(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2005-292875
(P2005-292875A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 19/10	G06K 19/00	R	2C005
B42D 15/10	B42D 15/10	521	5B035
G06K 17/00	G06K 17/00	S	5B058
G09C 1/00	G09C 1/00	660A	5J104

審査請求 未請求　請求項の数 10　ＯＬ　（全 24 頁）

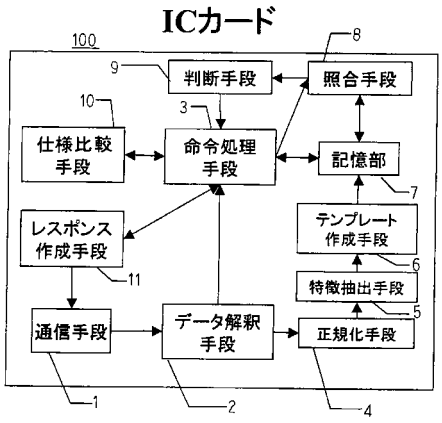
(21)出願番号　特願2004-102521 (P2004-102521)
(22)出願日　平成16年3月31日 (2004.3.31)

(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　100105647
弁理士　小栗　昌平
(74)代理人　100105474
弁理士　本多　弘徳
(74)代理人　100108589
弁理士　市川　利光
(74)代理人　100115107
弁理士　高松　猛
(74)代理人　100090343
弁理士　濱田　百合子

最終頁に続く

(54)【発明の名称】ＩＣカード及びシステム端末

(57)【要約】
【課題】　システム側セキュリティとカードユーザ側セキュリティを両立した上で効率的な認証処理を行う。
【解決手段】　予め定められた仕様に基づいてシステム端末との間で個人認証情報の照合に基づく認証処理を行う為のＩＣカード１００であって、システム端末側の仕様とＩＣカード１００側の仕様とを比較する仕様比較手段１０を備え、仕様比較手段１０は、比較結果に応じて、ＩＣカード１００の照合機能を用いた照合、システム端末の照合機能を用いた照合及びＩＣカード１００とシステム端末のそれぞれの照合機能を用いた照合から、個人認証情報の照合方法を選択する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
予め定められた仕様に基づいてシステム端末との間で個人認証情報の照合に基づく認証処理を行う為のＩＣカードであって、
前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較する比較手段と、
比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段と、
を備えるＩＣカード。
【請求項２】
請求項１記載のＩＣカードであって、
前記比較手段は、前記ＩＣカード及び前記システム端末がそれぞれ互いに要求する仕様を比較するＩＣカード。
【請求項３】
請求項１又は２記載のＩＣカードであって、
前記比較手段は、前記ＩＣカード及び前記システム端末のユーザがそれぞれ任意に設定した仕様を比較するＩＣカード。
【請求項４】
請求項１記載のＩＣカードであって、
前記比較手段は、前記ＩＣカード及び前記システム端末の機能仕様を比較するＩＣカード。
【請求項５】
予め定められた仕様に基づいてＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為のシステム端末であって、
前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較する比較手段と、
比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段と、
を備えるシステム端末。
【請求項６】
請求項５記載のシステム端末であって、
前記比較手段は、前記ＩＣカード及び前記システム端末がそれぞれ互いに要求する仕様を比較するシステム端末。
【請求項７】
請求項５又は６記載のシステム端末であって、
前記比較手段は、前記ＩＣカード及び前記システム端末のユーザがそれぞれ任意に設定した仕様を比較するシステム端末。
【請求項８】
請求項５記載のシステム端末であって、
前記比較手段は、前記ＩＣカード及び前記システム端末の機能仕様を比較するシステム端末。
【請求項９】
予め定められた仕様に基づいてシステム端末とＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為の認証プログラムであって、コンピュータを、
前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較する比較手段、
比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段、として機能させるための認証プログラム。
【請求項１０】

予め定められた仕様に基づいてシステム端末とＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為の認証方法であって、
前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較し、
比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する認証方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、予め定められた仕様に基づいてシステム端末とＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為のＩＣカード及び認証システム端末に関する。
【背景技術】
【０００２】
ＩＣカードを利用した個人認証が広く普及しつつある。ＩＣカードを用いた認証では、ＩＣカードに予め記録された個人情報と認証システム端末（またはＩＣカード）が取得した情報とをＩＣカード内で照合する方法（即ち、カード内照合）と、ＩＣカードが保持する個人情報を認証システム端末が読み出し、認証システム端末が取得した情報と認証システム端末内で照合する方法（即ち、カード外照合）の２種類がある。前者の例としては、ＩＣカードに登録された指紋情報と、ＩＣカードに搭載した指紋センサで取得した指紋情報とを照合して、整合性が確認された場合のみコンピュータのログイン名やパスワード情報をコンピュータへ転送するＩＣカード（特許文献１参照）などがある。一方、後者の例としては、ＩＣカードに登録された指紋情報とシステムの指紋センサで取得した指紋情報を照合し、更に、それら２つの指紋情報を遠隔のデータベースに予め登録された指紋情報と照合して認証精度を向上させた個人認証装置(特許文献２参照)などがある。
【０００３】
ところで、薄型で容量にも制約のあるＩＣカード内で照合処理を行わせる場合、処理負荷が高くなると認証に時間がかかるという問題や、カード自体の製造コストが高くなるという問題がある。そのため、例えば、暗証番号やパスワードの照合など処理量の少ないＰＩＮ認証はカード内で行い、画像処理を含む認証や特徴パターンの照合など高度で処理量の多い認証はカード外で行うなど、従来は、カード内またはカード外のいずれか一方に照合場所が固定されていた。
【０００４】
【特許文献１】特許第２９６７７６４号公報（第３－４頁、第２図）
【特許文献２】特許第２８７２１７６号公報（第４－６頁、第１図）
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、一般的には、カード内の個人情報が認証時にカード外へ送出されることはセキュリティ上好ましいことではないため、通常はカード内照合を基本とし、認証内容に応じてカード外照合（即ち、カード外への個人情報送出の許可）が決定されることが望ましい。例えば、ＩＣカードを保持する人員の入室可否を判断する入室管理システムでは、出入口の開閉を制御する権限を有するシステム側で個人認証の照合処理が行われることが好ましく、また、電子マネーシステムでは、決済に際して、擬似マネーを保有するカード側に照合処理の権限があることが好ましい。一方、カード側で照合処理を行うことが好ましいような場合でも、例えば、カード側に照合処理を行うための機能が搭載されていないなど、ＩＣカードまたは認証システム端末の仕様（ハードウェアやソフトウェアに係わる性能）によって、照合場所が強制的に決定される場合もある。このような場合、ユーザの意向やカードの可能性（追加ソフトウェアによる処理能力や精度の向上）を考慮したものではなく、カード保持者（カードユーザ）主導ではない。またカード内に生体情報、認証アル

ゴリズムが含まれている場合、システム側がインタフェースに対応することで、その認証方法を許容することができるのに、実際は固定的な場合が多く見られる。

【０００６】

今後、ＩＣカードの高性能化や高機能化、ダウンローダブル化に伴い、同じカードに入室管理機能や電子マネー機能など、複数の機能を付加したり変更可能なカードが多用されることも想定すると、特に、そのような使用環境では、認証内容に基づいて適応的にカード内照合・カード外照合が切り替えられることが好ましく、本人認証機能が一律に動作するのは生体情報を漏洩する危険が考えられ、容認できない。また、電子マネーは利用範囲が広く、どのシステムとも機器間での合意が取れれば、入退室管理機能と同様に個人情報を外部に出すというのは、生体情報を使ってカード保持者とカードを結び付けるシステム側のセキュリティのみ考慮されている。一般的に機器間での合意は、システム側で行われ、システム側のセキュリティ要件を満たす形で行われる。

【０００７】

本発明は、上記事情に鑑みてなされたものであって、システム側セキュリティとカードユーザ側セキュリティを両立した上で効率的な認証処理が可能なＩＣカード及びシステム端末を提供することを目的とする。

【課題を解決するための手段】

【０００８】

本発明のＩＣカードは、予め定められた仕様に基づいてシステム端末との間で個人認証情報の照合に基づく認証処理を行う為のＩＣカードであって、前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較する比較手段と、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段と、を備える。

【０００９】

上記構成によれば、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段を備えることにより、比較結果に応じて適応的にＩＣカード内、ＩＣカード外及びＩＣカード内外の組み合わせのいずれかで照合処理できるため、システム側セキュリティとカードユーザ側セキュリティを両立した上で効率的な認証処理が行える。

【００１０】

また、本発明のＩＣカードは、前記比較手段が、前記ＩＣカード及び前記システム端末がそれぞれ互いに要求する仕様を比較するものである。また、本発明のＩＣカードは、前記比較手段が、前記ＩＣカード及び前記システム端末のユーザがそれぞれ任意に設定した仕様を比較するものである。また、本発明のＩＣカードは、前記比較手段が、前記ＩＣカード及び前記システム端末の機能仕様を比較するものである。

【００１１】

また、本発明のシステム端末は、予め定められた仕様に基づいてＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為のシステム端末であって、前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較する比較手段と、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段と、を備える。

【００１２】

上記構成によれば、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段を備えることにより、比較結果に応じて適応的にＩＣカード内、ＩＣカード外及びＩＣカード内外の組み合わせのいずれかで照合処理できるため、システム側セキュリティとカードユーザ

側セキュリティを両立した上で効率的な認証処理が行える。

【００１３】

また、本発明のシステム端末は、前記比較手段が、前記ＩＣカード及び前記システム端末がそれぞれ互いに要求する仕様を比較するものである。また、本発明のシステム端末は、前記比較手段が、前記ＩＣカード及び前記システム端末のユーザがそれぞれ任意に設定した仕様を比較するものである。また、本発明のシステム端末は、前記比較手段が、前記ＩＣカード及び前記システム端末の機能仕様を比較するものである。

【００１４】

また、本発明の認証プログラムは、予め定められた仕様に基づいてシステム端末とＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為の認証プログラムであって、コンピュータを、前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較する比較手段、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段、として機能させるためのプログラムである。

【００１５】

さらに、本発明の認証方法は、予め定められた仕様に基づいてシステム端末とＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為の認証方法であって、前記システム端末側の仕様と前記ＩＣカード側の仕様とを比較し、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択するものである。

【発明の効果】

【００１６】

本発明によれば、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択することにより、比較結果に応じて適応的にＩＣカード内、ＩＣカード外及びＩＣカード内外の組み合わせのいずれかで照合処理できるため、システム側セキュリティとカードユーザ側セキュリティを両立した上で効率的な認証処理が行える。

【発明を実施するための最良の形態】

【００１７】

図１は本発明の実施の形態を説明するためのＩＣカードの構成を示す図であり、図２は本発明の実施の形態を説明するためのシステム端末の構成を示す図である。以下、システム端末２００とＩＣカード１００との間で生体情報の照合に基づく認証処理を行う例を説明する。

【００１８】

はじめに、本発明の実施の形態におけるＩＣカードの内部構成について説明する。ＩＣカード１００は、予め定められた仕様に基づいてシステム端末との間で個人認証情報の照合に基づく認証処理を行う為のものであり、図１に示すように、主に、通信手段１、データ解釈手段２、命令処理手段３、正規化手段４、特徴抽出手段５、テンプレート作成手段６、記憶部７、照合手段８、判断手段９、仕様比較手段１０、レスポンス作成手段１１、などで構成される。

【００１９】

通信手段１は、外部とデータの送受信を行うための手段で、ＵＳＢ、赤外線、無線等の通信規格やそれを実現するための機器を含み、ここでは、後述するシステム端末２００の通信手段との間でデータの送受信を行う。データ解釈手段２は、通信手段１から受信したデータを解釈し、データの形式を調査して、正規化が必要なデータを正規化手段４へ、ＩＣカード１００が処理可能なデータを命令処理手段３へ送信する。

