(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2017-531237
(P2017-531237A)
(43)公表日　平成29年10月19日(2017.10.19)

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

審査請求 未請求　予備審査請求 有　（全 86 頁）

(21)出願番号	特願2017-507700 (P2017-507700)
(86)(22)出願日	平成27年8月4日 (2015.8.4)
(85)翻訳文提出日	平成29年4月10日 (2017.4.10)
(86)国際出願番号	PCT/US2015/043539
(87)国際公開番号	WO2016/025227
(87)国際公開日	平成28年2月18日 (2016.2.18)
(31)優先権主張番号	62/037,047
(32)優先日	平成26年8月13日 (2014.8.13)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	14/577,878
(32)優先日	平成26年12月19日 (2014.12.19)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	14/583,465
(32)優先日	平成26年12月26日 (2014.12.26)
(33)優先権主張国	米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100112807
弁理士　岡田　貴志

最終頁に続く

(54)【発明の名称】多因子のキャンセル可能なバイオメトリックデータに基づく認証

(57)【要約】
アクセスを選択的に認証する方法は、認証デバイスにおいて、第１の合成バイオメトリックデータに対応する第１の情報を取得することを含む。方法はまた、認証デバイスにおいて、第１の共通合成データと第２のバイオメトリックデータとを取得することを含む。方法はさらに、認証デバイスにおいて、第１の情報および第２のバイオメトリックデータに基づいて第２の共通合成データを生成することを含む。方法はまた、認証デバイスによって、第１の共通合成データと第２の共通合成データの比較に基づいてアクセスを選択的に認証することを含む。
【選択図】図５

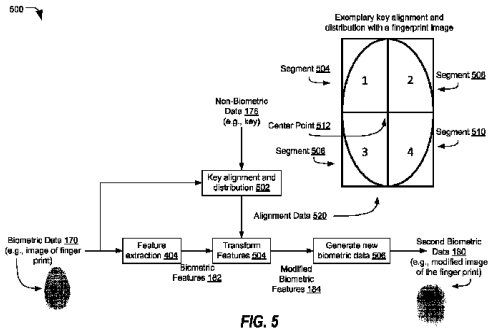

FIG. 5

【特許請求の範囲】
【請求項１】
ユーザからバイオメトリックデータを受信するように構成されたセンサと、
前記ユーザから非バイオメトリックデータを受信するように構成された入力インターフェースと、
合成バイオメトリックデータを生成するように構成されたプロセッサ、ここにおいて、前記合成バイオメトリックデータは、前記非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
ネットワークを介して、前記ユーザを認証するために、認証サーバに前記合成バイオメトリックデータを送信するように構成されたネットワークインターフェースと
を備える、装置。
【請求項２】
前記センサは、指紋スキャナを備え、前記バイオメトリックデータは、前記ユーザの指紋を備える、
請求項１に記載の装置。
【請求項３】
前記センサは、虹彩スキャナを備え、前記バイオメトリックデータは、前記ユーザの虹彩スキャンを備える、
請求項１に記載の装置。
【請求項４】
前記センサは、マイクロフォンを備え、前記バイオメトリックデータは、前記ユーザの発話信号を備える、
請求項１に記載の装置。
【請求項５】
前記センサは、カメラを備え、前記バイオメトリックデータは、前記ユーザの顔画像を備える、
請求項１に記載の装置。
【請求項６】
前記非バイオメトリックデータは、英数字鍵を備える、
請求項１に記載の装置。
【請求項７】
前記合成バイオメトリックデータは、合成指紋、合成虹彩スキャン、合成発話信号、合成画像、またはこれらの任意の組み合わせを備える、
請求項１に記載の装置。
【請求項８】
前記ネットワークインターフェースは、前記認証サーバが前記合成バイオメトリックデータに基づいて前記ユーザを認証するとき、前記ネットワークを介して別の電子デバイスと認証されたセッションを行うようにさらに構成される、
請求項１に記載の装置。
【請求項９】
前記バイオメトリックデータは、前記合成バイオメトリックデータから非復元可能である、
請求項１に記載の装置。
【請求項１０】
前記バイオメトリックデータは、第１の領域内にあり、前記非バイオメトリックデータは、前記第１の領域と異なる第２の領域内にある、
請求項１に記載の装置。
【請求項１１】
前記第１の領域は、オーディオ領域または画像領域のうちの１つに対応し、前記第２の領域は、前記オーディオ領域または前記画像領域のうちのもう一方に対応する、

請求項１０に記載の装置。
【請求項１２】
前記ネットワークインターフェースは、基本電話サービス（ＰＯＴＳ）インターフェースに対応し、前記合成バイオメトリックデータは、ＰＯＴＳ互換オーディオ信号として送信される、
請求項１に記載の装置。
【請求項１３】
デバイスにおいて、ユーザからバイオメトリックデータを受信することと、
前記デバイスにおいて、前記ユーザから第１の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第１の合成バイオメトリックデータを生成すること、ここにおいて、前記第１の合成バイオメトリックデータは、前記デバイスにおいて、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
ネットワークを介して前記デバイスから第１の認証サーバに、前記ユーザを認証するために前記第１の合成バイオメトリックデータを送信することと
を備える、方法。
【請求項１４】
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータは、前記第２の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
前記ユーザを認証するために、前記デバイスから第２の認証サーバに、前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１３に記載の方法。
【請求項１５】
前記第１の認証サーバは、前記ユーザに対応する認証データとして前記第１の合成バイオメトリックデータを記憶するように構成され、前記認証データと受信した合成バイオメトリックデータを比較することによって前記ユーザを認証するように構成される、
請求項１３に記載の方法。
【請求項１６】
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータを生成することは、前記第２の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
前記デバイスから前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信すること、ここにおいて、前記第２の合成バイオメトリックデータは、前記ユーザに対応する前記認証データとして前記第１の合成バイオメトリックデータを置き換える、と
をさらに備える、請求項１５に記載の方法。
【請求項１７】
プロセッサによって実行されると、前記プロセッサに、
ユーザからバイオメトリックデータを受信することと、
前記ユーザから第１の非バイオメトリックデータを受信することと、
第１の合成バイオメトリックデータを生成すること、ここにおいて、前記第１の合成バイオメトリックデータを生成することは、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
ネットワークを介して、前記ユーザを認証するために、第１の認証サーバに前記第１の合成バイオメトリックデータを送信することと

を備える、動作を実行させる命令を記憶した、コンピュータ可読記憶デバイス。
【請求項１８】
前記動作は、
前記バイオメトリックデータの特徴を抽出することと、
メモリに前記特徴を記憶することと
をさらに備え、前記第１の合成バイオメトリックデータは、前記第１の非バイオメトリックデータに基づいて前記特徴を修正することによって生成される、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項１９】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記第２の非バイオメトリックデータに基づいて前記特徴を修正することによって第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
を備え、前記第２の合成バイオメトリックデータは、前記ユーザに対応する認証データとして、前記第１の認証サーバにおいて、前記第１の合成バイオメトリックデータを置き換える、
請求項１８に記載のコンピュータ可読記憶デバイス。
【請求項２０】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れになったと決定することに応答して、第２のバイオメトリックデータを提供するように前記ユーザに促すことと、
前記ユーザから前記第２のバイオメトリックデータを受信することと、
前記第２のバイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２１】
前記動作は、前記バイオメトリックデータが第１のタイムスタンプに基づいて期限切れになったことかどうかを決定することをさらに備え、前記第１のタイムスタンプは、前記バイオメトリックデータが前記ユーザから受信される第１の時間、または前記バイオメトリックデータがメモリに記憶される第２の時間を示す、
請求項２０に記載のコンピュータ可読記憶デバイス。
【請求項２２】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れでないと決定することに応答して、前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
を備える、請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２３】
前記第１の非バイオメトリックデータは、第１の電子デバイスと関連付けられ、前記第１の合成バイオメトリックデータは、前記ユーザおよび前記第１の電子デバイスと関連付けられる第１の認証データに対応する、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２４】
前記動作は、
前記ユーザから第２の電子デバイスに関連付けられた第２の非バイオメトリックデータ

を受信することと、
前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備え、前記第２の合成バイオメトリックデータは、前記ユーザおよび前記第２の電子デバイスと関連付けられた第２の認証データに対応する、
請求項２３に記載のコンピュータ可読記憶デバイス。
【請求項２５】
前記第１の認証サーバは、建物のセキュリティシステム、または前記建物の温度制御器と関連付けられる、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２６】
前記第１の合成バイオメトリックデータは、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータに一方向性関数を適用することによって生成される、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２７】
前記一方向性関数は、ハッシュ関数、指数関数、剰余関数、双曲線正接関数、または別の双曲線関数のうちの少なくとも１つを含む、
請求項２６に記載のコンピュータ可読記憶デバイス。
【請求項２８】

ユーザからバイオメトリックデータを受信するための手段と、
前記ユーザから非バイオメトリックデータを受信するための手段と、
前記非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することによって合成バイオメトリックデータを生成するための手段と、
ネットワークを介して、前記ユーザを認証するために認証サーバに前記合成バイオメトリックデータを送信するための手段と
を備える、装置。
【請求項２９】
前記バイオメトリックデータを受信するための手段は、バイオメトリックセンサを含み、非バイオメトリックデータを前記受信するための手段は、ユーザ入力デバイスを含み、前記生成するための手段は、プロセッサを含み、前記送信するための手段は、ネットワークインターフェースを含む、
請求項２８に記載の装置。
【請求項３０】
バイオメトリックデータを前記受信するための手段、非バイオメトリックデータを前記受信するための手段、合成バイオメトリックデータを前記生成するための手段、および合成バイオメトリックデータを前記送信するための手段は、通信デバイス、携帯情報端末（ＰＤＡ）、タブレット、コンピュータ、音楽プレーヤー、ビデオプレーヤー、エンターテインメントユニット、ナビゲーションデバイス、またはセットトップボックスのうちの少なくとも１つに組み込まれる、
請求項２９に記載の装置。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
[0001]本出願は、その内容全体が参照により本明細書に明確に組み込まれる、同一出願人が所有する、２０１４年８月１３日に出願された米国仮特許出願第６２／０３７，０４７号、２０１４年１２月１９日に出願された米国本特許出願第１４／５７７，８７８号、および２０１４年１２月２６日に出願された米国本特許出願１４／５８３，４６５号の優先権を主張する。

【技術分野】
【０００２】
[0002]本開示は全般に、合成バイオメトリックデータおよび非バイオメトリックデータに基づくアクセス認証に関する。
【背景技術】
【０００３】
[0003]技術の進歩により、コンピューティングデバイスは、より小型でより強力になった。たとえば、携帯電話およびスマートフォンなどのワイヤレス電話、タブレット、ラップトップコンピュータを含む、小型で、軽量で、ユーザにより容易に携行される様々なポータブルパーソナルコンピューティングデバイスが存在する。これらのデバイスは、ワイヤレスネットワークを介して音声とデータパケットを通信することができる。さらに、多くのそのようなデバイスは、デジタルスチルカメラ、デジタルビデオカメラ、デジタルレコーダ、およびオーディオファイルプレーヤーなどの、追加の機能を組み込む。また、そのようなデバイスは、インターネットにアクセスするのに使用され得るウェブブラウザアプリケーション、コンピュータセキュリティシステムなどのソフトウェアアプリケーションを含む、実行可能命令を処理することができる。したがって、これらのデバイスはかなりの計算能力を含み得る。
【０００４】
[0004]コンピュータセキュリティシステムは、テキストパスワードおよび／またはバイオメトリックパスワードに依存し得る。一般に、より長いテキストパスワードがより短いテキストパスワードよりセキュアであると考えられるが、長いテキストパスワードはユーザにとって覚えるのがより難しいことがある。バイオメトリックパスワード（たとえば、指紋、虹彩スキャンなど）は、ユーザにより記憶される必要はないが、構成不可能である（たとえば、固定されている）傾向がある。たとえば、ユーザは一般に、指紋を変える能力を有しない。セキュリティを向上させるために、パスワードは頻繁に変更されることが一般に推奨されている。構成不可能なバイオメトリックパスワードは変更され得ないので、危うくなるとしても、ユーザは構成不可能なバイオメトリックパスワードを止むを得ず使用することがある。
【発明の概要】
【０００５】
[0005]合成バイオメトリックデータを生成するためのシステムおよび方法が開示される。ある特定の例では、デバイス（たとえば、携帯電話、デスクトップコンピュータなど）が、登録フェーズの間にコンピュータセキュリティシステムのパスワードを設定またはリセットするために使用されてよく、または、認証フェーズの間にコンピュータセキュリティシステムにアクセスするために使用されてよい。例示すると、ユーザは、コンピュータセキュリティシステムの登録オプション（たとえば、アカウント作成オプション、パスワードリセットオプションなど）を選択することができる。代替的に、ユーザは、コンピュータセキュリティシステムの認証オプション（たとえば、アカウントアクセスオプション）を選択することができる。ユーザは、コンピュータセキュリティシステムへの電話呼の間に、デバイスのグラフィックユーザインターフェース（ＧＵＩ）を介して、またはデバイスのアプリケーションを介して、登録オプションまたは認証オプションを選択することができる。
【０００６】
[0006]コンピュータセキュリティシステムは、登録フェーズの間に（たとえば、登録オプションの選択に応答して）、または認証フェーズの間に（たとえば、認証オプションの選択に応答して）、パスワードを提供するためのオプションを（たとえば、電話呼の間に、ＧＵＩを介して、またはアプリケーションを介して）示すことができる。ユーザは、パスワードを提供するためのオプションに応答して、バイオメトリックデータ（指紋、虹彩スキャン、発話信号などの）をデバイスに提供することができる。たとえば、ユーザは、指紋を提供するために、指を指紋スキャナ（たとえば、カメラ）の上に、またはその近く

