(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2019-4475
(P2019-4475A)
(43)公開日　平成31年1月10日(2019.1.10)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	673C	5J104
H04L 9/08	(2006.01)	H04L	9/00	601F	
H04L 9/14	(2006.01)	H04L	9/00	673D	
G06F 21/32	(2013.01)	H04L	9/00	641	
G06F 21/44	(2013.01)	G06F	21/32		

審査請求 有　請求項の数 13　ＯＬ　（全 40 頁）　最終頁に続く

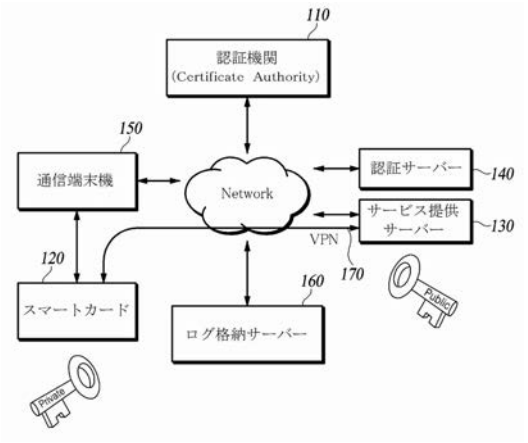
(21)出願番号　特願2018-143028 (P2018-143028)
(22)出願日　平成30年7月31日 (2018.7.31)
(62)分割の表示　特願2017-555598 (P2017-555598)の分割
原出願日　平成27年4月23日 (2015.4.23)

(71)出願人　517365186
チェ　ウノ
大韓民国　１３９－８４０，　ソウル，ノウォン－グ，　マドゥル－ロ１１１，３１－９１０
(74)代理人　100166006
弁理士　泉　通博
(74)代理人　100154070
弁理士　久恒　京範
(74)代理人　100153280
弁理士　寺川　賢祐
(72)発明者　チェ　ウノ
大韓民国　１３９－８４０，　ソウル，ノウォン－グ，　マドゥル－ロ１１１，３１－９１０

最終頁に続く

(54)【発明の名称】ユビキタス環境での認証

(57)【要約】　（修正有）
【課題】より強化されたサービス認証機能を提供する。
【解決手段】公開キー認証書に基づいて暗号化された生体情報をユーザーが保有または所持する装置（例：スマートカード、通信端末機など）に前もって格納しておき、装置内で生体マッチングを介するユーザー認証（１次ユーザー認証）を行う。サービス提供サーバーで行われる取引承認などのためのユーザー認証（２次ユーザー認証）のために、暗号化された生体情報にマッチングする公開キー認証書を用いる。１次・２次ユーザー認証のセキュリティーを強化するための追加的な認証要素として、Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ、キーストローク（Ｋｅｙｓｔｒｏｋｅ）、動的署名（Ｄｙｎａｍｉｃ　Ｓｉｇｎａｔｕｒｅ）、位置情報などを採用する。
【選択図】図１ａ



【特許請求の範囲】
【請求項１】
公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置によって行われるユーザー登録方法において、
前記公開キー認証書に規定された暗号化アルゴリズムを用いてユーザーの生体情報または生体情報の組合せを暗号化し、暗号化された生体情報を前記携帯用装置内に格納する工程と、
前記暗号化された生体情報または生体情報の組合せをトークン化して生体コードを生成する工程と、
前記公開キー認証書の拡張フィールドに少なくとも前記生体コードを含む検証コードを挿入して一つのキーペアー（個人キー及び公開キーを含む）を生成する工程と、
前記公開キーを遠隔客体に転送し、前記ユーザーの登録を要請する工程と、
を備える、
ユーザー登録方法。
【請求項２】
前記検証コードは、前記携帯用装置に与えられた固有識別情報を暗号化し、暗号化された固有識別情報をトークン化して生成された追加コードをさらに含む、
請求項１に記載のユーザー登録方法。
【請求項３】
前記検証コードは、前記ユーザーの行動特性を表す特性情報を暗号化し、暗号化された特性情報をトークン化して生成された追加コードをさらに含む、
請求項１に記載のユーザー登録方法。
【請求項４】
前記検証コードは、前記ユーザーの認証を要請する位置を表す位置情報を暗号化し、暗号化された位置情報をトークン化して生成された追加コードをさらに含む、
請求項１に記載のユーザー登録方法。
【請求項５】
前記検証コードは、前記ユーザーに与えられた固有識別情報を暗号化し、暗号化された固有識別情報をトークン化して生成された追加コードをさらに含む、
請求項１に記載のユーザー登録方法。
【請求項６】
複数の公開キー認証書にそれぞれ異なる生体情報または異なる生体情報の組合せから得られた生体コードを挿入して公開キー認証書ごとに一つのキーペアーを生成する、
請求項１に記載のユーザー登録方法。
【請求項７】
前記複数の公開キー認証書は使用用途が互いに異なる、
請求項６に記載のユーザー登録方法。
【請求項８】
前記一つのキーペアーを生成する工程は、
前記生体コードの生成に用いられた生体情報または生体情報の組合せとは異なる生体情報または生体情報の組合せから追加的な生体コードを生成する工程と、
前記公開キー認証書の拡張フィールドに少なくとも前記追加的な生体コードを含む追加的な検証コードをさらに挿入して一つのキーペアー（個人キー及び公開キーを含む）を生成する工程と、
を含む、
請求項１に記載のユーザー登録方法。
【請求項９】
前記追加的な検証コードは、他人からの強制による前記個人キーの使用であることを知らせるための用途に指定する、
請求項８に記載のユーザー登録方法。

【請求項１０】
前記追加的な検証コードは、既に転送された公開キーに基づいたユーザー登録を解除することを要請する用途に指定する、
請求項８に記載のユーザー登録方法。
【請求項１１】
前記追加的な検証コードは、前記遠隔客体によって管理される認証管理システムの初期化を要請する用途に指定する、
請求項８に記載のユーザー登録方法。
【請求項１２】
前記公開キー認証書の拡張フィールドには、前記公開キー認証書の指定した使用目的に対応する追加情報として、電子身分証明書、運転免許証、電子貨幣、及び医療カードのうち少なくとも一つに関するデータをさらに含む、
請求項１に記載のユーザー登録方法。
【請求項１３】
前記公開キー認証書の拡張フィールドには、前記公開キーを転送する遠隔客体のＵＲＬ情報を含む、
請求項１に記載のユーザー登録方法。
【請求項１４】
ＩｏＴデバイスに与えられたデバイス識別情報を暗号化し、暗号化されたデバイス識別情報をトークン化して生成された追加コードをさらに含む、
請求項１に記載のユーザー登録方法。
【請求項１５】
複数の公開キー認証書にそれぞれ異なる生体情報または異なる生体情報の組合せから得られた生体コード及び異なるＩｏＴデバイスのデバイス識別情報から得られた追加コードを挿入して、ＩｏＴデバイスごとに関連する一つのキーペアーを生成する、
請求項１４に記載のユーザー登録方法。
【請求項１６】
前記公開キーの転送には、仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いる、
請求項１に記載のユーザー登録方法。
【請求項１７】
前記携帯用装置は、スマートカードまたは移動通信端末機である、
請求項１に記載のユーザー登録方法。
【請求項１８】
公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置によって行われるユーザー認証方法において、前記携帯用装置は生体コードを含む検証コードが挿入された個人キー及び前記生体コードが得られた暗号化された生体情報または生体情報の組合せが格納されており、前記ユーザー認証方法は、
ユーザーの生体情報または生体情報の組合せを獲得する工程と、
前記ユーザーの生体情報または生体情報の組合せを前記携帯用装置に既に格納されている暗号化された生体情報及び前記生体コードのうち少なくとも一つと比較する工程と、
前記ユーザーの生体情報または生体情報の組合せが、前記暗号化された生体情報及び前記生体コードのうち少なくとも一つとマッチングすると、前記個人キーに挿入された検証コードを含む認証情報を遠隔客体に転送して前記ユーザーの認証を要請する工程と、
を備える、
ユーザー認証方法。
【請求項１９】
前記個人キーに挿入された検証コードは、前記携帯用装置に与えられた固有識別情報から得られた追加コード、前記ユーザーの認証を要請する位置を表す位置情報から得られた追加コード、前記ユーザーに与えられた固有識別情報から得られた追加コード、前記ユー

ザーの行動特性を表す特性情報から得られた追加コード、及びＩｏＴデバイスに与えられたデバイス識別情報から得られた追加コードのうち少なくとも一つをさらに含む、
請求項１８に記載のユーザー認証方法。
【請求項２０】
前記認証情報は、前記携帯用装置に内蔵されたＯＴＰ生成モジュールによって生成されたＯＴＰをさらに含む、
請求項１８に記載のユーザー認証方法。
【請求項２１】
前記認証情報は、前記認証情報の転送時点に関する情報をさらに含む、
請求項１８に記載のユーザー認証方法。
【請求項２２】
前記認証情報は、前記ユーザーの認証を要請する位置に関する情報をさらに含む、
請求項１８に記載のユーザー認証方法。
【請求項２３】
前記認証情報は、前記個人キーの生成時点に関する情報をさらに含む、
請求項１８に記載のユーザー認証方法。
【請求項２４】
前記認証情報の転送には、仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いる、
請求項１８に記載のユーザー認証方法。
【請求項２５】
前記仮想私設網の目的地ＵＲＬは、前記個人キーの拡張フィールドに含まれている、
請求項１８に記載のユーザー認証方法。
【請求項２６】
前記携帯用装置は、スマートカードまたは移動通信端末機である、
請求項１８に記載のユーザー認証方法。
【請求項２７】
公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置とネットワークで接続される遠隔客体によって行われる認証管理方法において、
前記携帯用装置からユーザーの生体情報または生体情報の組合せから得られた生体コードを含む検証コードが挿入された個人キーに対応する公開キーを受信し、受信した公開キーに基づいてユーザー登録を行う工程と、
前記携帯用装置から前記個人キーに挿入された検証コードを含む認証情報を受信し、前記公開キーを用いて受信した認証情報を検証し、検証結果に基づいて前記ユーザーの認証を行う工程と、
を備える、
認証管理方法。
【請求項２８】
公開キー認証書に基づいた認証管理システムでサービスを提供する公用端末機及び前記公用端末機を管理するサービス提供サーバーによって行われる認証管理方法において、
前記サービス提供サーバーが、携帯用装置からユーザーの生体情報または生体情報の組合せから得られた生体コードを含む検証コードが挿入された個人キーに対応する公開キーを受信し、受信した公開キーに基づいてユーザー登録を行う工程と、
前記公用端末機が、前記携帯用装置から前記個人キーに挿入された検証コードを含む認証情報を受信し、受信した認証情報の前記公開キーを用いた検証を前記サービス提供サーバーに要請し、前記検証の結果に基づいて前記ユーザーの認証を行う工程と、
前記ユーザーの認証に成功すると、前記公用端末機がサービスを提供する工程と、
を備える、
認証管理方法。
【請求項２９】

前記ユーザー登録を行う工程は、前記公用端末機と前記サービス提供サーバーが互いにオフライン状況におかれた場合に使用するための用途で、前記サービス提供サーバーが前記公開キーを応用した変形公開キーを生成し、前記変形公開キーを前記携帯用装置に伝達する工程を含む、

請求項２８に記載の認証管理方法。

【請求項３０】

前記公用端末機と前記サービス提供サーバーが互いにオフライン状況におかれると、前記公用端末機が前記携帯用装置から前記個人キーに挿入された検証コード及び前記変形公開キーに挿入された検証コードを受信し、受信した検証コードが同一の公開キー認証書に基づいて生成されたものか否かを検証し、検証成功すると、オンライン状況より制限された範囲のサービスを提供する工程と、

前記オフライン状況がオンライン状況に変わると、前記公用端末機が前記検証コード及びサービス提供情報を前記サービス提供サーバーに伝達し、前記サービス提供サーバーが前記検証コードを検証し、検証結果に基づいて前記サービス提供情報を生産する工程と、

をさらに備える、

請求項２９に記載の認証管理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、オンライン・オフライン認証を含むユビキタス環境でのユーザーの認証及びＩｏＴデバイスの認証に関する。

【背景技術】

【０００２】

この部分に記述した内容は単に本発明の実施例に係る背景情報を提供するのみであって、従来技術を構成するものではない。

【０００３】

産業全般にわたって、モノのインターネット（ＩｏＴ）の活用が論議されている。例えば、個人で使用する装置であるスマートＴＶ、ロボット掃除機、自動車のナビゲーション、そしてクラウドサービスが提供する様々な遠隔サービスのみならず、ダム、原発などといった、人が直接アクセスしづらい施設に対する遠隔管理・管制、交通制御システムにもＩｏＴの活用が試みられている。しかし、通信機能とともにデータを自ら確保して処理する機能が搭載されるＩｏＴデバイス及びＩｏＴシステムは、使用する主体及び所有者との関係が明確でないので、サイバー攻撃の的になり得る。

【０００４】

特に、現在ＩｏＴネットワークを構成するＩｏＴデバイスは、大体コンピューティング機能が単純でセキュリティー性も弱い場合が多いので、外部からの攻撃に弱い状態である。ＩｏＴネットワークの特性上、特定分野のセキュリティーの脆弱性及びこれを狙ったサイバー攻撃が他の産業分野にまで悪影響を及ぼすという副作用も起こり得る。

【０００５】

簡単な通信機能のみを搭載したＩｏＴデバイスの場合、個別的にセキュリティー・ソフトウェア（ＳＷ）をインストールして稼働させることは不可能なので、ＩｏＴデバイスにセキュリティー・ハードウェア（ＨＷ）モジュールを内蔵するか、または全体のシステムにセキュリティー・ソリューションを適用するなど、別途の工夫が必要である。ＩｏＴのセキュリティーが問題になる例として、ＩｏＴデバイスやネットワークに悪性コードが入れられ、大事な情報を流出させられるか、または偽造・変造されてシステムに障害をもたらし、攻撃者に遠隔で自由に操られてしまうという状況が挙げられる。特に、代表的な例として、悪性コードに感染した端末機がネットワークに接続すると、大変深刻な被害をもたらすことができることが挙げられる。例えば、無人自動車・電気自動車・スマート自動車を遠隔で制御して事故を起こし、病院の医療装置に誤作動を起こして患者の命をおびやかすなどの状況が発生し得る。

【０００６】
ＩｏＴネットワークでは、ＩｏＴデバイスの無欠性が保障されるべきであり、ネットワークに信頼できるＩｏＴデバイスが接続するのか否かを透明にすべきであり、正当なユーザーが端末やネットワークを利用しているのかを確認できなければならない。
【０００７】
従来の情報保護関連システムでは、不法なユーザーが正当なユーザーの個人情報、パスワード（ＰＷ）、生体情報などを取得し、ハッキングに用いてきた。他の脆弱例としては、認証機関（Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ）が発行した公開キー認証書に事実上の個人認証情報が収録されてないことから、公開キー認証書と認証書のＰＷさえ盗めば他人が無断で使用できるという脆弱性があった。さらに、ユーザーに関するＩＤ・ＰＷあるいは生体情報などの盗用された認証情報を知っている状況で遠隔で正当な端末機を用いて会社や政府機関などの業務システムにアクセスすると、何の問題もなく業務システムを自由に利用できるという問題があった。道で拾った従業員のＩＣチップでできた電子身分証明書さえあれば、写真などを盗用して正常な会社の出入口ゲートで認可されたユーザーのように使用できるという問題が、物理的なセキュリティー問題の代表的な例である。さらに、ＩＤ、ＰＷ、生体情報、トークン、ＯＴＰ、そしてＰＫＩ認証書を統合してＭｕｌｔｉ－Ｆａｃｔｏｒ認証として使用せずに、それぞれを個別的に使用して途中でハッカーが変更・偽造などの方法で使用するハッキングの例がメディアに報道されている。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明の実施例は、オンライン・オフライン認証を含むユビキタス環境でのユーザーの認証及びＩｏＴデバイスの認証と関連する方法、これを用いる装置及び認証システム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】
【０００９】
本発明の少なくとも一つの実施例においては、公開キー認証書に基づいて暗号化された生体情報をユーザーが保有または所持する装置（例えば、スマートカード、通信端末機など）に事前に格納しておき、装置内で生体マッチングを介したユーザー認証（１次ユーザー認証）を行う。さらに、サービス提供サーバーで行われる取引承認などのためのユーザー認証（２次ユーザー認証）のため、暗号化された生体情報にマッチングする公開キー認証書を用いる。また、本発明の少なくとも一つの実施例においては、１次・２次ユーザー認証のセキュリティーを強化するための追加的な認証要素（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆａｃｔｏｒ）として、Ｏｎｅ Ｔｉｍｅ Ｐａｓｓｗｏｒｄ（ＯＴＰ）、Ｋｅｙｓｔｒｏｋｅ、動的署名（Ｄｙｎａｍｉｃ Ｓｉｇｎａｔｕｒｅ）、位置情報などを採用する。さらに、本発明の少なくとも一つの実施例においては、ＩｏＴデバイスに対するアクセスを制御する場合に、１次ユーザー認証及び２次ユーザー認証で構成された認証メカニズムを応用する。
【００１０】
本発明の少なくとも一つの実施例においては、公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置によって行われるユーザー登録方法において、公開キー認証書に規定された暗号化アルゴリズムを用いてユーザーの生体情報または生体情報の組合せを暗号化し、暗号化された生体情報を携帯用装置内に格納する工程を含むユーザー登録方法を提供する。この方法は、暗号化された生体情報または生体情報の組合せをトークン化して生体コードを生成する工程、及び公開キー認証書の拡張フィールドに少なくとも生体コードを含む検証コードを挿入して一つのキーペアー（個人キー及び公開キーを含む）を生成する工程をさらに含む。この方法は、公開キーを遠隔客体に転送してユーザーの登録を要請する工程をさらに含む。
【００１１】
本発明の少なくとも一つの実施例において、公開キー認証書の領域には、生体コードの

他に携帯用装置に与えられた固有識別情報から得られた追加コード、ユーザーの認証を要請する位置を表す位置情報から得られた追加コード、ユーザーに与えられた固有識別情報から得られた追加コード、及びユーザーの行動特性を表す特性情報から得られた追加コード、ＩｏＴデバイスに与えられたデバイス識別情報から得られた追加コードのうち少なくとも一つをさらに含むことができる。

【００１２】

本発明の少なくとも一つの実施例においては、公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置によって行われるユーザー認証方法において、携帯用装置には、生体コードを含む検証コードが挿入された個人キー及び生体コードが得られた暗号化された生体情報または生体情報の組合せが格納されており、ユーザー認証方法は、ユーザーの生体情報または生体情報の組合せを獲得する工程と、ユーザーの生体情報または生体情報の組合せを携帯用装置に前もって格納されている暗号化された生体情報及び生体コードのうち少なくとも一つと比較する工程を含む。この方法は、ユーザーの生体情報または生体情報の組合せが暗号化された生体情報及び生体コードのうち少なくとも一つとマッチングされる場合、個人キーに挿入された検証コードを含む認証情報を遠隔客体に転送してユーザーの認証を要請する工程をさらに含む。