【００２０】

命令処理手段３は、データ解釈手段２より受信したデータを命令信号として処理する手段であり、命令内容によって、記憶部７や照合手段８にデータを送信したり、記憶部７からデータを取得したりする。また、命令処理手段３は、記憶部７から取得した予め定められた仕様を記述した仕様データを仕様比較手段１０に渡す機能や、仕様比較手段１０から、後述する仕様比較結果（図１７参照）を受け取り、比較結果に応じて、ＩＣカード１００の照合機能を用いた照合、システム端末２００の照合機能を用いた照合及びＩＣカード１００とシステム端末２００のそれぞれの照合機能を用いた照合から、生体情報（個人認証情報）の照合方法を選択する機能を有する。また、命令処理手段３は、選択した生体情報の照合方法をレスポンス作成手段１１に通知する。なお、ＩＣカード１００の仕様データは、ＩＣカード１００がシステム端末に要求する仕様やＩＣカード１００の機能仕様を示す情報を含む。また、ＩＣカード１００がシステム端末に要求する仕様は、ＩＣカード１００のユーザが任意に設定した仕様を含む。

【００２１】

正規化手段４は、データ解釈手段２より受信したデータを、ＩＣカード１００が保持する認証アルゴリズムに対応するデータに変換しやすいように、データのサイズ変更や縦横の補正、光学的処理などを行う。特徴抽出手段５は、正規化手段４より受信したデータから、ＩＣカード１００が保持している認証アルゴリズムに対応した部分を抽出する。テンプレート作成手段６は、特徴抽出手段５より受信したデータを、ＩＣカード１００が保持している認証アルゴリズムに対応したデータ形式、データ列に変換する。

【００２２】

記憶部７は、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＦｅＲＡＭ、ＦＬＡＳＨ等の一時的メモリを含む記憶装置で構成され、各種のデータを格納する。照合手段８は、命令処理手段３から受信したデータと記憶部７に格納されているデータを比較照合するための手段であり、判断手段９は、照合手段８の照合結果に基づいて、通信しているシステム端末２００との照合処理で設定されている閾値やパラメータ等から判断して、認証が成功であるか失敗であるか、また成功の度合いがどの程度であるかを命令処理手段３へ出力する。

【００２３】

仕様比較手段１０は、ＩＣカード１００の仕様とシステム端末２００の仕様とを比較する機能を有し、比較結果を命令処理手段３に通知する。また、仕様比較手段１０は、比較に基づいてどの照合方法を用いるかを判断し、更にその照合の妥当性を判断する仕様照合手段１０ａ（図１６参照）と、ＩＣカード１００内の仕様と照合結果を比較して、完全性、真正性を含めて内容の確認を行う仕様確認手段１０ｂ（図６参照）とを含む。尚、仕様の具体的内容及び仕様の比較方法については後述する。レスポンス作成手段１１は、命令処理手段３から照合方法選択結果の通知を受けて、システム端末２００へ送信するためのレスポンスを作成する。また、レスポンス作成手段３は、命令処理手段３からの仕様データやテンプレートを含むデータを受信して、システム端末２００へ送信するためのレスポンスを作成する。

【００２４】

次に、本発明の実施の形態におけるシステム端末の内部構成について説明する。システム端末２００は、予め定められた仕様に基づいてＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為のものであり、図２に示すように、主に、通信手段２１、データ解釈手段２２、命令処理手段２３、正規化手段２４、特徴抽出手段２５、テンプレート作成手段２６、記憶部２７、照合手段２８、判断手段２９、仕様比較手段３０、命令発行手段３１、などで構成され、外部に通信線３００を介してセンサ４００が接続される。

【００２５】

通信手段２１は、外部とデータの送受信を行うための手段で、ＵＳＢ、赤外線、無線等の通信規格やそれを実現するための機器を含み、ここでは、ＩＣカード１００との間でデータの送受信やセンサからのデータの受信を行う。データ解釈手段２２は、通信手段２１から受信したデータを解釈し、データの形式を調査して、正規化が必要なデータを正規化

手段２４へ、システム端末２００が対応可能な命令コードを命令処理手段２３へ送信するように切り分け、分岐や変換、データ形式の正当性を調査する。

【００２６】

命令処理手段２３は、データ解釈手段２２より受信したデータを命令信号として処理する手段であり、命令内容によって、記憶部２７や照合手段２８、命令発行手段３１へ特定のデータや処理データを送信したり、記憶部２７からデータを取得したりする。また、命令処理手段２３は、記憶部７から取得した予め定められた仕様を記述した仕様データを仕様比較手段３０に渡す機能や、仕様比較手段３０から、後述する仕様比較結果（図１４参照）を受け取り、比較結果に応じて、ＩＣカード１００の照合機能を用いた照合、システム端末２００の照合機能を用いた照合及びＩＣカード１００とシステム端末２００のそれぞれの照合機能を用いた照合から、生体情報（個人認証情報）の照合方法を選択する機能を有する。また、命令処理手段２３は、選択した生体情報の照合方法を命令発行手段３１に通知する。なお、システム端末の仕様データは、システム端末２００がＩＣカードに要求する仕様やシステム端末２００の機能仕様を示す情報を含む。また、システム端末２００がＩＣカードに要求する仕様は、システム端末２００のユーザが任意に設定した仕様を含む。

【００２７】

正規化手段２４は、データ解釈手段２２より受信したデータを、システム端末２００が保持する認証アルゴリズムに対応するデータに変換しやすいように、データのサイズ変更や縦横の補正、光学的処理などを行う。特徴抽出手段２５は、正規化手段２４より受信したデータから、システム端末２００が保持している認証アルゴリズムに対応した部分を抽出する。テンプレート作成手段２６は、特徴抽出手段２５より受信したデータを、システム端末２００が保持している認証アルゴリズムに対応したデータ形式、データ列に変換する。

【００２８】

記憶部２７は、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＨＤＤ、ＦＬＡＳＨ等の一時的メモリを含む記憶装置で構成され、テンプレート、システム端末側の仕様データや一時的なデータ、パラメータのデフォルト設定値などの各種のデータを格納する。照合手段２８は、命令処理手段２３から受信したデータと、記憶部２７に格納されているデータとを比較照合するための手段であり、判断手段２９は、成功と失敗を分ける閾値や成功の度合いを決めるパラメータ等を、照合手段２８の照合結果に基づいて、端末200が格納しているパラメータを使う場合と、通信しているＩＣカード100が格納する仕様データから導出する場合があり、認証が成功であるか失敗であるか、また成功の度合いがどの程度であるかを出力する。

【００２９】

仕様比較手段３０は、システム端末２００の仕様とＩＣカード１００の仕様とを比較する機能を有し、比較結果を命令処理手段２３に通知する。また、仕様比較手段３０は、比較に基づいてどの照合方法を用いるかを判断し、更にその照合の妥当性を判断する仕様照合手段３０ａ（図６参照）と、システム端末２００内の仕様と照合結果を比較して、完全性、真正性を含めて内容の確認を行う仕様確認手段３０ｂ（図１６参照）とを含む。尚、仕様の具体的内容及び仕様の比較方法については後述する。命令発行手段３１は、命令処理手段２３から照合方法選択結果の通知を受けて、ＩＣカード１００に対する命令を発行する。また、命令発行手段３１は、判断手段２９または命令処理手段２３より受信したデータから、ＩＣカード１００に対する命令を発行する。

【００３０】

また、通信線３００を介してシステム端末２００と接続されるセンサ４００は、主に、顔画像を撮影するための撮像装置や、温度や静電容量などを検知可能な指紋読取装置など、外部の対象物よりデータを取得するための読取手段４１、システム端末２００との間でデータの送受信を行う通信手段４２、で構成される。以下、読取手段４１で指紋、顔画像、虹彩などの生体情報を取得する場合について説明する。

【００３１】
次に、上記構成のＩＣカード及びシステム端末の間で行われる認証のための照合動作について、仕様の比較をカード外（即ち、システム端末内）で行う場合と、またはカード内で行う場合とに分けて説明する。
【００３２】
＜仕様の比較をシステム端末内で行う場合＞
図３は、システム端末で仕様比較及び照合処理を行う場合の認証処理手順を示すシーケンス図であり、システム端末で仕様の比較を行い、その結果、照合処理もシステム端末で行う場合を示す。センサ４００の読取手段４１で読み取られた生体情報が、通信手段４２、システム端末の通信手段２１、データ解釈手段２２を介して正規化手段２４で正規化処理される（ステップＳ１０１）。更に、特徴抽出手段２５で特徴抽出処理を行って（ステップＳ１０２）、テンプレート作成手段２６でサンプルテンプレートを作成する（ステップＳ１０３）。サンプルテンプレートは記憶部２７に格納される（ステップＳ１０４）。サンプルテンプレートとは、センサ４００から取得した生体情報に基づいて作成したテンプレートのことで、ＩＣカード内に予めカードのユーザーにより登録されているテンプレートと異なる。次に、命令処理手段２３が、命令発行手段３１に対して問い合わせコマンドの送信を命令し（ステップＳ１０５）、命令発行手段３１は、ＩＣカードに問い合わせコマンドを送信する（ステップＳ１０６）。
【００３３】
ＩＣカードでは、受信データをデータ解釈手段２で解釈し（ステップＳ１０７）、問い合わせコマンドを命令処理手段３へ送信する。命令処理手段３は、問い合わせコマンドに対応する仕様データを記憶部７から取得、加工してレスポンス作成手段１１へ送信する（ステップＳ１０８）。レスポンス作成手段１１は、ＩＣカードの仕様データを含む応答メッセージを、通信手段１を介してシステム端末側へ送信する（ステップＳ１０９）。
【００３４】
システム端末の通信手段２１を介して受信した応答メッセージをデータ解釈手段２２で解釈し（ステップＳ１１０）、命令処理手段２３は、仕様比較手段３０に対して仕様データの比較を行う命令を送信する（ステップＳ１１１）。仕様照合手段３０ａは、記憶部２７から読み出したシステム端末の仕様データと、応答メッセージに含まれていたＩＣカードの仕様データとを比較して、照合処理を行う場所をカード内とするかカード外とするかを判定する（ステップＳ１１２）。尚、この仕様照合手段３０ａにおける仕様の比較方法については後述する（ここでは、比較の結果、カード外照合と判定される）。
【００３５】
次に、命令処理手段２３は比較結果の通知用コマンドを作成して、命令発行手段３１に対してコマンドの送信を命令し（ステップＳ１１３）、命令発行手段３１は、ＩＣカードに通知用コマンドを送信する（ステップＳ１１４）。
【００３６】
ＩＣカードでは、受信データをデータ解釈手段２で解釈し（ステップＳ１１５）、通知用コマンドを命令処理手段３へ送信する。命令処理手段３は、仕様比較手段１０に通知用コマンドの内容確認を行う命令を送信し（ステップＳ１１６）、仕様確認手段１０ｂは、通知用コマンドに含まれる仕様データの内容を確認して、カード外照合となった結果を把握する（ステップＳ１１７）。カード外照合となったため、命令処理手段３は、ＩＣカードのステータスを、記憶部７に格納されたテンプレート（個人情報）を外部へ送出可とするステータスへ変更し（ステップＳ１１８）、レスポンス作成手段１１は、ＩＣカードがカード外照合を正常に確認した旨の応答メッセージを、通信手段１を介してシステム端末側へ送信する（ステップＳ１１９）。尚、通常ＩＣカードでは、テンプレートのカード外送出は不可のステータスとなっている。
【００３７】
システム端末のデータ解釈手段２２が応答メッセージを受信すると（ステップＳ１２０）、命令処理手段２３は、命令発行手段３１に対してＩＣカードのテンプレートを読み出

すための読み出しコマンドの発行を命令し（ステップＳ１２１）、命令発行手段３１は、テンプレート読み出しコマンドを送信する（ステップＳ１２２）。

【００３８】

ＩＣカードのデータ解釈手段２がテンプレート読み出しコマンドを受信すると（ステップＳ１２３）、命令処理手段３は、記憶部７に格納されたテンプレートの読み出しを命令する（ステップＳ１２４）。記憶部７から読み出されたテンプレートはデータ列に加工され（ステップＳ１２５）、レスポンス作成手段１１は、テンプレートを含む応答レスポンスとしてシステム端末側へ送信する（ステップＳ１２６）。

