(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2013-534652
(P2013-534652A)
(43)公表日　平成25年9月5日(2013.9.5)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/24	165C	4C038
A61B 5/117	(2006.01)	A61B	5/10	320Z	5B043
G06F 21/32	(2013.01)	G06F	21/20	132	
G06F 21/60	(2013.01)	G06F	21/24	160C	
G06T 7/00	(2006.01)	G06T	7/00	510B	

審査請求 未請求　予備審査請求 未請求　（全 52 頁）

(21)出願番号　特願2012-556636 (P2012-556636)
(86)(22)出願日　平成23年3月10日 (2011.3.10)
(85)翻訳文提出日　平成24年10月17日 (2012.10.17)
(86)国際出願番号　PCT/IB2011/051002
(87)国際公開番号　WO2011/111011
(87)国際公開日　平成23年9月15日 (2011.9.15)
(31)優先権主張番号　61/313,145
(32)優先日　平成22年3月12日 (2010.3.12)
(33)優先権主張国　米国 (US)

(71)出願人　512225955
オーエス　－　ニュー　ホライズン　パーソナル　コンピューティング　ソリューションズ　リミテッド
イスラエル国，９０８０５　メヴァスセレト　ザイオン，ピー．オー．ボックス　８４２７５，１０／３　エフロニ　ストリート
(74)代理人　100114775
弁理士　高岡　亮一
(74)代理人　100121511
弁理士　小田　直

最終頁に続く

(54)【発明の名称】保護個人データ処理および管理システム

(57)【要約】
高度に保護された個人データを管理するためのシステム、方法およびパーソナル装置を提供する。システムおよびパーソナル装置は補完的であり、高度に保護された個人データ、大量の、安全かつ保護されたデータへのアクセス、保存および管理手法のいずれも提供する。装置とサービスプロバイダとを安全に接続することにより、システムと独立して装置を用いることができる。装置は、固有ユーザにより固有に識別され、ユーザの複数の個人生物学的識別パラメータを読み出すための複数のバイオメトリックセンサを備えたセンサモジュールと、それ自体に保存されたユーザの個人生物学的識別パラメータの肯定的な認証を行う認証ユニットとを含む。この方法は、システムにアクセスし、高度に保護された個人データを、外部の事前登録済サービスプロバイダおよび他の登録済システムユーザと送受信するために、その所有者が、装置の安全かつ保護された動作を支援する。
【選択図】図１

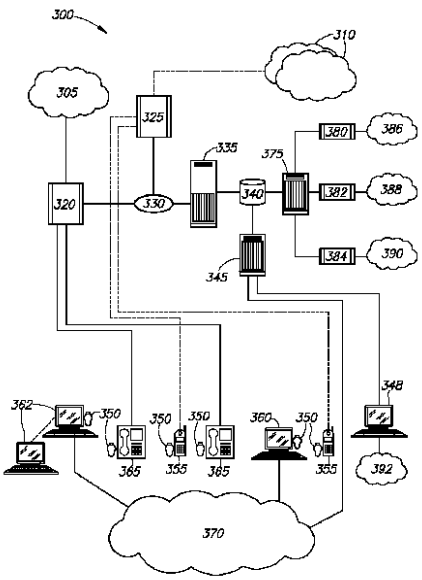


FIG.1

【特許請求の範囲】
【請求項１】
（ａ）ユーザにより固有に識別される装置を保持する前記ユーザの複数の個人生物学的識別パラメータを読み出すための複数のバイオメトリックセンサを備えたセンサモジュールと、
（ｂ）前記センサモジュールと通信し、前記個人生物学的識別パラメータを処理し、前記ユーザに関連する個人の保護データおよびドキュメンテーションファイルを処理および管理する処理モジュールと、
（ｃ）前記処理モジュールと通信し、前記センサモジュールにより読み出され、前記処理モジュールにより処理された、前記ユーザの個人生物学的識別パラメータと、それ自体に保存されている、事前に記録された個人生物学的識別パラメータセットと、を比較することにより、前記ユーザのアイデンティティを受信および確認するように構成されている認証ユニットと、
（ｄ）前記処理モジュールと通信し、前記ユーザのデータファイルの圧縮による暗号化および／または復号による復元を実行する暗号化モジュールと、
（ｅ）前記処理モジュールおよび前記暗号化モジュールと通信し、前記ユーザのデータおよびドキュメンテーションファイルを保存するメモリモジュールと、
（ｆ）前記処理モジュールと通信し、前記装置と外部デバイスとを接続する通信およびデータ接続手段と、を備えており、
前記ユーザが保存した個人データおよび前記固有ユーザに関連するドキュメンテーションファイルへのアクセスが、前記認証ユニットによる、前記ユーザの個人生物学的識別パラメータの肯定的な認証後のみに有効になる、それ自体に保存されている前記個人の保護データおよび前記ドキュメンテーションファイルを管理する装置。
【請求項２】
前記複数のバイオメトリックセンサは、前記装置を保持する前記ユーザに関連する複数の個人生物学的識別パラメータを連続的に読み出し、前記複数の個人生物学的識別パラメータのいずれかに変化が生じた場合に、前記保存された個人データファイルへのアクセスを拒絶し、前記装置の動作を完全に停止する、請求項１に記載の装置。
【請求項３】
前記複数のバイオメトリックセンサの少なくとも１つは、前記ユーザのライフサインパラメータの少なくとも１つを測定および記録するように構成されたライフサイン検出器である、請求項１に記載の装置。
【請求項４】
前記ユーザのライフサインパラメータの少なくとも１つは、脈拍測定インジケータ、体内酸素飽和度インジケータ、体温測定インジケータ、皮膚電気活性インジケータ、体内呼吸インジケータ、および物質的または感情的ストレスインジケータを含む群の任意のライフサインインジケータにより測定される、請求項３に記載の装置。
【請求項５】
前記ライフサインインジケータの群の任意の１つがクリティカルレベルを検出した時は常に、前記装置は、登録済緊急センタの任意の群に対して緊急呼出しを起動し、前記ユーザ識別データファイル、前記ユーザの個人医療データファイル、前記ユーザのライフサインパラメータおよび前記ユーザの位置の測定セットを含む、前記ユーザに関連する情報を含む任意の群のデータファイルを、前記登録済緊急センタに送信するように構成される、請求項３に記載の装置。
【請求項６】
前記処理モジュール、並びに前記通信およびデータ接続手段モジュールと通信する救急ボタンをさらに備えており、前記救急ボタンを作動させると、
前記装置と任意の群の登録済緊急センタとの通信が起動し、緊急呼出しにより、前記ユーザの前記識別データ、前記ユーザの前記個人医療データファイル、および前記ユーザの位置を含む、前記装置の前記固有ユーザに関連する情報を含む任意の群のデータファイル

が伝送される、請求項１に記載の装置。
【請求項７】
前記装置は、銀行、クレジットカード会社、クリニック、病院、医療保険会社、地方自治体、公益事業団体、および前記ユーザによって頻繁にアクセスされるウェブサイトを含む任意の群のサービスプロバイダと通信するように構成されており、これにより、前記ユーザは、前記サービスプロバイダの群によって処理、保存、および前記ユーザ装置に提供される前記ユーザ個人データおよびドキュメンテーションファイルにアクセスかつそれを管理可能になる請求項１に記載の装置。
【請求項８】
前記外部デバイスは、遠隔サーバ、ローカルサーバ、ホストコンピュータ、音声またはデータ通信手段、および携帯電話を含む群の任意の１つを備えている、請求項１に記載の装置。
【請求項９】
前記緊急呼出しは、前記装置の接続および通信手段によるインターネット、任意のホストコンピュータを通じたインターネット、音声およびデータ通信デバイス、および任意の携帯電話ネットワークを直接介した、保護サーバを含む通信手段の群の任意の１つを通じて起動される、請求項５に記載の装置。
【請求項１０】
前記緊急呼出しは、前記装置の接続および通信手段によるインターネット、任意のホストコンピュータを通じたインターネット、音声およびデータ通信デバイス、および携帯電話ネットワークを直接介した、保護サーバを含む通信手段の群の任意の１つを通じて起動される、請求項６に記載の装置。
【請求項１１】
前記通信およびデータ接続手段は、ホストコンピュータに取り付けられた任意のデータインターフェースコネクタ、携帯電話に取り付けられた小型ＵＳＢまたは互換性のある工業データインターフェースコネクタ、近接場無線通信インターフェース、磁気リーダインターフェース、および誘導またはＲＦ通信を利用した非接触通信インターフェースに基づくスマートカードリーダを含む接続および通信デバイスの群の少なくとも１つを備えている、請求項１に記載の装置。
【請求項１２】
前記メモリモジュールは、アクセス可能なメモリサイズである少なくとも１０ギガバイトの記憶容量を有する、Ｆｌａｓｈおよび／またはＮａｎｏ型の固体読み出しおよび書き込みメモリ要素を有する取り外しかつアップグレード可能な小型ＰＣＢ回路基板を備えている、請求項１に記載の装置。
【請求項１３】
前記ユーザの個人生物学的識別パラメータの肯定的な認証後のみに活性化可能な磁気帯要素をさらに備えており、
前記磁気帯は、前記装置内に隠れるように構成されており、活性化すると、機械に通されるために前記装置から外に延伸し、クレジットカードリーダ、ＡＴＭ、および販売時磁気帯読み出しデバイスを含む任意の群のデバイスにより読み出されるように構成されている、請求項１に記載の装置。
【請求項１４】
前記処理モジュールと通信し、前記ユーザのデータおよびドキュメンテーションファイルを安全に更新するように構成されている更新モジュールをさらに備えている、請求項１に記載の装置。
【請求項１５】
前記処理モジュールと通信し、ＲＦ作動クレジットカードリーダ、現金自動預け払い機、並びにＲＦＩＤベース技術を利用して遠隔から操作できる電子ロックまたはゲートおよびドアオープナーを含む任意の群の外部デバイスと通信するように構成されている統合デジタルデータエンコーダ／デコーダおよびＲＦトランシーバモジュールをさらに備えてい

る、請求項１に記載の装置。
【請求項１６】
前記ＲＦトランシーバと通信し、前記装置を電気的に充電し、同時に、前記装置内部の保護されたおよび非保護の保存データのバックアップを自動的に実行するように構成されている補助基地局デバイスをさらに備えている、請求項１５に記載の装置。
【請求項１７】
前記装置が接続されている通信デバイスの前記群の１つを通じて前記装置に接続されている前記コンピュータまたは携帯電話のオペレーティングシステムを自動的に検出する統合ソフトウェアモジュールをさらに備えており、前記コンピュータまたは携帯電話はキーボードおよびそれに関連する表示ユニットを有しており、前記ユーザは、これらを通じて前記装置の前記処理モジュールおよび前記メモリモジュールと情報を送受信し得、前記コンピュータまたは携帯電話は、前記装置の前記メモリモジュール、前記処理モジュール、および前記センサモジュールを利用してそれと情報を送受信するように構成されている、請求項１１に記載の装置。
【請求項１８】
前記装置の前記処理モジュールと通信する電力充電およびデータバックアップデバイスをさらに備えており、前記デバイスが、
ｉ．主電源、ＡＣ－ＤＣ変換器、電源供給ユニット、および再充電可能予備電池と接続するための充電プラグを備えた充電および電源サブモジュールと、
ｉｉ．マイクロプロセッサおよび大容量ユニットを備えた電子サブモジュールと、
ｉｉｉ．電子ブザー作動器、前記ブザー作動器に接続されているボタン、および前記電子ブザー作動器に接続されているＲＦトランスミッタを備えており、前記ブザーボタンを作動すると、前記ＲＦトランスミッタが、符号化信号を前記装置に送信することにより、前記ユーザが前記装置の位置を決定可能なように構成されている起動サブモジュールと、を備えており、
前記充電および電源サブモジュールと、前記電子サブモジュールと、前記起動サブモジュールとは互いに通信し、
前記装置の前記メモリモジュールは、前記デバイスの前記大容量ユニットと通信することによって、前記装置の前記メモリモジュールに保存されている前記データのバージョンと、前記デバイスの大容量ユニットに保存されているデータのバージョンとを比較かつ同期させる、請求項１に記載の装置。
【請求項１９】
前記処理モジュールと通信し、前記装置の地理的位置を正確に位置決めする統合ＧＰＳモジュールをさらに備えている、請求項１に記載の装置。
【請求項２０】
前記処理モジュールと通信する携帯電話モデムモジュール、および前記処理モジュールと通信するフラットディスプレイおよびタッチスクリーンモジュールを含む群から選択された少なくとも１つのモジュールをさらに備えている、請求項１に記載の装置。
【請求項２１】
ユーザ個人データおよびドキュメンテーションファイル各々を保存するための、前記一ユーザに固有に関連する個人識別ユニットを有する複数の前記固有ユーザ各々の個人の保護データおよびドキュメンテーションファイルを管理するための方法であって、前記個人識別ユニットが、
複数のバイオメトリックセンサを備えたセンサモジュールと、
前記センサモジュールと通信する処理モジュールと、
前記処理モジュールと通信する認証ユニットと、
前記処理モジュールと通信する暗号化モジュールと、
前記処理モジュールおよび前記暗号化モジュールと通信するメモリモジュールと、
前記処理モジュールと通信する通信およびデータ接続手段と、を備えており、前記方法が、

ａ．前記センサモジュールが、前記装置を保持する前記ユーザの複数の個人生物学的識別パラメータを読み出すステップと、
ｂ．前記認証モジュールが、前記ユーザの前記個人生物学的識別パラメータと、前記認証ユニットに保存されている、事前に記録された個人生物学的識別パラメータセットとを比較するステップと、
ｃ．前記認証ユニットが前記ユーザを肯定的に識別した場合に、前記ユーザに、前記メモリモジュールに保存されている前記ユーザ個人データおよびドキュメンテーションファイルへのアクセスを許可し、さらに、前記装置を通じた他の通信手段との通信を許可するステップと、を含む、方法。

【請求項２２】
前記バイオメトリックセンサが、前記装置を保持する前記ユーザの複数の個人生物学的識別パラメータを連続的に読み出すステップと、
前記複数の個人生物学的識別パラメータのいずれかに変化が生じた場合に、前記保存された個人データファイルへのアクセスを拒絶し、前記装置の動作を完全に停止するステップと、をさらに含む、請求項２１に記載の方法。

【請求項２３】
前記複数のバイオメトリックセンサの少なくとも１つは、脈拍測定インジケータ、体内酸素飽和度インジケータ、体温測定インジケータ、皮膚電気活性インジケータ、体内呼吸インジケータ、および物質的または感情的ストレスインジケータを含むライフサインインジケータの群の少なくとも１つを測定および記録するように構成されたライフサイン検出器であり、前記方法が、
前記任意のライフサインインジケータがクリティカルレベルを測定したときは常に、任意の群の登録済緊急センタへの緊急呼出しを起動するステップをさらに含み、
前記緊急呼出しは、前記ユーザの識別、前記ユーザの個人医療データファイル、前記ユーザのライフサインパラメータおよび前記ユーザの位置の測定セットを含む、前記ユーザに関連する任意の群のデータファイル情報を伝送する、請求項２１に記載の方法。

【請求項２４】
前記装置は、前記処理モジュール、並びに前記通信およびデータ接続手段モジュールと通信する救急ボタンをさらに備えており、前記方法が、
前記救急ボタンが作動したときに、前記装置と任意の群の登録済緊急センタとの通信を起動するステップと、
前記緊急呼出しにより、前記ユーザの識別、前記ユーザの個人医療データファイル、および前記ユーザの位置を含む、前記ユーザに関連する任意の群のデータファイル情報を転送するステップと、をさらに含む、請求項２１に記載の方法。

【請求項２５】
通信手段の群の任意の１つを通じて、銀行、クレジットカード会社、クリニック、病院および医療保険会社、地方自治体および公益事業団体、並びに前記ユーザによって頻繁にアクセスされるウェブサイトを含むサービスプロバイダの任意の群と通信することにより、前記ユーザに、前記サービスプロバイダの群によって保存されている前記ユーザ個人データおよびドキュメンテーションファイルにアクセスかつそれを管理可能にさせるステップをさらに含む、請求項２１に記載の方法。

【請求項２６】
前記装置は磁気帯要素をさらに備えており、前記方法が、
前記ユーザの個人生物学的識別パラメータの肯定的な認証後に、前記磁気帯を作動させることにより、それをクレジットカードリーダ、ＡＴＭ、および販売時磁気帯読み出しデバイスを含む任意の群のデバイスによって読み出すステップをさらに含む、請求項２１に記載の方法。

【請求項２７】
前記装置は電力充電およびデータバックアップデバイスをさらに備えており、前記デバイスは、充電および電源サブモジュール、電子サブモジュール、および大容量固体メモリ

ユニットを備えており、前記方法が、
前記装置の前記メモリモジュールの記憶内容と、前記デバイスの前記大容量固体メモリユニットの記憶内容とを比較するステップと、
前記装置の前記メモリモジュール内のデータが欠如している場合に、前記装置のメモリを、前記メモリサブモジュール内に保存されている前記データの最新バージョンを用いて更新するステップと、
前記デバイスの前記固体メモリユニット内のデータが欠如していた場合に、前記デバイスの前記固体メモリユニットを、前記装置の前記メモリサブモジュール内に保存されている前記データの最新バージョンを用いて更新するステップと、をさらに含む、請求項２１に記載の方法。

【請求項２８】
前記複数の固有ユーザ各々が、前記複数の固有ユーザの遠隔集中データ通信ストレージおよび管理システムを管理するシステム管理者と通信し、前記方法が、
ａ．前記システム管理者が各固有ユーザを登録し、前記集中システムに接続されているメモリサブシステム内の前記各固有ユーザの個人ＩＤデータファイルを保存するステップと、
ｂ．前記登録は、前記システム管理者が、Ｎ組の２つの異なるランダムに選択された、その長さがｎ個の英数字の組み合わせである文字列各々を、システムユーザごとに生成するステップをさらに含み、
ｃ．前記システム管理者が、前記システムのメモリサブシステム内の前記Ｎ組を保存し、前記固有ユーザの個人識別ユニットのメモリモジュールに保存するために、前記ｎ個の文字列の組を送信するステップと、
ｄ．前記個人識別ユニットが、前記関連ユーザ間の任意の識別またはリンクを、彼の登録済シークレットアクセスコードに割り当てること無く、前記複数の固有ユーザに関連する前記シークレットアクセスコードのリストを含む、特別なパーティション内の前記システムメモリにさらに保存するための、Ｌ個の英数字のシークレットアクセスコードを生成するステップと、をさらに含む、請求項２１に記載の方法。

【請求項２９】
登録、および前記システム管理者と各固有ユーザとの通信の正常起動後に、前記システム管理者は前記固有ユーザとさらに通信し、最初に、前記固有ユーザの個人識別ユニットに保存されている、前記固有ユーザのＩＤデータファイルおよび前記個人識別ユニットに固有に埋め込まれた特徴付け整理番号と、前記メモリサブシステムに保存されている前記対応するユーザＩＤおよび個人識別データとを比較し、前記２つの識別データセットが一致する場合に、
ｉ．前記システム管理者は、前記保存されたＮ列のコード化された英数字データの第１の文字列を、前記ユーザの個人識別ユニットに送信し、
ｉｉ．前記ユーザ個人識別ユニットは、前記ユーザ個人識別ユニットに固有に関連する前記同一の保存されたコード化された英数字データの組うちの第２の一致文字列に応答し、
ｉｉｉ．前記システム管理者は、前記コード化された英数字データのうちの受信した第２の文字列と、前記メモリサブシステムに事前に保存されているコード化された英数字データのうちの第２の文字列とを比較し、
ｉｖ．前記システム管理者は、前記固有ユーザに関連する前記個人識別ユニットの前記メモリに事前に保存されているコード化された英数字データのうちの前記受信した追加の異なる文字列と、前記メモリサブシステムに事前に保存されているコード化された英数字データのうちの前記追加の文字列とを、Ｎの中からＭの連続的な回数比較し、
ｖ．コード化された英数字データのうちの全てのＭ列が一致した場合に、前記システム管理者は、前記固有ユーザの認証を断言し、前記固有ユーザに、前記システムへのアクセスを許可する、請求項２８に記載の方法。

【請求項３０】

前記ユーザが前記システムへのアクセスを得た後に、前記ユーザは、前記システムメモリの非保護部を扱うか、前記システムメモリ内のプライベート保護メモリパーティションへの、各このようなユーザに唯一のアクセスを許可する前記シークレットアクセスコードを、前記個人識別ユニットから送信することにより、前記システムメモリに保存されている前記ユーザの保護個人データへのアクセスを得るかを選択する、請求項２９に記載の方法。

【請求項３１】

前記認証ステップ後、前記システム管理者は、前記固有ユーザの前記個人識別ユニットと、前記ユーザ個人識別ユニットのリクエストにおいて、前記システム管理者によって登録済の緊急センタまたはサービスプロバイダの任意の群とを接続するステップと、

前記個人識別ユニットにより救急医療呼出しが起動した場合に、前記ユーザの最新の医療データを前記緊急センタに転送するステップと、をさらに含む、請求項２８に記載の方法。

【請求項３２】

複数の固有ユーザの個人の保護データおよびドキュメンテーションファイルを管理するためのシステムであって、

ａ．前記システムの複数の前記固有ユーザの前記個人データを管理および更新し、前記複数の固有ユーザ各々と通信するシステム管理者と、

ｂ．前記システム管理者に接続し、前記複数の固有ユーザ各々の最新の個人データを保存するメモリサブシステムと、

ｃ．前記システム管理者、および前記メモリサブシステムに保存されている前記各固有ユーザの個人ＩＤデータファイルに登録済の各固有ユーザに関連する複数の個人識別ユニットと、

ｄ．前記システム管理者と通信し、彼らの対応する個人識別ユニットを通じて、前記システム管理者と前記複数の固有ユーザとの直接接続を可能にする、複数のコンピュータホストおよび携帯電話と、

ｅ．前記システム管理者と通信する複数の登録済緊急センタ、並びに銀行、クレジットカード会社、保険会社、クリニック、病院および医療保険会社、政府機関、地方自治体および公益事業団体、並びに前記複数のユーザによって頻繁にアクセスされる選択されたウェブサイトを含む複数の登録済サービスプロバイダと、を備えており、

前記固有ユーザ各々に関連する前記個人識別ユニットに保存されている前記個人データおよびドキュメンテーションファイル、並びに前記サービスプロバイダの群によって保存されている前記個人データおよびドキュメンテーションファイルへの前記システム管理者のアクセスおよび通信が、前記認証ユニットによる、前記固有ユーザの個人生物学的識別パラメータの肯定的な認証後のみに有効になる、システム。

【請求項３３】

前記複数の個人識別ユニット各々は、

ｉ．前記ユーザに固有に識別される前記個人識別ユニットを保持する前記ユーザの複数の個人生物学的識別パラメータを読み出すための複数のバイオメトリックセンサを備えたセンサモジュールと、