【００１３】

本発明の少なくとも一つの実施例においては、公開キー認証書に基づいた認証管理システムで、ユーザーが保有する携帯用装置とネットワークで接続される遠隔客体によって行われる認証管理方法において、認証管理方法は、携帯用装置から生体コードを含む検証コードが挿入された個人キーに対応する公開キーを受信し、受信した公開キーに基づいてユーザー登録を行う工程を含む。ここで、生体コードは、ユーザーの生体情報または生体情報の組合せから得られたものである。この認証管理方法は、携帯用装置から個人キーに挿入された検証コードを含む認証情報を受信し、公開キーを用いて受信した認証情報を検証し、検証結果に基づいてユーザーの認証を行う工程をさらに含む。

【００１４】

本発明の少なくとも一つの実施例においては、公開キー認証書に基づいた認証管理システムで、サービスを提供する公用端末機及びこれを管理するサービス提供サーバーによって行われる認証管理方法において、認証管理方法は、サービス提供サーバーが携帯用装置から生体コードを含む検証コードが挿入された個人キーに対応する公開キーを受信し、受信した公開キーに基づいてユーザー登録を行う工程を含む。ここで、生体コードは、ユーザーの生体情報または生体情報の組合せから得られたものである。この認証管理方法は公用端末機が携帯用装置から個人キーに挿入された検証コードを含む認証情報を受信し、受信した認証情報の公開キーを用いた検証をサービス提供サーバーに要請し、検証結果に基づいてユーザーの認証を行う工程と、ユーザーの認証に成功した場合に公用端末機がサービスを提供する工程をさらに含む。

【発明の効果】

【００１５】

上述した本発明の少なくとも一つの実施例によれば、より強化されたサービス認証機能を提供する。生体情報がコード化またはトークン化され、公開キー認証書の拡張領域に挿入された公開キー認証書（すなわち、生体認証書）を用いて、スマートカード（あるいは、通信端末機）に格納された暗号化された生体情報や電子署名の偽造・変造を防止することができるという効果を奏する。

【００１６】

さらに、本発明の少なくとも一つの実施例によれば、会計システム、電子決済システム、政府・公共機関・金融機関で発行した電子身分証明書、パスポート、年金、保険、交通カード、電子選挙、電子財布、クーポンなどに適用することができる。この場合、他人が特定ユーザーの簡単な個人情報やカード情報、生体情報または公認認証書情報などを知っていても、他人の無断使用を防止することができるという効果を奏する。

【００１７】

さらに、本発明の少なくとも一つの実施例によれば、業務システムへの遠隔接続に対する情報保護を強化することができるという効果を奏する。

【図面の簡単な説明】

【００１８】

【図１ａ】本発明の少なくとも一つの実施例に係るユビキタス環境でのユーザー認証管理システムの概略図である。

【００１９】

【図１ｂ】本発明の少なくとも一つの実施例に係るユビキタス環境でのユーザー認証管理システムの概略図である。

【００２０】

【図２ａ】本発明の少なくとも一つの実施例に係る通信端末機とスマートカード間の通信方式を示す概略図である。

【図２ｂ】本発明の少なくとも一つの実施例に係る通信端末機とスマートカード間の通信方式を示す概略図である。

【図２ｃ】本発明の少なくとも一つの実施例に係る通信端末機とスマートカード間の通信方式を示す概略図である。

【００２１】

【図３ａ】本発明の少なくとも一つの実施例に係るスマートカードの階層構造を示す概略図である。

【００２２】

【図３ｂ】本発明の少なくとも一つの実施例に係るスマートカードの物理的な構成を示す概略図である。

【００２３】

【図３ｃ】本発明の少なくとも一つの実施例に係るスマートカード機能ブロック図である。

【００２４】

【図４ａ】本発明の少なくとも一つの実施例に係るユーザー登録手続きを説明するための概略図である。

【００２５】

【図４ｂ】本発明の少なくとも一つの実施例に係るユーザー登録手続きを説明するための概略図である。

【００２６】

【図５】本発明の少なくとも一つの実施例に係るユーザー認証管理システムに適用する公開キー認証書のフォーマットを示す概略図である。

【００２７】

【図６】図５ｂに示す公開キー・秘密キーのＥＶ領域に格納するコードのフォーマットの例及びスマートカードから転送される認証情報のフォーマットの例を示す概略図である。

【００２８】

【図７ａ】本発明の少なくとも一つの実施例に係るユーザー認証手続きを示すフローチャートである。

【００２９】

【図７ｂ】本発明の少なくとも一つの実施例に係るユーザー認証手続きを示すフローチャートである。

【００３０】

【図８ａ】本発明の少なくとも一つの実施例に係るユビキタス環境でのＩｏＴデバイスのユーザー管理システムの概略図である。

【図８ｂ】本発明の少なくとも一つの実施例に係るユビキタス環境でのＩｏＴデバイスのユーザー管理システムの概略図である。

【００３１】

【図９ａ】本発明の少なくとも一つの実施例に係るデバイスユーザー（Ｄｅｖｉｃｅ　Ｕ

ｓｅｒ）登録手続きを説明するための概略図である。
【００３２】
【図９ｂ】本発明の少なくとも一つの実施例に係るデバイスユーザー登録手続きを説明するための概略図である。
【００３３】
【図１０ａ】本発明の少なくとも一つの実施例に係るデバイスユーザー認証手続きを説明するための概略図である。
【００３４】
【図１０ｂ】本発明の少なくとも一つの実施例に係るデバイスユーザー認証手続きを説明するための概略図である。
【００３５】
【図１１】オンライン・オフライン環境によるユビキタス認証システムの概念を示す概略図である。
【００３６】
【図１２】本発明の少なくとも一つの実施例に係るオフライン環境でのユーザー認証手続きを説明するための概略図である。
【００３７】
【図１３】本発明の少なくとも一つの実施例に適用可能な例示的な応用分野を示す表である。
【００３８】
【図１４】様々な生体情報あるいはこれらの組合せが様々な用途に分けられて利用可能であることを説明するための概略図である。
【発明を実施するための形態】
【００３９】
以下、添付図面を参照し、本明細書に開示された実施例を詳しく説明する。各図面の構成要素に参照符号を割り当てることにおいて、同一の構成要素に対しては、たとえ異なる図面上に示されていても、可能な限り同一の符号を割り当てている。また、本発明の実施例を説明することにおいて、関連する公知の構成または機能に関する具体的な説明が本発明の要旨を薄め得ると判断される場合には、その詳細な説明を省略する。
【００４０】
さらに、本発明の構成要素を説明することにおいて、第１、第２、Ａ、Ｂ、（ａ）、（ｂ）などの用語を用いることができる。このような用語は、当該構成要素を他の構成要素と区別するためのものであり、その用語によって当該構成要素の本質や順番などが限定されるものではない。明細書全体で、ある部分がある構成要素を「含む」または「備える」ということは、特に反対の記載がない限り、他の構成要素を除外することではなく、他の構成要素をさらに含むことができるとの意味である。また、明細書に記載した「部」、「モジュール」などの用語は、少なくとも一つの機能や動作を処理する単位を意味し、このような処理単位は、ハードウェアやソフトウェアまたはハードウェアとソフトウェアとの組み合わせにより実現することができる。さらに、本発明の説明に用いられる「モノのインターネット（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ：ＩｏＴ）」という用語は、それぞれの標準化団体別に用いられるＭ２Ｍ（Ｍａｃｈｉｎｅ　ｔｏ　Ｍａｃｈｉｎｅ）、ＭＴＣ（Ｍａｃｈｉｎｅ　Ｔｙｐｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）、ＳＤＣ（Ｓｍａｒｔ　Ｄｅｖｉｃｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ），ＭＯＣ（Ｍａｃｈｉｎｅ　Ｏｒｉｅｎｔｅｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）などを包括する意味として理解されるべきである。
【００４１】
図１ａは、本発明の少なくとも一つの実施例に係るユビキタス環境でのユーザー認証管理システムの概略図である。
【００４２】
図１ａに示すように、ユーザー認証管理システムは、認証機関（Ｃｅｒｔｉｆｉｃａｔ

ｅ Ａｕｔｈｏｒｉｔｙ：ＣＡ、１１０）、スマートカード（１２０、サービス提供サーバー（１３０）、認証サーバー（１４０）、通信端末機（１５０）、及びログ格納サーバー（１６０）を含む。

【００４３】

認証機関（ＣＡ、１１０）は、認証機関の情報（認証書のバージョン、有効期限、アルゴリズム、発行期間など）が収録された公開キー認証書（Ｐｕｂｌｉｃ Ｋｅｙ Ｃｅｒｔｉｆｉｃａｔｅ）を発行する。ユーザー登録の過程で、公開キー認証書はユーザーの生体情報とマッチングする公開キー認証書に変換される。すなわち、公開キー認証書は、ユーザーの生体情報とマッチングするコードが挿入された公開キー・個人キーの生成に用いられる。公開キー認証書は、Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ（ＰＫＩ）に基づいた公認認証書または私設認証書（Ｐｒｉｖａｔｅ Ｃｅｒｔｉｆｉｃａｔｅ）である。公開キー認証書は、ユーザーが認証機関（ＣＡ、１１０）のサーバーから発行されるのが一般的であるが、製品の設計や生産の際に通信端末機やスマートカードの安全な領域（例えば、ＩＣチップ、Ｓｅｃｕｒｅ Ｅｌｅｍｅｎｔ（ＳＥ）、Ｔｒｕｓｔｅｄ Ｅｘｅｃｕｔｅｄ Ｅｎｖｉｒｏｎｍｅｎｔｋ（ＴＥＥ）、ＯＳ、ＣＰＵ、メモリー、ＣｌｏｕｄＳＥなど）に前もってインストールしてあっても良い。

【００４４】

スマートカード（１２０）は、内蔵された生体センサー、ＩＣチップまたはメモリーなどに個人キー、センシングされた生体情報と比較するための暗号化された生体情報（Ｅｎｃｒｙｐｔｅｄ Ｂｉｏｍｅｔｒｉｃ Ｄａｔａ）及びその他の各種情報を格納している。個人キーには、暗号化された生体情報をコード化（またはトークン化）して生成した生体コードが挿入されている。

【００４５】

スマートカード（１２０）は、公開キー認証書に基づいてユーザーの生体情報を暗号化し、暗号化された生体情報をコード化（またはトークン化）して生体コードを生成する。スマートカード（１２０）は、生成された生体コードを公開キー認証書に挿入して一つのキーペアー（すなわち、公開キー及び個人キー）を生成する。生体コード（Ｂｉｏｍｅｔｒｉｃ Ｃｏｄｅ）あるいは個人キーは、暗号化された生体情報の無欠性（Ｉｎｔｅｇｒｉｔｙ）、拒絶防止（Ｎｏｎ－ｒｅｐｕｄｉａｔｉｏｎ）などを検証するのに用いられ、生体署名（Ｂｉｏ Ｓｉｇｎａｔｕｒｅ）として用いることができる。このように生成された生体コードは、トークン（Ｔｏｋｅｎ）のように用いるか、またはＯＴＰ（Ｏｎｅ Ｔｉｍｅ Ｐａｓｓｗｏｒｄ、Ｄｙｎａｍｉｃ Ｃｏｄｅとも称する）などと結合して用いることができる。ここで、公開キー認証書にコード化して挿入する生体情報は、登録された加入者の指紋情報、血管情報、音声情報、虹彩情報、手書き情報、顔面情報、心臓拍動などを含むことができる。スマートカード（１２０）は公開キーをサービス提供サーバー（１３０）または認証サーバー（１４０）に転送し、サービス提供サーバーまたは認証サーバーは受信した公開キーを後で認証手続きに利用する。

【００４６】

本発明の少なくとも一つの実施例において、スマートカード（１２０）は、ユーザーの互いに異なる複数の生体情報をそれぞれコード化した生体コードを併合（Ｍｅｒｇｅ）して一つの認証書に挿入する。例えば、指紋＋虹彩、顔面＋音声、心臓拍動＋虹彩などの互いに異なる種類の生体情報の組合せ、指紋１（親指）＋指紋２（人差し指）、虹彩１（右側）＋虹彩２（左側）のように同一種類の生体情報の組合せを用いることができる。複数の生体情報の組合せを用いる場合、それぞれの生体情報の入力順序（例えば、指紋１→指紋２→指紋３または指紋→虹彩）を認証要素として追加することができる。本発明の少なくとも一つの実施例において、スマートカードは、ユーザーの互いに異なる生体情報または生体情報の組合せをそれぞれ異なる公開キー認証書に挿入しても良い。本発明の少なくとも一つの実施例において、ユーザーの物理的署名（Ｈａｎｄ－ｗｒｉｔｔｅｎ ＳｉｇｎａｔｕｒｅまたはＤｙｎａｍｉｃ Ｓｉｇｎａｔｕｒｅ）あるいはＫｅｙ Ｓｔｒｏｋｅ、生体情報入力方式などから抽出したコードの値を追加的な認証要素として認証書に追

加することができる。この場合、ユーザーが物理的署名あるいは所定の意味の単語や数字を入力するＫｅｙ　Ｓｔｒｏｋｅを入力する行動特性（または行動パターン要素）である時間、速度、方向、圧力、位置情報などを追加的な認証要素として考慮することができる。

【００４７】

本発明の少なくとも一つの実施例において、スマートカード（１２０）は、生体コードに付加的な目的または認証要素として様々な追加コードを連鎖させて（Ｃｏｎｃａｔｅｎａｔｅｄ）一つのキーペアーを生成することができる。例えば、スマートカード（１２０）に与えられた固有識別情報から得られた追加コード、ユーザーの認証（あるいは登録）を要請する位置を表す位置情報から得られた追加コード、ユーザーに与えられた固有識別情報から得られた追加コード、及びユーザーの行動特性を表す特性情報から得られた追加コード、ＩｏＴデバイス与えられたデバイス識別情報から得られた追加コードのうち少なくとも一つを生体コードに連鎖させることができる。

【００４８】

さらに、スマートカード（１２０）は、公開キー認証書に生体コードを挿入して一つのキーペアー（公開キー・個人キー）を生成することにおいて、異なる生体情報または生体情報の組合せから複数の生体コードを生成し、公開キー認証書の拡張フィールドに複数の生体コードを互いに区分けられた形態で挿入することができる。それぞれの生体コードには前述した一つ以上の追加コードを連鎖させることができる。その結果、個人キー及び公開キーには複数の生体コードまたは追加コードが連鎖された複数の生体コードが含まれる。この場合、複数の生体コードは、互いに異なる目的で用いることができる。例えば、複数の生体コードのうち一つを個人キーの正当なユーザー認証を行うために指定する。残りの生体コードは、他人からの強制による個人キーの使用を知らせるために、既に転送された公開キーに基づいてなされたユーザー登録の解除を要請するために、遠隔客体（例えば、サービス提供サーバー、または認証サーバー、中央制御装置（Ｃｅｎｔｒａｌｉｚｅｄ　Ｃｏｎｔｒｏｌｌｅｒ）などによって管理される認証管理システムの初期化を要請するために指定することができる。

【００４９】

通信端末機（１５０）は、スマートカード（１２０）と有線または無線で接続され、スマートカード（１２０）から受信するトンネリング開始信号に応答してスマートカード（１２０）とサービス提供サーバー（１３０）間に仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を開設し、スマートカード（１２０）から登録された認証書に基づく認証情報を受信してサービス提供サーバー（１３０）に伝達する。通信端末機（１５０）は、スマートカード（１２０）の個人キー・公開キーを生成するユーザー登録手続きあるいはユーザー認証手続きで要求されるユーザーの生体情報、動的署名、ＩｏＴデバイスの識別情報などを獲得するための手段として用いることができる。通信端末機（１５０）は、一つ以上の生体センサー、タッチスクリーン、カメラ、ＭＩＣなどを備えるか、これらと接続することができる。通信端末機（１５０）は、個人が保有する通信端末機（例えば、携帯電話、タブレットＰＣ、デスクトップコンピューター、Ｓｅｔ－ｕｐ　Ｂｏｘなど）のみならず、公共で用いられるサービス端末機（ＡＴＭ、Ｋｉｏｓｋ、ＰＯＳなど）を含み、さらに、通信ネットワーク上の遠隔客体との通信を行うことができる全ての装置を包括する意味として理解されるべきである。

【００５０】

認証サーバーは、ユーザー登録手続きで獲得した公開キーを用いてスマートカード（または通信端末機）から転送された認証情報を検証する。例えば、認証サーバーは、ユーザー登録手続きでスマートカード（または通信端末機）が公開キー認証書（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｃｅｒｔｉｆｉｃａｔｅ）を用いて生成した公開キーを受け、その後ユーザー認証過程でサービス提供サーバーの要請によってスマートカード（または通信端末機）から転送された認証情報を公開キーに基づいて検証する。

【００５１】

サービス提供サーバー（１３０）は、銀行・クレジットカード（Ｂａｎｋ／Ｃｒｅｄｉｔ　Ｃａｒｄ）サービス、Ｐａｙｍｅｎｔサービス、ｅ－Ｇｏｖｅｒｎｍｅｎｔサービス、Ｃｌｏｕｄサービス、ＩｏＴデバイス連動サービス、Ｅｍｅｒｇｅｎｃｙサービスなどの様々なサービスを認証されたユーザーに提供するサービス提供者のサーバーを意味する。サービス提供サーバー（１３０）は、スマートカード（または通信端末機）を介してスマートカードから受信した認証情報に基づいてユーザーを認証する。例えば、サービス提供サーバーは、認証情報に対する検証を認証サーバーに要請し、その検証結果によってユーザーを認証することができる。本発明の少なくとも一つの実施例において、サービス提供サーバーと認証サーバーは、一つのサーバー内に機能的な構成要素で実現することができる。

【００５２】

ログ格納サーバー（１６０）は、通信端末機（１５０）を介したスマートカード（１２０）のサービス提供サーバーに対する接続履歴を表すログデータ及び認証結果を格納する。ログ格納サーバー（１６０）は、サービス提供サーバー（１３０）が認証機関サーバー、カード会社サーバーなどに接続してユーザーに対する情報を再び確認する場合、それに対するアクセスの試み及び結果を記録及び格納することができる。さらに、ログデータ格納サーバー（１６０）は、スマートカード（１２０）とサービス提供サーバー（１３０）間に開設したＶＰＮ（１７０）を監視し、不当なユーザーのアクセスを遮断するＶＰＮファイアウォールの役割を兼ねることもできる。さらに、ログ格納サーバーは、電子ウォレットの正当なユーザーであるか否かを確認し、生体コードが含まれた電子領収書を発行または印刷することができる。

