(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2013-541770
(P2013-541770A)
(43)公表日　平成25年11月14日(2013.11.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/35	(2013.01)	G06F	21/20	135	5B035
G06K 19/07	(2006.01)	G06K	19/00	H	5B058
G06K 19/10	(2006.01)	G06K	19/00	S	
G06K 17/00	(2006.01)	G06K	19/00	R	
		G06K	17/00	F	

審査請求 有　予備審査請求 未請求　（全 24 頁）　最終頁に続く

(21)出願番号　特願2013-531693 (P2013-531693)
(86)(22)出願日　平成23年9月23日 (2011.9.23)
(85)翻訳文提出日　平成25年5月24日 (2013.5.24)
(86)国際出願番号　PCT/US2011/053121
(87)国際公開番号　WO2012/047564
(87)国際公開日　平成24年4月12日 (2012.4.12)
(31)優先権主張番号　12/892,489
(32)優先日　平成22年9月28日 (2010.9.28)
(33)優先権主張国　米国 (US)

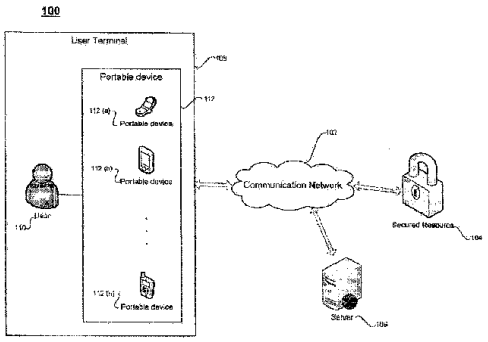
(71)出願人　310021766
株式会社ソニー・コンピュータエンタテインメント
東京都港区港南１丁目７番１号
(74)代理人　100099324
弁理士　鈴木　正剛
(72)発明者　スティーブン　オスマン
アメリカ合衆国、カリフォルニア州　９９４０４－２１７５、フォスター　シティー、イースト　ヒルスデイル　ブルバード　９１９、ソニー　コンピュータ　エンタテインメント　アメリカ　リミテッド　ライアビリテイ　カンパニー内

最終頁に続く

(54)【発明の名称】セキュアリソースへのアクセス方法およびシステム

(57)【要約】
ポータブルデバイスを使用してセキュアリソースにアクセスするためのシステムおよび方法を提供する。ポータブルデバイスを携帯しているユーザがロックされたドアやその他のセキュアリソースから非常に近い範囲にいる場合、確認プロセスが該デバイスで自動的に起動されうる。このユーザ確認はデバイス上のすべての入力および感知法を利用することも可能であった。この識別プロセスがうまくいくと、ロックされたドアやデバイスに有線または無線ネットワーク経由でアクセスコードが送信されうる。 これにより、これらのロックされたドアで必要とされる電子機器を減らすことができ、また、よりダイナミックなセキュリティ手段を講じることができる。

FIGURE 1



【特許請求の範囲】
【請求項１】
リソースのセキュアエリアに外部デバイスがアクセスするための方法であって、
前記デバイスを認証機能を有するものとして識別する信号を送信するステップを有し、
前記リソースとの通信の開始を受信するステップを有し、
前記デバイスの１以上の認証メカニズムに送信することにより前記通信の開始に応じるステップであって、前記認証メカニズムは、前記デバイスのユーザの属性を識別するためのハードウェアデバイスであり、
１以上の前記認証メカニズムの使用要求を受信するステップを有し、
前記要求された認証メカニズムの各々にトークンを送信するステップを有し、
前記リソースが前記１以上のトークンを受け取ったことに応答して、前記セキュアエリアへアクセスするステップを有する方法。
【請求項２】
前記開始は無線通信である、請求項１記載の方法。
【請求項３】
前記デバイスはポータブルデバイスである、請求項１記載の方法。
【請求項４】
前記認証メカニズムは前記デバイスの所持である、請求項１記載の方法。
【請求項５】
前記認証メカニズムはバイオメトリックである、請求項１記載の方法。
【請求項６】
前記バイオメトリックは網膜スキャンデータを含む、請求項１記載の方法。
【請求項７】
前記認証メカニズムは暗証番号である、請求項１記載の方法。
【請求項８】
前記デバイスは前記リソースへ起動信号を送信する、請求項１記載の方法。
【請求項９】
前記デバイスは前記リソースへ電力発生信号を送信する、請求項１記載の方法。
【請求項１０】
リソースが、外部デバイスに対して前記リソースのセキュアエリアへのアクセスを許可する方法であって、
認証機能を有する前記外部デバイスから信号を受信するステップを有し、
前記外部デバイスとの通信を開始するステップを有し、
前記外部デバイスが提供可能な１以上の認証トークンのリストを受信するステップであって、前記認証トークンは前記外部デバイスのユーザの属性を識別するためのハードウェアデバイスの結果によるものであり、
１以上の認証トークンの要求を送信するステップを有し、
前記要求に応じて１以上の認証トークンを受信するステップを有し、
前記１以上の認証トークンのアクセプタビリティに基づいて、前記外部デバイスに前記セキュアエリアへのアクセスを許可するステップを有する方法。
【請求項１１】
前記通信は無線通信である、請求項１０記載の方法。
【請求項１２】
前記認証トークンはバイオメトリックデバイスである、請求項１０記載の方法。
【請求項１３】
前記リソースは起動信号を前記外部デバイスに送信する、請求項１０記載の方法。
【請求項１４】
前記リソースは電力を前記外部デバイスに送信する、請求項１０記載の方法。
【請求項１５】
リソースのセキュアエリアへアクセスするためのポータブルデバイスであって、

前記デバイスを認証機能を有するものとして識別する信号を送信するトランスミッタと、
前記リソースとの通信の開始を受信するレシーバと、
前記デバイスの１以上の認証メカニズムに送信することにより前記通信の前記開始に応じるためのコントローラと、を含み、
前記レシーバは１以上の前記認証メカニズムの使用要求を受信し、
前記トランスミッタは前記要求された認証メカニズムの各々に対するトークンを送信し、
前記デバイスは前記リソースが前記１以上のトークンを受け取ると、前記セキュアエリアへアクセスする、ポータブルデバイス。
【請求項１６】
前記通信は無線通信である、請求項１５記載のデバイス。
【請求項１７】
外部デバイスに前記リソースのセキュアエリアへのアクセスを許可するためのリソースの認証ユニットであって、
認証機能を有する前記外部デバイスからの信号を受信する第１レシーバと、
前記外部デバイスとの通信を開始するためのコミュニケータと、を含み、
前記レシーバは前記外部デバイスが提供することのできる１以上の認証トークンのリストを受信するものであり、前記認証トークンは前記外部デバイスのユーザの属性を識別するためのハードウェアデバイスの結果によるものであって、
１以上の認証トークンの要求を送信するためのトランスミッタと、を含み、
前記レシーバは前記要求に応じて１以上の認証トークンを受信し、
前記１以上の認証トークンのアクセプタビリティに基づいて前記外部デバイス　に前記セキュアエリアへのアクセスを許可する認証部と、を含む認証ユニット。
【請求項１８】
前記通信は無線である、請求項１７記載の認証ユニット。
【発明の詳細な説明】
【技術分野】
【０００１】
概して、本発明はセキュアリソースへのセキュアなアクセスを可能にするための方法、装置およびシステムに関する。より詳細には、本発明は、デバイスおよび／又はユーザに認められるアクセスレベルを、ユーザが利用可能なデバイスやアクセスのセキュリティレベルに基づいて識別する技術に関する。
【背景技術】
【０００２】
典型的に、ドアやコンピュータ、およびその他のデバイスなどのセキュアリソースでは、セキュアデバイスは、ドアやコンピュータ又はその他のデバイスに物理的に接続されたカードリーダでユーザのＩＤとアクセスとが確認されると解除されることになる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
セキュアシステムに複数のデバイスが存在する場合、そのような識別プロセスは時間がかかり、ユーザにとって不便である。というのも、このようなシステムでは、ユーザはそれぞれのセキュアデバイスで１つずつ識別プロセスを行う必要があるからである。また、より多くの電子機器が必要となることから、セキュアシステムのコスト増にもなる。
【０００４】
従って、本発明はポータブルデバイスを使用してセキュアリソースにアクセスするためのシステムおよび方法に関する。
【課題を解決するための手段】
【０００５】
そのようなポータブルデバイスを携帯しているユーザがロックされたドアやデバイス（

リソース）から非常に近い範囲にいる場合、該デバイス上でこの確認プロセスが自動的に起動されうる。このユーザ確認プロセスはデバイス上の全ての入力および／又は感知法や機能又は任意の所望の入力／感知法の一部を利用するものであってよい。識別プロセスがうまくいくと、ロックされたドアやデバイスに有線または無線ネットワーク経由でアクセスコードが送信されうる。これにより、これらのロックされたドアで必要とされる電子機器を減らすことができ、また、よりダイナミックなセキュリティ手段を講じることができる。

【０００６】

本発明の一実施形態は、リソースのセキュアエリアへアクセスするための外部デバイスに対する方法に関する。該方法は、該デバイスが認証機能を有することを識別する信号を送信するステップを含む。識別されたデバイスから該リソースとの通信の開始が受信される。この通信の開始に対しては、デバイスの１以上の認証メカニズムに送信することで応答がなされる。この認証メカニズムは通常、デバイスのユーザの属性を識別するためのハードウェアデバイスである。１以上の認証メカニズムの使用要求が受信される。要求された認証メカニズムの各々に対するトークンがデバイスからリソースに送信される。リソースが１以上のトークンを受け取るとセキュアエリアへアクセスできるようになる。

【０００７】

本発明の別の実施形態は、通信が無線で行われる場合に上述したリソースのセキュアエリアにアクセスするための外部デバイスに対する方法に関する。

【０００８】

本発明の別の実施形態は、デバイスがポータブルデバイスの場合に、上述したリソースのセキュアエリアへアクセスするための外部デバイスに対する方法に関する。

【０００９】

本発明のさらに別の実施形態は、デバイスの所持を認証メカニズムとする場合に、上述したリソースのセキュアエリアへアクセスするための外部デバイスに対する方法に関する。

【００１０】

本発明のさらに別の実施形態は、認証メカニズムが生体（バイオメトリック）の場合に、上述したリソースのセキュアエリアへアクセスするための外部デバイスに対する方法に関する。