ｉｉ．前記センサモジュールと通信し、前記個人生物学的識別パラメータを処理し、前記ユーザに関連する前記個人の保護データおよびドキュメンテーションファイルを処理および管理する処理モジュールと、

ｉｉｉ．前記処理モジュールと通信し、前記センサモジュールにより読み出され、前記処理モジュールにより処理された、前記ユーザの個人生物学的識別パラメータと、前記認証ユニットに保存されている、事前に記録された個人生物学的識別パラメータセットと、を比較することにより、前記ユーザのアイデンティティを受信および確認するように構成されている認証ユニットと、

ｉｖ．前記処理モジュールと通信し、前記ユーザのデータファイルの圧縮による暗号化および／または復号による復元を実行する暗号化モジュールと、

ｖ．前記処理モジュールおよび前記暗号化モジュールと通信し、前記ユーザのデータおよびドキュメンテーションファイルを保存するメモリモジュールと、
ｖｉ．前記処理モジュールと通信し、前記個人識別ユニットと、前記システム管理者および複数のサービスプロバイダとを接続する通信およびデータ接続手段と、備えている、請求項３２に記載のシステム。
【請求項３４】
前記システム管理者は、
前記個人識別ユニットと通信し、前記固有ユーザの個人識別ユニットに保存されている前記ユーザのＩＤデータファイルと、前記メモリサブシステムに保存されている対応する識別データとを比較し、
前記２つの識別データセットが一致する場合に、当該システム管理者と前記ユーザ個人識別ユニットとの通信およびデータ更新能力が完全になる前に、さらなるセキュリティレベルでの識別を起動するように構成されており、
前記さらなるセキュリティレベルの識別は、前記システム管理者が、前記ユーザ個人識別ユニットに固有に関連するコード化された英数字データの第１の文字列を、前記ユーザ個人識別ユニットに送信することと、前記個人識別ユニットが、前記ユーザ個人識別ユニットに固有に関連するコード化された英数字データのうちの第２の文字列に応答することと、前記システム管理者が、コード化された英数字データのうちの前記受信した第２の文字列と、前記メモリサブシステムに事前に保存されているコード化された英数字データのうちの第２の文字列と、を認証することと、を含み、
前記システム管理者は、前記固有ユーザに関連する前記個人識別ユニットの前記メモリに事前に保存されているコード化された英数字データのうちの受信した追加の異なる文字列と、前記メモリサブシステムに事前に保存されている、計測器が生成したコード化された英数字データのうちの追加の文字列と、を連続的なＮ回、完全に一致するか比較することを含む、請求項３３に記載のシステム。
【請求項３５】
前記複数のバイオメトリックセンサは、彼に固有の個人識別ユニットを保持する前記ユーザに関連する複数の個人生物学的識別パラメータを連続的に読み出し、前記複数の個人生物学的識別パラメータのいずれかに変化が生じた場合に、前記保存された個人データファイルへのアクセスを拒絶し、前記識別ユニットの動作を完全に停止する、請求項３３に記載のシステム。
【請求項３６】
各個人識別ユニットは、前記処理モジュール、並びに前記通信およびデータ接続手段モジュールと通信する救急ボタンをさらに備えており、
前記複数のバイオメトリックセンサの少なくとも１つは、前記ユーザのライフサインパラメータの少なくとも１つを測定および記録するように構成されたライフサイン検出器であり、
前記ユーザのライフサインパラメータの少なくとも１つは、脈拍測定インジケータ、体内酸素飽和度インジケータ、体温測定インジケータ、皮膚電気活性インジケータ、体内呼吸インジケータ、および物質的または感情的ストレスインジケータを含む群の任意のライフサインインジケータにより測定され、
前記個人識別ユニットは、前記救急ボタンが作動するか、前記ライフサインインジケータの群の任意の１つがクリティカルレベルを検出したときは常に、任意の前記複数の登録済緊急センタへの緊急呼出しを起動するように構成され、
前記個人識別ユニットは、前記ユーザ識別データ、前記ユーザの個人医療データファイル、前記ユーザのライフサインパラメータおよび前記ユーザの位置の測定セットを含む、前記ユーザに関連する情報を含む任意の群のデータファイルを伝送するように構成されている、請求項３３に記載のシステム。
【請求項３７】
任意の前記複数の登録済緊急センタおよび複数の登録済サービスプロバイダからの電話

での呼び出しまたは緊急音声およびデータメッセージを受信し、任意の前記複数の携帯電話およびホストコンピュータと通信するように構成されたコンピュータ化されたコールセンタをさらに備えており、

前記コールセンタは、前記ユーザの位置座標に近い緊急救助隊と通信し、同時に、任意の前記複数の登録済緊急センタおよびサービスプロバイダと通信して前記ユーザの最新の医療データを受信し、前記データを、前記ユーザの個人識別ユニットに転送するように構成されている、請求項３６に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般的に、現代のコンピュータ世代のユーザが彼らの日常生活の多くの側面に関する個人情報に、容易に、手ごろな価格で、かつ即時にアクセスするための要求に関するものである。この個人情報は、彼らの金銭状況、経済状況、仕事関連の極秘データファイル、医療更新記録、他の重要な個人ファイル、並びに多くの登録済およびお気に入りのウェブサイトに要求されるアクセスデータを含む（ただし、これらに限定されない）。本発明はまた、複合コンピュータ、インターネット、および電話ベースシステムを通じた保護個人データの送受信、保存および処理プロセスにも関する。

【０００２】

より具体的には、本発明は、安全かつ保護された方法により、彼らの個人データにアクセス、それを保存および管理するための複数のユーザ解決策を支援する複合コンピュータ、インターネットおよび電話技術専用システムに関するものである。そしてこれは、高性能かつ進歩的なトークンとして機能する個人データによるユーザ識別を用いて、システムへの安全かつ高度に保護されたアクセスを得、彼らの最新かつ大量の個人データを、トークンを伝達することにより容易に保存する。

【０００３】

この方法、通信チャネル、現代のコンピュータシステムに要求されるデータ保存サイズ、それらのデータスループット能力、およびユーザの通信要求に起因して、要求される操作性能要求、データ保存容量、および関連する要求される技術力が急速に拡大している。現代のコンピュータシステムはまた、多くの場合に、ユーザと種々のコンピュータ支援サービスとの間の通信要求を支援し、サービス、情報提供者、および顧客間の大容量データファイルの処理および送受信を可能にする必要がある。このような巨大ファイルサイズの処理システムには、多くの場合に、ユーザおよび顧客のテキスト、数値、画像、音声、図形、およびシステムユーザに関連する非常に敏感な情報の多くの他の個人データファイルまたは顧客個人データの保護された管理が要求される。このようなシステムは、以下の組織に典型的に要求される。この組織には、例えば、より高いデータスループットおよび保存容量への迅速な変化に対応しながら、完全な保護および機密性においてユーザおよび顧客個人情報を保持する必要がある病院、政府および地方自治体、銀行、保険会社、並びに他の金融機関が含まれる。

【０００４】

同時に、今日、ますます多くのユーザが、彼ら自身の個人データを保存およびそれに容易にアクセス可能であり、さらに、小型の携帯デバイスにそれらを保存できる。そして、これらのデバイスを通じてさらに、彼らの個人データおよび日常の操作要求の全てではないにしてもそれらの大部分をダウンロード、検索および管理可能な新しい技術的な手法および方法を利用する意思がある。ユーザはまた、彼らの個人ＩＤデータを用いて個人ファイルおよび他の専有ファイルを作成し、特別に高度に保護された専用コンピュータ化されたシステムを通じて、他の大きいサイズのデータファイルにアクセスする必要がある。このような専用の保護された複合システムを用いることにより、ユーザは、極秘およびプライベート個人データ、並びに他の許可された識別ユーザ、および大規模サイズの個人データファイルの供給者が有する情報を安全に転送および送受信できる。これらのファイルは、生成した高度な個人データファイルを利用する外部サービス提供者および供給者、例え

ば、病院、銀行、保険会社、官庁および政府機関などにおいて高まっている、保護個人データ送受信、共有および転送要求に応えることができる。

【０００５】

ユーザは、多くのコンピュータ化されたシステム内の保護データファイルにアクセスするために、通常、保護データファイルへのアクセス前に、最初に、コンピュータ化されたシステムにより、正当な登録ユーザとして認識および識別される必要がある。ユーザはそれ故、これらのシステム各々において、最初に、秘密情報であるこのユーザに特有のいくつかのデータ列の、コンピュータ化されたシステムへの提供を要求される。これにより、正当なユーザとしてコンピュータ化されたシステムに認識され、ユーザはその後、システムへのエントリアクセスが許可される。コンピュータ化されたシステムにより認識および承認されるためのユーザの処理は、認証と呼ばれる。ユーザが彼自身の個人識別に２種類または２手段を用意する、２つの要素による認証処理により、安全性が向上する。この処理の１つは、典型的には、カードなどの物質的なトークンであり、もう１つは、典型的には、暗証番号などの記憶される何かである。この文脈では、これらを含む２つの要素は、ユーザが保持し、かつ既知の何かであり、口語ではパスコードと呼ばれることもある。２つの要素による認証の一般的な例に銀行カードがある。すなわち、カード自体が物質的なアイテムであり、暗証番号（ＰＩＮ）が第２要素であり、その銀行カードと組になる既知データである。

【０００６】

市販されているハードウェアトークン生成器は、現在、企業システムにおける認証に用いられている。しかしながら、ハードウェアトークン生成器は、それらの使用者または所有者による手入力のみでしか、使用される認証用のトークンを生成できない。例えば、２つの要素による認証では、第２要素が「物質的なトークン」、すなわち、ユーザが所有する何かであり、求めるサービスへのアクセスを提供する端末を用いて「物質的なトークン」の所有者が入力可能な第２要素のトークン（例えば、数値列）を入力する（すなわち、提示する）必要があり得る。しかしながら、ハードウェアトークン生成器の欠点は、紛失した、または盗難されたハードウェアトークン生成器を用いて、セキュリティを破壊して不正を行えることである。別の欠点として、認証目的のための追加の物質的なトークンをユーザが管理する必要がある。さらに別の欠点として、種々のシステムにおける複数の認証のために、複数のハードウェアトークン生成器が必要となることがある。さらに、ハードウェアトークン生成器は、第２要素とした現在入手可能なハードウェアトークン生成器を利用した２つの要素による認証は、未だに、「介入者」型の攻撃を受けやすいため、ハッカーおよび犯罪者によるフィッシング詐欺を十分に防止することができない。

【０００７】

これらの機能のいくつかを備えた先行技術は、詳細な明細書としていくつかの公開書類に記述されている。

【０００８】

ＵＳＢドングルデバイスを用いた、データの移植性および患者データの機密保護を向上した、医療処方薬の書き込み、患者の医療記録の保存およびそれへのアクセス方法は、２００９年８月１３日に出願された米国特許出願第２００９０２０４４３３号に開示されている。患者記録を含む携帯用のＵＳＢドングルデバイスおよびソフトウェアは、他のローカル端末に容易に送信および転送される。関連特許には、医療記録へのアクセスを制御する方法が記述されている。この方法は、Ａ）制御ソフトウェアおよび以前の医療記録を保存可能な携帯用メモリデバイスを提供することと、Ｂ）医療記録を選択的に制御して表示する、マイクロプロセッサに動作可能に接続されている表示デバイスを提供することと、Ｃ）指紋生体認証を利用することと、を含む。

【０００９】

米国フロリダ州３３１７８、マイアミの６３００Ｎ．Ｗ．９７Ａｖｅに存在するＷａｌｌｅｔｅｘ　Ｍｉｃｒｏｅｌｅｃｔｒｏｎｉｃｓ　Ｌｔｄ．（ｈｔｔｐ：／／ｗｗｗ．ｗａｌｌｅｔｅｘ．ｃｏｍ）が提供するメディカードは、ユーザの医療記録を保存する、ク

レジットカードサイズのＵＳＢフラッシュメモリ形状のカードである。メディカードは、ユーザの名前、写真、医師名、その電話番号、アレルギおよび医薬に関する情報、緊急時の第一連絡先などの他の救命事実が印字され得る。これは、高度なＡＥＳ暗号化、パスワード保護、メモリ分割（読み出し専用部、保護部、共有部）、大記憶容量（最大８ＧＢ）を提供するようにセキュリティを強化し、データおよびアプリケーションソフトウェアの両方を含み得る。選択的な特徴には、生体認証、磁気帯がある。

【００１０】

２００７年６月４日に出願された米国特許出願第２００８／００４１９４０Ａｌ号は、Ｗａｌｌｅｔｅｘのメディカードデバイス製品を完成させるいくつかの要素を部分的に含んでいる。この特許出願は、先行技術としてメディカード製品に部分的に関連するシステムに関する２つのみの請求項を含む。第１のシステム請求項は、個人データ、患者の医療記録、医療保険、および支払情報を記録および保存する、以下の動作を含むシステムに関する。すなわちこのシステムは、ａ）スマートカードまたは類似デバイスに含まれる患者の医療記録を保存し、医療保険を含む種々の支払情報を保存するクレジットカードサイズのＵＳＢフラッシュドライブまたは類似デバイスを、ＵＳＢフラッシュドライブおよびスマートカードの組み合わせが、その人の財布または着衣しているネックレスに容易に適合するように提供することと、ｂ）救急医療労働者、病院従事者、他の医療従事者および医療労働者が、患者の医療記録を確認および変更するためのＵＳＢジャックおよび他の手段を提供することと、ｃ）医療従事者および医療労働者が医療保険および支払情報を処理するためのスマートカードおよび手段を提供することと、を含む。このシステムにより、１つの小型のクレジットカードサイズのユニット内に個人の患者の医療記録、医療保険、および支払情報を含むことが可能になる。彼らの第２の請求項は、患者データを暗号化するメカニズムを提供する請求項１のうちのクレジットカードサイズのＵＳＢフラッシュドライブまたは他のデバイスである。このデータは、所有者がキーボードを通じてパスフレーズ、暗証番号または同等のフレーズを入力した場合にのみ確認され得る。カードの進歩によりこの特徴を利用可能になれば、バイオメトリック情報も入手可能になる。

【００１１】

関連する先行技術から我々が学べることは、必要なときに患者および医療治療チームに、医療データが容易に入手される必要があることである。しかしながら、米国特許出願第２００８／００４１９４０Ａｌ号だけでなく、Ｗａｌｌｅｔｅｘ製品もまた、いくつかの極めて重要な医療市場に要求される動作およびセキュリティ特徴および能力を保証できず、どちらも、完全に容認可能な業務上の解決策を達成できない。医療記録の過敏性に主に起因して、それへのアクセスは高度に保護される必要がある。しかしながら、前述の米国特許出願の第２の請求項の最後に記載されるような単純なパスワード、さらには１つのみの生体アクセス許可では、引用する特許本文それ自体におけるいかなる補助的な説明を考慮しても、悪意を有する第三者がユーザまたは患者に関する保護された集中データに確実にアクセスできないようにするには十分ではない。さらに、この発明のカードは、携帯電話、特に、急速に数および種類が増えているスマートフォンへのいかなる接続性およびアクセスを有さない。このため、種々のサービスプロバイダによるユーザの連続通話およびデータ通信能力をこれらの電話機が維持するためのサポートに加えて、ユーザが存在するとき常に必要となる、医療支援および援助サービスを含む現代の生活環境において実際に必要なアクセス能力を有さない。さらに、Ｗａｌｌｅｔｅｘデバイスおよび先行技術である米国特許出願第２００８／００４１９４０Ａｌ号の本質的な欠点は、存在する人をデバイスのユーザとして確認し、さらに、ユーザが実際に手でデバイスを保持していることを判断および感知するのに必要な能力が不足していることである。このため、ユーザのアクセスデータを利用し、さらには、彼の指紋をシリコンコピーして彼の存在を偽造することによる、ユーザの保護された個人情報へのアクセスを回避できない。この情報には、医療個人記録だけでなく、金銭記録にアクセスする場合にはより重大な関連データ、プライベートデータ記録、ユーザが組織に属し、彼が彼自身に伝える必要のある高度に保護された情報への特別な個人アクセス許可を有する場合には、機密扱いの組織記録も含まれる。

【００１２】
また、極秘の医療記録、または他の個人データファイルへのアクセスを与える場合に、工夫所有者の判断結果であるライフサインが正常でないときには、工夫内に自己始動する機能を有することが強く推薦される。この機能には、ユーザに接続している携帯電話を利用した緊急呼出し、または、ユーザとホストコンピュータとを接続することにより、緊急医療処置もしくは近くの病院へのユーザの緊急避難を要求するリモートコンピュータセンタへの安全なアクセスが含まれる。パーソナル緊急デバイスのこの要求は先行技術により扱われたが、今のところ、実用的デバイスは市場に成功的には導入されていない。
【００１３】
また、このようなデバイスに保存された極秘医療データへのアクセス許可レベルを階層化する必要がある。この階層化では、医療救助隊により要求される患者の医療データの詳細レベルおよび量は、病院の緊急治療室に彼が到着したときに、患者を専門的に診断および処置する必要がある場合の、患者に関するはるかに詳細な専門の医療データに要求されるアクセスとは異なる。すなわち、その内容および詳細がはるかに少ない。
【００１４】
従って、まず、識別ユーザを安全かつ効率的に確認するために、このユーザに極秘個人データファイルへのアクセスを与える前に、アクセス制御能力を改善および向上する必要がある。次に、ユーザが非常に高いセキュリティレベルおよび信頼性を有すると確認した後に、他の特定の確認および事前に承認されたユーザ、特に、広範囲の登録済および承認済サービス並びに専用データ提供者と、ユーザの個人保護データを保護かつ確実に通信および送受信できる。
【００１５】
スマートフォンとして周知の現代の携帯電話は、多くの場合に、個人データストレージおよびアクセスデバイス、さらには、ユーザの電話帳および個人データ記録を保持するアプリケーションとして用いられる。しかしながら、この手法に関連する問題として、現代の携帯電話の頻繁なモデル変更に起因した、これらの電話の多くの機械的な故障がある。これらの故障の全ては、多くの場合に、デバイスの反復処理、保守、管理手順中に、重大なユーザのデータを損失するか、損なう。そして、これによりさらに、ユーザは、携帯電話およびパーソナルコンピュータを頻繁に最新モデルまたはより新規のモデルに変更するという事実を招く。より良い手法は、それ故、ユーザの極秘およびプライベートデータの保存および管理機能を、携帯電話の通信および表示機能と分離することである。このプライベートおよび個人データ保存機能と通信機能との機能分離は、特に、あるデバイスから他のデバイスへの保護データ転送行為を隠す必要があるユーザのプライベートの全ての極秘活動において重要であると認識、理解および明確化される。ユーザのプライベートを保持する状況に対する要求があり、かつ分離した高度な動作による保護データを要求する信頼性のあるデバイスは、全ての変更においてユーザの携帯用プライベートデータ保存デバイスにおいて作動するようにそれに適応し、また、ユーザが携帯電話および／またはパーソナルコンピュータを用いて行う保守サイクルにおいて更新される。ユーザ個人の携帯用データ保存デバイスは、ユーザの新規または最新の携帯電話と接続可能であり、そして、それと自動かつ即座に通信および情報交換できる。同時に、要求される場合には、常に、パーソナルデバイスがユーザのパーソナルコンピュータに加えて、利用中の彼のコンピュータ端末と相互に接続可能である必要がある。
【００１６】
この組み合わせた能力の設定は、特に、ユーザが同一デバイスを利用して、高度に敏感なレベルのデータの金銭および／または医療記録に基づく彼個人の大量データを保存し、保護データ保守の高度な要求を確実にする場合に要求される。このデータは、識別ユーザ、連続的に更新した個人データ、金銭、医療、および他の現代の生活に関する管理情報の全てではないにしてもそれらの大部分を含む、テキスト、画像、音声、図形および図面を含むデータと組み合わされる。
【００１７】

これらの非常に高いセキュリティ、プライバシ保守要求、技術手段を急速に拡大するユーザの過敏性、財務関連データを送受信する操作トレンド、埋葬およびイントラネットなどの現代のコンピュータ化された通信回線およびネットワークを通じた金銭取引の実行に関連して、これらのネットワークを通じた、現在使用されているユーザとの相互作用手段および方法の改善要求がある。これらは、今日、主に、最良のセキュリティ保護手段としてユーザ名およびパスワード情報を単に提供および送受信することのみによって行われている。そしてこれにより、ユーザは金融機関および銀行にアクセス可能になり、次に、実際の金銭取引および株式取引の実行などの高度に敏感なかつトップセキュリティが要求される処置を実行可能になる。それ故、認証、通信およびデータへのアクセスの向上および改善を提供および支援するための、より進歩的かつ実用的な新規技術に基づく手段および手法の提供が、強く推薦され、かつ要求される。この手段および手法には、はるかに優れた個人金銭データ送受信を提供するための遠隔取引実行手段、極秘およびプライベート情報交換のためのセキュリティ向上の提供、保護されたかつ安全な極秘保存の提供、および安全性およびセキュリティがより高い処理の実行が含まれる。このような改善した金銭取引セキュリティ管理の現在の手法の欠点は、既存の市場の広大な範囲において、ハッカーおよび犯罪者が極秘の金銭データ、ユーザおよび組織の関連財源にアクセスする不運な機会を提供することである。彼らは、次に、それらへの犯罪行為を実行し、他のユーザの金を実際に用いて関連する広範囲において不当な取引を行う。これらの犯罪行為により、現在、ユーザおよび組織は、毎年何億米ドルもの直接的な損害を被り、この結果さらに、保険会社は、彼らの銀行およびクレジットカード会社を通じて彼らと保険契約を結ぶ。

【００１８】

それ故さらに、複数の認証、極秘および非常にプライベートな個人データへのアクセス、ユーザ個人の金銭および医療データの保存を支援する、専用複合コンピュータ、インターネット、および電話技術システムの必要性が広く認識され、さらにこれを有することが非常に有利になる。これはさらに、複数の前述のシステムの事前登録ユーザに関する日常業務を支援し、そしてこのシステムを利用することにより、許可、承認、保護された複数のサービス提供者と相互作用する必要のある彼らの日常の高度に保護されたデータの安全な通信および操作を実行できる。そしてこれを、新規の要素を実施により支援する、セキュリティに重大かつ強く要求されるものとして追加し、前述のシステムにアクセスする専用システムが、複数レベルの個人データによるユーザ識別の組み合わせ、個人または組織の大容量データの保護かつ暗号化、いずれの場所でもユーザが保持する彼の非常にプライベートな装置における極秘かつ非常にプライベートなデータに即時アクセスする能力を有する前述の携帯用装置を利用するが、前述の専用の携帯用デバイスを利用しても安全に通信できる。