【００５３】

ログ格納サーバー（１６０）に格納されたデータは、ディジタルフォレンジック（Ｄｉｇｉｔａｌ　Ｆｏｒｅｎｓｉｃ）に用いることができる。例えば、ログデータは、後でユーザーの行為に対する確認・証拠資料として用いることができる。例えば、スマートカードからサービス提供サーバー（１３０）に転送する認証情報にはユーザーの物理的な署名情報が含まれる場合があり、このような物理的署名情報をログデータとともに格納することで、後で電子領収書または請求書などに印刷物として出力するか、または電子的な形態で表示することができる。

【００５４】

図１ｂは、本発明の少なくとも一つの実施例に係るユビキタス環境でのアイデンティティ管理（Ｉｄｅｎｔｉｔｙ　Ｍａｎａｇｅｍｅｎｔ）のためのシステムを示す概略図である。

【００５５】

図１ａはスマートカード（１２０）が通信端末機（１５０）と独立的に構成されたものとして示しているが、図１ｂに示すように、本発明の少なくとも一つの実施例においては、スマートカード（１２０）の機能を通信端末機（１５０）に統合することができる。すなわち、ユーザーの生体情報にマッチングする認証書が通信端末機（１５０）内のＳｅｃｕｒｅ　Ｅｌｅｍｅｎｔ（ＳＥ：Ｓｅｃｕｒｅ　Ｍｅｍｏｒｙ　ａｎｄ　Ｅｘｅｃｕｔｉｏｎ　Ｅｎｖｉｒｏｎｍｅｎｔ）、ＣＰＵ、ＯＳなどに格納／管理することができる。通信端末機（１５０）内のＳｅｃｕｒｅ　Ｅｌｅｍｅｎｔは、例えば、ＳＩＭ、ＵＳＩＭ、ｍｉｃｒｏＳＤカード、ＮＦＣカードなどのＩＣチップ内に実現することができる。

【００５６】

通信端末機（１５０）は、スマートカードとの連動なしに、ユーザーの生体情報にマッチングする認証書を用いてユーザー認証手続きを行うことができる。さらに、通信端末機は、生体情報をセンシングするために様々な種類の生体センサーを含むことができ、ＩｏＴデバイスからデバイス情報を得るために適切な入力・センシング手段を備えるか、またはこのような手段を備える外部の装置と連動することができる。通信端末機（１５０）は、特に言及しなくても、本発明の全般にわたって説明するスマートカードの機能や動作上に与えられた様々な特徴に対応する特徴を有する。

【００５７】
図１ｂの通信端末機は、個人が保有する通信端末機（例えば、携帯電話、ウェアラブルデバイス（Ｗｅａｒａｂｌｅ　Ｄｅｖｉｃｅ：腕時計、メガネ、指輪など）、タブレットＰＣ、デスクトップコンピューター、Ｓｅｔ－ｕｐ　Ｂｏｘなどを含み、さらに、通信ネットワーク上の遠隔客体との通信を行える全ての装置を包括する意味として理解されるべきである。
【００５８】
図２ａ乃至図２ｃは、本発明の少なくとも一つの実施例に係る通信端末機とスマートカード間の通信方式を示す概略図である。図２ａ乃至図２ｃは、図１の通信端末機をスマートフォンのようなモバイル端末機として実現する場合を想定している。
【００５９】
本発明の少なくとも一つの実施例において、図２ａに示すように、スマートカードは小型ドングル（Ｐｏｃｋｅｔ－ｓｉｚｅｄ　Ｄｏｎｇｌｅ）を介して通信端末機と通信することができる。ドングルは、接触式または非接続式でスマートカードと情報を交換することができる。ドングルは、例えば、スマートフォンのオーディオ端子（Ａｕｄｉｏ　Ｊａｃｋ）またはマイクロＵＳＢ端子などに接続される。このような構成によれば、ユーザーはスマートフォンにドングルを接続し、スマートカードをドングルにタグ付け（Ｔａｇｇｉｎｇ）するか、またはスワイプ（Ｓｗｉｐｅ）することでスマートカードと通信端末機を通信可能に接続することができる。ドングルは、セキュリティーのため、ハードウェアに基づいた暗号化を提供するのが望ましい。
【００６０】
本発明の少なくとも一つの実施例においては、図２ｂに示すように、スマートカードは通信端末機と無線通信方式（例えば、ＮＦＣ、ＲＦＩＤなど）でダイレクトに通信可能に接続することができる。
【００６１】
本発明の少なくとも一つの実施例においては、図２ｃに示すように、スマートカードは通信端末機にダイレクトに接続可能なＵＳＢドングルタイプで実現することができる。
【００６２】
図３ａは、本発明の少なくとも一つの実施例に係るスマートカードの階層構造を示す概略図である。
【００６３】
スマートカードの物理的階層は、ＣＰＵ、Ｍｅｍｏｒｙ、及びＩ／Ｏ　Ｐｏｒｔを含む。メモリーは、Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ（ＲＯＭ）、Ｒａｎｄｏｍ－ａｃｃｅｓｓ　Ｍｅｍｏｒｙ（ＲＡＭ）、Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ（ＥＥＰＲＯＭ）、Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ（ＥＰＲＯＭ）、Ｆｌａｓｈ　ＥＥＰＲＯＭ、Ｆｅｒｒｏ　Ｅｌｅｃｔｒｉｃａｌ　ＲＡＭ（ＦｅＲＡＭ）などの様々な素子のうち一つまたはこれらの組合せとして実現することができる。オプションとして、スマートカードは、ディスプレイ及び／または一つ以上の生体センサーをさらに含むことができる。オプションとして、スマートカードは、Ｐｈｙｓｉｃａｌ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ（ＰＵＦ）回路をさらに含むことができる。
【００６４】
スマートカードのアプリケーション階層は、スマートカードのＯＳまたはａｐｐｌｅｔの機能的構成要素に関するもので、例えば、生体情報獲得モジュール（Ｂｉｏｍｅｔｒｉｃ　Ｄａｔａ　Ａｃｑｕｉｓｉｔｉｏｎ　Ｍｏｄｕｌｅ）、生体情報管理モジュール（Ｂｉｏｍｅｔｒｉｃ　ｄａｔａ　Ｍａｎａｍｇｅｍｅｎｔ　Ｍｏｄｕｌｅ）、生体認証モジュール（Ｂｉｏｍｅｔｒｉｃ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）、デバイス情報獲得モジュール（Ｄｅｖｉｃｅ　Ｄａｔａ　Ａｃｑｕｉｓｉｔｉｏｎ　Ｍｏｄｕｌｅ）、ＶＰＮ管理モジュール（ＶＰＮ　Ｍａｎａｇｅｍｅｎｔ　Ｍｏｄｕｌｅ）、ＯＴＰ生成モジュール（ＯＴＰ　Ｇｅｎｅｒａｔｉｏｎ　Ｍｏｄｕｌｅ）、キー管理モジュール

（Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｍｏｄｕｌｅ）、及び認証処理モジュール（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｅｘｅｃｕｔｉｏｎ　Ｍｏｄｕｌｅ）に分けることができる。それぞれの機能的構成要素に関する説明は、図３ｃを参照して後述する。

【００６５】

図３ｂは、本発明の少なくとも一つの実施例に係るスマートカードの物理的な構成を示す概略図である。

【００６６】

図３ｂに示すように、本発明の少なくとも一つの実施例において、スマートカード（３００）は、ＣＰＵ・メモリー・ＯＳ・ＰＵＦ回路などを内蔵したＩＣチップ（３０１）、一つ以上の生体センサー（３０３）、ディスプレイ（Ｄｉｓｐｌａｙ、３０４）を含む。

【００６７】

図３ｂのスマートカード（３００）は、内蔵された生体センサー（３０３）を用いてユーザー登録手続き及びユーザー認証手続きで必要な一つ以上の生体情報のうち少なくとも一部をユーザーからセンシングするように構成される。生体センサー（３０３）は、指紋認識センサー、虹彩認識センサー、音声認識センサー、血管認識センサー、手書き認識センサー、顔面（Ｆａｃｉａｌ）センサー、心臓拍動（Ｈｅａｒｔ　Ｂｅａｔ）センサー、動的署名（Ｄｙｎａｍｉｃ　Ｓｉｇｎａｔｕｒｅ）センサーなどで実現することができる。特に、動的署名センサーは、タッチスクリーンを含むディスプレイ（３０４）に結合することができる。

【００６８】

スマートカード（３００）は、ＩＣチップ（３０１）のＯＳ・ＣＰＵ・メモリーなどに内蔵されたＯＴＰ生成モジュールが生成したＯｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ（ＯＴＰ）をディスプレイ（３０４）に表示することができる。さらに、スマートカード（３００）は、次のような情報をディスプレイ（３０４）に表示することができる。

- 生体マッチング結果
- 入力された生体情報または生体情報の組合せに対応する個人キーの不在
- 入力された生体情報または生体情報の組合せに対応する複数の個人キーのリスト
- 入力された生体情報または生体情報の組合せに対応する個人キーの用途
- 登録された動的署名

【００６９】

図３ｃは、本発明の少なくとも一つの実施例に係るスマートカード機能ブロック図である。

【００７０】

図３ｃに示すスマートカードのそれぞれの構成要素は、論理的に区分けられる機能的構成要素（Ｆｕｎｃｔｉｏｎａｌ　Ｅｌｅｍｅｎｔ）または物理的構成要素と結合した機能的構成要素である。すなわち、それぞれの構成は、本発明の技術的思想を実現するための機能的構成要素に該当するので、それぞれの構成要素が統合または分離されて機能を行っても、本発明の機能的構成が行われ、機能し、実現できるのであれば、本発明の範囲内にあると解釈されるべきであり、同一または類似な機能を行う構成要素ならその名称上の一致・不一致とは無関係に本発明の範囲内にあると解釈されるべきである。

【００７１】

図３ｃに示すように、スマートカードの機能的要素は、生体情報獲得モジュール（３１１）、生体情報管理モジュール（３１２）、キー管理モジュール（３１３）、生体認証モジュール（３１４）、ＶＰＮ管理モジュール（３１５）、認証処理モジュール（３１６）、デバイス情報獲得モジュール（３１８）、ＯＴＰ生成モジュール（３１７）に分けることができる。

【００７２】

生体情報獲得モジュール（３１１）は、ユーザー登録手続き及びユーザー認証手続きでユーザーの生体情報を獲得する。本発明の少なくとも一つの実施例において、生体情報獲得モジュール（３１１）は、スマートカード（３１０）に内蔵された生体センサーからユ

ーザーの生体情報を獲得することができる。本発明の少なくとも一つの実施例において、生体情報獲得モジュール（３１１）は、生体センサーを備える通信端末機またはその他の外部装置（例えば、ＡＴＭ、Ｋｉｏｓｋ、ＰＯＳ、ＣＡＲＤ　Ｒｅａｄｅｒなど）からセンシングされた生体情報を獲得することができる。

【００７３】

生体情報管理モジュール（３１２）は、ユーザー登録手続きで生体情報獲得モジュール（３１１）が獲得した生体情報を公開キー認証書に基づいて暗号化し、暗号化された生体情報をスマートカード（例えば、スマートカードのＩＣチップに内蔵されたメモリー、スマートカードに内蔵された生体センサーなど）に格納及び管理する。本発明の少なくとも一つの実施例において、生体情報管理モジュール（３１２）は、加入者に対する複数の生体情報を暗号化して格納する。例えば、加入者の指に対する指紋情報をスマートカードに格納することができ、加入者の目の虹彩情報を格納することができる。さらに、加入者の指紋＋虹彩、虹彩＋顔面などの様々な組合せの生体情報を格納することができる。

【００７４】

キー管理モジュール（３１３）は、公開キー認証書に基づいて暗号化された生体情報をコード化（またはトークン化）して生体コードを生成し、生成した生体コードを公開キー認証書（１１０）に挿入して生体コードが挿入された一つのキーペアー（個人キー、公開キー）を生成する。キー管理モジュール（３１３）は、生成された個人キーをスマートカードのＩＣチップに内蔵されたＭｅｍｏｒｙ、ＣＰＵ、ＯＳ、Ａｐｐｌｉｃａｔｉｏｎなどにインストールまたは格納し、生成された公開キーを認証サーバー（またはサービス提供サーバー）に転送する。本発明の少なくとも一つの実施例において、キー管理モジュール（３１３）は、生体コードに、付加的な目的または認証要素として、様々な追加コードを連鎖させて（Ｃｏｎｃａｔｅｎａｔｅｄ）一つのキーペアーを生成することができる。以下では、曖昧さを避けるため、キーペアーの生成に用いられる公開キー認証書、すなわち、生体コードが挿入されてない公開キー認証書を「空認証書（Ｂｌａｎｋ　Ｃｅｒｔｉｆｉｃａｔｅ）」と称する。

【００７５】

本発明の少なくとも一つの実施例において、空認証書（Ｂｌａｎｋ　Ｃｅｒｔｉｆｉｃａｔｅ）は、事前にスマートカードにインストールまたは格納することができる。すなわち、スマートカードの生産・発行段階で政府・生産者・金融事業者・サービス提供者などが一つ以上の空認証書を前もってスマートカードのＩＣチップ、ＯＳ、ＣＰＵ、Ｍｅｍｏｒｙなどにインストールまたは格納しておくことができる。この場合、スマートカード（１２０）を発行する機関のみが認証書をスマートカードに格納できるように制限を設けるのが望ましい。本発明の少なくとも一つの実施例において、スマートカードは、通信端末機を介して認証機関（ＣＡ）のサーバーから空認証書を受信することができる。本発明の少なくとも一つの実施例において、認証書管理モジュール（３１３）は、コンピューターまたは通信端末機に格納された空認証書をコピーすることができる。空認証書は、例えば、サービスの種類や目的、サービス提供期間、ユーザーの信頼度などによって有効期限や使用目的が制限されても良い。空認証書の有効期限はスマートカードの有効期限と同一であっても良い。さらに、複数の空認証書はそれぞれの有効期限が異なっても良いし、その使用目的も異なっても良い。

【００７６】

生体認証モジュール（３１４）は、生体情報獲得モジュール（３１１）が獲得した生体情報をスマートカードに格納された暗号化された生体情報と比較する。さらに、生体認証モジュール（３１４）は、生体情報獲得モジュール（３１１）が獲得した生体情報をスマートカードに格納された公開キー認証書内に挿入された生体コードと比較する。すなわち、生体認証モジュール（３１４）は、生体情報が、既に格納されている暗号化された生体情報及び生体コードとマッチングするか否かを判断する。本発明の少なくとも一つの実施例において、生体認証モジュール（３１４）は、既に格納されている暗号化された生体情報または生体コードのうち一つのみを、獲得した生体情報と比較するように構成しても良

い。

【００７７】

ＶＰＮ管理モジュール（３１５）は、サービス提供サーバーなどの遠隔の客体（Ｒｅｍｏｔｅ　Ｅｎｔｉｔｙ）とのＶＰＮの開設及び管理を担当し、Ｅｎｄ　ｔｏ　Ｅｎｄ暗号化と安全な転送区間を提供する。例えば、獲得した生体情報が、既に格納されている暗号化された生体情報及び生体コードとマッチングすると判断された場合、ＶＰＮ管理モジュール（３１５）は、サービス提供サーバーとＶＰＮを開設するためのトンネリング開始信号を通信端末機に転送する。トンネリング開始信号は、ＶＰＮ開設の目的地ＵＲＬを含むことができる。ここで、通信端末機は、個人が保有する通信端末機（例えば、携帯電話、タブレットＰＣ、デスクトップコンピューター、Ｓｅｔ－ｕｐ　Ｂｏｘなど）のみならず、公共で用いられるサービス端末機（ＡＴＭ、Ｋｉｏｓｋ、ＰＯＳなど）を含み、さらに、通信ネットワーク上の遠隔客体との通信を行うことができる全ての装置を包括する意味として理解されるべきである。

【００７８】

また、生体情報管理モジュール（３１２）が複数の生体情報を管理する場合、ＶＰＮ管理モジュール（３１５）は、生体情報入力モジュール（３１１）を介して入力されるライブ生体情報が、既に格納されている複数の生体情報のうちどれとマッチングするかによって互いに異なるＶＰＮ開設の目的地ＵＲＬを指定してトンネリング開始信号を転送することができる。目的地ＵＲＬは、銀行・クレジットカード（Ｂａｎｋ／Ｃｒｅｄｉｔ　Ｃａｒｄ）サービス、Ｐａｙｍｅｎｔサービス、ｅ－Ｇｏｖｅｒｎｍｅｎｔサービス、Ｃｌｏｕｄサービス、ＩｏＴデバイス連動サービス、Ｅｍｅｒｇｅｎｃｙサービスなどの様々なサービスを認証されたユーザーに提供するサービス提供者のサーバーを意味する。このようなＵＲＬは、スマートカードの製造段階または認証書の発行段階、あるいは個人キー・公開キーの生成段階で指定することができる。例えば、ＵＲＬは、スマートカードに前もって格納された公開キー認証書（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｃｅｒｔｉｆｉｃａｔｅ）に挿入されているか、または公開キー認証書と同一の格納領域に格納することができる。格納領域は、ＩＣチップ内のデータの変更が不可能な領域であることが望ましい。本発明の少なくとも一つの実施例において、スマートカードで新規の公開キー認証書を追加で発行する場合、発行される公開キー認証書と関連するＵＲＬが一緒に受信されるか、または関連するＵＲＬが挿入された公開キー認証書が発行される。このような公開キー認証書は、ＩＣチップ内のデータの変更が可能な領域に格納するのが望ましい。さらに、ＵＲＬは、生体コードに併合した形態で個人キー・公開キーに挿入するのが望ましい。

【００７９】

さらに、複数の生体情報のうち、特定の生体情報あるいは複数の生体情報の組合せ（順序が与えられる場合がある）のうち特定の組合せは、ユーザーの緊急状況を知らせる用途として指定することができる。例えば、特定の生体情報に対応するトンネリング開始信号は、ユーザーの緊急状況を知らせるため、前もって設定したＵＲＬ（例えば、警視庁サーバー、安全管理サーバー）にＶＰＮを開設するように構成することができる。このような構成によれば、ユーザーが他人の威嚇によって強制的にスマートカード（１２０）を用いたユーザー認証手続きを行わなければならない場合に、登録された複数の生体情報のうち前もって設定した特定の生体情報を用いることで、威嚇する他人に気づかれないように警視庁サーバーにユーザーの緊急状況信号を転送することができる。このような緊急状況信号は、後で強制的な使用に対する保険処理または訴訟に対する証拠として活用することができる。

