【０００８】
また、本発明の電子キーは、前記記憶手段は、前記複数の記憶手段のうちの他の少なくとも１つの記憶手段と物理的に独立した構成を有する。
【０００９】
この構成により、本発明の電子キーは、記憶手段を他の少なくとも１つの記憶手段から物理的に独立させることによって、許可情報アクセス手段が本来アクセスすべき許可情報とは別の許可情報に誤ってアクセスすることを防ぐことができるので、許可情報の安全性を確保することができる。
【００１０】
また、本発明の電子キーは、前記許可情報アクセス手段は、前記複数の許可情報アクセス手段のうちの他の少なくとも１つの許可情報アクセス手段と異なる方法で前記記憶手段にアクセスを行う構成を有している。
【００１１】
この構成により、本発明の電子キーは、複数の許可情報アクセス手段のうちの他の少なくとも１つの許可情報アクセス手段と異なる方法で、許可情報アクセス手段が記憶手段にアクセスを行うことによって、アクセスされる方法が同じ記憶手段にのみ許可情報アクセス手段がアクセスを行うことができるので、許可情報の安全性を確保することができる。
【００１２】
また、本発明の電子キーは、前記機器認証手段は、前記電子機器に応じた方法で前記電子機器を認証する構成を有している。
【００１３】
この構成により、本発明の電子キーは、各電子機器に応じた方法で電子機器を認証するので、それぞれ別の許可情報を使用する電子機器同士を誤認することを防ぐことができ、許可情報の安全性を確保することができる。
【００１４】
また、本発明の電子キーは、前記機器認証手段は、前記許可情報の前記記憶手段からの読み出しが前記電子機器によって要求されたときと、前記許可情報の前記記憶手段への書き込みが前記電子機器によって要求されたときとで前記電子機器を認証する方法を変更する構成を有している。
【００１５】
この構成により、本発明の電子キーは、許可情報の記憶手段からの読み出しが電子機器によって要求されたときと許可情報の記憶手段への書き込みが電子機器によって要求されたときとで、異なる方法で電子機器を認証することができるので、許可情報の記憶手段から

の読み出しが電子機器によって要求されたときと許可情報の記憶手段への書き込みが電子機器によって要求されたときとで、許可情報の安全性の度合に差をつけることができる。

【００１６】

また、本発明の電子キーは、非接触ＩＣカード型運転免許証である構成を有する。

【００１７】

この構成により、本発明の電子キーは、許可情報をキーとしての機能だけでなく、非接触ＩＣカード型運転免許証としての機能でも利用することができる。

【００１８】

また、本発明の電子キーシステムは、電子キーと、複数の電子機器とを備え、前記電子機器は、前記機器認証情報を前記電子キーに送信する機器認証情報送信手段と、前記電子キーの前記許可情報アクセス手段にアクセスを行うキーアクセス手段とを有した構成を有する。

【００１９】

この構成により、本発明の電子キーシステムは、電子機器から送信された機器認証情報に基づいて電子キーが電子機器の認証を行い、認証が行われた電子機器が所定の許可情報アクセス手段にアクセスすることができるため、１つの電子キーによって複数の電子機器を作動させることができる。

【００２０】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

【００２１】

（第１の実施の形態）

まず、第１の実施の形態に係る電子キーシステムの構成について説明する。

【００２２】

図１に示すように、本実施の形態に係る電子キーシステム１００は、マンションの共用ドアの錠を開閉する電子機器としての共用ドア錠開閉装置１３０と、車両のドアの錠を開閉する電子機器としての車両ドア錠開閉装置１４０と、共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０に許可情報を送信することで、共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０の作動を許可する電子キー１１０とを備えている。

【００２３】

また、電子キー１１０は、機器認証情報を共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０から無線で受信する受信手段１１１と、許可情報及び電子キー１１０自身が電子キーであることを車両ドア錠開閉装置１４０に認証させるキー認証情報を共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０に無線で送信する送信手段１１２と、２４ビットの情報によって構成された機器認証情報に基づいて共用ドア錠開閉装置１３０を認証する第１の認証手段１１３ａと、６４ビットの情報によって構成された暗号化された機器認証情報（以下、暗号機器認証情報という。）を復号して、復号された機器認証情報に基づいて車両ドア錠開閉装置１４０を認証する第２の認証手段１１３ｂとを備えている。

【００２４】

なお、第１の認証手段１１３ａ及び第２の認証手段１１３ｂは、本発明の機器認証手段を構成している。

【００２５】

また、電子キー１１０は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）で構成され、共用ドア錠開閉装置１３０にマンションの共用ドアの錠の開閉を許可する許可情報を記憶する記憶手段としての第１の記憶手段１１４と、第１の記憶手段１１４の記憶領域に割り振られているアドレス番号の先頭番号から最後番号に向けて許可情報のアクセスを行う方法で、第１の記憶手段１１４のみに許可情報のアクセスを行う許可情報アクセス手段としての第１の許可情報アクセス手段１１５と、第１の記憶手段１１４とは物理的に独立したＲＡＭで構成され、車両ドア錠開閉装置１４０に車両のドアの錠の開閉を許可する暗号化された許可情報（以下、暗号許可情報という。）を記憶する記憶手段としての第２

