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

特許第4091611号
(P4091611)

(45)発行日　平成20年5月28日(2008.5.28)　(24)登録日　平成20年3月7日(2008.3.7)

(51)Int.Cl.		F I		
G06K 17/00	(2006.01)	G06K	17/00	T
E05B 49/00	(2006.01)	G06K	17/00	F
H04L 9/32	(2006.01)	E05B	49/00	J
G06K 19/07	(2006.01)	H04L	9/00	675A
G06K 19/10	(2006.01)	G06K	19/00	H

請求項の数 5　(全 13 頁)　最終頁に続く

(21)出願番号　特願2005-118786 (P2005-118786)
(22)出願日　平成17年4月15日 (2005.4.15)
(65)公開番号　特開2006-301731 (P2006-301731A)
(43)公開日　平成18年11月2日 (2006.11.2)
審査請求日　平成17年9月13日 (2005.9.13)

(73)特許権者　305021487
村上　剛康
神奈川県横浜市青葉区松風台２３番地２４
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(72)発明者　村上　剛康
神奈川県横浜市青葉区松風台２３番地２４

審査官　前田　浩

最終頁に続く

(54)【発明の名称】認証登録処理装置及び認証登録処理方法

(57)【特許請求の範囲】

【請求項１】

認証ユニットと、所定範囲内に存在する認証ユニットから識別データを受信できた場合に作動可能状態となるオブジェクトユニットとを各ユニットに対応する登録権限鍵を用いて関連付ける認証登録処理装置であって、

前記認証登録処理装置はコード判定手段と書込制御手段とを備え、

前記コード判定手段は、認証ユニットに格納された第１の固有データと、前記認証ユニットに対応した登録権限鍵に格納された第２の固有データとを読み取り、前記第１の固有データと前記第２の固有データとを照合する第１の権限照合処理と、

更に、オブジェクトユニットに格納された第３の固有データと、前記オブジェクトユニットに対応した登録権限鍵に格納された第４の固有データとを読み取り、前記第３の固有データと前記第４の固有データとを照合する第２の権限照合処理とを実行し、

前記コード判定手段が前記第１、第２の権限照合処理を完了した場合に、前記書込制御手段は、前記オブジェクトユニットに記録された識別データを前記認証ユニットに書き込み、更に前記認証ユニットに記録された識別データを前記オブジェクトユニットに書き込む相互登録処理を実行することを特徴とする認証登録処理装置。

【請求項２】

前記相互登録処理は、

前記オブジェクトユニットに既に認証ユニットの識別データが書き込まれている場合には、既に書き込まれている識別データを維持しながら、新たに権限照合処理を完了した識

別データを書き込み、
前記認証ユニットに既に前記オブジェクトユニットの識別データが書き込まれている場合には、既に書き込まれている識別データを維持しながら、新たに権限照合処理を完了した識別データを書き込むことを特徴とする請求項１に記載した認証登録処理装置。
【請求項３】
前記認証登録処理装置は、第１の権限照合処理を完了した場合に、前記認証ユニットに記録されたオブジェクトユニットの識別データの表示又は削除を許容することを特徴とする請求項１又は２に記載の認証登録処理装置。
【請求項４】
前記認証登録処理装置は、第２の権限照合処理を完了した場合に、前記オブジェクトユニットに記録された認証ユニットの識別データの表示又は削除を許容することを特徴とする請求項１～３のいずれか１項に記載の認証登録処理装置。
【請求項５】
認証ユニットと、所定範囲内に存在する認証ユニットから識別データを受信できた場合に作動可能状態となるオブジェクトユニットとを各ユニットに対応する登録権限鍵を用いて関連付ける認証登録処理方法であって、
認証ユニットに格納された第１の固有データと、前記認証ユニットに対応した登録権限鍵に格納された第２の固有データとを読み取り、前記第１の固有データと前記第２の固有データとを照合する第１の権限照合処理を実行する段階と、
更に、オブジェクトユニットに格納された第３の固有データと、前記オブジェクトユニットに対応した登録権限鍵に格納された第４の固有データとを読み取り、前記第３の固有データと前記第４の固有データとを照合する第２の権限照合処理を実行する段階と、
前記第１、第２の権限照合処理を完了した場合に、前記オブジェクトユニットの識別データを前記認証ユニットに書き込み、更に前記認証ユニットの識別データを前記オブジェクトユニットに書き込む相互登録処理を実行する段階と
を含むことを特徴とする認証登録処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証ユニットと、所定範囲内に存在する認証ユニットから識別データを受信できた場合に作動可能状態となるオブジェクトユニットとを関連付ける認証登録処理装置及び認証登録処理方法に関する。
【背景技術】
【０００２】
従来、セキュリティ向上を目的として、貴重品等の紛失や盗難の早期発見のために、カード紛失自動通報方法およびシステムに関する技術が開示されている（例えば、特許文献１を参照。）。この特許文献１に記載の技術によれば、携帯型リード／ライトユニットはタイマーをスタートさせた後、一定時間経過するとＩＤカードを読み取りにゆき、ＩＤカードの有無を判定する。ＩＤカードを紛失した場合には、ＩＤカードと携帯型リード／ライトユニットとの間の距離が通信可能範囲外となる。この場合、携帯電話機に対してＩＤカードの紛失を示すデータを送信し、携帯電話機は管理センターに発呼し、通信ネットワークを介して管理センターにＩＤカードを紛失したことを通報する。
【０００３】
また、本来の利便性を損なうことなく高度なセキュリティを実現することのできるセキュリティ装置及び方法に関する技術も開示されている（例えば、特許文献２を参照。）。この特許文献２に記載の技術によれば、２つの機器を、近距離無線通信を利用した相互認証によってペアとなし、ペアの条件が成立しなくなったときに携帯型情報機器が備える一部機能を一時的に失効させる。ペアの条件が成立すれば、再度、失効させた機能を有効に戻す。
【０００４】