【００８０】

認証処理モジュール（３１６）は、サービス提供サーバーに通信トンネルが開設されると、キー管理モジュール（３１３）で管理する個人キーに基づく認証情報を当該サービス提供サーバーに転送し、スマートカード（１２０）のユーザーが正当なユーザーであることを認証する処理を行う。認証情報は図６を参照して後述する。

【００８１】

スマートカードは、ＯＴＰ生成モジュール（３１７）をさらに含むことができる。ＯＴＰ生成モジュール（３１７）は、スマートカード（１２０）の発行機関によって前もって設定した方式で一回性のパスワード（Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ：ＯＴＰ）を生成する。本発明の少なくとも一つの実施例において、ＯＴＰ生成モジュール（３１７）で生成したＯＴＰは、スマートカード（１２０）のユーザーが認識できるようにスマートカードのディスプレイに表示され、ＯＴＰ生成モジュール（３１７）は、ユーザーが入力するＯＴＰを認証処理モジュール（３１６）に伝達する。本発明の少なくとも一つの実施例において、ＯＴＰ生成モジュール（３１７）が生成した一回性のパスワードは、ディスプレイに表示せずに、すぐ認証処理モジュール（３１６）に伝達することもできる。認証処理モジュール（３１６）に伝達されたＯＴＰは、認証書に基づいた認証情報とともに対象端末に転送される。これで当該スマートカード（１２０）が正当な発行機関によって発行されたものであることを検証（認証）することができる。当該技術分野での従来の技術では、スマートカードと別途のＯＴＰデバイスを用いていた。

【００８２】

スマートカード（１２０）は、デバイス情報獲得モジュール（３１８）をさらに含むことができる。デバイス情報獲得モジュール（３１８）は、ＩｏＴデバイスの識別情報を獲得する。ＩｏＴデバイスの識別情報は、生産、流通、または購買時点でそれぞれのＩｏＴデバイスに与えられる装置固有の識別情報を意味し、より具体的な内容は図６を参照して後述する。デバイス情報獲得モジュール（３１８）は、スマートカード（１２０）に内蔵されたセンサーまたは一つ以上のセンサーを備えた通信端末機（１５０）またはその他の外部装置（例えば、ＡＴＭ、Ｋｉｏｓｋ、ＰＯＳ、ＣＡＲＤ　Ｒｅａｄｅｒなど）からＩｏＴデバイスの識別情報を受信することができる。

【００８３】

図４ａは、本発明の少なくとも一つの実施例に係るユーザー登録手続きを説明するための概略図である。図４ａに示すユーザー登録手続きは、図１ａに示す構成を有するユーザー認証システムに適している。図４ａではスマートカードに前もって（例えば、スマートカードの製作または発行時に）公開キー認証書が格納されていることを仮定しているが、認証機関（ＣＡ）のサーバーから新規の公開キー認証書を受信することもできる。

【００８４】

まず、通信端末機は、ユーザーの生体情報を獲得し、獲得したユーザーの生体情報をスマートカードに伝達する（Ｓ４０１～Ｓ４０２）。ここで、生体情報の獲得には通信端末機に内蔵された生体センサーを用いるか、または通信端末機と接続する外部の生体センサーを用いることができる。図４ａに示す例とは異なり、本発明の少なくとも一つの実施例において、スマートカードは、内蔵された生体センサーを用いてユーザーの生体情報をダイレクトに獲得することができる。

【００８５】

ユーザーの生体情報を獲得したスマートカードは、ユーザーの生体情報を前もって格納された（Ｐｒｅ－ｓｔｏｒｅｄ）または既に存在する（Ｐｒｅ－ｅｘｉｓｔｉｎｇ）公開キー認証書に基づいて暗号化する（Ｓ４０３）。すなわち、スマートカードは、公開キー認証書に規定された暗号化アルゴリズムによって生体情報を暗号化する。

【００８６】

また、スマートカードは、暗号化された生体情報をコード化またはトークン化してコードの値を生成する（Ｓ４０４）。コード化またはトークン化アルゴリズムは、スマートカードのアプリケーションに内蔵されていても良いし、公開キー認証書に規定されていても良い。例えば、本発明の少なくとも一つの実施例においては、コード化またはトークン化には公開キー認証書に規定されているメッセージ縮約アルゴリズム（Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ）などを利用することができる。コードの値はユーザーの生体情報を公開キー認証書に基づいてコード化した情報であるので、「生体コード（Ｂｉｏｍｅｔｒｉｃ　Ｃｏｄｅ）」または「生体電子署名（Ｂｉｏｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ）」と称することもできる。

【００８７】
次に、スマートカードは、生体コードを公開キー認証書のＥＶ領域（Ｅｘｔｅｎｄｅｄ Ｖａｌｉｄａｔｉｏｎ Ｄｏｍａｉｎ）に挿入して一つのキーペアー（公開キー、個人キー）を生成する。すなわち、生成された個人キーと公開キーには生体コードが挿入されている。個人キーは、後でユーザー認証手続きに用いるため、暗号化された生体情報とともにスマートカード内に格納される（Ｓ４０５）。図４ａには図示してないが、追加的な認証要素として、生体コードと同一または類似の方式で生成された様々な追加コードを生体コードに連鎖させることができる。例えば、公開キー認証書の領域には、生体コードの他に、携帯用装置に与えられた固有識別情報から得られた追加コード、ユーザーの認証を要請する位置を表す位置情報から得られた追加コード、ユーザーに与えられた固有識別情報から得られた追加コード、及びユーザーの行動特性を表す特性情報から得られた追加コード、ＩｏＴデバイスに与えられたデバイス識別情報から得られた追加コードのうち少なくとも一つをさらに挿入することができる。追加コード関しては図６を参照して後述する。

【００８８】
また、スマートカードは、公開キーを、通信端末機を介して認証サーバー（またはサービス提供サーバー）に転送してユーザー登録を要請する（Ｓ４０６）。公開キーの転送には仮想私設網（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。認証サーバーは、ユーザーを登録し、公開キーを別の安全なＤＢで管理する（Ｓ４０７～Ｓ４０８）。

【００８９】
図４ｂは、本発明の少なくとも一つの実施例に係るユーザー登録手続きを説明するための概略図である。図４ｂに示すユーザー登録手続きは、図１ｂに示す構成を有するユーザー認証システムに適している。したがって、図４ｂの通信端末機は個人が保有する通信端末機（例えば、携帯電話、タブレットＰＣ、デスクトップコンピューター、Ｓｅｔ－ｕｐ Ｂｏｘなど）を含み、さらに、通信ネットワーク上の遠隔客体との通信を行うことができる全ての装置を包括する意味として理解されるべきである。

【００９０】
まず、通信端末機は、ユーザー登録のために、認証機関（ＣＡ）のサーバーに公開キー認証書の発行を要請する（Ｓ４５１）。公開キー認証書の発行要請を受けた認証機関（ＣＡ）のサーバーは、公開キー認証書を通信端末機に発行する（Ｓ４５２）。図４ａに示す例とは異なり、本発明の少なくとも一つの実施例において、通信端末機には前もって（例えば、通信端末機の生産または販売時に）公開キー認証書が格納されている。

【００９１】
次に、通信端末機は、ユーザーの生体情報を獲得する（Ｓ４５３）。ここで、生体情報の獲得には通信端末機に内蔵された生体センサーを用いるか、または通信端末機と接続した外部デバイスの生体センサーを用いることができる。

【００９２】
次に、通信端末機は、ユーザーの生体情報を発行された公開キー認証書で暗号化する（Ｓ４５４）。すなわち、通信端末機は公開キー認証書に規定された暗号化アルゴリズムによって生体情報を暗号化する。暗号化された生体情報は、後でユーザー認証手続きに用いるため、通信端末機内に格納される。

【００９３】
通信端末機は、暗号化された生体情報をコード化またはトークン化してコードの値（すなわち、生体コード）を生成する（Ｓ４５５）。コード化またはトークン化アルゴリズムは、通信端末機のアプリケーションに内蔵されるか、または公開キー認証書に規定されたものである。本発明の少なくとも一つの実施例において、コード化またはトークン化には公開キー認証書に規定されたメッセージ縮約アルゴリズム（Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ）などが用いられる。

【００９４】

次に、通信端末機は、生成された生体コードを公開キー認証書のＥＶ領域（Ｅｘｔｅｎｄｅｄ　Ｖａｌｉｄａｔｉｏｎ　Ｄｏｍａｉｎ）に挿入して一つのキーペアー（公開キー、個人キー）を生成する（Ｓ４５６）。すなわち、生成された個人キーと公開キーには、生体コードが挿入されている。個人キーは、後でユーザー認証手続きに用いるため、通信端末機内に格納される。図４ａには図示してないが、他の追加コードを、生体コードと同一または類似の方式で生成して公開キー認証書に追加的な認証として追加することができる。

【００９５】

また、通信端末機は、公開キーを認証サーバー（またはサービス提供サーバー）に転送してユーザー登録を要請する（Ｓ４５７）。公開キーの転送には仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。認証サーバーはユーザーを登録し、公開キーを別途の安全なＤＢで管理する（Ｓ４５８～Ｓ４５９）。

【００９６】

図５（ａ）及び図５（ｂ）は、本発明の少なくとも一つの実施例に係るユビキタス管理システムに適用する公開キー認証書（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｃｅｒｔｉｆｉｉｃａｔｅ）のフォーマットを示す概略図である。

【００９７】

公開キー認証書（例えば、公開キー基盤（ＰＫＩ）のＩＴＵ－Ｔ標準Ｘ。５０９認証書）は、インターネットのウェブ上でビジネスまたは取引をする際に、相手が信頼できるようにする一種の電子保証書を意味する。公開キー認証書は、特定の政府や金融機関などが指定した認証機関、私設認証機関、製品の生産者または装置サービス提供機関で発行することができる。

【００９８】

図５（ａ）には、ユーザー登録手続きを経てない公開キー認証書のフォーマットの例を示す。公開キー認証書には、バージョン、シリアル番号、署名アルゴリズム、発行者、有効期限、公開キー、発行者の電子署名などが収録される。ユーザー登録手続き経てない公開キー認証書のＥＶ領域（Ｅｘｔｅｎｄｅｄ　Ｖａｌｉｄａｔｉｎ　Ｄｏｍａｉｎ）が空いていることに注意すべきである。

【００９９】

図５（ｂ）には、ユーザー登録手続きを介して、公開キー認証書から生成された公開キー認証書（公開キー・個人キー）のフォーマットの例を示す。図５（ａ）に示す例とは異なり、ユーザー登録手続きを経た公開キー認証書またはこれから生成された公開キー・個人キーのＥＶ領域（Ｅｘｔｅｎｄｅｄ　Ｖａｌｉｄａｔｉｎ　Ｄｏｍａｉｎ）には、ユーザーの生体情報をコード化して生成された生体コード（Ｂｉｏｍｅｔｒｉｃ　Ｃｏｄｅ）が挿入されている。ＥＶ領域に格納された生体コードには付加的な認証要素として様々な追加コードを連鎖（Ｃｏｎｃａｔｅｎａｔｅｄ）させることができる。具体的な追加コードに関しては、図６を参照して後述する。

【０１００】

本発明の少なくとも一つの実施例においては、様々な発行主体、様々なフォーマットの公開キー認証書を用いることができる。したがって、生体コードが挿入される公開キー認証書のフォーマットは、図５（ａ）及び図５（ｂ）に限定されるものではなく、生体コードが挿入される公開キー認証書の拡張領域は、ＥＶ領域に限定されるものではない。

【０１０１】

図６は、図５（ｂ）に示す公開キー・秘密キーのＥＶ領域に格納するコードのフォーマットの例及びスマートカードから転送される認証情報のフォーマットの例を示す概略図である。

【０１０２】

前述のように、公開キー・秘密キーのＥＶ領域には単純にユーザーの生体情報をコード化して生成した生体コードの身を格納することもできるが（図６の（ａ）参照）、生体コードに様々な種類の一つ以上の追加コードを連鎖させて構成したコードを格納することも

できる。例えば、本発明の少なくとも一つの実施例においては、ユーザーが所有するＩｏＴデバイスの識別情報からコード化（またはトークン化）した追加コード（すなわち、Ｄｅｖｉｃｅ　Ｃｏｄｅ）を生体コードに連鎖させることができる（図６の（ｂ）、（ｃ）参照）。ここで、ＩｏＴデバイスの識別情報は生産、流通、または購買時点にそれぞれのＩｏＴデバイスに与えられる固有の識別情報を意味する。ＩｏＴデバイスの識別情報はデバイス番号、出庫情報、シリアル番号、Ｅｌｅｃｔｒｏｎｉｃ　Ｐｒｏｄｕｃｔ　Ｃｏｄｅ（ＥＰＣ）、Ｕｎｉｖｅｒｓａｌ　Ｐｒｏｄｕｃｔ　Ｃｏｄｅ（ＵＰＣ）、Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ（ＰＵＦ）、Ｇｌｏｂａｌ　Ｓｈｉｐｍｅｎｔ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ（ＧＳＩＮ）、ＭＡＣ　ａｄｄｒｅｓｓなどを含む。ＩｏＴデバイスの識別情報は、ＩｏＴデバイスに印刷物の形態で付着したＢａｒ　Ｃｏｄｅ、ＱＲ　ＣｏｄｅまたはＩｏＴデバイスに内蔵された電子素子から取集することができる。Ｄｅｖｉｃｅ　Ｃｏｄｅの使用用途は、図８を参照して後述する。

【０１０３】

本発明の少なくとも一つの実施例において、公開キー認証書が格納されたスマートカードまたは通信端末機の識別情報からコード化（またはトークン化）した追加コードを生体コードに連鎖させることができる（図６の（ｄ）参照）。ここで、公開キー認証書が格納されたスマートカードあるいは通信端末機の識別情報は、例えば、Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｈａｓｈ　Ｆｕｎｃｔｉｏｎｓ　Ｖａｌｕｅ、Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ（ＰＵＦ）、Ｐａｙｍｅｎｔ　Ｃａｒｄ　Ｎｕｍｂｅｒなどを含む。

【０１０４】

本発明の少なくとも一つの実施例において、政府や銀行などで公共の目的でユーザーに与えた固有識別情報（例えば、Ｓｏｃｉａｌ　Ｓｅｃｕｒｉｔｙ　Ｎｕｍｂｅｒ、Ｕｎｉｑｕｅ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ、Ｐｅｒｓｏｎａｌ　Ａｃｃｅｓｓ　Ｎｕｍｂｅｒ）やユーザーの行動特性と関連する情報（例えば、Ｋｅｙ　Ｓｔｒｏｋｅ、Ｄｙｎａｍｉｃ　Ｓｉｇｎａｔｕｒｅ）からコード化（またはトークン化）した追加コードを生体コードに連鎖させることができる。（図６の（ｅ）、（ｆ）参照）。ユーザーの行動特性と関連する情報は、スマートカードまたは通信端末機に備えられたタッチスクリーンを介して獲得することができる。

【０１０５】

本発明の少なくとも一つの実施例において、通信端末機（あるいは、スマートカード）の位置情報（例えば、Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ（ＧＰＳ）、Ｇｒｏｕｐ　ｏｎ　Ｅａｒｔｈ　Ｏｂｓｅｒｖａｔｉｏｎ（ＧＥＯ）　Ｌｏｃａｔｉｏｎ）からコード化（またはトークン化）した追加コードを生体コードに連鎖させることができる。追加コードは、正常な取引位置から外れた位置での取引行為（例えば、金融取引、信頼サービス行為、金融決済、Ｐａｙｍｅｎｔサービス、料金付加）であるか否かを累加認証要素として考慮することで盗難、紛失などによる不正取引を探知及び防止するか、または証明するのに適用することができる。

【０１０６】

さらに、生体コードに複数の追加コードを連鎖させることができる（図６の（ｇ）～（ｉ）参照）。図６の（ｊ）に生体コードに複数の追加コードを連鎖させたコードを示す。連鎖されたコードで生体コード及び追加コードの長さは互いに同一であっても良いし、互いに異なっても良い。

【０１０７】

このような追加コードを生成するアルゴリズムには、生体コードを生成するアルゴリズムと実質的に同一の方式を適用することができる。さらに、追加コードの生成過程で暗号化されたデータ（例えば、暗号化された動的署名）は、個人キーとともにスマートカードまたは通信端末機内に格納することができる。格納した暗号化されたデータはスマートカードまたは通信端末機内で行われる１次ユーザー認証（生体マッチングに基づく）の追加

認証手段として用いることができる。

【０１０８】

図６の（ｊ）は、ユーザー認証手続きでサービス提供サーバーに転送する認証情報に含まれたコードの例を示す。すなわち、認証情報は、個人キーに挿入された（連鎖された）コードを含む。これに関する詳細な説明は図７ａを参照して後述する。

【０１０９】

特に、個人キー・公開キーに挿入されたコード及びスマートカードから転送される認証情報は、応用例及び／またはセキュリティーのレベルによって様々なフォーマットを有することができ、図６に示す幾つかの順序または組合せに限定されるものではない。さらに、図６に示す認証要素以外の要素を追加的に用いることができる。

【０１１０】

図７ａは、本発明の少なくとも一つの実施例に係るユーザー認証手続きを示すフローチャートである。図７ａに示すユーザー登録手続きは、図１ａに示す構成を有するユーザー認証システムに適している。

【０１１１】

まず、通信端末機は、ユーザーの生体情報を獲得し、獲得したユーザーの生体情報をスマートカードに伝達する（Ｓ７０１～Ｓ７０２）。ここで、生体情報の獲得には通信端末機に内蔵された生体センサーを用いるか、または通信端末機と接続する外部の生体センサーを用いることができる。図７ａに示す例とは異なり、本発明の少なくとも一つの実施例において、スマートカードは内蔵された生体センサーを用いてユーザーの生体情報をダイレクトに獲得することができる。

【０１１２】

次に、スマートカードは、獲得した生体情報をスマートカードに格納されている暗号化された生体情報及び／またはスマートカードに格納されている個人キーに挿入された生体コードと比較する（Ｓ７０３）。すなわち、スマートカードは、獲得した生体情報が、既に格納されている暗号化された生体情報及び／または生体コードとマッチングするか否かを判断する。

【０１１３】

次に、スマートカードは、獲得した生体情報が、既に格納されている暗号化された生体情報及び生体コードとマッチングすると、個人キーに基づいた認証情報を通信端末機を介してサービス提供サーバーに転送する（Ｓ７０４）。認証情報の転送には仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。例えば、スマートカードは、サービス提供サーバーとＶＰＮを開設するためのトンネリング開始信号を通信端末機に転送し、通信端末機はトンネリング開始信号に対応してサービス提供サーバーはスマートカードとの間にＶＰＮを開設する。スマートカードは、開設したＶＰＮを介してサービス提供サーバーに認証情報を転送する。トンネリング開始信号にはＶＰＮの目的地ＵＲＬ情報が含まれても良い。

