

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005年2月3日 (03.02.2005)

PCT

(10) 国際公開番号
WO 2005/010806 A1

(51) 国際特許分類7: G06K 17/00, G06F 15/00, E05B 49/00

(21) 国際出願番号: PCT/JP2004/008682

(22) 国際出願日: 2004年6月15日 (15.06.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-279637 2003年7月25日 (25.07.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 沖電気工業株式会社 (OKI ELECTRIC INDUSTRY CO., LTD.) [JP/JP]; 〒105-0001 東京都港区虎ノ門1丁目7番12号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 井戸田 誠一

(ITODA, Seiichi) [JP/JP]; 〒105-0001 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内 Tokyo (JP).

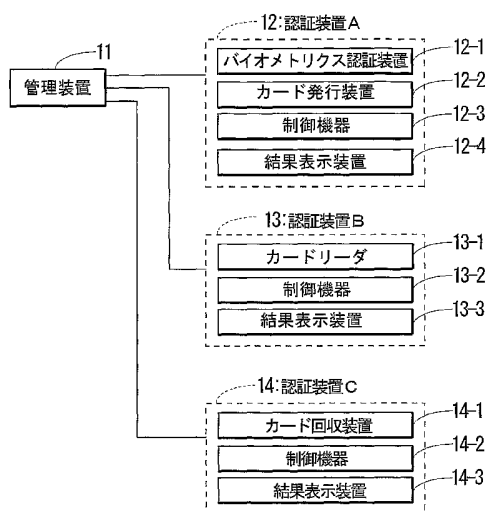
(74) 代理人: 佐藤 幸男 (SATO, Yukio); 〒160-0023 東京都新宿区西新宿7丁目18番5号 中央第7西新宿ビル404 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: COMPOSITE AUTHENTICATION METHOD AND SYSTEM USING BIOLOGICAL AUTHENTICATION IN COMBINATION

(54) 発明の名称: 生体認証併用複合認証方法及びシステム



- 11...MANAGEMENT DEVICE
- 12...AUTHENTICATION DEVICE A
- 12-1...BIOMETRICS AUTHENTICATION DEVICE
- 12-2...CARD ISSUING DEVICE
- 12-3...CONTROL DEVICE
- 12-4...RESULT DISPLAY DEVICE
- 13...AUTHENTICATION DEVICE B
- 13-1...CARD READER
- 13-2...CONTROL DEVICE
- 13-3...RESULT DISPLAY DEVICE
- 14...AUTHENTICATION DEVICE C
- 14-1...CARD COLLECTION DEVICE
- 14-2...CONTROL DEVICE
- 14-3...RESULT DISPLAY DEVICE

(57) Abstract: It is possible extract advantages of biological authentication and normal authentication. A composite authentication system using biological authentication in combination includes at least a first authentication device (A12), a second authentication device (B13), and a management device (11) for managing them. The first authentication device (A12) includes a biometrics authentication device (12-1) for performing biological authentication by using a physical feature of a device user to be authenticated and a card issuing device (12-2) for issuing a card as an authentication medium when the result of the biological authentication is affirmative. The second authentication device (B13) includes a card reader (13-1) for reading the card for authenticating the user by using the card and a control device (13-2) for allowing use of the device according to the result of authentication by the card. These devices are used according to the characteristic of the authentication of the respective methods. It should be noted that the card may be collected by a card collection device (14-1) arranged in an authentication device (C14).

(57) 要約: 生体認証と通常の認証との双方の利点を引き出す。生体認証併用複合認証システムは、少なくとも、第1の認証装置A12と、第2の認証装置B13とを備え、これらを管理する管理装置11を備える。第1の認証装置A12は、認証対象である機器使用者の身体上の特徴を用いて生体認証するバイオメトリクス認証装置12-1と、当該生体認証の結果が肯定的であるときに、認証媒体であるカードを発行するカード発行装置12-2を含む。第2の認証装置B13は、前記カードを用いて使用者を認証するために当該カードを読み取るカードリーダー13-1と、当該カードによる認証の結果に応じて機器の使用を許可する制御機器13-2を含む。これらの装置を各方式の認証の特性に応じて使い分ける。なお、カードは、認証装置C14に設けられたカード回収装置14-1で回収するようにしても良い。



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

規則4.17に規定する申立て:

— USのための発明者である旨の申立て (規則4.17(iv))

明 細 書

生体認証併用複合認証方法及びシステム

5 技術分野

本発明は、IC カードや磁気カード等の所有物による個人認証やパスワードによる認証と、バイオメトリクス認証を複合した認証方法及びシステムに関するものである。

10 背景技術

個人認証の方式として従来以下のものがある。

(1) 1 つは、所有物による個人認証方式である。これは、IC カードや磁気カードを個人が所有し、そのカードにあらかじめ個人の ID や情報を格納しておくことにより個人認証する方式である。

15 (2) もう 1 つは、バイオメトリクスを利用した個人認証方式である。これは、指紋や虹彩等の個人の身体的特徴を用いる認証方式である。

第 2 3 図において、上述の各認証方式の特徴を比較して示す。図示のように「所有物による個人認証」と「バイオメトリクス個人認証」とは対称的な特徴を示す。

すなわち、「所有物による個人認証」は低費用で認識でき、認証時間が高速である
20 るメリットがある。その反面、悪用される危険性があるとともに、所有物を携帯

していないときは認証できないなどのデメリットを有している。

一方、「バイオメトリクス認証」は悪用される危険性が低く、個人の身体特徴のため確実に認証可能であるメリットをもつ。その反面、認証装置が高価となり、認証時間に比較的長時間を要するデメリットを有する。

5

発明の開示

そこで、本発明は以上の点を解決するため、「所有物による個人認証」と「バイオメトリクス個人認証」を複合することでそれぞれのメリット、デメリットを補うシステムを構成する。

10 すなわち、次の構成を採用する。

〈構成 1〉

1 つは、生体認証併用複合認証方法であり、認証対象の身体上の特徴を用いて生体認証し、当該生体認証の結果が肯定的であるときに、その後、当該肯定的な生体認証の結果を前提とした簡易かつ迅速な認証を行える認証媒体を発行する過程と、前記認証媒体を用いて認証対象を認証し、当該認証媒体による認証の結果
15 に応じて機器の使用を許可する過程とから成ることを特徴とする。

これは、1 度、安全確実な生体認証を行った後は、簡易かつ迅速な認証を行うようにしたものである。

この方法は、例えば、認証対象の身体上の特徴を用いて生体認証する生体認証部と、当該生体認証の結果が肯定的であるときに、認証媒体を発行する媒体発行
20

部とから成る第 1 の認証装置と、前記認証媒体を用いて認証対象を認証する媒体認証部と、当該認証媒体による認証の結果に応じて機器の使用を許可する機器制御部から成る第 2 の認証装置を備えた生体認証併用複合認証システムにおいて使用される。

5 〈構成 2〉

もう 1 つは、構成 1 のシステムにおいて、第 1 の認証装置は機器使用者の所有物にその後の認証に必要なすべてのデータを書き込み、第 2 の認証装置は前記所有物から取得したデータのみをもとに単独で機器使用を許可するか否かを判定し得ることを特徴とする。

10 これは、第 1 の認証装置と、第 2 の認証装置とを通信回線で接続できない状況でも、構成 1 の方法を使用できるシステムである。

〈構成 3〉

さらにもう 1 つは、構成 1 の方法において、認証媒体である所有物を回収する過程で生体認証を伴うことを特徴とする。

15 あるいは、構成 1 または構成 2 のシステムにおいて、認証媒体である所有物を回収する回収部を備えた認識装置内に、当該所有物の回収時に生体認証する生体認証部を備えたことを特徴とする。

これらは、生体認証を活用して、所有物が機器使用者にとって不要となった後に、その所有物を他の者に利用させることができないような保証を作ろうとする

20 ものである。

図面の簡単な説明

第 1 図は、本発明の実施例 1 のシステム構成を示すブロック図である。

第 2 図は、第 1 図の管理装置の機能構成を示すブロック図である。

5 第 3 図は、第 1 図の認証装置 A の機能構成を示すブロック図である。

第 4 図は、第 1 図の認証装置 B の機能構成を示すブロック図である。

第 5 図は、第 1 図の認証装置 C の機能構成を示すブロック図である。

第 6 図は、認証データの一例を示す図である。

第 7 図は、登録者 D B の一例を示す図である。

10 第 8 図は、カード入力データの一例を示す図である。

第 9 図は、装置データの一例を示す図である。

第 10 図は、バイオメトリクスデータの一例を示す図である。

第 11 図は、認証装置 A での認証動作を示すフローチャートである。

第 12 図は、認証装置 B での認証動作を示すフローチャートである。

15 第 13 図は、認証装置 C での認証動作を示すフローチャートである。

第 14 図は、本発明の実施例 2 のシステム構成を示すブロック図である。

第 15 図は、第 14 図の認証装置 B の機能構成を示すブロック図である。

第 16 図は、第 14 図の認証装置 C の機能構成を示すブロック図である。

第 17 図は、実施例 2 でのカード入力データの一例を示す図である。

20 第 18 図は、実施例 2 の認証装置 B での認証動作を示すフローチャートである。

第 19 図は、実施例 2 の認証装置 C での認証動作を示すフローチャートである。

第 20 図は、本発明の実施例 3 のシステム構成を示すブロック図である。

第 21 図は、第 20 図の認証装置 C の機能構成を示すブロック図である。

第 22 図は、実施例 3 の認証装置 C での認証動作を示すフローチャートである。

5 第 23 図は、所有物による認証とバイオメトリクス認証との比較内容の説明図である。

発明を実施するための最良の形態

以下、本発明の最良の実施の形態を実施例を用いて説明する。

10 実施例 1

第 1 図は、本発明の実施例 1 のシステム構成図である。第 1 図において、管理装置 11 は本システム全体を管理し、所有物あるいはパスワードによる認証と、バイオメトリクス認証を複合した認証を行う。この管理装置 11 は、認証装置 A 12、認証装置 B 13、認証装置 C 14 とネットワークで接続されている。