更に、電源の有無を気にすることなく、貴重品管理を行なうことができる技術も開示されている（例えば、特許文献３を参照。）。この特許文献３に記載の技術によれば、貴重品に取り付けた電子タグを用い、この電子タグからの信号を携帯電話で受信する。

【０００５】

更に、無線通信技術を使用したワイヤレス電子鍵が、自動車の施錠、開錠システムに導入され始めている。この際、購入した自動車１台に対して１又は２個のワイヤレス電子鍵が購入者に提供される。購入した自動車には電子鍵の識別コード、電子鍵には自動車の識別コードが既に工場で書き込まれている。そして、自動車とワイヤレス電子鍵とが相互認証しあうことにより、本人認証を行なう。

【０００６】

このように監視装置と、その監視対象物とを関連付けることにより、セキュリティを向上させることができる。

【特許文献１】特開２００１－３１２７０２号公報（第１頁）

【特許文献２】特開２００３－２８８３２８号公報（第１頁）

【特許文献３】特開２００４－８６４１１号公報（第１頁）

【発明の開示】

【発明が解決しようとする課題】

【０００７】

今日、キャッシュカード、クレジットカードや電子マネーといった多様なカードを利用しているが、セキュリティ向上のため、ＩＣカード化が推進されている。また、ワイヤレス電子鍵が普及した社会では、上述の自動車の他にも、自宅の玄関ドアの鍵などにおいても利用される可能性がある。

【０００８】

このような環境では、監視対象物毎に監視装置が提供されると管理が煩雑である。そこで、利用者自身が、監視装置と様々な監視対象物とを関連付けとを行なうことができれば便利であるが、その際には監視対象物の正当な所有者の意思の確認が必要になる。

【０００９】

しかし、上記の例で示したようにワイヤレス電子鍵と自動車などの制御対象機器の間での相互の関連付けを、利用者自身が行なうことを想定していない。このため、利用者がその関連付けを行なう際に、ワイヤレス電子鍵や制御対象機器の正当な所有者たること又はその所有者の意思の確認ができる簡潔かつ効率的な方法は開示されていない。

【００１０】

また、ワイヤレス電子鍵の制御対象機器としてカードに注目すると、従来は、各カード会社が、独自のセキュリティ管理を行なっているため、システムに共通性がない。更に、このセキュリティ管理は、事業者側で決められるため、利用者側でセキュリティ上講じることのできる自衛策がなかった。

【００１１】

その上、利用者の本人認証として生体情報や印鑑などを使用する場合もある。しかし、このような認証方法においては、取引などの際に、指紋、静脈情報や印影を直接的に用いるため、取引毎にそれらの流失や、盗み取りの危険が発生する。

【００１２】

本発明は、上記課題を解決するためになされたものであり、その目的は、ワイヤレス電子鍵とその制御対象機器であるカードや自動車などのセキュリティを向上させながら、ワイヤレス電子鍵とカードや自動車の関連付けを安全で効率的に管理することができる認証登録処理装置及び認証登録処理方法を提供することにある。

【課題を解決するための手段】

【００１３】

上記問題点を解決するために、請求項１に記載の発明は、認証ユニットと、所定範囲内に存在する認証ユニットから識別データを受信できた場合に作動可能状態となるオブジェクトユニットとを各ユニットに対応する登録権限鍵を用いて関連付ける認証登録処理装置

であって、前記認証登録処理装置は前記コード判定手段と前記書込制御手段とを備え、前記コード判定手段は、認証ユニットに格納された第１の固有データと、前記認証ユニットに対応した登録権限鍵に格納された第２の固有データとを読み取り、前記第１の固有データと前記第２の固有データとを照合する第１の権限照合処理と、更に、オブジェクトユニットに格納された第３の固有データと、前記オブジェクトユニットに対応した登録権限鍵に格納された第４の固有データとを読み取り、前記第３の固有データと前記第４の固有データとを照合する第２の権限照合処理とを実行し、前記コード判定手段が前記第１、第２の権限照合処理を完了した場合に、前記書込制御手段は、前記オブジェクトユニットに記録された識別データを前記認証ユニットに書き込み、更に前記認証ユニットに記録された識別データを前記オブジェクトユニットに書き込む相互登録処理を実行することを要旨とする。

【００１４】

請求項２に記載の発明は、請求項１に記載した認証登録処理装置において、前記相互登録処理は、前記オブジェクトユニットに既に認証ユニットの識別データが書き込まれている場合には、既に書き込まれている識別データを維持しながら、新たに権限照合処理を完了した識別データを書き込み、前記認証ユニットに既に前記オブジェクトユニットの識別データが書き込まれている場合には、既に書き込まれている識別データを維持しながら、新たに権限照合処理を完了した識別データを書き込むことを要旨とする。

