

(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2004-145437  
(P2004-145437A)

(43) 公開日 平成16年5月20日(2004.5.20)

(51) Int. Cl. <sup>7</sup>	F I	テーマコード (参考)
<b>G06F 15/00</b>	G06F 15/00 330B	2C005
<b>B42D 15/10</b>	G06F 15/00 330G	2E250
<b>E05B 49/00</b>	B42D 15/10 501L	5B058
<b>G06K 17/00</b>	B42D 15/10 521	5B085
	E05B 49/00 J	
審査請求 未請求 請求項の数 15 O L (全 16 頁) 最終頁に続く		

(21) 出願番号	特願2002-306934 (P2002-306934)	(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
(22) 出願日	平成14年10月22日 (2002.10.22)	(74) 代理人	100097445 弁理士 岩橋 文雄
		(74) 代理人	100103355 弁理士 坂口 智康
		(74) 代理人	100109667 弁理士 内藤 浩樹
		(72) 発明者	今井 威 神奈川県横浜市港北区綱島東四丁目3番1号 松下通信工業株式会社内
		Fターム(参考)	2C005 MA04 MB07 NA02 NA06 TA21 TA22
		最終頁に続く	

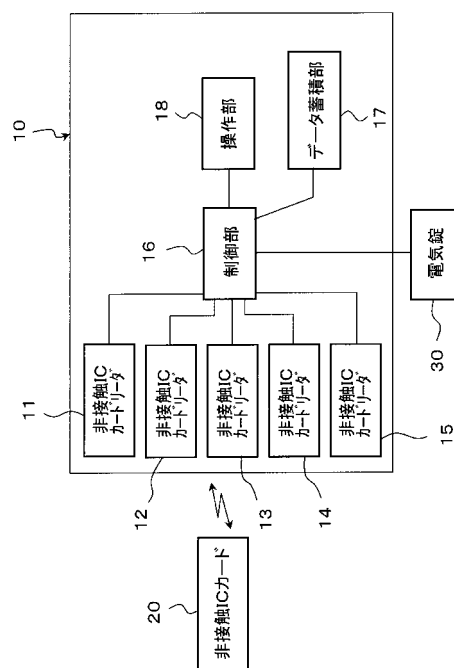
(54) 【発明の名称】 個人認証システム及び方法、セキュリティシステム並びにID情報読取りシステム

(57) 【要約】

【課題】 簡単な操作で個人認証ができると共に記録媒体を不正に入手した者を正規の者と認証することを防止できるようにした個人認証システムを提供することである。

【解決手段】 複数の読取り装置(11~15)と、記録媒体から前記複数の読取り装置のいずれかにて読み取られたID情報を取得するID情報取得手段(16)と、予め定められた登録ID情報と読取り装置との対応関係である登録対応関係を格納する対応関係格納手段(17)と、取得されたID情報とそのID情報を読み取った読取り装置との対応関係が、前記対応関係格納手段に格納された登録対応関係に合致するか否かを判定する判定手段(15)とを有し、前記判定手段での判定結果に基づいて個人認証を行うように構成される。

【選択図】 図1



**【特許請求の範囲】****【請求項 1】**

複数の読取り装置と、  
ID情報の記録された記録媒体から前記複数の読取り装置のいずれかにて読み取られた前記ID情報を取得するID情報取得手段と、  
予め定められた登録ID情報と読取り装置との対応関係である登録対応関係を格納する対応関係格納手段と、  
前記ID情報取得手段にて取得されたID情報とそのID情報を読み取った読取り装置との対応関係が、前記対応関係格納手段に格納された登録対応関係に合致するか否かを判定する判定手段とを有し、  
前記判定手段での判定結果に基づいて個人認証を行うようにしたことを特徴とする個人認証システム。

10

**【請求項 2】**

前記判定手段は、前記ID情報取得手段にて取得されたID情報が登録ID情報に一致するか否かを判定する第一の判定手段と、  
前記取得されたID情報が前記登録ID情報に一致するとの判定が前記第一の判定手段にてなされたときに、前記取得されたID情報を読み取った読取り装置が前記対応関係格納手段に格納された登録対応関係にて決まる前記取得されたID情報に一致した登録ID情報に対応する読取り装置に一致するか否かを判定する第二の判定手段とを有することを特徴とする請求項1記載の個人認証システム。

20

**【請求項 3】**

前記複数の読取り装置のそれぞれは非接触式ICカードリーダーであると共に、前記記憶媒体は非接触ICカードであり、  
前記ID情報取得手段は、ID情報の記録された非接触式ICカードから前記複数の非接触式ICカードリーダーのいずれかにて読み取られた前記ID情報を取得するようにしたことを特徴とする請求項1または2記載の個人認証システム。

**【請求項 4】**

前記複数の非接触式ICカードリーダーは、読取りエリア表示のなされたリーダー埋設部に埋設されると共に、前記読取りエリア表示を目安にした異なる位置で非接触式ICカードからID情報の読取りが可能となるように配置されたことを特徴とする請求項3記載の個人

30

**【請求項 5】**

前記対応関係格納手段は、前記登録対応関係を、読取り装置に対する記録媒体の読取り操作を行う者が認識し得る所定条件の内容に応じて複数種類格納し、  
前記判定手段は、前記複数の読取り装置のいずれかにて記録媒体から前記ID情報が読み取られる際における前記所定条件の内容を判定する条件判定手段を有し、  
前記条件判定手段により判定された前記所定条件の内容に対応する種類の前記登録対応関係を用いるようにしたことを特徴とする請求項1乃至4のいずれかに記載の個人認証システム。

**【請求項 6】**

前記所定条件は、環境的条件を含むことを特徴とする請求項5記載の個人認証システム。

40

**【請求項 7】**

前記所定条件は、時間的条件を含むことを特徴とする請求項5または6記載の個人認証システム。

**【請求項 8】**

ID情報の記録された記録媒体から複数の読取り装置のいずれかにて読み取られた前記ID情報を取得するID情報取得手順と、  
前記ID情報取得手順にて取得されたID情報とそのID情報を読み取った読取り装置との対応関係が、予め定められた登録ID情報と読取り装置との対応関係である登録対応関係に合致するか否かを判定する判定手順とを有し、