15 認証装置 A 12 は、バイオメトリクス認証装置 12-1 と、カード発行装置 12-2 と、制御機器 12-3 と、結果表示装置 12-4 を備えている。

制御機器 12-3 の例として、電気錠や課金装置があげられる。なお、図示の例では、カード発行装置 12-2 とともに、制御機器 12-3 を備えるようにしたが、制御機器を備えない構成でもよい。

20 結果表示装置 12-4 は、LED や LCD を使い使用者に結果を通知する装置である。

使用者は認証装置 A 12 を使い、バイオメトリクス認証を行う。そして、カードを受け取る。この際、図示のような構成のものでは、同時に、ドアの開錠や金銭の支払いをすることができる。

5 認証装置 B 13 は、カードリーダー 13-1 と、制御機器 13-2 と、結果表示装置 13-3 を備えている。

制御機器 13-2 の例として、電気錠や課金装置があげられる。

使用者は認証装置 B 13 においてカードを使いドアの開錠や支払いをすることができる。

10 認証装置 C 14 は、カード回収装置 14-1 と、制御機器 14-2 と、結果表示装置 14-3 を備えている。

カード回収装置 14-1 は、カードリーダーの機能を備えてもよい。

制御機器 14-2 の例として、電気錠や課金装置があげられる。なお、図示の例では、制御機器 14-2 を備えたが、制御機器は備えない構成でもよい。

15 使用者はカード回収装置 14-1 にてカードを返却する。この際、図示の構成のものでは、同時に、ドアの開錠や金銭の支払いをすることができる。

第 2 図から第 5 図までは、第 1 図の各機器の機能ブロック図である。

第 2 図は、管理装置 11 の機能ブロック図である。第 2 図において、認証データ受信部 101 は、認証装置 A 12 からの認証データを受信する。

20 第 6 図に認証データの一例を示す。認証データは登録者 D B 109 の I D とリンクしているユニークな番号である「I D」、認証装置 A 12 を識別するための「装

置 I D」等の情報から構成される。

第 2 図に戻り、登録者 D B 検索部 102 は、I D をキーにして登録者 D B 109 からデータを検索する。

第 7 図に登録者 D B 109 の例を示す。登録者 D B 109 はユニークな番号である

5 「I D」、「名前」、カードを発行済みか否かを判定する「カード発行状態」、カードを使用可能な有効期限を示す「カード有効期限」、使用権限のある装置を示す「使用権限」等の情報により構成される。

第 2 図に戻り、カード発行判定部 103 は、認証データの I D で検索された登録者 D B 109 の「カード発行状態」、「使用権限」等からカード発行するか否かを判定する。カード発行判定の一例としては「カード発行状態」が未発行であり、認
10 証装置 A 12 の使用権限が「使用可」である場合カードを発行可と判定する手法があげられる。

カード発行判定結果送信部 104 は、カード発行判定の結果およびカード入力データを認証装置 A 12 に送信する。

15 第 8 図にカード入力データの一例を示す。カード入力データは登録者 D B 109 の I D とリンクしているユニークな番号である「I D」等の情報により構成される。

第 2 図に戻り、登録者 D B 更新部 105 は、登録者 D B 109 の「カードの発行状況」と「カード有効期限」等を更新する。

20 装置データ受信部 106 は、認証装置 B 13 または認証装置 C 14 から装置データを

受信する。

第9図に装置データを示す。装置データは登録者DB109のIDとリンクしているユニークな番号である「ID」、装置を識別するために装置毎に固有に与えられた「装置ID」等の情報により構成される。

- 5 第2図に戻り、装置使用判定部107は、装置データのIDから検索された登録者DB109の「カード有効期限」および「使用権限」等より、装置の使用を許可するか否かを判定する。装置使用判定の一例としてはカードの有効期限内であり、使用権限が使用可になっている場合があげられる。

装置使用判定結果送信部108は、装置使用判定部107での判定結果を認証装置
10 B13または認証装置C14に送信する。

第3図は、認証装置A12の機能ブロック図である。第3図において、バイオメ
トリクス認証部121は、第1図のバイオメトリクス認証装置12-1を用いて使用者
のバイオメトリクスデータを取得する。そして、これを、あらかじめバイオメ
トリクスDB128に登録されているバイオメトリクスデータとマッチングすること
15 により使用者を認証する。

第7図にバイオメトリクスDB128の一例を示す。バイオメトリクスDBは登
録者DB109のIDとリンクしているユニークな番号の「ID」と個人を認証す
るためのデータである「バイオメトリクスデータ」等の情報から構成されている。

第3図に示す例では、バイオメトリクスDBを認証装置A12に設けたが、管理装
置11に設けてネットワークを介して管理装置11においてバイオメトリクス認証
20

を実施してもよい。

結果表示部 122 は、バイオメトリクス認証の結果やカード発行判定結果等を結果表示装置 12-4 により使用者に通知する。

認証データ送信部 123 は、認証データを管理装置 11 へ送信する。認証データは
5 バイオメトリクス DB 128 から取得した「ID」と認証装置 A 12 の装置 ID 等からなる（第 6 図参照）。

カード発行判定結果受信部 124 は、管理装置 11 から送信されたカード発行判定結果を受信する。

カード発行部 125 は、カード入力データを書込み、カードをカード発行装置 12-2
10 から発行する。

制御部 126 は、制御機器 12-3 を制御する。たとえば制御機器 12-3 が電子錠の場合は電子錠を開錠する。なお、ここでは制御機器 12-3 を制御するものとしたが、制御機器 12-3 が備えられていない構成ではカードの発行を実施後、制御機器の制御はしない。

15 第 4 図は、認証装置 B 13 の機能ブロック図である。第 4 図において、カードデータ読取り部 131 は、第 1 図のカードリーダ 13-1 を用いてカード入力データを読み込む。

装置データ送信部 132 は、装置データを管理装置 11 へ送信する。装置データはカード入力データおよび装置 ID からなる（第 9 図）。

20 装置使用判定結果受信部 133 は、第 1 図の管理装置 11 から装置使用判定結果を

受信する。

結果表示部 134 は、装置使用判定を第 1 図の結果表示装置 13-3 に表示する。

制御部 135 は、装置使用判定が OK の場合、第 1 図の制御機器 13-2 を制御する。

たとえば、制御機器 13-2 が電子錠の場合は電子錠を開錠する。

- 5 第 5 図は、認証装置 C14 の機能ブロック図である。第 5 図において、カードデータ読取り部 141 は、カード機能を持ったカード回収装置 14-1 を用いてカード入力データを読込む。

装置データ送信部 142 は、装置データを管理装置 11 へ送信する。

装置使用判定結果受信部 143 は、管理装置 11 から装置使用判定結果を受信する。

- 10 結果表示部 144 は、装置使用判定を結果表示装置 14-4 に表示する。

カード回収部 145 は、カード回収装置 14-1 を用いてカードを回収する。

- 制御部 146 は、装置使用判定が OK の場合、制御機器 14-2 を制御する。たとえば、制御機器 14-2 が電子錠の場合は電子錠を開錠する。なお、ここではカードのデータにより制御機器を制御しているが、カード回収のみを実施し制御機器の制御は実施しない形態でもよい。また、制御機器を制御するに際しては、カードのデータにより制御機器を制御せずに、カード回収をトリガにして制御機器を制御する手法もある。
- 15

〈実施例 1 の動作〉

- 第 1 1、1 2、1 3 図における実施例 1 の動作のフローチャートに沿って、本
- 20 実施例の動作を説明する。

第 11 図は、認証装置 A12 での認証動作を示す。

まず、S101 で、バイオメトリクス認証部 121 はバイオメトリクス認証を実施する。そして、認証ができた場合は S103 の処理へ移る。認証ができない場合は S102 の処理へ移る。