【００３９】

システム端末の通信手段２１を介して受信した応答レスポンスをデータ解釈手段２２で解釈し（ステップＳ１２７）、命令処理手段２３は、記憶部２７からサンプルテンプレートの読み出しを命令する（ステップＳ１２８）。記憶部２７からサンプルテンプレートが読み出される（ステップＳ１２９）と、照合手段２８は、応答レスポンスに含まれていたテンプレートとを比較して照合処理を行う（ステップＳ１３０）。次に、判断手段２９は、照合結果に基づいて本人であると認証するか否かの判断処理を行う（ステップＳ１３１）。

【００４０】

図４は、システム端末が仕様比較及び照合処理を行う場合にＩＣカードとシステム端末が備える最小限の構成を示す図であり、上記の認証処理手順をシステム端末が行うためにＩＣカード１０１とシステム端末２０１が備える最小限の要素を示す。ＩＣカード側に照合手段や判断手段などがないような場合には、上記のような手順で認証処理が実行される。

【００４１】

図５は、システム端末で仕様比較しＩＣカードで照合処理を行う場合の認証処理手順を示すシーケンス図であり、システム端末で仕様の比較を行い、その結果、照合処理をカード内で行う場合を示す。センサ４００の読取手段４１で読み取られた生体情報が、通信手段４２、システム端末の通信手段２１、データ解釈手段２２を介して正規化手段２４で正規化処理される（ステップＳ２０１）。更に、特徴抽出手段２５で特徴抽出処理を行って（ステップＳ２０２）、テンプレート作成手段２６でサンプルテンプレートを作成する（ステップＳ２０３）。サンプルテンプレートは記憶部２７に格納される（ステップＳ２０４）。次に、命令処理手段２３が、命令発行手段３１に対して問い合わせコマンドの送信を命令し（ステップＳ２０５）、命令発行手段３１は、ＩＣカードに問い合わせコマンドを送信する（ステップＳ２０６）。

【００４２】

ＩＣカードでは、受信データをデータ解釈手段２で解釈し（ステップＳ２０７）、問い合わせコマンドを命令処理手段３へ送信する。命令処理手段３は、問い合わせコマンドに対応する仕様データを記憶部７から取得、加工してレスポンス作成手段１１へ送信する（ステップＳ２０８）。レスポンス作成手段１１は、ＩＣカードの仕様データを含む応答メッセージを、通信手段１を介してシステム端末側へ送信する（ステップＳ２０９）。

【００４３】

システム端末の通信手段２１を介して受信した応答メッセージをデータ解釈手段２２で解釈し（ステップＳ２１０）、命令処理手段２３は、仕様比較手段３０に対して仕様データの比較を行う命令を送信する（ステップＳ２１１）。仕様照合手段３０ａは、記憶部２７から読み出したシステム端末の仕様データと、応答メッセージに含まれていたＩＣカードの仕様データとを比較して、照合処理を行う場所をカード内とするかカード外とするかを判定する（ステップＳ２１２）。尚、この仕様比較手段３０ａにおける仕様の比較方法については後述する（ここでは、比較の結果、カード内照合と判定される）。

【００４４】

次に、命令処理手段２３は比較結果の通知用コマンドを作成して、命令発行手段３１に対してコマンドの送信を命令し（ステップＳ２１３）、命令発行手段３１は、ＩＣカード

に照合内容の通知コマンドを送信する（ステップＳ２１４）。

【００４５】

ＩＣカードでは、受信データをデータ解釈手段２で解釈し（ステップＳ２１５）、通知用コマンドを命令処理手段３へ送信する。命令処理手段３は、仕様比較手段１０に通知用コマンドの内容確認を行う命令を送信し（ステップＳ２１６）、仕様確認手段１０ｂは、通知用コマンドに含まれる仕様データの内容を確認して、カード内照合となった結果を把握する（ステップＳ２１７）。カード内照合となったため、命令処理手段３は、ＩＣカードのステータスを、システム端末から送信されるサンプルテンプレート（個人情報）の記憶部７への書き込みを可とするステータスへ変更し（ステップＳ２１８）、レスポンス作成手段１１は、ＩＣカードがカード内照合を正常に確認した旨の応答メッセージを、通信手段１を介してシステム端末側へ送信する（ステップＳ２１９）。尚、通常ＩＣカードでは、記憶部７への書き込みは不可のステータスとなっている。

【００４６】

システム端末のデータ解釈手段２２が応答メッセージを受信すると（ステップＳ２２０）、命令処理手段２３は、記憶部２７からサンプルテンプレートを読み出す命令を送信する（ステップＳ２２１）。記憶手段２７から読み出されたサンプルテンプレートはデータ列に加工され（ステップＳ２２２）、更に命令処理手段２３は、命令発行手段３１に対してサンプルテンプレートを含む書き込みコマンドをＩＣカード側へ送信する命令を送信する（ステップＳ２２３）。命令発行手段３１は、サンプルテンプレートを含む書き込みコマンドを送信する（ステップＳ２２４）。

【００４７】

ＩＣカードのデータ解釈手段２が書き込みコマンドを受信すると（ステップＳ２２５）、命令処理手段３は、記憶部７に格納されたテンプレートの読み出しを命令する（ステップＳ２２６）。記憶部７からテンプレートが読み出されると（ステップＳ２２７）、照合手段８は、読み出したテンプレートと、書き込みコマンドに含まれていたサンプルテンプレートとを比較して照合処理を行う（ステップＳ２２８）。次に、判断手段９は、照合結果に基づいて本人であると認証するか否かの判断処理を行い、判断結果を応答メッセージとしてシステム端末側へ送信する（ステップＳ２２９）。尚、上記のステップＳ２１４において、ＩＣカード側に特別な設定がない場合は、通知コマンドを送信せずに、直接テンプレートを送信しても構わないし、また、通知とテンプレート書き込みを同時に行えるコマンドを送信してもかまわない。

【００４８】

図６は、システム端末で仕様比較しＩＣカードで照合処理を行う場合にＩＣカードとシステム端末が備える最小限の構成を示す図であり、上記の認証処理手順を実現するためにＩＣカード１０２とシステム端末２０２が備える最小限の要素を示す。システム端末側に照合手段や判断手段がないような場合には、上記のような手順で認証処理が実行される。

【００４９】

ここで、ＩＣカードの仕様照合手段１０ａやシステム端末の仕様照合手段３０ａで比較される仕様について具体的に説明する。

【００５０】

図７はＩＣカードの仕様の設定例を示す図であり、図８はシステム端末の仕様の設定例を示す図である。図に示すように、ＩＣカードとシステム端末でそれぞれ詳細な仕様が予め設定されており、仕様照合手段３０ａでは、これら双方の仕様を、予め定められた処理手順（後述）で比較することにより、認証のための照合処理をカード内で行うか、カード外で行うかを判断する。また、このようにする事で、カードやシステムに追加、改良された認証アルゴリズムの精度や処理速度を考慮することができ、カード外で行っていた処理をカード内に変更することや、新たな認証方法を機器間ごとに決めることができる。さらに、システム側ユーザやカードユーザの意向を仕様の中に入れることで、使用したデータの保存方法等のプライバシー保護の観点を明示する事ができ、双方が不安なく、納得した形で認証処理を行う事ができる。

【００５１】
例えば、システム端末の仕様の設定例では、図８に示すように、照合の種類、カード外照合の場合にＩＣカードが了承できる機能であるか否かを公開する項目、カード内照合の場合にＩＣカードの機能をチェックするための項目、などの項目がある。仕様は、システム端末がＩＣカード（相手側）に要求する要求仕様（例えば、ＩＣカードの機能をチェックするための項目）、システム端末の機能仕様（例えば、ＩＣカードが了承できる機能であるかを公開する項目の中の、認証アルゴリズムの種類、認証精度、処理速度など）、システム端末のユーザーが任意に設定した要求仕様（ＩＣカードが了承できる機能であるかを公開する項目の中の、システム端末側が実行するテンプレートの管理方法など）などに分類される。また、項目の中で権限とは、最終判断を行うか否かの設定であり、例えば、前述の入室管理システムの例では、システム端末側が最終判断の権限を持つように設定すればよい。

【００５２】
図９は、仕様のデータ形式例を示す図である。本発明の実施の形態では、上記のような仕様をデータ列で表現する。図に示すように、ＴＬＶ（Tag Length Value）形式で、ＩＣカードまたはシステム端末のいずれの仕様であるかを示すタグ、データ長、照合の種類を示すタグ、データ長、値、認証アルゴリズムを示すタグ、データ長、値、・・という順番でデータを保持する。

【００５３】
次に、図１０から図１３を参照して、送信されるコマンドやレスポンスの具定的なデータ構成例を説明する。図１０は、システム端末から送信されるコマンドやレスポンスの具体例を示す図であり、システム端末で仕様比較を行う場合の、仕様データ読み出しを要求する問い合わせコマンド、仕様データを含む応答メッセージ、比較結果の通知用コマンドのデータ構成例を示す。システム端末で仕様比較を行う場合の認証処理手順を示すシーケンス図（図５）で説明すると、ステップＳ２０６では、図１０（ａ）に示す形式のデータが、システム端末からＩＣカードへの問い合わせコマンドとして送信される。また、ステップＳ２０９では、図１０（ｂ）に示す形式のデータが、ＩＣカードからシステム端末への応答メッセージとして送信される。更に、ステップＳ２１４では、図１０（ｃ）に示す形式のデータが、システム端末からＩＣカードへの比較結果の通知用コマンドとして送信される。

【００５４】
図１１は、認証アルゴリズムの識別値を指すテーブルである。データ内部の値について具体的に説明すると、例えば、図１０（ｂ）の応答メッセージの認証アルゴリズムの値は“０００００１０００００５”となっており、これで所定の認証アルゴリズムが指定される。図１１に示すように、認証アルゴリズムの種類とメーカーが数値で対応している。従って、“０００００１０００００５”は、Ｅ社の虹彩認証アルゴリズムであること一義的に決まる。

【００５５】
図１２は、システム端末から送信されるコマンドの具体例を示す図であり、仕様比較の結果に基づいて、システム端末がＩＣカードのテンプレートを読み出す場合（即ち、カード外照合）のテンプレート読み出しコマンド、システム端末がＩＣカードにテンプレートの書き込みを行う場合（即ち、カード内照合）のテンプレート書き込みコマンド、のデータ構成例を示す。システム端末２００で仕様比較を行い、その結果、カード外照合を行う場合の認証処理手順を示すシーケンス図（図３）で説明すると、ステップＳ１２２では、図１２（ａ）に示す形式のデータが、システム端末からＩＣカードへのテンプレート読み出しコマンドとして送信される。また、システム端末で仕様比較を行い、その結果、カード内照合を行う場合の認証処理手順を示すシーケンス図（図５）で説明すると、ステップＳ２２４では、図１２（ｂ）に示す形式のデータが、システム端末からＩＣカードへのテンプレート書き込みコマンドとして送信される。データ内にはサンプルテンプレートのデータが含まれている。