50

前記判定手順での判定結果に基づいて個人認証を行うようにしたことを特徴とする個人認証方法。

【請求項 9】

前記判定手順は、前記 ID 情報取得手順にて取得された ID 情報が登録 ID 情報に一致するか否かを判定する第一の判定手順と、

前記取得された ID 情報が前記登録 ID 情報に一致するとの判定が前記第一の判定手順にてなされたときに、前記取得された ID 情報を読み取った読取り装置が前記登録対応関係にて決まる前記取得された ID 情報に一致した登録 ID 情報に対応する読取り装置に一致するか否かを判定する第二の判定手順とを有することを特徴とする請求項 8 記載の個人認証方法。

10

【請求項 10】

前記 ID 情報取得手順は、ID 情報の記録された記録媒体としての非接触式 IC カードから複数の読取り装置としての非接触式 IC カードリーダーのいずれかにて読み取られた前記 ID 情報を取得するようにした請求項 8 または 9 記載の個人認証方法。

【請求項 11】

前記登録対応関係が、読取り装置に対する記録媒体の読取り操作を行う者が認識し得る所定条件の内容に応じて複数種類用意され、

前記判定手順は、前記複数の読取り装置のいずれかにて記録媒体から前記 ID 情報が読み取られる際における前記所定条件の内容を判定する条件判定手順を有し、

前記条件判定手順により判定された前記所定条件の内容に対応する種類の前記登録対応関係を用いるようにしたことを特徴とする請求項 8 乃至 10 のいずれかに記載の個人認証方法。

20

【請求項 12】

請求項 1 乃至 8 のいずれかに記載された個人認証システムと、

前記個人認証システムにおいて、前記取得された ID 情報とその ID 情報を読み取った読取り装置との対応関係が前記対応関係格納手段に格納された登録対応関係に合致したとの判定が前記判定手段にてなされたときに、施錠された錠を解錠する解錠制御手段とを有することを特徴とするセキュリティシステム。

【請求項 13】

ID 情報の記録がなされた記録媒体から前記 ID 情報の読取りを行う複数の読取り装置を備え、

前記複数の読取り装置のそれぞれは、前記記録媒体から読み取った ID 情報を ID 情報とその ID 情報を読み取った読取り装置との対応関係に基づいて認証処理を行うシステムに供給するようにしたことを特徴とする ID 情報読取りシステム。

30

【請求項 14】

前記複数の読取り装置のそれぞれは、記録媒体としての非接触式 IC カードから前記 ID 情報を読み取る非接触式 IC カードリーダーとなることを特徴とする請求項 13 記載の ID 情報読取りシステム。

【請求項 15】

読取りエリア表示のなされたリーダー埋設部を有し、

前記複数の非接触式 IC カードリーダーは、前記リーダー埋設部に埋設され、前記読取りエリア表示を目安にした異なる位置で非接触式 IC カードから ID 情報の読取りが可能となるように配置されたことを特徴とする請求項 14 記載の ID 情報読取りシステムシステム。

40

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記録媒体から読取り装置により ID 情報を読み取り、その ID 情報に基づいて個人認証を行う個人認証システム及び方法に関する。

【0002】

また、本発明は、前記個人認証システムを用いたセキュリティシステムに関する。

50

## 【 0 0 0 3 】

更に、本発明は、前記個人認証システムに用いることのできるID情報読取りシステムに関する。

## 【 0 0 0 4 】

## 【 従来 の 技 術 】

従来、部屋の入退出管理や機器の使用管理等に磁気カード、接触式ICカード、非接触式ICカード等のカード（記録媒体）を利用した個人認証システムが用いられている。このような個人認証システムでは、カードの所持者がそのカードに磁気的あるいは電子的に記録されたID情報をカードリーダーに読み取らせ、そのカードリーダーによって読み取られたID情報が予め登録されたID情報と一致する場合に、そのカードの所持者が正規の者として認証される。

10

## 【 0 0 0 5 】

例えば、このような個人認証システムを施錠されたドアの解錠制御を行うセキュリティシステムに利用することができる。このセキュリティシステムでは、カードの所持者が前記個人認証システムにて正規の者として認証された場合に限り、施錠されたドアの解錠がなされる。従って、正規のカードを所持していない者ではその施錠されたドアの解錠を行うことができない。これにより、ドア内の空間の人的セキュリティを保つことができる。

## 【 0 0 0 6 】

しかし、前述したような個人認証システムでは、カードから読み取られたID情報が予め登録されたID情報と一致すればそのカードの所持者は必ず正規の者として認証されるので、そのカードを不正に入手した者であっても正規の者として認証されてしまう。このような欠点を解決するために、カードリーダーの近傍にテンキーユニットを併設しておき、カードリーダーによってカードから読み取られた前記ID情報及びテンキーユニットの操作によって入力された暗証番号の双方のチェックを行って個人認証を行うシステムが提案されている（例えば、特許文献1参照）。このようなシステムでは、カードを不正に入手した者は、その暗証番号を知らなければ、正規の者として認証されない。

20

## 【 0 0 0 7 】

## 【 特 許 文 献 1 】

特開平6 - 52242号公報

## 【 0 0 0 8 】

## 【 発 明 が 解 決 し よ う と す る 課 題 】

しかし、このような個人認証システムでは、正規のカード所持者は、カードの読取り操作の他に常に暗証番号の入力操作を行わなければならない、その操作が煩雑になるという問題がある。従って、このような個人認証システムを前述したような施錠されたドアの解錠制御を行うセキュリティシステムに適用した場合、その操作に時間がかかり、多くの人が頻繁に入退出を繰り返す部屋のドアでは、人のスムーズな入退出が阻害される可能性がある。

30

## 【 0 0 0 9 】

そこで、本発明は、前述したような問題を解決するためになされたもので、簡単な操作で個人認証ができると共にカードを不正に入手した者を正規の者と認証することを防止できるようにした個人認証システム及び方法を提供するものである。

40

## 【 0 0 1 0 】

また、本発明は、そのような個人認証システムが適用されるセキュリティシステムを提供するものである。

## 【 0 0 1 1 】

更に、本発明は、そのような個人認証システムに適用することのできるID情報読取りシステムを提供するものである。

## 【 0 0 1 2 】

## 【 課 題 を 解 決 す る た め の 手 段 】

本発明に係る個人認証システムは、複数の読取り装置と、ID情報の記録された記録媒体

50

から前記複数の読取り装置のいずれかにて読み取られた前記ID情報を取得するID情報取得手段と、予め定められた登録ID情報と読取り装置との対応関係である登録対応関係を格納する対応関係格納手段と、前記ID情報取得手段にて取得されたID情報とそのID情報を読み取った読取り装置との対応関係が、前記対応関係格納手段に格納された登録対応関係に合致するか否かを判定する判定手段とを有し、前記判定手段での判定結果に基づいて個人認証を行うように構成される。