5 S102 で、結果表示部 122 は使用者に認証ができなかったことを通知する。

S103 で、認証データ送信部 123 は認証データを管理装置 11 に送信する。

ここで、管理装置の動作が始まる。

まず、S104 で、認証データ受信部 101 は認証データを受信する。

そして、S105 で、登録者 DB 検索部 102 は受信した認証データの ID をもと
10 に登録者 DB109 上のデータを検索する。

S106 で、カード発行判定部 103 は検索したデータよりカード発行するか否かを判定する。

また、S107 で、登録者 DB 更新部 105 は登録者 DB109 のデータを更新する。

S108 で、カード発行判定結果送信部 104 は認証装置 A12 へ結果を送信する。

15 カード発行可の場合はカード発行可の結果とカード入力データを送信する。また、カード発行不可の場合はカード発行不可の結果を送信する。

ここで、認識装置 A の動作が再開される。

S109 で、カード発行判定結果受信部 124 はカード発行判定結果を受信する。

S110 で、結果表示部 122 はカード発行判定結果を使用者に通知する。

20 S111 で、カード発行部 125 はカード発行可の場合、S112 の処理へ移る。カー

ド発行不可の場合は終了する。

S 112 で、カード発行部 125 はカード入力データを書込んだカードを発行する。

S 113 で、制御部 126 は所定の動作を実施する。たとえば認証装置 A に電気錠が設けられているならば電気錠の開錠を実施する。

5 第 1 2 図は、認証装置 B 13 での認証動作を示す。

まず、S 121 で、カードデータ読取り部 131 は認証装置 A 12 で発行されたカードのカード入力データを読取る。

S 122 で、装置データ送信部 132 は装置データを管理装置 11 へ送信する。

ここで、管理装置の動作が始まる。

10 S 123 で、装置データ受信部 106 は装置データを受信する。

S 124 で、登録者 DB 検索部 102 は受信した認証データの ID をもとに登録者 DB 109 上のデータを検索する。

S 125 で、装置使用判定部 107 は検索したデータから認証装置 B 13 の使用許可するか否かを判定する。

15 S 126 で、装置使用判定結果送信部 108 は認証装置 B 13 へ結果を送信する。

ここで、認証装置 B の動作が再開される。

S 127 で、装置使用判定結果受信部 133 は結果を受信する。

S 128 で、結果表示部 134 は装置使用判定結果を使用者に通知する。

S 129 で、制御部 135 は装置使用可の場合は処理を S 130 へ移す。使用不可の場合
20 は処理を終了する。

S 130 で、制御部 135 は所定の動作を実施する。たとえば、認証装置 B 13 に電気錠が設けられているならば電気錠の開錠を実施する。

第 13 図は、認証装置 C 14 での認証動作を示す。

まず、S 141 で、カードデータ読取り部 141 は認証装置 A 12 で発行されたカード
5 D のカード入力データを読取る。

S 142 で、装置データ送信部 142 は装置データを管理装置 11 へ送信する。

ここで、管理装置の動作が始まる。

S 143 で、装置データ受信部 106 は装置データを受信する。

S 144 で、登録者 D B 検索部 102 は受信した認証データの I D をもとに登録者
10 D B 109 上のデータを検索する。

S 145 で、装置使用判定部 107 は検索したデータから認証装置 C 14 の使用許可
するか否かを判定する。

S 146 で、装置使用判定結果送信部 108 は認証装置 C 14 へ結果を送信する。

ここで、認証装置 C の動作が再開される。

15 S 147 で、装置使用判定結果受信部 143 は結果を受信する。

S 148 で、結果表示部 144 は装置使用判定結果を使用者に通知する。

S 149 で、カード回収部 145 は装置使用可の場合は処理を S 151 へ移す。使用不可
の場合は S 150 へ処理を移す。

S 150 で、カード回収部 145 はカードを使用者に返却する。これにより、処理
20 終了する。

S 151 で、カード回収部 145 はカードを回収する。

S 152 で、制御部 135 は所定の動作を実施する。たとえば、認証装置 C 14 に電気錠が設けられているならば電気錠の開錠を実施する。

5 なお、上述した実施例においては、カード等の所有物による認証とバイオメトリクス認証を複合させるものについて説明したが、本発明はこれに限らず、暗証すなわちパスワードによる認証とバイオメトリクス認証を複合させたものによっても同様に実現できるものである。この点、後述する実施例についても同様である。

〈実施例 1 の効果〉

10 以上詳述したように、実施例 1 のシステムによりバイオメトリクス認証と所有物による認証の両方の利便性を得ることが可能となる。すなわち、本システムによりバイオメトリクス認証による安全性および随時携帯しなくてよいという利便性を得るとともに、所有物による認証による即座に認証可能であるという利便性を得ることが可能となる。

15 例えば、会社等の施設での運用を考える。会社の門では認証装置 A 12 でバイオメトリクス認証を実施し、カードを取得する。ここでは、バイオメトリクス認証を実施するため高い安全性を確保できる。この際、カードはこの場で発行されるため、カードを携帯する必要はない。会社内ではこのカードと認証装置 B 13 を使う。このカードで食堂での支払いや、入退室管理を実施する。バイオメトリクス
20 では照合に時間がかかるケースがあるため食堂等で混雑する可能性があるが、カ

ードは即座に認証可能なため混雑することはない。このカードは最後会社から退社する際に認証装置 C 14 で回収する。従って会社の外にカードがもちだされることはないため盗難等の危険性は低い。

また、本システムをマンションの管理システムに応用した場合には、マンションの入口で本システムに登録された住民は認証装置 A 12 によりバイオメトリクス認証を受け、カードあるいはキーを取得する。ここで、バイオメトリクス認証の実施により高度のセキュリティを確保できる。この際、カードやキーはこの場で発行されるため、それらを携帯して外出する必要はない。自宅に入るときはこのカードあるいはキーと認証装置 B 13 を使う。このカードやキーは外出する際にマンションの出口に設けられた認証装置 C 14 で回収する。従ってマンションの外にこれらがもちだされることはないため盗難等の危険性は低くなる。

実施例 2

第 1 4 図は、実施例 2 のシステム構成図である。実施例 1 と異なる点は管理装置 11 と認証装置 A 12 はネットワークで接続されているが、認証装置 B 13 と認証装置 C 14 は管理装置 11 に接続されていない点である。その他の構成は実施例 1 と同様である。

第 1 5 図および第 1 6 図は、各機器の機能ブロック図である。管理装置と認証装置 A の機能ブロック図は、実施例 1 と同様である。第 1 7 図は、実施例 2 でのカード入力データの一例である。カード入力データはユニークな番号である「I D」、カードを使用可能な有効期限を示す「カード有効期限」、使用権限のある装

置を示す「使用権限」等の情報により構成される。

第 15 図は、認証装置 B 13 の機能ブロック図である。第 15 図において、カードデータ読取り部 231 は、カードリーダ 13-1 を用いてカード入力データを読込む。装置使用判定部 232 は、「カード有効期限」、「使用権限」等より装置の使用を許可
5 するか否かを判定する。装置使用判定の一例としてはカード有効期限内であり、装置毎に割り当てられている「装置 ID」の使用権限が使用可の場合、使用を許可する手法があげられる。

結果表示部 233 は、装置使用判定部 232 における結果を結果表示装置 13-3 に表示する。制御部 234 は、装置使用判定が OK の場合、制御機器 13-2 を制御する。

10 たとえば、制御機器 13-3 が電子錠の場合は電子錠を開錠する。

第 16 図は、認証装置 C 14 の機能ブロック図である。第 16 図において、カードデータ読取り部 241 は、カード機能を持ったカード回収装置 14-3 を用いてカード入力データを読込む。装置使用判定部 242 は、「カード有効期限」、「使用権限」等より装置の使用を許可するか否かを判定する。

15 結果表示部 243 は、装置使用判定を結果表示装置 14-4 に表示する。カード回収部 244 は、カード回収装置 14-1 を用いてカードを回収する。制御部 245 は、装置使用判定が OK の場合、制御機器 14-3 を制御する。たとえば、制御機器 14-3 が電子錠の場合は電子錠を開錠する。

〈実施例 2 の動作〉

20 第 18 図および第 19 図の実施例 2 の動作のフローチャートに沿って、本実施

例の動作を説明する。

実施例 1 における第 11 図の S101～S113 までの動作は実施例 2 も同じように行われるものである。ただし、カード入力データが第 17 図の内容になる。

第 18 図は、認証装置 B13 での認証動作である。

5 まず、S221 で、カードデータ読取り部 231 は認証装置 A12 で発行されたカードのカード入力データを読取る。

S222 で、装置使用判定部 232 はカード入力データから認証装置 B13 の使用許可するか否かを判定する。

そして、S223 で、結果表示部 233 は装置使用判定結果を使用者に通知する。

10 S224 で、制御部 234 は装置使用可の場合は処理を S225 へ移す。使用不可の場合は処理を終了する。

S225 で、制御部 234 は所定の動作を実施する。たとえば、認証装置 B13 に電気錠が設けられているならば電気錠の開錠を実施する。

第 19 図は、認証装置 C14 での認証動作を示す。

15 まず、S241 で、カードデータ読取り部 241 は認証装置 A12 で発行されたカードのカード入力データを読取る。

S242 で、装置使用判定部 242 はカード入力データから認証装置 C14 を使用許可するか否かを判定する。

そして、S243 で、結果表示部 243 は装置使用判定結果を使用者に通知する。

20 S244 で、カード回収部 244 は装置使用可の場合は処理を S246 へ移す。使用不

可の場合は S 245 へ処理を移す。

S 245 で、カード回収部 244 はカードを使用者に返却する。これで、処理を終了する。

S 246 で、カード回収部 244 はカードを回収する。

- 5 S 247 で、制御部 245 は所定の動作を実施する。たとえば、認証装置 C 14 に電気錠が設けられているならば電気錠の開錠を実施する。

〈実施例 2 の効果〉

- 以上詳述したように、実施例 2 によれば、実施例 1 と異なり、以下の効果がある。すなわち、実施例 1 では認証装置 B 13 と認証装置 C 14 がネットワークに接続
10 されている必要があったが、実施例 2 では、これらの装置はネットワークとは接続されていない。このため、これらの装置をネットワークにつなげることができないような環境でも、実施例 1 と同様の効果を得られる。

- 例えばコンドミニアムの運用を考える。コンドミニアムがある場所はネットワーク環境が整備されていないような場所とする。使用者は認証装置 A 11 を使い
15 カードを取得する。認証装置 A 11 はネットワーク接続可能な場所に設置されている。このカードを認証装置 B 13 が設置されているコンドミニアムで使用することでコンドミニアムの錠を開錠でき、設備の使用が可能となる。

実施例 3

- 第 20 図は実施例 3 のシステム構成図である。実施例 1 と異なる点は認証装置
20 C 14 にバイオメトリクス認証装置が備えられたことである。管理装置 11 と認証

装置 A 12 と認証装置 B 13 は実施例 1 と同様である。

認証装置 C 34 は、バイオメトリクス認証装置 34-1 と、カード回収装置 34-2 と、制御機器 34-3 と、結果表示装置 34-4 を備えている。ここでは、実施例 1 の構成に認証装置 C 34 を備えたが、実施例 2 の構成に認証装置 C 34 を備えてもよい。

5 第 2 1 図は各機器の機能ブロック図である。管理装置 11 と認証装置 A 12 と認証装置 B 13 は実施例 1 の機能ブロック図と同様である。

そこで、第 2 1 図では認証装置 C 34 の機能ブロックのみを示す。第 2 1 図において、バイオメトリクス認証部 341 は、バイオメトリクス認証装置 34-1 を用いて使用者のバイオメトリクスデータを取得し、あらかじめバイオメトリクス D B 349
10 に登録されているバイオメトリクスデータとマッチングすることにより使用者を認証する。

カードデータ読取り部 342 は、カードリーダ機能を持ったカード回収装置 34-2 を用いてカード入力データを読込む。カード所有者判定部 343 は、カード内の ID とバイオメトリクス認証で取得できた ID が一致するか否かを判定する。装置データ送信部 344 は、装置データを管理装置 11 へ送信する。装置使用判定結果受信部
15 345 は、管理装置 11 から装置使用判定結果を受信する。

