(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-162489
(P2017-162489A)
(43)公開日　平成29年9月14日(2017.9.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/32	(2013.01)	G06F	21/32		5B043
G06T 1/00	(2006.01)	G06T	1/00	400H	5B047
G06T 7/00	(2017.01)	G06T	7/00	510B	

審査請求 有　請求項の数 31　ＯＬ　外国語出願　（全 34 頁）

(21)出願番号　特願2017-85582(P2017-85582)
(22)出願日　平成29年4月24日(2017.4.24)
(62)分割の表示　特願2017-13383(P2017-13383)の分割
原出願日　平成20年9月9日(2008.9.9)
(31)優先権主張番号　60/995,200
(32)優先日　平成19年9月24日(2007.9.24)
(33)優先権主張国　米国(US)

(71)出願人　503260918
アップル　インコーポレイテッド
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　インフィニット　ループ　１
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】電子デバイスに組み込まれた認証システム

(57)【要約】　（修正有）
【課題】電子デバイスのリソースへのアクセスを制限するための認証システムを有する電子デバイスを提供する。
【解決手段】電子デバイス１００は、認証システム１１２を備える。認証システム１１２は、ユーザの生体情報を検出する１又は複数のセンサを備える。センサは、生体情報を提供するためのステップを実行するようユーザに要求することなく、ユーザがデバイスを操作した時に、センサが適切な生体情報を検出できるように、デバイスに配置される。認証システムは、ユーザを認証するために視覚的または時間的な入力パターンを検出する。認証に応答して、ユーザは、制限されたファイル、アプリケーション又は連絡先や保存したゲームプロファイルなどのアプリケーション設定にアクセスできる。
【選択図】図１

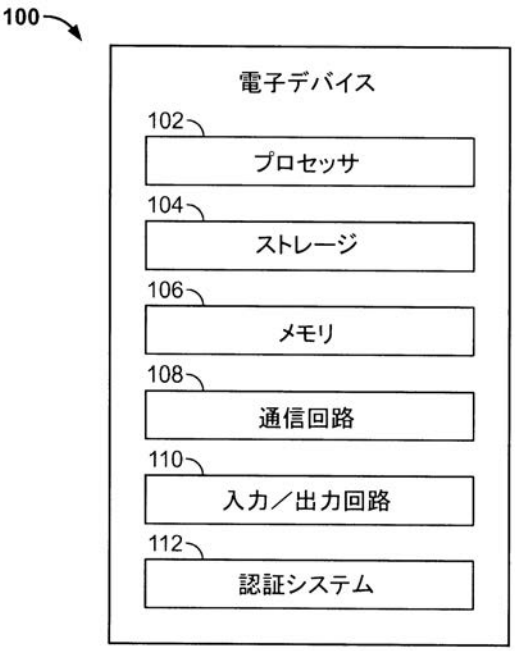

FIG. 1

【特許請求の範囲】
【請求項１】
電子デバイスのユーザをシームレスに認証するための方法であって、
前記電子デバイスの入力メカニズムを用いて、ユーザからの入力を受信する工程と、
前記入力メカニズムに隣接したセンサを用いて、前記入力を受信する時に前記ユーザの識別情報を検出する工程と、
前記検出した情報に基づいて前記ユーザを認証する工程と、を備える、方法。
【請求項２】
請求項１に記載の方法はさらに、
前記認証に応答して、制限された電子デバイスリソースへのアクセスを前記ユーザに提供する工程を備える、方法。
【請求項３】
請求項２に記載の方法であって、前記制限された電子デバイスリソースは、
アプリケーション、アプリケーションに関連づけられたデータ、および、データファイルの内の少なくとも１つを含む、方法。
【請求項４】
請求項１に記載の方法はさらに、
前記認証工程に応答して、個人用のディスプレイ画面を前記ユーザに提供する工程を備える、方法。
【請求項５】
請求項１に記載の方法であって、前記受信工程は、さらに、電子デバイスをロック解除するための入力を受信する工程を含む、方法。
【請求項６】
請求項５に記載の方法であって、前記入力は、ディスプレイを横断するオプションのドラッグを含む、方法。
【請求項７】
請求項１に記載の方法であって、前記識別情報は、
指紋、掌紋、手紋、指関節紋、血管パターン、網膜パターン、虹彩パターン、外耳道パターン、および、ＤＮＡ配列の内の少なくとも１つを含む、方法。
【請求項８】
請求項１に記載の方法であって、前記センサは、前記入力メカニズムに内蔵されている、方法。
【請求項９】
請求項８に記載の方法であって、前記センサは、タッチスクリーンの一部に内蔵されている、方法。
【請求項１０】
請求項８に記載の方法であって、前記センサは、キーボードと、ボタンと、マウスと、タッチパッドと、前記入力メカニズムに隣接した電子デバイス筐体と、の内の少なくとも１つに内蔵されている、方法。
【請求項１１】
電子デバイスのユーザを認証するための方法であって、
前記デバイスの検知素子に対して位置合わせするよう前記ユーザに案内することなく、前記ユーザが前記検知素子に対して位置合わせされていることを決定する工程と、
前記決定工程に応答して、前記検知素子を用いて前記ユーザの生体属性を検出する工程と、
前記検出工程に応答して、前記ユーザを認証する工程と、を備える、方法。
【請求項１２】
請求項１１に記載の方法であって、前記決定工程は、さらに、前記ユーザが前記センサの視野内にいることを決定する工程を備える、方法。
【請求項１３】

請求項１１に記載の方法であって、前記検出工程は、さらに、前記ユーザの顔の特徴および前記ユーザの眼の特徴の内の少なくとも１つを検出する工程を備える、方法。
【請求項１４】
請求項１１に記載の方法はさらに、
前記検知素子の指示を前記ユーザに提供しない工程を備える、方法。
【請求項１５】
ユーザをシームレスに認証するための電子デバイスであって、
ユーザから入力を受信する入力メカニズムと、
前記入力が受信される時に、前記ユーザの識別特徴を検出する検知素子と、
前記検出された識別特徴に基づいて、前記ユーザを認証するプロセッサと、を備える、電子デバイス。
【請求項１６】
請求項１５に記載の電子デバイスであって、前記検知素子は、前記入力メカニズムに内蔵されている、電子デバイス。
【請求項１７】
請求項１５に記載の電子デバイスであって、前記検知素子は、前記検知素子の視野が、前記入力メカニズムに入力を提供するユーザの少なくとも１つの識別特徴を捉えるよう配置される、電子デバイス。
【請求項１８】
請求項１５に記載の電子デバイスであって、前記入力メカニズムは、キーボードと、ボタンと、マウスと、タッチパッドと、タッチスクリーンと、スクロールホイールと、の内の少なくとも１つを備える、電子デバイス。
【請求項１９】
請求項１５に記載の電子デバイスであって、前記検知素子は、前記ユーザの皮膚の特徴およびユーザの皮下の特徴の少なくとも一方を検出する、電子デバイス。
【請求項２０】
ユーザ入力を要求することなくユーザを認証する電子デバイスであって、
前記電子デバイスから利用可能な少なくとも１つのアプリケーションのための画面を提供するディスプレイと、
前記ユーザが前記ディスプレイに向かい合った時に、前記ユーザに特有の属性を検出するセンサと、
プロセスと、を備え、前記プロセスは、
前記検出された特有の属性を受信し、
前記検出された特有の属性を、許可ユーザに関連づけられた属性のライブラリと比較し、
前記検出された属性が前記ライブラリの属性と適合するとの決定に応答して、制限されたリソースへのアクセスを提供する、電子デバイス。
【請求項２１】
請求項２０に記載の電子デバイスであって、前記センサは、さらに、ユーザの皮膚の属性を検出する、電子デバイス。
【請求項２２】
請求項２１に記載の電子デバイスであって、前記センサは、前記ディスプレイの表面と反対側の前記デバイスの表面上に配置される、電子デバイス。
【請求項２３】
請求項２０に記載の電子デバイスであって、前記センサは、さらに、前記ユーザの顔および前記ユーザの眼の少なくとも一方の属性を検出する、電子デバイス。
【請求項２４】
請求項２３に記載の電子デバイスであって、前記センサは、前記ディスプレイを含む前記デバイスの表面上に配置される、電子デバイス。
【請求項２５】

請求項２０に記載の電子デバイスであって、前記センサは、前記センサの検知領域内で前記ユーザを検出した時に、前記特有の属性を自動的に検出する、システム。
【請求項２６】
電子デバイスのユーザを認証するためのコンピュータ読み取り可能な媒体であって、
前記電子デバイスの入力メカニズムを用いて、ユーザから入力を受信し、
前記入力メカニズムに隣接したセンサを用いて、前記入力を受信する時に前記ユーザの識別情報を検出し、
前記検出した情報に基づいて前記ユーザを認証するためのコンピュータプログラムロジックを記録した、コンピュータ読み取り可能な媒体。
【請求項２７】
電子デバイスのユーザを認証するための方法であって、
複数の選択可能なオプションを表示する工程と、
前記選択可能なオプションのサブセットのユーザ選択を受信する工程と、
前記選択されたサブセットに含まれる選択可能なオプションが、共通の属性を共有していることを決定する工程と、
前記決定工程に応答して、前記ユーザを認証する工程と、を備える、方法。
【請求項２８】
請求項２７に記載の方法はさらに、
前記共通の属性を、メモリに格納された選択可能なオプションの属性と比較する工程と、
前記共通の属性が、前記メモリに格納された前記属性と適合するとの決定に応答して、認証する工程と、を備える、方法。
【請求項２９】
請求項２７に記載の方法はさらに、
メモリに格納された選択可能なオプションの属性を有する選択可能なオプションがすべて選択されたことを検出する工程と、
前記検出工程に応答して、認証する工程と、を備える、方法。
【請求項３０】
請求項２７に記載の方法であって、前記属性は、サイズと、色と、輪郭と、網掛けパターンと、形と、他のオプションとの配列と、他のオプションに対する位置と、ソースと、の内の少なくとも１つを含む、方法。
【請求項３１】
請求項２７に記載の方法であって、前記受信工程は、さらに、前記サブセットに含まれる選択可能なオプションの少なくとも一部を同時に受信する工程を備える、方法。
【請求項３２】
請求項２７に記載の方法であって、前記受信工程は、さらに、前記サブセットに含まれる選択可能なオプションの少なくとも一部を連続的に受信する工程をさらに備える、方法。
【請求項３３】
請求項２７に記載の方法はさらに、
前記認証工程に応答して、制限されたリソースへのアクセスを提供する工程を備える、方法。
【請求項３４】
請求項２７に記載の方法であって、選択可能なオプションの前記サブセットは、４から８個の範囲の選択可能なオプションを含む、方法。
【請求項３５】
電子デバイスのユーザを認証するための方法であって、
前記ユーザから複数の入力を受信する工程と、
連続した入力間の遅延を特定する工程と、
前記特定された遅延が、ライブラリに格納された遅延と適合することを決定する工程と

、
前記決定工程に応答して、前記ユーザを認証する工程と、を備える、方法。
【請求項３６】
請求項３５に記載の方法であって、前記受信工程は、さらに、入力メカニズムを用いて前記複数の入力を受信する工程を備える、方法。
【請求項３７】
請求項３５に記載の方法であって、前記受信工程は、さらに、前記電子デバイスの動きを検出する工程を備える、方法。
【請求項３８】
請求項３５に記載の方法であって、前記受信工程は、さらに、センサを用いて前記電子デバイスへの衝撃を検出する工程を備える、方法。
【請求項３９】
請求項３５に記載の方法であって、さらに、
前記受信した複数の入力を検出する工程と、
前記検出された複数の入力が、前記ライブラリに格納された入力と適合すると決定する工程と、を備える、方法。
【請求項４０】
請求項３５に記載の方法はさらに、
前記特定した遅延が、前記ライブラリに格納された遅延の許容範囲内にあるか否かを判定する工程を備える、方法。
【請求項４１】
請求項３５に記載の方法であって、少なくとも１つの遅延は０である、方法。
【請求項４２】
入力のパターンに基づいてユーザを認証するための電子デバイスであって、
複数の入力を検出するセンサと、
プロセッサと、を備え、前記プロセッサは、
前記検出された複数の入力のパターンを特定し、
前記パターンが、ライブラリに格納されたパターンと適合することを決定し、
前記決定に応答して前記ユーザを認証する、電子デバイス。
【請求項４３】
請求項４２に記載の電子デバイスであって、前記プロセッサは、さらに、入力の視覚的パターンを特定する、電子デバイス。
【請求項４４】
請求項４２に記載の電子デバイスであって、前記センサは、入力メカニズムと、加速度計と、ジャイロスコープと、の内の少なくとも１つを含む、電子デバイス。
【請求項４５】
請求項４２に記載の電子デバイスはさらに、
画面を表示するよう動作するディスプレイを備え、
前記プロセッサは、さらに、複数の選択可能なオプションを前記ディスプレイに表示させる、電子デバイス。
【請求項４６】
請求項４５に記載の電子デバイスであって、前記センサは、さらに、前記表示された複数の選択可能なオプションのサブセットの選択を検出する、電子デバイス。
【請求項４７】
請求項４６に記載の電子デバイスであって、前記プロセッサは、さらに、前記選択されたサブセットに含まれる選択可能なオプションに関連する共通の属性を特定する、電子デバイス。
【請求項４８】
請求項４７に記載の電子デバイスであって、前記属性は、サイズと、色と、輪郭と、網掛けパターンと、形と、他のオプションとの配列と、他のオプションに対する位置と、ソ