【0013】

このような構成により、登録されたID情報（登録ID情報）が記録された記録媒体を所持する者が予め定められた登録ID情報と読取り装置との対応関係（登録対応関係）にて決まる前記記録媒体に記録されたID情報（登録ID情報）に対応した読取り装置に対して前記記録媒体の読取り操作を行うと、前記読取り装置にて前記記録媒体から読み取られたID情報が取得され、その取得されたID情報と前記読取り装置との対応関係が、前記登録対応関係に合致するとの判定がなされる。この判定結果に基づいて前記記録媒体の所持者を正規の者として認証することができる。

10

【0014】

一方、登録されたID情報（登録ID情報）が記録された記録媒体を所持する者が予め定めた登録ID情報と読取り装置との対応関係（登録対応関係）にて決まる前記記録媒体に記録されたID情報（登録ID情報）に対応した読取り装置以外の読取り装置に対して前記記録媒体の読取り操作を行うと、前記読取り装置から取得されたID情報と前記読取り装置との対応関係が、前記登録対応関係に合致しないとの判定がなされる。この判定結果に基づいて前記記録媒体の所持者を正規の者とする認証がなされないようにすることができる。

20

【0015】

従って、予め定めた登録ID情報と読取り装置との対応関係（登録対応関係）にて決まる記録媒体に記録されたID情報に対応した読取り装置を知っている者は、その読取り装置に対して記録媒体の読取り操作を行うことにより正規の者として認証され得る。一方、記録媒体を不正に入手した者は、前記登録対応関係にて決まる記録媒体に記録されたID情報に対応した読取り装置を知らないため、そのような読取り装置に対して確実に記録媒体の読取り操作を行うことができない。そのため、記録媒体を不正に入手した者が前述したような読取り装置以外の読取り装置に対して記録媒体の読取り操作を行うと、その者は、

30

【0016】

前記記録媒体に記録すべきID情報は、正規の者として認証されるべき者に対して与えられる情報であれば特に限定されず、個人ごとに異なるものであっても、所定のグループごとに異なるものであっても、全ての個人に対して同一のもの（単一の登録ID情報）であってもよい。

【0017】

また、ID情報を記録した記録媒体は、接触、非接触を問わずそのID情報を読み取る読取り装置が存在するものであれば特に限定されず、磁気カード、接触式ICカード、非接触式ICカード、光学式カード等、カードリーダーにてID情報の読取りが可能となるカード状の記録媒体であっても、また、他の形状のものであってもよい。

40

【0018】

また、本発明に係る個人認証システムは、前記判定手段が、前記ID情報取得手段にて取得されたID情報が登録ID情報に一致するか否かを判定する第一の判定手段と、前記取得されたID情報が前記登録ID情報に一致するとの判定が前記第一の判定手段にてなされたときに、前記取得されたID情報を読み取った読取り装置が前記対応関係格納手段に格納された登録対応関係にて決まる前記取得されたID情報に一致した登録ID情報に対応する読取り装置に一致するか否かを判定する第二の判定手段とを有するように構成することができる。

【0019】

50

このような構成により、取得されたID情報とそのID情報を読み取った読取り装置との対応関係が、予め定められた登録ID情報と読取り装置との対応関係である登録対応関係に合致するか否かを判定することができるようになる。また、登録ID情報と異なるID情報が記録された記録媒体や、ID情報が正常に読み取れない状態の記録媒体については、読取り装置にて読み取られたID情報と読取り装置との対応関係を判定するまでもなく、読取り装置から取得されたID情報と登録ID情報とが一致しないとの判定により、そのような記録媒体を所持する者に対して認証を与えないものとするのが可能となる。

**【0020】**

更に、本発明に係る個人認証システムは、前記複数の読取り装置のそれぞれが非接触式ICカードリーダーであると共に、前記記憶媒体が非接触ICカードであり、前記ID情報取得手段が、ID情報の記録された非接触式ICカードから前記複数の非接触式ICカードリーダーのいずれかにて読み取られた前記ID情報を取得するように構成することができる。

10

**【0021】**

このような構成により、読取り装置に対する記録媒体の読取り操作が非接触にてなされるようになるので、実際に記録媒体の読取り操作のなされた読取り装置の位置を特定し難く、記録媒体の読取り操作の盗み見による正規の読取り装置の不正知得に対する耐性を向上させることが可能となる。

**【0022】**

また、本発明に係る個人認証システムは、前記複数の非接触式ICカードリーダーは、読取りエリア表示のなされたリーダー埋設部に埋設されると共に、前記読取りエリア表示を目安にした異なる位置で非接触式ICカードからID情報の読取りが可能となるように配置されるよう構成することができる。

20

**【0023】**

このような構成により、非接触式ICカードリーダーが常識的に埋設される読取りエリアの中央部以外の位置にて非接触式ICカードからID情報を読み取ることができるように複数の非接触式ICカードリーダーを配置することができる。その結果、カードの読取り操作の盗み見による正規のカードリーダーの不正知得に対する耐性を向上させることが可能となると共に、不正にカードを入手した者が偶然的に適正なカードリーダーにてカードの読取り操作を行う可能性を低減させることができる。

30

**【0024】**

本発明に係る個人認証システムは、前記対応関係格納手段が、前記登録対応関係を、読取り装置に対する記録媒体の読取り操作を行う者が認識し得る所定条件の内容に応じて複数種類格納し、前記判定手段が、前記複数の読取り装置のいずれかにて記録媒体から前記ID情報が読み取られる際における前記所定条件の内容を判定する条件判定手段を有し、前記条件判定手段により判定された前記所定条件の内容に対応する種類の前記登録対応関係を用いるように構成することができる。

**【0025】**

このような構成により、所定条件の内容に応じて判定に用いられる登録対応関係の種類を変えることができるようになるので、記録媒体を不正に入手し、その所定条件の内容に応じてどのような登録対応関係が適用されるかを知らない者を正規の者として認証することを更に確実に防止することができる。一方、その所定条件の内容に応じて判定に用いられる登録関係が変えられても、所定条件の内容に応じてどのような登録対応関係が適用されるかを知らぬ記録媒体の正当な所持者は、認識した所定条件の内容に応じて適正な読取り装置を選択して記録媒体の読取り操作を行うことができる。