【００５６】
図１３は、システム端末から送信されるコマンドやカードからのレスポンスの具体例を示す図であり、ＩＣカードで仕様の比較を行う場合の、システム端末の仕様データをＩＣカードへ送信する仕様送信コマンド、カード内照合かカード外照合かを示す照合結果をＩＣカードからシステム端末へ送信する通知コマンドのデータ構成例を示す図である。尚、送信されるタイミングは、後述する仕様の比較をカード内で行う場合のシーケンス図（図１５）の説明で具体的に紹介する。
【００５７】
図１４は、システム端末の仕様照合手段３０ａにおける仕様の比較手順例を示すフローチャートである。はじめに、ＩＣカードの仕様がカード外照合を指定しているか否かを判断する（ステップＳ３０１）。ＩＣカードの仕様においてカード外照合が指定されている場合は、一義的にカード外照合に決定される。一方、指定されていない場合は、次に、ＩＣカードの仕様がハイブリッド認証を指定しているか否かを判断する（ステップＳ３０２）。ハイブリッド認証が指定されている場合、次に、システム端末がハイブリッド認証に対応しているか否か、または指定された認証方法、精度を許容しているか否かを判断する（ステップＳ３０３）。ハイブリッド認証に対応し、指定された認証方法、精度を許容している場合、次に、ＩＣカード内のテンプレートの管理方法とハイブリッド認証方法が合致しているか否かを判断する（ステップＳ３０４）。合致している場合は、ハイブリッド認証またはハイブリッド複数認証（マルチモーダル認証）に決定される。尚、ハイブリッド認証とは、ＩＣカード内及びＩＣカード外（システム端末側）の両方で認証処理を分担して行う方法であり、ハイブリッド複数認証とは、複数のバイオメトリクス認証を組み合わせた方法にハイブリッド認証方法を適用した方法である。マルチモーダル認証とは、複数認証の一種で認証方法を協調させたり同時に適用する方法である。
【００５８】
一方、ステップＳ３０２、Ｓ３０３、Ｓ３０４のいずれにも仕様が該当しない場合、次に、ＩＣカード内の認証アルゴリズムはシステム端末が許容できる範囲であるか否かを判断する（ステップＳ３０５）。許容できる範囲である場合、次に、クロス認証を指定しているか否かを判断する（ステップＳ３０６）。クロス認証を指定している場合、次に、ＩＣカードのテンプレートを外部に送出してよいか否かの判断を行う（ステップＳ３０７）。仕様においてテンプレートを外部に送出してよい旨の設定がなされている場合は、クロス照合に決定される。
【００５９】
尚、クロス照合とは、照合処理をカードと端末の両方で行い、その結果を相互に確認しあう事でその正当性（妥当性）を確保する方法である。クロス照合は、以下の場合に行われる。カード内認証で、端末が規定している精度以上の算出ができる状態で、カード外認証も行うようにする場合、照合結果はＡＮＤ演算を取り、両方が成功した時のみ成功とする。これにより、認証精度が向上する。但し、テンプレートを外に出してもよいという設定のため個人情報を守るという観点ではセキュリティは低下する。また、カード内認証で、端末が規定している精度以下の算出しかできない状態で、カード外認証も行うようにする場合、カード内での認証結果が、カードで規定している精度以上であれば成功と判断した上で、カード外認証でも成功でなければならない。カードで規定している精度以下しかカード内の精度がなければ、複数回成功することをカード外認証に求めたり、複数の生体認証を求めたり、カードを排出することもある。カード外認証を完全に信用できない場合にこの方法が用いられ、カード内でも認証を行うため、セキュリティを向上できる。尚、最初から「カード外認証」を指定した場合は、カード外での認証を信用していると考えることができるため、クロス照合を行うシーンとしては除外している。
【００６０】
一方、外部へ送出しないように設定されている場合や、ステップＳ３０６でクロス認証を指定していない場合は、次に、カード内にシステム端末が要求する認証精度の有無を判断する（ステップＳ３０８）。要求以上の認証精度がある場合はカード内照合に決定され

る。要求以下の認証精度しか無い場合、次に、ＩＣカードが複数認証（またはマルチモーダル認証）に対応しているか否かの判断を行う（ステップＳ３０９）。対応している場合は、次に、複数認証で要求する認証精度に到達しているか否かを判断する（ステップＳ３１０）。到達している場合は、カード内複数認証に決定される。

【００６１】

一方、複数認証で要求する認証精度に到達していない場合や、ステップＳ３０９でＩＣカードが複数認証（またはマルチモーダル認証）に対応していない場合、更に、ステップＳ３０５でカード内の認証アルゴリズムが、システム端末が許容できない範囲にある場合は、次に、ＩＣカードのテンプレートを外部に送出してよいか否かの判断を行う（ステップＳ３１１）。仕様においてテンプレートを外部に送出してよい旨の設定がなされている場合は、カード外照合に決定される。

【００６２】

一方、テンプレートを外部へ送出しないように設定されている場合は、次に、システム端末側に最終判断の権限（assets）があるか否かの判断を行う（ステップＳ３１２）。システム端末側に権限がない場合はカードの排出（認証拒否）が決定される。システム端末側に権限がある場合、テンプレートの読み出し可否についてＩＣカード保持者の意思確認を行い（ステップＳ３１３）、読み出し可である場合はカード外照合に決定される。一方、読み出し不可である場合は、カードの排出（認証拒否）が決定される。以上の手順で、照合処理をカード内で行うか、カード外で行うかが決定される。

【００６３】

上記の通り、カード外照合を行う際は、双方の仕様を比較した結果に決定した場合でもカード内の個人情報を外部に出すか否かという意思をカード保持者に確認するので、カード保持者が知らないうちに個人情報が漏洩することを防止できる。例えば、警察官による免許証チェックが行われる場合、通常は、免許証と免許証保持者との関係を明確にすることが重要であるためカード内認証でも構わない。しかし、警視庁が保有する指名手配犯ＤＢ内の顔データと一致するかを調べるブラックリスト照合の場合は、カード外照合を行う必要がある。この場合、免許証保持者に「意思確認」を行うことにより、免許証保持者が知らないうちに個人情報が漏洩することを防止できる。同様に、パスポートの場合、身分証明に利用する際はカード内認証で本人確認を行い、入出国時のようにカード外照合を行う必要がある場合は「意思確認」を行うことにより、パスポート保持者が知らないうちに個人情報が漏洩することを防止できる。尚、ハイブリッド認証、クロス認証、マルチモーダル認証に決定された場合の認証処理手順については説明を省略する。

【００６４】

＜仕様の比較をカード内で行う場合＞

図１５は、ＩＣカードで仕様比較及び照合処理を行う場合の認証処理手順を示すシーケンス図であり、ＩＣカードの仕様比較手段で仕様の比較を行い、その結果、照合処理もＩＣカード内で行う場合を示す。センサ４００の読取手段４１で読み取られた生体情報が、通信手段４２、システム端末の通信手段２１、データ解釈手段２２を介して正規化手段２４で正規化処理される（ステップＳ４０１）。更に、特徴抽出手段２５で特徴抽出処理を行って（ステップＳ４０２）、テンプレート作成手段２６でサンプルテンプレートを作成する（ステップＳ４０３）。サンプルテンプレートは記憶部２７に格納される（ステップＳ４０４）。次に、命令処理手段２３が、命令発行手段３１に対して、システム端末の仕様データを含む問い合わせコマンドの送信を命令し（ステップＳ４０５）、命令発行手段３１は、ＩＣカード１００に仕様データを含む問い合わせコマンドを送信する（ステップＳ４０６）。この問い合わせコマンドは、図１３（ａ）に示すデータ形式で、システム端末で設定されている仕様のデータが含まれる。

【００６５】

ＩＣカードの通信手段１を介して受信した問い合わせメッセージは、データ解釈手段２が解釈し（ステップＳ４０７）、命令処理手段３は、仕様比較手段１０に対して仕様データの比較を行う命令を送信する（ステップＳ４０８）。仕様照合手段１０ａは、記憶部７

から読み出したＩＣカードの仕様データと、問い合わせコマンドに含まれていたシステム端末の仕様データとを比較して、照合処理を行う場所をカード内とするかカード外とするかを判定する（ステップＳ４０９）。尚、この仕様照合手段１０ａにおける仕様の比較方法については後述する（ここでは、比較の結果、カード内照合と判定される）。レスポンス作成手段１１は、カード内照合となった旨を通知する応答メッセージを、通信手段１を介してシステム端末２００側へ送信する（ステップＳ４１０）。この応答メッセージ（通知用レスポンス）は、図１３（ｂ）に示すデータ形式で、カード内照合に対応する仕様のデータが含まれる。このデータは、後述するように、システム端末の仕様確認手段３０ｂで把握される。

【００６６】

システム端末では、受信データをデータ解釈手段２２で解釈し（ステップＳ４１１）、応答メッセージを命令処理手段２３へ送信する。命令処理手段２３は、仕様比較手段３０の仕様確認手段３０ｂに応答メッセージの内容確認を行う命令を送信し（ステップＳ４１２）、仕様確認手段３０ｂは、応答メッセージに含まれる仕様データの内容を確認して、カード内照合となった結果と仕様を把握する（ステップＳ４１３）。次に、記憶部２７からサンプルテンプレートが読み出され（ステップＳ４１４）、命令発行手段３１が、サンプルテンプレートを含むコマンドをＩＣカード側へ送信する（ステップＳ４１５）。

【００６７】

ＩＣカードのデータ解釈手段２がサンプルテンプレートを含むコマンドを受信すると（ステップＳ４１６）、命令処理手段３は、記憶部７に格納されたテンプレートの読み出しを命令する（ステップＳ４１７）。記憶部７からテンプレートが読み出されると（ステップＳ４１８）、照合手段８は、読み出したテンプレートと、受信したコマンドに含まれていたサンプルテンプレートとを照合する（ステップＳ４１９）。次に、判断手段９は、照合結果に基づいて本人であると認証するか否かの判断処理を行い（ステップＳ４２０）、判断結果をレスポンス作成手段１１よりシステム端末側へ送信する（ステップＳ４２１）。

【００６８】

図１６は、ＩＣカードが仕様比較及び照合処理を行う場合にＩＣカードとシステム端末が備える最小限の構成を示す図であり、上記の認証処理手順を実現する為に、ＩＣカード１０３とシステム端末２０３が備える最小限の要素を示す。システム端末側に照合手段や判断手段がないような場合には、上記のような手順で認証処理が実行される。尚、ＩＣカード側で仕様の比較を行って、照合処理はカード外で行われる場合についての説明は省略する。

【００６９】

図１７は、ＩＣカードの仕様照合手段１０ａにおける仕様の比較手順例を示すフローチャートである。はじめに、システム端末の仕様がカード内照合を指定しているか否かを判断する（ステップＳ５０１）。システム端末の仕様においてカード内照合が指定されている場合は、一義的にカード内照合に決定される。一方、指定されていない場合は、次に、ＩＣカードのテンプレートを外部に送出してよいか否かの判断を行う（ステップＳ５０２）。外部へ送出しないように仕様が設定されている場合は、次に、ＩＣカード側に最終判断の権限（assets）があるか否かの判断を行う（ステップＳ５０３）。ＩＣカード側に権限がある場合はカードの排出（認証拒否）が決定される。

【００７０】

一方、ＩＣカード側に権限がない場合は、次に、テンプレートの読み出し可否についてＩＣカード保持者の意思確認を行い（ステップＳ５０４）、読み出し不可である場合は、カードの排出（認証拒否）が決定される。一方、読み出し可である場合と、ステップＳ５０２でＩＣカードのテンプレートを外部に送出してよいと設定されている場合は、次に、システム端末がハイブリッド認証を指定しているか否かを判断する（ステップＳ５０５）。ハイブリッド認証が指定されている場合、次に、ＩＣカードがハイブリッド認証に対応しているか否か、または指定された認証方法、精度を許容しているか否かを判断する（ス

テップＳ５０６）。ハイブリッド認証に対応し、指定された認証方法、精度を許容している場合は、ハイブリッド認証またはハイブリッド複数認証（マルチモーダル認証）に決定される。

【００７１】

一方、カードがハイブリッド認証に対応せず、指定された認証方法、精度を許容していない場合と、ステップＳ５０５でシステム端末がハイブリッド認証を指定していない場合は、次に、システム端末が複数認証（またはマルチモーダル認証）を指定しているか否かの判断を行う（ステップＳ５０７）。指定している場合は、次に、ＩＣカードが複数認証（またはマルチモーダル認証）に対応しているか否かの判断を行う（ステップＳ５０８）。対応している場合は、カード内複数認証（またはマルチモーダル認証）に決定される。