【００１１】

本発明のさらに別の実施形態は、外部デバイスがリソースに起動信号を送信する場合に、上述したリソースのセキュアエリアへアクセスするための外部デバイスに対する方法に関する。

【００１２】

本発明のさらに別の実施形態は、リソースのセキュアエリアへのアクセスを外部デバイスに許可するためのリソースに対する方法に関する。該方法は、認証機能を有する外部デバイスからの信号を受信するステップを含む。外部デバイスとの通信が開始される。外部デバイスが提供することのできる１以上の認証トークンのリストが受信される。この認証トークンは外部デバイスのユーザの属性を識別するためのハードウェアデバイスの結果によるものである。１以上の認証トークン要求が送信される。この要求に応じて１以上の認証トークンが受信される。この１以上の認証トークンのアクセプタビリティに基づいて外部デバイスはセキュアエリアへのアクセスが許可される。

【００１３】

本発明のさらに別の実施形態は、認証トークンがバイオメトリックである場合に、上述したリソースのセキュアエリアへのアクセスを許可するためのリソースに対する方法に関する。

【００１４】

本発明のさらに別の実施形態は、通信が無線で行われる場合に、上述したリソースのセキュアエリアへのアクセスを許可するためのリソースに対する方法に関する。

【００１５】
本発明のさらに別の実施形態は、リソースが外部デバイスに起動信号を送信する場合に、外部デバイスによるリソースのセキュアエリアへのアクセスを許可するためのリソースに対する方法に関する。この起動信号は、例えば、外部デバイスを起動させる信号、および／又はデバイスに動作電力を供給する信号であってよい。
【００１６】
本発明のさらに別の実施形態は、リソースのセキュアエリアへアクセスするためのデバイスに関する。該デバイスは、該デバイスが認証機能を有する識別する信号を送信するための第１トランスミッタを含む。第１レシーバはリソースとの通信の開始を受信する。コントローラはデバイスの１以上の認証メカニズムを送信することにより、この通信の開始に応じる。この認証メカニズムはデバイスのユーザの属性を識別するためのハードウェアデバイスである。第２レシーバはこの１以上の認証メカニズムの使用要求を受信する。第２トランスミッタは、要求された認証メカニズムの各々に対するトークンを送信する。該デバイスさらに、リソースが１以上のトークンを受け取るとセキュアエリアへアクセスできるようになる。
【００１７】
本発明のさらに別の実施形態は、通信が無線で行われる場合に上述したデバイスに関する。
【００１８】
本発明のさらに別の実施形態は、外部デバイスにリソースのセキュアエリアへのアクセスを許可するためのリソースの認証ユニットに関する。この認証ユニットは、認証機能を有する外部デバイスからの信号を受信するための第１レシーバを含む。外部デバイスとの無線通信がコミュニケータにより開始される。第２レシーバはこの外部デバイスが提供することのできる１以上の認証トークンのリストを受信する。この認証トークンは外部デバイスのユーザの属性を識別するためのハードウェアデバイスの結果によるものである。トランスミッタは１以上の認証トークン要求を送信する。第３レシーバはこの要求を受けて１以上の認証トークンを受信する。認証ユニットは、１以上の認証トークンのアクセプタビリティに基づいて外部デバイスのセキュアエリアへのアクセスを許可する。
【図面の簡単な説明】
【００１９】
【図１】本発明の一実施形態に係るシステムの一例を示す説明図。
【図２】本発明の一実施形態に係る概略図の一例を示す説明図。
【図３】本発明の一実施形態に係る一連のステップの一例を示す説明図。
【図４】本発明の一実施形態に係る認証メカニズムの一例を示す説明図。
【図５】本発明の一実施形態に係るセキュリティサービスモジュールの一例を示す説明図。
【図６】本発明の一実施形態に係る複数のセキュリティレベルを有するセキュアリソースのサービスにアクセスする一連のステップを示す説明図。
【図７】本発明の一実施形態に係るポータブルデバイスの一例を示す説明図。
【図８】本発明の一実施形態に係るセキュアリソースの一例を示す説明図。
【図９】ポータブルデバイスがセキュアリソースに電力供給する本発明の一実施形態に係るフローチャートの説明図。
【図１０】ポータブルデバイスの認証のためにセキュアリソースが電力供給する本発明の一実施形態に係るフローチャートの説明図。
【図１１】ポータブルデバイスに対する処理およびメモリモジュールの一例を示す説明図。
【発明を実施するための形態】
【００２０】
前述の、および関連する目的を達成するために、本発明の特定の実施形態が以下の記載と添付の図面とともに本文に記載されている。しかしこれらの実施形態は、本発明の原理

が採用されうる様々な方法のうちのいくつかを示しているに過ぎず、本発明はそのような態様およびそれらの等価物のすべてを含むものとする。本発明のその他の利点、実施形態、および新たな特徴は添付の図面と併せて検討される場合に本発明の以下の記載により明らかになりうる。

【００２１】

以下の記載は例として示されているものであり、本発明を記載した特定の実施形態に限定するものではなく、添付の図面と併せることで最もよく理解することができる。＃本開示において、特に請求項及び／又は段落において、「備える」、「備えられている」、「備えている」といった用語は、米国特許法による意味を持つ。つまり、これらの用語は「含む」、「含まれた」、「含まれる」、「含んでいる」などの意味を持つがこれらに限定されない。また、明確に列挙されていない要素を持つことが可能である。「必然的に成る」、「必然的に成っている」といった用語は、米国特許法による意味を持つ。つまり、これらの用語は明確に列挙されていない要素を持つことが可能であるが、従来技術に見られる要素や本発明の基本的あるいは新規な特徴に影響する要素は除かれる。

【００２２】

これらの、およびその他の実施形態は開示されているか、以下の説明により明らかであり、また、以下の説明に包含される。本出願で使用されているように、「構成要素」および「システム」なる用語は、ハードウェアか、ハードウェアとソフトウェアの組合せか、ソフトウェアか、または実行中のソフトウェアかのコンピュータ関連の実体を指すものとする。例えば、ある構成要素は、プロセッサ上で実行中のプロセス、プロセッサ、オブジェクト、実行ファイル、実行スレッド、プログラム、および／又はコンピュータであってもよいが、これらに限定されるものでない。

【００２３】

例として、サーバ上で実行中のアプリケーションとサーバの両方が構成要素であってよい。１つ以上の構成要素が、プロセスおよび／又は実行スレッド中に存在してもよく、また１つの構成要素が、１つのコンピュータ上に存在してもよく、および／又は２つ以上のコンピュータ間に分散してもよい。本発明の他の実施形態は上述の各方法を含むが、１以上の電子記憶媒体とともに動作中の１以上のプロセッサにより実行されるコンピュータコードとしてプログラムされた装置を使用して実行される。

【００２４】

さらに、詳細な説明においては、例示目的で本発明の各種実施形態を記載しているに過ぎない。また、本発明の各実施形態は記載された方法を含むとともに、電子媒体に接続された処理装置などの１以上の装置を使用して実行されうる。本発明の各実施形態は電子媒体（電子メモリ、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ）に記録されうるか、１以上の電子記憶媒体とともに動作中の１以上のプロセッサにより実行されるコンピュータコード（例えば、ソースコード、オブジェクトコード、あるいは、任意の適切なプログラム言語）としてプログラムされうる。この電子記憶媒体は、レジスタなどの非一時的電子記憶媒体か複数の非一時的電子記憶媒、又はビット、バイト、キロバイト、波形、電子信号、デジタルフォーマット、およびその他のデータタイプや形式などの電子形態で表わされるデータを記憶することができるデータのその他の電子レポジトリ又は電子記憶場所などを含みうる。

【００２５】

本発明の各実施形態は１以上の処理デバイス又は処理モジュールを利用して実行されうる。処理デバイス又は処理モジュールは、１以上の処理デバイスで一部の処理および／又はデータ操作が実行され、これが複数の処理デバイス間で共有される又は送信されるように接続されうる。

【００２６】

図１は、本発明の各実施形態を支援するネットワークシステム１００の一例を示す。図１に示すシステム１００はネットワーク１０２、セキュアリソース１０４、サーバ１０６、および１以上の複数のポータブルデバイス（１１２（ａ）、１１２（ｂ）．．．１１２（ｎ）（「ｎ」は任意の適切な数字）へのアクセスが可能なユーザ１１０を含む。

【００２７】
ネットワーク１０２は、例えば、データの送信と処理とを行うように構成された、（ネットワーク）接続されたコンピュータ、又は処理デバイスのどのような組み合わせであってもよい。ネットワーク１０２はプライベートインターネットプロトコル（ＩＰ）ネットワークであってもよいし、ワールドワイドウェブ（ｗｗｗ）ブラウジング機能の利用が可能なインターネットなどのパブリックＩＰネットワークであってもよい。有線ネットワークの一例として、通信バスおよびモデムやＤＳＬラインを使用したネットワーク、あるいは端末間でのデータの送受信を行うローカルエリアネットワーク（ＬＡＮ）や広域エリアネットワークなどが挙げられる。無線ネットワークの一例としては無線ＬＡＮが挙げられる。

【００２８】
無線システムの別の例として、グローバルシステムフォーモバイルコミュニケーションズ[ＧＳＭ(R)]が挙げられる。このＧＳＭ(R)ネットワークは３つの主要システムに分けられる。これらは、スイッチングシステム、ベースステーションシステム、およびオペレーションおよびサポートシステム[ＧＳＭ(R)]である。さらに、コンピュータシステムではＩＥＥＥ８０２．１１（Ｗｉ－Ｆｉ）も一般に利用される無線ネットワークである。このネットワークを利用することでインターネットやＷｉ－Ｆｉ機能を有するその他のコンピュータへの接続が可能になる。Ｗｉ－Ｆｉネットワークは別のコンピュータに接続されたＷｉ－Ｆｉレシーバによって受信されうる電波を送信する。

【００２９】
セキュアリソース１０４は、例えば、ドア、コンピュータ（又はメモリやコンピュータデバイスのアクセス可能な部分）、セキュアな物理的区画及び／又はエレクトロニックロケーション（例えばデータベース、ウェブサイト、その他の制限された、又は部分的に制限されたエリア等）、又はネットワークやネットワークの一部（ＶＰＮなど）であってよい。
場合によっては、セキュリティリソース１０４は、複数のセキュリティレベルを有することも可能であろう。例えば、電子メールやカレンダーへの簡単なアクセスから、財務諸表、アドレス帳、および／又は極秘資料などの、より厳しく制限されたエリア、レベル、又はリソースへのアクセス、又はアクセス制限のある情報を有するその他のエリアへのアクセス、といった様々な範囲のサービスを提供するコンピュータネットワークが望まれる。セキュアリソース１０４に接続されたセキュリティシステムは、ユーザが認証機能を有するポータブルデバイス１１２を携帯していることを識別し、そのポータブルデバイスへの有線又は無線接続をオープンすることができる。