【００１５】

請求項３に記載の発明は、請求項１又は２に記載の認証登録処理装置において、前記認証登録処理装置は、第１の権限照合処理を完了した場合に、前記認証ユニットに記録されたオブジェクトユニットの識別データの表示又は削除を許容することを要旨とする。

【００１６】

請求項４に記載の発明は、請求項１～３のいずれか１項に記載の認証登録処理装置において、前記認証登録処理装置は、第２の権限照合処理を完了した場合に、前記オブジェクトユニットに記録された認証ユニットの識別データの表示又は削除を許容することを要旨とする。

【００１７】

請求項５に記載の発明は、認証ユニットと、所定範囲内に存在する認証ユニットから識別データを受信できた場合に作動可能状態となるオブジェクトユニットとを各ユニットに対応する登録権限鍵を用いて関連付ける認証登録処理方法であって、認証ユニットに格納された第１の固有データと、前記認証ユニットに対応した登録権限鍵に格納された第２の固有データとを読み取り、前記第１の固有データと前記第２の固有データとを照合する第１の権限照合処理を実行する段階と、更に、オブジェクトユニットに格納された第３の固有データと、前記オブジェクトユニットに対応した登録権限鍵に格納された第４の固有データを読み取り、前記第３の固有データと前記第４の固有データとを照合する第２の権限照合処理を実行する段階と、前記書込制御手段は、前記第１、第２の権限照合処理を完了した場合に、前記オブジェクトユニットの識別データを前記認証ユニットに書き込み、更に前記認証ユニットの識別データを前記オブジェクトユニットに書き込む相互登録処理を実行する段階とを含むことを要旨とする。

【００１８】

（作用）

本発明によれば、登録権限鍵の照合を条件として、オブジェクトユニットに記録された識別データを認証ユニットに書き込み、更に認証ユニットに記録された識別データをオブジェクトユニットに書き込む。このため、利用者はこの登録権限鍵により本人の意思を確認した上で相互登録処理を行なうことができる。従って、万一、オブジェクトユニットが、所有者の意思によらず、第三者に渡ったとしても、第三者が勝手に相互登録処理を行なうことを抑制できる。このように、利用者において、オブジェクトユニットや認証ユニットとは別に登録権限鍵を管理させることにより、安全を確保できる。

【００１９】

本発明によれば、既に識別データが登録されている場合にも、新たに権限照合処理を完了した識別データは追記される。これにより、オブジェクトユニットや認証ユニットに書き込まれた識別データの内１つの識別データを受信できた場合に相互の認証を完了させるように構成することができる。この場合、書き込まれた識別データの内１つの識別データを認証ユニットから受信できた場合に作動可能状態にする。従って、権限登録鍵を用いてスペアキーとなる追加のワイヤレス電子鍵を作成し、本人以外の家族の者でも使用でき、セキュリティとともに利便性を確保することができる。

【００２０】

また、オブジェクトユニットや認証ユニットに書き込まれた識別データのすべての識別データを受信できた場合に相互の認証を完了させるように構成することもできる。この場合、書き込まれた識別データの全部の識別データを認証ユニットから受信できた場合に作動可能状態にすることにより、セキュリティを強化することができる。

【００２１】

本発明によれば、第１の権限照合処理を完了した場合に、認証ユニットに記録されたオブジェクトユニットの識別データの表示又は削除を許容するため、認証ユニットに記録された情報の漏洩や変更を抑制することができる。

【００２２】

本発明によれば、第２の権限照合処理を完了した場合に、オブジェクトユニットに記録された認証ユニットの識別データの表示又は削除を許容するため、オブジェクトユニットに記録された情報の漏洩や変更を抑制することができる。

【発明の効果】

【００２３】

本発明によれば、ワイヤレス電子鍵として使用する認証ユニットとその制御対象機器であるオブジェクトユニットのセキュリティを向上させながら、この認証ユニットとオブジェクトユニットの関連付けを安全で効率的に管理することができる認証登録処理装置及び認証登録処理方法を提供することができる。

【発明を実施するための最良の形態】

【００２４】

以下、本発明の一実施形態を図１～図５に従って説明する。本実施形態では、図１に示すように、制御対象物であるオブジェクトユニットとして、ＩＣカード５０を想定する。そして、このＩＣカード５０に対応させたワイヤレス電子鍵（キーホルダー型の認証ユニットとしての送信ユニット１０）を組み合わせて用いる。なお、送信ユニット１０は、身につけて携帯可能なものであれば、特に形状が限定されるものではない。

【００２５】

図１は、相互認証を行なうための送信ユニット１０及びＩＣカード５０の機能ブロック図を示している。送信ユニット１０は送信モジュール１００を内蔵する。この送信モジュール１００は、制御部１１０、通信部１２０、権限認証用メモリ１３０、第１メモリ１４０、第２メモリ１５０を備える。

【００２６】

制御部１１０は、後述する通信部１２０や各メモリ（１３０～１５０）を制御する。

通信部１２０は、所定の範囲内に相互認証を行なうための信号を無線電波として発信する。この信号は、送信ユニット１０から所定範囲内にあるＩＣカード５０により受信される。