結果表示部 346 は、装置使用判定を結果表示装置 34-4 に表示する。カード回収部 347 は、カード回収装置 34-2 を用いてカードを回収する。制御部 348 は、装置使用判定が O K の場合、制御機器 34-3 を制御する。たとえば、制御機器 34-3 が
20 電子錠の場合は電子錠を開錠する。ここではカードのデータにより制御機器を制

御しているが、カード回収をトリガにして制御機器を制御する手法や、カード回収のみを実施し、制御機器の制御は実施しない形態でもよい。

〈実施例 3 の動作〉

実施例 1 における第 1 1 図の S 101～S 113、第 1 2 図の S 121～S 130 までの動作は実施例 3 でも同じである。

第 2 2 図は認証装置 C 34 での認証動作を示す。

まず、S 341 で、バイオメトリクス認証部 341 はバイオメトリクス認証を実施する。認証ができた場合は S 343 の処理へ移る。認証ができない場合は S 342 の処理へ移る。

10 S 342 で、結果表示部 346 は認証結果 N G を使用者に通知する。そして、ここで処理を終了する。

一方、S 343 で、結果表示部 346 は認証結果 O K を使用者に通知する。

S 344 で、カードデータ読取り部 342 は認証装置 A 12 で発行されたカードのカード入力データを読取る。

15 S 345 で、カード所有者判定部 343 はバイオメトリクス認証で得られた ID とカード入力データの ID が一致するか否かを判定する。そして、一致する場合は S 347 の処理へ移行する。一致しない場合は S 346 の処理へ移行する。

S 346 で、結果表示部 346 は ID が一致しないことを使用者に通知する。

20 S 347 で、装置データ送信部 344 は装置データを管理装置 11 へ送信する。これにより、管理装置での処理が始められる。

S 348 で、装置データ受信部 106 は装置データを受信する。

S 349 で、登録者 DB 検索部 102 は受信した認証データの ID をもとに登録者 DB 109 上のデータを検索する。

S 350 で、装置使用判定部 107 は検索したデータから認証装置 C 34 の使用許可
5 するか否かを判定する。

S 351 で、装置使用判定結果送信部 108 は認証装置 C 34 へ結果を送信する。これにより、認証装置 C の動作が再開される。

S 352 で、装置使用判定結果受信部 345 は結果を受信する。

S 353 で、結果表示部 346 は装置使用判定結果を使用者に通知する。

10 S 354 で、カード回収部 347 は装置使用可の場合は処理を S 356 へ移す。使用不可の場合は S 355 へ処理を移す。

S 355 で、カード回収部 347 はカードを使用者に返却する。これで処理を終了する。

S 356 では、カード回収部 347 はカードを回収する。

15 S 357 で、制御部 348 は所定の動作を実施する。たとえば、認証装置 A に電気錠が設けられているならば電気錠の開錠を実施する。

〈実施例 3 の効果〉

実施例 3 によりある人がバイオメトリクス認証を実施して取得したカードを第三者が取得して不正利用することを防止することができる。

20 例としてスキー場のリフト券を考える。スキー場ではリフト券の転売問題が存

在する。ある人が購入したリフト券を第三者に転売することで同じリフト券で2名以上が使用する問題である。認証装置C34を使用することでそのリフト券が購入者のものか否かを判定できるため転売問題のような不正利用を防止できる。

具体的には、リフト券の購入時に認証装置Aでその購入者から保証金を預かり、

- 5 認証装置Cでリフト券の返還を条件としてバイオメトリクス認証で確認したその購入者にその保証金を返すようにする。

請求の範囲

1. 認証対象の身体上の特徴を用いて生体認証し、当該生体認証の結果が肯定的であるときに、その後、当該肯定的な生体認証の結果を前提とした簡易かつ

5 迅速な認証を行える認証媒体を発行する過程と、

前記認証媒体を用いて認証対象を認証し、当該認証媒体による認証の結果に応じて機器の使用を許可する過程とから成ることを特徴とする生体認証併用複合認証方法。

2. 前記認証媒体は、認証対象である機器使用者の所有物であることを特徴とする請求の範囲第1項記載の生体認証併用複合認証方法。

3. 前記認証媒体は、パスワードであることを特徴とする請求の範囲第1項記載の生体認証併用複合認証方法。

4. 前記認証媒体である所有物を回収する過程を伴うことを特徴とする請求の範囲第2項記載の生体認証併用複合認証方法。

15 5. 認証対象の身体上の特徴を用いて生体認証する生体認証部と、当該生体認証の結果が肯定的であるときに、認証媒体を発行する媒体発行部とから成る第1の認証装置と、

前記認証媒体を用いて認証対象を認証する媒体認証部と、当該認証媒体による認証の結果に応じて機器の使用を許可する機器制御部から成る第2の認証装置を

20 備えたことを特徴とする生体認証併用複合認証システム。

6. 前記認証媒体は、認証対象である機器使用者の所有物であることを特徴とする請求の範囲第5項記載の生体認証併用複合認証システム。

7. 前記認証媒体は、パスワードであることを特徴とする請求の範囲第5項記載の生体認証併用複合認証システム。

5 8. 前記認証媒体である所有物を回収する回収部を備えたことを特徴とする請求の範囲第6項記載の生体認証併用複合認証システム。

9. 前記第1の認証装置は機器使用者の所有物にその後の認証に必要なすべてのデータを書き込み、

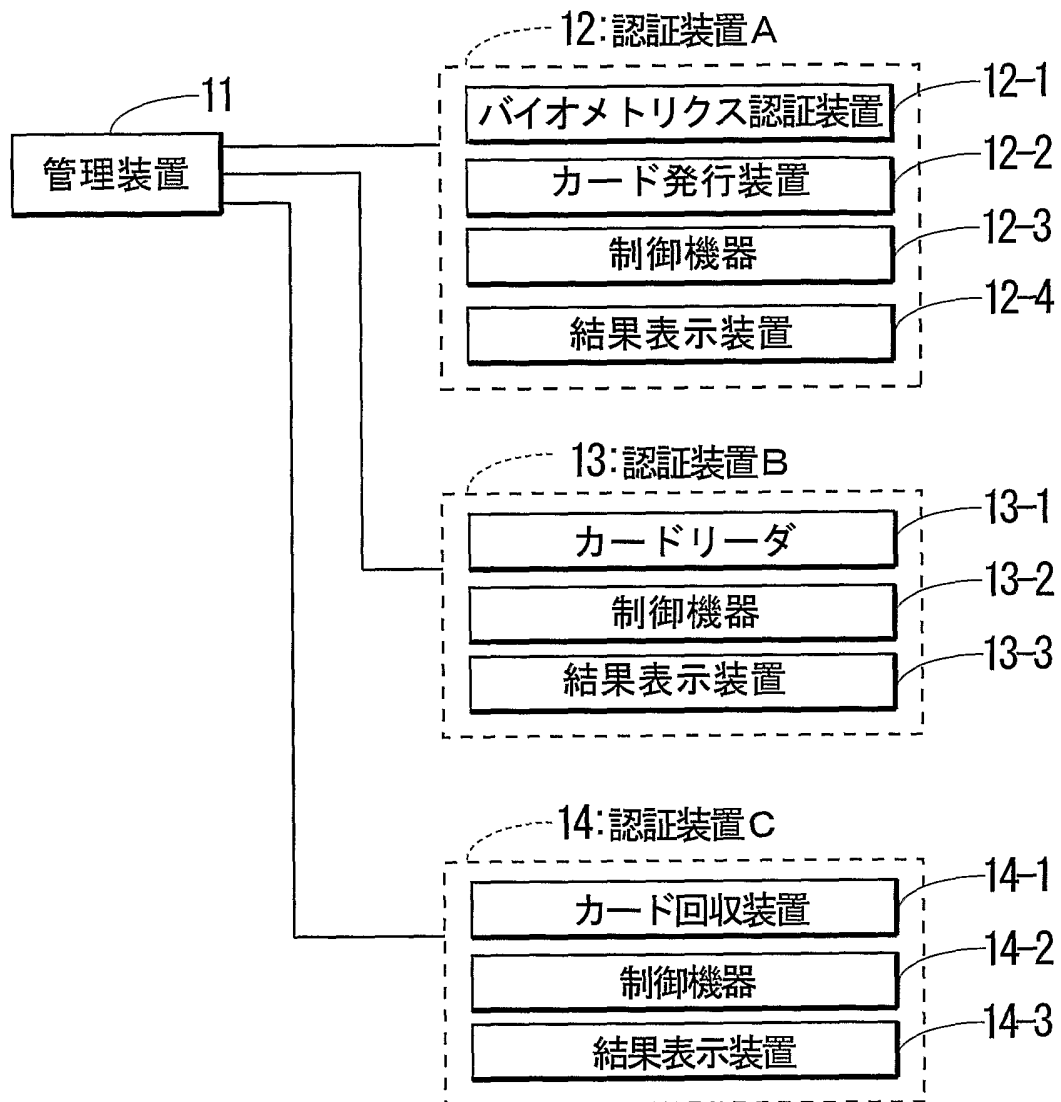
前記第2の認証装置は前記所有物から取得したデータのみをもとに単独で機器
10 使用を許可するか否かを判定し得ることを特徴とする請求の範囲第6項記載の生体認証併用複合認証システム。

10. 前記認証媒体である所有物を回収する過程において生体認証を伴うことを特徴とする請求の範囲第4項記載の生体認証併用複合認証方法。

11. 前記認証媒体である所有物を回収する回収部を備えた認識装置内に、
15 当該所有物の回収時に生体認証する生体認証部を備えたことを特徴とする請求の範囲第8項記載の生体認証併用複合認証システム。