の記憶手段１１６と、第２の記憶手段１１６の記憶領域に割り振られているアドレス番号の最後番号から先頭番号に向けて暗号許可情報のアクセスを行う方法で、第２の記憶手段１１６のみに暗号許可情報のアクセスを行う許可情報アクセス手段としての第２の許可情報アクセス手段１１７とを備えている。

【００２６】

なお、車両のドアの錠の開閉を許可する許可情報は、車両の所有者等の特定の人物のみによって使用されるので、例えば住所情報等の個人情報であっても良い。また、マンションの共用ドアの錠の開閉を許可する許可情報は、マンションの居住者等の複数人によって使用されるので、車両のドアの錠の開閉を許可する許可情報よりも秘密性の度合が低い、例えば無意味な数字の羅列で構成された情報であっても良い。

【００２７】

また、電子キー１１０は、キー認証情報を生成するキー認証情報生成手段１１８と、共用ドア錠開閉装置１３０及び第１の許可情報アクセス手段１１５を関連付け、車両ドア錠開閉装置１４０及び第２の許可情報アクセス手段１１７を関連付け、第１の認証手段１１３ａによって共用ドア錠開閉装置１３０が認証されたとき、第１の認証手段１１３ａによって認証された共用ドア錠開閉装置１３０に関連付けられた第１の許可情報アクセス手段１１５を選択し共用ドア錠開閉装置１３０にアクセスを行わせ、第２の許可情報アクセス手段１１３ｂによって車両ドア錠開閉装置１４０が認証されたとき、第２の認証手段１１３ｂによって認証された車両ドア錠開閉装置１４０に関連付けられた第２の許可情報アクセス手段１１７を選択し車両ドア錠開閉装置１４０にアクセスを行わせる選択アクセス手段１１９とを備えている。即ち、選択アクセス手段１１９は、第１の認証手段１１３ａ又は第２の認証手段１１３ｂによる認証結果に応じた第１の許可情報アクセス手段１１５又は第２の許可情報アクセス手段１１７を選択し、共用ドア錠開閉装置１３０又は車両ドア錠開閉装置１４０にアクセスを行わせるようになっている。

【００２８】

また、共用ドア錠開閉装置１３０は、２４ビットの情報によって構成された機器認証情報を生成する機器認証情報生成手段１３１と、機器認証情報を電子キー１１０に無線で送信する機器認証情報送信手段としての送信手段１３２と、許可情報を電子キー１１０から無線で受信する受信手段１３３とを備えている。

【００２９】

また、共用ドア錠開閉装置１３０は、受信手段１３３によって受信された許可情報が予め記憶された情報と一致するか否かを判定し、一致すると判定したとき、受信手段１３３によって受信された許可情報が正規の許可情報であると認証を行う許可情報認証手段１３４と、受信手段１３３によって受信された許可情報が正規の許可情報であると許可情報認証手段１３４によって認証された場合、マンションの共用ドアの錠を開閉する共用ドア錠開閉手段１３５とを備えている。

【００３０】

なお、許可情報認証手段１３４によって正規の許可情報であると認証される許可情報は電子キー１１０の第１の許可情報アクセス手段１１５によって電子キー１１０の第１の記憶手段１１４から読み出されるので、許可情報認証手段１３４は、電子キー１１０の第１の許可情報アクセス手段１１５にアクセスを行うキーアクセス手段を構成している。

【００３１】

また、車両ドア錠開閉装置１４０は、６４ビットの情報によって構成された機器認証情報を生成し、生成された機器認証情報を所定の暗号化ルールで暗号化することで暗号機器認証情報を生成する機器認証情報生成手段１４１と、暗号機器認証情報を電子キー１１０に無線で送信する機器認証情報送信手段としての送信手段１４２と、キー認証情報及び暗号許可情報を電子キー１１０から無線で受信する受信手段１４３とを備えている。

【００３２】

また、車両ドア錠開閉装置１４０は、暗号許可情報を復号し、復号された許可情報が予め記憶された情報と一致するか否かを判定し、一致すると判定されたとき、復号された許可

情報が正規の許可情報であると認証を行う許可情報認証手段１４４と、キー認証情報に基づいて、電子キー１１０が電子キーであることの認証を行うキー認証手段１４５と、許可情報認証手段１４４によって復号された許可情報が正規の許可情報であると認証された場合、車両のドアの錠を開閉する車両ドア錠開閉手段１４６とを備えている。

【００３３】

なお、許可情報認証手段１４４によって正規の許可情報と認証される許可情報は電子キー１１０の第２の許可情報アクセス手段１１７によって電子キー１１０の第２の記憶手段１１６から読み出されるので、許可情報認証手段１４４は、電子キー１１０の第２の許可情報アクセス手段１１７にアクセスを行うキーアクセス手段を構成している。