【００２７】

権限認証用メモリ１３０には、相互認証用のコードをメモリに書き込む場合に、本人の意思確認用の第１の固有データとしての固有コードが記録される。第１メモリ１４０、第２メモリ１５０には、相互認証を行なう場合に用いる識別データが記録される。送信ユニット１０の第１メモリ１４０には、この送信モジュール１００を特定する識別コードデータが記録される。送信ユニット１０の第２メモリ１５０には、この送信モジュール１００と相互認証を行なう受信モジュール５００を特定する識別コードデータが記録される。な

お、第２メモリ１５０には、複数の識別コードの書き込みが可能である。

【００２８】

一方、ＩＣカード５０は、他の利用装置７０を使用する場合に用いるＩＣカードである。例えば、現金自動預支払機に用いるキャッシュカードや、店舗等で用いるクレジットカード、電子マネー用ＩＣカード等に応用することができる。このために、ＩＣカード５０は、各種情報を記録したＩＣチップ５１を搭載している。

【００２９】

更に、ＩＣカード５０は、ＩＣチップ５１を制御する受信モジュール５００を備えている。この受信モジュール５００は、制御部５１０、通信部５２０、権限認証用メモリ５３０、第１メモリ５４０、第２メモリ５５０を備える。

【００３０】

制御部５１０は、後述する通信部５２０や各メモリ（５３０～５５０）を制御する。

通信部５２０は、所定の範囲内に相互認証を行なうための信号を無線電波として受信する。ＩＣカード５０から所定範囲内にある送信ユニット１０により発信された信号を受信する。

【００３１】

権限認証用メモリ５３０には、相互認証用のコードをメモリに書き込む場合に、本人の意思確認用の第３の固有データとしての固有コードが記録される。第１メモリ５４０、第２メモリ５５０には、相互認証を行なう場合に用いる識別データが記録される。ＩＣカード５０の第１メモリ５４０には、この受信モジュール５００を特定する識別コードデータが記録される。ＩＣカード５０の第２メモリ５５０には、この受信モジュール５００と相互認証を行なう送信モジュール１００を特定する識別コードデータが記録される。なお、第２メモリ５５０には、複数の識別コードを書き込むことができる。

【００３２】

このように、図２に示すように、送信ユニット１０とＩＣカード５０とは、電波到達範囲Ａの距離にある限り、相互認証を行なうことができる。

（登録管理処理）

送信ユニット１０とＩＣカード５０とが相互認証処理を行なう場合、予め相互認証のための登録管理処理を行なっておく必要がある。この登録管理処理には、図３に示す認証登録処理装置としてのモジュール相互書込装置３０と、送信ユニット登録権限鍵２０及び受信ユニット登録権限鍵６０を用いる。この送信ユニット登録権限鍵２０及び受信ユニット登録権限鍵６０は、利用者が送信ユニット１０やＩＣカード５０の各ユニットを取得する場合に提供される。そして、送信ユニット登録権限鍵２０はメモリ２１を備える。このメモリ２１には、この送信ユニット登録権限鍵２０に対応する送信ユニット１０の権限認証用メモリ１３０に記録された固有コードと同一のコードが記録される。また、受信ユニット登録権限鍵６０はメモリ６１を備える。このメモリ６１には、この受信ユニット登録権限鍵６０に対応するＩＣカード５０の権限認証用メモリ５３０に記録された固有コードと同一のコードが記録される。

【００３３】

そして、モジュール相互書込装置３０は、送信ユニット登録権限鍵２０及び受信ユニット登録権限鍵６０、送信ユニット１０、ＩＣカード５０との間でデータ交換を行なうためのインターフェイス部を備える。更に、モジュール相互書込装置３０は、各インターフェイス部に接続されたコード判定手段としてのコード判定部３１や書込制御手段としての書込制御部３２、選択キー３３を備える。

【００３４】

コード判定部３１は、送信ユニット登録権限鍵２０、受信ユニット登録権限鍵６０のメモリ（２１、６１）、送信ユニット１０、ＩＣカード５０の権限認証用メモリ（１３０、５３０）に記録されたデータを読み取る。

【００３５】

書込制御部３２は、送信ユニット１０、ＩＣカード５０の第１メモリ（１４０、５４０

）に記録されたデータを読み取る。更に、登録管理処理を行なう場合には第２メモリ（１５０、５５０）に識別データを記録する。選択キー３３は、利用者が各種処理を選択する場合に用いる。本実施形態では、後述するように相互登録処理モード、表示モードや削除モードの各処理を選択することができる。

【００３６】

モジュール相互書込装置３０は、図４に示す登録管理処理を実行する。

まず、モジュール相互書込装置３０のコード判定部３１は、固有コードの取得を行なう（ステップＳ１－１）。具体的には、コード判定部３１は、第１の権限照合処理を実行するために、インターフェイス部を介して、送信ユニット１０に搭載された送信モジュール１００の権限認証用メモリ１３０に予め設定された固有コード（第１の固有データ）の読み取りを行なう。更に、この送信ユニット１０に対応したインターフェイス部を介して、送信ユニット登録権限鍵２０のメモリ２１に予め設定された固有コード（第２の固有データ）の読み取りを行なう。