ースと、の内の少なくとも１つを含む、電子デバイス。
【請求項４９】
請求項４２に記載の電子デバイスであって、前記プロセッサは、さらに、入力の時間的パターンを特定する、電子デバイス。
【請求項５０】
請求項４９に記載の電子デバイスであって、前記プロセッサは、さらに、前記検出された複数の入力の連続した入力間の時間的遅延を検出する、電子デバイス。
【請求項５１】
電子デバイスのユーザを認証するためのコンピュータ読み取り可能な媒体であって、
選択可能なオプションのサブセットのユーザ選択を受信し、
前記受信されたサブセットに含まれる選択可能なオプションのパターンを特定し、
前記特定されたパターンが、ライブラリに格納されたパターンと適合することを決定し、
前記決定に応答して、前記ユーザを認証するためのコンピュータプログラムロジックを記録した、コンピュータ読み取り可能な媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、内蔵認証システムを備えた電子デバイスに関する。
【背景技術】
【０００２】
電子デバイス、特に携帯型電子デバイスは、個人情報を格納するために用いられる。例えば、ユーザは、ユーザが用いる連絡先、電子メール、カレンダー情報、文書、および、その他の情報を格納するために、携帯電話、ＰＤＡ、スマートフォン、または、その他の電子デバイスを用いてよい。この情報は、必ずしも秘密にしなくてもよいが、ユーザは、情報の少なくとも一部を他人に利用できなくするよう望んでもよい。許可されていない人物がユーザの個人情報にアクセスし閲覧することを防ぐ方法の１つとして、デバイス機能を有効にする前、または、デバイスリソースにアクセスする前に、パスワードまたはパスコードの提供を電子デバイスのユーザに要求する方法が挙げられる。例えば、電子デバイスは、デバイスのホームスクリーン（例えば、スプリングボード）またはメニューを表示する前に、４つの数字または４つの文字のＰＩＮを入力するよう、ユーザに要求してよい。別の例として、ユーザの指紋を検出するためまたはユーザの網膜を走査するための付属デバイスをデバイスに接続することによって、ユーザが、デバイスへのアクセス権を受ける前に、承認された指紋または網膜を最初に示さなければいけないようにしてもよい。
【０００３】
これらの方法は両方とも有効でありうるが、パスワードまたはパスコードに基づくアクセス制限は、パスワードまたはパスコードを知っている他のユーザがいない限りは、効果的である。パスワードまたはパスコードが知られると、制限メカニズムは、効果がなくなりうる。また、パスワードまたはパスコードを忘れて、許可ユーザがデバイスにアクセスできなくなる場合もある。さらに、ユーザに指紋を提供するまたは網膜スキャンを受けるよう要求することは、ユーザがデバイスにアクセスできるまでに求めるステップを増やすため、時間がかかり、ユーザにとって煩わしい場合がある。この方法は、パスワードまたはパスコードの入力よりも安全であるが、ハードウェア（例えば、必要なスキャナ、検出器、または、リーダ）のコストと時間がかかる。したがって、例えば、ユーザがデバイスをオンにする、ロック解除する、または、起動する時に、デバイスが迅速かつシームレスにユーザを認証するように、生体認証および他の認証メカニズムを実装した電子デバイスを提供することが望ましい。
【発明の概要】
【０００４】
電子デバイスのユーザを認証するための方法、電子デバイス、および、コンピュータ読

み取り可能な媒体が提供されている。一部の実施形態において、電子デバイスは、ユーザをシームレスに認証しうる。電子デバイスは、ユーザから入力を受信してよく、その入力は、電子デバイスの入力メカニズムによって提供される。電子デバイスは、ユーザが、入力メカニズムの中またはその近傍に組み込まれた１または複数のセンサから入力を提供する時に、識別情報を検出してよい。電子デバイスは、検出した識別情報を、デバイスのライブラリに格納されている識別情報と比較することによって、ユーザを認証してよい。例えば、センサは、ユーザの皮膚の特長、または、ユーザの皮下の特長を検出するためのセンサを含んでよい。センサは、タッチスクリーン、ボタン（例えば、キーボードまたはマウスのボタン）、入力メカニズム近傍のデバイスの筐体（例えば、キーボードの近くのラップトップ筐体）、または、任意の他の適切な位置の少なくとも一カ所に組み込まれてよい。

【０００５】

一部の実施形態において、電子デバイスは、デバイスの検知素子に対して位置合わせするようユーザに指示することなく、ユーザが検知素子に対して位置合わせされていることを決定してよい。例えば、検知素子は、センサの検知領域が、電子デバイスを操作する際に予期されるユーザの位置を含むように配置されてよい。センサは、検知素子を用いて、ユーザの１または複数の生体属性（例えば、顔または眼の特長）を検出してよい。例えば、センサは、デバイスのディスプレイに隣接したカメラまたは光学センサを備えてよい。次いで、ユーザは、検出された生体属性を、電子デバイスに格納された、または、電子デバイスがアクセスできる生体属性のライブラリと比較することによって認証されてよい。

【０００６】

一部の実施形態において、電子デバイスは、ユーザによって選択されたオプションの共通の属性に基づいて、ユーザを認証してもよい。電子デバイスは、ユーザによる選択のために、いくつかの選択可能なオプションを表示してよく、オプションのサブセット（一部）のユーザ選択を受信してよい。次いで、電子デバイスは、選択されたオプションの一部または全部に共通する１または複数の属性を特定してよい。属性は、例えば、サイズ、色、輪郭、網掛けパターン、形状、他のオプションとの配列、他のオプションに対する位置、オプションのソース、または、任意の他の適切な属性の内の少なくとも１つを含んでよい。次いで、電子デバイスは、特定された属性に基づいてユーザを認証してよい。例えば、ユーザが、特定のユーザに関連づけられた属性を共有する形状をすべて選択した場合、電子デバイスは、そのユーザを認証してよい。

【０００７】

一部の実施形態において、電子デバイスは、デバイスが受信した入力のパターンに基づいて、ユーザを認証してもよい。電子デバイスは、ユーザによって提供される複数の入力を検出するセンサを備えてよい。例えば、センサは、ユーザによって提供された入力を受信する入力メカニズムを備えてよい。別の例として、センサは、電子デバイスの動き、または、電子デバイスとの接触を検出する加速度計またはジャイロスコープを備えてもよい。電子デバイスは、検出した入力のパターンを特定し、特定したパターンを、メモリに格納されたパターンと比較して、ユーザを認証するよう動作してよい。パターンは、時間的パターン（例えば、連続する入力の間の遅延に関するパターン）、視覚的パターン（例えば、ユーザが選択したいくつかのオプションの属性、または、ユーザが提供した入力に関するパターン）、または、これらの組み合わせを含みうる。ユーザを認証すると、電子デバイスは、制限された電子デバイスリソースへのアクセスをユーザに提供してよい。

【図面の簡単な説明】

【０００８】

【図１】本発明の一実施形態による認証システムと共に使用するための電子デバイスの一例を示す概略図。

【図２】本発明の一実施形態に従って、電子デバイスのディスプレイスクリーンの一例を示す概略図。

【図３】本発明の一実施形態に従って、ユーザに認証を指示するためのディスプレイスク

リーンの一例を示す図。
【図４】本発明の一実施形態に従って、ユーザがデバイスリソースにアクセスする前に、ユーザに認証を指示するためのディスプレイスクリーンの一例を示す概略図。
【図５Ａ】本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。
【図５Ｂ】本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。
【図５Ｃ】本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。
【図６】本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスのディスプレイの一例を示す概略図。
【図７】本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスの別の例を示す概略図。
【図８Ａ】本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図。
【図８Ｂ】本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図。
【図９】本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図。
【図１０】本発明の一実施形態に従って、ユーザの皮膚の下の特徴を検出するセンサを有するデバイスの一例を示す概略図。
【図１１】本発明の一実施形態に従って、ユーザの顔の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図。
【図１２】本発明の一実施形態に従って、ユーザの眼の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図。
【図１３】本発明の一実施形態に従って、視覚的パターンを提供するためのディスプレイの一例を示す概略図。
【図１４】本発明の一実施形態に従って、視覚的パターンを提供するためのディスプレイの一例を示す概略図。
【図１５】本発明の一実施形態に従って、ユーザを認証するための方法の一例を示すフローチャート。
【発明を実施するための形態】
【０００９】
電子デバイスのリソースへのアクセスを制限するための認証システムを有する電子デバイスが提供されている。例えば、デバイスに格納されたまたはデバイスから利用できるファイルまたはデータへのアクセスなど、任意の適切な電子デバイスリソースへのアクセスが制限されてよい。別の例として、特定のアプリケーション（例えば、特定のユーザが購入したアプリケーション、または、管理者タスクまたは管理者特権と関連づけられたアプリケーション）へのアクセスが制限されてもよい。さらに別の例として、ユーザが認証されるまで、個人設定（例えば、表示されるオプション、背景画像、または、アプリケーションに用いるアイコン）へのアクセスが制限されてもよい。
【００１０】
任意の適切な認証システムが実装されてよい。一部の実施形態において、認証システムは、ユーザの生体特徴または属性を検出するためのシステムを備えてよい。例えば、電子デバイスは、指紋、手紋（hand print）、掌紋、指関節紋（knuckle print）、血管パターン、または、任意のその他の適切なユーザの皮膚の一部もしくは皮下の一部など、ユーザの皮膚の特徴または皮下の特徴に基づいて、ユーザを検出および認証するシステムを備えてよい。別の例として、電子デバイスは、ユーザの眼または顔の特徴もしくはユーザの眼（眼球）の動きに基づいて、ユーザを検出および認証するシステムを備えてもよい。さらに別の例として、電子デバイスは、ユーザの外耳道の特徴、ユーザに関連した匂い、ユ

ーザのＤＮＡ、または、ユーザに関連した任意のその他の適切な生体属性もしくは情報を検出するシステムを備えてもよい。

【００１１】

一部の実施形態において、認証システムは、ユーザによって提供される視覚的または時間的な入力パターンに基づいてユーザを特定するシステムを備えてよい。例えば、電子デバイスは、視覚的なパターンを形成するいくつかの選択可能なオプションまたは図形を表示してよい。ユーザは、認証のために、表示されたオプションから任意の適切な所定のサブセット（一部）を選択してよい。例えば、ユーザは、共通する所定の属性（例えば、サイズ、色、形状、または、輪郭）を有する１または複数のオプションを選択してよい。別の例として、ユーザは、ディスプレイの所定の領域に配置された１または複数のオプションを（例えば、選択するオプションの属性とは無関係に）選択してもよい。ユーザは、同時に、逐次的に、または、これらの組み合わせとして、オプションを選択してよい。

【００１２】

別の例として、ユーザは、特定のペースまたは特定のパターンで、一連の入力を提供してもよい。例えば、ユーザは、特定の遅延（例えば、２つの選択の間の中断）を伴って、オプションを選択してよい。あるいは、ユーザは、所定の時間的パターンに従って、デバイスのセンサ（例えば、加速度計またはジャイロスコープ）で検出される入力を提供してもよい。デバイスは、デバイスまたはデバイスに隣接した領域をタッピングしたり特定の方法でデバイスを動かしたりすることによって引き起こされる振動から入力を検出するなど、入力を検出するための任意の適切な方法で検出してよい。

【００１３】

電子デバイスは、例えば、生体認証システムおよびパターンに基づく認証システム、いくつかの生体認証システム、または、いくつかのパターンに基づくシステムなど、任意の適切な組み合わせの認証システムを提供してよい。一部の実施形態において、異なるリソースに異なる認証システムを関連づけてよく、その結果、ユーザは、特定の制限されたリソース（例えば、プライベートまたは個人情報）に最終的にアクセスする前に、いくつかのシステムに認証情報を提供しうる。電子デバイスは、どの認証システムを組み合わせるかを選択するために任意の適切な方法を用いてよい。例えば、ユーザが、いくつかの認証システムを特定のリソースと関連づけてもよいし、あるいは、電子デバイスが、自動的に（例えば、デフォルトとして）特定の認証システムを特定のリソースに割り当ててもよい。

【００１４】

図１は、本発明の一実施形態による認証システムと共に使用するための電子デバイスの一例を示す概略図である。電子デバイス１００は、プロセッサ１０２、ストレージ１０４、メモリ１０６、通信回路１０８、入力／出力回路１１０、認証システム１１２、および、電源１１４を備えてよい。一部の実施形態において、電子デバイス１００の構成要素の内の１または複数を組み合わせたり省略したりしてもよい（例えば、ストレージ１０４およびメモリ１０６を組み合わせる）。一部の実施形態において、電子デバイス１００は、図１に示した構成要素に一体化されていないまたは備えられていない他の構成要素（例えば、ディスプレイ、バス、または、入力メカニズム）を備えてもよいし、図１に示した構成要素を複数備えてもよい。簡単のために、図１には各構成要素について１つだけ図示している。

【００１５】

プロセッサ１０２は、電子デバイス１００の動作および実行を制御する任意の処理回路を備えてよい。例えば、プロセッサ１００は、オペレーティングシステムアプリケーション、ファームウェアアプリケーション、メディア再生アプリケーション、メディア編集アプリケーション、または、任意の他のアプリケーションを実行するために用いられてよい。一部の実施形態において、プロセッサは、ディスプレイを駆動し、ユーザインターフェースから受信した入力を処理してよい。

【００１６】

ストレージ１０４は、例えば、ハードドライブ、ソリッドステートドライブ、フラッシュメモリ、ＲＯＭのような永久メモリ、任意の他の適切なタイプの記憶素子、または、それらの任意の組み合わせなど、１または複数の記憶媒体を含んでよい。ストレージ１０４は、例えば、メディアデータ（例えば、音楽ファイルおよびビデオファイル）、（例えば、デバイス１００に機能を実装するための）アプリケーションデータ、ファームウェア、ユーザプリファレンス情報データ（例えば、メディア再生設定）、認証情報（例えば、許可ユーザに関連づけられたデータのライブラリ）、ライフスタイル情報データ（例えば、食べ物の好み）、エクササイズ情報データ（例えば、エクササイズ監視装置で取得した情報）、取引情報データ（例えば、クレジットカード情報などの情報）、無線接続情報データ（例えば、電子デバイス１００が無線接続を確立することを可能にしうる情報）、定期購読情報データ（例えば、ユーザが加入するポッドキャスト、テレビ番組、または、その他のメディアを把握する情報）、連絡先データ（例えば、電話番号および電子メールアドレス）、カレンダー情報データ、および、任意の他の適切なデータまたはこれらの任意の組み合わせを格納しうる。

【００１７】

メモリ１０６は、キャッシュメモリ、ＲＡＭなどの半永久メモリ、および／または、データを一時的に格納するために用いられる１または複数の異なるタイプのメモリを含みうる。一部の実施形態において、メモリ１０６は、電子デバイスアプリケーションを動作させるために用いるデータ、または、ストレージ１０４に格納されうる任意の他のタイプのデータを格納するために利用可能である。一部の実施形態において、メモリ１０６およびストレージ１０４は、単一の記憶媒体として組み合わされてもよい。