【００３０】
サーバモジュール又はファシリティ又はユニット１０６は、通常は対応のメモリを備えたコンピュータなどの１以上のプロセッサ、又はデスクトップコンピュータ、ノート型パソコン、携帯端末（ＰＤＡ）、無線携帯デバイス、携帯電話、ＰＬＡＹＳＴＡＴＩＯＮ(ＴＭ)、ＰＳＰ(ＴＭ)などのその他の処理デバイスである。これらのデバイスは、それ自体でデータの処理と記憶とを行うことができるものであってもよいし、別の場所から処理済の記憶されたデータにアクセスするだけのものであってもよい（つまり、シンクライアントターミナル及びファットクライアントターミナルのいずれでも良い）。

【００３１】
ユーザ端末１０８は、ユーザ１１０と、該ユーザ１１０が利用又は所持しうる１以上のポータブルデバイス１１２とを含むものとして示されている。ユーザ１１０は、ユーザ端末１０８において複数のポータブルデバイス１１２（ａ）．．．（ｎ）（本文においては１１２と称する）のうちの１つ以上を携帯するか利用しうる。ポータブルデバイス１１２は通常、処理機能やメモリや出力表示部を備えたデバイスであり、携帯電話、携帯端末、無線携帯デバイス、ＰＬＡＹＳＴＡＴＩＯＮ(ＴＭ)、ＰＳＰ(ＴＭ)などが挙げられる。ポータブルデバイス１１２はそれ自体でデータの処理や記憶、表示を行うことができるものであってもよいし、別の場所から処理済の記憶されたデータにアクセスし(つまり、シン

クライアントターミナルとファットクライアントターミナルの双方を備えたもの）、アクセスした、又は読み出したデータを表示するだけのものであってもよい。本発明の一実施形態はさらに、サーバ１０６の機能をセキュアリソース１０４および／又はポータブルデバイス１１２の一部とすることもできる。

【００３２】

ユーザ端末１０８はポータブルデバイス１１２を用いてセキュリティトークンをネットワーク１０２経由でサーバモジュール１０６に送信する。サーバモジュール１０６はユーザ端末１０８からセキュリティトークンを受信し、これをセキュリティリソース１０４へ送信する。次に、セキュリティリソース１０４は受信したトークンに基づいて識別プロセスを実行する。

【００３３】

セキュリティリソース１０４、サーバモジュール１０６、およびユーザ端末１０８は対応の双方向通信媒体を介してネットワーク１０２に接続される。この双方向通信媒体は、例えばＩＥＥＥ１３９４などのシリアルバスや、その他の有線又は無線送信媒体であってよい。セキュリティリソース１０４、サーバモジュール１０６、およびユーザ端末１０８は通信器具、又はユーザ位置、又はサブスクライバデバイス、又はクライアント端末であってよい。

【００３４】

図２に、本発明の一実施形態に従うシステム２００の一例の概略を示す。

【００３５】

ユーザ１１０がロックされた部屋や仕切られたコンパートメントや区画、又は制限されたエリアやネットワークの一部、又は電子記憶エリアやデータベースなどのセキュアリソース１０４へのアクセスを望む場合、ユーザはユーザ自身の、指紋スキャナを備えるとして図２に図示したポータブルデバイス（図１の要素１１２および図２の要素２１６として図示）を使用してセキュアリソース１０４（ロックされた部屋など）との有線又は無線通信２５０を行う。セキュアリソース１０４により、指紋スキャンが適切であるとの決定がなされれば、ユーザ１１０はポータブルデバイス２１６上でユーザ自身の指２０８をスワイプする。その後、ポータブルデバイス２１６はユーザの指紋認証情報に関してセキュアリソース１０４と通信する。セキュアリソース１０４が指紋を承認すると、セキュアリソース１０４、つまりロックされた部屋の鍵が開く。

【００３６】

さらに、図２に示すように、ポータブルデバイス２１０と２１２とは、その他の利用可能セキュリティメカニズムを備えたポータブルデバイスのその他の例を示す。例えば、ポータブルデバイス２１０は、数字のタッチパッドおよび／又はパスコードを備えており、ユーザ１１０はこれを使って数字のパスワードやユーザＩＤ、あるいは暗証番号（ＰＩＮ）を入力することができる。さらに、ポータブルデバイス２１２は網膜スキャナを備える。この網膜スキャナを使ってユーザは自分の目２１４の位置をあわせることができ、人物の身元確認を行う。セキュアリソース２０４はパソコンベースのリソースなど別のタイプのセキュアリソースを示す。

【００３７】

各種のセキュアリソース（１０４、２０４として図示）は、１以上のポータブルデバイスによりアクセスされうる。各セキュアリソース（１０４、２０４）のリソースセキュリティのレベルは様々に異なるものであってもよい。例えば、数字コードの入力が可能な数字ボタンを有するキーパッドはセキュリティレベルの低いリソースへのアクセスに適している。一方で特定個人の網膜スキャナへアクセスするには高レベルのリソースセキュリティが要求されうる。

【００３８】

図２に示すように、セキュリティリソース１０４は様々なサービスに対して複数のセキュリティレベルを有することも可能であった。ユーザがセキュアリソースへのアクセスを許可され、特定のサービスを要求する場合、セキュリティシステムのセキュリティトーク

ンモジュールは、ユーザにより提供されたセキュリティトークンに従い、要求したサービスへのユーザのアクセスがユーザに許可されているかどうかの決定を行う。

【００３９】

図３は本発明の一実施形態に従うセキュアリソースへアクセスする一連のステップを示す。図３は一連のステップなどのプロセス、又は電子メモリやコンピュータ可読媒体に記憶されるアルゴリズムやプログラムコードを示す。例えば、図３の各ステップはＲＯＭ、ＲＡＭ、ＥＥＲＯＭ、ＣＤ、ＤＶＤなどのコンピュータ可読媒体、又はその他の不揮発性メモリ、又は非一時的コンピュータ可読媒体に記憶されうる。該プロセスはまた、該機能を実行するためにプログラムコードが記憶された電子メモリを含むモジュールであってもよい。該メモリは構造物品である。

【００４０】

図３に示すように、一連のステップをフローチャート３００として表すことができる。該ステップはプロセッサや処理ユニットにより実行されるか、あるいは、実行して識別した機能を実行するようにしてもよい。さらに該ステップは１以上のメモリおよび／又は１以上の電子媒体および／又はコンピュータ可読媒体に記憶されうる。ここでいう媒体には、いわゆるノントランジトリーな非一時的媒体や信号などが含まれる。例えば、図３の各ステップをＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、ＣＤ、ＤＶＤなどのコンピュータ可読媒体や、その他の不揮発性メモリ、非一時的メモリに記憶することができる。電子記憶媒体に記憶されるプログラムコードは構造要素である。コンピュータプログラムコード３００は、フローチャート３００に変わるものとして、本文に記載したいずれのメモリに、例えば、ポータブルデバイス１１２、サーバ１０６又はセキュアリソース１０４に記憶されうる。プロセス３００はステップ３０２より開始する。

【００４１】

ステップ３０４では、ポータブルデバイスを所持するユーザはセキュアリソースに近づき、セキュアリソースへのアクセスを要求する。ステップ３０６では、セキュアリソースはポータブルデバイスがセキュアリソースの範囲内にあるかどうかを識別する。認証機能を有するポータブルデバイスが識別されなければ、「ｎｏ」の矢線３０７からステップ３０８に進む。ユーザと、従ってポータブルデバイスとはセキュアリソースから非常に近いところにデバイスが存在するようにセキュアリソースにさらに近づくことができる（リソースがポータブルデバイスと通信できるようにリソースに十分近い距離）。その後ステップ３０４で再度アクセス要求を行う。矢線３１１に示すように、セキュアリソースの電力要求が識別されうる。

【００４２】

本実施形態は図９を参照して詳細に記載される。同様に、ポータブルデバイスで利用可能な電力が識別される。ポータブルデバイスの電力レベルはセキュアリソース（又はセキュアリソースの一部）の起動に有効である。ポータブルデバイスの電力レベルとは、セキュアリソースを起動する、又はセキュアリソースに信号を送るためのポータブルデバイスの電力のことである。さらに、セキュアリソースの起動電力を決定することができる。この起動電力は休止状態の、又は非アクティブ状態からアクティブ状態へと、セキュアリソース（又はその一部）をアクティブにするのに必要な電力である。ポータブルデバイスの電力レベルが識別されると、ポータブルデバイスの電力レベルがリソース（又はその一部）の起動に十分であるかどうかについての決定がされうる。ポータブルデバイスの電力が適切であれば、ポータブルデバイスは起動信号をセキュアリソースに送信し、セキュアリソースを起動する。

【００４３】

ポータブルデバイスがセキュアリソースと通信しうる距離とは通常、各々のデバイスの送信電力および／又は受信電力の関数となる。ステップ３０６で認証機能を有するポータブルデバイスが識別されれば、「ｙｅｓ」の矢線３０９からステップ３１０へと進む。ステップ３１０では、セキュリティシステムは識別されたポータブルデバイスに対して有線又は無線接続であってよい接続をオープンする。ステップ３１２では、ポータブルデバイ

スは利用可能な認証メカニズムを送信することで応答する。これについては図４に示す。

【００４４】

ステップ３１４では、セキュリティシステムは利用可能な認証メカニズムの１つ又はその組み合わせが使用に適しているかどうか決定する。適しているものがなければ「ｎｏ」の矢線３１５からステップ３１６へと進む。ステップ３１６では、セキュリティシステムは、ユーザがその他のポータブルデバイスを携帯しているかどうかを決定する。認証機能を有するその他のポータブルデバイスをユーザが携帯してないとの決定がなされれば、「ｎｏ」の矢線３１２から最終ステップとなる３３０へと進む。そうでない場合、つまりその他のポータブルデバイスが識別されれば「ｙｅｓ」の矢線３１９からステップ３１０へと戻る。従って、ポータブルデバイスの認証機能の決定は繰り返し行われ、適切な認証機能や機能の識別が繰り返し行われる。