【００１９】

高度に保護され、コンピュータ化された通信システムに対する要求もある。このようなシステムは、事前登録済および向上したセキュリティ確認により承認済の顧客のみに開放され、さらに、システムに登録済の顧客は、彼らの進歩的なシステムを用いてのみ、前述のシステムにアクセスできる。また、トークンの概念を管理する事前登録を利用した認証は、電子的手段による、金銭取引を実行する犯罪行為の事例を著しく低減し、このようないかなる不審な取引の監視および発見をより優れたものにし、さらに、保護されたシステムに侵入するハッカーの試みを迅速かつ容易に追跡することが期待されている。彼らのトークンの利用のみにより可能になる、保護されたシステムとのシステムユーザの相互作用は、このシステムユーザ各々に、以下の動作を行う最善の方法を提供する。すなわち、最初に、彼のエントリおよびシステムとの相互作用が完全に確認され、それ故、高度に保護され、次に、それらの処理に伴う彼の取引を追跡し、このような各取引がユーザによって最終承認され、終了される前に、彼らの最終実行結果を観察する。

【発明の概要】

【発明が解決しようとする課題】

【００２０】

それ故、運用上の信頼性のある手法が強く推薦され、かつそれに対する要求がある。この手法では、専用システムを通じた複数の登録ユーザの保護通信および要求されるデータ管理が支援され、システムユーザが、ユーザと組み合わさる個人データによるユーザ識別として提案された彼らのプライベートパーソナルトークン、および保護された大容量の個人または組織の携帯用データストレージとして処理デバイスの両方を用いる必要があり、システムユーザの極秘プライベート情報を含む前述の保護されたシステムおよび外部データベースへの保護されたかつ安全なアクセスを提供する。

【課題を解決するための手段】

【００２１】

以下の実施形態およびその態様は、システム、装置および方法と併せて記述かつ示され、これらは例示および実例であり、範囲の限定を意図しない。種々の実施形態では、前述の制限および現代のユーザにより高まっている新たな要求の１つ以上が解決、軽減または除去され、他の実施形態は、他の有利点または改善点に関連する。

【００２２】

本発明の核心は、進歩的かつ高い信頼性を有する新世代の物質的に安全なエントリを達成する、小型手のひらサイズの、保護アクセスを支援するトークンと、現代のコンピュータ化されたシステムに要求されるユーザの保護されたエントリを提供および支援するように適合する携帯用装置にある。本発明の装置は、統合され、高度に保護された個人データ通信および管理能力を有し、複数レベルのユーザの内蔵型生体パラメータ測定および認証モジュールと一体化する。同時に、本発明の装置は、大容量データ保存容量へのかつそこからの保護データ通信能力に関するユーザ要求を完全に支援し、本発明の装置内の一体部分であり、かつそこに常駐する固体メモリモジュールを有する。

【００２３】

本発明に従い、コンピュータ、インターネット、および電話技術コンポーネントと一体化する、高度に保護された個人データ保存および処理複合システムがさらに提供される。システムの支援、およびそのユーザの高度に保護された要求される個人データ処理は、一体内蔵型の本発明の専用装置により行われる。この装置は、少なくとも２つのバイオセンサによる複数のセキュリティレベルセットを提供し、ユーザ独自の個人の生物学的パラメータを測定し、さらに、ユーザが測定した生物学的パラメータセットの処理に基づく、高い信頼性を有し、かつ安全な認証能力を提供する。複合システムは、複数のユーザによる、極めて極秘の個人データファイルの交換、ローカルメモリおよび遠隔データ供給者による保護アクセス、高度に保護された個人データ送受信、並びに保護個人データ保存を可能にする。システム登録ユーザは、そのユーザの個人データ保存容量用に作成された高度に保護かつ暗号化された大容量の専用の携帯用個人データの認証符号装置を用いて、複数の特別に許可されたサービス提供者との専用システムを通じた通信を機能させる。それ故、本発明のシステムに事前登録済の許可されたサービス提供者からの最新の個人データを、装置のメモリにアップロード、かつそこからダウンロードすることが可能になる。この装置は大記憶容量固体データ保存モジュールを備えている。これが、ユーザ個人データを保存するように適応することにより、属する最新の個人データを、単一かつ固有ユーザが容易に入手可能になる。本発明の装置は、任意のユーザに、プライベートおよびパーソナルレベルを提供し得、代替的に、従業員による保護データ処理、および組織内部の全ての私有データを安全に管理するための種々の組織における管理を提供する。その上、このような各従業員は、企業の私有情報に関する安全性の高いアクセスキーとして本発明の携帯用装置を使用している。本発明のシステムを使用するために、本発明のシステムの複数のユーザ各々は、本発明の装置を用いて、彼ら自身に、高度に保護された専用本発明のシステムと連結した、保護されたかつ安全なアクセスを提供する必要がある。

【００２４】

このような高度に保護された通信システムの存在は、本発明に従い開放公衆へのアクセスを閉じ、固有に保護された、個人データ管理の手法を提供する。このシステムは、事前登録済および向上したセキュリティ確認により承認済の顧客またはユーザのみに開放され

る。システムに登録済の顧客は、彼らの進歩的、さらには本発明の装置により事前登録済である認証管理トークンを用いることのみにより、本発明のシステムにアクセスできる。この新しい概念は、不完全な金銭取引を実行するための電子的手段を利用して、コンピュータ化された金銭システムに侵入することにより実行される犯罪行為の事例を著しく低減することが期待されている。これはさらに、犯罪意図を有する金銭システム侵入者の迅速な割当および捕獲に基づき、このようないかなる不審な取引の監視および発見をより優れたものにする。さらに、保護されたシステムに侵入し、その適切な正常機能に損害を与えようとするハッカーの試みの追跡を容易にする。彼らのパーソナルデバイスの利用のみにより可能になる、保護されたシステムとのシステムユーザの相互作用は、このシステムユーザ各々に、以下の動作を行う最善の方法を提供する。すなわち、最初に、彼のエントリおよびシステムとの相互作用が完全に確認され、それ故、高度に保護されたことを認証し、次に、それらの処理に伴う彼の取引を追跡し、このような各取引がユーザによって最終承認され、終了される前に、彼らの最終実行結果を観察する。これは、確認済ユーザのみを意味し、他のユーザの誰も、そのユーザの個人ファイルおよび預金口座にアクセスする可能性を有さず、確認済ユーザによるか、それを通じてのみ任意の種類の取引が可能になる。

【００２５】

本発明の別の代表的な実施形態では、本発明のシステムを操作する方法を開示する。この方法は以下のステップを含む。すなわち、Ａ）システムユーザが、一連の複数レベルの生体個人パラメータ測定を実施し、この測定パラメータを処理し、次に、その結果をユーザ認証に利用するステップを最初に適用し、次に、Ｂ）確認済ユーザによる彼の個人データ管理を可能にし、さらに、彼の個人データへのフルアクセスに加えて、彼のパーソナル装置でのユーザ個人データの更新および保存を可能にする。この処理は、本発明のシステムを通じて、複数のこのような高度に保護された他のシステムユーザをユーザにより安全に接続することにより可能になる。これにより、複数の専用の、承認され、高度に保護されたサービス提供者と保護かつ暗号化されたデータを通信および送受信することが可能になる。本発明のシステムユーザ各々は、本発明の携帯用専用装置内に全て一体化された、統合され、高度に保護かつ暗号化された大容量の個人または組織のデータモジュールを有する、専用の携帯用個人データによるユーザ識別を利用することにより、彼ら自身に、複数のユーザ保護個人データを処理および管理するための一体化した、保護された専用システムへの保護されたかつ安全なアクセスを提供するために、彼らの非常に個人的かつ高度に保護された本発明の装置を用いる必要がある。

【００２６】

本発明は、新規の安全かつ保護された通信、および保護個人データ送受信を実行する、私用および組織的なスタッフユーザの更新方法を提供する。これは、大量サイズの高度に個人化および／または組織化されたプライベートの、今日では存在していない秘密データパッケージの処理、交換および保存を支援するために強く要求されている。このシステム、およびその運用方法はさらに、彼の高度に敏感な個人データベース、および種々の登録済データおよびサービスプロバイダにより保存され、連続的に更新されたファイルの大容量記憶データ容量への保護された安全なアクセスを能動的に管理する能力をユーザに与える。この能力はまた、大容量データ保存容量バンクとして構成された、本発明のシステムメモリ内のユーザのプライベートかつ保護されたメモリパーティションを用いても与えられる。ユーザは、別のシステムユーザ、または特定の、承認され、高度に保護された特別なサービス提供者にどの部分を送信するかの決定を所望する場合には、システムメモリから新規データを得、それを本発明の装置にダウンロードし、彼の個人データ保存デバイスとして機能させる。

【００２７】

本発明の別の実施形態に従い、装置所有者およびユーザ個人の生物学的および物理的パラメータ測定および認証を独占的かつ単独で支援する、少なくとも２つの特別なバイオセンサおよび物理的パラメータ測定手段と一体化された装置を提供する。この装置はさらに

、装置に事前定義された正当に測定された物理的な、複数レベルの生体個人パラメータの肯定的な認証処理を連続的に実行する。この装置は、一人のみの識別ユーザの個人データ保存、アクセス、およびデータ送受信を常に暗号化でき、そのプライベートユーザによる大量の記憶容量の個人データ保存を実行するものとして機能する。この装置によりさらに、デバイスの個人所有者が、専用システムを通じて、専用の携帯用個人生体パラメータを用いて測定されたデータによるユーザ識別、および内蔵型および一体化された保護かつ暗号化された大容量の個人または組織の高度に敏感な個人データを用いることによる、複数の特別に承認済のサービス提供者との通信および動作が可能になる。専用システムユーザ各々は、彼ら自身に、一体化した、高度に安全かつ保護されたシステムへの保護されたかつ安全なアクセスを提供するために、彼らの非常に個人的な装置を用いる必要がある。

【００２８】

本発明の別の実施形態に従い、ユーザの起こり得る緊急事態を検出し、さらに、装置所有者のライフサイン測定結果が正常でないことを解析する装置が提供される。この装置は、ユーザに接続している携帯電話を通じて、緊急呼出しを自己始動するか、ユーザが彼専用装置をホストコンピュータに接続している場合には、インターネットを通じてメッセージを伝送する機能を有する。また、緊急医療処置もしくは近くの病院へのユーザの緊急避難を要求するリモートコンピュータセンタに安全にアクセする機能を有する。この装置を、現代の携帯電話と容易かつシームレスに接続かつ通信するように電子および通信手段と一体化するか、任意の種類のホストコンピュータを、本発明の専用の保護パーソナル集中データの保存と一体化することにより、管理コンピュータシステムは、ユーザの位置識別から計算され得る病人の位置情報、任意の現代の携帯電話の固有デバイスの位置識別能力から導かれ得る情報に基づいて近くの病院の救急室を呼び出すことができる。

【００２９】

本発明の装置およびシステムを利用するユーザの利益をより良く理解するために、現在のユーザが、彼らの電磁駆動ハードディスクの機械的または電気的不全に起因する、彼らが保存した個人的な重要なデータファイルを頻繁に何度も紛失する状況、極秘データファイル不全に悩む状況、および彼らのパーソナルコンピュータまたはスマートフォンの機能不全に伴う損害を理解することが要求される。多くの場合に高度に個人化された重要なデータである極秘データファイルを損失する別の原因には、ユーザのパーソナルコンピュータまたはスマートフォンの起動中におけるソフトウェアの機能不全の問題がある。このような問題はまた、ユーザのコンピュータまたは携帯電話におけるウイルスおよびアドウェアの感染によっても頻繁に発生する。これらの全ての問題は、彼らの日常においてバックアップメモリの支援を要求する場合に、その大容量固体メモリデータ保存容量と共に、ユーザが、彼らに提供される彼らの発明装置を利用することにより、除去、または少なくともかなり低減できる。本発明の装置は、それ故、高い信頼性を有する保護データ、固体ベースメモリに関する現代のユーザ要求を完全に支援し、埋め込み型、関連型、進歩的なアンチウイルス、アンチアドウェアソフトウェアによりウイルスから保護される。これらは、ユーザが彼専用装置をシステムに接続するか、彼のホストコンピュータを通じてインターネットに接続する度にそのデータベースを頻繁に更新する。極秘かつ重要なデータファイルを頻繁に損失する別の一般的な例には、現代のユーザの習慣に典型的な、彼らのホストコンピュータの頻繁な変更またはアップグレードがある。なおさらに、ユーザの携帯電話のモデルチェンジも頻繁に行われ、ユーザはこの度に、彼らの変更したデバイス内に保存された電話帳などの極秘データを紛失する危険性がある。この主な原因は、コンピュータまたは電話を変更する前に、ユーザ、関連する携帯電話サービスプロバイダ、または携帯電話提供業者が十分に注意せず、全ての保存済データの専門の完全補償バックアップを実行しないことにある。多くのユーザは、携帯電話をアップグレードした時における、彼らの電子電話帳の内容が完全な消去ではないにしても損害を受けた場合の対処に詳しい。本発明の装置に含まれる医療記録、金銭記録、クレジットカードアクセスデータ、電話帳などの全てのユーザの極秘データを保持するために、本発明のシステムは、常に、ユーザの個人的な本発明の装置に保存された全てのファイルごとにメモリバックアップファイル

を自動的に作成する。また、前述の頻繁に起こる、ありふれたシステム不全、およびデータを紛失する事例においても、彼らの極秘個人データファイルを紛失することなく、現代のユーザの日常および高まる要求を支援できる。

【００３０】

本発明の装置は、それ故、保護アクセスおよび暗号化されたフォーマット構造において極秘データを保存可能な１つの小型の携帯デバイスにおけるユーザのデータ保存要求を完全に満たす。

【００３１】

近年、スマートフォンにおける全ての現代のユーザ通信要求は増大する傾向があるが、本発明の装置の運動機能および能力に記述するような、分離デバイスにデータを提供しながらの、日常生活においてユーザが蓄積したデータの保存容量および安全性の管理および保護機能ははるかに優れてきている。

【００３２】

現代のユーザは、それ故、スマートフォンに加えて本発明の装置の両方を持ち運び、日常的な原理を利用することにより、日常の要求に対する最善の手法を得ることができる。本発明の装置を紛失するか、盗難した場合でさえも、その中のデータに加えて、ユーザの金融機関などの他のサービスプロバイダへの、それにより与えられるユーザアクセスは保護され、この特定装置の所有者以外のいなかる他の人も極秘データにアクセスできない。

【００３３】

本発明の装置を用いたセキュリティおよび安全性の高い全てのデータ処理に起因して、これは、本発明の装置のメモリに加えて本発明のシステムサーバメモリの両方において、取引段階およびパートナの完全な記録を保持しながらの、完全に保護された金銭取引の処理にも役立ち得る。

【００３４】

本発明の装置の好ましい一実施形態では、この装置は、それ自体に保存された個人保護データおよびドキュメンテーションファイルを管理する。この装置は以下を備えている。すなわち、Ａ）ユーザにより固有に識別される装置を保持するユーザの複数の個人生物学的識別パラメータを読み出すための複数のバイオメトリックセンサを備えたセンサモジュールと、Ｂ）センサモジュールと通信し、彼らの個人生物学的識別パラメータを処理し、装置ユーザに関連する個人保護データおよびドキュメンテーションファイルを処理および管理するための処理モジュールと、Ｃ）処理モジュールと通信し、センサモジュールによる読み出し、処理モジュールによる処理が実行されたときに、装置のそこに保存され、事前記録された個人生物学的識別パラメータセットを用いて、装置の固有ユーザの個人生物学的識別パラメータと比較することにより、装置ユーザのアイデンティティを受信および確認するように構成された認証ユニットと、Ｄ）装置の処理モジュールと通信し、装置のユーザのデータファイルの圧縮による暗号化および／または復号による復元を実行する暗号化モジュールと、Ｅ）処理モジュールおよび暗号化モジュールと通信し、装置のユーザのデータおよびドキュメンテーションファイルを保存するためのメモリモジュールと、Ｆ）処理モジュールと通信し、装置と外部デバイスとを接続するための通信およびデータ接続手段セットとを備えている。固有ユーザに関連するユーザが保存した個人データおよびドキュメンテーションファイルへのアクセスは、認証ユニットによる、ユーザの個人生物学的識別パラメータの肯定的な認証後のみに可能になる。

【００３５】

本発明の装置の別のさらなる実施形態では、装置に一体化した複数のバイオメトリックセンサの少なくとも１つは、ライフサイン検出器である。ライフサイン検出器は、ユーザのライフサインパラメータの少なくとも１つを測定および記録するように構成される。

【００３６】

本発明の装置の別のさらなる実施形態ではさらに、ユーザのライフサインパラメータの少なくとも１つは、脈拍測定インジケータ、体内酸素飽和度インジケータ、体温測定インジケータ、皮膚電気活性インジケータ、体内呼吸インジケータ、および物質的または感情

的ストレスインジケータを含む群の任意のライフサインインジケータによって測定される。

【００３７】

本発明の装置の別の実施形態では、ライフサインインジケータの群の任意の１つがクリティカルレベルを検出すると、装置は、登録済緊急センタの任意の群に対して緊急呼出しを起動し、ユーザに関連する情報を含む任意の群のデータファイルを登録済緊急センタに送信するように構成される。この情報には、ユーザ識別データファイル、ユーザの個人医療データファイル、ユーザのライフサインパラメータおよびユーザの位置の測定セットが含まれる。

【００３８】

本発明の装置の別のさらなる実施形態では、装置は、処理モジュールと通信する一体化救急ボタン、および装置通信およびデータ接続手段モジュールを有する。救急ボタンが作動すると、装置と任意の群の登録済緊急センタとの通信が起動し、装置の緊急呼出しにより、本発明の装置の固有ユーザに関連する情報を含む任意の群のデータファイルが伝送される。この情報には、ユーザ識別データ、ユーザの個人医療データファイル、およびユーザの位置が含まれる。

【００３９】

本発明の別のさらなる実施形態では、装置は、コンピュータまたは携帯電話のオペレーティングシステムを自動的に検出する統合ソフトウェアモジュールをさらに備えている。これは、装置が接続されている通信デバイスの群の１つを通じて装置に接続されている。コンピュータまたは携帯電話は、キーボードおよびそれに関連する表示ユニットを有し、これにより、ユーザは、外部デバイスのキーボードおよび表示ユニットを手段として、装置のメモリモジュールおよび処理モジュールと情報を送受信することができる。すなわち、コンピュータまたは携帯電話は、装置のメモリモジュール、処理モジュール、およびセンサモジュールを利用してそれと情報を送受信するように構成されている。

【００４０】

本発明の別の実施形態では、複数の固有ユーザの個人保護データおよびドキュメンテーションファイルを管理するための方法が提供される。この複数の固有ユーザ各々は個人識別ユニットを有し、これは、ユーザ個人データおよびドキュメンテーションファイル各々を保存するために、一ユーザに固有に関連する。個人識別ユニット各々は、複数のバイオメトリックセンサを備えたセンサモジュールと、センサモジュールと通信する処理モジュールと、処理モジュールと通信する認証ユニットと、処理モジュールと通信する暗号化モジュールと、処理モジュールおよび暗号化モジュールと通信するメモリモジュールと、処理モジュールと通信する通信およびデータ接続手段とを備えている。この方法は以下のステップを含む。すなわち、ａ）センサモジュールが、装置を保持するユーザの複数の個人生物学的識別パラメータを読み出すことと、ｂ）認証モジュールが、ユーザの個人生物学的識別パラメータと、認証ユニットに保存されている、事前記録された個人生物学的識別パラメータセットとを比較することと、ｃ）認証ユニットがユーザを肯定的に識別した場合に、ユーザに、メモリモジュールに保存されているユーザ個人データおよびドキュメンテーションファイルへのアクセス、さらに、装置を通じた他の通信手段との通信を許可することとを含む。

【００４１】

本発明の別の実施形態では、複数の固有ユーザの個人保護データおよびドキュメンテーションファイルを管理するためのシステムが提供される。このシステムは、Ａ）複数の固有ユーザ各々と通信して、システムの複数の固有ユーザの個人データを管理および更新するシステム管理者と、Ｂ）システム管理者に接続されており、複数の固有ユーザ各々の最新の個人データを保存するメモリサブシステムと、Ｃ）その各々が固有ユーザに関連する複数の個人識別ユニットと、ここで、各固有ユーザはシステム管理者に登録されており、そして各固有ユーザの個人ＩＤデータファイルはメモリサブシステムに保存されており、そして、Ｄ）システム管理者と通信し、システム管理者と、彼らの対応する個人識別ユニ

ットを通じて複数の固有ユーザとの直接接続を可能にする複数のコンピュータホストおよび携帯電話と、Ｅ）システム管理者と通信する複数の登録済緊急センタおよび複数の登録済サービスプロバイダとを備えている。この複数のサービスプロバイダには、銀行、クレジットカード会社、保険会社、クリニック、病院、医療保険会社、政府機関、地方自治体、公益事業団体、および複数のユーザが頻繁にアクセスする選択されたウェブサイトが含まれる。固有ユーザ各々に関連する個人識別ユニットに保存されている個人データおよびドキュメンテーションファイル、並びにサービスプロバイダの群により保存された個人データおよびドキュメンテーションファイルへのシステム管理者のアクセスおよび通信は、認証ユニットにより、固有ユーザの個人生物学的識別パラメータが肯定的に認証された後のみに可能になる。

【００４２】

本発明のさらなる別の実施形態では、複数の固有ユーザの個人保護データおよびドキュメンテーションファイルを管理するための、コンピュータ化されたコールセンタをさらに備えているシステムが提供される。このコールセンタは、複数の登録済緊急センタおよび複数の登録済サービスプロバイダのいずれかからの電話の呼び出しまたは緊急音声、およびデータメッセージを受信し、複数の携帯電話およびホストコンピュータのいずれかと通信するように構成されている。コールセンタは、ユーザの位置座標を緊急救助隊に通信し、同時に、複数の登録済緊急センタおよびサービスプロバイダのいずれかと通信してユーザの最新の医療データを受信し、このデータをユーザの個人識別ユニットに転送するように構成されている。

【００４３】

本発明を、添付図面に関連する例示としてのみ本明細書に記載する。

【図面の簡単な説明】

【００４４】

【図１】本発明の高度に保護された個人データ専用通信および管理システムに関連する本発明の実施形態を示す概略図である。

【図２】可能な概念モジュール構造、本発明の装置の内部サブモジュール配置、および機能性のいずれかに関連する本発明の実施形態を示す概略ブロック図である。

【図３】本発明の装置の一実施形態の概念的外部デバイス外観および機能性に関連する本発明の装置の実施形態を示す概略図である。

【図４】本発明の装置を使用するための処理の可能な一フローチャートに関連する本発明の実施形態を示す概略図である。携帯電話と装置との間の種々の動作を作動させるために、携帯電話またはホストパーソナルコンピュータを相間付け、携帯電話またはホストコンピュータの表示部、並びにキーボードハードウェアおよびその機能を用いる。

【図５】本発明のシステムサーバと情報を送受信するために本発明の装置を使用するのに可能なフローチャートに関連する本発明の実施形態を示す概略図である。これはユーザの認証から開始され、ユーザがシステムサーバのデータへの承認済アクセスを得、さらには、システムと彼とのさらなる相互作用に至るステージまで続く。