【００３７】

次に、コード判定部３１は、取得した二つの固有コードが一致しているかどうかを照合する（ステップＳ１－２）。そして、２つの固有コードが一致している場合（ステップＳ１－２において「ＹＥＳ」の場合）のみ、コード判定部３１は、書込制御部３２に対して、ユニットの各メモリへのアクセスを許可する（ステップＳ１－３）。ここでは、送信ユニット１０に内蔵される送信モジュール１００の第２メモリ１５０に対するアクセスを許可する。このアクセスにより、送信モジュール１００の第２メモリ１５０への書き込みや、書込済みの識別コードを削除することができる。更に送信モジュール１００の第１メモリ１４０に予め設定された識別コードの読み出しを許可する。なお、両者が一致しない場合（ステップＳ１－２において「ＮＯ」の場合）には、アクセス権限がないものとして処理を終了する。

【００３８】

同様に、モジュール相互書込装置３０のコード判定部３１は、第２の権限照合処理を実行するために、ＩＣカード５０についても固有コードの読み取りを行なう（ステップＳ１－１）。具体的には、インターフェイス部を介して、ＩＣカード５０に搭載された受信モジュール５００の権限認証用メモリ５３０に予め設定された固有コード（第３の固有データ）を取得する。更に、このＩＣカード５０に対応したインターフェイス部を介して、受信ユニット登録権限鍵６０のメモリ６１に予め設定された固有コード（第４の固有データ）の読み取りを行なう。

【００３９】

次に、コード判定部３１は、受信モジュール５００について取得した２つの固有コードが一致しているかどうかを判定する（ステップＳ１－２）。送信ユニット１０の場合と同様に、２つの固有コードが一致している場合（ステップＳ１－２において「ＹＥＳ」の場合）のみ、コード判定部３１は、書込制御部３２に対して、各ユニットへのアクセスを許可する（ステップＳ１－３）。ここでは、ＩＣカード５０の受信モジュール５００の第２メモリ５５０に対するアクセスを許可する。このアクセスにより、受信モジュール５００の第２メモリ５５０への書き込みや、書込済みの識別コードを削除することができる。更に受信モジュール５００の第１メモリ５４０に予め設定された識別コードの読み出しを許可する。なお、両者が一致しない場合（ステップＳ１－２において「ＮＯ」の場合）には、アクセス権限がないものとして処理を終了する。

【００４０】

そして、各メモリへのアクセスを許可された書込制御部３２は、指定された各種処理を実行する（ステップＳ１－４）。この処理は、モジュール相互書込装置３０の選択キー３３により選択される。

【００４１】

＜相互登録処理＞

相互登録処理モードが選択されている場合、書込制御部３２は、送信モジュール１００

の第１メモリ１４０に予め設定された識別コードを、受信モジュール５００の第２メモリ５５０に書き込む。更に、書込制御部３２は、受信モジュール５００の第１メモリ５４０に予め設定された識別コードを、送信モジュール１００の第２メモリ１５０に書き込む。なお、送信モジュール１００や受信モジュール５００の第２メモリ（１５０、５５０）に対して識別コードを書き込む場合に、識別コードを暗号化することも可能である。これにより、更にセキュリティを向上させることができる。

【００４２】

＜表示処理＞

表示処理モードが選択されている場合の処理を以下に説明する。

送信ユニット１０及び送信ユニット登録権限鍵２０に記録された固有コードの権限照合処理を完了した場合、書込制御部３２は、送信モジュール１００の第１メモリ１４０に書き込まれた送信モジュール１００を特定する識別コードと、送信モジュール１００の第２メモリ１５０に書き込まれた受信モジュール５００の識別コードを表示する。

【００４３】

一方、ＩＣカード５０及び受信ユニット登録権限鍵６０に記録された固有コードの権限照合処理を完了した場合には、書込制御部３２は、受信モジュール５００の第１メモリ５４０に書き込まれた受信モジュール５００を特定する識別コードと、受信モジュール５００の第２メモリ５５０に書き込まれた送信モジュール１００の識別コードを表示する。なお、第２メモリ１５０や第２メモリ５５０に複数の識別コードが記録されている場合には、すべてを表示する。

【００４４】

＜削除処理＞

削除処理モードが選択されている場合の処理を以下に説明する。

送信ユニット１０及び送信ユニット登録権限鍵２０に記録された固有コードの権限照合処理を完了した場合、書込制御部３２は、送信モジュール１００の第２メモリ１５０へ書き込まれた受信モジュール５００の識別コードの削除を実行する。

【００４５】

一方、ＩＣカード５０及び受信ユニット登録権限鍵６０に記録された固有コードの権限照合処理を完了した場合には、書込制御部３２は、受信モジュール５００の第２メモリ５５０へ書き込まれた送信モジュール１００の識別コードの削除を実行する。なお、第２メモリ１５０や第２メモリ５５０に複数の識別コードが記録されている場合には、選択キー３３を用いて識別コードを選択することができ、ここで選択した識別コードのみを削除することもできる。

【００４６】

（相互認証処理）

次に、相互認証処理について、図５を用いて説明する。ＩＣカード５０の利用者は、送信ユニット１０をＩＣカード５０とは別に携帯する。そして、ＩＣカード５０が利用装置７０に挿入等されると、利用装置７０はＩＣカード５０を認識し、利用装置７０の電源からＩＣチップ５１に電力を供給する。この電力はＩＣチップ５１を介して受信モジュール５００にも供給される（ステップＳ２－１において「ＹＥＳ」）。これにより、ＩＣチップ５１と受信モジュール５００とが作動する。