40

**【0026】**

前記所定条件は、記録媒体の読取り操作を行う者がその内容を直接的または間接的に認識できる条件であれば特に限定されず、例えば、環境的条件、時間的条件等を含むことができる。

**【0027】**

50

本発明に係る個人認証方法は、ID情報の記録された記録媒体から複数の読取り装置のいずれかにて読み取られた前記ID情報を取得するID情報取得手順と、前記ID情報取得手順にて取得されたID情報とそのID情報を読み取った読取り装置との対応関係が、予め定められた登録ID情報と読取り装置との対応関係である登録対応関係に合致するか否かを判定する判定手順とを有し、前記判定手順での判定結果に基づいて個人認証を行うように構成される。

【0028】

また、本発明に係る個人認証方法は、前記判定手順が、前記ID情報取得手順にて取得されたID情報が登録ID情報に一致するか否かを判定する第一の判定手順と、前記取得されたID情報が前記登録ID情報に一致するとの判定が前記第一の判定手順にてなされたときに、前記取得されたID情報を読み取った読取り装置が前記登録対応関係にて決まる前記取得されたID情報に一致した登録ID情報に対応する読取り装置に一致するか否かを判定する第二の判定手順とを有するように構成することができる。

10

【0029】

更に、本発明に係る個人認証方法は、前記ID情報取得手順が、ID情報の記録された記録媒体としての非接触式ICカードから複数の読取り装置としての非接触式ICカードリーダーのいずれかにて読み取られた前記ID情報を取得するように構成することができる。

【0030】

本発明に係る個人認証方法は、前記登録対応関係が、読取り装置に対する記録媒体の読取り操作を行う者が認識し得る所定条件の内容に応じて複数種類用意され、前記判定手順が、前記複数の読取り装置のいずれかにて記録媒体から前記ID情報が読み取られる際における前記所定条件の内容を判定する条件判定手順を有し、前記条件判定手順により判定された前記所定条件の内容に対応する種類の前記登録対応関係を用いるように構成することができる。

20

【0031】

更に、前述した個人認証システムが適用される本発明に係るセキュリティシステムは、前述したいずれかの個人認証システムと、前記個人認証システムにおいて、前記取得されたID情報とそのID情報を読み取った読取り装置との対応関係が前記対応関係格納手段に格納された登録対応関係に合致したとの判定が前記判定手段にてなされたときに、施錠された錠を解錠する解錠制御手段とを有するように構成される。

30

【0032】

このような構成により、予め定められた登録ID情報と読取り装置との対応関係である登録対応関係にて決まる記録媒体に記録されたID情報に対応した読取り装置を知っている者がその読取り装置に対して記録媒体の読取り操作を行うと、前記ID情報とそのID情報を読み取った読取り装置との対応関係が、前記対応関係格納手段に格納された登録対応関係に合致するとの判定がなされる。その結果、施錠された錠の解錠がなされる。一方、予め定められた登録ID情報と読取り装置との対応関係となる登録対応関係にて決まる記録媒体に記録されたID情報に対応した読取り装置を知らない前記カードの不正所持者が、その読取り装置以外の読取り装置に対して記録媒体の読取り操作を行うと、前記ID情報とそのID情報を読み取った読取り装置との対応関係が、前記対応関係格納手段に格納された登録対応関係に合致しないとの判定がなされる。その結果、施錠された錠の解錠はなされない。

40

【0033】

また、本発明に係るID情報読取りシステムは、ID情報の記録がなされた記録媒体から前記ID情報の読取りを行う複数の読取り装置を備え、前記複数の読取り装置のそれぞれは、前記記録媒体から読み取ったID情報をID情報とそのID情報を読み取った読取り装置との対応関係に基づいて認証処理を行うシステムに供給するように構成される。

【0034】

このような構成により、複数の読取り装置のうちの記録媒体からID情報を実際に読み取った読取り装置とそのID情報との対応関係に基づいて個人認証を行うことができるよう

50

になる。

【0035】

また、本発明に係るID情報読取りシステムは、前記複数の読取り装置のそれぞれは、記録媒体としての非接触式ICカードから前記ID情報を読み取る非接触式ICカードリーダーとなるように構成することができる。

【0036】

更に、本発明に係るID情報読取りシステムは、読取りエリア表示のなされたリーダー埋設部を有し、前記複数の非接触式ICカードリーダーは、前記リーダー埋設部に埋設され、前記読取りエリア表示を目安にした異なる位置で非接触式ICカードからID情報の読取りが可能となるように配置されるように構成することができる。

【0037】

【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。

【0038】

本発明の第一の実施の形態に係るセキュリティシステムは図1に示すように構成される。

【0039】

図1において、このセキュリティシステムは、認証システム10と、セキュリティを確保するための部屋の扉に設けられた電気錠30とを有する。認証システム10は、複数(5台)の非接触式ICカードリーダー11、12、13、14、15(読取り装置)、制御部16、データ蓄積部17及び操作部18を有している。非接触式ICカードリーダー11~15のそれぞれは、その所定範囲に存在する非接触式ICカード20(記録媒体)と無線通信を行って、非接触式ICカード20に記録されたID番号(ID情報)の読取りを行う。制御部16は、複数の非接触式ICカードリーダー11~15のいずれかにて読み取られたID番号に基づいて認証処理を行う。データ蓄積部17は、制御部16での認証処理にて必要な情報を蓄積する。操作部18は、オペレータにより操作され、そのオペレータによる操作に基づいた情報を制御部16に供給する。個人認証システム10の制御部16は、認証処理により得られた結果に基づいて施錠された電気錠30の解錠制御を行う。

【0040】

前記複数の非接触式ICカードリーダー11~15は、例えば、電気錠30が設けられた扉近傍の壁に、図2に示すように設置される。

【0041】

図2において、電気錠30が設けられた扉近傍の壁の表面には円形の読取りエリアマーク40が描かれている。その読取りエリアマーク40が表示された壁内に5台の非接触式ICカードリーダー11、12、13、14、15が埋設されている。非接触式ICカードリーダー13が読取りエリアマーク40内の中央部に配置され、非接触式ICカードリーダー11、15が非接触式ICカードリーダー13の上下に配置され、更に、非接触式ICカードリーダー12、14が非接触式ICカードリーダー13の左右に配置されている。これらの非接触式ICカードリーダー11~15は、前記のように配置させることにより、前記読取りエリアマーク40を目安とした異なる位置で非接触式ICカード20からID番号の読取りが可能となる。