【図６】本発明のシステムを利用するモードの可能なフローチャートに関連する本発明の実施形態を示す概略図である。ユーザは本発明の装置を適用してシステムサーバと情報を送受信する。これは、ユーザがシステムサーバのデータへの承認済アクセスを得るステージから開始され、次に、種々の保護された金銭取引を実行するための、本発明のシステムとユーザとのさらなる相互作用を実行する。

【図７】本発明のシステムを利用する別の可能なフローチャートに関連する本発明の実施形態を示す概略図である。ユーザは本発明の装置を適用して本発明のシステムサーバと情報を送受信する。これは、ユーザがシステムサーバのデータへの承認済アクセスを得るステージから開始され、次に、高度に保護されたインポートおよびエクスポート保存、および個人医療ファイルに関する処理を実行するための、システムとユーザとのさらなる相互作用を実行する。

【図８】本発明のシステムを利用する別の可能なフローチャートに関連する本発明の実施

形態を示す概略図である。ユーザは本発明の装置を適用してシステムサーバと情報を送受信する。これは、本発明のシステムサーバのデータへの承認済アクセスを得るステージから開始され、次に、任意のユーザの個人データファイルのアップロードまたはダウンロードを実行するために要求される、本発明のシステムとユーザとのさらなる相互作用を実行する。

【図９】本発明の装置の変更およびデータバックアップ動作のための本発明の専用デバイスに関連する本発明の一実施形態を示す概略図である。このデバイスは、可能な一概念モジュール構造ブロック図、内部サブモジュール配置、および本発明のデバイスの機能的能力の機能性を実証する。

【発明を実施するための形態】

【００４５】

本発明は、これらの図面と共に、以下の実施形態の詳細な説明から、より完全に理解される。

【００４６】

それ故、ユーザのパーソナル携帯デバイスレベルに加えて、マルチユーザシステムレベルの両方における機密性の高い個人データおよび情報管理、並びに保存と組み合わせた手法を有することが非常に有利となる。これにより、改善かつ高度に保護された個人または組織のデータへのアクセス、局所的および遠隔での保存および管理、保護されたかつ機密性の高いプライベートユーザに加えて、大組織の内部スタッフのデータへのアクセスという日常の要求に対する提供が可能になる。

【００４７】

以下の記述において、本発明の種々の態様を説明する。本発明を理解するための説明目的として、特定の詳細を記述する。その本質的性質に影響を与えることなく、詳細が異なる本発明の他の実施形態が可能なことが当業者に明らかである。それ故、本発明は、図面に示し、本明細書に記述した形態には限定されず、添付の請求項によってのみ示される。請求項の広範な解釈によってのみ本発明の適切な範囲が決定される。

【００４８】

以下の詳細な説明では、本開示の理解を与えるために多くの特定の詳細を説明する。しかしながら、これらの特定の詳細がなくとも、本開示が実施可能であることを当業者は理解する。他の例では、周知の方法、手順、構成要素、および回路は、本開示を曖昧にしないために、詳細には記述しない。

【００４９】

特に他に明確に記述しない限り、以下の記述から明白なように、例えば、「保存」「計算」「通信」「確認」などの用語を用いた本明細書の至る所の記述が、コンピュータまたはコンピューティングシステム、または物理的に示されたデータを操作および／または変換する類似の電子計算デバイスの処置および／または処理を意味することが理解される。この処理は例えば、コンピューティングシステムのレジスタおよび／またはメモリ内の電子量を、コンピューティングシステムメモリ、レジスタまたは他のこのような情報ストレージ、送信または表示デバイス内の同様の物理量で示された他のデータに変換する処理である。

【００５０】

本開示は、専らハードウェアの実施形態、ソフトウェアの実施形態、またはハードウェアおよびソフトウェアエレメントの両方を含む実施形態の形を取り得る。好ましいシステムの実施形態では、本開示は、ファームウェア、常駐ソフトウェア、マイクロコードなどを含む（ただし、これらに限定されない）ソフトウェアにおいて実施される。

【００５１】

本開示の実施形態は、本明細書に記載する動作を実行するための装置を含み得る。この装置は、所望の目的のために特別に構成され得るか、コンピュータに保存されたコンピュータプログラムによって選択的に作動するか、再設定される汎用コンピュータにより制御されるデバイスを含み得る。

【００５２】
本開示はさらに、プログラムコードを提供するコンピュータ使用可能またはコンピュータ可読媒体からアクセス可能なコンピュータプログラム製品の形態を取り得る。これは、コンピュータまたは任意の命令実行システムを用いてか、それと接続することによって用いられる。この説明目的のため、コンピュータ使用可能またはコンピュータ可読媒体は、命令実行システム、装置またはデバイスを用いてか、それと接続するプログラムを含有、保存、通信、伝達、または送信し得る任意の装置でもよい。
【００５３】
本発明のデータ処理、管理、および保存システムだけでなく、本発明の装置もまた、プログラムコードの保存および／または実行に適応する。そして、この装置は、システムバスを通じて記憶素子と直接または間接的に連結する少なくとも１つのプロセッサを含み得る。記憶素子は、プログラムコードの実際の実行中に用いられるローカルメモリ、大容量記憶装置、および少なくとも一部のプログラムコードを一時的に保存するキャッシュメモリを含み得る。これらにより、実行中に大容量記憶装置からコードを検索する回数を減らすことができる。入力／出力またはＩ／Ｏデバイス（キーボード、ディスプレイ、ポインティングデバイスなどを含むがこれらに限定されない）が、直接的に、介在Ｉ／Ｏコントローラを介してシステムに連結され得る。
【００５４】
本発明は、本発明のコンピュータ化されたインターネットおよび電話ベース専用システムを通じて、それにより実行される高度に保護されたデータ暗号化、個人極秘データの保存、転送、管理および処理を組み合わせ、かつ支援するシステム、装置および方法に関する。システムの支援、並びにその登録済および事前に承認されたユーザの保護アクセス要求は、デバイスを所有するユーザ個人パラメータにより測定されたデータを収集および測定するための、複数レベルセットのバイオセンサと統合するか、それを内蔵する本発明の専用装置により行われる。本発明の装置は、高い信頼性を有し、保護かつ承認されたデバイス所有者の認証に用いられる。本発明の複合専用システムは、複数の類似のこのような事前に承認されたユーザによる、極めて極秘の個人データへのアクセス、個人プライベートデータの送受信、および個人プライベートデータの保存を可能にする。そして、複数の特別に許可された、事前承認のサービス提供者が有する前述の専用システムを通じて通信および動作する。システムに登録されているユーザは、高度に安全かつ保護されたアクセスキーとして、彼らに専用の携帯用デバイスまたは装置を用いている。これらは、彼の個人データ入力によるユーザ認証を通じて、このようなシステムに登録済のユーザごとに機能する。本発明の装置は、内蔵型の、高度に保護かつ暗号化された大容量固体データ保存モジュールを備えており、これらのいずれも、前述の個人または組織の携帯用の小型の専用装置内に組み込まれる。本発明のシステムに事前に承認されたユーザ各々は、彼ら自身が、本発明の複合かつ高度に保護された専用システムへの保護されたかつ安全なアクセスを得るために、彼に固有の個人的かつプライベートの本発明の装置を用いる必要がある。
【００５５】
本発明に従うシステムおよび装置の原理、構成要素および機能モジュールの配置、並びに種々の機能操作は、図面およびそれに伴う説明を参照してより良く理解され得る。
【００５６】
ここで図面を参照し、図１に、本発明の実施形態に関連する専用システム３００を示す。このシステムでは、事前に承認されたユーザは、システムサーバベースのマルチユーザＩ／Ｏ端末３６２、または任意の種類のホストパーソナルコンピュータ３６０の任意の１つを通じてシステムへのアクセスを得るか、代替的に、デジタル陸線電話３６５または携帯電話端末３５５を通じてアクセスを得る。保護されたシステムへのアクセスは、ユーザ装置３５０により実行される、一連の少なくとも３つの生体パラメータ測定および認証処理を通じてユーザに提供され得る。
【００５７】
３０５は、典型的な陸線電話通信ネットワークインフラであり、本発明の彼専用装置３

５０を有するユーザは、デジタルスマートフォン端末３６５と接続できる。陸線ベースのデジタルスマートフォン端末３６５は、スイッチ３２０、陸線電話ネットワーク３０５、および一般通信マルチプレクササブモジュール３３０を通じてシステム管理者３３５に接続されている。ユーザは、彼専用装置３５０を、スマートフォン３５５および彼の電話に接続し、次に、スイッチ３２５を介して、携帯電話インフラネットワーク３１０に接続し得、かつそこから一般通信マルチプレクササブモジュール３３０を介してシステムサーバ３３５に連結する。別のシステムユーザは、コンピュータ端末３６０にリンクされている彼のパーソナル装置３５０を用いてシステム３００にアクセスできる。コンピュータ端末３６０は、国際インターネットネットワーク３７０を通じてインターネット通信システムサーバ３４５に接続されている。３４０は、本発明のシステム３００の大容量サブシステムであり、典型的には大規模サイズの記憶容量である、システム３００全体のテラバイト状態を保存および管理する。これには、高度に保護、守りかつ暗号化されたフォーマットにおける、全てのシステム３００ユーザの個人データが含まれる。

【００５８】

システム３００全体は、コンピュータ化されたサーバ管理者サブシステム３３５によって制御および管理され、全てのシステムユーザのＩＤデータ、ストレージサブシステム３４０に保存される安全な大記憶容量個人専用データのセットを安全に伝送、受信、処理および保存する。このシステムは、システムウェブサイトサーバ３４５を用いることにより、インターネットインフラ３７０を通じてこの機能を相間付けている。マルチプレクササブモジュール３３０により、スイッチ３２０および３２５を通じた陸線および携帯電話および電話ネットワーク３０５，３１０と、集中システムサーバ３３５との通信およびデータ転送、さらには、マルチプレクサモジュール３３０を通じたシステムサーバとの多重送信が可能になる。システムセバー３７５は、システム３００の複数のユーザのデータ管理センタの別のサーバサブシステムであり、スイッチ３８０により守られた安全なファイアウォールゲートを通じてシステムの安全な接続および通信を管理する。また、インターネットを通じてシステムの安全な接続およびデータ送受信通信を管理するか、ポイント通信回線およびチャネル３８６への複数の専用ポイントを通じて、事前承認された複数のポイントに接続される。この複数のポイントには、官庁、地方自治体、他の選択された保護サービス、および製品購買提供者に加えて、システムが関連データを登録済の複数のユーザと安全に通信および送受信するのに必要な外部パーソナルメモリデータバンクが含まれる。

【００５９】

サーバ３７５はまた、安全なファイアウォールゲートにより守られたスイッチ３８２を通じた通信の管理にも関与する。これは、インターネットを通じたシステムの安全な接続および通信を管理するか、ポイント通信回線およびチャネル３８８への複数の専用ポイントを通じて多数のポイントに接続される。このポイントには、登録済銀行および保険機関、並びにシステムの複数のユーザ各々に関連する高度に保護された個人データを蓄積および連続的に更新し、システム３００に登録済の複数のユーザ各々に関連するデータを通信、ダウンロード、およびアップロードする必要がある他の金融機関が含まれる。

【００６０】

サーバ３７５はまた、安全なファイアウォールゲートにより守られたスイッチ３８４を通じた通信の管理にも関与する。これは、インターネットを通じたシステムの安全な接続および通信を管理するか、ポイント通信回線およびチャネル３９０への複数の専用ポイントを通じて多数のポイントに接続される。このポイントには、システムユーザ各々に関する高度に保護された医療個人データを生成、蓄積および連続的に更新し、システム３００に登録済の複数のユーザ各々に関連するデータを通信、ダウンロード、およびアップロードする必要がある登録済病院、医療保険会社、クリニック、医療検証研究室、および医学画像センタが含まれる。

【００６１】

システム３００は緊急管理統合セクションを有し、これにより、任意のシステム登録ユ

ーザは、緊急の場合にシステムに即座に接続できる。接続は、装置３５０が携帯電話３５５またはホストコンピュータ３６０に接続しているときに、ユーザが有する彼専用装置３５０における統合専用救急ボタンを押すことにより有効になる。このような場合では、ユーザ装置３５０とシステムサーバ３３５’との間の接続シーケンスが生成される。次に、システムサーバ３３５は、緊急メッセージとしてこの接続を識別し、この緊急メッセージを緊急サーバ３４５に伝える。緊急メッセージには、装置３５０に保存されている連続的に更新する医療情報およびユーザＩＤ詳細データパッケージが含まれる。

【００６２】

緊急サーバ３４５からのユーザ緊急メッセージは、システムの特別制御部および緊急管理センタ３４８に転送される。この緊急センタは、ユーザの緊急事態におけるさらなる処理および最善の管理を行うために、人間オペレータにより定期的に管理される。センタ３４８は、次に、緊急管理ネットワーク３９２を通じて、ユーザに最適な、地理的に最も近い医療救助隊に加えて、最終仕向地である病院または医療処置センタを選択して呼び出すことができる。そして、緊急救助隊および病院に、ユーザ名およびＩＤデータ、現在の地理的位置、並びにこのユーザに関連するシステムメモリに保存されているユーザの全ての個人および医療データファイルを提供する。病院は、システムメモリに保存されている、識別ユーザに関する健康および医療関連データファイルのフルセットを受信する。一方、救助隊は、ユーザ装置３５０に保存されている緊急データパッケージのみを得る。緊急センタ３４８はまた、人の介入が無くても自動的に動作し得、緊急センタ３４８に人間が存在しない場合には、ナショナル医療緊急サービスに電話番号を通じて連絡し、合成音声を読み出す。例えば、ユーザパーソナル装置３５０が作成および生成した緊急メッセージの内容を読み出し、同時に、同一の緊急メッセージの内容を、ナショナル緊急センタのウェブサイトにおける緊急メッセージ受信セクションに転送する。ユーザが彼の携帯電話を通じてシステムに接続する場合には、本発明の装置は、接続されている携帯電話がＧＰＳ装置を内蔵しているか否かを検出する。大抵のスマートフォンにおいてＧＰＳが非常に一般的なモジュールとなっているため、次に、装置のコントローラは携帯電話から、緊急の場合におけるユーザの局所的位置を読み出し得る。さらに、ユーザの現位置データ情報を救助隊にも通知するために、システムの緊急管理センタ３４８に伝送する。

【００６３】

本発明の装置の好ましい実施形態における、本発明の装置の可能なブロック図配置構造、および安全にデータを通信および保存するための装置を利用した関連する装置のユーザ操作を図２に示す。

【００６４】

装置１００は、少なくとも５つの異なる主なかつ必須のサブモジュールから構成され、さらに、追加の選択的な５つのサブモジュールの任意の組み合わせから構成されてもよい。各モジュールは、本発明の装置の関連部品であり、特別な機能特徴を提供し、特別な特徴および能力を備えている。装置１００は、可能な限り小型かつ重量が軽いことが好ましく、考えられるユーザの片手のひらで容易に保持および操作可能なように人間工学的に設計され、ホストコンピュータまたは携帯電話のＵＳＢまたは類似のデータ通信ポートに容易に取り付けられる。少なくとも数年間の日常使用において要求される、装置１００の信頼性のある操作を支援するために、これはまた、現代の携帯電話の耐久性と同じレベルにおける激しい衝撃および振動に耐性を有するように設計され得る。これはさらに、耐水性を有し、高温、工業用の耐久能力も有する。極めて重要な用途に用いる特別なユーザのために、この装置は内蔵されて防水性を有し得る。このような場合では、広範な操作および保存条件における広範囲の振幅、振動および衝撃に対しても強い耐久性を有する。

【００６５】

モジュール１１０は、装置ホスト端末、携帯電話、および他の付属の接続サポートである。モジュール１１０は、装置ケースから外へ延在する標準型ＵＳＢおよび／または非標準データコネクタ１１２、無線ブルートゥース通信相間１１８、ＲＦ媒体の短距離通信相間１１７、および外界とのデータ通信相間である別の室内ＩＲ通信相間１１４の任意の組

み合わせを含み得る。これらは、迅速かつ値段が手ごろな非接触通信の支援に加えて、本発明の装置１００と、任意のコンピュータ端末、携帯電話デバイス、ＡＴＭおよび自動販売機などとの物理接続を支援する。このようなコネクタは、大抵の標準的なＰＣコンピュータおよびラップトップ、並びに小型ＵＳＢに一体化されているＵＳＢデータコネクタ１１２でもよく、また、全ての現代のスマートフォンの携帯電話モデルにあるような互換性のある小型ＵＳＢデータコネクタ１１６でもよい。この図に示す好ましい実施形態の装置は、端末接続ユニット１１０内にブルートゥース無線通信相間回路１１８を備えている。これは、大抵の市場で入手可能な携帯電話、入手可能なブルートゥースＵＳＢプラグインを通じた無線ブルートゥースデータ通信機能を内蔵するいくつかのモデルのラップトップおよびノートパソコン、全ての現代のＰＣおよびラップトップまたはノートパソコン、種々のホストコンピュータとの非接触短距離接続を可能にするトークンまたはドングルタイプ工夫との容易かつ迅速なデータ通信および非接触短距離接続を可能にする。

【００６６】

モジュール１２０は、バイオセンサによる装置認証専用セットを含むモジュールである。この図に示す好ましい実施形態では、この装置は、撮像に基づく光学が異なる２つのバイオメトリックセンサを含む。センサ１２４は、ユーザ固有の顔パターンまたはユーザの眼の虹彩を撮像する撮像カメラベースセンサである。これはまた、識別ユーザの顔または眼の虹彩パターンおよび色の処理および圧縮に基づいて、ユーザの顔パターンまたは彼の虹彩構造およびパターンに固有のパラメータセットを生成する。画像センサ１２４は、従来の二次元黒白固体小型カメラ、類似の色カメラ、またはユーザの三次元顔パターンの従来の三次元画像成分、またはレーザホログラフィック画像の２つの透視画像を結合する三次元撮像カメラでもよい。カメラセンサ１２４の操作は、カメラのオン・オフボタンを押すことにより行われる。ユーザは、認証処理の実行が必要なときはいつでも、ボタン１９６を押すことができる。カメラは、ユーザ独自の顔構造パラメータの処理を可能にするために、使用可能な良質の顔特徴の画像を取得するまで動作する。ユーザの顔画像の取得後、装置の電池残量を節約するためにカメラの電源を切る。カメラが必要なときにシャットダウンしない場合には、ユーザは常に、ボタン１９６を再度押すことによりカメラをショットダウンできる。

【００６７】

画像センサ１２６は、１つまたは２つのユーザの指紋を撮像および解析する１つ以上の指紋センサである。センサ１２８は、生物学的ライフサインを検出および測定する専門の電気光学センサである。これは例えば、ユーザが保持する手のひら内部の血管にダイオードレーザを照射して、これらの血管からの後方反射光信号を検出、処理および測定することによりライフサインを検出および測定する。これはユーザの心拍を測定しつつ、彼が手のひらで装置を保持している間、その瞬間のユーザの血液内の酸素（O_2）含有量をパーセント単位で測定する。これらの２つのセンサは単一電気光学ユニットに基づくものであり、これは、ユーザの手のひらにレーザまたはＬＥＤダイオード光を照射し、次に、後方反射光の変調を撮影および解析することにより、ユーザの赤血球中の酸素量およびユーザの心拍のビットレートに起因する彼の血管における脈動の変動を計算および観察する。別の人のデバイスを使用する必要がある状況などの、ユーザがストレス状態にある場合には、血液の脈拍数が正常範囲から外れる。この場合には、装置は、心拍のビットレートが正常に戻るまでの少なくとも一定期間、認証処理を肯定的に終了できない。センサ１２８は、ユーザがそれを用いるたび、および心拍の移動平均が活発に時間変動するたびに心拍のビットレートを測定するような適応センサでもよい。この時間変動は、典型的な装置の個人ユーザに特に適応する適応的閾値、または正常な心拍のビットレートに関連して機能するものである。このセンサの酸素含有量測定部はユーザの健康度を測定し、測定した酸素濃度にいかなる急変があった場合には認証処理を停止し、さらに、測定した酸素濃度が９０～１００パーセントの酸素含有量である正常範囲にない場合にも認証処理を停止する。

【００６８】

本発明の装置の別の可能な実施形態は、センサ１２８と置換、またはその上に追加され

る１つ以上のセンサにより示される代替的なライフパラメータ測定を含み得る。このセンサは感情センサと呼ばれ、ユーザの証拠的な正常または異常な感情を検出する。これらを用いてユーザの感情、認知、および物理的な覚醒に関する情報を検出する。これらのセンサは、ユーザの感情の状態に関連するパターンを区別および分類するように特別に設計されたアルゴリズムと連動している。この群の装置は、皮膚電位および呼吸などの生理学的信号を検出できるセンサを備え得る。

【００６９】

皮膚電位の測定は、カナダ国ケベック州の企業Ｉｎｆｕｓｉｏｎ Ｓｙｓｔｅｍｓ Ｌｔｄ．により開発された、Ｂｉｏｗａｖｅなどの皮膚電位センサによって行われる。この企業は皮膚表面の電圧を記録するセンサを開発してきた。

【００７０】

別の類似のセンサには、カリフォルニア州９５４０４サンタローザの米国企業ＷｏｒｌｄＷｏｒｋｓ，Ｕｎｌｉｍｉｔｅｄが販売しているＳｋｉｎ Ｃｏｎｄｕｃｔａｎｃｅ（ＳＣ）ｓｅｎｓｏｒ Ｆｌｅｘ／Ｐｒｏ Ｓｅｎｓｏｒ ＳＡ９３０９Ｍがある。このセンサは、電気を通す皮膚の能力を測定する。ユーザが感知できない程度に小さいわずかな電界が、通常、片手の２本の指に接続されている２本の電極を通じて印加され、ユーザが可変抵抗器となり電気回路が構築される。抵抗の逆数であるコンダクタンスのリアルタイム変換（代替的には、電気皮膚反応の測定）値が計算され、ＳＣの変化が、ユーザの交感神経系の活動の変化を反映する。ユーザのストレスが増減すると、それに比例して、皮膚コンダクタンスが増減する。皮膚コンダクタンス、電気皮膚反応、および皮膚電気反応（ＥＤＲ）は、類似の生理学的測定における異なる用語である。コンダクタンスに標準的な測定単位はジーメンスと呼ばれる。皮膚コンダクタンスは、マイクロジーメンス単位で測定される。一部のバイオフィードバックシステムは、マイクロモー単位で皮膚コンダクタンスを表示する。