に置くことができる。別の例として、ユーザは、虹彩スキャンを提供するために、目を虹彩スキャナ（たとえば、カメラ）の上に、またはその近くに置くことができる。さらなる例として、ユーザは、発話信号を提供するために、マイクロフォンに向かってある語句（たとえば、「いち－に－さん－し」）を話すことができる。バイオメトリックデータは、画像データ（たとえば、虹彩スキャンまたは指紋）として、またはオーディオデータ（たとえば、発話信号）として提供され得る。

【０００７】

[0007]ユーザはまた、ユーザ入力（たとえば、パスワード）をデバイスに提供することができる。たとえば、ユーザは、キーボードまたはタッチスクリーン上でタイピングすることによって、ユーザ入力（たとえば、パスワード）を提供することができる。別の例として、ユーザは、身分証明（ＩＤ）カードをＩＤスキャナ（たとえば、カメラ）の上に、またはその近くに置くことによって、ユーザ入力（たとえば、識別子）を提供することができる。さらなる例として、ユーザは、マイクロフォンに向かって話す（たとえば、「いち－に－さん－し」）ことによって、ユーザ入力を提供することができる。ユーザ入力は、テキスト、画像データ（たとえば、パスワードのスキャンされた画像）、またはオーディオデータ（たとえば、「いち－に－さん－し」に対応する発話信号）として提供され得る。

【０００８】

[0008]デバイスは、ユーザ入力に基づいて鍵（たとえば、「１２３４」などの非バイオメトリックデータ）を生成することができる。たとえば、鍵は、ユーザ入力として受け取られたテキスト（たとえば、「１２３４」）に対応し得る。別の例として、デバイスは、鍵を生成するために、ユーザ入力（たとえば、「１２３４」という画像）に対する画像認識を実行することができる。さらなる例として、デバイスは、鍵を生成するために、ユーザ入力に対する発話認識（たとえば、「１２３４」に対応する発話信号）を実行することができる。ある特定の例では、デバイスは、鍵に基づいて複数の鍵値（たとえば、「１」、「２」、「３」、および「４」）を生成することができる。

【０００９】

[0009]デバイスは、バイオメトリックデータおよび鍵（たとえば、非バイオメトリックデータ）に基づいて認証データ（たとえば、合成バイオメトリックデータ）を生成することができる。たとえば、デバイスは、バイオメトリックデータの特徴を抽出することができる。デバイスは、鍵に基づいて特徴を修正することによって、修正された特徴を生成することができる。たとえば、デバイスは、特徴の各々と、複数の鍵値のうちの特定の鍵値との間の、特徴の一致を決定することができる。例示すると、特徴の一致は、特徴の第１のサブセットが複数の鍵値のうちの第１の鍵値（たとえば、「１」）に対応することを示すことがあり、特徴の第２のサブセットが複数の鍵値のうちの第２の鍵値（たとえば、「２」）に対応することを示すことがあり、以下同様である。特徴は、指紋スキャンのスパイク、虹彩スキャンの虹彩特徴、顔の画像の顔特徴、または発話信号の発話特徴を含み得る。デバイスは、特定の特徴と複数の鍵値のうちの対応する鍵値との積、比、和、または差に関数を適用することで特定の特徴（特定のスパイク、特定の虹彩特徴、特定の顔特徴、または特定の発話特徴）を修正することによって、修正された特徴を生成することができる。

【００１０】

[0010]デバイスは、修正された特徴に基づいて認証データ（たとえば、第２のバイオメトリックデータ、特定の画像、またはオーディオデータ）を生成することができる。たとえば、修正された特徴は、修正された指紋、修正された虹彩スキャン、修正された顔の画像、または修正された発話信号に対応し得る。デバイスは、修正された特徴に基づいて、第２のバイオメトリックデータ（たとえば、第２の指紋スキャン、第２の虹彩スキャン、第２の顔の画像、または第２の発話信号）を生成することができる。認証データは第２のバイオメトリックデータを含み得る。

【００１１】

[0011]ある特定の例では、デバイスは複数の画像のうちの第１の画像を選択することができる。第１の画像はバイオメトリックデータに基づいて選択され得る。デバイスは、鍵（たとえば、非バイオメトリックデータ）に基づいて第１の画像を修正することによって、第２の画像を生成することができる。たとえば、デバイスは、修正された特徴に基づいて第１の画像を選択することができ、回転関数、スケーリング関数、ぼかし関数（blurring function）、またはシェーディング関数のうちの少なくとも１つを適用することによって第２の画像を生成することができ、第１の画像の修正の程度は鍵に基づく。認証データは第２の画像を含み得る。

【００１２】

[0012]別の例では、デバイスは、鍵に基づいてバイオメトリックデータを変換する（たとえば、可聴化する）ことによって、オーディオデータを生成することができる。例示すると、デバイスは、バイオメトリックデータの特徴に基づいてスペクトルエンベロープを生成することができ、鍵に基づいて音符シーケンスを生成することができる。スペクトルエンベロープは、ユーザの声／発話の音質に対応し、またはそれを表し得る。オーディオデータは、スペクトルエンベロープと音符シーケンスとを含み得る。認証データはオーディオデータを含み得る。

【００１３】

[0013]デバイスは、コンピュータセキュリティシステムの認証デバイスに認証データを送信することができる。認証デバイスは、登録フェーズの間に、認証データをメモリに記憶することができる。認証デバイスは、認証フェーズの間に、認証データをメモリに以前に記憶された登録認証データと比較することができ、比較の結果に基づいてコンピュータセキュリティシステムへのアクセス権を選択的に提供することができる。

【００１４】

[0014]バイオメトリックデータは第１のフォーマット（たとえば、画像またはオーディオ）を有し得る。ユーザ入力（たとえば、非バイオメトリックデータ）は第２のフォーマット（たとえば、画像、オーディオ、またはテキスト）を有し得る。認証データは第３のフォーマット（たとえば、画像、オーディオ、またはテキスト）を有し得る。デバイスは、バイオメトリックデータとユーザ入力とを共通のフォーマット（たとえば、第３のフォーマット）に変換することによって、認証データを生成することができる。第１のフォーマットおよび第２のフォーマットは別個または同一であり得る。第３のフォーマットは、第１のフォーマットと、第２のフォーマットと、またはそれらの両方と、同じであってよく、もしくは別であってよい。

【００１５】

[0015]ある特定の例では、バイオメトリックデータは複数のタイプのバイオメトリックデータを含み得る。例示すると、バイオメトリックデータは、ユーザの指紋、虹彩スキャン、または発話信号のうちの少なくとも２つを含み得る。様々なタイプのバイオメトリックデータが、同じフォーマット（たとえば、画像またはオーディオ）または別のフォーマットを有し得る。デバイスは、バイオメトリックデータを共通のフォーマットに変換することができ、変換されたバイオメトリックデータを組み合わせることによって認証データを生成することができる。たとえば、バイオメトリックデータは、指紋（たとえば、画像データ）と発話信号（たとえば、オーディオデータ）とを含み得る。デバイスは、指紋を可聴化し、可聴化された指紋と発話信号を組み合わせることによって、認証データ（たとえば、オーディオデータ）を生成することができる。ある特定の例では、指紋は鍵（たとえば、非バイオメトリックデータ）に基づいて可聴化され得る。例示すると、デバイスは、第１の指紋に基づいてスペクトルエンベロープを生成することができ、鍵に基づいて音符シーケンスを生成することができ、可聴化された指紋は、スペクトルエンベロープと音符シーケンスとを含み得る。

【００１６】

[0016]ある特定の態様では、アクセスを選択的に認証する方法は、認証デバイスにおいて、第１の合成バイオメトリックデータに対応する第１の情報を取得することを含む。方

法はまた、認証デバイスにおいて、第１の共通合成データと第２のバイオメトリックデータとを取得することを含む。方法はさらに、認証デバイスにおいて、第１の情報および第２のバイオメトリックデータに基づいて第２の共通合成データを生成することを含む。方法はまた、認証デバイスによって、第１の共通合成データと第２の共通合成データの比較に基づいてアクセスを選択的に認証することを含む。

【００１７】

[0017]別の態様では、アクセスを選択的に認証するための装置はメモリとプロセッサとを含む。メモリは、命令を記憶するように構成される。プロセッサは、第１の情報および第２のバイオメトリックデータに基づいて第２の共通合成データを生成するための命令を実行するように構成される。第１の情報は第１の合成バイオメトリックデータに対応する。プロセッサはまた、第１の共通合成データと第２の共通合成データの比較に基づいて車両のシステムへのアクセスを選択的に認証するように構成される。

【００１８】

[0018]別の態様では、アクセスを選択的に認証するためのコンピュータ可読記憶デバイスは、プロセッサによって実行されると、プロセッサに、第１の合成バイオメトリックデータに対応する第１の情報を取得することと、第１の共通合成データと第２のバイオメトリックデータとを取得することとを含む動作を実行させる、命令を記憶する。動作はまた、第１の情報および第２のバイオメトリックデータに基づいて第２の共通合成データを生成することを含む。動作はさらに、第１の共通合成データと第２の共通合成データの比較に基づいてアクセスを選択的に認証することを含む。

【００１９】

[0019]開示される態様のうちの少なくとも１つによって提供される１つの具体的な利点は、認証データがバイオメトリックデータおよび非バイオメトリックデータに基づくということである。ユーザは、異なる非バイオメトリックデータを提供して異なる認証データを生成することによって、パスワードを変更することができる。バイオメトリックデータおよび非バイオメトリックデータに基づいて生成される認証データは、一般にバイオメトリックデータと関連付けられるより高いセキュリティと、一般に非バイオメトリックデータと関連付けられる構成可能性との両方の利点を有し得る。

【００２０】

[0020]本開示の他の態様、利点、および特徴は、以下のセクション、すなわち、図面の簡単な説明と、発明を実施するための形態と、特許請求の範囲とを含む本出願全体の検討の後に明らかになるであろう。

【図面の簡単な説明】

【００２１】

【図１】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するように動作可能なシステムの特定の説明のための実施形態のブロック図。

【図２】図１のシステムの認証データ生成器のある特定の実施形態の図。

【図３】図１のシステムの認証データ生成器の別の特定の実施形態の図。

【図４】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成する方法のある特定の実施形態の図。

【図５】第１のバイオメトリックデータおよび非バイオメトリックデータに基づいて第２のバイオメトリックデータを含む認証データを生成する方法のある特定の実施形態の図。

【図６】認証データを生成するためにある特定の画像を選択するように構成されるシステムのある特定の実施形態の図。

【図７】非バイオメトリックデータに基づいてバイオメトリックデータを可聴化することによって認証データを生成する方法のある特定の実施形態の図。

【図８】非バイオメトリックデータに基づいてバイオメトリックデータを可聴化することによってスペクトルエンベロープを生成するように構成されるシステムのある特定の実施形態の図。

【図９】指紋のスパイクのある特定の実施形態の図。

【図１０】バイオメトリックデータのアラインメントの図。
【図１１】認証データを生成するように構成されるシステムのある特定の実施形態の図。
【図１２】認証データを生成するように構成されるシステムの別の特定の実施形態の図。
【図１３】バイオメトリックデータに基づいて可聴化されたオーディオ信号を生成する方法のある特定の実施形態の流れ図。
【図１４】第１のバイオメトリックデータと第２のバイオメトリックデータとを共通のフォーマットに変換することによって認証データを生成する方法のある特定の実施形態の図。
【図１５】認証データを生成するように構成されるシステムの別の特定の実施形態の図。
【図１６】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するある特定の例示的な実施形態の流れ図。
【図１７】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するある特定の例示的な実施形態の流れ図。
【図１８】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するある特定の例示的な実施形態の流れ図。
【図１９】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成する方法のある特定の例示的な実施形態の流れ図。
【図２０】バイオメトリックデータに基づいて認証データを生成する方法のある特定の実施形態の流れ図。
【図２１】バイオメトリックデータに基づいて認証データを生成する方法の別の特定の実施形態の流れ図。
【図２２】バイオメトリックデータに基づいて認証データを生成する方法の別の特定の実施形態の流れ図。
【図２３】バイオメトリックデータに基づいて認証データを生成する方法の別の特定の実施形態の流れ図。
【図２４】バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するように構成されるシステムの別の特定の実施形態の図。
【図２５】バイオメトリックデータおよび非バイオメトリックデータに基づいてアクセスを選択的に認証するように構成されるシステムの特定の実施形態の図。
【図２６】バイオメトリックデータおよび非バイオメトリックデータに基づいてアクセスを選択的に認証するように構成されるシステムの別の特定の実施形態の図。
【図２７】図１のシステムを使用してバイオメトリックデータおよび非バイオメトリックに基づいて、認証データを生成すること、アクセスを選択的に認証すること、またはこれらの両方のためのデバイスのブロック図。
【発明を実施するための形態】
【００２２】
[0048]本明細書で説明される原理は、たとえば、認証データを生成するように構成されるヘッドセット、ハンドセット、または他のデバイスに適用され得る。文脈によって明確に限定されない限り、「信号」という用語は、本明細書では、ワイヤ、バス、または他の伝送媒体上で表されたメモリ位置（もしくは、メモリ位置のセット）の状態を含む、その通常の意味のいずれをも示すために使用される。文脈によって明確に限定されない限り、「生成すること（generating）」という用語は、本明細書では、計算すること（computing）または別様に作成すること（producing）などの、その通常の意味のいずれをも示すために使用される。文脈によって明確に限定されない限り、「算出すること（calculating）」という用語は、本明細書では、計算すること（computing）、評価すること（evaluating）、平滑化すること（smoothing）、および／または複数の値から選択すること（selecting）などの、その通常の意味のいずれも示すために使用される。文脈によって明確に限定されない限り、「取得すること（obtaining）」という用語は、算出すること（calculating）、導出すること（deriving）、（たとえば、別のコンポーネント、ブロック、もしくはデバイスから）受信すること（receiving）、および／または（たとえば、メモリ