【0042】

データ蓄積部17は、図3に示すような登録対応関係テーブルを格納する。各非接触式ICカードリーダー11、12、13、14、15にはそれらを特定する番号(非接触式ICカードリーダー番号)1、2、3、4、5が付与されている。前記登録対応関係テーブルは、予め定められた各登録ID番号と非接触式ICカードリーダー番号との対応関係(以下、必要に応じて登録対応関係という)を表す。ID番号が登録される毎に、その登録ID番号に対応する非接触式ICカードリーダー番号が決められ、それらの対応関係が登録対応関係として操作部18から入力される。その操作部18から入力された登録対応関係が制御部16を介してデータ蓄積部17の登録対応関係テーブルに追加される。

【0043】

10

20

30

40

50

制御部 16 は、図 4 に示す手順に従って処理を行う。

【 0 0 4 4 】

図 4 において、制御部 16 は、複数の非接触式 IC カードリーダ 11 ~ 15 のいずれかによって非接触式 IC カード 20 から読み取られる ID 番号の入力待ち状態にある (S1)。電気錠 30 の解錠を希望する者は、所持する非接触式 IC カード 20 を読み取りエリアマーク 40 を目安として図 2 に示すように配置された非接触式 IC カードリーダ 11 ~ 15 のいずれかの埋め込み部位にかざす。その非接触式 IC カード 20 がかざされた部位に埋め込まれた非接触式 IC カードリーダは、非接触式 IC カード 20 と無線通信を行ってその非接触式 IC カード 20 から ID 番号を読み取る。

【 0 0 4 5 】

前記 ID 番号を読み取った非接触式 IC カードリーダはその ID 番号を制御部 16 に供給する。前述したように ID 番号の入力待ち状態にある制御部 16 は、前記非接触式 IC カードリーダから ID 番号を取得すると (S1 で YES)、データ蓄積部 17 に格納された前記登録対応関係テーブル (図 3 参照) を参照して前記取得した ID 番号の検索処理を行い (S2)、登録対応関係テーブル内にその取得した ID 番号と同じ登録 ID 番号が有るか否かを判定する (S3)。前記取得した ID 番号と同じ登録 ID 番号が登録対応関係テーブル内に有るとの判定がなされると (S3 で YES)、制御部 16 は、更に、登録対応関係で決まる前記取得した ID 番号と同じ登録 ID 番号に対応した非接触式 IC カードリーダ番号と前記 ID 番号を読み取った非接触式 IC カードリーダに付与されている番号とを比較し (S4)、それらの番号が一致するか否かを判定する (S5)。

10

20

【 0 0 4 6 】

それらの番号が一致すると判定がなされると (S5 で YES)、取得した ID 番号とその ID 番号を読み取った非接触式 IC カードリーダとの対応関係が登録対応関係に合致することから、制御部 16 は、非接触式 IC カード 20 の非接触式 IC カードリーダに対する読取り操作を行った者を正規の者として認証し、電気錠 30 に対して解錠制御信号を供給する (S6)。その解錠制御信号により、施錠された電気錠 30 は解錠される。一方、前記各番号が一致しないとの判定がなされると (S5 で NO)、取得した ID 番号とその ID 番号を読み取った非接触式 IC カードリーダとの対応関係が登録対応関係テーブルに含まれるいずれの登録対応関係にも合致せず、制御部 16 は、非接触式 IC カード 20 の非接触式 IC カードリーダに対する読取り操作を行った者の正規の者としての認証を行うことなく、警告メッセージの出力等、解錠拒否に係る所定の処理を行う (NG)。これにより、電気錠 30 の解錠はなされない。

30

40

【 0 0 4 7 】

前述したような処理がなされることから、登録対応関係にて決められた自己の非接触式 IC カード 20 に記録された ID 番号 (登録 ID 番号) に対応する非接触式 IC カードリーダ (番号) を知っている、即ち、その埋設部位を知っている非接触式 IC カード 20 の正規の所持者は、非接触式 IC カード 20 を読取りエリアマーク 40 を目安にしてその非接触式 IC カードリーダが埋設された部位にかざすことにより、施錠された電気錠 30 の解錠を行うことができる。一方、非接触式 IC カード 20 の不正所持者は、登録対応関係にて決められたその非接触式 IC カード 20 に記録された ID 番号に対応する非接触式 IC カードリーダを知りえないので、読取りエリアマーク 40 内の任意の位置にその非接触式 IC カード 20 をかざしても、ID 番号を読み取った非接触式 IC カードリーダとその ID 番号との対応関係が登録対応関係に合致せず、電気錠 30 の解錠を行うことができない。

【 0 0 4 8 】

前述したようなセキュリティシステムによれば、非接触式 IC カード 20 の正規の所持者は、登録対応関係で決まる正規の非接触式 IC カードリーダの埋設部位にその非接触式 IC カード 20 をかざすという通常の操作だけで、正規の者であるとの認証がなされて電気錠 30 を解錠させることができる。しかし、非接触式 IC カード 20 の不正所持者は登録対応関係で決まる正規の非接触式 IC カードリーダに対する操作を行えないので、その者

50

が正規の者として認証されることが防止され、その結果、電気錠30の解錠が防止される。従って、非接触式ICカード20の正規の所持者に余分な操作を強いることなく、セキュリティ性を向上させることができる。

【0049】

また、読取りエリアマーク40を目安にして正規の非接触式ICカードリーダーの埋設部位に非接触式ICカード20をかざす操作を不正者に盗み見されたとしても、その操作から正規の非接触式ICカードリーダーの埋設部位を正確に判断することが難しい。このため、その正規の非接触式ICカードリーダーの埋設部位の不正知得に対する耐性は高い。

【0050】

更に、読取りエリアマーク40が描かれていることから、通常の者(不正者も含む)は、その中央部に非接触式ICカード20をかざすようになる。従って、読取りエリアマーク40の中央部以外の部位に埋設された非接触式ICカードリーダー11、12、14、15(図2参照)のいずれかと対応関係が定められたID番号を記録した非接触式ICカード20については、不正者がその非接触式ICカード20を偶然的に正規の非接触式ICカードリーダーの埋設部位にかざす可能性は低減される。