【００７１】

モジュール１３０は、ユーザ最終認証を実行するための装置のサブモジュール１４０を含む、ハードウェアとソフトウェアとの結合モジュールである。これは、最初に、モジュール１２０センサセットの出力をデジタル化および処理し、次に、複数のセンサが検出した測定結果を組み合わせて、最終のユーザの認証結果の「是非」を出力する。肯定的な認証結果は、本明細書に詳しく記載したような少なくとも３つの生物学的パラメータ測定センサ１２４，１２６，１２８から導きだれた場合のみに実現される。このモジュールはまた、暗号化せずにオリジナルのデジタル形式で保存され得る、プライベートの、なおも非安全なものとしてユーザに定義されたデータファイルセットを保存するサブモジュール１５０を備えている。これらのデータファイルは、装置所有者のフルネーム、彼のナショナルＩＤ番号またはナショナルセキュリティ番号、パスポート番号、運転免許番号、出生日および出生国、住所、およびカードに記載されたユーザの種々の任意の追加の類似情報、および彼の写真を保存し得る。この写真、さらには身長、目の色などの他の情報は、例えば事故の場合に、高い信頼性を有する患者識別情報として救助隊に送信される。これはさらに、初期の医療処置などの緊急時に必要となる装置所有者のプライベートの主要医療データを含み得る。このデータは、装置１００の所有者などのユーザの血液型、医薬に対する過敏性、慢性疾患、最後の標準的な血液型検証結果、およびユーザの最近の医療処置データなどの医療データを含み得る。これはさらに、緊急時に救助隊、医療チームが連絡する選択された肉親、緊急連絡先の氏名および詳細な連絡先、および心臓または胃などのユーザの慢性疾患を処置している彼の私的な医師の詳細な連絡先を含む。

【００７２】

救急医療チームは、装置１００のＵＳＢプラグ１１２に接続され得る特別なトークンを有し得、必要なときに救急ボタン１９２を押すことにより、サブモジュール１５０に保存されている、装置１００が保存している救急データが、この緊急チームの特別なトークンに、ユーザ装置がこの識別ユーザに属しているかを認証するためのユーザの写真と共に自動的にダウンロードされる。装置１００のユーザである彼の体調が悪い時、または彼が事

故に巻き込まれた場合でも、彼自身が救急ボタン１９２を押すことができる。ユーザである彼が手で装置を保持しながら、救急ボタン１９２を押すと常に、ユーザは装置１００のコントローラモジュール１６０により確認される。このステージでは、メモリモジュール１５０に保存されているユーザの名前、彼のＩＤデータ、およびユーザの緊急医療データは全て本発明のシステムサーバに送信され、そこから緊急制御室ユニット３４８に送信される。

【００７３】

そこから緊急呼出しが、専用通信回線のネットワークおよびインターネットネットワークインフラを通じて種々の医療ユニットに転送される。システムの緊急制御室を利用することにより、関連するユーザの緊急事態保全サービスによる、緊急救助隊が支援するユーザまたは制御室管理者のための信頼性のあるより迅速なサービスが可能になる。そして、第一の医療扶助および医療扶助ユニットの範囲内の他の種類の援助を提供する。

【００７４】

装置１００が、携帯電話３５５またはホストコンピュータ端末３６０を通じて外界と通信する必要がある場合には、この装置は最初に、ユーザ装置とインターネットとを接続するためのコマンドを送信する。次に、装置１００は、選択されたサービスプロバイダウェブサイト、特定のサイトユーザの登録済ユーザ名などの、ユーザとこの特定のウェブサイトとの接続に必要なデータ、彼のパスワード、および必要な場合にはさらに金融機関の預金口座番号または会員番号を送信する。サービスプロバイダウェブサイトに接続されているときに、一部の場合では、装置はサービスプロバイダウェブサイト管理者により、別のデータファイルの提供をリクエストされ得る。このデータファイルは特定装置のＩＤ固有埋め込み番号およびそのユーザＩＤデータを含み、このファイルを転送することにより、正当な登録済ユーザに特定の装置であるかを識別する。要求およびリクエストされる場合には、この追加のデータファイルは、ユーザのナショナルＩＤカード番号、彼のナショナルセキュリティ番号、および／またはパスポートまたは運転免許番号を含み得る。そして、これらを受信する全ての医療研究所または銀行が、このデータと、装置とそのユーザとが保護個人データの交換を開始する前にメモリに保存されている参照データとを比較できる。

【００７５】

モジュール１６０は、装置１００の中央コントローラおよびデータ処理ユニットである。ユニット１６０は、ＡＲＭなどの最新世代の低出力ＣＰＵプロセッサである。ＡＲＭは、英国ケンブリッジのＡＲＭ　Ｈｏｌｄｉｎｇｓの技術企業の本部が提供する、インストラクションセットアーキテクチャ（ＩＳＡ）を備えた３２ビットの縮小命令セットコンピュータ（ＲＩＳＣ）である。ＡＲＭプロセッサの比較的簡単な構成は、低出力の用途に適しており、移動性および携帯用の電子デバイス内の好ましいＣＰＵの手法となる。

【００７６】

モジュール１６０は、装置の全てのサブモジュールの動作の制御に加えて、サブモジュール１７２を通じて、メモリサブモジュール１７２により実行されるデータ処理作業の暗号化および解読も行う。これは、安全な大容量サブモジュール１７４に保存されている全ての高度に保護されたユーザ個人データファイルの保存および検索処理において実行される。モジュール１６０はまた、サブモジュール１４０を通じて、少なくとも３つのバイオセンサが一体化した装置の出力に要求されるデータ処理を実行する。モジュール１４０は、登録済ユーザのオリジナルの、初期の登録ステップ、および参照用に測定されたバイオセンサの出力を保存する。モジュール１４０はまた、センサの基準出力からのパラメータ出力データフォーマット済参照ファイルを処理および認証する。モジュール１６０は、認証サブモジュール１４０を通じて、前述の特定装置の正当な所有者およびユーザのみが装置１００を操作可能になるのに要求される認証処理および関連する決定を作成する。モジュール１６０はまた、救急ボタン１９２との相間回路として機能するサブモジュール１６８を含む。これは、データが保存されているモジュール１５０の処理をトリガして、ユーザのプライベートおよび専用救急医療事態データパッケージを作成し、必要なときに、緊

急サービスおよび救助隊、並びにシステムの緊急センタ３４８に送信する。

【００７７】

モジュール１６０は、埋め込み型ＳＷサブモジュール１６２をさらに含む。これは、ユーザが彼専用装置１００とリンクされている外部ホストコンピュータまたは携帯電話に常駐の、全ての一般的なオペレーティングシステム（ＯＳ）ソフトウェアパッケージとの双方向通信を可能にするのに要求される装置１００の自動適応を支援する機能を有する。この自動適応は、装置のコントローラユニット１６０が行う、外部ＣＰＵのＯＳが要求する迅速な適応であり、以下を実行するために強く要求される。すなわち、単一装置のデータ更新および管理処理を行う場合のホストまたは携帯電話の動作、または他のユーザもしくはシステムとの通信のために要求される。これは、外界と通信する大抵の場合に要求される、本発明の保護通信および個人データ保存、並びに管理システム３００を通じた通信の大抵の場合に適用される。このようなＯＳの自動識別、相間付け、およびサブモジュール１６２に常駐のＳＷパッケージとの通信により、自動的な認識、それ自体への適応、およびデータ接続サブモジュール１１０を通じた、任意のホストコンピュータとの通信が可能になる。この通信には、このようなホストコンピュータに常駐のマイクロソフトウィンドウズ（登録商標）、マックＯＳ、またはユニックスＯＳを起動する任意のホストコンピュータとの通信、またはスマートフォンとも呼ばれる進歩的な全ての一般的な携帯電話、例えば、シンビアン、アンドロイ、組み込みリナックス（登録商標）、パーム、またはブラックベリＯＳなどのＲＩＭの携帯電話のＯＳとの相間付けが含まれる。

【００７８】

オペレーティングシステムは、アプリケーションプログラムに多くのサービスを提供している。アプリケーションは、アプリケーションプログラミングインターフェース（ＡＰＩ）またはシステムコールを通じて、これらのサービスにアクセスする。これらのインターフェースを起動することにより、アプリケーションは、オペレーティングシステムからのサービスをリクエストし、パラメータをパスし、動作結果を受信できる。ホストコンピュータが、大規模システムの端末の一群の複数のアレイ内の１つの代表的な端末３６０、例えば、ＧＮＵ／Ｌｉｎｕｘ（登録商標）およびＢＳＤなどの、ｈｔｒｐ：／／ｅｎ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／Ｆｒｅｅ＿ｓｏｆｔｗａｒｅにおけるフリーユニックスの異形などのユニックスのようなシステムである場合には、ホスト側のユーザインターフェースは、常に、外部のホストオペレーティングシステムを起動するソフトウェアとして実施される。ウィンドウズ（登録商標）などのいくつかの他のＯＳでは、ウィンドウマネージャは、オペレーティングシステムそれ自体の一部でもよい。

【００７９】

サーバは、通常、ユニックスまたはいくつかのユニックスのようなオペレーティングシステムを起動するが、市場の埋め込みシステムは、いくつかのオペレーティングシステムに分割される。また、現時点では、マイクロソフトウィンドウズ（登録商標）の系列が、オペレーティングシステムの顧客のＰＣ市場のほぼ９０パーセントを占めるが、他のこのようなＯＳ、例えば、マックＯＳ、グーグルクロムＯＳ、または他のホスト型の常駐ＯＳを用いてもよい。

【００８０】

装置のコントローラユニット１６０は、装置１００に接続されているホストまたは携帯電話を管理する全ての一般に入手可能なオペレーティングシステムと通信および情報交換するために、それを自動的に検出かつそれに適応できる。ただし、ユニット１６０はさらに、装置１００に接続されているホストコンピュータまたは携帯電話の種類に関わらず、それが接続している外部ホストコンピュータまたは携帯電話工夫と相間し得る。表示された画面およびホストコンピュータモニタまたは携帯電話の表示画面に表示された、装置１００が支援する操作機能の選択メニューは、全て同一に表示され、同様に機能する。

【００８１】

本発明の装置１００は、そのコントローラの操作メモリに、専用ソフトウェアパッケージ１６４を保持する。これは、装置１００に接続されているホストコンピュータまたは携

帯電話のオペレーティングシステムを（ＳＷモジュール１６２を用いて）識別できる。次に、専用ＳＷパッケージ１６４は、全ての用意かつ保存された相互作用画面、および装置１００のメニューを、オペレーティングシステムが理解し、かつホストコンピュータまたは携帯電話に適するように自動的に変換し、装置１００内において、ＳＷモジュールを相間付けるホストまたは携帯電話の補正および要求される適応を自動的に実行する。これにより、ユーザによって装置１００に接続されている特定のホストまたは携帯電話の種類およびモデルに関わらず、ホストまたは携帯電話の画面に表示された画面およびメニューは、ホストコンピュータまたは携帯電話の画面を確認しつつ、常に、ユーザに同じ画面を表示する。

【００８２】

大容量保護データモジュール１７０は暗号化ＳＷおよびハードウェアサブモジュール１７２を含む。これは、ユーザの高度に敏感なプライベートおよび個人医療および金銭データファイルを暗号化および圧縮し、さらに、必要なときに、サブモジュールに保存された保護個人データの、上とは反対操作である復元および解読操作を実行する。

【００８３】

暗号化コードを解読し、装置１００のユーザの高度に保護された個人データを読み出そうとする、起こり得るハッカーの試みに、暗号化処理が大きな影響を受けないことを確実にするために、サブモジュール１７４内の保護データの暗号化および解読に要求される暗号化キーが、安全なメモリ保存構造に基づく他のメモリモジュール１５０に位置する個々の特別なメモリパーティションに保存される。この保存構造では、ハッカーが保護データメモリサブモジュール１７４に保存されたデータの暗号化コードを解読しようとする場合に、その位置を定めて、かつ利用することが非常に困難となる。サブモジュール１５０は、メモリおよびより大きい認証モジュール１３０の一部である。

【００８４】

装置ユーザサブモジュール１７４は、固体メモリチップに基づく大容量データ記憶媒体であり、これに限定されないがフラッシュメモリ型であることが好ましい。サブモジュール１７４の典型的な手法として、Ｎａｎｏ－ＲＡＭなどの新世代の消去可能な多重使用メモリデバイスを用いてもよい。Ｎａｎｏ－ＲＡＭは、企業Ｎａｎｔｅｒｏが所有するコンピュータメモリ技術である。これは、チップ様基板に堆積したカーボンナノチューブの機械的位置に基づく不揮発性ランダムアクセスメモリの種類である。理論上は、小型のナノチューブでは非常に高いメモリ密度が可能になる。Ｎａｎｔｅｒｏは、要約すれば、ＮＲＡＭとしても参照される。

【００８５】

サブモジュール１７４に要求される保存スペースは、典型的には、１６～２５６ギガバイトのデータ保存容量の範囲であり、ＮＲＡＭなどの進歩的なメモリ要素を用いて構成されることが好ましい。これは、最大数百ギガバイトのデータ保存容量を有し、特定のユーザの要求に応じて、最大数テラバイトの圧縮データ保存容量までアップグレードされ得る。これと同時に、装置１００などの小型携帯デバイスに要求される、非常に小型かつ最小の物理的容積をなおも維持する。

【００８６】

サブモジュール１９０は、ＲＦＩＤユニットと一体化した他のシステムによる装置およびそのユーザの遠隔識別を可能にするＲＦＩＤ受信機およびトランスミッタユニットである。サブモジュール１９０は電子非接触キーとして装置１００の使用を支援し得、保護されたエントランスゲートおよびドアを通じた、安全な、保護され、かつ容易なアクセスを可能にする。さらに他の場合には、ＲＦＩＤボタン１９７を押すことにより、安全な遠隔位置でのプライベートホームおよびオフィスのオープンおよびロック、キーを用いないＲＦ操作によるドアロックおよび車の操作により、装置１００の使用が可能になる。

【００８７】

サブモジュール１９８はＲＦトランシーバユニットであり、これは、遠隔に位置する装置の専用充電器、および図９に示すデータバックアップユニット１０００からの符号化さ

れたＲＦコマンドを受信できる。ユニット１０００は、通常、装置１００から離れた媒体近辺に位置する。サブモジュール１９８は、充電器およびデータバックアップユニット１０００から受信したコード化されたＲＦ信号により一度トリガされると、コントローラモジュール１６０に位置する電子音ブザー回路１６６を作動して、装置の個人ユーザによる装置１００の迅速かつ容易な検出および配置を可能にする。

【００８８】

ユニット１１５および１１３は、共に、装置１００の一体化した電気電源および複数の電圧電源サブモジュールを形成し得る。ユニット１１５は、必要に応じて、バッテリを変更するために開放し得る電池ケース部内に配置されるリチウム、ニッケルカドミウム、または他の乾電池である充電式バッテリでもよい。ユニット１１５は、モジュール１１０と一体化したコネクタが充電用に差し込まれていると、バッテリ１１５が再充電する端末１１０に加えて、専用デバイス１０００内のメモリバックアップにも接続される。電源供給ユニット１１３は、全ての要求電圧を、電子モジュール１６０、並びにメモリモジュール１３０および１７０に供給できる。さらに、センサユニット１２０、並びにＲＦトランシーバおよびＲＦＩＤユニット１９８および１９０に要求される電圧も供給できる。装置の主電源スイッチ１９９は、電源供給ユニット１１３動作のオン・オフ状態を制御し、それを通じて、装置１００全体のオン・オフ動作状態を制御する。

【００８９】

装置１００は、別の好ましい実施形態では、そのデータバスサブモジュール１８２を通じてコントローラモジュール１６０に接続する選択的な追加のＧＰＳモジュール１８０を含み得る。ＧＰＳ選択モジュール１８０は、ユーザが装置１００の救急ボタン１９２を押したときの緊急時における装置およびそのユーザのその瞬間の正確な地理的位置の正確な測定および計算を可能にする。または代替的に、装置に一体化するバイオセンサモジュール１２０が、前述の装置ユーザの医療的な異常状態に基づく緊急状況、例えば、ユーザの脈拍および血中酸素飽和度が共に正常範囲からはるかに外れたことを検出した場合に、ユーザは装置を彼の手のひらに保持し、ユーザの携帯電話でも、またはインターネットネットワークに接続されている任意のホストコンピュータに接続して、装置１００をシステム３００と接続かつそれと通信させる。この場合には、コントローラモジュール１６０が管理する専用処理および保存サブモジュール１５０に保存されている緊急更新データパッケージは、システムサーバ３４５に転送される。ここから、緊急時のデータは、ユーザの緊急事態通知のさらなる処理のために、システムの特別制御および緊急管理センタ３４８に転送される。次に、緊急管理センタ３４８は、緊急管理ネットワーク３９２を通じて、ユーザに最適かつ最も近い医療救助隊を選択して呼び出し、その救助隊に、ユーザ名およびＩＤデータ、彼の現在の地理的位置、並びにこのユーザに関連するシステムメモリに保存されているユーザの全ての個人および医療データファイルを提供する。

【００９０】

システム３００が応答しない場合には、装置のコントローラ１６０は、接続されている携帯電話を通じて自動的にその番号にダイヤルを回し、ナショナル救急医療呼出しセンタに接続する。そして、コントローラ１６０は、特別な合成音声回路により生成された合成音声により、地理的位置および識別ユーザの医療データパッケージに保存されている緊急事態を示す。代替的、またはこれと同時に、装置１００がホストコンピュータまたはスマートフォンを通じて、ユーザによりインターネットネットワークに接続され得る場合には、装置は、ホストまたは電話を通じてナショナル医療緊急サービスのウェブサイトに接続する。そして、このウェブサイトに、緊急時の通知、および暗号化せずに保存されているユーザ名およびＩＤデータ、並びにユーザの全ての個人および医療データファイルを含むデータファイルを送信し、ユーザ装置１００のメモリサブモジュール１５０へのアクセスを開放する。

【００９１】

ユーザの緊急の医療状況時における装置およびそのユーザの配置に関するユーザの位置が代替的に計算され、そしてユーザが彼専用装置１００と携帯電話３５５とを接続してい

る場合には、その位置が携帯電話サービスプロバイダによりユーザ装置１００に伝送され得ることに当然ながら留意されたい。これらの携帯電話の位置サービスは、今日、大抵の携帯電話サービス提供企業により提供されている。このような接続は、システム３００の構造および操作方法を含むセクションにおいて事前に説明されている。それ故、より正確なユーザの地理的位置データを必要とする場合には、装置１００内のＧＰＳサブモジュール１８０が選択される。そしてこれは、装置１００のユーザが緊急の場合に、救助および医療チームに送る、より正確な位置の表示を要求するユーザのためのみに、装置１００に一体化され得る。

【００９２】

装置１００は、そのモジュール構造において、２つの追加の選択モジュールに加えて、ＧＰＳ選択モジュール１８０を含み得る。１つの追加の選択モジュール１８５は、表示およびタッチスクリーン選択モジュール１８５でもよい。このモジュールにより、ユーザは、所有する外部の携帯電話をホストコンピュータに接続しなくても、装置１００を用いて遠隔システム３００と通信し、インターネット上のメニューおよびデータ型定義を通じて、外部サービス提供者にアクセスかつそれと通信可能になる。タッチスクリーンモジュール１８５は、バス１８２および相間サブモジュール１６９を通じて装置のコントローラモジュール１６０と通信する。選択的な第３のモジュール１９５は、装置のデータ通信モジュールとして機能する携帯電話モデムであり、データバス１８２および相間サブモジュール１６９を通じて装置のコンピュータコントローラモジュール１６０に接続される。この接続により、外部ホストコンピュータへの接続、または装置と携帯電話とを接続しなくとも、全面的な動作および装置１００の全ての機能の実行を支援できる。選択モジュール１９５および１８５の一体化には、いくつかの欠点がある。例えば、はるかに大きいサイズの装置１００が必要になり、消費電力がより大きくなり、充電電池のライフサイクルがより短くなり、携帯電話として機能する場合の値段および運用コスト、さらには携帯電話会社に登録する費用が高くなる。そしてより重要なことは、装置の表示部および視覚的なキーボードの小型化に起因して、ユーザの相互作用の機能性が非常に制限されてしまうことである。

【００９３】

本発明の装置の別の実施形態は、装置の物理的構造、設計および外観に関連する本発明の装置の好ましい一実施形態を実証し、さらに、それに関連するＩ／Ｏ相間、およびその複数のセンサの一体化に関する、図３Ａおよび図３Ｂに示す、装置１００に特有の実施形態の設計および構造に一体化されるような好ましい手法を実証する。

【００９４】

図３Ａに示す装置の正面図２００は、好ましい実施形態の正面側面図を示し、装置の外観２００Ａは、装置１００の同一の実施形態における後方側面図を示す。

【００９５】

正面図２００に示す装置１００内の要素２１０は、断面の薄い延在する磁気カード要素である。これは、装置１００と相間付けられ得、例えば、任意の店舗、ガソリンスタンド、または現金自動預け払い機に備え付けられている磁気カードリーダ、カードライタである。磁気カード要素２１０は、通常では、装置１００ケース内に隠れるように設計され、ユーザによってハウジングから外に延在され得る。そして、任意の磁気カードリーダと容易に相間付けられ、それと相互作用する。次に、それとデータを送受信し、さらに、任意の現金自動預け払い機、または任意の購買時の磁気カードリーダを通じた取引の実行を可能にする。装置１００ケースから外への磁気カード要素の伸長は、ユーザが要素２１０を完全に引っ張り出して、伸ばすことにより行われ得る。例えば、最初に、図２に示す装置のコントローラ１６０を用いて、装置１００のハウジング内部に位置する内部の電子作動を保護する止めピンを解放する。保護ピンの解放は、元の装置１００の所有者およびユーザが、彼の手で実際に装置を保持しているときに、図２に示す装置の認証メモリサブモジュール１４０に保存されている、バイオセンサが測定した現在の装置の所有者のパラメータセットと、バイオセンサが測定した装置１００の正当なユーザおよび所有者の関連する

パラメータとを比較することによって、装置のコントローラ１６０によりユーザが認識および肯定的な確認をされた後のみに、図２に示すコントローラ１６０により行われる。

【００９６】

２つの要素２６０および２６５各々は、二重に選択可能な、ユーザの個人バイオＩＤセンサユニットを示し、これは、画像センサ、指紋走査および解析センサ、ユーザ虹彩読み出しセンサ、並びに３Ｄホログラフィックまたはレーザ走査画像センサのセンサ群を含むがこれらに限定されない。装置１００の正面図２００に示す好ましい実施形態では、なおも良質のユーザの顔写真を取得するようにカメラにアパーチャ２６０が形成され、次に、顔写真を、ユーザを独占的に特徴づける非常に高い信頼性を有するパラメータセットに処理する。この処理は、ユーザの顔構造および主な顔の要素間の測定距離に関連するパラメータを特徴づける個人ＩＤセットにより特徴づけられる。要素２６２はセンサ２６０の動作起動ボタンであり、これを利用して装置１００の電池の消費電力を節約できる。例えば、満足のいくユーザの顔画像を取得したときはいつでも、センサ２６０はそれ自体の動作を停止できる。