【００１８】

通信回路１０８は、デバイス１００が、任意の適切な通信プロトコルを用いて、１または複数のサーバまたはその他のデバイスと通信することを可能にすることができる。電子デバイス１００は、異なる通信ネットワークを用いていくつかの通信動作を同時に実行するために、複数の通信回路１０８を備えてもよいが、図が複雑になることを避けるために図１には１つしか図示していない。例えば、通信回路１０８は、Ｗｉ－Ｆｉ（例えば、８０２．１１プロトコル）、イーサーネット（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）（Ｂｌｕｅｔｏｏｔｈ Ｓｉｇ社の商標）、無線周波数システム、セルラーネットワーク（例えば、ＧＳＭ（登録商標）、ＡＭＰＳ、ＧＰＲＳ、ＣＤＭＡ、ＥＶ－ＤＯ、ＥＤＧＥ、３ＧＳＭ、ＤＥＣＴ、ＩＳ－１３６／ＴＤＭＡ、ｉＤｅｎ、ＬＴＥ、または、任意のその他の適切なセルラーネットワークまたはプロトコル）、赤外線、ＴＣＰ／ＩＰ（例えば、ＴＣＰ／ＩＰ層の各層で用いられるプロトコルのいずれか）、ＨＴＴＰ、ＢｉｔＴｏｒｒｅｎｔ、ＦＴＰ、ＲＴＰ、ＲＴＳＰ、ＳＳＨ、ボイスオーバーＩＰ（ＶＯＩＰ）、任意のその他の通信プロトコル、または、それらの任意の組み合わせをサポートしてよい。

【００１９】

入力／出力回路１１０は、アナログ信号およびその他の信号をデジタルデータに変換（および、必要であればエンコード／デコード）するよう動作してよい。一部の実施形態において、入力／出力回路は、デジタルデータを任意のその他のタイプの信号に変換してもよく、その逆を行うこともできる。例えば、入力／出力回路１１０は、（例えば、マルチタッチスクリーンからの）物理接触入力、（例えば、マウスまたはセンサからの）物理的な動き、（例えば、マイクロホンからの）アナログ音声信号、または、任意のその他の入力を受信して変換してよい。デジタルデータは、プロセッサ１０２、ストレージ１０４、メモリ１０６、または、電子デバイス１００の任意の他の構成要素に供給し、また、そこから受信することができる。入力／出力回路１１０は、電子デバイス１００の単一の構成要素として、図１に示されているが、複数の入力／出力回路を電子デバイス１００に備えてもよい。

【００２０】

電子デバイス１００は、入力／出力回路１１０にユーザが入力を提供することを可能にする任意の適切なメカニズムまたは構成要素を備えてよい。例えば、電子デバイス１００

は、例えば、ボタン、キーパッド、ダイヤル、クリックホイール、または、タッチスクリーンなど、任意の適切な入力メカニズムを備えてよい。一部の実施形態において、電子デバイス１００は、静電容量式検知メカニズムまたはマルチタッチ静電容量式検知メカニズムを備えてよい。いくつかの検知メカニズムは、２００４年７月１０日に出願された同時係属している本願出願人の米国特許出願第１０／９０２，９６４号「Ｇｅｓｔｕｒｅｓ ｆｏｒ Ｔｏｕｃｈ Ｓｅｎｓｉｔｉｖｅ Ｉｎｐｕｔ Ｄｅｖｉｃｅ」、および、２００５年１月１８日に出願された米国特許出願第１１／０２８，５９０号「Ｍｏｄｅ－Ｂａｓｅｄ Ｇｒａｐｈｉｃａｌ Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅｓ ｆｏｒ Ｔｏｕｃｈ Ｓｅｎｓｉｔｉｖｅ Ｉｎｐｕｔ Ｄｅｖｉｃｅ」に記載されており、両方とも本明細書に全体が組み込まれる。

【００２１】

一部の実施形態において、電子デバイス１００は、例えば、１または複数のオーディオ出力などの出力デバイスに関連する専用の出力回路を備えてもよい。オーディオ出力は、電子デバイス１００に内蔵された１または複数のスピーカ（例えば、モノラルスピーカまたはステレオスピーカ）、または、電子デバイス１００と遠隔接続されたオーディオ構成要素（例えば、有線または無線で通信デバイスと接続できるヘッドセット、ヘッドホン、または、イヤホン）を含んでよい。

【００２２】

一部の実施形態において、Ｉ／Ｏ回路１１０は、ユーザに可視表示を提供するディスプレイ回路（例えば、スクリーンまたは投影システム）を備えてよい。例えば、ディスプレイ回路は、電子デバイス１００に組み込まれたスクリーン（例えば、ＬＣＤスクリーン）を備えてよい。別の例として、ディスプレイ回路は、移動可能なディスプレイ、または、電子デバイス１００から離れた面にコンテンツの表示を提供するための投影システム（例えば、ビデオプロジェクタ）を備えてもよい。一部の実施形態において、ディスプレイ回路は、デジタルメディアデータをアナログ信号に変換するためにコーダ／デコーダ（コーデック）を備えてよい。例えば、ディスプレイ回路（または、電子デバイス１００内のその他の適切な回路）は、ビデオコーデック、オーディオコーデック、または、任意のその他の適切なタイプのコーデックを備えてよい。

【００２３】

また、ディスプレイ回路は、ディスプレイドライバ回路、ディスプレイドライバを駆動するための回路、または、その両方を含みうる。ディスプレイ回路は、プロセッサ１０２の指示を受けて、コンテンツ（例えば、メディア再生情報、電子デバイスに実装されたアプリケーションのアプリケーション画面、継続中の通信動作に関する情報、入ってくる通信要求に関する情報、または、デバイス操作画面）を表示するよう動作してよい。

【００２４】

認証システム１１２は、デバイス１００のユーザを特定する入力を受信または検出する任意の適切なシステムまたはセンサを備えてよい。例えば、認証システム１１２は、皮膚のパターンを検知するメカニズム、ユーザの顔のパターン、眼の特徴（例えば、網膜）、または、静脈パターンに基づいてユーザを特定するための光学システム、または、任意の他のユーザ特有の生体特徴または属性を検出するための任意の他のセンサを備えてよい。別の例として、認証システム１１２は、ユーザを特定する秘密または機密の入力（例えば、デバイス上でのジェスチャ、または、ディスプレイ上のオブジェクトまたは色を特定のパターンで触ること、など）を受信するよう動作してもよい。さらに別の例として、認証システム１１２は、ユーザによるデバイスの特定の動きまたは振動を検出するよう動作してもよい。認証システム１１２は、電子デバイス１１２の任意の他の構成要素（例えば、ディスプレイまたはカメラ）に一体化または内蔵されてもよく、また、電子デバイスの様々なセンサ（例えば、加速度計または近接センサ）によって検出されたイベントを利用してもよい。一部の実施形態において、複数種類の認証システムが、電子デバイスに組み込まれたり実装されたりしてよい。

【００２５】

一部の実施形態において、電子デバイス１００は、制御プロセッサ１０２、ストレージ１０４、メモリ１０６、通信回路１０８、入力／出力回路１１０、認証システム１１２、および、電子デバイスに備えられた任意の他の構成要素とのデータのやり取り、または、それら構成要素の間でのデータのやり取りのためのデータ転送パスを提供するバスを備えてよい。

【００２６】

メモリまたはストレージに格納されたデータまたは情報への不正アクセスを防ぐために、電子デバイスは、ユーザを特定し、要求されたリソースへのアクセスを許可するよう、認証システムに指示してよい。電子デバイスは、任意の電子デバイスリソースへのアクセスを提供する前に、認証を要求してよい。一部の実施形態において、電子デバイスは、異なるアプリケーション、または、異なるアプリケーションに関連づけられた異なるデータまたはファイルへのアクセスを提供する前に、異なるレベルの認証を要求してもよい。例えば、電子デバイスは、アプリケーションまたはデータへのアクセスを提供する前に、いくつかの認証システムを満たすようにユーザに要求してよい（例えば、パスコードなどの第１または初期認証に加えて、生体認証などを用いる第２認証を、デバイスのロック解除に利用する）。

【００２７】

図２は、本発明の一実施形態に従って、電子デバイスのディスプレイスクリーンの一例を示す概略図である。ディスプレイスクリーン２００は、ユーザが電子デバイスをロック解除したことに応答して表示されてよい。ディスプレイスクリーン２００は、様々なデバイス機能にアクセスするための選択可能なオプション２１０を備えてよい。例えば、各オプション２１０は、電子デバイスで利用可能な異なるアプリケーションと関連づけられてよい。別の例として、各オプションは、ユーザが利用可能な特定のデータまたはファイルと関連づけられてもよい。電子デバイスは、ディスプレイ２００にアクセスするための認証を要求してもよいし要求しなくてもよい。例えば、ディスプレイ２００は、ユーザが利用可能な基本的またはデフォルトのアプリケーションを含んでよい。別の例として、ディスプレイ２００は、すべてのユーザが利用可能なデフォルトの機能を含んでもよい。

【００２８】

一部の実施形態において、１または複数のアプリケーションが、１または複数のユーザの個人的なデータまたはリソースへのアクセスを提供したり利用したりしてよい。例えば、それぞれ、電話およびメールのアプリケーションと関連づけられたオプション２１２および２１４は、電子デバイスのすべてのユーザには関連づけられていない個人のアカウントまたは連絡先を含んでよい。かかるアプリケーションへのアクセス、または、かかるアプリケーションを介して利用可能な個人的または秘密の機能またはリソースへのアクセスを提供する前に、電子デバイスは、ユーザに認証を要求してよい。一部の実施形態において、アプリケーションのデフォルトの機能は、認証なしに利用可能であってもよい（例えば、すべてのユーザが電話をかけることができるが、連絡先リストにはアクセスできない）。

【００２９】

図３は、本発明の一実施形態に従って、ユーザに認証を行わせるディスプレイスクリーンの一例を示す図である。ディスプレイスクリーン３００は、認証プロトコルによって制限されたリソース（例えば、情報またはアプリケーション）にアクセスするための命令をユーザから受信したことに応答して表示されてよい。ディスプレイスクリーン３００は、選択されたリソースに関連づけられた情報３１０を含んでよい。認証前には、無許可ユーザがリソースを閲覧することを防ぐために、情報３１０は、不鮮明になっていてもよいし、ビューから隠されてもよい（例えば、特定のフィールドのエントリが取得不可能になってよい）。一部の実施形態において、ディスプレイスクリーン３００は、ユーザが認証されるまで情報を含まなくてもよい。

【００３０】

ディスプレイスクリーン３００は、要求されたリソースにアクセスする前にユーザが認

証を行うよう指示する通知３２０を備えてよい。通知３２０は、ポップアップ、オーバーレイ、新たなディスプレイスクリーン、または、ユーザに指示を提供するための任意の他の適切なタイプのディスプレイを含みうる。通知３２０は、例えば、ユーザが認証を行う方法など、任意の適切な指示を含んでよい（例えば、使用すべき特定の認証システムを指定する指示など）。例えば、通知３２０は、指紋の提供、または、所定の視覚的または時間的パターンに適合する入力の提供をユーザに指示してよい。ユーザが適切に認証されると、電子デバイスは、ユーザが識別できるように情報３１０を表示し、選択されたリソースに関連づけられた選択可能オプションまたはその他の機能を有効にしてよい。

【００３１】

一部の実施形態において、ユーザは、電子デバイスをロック解除する前に（例えば、デバイスの任意のリソースにアクセスする前に）、認証を要求されてよい。図４は、本発明の一実施形態に従って、ユーザがデバイスリソースにアクセスする前に、ユーザに認証を指示するためのディスプレイスクリーンの一例を示す概略図である。ディスプレイスクリーン４００は、ディスプレイのロックを解除するためのオプション４１０を備えてよい。例えば、オプション４１０は、スクリーンの一部を横切って（横断して）ドラッグされるスライダを備えてよい。別の例として、オプション４１０は、ユーザが選択すべきオプションまたは一連のオプション（例えば、いくつかのキーを同時または連続的に押す、または、ディスプレイスクリーン４００のいくつかの領域に触れる、など）を備えてもよい。

【００３２】

ディスプレイスクリーン４００は、デバイスリソースにアクセスする前に、認証を受けるようユーザに指示する通知４２０を含んでよい（例えば、情報およびアプリケーションを起動するホームスクリーン）。通知４２０は、例えば、ポップアップ、オーバーレイ、新たなディスプレイスクリーン、または、ユーザに指示を提供するための任意の他の適切なタイプのディスプレイなど、任意の適切なタイプの通知を含みうる。電子デバイスは、例えば、ユーザがデバイスのスイッチを入れた時（例えば、その後ディスプレイスクリーン４００を見る時）、第１の認証なしにユーザがデバイスリソースへのアクセスを試みたことに応じて（例えば、エラーメッセージとして）、ユーザによるヘルプの要求に応じて、または、任意のその他の適切な時点など、任意の適切な時に通知４２０を表示してよい。通知４２０は、例えば、ユーザが認証を行う方法、許可ユーザのリスト、または、任意のその他の適切な情報など、任意の適切な指示を含んでよい。

【００３３】

ユーザが適切に認証されると、電子デバイスは、認証されたユーザに関連づけられたオプション（例えば、特定のユーザが購入したアプリケーションのオプション）を表示してよい。一部の実施形態において、電子デバイスは、以前には利用できなかったリソースまたはコンテンツ（例えば、電話または電子メールアプリケーションの連絡先リストまたは以前のメッセージ、など）へのアクセスを提供してよい。図５ＡないしＣは、本発明の実施形態に従って、ユーザ認証に応答して提供された異なるユーザに関連づけられたディスプレイスクリーンの例を示す概略図である。ディスプレイスクリーン５００Ａは、いくつかのオプション５１０Ａを備えてよい。表示されたオプションは、電子デバイスのデフォルトまたは基本的なディスプレイに共通するいくつかのオプションを含んでよい（例えば、ディスプレイスクリーン５００Ａは、図２のディスプレイスクリーン２００とオプションを共有している）。ディスプレイスクリーン５００Ａは、特定の認証済みユーザにだけ利用可能な追加のアプリケーションまたはリソースのためのいくつかのオプション５１２Ａを備えてよい。例えば、ディスプレイスクリーン５１０Ａは、ゲーム、システム、および、メディアアプリケーションのための追加のオプション５１２Ａを備えてよい。