10

【0051】

前述したように、通常の者は、読取りエリアマーク40の中央部に非接触式ICカード20をかざすようになるので、その読取りエリアマーク40の中央部には非接触式ICカードリーダーを埋設しないようにすることもできる。その中央部に非接触式ICカードリーダー13を埋設する場合、その非接触式ICカードリーダー13(番号3)と登録ID番号との登録対応関係をつくらないこともできる。更に、読取りエリアマーク40の中央部に非接触式カードリーダー13を埋設する場合、その非接触式ICカードリーダー13と対応関係にある登録ID番号を他の非接触式ICカードリーダー、例えば、非接触式カードリーダー11とも対応付けておくこともできる。この場合、その登録ID番号と同一のID番号が非接触式ICカードリーダー13にて読み取られ、更に、非接触式カードリーダー11にて読み取られたときに、正規の認証がなされるようにすることができる。

20

【0052】

前述したような通常の者が読取りエリアマーク40の中央部に非接触式ICカードをかざすようになることに起因した工夫により、更に、セキュリティの向上を図ることができる。

30

【0053】

なお、前述した処理(図4参照)において、非接触式ICカードリーダーから取得したID番号と同じ登録ID番号がないとの判定がなされた場合(S3でNO)、制御部16は、非接触式ICカード20の非接触式ICカードリーダーに対する読取り操作を行った者の正規の者としての認証を行うことなく、警告メッセージの出力等、解錠拒否に係る所定の処理を行う(NG)。このような処理により、登録ID番号と異なるID番号が記録された非接触式ICカードや、ID番号が正常に読み取れない状態の非接触式ICカードについては、非接触式ICカードリーダーにて読み取られたID番号とその非接触式ICカードリーダーとの対応関係を判定するまでもなく、解錠拒否に係る所定の処理がなされる。従って、処理の簡略化が図られる。

40

【0054】

次に、本発明の第二の実施の形態に係るセキュリティシステムは、図5に示すように構成される。この第二の実施の形態に係るセキュリティシステムは、照度を考慮して認証及び電気錠30の解錠制御を行う点で前記第一の実施の形態に係るセキュリティシステムと相違する。

【0055】

図5において、このセキュリティシステムは、前記第一の実施の形態と同様に、認証システム10と電気錠30とを有している。また、認証システム10は、前記第一の実施の形態と同様に、図2に示すように壁内に埋設された複数(5台)の非接触式ICカードリーダー11、12、13、14、15、制御部16、データ蓄積部17及び操作部18を有し

50

ている。この認証システム 10 は、更に、前記非接触式 IC カード 11 ~ 15 の埋設された壁周辺の照度（明るさ）を測定する照度計 19 を有する。

【0056】

また、データ蓄積部 17 は、図 6 に示すような登録対応関係テーブルを格納する。この登録対応関係テーブルには、登録 ID 番号と非接触式 IC カードリーダ番号との対応関係となる登録対応関係が照度範囲に応じて複数種類設定されている。即ち、20 ルックス（Lx）未満の照度範囲、20 ルックス以上 40 ルックス未満の照度範囲、40 ルックス以上 60 ルックス未満の照度範囲、60 ルックス以上 80 ルックス未満の照度範囲、及び 80 ルックス以上の照度範囲のそれぞれに対して異なる種類の登録対応関係（各登録 ID 番号と非接触式 IC カードリーダ番号との対応関係）が設定されている。

10

【0057】

制御部 16 は、図 7 に示す手順に従って処理を行う。

【0058】

図 7 において、制御部 16 は、複数の非接触式 IC カードリーダ 11 ~ 15 のいずれかによって非接触式 IC カード 20 から読み取られる ID 番号の入力待ち状態にある（S11）。電気錠 30 の解錠を望む者が、非接触式 IC カード 20 を読取りエリアマーク 40（図 2 参照）を目安として非接触式 IC カードリーダ 11 ~ 15 のいずれかの埋め込み部位にかざすと、その非接触式 IC カード 20 がかざされた部位に埋め込まれた非接触式 IC カードリーダが非接触式 IC カードと無線通信を行ってその非接触式 IC カード 20 から ID 番号を読み取る。

20

【0059】

前述したように ID 番号の入力待ち状態にある制御部 16 は、前記 ID 番号を読み取った非接触式 IC カードリーダからその ID 番号を取得すると、照度計 19 に照度測定の実行を行い（S12）、その測定照度を入力待ち状態となる（S13）。制御部 16 から照度測定の実行を受けた照度計 19 は、照度の測定を行い、その測定照度値を制御部 16 に送る。測定照度を入力待ち状態となる制御部 16 は、照度計 19 から測定照度値を入力すると（S13 で YES）、データ蓄積部 17 に格納された前記登録対象テーブル（図 6 参照）を参照して前記取得した ID 番号の検索処理を行い（S14）、登録対応テーブル内にその取得した ID 番号と同じ登録 ID 番号が有るか否かを判定する（S15）。

【0060】

前記取得した ID 番号と同じ登録 ID 番号が登録対応関係テーブルに有るとの判定がなされると（S15 で YES）、制御部 16 は、更に、照度計 19 から入力された測定照度値と前記取得した ID 番号と同じ登録 ID 番号とに基づいて、前記測定照度値を含む照度範囲に対して設定された種類の登録対応関係にて決まる前記登録 ID 番号に対応した非接触式 IC カードリーダ番号を検索する（S16）。そして、制御部 16 は、その検索の結果得られた非接触式 IC カードリーダ番号と前記 ID 番号を読み取った非接触式 IC カードリーダに付与されている番号とを比較し（S17）、それらの番号が一致するか否かを判定する（S18）。

30

【0061】

それらの番号が一致すると判定がなされると（S18 で YES）、取得した ID 番号とその ID 番号を読み取った非接触式 IC カードリーダとの対応関係が前記測定照度値を含む照度範囲に対して設定された種類の登録対応関係に合致することから、制御部 16 は、非接触式 IC カード 20 の非接触式 IC カードリーダに対する読取り操作を行った者を正規の者として認証し、電気錠 30 に対して解錠制御信号を供給する（S19）。その解錠制御信号により、施錠された電気錠 30 は解錠される。

40

【0062】

一方、前記番号が一致しないと判定がなされると（S18 で NO）、取得した ID 番号とその ID 番号を読み取った非接触式 IC カードリーダとの対応関係が前記測定照度値を含む照度範囲に対して設定された種類のいずれの登録対応関係にも合致せず、制御部 16 は、警告メッセージの出力等、解錠拒否の所定の処理を行う（NG）。これにより、電気