【００４７】

この場合、送信ユニット１０とＩＣカード５０との間で識別コードの発信処理が行なわれる（ステップＳ２－２）。具体的には、ＩＣカード５０の受信モジュール５００の制御部５１０は、第１メモリに記録された識別コードを発信するとともに、送信モジュール１００からの電波の受信を行なう。詳細には、受信モジュール５００から受信した識別コードが第２メモリ１５０に記録されている場合、送信モジュール１００は、第１メモリ１４０に記録された識別コードを発信する。ここで、第２メモリ１５０に複数の識別コードが記録されている場合には、その内の１つの識別コード信号を受信することを条件に、制御部１１０は第１メモリ１４０に記録された識別コードを発信する。そして、受信モジュー

ル５００が送信モジュール１００からの電波を受信した場合、識別コードの検出を行なう。この場合、電波到達範囲Ａを２ｍ程度の範囲内として、その範囲内で信号を受信できるようにしておく。

【００４８】

そして、送信モジュール１００と受信モジュール５００とは、信号を相互に送受信して相互に識別コードを確認する（ステップＳ２－３）。具体的には、受信した識別コードが、第２メモリに記録されている識別コードと一致するかどうかを確認する。そして、識別コードと一致する場合（ステップＳ２－３の「ＹＥＳ」の場合）、識別コードを確認した受信モジュール５００の制御部５１０は、ＩＣチップ５１に対して、作動信号の送り出しを行なう（ステップＳ２－４）。この作動信号の送り出しは、受信モジュール５００が送信モジュール１００から、確認された識別コード信号を受信している間、継続される。ここで、第２メモリ５５０に複数の識別コードが記録されている場合には、その内の１つの識別コード信号を受信することを条件に、制御部５１０は、ＩＣチップ５１に対して作動許可を与え、ＩＣチップ５１は作動可能状態になる。本実施形態では、ＩＣチップ５１の出力回路にスイッチを設けて、識別コード信号を受信可能な場合には、このスイッチのオン状態を維持させる。

【００４９】

一方、送信ユニット１０またはＩＣカード５０の一方を紛失、又は盗難に遇ったときは、受信モジュール５００と送信モジュール１００との距離が離れる。この場合、受信モジュール５００は、送信モジュール１００から、識別コード信号を受信できないため、受信モジュール５００の制御部５１０は、ＩＣチップ５１に対して作動信号の送り出しをしない。

【００５０】

上記実施形態の認証登録処理によれば、以下のような効果を得ることができる。

・　上記実施形態では、モジュール相互書込装置３０のコード判定部３１は、登録権限鍵（２０、６０）の固有コードの取得を行なう（ステップＳ１－１）。そして、送信モジュール１００の権限認証用メモリ１３０や、受信モジュール５００の権限認証用メモリ５３０に記録された固有コードが一致している場合のみ、コード判定部３１は、書込制御部３２に対して、各ユニットへのアクセスを許可する（ステップＳ１－３）。この登録権限鍵（２０、６０）を、所有者が確実に管理することにより、対象物の所有者や所有者の意思を確認しながら、送信ユニット１０とＩＣカード５０との相互認証登録を行なうことができる。登録権限鍵がないと、相互認証登録を行なうことができないため、例えば、所有者自身が所有する自動車、玄関ドアやキャッシュカード、クレジットカードが、所有者の意思によらず、他人により勝手に識別コードを登録されることがない。

【００５１】

また、登録権限鍵がないと、各メモリへのアクセスが許容されないため、その登録内容を盗み見たり、あるいはその登録コードを抹消したりすることができない。従って、セキュリティを高く維持することができる。

【００５２】

・　上記実施形態では、モジュール相互書込装置３０や登録権限鍵（２０、６０）を用いて、相互認証登録を行なうことができる。このため、利用者のニーズに応じて自由な認証関係を形成することができる。特に、今後のワイヤレス電子鍵の普及に従い、対象となる品目は増加する。またワイヤレス電子鍵の使用方法の高度化によってワイヤレス電子鍵が多目的な用途に使用されることとなる可能性があり、ワイヤレス電子鍵と対象物の識別コードの登録の必要性と件数は飛躍的に増大する。従って、ＩＣカードの発行会社や、ＩＣカードの種類に係わりなくＩＣカードの安全を共通して確保できるため、フレキシビリティを確保しながら、利用者の安全性と利便性を向上させることができる。

【００５３】

・　上記実施形態では、一つの送信ユニット１０に対して、複数の受信モジュールを対応させることも可能である。このため、様々なＩＣカードを一括して管理することができ

る。

【００５４】

また、上記実施形態では、第２メモリ１５０に複数の識別コードが記録されている場合には、その内の１つの識別コード信号を受信することを条件に、制御部１１０は第１メモリ１４０に記録された識別コードを発信する。また、第２メモリ５５０に複数の識別コードが記録されている場合には、その内の１つの識別コード信号を受信することを条件に、制御部５１０は、ＩＣチップ５１に対して作動信号を送り出す。これにより、相互認証登録を行なった追加の送信ユニット１０を用いて、第三者（例えば家族の者）でもＩＣカード５０を利用できるように設定でき、利便性を確保することができる。