【０１１４】

サービス提供サーバーは、受信した認証情報の検証を認証サーバーに要請する（Ｓ７０５）。認証サーバーは、既に登録されている公開キーを用いて認証情報を検証する。サービス提供サーバーは、認証サーバーの検証結果に基づいてユーザー認証を完了する（Ｓ７０６～Ｓ７０８）。

【０１１５】

一方、サービス提供サーバーに転送する認証情報は、スマートカードに格納された個人キーに挿入されたコード（図６の（ａ）～（ｉ）参照）に基づいて生成される。例えば、認証情報は公開キー認証書のＥＶ領域に挿入された生体コードあるいは連鎖されたコードそのものを含む（Ｃｏｎｔａｉｎ）ことができる。本発明の少なくとも一つの実施例において、認証情報は認証書のＥＶ領域に挿入されたコードのみならず、スマートカードに内蔵されたソフトウェアに基づいたＯＴＰ生成器によって生成されたＯＴＰも追加で含む（Ｃｏｎｔａｉｎ）ことができる（図６の（ｊ）参照）。それぞれの認証要素（Ｂｉｏｍｅ

ｔｒｉｃ Ｃｏｄｅ、ＯＴＰ、ＰＵＦなど）を独立した形態で転送することもできるが、認証要素が連鎖された（Ｃｏｎｃａｔｅｎａｔｅｄ）一つの認証データとして転送することができる。

【０１１６】

本発明の少なくとも一つの実施例において、サービス提供サーバーに伝達する認証情報には、ユーザーの認証行為を証明するための固有情報をさらに含むことができる。固有情報は、ユーザーの認証が可能なバーコード（Ｂａｒ Ｃｏｄｅ）、ユーザーの電子署名（ｅ－Ｓｉｇｎｉｎｇ）などの形態で実現することが望ましい。また、このようなバーコード、ユーザーの電子署名などは印刷物で出力可能な形態でもよい。スマートカードを用いた認証行為は、領収書や伝票などにバーコードまたは署名の形態で印刷できるようにすることで、相互間の契約に対する信頼性を高められる。本発明の少なくとも一つの実施例において、サービス提供サーバーに伝達される認証情報には、認証情報の転送時点に関する時点情報をさらに含むことができる。本発明の少なくとも一つの実施例において、サービス提供サーバーに伝達される認証情報には、ユーザー登録時点（例えば、Ｐｒｉｖａｔｅ Ｋｅｙ／Ｐｕｂｌｉｃ Ｋｅｙの生成時点あるいは認証サーバーのユーザー登録完了時点）に関する時点情報（すなわち、Ｔｉｍｅ Ｓｔａｍｐ）をさらに含むことができる。

【０１１７】

このようなユーザー認証手続きによると、従来の技術に比べ、次のようなユーザーの経験（Ｕｓｅｒ Ｅｘｐｅｒｉｅｎｃｅ）を提供することができる。例えば、スマートカードを用いてインターネットバンキングに接続する場合を仮定する。インターネットバンキングサービスを提供するサービス提供サーバーに接続するために必要であったユーザーのＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）を入力する従来の過程は、ユーザーの生体情報に基づいた通信トンネルの開設過程で代替することができる。さらに、ユーザーのパスワードを入力する従来の過程は、開設した通信トンネルを介して個人キーに挿入されたコードを含む認証情報を転送する過程で代替することができる。さらに、公開キー認証書のパスワードを入力する従来の過程は、ユーザーの生体情報と公開キー認証書に含まれたマッチング情報を比較する過程で代替することができる。すなわち、本発明の少なくとも一つの実施例によれば、従来のサービス提供サーバーで要求される認証書及びパスワードの入力過程を省略することができる。このように、スマートカードを用いてトンネリング及び認証処理を行うことで、生体情報を用いたシングルサインオン（Ｓｉｎｇｌｅ Ｓｉｇｎ Ｏｎ）が実現可能になる。

【０１１８】

さらに、従来技術のＭｕｌｔｉ－Ｆａｃｔｏｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎによると、ＩＤ・パスワード・認証書パスワード・ＯＴＰなどの全ての認証要素がそれぞれ客体的な認証要素として管理されていた。これに対し、本発明の少なくとも一つの実施例によれば、暗号化されたユーザーの生体情報、生体コード、追加コードが連鎖された形態で認証情報として活用される。したがって、Ｏｎｅ－Ｓｔｏｐ、Ｔａｐ＆Ｐａｙユビキタス認証、よりセキュリティーの強化されたＭｕｌｔｉ－Ｆａｃｔｏｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎの実現が可能になる。

【０１１９】

図７ｂは、本発明の少なくとも一つの実施例に係るユーザー認証手続きを示すフローチャートである。図７ｂに示すユーザー登録手続きは、図１ｂに示す構成を有するユーザー認証システムに適している。

【０１２０】

まず、通信端末機は、ユーザーの生体情報を獲得する（Ｓ７５１）。ここで、生体情報の獲得には、通信端末機に内蔵された生体センサーを用いるか、または通信端末機と接続する外部デバイスの生体センサーを用いることができる。

【０１２１】

次に、通信端末機は、獲得した生体情報を通信端末機に格納されている暗号化された生体情報及び／または通信端末機に格納されている個人キーに挿入された生体コードと比較

する（Ｓ７５２）。すなわち、通信端末機は、獲得した生体情報が、既に格納されている暗号化された生体情報及び／または生体コードとマッチングするか否かを判断する。

【０１２２】

次に、獲得した生体情報が、既に格納されている暗号化された生体情報及び生体コードとマッチングすると判断すると、通信端末機は個人キーに基づいた認証情報をサービス提供サーバーに転送する（Ｓ７５３）。認証情報の転送には仮想私設網（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。例えば、通信端末機はサービス提供サーバーとスマートカード間にＶＰＮを開設し、スマートカードは開設されたＶＰＮを介してサービス提供サーバーに認証情報を転送する。

【０１２３】

サービス提供サーバーは、受信した認証情報の検証を認証サーバーに要請する（Ｓ７５４）。認証サーバーは、既に登録されている公開キーを用いて認証情報を検証する。サービス提供サーバーは認証サーバーの検証結果に基づいてユーザー認証を完了する（Ｓ７５５～７５７）。

【０１２４】

以上の説明では、生体コードが挿入された個人キー・公開キーを用いたユーザー認証方法を説明した。以下で説明する本発明の少なくとも一つの実施例では、ユーザーの生体コードとＩｏＴデバイスの識別情報を関連付けることでＩｏＴデバイスの管理・制御に活用する。以下、図８、図９、図１０ａ、及び図１０ｂを参照してＩｏＴデバイスに関する本発明の少なくとも一つの実施例を説明する。

【０１２５】

図８ａ及び図８ｂは、本発明の少なくとも一つの実施例に係るユビキタス環境でのＩｏＴデバイスのユーザー管理システムの概略図である。

【０１２６】

図８ａに示すように、有無線通信機能を有する複数のＩｏＴデバイス（８５０）が、ＩｏＴネットワーク（８００）を形成している。前述のように、スマートカード（８１０）は、公開キー認証書から個人キー・公開キーを生成することにおいて、生体コードの他にもユーザーが所有するＩｏＴデバイスの識別情報をコード化して生成した追加コード（すなわち、Ｄｅｖｉｃｅ Ｃｏｄｅ）を挿入することができる。これによると、ユーザーの生体コードとＩｏＴデバイスの識別情報を関連付けることで、ユーザーとＩｏＴデバイスの所有関係を証明することができる。

【０１２７】

本発明の少なくとも一つの実施例によれば、スマートカード（８１０）が、生体コードとＤｅｖｉｃｅ Ｃｏｄｅが挿入された個人キー及び公開キーを生成し、個人キーは内部に格納しておき、公開キーは関連するＩｏＴデバイス（８５０）に伝達する。スマートカード（８１０）は、個人キーに基づいた認証情報をＩｏＴデバイス（８５０）に転送し、ＩｏＴデバイス（８５０）は公開キーを用いて認証情報を検証することで、ユーザー（所有者）認証を行うことができる。

【０１２８】

一方、企業・ビル・事業場・Ｈｏｍｅ・Ｃａｒなどの所定の領域をカバーするネットワークでは、ネットワークに接続する各種のＩｏＴデバイスを管理（登録、監視、制御など）するＩｏＴデバイス（例えば、ホームネットワークでのＳｅｔ－ｕｐ Ｂｏｘ、Ａｃｃｅｓｓ Ｐｏｉｎｔなど）、すなわち、中央制御装置（Ｃｅｎｔｒａｌｉｚｅｄ Ｃｏｎｔｒｏｌｌｅｒ、８３０）が存在し得る。中央制御装置（８３０）は、ユーザーインターフェースの役割を追加で行うことができ、さらに、それぞれのＩｏＴデバイス（８５０）の機能を組み合わせて様々な統合サービスを提供する機能を有することができる。この場合、スマートカード（８１０）は、個別ＩｏＴデバイス（８５０）に対応する公開キーを中央制御装置（８３０）に伝達することでネットワーク上のＩｏＴデバイス（８５０）の登録、ＩｏＴデバイス（８５０）の遠隔制御（Ｒｅｍｏｔｅ Ｃｏｎｔｒｏｌ）のためのユーザー（所有者）認証などに用いることができる。

【０１２９】
さらに、スマートカード（８１０）は、公開キーをＩｏＴサービスを提供するＩｏＴサービス事業者のサーバー（８４０）に転送することで、ネットワーク上のＩｏＴデバイスの登録、ＩｏＴデバイスの遠隔制御（Ｒｅｍｏｔｅ　Ｃｏｎｔｒｏｌ）のためのユーザー（所有者）認証などに利用することができる。
【０１３０】
さらに、スマートカード（８１０）は、公開キーをＩｏＴデバイス（８５０）の生産者・販売者のサーバーに転送することで、ＩｏＴデバイスの所有者登録・変更・譲渡などに必要なユーザー（所有者）認証に用いることができる。
【０１３１】
さらに、スマートカードは、通信端末機（８２０、例えば、携帯電話）にそれぞれのＩｏＴデバイスと関連する公開キーを転送し、通信端末機（８２０）は、ＩｏＴデバイスの公開キーを用いることで、それぞれのＩｏＴデバイスを制御する統合リモコンとして使用することができる。例えば、ユーザーはスマートカードに格納された個人キーを用いて通信端末機（８２０）にユーザー認証手続き（１次認証）を行い、１次認証に成功すると、スマートカードとの連動なしで通信端末機（８２０）に格納された公開キーを用いて個別ＩｏＴデバイスまたは中央制御装置（８３０）に制御を行うことができる。
【０１３２】
一方、本発明の少なくとも一つの実施例によれば、特定の生体情報の組合せはＩｏＴデバイスのリセット（Ｒｅｓｅｔ）機能のための用途あるいはＩｏＴデバイスの必須機能を制御するための用途で使用することができる。例えば、特定の生体情報の組合せから生成されたコード情報が挿入された個人キー・公開キーは、ＩｏＴデバイスが故障、制御不能などの状態に陥った時、ＩｏＴデバイスのリセット機能のための用途あるいはＩｏＴデバイスの必須機能を制御するための用途で使用することができる。
【０１３３】
一方、図８ａのスマートカード（８１０）の機能は、通信端末機（８２０）に統合することができる。すなわち、本発明の少なくとも一つの実施例によれば、図８ｂに示すように、通信端末機（８６０）が生体コードとデバイスコードが挿入された個人キー及び公開キーを生成する。通信端末機（８６０）は個人キーを内部に格納しておき、公開キーを関連するＩｏＴデバイス（８５０）、ＩｏＴサービス事業者のサーバー（８４０）、ＩｏＴデバイスの生産者・販売者のサーバー、中央制御装置（８３０）に伝達する。
【０１３４】
以下では、図９ａ乃至図１０ｂを参照して中央制御装置に対して行われるＩｏＴデバイスのユーザー（所有者）登録及び認証手続きを説明する。同一または類似な手続きを個別のＩｏＴデバイス、ＩｏＴサービス事業者のサーバー及びＩｏＴデバイスの生産者・販売者のサーバーに対して行えることは自明である。
【０１３５】
図９ａは、本発明の少なくとも一つの実施例に係るデバイスユーザー（Ｄｅｖｉｃｅ　Ｕｓｅｒ）登録手続きを説明するための概略図である。図９ａに示すユーザー登録手続きは、図８ａに示す構成を有するデバイスユーザー認証システムに適している。
【０１３６】
選択的な（Ｏｐｔｉｏｎａｌ）事前手続きとして、スマートカード（８１０）は、既に格納されている暗号化された生体情報及び／または生体コードが挿入された個人キーを用いてデバイスユーザー登録手続きを行うユーザーに対して生体認証を行うことができる。すなわち、スマートカード（８１０）は、登録されたユーザーのみにデバイスユーザー登録手続きを許容するように構成することができる。
【０１３７】
まず、通信端末機（８２０）は、ユーザーの生体情報を獲得し、獲得したユーザーの生体情報をスマートカード（８１０）に伝達する（Ｓ９０１～Ｓ９０２）。ここで、生体情報の獲得には、通信端末機（８２０）に内蔵された生体センサーを用いるか、または通信

端末機（８２０）と接続する外部機器に備えられた生体センサーを用いることができる。図９ａに示す例とは異なり、他の実施例では、スマートカード（８１０）は、内蔵された生体センサーを用いてユーザーの生体情報をダイレクトに獲得することができる。

【０１３８】

スマートカード（８１０）は、ユーザーの生体情報を既に格納されている公開キー認証書を用いて暗号化し、暗号化された生体情報をコード化（またはトークン化）して生体コードを生成する（Ｓ９０３）。暗号化及びコード化（またはトークン化）アルゴリズムは、スマートカード（８１０）のアプリケーションに内蔵されていても良いし、または公開キー認証書に規定されていても良い。

【０１３９】

次に、スマートカード（８１０）は、通信端末機を介してＩｏＴデバイスに与えられたデバイス識別情報（Ｄｅｖｉｃｅ　Ｉｄｅｎｔｉｔｙ　Ｄａｔａ）を獲得する（Ｓ９０４～Ｓ９０５）。ここで、デバイス識別情報は、通信端末機（８２０）に内蔵されたセンサーを用いるか、または通信端末機（８２０）と接続する外部機器に備えられたセンサーを用いることができる。図９ａに示す例とは異なり、スマートカードは、内蔵されたセンサーを用いてデバイス識別情報をダイレクトに獲得することもできる。

【０１４０】

次に、スマートカード（８１０）は、生体コードと同一または類似の方式でデバイス識別情報からデバイスコードを生成する（Ｓ９０６）。すなわち、スマートカード（８１０）は、デバイス識別情報を暗号化し、暗号化されたデバイス識別情報をコード化またはトークン化してデバイスコードを生成する。

【０１４１】

次に、スマートカード（８１０）は、生体コード及びデバイスコードを公開キー認証書のＥＶ領域（Ｅｘｔｅｎｄｅｄ　Ｖａｌｉｄａｔｉｎ　Ｄｏｍａｉｎ）に挿入して一つのキーペアー（公開キー、個人キー）を生成する。すなわち、生成された個人キー及び公開キーには生体コード及びデバイスコードが挿入されている。個人キー及び公開キーに挿入された生体コードとデバイスコードは、互いに連鎖された（Ｃｏｎｃａｔｅｎａｔｅｄ）形態であっても良い。個人キーは、スマートカード（８１０）内に暗号化された生体情報とともにスマートカード（８１０）に格納される（Ｓ９０７）。図９ａには示してないが、生体コードと同一または類似の方式で生成された他の追加コードを個人キー及び公開キーの生成に用いることができる。公開キー認証書のＥＶ領域に追加的な認証要素として追加することができる。

【０１４２】

次に、スマートカード（８１０）は、通信端末機を介して、中央制御装置に公開キーを提供しながら、デバイスユーザー登録を要請する（Ｓ９０８）。公開キーの転送には、仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。中央制御装置（８３０）は、デバイスユーザーを登録し、公開キーを別の安全なＤＢで管理する（Ｓ９０９～Ｓ９１０）。

【０１４３】

図９ｂは、本発明の少なくとも一つの実施例に係るデバイスユーザー登録手続きを説明するための概略図である。図９ｂに示すユーザー登録手続きは、図８ｂに示す構成を有するデバイスユーザー認証システムに適している。

【０１４４】

選択的な（Ｏｐｔｉｏｎａｌ）事前手続きとして、通信端末機（８６０）は、既に格納されている暗号化された生体情報及び／または生体コードが挿入された個人キーを用いてデバイスユーザー登録手続きを行うユーザーに対して生体認証を行うことができる。すなわち、通信端末機（８６０）は、登録されたユーザーのみにデバイスユーザー登録手続きを許容するように構成することができる。

【０１４５】

まず、通信端末機（８６０）は、ユーザーの生体情報を獲得する（Ｓ９５１～Ｓ９５２

）。ここで、生体情報の獲得には通信端末機（８６０）に内蔵された生体センサーを用いるか、または通信端末機（８６０）と接続する外部機器に備えられた生体センサーを用いることができる。

【０１４６】

通信端末機（８６０）は、ユーザーの生体情報を既に格納されている公開キー認証書を用いて暗号化し、暗号化された生体情報をコード化（またはトークン化）して生体コードを生成する（Ｓ９５３）。暗号化及びコード化（またはトークン化）アルゴリズムは、スマートカードのアプリケーションに内蔵されていても良いし、または公開キー認証書に規定されていても良い。

【０１４７】

次に、通信端末機（８６０）は、ＩｏＴデバイスに与えられたデバイス識別情報を獲得する（Ｓ９５４～Ｓ９５５）。ここで、デバイス識別情報の獲得には、通信端末機に内蔵されたセンサーを用いるか、または通信端末機と接続する外部機器に備えられたセンサーなどを用いることができる。

【０１４８】

次に、通信端末機（８６０）は、生体コードと同一または類似の方式で、デバイス識別情報からデバイスコードを生成する（Ｓ９５６）。すなわち、通信端末機（８６０）は、デバイス識別情報を暗号化し、暗号化されたデバイス識別情報をコード化またはトークン化してデバイスコードを生成する。

【０１４９】

次に、通信端末機（８６０）は、生体コード及びデバイスコードを公開キー認証書のＥＶ領域（Ｅｘｔｅｎｄｅｄ　Ｖａｌｉｄａｔｉｎ　Ｄｏｍａｉｎ）に挿入して一つのキーペアー（公開キー、個人キー）を生成する。すなわち、生成された個人キー及び公開キーには、生体コード及びデバイスコードが挿入されている。個人キー及び公開キーに挿入された生体コードとデバイスコードは、互いに連鎖された（Ｃｏｎｃａｔｅｎａｔｅｄ）形態であっても良い。個人キーは暗号化された生体情報とともに通信端末機（８６０）に格納される（Ｓ９５７）。図９ａには示してないが、生体コードと同一または類似の方式で生成された他の追加コードを個人キー及び公開キーの生成に用いることができる。公開キー認証書のＥＶ領域に追加的な認証要素として追加することができる。