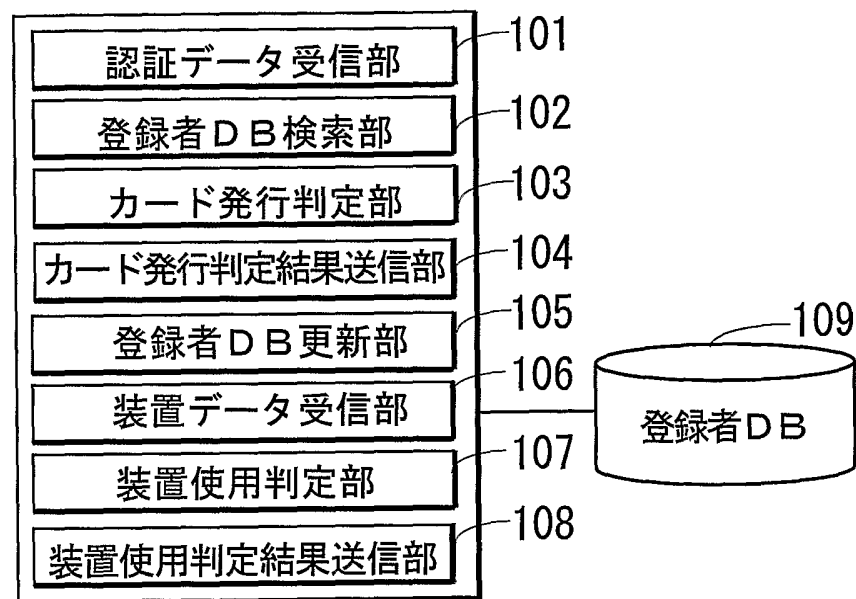
1 / 18

第1図



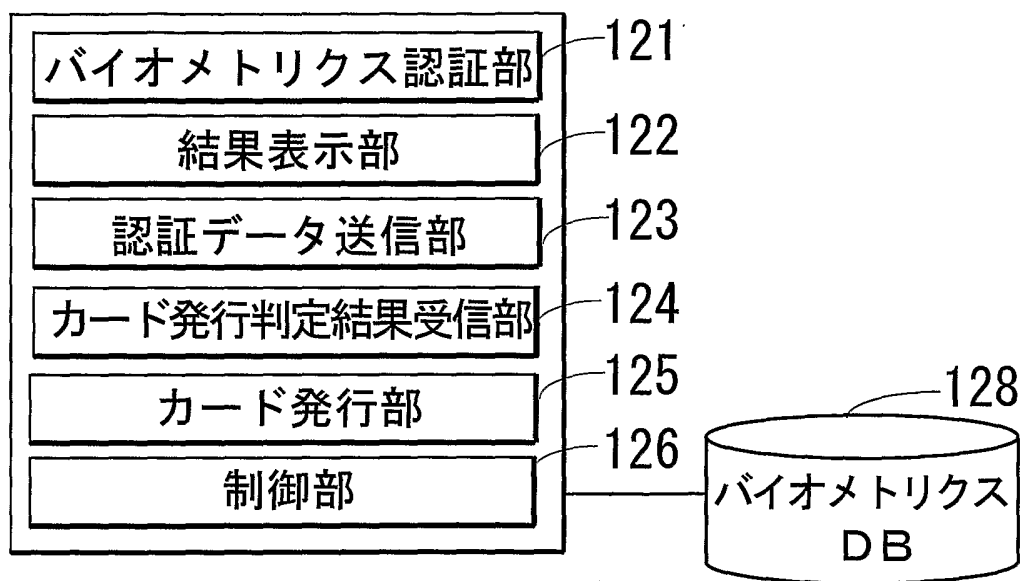
2 / 18

第2図



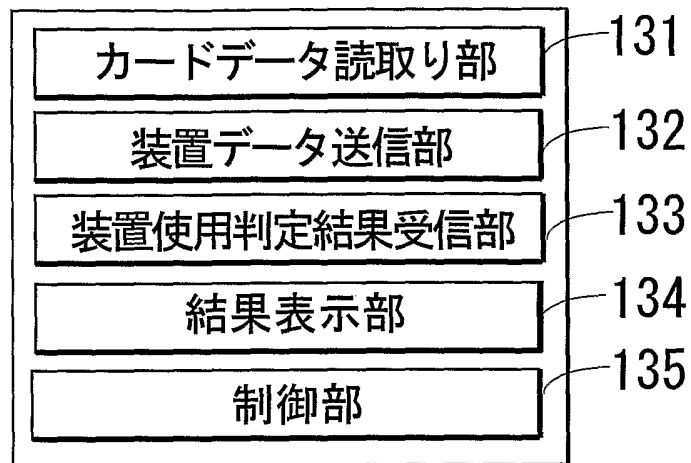
3 / 18

第3図

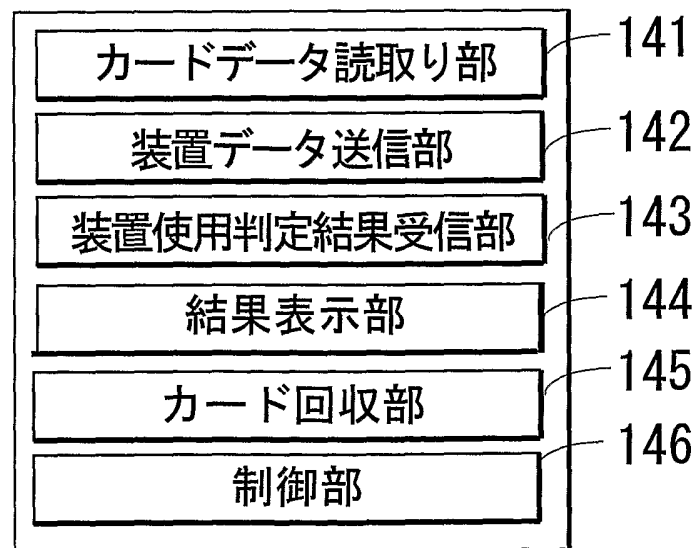


4 / 18

第4図



第5図



第6図

I D	装置 I D
X X X X X X	A A A A A A
X X X X X X	A A A A A A
.	

第8図

I D
X X X X X X
X X X X X X
.

第9図

I D	装置 I D
X X X X X X	A A A A A A
X X X X X X	A A A A A A
.	.

第10図

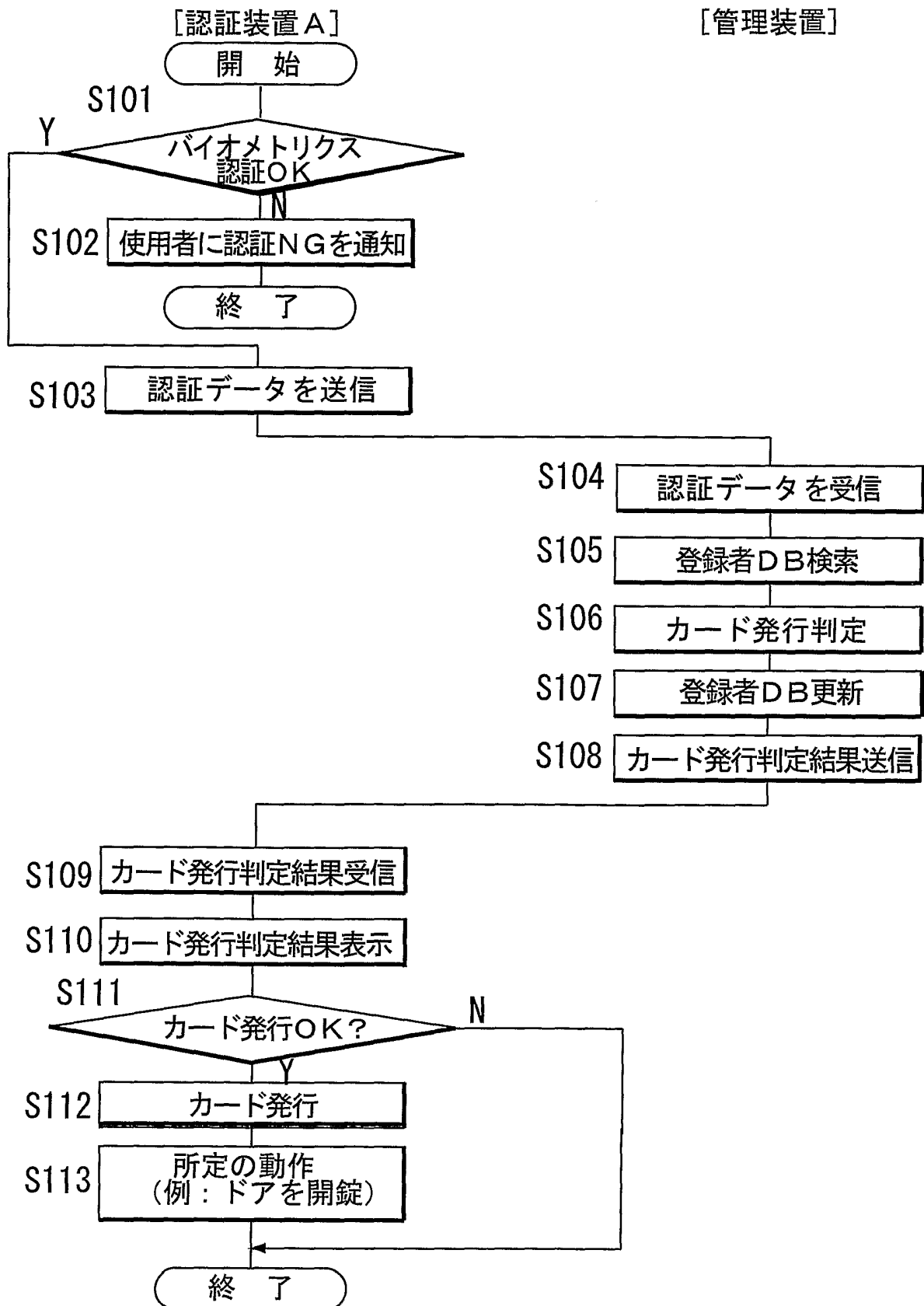
I D	バイオメトリクスデータ
X X X X X X	* * * * * * * *
X X X X X X	* * * * * * * *
.	.