50

錠 30 の解錠はなされない。

【 0 0 6 3 】

各照度範囲において設定された種類の登録対応関係にて決められる自己の非接触式 IC カード 20 に記録された ID 番号（登録 ID 番号）に対応する非接触式 IC カードリーダ（番号）を知っている、即ち、その埋設部位を知っている非接触式 IC カード 20 の正規の所持者は、現在の明るさ（照度）を判断して、その明るさにおける前記登録対応関係により正規の非接触式 IC カードリーダとして決められた非接触式 IC カードリーダの埋設部位に非接触式 IC カード 20 をかざすことできる。このような操作に対する認証システム 10 での前述したような処理により、非接触式 IC カード 20 の正規の所持者は、正規の者としての認証を受けて施錠された電気錠 30 の解錠を行うことができる。

10

【 0 0 6 4 】

一方、非接触式 IC カード 20 の不正所持者は、各照度範囲において設定された種類の登録対応関係にて決められるその非接触式 IC カード 20 に記録された ID 番号（登録 ID 番号）に対応する非接触式 IC カードリーダ（番号）を知りえない。従って、非接触式 IC カード 20 の不正所持者が、その非接触式 IC カードを讀取りエリアマーク 40 内の任意の位置にその非接触式 IC カードをかざしても、ID 番号を讀み取った非接触式 IC カードリーダとその ID 番号との対応関係は、その時点での照度（明るさ）に対して設定された種類の登録対応関係に合致せず、電気錠 30 の解錠を行うことはできない。

【 0 0 6 5 】

また、不正者が、非接触式 IC カード 20 の正規の所持者が行う操作を盗み見してその非接触式 IC カード 20 のかざす部位を知った後に、その非接触式 IC カード 20 を不正に入手することが考えられる。このような場合、その不正者が入手した非接触式 IC カード 20 を用いて実際に電気錠 30 の解錠を行おうとした際の照度（明るさ）と前記盗み見した際の照度が異なっていれば、それぞれにおいて適用される登録対応関係が異なる。従って、その不正者が盗み見して知った部位に非接触式 IC カード 20 をかざしたとしても、その部位に埋設された非接触式 IC カードリーダとそれより讀み出された ID 番号との対応関係は、その際の照度に適用される登録対応関係に合致せず、電気錠 30 は解錠されることはない。

20

【 0 0 6 6 】

前述したように、照度条件の内容（照度範囲）に従って認証の際に適用される登録対応関係（登録 ID 番号と非接触式 IC カードリーダとの対応関係）を変えることにより、セキュリティ性を更に向上させることができる。

30

【 0 0 6 7 】

なお、前記第二の実施の形態では、複数の非接触式 IC カードリーダ 11 ~ 15 の埋設された壁周辺の照度条件の内容に従って認証の際に適用される登録対応関係を変えるようにしたが、他の環境的条件、例えば、気温条件、湿度条件、気圧条件の内容に応じて前記登録対応関係を変えることもできる。その場合、適用される環境的条件の内容を判定するために必要な測定器（温度計、湿度計、気圧計）が用いられる。

【 0 0 6 8 】

また、前述したような環境条件以外にも、時間的条件や他の条件の内容に応じて認証の際に適用される登録対応関係を変えることもできる。時間的条件の内容に応じて認証の際に適用される登録対応関係を変える場合、時間帯ごとに（例えば、3 時間毎に、午前の時間帯と午後の時間帯で、就業時間帯とそれ以外の時間帯で）異なる種類の登録対応関係（登録 ID 番号と非接触式 IC カードリーダ番号との対応関係）を前記登録対応関係テーブルに設定すればよい。そして、認証システム 10 は照度計 19 に代えてその時間帯を判定するための時計を備えればよい。

40

【 0 0 6 9 】

前記他の条件として、セキュリティシステム（認証システム 10）を利用する者達の間でルールとして定められた条件を用いることができる。この場合、その条件の内容をその者達が認識できかつ認証システム 10 が判定できるものであれば、特に限定されない。例え

50

ば、複数の非接触式ＩＣカードリーダー１１～１５の近傍に設けられた表示器に表示させるマークや数字、複数の非接触式ＩＣカードリーダー１１～１５の近傍に設けられた所定機器の動作状態等をその条件として用いることができる。表示器に表示させるマークや数字をその条件として用いる場合、表示されるマークの形、色や数字に応じて異なる種類の登録対応関係を前記登録対応関係テーブルに設定すればよい。また、所定機器の動作状態をその条件として用いる場合、所定機器の高速運転、中速運転、低速運転等に応じて異なる種類の登録対応関係を前記登録対応テーブルに設定すればよい。

#### 【００７０】

また、なお、前述したような環境的条件の内容や時間的条件の内容に応じて登録対応関係を変えるようにしたシステムでは、現在の環境的条件や時間的条件の内容を表示する表示器を複数の非接触式ＩＣカードリーダー１１～１５を設置した近傍に配置させることもできる。これにより、非接触式ＩＣカード２０の正規の所持者は、非接触式ＩＣカードリーダーに対する非接触式ＩＣカード２０の読取り操作を行う際の環境的条件や時間的条件の内容を正確に認識することができるようになる。従って、非接触式ＩＣカード２０の正規の所持者による誤操作を防止することができる。

10

#### 【００７１】

更に、前述した第一及び第二の実施の形態は、非接触式ＩＣカードと非接触式ＩＣカードリーダーを用いたシステムであったが、これに限定されず、磁気カードと磁気カードリーダーを用いたシステムであっても、接触式ＩＣカードと接触式ＩＣカードリーダーを用いたシステムであっても、また、物体とその物体に記述されたＩＤ情報（バーコード表示などされた）を読み取る光学式の読取り装置を用いたシステムであっても、更に、半導体メモリユニットとその半導体メモリユニットが接続可能となる読取り装置を用いたシステムであっても、本発明の適用は可能である。

20

#### 【００７２】

##### 【発明の効果】

以上、説明したように、本願発明によれば、予め定めた登録ＩＤ情報と読取り装置との対応関係（登録対応関係）にて決まる記録媒体に記録されたＩＤ情報に対応した読取り装置を知っている者は、その読取り装置に対して記録媒体の読取り操作を行うことにより正規の者として認証される一方、前記登録対応関係にて決まる記録媒体に記録されたＩＤ情報に対応した読取り装置を知らないカードの不正所持者は、そのような読取り装置に対して確実に記録媒体の読取り操作を行うことができないので、正規の者として確実に認証されることはない。従って、簡単な操作で個人認証ができると共に記録媒体を不正に入手した者を正規の者と認証することを防止できるようにした個人認証システム及び方法を提供することができる。