【００４５】

ステップ３１４に戻って、利用可能な認証メカニズムのうちの１つ、又はこの組み合わせが許容されるとの決定がなされれば、「ｙｅｓ」矢線３１７からステップ３１８へと進む。ステップ３１８では、セキュリティシステムは、この適切な認証メカニズムに対応するもののうち、使用が要求されている認証メカニズムをポータブルデバイスに知らせる。ステップ３２０では、要求されるセキュリティメカニズムに関する情報をポータブルデバイスが受信後、該ポータブルデバイスは要求される認証メカニズムを介してユーザおよび／又はポータブルデバイスからセキュリティトークンを取得する。例えば、要求された認証メカニズムが網膜スキャナであれば、ポータブルデバイスはユーザに対して、ユーザの目をこの網膜スキャナの近くにあわせるように要求する。また、要求された認証メカニズムが指紋スキャナであれば、ポータブルデバイスはユーザに対して、ユーザの指をこの指紋スキャナの近くに置くように要求する。次いで、ステップ３２２では、ステップ３２０で取得したセキュリティトークンがセキュアリソースのセキュリティシステムに送信される。

【００４６】

ステップ３２４では、セキュリティシステムは受信したセキュリティトークンが正確であるか、および／又はセキュアリソースへのユーザアクセスを許可するのに十分なものであるかどうかの決定を行う。セキュリティトークンが正確でなければ、又は十分なものでなければ、「ｎｏ」矢線３２５からステップ３２６へと進む。ステップ３２６では、セキュリティシステムは他のセキュリティトークンを提供するようにポータブルデバイスに要求する。ポータブルデバイスから提供されるセキュリティトークンがそれ以上なければ、「ｎｏ」矢線３２９からステップ３１６へと戻る。

【００４７】

ステップ３１６では、セキュリティシステムはユーザがその他のポータブルデバイスを携帯しているかどうかの決定を行う。ステップ３２６において、ポータブルデバイスがユーザから取得したその他のセキュリティトークンを提供すれば「ｙｅｓ」矢線３１１からステップ３２０へと戻る。ステップ３２４に戻って、セキュリティトークンが正確で十分なものであれば、「ｙｅｓ」矢線３２７からステップ３２８へと進む。ステップ３２８では、ユーザはセキュアリソースへのアクセスを許可され、終了ステップ３３０に到達する。

【００４８】

図２について上述したように、セキュリティリソース１０４は様々なサービスに対して様々なセキュリティレベルを有することも可能であった。ユーザがセキュアリソースへのアクセスを許可され、特定のサービスを要求する場合、セキュリティシステムのセキュリティトークンモジュールは、ユーザに提供されたセキュリティトークンに従い、要求したサービスへのアクセスがユーザに許可されているかどうかの決定を行う。

【００４９】

図４に、本発明の一実施形態に従う認証メカニズム４００に関する情報の一例を示す。認証機能を有するポータブルデバイスはセキュリティシステムにその認証システム４００

に関する情報を送信する。これには例えば、物理的キーパッド４０２、バーチャルキーパッド用タッチスクリーン４０４、ジェスチャ入力用タッチスクリーン又はタッチパッド４０６、ジェスチャ入力用モーションセンサ４０８、特定の無線信号（ブルートゥース、ＲＦ、ＩＲなど）の送信が可能な送信デバイス４１０、あるいはセキュアシステムにアクセスするためのキーとして使用される特定のファイル、指紋スキャナ４１２、顔認識用カメラ４１４、網膜スキャナ４１６、音声認識用マイクロフォン４１８などが挙げられる。図４との関連で例示の認証メカニズムを示してきたが、更なる認証メカニズムを使用することも可能であった。

【００５０】

図５に、本発明の一実施形態に従うセキュリティモジュール５００の一例を示す。セキュリティサービスモジュール５００は、プロセッサモジュール５０２、メモリモジュール５０４、およびセキュリティサービスレジストレーションモジュール５０６を含む。セキュリティサービスモジュール５００は、「プラグイン」ユニット、スタンドアローン型ユニット、又は別のモジュールやデバイスに備わっているその他のファシリティであってよい。例えば、セキュリティサービスモジュールは本文中に記載しているように、ポータブルデバイス１１２、サーバ１０６、および／又はセキュアリソース１０４の構成要素であってもよいし、又はこれらによって実行されるものであってもよい。

【００５１】

プロセッサモジュール５０２は関連する通信リンクを介してセキュリティサービスレジストレーションモジュール５０６に接続され、プロセッサモジュール５０２とメモリ５０４とが図５に示すモジュールの処理操作を調整できるようにしている。プロセッサモジュール５０２はＣＰＵ５１０を含む。通常これはプロセッサであり、算術および論理演算を実行する算術論理演算ユニット（ＡＬＵ）を含む。さらに制御ユニット（ＣＵ）を含む。この制御ユニットは必要時にＡＬＵを使用してメモリからの命令を抽出してデコードし、これらを実行するものである。プロセッサモジュール５０２の構成要素を動作可能に接続するために入出力インタフェースを使用してもよい。

【００５２】

メモリモジュール５０４はプログラムを記憶する。これにはウェブブラウザ、アルゴリズムの他、典型的なオペレーションシステムプログラム（不図示）、入力／出力（Ｉ／Ｏ）プログラム（不図示）、ＢＩＯＳプログラム（不図示）およびセキュリティサービスモジュール５００の操作を容易にするその他のプログラムなどが含まれる。ウェブブラウザ（不図示）は、例えばインターネットエクスプローラ（ＴＭ）などのインターネットブラウザプログラムなどである。メモリモジュール５０４は例えばセキュリティサービスモジュール５００により使用されるデータを記憶可能な電子記憶レポジトリなどである。

【００５３】

メモリモジュール５０４は例えばＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ又はその他のメモリ媒体であって、例えば光学ディスク、光学テープ、ＣＤ、フロッピィディスク、ハードディスク、又は取り外し可能カートリッジであり、ビット形式でデジタル情報が記憶されるものである。さらにメモリモジュール５０４は有線又は無線の双方向通信媒体を介して処理モジュール５０２に接続された遠隔メモリであってもよい。ポータブルデバイスからの信号を受信するために、レシーバ／トランスミッタ、又はトランシーバ５０５が使用される。該トランスミッタは、セキュアリソースからポータブルデバイスへ信号を送信するために使用される。

【００５４】

セキュリティサービスレジストレーションモジュール５０６は様々なセキュリティレベルの全てのセキュリティサービスを含む。例えば、サービスグループ５１２はセキュリティレベル１のサービスを含む。これは例えばＥメールや電子カレンダーへのアクセスなどのサービスである。サービスグループ５１４はセキュリティレベル２のサービスを含む。これは例えば財務諸表やアドレス帳へのアクセスなどのサービスである。サービスグループ５１６はセキュリティレベル３のサービスを含む。これは例えば極秘ドキュメントへの

アクセスなどのサービスである。

【００５５】

図６は、本発明の一実施形態に従う複数のセキュリティレベルを有するセキュアリソースのサービスへアクセスする一連のステップを示す。図６はあるプロセスを示す。これは例えば、一連のステップ、又はプログラムコード、又は電子メモリやコンピュータ可読媒体に記憶されるアルゴリズムである。例えば、図６の各ステップは、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、ＣＤ、ＤＶＤなどのコンピュータ可読媒体やその他の揮発性メモリ又は非一時的コンピュータ可読媒体に記憶されうる。また、該プロセスは機能性を実行するためにプログラムコードが記憶された電子メモリを含むモジュールであってもよい。このメモリは構造物品である。コンピュータプログラムコードは、フローチャート６００の代替形式として本文に記載されているように、ポータブルデバイス１１２、サーバ１０６、又はセキュアリソース１０４などいずれのメモリに記憶されてもよい。図６に図示するように、一連のステップは、図５のセキュリティサービスモジュールにより実行されうるフローチャート６００として表されうる。プロセス６００はステップ６０２から開始する。

【００５６】

ステップ６０４では、ユーザは複数のセキュリティレベルを有するコンピュータなどのセキュアリソースへのアクセスが許可される。ステップ６０６では、ユーザはセキュアリソースにおいて、極秘ドキュメントへのアクセスといった特定のサービスへのアクセスを要求する。矢線６０７は、セキュアリソースがポータブルデバイスへ電力を供給する実施形態に対するフローチャートは、図１０との関連で記載しているように、本発明の一実施形態であることを示す。

【００５７】

ステップ６０８では、セキュリティシステムは、ユーザが、セキュアリソースへのアクセスが許可されたときにユーザに提供されるセキュリティトークンが正確であり、要求されたサービスにアクセスするのに十分なものであるかどうかの決定を行う。セキュリティトークンが正確でなければ、又は十分なものでなければ、「ｎｏ」矢線６０９からステップ６１０へと進む。ステップ６１０では、セキュリティシステムは他のセキュリティトークンを提供するようにポータブルデバイスに要求する。ポータブルデバイスから提供されるトークンがなければ、「ｎｏ」矢線６１１からステップ６１２へと進む。ステップ６１２では、該サービスへのアクセス要求が拒絶され、終了ステップ６１６に到達する。ステップ６１０において、ポータブルデバイスがユーザから取得したその他のセキュリティトークンを提供すれば、「ｙｅｓ」矢線６１３からステップ６０８に戻る。ステップ６０８に戻って、セキュリティトークンが正確で十分なものであれば「ｙｅｓ」矢線６１５からステップ６１４へと進む。ステップ６１４では、ユーザは要求したサービスへのアクセスが許可され、終了ステップ６１６に到達する。

【００５８】

図７は本発明の一実施形態に従うポータブルデバイス１１２の一例を示す。ポータブルデバイス１１２は図７においては携帯電話として示されている。キーパッド７０４はセキュアリソースにアクセスするために使用されうる複数のキーを有する。メニュボタン７０２およびオプションボタン７０６は電話をかけるのではなく、アクセスモードでの操作を容易にするために使用されうる。バイオメトリックモジュール７０８はユーザからバイオメトリック情報（例えば、網膜スキャン、指紋）を取得するために使用されうる。表示エリアであるユーザインタフェース又は画面７１８は利用可能なリソース７２０（ａ）．．．（ｎ）（「ｎ」は任意の適切な数字）を表示するために使用されうる。トランスミッタ７３０は、デバイス１１２からの信号を（本文に記載されているように）任意の数のリソースに送信しうる。トランスミッタ７３０の送信強度に応じて、デバイスは該デバイス１１２の信号距離の範囲内にあるいずれのリソースとの通信（例えば、無線通信）を開始しうる。また、デバイス１１２がリソースとの通信を開始できるかどうかを決定するためにセンサ７４０を使用することもできる。