レジスタもしくは記憶素子のアレイから）取り出すこと（retrieving）などの、その通常の意味のいずれも示すために使用される。

【００２３】

[0049]文脈によって明確に限定されない限り、「作成すること（producing）」という用語は、算出すること（calculating）、生成すること（generating）、および／または提供すること（providing）などの、その通常の意味のいずれも示すために使用される。文脈によって明確に限定されない限り、「提供すること（providing）」という用語は、算出すること（calculating）、生成すること（generating）、および／または作成すること（producing）などの、その通常の意味のいずれも示すために使用される。文脈によって明確に限定されない限り、「結合される（coupled）」という用語は、直接的または間接的な電気的接続または物理的接続を示すために使用される。接続が間接的である場合、「結合される（coupled）」構造の間に他のブロックまたはコンポーネントが存在し得ることが、当業者によりよく理解される。

【００２４】

[0050]「構成（configuration）」という用語は、具体的な文脈によって示されるように、方法、装置／デバイス、および／またはシステムに関して使用され得る。「備える（comprising）」という用語は、本明細書および特許請求の範囲において使用される場合、他の要素または動作を除外するものではない。（「ＡはＢに基づく」などの場合の）「に基づく」という用語は、（ｉ）「少なくとも～に基づく」（たとえば、「Ａは少なくともＢに基づく」）、および特定の文脈において適切な場合、（ｉｉ）「に等しい」（たとえば、「ＡはＢに等しい」）という場合を含む、その通常の意味のいずれも示すために使用される。「ＡがＢに基づく」が「に少なくとも基づく」を含むケース（ｉ）では、これは、ＡがＢに結合される構成を含み得る。同様に、「に応答して」という用語は、「に少なくとも応答して」を含む、その通常の意味のいずれも示すために使用される。同様に、「少なくとも１つ」という用語は、「１つまたは複数」を含む、その通常の意味のいずれも示すために使用される。同様に、「少なくとも２つ」という用語は、「２つ以上」を含む、その通常の意味のいずれも示すために使用される。（「Ａおよび／またはＢ」などの場合の）「および／または」という用語は、「ＡまたはＢ」、「ＡおよびＢ」、または「（ＡおよびＢ）ならびに（ＡまたはＢ）」を含む、その通常の意味のいずれも示すために使用される。

【００２５】

[0051]「装置」および「デバイス」という用語は、具体的な文脈によって別段に規定されていない限り、一般的に、互換的に使用される。別段に規定されていない限り、特定の特徴を有する装置の動作のいかなる開示も、類似の特徴を有する方法を開示すること（その逆も同様）がまた明確に意図され、特定の構成による装置の動作のいかなる開示も、類似の構成による方法を開示すること（その逆も同様）がまた明確に意図される。「方法」、「プロセス」、「手順」、および「技法」という用語は、具体的な文脈によって別段に規定されていない限り、一般的に、互換的に使用される。「要素」および「モジュール」という用語は、より大きい構成の一部分を示すために使用され得る。

【００２６】

[0052]本明細書で使用される「通信デバイス」という用語は、ワイヤレス通信ネットワークを介した音声および／またはデータの通信に使用され得る電子デバイスを指す。通信デバイスの例は、携帯電話、携帯情報端末（ＰＤＡ）、ハンドヘルドデバイス、ヘッドセット、ワイヤレスモデム、ラップトップコンピュータ、パーソナルコンピュータなどを含む。

【００２７】

[0053]図１を参照すると、バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するように動作可能なシステムのある特定の説明のための実施形態が開示されており、全体的に１００と指定されている。ある特定の実施形態では、システム１００の１つまたは複数のコンポーネントは、通信デバイス、携帯情報端末（ＰＤ

Ａ）、タブレット、コンピュータ、音楽プレーヤー、ビデオプレーヤー、エンターテインメントユニット、ナビゲーションデバイス、またはセットトップボックスに組み込まれる。

【００２８】

[0054]以下の説明では、図１のシステム１００によって実行される様々な機能が、いくつかのコンポーネントまたはモジュールによって実行されるものとして説明されることに留意されたい。しかし、このコンポーネントおよびモジュールという区分は、説明のためにすぎない。代替の実施形態では、特定のコンポーネントまたはモジュールによって実行される機能は、複数のコンポーネントまたはモジュールに分割され得る。その上、代替の実施形態では、図１の２つ以上のコンポーネントまたはモジュールが、単一のコンポーネントまたはモジュールに統合され得る。図１に示される各コンポーネントまたはモジュールは、ハードウェア（たとえば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）デバイス、特定用途向け集積回路（ＡＳＩＣ）、デジタルシグナルプロセッサ（ＤＳＰ）、コントローラなど）を使用して実装されることがあり、ソフトウェア（たとえば、プロセッサによって実行可能な命令）を使用して実装されることがあり、またはこれらの任意の組合せを使用して実装されることがある。

【００２９】

[0055]システム１００は、ネットワーク１２０を介して認証デバイス１０４に結合されるモバイルデバイス１０２を含む。図１の例では、認証デバイス１０４はハンドヘルドデバイスとして示されている。代替の実施形態では、認証デバイス１０４は、金融機関、ホームオートメーションシステム、クラウドコンピューティング／ストレージシステムなどと関連付けられる認証サーバなどの、認証サーバであり得る。モバイルデバイス１０２は、メモリ１３２に結合される認証データ生成器１１０を含む。モバイルデバイス１０２は、第１のインターフェース１３４、第２のインターフェース１３６、送受信機１４２、またはこれらの組合せを含み得る。認証デバイス１０４は、コンピュータセキュリティシステムと関連付けられ、またはそれに結合され得る。

【００３０】

[0056]動作の間に、ユーザ１０６は、コンピュータセキュリティシステム（たとえば、認証デバイス１０４）の登録オプションまたは認証オプションにアクセスすることができる。たとえば、ユーザ１０６は、登録オプションまたは認証オプションにアクセスするために、電話アクセスシステム、グラフィカルユーザインターフェース、インターネットのウェブサイト、および／またはモバイルデバイス１０２のアプリケーションを使用することができる。登録オプションの選択（たとえば、登録フェーズの間の）に応答して、または、認証オプションの選択（たとえば、認証フェーズの間の）に応答して、コンピュータセキュリティシステム（たとえば、認証デバイス１０４）は、パスワードを提供するためのオプションを示し得る。ユーザ１０６は、たとえばパスワードを提供するためのオプションに応答して、バイオメトリックデータ１７０（たとえば、指紋、虹彩スキャン、顔の画像、および／または発話信号）をモバイルデバイス１０２に提供することができる。たとえば、ユーザ１０６は、指紋を提供するために、モバイルデバイス１０２に結合された指紋スキャナ（たとえば、カメラ）の上に、またはその近くに指を置くことができる。

【００３１】

[0057]別の例として、ユーザ１０６は、虹彩スキャンを提供するために、モバイルデバイス１０２に結合された虹彩スキャナ（たとえば、カメラ）の上に、またはその近くに目を置くことができる。追加の例として、ユーザ１０６は、顔の画像を取り込むために、モバイルデバイス１０２に結合されたカメラを使用することができる。さらなる例として、ユーザは、発話信号を提供するために、モバイルデバイス１０２に結合されたマイクロフォンに向かってある語句（たとえば、「いち－に－さん－し」）を話すことができる。バイオメトリックデータ１７０は、画像データ（たとえば、虹彩スキャン、顔の画像、または指紋）またはオーディオデータ（たとえば、発話信号）を含み得る。ある特定の実施形態では、モバイルデバイス１０２は、１つまたは複数のインターフェース（たとえば、第

１のインターフェース１３４、第２のインターフェース１３６、または両方）を介してバイオメトリックデータ１７０を受信することができる。たとえば、第１のインターフェース１３４は、指紋スキャナ、虹彩スキャナ、カメラ、またはこれらの組合せに結合され得る。第２のインターフェース１３６はマイクロフォンに結合され得る。

【００３２】

[0058]ユーザ１０６はまた、ユーザ入力１７２（たとえば、パスワード）をモバイルデバイス１０２に提供することができる。たとえば、ユーザ１０６は、モバイルデバイス１０２に結合されたキーボードまたはタッチスクリーンにおいてタイピングすることによって、ユーザ入力１７２を提供することができる。別の例として、ユーザ１０６は、身分証明（ＩＤ）カードをモバイルデバイス１０２に結合されたＩＤスキャナ（たとえば、カメラ）の上に、またはその近くに置くことによって、ユーザ入力１７２（たとえば、識別子）を提供することができる。さらなる例として、ユーザ１０６は、モバイルデバイス１０２に結合されたマイクロフォンに向かって話す（たとえば、「いち－に－さん－し」）ことによって、ユーザ入力１７２を提供することができる。ユーザ入力１７２は、テキスト（たとえば、キーボードでタイピングされるパスワード）、画像データ（たとえば、パスワードのスキャンされた画像）、またはオーディオデータ（たとえば、「いち－に－さん－し」に対応する発話信号）を含み得る。

【００３３】

[0059]認証データ生成器１１０は、ユーザ入力１７２に基づいて鍵（たとえば、非バイオメトリックデータ１７６）を生成することができる。非バイオメトリックデータ１７６は英数字の鍵を含み得る。たとえば、非バイオメトリックデータ１７６（たとえば、「１２３４」）は、ユーザ入力として受け取られたテキスト（たとえば、「１２３４」）に対応し得る。別の例として、認証データ生成器１１０は、非バイオメトリックデータ１７６を生成するために、ユーザ入力１７２（たとえば、「１２３４」の画像）に対する画像認識を実行することができる。さらなる例として、認証データ生成器１１０は、非バイオメトリックデータ１７６を生成するために、ユーザ入力１７２（たとえば、「いち－に－さん－し」に対応する発話信号）に対する発話認識を実行することができる。ある特定の実施形態では、認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて複数の鍵値（たとえば、「１」、「２」、「３」、および「４」）を生成することができる。

【００３４】

[0060]ある特定の実施形態では、認証データ生成器１１０は、ユーザ入力１７２（たとえば、「いち－に－さん－し」に対応する発話信号）に対する話者認識を実行することができ、話者認識と関連付けられる話者信頼性スコアを決定することができる。認証データ生成器１１０は、ユーザ入力１７２（たとえば、「いち－に－さん－し」に対応する発話信号）に対する発話認識を実行することができ、発話認識と関連付けられるテキスト（たとえば、「１２３４」）を決定することができる。認証データ生成器１１０は、話者信頼性スコアおよびテキストに基づいて非バイオメトリックデータ１７６を決定することができる。認証データ生成器１１０は、ユーザ入力１７２、非バイオメトリックデータ１７６、または両方を、メモリ１３２に記憶することができる。

【００３５】

[0061]認証データ生成器１１０は、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて認証データ１７８を生成することができる。たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０のバイオメトリック特徴１８２を抽出することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいてバイオメトリック特徴１８２を修正することによって、修正されたバイオメトリック特徴１８４を生成することができる。たとえば、認証データ生成器１１０は、バイオメトリック特徴１８２の各々と、複数の鍵値のうちの特定の鍵値との間の、特徴の一致を決定することができる。例示すると、特徴の一致は、バイオメトリック特徴１８２の第１のサブセットが複数の鍵値のうちの第１の鍵値（たとえば、「１」）に対応することを

示すことがあり、バイオメトリック特徴１８２の第２のサブセットが複数の鍵値のうちの第２の鍵値（たとえば、「２」）に対応することを示すことがあり、以下同様である。バイオメトリック特徴１８２は、指紋スキャンのスパイク、虹彩スキャンの虹彩特徴、顔の画像の顔特徴、または発話信号の発話特徴を含み得る。認証データ生成器１１０は、特定の特徴（たとえば、特定のスパイク、特定の虹彩特徴、特定の顔特徴、または特定の発話特徴）を修正することによって、修正されたバイオメトリック特徴１８４を生成することができる。たとえば、認証データ生成器１１０は、特定の特徴と、複数の鍵値のうちの対応する鍵値との積、比、和、または差に一方向性関数を適用することによって、修正されたバイオメトリック特徴１８４の修正された特徴を生成するように、特定の特徴を修正することができる。一方向性関数は、ハッシュ関数、双曲線正接関数、または別の双曲線関数を含み得る。

【００３６】

[0062]認証データ生成器１１０は、修正されたバイオメトリック特徴１８４に基づいて認証データ１７８（たとえば、第２のバイオメトリックデータ１８０、第２の画像１９６、またはオーディオデータ１９８）を生成することができる。たとえば、修正されたバイオメトリック特徴１８４は、修正された指紋、修正された虹彩スキャン、修正された顔の画像、または修正された発話信号に対応し得る。認証データ生成器１１０は、図３～図４を参照して説明されたように、修正されたバイオメトリック特徴１８４に基づいて、第２のバイオメトリックデータ１８０（たとえば、第２の指紋スキャン、第２の虹彩スキャン、第２の顔の画像、または第２の発話信号）を生成することができる。認証データ生成器１１０は、第２のバイオメトリックデータ１８０をメモリ１３２に記憶することができる。バイオメトリックデータ１７０は、第２のバイオメトリックデータ１８０から「復元不可能（ｉｒｒｅｃｏｖｅｒａｂｌｅ）」または「非復元可能（ｎｏｎ－ｒｅｃｏｖｅｒａｂｌｅ）」であることがあり、それは、第２のバイオメトリックデータ１８０が、一方向性関数をバイオメトリックデータ１７０に適用することによって生成されるからであり、ここで一方向性関数の性質が、ある合理的な（たとえば、閾値の）時間の量以内での、第２のバイオメトリックデータ１８０からのバイオメトリックデータ１７０の復元を困難にし、非現実的にし、および／または不可能にする。