【００７２】

一方、ＩＣカードが複数認証に対応していない場合と、ステップＳ５０７でシステム端末が複数認証を指定していない場合は、次に、クロス認証を指定しているか否かを判断する（ステップＳ５０９）。クロス認証を指定している場合は、クロス照合に決定される。また、クロス認証を指定していない場合は、カード外照合に決定される。以上の手順で、照合処理をカード内で行うか、カード外で行うかが決定される。尚、ハイブリッド認証、クロス認証、マルチモーダル認証に決定された場合の認証処理手順については説明を省略する。

【００７３】

実際の利用分野を検討すると、社員証に実装した場合が考えられる。カードに入退室機能、電子マネー、パソコンやネットワークへのアクセス機能が含まれている場合、利用環境は社内外で考えられる。会社内の入退出機能に関しては、カード外で行う方がログや生体情報（顔認証の場合は顔データ）が残り、追跡することが可能でありシステム上都合がよい。電子マネーは、社内の食堂など利用用途が明確で、一定のセキュリティを保持している場所であれば、利便性を考えカード外認証でも許容できる。しかし、社外で利用する際は、使用後のデータの扱いやカードユーザのプライバシー保護から見ても、カード内認証をするべきである。また、家庭から会社のパソコンにアクセスする際は、家庭のパソコンに端末用ソフトウェアをインストールできる面や情報漏洩の危険性からもカード外認証で構わないが、他人のパソコンや不特定多数の人が利用するインターネットカフェなどからアクセスする場合は、カード内認証を行う方が安全である。このように同じアプリケーションでも利用環境によって、カード内、カード外の選択が必要であり、カードにおいて、この機能の必要性は明確である。

【００７４】

また、社員証内の認証アルゴリズムが更新されたり、システムに付いているセンサーの精度が向上したことによる認証率の向上などを仕様に反映することで、カード外で行っていた処理をカード内に変更することが可能である。

【００７５】

また、システム側ユーザにおいても、仕様を変更する事で、平日は守衛がいるため、カード内照合を許容した場合でも、休日や時間外は無人になるため、カード外照合を求めるように設定したり、求める認証精度を高く設定することができる。場所や利用率によって仕様を変更しても、同様の効果が得られ、同じシステム構成で複数の利用用途に対応可能になる。

【００７６】

ユーザによっては、プライバシー保護の観点よりも、利便性を選択する場合もあり、完全なセキュリティよりも、外部によっては信用してデータを渡し、端末の持つスペックを用いて高速化を適用することも考えられる。それに対しても、仕様により対応できる範疇であり、外部にデータを出力しても良い許容範囲内で最適な効率の認証方法を選択することが可能である。

【００７７】

図１８は、ＩＣカードが仕様データを保持していない場合の認証処理手順を示すシーケ

ンス図であり、システム端末で仕様の比較を行う際にＩＣカードが仕様データを保持していない場合や仕様比較に未対応の場合を示す。この場合の処理手順は図３で説明したシーケンスとほぼ同様であるが、ステップＳ１１２で仕様照合手段３０ａが仕様データ無しと判断し、照合処理をカード外で行うと決定する。その後システム端末が図３で説明したステップＳ１１４までを実行した後、ＩＣカードがステップＳ１２３～Ｓ１２６の手順を行い、システム端末がステップＳ１２７～Ｓ１３１の手順を行う。尚、ステップＳ１１２における仕様照合方法は、システム端末が最適と考える方法で良い。

【００７８】

図１９は、システム端末が仕様データを保持していない場合の認証処理手順を示すシーケンス図であり、システム端末が仕様データを保持していない場合や仕様比較に未対応の場合を示す。この場合の処理手順のステップＳ６０１～Ｓ６０５は、図１５で説明したステップＳ２０１～Ｓ２０５と同様である。そして、システム端末が仕様データを保持していない（仕様比較に未対応である）場合、システム端末において、命令処理手段２３が、命令発行手段３１に対して仕様データ問い合わせコマンドを送信しないで、テンプレート読み出しコマンドを送信する（ステップＳ６０６）。一方、ＩＣカードは、テンプレート読み出しコマンドを受信しデータ解釈処理する（ステップＳ６０７）が、ステータス未変更のため読み出しができず（ステップS６０８）、システム端末に読み出し失敗を通知するレスポンスを作成し（ステップS６０９）送信する。通常であればここで通信終了するが、システム端末、カード間で相互認証やＰＩＮ照合によってテンプレートの読出しを可能にしていれば、読出しすることも可能である。読出し失敗の通知メッセージを受けたシステム端末は、メッセージをデータ解釈手段２２で解釈し（ステップＳ６１０）、命令処理手段２３がＰＩＮ照合のＶｅｒｉｆｙコマンドの送信を命令発行手段３１に指示し（ステップＳ６１１）、命令発行手段３１がＶｅｒｉｆｙコマンドを発行する（ステップＳ６１２）。ＩＣカードでは、データ解釈手段２がコマンドを解釈し（ステップＳ６１３）、命令処理手段３がＰＩＮ照合の成功後ステータスを遷移し（ステップS６１４）、レスポンス作成手段１１が正常終了を通知するレスポンスを作成し（ステップＳ６１５）送信する。システム端末が正常終了通知を受けた後の処理手順（ステップＳ６１６～Ｓ６２６）は、図３に示すステップＳ１２０～Ｓ１３１と同様である。

【００７９】

図２０は、仕様比較を行う主体を切り替える場合の処理手順を示すシーケンス図であり、初めはシステム端末が仕様比較を行うが、仕様比較処理の優先権がカードにあると判断して途中からＩＣカードで仕様比較を行う場合を示す。この場合の処理手順のステップＳ７０１～Ｓ７１１は、図３で説明したステップＳ１０１～Ｓ１１１と同様である。そして、システム端末の仕様照合手段３０ａが、優先権がカードにあることを確認し、カードに仕様比較手段が在ることも確認する（ステップＳ７１２）。その後、命令処理手段２３がシステム端末の仕様データを含む問い合わせコマンドを発行するよう命令発行手段３１に指示し（ステップＳ７１３）、命令発行手段３１が問い合わせコマンドを発行する（ステップＳ７１４）。ＩＣカードが問い合わせコマンドを受けた後の処理手順（ステップＳ７１５～Ｓ７１９）は、図１５に示すステップＳ４０７～Ｓ４１０とほぼ同様である。また、システム端末が照合結果（照合方法の選択結果）の通知を受けた後、結果に応じた照合処理が行われる。上記の通り、優先権を持っている側の照合手段を利用することによって、優先権を持っている側のセキュリティ情報の漏洩防止を考慮することができる。

【００８０】

尚、誤った場所で比較照合をした場合の例を示す。電子カルテをカード内に保持している場合に、仕様比較処理を不正な端末側で行うと、実際はカード内認証でできる場合でも端末で処理を行うという結果を出されてしまい、カード外照合を行うためにカード内の生体情報を外部に出力する必要がでてきてしまう。電子カルテのような複製がされにくく、価値のあるデータを持っている場合は信憑性を尊重し、端末側の要求を拒否して、カード内で仕様比較を行うことが望ましい。逆に、入退出システムの場合は、その場所にシステムが固定され、移動不可能の点を考えれば、端末側で仕様比較を行う方が好ましい。

【００８１】
図２１は仕様比較手段を有する側（システム端末）が相手（ＩＣカード）に対して、仕様データのうち必要な部分のみに関する問い合わせを出し、相手側がそれに返答して仕様の比較を行う方法（抽出方法）による認証処理手順を示すシーケンス図であり、図２２は抽出方法による仕様比較で使用されるコマンドとレスポンスの形式例を示す図である。この場合の処理手順のステップＳ８０１～Ｓ８０８は、図３で説明したステップＳ１０１～Ｓ１０８とほぼ同様であるが、システム端末がＩＣカードに仕様の問い合わせを行う際、命令発行手段３１ａが発行する問い合わせ用コマンドにタグが含まれている（図２２参照）点が異なる（ステップＳ８０６）。その後、ＩＣカードの仕様抽出手段がコマンドに含まれるタグを解釈し、指定されたデータを仕様データの中から抽出し書込む（ステップＳ８０９）。レスポンス作成手段１１は、抽出したＩＣカードの仕様データを含む応答メッセージを、システム端末側へ送信する（ステップＳ８１０）。また、システム端末が仕様データを含む応答メッセージを受信した後の処理手順（ステップＳ８１１～Ｓ８１４）は、図３に示すステップＳ１１０～Ｓ１１３と同様であるが、ステップＳ８１５では図３に示すステップＳ１２２と同様に命令発行手段３１がテンプレート読出しコマンドを送信する。その後の処理手順ステップＳ８１６～Ｓ８２４は、図３に示すステップＳ１２３～Ｓ１３１と同様である。

【００８２】
抽出方法を用いれば、仕様に含まれる項目やデータ量が増大しても、やり取りするデータ量を最小限に抑えることができる。また、抽出方法を用いてシステム端末で仕様を比較する際、コマンドの送信側と受信側とでタグやデータ形式を共有している場合にのみ仕様を読み出すことができるため、セキュリティが向上する。一方、ＩＣカードで仕様を比較する際、通信回数は増加するが、カード内のデータ領域を小さくすることができる。

【００８３】
尚、上記の実施の形態において、仕様の項目や設定値は一例であり、これにとらわれるものではなく、認証の内容、ＩＣカードやシステム端末のハードウェア・ソフトウェアに係わる設計上の制約、ＩＣカードやシステム端末のユーザーの意向、などにより任意に設定可能である。

【００８４】
また、上記の実施の形態において、仕様の比較手順（図１４及び図１７のフローチャート）も同様に一例であり、仕様を比較して認証を行う照合場所（カード内またはカード外）を決定する手順も任意に設定可能であることは言うまでもない。

【００８５】
尚、上記の実施の形態では、個人認証情報として生体情報を用いる生体認証を認証の一例として説明したが、これにとらわれるものではない。照合する個人認証情報は、個人を特定するための情報であればよい。また、照合処理として、暗証番号やパスワード等の個人情報からなるデータを照合するＰＩＮ照合、顔、指紋、虹彩、血流、ＤＮＡ等の人間固有の身体的特徴を使った照合、声紋やサインといった固有の身体的特性、行動特性を使った照合及びそれらを組み合わせた照合処理を利用できる。また、照合方法として、常に一定の決まったデータを入力する静的な方法、毎回入力するデータが異なる動的な方法（チャレンジレスポンス方式）及びそれらを組み合わせた方法を利用できる。

【００８６】
また、ＩＣカードは接触型、非接触型のいずれの形態であっても本発明の趣旨を実現可能であることは言うまでもない。更に、システム端末の記憶部は、端末に内蔵する形態にとらわれず、遠隔に接続されたデータベースやネットワーク上のデータサーバなどであってもかまわない。

【００８７】
尚、上記の実施の形態において、センサは通信線でシステム端末に接続する形態としたが、システム端末に内蔵する形態としてもよいし、また、図２３に示すように、ＩＣカード１０４に個人認証情報の読取手段４１が搭載された形態でも本発明を実現可能であるこ

とは言うまでもない。読取手段をカードに内蔵すれば、外部に一切個人認証情報が出ない為、セキュリティが向上する。

【産業上の利用可能性】

【００８８】

本発明のＩＣカード及びシステム端末は、比較結果に応じて、前記ＩＣカードの照合機能を用いた照合、前記システム端末の照合機能を用いた照合及び前記ＩＣカードと前記システム端末のそれぞれの照合機能を用いた照合から、前記個人認証情報の照合方法を選択する選択手段を備えることにより、比較結果に応じて適応的にＩＣカード内、ＩＣカード外及びＩＣカード内外の組み合わせのいずれかで照合処理できるため、システム側セキュリティとカードユーザ側セキュリティを両立した上で効率的な認証処理が行える効果を有し、予め定められた仕様に基づいてシステム端末とＩＣカードとの間で個人認証情報の照合に基づく認証処理を行う為のＩＣカード及び認証システム端末等に有用である。