【００５９】

センサ７４０を使用して、デバイス１１２がアクセス可能なリソースからの信号が感知される。該センサを使用して、デバイスがリソースから十分近いところに存在するという表示７４２を出力するようにしてもよい。インジケータ７４２はセンサ７４０を音声および／又は視覚表示するものであってもよく、ＬＥＤ、光、音響信号、着信音又はその他のアラートなどのリソースを検出する。

【００６０】

起動又はバッテリモジュール７５０は、リソースが節電のために電源を切られた状態（パワーダウンモード）にあること、つまり「スリープ」モードにあることを識別するために使用されうる。この起動モジュール７５０は、ポータブルデバイス１１２からリソースへ信号を送信し、該リソースがパワーダウンモードではなくアクティブモードで動作する必要があることを知らせるために、トランスミッタモジュール７３０とともに動作しうる。従って、ポータブルデバイス１１２は長期間にわたって休止状態であったリソースをバッテリ又は起動モジュール７５０を利用して起動することができる。

【００６１】

ポータブルデバイス１１２は任意の数のリソースに予め登録されていてもよい。従って、該ポータブルデバイス１１２が所定の距離の範囲内に存在する場合はいつでも、該ポータブルデバイス１１２は特定のリソースとの通信を開始することになる。１つ以上のデバイスを、１つ以上のリソースのオープン、アクセス、又は検知について認証されたものとして関連付けるために、コードやデバイス識別子（ＰＩＮやデバイス番号）を使うこともできる。

【００６２】

ポータブルデバイス１１２はさらに、本文に記載されているように、アクセス関数を実行するために有用なアルゴリズムおよびプログラムを記憶するために使用される１以上のメモリを含みうる。

【００６３】

従って、該ポータブルデバイスがセキュアリソースに電力を供給しうるのもまた本発明の実施形態である。例えば、アクセスがほとんどないセキュリティシステムでは、電子メカニズムを稼動させておくために電子ドアへの電力を供給し続ける必要はなく、従って、電子ドアを起動させるために該ポータブルデバイスが電力を供給しうる。

【００６４】

図８は、本発明の一実施形態に従うセキュアリソース１０４の一例を示す。リソース１０４はトランスミッタ８０２、認証モジュール８６０、近接モジュール８７０、アクセスモジュール８０６、電源レセプタクルモジュール８４２、メモリ８２４、およびプロセッサ８２６を含む。これらの要素又はモジュールはバス８９０に動作可能に接続されうる。認証モジュール８６０、近接モジュール８７０などの各モジュールは例えば非一時的電子記憶レジスタであってもよい。これは該レジスタに記憶されたプログラムコードやアルゴリズムの関数を実行するためにプロセッサ８２６とともに動作するものである。

【００６５】

トランスミッタ８０２によってリソース１０４からの信号がポータブルデバイスに送信される。近接モジュール８７０によってポータブルデバイスがリソースの送信信号距離の範囲内にあることが検出される。認証ユニット８６０によってポータブルデバイスからの送信信号を受信し、ポータブルデバイスにより送信されたトークンが一定のレベルのアクセスを受け入れることができるかどうかが確認される。受信するトークンの種類に応じて、許可されるアクセスのレベルは変わる。

【００６６】

認証モジュール８６０により許可されたリソース１０４のエリアにアクセスするためにアクセスモジュール８０６が使用される。アクセスモジュール８０６はロックやラッチ、又は電子アクセス機能を有するものであってもよい。このアクセスモジュール８０６は、承認が受理されたことを受信するとオープンする（つまり、アクセスできるようになる）。必要な承認が受信されない場合、アクセスモジュール８０６はオープンしない（つまり

、アクセスが拒否される）。アクセスモジュール８０６は選択的アクセスを許容することができる。例えば、アクセスモジュール８０６は、データベースの特定部分へのユーザのアクセスを認めるか、該部分をユーザに表示する一方で、より高度な認証を必要とするデータベースのその他の部分をユーザに表示しないようにすることができる。

【００６７】

電源レセプタクルモジュール８４２は、リソース１０４の動作モードを変更すべく、ポータブルデバイスから信号を受信するために使用される。例えば、ポータブルデバイスは、リソースが省エネや節電の動作状態から起動するように起動信号を送信しうる。パワーモジュール８４２はまた、セキュアリソースを起動するためにポータブルデバイスから受信を要求されている最小電力を示す最小電力閾値を記憶するように使用されてもよい。

【００６８】

さらに、パワーモジュール８４２は、セキュアリソースが電力信号をポータブルデバイスに送信する場合などにポータブルデバイスに対する最小電力閾値を記憶しうる。さらに、パワーモジュール８４２はポータブルデバイスを起動すべく、電力起動信号又は電力送信信号を受信しうる。この起動信号は、例えば、ポータブルデバイスを「ウェイクアップ」モードで（「スリープ」モードに対するものとして）動作させるようにするものであってもよいし、ポータブルデバイスの場所を示す信号をポータブルデバイスに送信させるようにするものであってもよい。

【００６９】

従って、ポータブルデバイスとセキュアリソースとは相互間で電力を送信することができる。また、ポータブルデバイスを使用して、セキュアリソースを起動する（ウェイクアップ状態にするかアクセス許可する）ことができる。さらに、リソースとポータブルデバイス間に送信される電力は、リソースおよび／又はポータブルデバイスを動作させるために使用されうる。例えば、該リソースは磁気コイル、又は動作電力をリソースに供給するために使用されうるその他の電力装置を有しうる。電力装置はポータブルデバイスからの信号により起動されうる。さらに、ポータブルデバイスはリソースにより充電、再充電、又は電力供給されうる。具体的には、ポータブルデバイスは、リソースからの動作電力を受信するためにリソースに接続されうる。

【００７０】

メモリモジュール８２４および処理モジュール８２６はそれぞれリソース１０４のデータを記憶し、命令を実行するために使用される。

【００７１】

図９は、ポータブルデバイスがセキュアリソースに電力供給する本発明の一実施形態に対するフローチャート９００を示す。上述したように、図３との関連で、ポータブルデバイスが特定のセキュアリソースの所定の距離の範囲内にある場合に、ステップ９０２に示すようにセキュアリソースに起動信号を送信することは本発明の実施形態である。ステップ９０４では、セキュアリソースへの電力供給が必要であるかどうかの決定がなされる。必要でなければ「ｎｏ」矢線９０７からステップ９１０へ進む。ステップ９１０ではセキュアリソースが起動されうる。ステップ９０４で電力が必要であるとの決定がなされれば、「ｙｅｓ」矢線９０５からステップ９０６に進む。

【００７２】

ステップ９０６では、セキュアリソースに組み込まれている場合もある発電機の磁気コイルなどの電源装置が起動しうる。次いで、ステップ９０８に示すように、発電機はセキュアリソースに、セキュアリソースの電力要求を満たす十分な電力を供給する。その後、ステップ９１０に示すように、セキュアリソースが起動しうる。この時点で、本文において記載しているように、セキュアリソースは、ポータブルデバイスがセキュアリソースの１以上のエリアへアクセスできるかどうかを決定するための電力を有する。終了ステップ９１２は本プロセスの終了を示す。換言すれば、セキュアリソースは、オペレーションモード（「スリープモード」に対するものとしての「ウェイクアップ」モード）を起動するためにポータブルデバイスを電源として使用し、発電した電力を動作のために使用するこ

とができる。又は、セキュアリソースは、セキュアリソースへのアクセスを許可するためにポータブルデバイスの信号を使用することができる。従って、ポータブルデバイスとセキュアリソースとは相互に電力を送信することができる。

【００７３】

図１０は、セキュアリソースが、ポータブルデバイスを認証するための電力を供給するという本発明の実施形態のフローチャート１０００を示す。上述したように、図６との関連で、セキュアリソースがポータブルデバイスを認証するための電力要求を識別することができるのはステップ１００２に示すように本発明の一実施形態である。ステップ１００４では、セキュアリソースはポータブルデバイスにおいて現在利用可能な電力量を識別する。ステップ１００６では、ポータブルデバイスが電力要求を満たすのに適切な電力を有するかどうかの決定がなされる。適切な電力を有さない場合、「ｎｏ」矢線１００７からステップ１００８へ進む。ステップ１００８では、セキュアリソースがポータブルデバイスの電力要求を満たすための適切な電力を有するかどうかの決定がなされる。適切な電力を有さない場合、「ｎｏ」矢線１０１３からステップ１０１８に進む。ステップ１０１８では、ポータブルデバイスで利用可能な電力量が示される。

【００７４】

ステップ１００８では、セキュアリソースがポータブルデバイスに適切な電力を供給することができれば、「ｙｅｓ」矢線１０１１からステップ１０１０に進む。ステップ１０１０では、ユーザがポータブルデバイスをセキュアリソースに差し込む動作により、セキュアリソースは認証のための電力をポータブルデバイスに供給する。この電力送信は無線送信によって行うこともできる。矢線１０２３からステップ１００４に戻る。ステップ１００４では、ポータブルデバイスの電力量が示される。ステップ１００６では、ポータブルデバイスが電力要求を満たすのに十分な電力を有するとの決定がなされれば、「ｙｅｓ」矢線１００９からステップ１０１２へと進む。

【００７５】

ステップ１０１２では、ユーザによりポータブルデバイスが更なる電力を必要としているかどうかの判断がなされる。更なる電力を必要としていなければ、「ｎｏ」矢線１０１７からステップ１０１８へと進む。ステップ１０１８では、ポータブルデバイスで利用可能な電力量が示される。ステップ１０１２においてポータブルデバイスが更なる電力を必要としているとの決定がなされれば「ｙｅｓ」矢線１０１５からステップ１０１４へと進む。ステップ１０１４では、ユーザがポータブルデバイスをセキュアリソースに差し込む動作により、セキュアリソースはポータブルデバイスに電力供給する。この電力送信は無線通信により行われてもよい。ステップ１０１６では、電力供給プロセスが終わったか、又は終了したかどうかの決定がユーザによりなされる。まだであれば、「ｎｏ」矢線１０１９からステップ１０１４に戻る。ステップ１０１４では、電力がポータブルデバイスに供給される。電力供給プロセスが終わった、又は終了したとの決定がユーザによりなされれば、「ｙｅｓ」矢線１０２１からステップ１０１８へと進む。ステップ１０１８では、ポータブルデバイスで利用可能な電力量が示される。終了ステップ１０２０は本プロセスが終了することを示す。