【００３７】

[0063]ある特定の実施形態では、認証データ生成器１１０は画像１９０の第１の画像１９４を選択することができる。第１の画像１９４はバイオメトリックデータ１７０に基づいて選択され得る。画像１９０は非バイオメトリック画像を含み得る。たとえば、画像１９０は、風景の画像、ランドマークの画像、漫画のキャラクターの画像、絵画の画像、ロゴの画像などを含み得る。

【００３８】

[0064]認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて第１の画像１９４を修正することによって、第２の画像１９６を生成することができる。たとえば、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４および画像マッピング１９２に基づいて第１の画像１９４を選択することができる。画像マッピング１９２は、様々なバイオメトリック特徴を画像１９０にマッピングすることができる。たとえば、画像マッピング１９２は、修正されたバイオメトリック特徴１８４が第１の画像１９４にマッピングすることを示し得る。画像マッピング１９２は、デフォルト値、ユーザ選好、または両方を含み得る。

【００３９】

[0065]認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて第１の画像１９４を修正することによって、第２の画像１９６を生成することができる。たとえば、認証データ生成器１１０は、図６を参照して説明されるように、非バイオメトリックデータ１７６に基づいて、回転関数、スケーリング関数、ノイズ関数、ぼかし関数、またはシェーディング関数のうちの少なくとも１つを第１の画像１９４に適用することによって、第２の画像１９６を生成することができる。第１の画像１９４の修正の程度は非バイ

オメトリックデータ１７６に基づき得る。認証データ生成器１１０は、第２の画像１９６をメモリ１３２に記憶することができる。

【００４０】

[0066]ある特定の実施形態では、認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいてバイオメトリックデータ１７０を可聴化する（たとえば、オーディオデータに変換する、または非オーディオデータを表すオーディオデータを生成する）ことによって、オーディオデータ１９８を生成することができる。たとえば、認証データ生成器１１０は、図３および図６～図７を参照して説明されるように、バイオメトリック特徴１８２に基づいてスペクトルエンベロープ１６０を生成することができ、非バイオメトリックデータ１７６に基づいて音符シーケンス１６２を生成することができる。オーディオデータ１９８は、スペクトルエンベロープ１６０と音符シーケンス１６２とを含み得る。認証データ生成器１１０は、オーディオデータ１９８をメモリ１３２に記憶することができる。

【００４１】

[0067]ある特定の実施形態では、認証データ生成器１１０は、バイオメトリックデータ１７０、ユーザ入力１７２、または両方を、メモリ１３２に記憶するのを控えることができる。ある特定の実施形態では、認証データ生成器１１０は、認証データ１７８を生成した後で、バイオメトリックデータ１７０、ユーザ入力１７２、または両方を、メモリ１３２から除去する（たとえば、削除のためにマークする）ことができる。

【００４２】

[0068]認証データ生成器１１０は、認証データ１７８をユーザ１０６に提供することができる。たとえば、認証データ生成器１１０は、モバイルデバイス１０２に結合されたディスプレイデバイスにおいて認証データ１７８を表示することができ、または、モバイルデバイス１０２に結合されたスピーカーを介して認証データ１７８を出力することができる。ユーザ１０６は、認証データ１７８を受け入れる入力または拒絶する入力を提供することができる。認証データ生成器１１０は、認証データ１７８がユーザ１０６によって拒絶されることを示す入力を受け取ったことに応答して、バイオメトリックデータ１７０とユーザ入力１７２とを再び提供するようにユーザ１０６に促すことができ、認証データ１７８を再生成することができる。

【００４３】

[0069]認証データ生成器１１０は、送受信機１４２を介して、たとえば認証データ１７８がユーザ１０６によって受け入れられることを示す入力を受け取ったことに応答して、認証データ１７８を認証デバイス１０４に送信することができる。たとえば、認証データ生成器１１０は、コンピュータセキュリティシステムにパスワードを提供するためのオプションの選択として、認証データ１７８を認証デバイス１０４に提供することができる。認証データ生成器１１０は、送信の前に、特定の暗号化システム（たとえば、Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ（ＲＳＡ）アルゴリズム、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式、楕円曲線暗号化方式）に基づいて、認証データ１７８を暗号化することができる。ある特定の実施形態では、モバイルデバイス１０２および認証デバイス１０４は、認証されたデバイス１０４が認証データ１７８に基づいてユーザ１０６を認証するとき、認証されたセッションを行うことができる。データの符号化および認証されたセッションの実行はさらに、図２０～図２２を参照して説明される。

【００４４】

[0070]認証デバイス１０４は、登録フェーズの間に、認証データ１７８をメモリに記憶することができる。認証デバイス１０４は、認証フェーズの間に、認証データ１７８をメモリに以前に記憶された登録認証データと比較することができ、比較に基づいてコンピュータセキュリティシステムへのアクセス権を選択的に提供することができる。

【００４５】

[0071]ある特定の実施形態では、認証データ生成器１１０は、認証データ１７８を生成する前にバイオメトリックデータ１７０をアラインすることができる。たとえば、認証デ

ータ生成器１１０は、他のバイオメトリックデータ（たとえば、登録バイオメトリックデータ）へのアクセス権を有し得る。例示すると、認証データ生成器１１０は、登録フェーズの間にユーザ１０６から登録バイオメトリックデータを受け取ることができ、登録バイオメトリックデータに基づいて登録認証データを生成することができ、登録認証データを認証デバイス１０４に提供することができる。認証データ生成器１１０は、登録バイオメトリックデータをメモリ１３２に記憶することができる。認証データ生成器１１０は、認証フェーズの間にバイオメトリックデータ１７０を受信することができる。認証データ生成器１１０は、図１０を参照して説明されるように、認証データ１７８が登録認証データに対応する可能性を上げるために、認証データ１７８を生成する前に、バイオメトリックデータ１７０を登録バイオメトリックデータとアラインすることができる。

【００４６】

[0072]ある特定の実施形態では、バイオメトリックデータ１７０は第１のフォーマット（たとえば、画像またはオーディオ）を有し得る。ユーザ入力１７２は第２のフォーマット（たとえば、画像、オーディオ、またはテキスト）を有し得る。認証データ１７８は第３のフォーマット（たとえば、画像、オーディオ、またはテキスト）を有し得る。認証データ生成器１１０は、バイオメトリックデータ１７０とユーザ入力１７２とを共通のフォーマット（たとえば、第３のフォーマット）に変換することによって、認証データ１７８を生成することができる。第１のフォーマットおよび第２のフォーマットは別個または同一であり得る。第３のフォーマットは、第１のフォーマットと、第２のフォーマットと、またはそれらの両方と、同じであってよく、もしくは別であってよい。

【００４７】

[0073]たとえば、認証データ生成器１１０は、ある画像フォーマット（たとえば、指紋スキャン、虹彩スキャン、または顔の画像）のバイオメトリックデータ１７０を受信することができる。認証データ生成器１１０は、一方向性関数をバイオメトリック特徴１８２に適用することによって、修正されたバイオメトリック特徴１８４を生成することができる。認証データ生成器１１０は、修正されたバイオメトリック特徴１８４に基づいてバイオメトリックオーディオ１８６を生成することができる。たとえば、認証データ生成器１１０は、図７を参照して説明されるように、オーディオデータ１９８を生成するために修正されたバイオメトリック特徴１８４を可聴化することができる。ある特定の実施形態では、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４を可聴化することによって中間オーディオデータを生成することができ、中間オーディオデータを非バイオメトリックデータ１７６（または非バイオメトリックデータ１７６のオーディオバージョン）と組み合わせることによってオーディオデータ１９８を生成することができる。

【００４８】

[0074]別の例として、認証データ生成器１１０は、あるオーディオフォーマット（たとえば、発話信号）のバイオメトリックデータ１７０を受信することができる。認証データ生成器１１０は、一方向性関数をバイオメトリック特徴１８２に適用することによって、修正されたバイオメトリック特徴１８４を生成することができる。認証データ生成器１１０は、図３を参照して説明されるように、修正されたバイオメトリック特徴１８４に基づいて第２の画像１９６または第２のバイオメトリックデータ１８０（たとえば、合成指紋または合成虹彩スキャン）を生成することができる。ある特定の実施形態では、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４に対して画像処理を実行することによって中間画像データを生成することができ、中間画像を非バイオメトリックデータ１７６（または非バイオメトリックデータ１７６に対応する画像）と組み合わせることによって第２の画像１９６または第２のバイオメトリックデータ１８０を生成することができる。

【００４９】

[0075]ある特定の実施形態では、バイオメトリックデータ１７０は複数のタイプのバイオメトリックデータを含み得る。たとえば、バイオメトリックデータ１７０は、ユーザ１０６の指紋、虹彩スキャン、または発話信号のうちの１つに対応する第１のバイオメトリ

ックデータを含んでよく、ユーザ１０６の指紋、虹彩スキャン、または発話信号のうちの別のものに対応する第２のバイオメトリックデータを含んでよい。バイオメトリックデータ１７０は、複数のインターフェースを介して受信され得る。たとえば、指紋は第１のインターフェース１３４を介して受信されてよく、発話信号は第２のインターフェース１３６を介して受信されてよい。第１のバイオメトリックデータおよび第２のバイオメトリックデータは、同じフォーマット（たとえば、オーディオまたは画像）または別のフォーマットを有し得る。

【００５０】

[0076]認証データ生成器１１０は、第１のバイオメトリックデータと第２のバイオメトリックデータとを共通のフォーマットに変換することができ、変換されたバイオメトリックデータを組み合わせることによって認証データ１７８を生成することができる。たとえば、第１のバイオメトリックデータは指紋（たとえば、画像データ）を含んでよく、第２のバイオメトリックデータは発話信号（たとえば、オーディオデータ）を含んでよい。認証データ生成器１１０は、第１のバイオメトリックデータ（たとえば、指紋）を可聴化することができ、図１４を参照して説明されるように、可聴化された第１のバイオメトリックデータ（たとえば、可聴化された指紋）と第２のバイオメトリックデータ（たとえば、発話信号）とを組み合わせてバイオメトリックデータ１７０を生成することができる。認証データ生成器１１０は、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて認証データ１７８を生成することができる。ある特定の実施形態では、非バイオメトリックデータ１７６は第２のバイオメトリックデータに基づいて生成され得る。たとえば、認証データ生成器１１０は、本明細書で説明されるように、非バイオメトリックデータ１７６を生成するために、第２のバイオメトリックデータに対して発話認識または話者認識を実行することができる。

【００５１】

[0077]図１のシステム１００はしたがって、ユーザ１０６が異なる非バイオメトリックデータを提供することによってコンピュータセキュリティシステムのパスワードを修正することを可能にし得る。加えて、パスワードは、バイオメトリックデータに基づいてよく、非バイオメトリックデータだけに基づくパスワードよりセキュアであり得る。一方向性関数を使用してパスワードを生成することは、バイオメトリックデータをパスワードから導出すること（たとえば、リバースエンジニアリング）を難しくし得る。

【００５２】

[0078]図２を参照すると、認証データ生成器のある特定の実施形態の図が開示されており、全体的に２００と指定されている。システム２００は、図１のシステム１００の部分に対応し得る。たとえば、システム２００は、図１の認証データ生成器１１０を含む。

【００５３】

[0079]認証データ生成器１１０は、図１を参照して説明されたように、バイオメトリックデータ１７０（たとえば、指紋、虹彩スキャン、顔の画像、および／または声紋）を受信することができる。認証データ生成器１１０は、ユーザ入力１７２に基づいて鍵（たとえば、非バイオメトリックデータ１７６）を受信することができる。非バイオメトリックデータ１７６（または鍵）は、ユーザ入力１７２に対して話者認識を実行することによって生成される話者認識スコア、テキスト（たとえば、ユーザ入力１７２に対して発話認識を実行することによって生成される）、または両方を含み得る。

【００５４】

[0080]認証データ生成器１１０は、一方向性関数をバイオメトリックデータ１７０および非バイオメトリックデータ１７６（たとえば、鍵）に適用して、認証データ１７８を生成することができる。ある特定の実施形態では、一方向性関数は、デフォルトの関数、ユーザにより選択される関数、または両方であり得る。バイオメトリックデータ１７０（ｂ）は第１の長さ（長さ（ｂ））を有し得る。ある特定の実施形態では、第１の長さ（長さ（ｂ））は、バイオメトリックデータ１７０（ｂ）のバイオメトリック特徴１８２に含まれる特徴のカウントに対応し得る。たとえば、バイオメトリックデータ１７０（ｂ）は指

紋スキャンを含んでよく、バイオメトリック特徴１８２は指紋スキャンのスパイクを含んでよく、第１の長さ（長さ（ｂ））はスパイクのカウントを含んでよい。別の例として、バイオメトリック特徴１８２は、虹彩特徴、顔特徴、または発話特徴を含み得る。この例では、第１の長さ（長さ（ｂ））は、虹彩特徴のカウント、顔特徴のカウント、または発話特徴のカウントを含み得る。