【０１５０】

次に、通信端末機（８６０）は、中央制御装置（８３０）に公開キーを提供しながら、デバイスユーザー登録を要請する（Ｓ９５８）。公開キーの転送には仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。中央制御装置（８３０）は、デバイスユーザーを登録し、公開キーを別の安全なＤＢで管理する（Ｓ９５９～Ｓ９６０）。

【０１５１】

図９ａ及び図９ｂに示すデバイスユーザー登録手続きでは、過去に生成されてスマートカード（８１０）または通信端末機（８６０）に既に格納されている個人キーとは無関係に、新規のキーペアー（個人キー、公開キー）を生成するものとして説明した。しかし、他の実施例では、既に格納されている個人キーに追加的にデバイスコードを挿入する方式で新規のキーペアー（個人キー、公開キー）を生成することができる。

【０１５２】

図１０ａは、本発明の少なくとも一つの実施例に係るデバイスユーザー認証（Ｄｅｖｉｃｅ　Ｕｓｅｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）手続きを説明するための概略図である。図１０ａに示すユーザー認証手続きは、図８ａに示す構成を有するデバイスユーザー認証システムに適している。

【０１５３】

まず、通信端末機（８２０）は、ユーザーの生体情報を獲得し、獲得したユーザーの生体情報をスマートカード（８１０）に伝達する（Ｓ１００１～Ｓ１００２）。ここで、生体情報の獲得には、通信端末機（８２０）に内蔵された生体センサーを用いるか、または

通信端末機（８２０）と接続する外部の生体センサーを用いることができる。図１０ａに示す例とは異なり、他の実施例では、スマートカード（８１０）は、内蔵された生体センサーを用いてユーザーの生体情報をダイレクトに獲得することができる。

【０１５４】

次に、スマートカード（８１０）は、獲得した生体情報を、スマートカード（８１０）に既に格納されている暗号化された生体情報及び／またはスマートカード（８１０）に既に格納されている個人キー内に挿入された（Ｃｏｎｔａｉｎｅｄ）生体コードと比較する（Ｓ１００３）。すなわち、スマートカード（８１０）は、獲得したライブ生体情報（Ｌｉｖｅ　Ｂｉｏｍｅｔｒｉｃ　Ｄａｔａ）が既に格納されている暗号化された生体情報及び／または生体コードとマッチングするか否かを判断する。

【０１５５】

次に、スマートカード（８１０）は、獲得した生体情報が、既に格納されている暗号化された生体情報及び／または生体コードとマッチングすると、個人キーに基づいた認証情報を中央制御装置（８３０）に転送する（Ｓ１００４）。認証情報の転送には仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。例えば、スマートカード（８１０）は中央制御装置（８３０）とＶＰＮを開設するためのトンネリング開始信号を通信端末機（８２０）に転送し、通信端末機（８２０）はトンネリング開始信号に対応して中央制御装置（８３０）とスマートカード（８１０）間にＶＰＮを開設し、スマートカード（８１０）は開設されたＶＰＮを介して中央制御装置（８３０）に認証情報を転送する。

【０１５６】

中央制御装置（８３０）は、既に登録されている公開キーを用いて受信した認証情報を検証し、検証結果に基づいてデバイスユーザー認証を完了する（Ｓ１００５～Ｓ１００７）。本発明の少なくとも一つの実施例において、中央制御装置（８３０）は、ＩｏＴサービス提供サーバー（８４０）または認証サーバー（不図示）にスマートカード（８１０）から受信した認証情報の検証を要請し、その検証結果に基づいてデバイスユーザー認証を完了することもできる。

【０１５７】

図１０ｂは、本発明の少なくとも一つの実施例に係るＵｓｅｒ　Ｄｅｖｉｃｅ認証手続きを説明するための概略図である。図１０ｂに示すユーザー認証手続きは、図８ｂに示す構成を有するデバイスユーザー認証システムに適している。

【０１５８】

まず、通信端末機（８６０）は、ユーザーの生体情報を獲得する（Ｓ１０５１～Ｓ１０５２）。ここで、生体情報の獲得には通信端末機（８６０）に内蔵された生体センサーを用いるか、または通信端末機（８６０）と接続する外部デバイスの生体センサーを用いることができる。

【０１５９】

次に、通信端末機（８６０）は、獲得した生体情報を既に格納されている暗号化された生体情報及び／または既に格納されている個人キー内に挿入された（Ｃｏｎｔａｉｎｅｄ）生体コードと比較する（Ｓ１０５３）。すなわち、通信端末機（８６０）は、獲得した生体情報が、既に格納されている暗号化された生体情報及び／または生体コードとマッチングするか否かを判断する。

【０１６０】

次に、通信端末機（８６０）は、獲得した生体情報が、既に格納されている暗号化された生体情報及び生体コードとマッチングすると、個人キーに基づいた認証情報を中央制御装置（８３０）に転送する（Ｓ１０５４）。認証情報の転送には、仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いることができる。例えば、通信端末機（８６０）は、中央制御装置（８３０）とＶＰＮを開設し、開設したＶＰＮを介して中央制御装置（８３０）に認証情報を転送する。

【０１６１】

中央制御装置（８３０）は、既に登録された公開キーを用いて受信した認証情報を検証し、検証結果に基づいてデバイスユーザー認証を完了する（Ｓ１０５５～Ｓ１０５７）。一部の実施例によっては、中央制御装置（８３０）は、ＩｏＴサービス提供サーバー（８４０）あるいは認証サーバー（不図示）に受信した認証情報の検証を要請し、その検証結果に基づいてデバイスユーザー認証を完了することもできる。

【０１６２】

図１１は、オンライン・オフライン環境によるユビキタス認証システムの概念を示す概略図である。

【０１６３】

あらゆるユビキタス認証がオンライン状態での認証を扱っているが、開発途上国の環境では、全ての地域にインターネットや最低限の通信手段が提供されるわけではない。さらに、地震・台風・洪水・停電・豪雪などの災害によって一時的なオンライン障害が発生する場合がある。このような一時的な・非一時的な制約を克服するために、オンライン環境に基づく認証システムの適切な補完が必要である。例えば、ＡＴＭ、ＰＯＳ、Ｋｉｏｓｋのようなサービス端末機（または公用端末機）は、オフライン環境下でも最小限の現金引出や決済を許容する必要がある。他の例として、スマートホームネットワークが一時的にオフライン環境におかれても、ホーム内のＩｏＴデバイスを統合管理する中央制御装置（Ｃｅｎｔｒａｌｉｚｅｄ　Ｃｏｎｔｒｏｌｌｅｒ）に制限されたアクセス権限を許容する必要がある。さらに他の例として、スマートカーは、オンライン上では無人運転、自動運転、位置情報、ナビゲーションなどの機能を果たすために内部で複数のセンサーまたはＩｏＴデバイスがネットワークを構成している。このようなスマートカーがオフライン環境におかれても、オンライン環境よりは制限された範囲の権限を与える（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）必要がある。

【０１６４】

本発明は、オンライン状態の生体情報（生体コード）、ＰＫＩ、ＯＴＰなどの様々な認証手段のうち一部を用いてオフライン環境での最小限の電力で一部制限されたサービス（例えば、現金引出、飲食購入のための決済、アクセス制御など）を可能にするユーザー認証方法を提供する。本発明の少なくとも一つの実施例において、サービス提供サーバーは、ユーザー登録が完了したユーザーにオフライン環境でのユーザー認証に利用できる所定の認証情報（Ｃｒｅｄｅｎｔｉａｌｓ）またはトークン（Ｔｏｋｅｎ）を提供する。例えば、認証情報は、ユーザー登録手続きでユーザーが保有または所持するスマートカードまたは通信端末機から受信した公開キーから派生した変形公開キーでも良い。

【０１６５】

図１２は、本発明の少なくとも一つの実施例に係るオフライン環境でのユーザー認証手続きを説明するための概略図である。図１２は、スマートカードの使用を仮定しているが、スマートカードの代わりに通信端末機（例えば、スマートフォン）を使用する場合も実質的に同一の方式で適用される。

【０１６６】

まず、オフライン環境での公用端末機（例えば、ＡＴＭ、ＰＯＳ、Ｃｅｎｔｒａｌｉｚｅｄ　Ｃｏｎｔｒｏｌｌｅｒなど）は、ユーザーの生体情報を獲得し、獲得したユーザーの生体情報をスマートカードに伝達する（Ｓ１２０１～Ｓ１２０２）。ここで、生体情報の獲得には、公用端末機に内蔵された生体センサーを用いるか、または公用端末機と接続する外部の生体センサーを用いることができる。図１２に示す例とは異なり、他の実施例では、スマートカードは、内蔵された生体センサーを用いてユーザーの生体情報をダイレクトに獲得することができる。

【０１６７】

次に、スマートカードは、獲得した生体情報を、スマートカードに既に格納されている暗号化された生体情報及び／またはスマートカードに既に格納されている個人キー内に挿入された（Ｃｏｎｔａｉｎｅｄ）生体コードと比較する（Ｓ１２０３）。すなわち、スマートカードは、獲得したライブ生体情報（Ｌｉｖｅ　Ｂｉｏｍｅｔｒｉｃ　Ｄａｔａ）が

、既に格納されている暗号化された生体情報及び／または生体コードとマッチングするか否かを判断する。

【０１６８】

次に、スマートカードは、獲得した生体情報（Ｂｉｏｍｅｔｒｉｃ　Ｄａｔａ）が、既に格納されている暗号化された生体情報及び／または生体コードとマッチングすると、Ｐｒｉｖａｔｅ　Ｋｅｙに基づいた認証情報及び事前にサービス提供サーバーから提供された変形公開キーに基づいた認証情報を公用端末機に転送する（Ｓ１２０４）。

【０１６９】

オフライン環境にある公用端末機は、受信した認証情報の検証をサービス提供サーバーに要請せずに、オンライン環境より制限された範囲のＡｕｔｈｅｎｔｉｃａｔｉｏｎを行う。すなわち、所定の範囲に制限されたサービス・取引・アクセス権限を許容する。一部の実施例では、公用端末機は、受信した認証情報に挿入された検証コードが同一の公開キー認証書に基づいて生成されたものであるかを検証することができる。

【０１７０】

関連する取引情報（すなわち、取引詳細またはサービス提供詳細及び関連する認証情報）は、後でオンライン上での取引詳細の精算のため、スマートカード及び／または公用端末機のＳｅｃｕｒｅ　Ｅｌｅｍｅｎｔなどの安全な領域格納される（Ｓ１２０５）。さらに、取引情報は、個人キー・公開キーを用いて暗号化された状態で格納することができる。

【０１７１】

再びオンライン環境に復帰すると、公用端末機は、格納された取引情報をサービス提供サーバーに転送する（Ｓ１２０６）。サービス提供サーバーは、認証サーバーを介して取引情報に含まれた認証情報を検証し、検証結果に基づいて取引情報に含まれた取引詳細を精算する（Ｓ１２０７～Ｓ１２０９）。

【０１７２】

図１３は、本発明の少なくとも一つの実施例に適用可能な例示的な応用分野を示す表である。

【０１７３】

ユーザー認証には複合的な方式の認証を用いることができるが、徐々にスマートカードにクレジットカード＋電子身分証明書＋電子パスポート＋運転免許証などの様々な用途の情報を統合して使用することができる。

【０１７４】

図１３の表に示すように、本発明の多様な実施例を適用可能な応用分野は大きく４つの領域に分けることができる。

【０１７５】

金融及び身分証明領域（Ｆｉｎａｎｃｉａｌ　ａｎｄ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｓｅｃｔｉｏｎ）は、オンライン・オフライン上の金融取引及び様々な身分証明に伴うユーザー認証を意味する。このような分野に適用するため、スマートカード（または通信端末機）は、電子身分証明書、年金、医療保険、電子ウォレット、デジタル貨幣、医療記録、運転免許証、電子選挙、割引クーポン（Ｃｒｅｄｉｔ　Ｃａｒｄ／Ｄｅｂｉｔ　Ｃａｒｄ／Ｃｙｂｅｒ　Ｍｏｎｅｙ／Ｅ－Ｗａｌｌｅｔ／Ｄｉｇｉｔａｌ　Ｃｏｕｐｏｎ／Ｆｉｎａｎｃｉａｌ　Ｄａｔａ／Ｎａｔｉｏｎａｌ　ＩＤ／Ｄｒｉｖｅｒ‘ｓ　Ｌｉｃｅｎｓｅ／Ｍｅｄｉｃａｌ　Ｉｎｆｏｒｍａｔｉｏｎ／ｅ－Ｖｏｔｉｎｇ／Ｐｅｎｓｉｏｎ）などの多様な情報をさらに格納することができる。このような情報のうち一部の情報は、関連するサービス用途の公開キー認証書のＥＶ領域に挿入された形態であっても良い。例えば、電子身分証明書の用途で使用するために発行された公開キー認証書のＥＶ領域には、個人に与えられた固有識別情報（例えば、住民登録番号、社会保障番号など）を表すコードが挿入されても良い。さらに、一部の情報は関連するサービス用途の公開キー認証書と同一の領域に前もって格納されても良い。

【０１７６】

物理的アクセス領域（Ｐｈｙｓｉｃａｌ　Ａｃｃｅｓｓ　Ｓｅｃｔｉｏｎ）は出入制御などを目的とする応用領域で、スマートカード（または通信端末機）はＩＤ　Ｂａｄｇｅまたは出入カードの役割を果たすことができる。このような応用領域で用いるための個人キー・公開キーにはスマートカード（または通信端末機）の使用位置情報（例えば、ＧＥＯ、ＧＩＳ、ＧＰＳ情報など）あるいはこれをコード化したコードを追加することができる。追加した位置情報またはコードは、変造、偽装出入などを摘発するための追加的な認証要素として活用することができる。

【０１７７】

シングルサインオン（ＳＳＯ　Ｓｅｃｔｉｏｎ：統合認証）領域は、１回のユーザー認証過程で幾つかの独立したソフトウェアシステム上の資源を利用可能にする認証機能である。本発明の少なくとも一つの実施例においては、生体マッチング及び生体コードが挿入された個人キー・公開キーに基づいて認証手続きを行うことで、サービス提供サーバー（１３０）で要求される認証書及びパスワードの入力過程を省略することができ、生体シングルサインオン（Ｓｉｎｇｌｅ　Ｓｉｇｎ　Ｏｎ）の実現が可能である。本発明の少なくとも一つの実施例においては、さらに、ユーザーが保有または所持する任意の通信端末機（例えば、スマートフォン）で生成された個人キーを自身のＣｌｏｕｄに格納しておき、ユーザーが保有または所持する他の通信端末機（例えば、タブレットＰＣ、スマートウォッチなど）で当該個人キーをダウンロードして使用することができる。これによると、同一目的の個人キーを通信端末機ごとに生成する必要がなく、一台の通信端末機で生成された個人キーをユーザーが保有または所持する複数の通信端末機で共有することができる。

【０１７８】

デバイスユーザー認証セクション（Ｄｅｖｉｃｅ　Ｕｓｅｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｃｔｉｏｎ）は、ＩｏＴデバイスの登録あるいはＩｏＴデバイスへのアクセス制御のためのユーザー認証を支援するための応用領域を表す。このような応用領域に用いられる公開キー・個人キーには、生体コードのみならず、ＩｏＴデバイスの識別情報をコード化したＤｅｖｉｃｅ　Ｃｏｄｅがさらに挿入されている。さらに、公開キーはそれぞれのＩｏＴデバイス、中央制御装置、ＩｏＴサービスサーバー、ＩｏＴ　Ｖｅｎｄｏｒサーバーなどに伝達され、デバイスユーザー認証、遠隔制御などに用いられる。

【０１７９】

図１４は、様々な生体情報あるいはこれらの組合せが様々な用途に分けられて利用可能であることを説明するための概略図である。様々な生体情報あるいはこれらの組合せを様々な用途に分けて使用できることを説明するための図である。

【０１８０】

前述のように、本発明の少なくとも一つの実施例においては、ユーザーの互いに異なる複数の生体情報及び／またはこれらの組合せを用いることができる。例えば、図１４は、同一種類の異なる生体情報の例として、１０個の指紋情報が互いに異なる用途で用いられる例を示している。すなわち、本発明の少なくとも一つの実施例においては、同一種類の生体情報をそれぞれコード化して一つの個人キー・公開キーに挿入するか、またはそれぞれの生体情報ごとに別個の個人キー・公開キーをそれぞれ生成することもできる。

【０１８１】

さらに、図１４には、生体情報の様々な組合せが互いに異なる用途で用いられることが例示されている。すなわち、本発明の少なくとも一つの実施例においては、複数の生体情報の組合せをそれぞれコード化し、一つの個人キー・公開キーに挿入することができ、それぞれの組合せごとに別個のキーペアー（個人キー・公開キー）を生成することもできる。さらに、同一の生体情報の組合せにはそれぞれ生体情報の入力順序を与えることができる。

【０１８２】

一方、本発明の様々な実施例の説明において、明細書全般にわたって、生体コードが挿入された個人キーの他に、生体マッチングに用いられる暗号化された生体情報がスマートカードまたは通信端末機に格納されていることを前提とした。しかし、このような特徴が

、本発明の全ての実施例で必須的な構成要素をして扱われるのは望ましくない。例えば、実施例によっては、暗号化された生体情報がスマートカードまたは通信端末機に格納されずに、生体マッチングには個人キーに挿入された生体コードのみを用いることができる。さらに、実施例によっては、政府機関（例えば、行政部、捜査機関、出入国管理部など）で管理する個人の生体情報のハッシュ値（Ｈａｓｈ　Ｖａｌｕｅ）を用いることができる。ハッシュ値はスマートカードの一部領域に前もって格納することができ、関連する機関で発行した公開キー認証書のＥＶ領域に挿入することもできる。さらに、生体マッチングに用いる暗号化された生体情報は、公開キー認証書に規定した暗号化アルゴリズムによって暗号化された生体情報でも良いし、生体コードが挿入された個人キーを用いて暗号化された生体情報でも良い。さらに、公開キー認証書を用いて暗号化された生体情報を個人キーで追加に暗号化した状態で個人キーとともに格納しても良い。