【００３４】

次に、本実施の形態に係る電子キーシステム１００が、共用ドア錠開閉装置１３０にマンションの共用ドアの錠を開閉させる動作について説明する。

【００３５】

まず、共用ドア錠開閉装置１３０の機器認証情報生成手段１３１によって予め記憶された配列によって構成された２４ビットの情報が機器認証情報として生成され、生成された機器認証情報が共用ドア錠開閉装置１３０の送信手段１３２によって電子キー１１０に無線で送信される。

【００３６】

次いで、電子キー１１０の受信手段１１１によって機器認証情報が無線で受信され、受信された機器認証情報が第１の認証手段１１３ａ及び第２の認証手段１１３ｂに出力される。

【００３７】

続いて、第１の認証手段１１３ａに機器認証情報が入力され、入力された機器認証情報を構成する２４ビットの情報と第１の認証手段１１３ａによって予め記憶された２４ビットの情報とが一致するか否かが第１の認証手段１１３ａによって判定される。判定の結果、一致するので、機器認証情報を送信した共用ドア錠開閉装置１３０は、第１の認証手段１１３ａによって共用ドア錠開閉装置１３０であると認証される。

【００３８】

また、第２の認証手段１１３ｂに機器認証情報が入力され、入力された機器認証情報は暗号化されていないので復号されず、入力された機器認証情報を構成する２４ビットの情報が第２の認証手段１１３ｂによって予め記憶された６４ビットの情報と一致するか否かが第２の認証手段１１３ｂによって判定される。しかしながら、ビット数が異なるため一致せず、第２の認証手段１１３ｂに入力された機器認証情報は、第２の認証手段１１３ｂによって破棄される。

【００３９】

次に、共用ドア錠開閉装置１３０が第１の認証手段１１３ａによって共用ドア錠開閉装置１３０であると認証されることで、共用ドア錠開閉装置１３０に関連付けられた第１の許可情報アクセス手段１１５が選択アクセス手段１１９によって選択される。

【００４０】

次いで、第１の記憶手段１１４によって予め記憶された許可情報が、第１の許可情報アクセス手段１１５によって第１の記憶手段１１４の記憶領域に割り振られたアドレス番号の先頭番号から最後番号に向けて読み出され、読み出された許可情報が電子キー１１０の送信手段１１２によって共用ドア錠開閉装置１３０に無線で送信される。

【００４１】

次いで、共用ドア錠開閉装置１３０の受信手段１３３によって許可情報が無線で受信され、受信された許可情報が許可情報認証手段１３４に出力される。

【００４２】

続いて、許可情報認証手段１３４によって予め記憶された情報と許可情報認証手段１３４に入力された許可情報とが一致するか否かが許可情報認証手段１３４によって判定される。判定の結果、一致するので、許可情報認証手段１３４に入力された許可情報は、許可情

報認証手段１３４によって正規の許可情報として認証される。
【００４３】
次に、許可情報認証手段１３４によって許可情報が正規の許可情報として認証されることによって、共用ドア錠開閉手段１３５によってマンションの共用ドアの錠が開閉される。
【００４４】
次いで、本実施の形態に係る電子キーシステム１００が、車両ドア錠開閉装置１４０に車両のドアの錠を開閉させる動作について説明する。
【００４５】
まず、電子キー１１０のキー認証情報生成手段１１８によって予め記憶された配列によって構成された情報がキー認証情報として生成され、生成されたキー認証情報が電子キー１１０の送信手段１１２によって車両ドア錠開閉装置１４０に無線で送信される。
【００４６】
次いで、車両ドア錠開閉装置１４０の受信手段１４３によってキー認証情報が無線で受信され、受信されたキー認証情報がキー認証手段１４５に出力される。
【００４７】
続いて、キー認証手段１４５にキー認証情報が入力され、入力されたキー認証情報とキー認証手段１４５によって予め記憶された情報とが一致するか否かがキー認証手段１４５によって判定される。判定の結果、一致するので、キー認証情報を送信した電子キー１１０は、キー認証手段１４５によって電子キーであると認証される。
【００４８】
次いで、キー認証手段１４５によって電子キー１１０が電子キーであると認証されると、機器認証情報生成手段１４１によって予め記憶された配列によって構成された６４ビットの情報が機器認証情報として機器認証情報生成手段１４１によって生成され、生成された機器認証情報が機器認証情報生成手段１４１によって所定の暗号化ルールで暗号化されることで暗号機器認証情報が生成され、生成された暗号機器認証情報が車両ドア錠開閉装置１４０の送信手段１４２によって電子キー１１０に無線で送信される。
【００４９】
次に、電子キー１１０の受信手段１１１によって暗号機器認証情報が無線で受信され、受信された暗号機器認証情報が第１の認証手段１１３ａ及び第２の認証手段１１３ｂに出力される。
【００５０】
次いで、第１の認証手段１１３ａに暗号機器認証情報が入力され、入力された暗号機器認証情報を構成する６４ビットの情報と第１の認証手段１１３ａによって予め記憶された２４ビットの情報とが一致するか否かが第１の認証手段１１３ａによって判定される。しかしながら、ビット数が異なり、暗号機器認証情報は暗号化されたままなので一致せず、第１の認証手段１１３ａに入力された暗号機器認証情報は、第１の認証手段１１３ａによって破棄される。
【００５１】
また、第２の認証手段１１３ｂに暗号機器認証情報が入力され、入力された暗号機器認証情報が復号され、復号された機器認証情報を構成する６４ビットの情報と第２の認証手段１１３ｂによって予め記憶された６４ビットの情報とが一致するか否かが第２の認証手段１１３ｂによって判定される。判定の結果、一致するので、暗号機器認証情報を送信した車両ドア錠開閉装置１４０は、第２の認証手段１１３ｂによって車両ドア錠開閉装置１４０であると認証される。
【００５２】
続いて、車両ドア錠開閉装置１４０が第２の認証手段１１３ｂによって所定の車両ドア錠開閉装置１４０であると認証されることで、車両ドア錠開閉装置１４０に関連付けられた第２の許可情報アクセス手段１１７が選択アクセス手段１１９によって選択される。
【００５３】
次に、第２の記憶手段１１６によって記憶され、所定の暗号化ルールで暗号化された暗号