【００５５】

[0081]非バイオメトリックデータ１７６（ｋ）は第２の長さ（長さ（ｋ））を有し得る。ある特定の実施形態では、第２の長さ（長さ（ｋ））は、非バイオメトリックデータ１７６（ｋ）から生成される複数の鍵値（たとえば、「１」、「２」、「３」、および「４」）のカウント（たとえば、４）に対応し得る。ある特定の実施形態では、ｋ（ｉ）は、複数の鍵値のうちのある特定の鍵値に対応し得る。Ｎは、第１の長さ（長さ（ｂ））と第２の長さ（長さ（ｋ））の小さい方であり得る。認証データ生成器１１０は、一方向性関数（たとえば、ハッシュ関数、双曲線正接関数、または別の双曲線関数）をｂおよびｋの対応する値の比に適用するよって、認証データ１７８（ｙ）の特定の値（たとえば、ｙ（ｉ））を生成することができる。たとえば、第１の長さ（長さ（ｂ））が第２の長さ（長さ（ｋ））より大きい場合、認証データ生成器１１０は、一方向性関数をｂ（ｉ）／ｋ（ｉ　ｍｏｄ　Ｎ）に適用することによってｙ（ｉ）を生成することができる。別の例として、第１の長さ（長さ（ｂ））が第２の長さ（長さ（ｋ））以下である場合、認証データ生成器１１０は、一方向性関数をｂ（ｉ　ｍｏｄ　Ｎ）／ｋ（ｉ）に適用することによってｙ（ｉ）を生成することができる。

【００５６】

[0082]したがって、システム２００は、一方向性関数をバイオメトリックデータ１７０および鍵（たとえば、非バイオメトリックデータ１７６）に適用することによって、認証データ１７８を生成することができる。バイオメトリックデータ１７０および非バイオメトリックデータ１７６は、別の長さまたは同じ長さを有し得る。一方向性関数を使用して認証データ１７８を生成することは、バイオメトリックデータ１７０を認証データ１７８から導出することを難しくでき、したがって、バイオメトリックデータ１７０が危うくなることのリスクを減らすことができる。

【００５７】

[0083]図３を参照すると、認証データ生成器１１０を含むシステムのある特定の実施形態の図が開示されており、全体的に３００と指定されている。認証データ生成器１１０は、特徴抽出器３０６に結合されたアライナ３０４を含み得る。特徴抽出器３０６は、領域変換器３０８および画像生成器３１２に結合され得る。認証データ生成器１１０はまた、画像生成器３１２に結合された非バイオメトリックデータ分析器３０２を含み得る。領域変換器３０８および非バイオメトリックデータ分析器３０２は、オーディオ生成器３１４に結合され得る。

【００５８】

[0084]ある特定の実施形態では、認証データ生成器１１０は、図３に示されるものよりも少数のコンポーネント、多数のコンポーネント、および／または異なるコンポーネントを含み得る。ある特定の実施形態では、認証データ生成器１１０の２つ以上のコンポーネントは組み合わされ得る。認証データ生成器１１０の１つまたは複数のコンポーネントはハードウェアで実装され得る。ある特定の実施形態では、認証データ生成器１１０の１つまたは複数のコンポーネントは、本明細書で説明される１つまたは複数の動作を実行するための命令を実行するように構成されるプロセッサを含み得る。

【００５９】

[0085]認証データ生成器１１０は、図１を参照して説明されたように、第１のインターフェース１３４を介して、バイオメトリックデータ１７０（たとえば、指紋、虹彩スキャン、顔の画像、および／または声紋）を受信することができる。たとえば、アライナ３０４、特徴抽出器３０６、または両方が、第１のインターフェース１３４を介してバイオメトリックデータ１７０を受信することができる。たとえば、アライナ３０４は、バイオメ

トリックデータ１７０が登録フェーズの間に受信されるとき、バイオメトリックデータ１７０を受信することができる。図４を参照してさらに説明されるように、アライナ３０４は、バイオメトリックデータ１７０に基づいて、アラインされたバイオメトリックデータ３７０を生成することができる。アライナ３０４は、アラインされたバイオメトリックデータ３７０を特徴抽出器３０６に提供することができる。

【００６０】

[0086]図４を参照してさらに説明されるように、特徴抽出器３０６は、バイオメトリックデータ１７０またはアラインされたバイオメトリックデータ３７０に基づいて、バイオメトリック特徴１８２を生成することができる。特徴抽出器３０６は、領域変換器３０８および画像生成器３１２にバイオメトリック特徴１８２を提供することができる。

【００６１】

[0087]領域変換器３０８は、図４を参照してさらに説明されるように、中間オーディオデータ３９８を生成することができる。たとえば、バイオメトリックデータ１７０は第１の領域またはフォーマット（たとえば、画像またはオーディオ）にあり得る。図４を参照してさらに説明されるように、領域変換器３０８は、バイオメトリック特徴１８２に対して特徴領域移行を実行して、第２の領域またはフォーマットの中間データ（たとえば、中間オーディオデータ３９８または中間画像データ）を生成することができる。

【００６２】

[0088]領域変換器３０８は、中間オーディオデータ３９８をオーディオ生成器３１４に提供することができる。非バイオメトリックデータ分析器３０２は、第２のインターフェース１３６を介してユーザ入力１７２を受信することができる。図１を参照してさらに説明されるように、非バイオメトリックデータ分析器３０２は、ユーザ入力１７２に基づいて、非バイオメトリックデータ１７６を生成することができる。非バイオメトリックデータ分析器３０２は、画像生成器３１２およびオーディオ生成器３１４に非バイオメトリックデータ１７６を提供することができる。図４を参照してさらに説明されるように、画像生成器３１２は、第２のバイオメトリックデータ１８０、第２の画像１９６、または両方を生成することができる。図４を参照してさらに説明されるように、オーディオ生成器３１４は、中間オーディオデータ３９８および非バイオメトリックデータ１７６に基づいて、オーディオデータ１９８を生成することができる。

【００６３】

[0089]したがって、認証データ生成器１１０は、第１の領域（たとえば、画像またはオーディオ）でのバイオメトリックデータの受信と、第２の領域（たとえば、オーディオまたは画像）での認証データの生成とを可能にし得る。したがって、ユーザは、第１のフォーマットでバイオメトリックデータを提供し、第２のフォーマットで認証データを生成することができる。たとえば、ユーザは、画像フォーマットでバイオメトリックデータを提供し、基本電話サービス（ＰＯＴＳ）デバイス（または音声呼を行うように構成されるデバイス）を使用して、オーディオフォーマットの認証データを認証デバイスに送ることができる。例示すると、認証データは、３００ヘルツ（Ｈｚ）から３４００Ｈｚの周波数範囲にあるＰＯＴＳ互換アナログオーディオ信号を含み得る。

【００６４】

[0090]図４を参照すると、バイオメトリックデータおよび非バイオメトリックに基づいて認証データを生成する方法のある特定の実施形態の図が開示されており、全体的に４００と指定されている。方法４００は、図１のシステム１００、図３のシステム３００、または両方によって実行され得る。たとえば、方法４００の１つまたは複数の動作は、認証データ生成器１１０、モバイルデバイス１０２、認証デバイス１０４、またはこれらの組合せによって実行され得る。

【００６５】

[0091]４０２、４０４、４０６、４１０、および４１２によって示される１つまたは複数のローカル動作は、図１の認証データ生成器１１０によって実行され得る。４１４および４１６によって示される１つまたは複数の遠隔動作は、図１の認証デバイス１０４によ

って実行され得る。ある特定の実施形態では、認証データ生成器１１０、認証デバイス１０４、または両方が、４０２、４０４、４０６、および４１４によって示される画像領域動作を実行することができ、４１０、４１２、および４１６によって示されるオーディオ領域動作を実行することができ、またはこれらの組合せであってよい。

【００６６】

[0092]動作の間に、認証データ生成器１１０は、バイオメトリックデータ１７０と非バイオメトリックデータ１７６（たとえば、パスワードなどの鍵）を受信することができる。方法４００は、４０２において、アラインメントを含み得る。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０と非バイオメトリックデータ１７６とを受信することができる。図３のアライナ３０４は、図９を参照して説明されるように、アラインされたバイオメトリックデータ３７０を生成するために、バイオメトリックデータ１７０のいくつかの特徴と他のバイオメトリックデータ（たとえば、テンプレートバイオメトリックデータまたは登録バイオメトリックデータ）とを揃えるように、バイオメトリックデータ１７０を修正する（たとえば、それに回転関数、変換関数、またはスケーリング関数を適用する）ことができる。たとえば、認証データ生成器１１０は、登録フェーズの間に登録バイオメトリックデータを受信することができ、認証フェーズの間にバイオメトリックデータ１７０を受信することができ、アラインされたバイオメトリックデータ３７０を生成するために、バイオメトリックデータ１７０を登録バイオメトリックデータとアラインすることができる。別の例として、認証データ生成器１１０は、登録フェーズの間にバイオメトリックデータ１７０を受信することができ、アラインされたバイオメトリックデータ３７０を生成するために、バイオメトリックデータ１７０をテンプレートバイオメトリックデータとアラインすることができる。テンプレートバイオメトリックデータはデフォルトデータを含み得る。

【００６７】

[0093]方法４００はまた、４０４において、特徴抽出を含み得る。たとえば、図３の特徴抽出器３０６は、バイオメトリックデータ１７０（またはアラインされたバイオメトリックデータ３７０）からバイオメトリック特徴１８２を抽出することができる。例示すると、バイオメトリックデータ１７０が指紋（たとえば、指紋スキャン画像）に対応する場合、バイオメトリック特徴１８２は、図８を参照して説明されるように、指紋のスパイク（たとえば、特異点および特徴点）を示し得る。認証データ生成器１１０は、バイオメトリック特徴１８２を抽出するために指紋特徴抽出技法を使用することができる。たとえば、認証データ生成器１１０は、画像処理（たとえば、グレースケールへの変換、バイナリ化、テンプレートパターン照合など）を使用して、指紋スキャン画像からバイオメトリック特徴１８２を抽出することができる。

【００６８】

[0094]別の例として、バイオメトリックデータ１７０（たとえば、虹彩スキャン画像）が虹彩スキャンに対応する場合、バイオメトリック特徴１８２は、放射状のファロー（furrow）、同心円のファロー、クリプト、捲縮輪（collarette）、または瞳孔サイズのうちの少なくとも１つを示し得る。認証データ生成器１１０は、バイオメトリック特徴１８２を抽出するために虹彩特徴抽出技法を使用することができる。たとえば、認証データ生成器１１０は、画像処理（たとえば、セグメント化、正規化、テンプレート照合など）を使用して、虹彩スキャン画像からバイオメトリック特徴１８２を抽出することができる。

【００６９】

[0095]さらなる例として、バイオメトリックデータ１７０が顔の画像に対応する場合、バイオメトリック特徴１８２は、目、鼻、口、または頭のサイズ、形状、もしくは場所のうちの少なくとも１つを示し得る。認証データ生成器１１０は、バイオメトリック特徴１８２を抽出するために顔特徴抽出技法を使用することができる。たとえば、認証データ生成器１１０は、画像処理（たとえば、グレースケールへの変換、ガボールフィルタの適用など）を使用して、顔の画像からバイオメトリック特徴１８２を抽出することができる。

【００７０】

[0096]追加の例として、バイオメトリックデータ１７０が発話信号に対応する場合、バイオメトリック特徴１８２は、発話信号のフォルマント位置とスペクトル傾斜とを示し得る。認証データ生成器１１０は、発話信号処理を使用して（たとえば、メル周波数ケプストラム係数（ＭＦＣＣ：mel-frequency cepstral coefficients）、線形予測ケプストラム係数（ＬＰＣＣ）、またはメル周波数離散ウェーブレット係数（ＭＦＤＷＣ）を生成して）発話信号に対応するバイオメトリック特徴１８２（たとえば、推定されるスペクトルエンベロープ）を生成することができる。

【００７１】

[0097]方法４００はさらに、４０６において、人工的な指紋／画像の生成を含み得る。たとえば、図３の画像生成器３１２は、バイオメトリック特徴１８２に基づいて第２のバイオメトリックデータ１８０を生成することができる。画像生成器３１２は、本明細書で説明されるように、非バイオメトリックデータ１７６に基づいて図１の修正されたバイオメトリック特徴１８４を生成するために、一方向性関数をバイオメトリック特徴１８２に適用することができる。一方向性関数は、ハッシュ関数、双曲線正接関数、または別の双曲線関数を含み得る。画像生成器３１２は、修正されたバイオメトリック特徴１８４を生成するために、一方向性関数に基づいて非バイオメトリックデータ１７６をバイオメトリック特徴１８２に配分することができる。

【００７２】

[0098]画像生成器３１２は、一方向性関数を非バイオメトリックデータ１７６の鍵値およびバイオメトリック特徴１８２の特徴値に適用することによって、修正されたバイオメトリック特徴１８４の各々の修正された特徴値を生成することができる。ある特定の実施形態では、画像生成器３１２は、修正された特徴値を生成するために、鍵値と特徴値との比、積、和、および／または差に一方向性関数を適用することができる。

【００７３】

[0099]たとえば、バイオメトリックデータ１７０が指紋（たとえば、指紋スキャン画像）に対応する場合、バイオメトリック特徴１８２は、指紋のスパイク（たとえば、特異点および特徴点）を示し得る。画像生成器３１２は、スパイクを修正するために、一方向性関数をバイオメトリック特徴１８２に適用することができる。

【００７４】

[00100]別の例として、バイオメトリックデータ１７０（たとえば、虹彩スキャン画像）が虹彩スキャンに対応する場合、バイオメトリック特徴１８２は、放射状のファロー、同心円のファロー、クリプト、捲縮輪、または瞳孔サイズのうちの少なくとも１つを示し得る。画像生成器３１２は、修正されたバイオメトリック特徴１８４を生成するように、放射状のファロー、同心円のファロー、クリプト、捲縮輪、または瞳孔サイズのうちの少なくとも１つを修正するために、バイオメトリック特徴１８２に一方向性関数を適用することができる。