【００７６】

図１１に、本発明の一実施形態に従うポータブルデバイス１１２の処理およびメモリモジュールの一例を示す。ポータブルデバイス１１２はＣＰＵモジュール１１０３とメモリモジュール１１０５とを含む。

【００７７】

ＣＰＵ１１０３とメモリ１１０５とはＣＰＵ１１０３がメモリ１１０５に記憶されたデータの処理を実行できるように動作可能に接続される。通常、ＣＰＵモジュール１１０３は、ＡＬＵを含む市販のコンピュータプロセッサや、データ処理を実行するためのその他の電子的構成要素や回路などである。

【００７８】

メモリモジュール１１０５はパワーモジュール９００、スキャナモジュール（指紋）１

１１２、近接センサモジュール１１０９、モーションセンサモジュール１１０８、カメラモジュール１１１４、スキャナモジュール（網膜）１１１６、音声認識モジュール１１１８、および認証モジュール１１５０を含む。さらに、図１１にはＩ／Ｏモジュール１１１５とＧＵＩ１１０４を示す。メモリ１１１５に記憶されるとして記載されている各モジュールは通常は非一時的コンピュータ可読媒体に記憶される命令を実行するプログラムコードであり、また、図４に示した１以上のセンサモジュールなどのハードウェア構成要素とともに動作するソフトウェア構成要素である。

【００７９】

パワーモジュール９００は、各処理、各ステップ、および各プログラムコードを記憶するために使用される記憶モジュールであり、例えば、図９との関連で記載しているように、ポータブルデバイス１１２がセキュアリソースに電力供給できるかどうかを決定するために、ＣＰＵ１１０３などのプロセッサにより実行されうる非一時的コンピュータ可読媒体に記憶される命令を記憶するために使用される記憶モジュールである。パワーモジュール９００を使用してセキュアリソースの起動信号が送信され、電力信号が送られる。パワーモジュール９００は、セキュアリソースを起動するために必要とされる最小電力である電力閾値を記憶しうる。セキュアリソースを起動させる余計な電力を無駄にしないように最小マグニチュードが使用される。

【００８０】

スキャナモジュール１１１２は、非一時的コンピュータ可読媒体に記憶された命令などのコンピュータコードであって、ハードウェア構成要素とともに使用される場合に、要素２１６として図２に示したような指紋入力デバイスによって取得した指紋データなどのバイオメトリックを識別できるようにするコンピュータコードを提供するモジュールである。

【００８１】

近接センサモジュール１１０９は例えば、セキュアリソースがポータブルデバイスを認識できる距離を決定するセンサを制御するプログラムコードである。この距離はセキュアリソースやポータブルデバイスの種類、使用できるポータブルデバイスの数、ポータブルデバイスやセキュアリソースのセキュリティレベルに応じたものである。例えば、セキュアリソースが要求するセキュリティの閾値が低ければ、ポータブルデバイスがセキュアリソースを識別する可能性が高い。セキュアリソースの閾値が高ければ、セキュアリソースはポータブルデバイスが検出できる信号を送信しない場合がある。従って、ポータブルデバイスは、ポータブルデバイスが選択したセキュアリソースの距離内にあることを識別できない。

【００８２】

この近接センサモジュール１１０９は、通常はＩ／Ｏモジュール１１１５を介して信号の送受信が可能なハードウェアとソフトウェアの構成要素を組み合わせたものである。近接センサモジュールのプログラムコードモジュールを図１１に示し、このハードウェアを図７に要素７４０として示す。近接センサモジュール（ハードウェアおよびソフトウェア）は、ポータブルデバイス１１２がセキュアリソースの選択した部分又はエリアにアクセスできる距離を決定するように構成されている。

【００８３】

モーションセンサモジュール１１０８は、ポータブルデバイス１１２に対するユーザの動作を検出するために使用される。モーションセンサモジュール１１０８は、例えば、図４に示すセンサ４０６からの入力を処理する非一時的コンピュータ可読媒体に記憶されたプログラムコードである。モーションセンサモジュール１１０８のプログラムコードは、ユーザが行っているジェスチャの種類や、ユーザが予め選択されたポータブルデバイスの距離内にいるかどうかを決定する。自動ドアなどのセキュアリソース、又はポータブルデバイスに対してユーザが存在するだけで起動しうるようなその他のセキュアリソースをオープンするには、又はこれらにアクセスには動作が感知されれば十分である。

【００８４】

カメラモジュール１１１４はメモリロケーション記録命令(MLSI:memory location storing instruction)として示されており、カメラ又は図４に示すカメラ４１４などのその他の画像取得デバイスから取得した画像を識別する。該カメラモジュール１１１４およびハードウェア構成要素４１４は、顔の特徴又はその他の画像を認識し、セキュアリソースへのアクセスを許容するために使用されうる。

【００８５】

スキャナモジュール１１１６は、本文で記載しているように、セキュアリソースへのアクセスを決定するために網膜などのバイオメトリックデータを検出するためのスキャナとともに動作するプログラムコードを記憶する記憶場所として示される。

【００８６】

音声認識モジュール１１１８は、図４に示すマイクロフォン４１８により取得した音や声などの音声データを操作し認識するためのプログラムコードを記憶する記憶場所として示される。この音声認識モジュール１１１８のソフトウェアは、受信した音声信号が記憶され承認された音声信号と一致するかどうか決定し、一致を認める、又は否定する信号又はその他のアウトプットを出力するように構成されている。

【００８７】

認証モジュール１１５０は、ＣＰＵ１１０３により実行されうる命令を記憶するために使用されうるメモリ１１０５に記憶されたプログラムコードである。このプログラムコードは、セキュアリソースがポータブルデバイスと通信可能かどうかを決定し、さらに、セキュアリソースに対して、ポータブルデバイスへのアクセスを認める権原を与え、従って、ポータブルデバイスを所持するユーザへのアクセスを認める権限を与えるものである。@認証モジュール１１５０はＩ／Ｏモジュール１１１５とともに動作するものであり、例えばトランスミッタやレシーバ、又はトランシーバなどである。これらはセキュアリソースやサーバ、又はポータブルデバイスを使用してセキュアリソースの認識オペレーション、および／又はセキュアリソースへのアクセスオペレーションを容易にするためのその他の場所へ受信信号や認証データを送信するか、これらの場所から受信信号や認証データを受信するように動作する。

【００８８】

ＧＵＩ１１０４は、ユーザに対して、ユーザ入力を介してポータブルデバイス１１２を操作し制御するためのユーザインタフェースを提供する。これらは、キーボード、タッチ画面、マウス、その他の入力デバイス（不図示）が含まれ、さらに、画像データを表示するための画面、ディスプレイ、モニタ（不図示）、音声データを出力するための音声出力デバイス（不図示）であり得る。

【００８９】

本発明の各実施形態の各種実施形態を上述の記載および図面との関連で以下に記載する。例えば、ある場合では、ポータブルデバイスそれ自体がセキュリティトークンである。オフィスビルで広く利用されているキーレスエントリシステムでは、ドア付近のセンサの前でバッジを振るだけで入ることができ、その他の認証は不要である。その他の場合では、特定のポータブルデバイスが必要である。例えば、セキュアリソースにアクセスするために網膜スキャンが要求される場合、ユーザが網膜スキャナを備えたユーザ自身のポータブルデバイスを使用するかどうか、あるいは、ユーザが別のユーザからポータブルデバイスを借りるかどうかは重要ではない。それは、ポータブルデバイスではなく、セキュリティトークンがユーザの網膜の画像であるからである。

【００９０】

上述のことから、本発明は記憶媒体に提供されうるコンピュータソフトウェアとして、又はローカルエリアネットワークやインターネットなどの広域ネットワークなどの伝達媒体を介して実行されうることが分かるであろう。さらに、添付の図面に示す構成システムの構成要素および方法ステップの一部をソフトウェアで実行することができるために、システムの構成要素（あるいは処理ステップ）間の実際の接続は本発明がプログラムされる方法に応じて異なる場合がある。本文において与えられた教示を前提とすると、当業者で

あればこれらの実施や類似の実施、又は本発明の構成を検討することができるであろう。

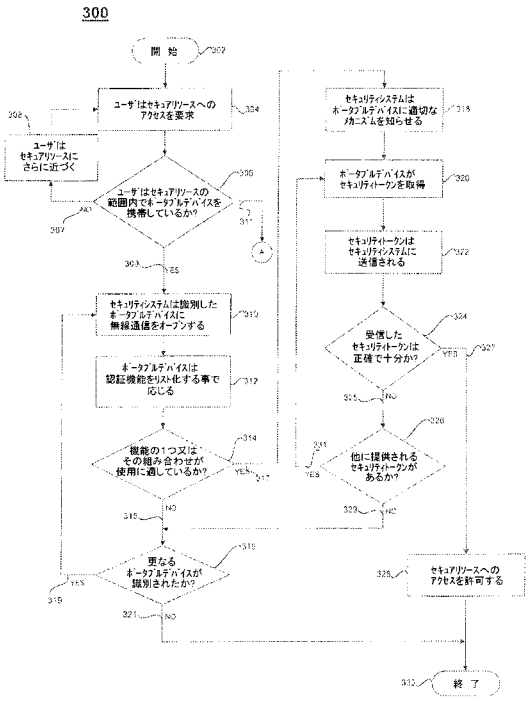
【００９１】

本発明をハードウェア、ソフトウェア、ファームウェア、特定用途のプロセス、又はこの組み合わせなどの各種形態で実行できることを理解されたい。一実施形態では、本発明は非一時的コンピュータ可読媒体などのコンピュータ可読記憶装置に具体化されるアプリケーションプログラムとしてソフトウェアで実行することができる。このアプリケーションプログラムは、プロセッサ、ＣＰＵあるいはコンパイラなど、任意の適切な構造からなるコンピュータにアップロードされ、さらにこれらにより実行されうる。