許可情報が、第２の許可情報アクセス手段１１７によって第２の記憶手段１１６の記憶領域に割り振られたアドレス番号の最後番号から先頭番号に向けて読み出され、読み出された暗号許可情報が電子キー１１０の送信手段１１１によって車両ドア錠開閉装置１４０に無線で送信される。

【００５４】

次に、車両ドア錠開閉装置１４０の受信手段１４３によって暗号許可情報が無線で受信され、受信された暗号許可情報が許可情報認証手段１４４に出力される。

【００５５】

次いで、許可情報認証手段１４４に暗号許可情報が入力され、入力された暗号許可情報が許可情報認証手段１４４によって復号され、復号された許可情報と許可情報認証手段１４４によって予め記憶された情報とが一致するか否かが許可情報認証手段１４４によって判定される。判定の結果、一致するので、復号された許可情報は正規の許可情報として認証される。

【００５６】

続いて、許可情報認証手段１４４によって復号された許可情報が正規の許可情報として認証されることによって、車両ドア錠開閉手段１４６による車両のドアの錠の開閉が許可される。

【００５７】

以上に説明したように、電子キー１１０は、第１の記憶手段１１４及び第２の記憶手段１１６がそれぞれ別の許可情報を記憶し、第１の許可情報アクセス手段１１５及び第２の許可情報アクセス手段１１７がそれぞれ第１の記憶手段１１４又は第２の記憶手段１１６のみに許可情報のアクセスを行い、共有ドア錠開閉装置１３０又は車両ドア錠開閉装置１４０にアクセスを行わせる第１の許可情報アクセス手段１１５又は第２の許可情報アクセス手段１１７を第１の機器認証手段１１３ａ又は第２の機器認証手段１１３ｂによる認証結果に応じて選択アクセス手段１１９が選択するので、共有ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０という複数の電子機器の作動を許可することができる。

【００５８】

また、電子キー１１０は、第１の記憶手段１１４と第２の記憶手段１１６とを互いに物理的に独立させることによって、第１の許可情報アクセス手段１１５及び第２の許可情報アクセス手段１１６が本来アクセスすべき許可情報とは別の許可情報に誤ってアクセスすることを防ぐことができるので、許可情報の安全性を確保することができる。

【００５９】

なお、本発明によれば、第１の記憶手段１１４及び第２の記憶手段１１６は同一のＲＡＭによって構成されていても良い。

【００６０】

また、電子キー１１０は、第１の許可情報アクセス手段１１５が第１の記憶手段１１４の記憶領域に割り振られたアドレス番号の先頭番号から最後番号に向かって許可情報のアクセスを行い、第２の許可情報アクセス手段１１７が第２の記憶手段１１６の記憶領域に割り振られたアドレス番号の最後番号から先頭番号に向かって許可情報のアクセスを行うというように、第１の許可情報アクセス手段１１５及び第２の許可情報アクセス手段１１７はそれぞれ異なる方法で第１の記憶手段１１４及び第２の記憶手段１１６にアクセスを行うので、第１の許可情報アクセス手段１１５が第２の記憶手段１１６に許可情報のアクセスを行わず、第２の許可情報アクセス手段１１７が第１の記憶手段１１４に許可情報のアクセスを行わないので、許可情報の安全性を確保することができる。

【００６１】

また、第１の許可情報アクセス手段１１５及び第２の許可情報アクセス手段１１７は、それぞれ異なる方法で第１の記憶手段１１４及び第２の記憶手段１１６にアクセスを行うので、アクセスが行われる許可情報の秘密性の度合に応じて、他者に対して隠匿されるアクセスの方法及び他者に対して公開されても良いアクセスの方法を設定することができる。