【００３４】

ディスプレイスクリーン５００Ｂは、ユーザに利用可能なリソースまたはアプリケーションのためのオプション５１０Ｂを備えてよい。一部の実施形態において、オプション５１０Ｂは、デフォルトスクリーンのオプションと完全に異なるものであってよい（例えば、ディスプレイスクリーン５００Ｂは、図２のディスプレイスクリーン２００とオプショ

ンを共有しない）。ディスプレイスクリーン５００Ｂは、オプション５１０Ｂに関連づけられたアプリケーションまたはリソースを特定するラベルを含まないよう、さらにカスタマイズされてよい。

【００３５】

ディスプレイスクリーン５００Ｃは、ユーザに利用可能なリソースまたはアプリケーションのためのオプション５１０Ｃを備えてよい。一部の実施形態において、他のディスプレイスクリーンと同じリソースのためのオプション５１０Ｃが、異なるアピアランス（例えば、異なるアイコン）を有してもよい。例えば、図５Ｃにおいて、メール、時計、写真、ＹｏｕＴｕｂｅ（登録商標）、および、電卓アプリケーションのために表示されているオプションは、図５Ａのディスプレイスクリーン５００Ａに表示されるオプションと異なっていてよい。ディスプレイスクリーン５００Ｃは、カスタムすなわち個人用の背景５１２Ｃ（例えば、異なる背景画像）を、さらに備えてよい。一部の実施形態において、ディスプレイスクリーン５００Ｃは、（例えば、ドック５１２Ｂに配置されるオプション５１０Ｂと異なり）、いくつかのオプション５１０Ｃを固定位置に維持するためのドックまたはその他の機能を備えなくてもよい。

【００３６】

一部の実施形態において、電子デバイスは、認証済みユーザのアイデンティティに基づいて、異なる範囲の電子デバイスリソースへのアクセスを提供してよい。例えば、電子デバイスが複数のユーザによって利用されている場合（例えば、同一家族の両親と子供たち）、ユーザは、リソースのすべてではなく一部を共有してよい（例えば、すべてのユーザが家族の連絡先リストにアクセスできるが、他の家族の電子メールにはアクセスできない）。別の例として、電子デバイスのユーザは、ユーザのグループまたは階層に体系化されてもよい。いくつかのリソースが、特定のユーザに関連づけられる代わりにまたはそれに加えて、ユーザのグループまたは階層に関連づけられてよい。特定のユーザがグループの一員として認証および特定されると、電子デバイスは、そのグループに関連づけられたリソース（例えば、共通または供用の連絡先、供用の通信、または、供用の文書）、および、特定のユーザに関連づけられたリソース（例えば、個人的な連絡先、電子メールアカウント、および、通話リスト）へのアクセスを、そのユーザに提供してよい。

【００３７】

電子デバイスは、特定のリソースを１または複数の認証システムと関連づけてよい。例えば、ユーザは、リソースを特定し、保護またはセキュリティの命令を（例えば、適切なオプションを選択することによって）提供してよい。ユーザは、さらに、リソースへのアクセスを提供する前に、満たすべき１または複数の認証システムを選択してよい。リソースが供用ではない（例えば、すべてのユーザに利用可能なままであるデフォルトのアプリケーションまたはファイルではない）場合、または、リソースがユーザによって作成または購入された場合、電子デバイスは、選択されたリソースを１または複数の選択された認証システムと関連づけてよい。あるいは、ユーザが十分な特権を有する（例えば、管理者である）場合、任意のリソースが、１または複数の選択された認証システムを用いて保護されてもよい。

【００３８】

電子デバイスは、ユーザが電子デバイスをロック解除または操作するたびに、ユーザに認証を要求しなくてもよい。一部の実施形態において、電子デバイスは、ユーザが認証された状態を特定の期間だけ維持してよい。例えば、一旦認証が済むと、電子デバイスは、ユーザが認証された時間から１０時間、制限されたリソースにユーザがアクセスすることを許容してよい。別の例として、電子デバイスは、ユーザの最後の命令を受信した後またはスタンバイモードに入った後、特定の期間だけユーザの認証を保持（例えば、入力後３０分間認証を保持）してもよい。電子デバイスが認証情報を保持する期間の長さは、デバイスまたはユーザによって設定されてよく、認証情報によって保護される特定のタイプまたはリソースに基づいてよい（例えば、ユーザの個人的な連絡先よりも、特定のユーザが購入したゲームへのアクセスについては認証期間が長くてよい）。ユーザがデバイスを操

作するたびに電子デバイスが認証を要求しなくてもよいため、電力消費を節約することができる。

【００３９】

電子デバイスは、デバイスリソースへの不正アクセスを防ぐために任意の適切なタイプの認証システムを用いてよい。一部の実施形態において、電子デバイスは、ユーザ特有の皮膚のパターンに基づいた認証システムを備えてよい。例えば、電子デバイスは、ユーザの指紋、手紋、掌紋、指関節紋、または、ユーザに特有な任意の他の適切な紋理または皮膚の特徴を検出する認証システムを備えてよい。認証システムは、ユーザに特有な皮膚のパターンまたは特徴を検出するセンサを備えてよい。

【００４０】

センサは、ユーザの皮膚に特有な特徴またはパターンを検出するための任意の適切なタイプのセンサを含んでよい。例えば、センサは、ユーザの皮膚の特徴を検出する光学スキャナを含みうる。光学センサは、電荷結合素子、または、センサ（例えば、電荷結合素子）によって受光した光を記録する任意の他の適切な受光素子（例えば、ダイオード）のアレイを備えてよい。例えば、電荷結合素子が受光素子アレイを備える場合、光学センサは、アレイの各受光素子について、特定の受光素子が受光した光を表すピクセルを記録するよう動作してよい。各ピクセルの値は、ピクセルに関連づけられたユーザの皮膚の特定の部分（例えば、隆線または谷線）のセンサからの距離を反映しうる。記録されたピクセルは、電子デバイスが許可ユーザに関連づけられた画像のライブラリと比較できる画像（例えば、ユーザの皮膚の特定の部分の画像など）を形成しうる。

【００４１】

別の例として、センサは、ユーザの皮膚の特徴を検出する容量センサを含んでもよい。容量センサは、セルのアレイを含む１または複数のチップを備えてよく、各セルは、絶縁層によって隔てられた少なくとも２つの導体板を備えてよい。センサは、チップの各セルの少なくとも２つの導体板の間の電圧を変化させる反転増幅器に接続されてよい。ユーザの指がセルアレイ上に置かれると、センサは、各セルの容量値の違い（例えば、谷線の下のセルは隆線の下のセルよりも低い容量値を有する）に基づいて、谷線（例えば、指紋の谷線）の置かれたセルと隆線（例えば、指紋の隆線）の置かれたセルを区別するよう動作しうる。チップの各セルで検出された容量値を用いて、センサは、電子デバイスが利用できる画像または表現のライブラリと比較可能な画像または表現を、センサに置かれた皮膚について生成しうる。

【００４２】

認証システムは、例えば、画像（例えば、印刷した画像）または３次元構造（例えば、ポリマ鋳造物）を認証システムのセンサに近接させることによって、無許可ユーザが許可ユーザの皮膚パターンをまねることを防止する任意の適切な対応策を備えてよい。例えば、認証システムは、光学および容量センサの組み合わせ、ソナーまたは高周波センサ、ユーザの脈拍を検出するセンサ、センサに触れた物体の温度を決定する熱センサ（例えば、温度が人間の皮膚温度の予測の範囲内にあるか否かを判定するため）、または、任意のその他の適切な対応策を備えてよい。

【００４３】

センサは、任意の適切な方法を用いて、ユーザの皮膚の特徴を検出するよう動作しうる。一部の実施形態において、センサは、ユーザの皮膚がセンサ上で移動された時に、ユーザの皮膚の特徴を検出するよう動作してよい。例えば、センサは、ユーザの指がセンサ上でスライドまたは回転した時にユーザの指の特徴を検出する一次元センサすなわち固定センサ（stagnant sensor）（例えば、一列の検知素子）を備えてよい。センサは、ユーザの皮膚の特徴の正確な表現を提供するために、ユーザの皮膚を動かすべき方向を有してよい。例えば、センサは、指の軸に沿ってまたは指の軸に直交に指先を動かすよう、ユーザに要求してよい。

【００４４】

一部の実施形態において、センサは、皮膚がセンサ上で動かないよう保持された時に、

ユーザの皮膚の特徴を検出するよう動作してもよい。例えば、センサは、指がセンサの上で静止している時にユーザの指の特徴を検出する２次元センサすなわち移動センサを備えてよい。センサは、静止したユーザの指の下で規則的なペースまたは速度で動くよう動作してもよいし、（例えば、ユーザの指がセンサ上で動く状態で）ある時点のユーザの指の瞬間的または略瞬間的な二次元表現を検出するよう動作してもよい。二次元センサは、一次元センサと違って、ユーザが規則的または一様なペースでセンサ上で皮膚を移動させることには依存しないので、二次元センサを用いることにより、ユーザの皮膚特徴のより正確な表現を提供できる。

【００４５】

センサは、電子デバイス内の任意の適切な位置に配置されてよい。一部の実施形態において、センサは、ユーザが電子デバイスを操作する時または操作し始める時に、ユーザの皮膚の適切な部分を検出するよう動作できるように配置されてよい。センサの位置は、検出すべきユーザの皮膚の部分（例えば、指、手、または、掌）によって異なってよい。図６は、本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスのディスプレイの一例を示す概略図である。ディスプレイ６００は、電子デバイスのロックを解除するようユーザに指示するスクリーン６０２を備えてよい。例えば、スクリーン６０２は、ブロック６１０に指を置いてトラック６１２に沿って指をドラッグすることによって、トラック６１２に沿ってブロック６１０をスライドさせて電子デバイスのロックを解除するよう、ユーザに指示する矢印を有するブロック６１０を備えてよい。

【００４６】

ロック解除処理中にユーザを認証するために、ディスプレイ６００は、トラック６１２に沿ってディスプレイ内にセンサ６２０を備えてよい。例えば、センサ６２０は、ディスプレイスタック（例えば、容量検知素子、光源、および、ディスプレイ面を備えうるディスプレイスタック）内に組み込まれてよい。別の例として、センサ６２０は、ディスプレイスタックの下に配置されてもよい。さらに別の例として、センサ６２０は、ディスプレイスタックの既存の構成要素を含んでもよい（例えば、タッチスクリーンディスプレイのディスプレイスタックは、容量センサを備えうる）。かかる例において、認証システムは、ユーザの皮膚の隆線と谷線を区別するのに十分な解像度を有する（例えば、タッチスクリーンディスプレイの）ディスプレイスタックの容量検知素子の検出出力を用いてよい。一部の実施形態において、ディスプレイスタックの容量検知素子は、ディスプレイの特定の部分を用いた認証を可能にするために、いくつかのタイプまたは密度の容量検知素子を備えてよい（例えば、トラック６１２の少なくとも一部に沿ったディスプレイスタックには、認証のために非常に精細な検知素子を用いて、ディスプレイ６００の残りの領域にはあまり精細でない検知素子を用いる）。

【００４７】

一部の実施形態において、センサ６２０は、ディスプレイ６００内で見えないように、電子デバイスに埋め込まれてよい。例えば、センサ６２０は、ユーザが指紋スキャナを見ることができないように、ディスプレイ６００上に組み立てられ、印刷され、または、直接エッチング（例えば、ガラス上にエッチング）されてよい。ユーザがセンサ６２０に適切な指紋を提供するのが困難な場合、ディスプレイ６００は、認証の際にユーザを支援するために、センサ６２０の輪郭を強調してよい（例えば、センサ６２０の上に位置するアイコン上に指を置くよう指示するアイコンを表示する、など）。

【００４８】

図７は、本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスの別の例を示す概略図である。電子デバイス７００は、ユーザが電子デバイス７００に入力を提供するために作動させうる入力メカニズム７１０および７１２を備えてよい。例えば、入力メカニズム７１０は、キーボードを含んでよく、入力メカニズム７１２は、タッチパッドまたはトラックパッドを含んでよい。ただし、電子デバイス７００と遠隔接続された入力メカニズム（例えば、有線または無線マウス）など、任意の他の入力メカニズムが、電子デバイス７００で用いられてもよいことを理解されたい。

【００４９】
リソースへの安全なアクセスを提供するために、電子デバイス７００は、ユーザを特定するためにユーザの指紋の特徴を検出する少なくとも１つのセンサ７２０を備えてよい。シームレスなユーザ体験を提供するために、センサ７２０は、入力メカニズム７１０および７１２の少なくとも一方の中または下に組み込まれてよい。一部の実施形態において、入力メカニズム７１０は、ユーザが電子デバイス７００に入力を提供するために押下しうる複数の別個のキーを備えうるため、１または複数のキーに内蔵されたセンサ７２０を備えてよい。例えば、光学または容量センサは、ユーザが指をキーに置いた（例えば、ユーザの人差し指を「Ｆ」または「Ｊ」キーに置いた）時に、センサがユーザを認証するためにユーザの指先の特徴を検出できるように、キーの上面に配置されてよい。ユーザの指がキーの上に置かれている間にユーザを認証するために、二次元すなわち移動センサが、用いられ得る。

【００５０】
センサ７２０は、電子デバイスにおいてユーザが押下しうる任意のボタンまたはその他の物理的入力の中、近傍、または、裏側に配置されてもよい。例えば、センサ７２０は、携帯型メディアプレーヤまたは携帯電話のホームボタン（例えば、図８Ｂのボタン８１２）の背後に配置されてよい。センサ７２０は、外部のカバーまたは表面（例えば、ガラスまたはプラスチック表面）と、スイッチまたは電子回路に作用する機械的構成要素との間に配置されてよい。例えば、指紋検知メカニズムが、透明な表面の下に組み込まれてよく、そうすれば、検知メカニズムは、その表面を介して、ユーザの指紋の隆線および谷線を検出することができる。一部の実施形態においては、透明な表面を追加しなくてもよい（例えば、検知メカニズムが、ユーザが指を置くことのできる表面を備える場合）。