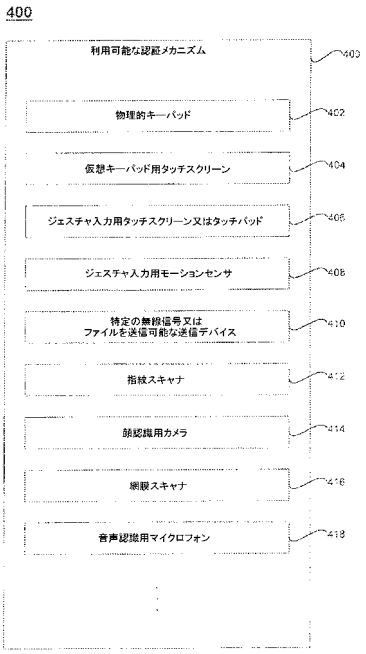
【００９２】

本発明は様々に、しかし、本文に記載された教示による利益を受ける当業者にとっては明らかな等価の方法で変形および実行することができるために、上記に開示した特定の実施形態の各々は単なる例示に過ぎない。さらに、以下の請求の範囲において記載した以外に、本明細書に示した構造や設計の詳細に限定することを意図していない。従って、これまでに開示した特定の実施形態の各々を変形又は修正できることは明らかであり、そのような変形のすべては本発明の範囲および精神の範囲内であると考えられる。本発明の例示的実施形態を添付の図面とともに本明細書において詳述してきたが、本発明はこれらの正確な実施形態に限定されず、添付の請求の範囲において定義されているように、本発明の範囲および精神から逸脱することなく、当業者により各種の変更および修正が行われてもよいことを理解されたい。

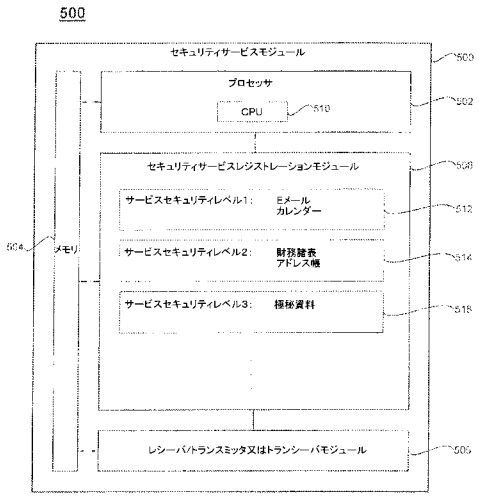
【図３】



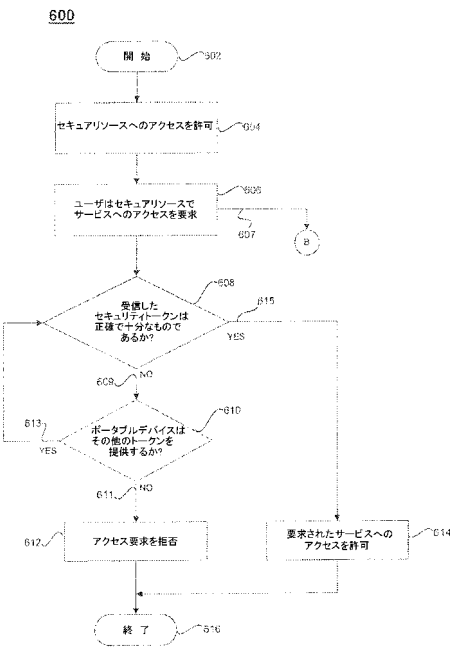
【図４】



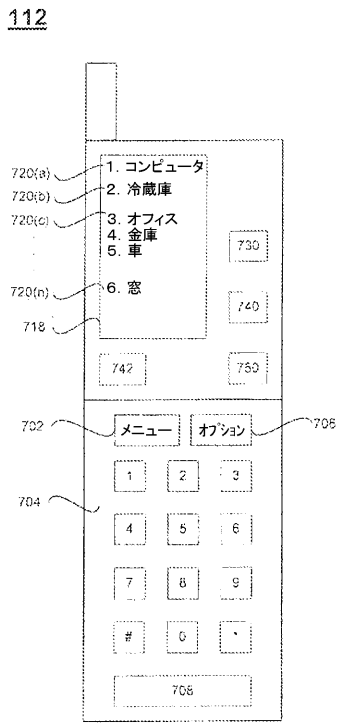
【図５】


500
セキュリティサービスモジュール
503
プロセッサ
CPU
510
502
セキュリティサービスレジストレーションモジュール
508
サービスセキュリティレベル1:
Eメール
カレンダー
512
サービスセキュリティレベル2:
財務諸表
アドレス帳
514
サービスセキュリティレベル3:
極秘資料
518
504
メモリ
レシーバ/トランスミッタ又はトランシーバモジュール
505

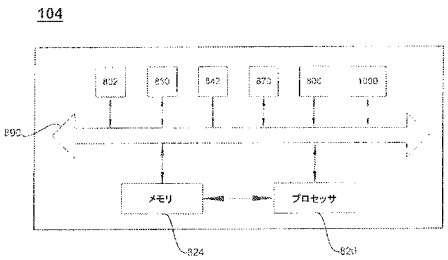
【図６】


600
開 始
602
セキュリアソースへのアクセスを許可
604
ユーザはセキュアリソースで
サービスへのアクセスを要求
606
607
B
受信した
セキュリティトークンは
正確で十分なもので
あるか?
608
615
YES
609
NO
ポータブルデバイスは
その他のトークンを
提供するか?
610
613
YES
611
NO
アクセス要求を拒否
612
要求されたサービスへの
アクセスを許可
614
終 了
616

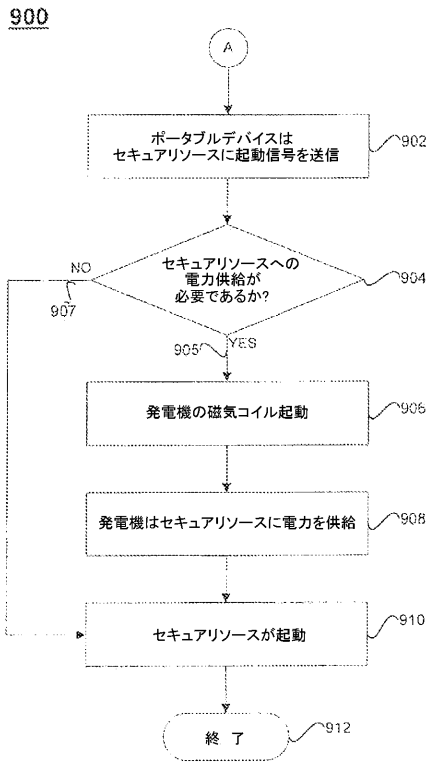
【図７】


112
720(a)
720(b)
720(c)
720(n)
718
1. コンピュータ
2. 冷蔵庫
3. オフィス
4. 金庫
5. 車
6. 窓
730
740
742
750
702
メニュー
オプション
706
704
1
2
3
4
5
6
7
8
9
#
0
*
708

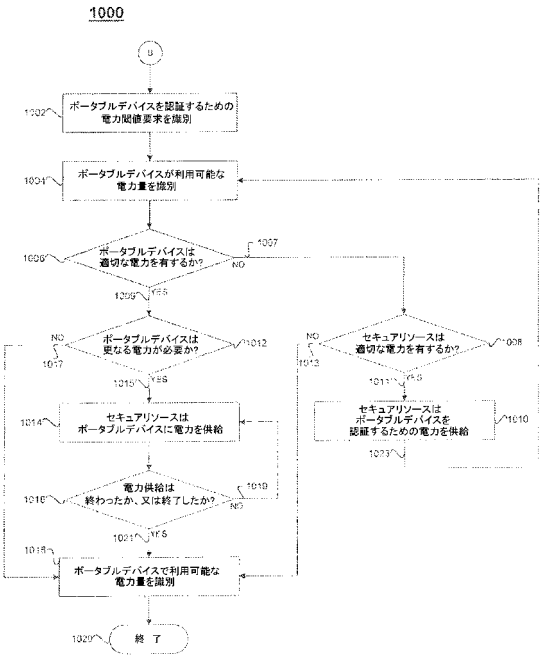
【図８】


104
822
850
842
870
890
1000
890
メモリ
プロセッサ
824
820

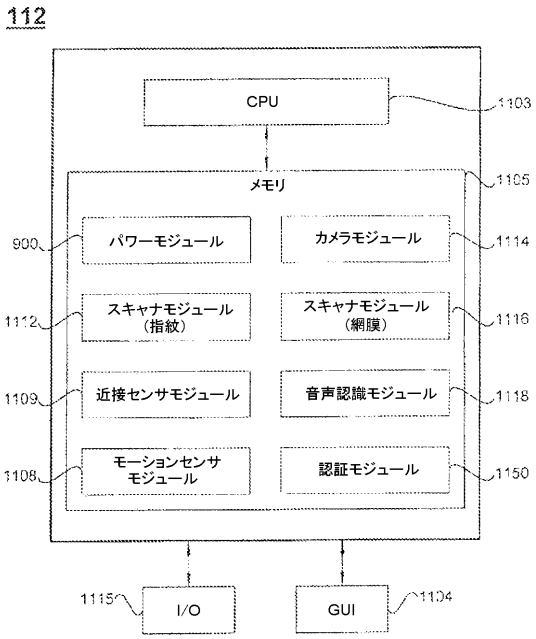
【図９】


900
A
ポータブルデバイスは
セキュアリソースに起動信号を送信
902
セキュアリソースへの
電力供給が
必要であるか?
904
NO
907
YES
905
発電機の磁気コイル起動
906
発電機はセキュアリソースに電力を供給
908
セキュアリソースが起動
910
終 了
912