【００６２】

なお、本発明によれば、第１の許可情報アクセス手段１１５が第１の記憶手段１１４に許可情報のアクセスを行う方法及び第２の許可情報アクセス手段１１７が第２の記憶手段１１６に許可情報のアクセスを行う方法が同一であっても良い。

【００６３】

また、電子キー１１０は、共用ドア錠開閉装置１３０からの２４ビットの機器認証情報が予め記憶された情報と一致するか否かで共用ドア錠開閉装置１３０を認証し、車両ドア錠開閉装置１４０と互いに暗号化された６４ビットの機器認証情報又はキー認証情報を送受信し、互いに予め記憶された情報と受信された機器認証情報又はキー認証情報とが一致するか否かで車両ドア錠開閉装置１４０を認証するというように、共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０を互いに異なる方法で認証しているので、それぞれ別の許可情報を使用する共用ドア錠開閉装置１３０と車両ドア錠開閉装置１４０とを誤認することを防ぐことができ、許可情報の安全性を確保することができる。

【００６４】

なお、本発明によれば、電子キー１１０が共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０を認証する方法が同一であっても良い。

【００６５】

また、本発明の電子キー１１０は、非接触ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）カード型運転免許証を構成するようになっている場合、許可情報として住所情報等の個人情報が設定されたとき、許可情報をキーとしての機能だけでなく、非接触ＩＣカード型運転免許証としての機能でも利用することができる。

【００６６】

また、電子キーシステム１００は、共用ドア錠開閉装置１３０又は車両ドア錠開閉装置１４０から送信された機器認証情報に基づいて電子キー１１０が共用ドア錠開閉装置１３０又は車両ドア錠開閉装置１４０の認証を行い、認証が行われた共用ドア錠開閉装置１３０又は車両ドア錠開閉装置１４０がそれぞれ第１の許可情報アクセス手段１１５又は第２の許可情報アクセス手段１１７にアクセスすることができるため、１つの電子キー１１０によって共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０という複数の電子機器を作動させることができる。

【００６７】

また、電子キーシステム１００は、本実施の形態において、１つの電子キー１１０によって共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０という２つの電子機器を作動させるようになっていたが、本発明によれば、１つの電子キー１１０によって３つ以上の電子機器を作動させるようになっていても良い。

【００６８】

また、電子キーシステム１００は、本実施の形態において、共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０を作動させるようになっていたが、本発明によれば、車載ナビゲーションシステム起動装置、メモリリーダ及びメモリライタ等、共用ドア錠開閉装置１３０及び車両ドア錠開閉装置１４０以外の電子機器を作動させるようになっていても良い。

【００６９】

また、本実施の形態において、機器認証情報として、２４ビットの情報及び６４ビットの情報を用いたが、本発明の機器認証情報は、２４ビット及び６４ビット以外のビット数の情報でも良い。

【００７０】

（第２の実施の形態）

まず、第２の実施の形態に係る電子キーシステムの構成について説明する。

【００７１】

なお、本実施の形態に係る電子キーシステムの構成のうち第１の実施の形態に係る電子キーシステムの構成と同様である構成については、第１の実施の形態に係る電子キーシステムの構成と同一の符号を付して詳細な説明を省略する。