30

#### 【００７３】

また、本願発明によれば、前記個人認証システムが適用されるセキュリティシステムを提供することができる。

#### 【００７４】

更に、本願発明によれば、前記個人認証システムに適用することのできるＩＤ情報読取りシステムを提供することができる。

40

#### 【図面の簡単な説明】

【図１】本発明の第一の実施の形態に係るセキュリティシステムの構成を示すブロック図

【図２】非接触式ＩＣカードリーダーの埋設位置の一例を示す図

【図３】登録対応関係テーブルの一例を示す図

【図４】図１に示すシステムにおける制御部の処理手順の一例を示すフローチャート

【図５】本発明の第二の実施の形態に係るセキュリティシステムの構成を示すブロック図

【図６】登録対応テーブルの他の例を示す図

【図７】図５に示すシステムにおける制御部の処理手順の一例を示すフローチャート

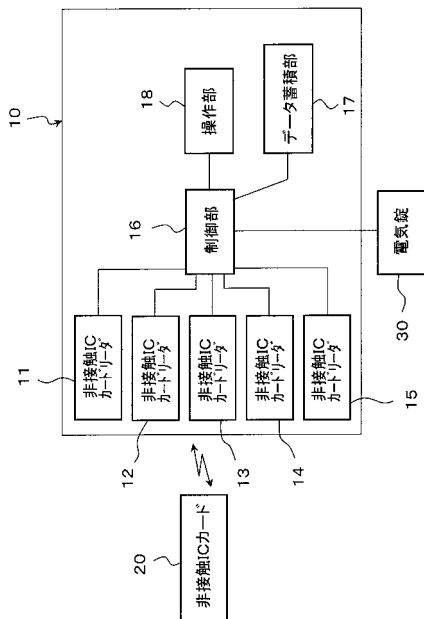
#### 【符号の説明】

１０ 認証システム

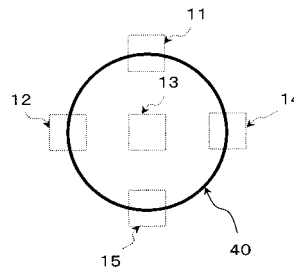
50

- 1 1、1 2、1 3、1 4、1 5 非接触式 I C カードリーダ
- 1 6 制御部
- 1 7 データ蓄積部
- 1 8 操作部
- 1 9 照度計
- 2 0 非接触式 I C カード
- 3 0 電気錠

【 図 1 】



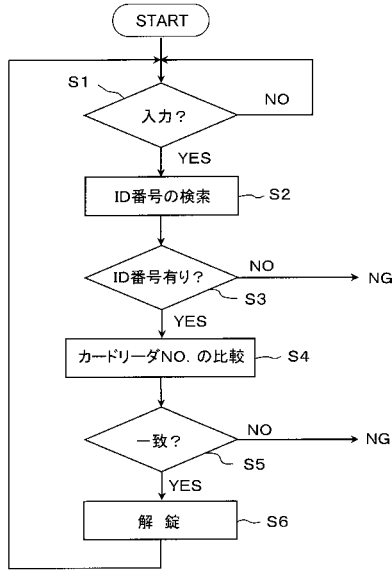
【 図 2 】



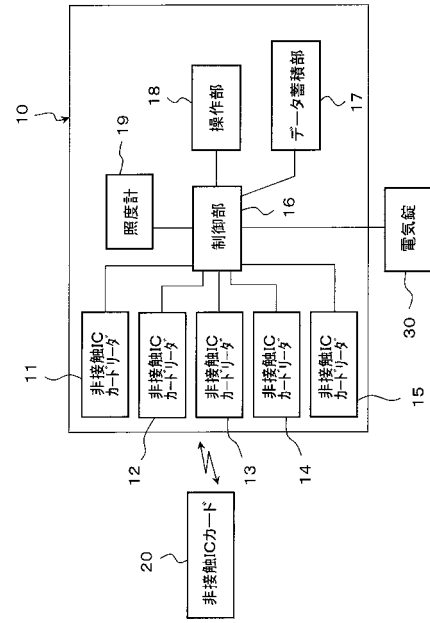
【 図 3 】

ID番号	非接触ICカードリーダ番号
10394593	5
32048940	2
40595951	5
44292406	3
53293439	1
54959404	2
56059590	1
78087722	4
⋮	⋮

【 図 4 】



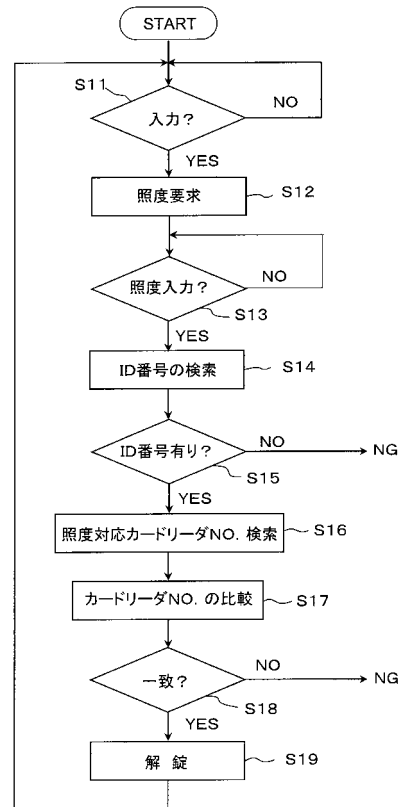
【 図 5 】



【 図 6 】

ID番号	非接触ICカードリーダー番号				
	Lx<20	20≤Lx<40	40≤Lx<60	60≤Lx<80	80≤Lx
10394593	4	5	2	3	1
32048940	5	2	1	4	3
40595951	1	5	2	4	3
44292406	4	5	3	2	1
53293439	3	2	4	1	5
⋮	⋮	⋮	⋮	⋮	⋮

【 図 7 】



## フロントページの続き

(51) Int.Cl.<sup>7</sup>

F I

テーマコード(参考)

G 0 6 K 17/00

F

G 0 6 K 17/00

T

F ターム(参考) 2E250 AA04 AA12 BB08 BB25 CC13 DD06 FF28 FF35 FF36 FF37  
5B058 CA17 CA27 KA02 KA13 KA31 KA33 YA11 YA13  
5B085 AE04 AE12 AE15 AE23 BE01 BE04