【００５１】
一部の実施形態において、入力メカニズム７１２は、パッドの一部または全体の下に組み込まれたセンサ７２０を備えてよく、そうすれば、（例えば、ディスプレイ７１５上のインジケータを動かすために）ユーザが入力メカニズム７１２上に指を置いた時に、センサ７２０がユーザを認証するためにユーザの指の特徴を検出することができる。センサ７２０は、ユーザがパッドを横切って指を移動させた時にユーザを認証する一次元センサであってもよいし、ユーザの指をパッド上で静止させた時（例えば、ユーザが最初に指をパッドの上に置いた時）にユーザを認証する二次元センサであってもよい。センサ７２０は、認証のためにユーザが入力メカニズム７１２の特定の部分の上に指を置く必要がないように、入力メカニズム７１２の表面全体を網羅してよい。電子デバイス７００は、ユーザが十分に検出可能な入力を提供するのを支援するために、例えば、強調表示、ディスプレイ上の指示、または、任意のその他の適切な方法を用いて、各センサ７２０の位置を特定するよう動作してよい。一部の実施形態において、任意の他の適切な入力メカニズム（例えば、ボタン、ホイール、キー、または、スクリーン）が、ユーザの指紋の特徴をシームレスに検出するセンサ７２０を備えてもよい。

【００５２】
図８Ａおよび８Ｂは、本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図である。電子デバイス８００は、ディスプレイ８１０を保持する筐体８０２を備えてよい。筐体８０２は、電子デバイスの構成要素を保護するために、電子デバイス８００の背面（例えば、ディスプレイ８１０を備えない側の表面）を実質的に構成してよい。ユーザが電子デバイス８００を持つ時、ユーザの手８３０は、図８Ｂに示すように、ディスプレイ８１０が見えるように、筐体８０２の周りで凹状にされてよく、その時、少なくともユーザの掌８３２が背面８０４に触れるよう配置される。電子デバイス８００は、背面８０４内に組み込まれユーザの掌または手の特徴を検出するセンサ８２０を備えてよい。背面８０２（または、ディスプレイ８１０の表面と反対側にある電子デバイスの任意の表面）にセンサ８２０を配置することにより、センサ８２０は、ユーザが電子デバイス８００を持った時に、ユーザを認証することができる。センサ８２０は、二次元センサを備えてよく、それにより、電子デバイス８００は、背面８０４に触れ

て手を移動またはスライドさせるようユーザに要求することなく、ユーザをシームレスに認証することがきる。

【００５３】

図９は、本発明の一実施形態に従って、ユーザの手紋を検出するための電子デバイスの一例を示す概略図である。電子デバイス９００は、ユーザがデバイスに入力を提供するための入力メカニズム９１０を備えてよい。入力メカニズム９１０は、ユーザの指が入力メカニズム９１０の上に置かれた時に、ユーザの掌および手首が筐体９１２の上に置かれるまたはその上方に伸びるように、配置されてよい。電子デバイス９００は、デバイスのユーザを認証するために、筐体９１２内に組み込まれたまたは筐体９１２上に配置された１または複数のセンサ９２０を備えてよい。センサ９２０は、ユーザが、入力メカニズム９１０を操作するために筐体９１２の上にユーザの手を置いた時に、ユーザの手、掌、または、手首がセンサ９２０に対して位置合わせされるように、配置されてよい。センサ９２０は、ユーザの手が筐体９１２の上に置かれた時に、例えば、二次元センサを用いて、ユーザの皮膚の特徴を検出するよう動作してよい。

【００５４】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの皮膚の下の特徴を検出する検知メカニズムを備えてもよい。例えば、認証システムは、ユーザの静脈、動脈、毛包の分布パターン、または、検出可能なユーザの皮下の任意の他の適切な特徴を検出するセンサを備えてよい。センサは、例えば、電子デバイスの表面上に配置された光学センサ（例えば、カメラ）など、任意の適切なタイプのセンサを含みうる。センサは、電子デバイスの使用中に、ユーザの皮膚の任意の適切な部分の下の特徴を検出するよう配置されてよい。例えば、センサは、ユーザの指、手、手首、腕、顔、または、任意の他の適切な領域の皮膚の下の特徴を検出するよう配置されてよい。

【００５５】

図１０は、本発明の一実施形態に従って、ユーザの皮膚の下の特徴を検出するセンサを有するデバイスの一例を示す概略図である。電子デバイス１０００は、筐体１０１２の一部の上に配置された、または、筐体１０１２の一部にわたって拡がる入力メカニズム１０１０を備えてよい。入力メカニズム１０１０は、使用時に、ユーザの手および手首が（例えば、入力メカニズム１０１０の上ではなく）筐体１０１２の上に配置されるように構成されてよい。電子デバイス１０００は、ユーザの皮膚の下の特徴を検出するセンサ１０２０を備えてよい。例えば、センサ１０２０は、ユーザの手首付近のユーザの静脈パターンを検出する光学センサを含みうる。センサ１０２０は、例えば、入力メカニズム１０１０を用いて入力を提供するためにユーザの手を配置した時にユーザの手首がセンサ１０２０に近接しうるように、筐体１０１２の上に配置または中に組み込まれる、など、電子デバイス１０００の任意の適切な表面に配置されてよい。かかる配置によると、ユーザがデバイス１０００を操作する間に、ユーザの皮膚の下の特徴（例えば、ユーザの手首付近の静脈パターン）を検出することによって、シームレスなユーザ認証を行うことができる。

【００５６】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの顔の特徴を検出するセンサを備えてもよい。例えば、認証システムは、ユーザの顔がセンサと向かい合うように配置された時に、ユーザの顔の１または複数の顕著な特徴によって放射または反射される放射線を検出するセンサを備えてよい。センサは、任意の適切な種類の放射線を検出するよう動作してよい。例えば、センサは、光センサ（例えば、カメラ）、赤外線センサ、紫外線センサ、スキャニングレーザ、超音波センサ（例えば、ソナー）、または、所望の放射線（例えば、特定の範囲の放射線周波数または周期を持つもの）を検出する任意の他の適切なセンサを含みうる。

【００５７】

認証システムは、ユーザの顔の任意の適切な要素を検出するよう動作してよい。例えば、認証システムは、ユーザの頭部、鼻、口、耳、頬骨、あご、または、ユーザの顔の任意の他の属性の相対的な位置およびサイズを解析することにより、顔を特定しうる。別の例

として、認証システムは、ユーザの顔の特徴の曲面または深さ（例えば、眼窩、あご、または、鼻の輪郭）を取り込んで解析するために、三次元認証システムを用いてユーザの顔の特徴を特定してもよい。さらに別の例として、認証システムは、（例えば、皮膚テクスチャ解析を用いて）ユーザの皮膚に特有の線、パターン、または、染みを検出してもよい。認証を向上または円滑化するために、これらの方法を併用してもよい。

【００５８】

ユーザの顔の特徴を検出するためのセンサは、電子デバイスの任意の適切な場所に配置されてよい。一部の実施形態において、センサは、別の目的で電子デバイスに提供されたカメラまたは他のセンサ（例えば、チャットのための内蔵ウェブカメラ）を含んでもよい。図１１は、本発明の一実施形態に従って、ユーザの顔の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図である。電子デバイス１１００は、ユーザが電子デバイスリソースに対して閲覧またはアクセスを行うためにディスプレイ１１１０の方を向いた時に、ユーザの顔およびユーザの顔における対象となる特徴が、センサ１１２０に対して（例えば、センサ１１２０の視野内に）位置が合いうるように、ディスプレイ１１１０に隣接して配置されたセンサ１１２０を備えてよい。センサ１１２０と対向したユーザの顔の検出に応答して、電子デバイス１１００は、ユーザの顔の特徴を捉えて解析するようセンサ１１２０に指示し、解析された特徴を許可ユーザに関連づけられた特徴のライブラリと比較してよい。許可ユーザが検出された場合、電子デバイス１１００は、制限されたコンテンツ１１１２をディスプレイ１１１０に表示したり、コンテンツへのアクセスを提供したりしてよい。

【００５９】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの眼の属性に基づいて、ユーザを認証するセンサを備えてもよい。例えば、センサは、ユーザの網膜、虹彩、または、網膜血管を走査して、ユーザに特有のパターンを検出するよう動作してよい。センサは、光（例えば赤外線など）を放射する光源を備えてよく、その光は、ユーザの眼によって反射され、レンズまたは光学センサによって検出される。センサは、受信した光を解析して、許可ユーザの眼のライブラリと比較することができるユーザの眼の表現を作成する。

【００６０】

別の例として、センサは、代替的または追加的に、例えば、ユーザの網膜、虹彩、血管、または、ユーザの眼の任意の他の特徴の位置および動きを追跡することにより、ユーザの眼の動きを検出するよう動作してもよい。電子デバイスリソースへのアクセスをユーザに提供する前に、電子デバイスは、許可ユーザによって設定された所定の眼の動きを検出するようセンサに指示してよい。例えば、各許可ユーザは、センサを見つつ、特定の方法で（例えば、上、下、左、右、瞬き、瞬き、など）眼を動かすことにより、眼の動きの流れを作成してよい。デバイスのユーザが所定の眼の動きと適合するように眼を動かした場合に、電子デバイスは、デバイスのロックを解除したり、制限されたリソースへのアクセスを提供したりしてよい。

【００６１】

センサは、例えば、ユーザの眼と向かい合うデバイスのディスプレイまたはその他の部分に隣接する位置など、デバイスの任意の適切な位置に配置されてよい（例えば、ユーザの眼の特徴からユーザを認証するのに利用できる図１１のセンサ１１２０と同様の位置）。図１２は、本発明の一実施形態に従って、ユーザの眼の特徴を検出するためのセンサを有する電子デバイスの一例を示す概略図である。電子デバイス１２００は、ユーザが電子デバイスリソースに対して閲覧またはアクセスを行うためにディスプレイ１２１０の方を向いた時に、ユーザの眼が、センサ１２２０に対して（例えば、センサ１２２０の視野内に）位置合わせされうるように、ディスプレイ１２１０に隣接して配置されたセンサ１２２０を備えてよい。センサ１２２０を用いて、電子デバイス１２００は、ユーザを認証し、制限されたデバイスリソースへのアクセスを提供するために、ユーザの眼の特徴または動きを検出してよい。一部の実施形態において、センサ１２２０は、（例えば、図１１の

センサ１１２０のように）ユーザの顔の特徴に基づいてユーザを認証するよう実装されてもよい。

【００６２】

一部の実施形態において、認証システムは、声の属性または質に基づいて、ユーザを認証するよう動作してもよい。例えば、認証システムは、特定の声の高さまたは声紋を検出するよう動作してよい。認証システムは、文字列に依存してもよいし（例えば、ユーザは、「私の声が私のパスワード」など、認証のための特定のフレーズを言わなければならない）、文字列に依存しなくてもよい（例えば、ユーザの認証のために、任意の適切な言葉を言えばよい）。一部の実施形態において、認証システムは、認証のために秘密のパスワードを言うようユーザに要求してよく、そうすれば、そのユーザのパスワードを知っていることと、そのユーザの声の高さを有することの両方を要求して、適切な認証を行うことができる。認証システムは、例えば、マイクロホンなど、ユーザを認証するための任意の適切な構成要素を備えてよい。一部の実施形態において、マイクロホンは、主に別の目的（例えば、電話通信またはビデオ会議）に用いられてもよい。

【００６３】

一部の実施形態において、他のタイプの認証システムが用いられてもよい。一部の実施形態において、認証システムは、外耳道の形からユーザを特定して認証するよう動作してよい。例えば、認証システムは、ユーザの外耳道の特有な特徴（例えば、形および長さ）を検出するセンサ（例えば、光学センサ、レーダー、または、ソナー）を備えてよい。例えば、センサは、（例えば、デバイスが電話である場合には）デバイスのスピーカの近くに配置されてよい。一部の実施形態において、認証システムは、ユーザに特有の匂いに基づいてユーザを特定するよう動作してもよい。例えば、認証システムは、ユーザの皮膚または汗腺の匂いに特有の属性を検出するセンサを備えてよい。センサは、例えば、入力デバイスの場所またはその近傍（例えば、ユーザがデバイスに触れる場所）など、デバイス上の任意の適切な場所に配置されてよい。

【００６４】

一部の実施形態において、認証システムは、ＤＮＡ配列に基づいて、ユーザを特定するよう動作してもよい。例えば、認証システムは、ユーザのＤＮＡを有する細胞を（例えば、ユーザの皮膚または口から）取得するプロセッサに接続されたセンサを備え、特定のＤＮＡ配列が存在するか否かを判定してよい。ＤＮＡ配列の長さまたは変異は、適切な認証を提供しつつ認証処理を十分に速やかに実行できるように選択されてよい（例えば、ＤＮＡ鎖全体を解析する必要はない）。センサは、例えば、ユーザが触れうる入力メカニズムまたはその他の構成要素上、または、その近傍など、デバイス上の任意の適切な場所に配置されてよい。

【００６５】

電子デバイスは、任意の適切な方法を用いて、許可ユーザを反映する生体情報を取得してよい。例えば、ユーザが特定のデバイスリソースに対して用いるよう認証システムを選択すると、電子デバイスは、ライブラリに格納すべき生体情報（例えば、指紋、眼の走査結果、または、ＤＮＡ配列）を提供するようユーザに指示してよい。電子デバイスは、例えば、視覚的な合図、聴覚的な合図を用いる方法、および、認証システムのセンサの位置を強調または特定する方法など、任意の適切な方法を用いて、生体情報入力を提供するようユーザに指示してよい。取得されてライブラリに格納された生体情報は、ユーザが認証を試みる時に取り出され、ユーザによって提供された生体情報と比較されてよい。提供された生体認証情報がライブラリに格納された情報（例えば、要求されたリソースに関連づけられた情報）と適合する場合、電子デバイスは、制限されたリソースへのアクセスを提供してよい。一部の実施形態において、同様の方法を用いて、非生体認証情報を受信してもよい。

【００６６】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザに電子デバイスリソースへのアクセスを提供するために、生体パラメータを要求しなくてもよい。非