【図面の簡単な説明】

【００８９】

【図１】本発明の実施の形態を説明するためのＩＣカードの構成を示す図

【図２】本発明の実施の形態を説明するためのシステム端末の構成を示す図

【図３】システム端末で仕様比較及び照合処理を行う場合の認証処理手順を示すシーケンス図

【図４】システム端末が仕様比較及び照合処理を行う場合にＩＣカードとシステム端末が備える最小限の構成を示す図

【図５】システム端末で仕様比較しＩＣカードで照合処理を行う場合の認証処理手順を示すシーケンス図

【図６】システム端末で仕様比較しＩＣカードで照合処理を行う場合にＩＣカードとシステム端末が備える最小限の構成を示す図

【図７】ＩＣカードの仕様の設定例を示す図

【図８】システム端末の仕様の設定例を示す図

【図９】仕様のデータ形式例を示す図

【図１０】システム端末から送信されるコマンドやカードからのレスポンスの具体例を示す図

【図１１】認証アルゴリズムの識別値を指すテーブル

【図１２】システム端末から送信されるコマンドの具体例を示す図

【図１３】システム端末から送信されるコマンドやカードからのレスポンスの具体例を示す図

【図１４】システム端末の仕様照合手段３０ａにおける仕様の比較手順例を示すフローチャート

【図１５】ＩＣカードで仕様比較及び照合処理を行う場合の認証処理手順を示すシーケンス図

【図１６】ＩＣカードが仕様比較及び照合処理を行う場合にＩＣカードとシステム端末が備える最小限の構成を示す図

【図１７】ＩＣカードの仕様照合手段における仕様の比較手順例を示すフローチャート

【図１８】ＩＣカードが仕様データを保持していない場合の認証処理手順を示すシーケンス図

【図１９】システム端末が仕様データを保持していない場合の認証処理手順を示すシーケンス図

【図２０】仕様比較を行う主体を切り替える場合の処理手順を示すシーケンス図

【図２１】抽出方法による認証処理手順を示すシーケンス図

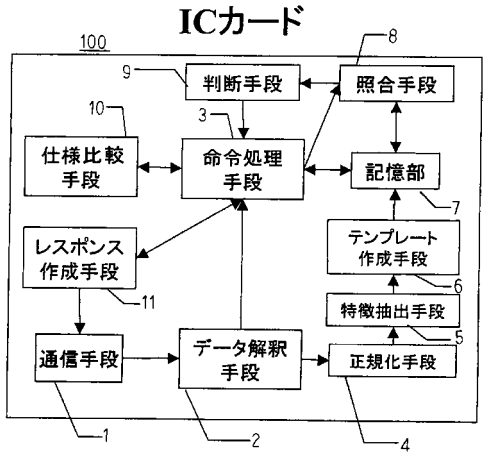
【図２２】抽出方法による仕様比較で使用されるコマンドとレスポンスの形式例を示す図

【図２３】ＩＣカードに読取手段が搭載された場合にＩＣカード及びシステム端末が備える最小限の構成を示す図

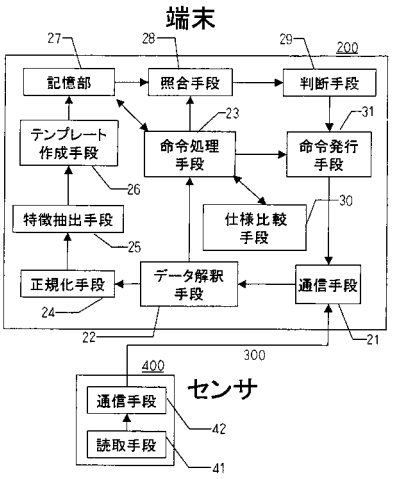
【符号の説明】

【００９０】
１０　仕様比較手段
１０ａ　仕様照合手段
１０ｂ　仕様確認手段
３０　仕様比較手段
３０ａ　仕様照合手段
３０ｂ　仕様確認手段
３２　表示手段
４１　読取手段
１００、１０１、１０２、１０３、１０４　ＩＣカード
２００、２０１、２０２、２０３、２０４　システム端末
３００　通信線
４００　センサ

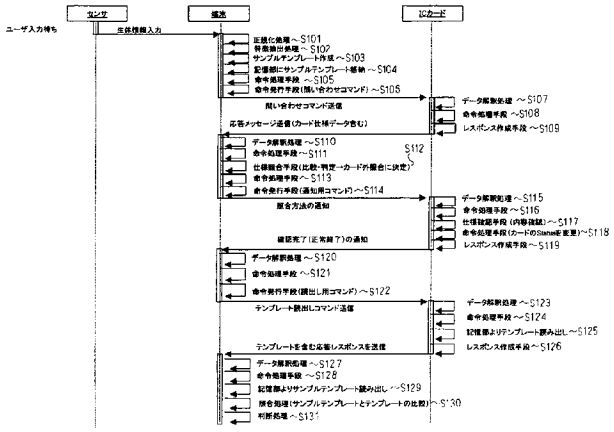
【図１】



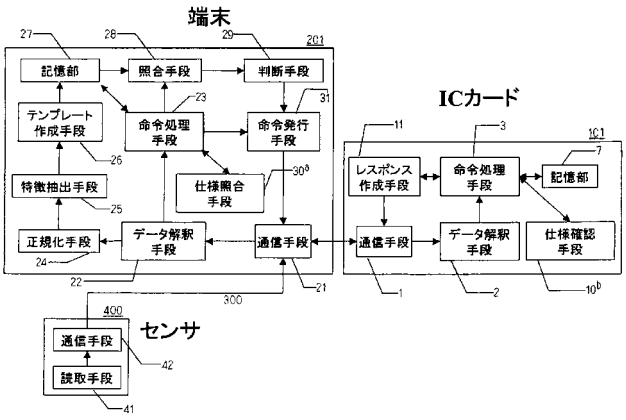
【図２】



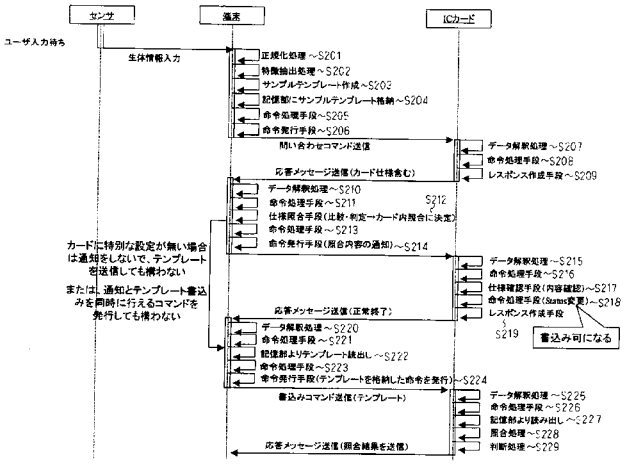
【図３】


センサ
端末
ICカード
ユーザ入力待ち
生体情報入力
正規化処理～S101
特徴抽出処理～S102
サンプルテンプレート作成～S103
記憶部にサンプルテンプレート格納～S104
命令処理手段～S105
命令発行手段(問い合わせコマンド)～S105
問い合わせコマンド送信
データ解釈処理～S107
命令処理手段～S108
レスポンス作成手段～S109
応答メッセージ送信(カード仕様データ含む)
データ解釈処理～S110
命令処理手段～S111
S112
仕様照合手段(比較・判定→カード内整合に決定)
命令処理手段～S113
命令発行手段(通知用コマンド)～S114
照合方法の通知
データ解釈処理～S115
命令処理手段～S116
仕様確認手段(内容確認)～S117
命令処理手段(カードのStatusを変更)～S118
レスポンス作成手段～S119
確認完了(正常終了)の通知
データ解釈処理～S120
命令処理手段～S121
命令発行手段(読出し用コマンド)～S122
テンプレート読出しコマンド送信
データ解釈処理～S123
命令処理手段～S124
記憶部よりテンプレート読み出し～S125
テンプレートを含む応答レスポンスを送信
レスポンス作成手段～S126
データ解釈処理～S127
命令処理手段～S128
記憶部よりサンプルテンプレート読み出し～S129
照合処理(サンプルテンプレートとテンプレートの比較)～S130
判断処理～S131

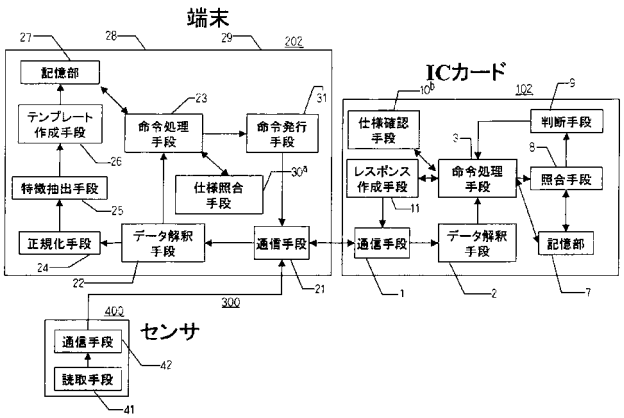
【図４】


端末
27
28
29
201
記憶部
照合手段
判断手段
テンプレート作成手段
命令処理手段
命令発行手段
23
31
26
特徴抽出手段
仕様照合手段
30b
25
正規化手段
データ解釈手段
通信手段
24
22
21
300
ICカード
11
3
101
7
レスポンス作成手段
命令処理手段
記憶部
通信手段
データ解釈手段
仕様確認手段
1
2
10b
センサ
400
通信手段
42
読取手段
41

【図５】


センサ
端末
ICカード
ユーザ入力待ち
生体情報入力
正規化処理～S201
特徴抽出処理～S202
サンプルテンプレート作成～S203
記憶部にサンプルテンプレート格納～S204
命令処理手段～S205
命令発行手段～S206
問い合わせコマンド送信
データ解釈処理～S207
命令処理手段～S208
レスポンス作成手段～S209
応答メッセージ送信(カード仕様含む)
データ解釈処理～S210
命令処理手段～S211
S212
仕様照合手段(比較・判定→カード内整合に決定)
命令処理手段～S213
命令発行手段(照合内容の通知)～S214
カードに特別な設定が無い場合は通知をしないで、テンプレートを送信しても構わない
または、通知とテンプレート書込みを同時に行えるコマンドを発行しても構わない
データ解釈処理～S215
命令処理手段～S216
仕様確認手段(内容確認)～S217
命令処理手段(Status変更)～S218
レスポンス作成手段
S219
書込み可になる
応答メッセージ送信(正常終了)
データ解釈処理～S220
命令処理手段～S221
記憶部よりテンプレート読出し～S222
命令処理手段～S223
命令発行手段(テンプレートを格納した命令を発行)～S224
書込みコマンド送信(テンプレート)
データ解釈処理～S225
命令処理手段～S226
記憶部より読み出し～S227
照合処理～S228
判断処理～S229
応答メッセージ送信(照合結果を送信)

【図６】


端末
27
28
29
202
記憶部
テンプレート作成手段
命令処理手段
命令発行手段
23
31
26
特徴抽出手段
仕様照合手段
30A
25
正規化手段
データ解釈手段
通信手段
24
22
21
300
ICカード
10b
102
9
仕様確認手段
判断手段
3
8
レスポンス作成手段
命令処理手段
照合手段
11
通信手段
データ解釈手段
記憶部
1
2
7
センサ
400
通信手段
42
読取手段
41

【図７】

仕様の概念とデータ形式例(カード側)