【００５５】

・　上記実施形態では、ＩＣチップ５１に電力が供給された場合（ステップＳ２－１）、制御部５１０は、受信モジュール５００の第１メモリに記録された識別コードを発信するとともに、送信モジュール１００からの電波の受信を行なう。送信モジュール１００は、受信モジュール５００から受信した識別コードが第２メモリ１５０に記録されている場合、第１メモリ１４０に記録された識別コードを発信する。これにより、送信モジュール１００は、受信モジュール５００から要求があった場合のみ、識別コードを発信し、省電力化を図ることができる。

【００５６】

なお、上記実施形態は、以下の態様に変更してもよい。

○　上記実施形態では、オブジェクトユニットとしてＩＣカード５０を用いて説明した。このオブジェクトユニットは、ＩＣチップを搭載したものであれば、ＩＣカード５０に限られるものではなく、自動車、玄関ドア等あるいはワイヤレス電子鍵自体であってもよい。この場合には、モジュール相互書込装置３０に、その制御対象機器に適したインターフェイス部を設け、識別コードを相互に登録できるようにする。

【００５７】

○　上記実施形態では、モジュール相互書込装置３０と、送信ユニット登録権限鍵２０及び受信ユニット登録権限鍵６０を用いて登録管理処理を行なう。これに加えて、モジュール相互書込装置３０に３以上のインターフェイス部を設け、同時に相互認証登録をさせてもよい。この場合には、他のユニットの第１メモリの記録された識別コードを、各ユニットの第２メモリに記録する。

【００５８】

○　上記実施形態では、送信ユニット１０とＩＣカード５０とを用いて、相互認証処理を行なう。これに加えて、送信ユニット１０とＩＣカード５０との間に他の中間認証用モジュールを介在させてもよい。この場合、送信ユニット１０と中間認証用モジュールとが第１の相互認証処理を実行し、中間認証用モジュールとＩＣカード５０とが第２の相互認証処理を実行する。これにより、ＩＣカード５０だけの紛失、中間認証用モジュールとＩＣカード５０の同時紛失、あるいは、送信ユニット１０とＩＣカード５０の同時紛失の場合にも、送信ユニット１０、中間認証用モジュールとＩＣカード５０の３つ全部を同時に紛失しなければ、ＩＣカード５０のセキュリティを維持することができる。また、中間認証用モジュールに関しても、連鎖的に複数のモジュールを介在させてもよい。これにより、更にセキュリティを向上させることができる。

【００５９】

○　上記実施形態では、送信モジュール１００は、受信モジュール５００から受信した識別コードが第２メモリ１５０に記録されている場合、第１メモリ１４０に記録された識別コードを発信する。これに代えて、送信モジュール１００は常に、識別コードの信号を電波で発信させておいてもよい。そして、電波到達範囲Ａを２ｍ程度の範囲内として、その範囲内で信号を受信できるようにしておく。これにより、迅速な処理を行なうことができる。

【００６０】

○　上記実施形態では、第２メモリ１５０に複数の識別コードが記録されている場合に

は、その内の１つの識別コード信号を受信することを条件に、制御部１１０は第１メモリ１４０に記録された識別コードを発信する。また、第２メモリ５５０に複数の識別コードが記録されている場合には、その内の１つの識別コード信号を受信することを条件に、制御部５１０は、ＩＣチップ５１に対して作動信号を送り出す。これに代えて、第２メモリ（１５０、５５０）に記録されている全識別コードの受信を条件に、識別コードの発信やＩＣチップ５１に対する作動信号の送り出しをしてもよい。これにより、セキュリティの向上を図ることができる。

【００６１】

○　上記実施形態では、制御部５１０は、ＩＣチップ５１に対して作動信号を送り出す場合、ＩＣチップ５１の出力回路にスイッチを設けて、識別コード信号を受信可能な場合には、このスイッチのオン状態を維持する。この場合、識別コード信号の受信を条件にＩＣチップ５１を作動させる方法は、これに限られるものではない。例えば、ＩＣチップ５１に対して可逆的な電磁シールドを設け、識別コード信号の受信を条件にこの電磁シールドを解除できるようにしてもよい。

【００６２】

○　上記実施形態では、相互登録処理において、相互登録処理モードが選択されている場合、書込制御部３２は、受信モジュール５００の第１メモリ５４０に予め設定された識別コードを送信モジュール１００の第２メモリ１５０に書き込む。そして、送信モジュール１００は、受信モジュール５００から受信した第２メモリ１５０に記録されている場合、第１メモリ１４０に記録された識別コードを発信する。これに代えて、送信モジュール１００の第２メモリ１５０への識別コードの書き込みを省略しても良い。この場合、受信モジュール５００が送信モジュール１００から受信した識別コードと、受信モジュール５００の第２メモリ５５０に記録された識別コードの照合を行なう。そして、照合を完了できれば、作動信号の送り出しをする。これにより、送信モジュール１００のメモリ容量を削減することができる。