【００７５】

[00101]さらなる例として、バイオメトリックデータ１７０が顔の画像に対応する場合、バイオメトリック特徴１８２は、目、鼻、口、または頭のサイズ、形状、もしくは場所のうちの少なくとも１つを示し得る。画像生成器３１２は、修正されたバイオメトリック特徴１８４を生成するように、目、鼻、口、または頭のサイズ、形状、もしくは場所のうちの少なくとも１つを修正するために、バイオメトリック特徴１８２に一方向性関数を適用することができる。

【００７６】

[00102]追加の例として、バイオメトリックデータ１７０が発話信号に対応する場合、バイオメトリック特徴１８２は、発話信号のフォルマント位置とスペクトル傾斜とを示し得る。画像生成器３１２は、修正されたバイオメトリック特徴１８４を生成するために、フォルマント位置および／またはスペクトル傾斜を修正するように、バイオメトリック特徴１８２に一方向性関数を適用することができる。

【００７７】

[00103]ある特定の実施形態では、画像生成器３１２は、修正されたバイオメトリック特徴１８４、第２のバイオメトリックデータ１８０、または両方を生成するために、回転関数、スケーリング関数、ぼかし関数、シェーディング関数、ノイズ関数、またはこれらの組合せを、バイオメトリック特徴１８２、バイオメトリックデータ１７０、またはアラインされたバイオメトリックデータ３７０に適用することができる。

【００７８】

[00104]画像生成器３１２は、修正されたバイオメトリック特徴１８４に基づいて第２のバイオメトリックデータ１８０を生成することができる。たとえば、バイオメトリックデータ１７０が指紋（たとえば、指紋スキャン画像）に対応する場合、画像生成器３１２は、修正されたバイオメトリック特徴１８４によって示される修正されたスパイクに対応する第２のバイオメトリックデータ１８０を生成するために、合成指紋生成技法を使用することができる。

【００７９】

[00105]別の例として、バイオメトリックデータ１７０（たとえば、虹彩スキャン画像）が虹彩スキャンに対応する場合、画像生成器３１２は、修正されたバイオメトリック特徴１８４によって示されるような、修正された放射状のファロー、修正された同心円のファロー、修正されたクリプト、修正された捲縮輪、および／または修正された瞳孔サイズに対応する第２のバイオメトリックデータ１８０を生成するために、合成虹彩スキャン生成技法を使用することができる。

【００８０】

[00106]さらなる例として、バイオメトリックデータ１７０が顔の画像に対応する場合、画像生成器３１２は、修正されたバイオメトリック特徴１８４によって示される、目、鼻、口、または頭の、修正されたサイズ、修正された形状、もしくは修正された場所に対応する第２のバイオメトリックデータ１８０を生成するために、合成顔画像生成技法を使用することができる。

【００８１】

[00107]追加の例として、バイオメトリックデータ１７０が発話信号に対応する場合、画像生成器３１２は、修正されたバイオメトリック特徴１８４によって示される、修正されたフォルマント位置および／または修正されたスペクトル傾斜に対応する第２のバイオメトリックデータ１８０を生成するために、合成声生成技法を使用することができる。

【００８２】

[00108]別の例として、画像生成器３１２は、バイオメトリック特徴１８２に基づいて図１の第１の画像１９４を選択することができる。例示すると、図１の画像マッピング１９２は、バイオメトリック特徴１８２と第１の画像１９４との間のマッピングを示すことができ、画像生成器３１２は、マッピングに基づいて第１の画像１９４を選択することができる。画像生成器３１２は、図１を参照して説明されるように、非バイオメトリックデータ１７６に基づいて第１の画像１９４を修正することによって、第２の画像１９６を生成することができる。

【００８３】

[00109]方法４００はさらに、または代替的に、４１０において、特徴領域移行を含み得る。たとえば、図１の認証データ生成器１１０は、第１の領域またはフォーマット（たとえば、画像またはオーディオ）のバイオメトリックデータ１７０を受信することができる。図３の領域変換器３０８は、バイオメトリック特徴１８２に対して特徴領域移行を実行して、第２の領域またはフォーマットの中間データ（たとえば、中間オーディオデータ３９８または中間画像データ）を生成することができる。

【００８４】

[00110]ある特定の実施形態では、認証データ生成器１１０は、画像データ（たとえば、指紋スキャン、虹彩スキャン、または顔の画像）としてバイオメトリックデータ１７０を受信することができ、領域変換器３０８は、中間オーディオデータ３９８を生成するためにバイオメトリック特徴１８２を可聴化することができる。たとえば、認証データ生成

器１１０は、図６を参照して説明されるように、バイオメトリック特徴１８２に基づいてスペクトルエンベロープ１６０を生成することができる。スペクトルエンベロープ１６０は、中間オーディオデータ３９８に対応し得る。

【００８５】

[00111]別の特定の実施形態では、認証データ生成器１１０は、オーディオデータ（たとえば、発話信号）としてバイオメトリックデータ１７０を受信することができ、領域変換器３０８は、バイオメトリック特徴１８２に基づいて中間画像データを生成することができる。中間画像データは、合成されたバイオメトリックデータまたは画像１９０のうちのある特定の画像を含み得る。たとえば、バイオメトリック特徴１８２は、発話信号の推定されるスペクトルエンベロープを示し得る。領域変換器３０８は、合成されたバイオメトリックデータを生成するために、推定されたスペクトルエンベロープに基づいてバイオメトリックテンプレート（たとえば、虹彩スキャンテンプレート、指紋テンプレート、テンプレート顔画像）を修正することができる。

【００８６】

[00112]方法４００はさらに、４１２において、音声生成を含み得る。たとえば、図３のオーディオ生成器３１４は、中間オーディオデータ３９８（たとえば、スペクトルエンベロープ１６０）および非バイオメトリックデータ１７６に基づいてオーディオデータ１９８を生成することができる。例示すると、オーディオ生成器３１４は、図６を参照して説明されるように、非バイオメトリックデータ１７６に基づいて音符シーケンス１６２を生成することができる。オーディオデータ１９８は、スペクトルエンベロープ１６０と音符シーケンス１６２とを含み得る。

【００８７】

[00113]ある特定の実施形態では、図３の画像生成器３１２は、中間画像データに基づいて第２のバイオメトリックデータ１８０または第２の画像１９６を生成することができる。たとえば、画像生成器３１２は、非バイオメトリックデータ１７６に基づいて中間画像データ（たとえば、合成されたバイオメトリックデータまたは画像１９０のうちの特定の画像）を修正することができる。ある特定の実施形態では、画像生成器３１２は、第２のバイオメトリックデータ１８０（または第２の画像１９６）を生成するために、回転関数、スケーリング関数、シェーディング関数、ぼかし関数、ノイズ関数、またはこれらの組合せを、合成されたバイオメトリックデータ（または特定の画像）に適用することができる。

【００８８】

[00114]方法４００はまた、４１４において、指紋／画像認識を含み得る。たとえば、図１の認証データ生成器１１０は、第２のバイオメトリックデータ１８０または第２の画像１９６を認証デバイス１０４に提供することができる。認証デバイス１０４は、第２のバイオメトリックデータ１８０または第２の画像１９６を別の画像と比較することによって、画像認識を実行することができる。たとえば、他の画像は、登録フェーズの間に認証デバイス１０４によって受信されてよく、メモリに記憶されてよい。認証デバイス１０４は、比較に基づいてコンピュータセキュリティシステムへのアクセスを選択的に提供することができる。たとえば、認証デバイス１０４は、比較に基づいて類似性（または信頼性）スコアを生成することができ、類似性スコアが特定の閾値を満たすと決定したことに基づいて、コンピュータセキュリティシステムへのアクセス権を提供することができる。ある特定の実施形態では、認証デバイス１０４は、登録フェーズの間に第２のバイオメトリックデータ１８０または第２の画像１９６を受信することができ、第２のバイオメトリックデータ１８０または第２の画像１９６をメモリに記憶することができる。

【００８９】

[00115]方法４００はさらに、または代替的に、４１６において、オーディオ指紋生成を含み得る。たとえば、図１の認証データ生成器１１０は、オーディオデータ１９８を認証デバイス１０４に提供することができる。認証デバイス１０４は、オーディオデータ１９８を別のオーディオデータと比較することによって、オーディオ指紋認識を実行するこ

とができる。たとえば、他のオーディオデータは、登録フェーズの間に認証デバイス１０４によって受信されてよく、メモリに記憶されてよい。認証デバイス１０４は、比較に基づいてコンピュータセキュリティシステムへのアクセスを選択的に提供することができる。たとえば、認証デバイス１０４は、比較に基づいて類似性（または信頼性）スコアを生成することができ、類似性スコアが特定の閾値を満たすと決定したことに基づいて、コンピュータセキュリティシステムへのアクセス権を提供することができる。ある特定の実施形態では、認証デバイス１０４は、登録フェーズの間にオーディオデータ１９８を受信することができ、オーディオデータ１９８をメモリに記憶することができる。

【００９０】

[00116]ある特定の実施形態では、認証データ生成器１１０は、ユーザ選好に基づいて方法４００の１つまたは複数の動作を実行することができる。たとえば、画像認証データが生成されるべきであることをユーザ選好が示す場合、認証データ生成器１１０は、４０２と、４０４と、４０６とを実行することができる。この例では、認証デバイス１０４は４１４を実行することができる。別の例として、オーディオ認証データが生成されるべきであることをユーザ選好が示す場合、認証データ生成器１１０は、４０２と、４０４と、４１０と、４１２とを実行することができる。この例では、認証デバイス１０４は４１６を実行することができる。

【００９１】

[00117]ある特定の実施形態では、認証データ生成器１１０は、認証データ送信のモードに基づいて方法４００の１つまたは複数の動作を実行することができる。たとえば、認証データ生成器１１０は、認証データ送信のモードが基本電話サービス（ＰＯＴＳ）に対応すると決定したことに応答して、４０２と、４０４と、４１０と、４１２とを実行することができる。この例では、認証デバイス１０４は４１６を実行することができる。別の例として、認証データ生成器１１０は、認証データ送信のモードがインターネットに対応すると決定したことに応答して、４０２と、４０４と、４０６と、４１０と、４１２とを実行することができる。例示すると、認証データ生成器１１０は、第２のバイオメトリックデータ１８０、第２の画像１９６、オーディオデータ１９８、またはこれらの組合せを送信することができる。この例では、認証デバイス１０４は、４１４、４１６、または両方を実行することができる。

【００９２】

[00118]ある特定の実施形態では、認証データ生成器１１０は、動作４０２と、４０４と、４０６と、４１２とを実行することができる。たとえば、認証データ生成器１１０は、画像領域のバイオメトリックデータ１７０を受信することができる。認証データ生成器１１０は、アラインメント４０２を実行してバイオメトリックデータ１７０に基づいてアラインされたバイオメトリックデータ３７０を生成することができ、特徴抽出４０４を実行してアラインされたバイオメトリックデータ３７０に基づいてバイオメトリック特徴１８２を生成することができ、人工的な指紋／画像生成４０６を実行して、バイオメトリックデータ１７０、バイオメトリック特徴１８２、および／または非バイオメトリックデータ１７６に基づいて、第２のバイオメトリックデータ１８０、第２の画像１９６、または両方を生成することができる。認証データ生成器１１０は、第２のバイオメトリックデータ１８０、第２の画像１９６、または両方に基づいて音声生成４１２を実行することができる。認証データ生成器１１０は、第２のバイオメトリックデータ１８０、第２の画像１９６、または両方を可聴化することによって、オーディオデータ１９８を生成することができる。

【００９３】

[00119]オーディオデータのマッピングは、画像（たとえば、画像１９０、画像１９０の修正されたバージョン、および／または第２の画像１９６）をオーディオデータ（たとえば、スペクトルエンベロープ、音波など）にマッピングすることができる。認証データ生成器１１０は、オーディオデータのマッピングおよび第２の画像１９６に基づいて、オーディオデータ１９８（たとえば、スペクトルエンベロープ、音波など）を選択すること

ができる。別の例として、認証データ生成器１１０は、第２のバイオメトリックデータ１８０に基づいて、オーディオデータ１９８（たとえば、スペクトルエンベロープ）を生成することができる。認証データ生成器１１０は、オーディオデータ１９８を認証デバイス１０４に提供することができる。認証デバイス１０４は、オーディオデータ１９８に基づいて動作４１６を実行することができる。

【００９４】

[00120]したがって、方法４００は、第１の領域（たとえば、画像またはオーディオ）でのバイオメトリックデータの受信と、第２の領域（たとえば、オーディオまたは画像）での認証データの生成とを可能にし得る。したがって、ユーザは、第１のフォーマットでバイオメトリックデータを提供し、第２のフォーマットで認証データを生成することができる。たとえば、ユーザは、画像フォーマットでバイオメトリックデータを提供し、基本電話サービス（ＰＯＴＳ）デバイス（または音声呼を行うように構成されるデバイス）を使用して、オーディオフォーマットの認証データを認証デバイスに送ることができる。

【００９５】

[00121]図５を参照すると、認証データを生成する方法のある特定の実施形態の図が示されており、全体的に５００と指定されている。認証データは、第１のバイオメトリックデータに基づいて生成される第２のバイオメトリックデータを含み得る。特定の実施形態では、方法５００は図１の認証データ生成器１１０によって実行され得る。方法５００は図４の特徴抽出４０４を含み得る。たとえば、図１の認証データ生成器１１０は、図１および図３～図４を参照して説明されるように、バイオメトリックデータ１７０に基づいてバイオメトリック特徴１８２を生成することができる。