【００９７】

装置の正面図２００の実施形態に示すアパーチャ２６５には、電気光学センサが存在し、これは、ユーザの眼の虹彩並びにその固有パターンおよび色に関する良質の画像を取得し、次に、それを、識別ユーザの眼の虹彩構造および色に関連する、ユーザを特徴づける非常に高い信頼性を有するパラメータセットに処理する。

【００９８】

正面図２００に示す、装置１００内の要素２２０は、可変長または固定ＵＳＢコネクタ、または任意の類似の工業用に入手可能なデータアクセスコネクタである。これは、ユーザが装置１００と彼のホストＰＣコンピュータとの接続、または任意の複数ユーザのコンピュータ化されたサーバベースシステムとの接続を所望する場合に用いられ、コンピュータ端末と一体化した任意の種類のデータコネクタとのデータ相間付け能力を有するコンピュータ端末を利用する。装置の正面図２００における要素２９５は、固定または可変長小型ＵＳＢデータ転送コネクタ、または任意の他の同等の工業用のデータ用小型コネクタである。これらは、全ての現代の携帯電話に統合されており、装置１００のユーザが彼の携帯電話を通じて外界との接続を所望する場合に用いられ得る。

【００９９】

要素２６２は、カメラ２６０ユニットの電源スイッチである。装置１００のこの好ましい実施形態における要素２８０は第３のバイオセンサユニットであり、これは、彼が右利きであり、左の手のひらで自然に装置１００を保持する場合に、ユーザの親指の指紋走査および解析を実行する。

【０１００】

装置１００のこの好ましい実施形態における要素２７０は第４の選択的なバイオセンサユニットであり、これは、彼が右利きであり、左の手のひらで自然に装置１００を保持する場合に、ユーザの左手中指の第２の指紋走査および解析を実行する。

【０１０１】

要素２５４は選択的な背面照明ＬＣＤ表示およびタッチスクリーンユニットであり、これは、スマートフォンを所有せず、ホストコンピュータへの容易なアクセスを所有しないユーザであって、装置１００のコントローラと情報を送受信し、メニュー画面を再確認し、さらに、システム３００のサーバと通信する必要があるユーザのために、装置１００と一体化され得る。このようなユーザ要求において、装置１００の選択的な構造は、当然ながら、（図２に示す）選択的な携帯電話モデム１９５を支援し、かつこれを備えている。これにより、装置１００は単純な携帯電話としても機能しつつ、さらに、ダイヤル回し、および装置との相互作用は、（外観図２００に示す）装置１００の表示ユニットオプション２５４の一部であるタッチスクリーンの機能的能力により実行される。

【０１０２】

好ましい実施形態の装置１００の正面図２００における要素２９０は、装置１００の一

般的な電源スイッチである。これは、一体化されたオン状態表示赤色発光ダイオードを有する。

【０１０３】

要素２４０は、装置１００に一体化されたＲＦサブモジュール通信のための、ＲＦＩＤ起動スイッチに関する押しボタン機能であり、遠隔での操作および安全な動作のために用いられる。この操作および動作には、例えば、安全なサイトへの非接触アクセス、進歩的な非接触現金自動預け払い機、スマートカードリーダ、およびＲＦＩＤとの通信、ＲＦＩＤ操作による車のドアなどのドアロック、並びに／またはイグニションスイッチの操作が含まれる。

【０１０４】

救急ボタン２１５は、緊急時のユーザにより押されるためのものである。このような緊急時では、ユーザが彼専用装置１００と彼の携帯電話とを接続、または彼専用装置１００を、インターネットネットワークに接続されている任意のホストコンピュータに接続する場合に、装置１００はシステム３００と接続および通信する。

【０１０５】

装置１００の背面図２００Ａは、正面図２００に示すのと同じ装置１００の好ましい実施形態の後方側面図を示す。

【０１０６】

図２００Ａの要素２５０は、ライフサイン検出バイオセンサの検出アパーチャであり、これにより、生存している健康人であるオペレータによる、本発明の装置１００のリアルタイムの動作を検出かつ示すことができる。この検出機能は、使用可能なライフサイン表示バイオセンサのリストから選択され得る専用センサまたは統合センサセットにより実行される。これらは例えば、少なくとも、体温測定センサ、脈拍測定センサ、体内酸素飽和度センサ、皮膚電位センサ、および呼吸センサを含む群から選択される１つ以上の使用可能なバイオセンサである。装置１００の図２００Ａに示す好ましい実施形態では、後部アパーチャ２５０には、一体化および統合した２つのライフサイン表示の二重チャネル電気光学センサから構成される専用統合ライフサイン測定センサモジュールが存在し得る。これは、１つのチャネル内の人間の脈拍と、他のチャネル内の血中酸素飽和度との両方の測定を同時に実行する。これは、イスラエル国クファールサバの企業ＳＰＯ Ｍｅｄｉｃａｌ Ｅｑｕｉｐｍｅｎｔ Ｌｔｄ．（ｗｗｗ．ＳＰＯｍｅｄｉｃａｌ．ｃｏｍ）により提供される。

【０１０７】

図２００Ａに示す要素２９７は、装置１００の充電式電池ケース部の外開のリードおよびカバーである。ハウジング内の再充電可能食堂の交換または確認は、カバーリード２９７を取り外すことにより実行できる。

【０１０８】

本発明の装置を限定数の実施形態に関連して記述したが、本発明の装置の多くの変形、変更、および他の用途が可能であることが当然ながら理解される。

【０１０９】

本発明の装置の使用に必要な一連のステップおよび関連処理を示す可能な一フローチャートを、４００で概略を指定して示す。これは携帯電話および／またはホストコンピュータと、装置との間の種々の動作の起動のために、ホストパーソナルコンピュータまたは携帯電話を相間付け、さらに、携帯電話の表示画面およびキーボードの操作機能を用いた、本発明の装置とユーザとの相互作用のために、ホストＰＣモニタとキーボードとを相間付ける。これを図４に示す。

【０１１０】

ステージ４０１において、装置１００と、携帯電話の小型ＵＳＢまたは互換コネクタとを接続するか、装置１００の標準サイズのＵＳＢとパーソナルコンピュータとを接続し、次に、ユーザは装置１００の電源を入れる。

【０１１１】

ステージ４０２において、ユーザが彼の手のひらで適切に装置１００を保持し、装置統合センサセットの信頼性のある正確な検出が可能であるか否かを確認する。

【０１１２】

ステージ４０３において、パラメータ検証処理に必要な、装置を保持するユーザのバイオメトリックの実行を通じて、ユーザは装置１００のユーザの認証シーケンスの実行を開始する。これは、（本明細書の好ましい一実施形態に記載したような）少なくとも３つのバイオメトリックパラメータの測定および処理に基づいて行われる。当業者に理解されるように、別の実施形態では、少なくとも２つのパラメータなどのより少ないバイオメトリックパラメータでも処理できる。バイオメトリック検証処理の実行では、第１の検証パラメータはライフサインを表示するセンサ出力である。このライフサインは、いずれも正常状態の、通常では５０～８０ＰＰＭの範囲である、事前定義された非活動状態である正常時の彼の脈拍、正常範囲では９０～１００％である彼の酸素飽和度、または正常範囲が摂氏３６～４１度である彼の体温である。第２の検証パラメータは、ユーザの２つのバイオメトリック測定パラメータの第１の１つを測定および評価できる。このパラメータには、例えば、装置が保持する彼の１つまたは２つの指紋および／またはユーザの顔パターンの測定パラメータセット、並びに／またはユーザを判断および解析する虹彩パターンがある。第３の検証パラメータは、ユーザの第２の測定したバイオメトリックパラメータを測定および評価できる。このパラメータには、例えば、装置を保持する１つまたは２つのユーザの指紋および／またはユーザの顔パターンの測定個人パラメータセット、並びに／またはユーザを検出する眼の虹彩パターンがある。

【０１１３】

ステージ４０４において、少なくとも３つの現在測定パラメータが、装置１００の内部コントローラおよびデータ処理ユニット１６０により、比較および解析されてユーザが認証される。少なくとも３つの現在測定パラメータは、予め測定、解析、およびメモリユニット１４０に保存されている、同一の装置所有者の対応する少なくとも３つのパラメータと比較される。この認証において装置１００により肯定的な応答が生成されると、ステージ４０６に継続する。

【０１１４】

認証処理が失敗した場合には、次に、装置１００のコントローラユニット１６０は、装置１００をステージ４０５にシフトする。ここで、装置はそれ自体の電源を切り、事前に定義されたその期間中の装置のさらなる使用または動作を抑制する。

【０１１５】

ステージ４０６において、装置ユニット１６０は、相間付けユニット１１０を通じて、それに接続されている携帯電話またはホストに、電話またはホストユニットが起動しているオペレーティングシステムを識別するためのリクエストを送信する。

【０１１６】

ステージ４０７において、装置のメモリバンク内の既知のオペレーティングシステムの識別における肯定的な応答をユニット１６０が得た場合には、次に、関連する保存されたオペレーティングシステム専用通信相間ＳＷパッケージの動作を起動し、ステージ４０８に継続する。

【０１１７】

別の方法では、ステージ４０５に戻り、装置１００のコントローラユニット１６０は装置の電源を切り、事前に定義された期間中の装置のさらなる使用または動作を抑制する。

【０１１８】

ステージ４０８において、装置は、携帯電話またはホストＰＣ画面に表示される、ユーザが４つのオプションのうちから選択可能な以下に示すメインメニュー画面を起動する。

Ａ：４１０－装置のメモリから保存データを検索し、ステージ４１１に進む。

Ｂ：４２０－ホストまたは携帯電話メモリからのファイルを、装置のメモリ１５０または１９０内に保存し、ステージ４２１に進む。

Ｃ：４４５－インターネット上で、選択した医療研究所、金融機関、または他の機関のウ

ェブサイトを検索し、ステージ４３０に進む。
Ｄ：４５０－ステージ４５１に進むメニューを選択する。このメニューでは、ユーザは、ユーザが手で組織する機能を用いて作成した、ユーザの種々の必要な容易にアクセス可能なパーソナル保存データを含む、装置１００内の保存データからのデータおよび情報を選択、検索または更新可能なフレームを視認できる。この情報は、彼が頻繁に訪問するウェブサイト４５２、公的資格カード４５４、販売サービスプロバイダのポイント４５６に関する全てのユーザの登録済会員のデータセットのパーソナル表形式データベースを含む。
【０１１９】
ステージ４５２において、ユーザに、ユーザのＩＤ番号、ユーザ名、並びに登録および整理記録ツールを必要とする全ての彼のお気に入りのウェブサイトに関するパスワードコードに加えて、ユーザの個人電話帳および重要なメモを提供する。
【０１２０】
このメニューで選択され得る別のオプションには４５６がある。これは、ユーザが装置を用いて店舗で購買する場合に実施される。ユーザは、彼専用装置に保存されている顔写真を商人に示し、これにより商人は、ユーザに取引を最終的に承認する前に、その写真と、彼がリアルタイムで観察しているユーザの顔とを比較できる。オプション４５４は、パスポート、運転免許などの人が必要な全ての公的カード（証明書）に関する。
【０１２１】
この処理は、最終ステージ９９９を選択してシフトすることにより、終了する。
【０１２２】
ステージ４１１において、ユーザは、選択オプションを表示する携帯電話またはＰＣホストの新規の画面を視認することができる。例えば、Ａ）医療データの選択４１２、Ｂ）金銭データの選択４１５、Ｃ）他の個人データの選択４１６画面を含む。
【０１２３】
ステージ４１２において、装置は携帯電話またはホスト画面に表示される、ユーザが以下のオプションから選択可能なメニューを起動する。このオプションは、Ａ）負傷し、確認される身体部分、Ｂ）リクエストされた医師のＩＤコード、Ｃ）要求されるＨＭＯ（医療保険会社）、およびＤ）要求される病院を含む。次に、ステージ４１３に移動する。
【０１２４】
ステージ４１３において、装置は、そのメモリユニット１５０および１７０に保存されている関連データの検索および表示のための内部メモリ検索を起動する。
【０１２５】
ステージ４１４において、装置は、種々の期間および日付において保存された、データソース内の医療、金銭、および他のデータの比較をユーザが可能になる操作上の有効なアプリケーションを支援する。
【０１２６】
ステージ４１８において、操作シーケンスにより、装置を、ユーザが新規オプションを選択可能なステージ４０８に戻す。
【０１２７】
ステージ４１５において、ユーザは、入力する代表的なキーワードを用いて、ユーザ個人データベースの保存データを検索することにより、関連する階層的な合成画面から、５以上のキーワード探索オプション選択できる。すなわち、Ａ）銀行、Ｂ）保険会社および金融機関、Ｃ）日付、Ｄ）クレジットおよび負債取引、Ｅ）取引に関する支出および収入を算出した預金口座の種類を選択できる。次に、シーケンスは、データベースから検索するステージ４１３に戻る。
【０１２８】
ステージ４１６において、ユーザは、検索キーワードとして用いられる主題から、保存データを検索するための主題を選択するメニュー画面を得る。
【０１２９】
ステージ４１７において、ユーザは、ステージ４１３に戻る以外に、ステージ４１６で

選択した主題を参照するデータを検索するためのキーを選択できる。

【０１３０】

ステージ４２１において、ホストまたは携帯電話の表示部に示される画面において、ステージ４０８のメインメニューから論理的に現れた新規データの保存を参照する。ファイルの主題および日付などのデータの保存をリクエストするためのキーワードは、メインキーワードであり、ユーザは、提案される既製リストから最大５つの追加のデータ保存キーを選択できる。このリストは、ステージ４１１および４１５に記載する各主題とは異なる。

【０１３１】

ステージ４２２において、装置のコントローラは、最後に処理されたユーザ個人データベースの記録番号に数１を追加する。この番号は、装置のメモリ内に新規に保存した記録の記録番号となる。

【０１３２】

ステージ４２３において、コントローラは、新規に処理した記録ごとに暗号化コードを生成し、それを装置１００の安全な大容量記憶モジュール１７０に保存する。

【０１３３】

ステージ４２４において、装置１００のコントローラ１６０は、ユーザ画面を、ステージ４０８のメニュー選択画面に戻すようにシフトする。

【０１３４】

ステージ４４５において、ユーザは、インターネットへのアクセスを得るためのメニューオプションを選択する。

【０１３５】

ステージ４３０において、ユーザは、装置の個人ユーザの個人保護データ内の好ましいお気に入りのサイトのリストを、ホストまたは携帯電話の画面で視認する。ステージ４３１において、ユーザがそれらの任意の１つをクリックすると、コントローラはステージ４３２に移動する。または、ユーザがオープンデータ供給フィールド内の新規のウェブサイトアドレスをクリックする場合には、コントローラ１６０はシーケンスをステージ４３５に移動する。

【０１３６】

ステージ４３２において、コントローラ１６０は、ユーザが選択した好ましいお気に入りのウェブサイトのＵＲＬ（インターネットアドレス）を検出する。次に、コントローラは、メモリ１５０からの、保存されている特定のサイト、事前定義されたユーザ名、およびパスワードを、選択したページのユーザＩＤデータ供給スペースに転送する。これにより、ユーザは、登録済およびアクセス許可された会員として、任意のこのような選択されたお気に入りのウェブサイトへの容易かつ自動アクセスを得ることができる。

【０１３７】

ステージ４３３において、ホストまたは携帯電話は自動的に移動して、選択したウェブサイトアドレスにおける第１の登録済ユーザのウェブサイトのエントランス画面、および選択したサイトの登録済会員のホームページを表示する。これにより、ユーザは、選択したウェブサイト、および彼がそこでの確認を所望する関連する個人データとさらに情報を送受信できる。このデータは、彼の個人医療検査結果、処方薬、および銀行取引明細書を含む。

【０１３８】

ステージ４３４において、画面は、どの日に保存するか、どの探索キーに基づくかを示すステージ４２１に戻り、彼が訪問したウェブサイトから得た保存された彼の個人データへのユーザのリクエストを表示する。代替的に、ユーザは、メインメニューから別の装置の動作の選択的な活動を選択できるステージ４０８に戻ることができる。

【０１３９】

ステージ４３５において、ユーザはインターネット画面を得て、彼の好みの新規アドレスを打ち込んで、彼が所望する情報を得ることができる。ステージ４３６において、コン

トローラは２つのオプション選択画面を生成する。このうちの１つは、デバイス１００メモリ内の検索された個人結果を保存し、次に、ステージ４３４に進む。別の１つは、サービスまたは製品の購入をユーザに提案し、むしろ、ステージ４３７に進む。

【０１４０】

ステージ４３７では、ユーザは、装置から得たクレジットカードの詳細の使用を所望するか否かを質問される。

【０１４１】

ステージ４３８において、ユーザは、実行を所望するクレジットカードの種類、選択された購買取引の明示をリクエストされる。そして、この取引に、好ましいクレジットカードをユーザが選択した後に、コントローラは、装置の保護メモリ１７０からファイルを得る。このファイルは、ユーザのクレジットカード番号、ユーザ名、カードの有効期限、および他のカードのシークレットコード番号を含む。そして次に、このデータを売人に送信する（ステージ４３９）。

【０１４２】

ステージ４４０において、次に、取引が承認される。

【０１４３】

ステージ４４１において、画面は、取引詳細を保存するか否かの質問をユーザに示し、次に、４２１に進む。これ以外の場合では、ユーザは、メインメニュー画面４０８から転送された別の活動オプションを選択する。

【０１４４】

ステージ９９９において、ユーザを装置のホストの操作処理から分離させ、装置１００とホストコンピュータまたは携帯電話との間の全ての通信を切断する。

【０１４５】

本発明の装置の使用に関連する処理ステップを示す可能なフローチャートを、図５に５００で概略を指定して示す。この図では、ユーザが本発明のシステムとの接続を構築し、本発明の装置を認証に適用して、システムサーバへのアクセスを得るステップを示す。図５に示すフローチャートに記述する処理５００は、ユーザ認証ステージから開始され、システムサーバのデータへの承認済アクセスを得て、特定データの検索および更新タスクを実現するためのシステムとのさらなる相互作用をユーザが得るステージまで続く。

【０１４６】

ステージ５０１において、ユーザ装置１００と、彼の携帯電話の小型ＵＳＢまたは互換コネクタとを接続するか、装置のＵＳＢコネクタとパーソナルコンピュータ内のＵＳＢスロットとを接続する。または、ユーザが装置１００の電源を入れるときに、装置とユーザの携帯電話とのブルートゥース無線データ接続を構築する。

【０１４７】

ステージ５０２において、ユーザは彼の手のひらで装置１００を保持し、図３Ａに示す指紋センサ２７０および２８０を指で押す。そして、装置のカメラアパーチャ２６０から覗いて、かつ／または彼の場所のラインを、虹彩画像センサアパーチャ２６５の中心に合わせる。同時に、装置の反対側において、ユーザは彼の手のひらを、ユーザの心拍のビットレートおよび彼の血液中の血中酸素飽和度を検出する生理学的センサパーチャ２５０に添える。次に、認証処理を開始する電源ボタン２９０を押す。

【０１４８】

ステージ５０３において、装置は、次に、ユーザが保有する３つのバイオメトリックパラメータに関するバイオメトリック検出および検証シーケンスを実行する。このうちの１つはライフサイン表示センサ（１２８）の出力であり、通常では５０～８０ＰＰＭの範囲である事前定義された非活動状態である正常時の彼の脈拍、正常範囲では９０～１００％である彼の酸素飽和度、または正常範囲が摂氏３６～４１度である彼の体温を出力する。他の２つの測定および評価されるパラメータは、１つまたは２つのユーザの指紋および／または装置を保持するユーザの顔パターンを取得および処理した測定パラメータセット、並びに／または取得し、その構造およびパターンを解析したユーザの眼の虹彩画像を含む

。

【０１４９】

ステージ５０４はオプション評価と決定ステージとの分岐点である。ユーザに関して測定され、処理された生体パラメータセットが、ユニット１４０内に保存された、装置のオリジナルのユーザの第１の登録である生体パラメータセットに適合する場合には、処理はステージ５０６に継続する。適合しない場合には、処理はステージ５０５で停止する。

【０１５０】

ステージ５０５において、ユーザは、認証処理が失敗した、接続されている携帯電話またはホストコンピュータの画面上でテキストメッセージを受信し、次に、装置は電源を切り、ユーザはそのステージまで同じ処理を再開し、繰り返す必要がある。

【０１５１】

ステージ５０６において、装置のコントローラは、今測定された、ユーザのライフ表示センサの出力結果を確認する。そしてこの測定パラメータが、ユーザに関する以前のライフ表示検査の変動する平均結果と１５パーセント超異なる場合には、ステージ５２４に進み、相違が１５パーセント以下である場合には、ステージ５０７に継続する。

【０１５２】

ステージ５０７において、ユーザは、ホストまたは携帯電話の表示画面上にメニュー画面を得る。ユーザはこの画面上で、さらなる相互作用のために、ステージ５０８において本発明のシステムと接続するか、または、前述の処理４００で記述したように、ステージ４０８において、彼のホストコンピュータまたはスマートフォンのみとの操作上の相互作用を継続するかを選択できる。

【０１５３】

ステージ５０８において、ユーザが本発明のシステムと最初に相互作用した新規ユーザである場合には、彼は、装置の登録済製品の埋め込み整理番号を有する特定装置の正当な所有者であるか否かを認証するための、検証および認証手順をパスする必要がある。それ故、この処理は、ユーザ本人が本発明のシステムのサービスステーションを直接訪問し、システム従業員の面前で、彼自身に加えて、彼のパーソナル装置が直接識別されることが要求される段階５２２に継続し、ステージ５０９でその手順が行われる。ユーザが初めてのシステムエントリユーザではない場合には、この処理はステージ５３０に進む。

【０１５４】

ステージ５０９において、ユーザは、ナショナルＩＤカードおよびパスポートまたは運転免許などの少なくとも１つの追加のＩＤ証書を示すことにより、システム従業員の面前で識別される。次に、本発明のシステム従業員は、装置とシステムコンピュータ端末とを接続することにより、装置の埋め込み整理番号を読み出す。そしてこの番号は、従業員がユーザのＩＤデータセットを手入力したのと同じ一時ファイルにおいてシステムメモリに自動的に入力される。このＩＤデータセットには、彼のナショナルＩＤ番号、国籍、フルネーム、生年月日、および現住所が含まれる。

【０１５５】

ステージ５１０において、本発明のシステムは、新規カスタマとしてユーザを登録し、システムメモリ内の専用の新規カスタマの基本データファイルを開き、そのユーザのデータファイルを、システムメモリの非保護セクション内の、事前定義された専用およびプライベートメモリスペースに割り当てる。システム管理者は各ユーザを登録し、システムに接続されているメモリサブシステム内に、各ユーザの個人ＩＤデータファイルを保存する。この登録は、システム管理者が、ユーザごとに、Ｎ組の２つの異なるランダムに選択された、ｎ個の英数字が結合した長さである英数字文字列を生成する追加ステップをさらに含む。