生体認証システムは、生体認証システムよりも容易に破られる場合もあるが、非常に効果的で安全なものもある。一部の実施形態において、認証システムは、キーまたはトークンが電子デバイスから特定の距離の範囲内にあるとの検出に応答して、電子デバイスリソースへのアクセスを提供してよい。例えば、ユーザは携帯電話およびコンピュータを有してよい。一方または両方のデバイスは、それらのデバイスが互いに特定の範囲内にあることを検出するための回路を備えてよい（例えば、ユーザがポケットに携帯電話を入れてコンピュータを使うためにデスクに座った時に認証されうるように５フィートの範囲など）。デバイスが互いに近接していると判定した場合、一方または両方のデバイスのリソースが利用可能になってよい。この方法は、ユーザが携帯型デバイスを持ち続けうることを利用しつつ、据え付け型のデバイスへのアクセスを保護するのに特に有効である。本実施形態および他の実施形態の詳細は、２００７年６月２７日に出願された同時係属している本願出願人の米国特許出願第１１／８２３，６５６号（代理人整理番号１０４６７７－００５９－１０１、Ｐ４８８４ＵＳ１）に記載されている。

【００６７】

一部の実施形態において、電子デバイスは、ユーザによって提供される特定の一連の入力に基づいて、ユーザを認証してもよい。例えば、電子デバイスは、電子デバイスによって提供された視覚的パターンと対応する入力を提供するようユーザに要求してよい。図１３および図１４は、本発明の一実施形態に従って、視覚的パターンを提供するためのディスプレイの一例を示す概略図である。ディスプレイ１３００は、オプションすなわち図形１３１２の分布１３１０を備えてよい。ディスプレイ１４００は、オプションすなわち図形１４１２の分布１４１０を備えてよい。図形１３１２および１４１２の各々は、異なる網掛けパターン（例えば、異なる線方向）、単色または多色、形状または輪郭、サイズ（例えば、周囲長または面積）、表示された他の図形との近さまたは相対位置、他の形状との配列（例えば、４つの黄色の図形を選択すると直線を形成する、など）、ソース（例えば、特定のアルバムまたはライブラリの写真を示す図形）、または、任意のその他の適切な特徴を有してよい。分布１３１０または１４１０は、例えば、複数の一様に分布した図形（例えば、２０の一様に分布した図形１３１０）、または、見かけ上不規則な分布の図形（例えば、任意に分布した形１４１０）など、任意の適切な数および分布の図形を含んでよい。

【００６８】

認証を行うために、ユーザは、表示された図形すなわちオプションから任意の適切なサブセットを（例えば、入力メカニズムまたはその他のセンサによって検出された通りに）選択してよい。サブセットは、１または複数の属性を共有する一部またはすべての図形を含みうる。例えば、ユーザは、特定の色である一部またはすべての図形（例えば、黄色を含む図形すべて）を選択してよい。別の例として、ユーザは、同じ輪郭を有する一部またはすべての図形（例えば、すべての正方形）を選択してもよい。さらに別の例として、ユーザは共通する特定の属性を有する一部またはすべての図形（例えば、５つの辺を持つ図形すべて、または、デバイスが格納する特定のアルバムに関連づけられた写真を表す図形すべて）を選択してもよい。さらにまた別の例として、ユーザは、特定の分布の色を含む一部またはすべての図形（例えば、青い部分に隣接して赤い部分を含む図形）を選択してもよい。（青い図形を上から２つ、および、正方形を下から２つ選択するなど、上述の例を組み合わせたものも含め）任意の適切な基準または属性が、表示された図形の特定のサブセットを選択するために用いられてよい。

【００６９】

任意の適切な数の図形すなわちオプションが、認証のために選択すべきサブセットに関連づけられてよい。例えば、かかる図形の数は、表示された図形の総数に関連してよい（例えば、表示された図形の２０％を選択する、など）。別の例として、かかる図形の数は、（例えば、ユーザが片手ですべての図形を同時に選択できるように）５以下、または、（ユーザが両手ですべての図形を同時に選択できるように）１０以下など、決まった数であってもよい。かかる図形の数は、セキュリティを最適化するように選択されてもよい（

例えば、どの図形を選択すべきかを容易には推測できないほど十分な数の図形を要求する、など）。

【００７０】

ユーザは、任意の適切な方法を用いて、サブセットに含まれる図形を選択してよい。マルチタッチディスプレイが提供されている場合、認証システムは、認証に用いる図形すべてを同時に選択するようユーザに要求してよい。別の例として、認証システムは、ユーザが、認証に用いられる図形を順次選択することを許容してもよい。図形は、任意または特定の順序（例えば、上から下、または、左から右）で選択されてよい。さらに別の例として、認証システムは、一筆書きの入力で（例えば、ディスプレイにわたって指をドラッグして）、許可されたサブセットの図形だけを選択するようユーザに要求してもよい。サブセットに含まれる図形を選択するための任意の他の適切な方法を用いてもよい。

【００７１】

（例えば、表示されたキーパッドを用いて数字のパスコードを入力する場合と同様に）、ディスプレイ上の同じ相対位置に表示された図形をユーザに毎回選択させることを避けるために、電子デバイスは、認証のために選択すべき図形の分布を変更してもよい。次いで、ユーザは、認証を行うために、認証プロトコルに関連づけられた属性を共有する図形を特定してよい。ユーザがデバイスリソースにアクセスするたびに、認証に用いられる図形の位置が変化しうるため、選択された図形の全体的な分布をユーザの肩越しに見た人物が、認証のために同じ分布で図形を選択することはできない（例えば、縞模様の図形が、デバイスの同じ領域に分布されなくてもよい）。

【００７２】

無許可ユーザが適切な図形サブセットを推測することを防ぐために、認証のために図形を選択する試みを失敗した後には、電子デバイスは、表示された図形の分布を変更させてもよいし、図形を変化させてもよい（例えば、異なる色または輪郭を用いる、など）。電子デバイスは、適切な図形サブセットを選択する試みに特定の回数失敗した後に、デバイスをロックしてよい。ロックされると、ユーザは、デバイスを再度有効にするためにデバイスをホストに接続する（例えば、携帯型デバイスを据え付け型デバイスに接続する）必要があってもよいし、デバイスを再度有効にするために別の認証システム（例えば、生体認証システムなど）を用いる必要があってもよい。

【００７３】

一部の実施形態においては、特定の図形を選択するのではなく、ユーザは、スクリーンの所定の部分に位置する図形を単に選択してもよい。例えば、ユーザは、実際に表示されている図形と無関係に、いくつかの図形位置に１または複数の指を置いてよい。別の例として、ユーザは、電子デバイスに表示された特定の図形上に１または複数の指を置いて、表示されている図形と無関係に、所定の方法で１または複数の指を動かしてもよい（例えば、１または複数の指をスライドしてよい）。さらに別の例として、ユーザは、ディスプレイの所定の位置に配置されたいくつかの図形を連続的に選択してもよい（例えば、所定のパターンを形成するように特定の位置の図形を選択する、など）。一部の実施形態において、電子デバイスは、ユーザが１または複数の指を用いて１または複数のパターンをその上に描きうる空白または一様なディスプレイ画面を提供してもよい。かかる方法は、表示された図形で視覚的に引きつけることにより、無許可ユーザを混乱させたり注意をそらしたりすることができる。

【００７４】

一部の実施形態において、電子デバイスは、代替的または追加的に、ユーザから受信した入力の時間的パターンに基づいて、ユーザを認証してもよい。例えば、ユーザは、認証のために、特定の速度で特定の回数の入力を提供してよい。電子デバイスは、任意の適切な方法を用いて入力を検出してよい。例えば、電子デバイスは、デバイスの入力メカニズムを用いて提供された入力（例えば、タッチスクリーンが受けた入力）を検出してよい。別の例として、電子デバイスは、デバイスの適切なセンサ（例えば、加速度計）によって検出された動き、接触、振動、または、その他の衝撃から入力を検出してもよい。かかる

方法において、ユーザは、デバイスの任意の部分（または、デバイスが置かれているテーブルなど、デバイスと接触する物体）をタップ（たたく）してよく、デバイスのセンサが、それらのタップを検出して、許可された時間的パターンに対応しているか否かを判定する。さらに別の例として、電子デバイスは、デバイスのセンサ（例えば、加速度計またはジャイロスコープ）を用いて、特定の方法（例えば、２回振った後に回転させる、など）で動かされたことを検出してよい。正確な時間的パターンの検出に応答して、電子デバイスは、制限されたリソースへのアクセスを提供してよい。

【００７５】

一部の実施形態において、認証システムは、認証のための時間的パターンおよび視覚的パターンを組み合わせてもよい。例えば、ユーザは、或る特定の速度（例えば、最初の２つの図形を素早く、次いで、休止した後に、最後の２つを同時に選択）で、特定の表示された図形を選択するよう要求されてよい。別の例として、ユーザは、最初に適切な図形を選択し、次いで時間的パターンの入力を提供するよう要求されてもよい。さらに別の例として、ユーザは、１または複数の図形を選択し、デバイスを動かす（例えば、デバイスを振る）よう要求されてもよい。任意の他の適切な組み合わせの入力が、認証のために要求されてもよい。

【００７６】

電子デバイスは、任意の適切な方法を用いて、許可ユーザに対して視覚的または時間的パターンを設定してよい。一部の実施形態において、ユーザが、特定のデバイスリソースへのアクセスを制限するために時間的または視覚的パターンを用いると選択した場合、電子デバイスは、時間的または視覚的パターンを提供または選択するようユーザに指示してよい。例えば、電子デバイスは、ユーザがパターンを形成するために選択できる図形の属性（例えば、色または輪郭）のリストを提供してよい。別の例として、電子デバイスは、表示された図形を選択するか時間的パターンを提供するようユーザに指示して、受信した入力からパターンを抽出または特定してもよい。電子デバイスは、ユーザが、意図的に行ったこと、および、選択したパターンを記憶していることを保証するために、パターンを受け付ける前に複数回提供するようユーザに指示してもよい。

【００７７】

電子デバイスは、任意の適切な数およびタイプの認証システムを備えてよい。例えば、電子デバイスは、上述の認証システムまたは認証方法の内の１つ、複数、または、すべてを備えてよい。様々なリソースへのアクセスが、１または複数の認証システムを用いて制限されてよく、用いられる認証システムは、ユーザが選択または設定してよい。一部の実施形態において、特定の制限されたリソースへのアクセスが提供される前に、複数の認証システムが連続的に用いられてもよい。

【００７８】

図１５は、本発明の一実施形態に従って、ユーザを認証するための方法の一例を示すフローチャートである。処理１５００は工程１５０２で始まる。工程１５０４で、電子デバイスは、デバイスのユーザを特定してよい。例えば、電子デバイスは、ユーザに関連づけられたユーザ名またはパスワードを受信してよい。別の例として、電子デバイスは、認証システムを用いて認証情報を受信し、受信した認証システムからユーザを特定してもよい。電子デバイスは、例えば、ユーザがデバイスを操作する時に認証情報をシームレスに取得できるように認証システムのセンサを配置することによって、ユーザからの明示的な入力を要求することなく、認証情報を自動的に受信しうる。別の例として、センサは、ユーザがセンサの視野すなわち検知領域内に入るとすぐに、ユーザの属性の特徴を検出するよう動作してもよい。一部の実施形態において、処理１５００は、工程１５０２から工程１５０６に直接移行してもよい。

【００７９】

工程１５０６で、電子デバイスは、制限されたリソースへのアクセス要求が受信されたか否かを判定してよい。例えば、電子デバイスは、ユーザが、特定のユーザに関連づけられたデータ（例えば、連絡先リストまたは他の個人情報）にアクセスするための命令を提

供したか否かを判定してよい。別の例として、電子デバイスは、ユーザが、制限されたアプリケーション（例えば、管理者などの特定の階層のユーザに制限されたアプリケーション、または、特定のユーザが購入したアプリケーション）にアクセスするための命令を提供したか否かを判定してもよい。制限されたリソースにアクセスするための命令を受信していないと、電子デバイスが判定した場合、処理１５００は、工程１５０６に戻って、ユーザから受ける入力を監視し続けてよい。

【００８０】

一方、工程１５０６で、制限されたリソースにアクセスするための命令を受信したと、電子デバイスが判定した場合、処理１５００は、工程１５０８に進んでよい。工程１５０８で、電子デバイスは、特定されたユーザがリソースへのアクセスを許可されているか否かを判定してよい。例えば、電子デバイスは、ユーザが、制限されたリソースにアクセスするのに適切な認証情報を提供したか否かを判定してよい。電子デバイスは、例えば、通常の使用中に認証情報を取得できるように、デバイスに認証センサを内蔵することによって、ユーザの知るところなく、適切な認証情報を取得してよい。特定されたユーザが許可されていないと、電子デバイスが判定した場合、処理１５００は、工程１５１０に進んでよい。工程１５１０で、電子デバイスは、認証を行うようユーザに指示してよい。例えば、電子デバイスは、認証システム（例えば、上述の認証システムのいずれか）に認証情報を提供するようユーザに指示してよい。一部の実施形態において、電子デバイスは、ユーザによる複数の入力を検出し、それらの入力が、許可ユーザに関連づけられたパターンを有しているか否か、または、許可ユーザに関連づけられた属性を共有しているか否かを判定してよい（例えば、ユーザが、許可ユーザの属性またはパターンに対応する適切な入力を提供したか否かを判定する、または、入力の属性またはパターンが、許可ユーザに関連づけられた属性またはパターンと適合するか否かを判定する）。次いで、処理１５００は、ユーザが適切な認証情報を提供したか否かを判定する工程１５０８に戻ってよい。

【００８１】

一方、工程１５０８で、ユーザが許可されていると、電子デバイスが判定した場合、処理１５００は、工程１５１２に進んでよい。工程１５１２で、電子デバイスは、要求された制限されたリソースへのアクセスをユーザに提供してよい。例えば、電子デバイスは、個人データへのアクセスまたはユーザに固有のアプリケーションへのアクセスをユーザに提供してよい。次いで、処理１５００は、工程１５１４で終了してよい。