第 7 図

ID	名前	カード 発行状態	カード 有効期限	使用権限		
				装置ID1	装置ID2	
XXXXXX	沖 太郎	未発行	——	使用可	使用可	・
XXXXXX	山田 次 郎	発行	hh:mm:ss	使用不可	使用可	・
・	・	・	・	・	・	・

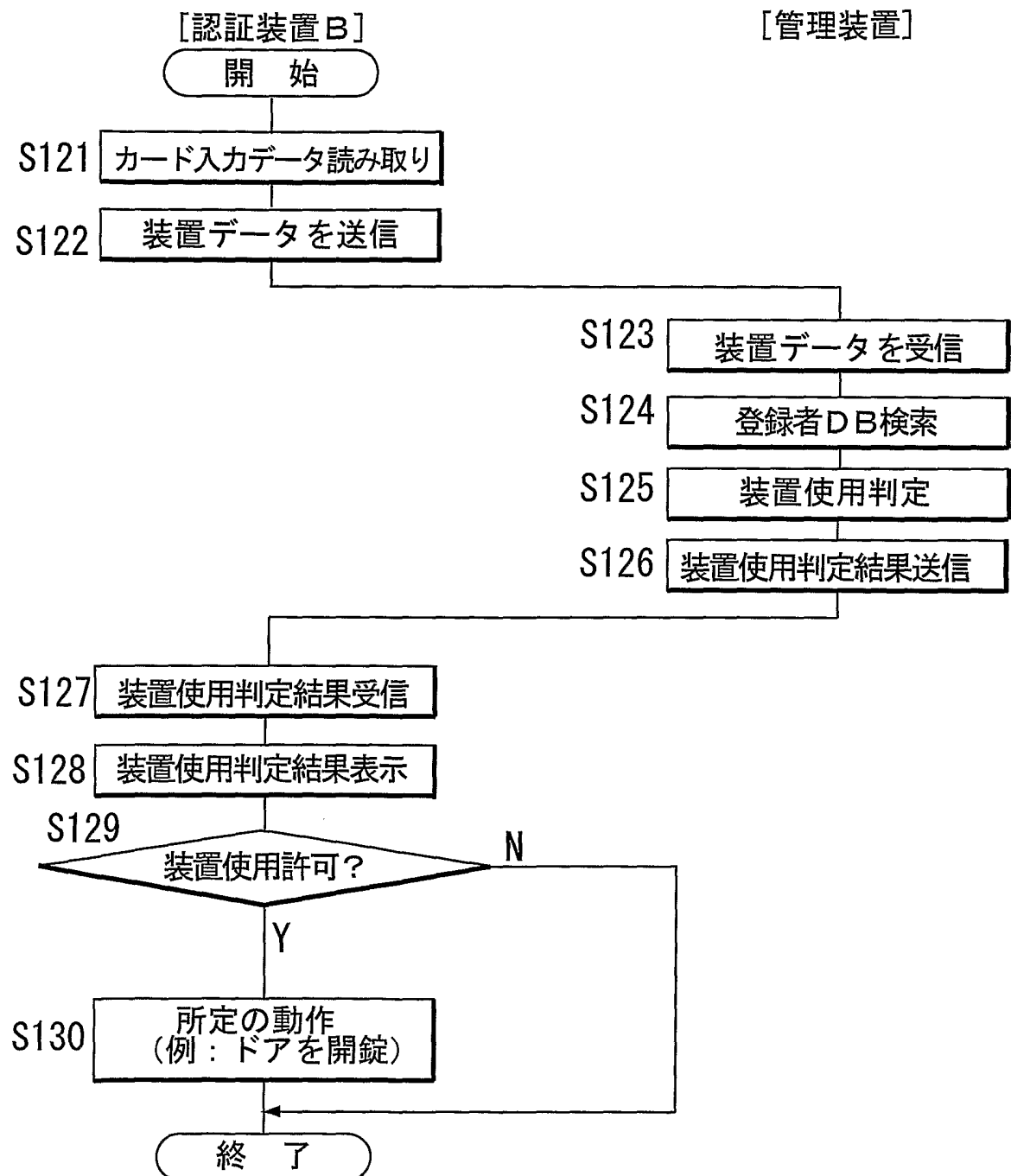
7 / 18

第 1 1 図



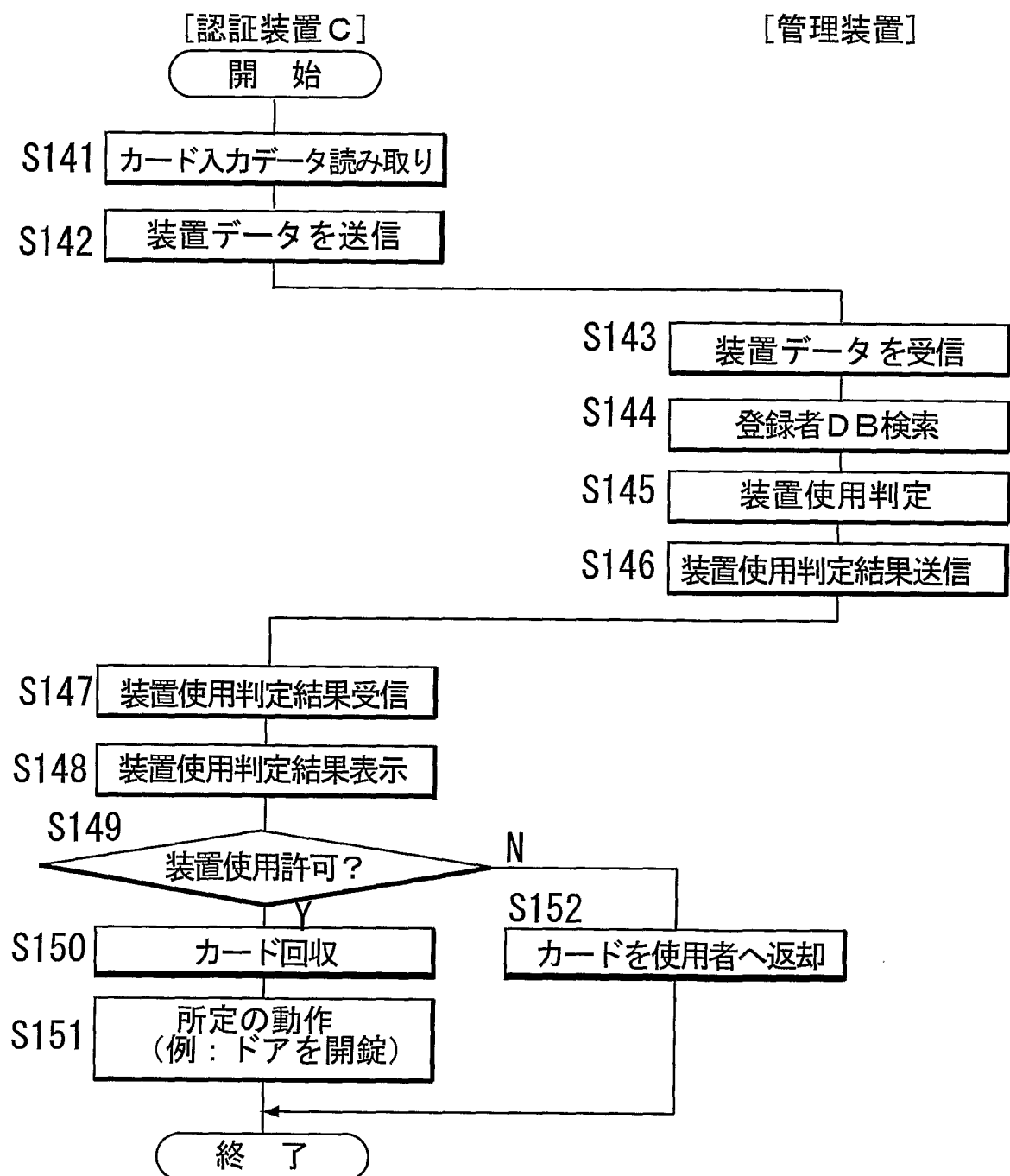
8 / 18

第 12 図



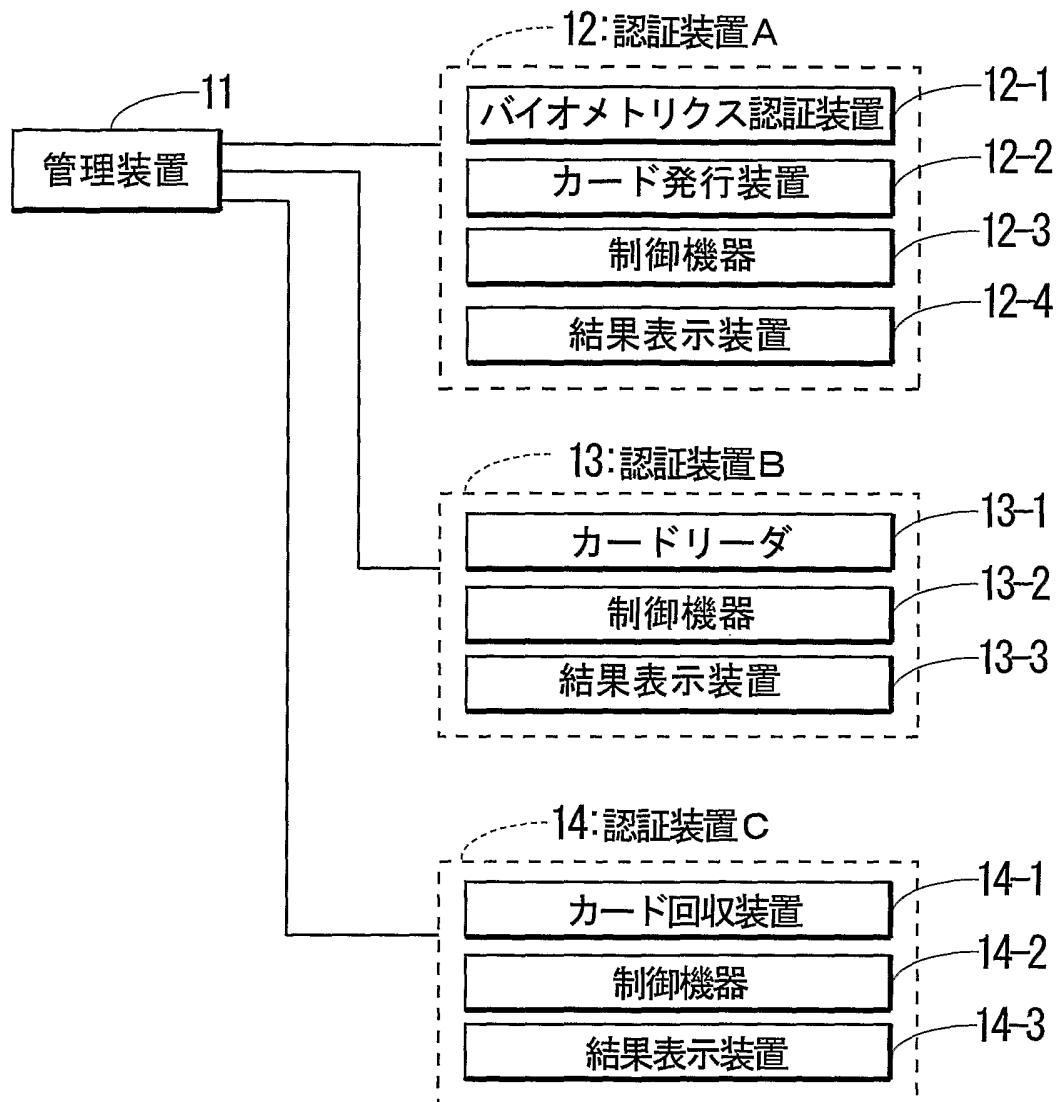