【図面の簡単な説明】

【００６３】

【図１】本発明の一実施形態の機能ブロックの概略図。

【図２】相互認証の説明図。

【図３】モジュール相互書込装置の説明図。

【図４】登録管理処理の説明図。

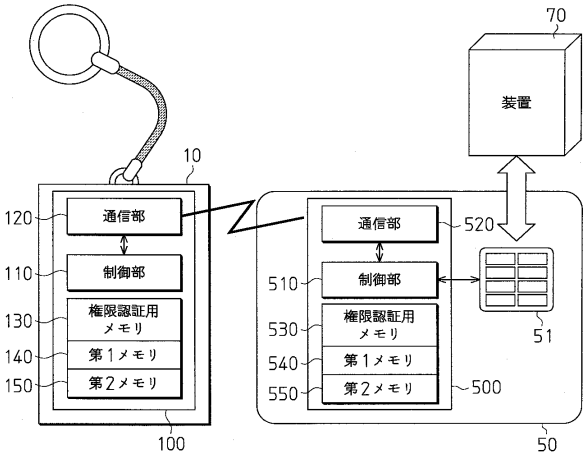
【図５】相互認証処理の説明図。

【符号の説明】

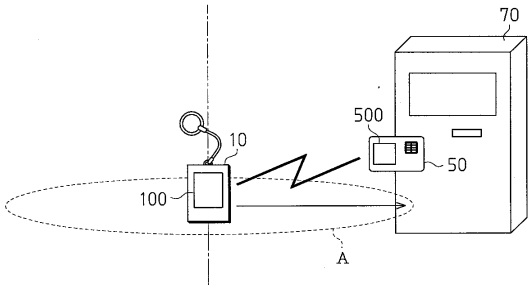
【００６４】

１０…送信ユニット、１００…送信モジュール、１２０…通信部、１３０…権限認証用メモリ、２０…登録権限鍵、３０…モジュール相互書込装置、３１…コード判定部、３２…書込制御部、５０…ＩＣカード、５００…受信モジュール、５２０…通信部、５３０…権限認証用メモリ、６０…登録権限鍵。

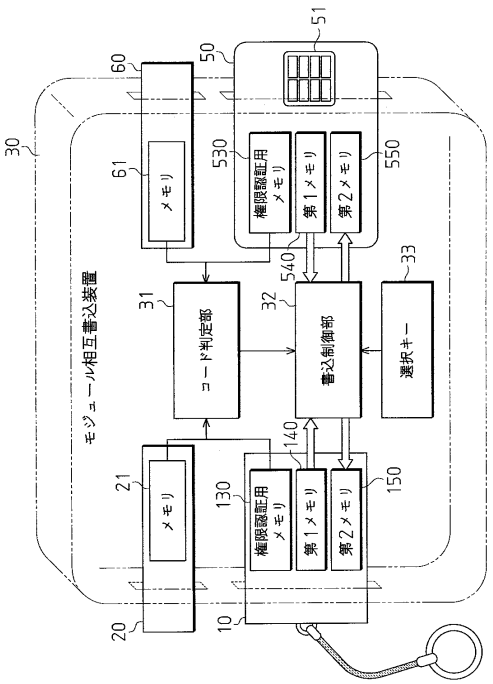
【図１】


70
装置
10
120
通信部
110
制御部
130
権限認証用
メモリ
140
第１メモリ
150
第２メモリ
100
通信部
520
510
制御部
530
権限認証用
メモリ
540
第１メモリ
550
第２メモリ
500
51
50

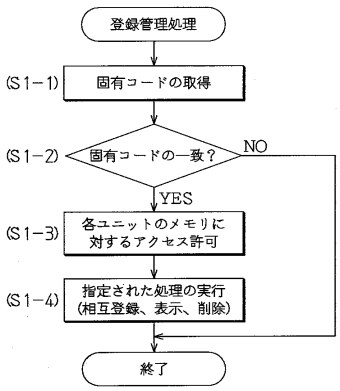
【図２】


70
500
10
50
100
A

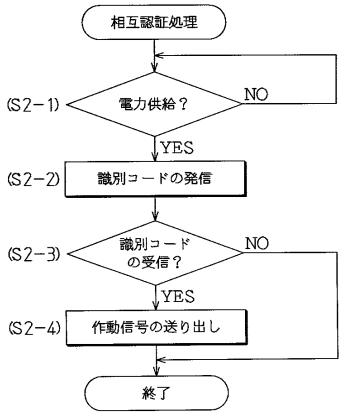
【図３】


51
60
50
30
61
メモリ
530
権限認証用
メモリ
第１メモリ
第２メモリ
550
モジュール相互書込装置
31
コード判定部
32
書込制御部
33
選択キー
540
140
21
メモリ
130
権限認証用
メモリ
第１メモリ
第２メモリ
150
20
10

【図４】


登録管理処理
(S1−1)
固有コードの取得
(S1−2)
固有コードの一致？
NO
YES
(S1−3)
各ユニットのメモリに
対するアクセス許可
(S1−4)
指定された処理の実行
(相互登録、表示、削除)
終了

【図５】


相互認証処理
(S2−1)
電力供給？
NO
YES
(S2−2)
識別コードの発信
(S2−3)
識別コード
の受信？
NO
YES
(S2−4)
作動信号の送り出し
終了

フロントページの続き

(51)Int.Cl. F I
G06K 19/00 R

(56)参考文献 特開２００３－２８８３２８（ＪＰ，Ａ）
特開２００４－２２０４０２（ＪＰ，Ａ）
特開平０５－２８２３３５（ＪＰ，Ａ）
特開昭６３－２１１０４２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｋ １７／００－１９／１８