【００７２】
図２に示すように、本実施の形態に係る電子キーシステム２００は、コンピュータを起動し、コンピュータの起動を許可する許可情報として新規の許可情報である新規許可情報を書き込むことができる電子機器としてのコンピュータ起動装置２５０と、コンピュータ起動装置２５０に許可情報を送信することで、コンピュータ起動装置２５０の作動を許可する電子キー２１０とを備えている。
【００７３】
電子キー２１０の構成は、コンピュータ起動装置２５０にコンピュータの起動を許可する許可情報を記憶する記憶手段としての第３の記憶手段２２１と、第３の記憶手段２２１にのみ許可情報のアクセスを行う許可情報アクセス手段としての第３の許可情報アクセス手段２２２とを第１の実施の形態に係る電子キーシステム１００（図１参照）の電子キー１１０（図１参照）が有し、機器認証情報をコンピュータ起動装置２５０から受信する受信手段２１１と、暗号許可情報をコンピュータ起動装置２５０に送信する送信手段２１２と、第３の許可情報アクセス手段２２２が第３の記憶手段２２１から許可情報を読み出すとき、機器認証情報に基づいてコンピュータ起動装置２５０を認証する機器認証手段としての読み出し認証手段２２０ａと、第３の許可情報アクセス手段２２２が第３の記憶手段２２１に新規許可情報を書き込むとき、機器認証情報に基づいてコンピュータ起動装置２５０を認証する機器認証手段としての書き込み認証手段２２０ｂと、コンピュータ起動装置２５０及び第３の許可情報アクセス手段２２２を関連付け、読み出し認証手段２２０ａ又は書き込み認証手段２２０ｂによって認証コンピュータ起動装置２５０が認証されたとき、読み出し認証手段２２０ａ又は書き込み認証手段２２０ｂによって認証されたコンピュータ起動装置２５０に関連付けられた第３の許可情報アクセス手段２２２を選択しコンピュータ起動装置２５０にアクセスを行わせる選択アクセス手段２１９とを、受信手段１１１（図１参照）と、送信手段１１２（図１参照）と、第１の認証手段１１３ａと、第２の認証手段１１３ｂ（図１参照）と、選択アクセス手段１１９（図１参照）とに代えて電子キー１１０が有した構成と同様である。
【００７４】
また、受信手段２１１は、コンピュータ起動装置２５０が第３の許可情報アクセス手段２２２にアクセスを行うことで第３の記憶手段２２１に新規許可情報を書き込む場合に、コンピュータ起動装置２５０を電子キー２１０に認証させる機器認証情報である暗号化された書き込み用認証情報（以下、暗号書き込み用認証情報という。）と、コンピュータ起動装置２５０が第３の許可情報アクセス手段２２２にアクセスを行うことで第３の記憶手段２２１から許可情報を読み込む場合に、コンピュータ起動装置２５０を電子キー２１０に認証させる機器認証情報である読み出し用認証情報と、暗号化された新規許可情報（以下、暗号新規許可情報という。）とをコンピュータ起動装置２５０から無線で受信するようになっている。
【００７５】
また、読み出し認証手段２２０ａは、２４ビットの情報によって構成された読み出し用認証情報に基づいて、コンピュータ起動装置２５０を認証するようになっており、また、書き込み認証手段２２０ｂは、６４ビットの情報によって構成された暗号書き込み用認証情報を復号し、復号された書き込み用認証情報に基づいて、コンピュータ起動装置２５０を認証するようになっている。
【００７６】
また、第３の記憶手段２２１は、第１の記憶手段１１４及び第２の記憶手段１１６とは互いに独立したＲＡＭで構成され、コンピュータ起動装置２５０にコンピュータを起動させるよう許可する暗号許可情報として、暗号化された個人名情報を記憶するようになっている。また、第３の許可情報アクセス手段２２２は、第３の記憶手段２２１の記憶領域に割り振られているアドレス番号の先頭番号及び最後番号以外の所定の番号から最後番号に向けて暗号許可情報のアクセスを行う方法で、第３の記憶手段２２１のみに暗号許可情報のアクセスを行うようになっている。

【００７７】
また、コンピュータ起動装置２５０は、２４ビットの情報によって構成された読み出し用認証情報を生成する読み出し用認証情報生成手段２５１ａと、６４ビットの情報によって構成された書き込み用認証情報を生成し、生成された書き込み用認証情報を所定の暗号化ルールで暗号化することで暗号書き込み認証情報を生成する書き込み用認証情報生成手段２５１ｂと、読み出し用認証情報、暗号書き込み用認証情報及び暗号新規許可情報を電子キー２１０に無線で送信する機器認証情報送信手段としての送信手段２５２とを備えている。
【００７８】
また、コンピュータ起動装置２５０は、暗号許可情報を電子キー２１０から無線で受信する受信手段２５３と、暗号許可情報を復号し、復号された許可情報が予め記憶された情報と一致するか否かを判定し、一致すると判定されたとき、復号された許可情報が正規の許可情報であると認証を行う許可情報認証手段２５４と、許可情報認証手段２５４によって復号された許可情報が正規の許可情報であると認証された場合、コンピュータを起動する起動手段２５５と、新規許可情報を生成し、生成された新規許可情報を所定の暗号化ルールで暗号化することで暗号新規許可情報を生成する新規許可情報生成手段２５６とを備えている。
【００７９】
なお、許可情報認証手段２５４によって正規の許可情報と認証される許可情報は電子キー２１０の第３の許可情報アクセス手段２２２によって電子キー２１０の第３の記憶手段２２１から読み出されるので、許可情報認証手段２５４は、電子キー２１０の第３の許可情報アクセス手段２２２にアクセスを行うキーアクセス手段を構成している。
【００８０】
次に、本実施の形態に係る電子キーシステム２００が、コンピュータ起動装置２５０にコンピュータを起動させる動作について説明する。
【００８１】
まず、コンピュータ起動装置２５０の読み出し用認証情報生成手段２５１ａによって予め記憶された配列によって構成された２４ビットの情報が読み出し用認証情報として生成され、生成された読み出し用認証情報がコンピュータ起動装置２５０の送信手段２５２によって電子キー２１０に無線で送信される。
【００８２】
次いで、電子キー２１０の受信手段２１１によって読み出し用認証情報が無線で受信され、受信された読み出し用認証情報が読み出し認証手段２２０ａ及び書き込み認証手段２２０ｂに出力される。
【００８３】
続いて、読み出し認証手段２２０ａに読み出し用認証情報が入力され、入力された読み出し用認証情報を構成する２４ビットの情報と読み出し認証手段２２０ａによって予め記憶された２４ビットの情報とが一致するか否かが読み出し認証手段２２０ａによって判定される。判定の結果、一致するので、読み出し用認証情報を送信したコンピュータ起動装置２５０は、電子キー２１０の読み出し認証手段２２０ａによってコンピュータ起動装置２５０であると認証される。
【００８４】
また、書き込み認証手段２２０ｂに読み出し用認証情報が入力され、入力された読み出し用認証情報は暗号化されていないので復号されず、入力された読み出し用認証情報を構成する２４ビットの情報が書き込み認証手段２２０ｂによって予め記憶された６４ビットの情報と一致するか否かが書き込み認証手段２２０ｂによって判定される。しかしながら、ビット数が異なるため一致せず、書き込み認証手段２２０ｂに入力された機器認証情報は、書き込み認証手段２２０ｂによって破棄される。
【００８５】
次に、コンピュータ起動装置２５０が読み出し認証手段２２０ａによってコンピュータ起