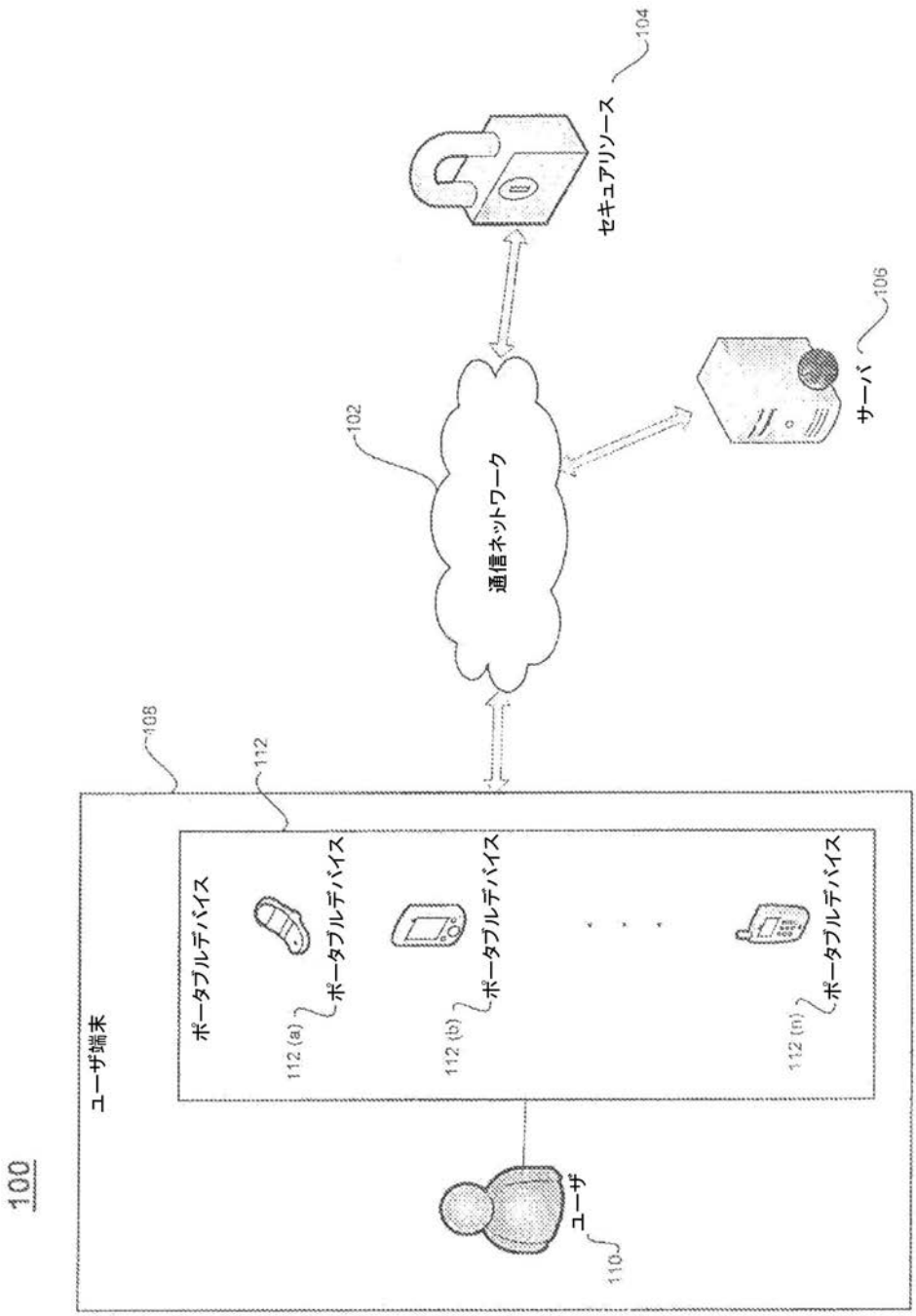
【図１０】


1000
B
ポータブルデバイスを認証するための
電力閾値要求を識別
1002
ポータブルデバイスが利用可能な
電力量を識別
1004
ポータブルデバイスは
適切な電力を有するか?
1006
NO
1007
YES
1009
ポータブルデバイスは
更なる電力が必要か?
1012
NO
1017
YES
1015
セキュアリソースは
ポータブルデバイスに電力を供給
1014
電力供給は
終わったか、又は終了したか?
1016
NO
1019
YES
1021
ポータブルデバイスで利用可能な
電力量を識別
1018
終 了
1020
セキュアリソースは
適切な電力を有するか?
008
NO
1013
YES
1011
セキュアリソースは
ポータブルデバイスを
認証するための電力を供給
1010
1023

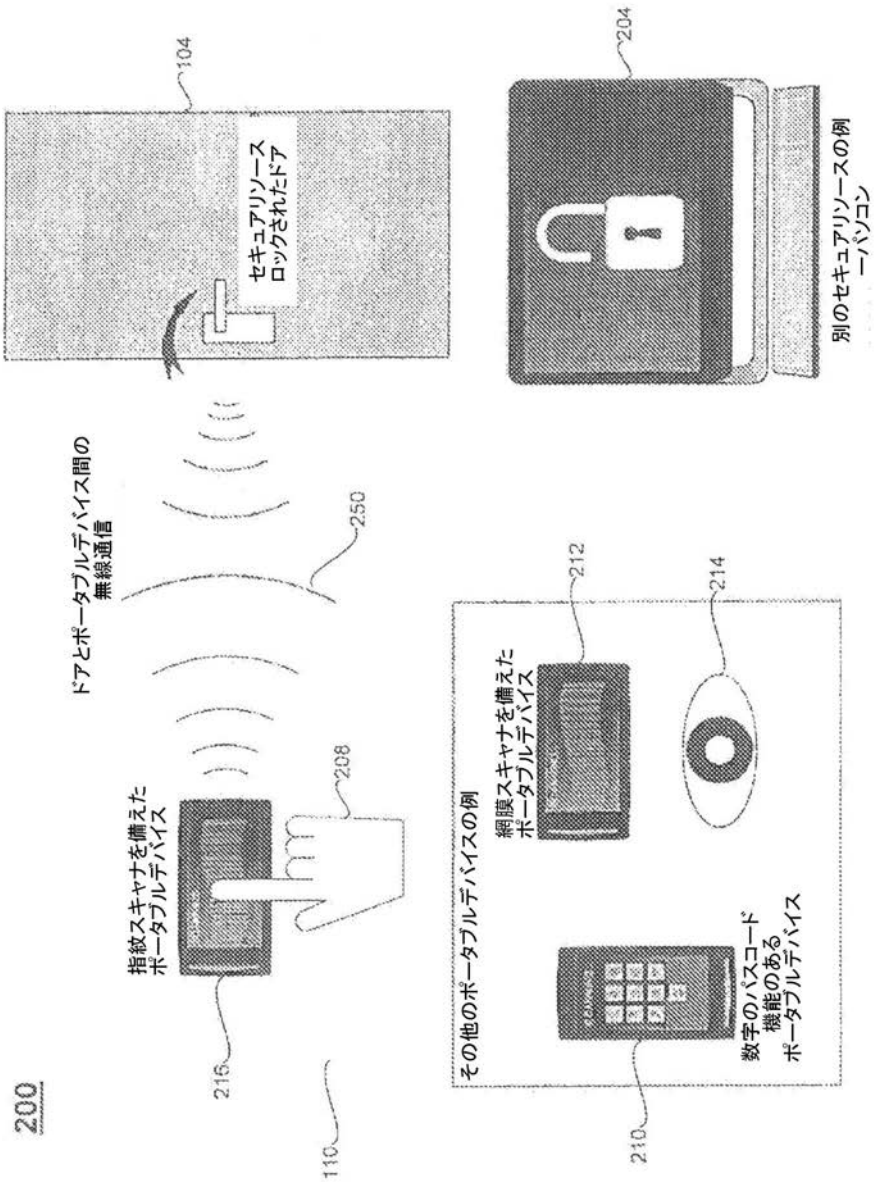
【図１１】


112
CPU
1103
メモリ
1105
900
パワーモジュール
カメラモジュール
1114
1112
スキャナモジュール
(指紋)
スキャナモジュール
(網膜)
1116
1109
近接センサモジュール
音声認識モジュール
1118
1108
モーションセンサ
モジュール
認証モジュール
1150
1115
I/O
GUI
1104

【図１】


100
ユーザ端末
108
ポータブルデバイス
112
112 (a)
ポータブルデバイス
112 (b)
ポータブルデバイス
112 (n)
ポータブルデバイス
ユーザ
110
通信ネットワーク
102
セキュアリソース
104
サーバ
106

【図２】


200
104
セキュアリソース
ロックされたドア
204
別のセキュアリソースの例
ーパソコン
ドアとポータブルデバイス間の
無線通信
250
指紋スキャナを備えた
ポータブルデバイス
208
216
110
その他のポータブルデバイスの例
網膜スキャナを備えた
ポータブルデバイス
212
214
数字のパスコード
機能のある
ポータブルデバイス
210

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/53121

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/00 (2012.01)
USPC - 713/185
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)
USPC: 713/185

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/150, 155-159, 168-173, 182-185; 705/1.1, 64, 65, 67 (keyword limited - see search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (PGPB, USPT, USOC, EPAB, JPAB); GOOGLE; Google Scholar
Terms: access, secure, resource, identity, mobile, device, wireless, signal, authentication, token, transmit, passcode, biometric, retina.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/0320118 A1 (Muller et al.) 24 December 2009 (24.12.2009), entire document, especially abstract, para [0001], [0003], [0004], [0007], [0013], [0014], [0017], [0037], [0044], [0066], [0067], [0101], [0105], [0123].	1-18
Y	US 2009/0198618 A1 (Chan et al.) 06 August 2009 (06.08.2009), entire document, especially abstract, para [0014], [0016], [0021], [0111], [0204].	1-18
A	US 2010/0194571 A1 (Ortiz et al.) 05 August 2010 (05.08.2010), entire document, especially abstract, para [0002], [0003], [0007], [0015], [0026], [0052], [0067].	1-18

☐ 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
29 January 2012 (29.01.2012)	09 FEB 2012
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

(51)Int.Cl.	FI	テーマコード（参考）
	G06K 17/00 T	

(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,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA

(72)発明者 ジェフリー ロジャー スタッフォード
アメリカ合衆国、カリフォルニア州 ９９４０４－２１７５、フォスター シティー、イースト ヒルスデイル ブルバード ９１９、ソニー コンピュータ エンタテインメント アメリカ リミテッド ライアビリテイ カンパニー内
(72)発明者 ヤンペン ズ
アメリカ合衆国、カリフォルニア州 ９９４０４－２１７５、フォスター シティー、イースト ヒルスデイル ブルバード ９１９、ソニー コンピュータ エンタテインメント アメリカ リミテッド ライアビリテイ カンパニー内

Ｆターム(参考) 5B035 AA13 AA14 BB09 CA23
5B058 CA15 KA31 KA33 KA38