9 / 18

第 13 図



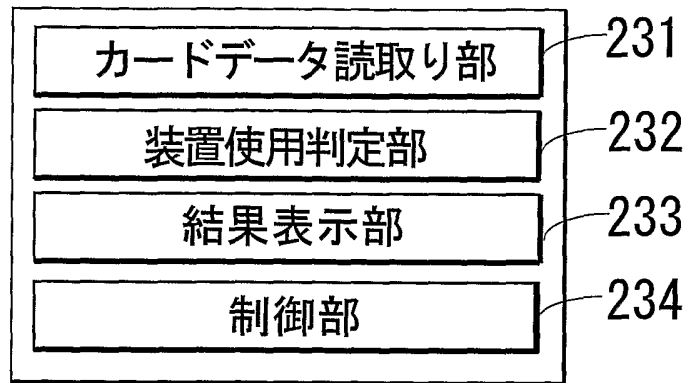
10 / 18

第14図

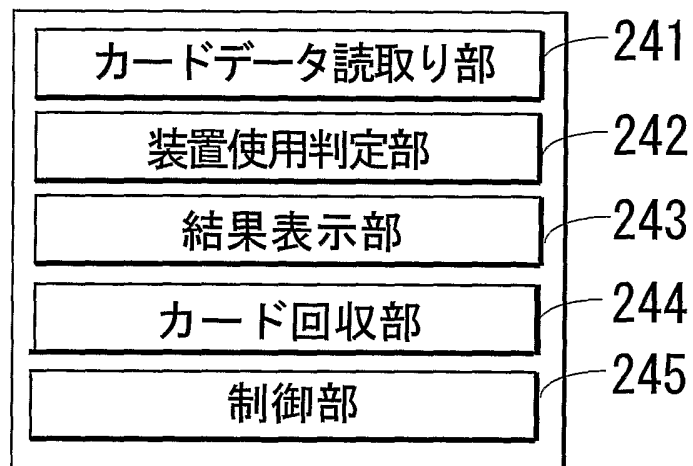


11 / 18

第15図



第16図

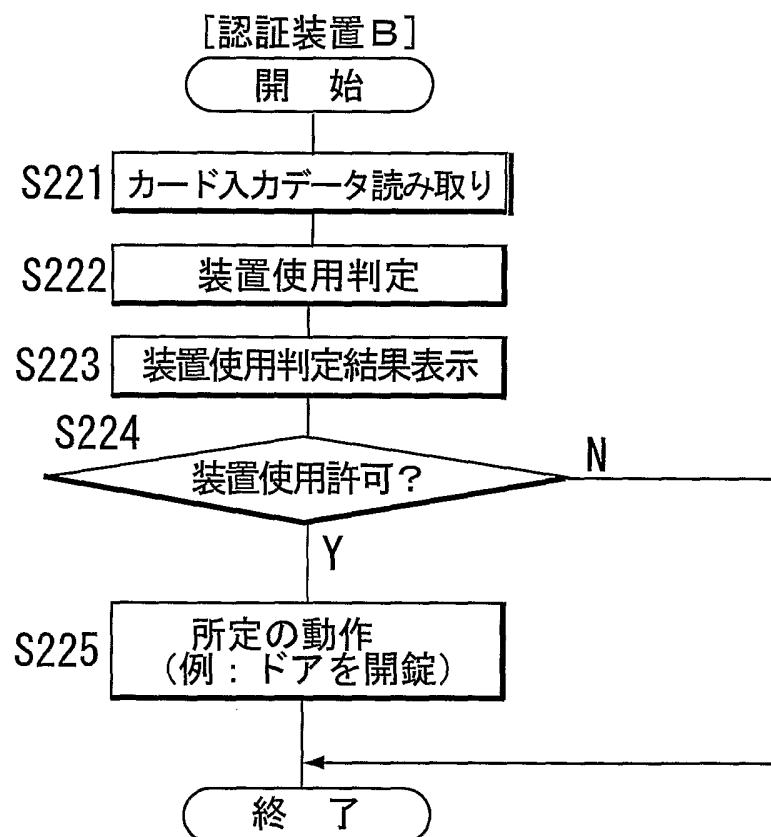


第 1 7 図

ID	カード 有効期限	使用権限		
		装置ID1	装置ID2	・
XXXXXX	————	使用可	使用可	・
XXXXXX	hh:mm:ss	使用不可	使用可	・
・	・	・	・	・