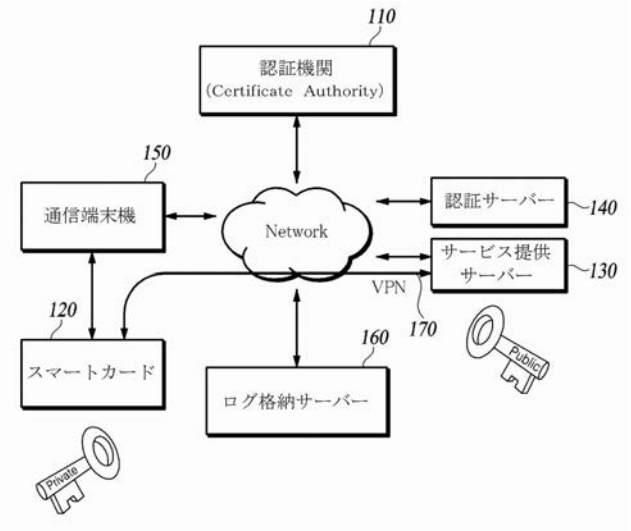
【０１８３】

一方、前述した方法は、コンピューターで読み取り可能な記録媒体にコンピューターで読み取り可能なコードとして実現することができる。コンピューターで読み取り可能な記録媒体は、コンピューターシステムによって読み込み可能なデータを格納するあらゆる種類の記録装置を含む。すなわち、コンピューターで読み取り可能な記録媒体は、マグネチック格納媒体（例えば、ＲＯＭ、フロッピーディスク、ハードディスクなど）、光学的判読媒体（例えば、ＣＤ－ＲＯＭ、ＤＶＤなど）、及びキャリアウェーブ（例えば、インターネットを介しての転送）のような格納媒体を含む。さらに、コンピューターで読み取り可能な記録媒体は、ネットワークで接続したコンピューターシステムに分散されて分散方式でコンピューターで読み取り可能なコードを格納し、実行することができる。

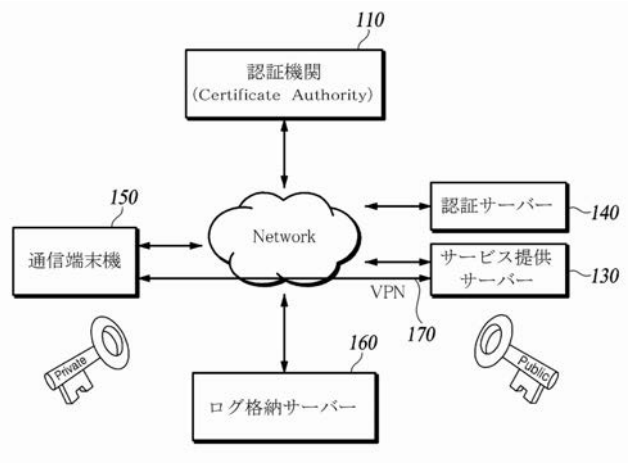
【０１８４】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることが可能であることが当業者に明らかである。そのような変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

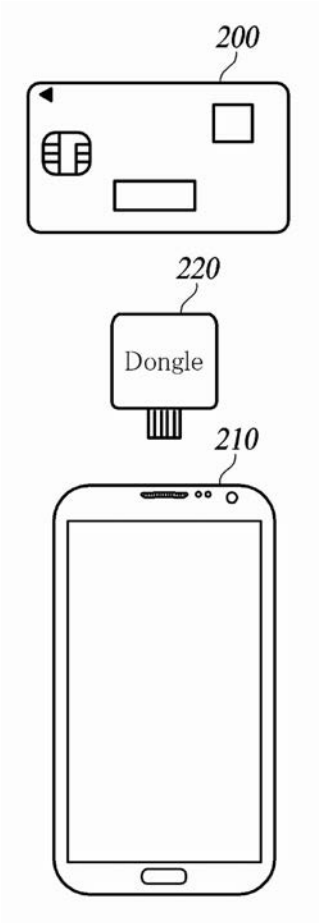
【図１ａ】



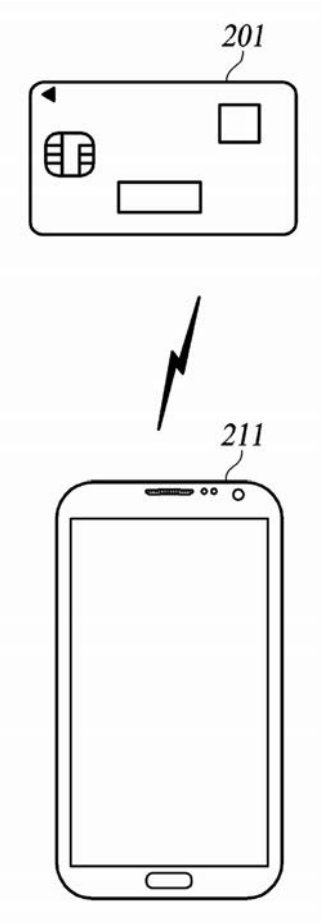
【図１ｂ】



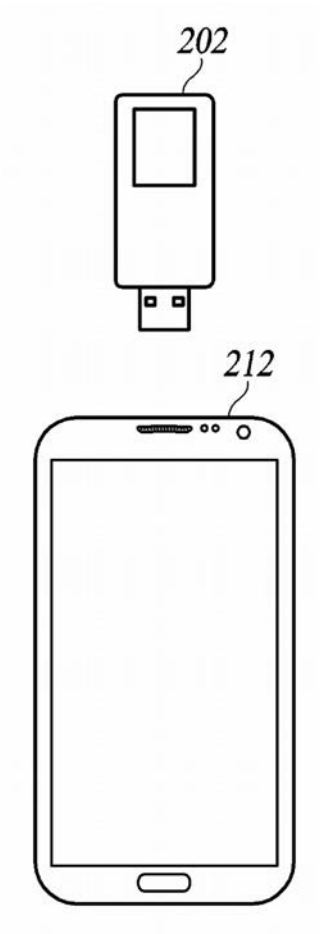
【図２ａ】



【図２ｂ】



【図２ｃ】

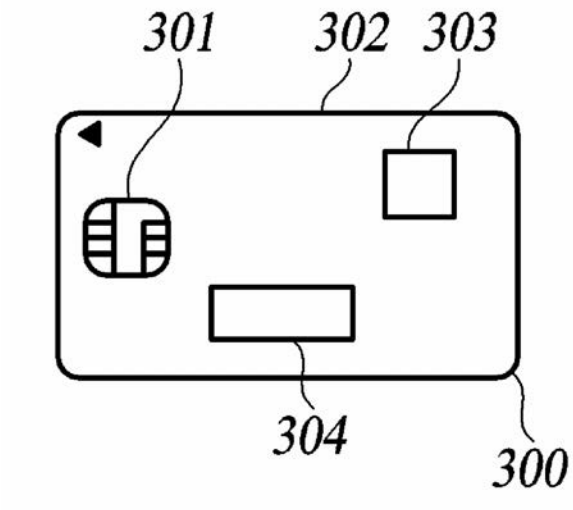


【図３ａ】

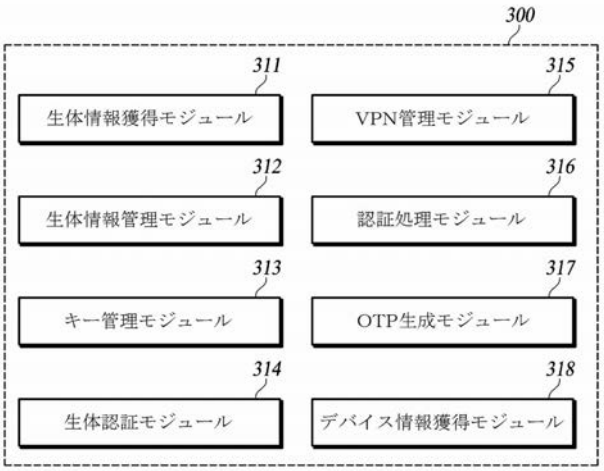
Application Layer
• 生体情報獲得モジュール (Biometric Data Acquisition Module) • 生体情報管理モジュール (Biometric data Manamgement Module) • 生体認証モジュール (Biometric Authentication Module) • デバイス情報獲得モジュール (Device Data Acquisition Module) • VPN管理モジュール (VPN Management Module) • OTP生成モジュール (OTP Generation Module) • キー管理モジュール (Key Management Module) • 認証処理モジュール (Authentication Execution Module)

Physical Layer
• CPU • Memory • I/O Port • Display (optional) • Biometric sensor (optional) • Physical Unclonable Function (PUF) circuit (optional)

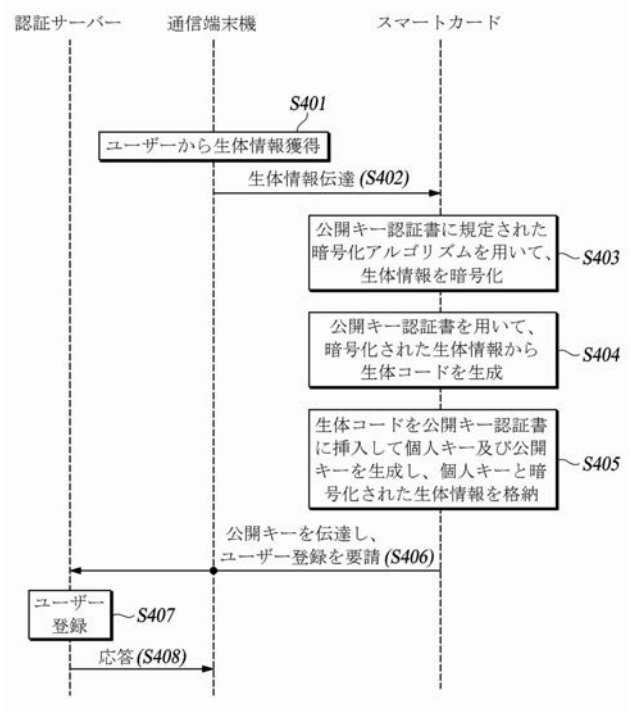
【図３ｂ】



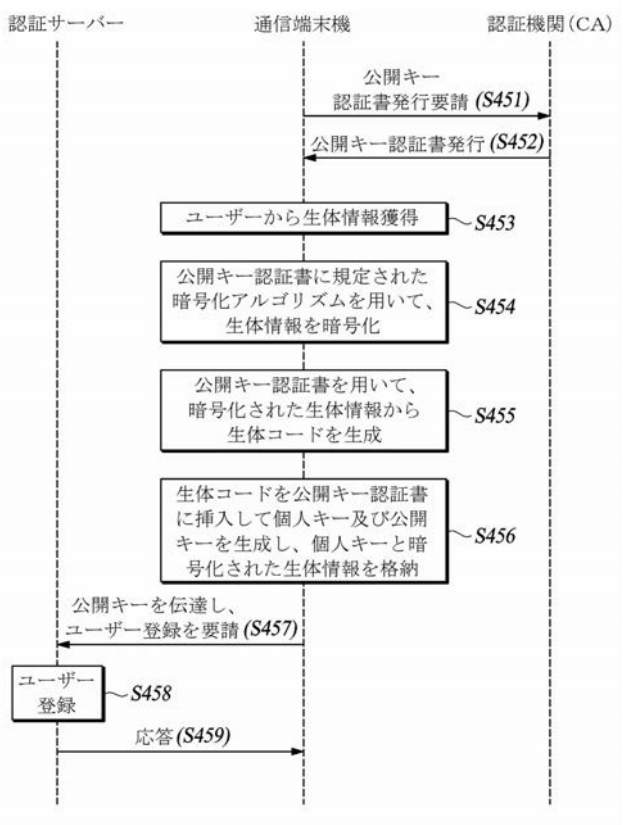
【図３ｃ】



【図４ａ】



【図４ｂ】



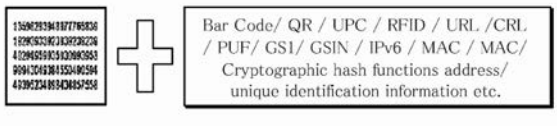
【図５】

<ユーザー登録前>

Public Key Certificate
Version / Serial Number / Signature algorithm / Hash algorithm / Issuer Name / Validity Period / Public Key Subject Distinguished Name / Subject Public Key Information / 発行者署名
拡張フィールド
(Empty)

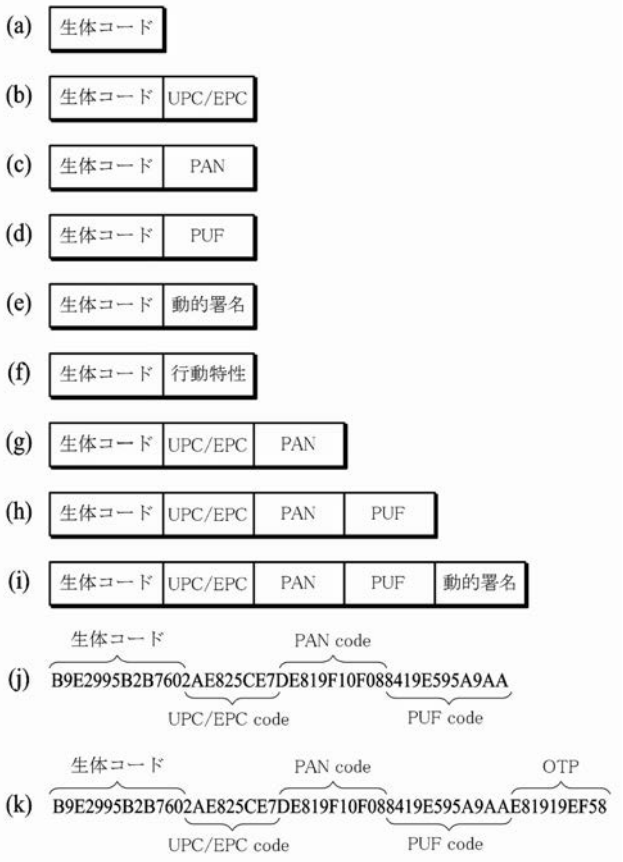
(a)

<ユーザー登録後>

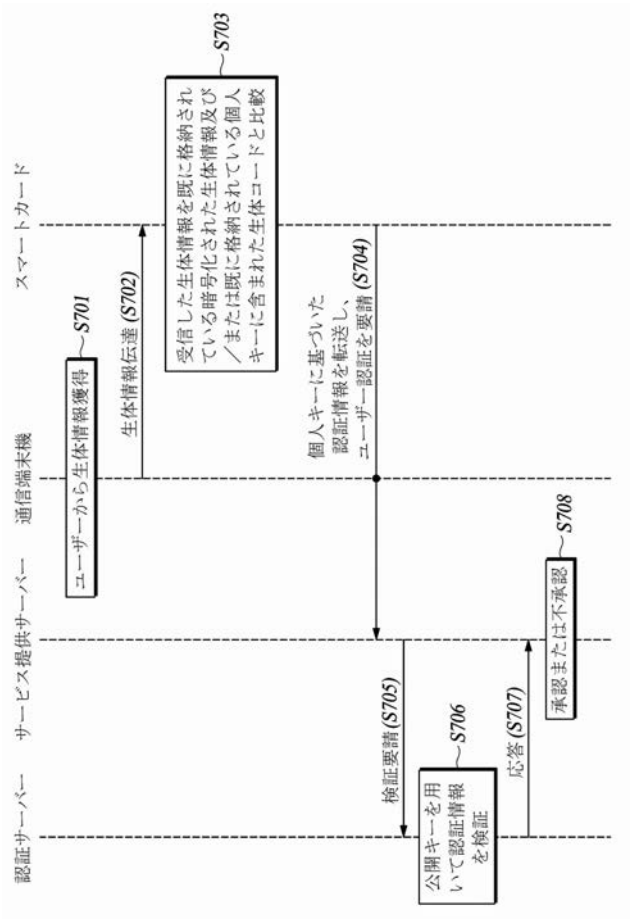
Public Key Certificate
Version / Serial Number / Signature algorithm / Hash algorithm / Issuer Name / Validity Period / Public Key Subject Distinguished Name / Subject Public Key Information / Issuer's Signature
拡張フィールド
• 生体コード＋一つ以上の追加コード 

(b)