【０１５６】

システム管理者は、システムのメモリサブシステム内にそのＮ組を保存し、さらに、ユーザパーソナル装置に保存するためのｎ桁の文字列のＮ組を送信する。ステージ５１１において、装置は、なおもシステムコンピュータ端末に接続されており、Ｌ桁のランダム英

数字データ列を生成する。これは、システムメモリ内の彼の保護プライベートメモリパーティションへの固有ユーザシークレットアクセスコードとして機能する。

【０１５７】

ステージ５１２において、処理されたＬ桁の文字列が本発明のシステムに入力される。そして、処理されたＬ桁の文字列が、別の登録済ユーザ装置によって既に処理され、過去にシステムメモリに入力されていない場合には、それがシステムコンピュータによって確認される。システムコンピュータが、その記録内に、別の既に登録済のユーザの同一メモリＩＤデータ列を認識した場合には、ステージ５１１に戻り、そこで装置は、新規のランダムに選択されたＬ桁の英数字文字列を生成する。システムが、その記録内に、別の登録済ユーザに既に供給および提供された同一メモリＩＤデータ列を認識しない場合には、この文字列は、新規登録済ユーザのための新規シークレットアクセスコードとして選択される。

【０１５８】

ステージ５１３において、システムコンピュータは、ユーザに定義され、さらに割り当てられた、システムの大容量記憶装置内の保護プライベートメモリスペースに新規登録済ユーザを作成する。これは、ユーザが所有する装置のみに保存される、Ｌ桁のデータ列を有する識別ユーザシークレットアクセスコードを用いてのみアクセスできる。

【０１５９】

ステージ５１４において、ユーザおよびシステム従業員は、システムコンピュータからの記入済の表示メッセージを受信する。このメッセージは、新規ユーザ登録が首尾よく終了し、ユーザが、識別および認証に彼の登録済のパーソナル装置をなおも使用しつつ、今後は、任意の遠隔位置から本発明のシステムを操作して、それと情報を送受信することができることを表す。ステージ５１５において、任意の携帯電話またはホストコンピュータに接続されているユーザおよび彼専用装置は、ここで、動作のために移動し得る。

【０１６０】

ステージ５３０において、システム管理者と各ユーザとの通信が正常起動し、システム管理者はそのユーザとさらに通信する。そしてさらに、最初に、ユーザのＩＤデータファイルと、ユーザのパーソナル装置に保存されたような、彼のパーソナル装置に固有に埋め込まれた特徴付け整理番号とを比較する。この比較は、対応するユーザおよび装置の識別データシステムメモリに保存されているモジュールを用いて行われる。２つの識別データセットが一致する場合には、システム管理者は、保存されたＮ列のコード化された英数字データのうちの第１の文字列をユーザ装置に送信し、ユーザ装置は、ユーザ装置に固有に関連する、同一の保存された組のコード化された英数字データからの第２の一致文字列を応答する。そして、システム管理者は、コード化された英数字データのうちの受信した第２の文字列と、システムメモリ内に事前に保存された、コード化された英数字データのうちの第２の文字列とを比較する。次に、システム管理者は、ユーザ装置のメモリ内に事前に保存された、固有ユーザに関連する、コード化された英数字データのうちの受信した追加の異なる文字列と、システムメモリ内に事前に保存された、コード化された英数字データのうちの追加の文字列とを、Ｎの中からＭの連続的な回数比較する。

【０１６１】

ステージ５３１において、コード化された英数字データのうちの全てのＭ列が一致した場合には、システム管理者はユーザを確認し、システムへのユーザのアクセスを許可し、この処理はステージ５１５に進む。別の方法では、システムはこのセッションを終了するステージ５０５に進む。

【０１６２】

ステージ５１５では、ユーザは既にシステムに登録済のユーザであり、本明細書に詳しく記載したような短い識別および認証シーケンス後にシステムに接続され得る。このステージでは、ユーザは、彼のホスト画面に表示されたメインメニューから、システムと動作し、それと情報を送受信するオプションを選択できる。これは、いくつかの相互作用オプションから選択できる。ユーザは、システムの非保護部内の保存データの利用を選択する

場合には、ステージ５２０に進むメニューオプションを選択できる。ユーザは、システムの保護および守られた部内の保存データの利用を選択する場合には、ステージ５１６に進むメニューオプションを選択できる。ユーザは、金銭および保険に関する問題に関して、システムを通じた動作および相互作用を選択する場合には、システムを通じてそれを実行し得、全ての彼に関連する銀行、サービス、保険会社、投資信託会社、年金基金などへの安全かつ保護されたアクセスを得ることができる。全ての関連データは、専用メニュー画面を通じてシステムにより容易にアクセスおよび管理され、ユーザは、ステージ５１８に進むメニューオプションを選択する。ユーザは、彼の医療問題に関して、システムを通じた動作および相互作用を選択する場合には、専用メニューを通じてシステムに管理される全ての、全て彼に関連する医療サービス、病院、およびクリニックデータへのアクセスを、システムを通じて得ることができる。そしてユーザは、ステージ７２０に進むメニューオプションを選択する。ユーザは、システムとの相互作用の終了を所望する場合には、システムとの通信を終えるオプション９９９を選択する。

【０１６３】

ステージ５１６において、ユーザ装置は、システムに接続されているホストまたは携帯電話を介して、ステージ５１２で生成されたメモリＩＤデータ列である保護アクセスコードを送信する。

【０１６４】

ステージ５１７において、文字列がユーザに関連する正当な文字列として認識された場合には、処理は８０１に継続し、認識されない場合には、ユーザをステージ５１５にシフトして、いくつかの選択オプションを有するメインメニューを再び彼に表示する。

【０１６５】

ステージ５１８において、ユーザが救急ボタンを押した場合には、システムはその間中バックグラウンドを確認し、ステージ５２４では代替的に、生理学的センサがユーザの体調における異常を検出した場合には、ユーザが正常な健康状態ではないというアラームを送信する。緊急であると示された場合には、システムはステージ５２５に進み、それ以外の場合では、金銭に関連すると定められた活動を処理するステージ６５０に継続する。システムは、ユーザがそのサービスの金銭セクションに接続されていることを連続的に確認し、代替的に、ユーザが彼専用装置の救急ボタンを押した場合には、ステージ５２４において、生理学的センサがユーザの体調における異常を検出したときに、ユーザが正常な健康状態ではないというアラームを送信する。そして、システムが承諾してステージ５２５に進む場合には、金銭サービスセクションにおいて支援されるユーザとシステムとの相互作用を停止する。

【０１６６】

ステージ５２０において、ユーザは（およびユーザ装置は、非保護データとの相互作用をリクエストするステージ後）、装置のメモリが提供するユーザＩＤデータおよび装置の埋め込み整理番号を、システムに転送することをシステムによりリクエストされる。

【０１６７】

ステージ５２１において、システムは、そのメモリ内に保存された番号およびデータが、リンクされたユーザ装置から受信したそれらと一致するか否かを確認し、この結果が肯定的な場合には、システムおよび外部サービス提供者とのさらなる相互作用を行うステージ５４５に継続し、一致しない場合には、第２の認証ステージであるステージ５２２に進む。

【０１６８】

ステージ５２２において、第２の人間オペレータベースの認証シーケンスが、システム顧客セキュリティセンタにおいてユーザにより着手され、装置がそれを保持するユーザに属するか否かが確認される。この処理は、詳細にはステージ５１６および５１７並びに／または５２０および５２１に示すように、任意のユーザによるアクセス確認ステージ中に、システムがユーザを確認しないたびに実行される。従業員は、システムセキュリティセンタにおいて、装置のメモリに保存されている正当な装置のユーザの顔写真が、オフィス

に来たユーザの顔と一致するか否かを確認する。システム従業員はさらに、彼が彼の所有物であると主張する装置の、システム従業員の面前での承認処理動作をユーザに求める。その第２の人物が監督した認証処理結果が否定的である場合には、そのユーザに関するセキュリティ調査を開始する。

【０１６９】

ステージ５２５は、システムの特別制御および緊急管理センタ３４８において受信する緊急時メッセージに関連する。センタ３４８チームは、通信回線を通じてユーザ装置から、ユーザ装置に保存されたユーザＩＤデータ全部を自動的に受信する。このデータには、彼のナショナルＩＤ番号、医療保険番号、および登録済の医療保険会社名が含まれる。さらに、センタ３４８チームは、彼専用装置のメモリに保存されたユーザの緊急連絡先に関するデータを受信する。

【０１７０】

ステージ５２６において、緊急センタチームは、彼の携帯電話を通じて彼本人に連絡し、さらにユーザの緊急時連絡先に連絡して、可能な限り早くこの本人の存在位置を得るためのリクエストをする。

【０１７１】

ステージ５２７において、緊急センタが呼び出したユーザが彼の電話に応答し、医療または他の種類の即時の手助けをリクエストする場合には、処理はステージ５２８に進む。これ以外の場合では、ユーザは、ステージ７２０に着手された処理において、システムメモリに保存されている最新の医療記録にアクセスし得る。ユーザは次に、彼自身が医療扶助を受ける前に、ホストコンピュータまたは携帯電話を通じて彼専用装置にそれらをダウンロードする。

【０１７２】

ステージ５２８において、緊急センタチームは、ユーザの位置に最も近い救助隊を呼び出し、ユーザの正確な位置、および彼のパーソナル装置に保存されているユーザの救急医療時の記録に関する要点を電話で説明する。同時に、緊急センタチームは、システムメモリに保存されているそのユーザの全ての医療記録を更新し、このユーザに関する完全な医療ファイルレポートを作成する。これは、さらなる治療のために、救助隊がユーザの搬送を意図している選択された病院の緊急治療室チームに電子的に転送されるか、ファックスされる。

【０１７３】

ステージ５４５において、ユーザは、政府機関、地方自治体、大学、カスタマズクラブなどとのユーザの相互作用に必要な関連する接続を含む、非保護個人データを扱い、それらと情報を送受信するための、全てのユーザ要求を支援するメニューに接続されている。

【０１７４】

ステージ６５０において、ユーザは、銀行、他の金融機関、保険会社などとのユーザの相互作用に必要な関連する保護個人データを扱い、それらと情報を送受信するための、全てのユーザ要求を支援するメニューに接続されている。

【０１７５】

ステージ７２０において、ユーザは、病院とのユーザの相互作用に必要な関連する保護個人データを扱い、かつそれと情報を送受信するための、全てのユーザ要求を支援するメニューに接続されている。

【０１７６】

ステージ８０１において、ユーザは、彼のパーソナル装置へのかつそこからの彼の保護個人データの保存および検索に関連するメニューを受信して、彼のホストの表示部に表示する。

【０１７７】

ステージ９９９において、ユーザは、システムとの相互作用を終了するか、ステージ５１５に示すようなシステムのメインメニューとの相互作用に戻すように移動することを選択できる。

【０１７８】
本発明の装置の使用に関連する処理ステップを示す別の可能なフローチャートを、６００で概略を指定して示す。ここでは、ユーザが肯定的に確認され、本発明のシステムへの承認済アクセスを得て、本発明のシステムとの接続を構築した後に実行されるユーザと本発明のシステムとの相互作用を示す。このフローチャートに記述する処理６００は、ユーザが、種々の銀行、クレジットカード会社、および金融機関への、システムを通じた保護アクセスを得、必要に応じて、特定の関連するデータ検索を実行するステージから開始され、ユーザが第１ステージに到達したときに、金銭取引の更新および実行を記録する処理を開始する。この本発明のシステムユーザのアクセス生成処理において開始される処理６００を図６に示す。

【０１７９】
処理６００の第１ステージ６５０において、ユーザはメニュー画面を受信し、この画面において、ステージ６６４にシフトするクレジットカード会社、ステージ６５１にシフトする銀行、またはステージ６７１にシフトする保険会社を選択できる。ユーザは、これらのいずれのルートへの継続も所望しない場合には、図５に関して前述したステージ５１５に戻ることを選択できる。

【０１８０】
ステージ６５１において、ユーザは、銀行選択オプションを選択して、システムに登録済の銀行メニューのリストを得る。このリストで興味があるか、預金口座を有する銀行を選択する。

【０１８１】
ステージ６５２において、本発明のシステムは、高度に保護された通信回線を通じて、ユーザが選択した銀行および彼に関与する特定の支店に接続できる。

【０１８２】
ステージ６５３において、ユーザ装置は、選択した銀行および支店に、特定の選択された銀行がリクエストしたフォーマットにおいて、ユーザの銀行の預金口座番号およびユーザＩＤデータ（例えば、ユーザ名およびパスワード）を送信する。

【０１８３】
ステージ６５４において、銀行のコンピュータは、特定のユーザ登録済銀行へのアクセス許可データの詳細および預金状態をそのメモリに割り当て、それらを、ユーザ装置のメモリから抽出したユーザ関連の詳細と比較する。この詳細が一致し、リクエストされた銀行の預金口座番号が銀行記録に検出された場合には、この処理はステージ６５５に進む。検出されない場合には、ユーザはステージ６５０に戻る。

【０１８４】
ステージ６５５において、ユーザは、彼の預金口座または実行した金銭取引の詳細検索を選択可能なメニューを受信する。ユーザが預金口座において金銭取引の実行を所望する場合には、ステージ６５６に進む。ユーザが、彼が選択した過去の取引の詳細検索を所望する場合には、ステージ６６０に進む。

【０１８５】
ステージ６５６において、ユーザは、ステージ６５８に継続することによって、彼専用装置の保護メモリサブモジュール内の電子財布セクションへの金銭の振込を選択できる。または、ステージ６５７に進むことによって、第三者の預金口座への送金操作を選択できる。

【０１８６】
ステージ６５７において、ユーザは、本発明のシステムを通じて銀行のコンピュータと安全に相互作用できるホストの画面において、送金先の第三者名、彼の預金口座番号、並びに彼の銀行および支店の詳細などの画面の空欄を埋めることをリクエストされる。

【０１８７】
ステージ６５８では、ユーザは、ホスト画面において、送金する金額に関する画面上の空欄の入力をリクエストされる。

【０１８８】
ステージ６５９において、銀行がこの取引を承認するとステージ６６２に進む。承認しない場合には、この処理はステージ６５５に戻る。
【０１８９】
ステージ６６０では、ユーザは、ホストの表示部の画面において、取引日の時間範囲または取引番号などの、彼が検索を所望する金銭取引の詳細のパラメータの入力をリクエストされる。
【０１９０】
ステージ６６１において、銀行はリクエストされた金銭データを検索し、専用通信チャネルを通じた高度に保護された方法で、本発明のシステムに送信し、次に、システムを通じて、関連するユーザの金銭データをユーザのホストコンピュータに転送して、その画面上に表示する。
【０１９１】
ステージ６６２では、ユーザは彼のホストにおいて、どのリクエストされた金銭データの保存を彼が所望するかの選択を要求する画面を受信する。彼は、そのデータを、彼専用装置のメモリに保存するか、システムデータバンクにおける彼の個人データメモリセクタに保存するか、またはその両方のメモリに同時に保存するかを選択できる。
【０１９２】
ステージ６６３において、この処理は、図８に記述するステージ８０１に戻る。
【０１９３】
ステージ６６４において、ユーザは、クレジットカード会社をリストから選択するメニュー画面を受信し、ステージ６５０に戻る。
【０１９４】
ステージ６６５において、本発明のシステムは、選択されたクレジットカード会社に接続する。
【０１９５】
ステージ６６６において、ユーザ装置は、特定のクレジットカード会社が同意した保護フォーマットにおいて、システムを通じて、ユーザ名に関連するユーザのクレジットカード番号および追加のクレジットカードデータをクレジットカード会社に送信する。
【０１９６】
ステージ６６７において、クレジットカード会社は、このカードを承認し得、この処理は６６８に継続する。承認しない場合には、この処理はステージ６６４に戻る。
【０１９７】
ステージ６６８では、ユーザは、ホストの表示部の画面において、クレジットされる資金および金額を得るべく選択された団体の詳細を埋めることをリクエストされる。
【０１９８】
ステージ６６９において、ユーザは、クレジットされる団体の詳細を入力し、要求される詳細の一部のみしか知らない場合には、選択された団体との過去のあらゆる以前の取引に関する、選択された団体の詳細のフルセットに関する示唆を、彼専用装置により自動的に提供される。選択された詳細は、次に、システムを通じてクレジットカード会社に送信される。取引が承認された場合には、処理は６７０に継続する。承認されない場合には、クレジットカード会社との相互作用を開始するステージ６６４に戻る。
【０１９９】
ステージ６７０において、クレジットカード会社は、取引を承認し、ステージ６７１に継続する。承認しない場合には、取引は拒否され、処理はステージ６６４に戻る。
【０２００】
ステージ６７１において、クレジットカード会社は、リクエストされた取引を実行し、本発明のシステムを通じて、取引承認の詳細なメモをユーザ装置に送信する。
【０２０１】
ステージ６７２において、ユーザは、任意のクレジットカード会社を通じた別の取引の

処理を所望するか否かを問う画面を得る。これを所望する場合には、この処理はステージ６６４に戻る。所望しない場合には、処理は選択されたメモリ内に取引を維持するステージ６６２に戻る。

【０２０２】

ステージ６７３において、ユーザは、システム管理者により承認され、かつシステムサーバに登録済のリストから保険会社を選択するメニュー画面を受信する。または、代替的に、ステージ６５０に戻る。

【０２０３】

ステージ６７４において、システムサーバは、ユーザが選択した保険会社のサーバへのダイレクトアクセスを生成し、それに接続する。

【０２０４】

ステージ６７６において、ユーザ装置は、システムを介して保険会社のサーバに、ユーザＩＤデータに加えて、特定の選択した保険会社における彼の登録済ユーザ名およびパスワードを送信する。

【０２０５】

ステージ６７７において、保険会社のサーバは、登録済の顧客としてユーザを承認し、ユーザに、その保険会社における彼の預金口座へのダイレクトアクセスを開放する。ユーザが送信したＩＤおよびアクセスデータが承認されなかった場合には、ユーザは、別の保険会社へのアクセスを試みるステージ６７３に戻る。

【０２０６】

ステージ６７８において、保険会社は、ユーザからの特定の命令、例えば、彼専用装置への特定の保険契約証書のダウンロード、または別の契約証書内のデータの更新などを受け取り、次に、保険会社のサーバはユーザのリクエストを承認する。ユーザとの相互作用処理の終わりに、保険会社のサーバへのユーザのアクセスは閉じられ、ユーザはステージ６７３に戻る。

【０２０７】

本発明の装置の使用に関連する処理ステップを示す別の可能なフローチャートを示す。ここでは、ユーザが肯定的に確認され、本発明のシステムへの承認済アクセスを得て、本発明のシステムとの接続を構築したステージ後に実行されるユーザと本発明のシステムとの相互作用を示す。このフローチャートに記述する処理は、ユーザが、種々の病院、医療クリニック、ＨＭＯおよび他の中間団体、並びにサービス提供者への、システムを通じた保護アクセスを得、記録の更新およびユーザの医療記録の更新を実行するための、前述の図５に示すような、特定の関連するデータ検索を実行するステージから開始される。この処理は、図７に示す本発明のシステムユーザのアクセス生成処理７００においてユーザがステージ７２０に到達するところから開始される。

【０２０８】

処理７００のステージ７２０において、ユーザは、図５に関して記述したような本発明のシステムへのフルアクセスを受信し、彼の相互作用画面において、彼の医療記録を処理するシステムメモリへのアクセスを得るオプションを選択し、システムを通じて、種々のシステムに登録済の医療サービスプロバイダへの保護アクセスを得る。

【０２０９】

ステージ７２０において、ユーザは、医療保険会社（ＨＭＯ）の選択を彼にリクエストするメニュー画面を受信し、次に、彼はステージ７２１に進む。または、代替的に、病院を選択してステージ７４０に進むか、ステージ５１５に戻って処理を終了する。

【０２１０】

ステージ７２１において、システムは、ユーザ装置のメモリに保存されている医療記録内の関連データに従い、ユーザが会員である医療保険会社のサーバへの保護アクセスを生成する。

【０２１１】

ステージ７２２において、装置は、ユーザ会員のユーザ名および医療保険の会員ＩＤ番

号、さらにリクエストされた場合には、医療保険ウェブサイトへのユーザのアクセスパスワードを、医療保険サーバに送信する。

【０２１２】

ステージ７２３において、医療保険会社のサーバは、ユーザの医療ファイルＩＤデータが、本発明のシステムを通じてユーザ装置から受信したＩＤおよびユーザのデータに適合するか否かを確認する。この結果が肯定的である場合にはステージ７２４に継続し、否定的である場合には、ステージ７２０に戻る。

【０２１３】

ステージ７２４において、システムは、彼のホストまたは携帯電話の表示画面を通じて得るメニュー画面において、いくつかのオプションの選択をユーザにリクエストする。オプション７２５において、ユーザは医師またはクリニックの予約を選択できる。選択オプション７３０において、ユーザは、全ての彼の過去の医療検査結果をリクエストする。別の方法では、ユーザはステージ７２０に戻るように導かれ、彼が選択したさらなる処理事項が無い場合には、処理を停止する。

【０２１４】

ステージ７２５において、ユーザは、彼のホストの表示部に、システムを通じて医療保険からの画面を受信する。この画面において、ユーザは、彼が面会を所望する医師の種類および名前の選択をリクエストされる。

【０２１５】

ステージ７２６において、ユーザは、選択した医師の受付可能日および時間を表示する画面を得る。

【０２１６】

ステージ７２７において、ユーザは、選択した医師への予約として彼の都合の良い日および時間を選択する。

【０２１７】

ステージ７２８において、ユーザは、医療保険コンピュータから、彼が最終承認した医療予約の時間および日に関する最終確認通知を表示するホスト画面を受信する。次に、ステージ７２９に進む。

【０２１８】

ステージ７２９において、ユーザは、彼が別の予約を所望するか否かを選択するメニューを表示したホストの表示画面を受信する。次に、７２５に移動するか、彼の過去の医療検査結果を確認する７３０に進むか、メインメニュー７２０に戻るか、ステージ８０１において保存される。

【０２１９】

ステージ７３０において、ユーザは、医療保険サーバから、彼が再確認を所望する医療検査結果を選択するメニュー画面を表示したホストの表示画面を受信する。

【０２２０】

ステージ７３１において、ユーザが検査結果のリクエストを選択すると、ユーザ装置は、彼専用装置のメモリに特定の検査による最新結果が有る場合には、それをホスト画面に転送する。

【０２２１】

ステージ７３２において、医療保険会社のサーバは、このユーザにより関連深い最新の検査データが検出できるか否かを確認するためにそのメモリ記録を検索し、次に、検出したファイルをユーザのホストに送信する。これによりユーザは、画面にその結果を表示するか、かつ／または長期保存のために彼専用装置のメモリにそれを保存するかを選択できる。