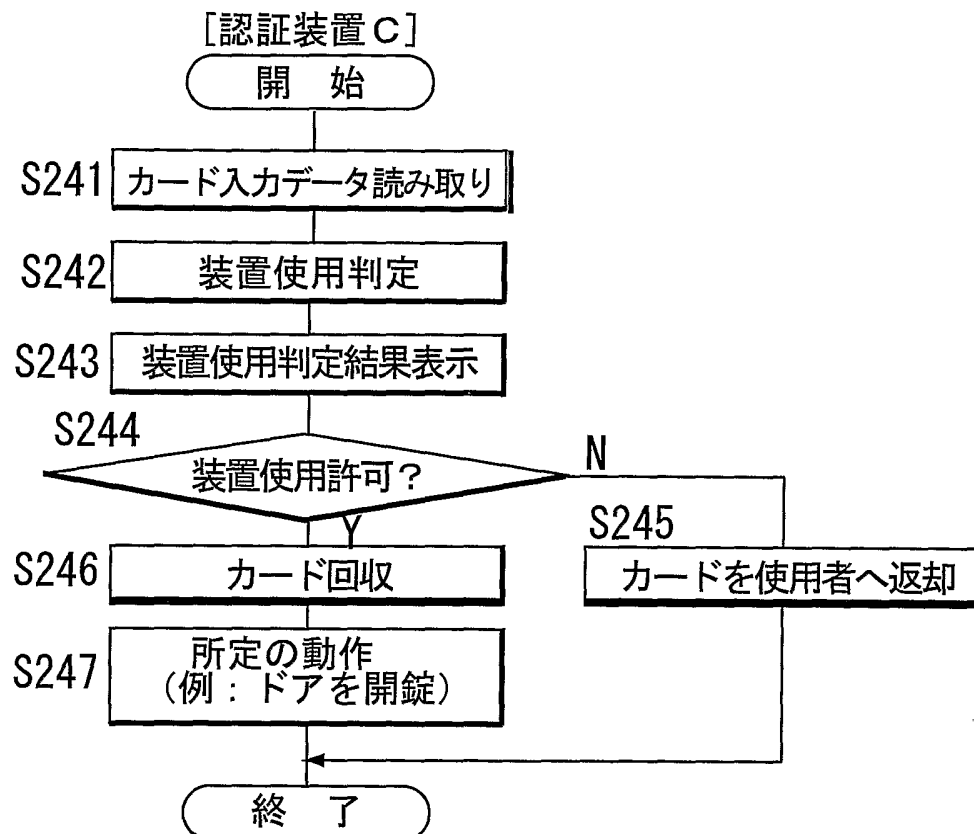
13 / 18

第18図



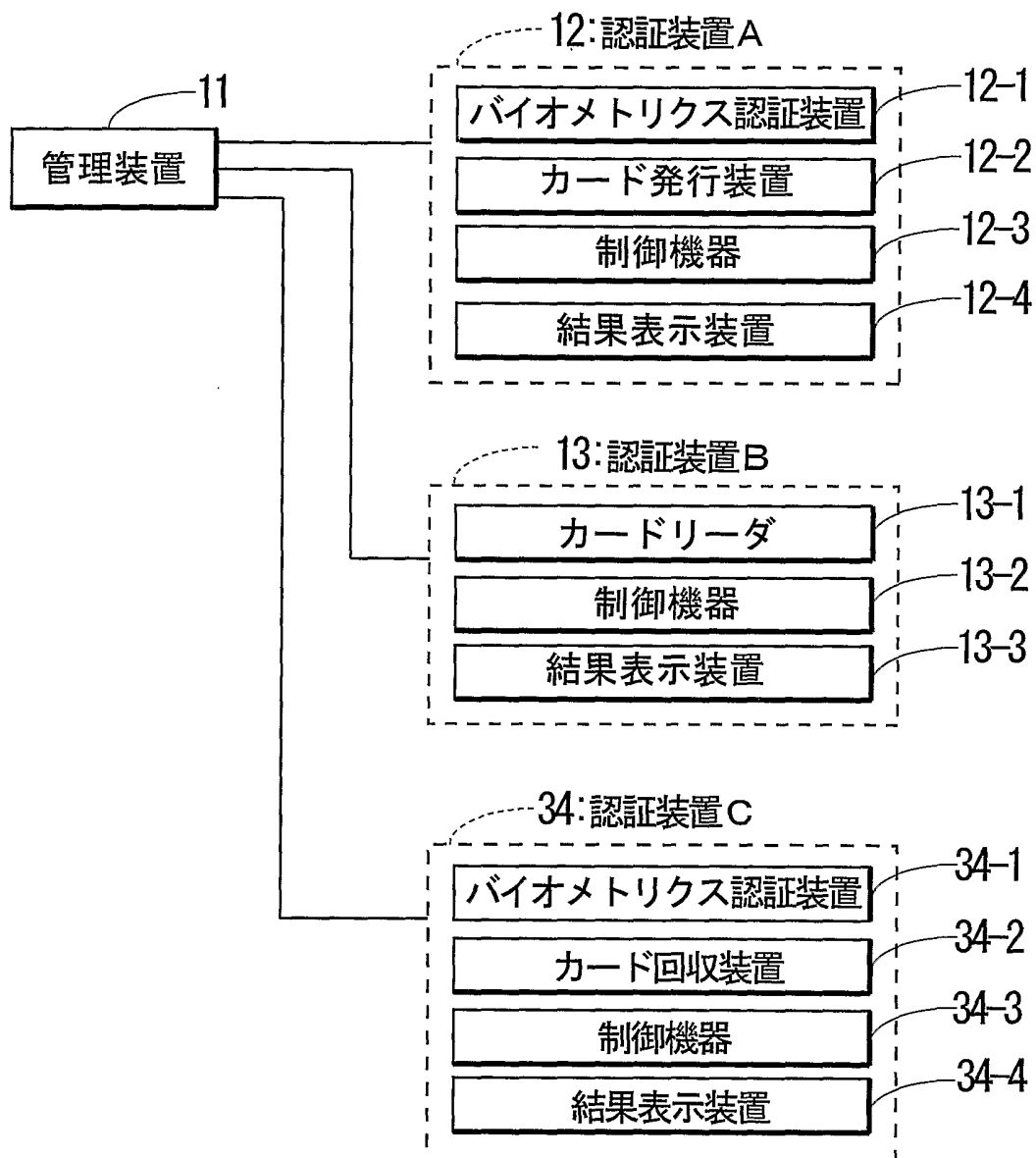
14 / 18

第19図



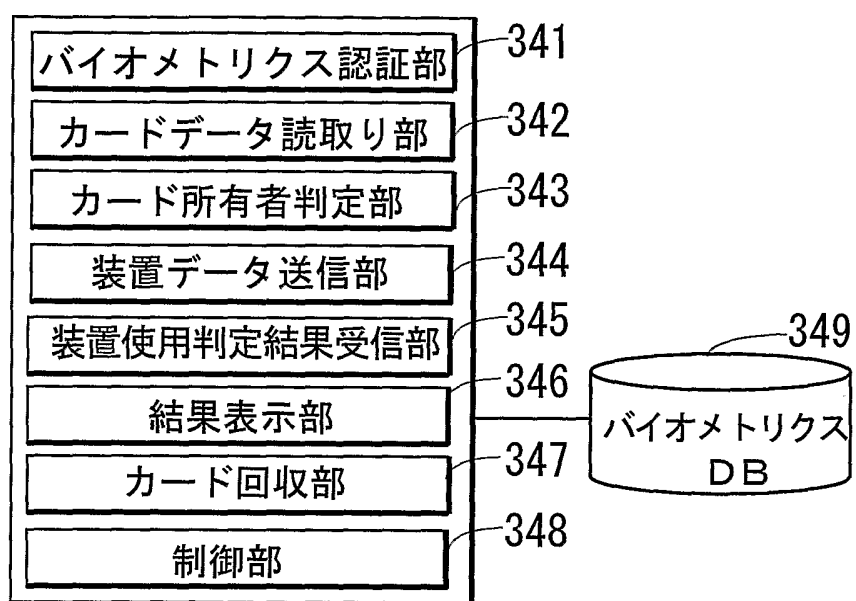
15 / 18

第20図



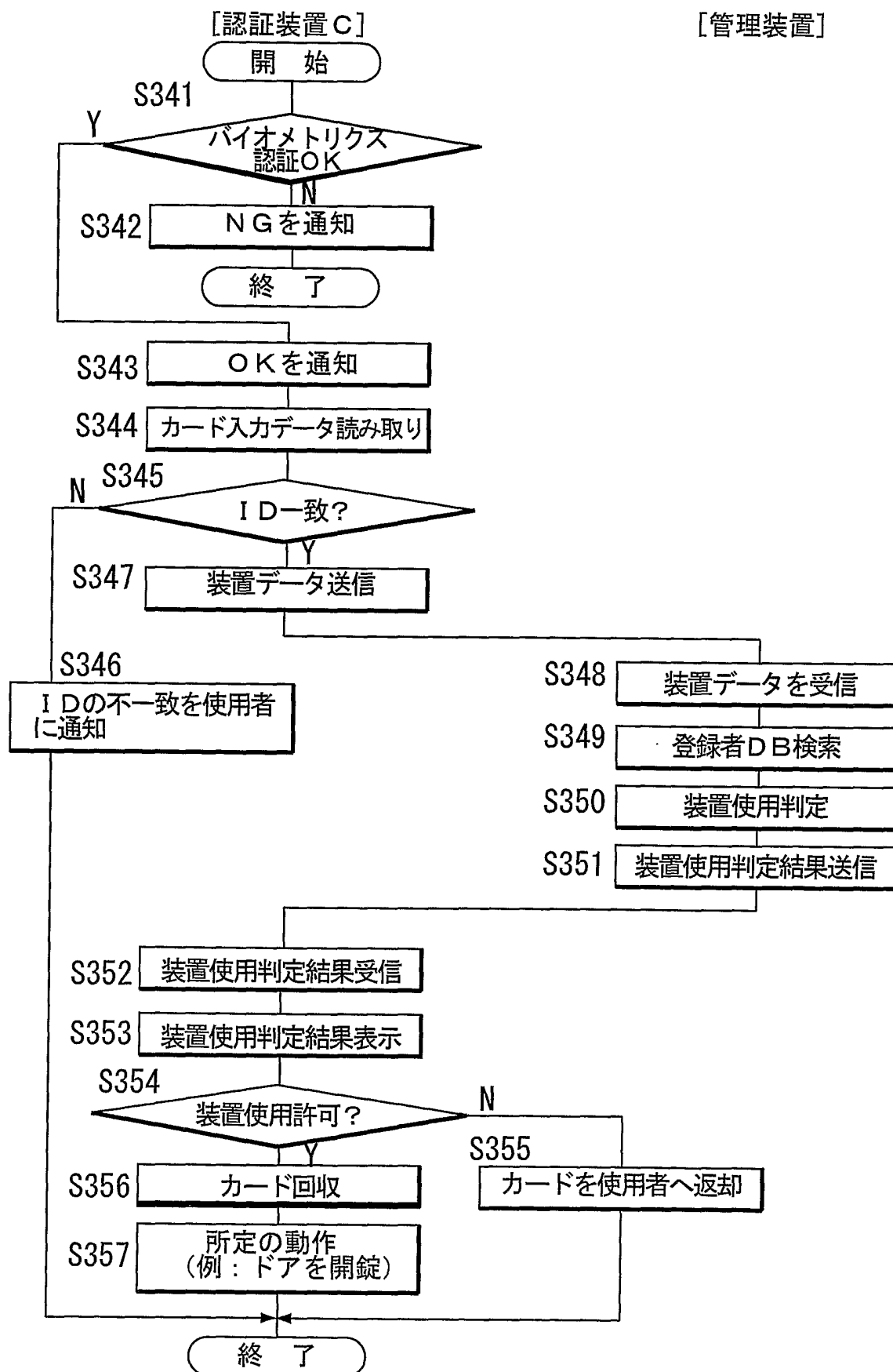
16 / 18

第21図



17 / 18

第22図



第23図

	所有物		バイオメトリクス
	磁気カード、ICカードなど	指紋、虹彩、顔貌など	
費用の安さ	○	×	・ 所有物による個人認証に比べ高価
悪用の困難さ	×	◎	・ 偽造は困難
認証時間の速さ	○	△	・ 認証に時間を要するケースがある
確実な認証	△	◎	・ 身体特徴のため確実に認証可能

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/008682

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06K17/00, G06F15/00, E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06K17/00, G06F15/00, E05B49/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-246041 A (Glory Ltd.), 14 September, 1998 (14.09.98), Full text; Figs. 1 to 11 (Family: none)	1-11
Y	JP 2003-44892 A (Matsushita Electric Industrial Co., Ltd.), 14 February, 2003 (14.02.03), Par. Nos. [0062] to [0102]; Figs. 8 to 21 (Family: none)	1-11
Y	JP 9-44617 A (Toshiba Corp.), 14 February, 1997 (14.02.97), Full text; Figs. 1 to 10 (Family: none)	3, 7

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 July, 2004 (20.07.04)

Date of mailing of the international search report
03 August, 2004 (03.08.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ G06K17/00, G06F15/00, E05B49/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ G06K17/00, G06F15/00, E05B49/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国実用新案登録公報 1996-2004年

日本国登録実用新案公報 1994-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-246041 A (グローリー工業株式会社) 1998.09.14, 全文, 第1-11図 (ファミリーなし)	1-11
Y	JP 2003-44892 A (松下電器産業株式会社) 2003.02.14, 段落【0062】-【0102】, 第8-21図 (ファミリーなし)	1-11
Y	JP 9-44617 A (株式会社東芝) 1997.02.14, 全文, 第1-10図 (ファミリーなし)	3, 7

☐ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

20.07.2004

国際調査報告の発送日

03.8.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

安田 太

5N

9177

電話番号 03-3581-1101 内線 3585