【００９６】

[00122]特定の実施形態では、バイオメトリックデータ１７０は指紋スキャンに対応し得る。認証データ生成器１１０は、指紋スキャンに基づいて、密度マップと方向マップとを生成することができる。たとえば、指紋スキャンは、複数の隆線を含むスパイクを示し得る。認証データ生成器１１０は、複数の隆線の密度を示すために密度マップを生成することができ、複数の隆線に対する正接の方向を示すために方向マップを生成することができる。バイオメトリック特徴１８２は、方向マップと密度マップとを含み得る。

【００９７】

[00123]方法５００はまた、５０２において、鍵のアラインメントと分配とを実行することを含み得る。たとえば、図１の認証データ生成器１１０は、アラインメントデータ５２０を生成するために、非バイオメトリックデータ１７６およびバイオメトリックデータ１７０に対して鍵のアラインメントと分配とを実行することができる。認証データ生成器１１０は、バイオメトリックデータ１７０の中心点５１２を特定することによって、バイオメトリックデータ１７０をアラインすることができる。たとえば、バイオメトリックデータ１７０は、虹彩スキャン、指紋スキャン、顔の画像、または発話信号に対応し得る。認証データ生成器１１０は、虹彩スキャンによって示される虹彩の中心（または重心）として、指紋スキャンによって示される指の中心（または重心）として、顔の画像によって示される鼻の中心（または重心）として、または発話信号によって示される発声の中点として、中心点５１２を特定することによって、バイオメトリックデータ１７０をアラインすることができる。

【００９８】

[00124]非バイオメトリックデータ１７６は、第１の数（たとえば、４つ）の値（ｋ）（たとえば、「１」、「２」、「３」、および「４」）を含み得る。認証データ生成器１１０は、中心点５１２に基づいてバイオメトリックデータ１７０（たとえば、指紋スキャン、虹彩スキャン、顔の画像、または発話信号）を第１の数（たとえば、４つ）のセグメント（ｂ）へと分割することによって、非バイオメトリックデータ１７６を分配することができる。

【００９９】

[00125]アラインメントデータ５２０は、バイオメトリックデータ１７０の各セグメン

ト（たとえば、ｂ（ｉ））に対応する非バイオメトリックデータ１７６の特定の値（たとえば、ｋ（ｉ））を示し得る。たとえば、アラインメントデータ５２０は、バイオメトリックデータ１７０のセグメント５０４（たとえば、ｂ（０））が非バイオメトリックデータ１７６の第１の鍵値に対応し（たとえば、ｋ（０）＝１）、バイオメトリックデータ１７０のセグメント５０６（たとえば、ｂ（１））が非バイオメトリックデータ１７６の第２の鍵値に対応し（たとえば、ｋ（１）＝２）、バイオメトリックデータ１７０のセグメント５０８（たとえば、ｂ（２））が非バイオメトリックデータ１７６の第３の鍵値に対応し（たとえば、ｋ（２）＝３）、バイオメトリックデータ１７０のセグメント５１０（たとえば、ｂ（３））が第４の鍵値に対応する（たとえば、ｋ（３）＝４）ことを示し得る。

【０１００】

[00126]たとえば、バイオメトリックデータ１７０が指紋スキャンに対応する場合、セグメント５０４、５０６、５０８、および５１０の各セグメントは、指紋の別個の部分に対応し得る。別の例として、バイオメトリックデータ１７０が虹彩スキャンに対応する場合、セグメント５０４、５０６、５０８、および５１０の各セグメントは、虹彩の画像の別個の部分に対応し得る。さらなる例として、バイオメトリックデータ１７０が顔の画像に対応する場合、セグメント５０４、５０６、５０８、および５１０の各々は、顔の画像の別個の部分に対応し得る。追加の例として、バイオメトリックデータ１７０が発話信号に対応する場合、セグメント５０４、５０６、５０８、および５１０の各々は、発話信号の別個の部分に対応し得る。

【０１０１】

[00127]方法５００はさらに、５０４において、特徴を変換することを含み得る。たとえば、図１の認証データ生成器１１０は、修正されたバイオメトリック特徴１８４を生成するために、アラインメントデータ５２０に基づいてバイオメトリック特徴１８２を修正することができる。例示すると、認証データ生成器１１０は、アラインメントデータ５２０によって示される各バイオメトリック値（たとえば、ｂ（ｉ））および対応する鍵値（たとえば、ｋ（ｉ））に一方向性関数を適用することによって、修正されたバイオメトリック特徴１８４の各々の修正された特徴（たとえば、ｙ（ｉ））を生成することができる。たとえば、認証データ生成器１１０は、セグメント５０４、５０６、５０８、および５１０の特定のセグメントならびに対応する鍵値（たとえば、１、２、３、または４）に一方向性関数を適用することによって、第２のバイオメトリックデータ１８０の各セグメントを生成することができる。

【０１０２】

[00128]ある特定の実施形態では、バイオメトリックデータ１７０は指紋スキャンに対応し、バイオメトリック特徴１８２は指紋のスパイクに対応する。この実施形態では、修正されたバイオメトリック特徴１８４は修正されたスパイクに対応する。たとえば、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４を生成するために、非バイオメトリックデータ１７６に基づいて、スパイクの位置、角度、またはサイズを修正することができる。

【０１０３】

[00129]認証データ生成器１１０は、一方向性関数、密度マップ、第１の指紋のスパイク、および非バイオメトリックデータ１７６に基づいて、修正された密度マップを生成することができる。ある特定の実施形態では、修正された密度マップの特定の値は、

【０１０４】

【数１】

$$f\big(x(i),y(i)\big)=\tanh\left(\frac{f'(x(i),y(i))}{k(i)}\right), \qquad \text{式}1$$

【０１０５】

に対応してよく、ここでｘ（ｉ）＝スパイクｉのｘ座標、ｙ（ｉ）＝スパイクｉのｙ座標、ｋ（ｉ）＝スパイクｉに対応する非バイオメトリックデータ１７６の鍵値、ｆ’（ｘ（

ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する密度マップの値、ｆ（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する修正された密度マップの値である。

【０１０６】

[00130]たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０に基づいて、スパイクの各スパイクに対応するｘ座標ｘ（ｉ）とｙ座標ｙ（ｉ）とを決定することができる。認証データ生成器１１０は、ｘ（ｉ）およびｙ（ｉ）に対応する密度マップの密度値ｆ’（ｘ（ｉ），ｙ（ｉ））を決定することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて、スパイクに対応する鍵値ｋ（ｉ）を決定することができる。認証データ生成器１１０は、密度値ｆ’（ｘ（ｉ），ｙ（ｉ））と鍵値ｋ（ｉ）の比に一方向性関数（たとえば、双曲線正接関数）を適用することによって、スパイクに対応する修正された密度値ｆ（ｘ（ｉ），ｙ（ｉ））を決定することができる。

【０１０７】

[00131]認証データ生成器１１０は、一方向性関数、指紋のスパイク、方向マップ、および非バイオメトリックデータ１７６に基づいて、修正された方向マップを生成することができる。認証データ生成器１１０は、修正された密度マップを生成するために第１の一方向性関数を使用することができ、修正された方向マップを生成するために第２の一方向性関数を使用することができる。第１の一方向性関数および第２の一方向性関数は、同じ関数または別の関数であり得る。ある特定の実施形態では、修正された方向マップの特定の値は、

【０１０８】

【数２】

$$f\big(x(i),y(i)\big) = f'(\tanh\left(\frac{x(i)}{k(i)}\right),\tanh(\frac{y(i)}{k(i)})), \qquad \text{式２}$$

【０１０９】

に対応してよく、ここでｘ（ｉ）＝スパイクｉのｘ座標、ｙ（ｉ）＝スパイクｉのｙ座標、ｋ（ｉ）＝スパイクｉに対応する非バイオメトリックデータ１７６の鍵値、ｆ’（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する方向マップの値、ｆ（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する修正された密度マップの値である。

【０１１０】

[00132]たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０に基づいて、スパイクの特定のスパイクに対応するｘ座標ｘ（ｉ）とｙ座標ｙ（ｉ）とを決定することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて、特定のスパイクに対応する鍵値ｋ（ｉ）を決定することができる。認証データ生成器１１０は、一方向性関数をｘ（ｉ）と鍵（ｉ）の比に適用することによって、修正されたｘ座標を決定することができ、一方向性関数をｙ（ｉ）と鍵（ｉ）の比に適用することによって、修正されたｙ座標を決定することができる。認証データ生成器１１０は、修正されたｘ座標および修正されたｙ座標に対応する密度マップの方向値

【０１１１】

【数３】

$$f'(\tanh\left(\frac{x(i)}{k(i)}\right),\tanh(\frac{y(i)}{k(i)}))$$

【０１１２】

を決定することができる。認証データ生成器１１０は、方向値に基づいて、特定のスパイクに対応する修正された方向値ｆ（ｘ（ｉ），ｙ（ｉ））を決定することができる。ある特定の実施形態では、認証データ生成器１１０は、一方向性関数および非バイオメトリックデータ１７６に基づいて、方向マップの方向値を異なる座標に移すことによって、修正された方向マップを生成することができる。

【０１１３】

[00133]ある特定の実施形態では、修正された密度マップの特定の値は、

【０１１４】
【数４】

$$f\left(x(i),y(i)\right)=k(i)^{f'(x(i),y(i))}mod\ p, \qquad 式3$$

【０１１５】
に対応してよく、ここでｘ（ｉ）＝スパイクｉのｘ座標、ｙ（ｉ）＝スパイクｉのｙ座標、ｋ（ｉ）＝スパイクｉに対応する非バイオメトリックデータ１７６の鍵値、ｆ’（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する密度マップの値、ｆ（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する修正された密度マップの値であり、ｐは特定の数（たとえば、素数）である。

【０１１６】
[00134]たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０に基づいて、各スパイクに対応するｘ座標ｘ（ｉ）とｙ座標ｙ（ｉ）とを決定することができる。認証データ生成器１１０は、ｘ（ｉ）およびｙ（ｉ）に対応する密度マップの密度値ｆ’（ｘ（ｉ），ｙ（ｉ））を決定することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて、スパイクに対応する鍵値ｋ（ｉ）を決定することができる。認証データ生成器１１０は、ｋ（ｉ）値および密度値ｆ’（ｘ（ｉ），ｙ（ｉ））に一方向性関数（たとえば、剰余関数および指数関数）を適用することによって、スパイクに対応する修正された密度値ｆ（ｘ（ｉ），ｙ（ｉ））を決定することができる。

【０１１７】
[00135]認証データ生成器１１０は、一方向性関数、指紋のスパイク、方向マップ、および非バイオメトリックデータ１７６に基づいて、修正された方向マップを生成することができる。ある特定の実施形態では、修正された方向マップの特定の値は、

【０１１８】
【数５】

$$f\left(x(i),y(i)\right)=\left(k(i)^{x(i)}mod\ p,k(i)^{y(i)}\ mod\ p\right), \qquad 式4$$

【０１１９】
に対応してよく、ここでｘ（ｉ）＝スパイクｉのｘ座標、ｙ（ｉ）＝スパイクｉのｙ座標、ｋ（ｉ）＝スパイクｉに対応する非バイオメトリックデータ１７６の鍵値、ｆ’（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する方向マップの値、ｆ（ｘ（ｉ），ｙ（ｉ））＝ｘ（ｉ）およびｙ（ｉ）に対応する修正された密度マップの値である。

【０１２０】
[00136]たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０に基づいて、スパイクの各スパイクに対応するｘ座標ｘ（ｉ）とｙ座標ｙ（ｉ）とを決定することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて、スパイクに対応する鍵値ｋ（ｉ）を決定することができる。認証データ生成器１１０は、一方向性関数（たとえば、剰余関数および指数関数）をｘ（ｉ）と鍵（ｉ）に適用することによって、修正されたｘ座標を決定することができ、一方向性関数をｙ（ｉ）と鍵（ｉ）に適用することによって、修正されたｙ座標を決定することができる。認証データ生成器１１０は、修正されたｘ座標および修正されたｙ座標に対応する密度マップの方向値ｆ’（ｋ（ｉ）$^{x(i)}$ ｍｏｄ ｐ，ｋ（ｉ）$^{y(i)}$ ｍｏｄ ｐ）を決定することができる。認証データ生成器１１０は、方向値に基づいて、スパイクに対応する修正された方向値ｆ（ｘ（ｉ），ｙ（ｉ））を決定することができる。ある特定の実施形態では、認証データ生成器１１０は、一方向性関数および非バイオメトリックデータ１７６に基づいて、方向マップの方向値を異なる座標に移すことによって、修正された方向マップを生成することができる。