【０２２２】

ステージ７３３において、ユーザは、検索した医療検査結果の処理に関する選択を実行し、システムは図８に示す保存ステージ８０１に接続し得るステージ７２９に戻る。

【０２２３】

ステージ７４０において、ユーザは、ホストの表示部に、リストから病院を選択するメニュー画面を受信するか、ステージ７２０に戻る。次に、彼は、リストから好ましい病院を選択し、ステージ７４１に進む。

【０２２４】

ステージ７４１において、システムサーバは、表示リストに示す病院各々との、サーバが有する保護通信チャネルを介して選択された病院に連絡し、病院サーバとの開放通信リンクを生成する。

【０２２５】

ステージ７４２において、ユーザのパーソナル装置は、フルネーム、ＩＤカード番号、および詳細を含むユーザのＩＤデータファイルを送信する。

【０２２６】

ステージ７４３において、選択された病院サーバは、識別ユーザがその病院のクリニックの入院患者であったか、そこで治療されたかの記録を有するか否かを確認する。その記録が有る場合には、ステージ７４４に進み、無い場合には、ステージ７４０に戻る。

【０２２７】

ステージ７４４において、ユーザは、病院が公開している医療レポートまたは医療検査結果を彼が必要であるか否かの選択をリクエストするメニューを表示した画面を受信し、その画面上で選択する。

【０２２８】

ステージ７４５において、病院サーバは、選択されたデータファイルを検索し、７４６に進む。リクエストされたデータファイルを検出できない、および検出しない場合には、この処理はステージ７４０に戻る。

【０２２９】

ステージ７４６において、ユーザは、病院からの情報を彼のホスト画面上で受信する。

【０２３０】

ステージ７４７において、ユーザは、検索された病院データをどこに保存するかの選択をリクエストするメニュー画面を受信する。例えば、ユーザの個人医療データファイルが保存されているシステムメモリ、ユーザのパーソナル装置のメモリ、またはこれらの両方に保存するかを選択する。次に、ステージ８０１に進む。

【０２３１】

ステージ８０１において、新規医療ファイルを、１つまたは２つの選択された保存メモリに保存および記憶した後に、この処理はステージ７２０に戻る。このステージで、ユーザは、本発明のシステムおよび外部医療サービス提供者を利用した別の医療データ処理シーケンスを開始する新規のメニュー画面を得るか、図５に示すステージ５１５に戻る。

【０２３２】

本発明の装置の使用に関連する専用処理ステップを示す別の可能なフローチャートを示す。ここでは、ユーザが肯定的に確認され、本発明のシステムへの承認済アクセスを得て、本発明のシステムとの開放接続リンクを構築したステージの後に実行されるユーザと本発明のシステムとの相互作用を示す。このフローチャートに記述する専用処理は、ユーザが、システムメモリバンクにかつそこから外部にデータを保存および検索する必要があるステップに関連する。この関連処理を、本発明のシステムメモリにおけるデータを保存および検索する処理８００を含む図８に示す。

【０２３３】

ステップ８０１において、ユーザは、彼のホスト画面上のメニューにおいて、システムメモリからデータ検索の選択をリクエストされる。次に、この処理はステージ８０５に進む。代替的に、ユーザが、システムメモリ内のデータを保存するオプションを選択する場合には、処理はステージ８２０に進み、ユーザがこの処理の終了を所望する場合には、ステージ９９９に進む。

【０２３４】

ステップ８０５において、リクエストされたデータが、システムの大容量バンクの非保

護データメモリパーティションからのものである場合には、処理は８１０に進む。または、ユーザが、システムメモリの保護データパーティションからの保護データの検索を必要とする場合には、処理は８１６に進む。

【０２３５】

ステージ８１０において、ユーザのパーソナル装置は、ユーザのＩＤデータファイルを送信する。

【０２３６】

ステージ８１２において、システムサーバはユーザＩＤを承認し、ユーザが選択したデータ検索キーワードを得るために彼にリクエストする。これにより、システムサーバは、システムメモリの巨大データベースからリクエストされたデータを検出できる。

【０２３７】

ステージ８１４において、システムサーバは選択された検索キーワードを承認し、所定のキーワードに従いリクエストされたデータファイルを検出し、ステージ８０５に戻る。

【０２３８】

ステージ８１６において、ユーザがステージ８０５で選択したオプションにおいて保護データファイルを検索する場合には、ユーザ装置は、識別が保護されている、装置のメモリに保存されているＬ列の英数字をシステムサーバに送信する。この英数字は、第１のユーザ登録ステージの機能により、システムサーバにおいて生成された保護アクセスコード、セキュリティ文字列であり、装置のメモリに加えて、識別ユーザのデータを保存しているシステムメモリセクタにも保存される。

【０２３９】

ステージ８１７において、システムサーバは、リクエストされた保護データファイル関連データベースアクセスキーワードの入力をユーザにリクエストし、ステージ８１８に進む。

【０２４０】

ステージ８１８において、システムサーバは、ユーザが選択した検索キーワードに従い、ユーザがリクエストした保護データファイルを検索し、ユーザは、ホストを通じて８０１に戻るか否かの返答をリクエストされる。ユーザがさらなるデータの保存、または検索シーケンスの起動を所望する場合には、８０５に戻る。または、終了ステージ９９９に進み、処理を停止する。

【０２４１】

ステージ８２０において、ユーザは、彼のホストのメニュー画面を通じて、ステージ８２１においてシステムの非保護データメモリセクタ内の検索されたまたは新規データを保存するか否かの返答をリクエストされる。または、システムの保護データメモリセクタ内の新規データの保存を所望する場合には、ステージ８２６に進み、または、ステージ８０１に戻り、処理８００全体を再開する。

【０２４２】

ステージ８２１において、ユーザのパーソナル装置は、ユーザのＩＤカード番号を送信する。

【０２４３】

ステージ８２２において、システムサーバは、ユーザとの接続中に、彼が接続しているホストまたは携帯電話を通じて、ユーザが選択したデータベースの保存、およびシステムのデータベース内の彼の個人ファイルセクタに彼が保存を所望する特定の新規データファイルに関連する検索キーワードの取得をユーザにリクエストする。

【０２４４】

ステージ８２４において、パーソナル装置は、処理中の特定ファイルを暗号化し、それを、ユーザが検索可能な、システムのデータベース内のユーザの個人ファイルセクタに送信し、ステージ８０１に戻る。

【０２４５】

ステージ８２６において、パーソナル装置は、保護アクセスコードの、ユーザシステム

が承諾した秘密のＬ桁の英数字の識別文字列をシステムサーバに送信する。

【０２４６】

ステージ８２８において、システムセバーは、ユーザが選択したデータベースに保存された、彼がアクセスできないシステムのデータベース内の個人ファイルセクタ内に安全に暗号化された保存を所望する特定の新規データファイルに関する検索キーワードを定義して送信することをユーザにリクエストする。

【０２４７】

ステージ８２９において、パーソナル装置はユーザファイルを暗号化し、それを、システムの保護かつ暗号化されたデータファイルメモリセクタに保存するために、システムサーバに送信する。次に、ユーザは、データ処理プロセスを繰り返してステージ８０１に進むか、処理を終了して終了ステージ９９９に進むかを選択できる。

【０２４８】

ステージ９９９において、この処理は終了し、ユーザは、共に電源を切られたシステムサーバおよび彼のパーソナル装置から切断される。

【０２４９】

ここで図９を参照すると、本発明に関連する専用デバイス１０００を示す。これは、本発明の装置のための充電およびユーザ個人データバックアップデバイスの可能な一実施形態として機能する。図９は、本発明の装置の充電およびデータバックアップデバイスに関する概念モジュール構造、並びに関連デバイスの内部サブモジュール配置および機能性の実例を示す。

【０２５０】

図９に示すブロック１０１０は、デバイス１０００の主要プラグイン充電モジュールであり、デバイス１０００の主電源に接続された充電プラグ１０１２、ＡＣ－ＤＣ変換ユニット１０１４、および電源供給ユニット１０１６を含む。ユニット１０１４は、主要な交流電圧から直流電圧に変換し、電源供給ユニット１０１６は、変換された直流電圧から、デバイス１０００の電子サブモジュール１０２０の種々の電子的構成要素の駆動に必要な全ての直流電圧を生成する。

【０２５１】

サブモジュール１０４０は充電器および充電式バッテリを含み、主電力からの電圧源が無い場合でも、電力のバックアップおよびデバイス１００の安全操作が可能になる。サブモジュール１０２０はデバイスの主電子モジュールであり、マイクロプロセッサおよび関連する電子サブモジュール１０２４、並びに大容量固体フラッシュメモリベースのサブモジュール１０２８を含む。これは、装置１００のメモリユニット１５０とメモリユニット１７０とを合わせたデータ保存容量と同等の記憶容量サイズを有する。電子ユニット１０２０は、装置１００がその相間データプラグ１１０を通じて、デバイス１０００の接続プラグユニット１０３０に接続しているときは常に、メモリサブモジュール１０２８の更新要求を自動的に確認する。プロセッササブモジュール１０２４は、装置１００が最後に更新された日付、並びにそれに関連する保護および非保護メモリのデータコンテンツおよびその状態を確認する。そして、それがデバイスのメモリ１０２８に保存されたデータの次に新しい場合には、メモリユニット１０２８内に、装置１００のメモリサブモジュール１５０および１７０のコンテンツのミラーイメージを作成する。装置１００の記憶内容が、何らかの理由により消去または損なわれた場合には、サブモジュール１０２４がそれを検出し、工夫１０００のメモリモジュール１０２８に保存されたデータの最新バージョンを用いて、装置１００のメモリユニット１５０および１７０を自動的に更新する。

【０２５２】

サブモジュール１０５０は電子ブザー起動モジュールであり、これは、ボタンを押すと動作し、デバイス１０００のハウジングに配置される。ＲＦトランスミッタもこのサブモジュール１０５０に一体化される。ユーザが家庭またはオフィス環境における彼専用装置の正確な位置への配置を必要とする場合に、モジュール１０５０のブザーボタンを押すと、統合ＲＦトランスミッタサブモジュール１０５０が、装置１００のハウジング内に埋め

込まれたブザーＲＦ受信サブモジュール１９８に符号化信号を送信し、検知された符号化信号により、容易に感知可能な音を出す電子音ブザーが作動する。音ブザーは、装置１００のサブモジュール１６６内に一体化される。部屋または空間における装置１００の位置を示す発生音を通じて、ユーザは、装置の位置を容易に定めることができる。

【図１】

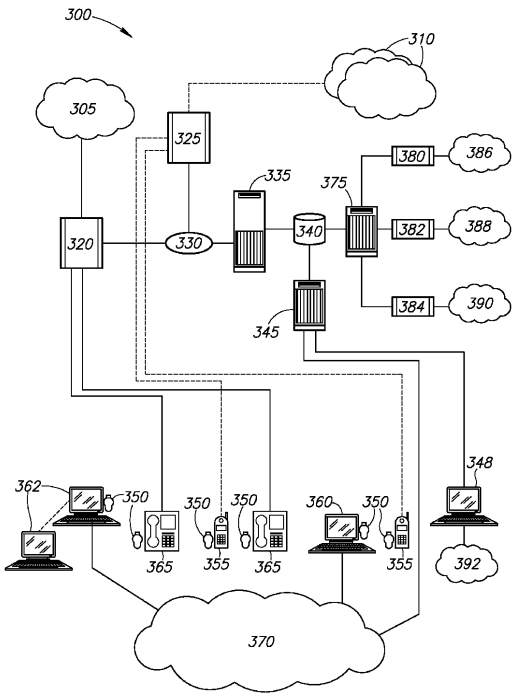


FIG.1

【図２】

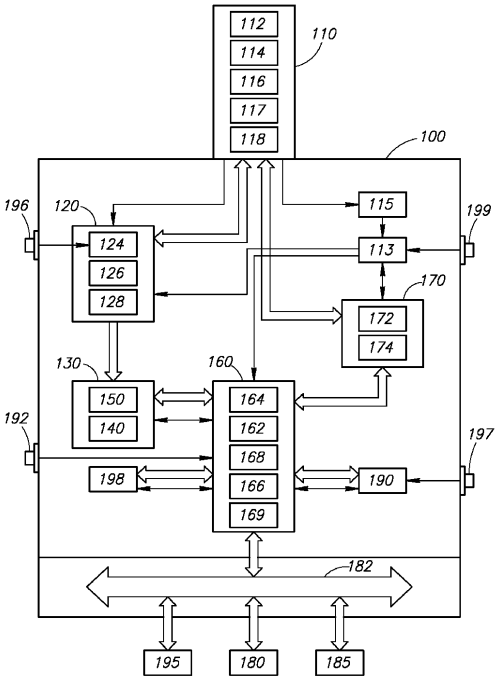


FIG.2

【図３Ａ】

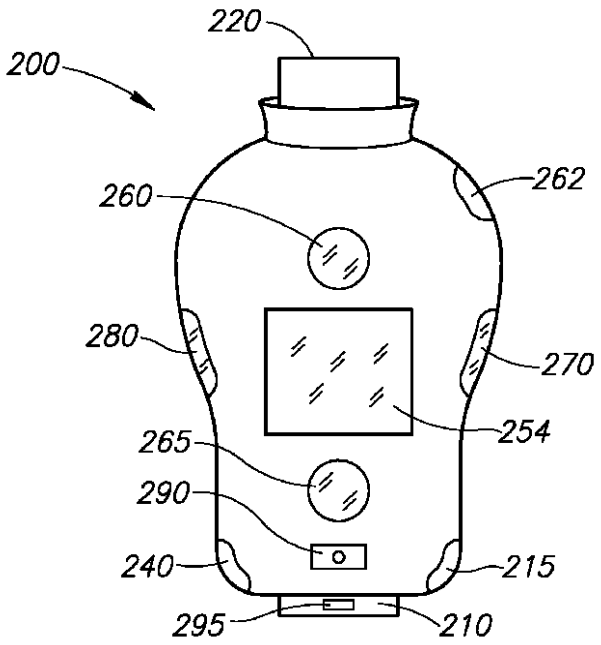


FIG.3A

【図３Ｂ】

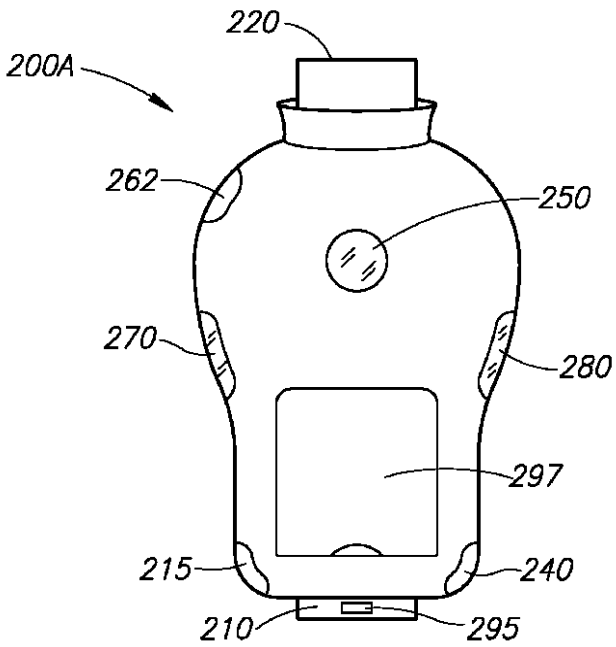
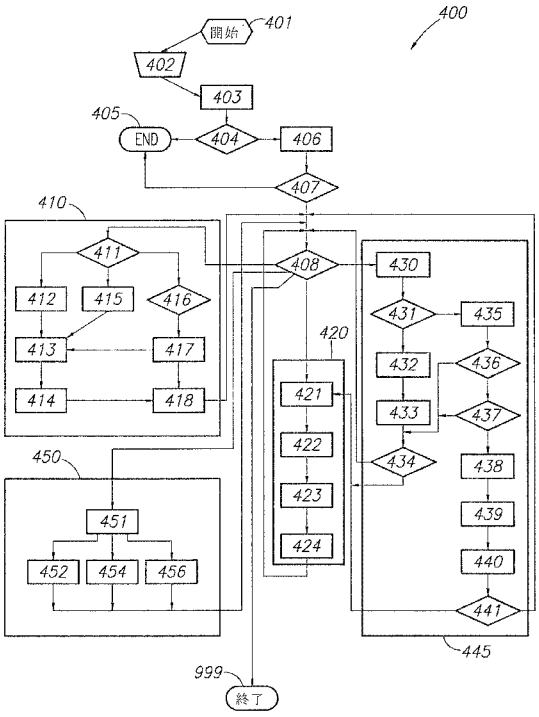
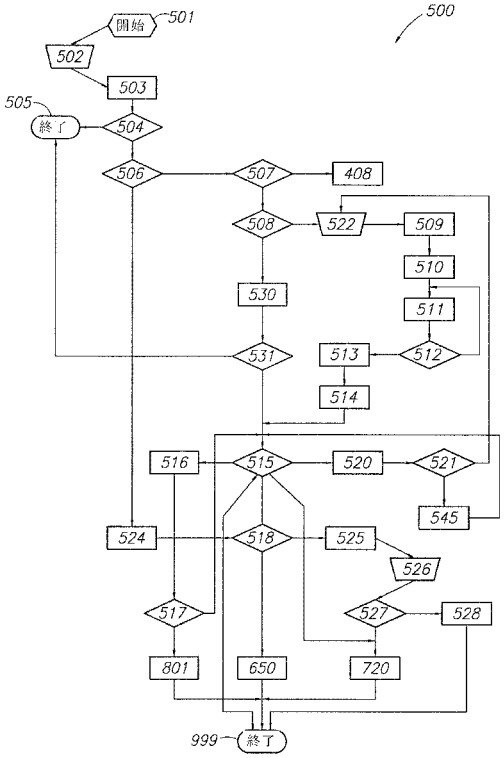


FIG.3B

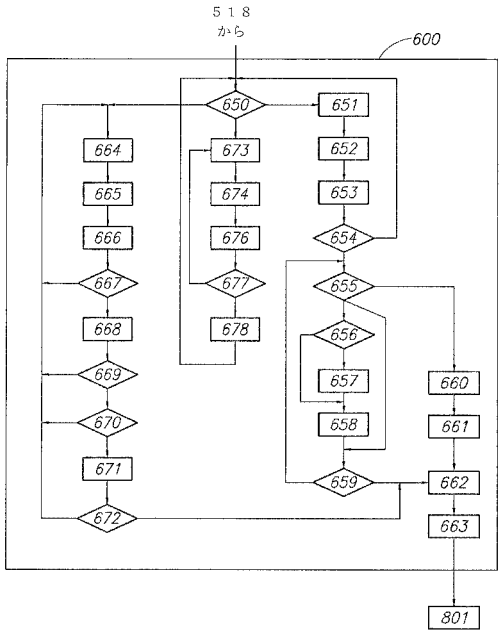
【図４】



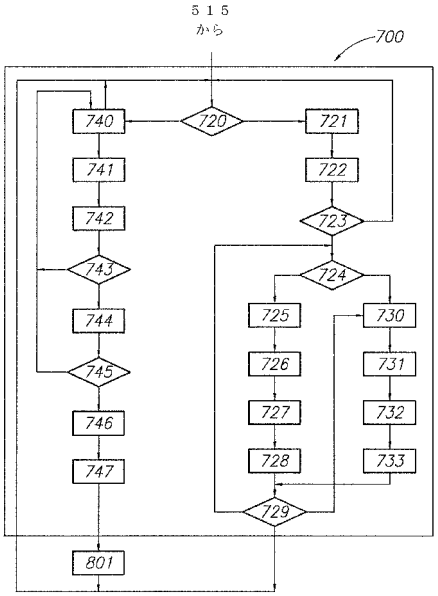
【図５】



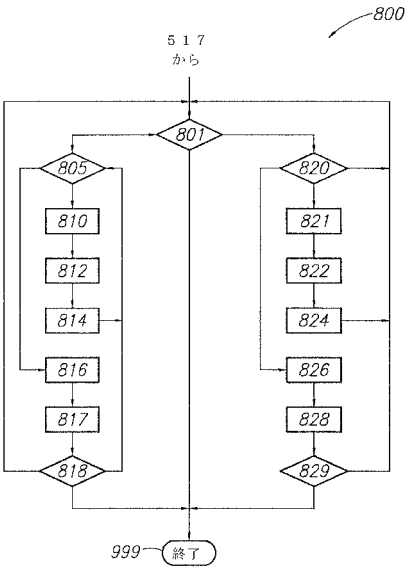
【図６】



【図７】



【図８】



【図９】

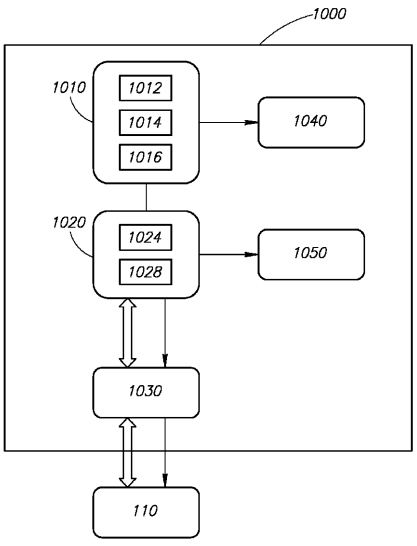


FIG.9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 11/51002

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/00 (2011.01)
USPC - 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
713/186; G06F 21/00 (2011.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
713/150; 713/182, 713/186 G06F 21/00; G05F$ Key Word Limited - See terms below

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWest (PGPB, USPT, EPAB, JPAB); Google Patents
Search Terms: Personal, private, secure, access, exclusive, secluded, secret, Data, Information, details, facts, material, knowledge, goods biometric, biologic$5, identify$5, authentic$5, verif$5, real, genuine, confirm$3, corroborat$4, user, consumer, client, Encrypt$5,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2009/0204433 A1 (Darian et al.) 13 August 2009 (13.08.2009), entire document, especially FIG 1-2 and para [0031]-[0061]	21, 24-25, and 27-34 --- 1-20, 22-23, 26, and 35-37
Y	US 2002/0095587 A1 (Doyle et al.), 18 July 2002 (18.07.2002), entire document, especially para [0003]-[0068]	1-20, 22-23, 26 and 35-37
Y	US 2008/0249856 A1 (Angell et al.), 9 October 2008 (09.10.2008), entire document, especially para [0038]	4, 23, and 36-37
A	US 2008/0109883 A1 (Hernoud et al.) 8 May 2008 (08.05.2008), entire document	1-37

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2011 (18.07.2011)	04 AUG 2011
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 フィッシュ，ジラ
イスラエル国，９０８０５ メヴァスセレト ザイオン，ピー．オー．ボックス ８４２７５，１０／３ エフロニ ストリート
(72)発明者 コーマン，エイヴナー
イスラエル国，４６３６２ ヘルズリア，１ ブネイ ビンヤミン ストリート

Ｆターム(参考) 4C038 VA07
5B043 AA04 AA09 BA02 BA04 DA04 DA05 DA09 GA13 GA18