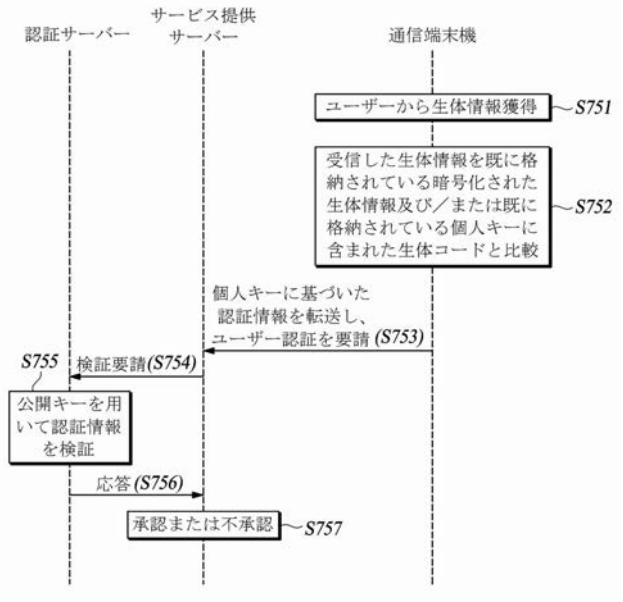
【図６】



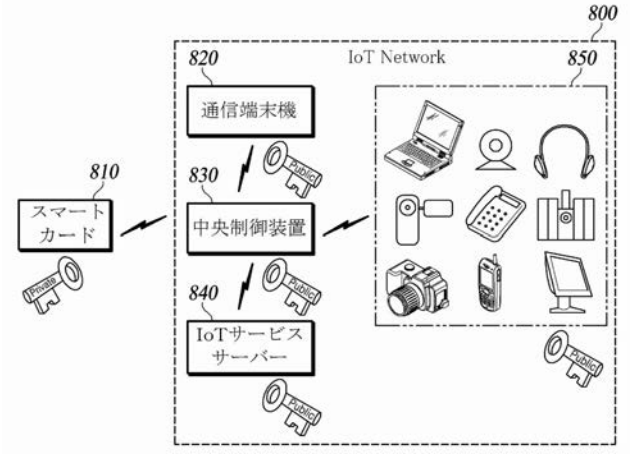
【図７ａ】



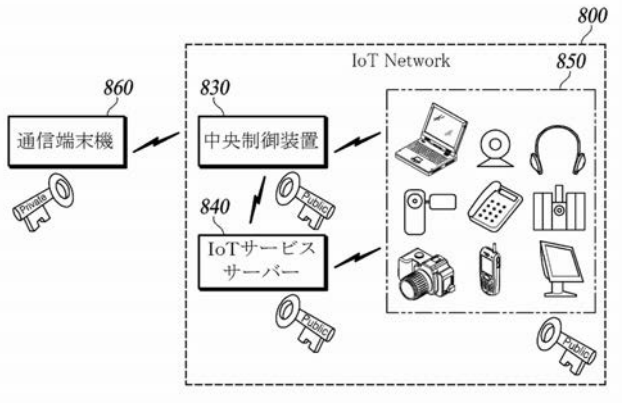
【図７ｂ】



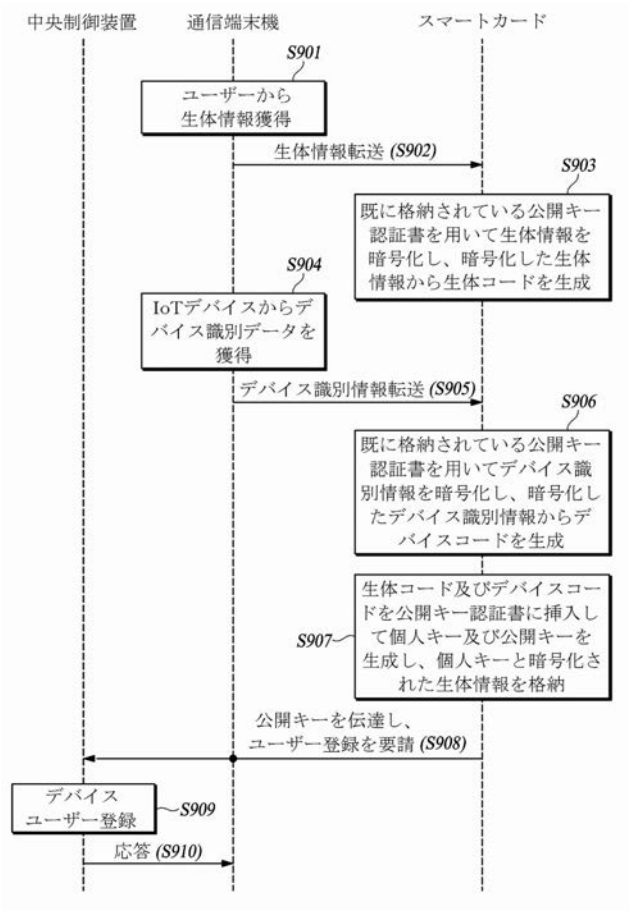
【図８ａ】



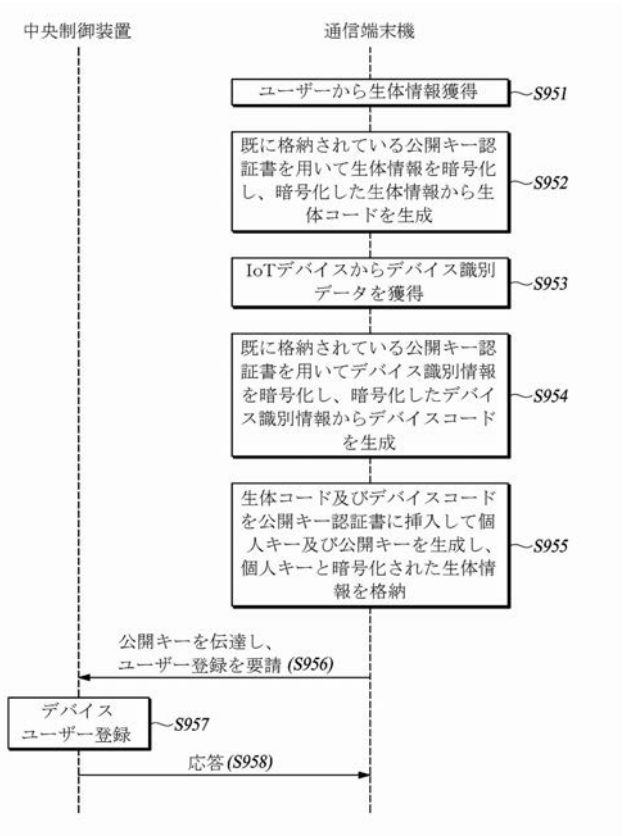
【図８ｂ】



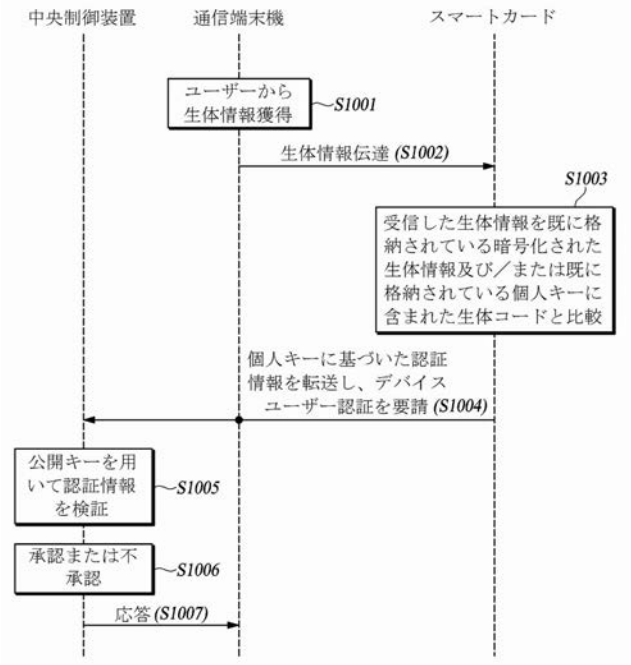
【図９ａ】



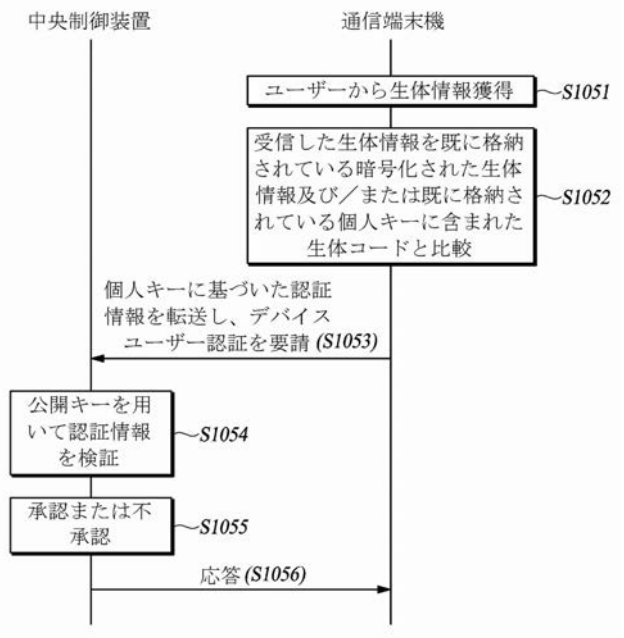
【図９ｂ】



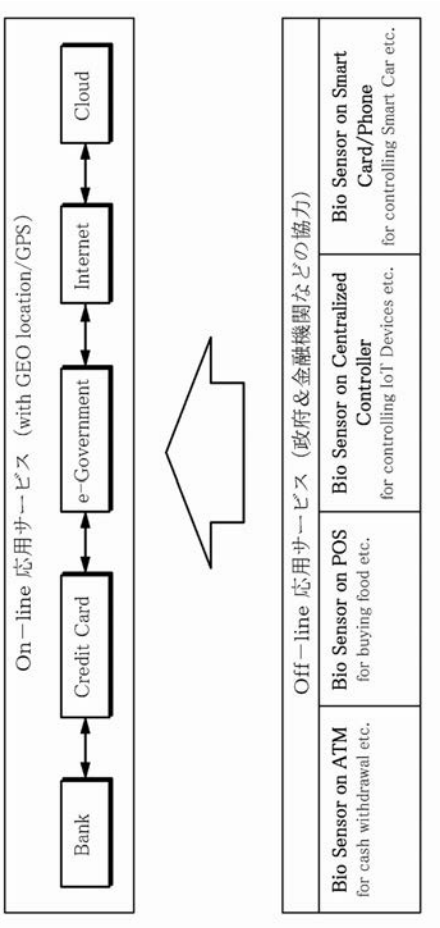
【図１０ａ】



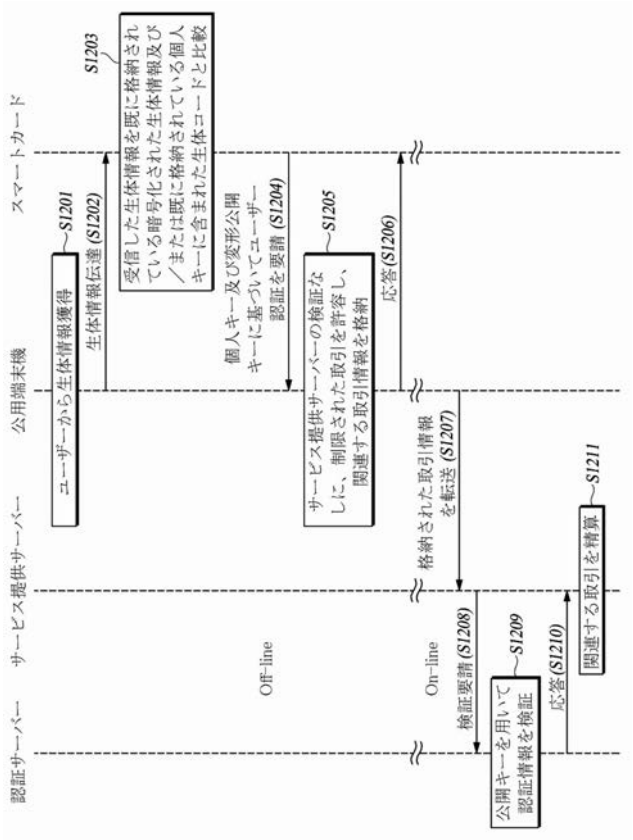
【図１０ｂ】



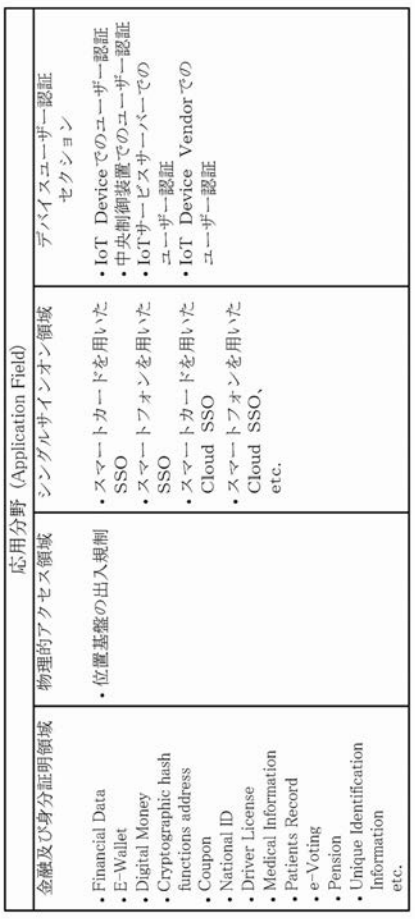
【図１１】



【図１２】

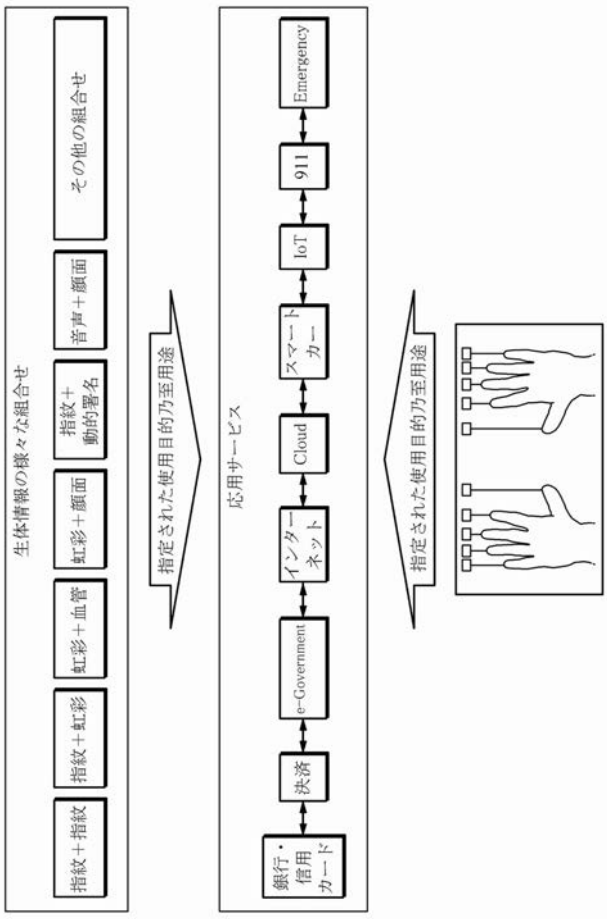


【図１３】



応用分野 (Application Field)			
金融及び身分証明領域	物理的アクセス領域	シングルサインオン領域	デバイスユーザー認証セクション
• Financial Data • E-Wallet • Digital Money • Cryptographic hash functions address • Coupon • National ID • Driver License • Medical Information • Patients Record • e-Voting • Pension • Unique Identification Information etc.	• 位置基盤の出入規制	• スマートカードを用いた SSO • スマートフォンを用いた SSO • スマートカードを用いた Cloud SSO • スマートフォンを用いた Cloud SSO、 etc.	• IoT Device でのユーザー認証 • 中央制御装置でのユーザー認証 • IoTサービスサーバーでのユーザー認証 • IoT Device Vendor でのユーザー認証

【図１４】



【手続補正書】
【提出日】平成30年7月31日(2018.7.31)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置によって行われるユーザー認証方法において、前記携帯用装置は生体コードを含む検証コードが挿入された個人キー及び前記生体コードが得られた暗号化された生体情報または生体情報の組合せが格納されており、前記ユーザー認証方法は、
ユーザーの生体情報または生体情報の組合せを獲得する工程と、
前記ユーザーの生体情報または生体情報の組合せを前記携帯用装置に既に格納されている暗号化された生体情報及び前記生体コードのうち少なくとも一つと比較する工程と、
前記ユーザーの生体情報または生体情報の組合せが、前記暗号化された生体情報及び前記生体コードのうち少なくとも一つとマッチングすると、前記個人キーに挿入された検証コードを含む認証情報を遠隔客体に転送して前記ユーザーの認証を要請する工程と、
を備える、
ユーザー認証方法。
【請求項２】
前記個人キーに挿入された検証コードは、前記携帯用装置に与えられた固有識別情報から得られた追加コード、前記ユーザーの認証を要請する位置を表す位置情報から得られた追加コード、前記ユーザーに与えられた固有識別情報から得られた追加コード、前記ユーザーの行動特性を表す特性情報から得られた追加コード、及びＩｏＴデバイスに与えられたデバイス識別情報から得られた追加コードのうち少なくとも一つをさらに含む、
請求項１に記載のユーザー認証方法。
【請求項３】
前記認証情報は、前記携帯用装置に内蔵されたＯＴＰ生成モジュールによって生成されたＯＴＰをさらに含む、
請求項１に記載のユーザー認証方法。
【請求項４】
前記認証情報は、前記認証情報の転送時点に関する情報をさらに含む、
請求項１に記載のユーザー認証方法。
【請求項５】
前記認証情報は、前記ユーザーの認証を要請する位置に関する情報をさらに含む、
請求項１に記載のユーザー認証方法。
【請求項６】
前記認証情報は、前記個人キーの生成時点に関する情報をさらに含む、
請求項１に記載のユーザー認証方法。
【請求項７】
前記認証情報の転送には、仮想私設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）を用いる、
請求項１に記載のユーザー認証方法。
【請求項８】
前記仮想私設網の目的地ＵＲＬは、前記個人キーの拡張フィールドに含まれている、
請求項７に記載のユーザー認証方法。
【請求項９】
前記携帯用装置は、スマートカードまたは移動通信端末機である、

請求項１に記載のユーザー認証方法。
【請求項１０】
公開キー認証書に基づいた認証管理システムでユーザーが保有する携帯用装置とネットワークで接続される遠隔客体によって行われる認証管理方法において、
前記携帯用装置からユーザーの生体情報または生体情報の組合せから得られた生体コードを含む検証コードが挿入された個人キーに対応する公開キーを受信し、受信した公開キーに基づいてユーザー登録を行う工程と、
前記携帯用装置から前記個人キーに挿入された検証コードを含む認証情報を受信し、前記公開キーを用いて受信した認証情報を検証し、検証結果に基づいて前記ユーザーの認証を行う工程と、
を備える、
認証管理方法。
【請求項１１】
公開キー認証書に基づいた認証管理システムでサービスを提供する公用端末機及び前記公用端末機を管理するサービス提供サーバーによって行われる認証管理方法において、
前記サービス提供サーバーが、携帯用装置からユーザーの生体情報または生体情報の組合せから得られた生体コードを含む検証コードが挿入された個人キーに対応する公開キーを受信し、受信した公開キーに基づいてユーザー登録を行う工程と、
前記公用端末機が、前記携帯用装置から前記個人キーに挿入された検証コードを含む認証情報を受信し、受信した認証情報の前記公開キーを用いた検証を前記サービス提供サーバーに要請し、前記検証の結果に基づいて前記ユーザーの認証を行う工程と、
前記ユーザーの認証に成功すると、前記公用端末機がサービスを提供する工程と、
を備える、
認証管理方法。
【請求項１２】
前記ユーザー登録を行う工程は、前記公用端末機と前記サービス提供サーバーが互いにオフライン状況におかれた場合に使用するための用途で、前記サービス提供サーバーが前記公開キーを応用した変形公開キーを生成し、前記変形公開キーを前記携帯用装置に伝達する工程を含む、
請求項１１に記載の認証管理方法。
【請求項１３】
前記公用端末機と前記サービス提供サーバーが互いにオフライン状況におかれると、前記公用端末機が前記携帯用装置から前記個人キーに挿入された検証コード及び前記変形公開キーに挿入された検証コードを受信し、受信した検証コードが同一の公開キー認証書に基づいて生成されたものか否かを検証し、検証に成功すると、オンライン状況より制限された範囲のサービスを提供する工程と、
前記オフライン状況がオンライン状況に変わると、前記公用端末機が前記検証コード及びサービス提供情報を前記サービス提供サーバーに伝達し、前記サービス提供サーバーが前記検証コードを検証し、検証結果に基づいて前記サービス提供情報を生産する工程と、
をさらに備える、
請求項１２に記載の認証管理方法。

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
Ｇ０６Ｆ　21/62	*(2013.01)*	Ｇ０６Ｆ	21/44	
		Ｇ０６Ｆ	21/62　３０９	

Ｆターム(参考) 5J104 AA07 AA16 EA05 KA01 KA16 NA02 NA37 NA38 PA07