動装置２５０であると認証されることで、コンピュータ起動装置２５０に関連付けられた第３の許可情報アクセス手段２２２が選択アクセス手段２１９によって選択される。

【００８６】

次いで、第３の記憶手段２２１によって記憶され、所定の暗号化ルールで暗号化された個人名情報が暗号許可情報として、第３の許可情報アクセス手段２２２によって第３の記憶手段２２１の記憶領域に割り振られたアドレス番号の所定の番号から最後番号に向けて読み出され、読み出された暗号許可情報が電子キー２１０の送信手段２１１によってコンピュータ起動装置２５０に無線で送信される。

【００８７】

次に、コンピュータ起動装置２５０の受信手段２５３によって暗号許可情報が受信され、受信された暗号許可情報が許可情報認証手段２５４に出力される。

【００８８】

次いで、許可情報認証手段２５４に暗号許可情報が入力され、入力された暗号許可情報が復号され、復号された許可情報を構成する個人名情報と許可情報認証手段２５４によって予め記憶された個人名情報とが一致するか否かが許可情報認証手段２５４によって判定される。判定の結果、一致するので、復号された許可情報は許可情報認証手段２５４によって正規の許可情報として認証される。

【００８９】

続いて、許可情報認証手段２５４によって復号された許可情報が正規の許可情報として認証されることによって、起動手段２５５によってコンピュータが起動される。

【００９０】

次いで、本実施の形態の電子キーシステム２００が、新規許可情報を電子キー２１０に書き込む動作について説明する。

【００９１】

まず、コンピュータ起動装置２５０の書き込み用認証情報生成手段２５１ｂによって予め記憶された配列によって構成された６４ビットの情報が書き込み用認証情報として書き込み用認証情報生成手段２５１ｂによって生成され、生成された書き込み用認証情報は、書き込み用認証情報生成手段２５１ｂによって所定の暗号化ルールで暗号化されることで暗号書き込み用認証情報が生成される。

【００９２】

次に、コンピュータ起動装置２５０の利用者によって指示された個人名情報が新規許可情報として新規許可情報生成手段２５６によって生成され、生成された新規許可情報は、新規許可情報生成手段２５６によって所定の暗号化ルールで暗号化されることで暗号新規許可情報が生成される。

【００９３】

次いで、コンピュータ起動装置２５０の送信手段２５２によって暗号書き込み用認証情報及び暗号新規許可情報が電子キー２１０に送信される。

【００９４】

続いて、電子キー２１０の受信手段２１１によって暗号書き込み用認証情報及び暗号新規許可情報が受信され、受信された暗号書き込み用認証情報及び暗号新規許可情報が読み出し認証手段２２０ａ及び書き込み認証手段２２０ｂに出力される。

【００９５】

次に、読み出し認証手段２２０ａに暗号書き込み用認証情報及び暗号新規許可情報が入力され、暗号書き込み用認証情報を構成する６４ビットの情報と読み出し認証手段２２０ａによって予め記憶された２４ビットの情報とが一致するか否かが読み出し認証手段２２０ａによって判定される。しかしながら、ビット数が異なり、暗号書き込み用認証情報は暗号化されたままなので一致せず、読み出し認証手段２２０ａに入力された暗号書き込み用認証情報及び暗号新規許可情報は、読み出し認証手段２２０ａによって破棄される。

【００９６】

また、書き込み認証手段２２０ｂに暗号書き込み用認証情報及び暗号新規許可情報が入力

され、入力された暗号書き込み用認証情報が復号され、復号された書き込み用認証情報を構成する６４ビットの情報と書き込み認証手段２２０ｂによって予め記憶された６４ビットの情報とが一致するか否かが書き込み認証手段２２０ｂによって判定される。判定の結果、一致するので、暗号書き込み用認証情報及び暗号新規許可情報を送信したコンピュータ起動装置２５０は、書き込み認証手段２２０ｂによってコンピュータ起動装置２５０であると認証される。