【００８２】

上述の本発明の実施形態は、限定ではなく例示の目的としたものであり、本発明は、以下の特許請求の範囲によってのみ限定される。

【図１】

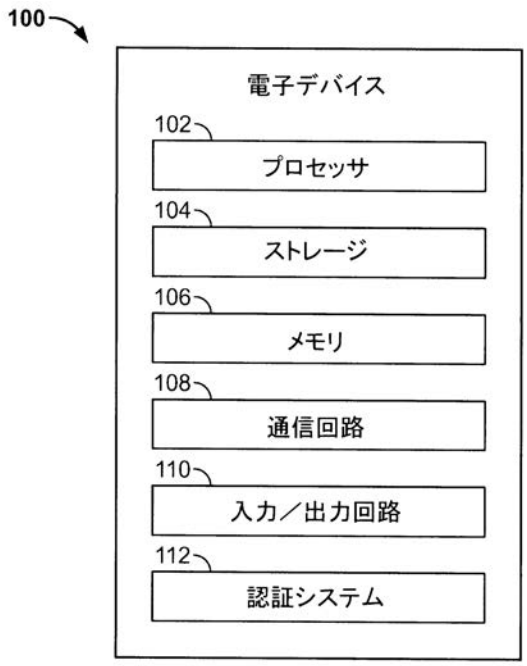

FIG. 1

【図２】

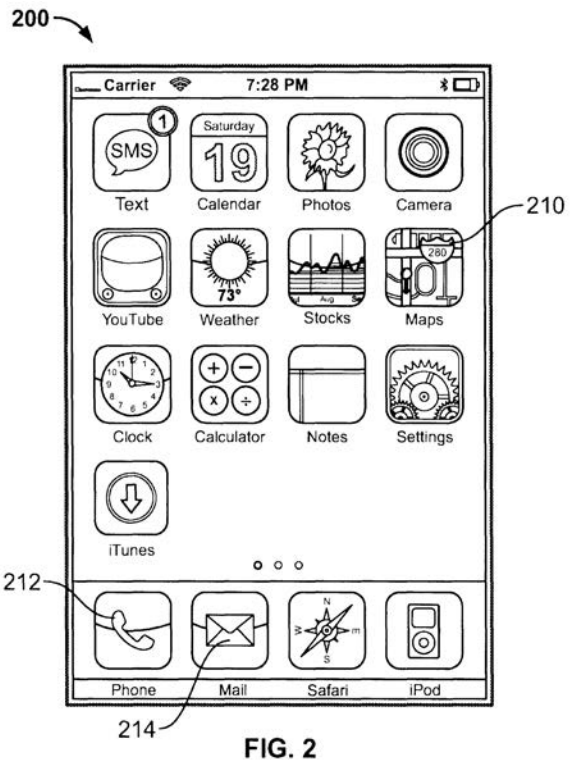

FIG. 2

【図３】

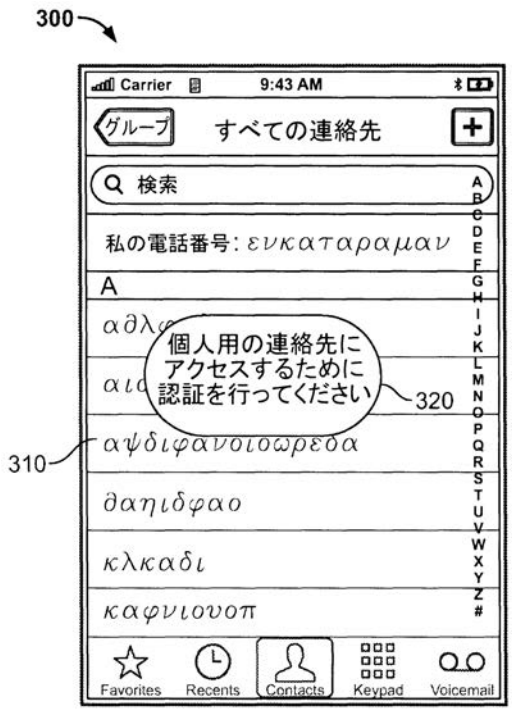

FIG. 3

【図４】

FIG. 4

【図５Ａ】

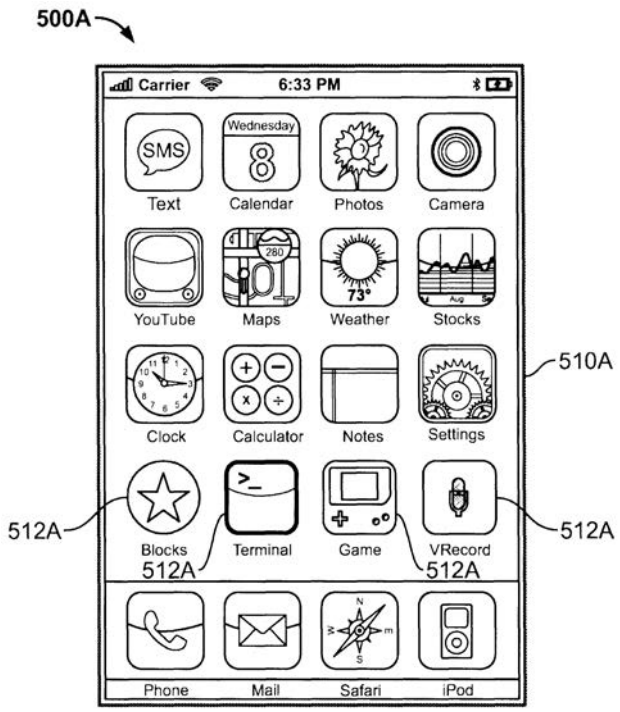

FIG. 5A

【図５Ｂ】

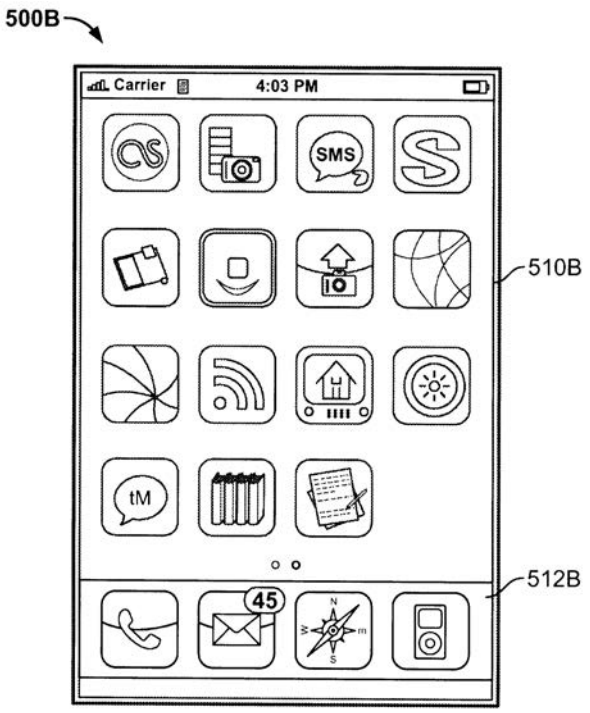

FIG. 5B

【図５Ｃ】

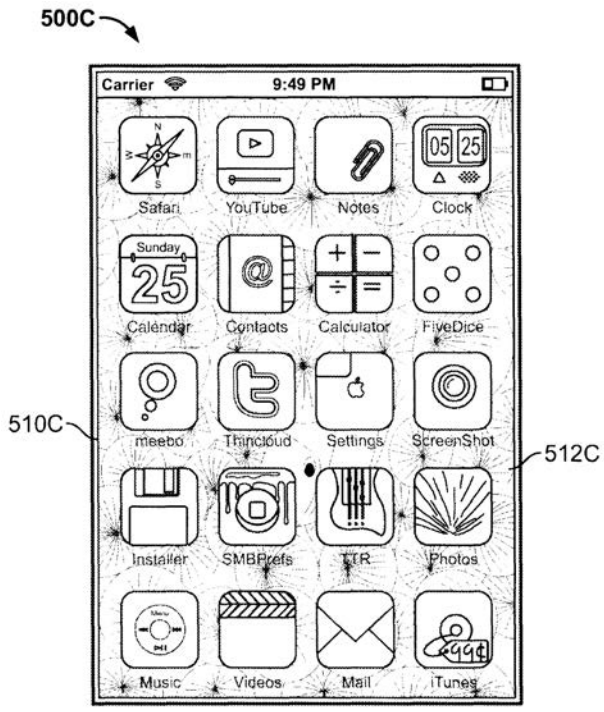

FIG. 5C

【図６】

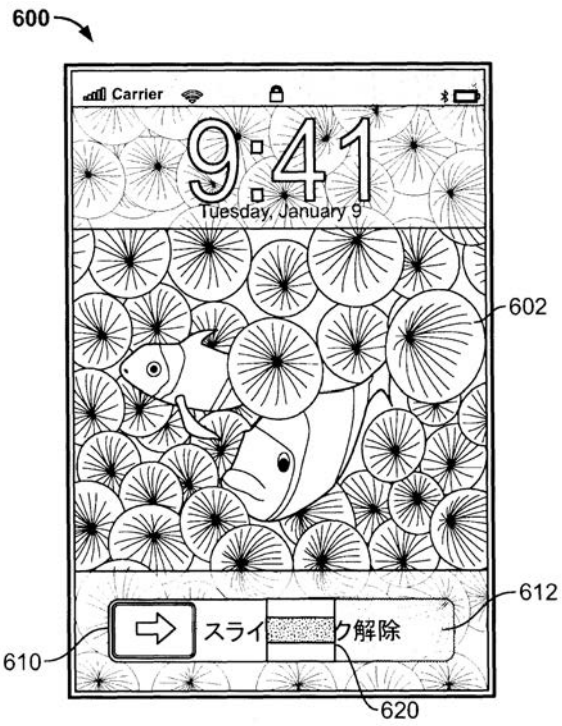

FIG. 6

【図７】

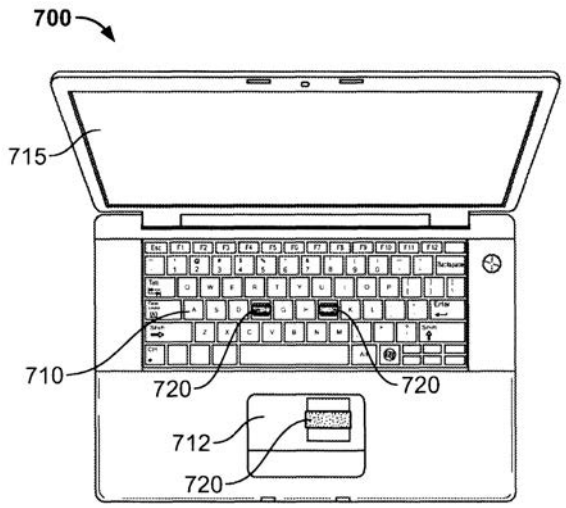

FIG. 7

【図８Ａ】

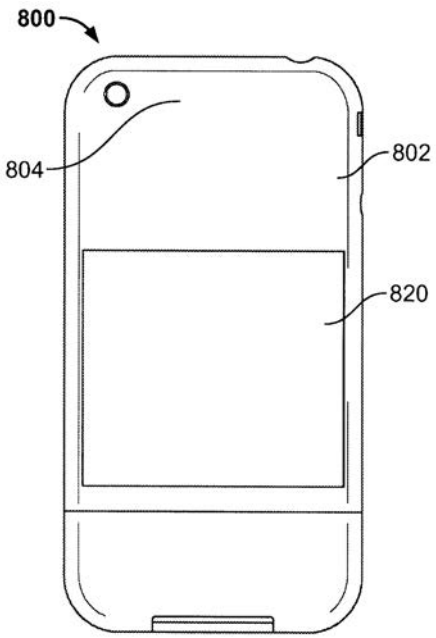

FIG. 8A

【図８Ｂ】

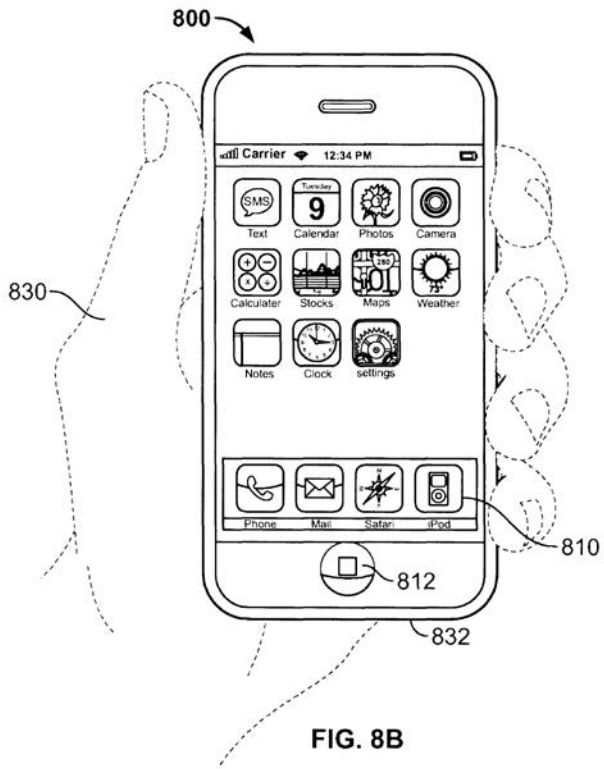

FIG. 8B

【図９】

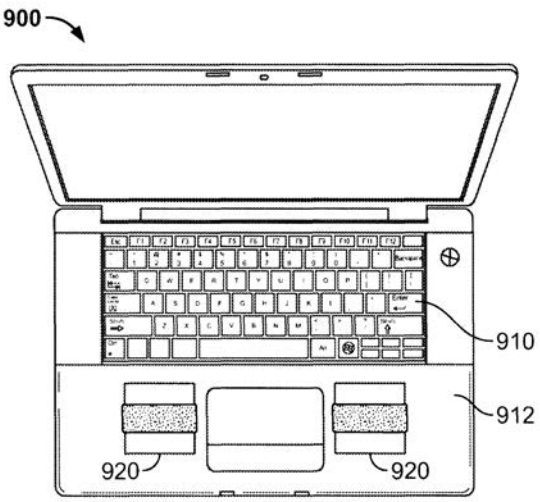

FIG.9

【図１０】

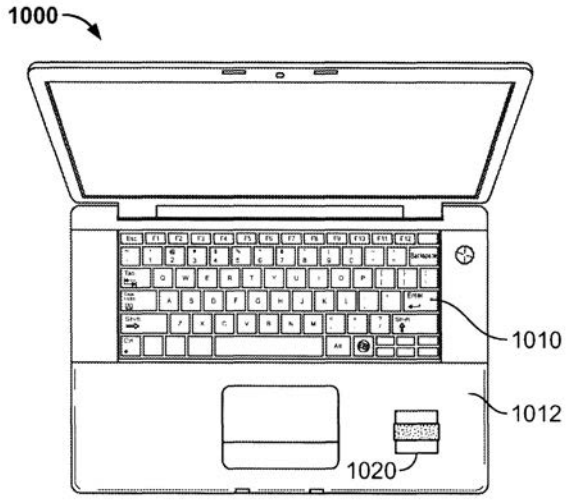

FIG. 10

【図１１】

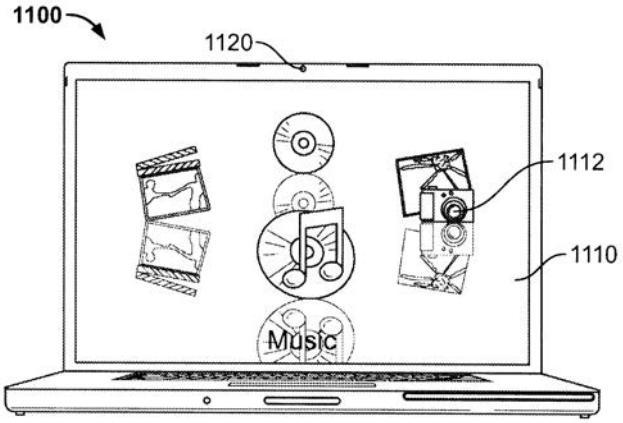

FIG. 11

【図１２】

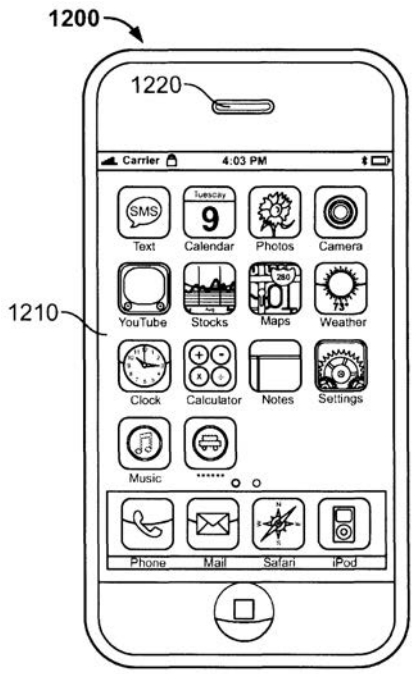

FIG.12

【図１３】

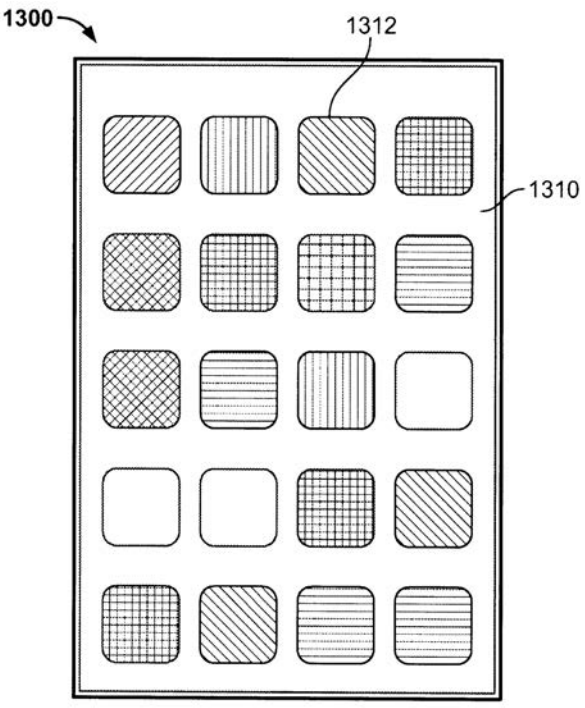

FIG.13

【図１４】

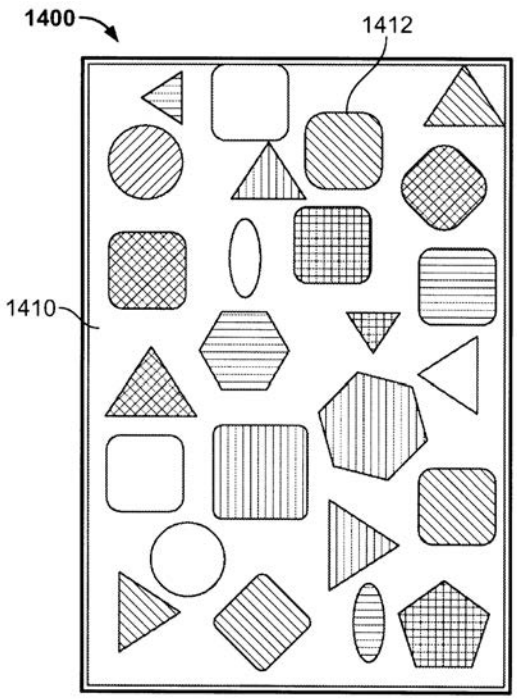

FIG.14

【図１５】

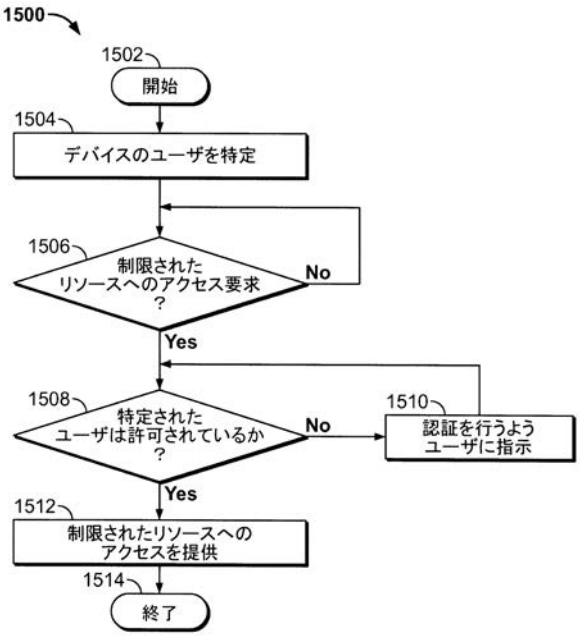

FIG. 15

【手続補正書】
【提出日】平成29年5月12日(2017.5.12)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ディスプレイと１つ以上のイメージセンサとを有する電子デバイスにおいて、
前記ディスプレイにロック画面を表示することと、
前記１つ以上のイメージセンサから画像データを取り込むことと、
前記取り込まれた画像データからユーザの顔の１つ以上の属性を検出することと、
前記取り込まれた画像データからの前記１つ以上の属性に基づいて前記ユーザを認証することと、
前記ユーザを認証したことに応じて、前記ロック画面の表示を前記ディスプレイでのロック解除されたユーザインタフェースの表示に置き換えることと
を有する方法。
【請求項２】
前記１つ以上の画像センサは、可視光イメージセンサを含む、請求項１に記載の方法。
【請求項３】
前記１つ以上のイメージセンサは、可視光スペクトル外の光を検出するイメージセンサを含む、請求項１に記載の方法。
【請求項４】
前記１つ以上のイメージセンサは、赤外線イメージセンサを含む、請求項３に記載の方

法。
【請求項５】
前記１つ以上のイメージセンサは、可視光イメージセンサと赤外線イメージセンサとを含む、請求項１に記載の方法。
【請求項６】
前記取り込まれた画像データは、前記可視光イメージセンサからのデータと前記赤外線イメージセンサからのデータとを含み、
１つ以上の属性を検出することは、前記可視光イメージセンサからの第１属性と前記赤外線イメージセンサからの第２属性とを検出することを含み、
前記１つ以上の属性に基づいて前記ユーザを認証することは、前記第１属性と前記第２属性とに基づいて前記ユーザを認証することを含む、請求項５に記載の方法。
【請求項７】
前記１つ以上のイメージセンサは、前記ユーザの顔の特徴物の深さを取り込むための３次元キャプチャデバイスを含む、請求項１に記載の方法。
【請求項８】
前記取り込まれた画像データは、前記ユーザの顔についての深さデータを含む、請求項１に記載の方法。
【請求項９】
１つ以上の属性を検出することは、前記深さデータから第３属性を検出することを含み、
前記１つ以上の属性に基づいて前記ユーザを認証することは、前記第３属性に基づいて前記ユーザを認証することを含む、請求項８に記載の方法。
【請求項１０】
ユーザの顔が前記１つ以上の画像センサに向かい合っていることを検出することを更に有し、前記画像データの取り込みは前記ユーザの顔を検出したことに応じて生じる、請求項１に記載の方法。
【請求項１１】
前記１つ以上の属性に基づいて前記ユーザを認証することは、認証されたユーザに関連するライブラリ内の属性に対して前記１つ以上の属性を比較することを含む、請求項１に記載の方法。
【請求項１２】
前記１つ以上のセンサは、紫外線センサ、スキャニングレーザ、超音波センサ又はこれらの組み合わせを含む、請求項１に記載の方法。
【請求項１３】
前記１つ以上の属性は、前記ユーザの眼窩、あご、鼻又はこれらの組み合わせの３次元輪郭を含む、請求項１に記載の方法。
【請求項１４】
前記電子デバイスは、前記ユーザの眼によって反射され前記１つ以上のセンサによって取り込まれる赤外光を照射するように動作する光源を含む、請求項１に記載の方法。
【請求項１５】