	大項目	小項目	データ形式	
カード	照合の種類	カード側が希望する認証手段	1byte:カード内照合、カード外照合、ハイブリッド照合、複数、マルチモーダル、クロス照合(両方で認証し結果を比較)、カード側の認証手段に合わせるなどが選択可能	
	カード内認証の性能に関する項目	認証アルゴリズム	3byte(バイオメトリクスタイプ(2byte)+フォーマット所有者(2byte))	
		FAR値(%)	3byte:整数部8bit/小数部16bit	
		FRR値(%)	3byte:整数部8bit/小数部16bit	
		処理速度(ms)	3byte(0～2^{24}-1:16777215ms)	
	外部に出力する際の要望、禁止、制約に関する項目	認証アルゴリズム	バイオメトリクスタイプ(2byte)+フォーマット所有者(2byte)	
		FAR値(%)	3byte:整数部8bit/小数部16bit	
		FRR値(%)	3byte:整数部8bit/小数部16bit	
		処理速度(ms)	3byte(0～2^{24}-1:16777215ms)	
		暗号通信	1byte:1bitで暗号通信の有無 7bitで暗号通信の種類	
		カード側が要求するテンプレートの管理方法	出力時のテンプレートの扱い方	・出力してはいけない ・一部を出力しても良い ・全部を出力しても良い ・暗号化するなら出力しても良い ・ユーザの許可があれば出力しても良い ・中間テンプレートは出力可能(カード内でテンプレート作成できる場合のみ)
			出力後のテンプレートの扱い方(各項目を割り当てて1byteで表す。最大256種類。)	・使用後削除 ・使用後DB保管 ・使用後暗号化してDB保管 ・使用後サーバに転送して保管 ・使用後テンプレートの一部のみを保管 ・使用後サーバと端末で分割して保管 ・システム(端末を含む)側の仕様に任せる
	ハイブリッド照合の場合 :システム(端末を含む)で照合する場合は、カードでどこまで処理可能であるかを提示し、カードで照合する場合は、カードが受取り可能なデータ形式を提示するための項目	認証アルゴリズムの種類	バイオメトリクスタイプ(2byte)+フォーマット所有者(2byte)	
		受け取り可能な処理形態: システム側(端末を含む)で照合する場合とカード側で照合する場合の2パターンがある	システム(端末を含む)で照合	・・・・(内容は端末側の仕様ほぼ同じ)
			カードで照合	・・・・(内容は端末側の仕様とほぼ同じ)
	マルチモーダル照合	評価基準	種類ごとの優先度や決定権をもつ認証アルゴリズム等を16進数にて記載する	
	カードの権限	判断基準	最終判断をカードが持つか持たないかを記述する(アプリケーションごとに設定可能)	
	カードの構成	ハードウエア/センサ構成	仕様比較手段の有無/センサ内蔵か/メモリサイズ(Flashやe2PROMサイズ)/CPU Hz数	

【図８】

仕様の概念とデータ形式例(端末側)

	大項目	小項目	データ形式	
端末	照合の種類	システム(端末を含む)が希望する認証手段	1byte:カード内照合、カード外照合、ハイブリッド照合、複数、マルチモーダル、クロス照合(両方で認証し結果を比較)、カード側の認証手段に合わせるなどが選択可能	
	システム(端末を含む)内照合の場合(カード外照合):カードが了承できる機能であるかを公開する項目	認証アルゴリズムの種類	3byte(バイオメトリクスタイプ(3byte)+フォーマット所有者(2byte)):複数対応もここに記入	
		認証精度:FAR値(%)	3byte:整数部8bit/小数部16bit	
		認証精度:FRR値(%)	3byte:整数部8bit/小数部16bit	
		処理速度(ms)	3byte(0～2^{24}-1:16777215ms)	
		システム(端末を含む)側が実施するテンプレートの管理方法(1byteを各項目を16進数に割り当てて最大256種類表す。)	・使用後削除 ・使用後DB保管 ・使用後暗号化してDB保管 ・使用後サーバに転送して保管 ・使用後テンプレートの一部のみを保管 ・使用後サーバと端末で分割して保管 ・テンプレートの管理方法はカードの仕様に任せる	
	カード内照合の場合:カードの機能をチェックするための項目	要求認証アルゴリズムの種類	バイオメトリクスタイプ(3byte)+フォーマット所有者(2byte)	
		要求認証精度:FAR値(%)	3byte:整数部8bit/小数部16bit	
		要求認証精度:FRR値(%)	3byte:整数部8bit/小数部16bit	
		要求処理速度(ms)	3byte(0～2^{24}-1:16777215ms)	
		暗号通信の有無	1byte:1bitで暗号通信の有無 7bitで暗号通信の種類	
	ハイブリッド照合の場合:システム(端末を含む)で照合する場合は、処理可能であるデータ形式を提示し、カードで照合する場合は、カードには出力可能なデータ形式を提示するための項目	認証アルゴリズムの種類	バイオメトリクスタイプ(3byte)+フォーマット所有者(2byte)	
		受け取り可能な処理形態: システム(端末を含む)側で照合する場合とカード側で照合する場合の2パターンがある	システム(端末を含む)で照合	・カードで正規化だけ ・カードで正規化＋特徴抽出まで ・カードで特徴抽出だけ ・カードで特徴抽出＋一部のテンプレート作成まで ・カードでテンプレート作成だけ
			カードで照合	・システム(端末を含む)で正規化だけ ・システム(端末を含む)で正規化＋特徴抽出 ・システム(端末を含む)で特徴抽出 ・システム(端末を含む)で特徴抽出＋一部のテンプレート作成
	マルチモーダル照合	評価基準	種類ごとの優先度や決定権をもつ認証アルゴリズム等を16進数にて記載する	
	端末の権限	判断基準	最終判断を端末が持つかを記述する。(アプリケーションごとに設定可能)	
	システムの構成(端末を含む)	ハードウエア/センサ構成	仕様比較手段の有無/センサ内蔵か/センサ接続状況/DBの有無/ネットワーク接続の有無	

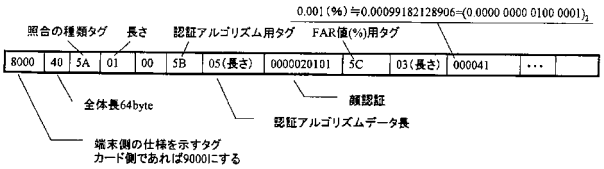
【図９】

仕様のデータ形式例

■TLV形式にてデータを保持

Tag	Length	Tag	Length	Value	Tag	Length	Value	…	

■種類のそれぞれにTagを割り当て、端末-カード間で共有する



【図１０】

■端末がカードに送信するデータ形式
カード内の特定のファイル(仕様を含む)を読み出すコマンド

00B0 009F 40 (a)

ISO7816-4にて規定されているRead Binaryコマンド(00B0)を使用

■カードが端末に仕様を返信するデータ形式

9000 3D 5A **01** 00 5B05 **0000100005** 5C03 **000006** 5E03 **0003E8** ・・・・・・・・・・・・・・ 9000 (b)

正常終了

0.0001(%)≒0.000091552734375 = $(0.00000000\ 00000110)_2$

1(s) = 1000(ms)= $(00000000\ 00000011\ 11101000)_2$

※応答レスポンスデータの説明
9000(カード仕様を表すTag)+全体長(61byte)+5A(認証の方法を表すTag)+長さ(1byte)+00(カード内認証)
+5B(認証アルゴリズムを表すTag)+長さ(5byte)+0000100005(E社の虹彩認証)+5C(認証精度FARを表すTag)+
長さ(3byte)+000006(0.0001%を示す16進数)+・・・・・・・・+9000(正常終了を示す16進)

■端末で仕様の比較し、照合方法をカードに通知するためのコマンド

00D0 0000 80 8001 1A 6A **01** 00 6B05 **0000100005** 6C 03 **000006** 6E 03 **0003E8** 6F 01 **00** FE 01 **00** (c)

照合結果通知データ

【図１１】

バイオメトリクスタイプ名	識別値
複数認証適用	0001
顔	0010
音声	0100
指紋	1000
虹彩	00010000
網膜	00100000
腕の幾何学的情報	01000000
署名	10000000
キーストローク	0001000000000
唇の動き	0010000000000
顔の温度イメージ	0100000000000
手の温度イメージ	1000000000000
歩き方	0001000000000000
体臭	0010000000000000
DNA	0100000000000000
耳形	1000000000000000
指の幾何学的情報	0000100000000000000000
手のひらの幾何学的情報	0001000000000000000000
静脈パターン	0010000000000000000000

0001	A社
0002	B社
0003	C社
0004	D社
0005	E社
・・・・	
1111	標準化団体A
・・・・	
EEEE	プライベート利用(実験用)
FFFF	使わない

【図１２】

■カード外照合の場合:カードに照合方法を通知し、確認を得た後、テンプレートを読み出すコマンドを送信する。
カードに照合方法を通知し正常終了(9000)を得た後、端末は、テンプレート読出しコマンドを送信する。

00B0 00EE 80 (a)

ISO7816-4にて規定されているRead Binaryコマンド(00B0)を使用

■カード内照合の場合:端末がサンプルテンプレートをカードに送信する

00D0 0000 80 0102030405060708090a0b0c0d0e0f101112131415161718191A1B・・・ (b)

サンプルテンプレートデータ(例)

ISO7816-4にて規定されているWrite Binaryコマンド(00D0)を使用

【図１３】

■端末がカードに仕様を送信するデータ形式

00D0 0000 42 8000 40 5A01 **00** 5B05 **0000020101** 5C03 **000041**・・・・ (a)

ISO7816-4にて規定されているWrite Binaryコマンド(00D0)を使用

■カードが端末に結果を応答するデータ形式(通知用レスポンス)

9001 1A 6A **01** 00 6B05 **0000100005** 6C03 **000006** 6E03 **0003E8** 6F01 **00** FE01 **00** 9000 (b)

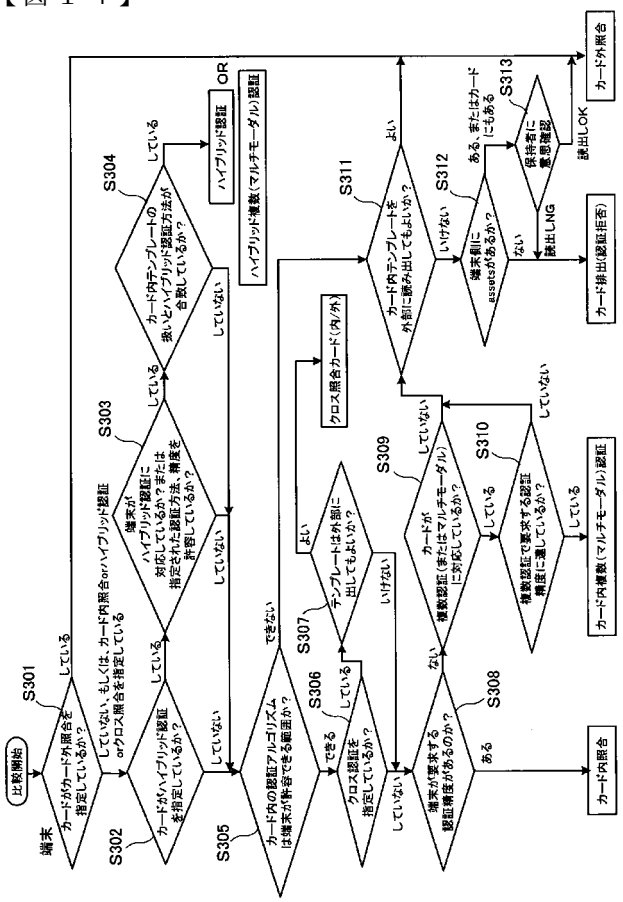
正常終了

0.0001(%)≒0.000091552734375 = $(0.00000000\ 00000110)_2$

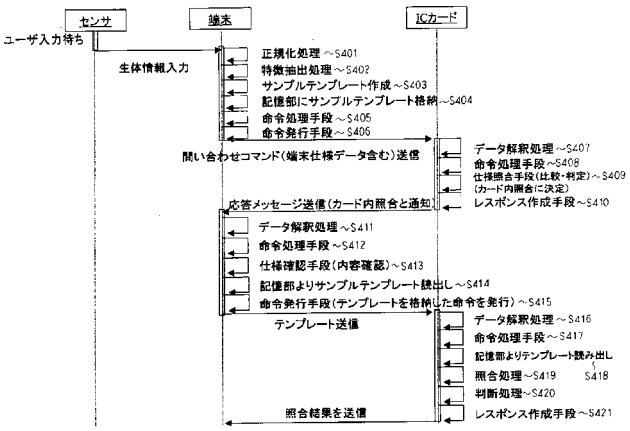
1(s) = 1000(ms)= $(00000000\ 00000011\ 11101000)_2$