【００９７】

次いで、コンピュータ起動装置２５０が書き込み認証手段２２０ｂによってコンピュータ起動装置２５０であると認証されることで、選択アクセス手段２１９によってコンピュータ起動装置２５０に関連付けられた第３の許可情報アクセス手段２２２が選択され、選択された第３の許可情報アクセス手段２２２に暗号新規許可情報が出力される。

【００９８】

続いて、第３の許可情報アクセス手段２２２に入力された暗号新規許可情報が、第３の許可情報アクセス手段２２２によって第３の記憶手段２２１の記憶領域に割り振られたアドレス番号の所定の番号から最後番号に向けて書き込まれる。

【００９９】

以上に説明したように、電子キー２１０は、許可情報の第３の記憶手段２２１からの読み出しがコンピュータ起動装置２５０によって要求されたとき、コンピュータ起動装置２５０からの２４ビットの読み出し用認証情報が予め記憶された情報と一致するか否かでコンピュータ起動装置２５０を読み出し認証手段２２０ａが認証し、許可情報の第３の記憶手段２２１への書き込みがコンピュータ起動装置２５０によって要求されたとき、コンピュータ起動装置２５０からの暗号化された６４ビットの書き込み用認証情報を書き込み認証手段２２０ｂが復号し、復号された書き込み用認証情報が予め記憶された情報と一致するか否かでコンピュータ起動装置２５０を書き込み認証手段２２０ｂが認証するので、第３の記憶手段２２１からの許可情報の読み出しがコンピュータ起動装置２５０によって要求されたときと第３の記憶手段２２１への許可情報の書き込みがコンピュータ起動装置２５０によって要求されたときとで、許可情報の安全性の度合に差をつけることができる。

【０１００】

なお、本実施の形態において、読み出し用認証情報として２４ビットの情報を、書き込み用認証情報として６４ビットの情報を用いたが、本発明の読み出し用認証情報及び書き込み用認証情報は、２４ビット及び６４ビット以外のビット数の情報でも良い。

【０１０１】

また、本実施の形態の動作において、読み出される場合と比較して書き込まれる場合に安全性が高く設定される許可情報として個人名情報を用いたが、本発明の許可情報は、読み出される場合と書き込まれる場合とで安全性に差が設定される個人情報であれば、個人名情報以外の情報でも良い。

【０１０２】

【発明の効果】

以上に説明したように、本発明によれば、複数の電子機器の作動を許可することができる電子キー及び電子キーシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る電子キーシステムのブロック図

【図２】本発明の第２の実施の形態に係る電子キーシステムのブロック図

【符号の説明】

１００　電子キーシステム

１１０　電子キー

１１３ａ　第１の認証手段（認証手段）

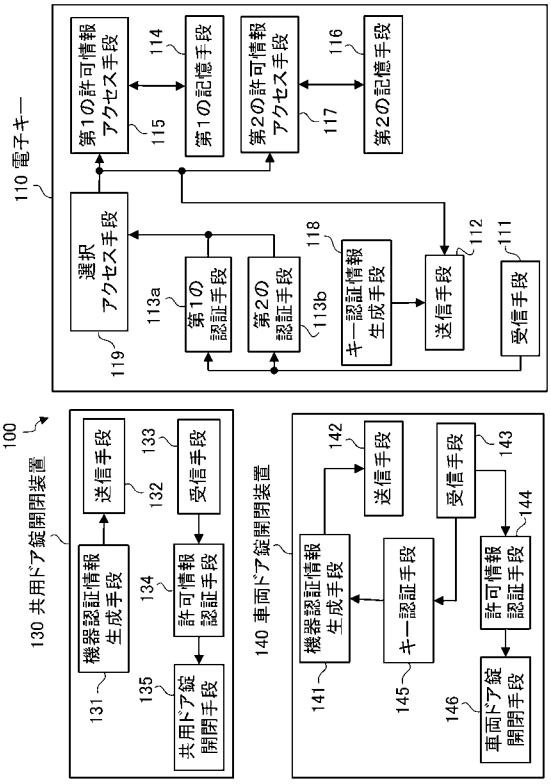
１１３ｂ　第２の認証手段（認証手段）

１１４　第１の記憶手段（記憶手段）

１１５　第１の許可情報アクセス手段（許可情報アクセス手段）

１１６　第２の記憶手段（記憶手段）
１１７　第２の許可情報アクセス手段（許可情報アクセス手段）
１１９　選択アクセス手段
１３０　共用ドア錠開閉装置（電子機器）
１３２　送信手段（機器認証情報送信手段）
１４０　車両ドア錠開閉装置（電子機器）
１４２　送信手段（機器認証情報送信手段）
２００　電子キーシステム
２１０　電子キー
２１９　選択アクセス手段
２２０ａ　読み出し認証手段（認証手段）
２２０ｂ　書き込み認証手段（認証手段）
２２１　第３の記憶手段（記憶手段）
２２２　第３の許可情報アクセス手段（許可情報アクセス手段）
２５０　コンピュータ起動装置（電子機器）
２５２　送信手段（機器認証情報送信手段）

【図１】



【図２】