前記ロック解除されたユーザインタフェースは、相異なるアプリケーションを起動するための複数のアプリケーションアイコンを含むアプリケーション起動ユーザインタフェースである、請求項１に記載の方法。
【請求項１６】
ディスプレイと、
１つ以上のイメージセンサと、
１つ以上のプロセッサと、
前記１つ以上のプロセッサによって実行されるように構成された１つ以上のプログラムを格納するメモリとを備えた電子デバイスであって、前記１つ以上のプログラムは、
前記ディスプレイにロック画面を表示することと、

前記１つ以上のイメージセンサから画像データを取り込むことと、
前記取り込まれた画像データからユーザの顔の１つ以上の属性を検出することと、
前記取り込まれた画像データからの前記１つ以上の属性に基づいて前記ユーザを認証することと、
前記ユーザを認証したことに応じて、前記ロック画面の表示を前記ディスプレイでのロック解除されたユーザインタフェースの表示に置き換えることと
のための命令を含む、電子デバイス。
【請求項１７】
前記１つ以上の画像センサは、可視光イメージセンサを含む、請求項１６に記載の電子デバイス。
【請求項１８】
前記１つ以上のイメージセンサは、可視光スペクトル外の光を検出するイメージセンサを含む、請求項１６に記載の電子デバイス。
【請求項１９】
前記１つ以上のイメージセンサは、赤外線イメージセンサを含む、請求項１８に記載の電子デバイス。
【請求項２０】
前記１つ以上のイメージセンサは、可視光イメージセンサと赤外線イメージセンサとを含む、請求項１６に記載の電子デバイス。
【請求項２１】
前記取り込まれた画像データは、前記可視光イメージセンサからのデータと前記赤外線イメージセンサからのデータとを含み、
１つ以上の属性を検出することは、前記可視光イメージセンサからの第１属性と前記赤外線イメージセンサからの第２属性とを検出することを含み、
前記１つ以上の属性に基づいて前記ユーザを認証することは、前記第１属性と前記第２属性とに基づいて前記ユーザを認証することを含む、請求項２０に記載の電子デバイス。
【請求項２２】
前記１つ以上のイメージセンサは、前記ユーザの顔の特徴物の深さを取り込むための３次元キャプチャデバイスを含む、請求項１６に記載の電子デバイス。
【請求項２３】
前記取り込まれた画像データは、前記ユーザの顔についての深さデータを含む、請求項１６に記載の電子デバイス。
【請求項２４】
１つ以上の属性を検出することは、前記深さデータから第３属性を検出することを含み、
前記１つ以上の属性に基づいて前記ユーザを認証することは、前記第３属性に基づいて前記ユーザを認証することを含む、請求項２３に記載の電子デバイス。
【請求項２５】
前記１つ以上のプログラムは、ユーザの顔が前記１つ以上の画像センサに向かい合っていることを検出するための命令を更に有し、前記画像データの取り込みは前記ユーザの顔を検出したことに応じて生じる、請求項１６に記載の電子デバイス。
【請求項２６】
前記１つ以上の属性に基づいて前記ユーザを認証することは、認証されたユーザに関連するライブラリ内の属性に対して前記１つ以上の属性を比較することを含む、請求項１６に記載の電子デバイス。
【請求項２７】
前記１つ以上のセンサは、紫外線センサ、スキャニングレーザ、超音波センサ又はこれらの組み合わせを含む、請求項１６に記載の電子デバイス。
【請求項２８】
前記１つ以上の属性は、前記ユーザの眼窩、あご、鼻又はこれらの組み合わせの３次元

輪郭を含む、請求項１６に記載の電子デバイス。
【請求項２９】
前記ユーザの眼によって反射され前記１つ以上のセンサによって取り込まれる赤外光を照射するように動作する光源を更に備える、請求項１６に記載の電子デバイス。
【請求項３０】
前記ロック解除されたユーザインタフェースは、相異なるアプリケーションを起動するための複数のアプリケーションアイコンを含むアプリケーション起動ユーザインタフェースである、請求項１６に記載の電子デバイス。
【請求項３１】
ディスプレイと１つ以上のイメージセンサとを有する電子デバイスによって実行された場合に、前記電子デバイスに請求項１乃至１５の何れか１項に記載の方法を実行させる命令を有するプログラム。

フロントページの続き

(74)代理人 100134175
弁理士 永川 行光
(72)発明者 ファデル・アンソニー
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１
(72)発明者 ホッジ・アンドリュー
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１
(72)発明者 シェル・スティーブン
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１
(72)発明者 カバレロ・ルーベン
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１
(72)発明者 ドログスカー・ジェシー リー
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１
(72)発明者 ザデスキー・スティーブン
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１
(72)発明者 サンフォード・エメリー
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ，インフィニット・ループ，１

Ｆターム(参考) 5B043 AA04 BA02 BA03 BA04 BA07 DA05 DA07 EA05 FA07 GA18
5B047 AA23 BA02 BB04

【外国語明細書】
2017162489000001.pdf