※応答レスポンスデータの説明
9001(カードからの応答を表すTag)+全体長(28byte)+6A(認証の方法を表すTag)+長さ(1byte)+00(カード内認証)
+6B(認証アルゴリズムを表すTag)+長さ(5byte)+0000100005(E社の虹彩認証)+6C(認証精度FARを表すTag)+
長さ(3byte)+000006(0.0001%を示す16進数)+6E(処理速度を表すTag)+長さ(3byte)+0003E8(1秒を示す16進数)
+6F(暗号通信を表すTag)+長さ(1byte)+00(暗号化しない)+FE(テンプレートの扱い方を表すTag)+長さ(1byte)
+00(出力してはいけないを示す:カード内照合なので、関係ない)+9000(正常終了を示す16進)

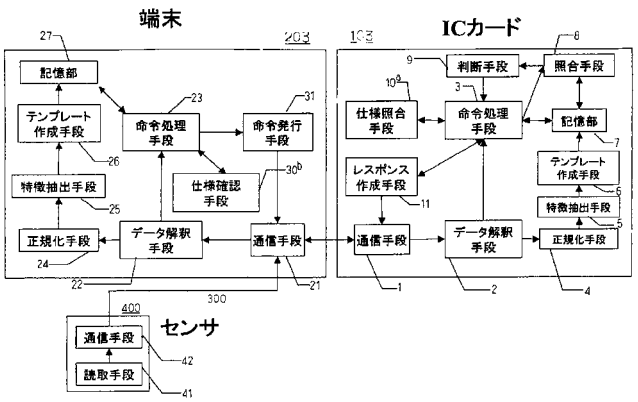
【図１４】



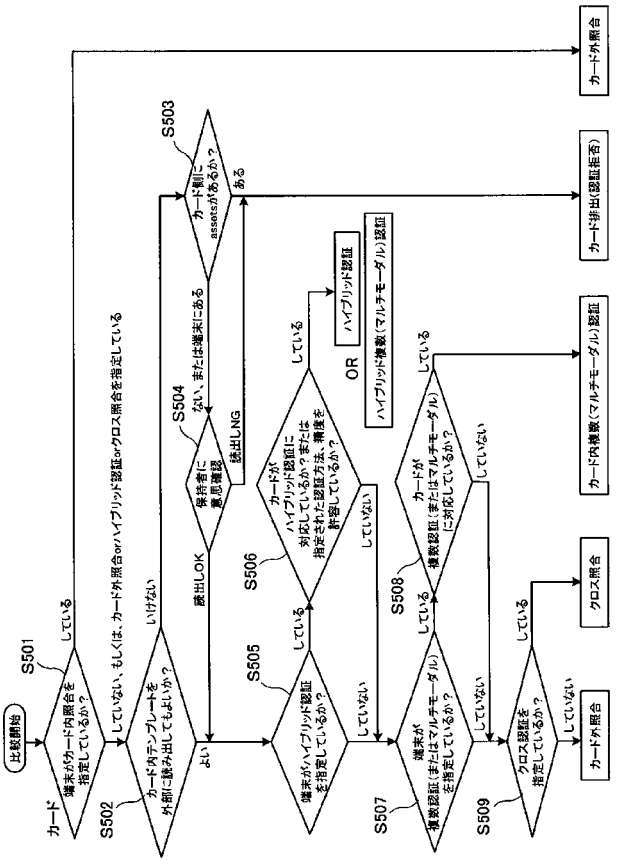
【図１５】



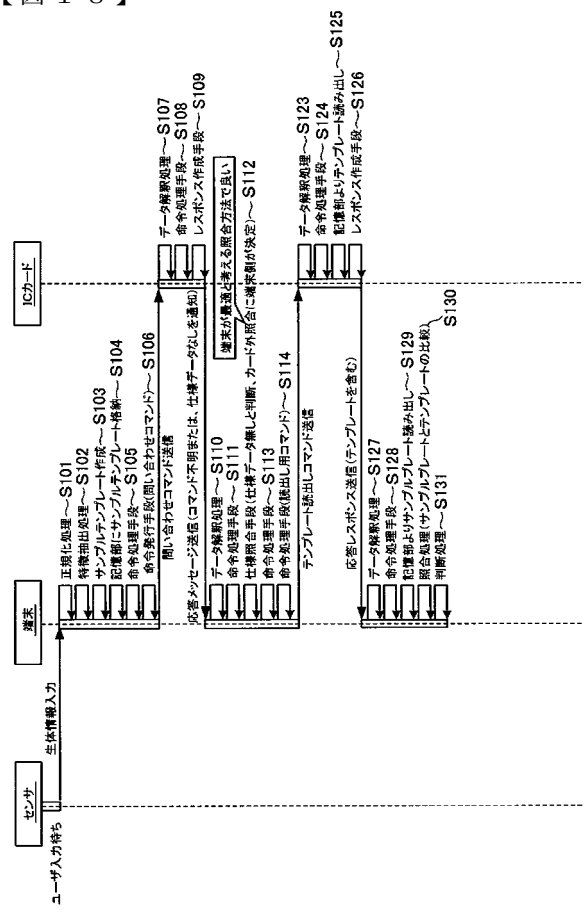
【図１６】



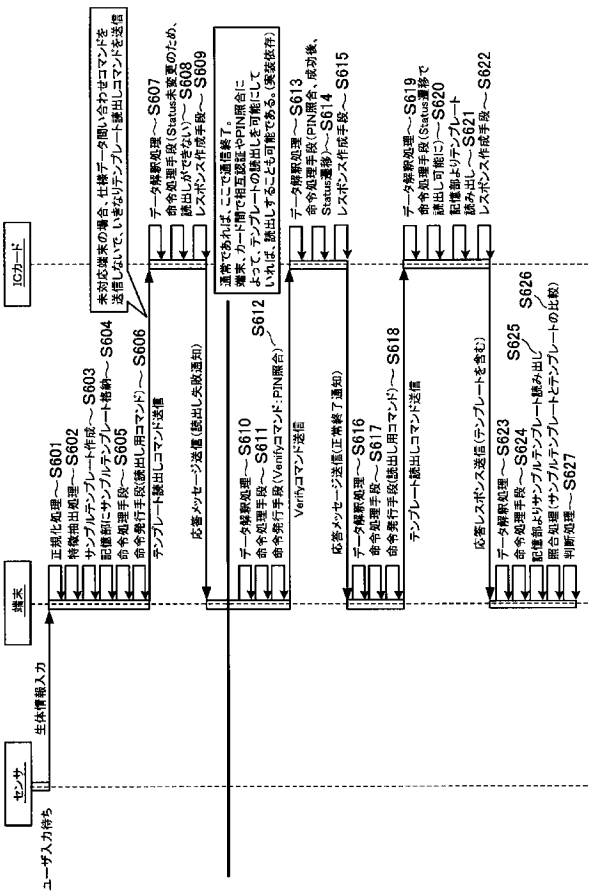
【図１７】



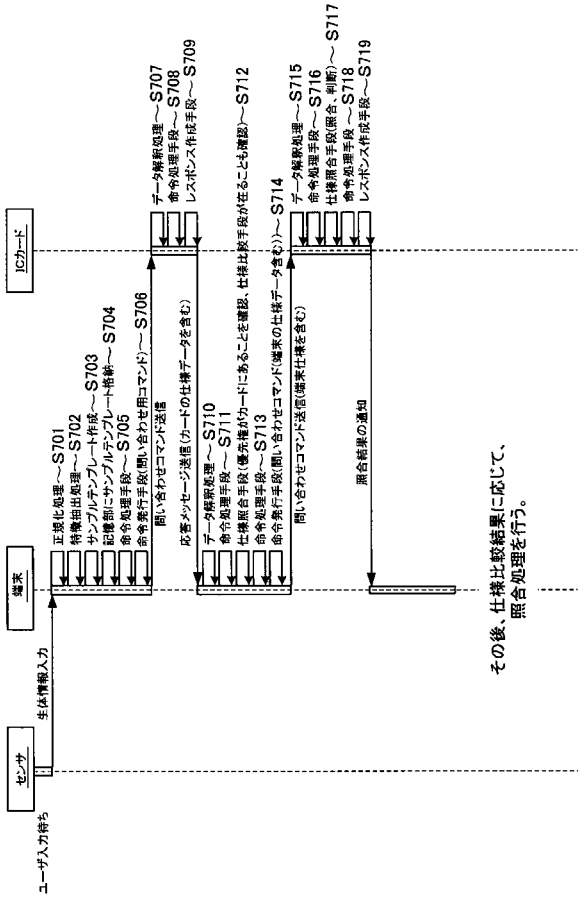
【図１８】



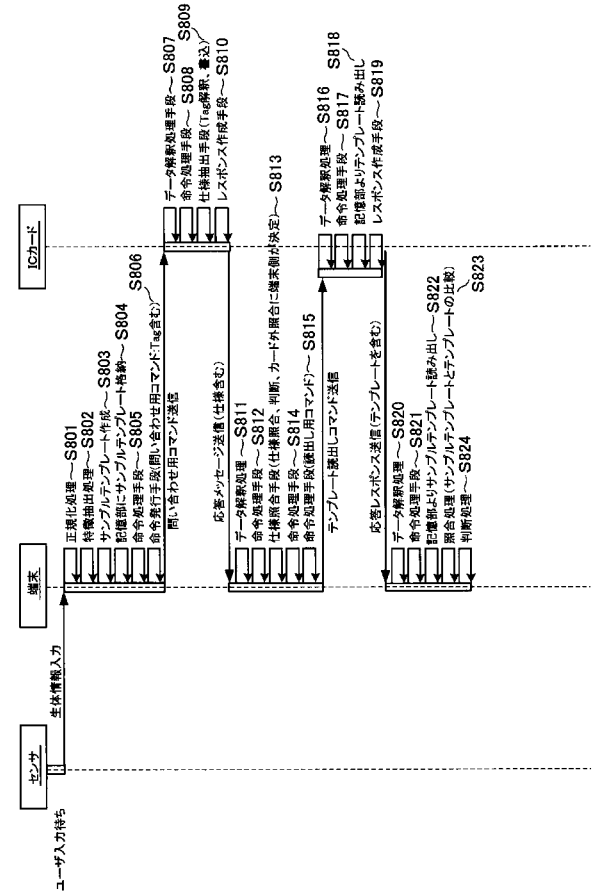
【図１９】



【図２０】

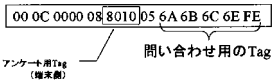


【図２１】



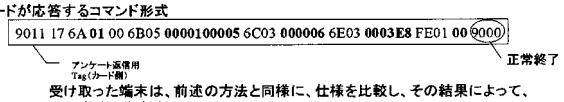
【図２２】

■端末が送信するコマンド形式



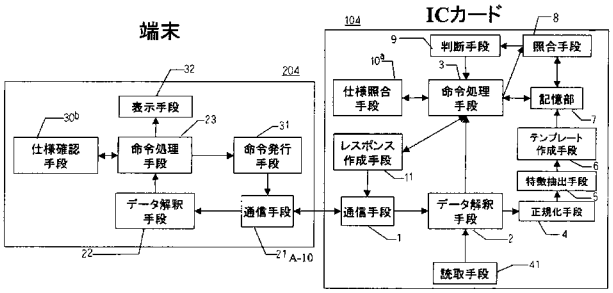
新規コマンドを定義。このコマンドを送信後、受信側はTagに対応する値を繋げて、応答レスポンスとして、以下を返信する。

■カードが応答するコマンド形式



受け取った端末は、前述の方法と同様に、仕様を比較し、その結果によって、照合方法を決定する。

【図２３】



フロントページの続き

(72)発明者　竹内　康雄
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　井上　和紀
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) 2C005 MA05 MB01 SA06
5B035 AA13 BB09 CA38
5B058 CA01 KA31
5J104 AA07 KA01 KA04 NA05 NA35 NA38