【０１２１】
[00137]ある特定の実施形態では、認証データ生成器１１０は、密度マップの後処理を実行することができる。たとえば、認証データ生成器１１０は、

【０１２２】
【数６】

$$f\big(x(i),y(i)\big) = f(x(i),y(i))^{common} mod\ p, \qquad 式5$$

【０１２３】
に基づいて密度マップの特定の値を修正することができ、ここでｃｏｍｍｏｎはある特定の数である。たとえば、ｃｏｍｍｏｎは、モバイルデバイス１０２と認証デバイス１０４との間で共有される、またはこれらの両方に提供される、共通の鍵（たとえば、英数字の非バイオメトリックデータ）を含み得る。ある特定の実施形態では、図２０～図２１を参照して説明されるように、モバイルデバイス１０２の認証データ生成器１１０は、ユーザ１０６の合成バイオメトリックデータ（たとえば、密度マップ）を生成することができ、認証デバイス１０４の認証データ生成器１１０は、認証デバイス１０４の合成バイオメトリックデータ（たとえば、密度マップ）を生成することができる。ユーザ１０６および認証デバイス１０４の密度マップは、
【０１２４】
【数７】

$$f\big(x(i),y(i)\big) = f(x(i),y(i))^{common} mod\ p, \qquad 式5$$

【０１２５】
に基づいて修正され得る。
【０１２６】
[00138]ある特定の実施形態では、モバイルデバイス１０２の認証データ生成器１１０および認証デバイス１０４の認証データ生成器は、共通の数の特徴（たとえば、スパイク）を含むように、モバイルデバイス１０２および認証デバイス１０４の密度マップを修正することができる。たとえば、モバイルデバイス１０２の第１の密度マップは第１の数の特徴（たとえば、６つ）を含んでよく、認証デバイス１０４の第２の密度マップは第２の数（たとえば、５つ）の特徴を含んでよい。特徴の第１の数は特徴の第２の数より小さい（または大きい）ことがある。モバイルデバイス１０２の第１の修正された密度マップは、第１の数の特徴（または第２の数の特徴）を含み得る。認証デバイス１０４の第２の修正された密度マップは、第１の数の特徴（または第２の数の特徴）を含み得る。
【０１２７】
[00139]ある特定の実施形態では、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４を生成するために、指紋の形状および／またはサイズを修正することができる。ある特定の実施形態では、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４を生成するために、非バイオメトリックデータ１７６に基づいて、ぼかし関数、回転関数、シェーディング関数、ノイズ関数、またはこれらの組合せを、バイオメトリック特徴１８２に適用することができる。
【０１２８】
[00140]方法５００はまた、５０６において、新たなバイオメトリックデータを生成することを含み得る。たとえば、図１の認証データ生成器１１０は、図１および図４を参照して説明されるように、修正されたバイオメトリック特徴１８４に基づいて第２のバイオメトリックデータ１８０を生成することができる。バイオメトリックデータ１７０は、指紋、虹彩スキャン、顔の画像、または発話信号に対応し得る。認証データ生成器１１０は、修正されたバイオメトリック特徴１８４に基づいて、第２の指紋、第２の虹彩スキャン、第２の顔の第２の画像、または第２の発話信号を生成することができ、第２のバイオメトリックデータ１８０は、第２の指紋、第２の虹彩スキャン、第２の顔の第２の画像、または第２の発話信号を含み得る。
【０１２９】
[00141]たとえば、認証データ生成器１１０は、修正されたスパイク、修正された密度マップ、および修正された方向マップに基づいて、第２の指紋を生成することができる。

例示すると、認証データ生成器１１０は、第１のフィルタを修正されたスパイクに適用することによって、中間の指紋を生成することができる。第１のフィルタは修正された方向マップに対応し得る。認証データ生成器１１０は、第２のフィルタを中間の指紋に適用することによって、第２の指紋を生成することができる。第２のフィルタは修正された密度マップに対応し得る。

【０１３０】

[00142]ある特定の実施形態では、第２の指紋は、修正されたスパイクを含むことがあり、修正されたサイズを有することがあり、修正された形状を有することがあり、またはこれらの組合せであることがある。ある特定の実施形態では、第２の指紋または第２の指紋の部分は、指紋と比較して、ぼかされていることがあり、回転されていることがあり、シェーディングされていることがあり、ノイズが多いことがあり、またはこれらの組合せであることがある。

【０１３１】

[00143]したがって、方法５００は、非バイオメトリックデータに基づいてユーザの第１のバイオメトリックデータを修正することによる、第２のバイオメトリックデータの生成を可能にし得る。ユーザは、認証のためにバイオメトリックデータを使用するコンピュータセキュリティシステムへの登録および認証の間に、第２のバイオメトリックデータを使用することができる。ユーザは、コンピュータセキュリティシステムの再設計を伴わずに、認証のための構成可能なバイオメトリックデータを使用することができる。

【０１３２】

[00144]図６を参照すると、認証データを生成するためにある特定の画像を選択するように構成されるシステムのある特定の実施形態の図が開示されており、全体的に６００と指定されている。認証データは、バイオメトリックデータおよび非バイオメトリックデータに基づいて生成され得る。特定の実施形態では、システム６００は図１のシステム１００に対応し得る。たとえば、システム６００は、図１の認証データ生成器１１０、画像マッピング１９２、画像１９０、またはこれらの組合せを含み得る。

【０１３３】

[00145]画像１９０は、第１の画像６２２、第２の画像６２４、第３の画像６２６、またはこれらの組合せを含み得る。ある特定の実施形態では、図１の第１の画像１９４は、第１の画像６２２、第２の画像６２４、または第３の画像６２６に対応し得る。画像マッピング１９２は、第１のバイオメトリック特徴６３２が第１の画像６２２にマッピングすること、第２のバイオメトリック特徴６３４が第２の画像６２４にマッピングすること、第３のバイオメトリック特徴６３６が第３の画像６２６にマッピングすること、またはこれらの組合せを示し得る。ある特定の実施形態では、バイオメトリック特徴６３２、６３４、および６３６は、指紋のスパイク、虹彩スキャンの虹彩特徴、顔の画像の顔特徴、または発話信号の発話特徴に対応し得る。たとえば、第１のバイオメトリック特徴６３２は、単一の渦と単一のデルタとを含み得る。第２のバイオメトリック特徴６３４は、渦を含まないことがあり、複数の渦を含むことがあり、デルタを含まないことがあり、または複数のデルタを含むことがある。第２のバイオメトリック特徴６３４はまた、２つ以上のループを含むことがある。第３のバイオメトリック特徴６３６は、渦を含まないことがあり、複数の渦を含むことがあり、デルタを含まないことがあり、または複数のデルタを含むことがある。第３のバイオメトリック特徴６３６はまた、２つよりも少ないループを含むことがある。

【０１３４】

[00146]別の例として、第１のバイオメトリック特徴６３２は、第１の範囲の瞳孔サイズを含み得る。第２のバイオメトリック特徴６３４は第２の範囲の瞳孔サイズを含むことがあり、ここで第２の範囲は第１の範囲の外にある。第２のバイオメトリック特徴６３４はまた、第１の数以上のクリプトを含むことがある。第３のバイオメトリック特徴６３６は、第２の範囲の瞳孔サイズと、第１の数未満のクリプトとを含むことがある。

【０１３５】

[00147]さらなる例として、第１のバイオメトリック特徴６３２は、第１の形状の頭を含むことがある。第２のバイオメトリック特徴６３４は、第１の形状以外の形状の頭を含むことがあり、目と目の間の第１の範囲の距離を含むことがある。第３のバイオメトリック特徴６３６は、第１の形状以外の形状の頭を含むことがあり、目と目の間の第２の範囲の距離を含むことがあり、第２の範囲は第１の範囲と別である。

【０１３６】

[00148]さらに別の例として、第１のバイオメトリック特徴６３２は、第１のセットのフォルマント位置を含むことがある。第２のバイオメトリック特徴６３４は、第１のセットとは別の第２のセットのフォルマント位置を含むことがあり、第１の範囲のスペクトル傾斜を含むことがある。第３のバイオメトリック特徴６３６は、第２のセットのフォルマント位置を含むことがあり、第１の範囲とは別の第２の範囲のスペクトル傾斜を含むことがある。

【０１３７】

[00149]動作の間に、図１の認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０と非バイオメトリックデータ１７６（たとえば、鍵）とを受信することができる。バイオメトリックデータ１７０は指紋スキャンに対応してよく、非バイオメトリックデータ１７６は（たとえば、図１のユーザ入力１７２に基づいて）ユーザにより定義されてよい。非バイオメトリックデータ１７６は、第１の鍵６０８（たとえば、「９１２２」）、第２の鍵６１０（たとえば、「１０３４」）、または第３の鍵６１２（たとえば、「４２１４」）に対応してよく、またはそれらを含んでよい。

【０１３８】

[00150]図１および図４～図５を参照して説明されるように、認証データ生成器１１０は、バイオメトリックデータ１７０からバイオメトリック特徴１８２を抽出することができ、非バイオメトリックデータ１７６に基づいてバイオメトリック特徴１８２を修正することによって、修正されたバイオメトリック特徴１８４を生成することができる。たとえば、認証データ生成器１１０は、第１の鍵６０８に基づいて第１のバイオメトリック特徴６３２を生成することができ、第２の鍵６１０に基づいて第２のバイオメトリック特徴６３４を生成することができ、または、第３の鍵６１２に基づいて第３のバイオメトリック特徴６３６を生成することができる。修正されたバイオメトリック特徴１８４は、第１のバイオメトリック特徴６３２、第２のバイオメトリック特徴６３４、または第３のバイオメトリック特徴６３６を含み得る。

【０１３９】

[00151]認証データ生成器１１０は、図１の画像１９０のうちのある特定の画像を選択することができる。特定の画像は、画像マッピング１９２および修正されたバイオメトリック特徴１８４に基づいて選択され得る。たとえば、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４が第１のバイオメトリック特徴６３２を含むことと、第１のバイオメトリック特徴６３２が第１の画像６２２に対応することを画像マッピング１９２が示すこととを、決定したことに応答して、第１の画像６２２を選択することができる。別の例として、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４が第２のバイオメトリック特徴６３４を含むことと、第２のバイオメトリック特徴６３４が第２の画像６２４に対応することを画像マッピング１９２が示すこととを、決定したことに応答して、第２の画像６２４を選択することができる。さらなる例として、認証データ生成器１１０は、修正されたバイオメトリック特徴１８４が第３のバイオメトリック特徴６３６を含むことと、第３のバイオメトリック特徴６３６が第３の画像６２６に対応することを画像マッピング１９２が示すこととを、決定したことに応答して、第３の画像６２６を選択することができる。

【０１４０】

[00152]認証データ生成器１１０は、第２の画像１９６を生成するために、非バイオメトリックデータ１７６に基づいて選択された画像を修正することができる。たとえば、認証データ生成器１１０は、第１の修正された画像６０２、第２の修正された画像６０４、

または第３の修正された画像６０６を生成するために、それぞれ、第１の鍵６０８、第２の鍵６１０、または第３の鍵６１２に基づいて、第１の画像６２２、第２の画像６２４、または第３の画像６２６を修正することができる。たとえば、認証データ生成器１１０は、第１の鍵６０８に基づいて第１の修正された画像６０２を生成するために、画像処理関数（たとえば、回転関数、ぼかし関数、スケーリング、および／またはシェーディング関数）を第１の画像６２２に適用することができる。例示すると、認証データ生成器１１０は、第１の鍵６０８に基づいて回転の角度（たとえば、９０度）を決定することができ、回転の角度に基づいて第１の画像６２２を回転することによって、第１の修正された画像６０２を生成することができる。

【０１４１】

[00153]別の例として、認証データ生成器１１０は、第２の鍵６１０に基づいて第２の修正された画像６０４を生成するために、画像処理関数（たとえば、回転関数、ぼかし関数、スケーリング関数、および／またはシェーディング関数）を第２の画像６２４に適用することができる。例示すると、認証データ生成器１１０は、第２の鍵６１０に基づいてスケーリングの程度（たとえば、２００パーセント）を決定することができ、そのスケーリングの程度（たとえば、２００パーセント）に対応するスケーリング関数を第２の画像６２４に適用して、第２の修正された画像６０４を生成することができる。さらなる例として、認証データ生成器１１０は、第３の鍵６１２に基づいて第３の修正された画像６０６を生成するために、画像処理関数（たとえば、回転関数、ぼかし関数、スケーリング関数、および／またはシェーディング関数）を第３の画像６２６に適用することができる。例示すると、認証データ生成器１１０は、第３の鍵６１２に基づいて回転の角度（たとえば、１８０度）とぼかしの程度（たとえば、４０パーセント）とを決定することができる。認証データ生成器１１０は、回転の角度（たとえば、１８０度）に基づいて第３の画像６２６を回転することができ、そのぼかしの程度（たとえば、４０パーセント）に基づくぼかしフィルタを回転された画像に適用して、第３の修正された画像６０６を生成することができる。第２の画像１９６は、第１の修正された画像６０２、第２の修正された画像６０４、もしくは第３の修正された画像６０６に対応してよく、またはそれを含んでよい。

認証データ生成器１１０は、図１を参照して説明されるように、第２の画像１９６を送信することができる。

【０１４２】

[00154]ある特定の実施形態では、認証データ生成器１１０は、第２の画像１９６を生成するために、非バイオメトリックデータ１７６に基づいて一方向性関数を適用することによって、選択された画像（たとえば、第１の画像６２２、第２の画像６２４、または第３の画像６２６）を修正することができる。たとえば、認証データ生成器１１０は、一方向性関数を非バイオメトリックデータ１７６（たとえば、第１の鍵６０８、第２の鍵６１０、または第３の鍵６１２）に適用することによって、回転の角度、ぼかしの程度、スケーリングの程度、および／またはシェーディングの程度を決定することができ、第２の画像１９６（たとえば、第１の修正された画像６０２、第２の修正された画像６０４、または第３の修正された画像６０６）を生成するために、回転の角度、ぼかしの程度、スケーリングの程度、および／またはシェーディングの程度に基づいて、選択された画像を修正することができる。

【０１４３】

[00155]したがって、システム６００は、構成可能な認証データをユーザがバイオメトリックデータに基づいて生成することを可能にし得る。ユーザは、認証のために非バイオメトリック画像を使用するコンピュータセキュリティシステムへの登録および認証の間に、バイオメトリックデータを使用することができる。ユーザは、コンピュータセキュリティシステムの再設計を伴わずに、認証のための構成可能なバイオメトリックデータを使用することができる。バイオメトリックデータは、認証データから導出する（たとえば、リバースエンジニアリングする）ことが難しいことがあるので、バイオメトリックデータが

危うくなることの可能性が下がる。

【０１４４】

[00156]図７を参照すると、認証データを生成する方法のある特定の実施形態の図が示されており、全体的に７００と指定されている。認証データは、バイオメトリックデータを可聴化することによって生成され得る。特定の実施形態では、方法７００は図１の認証データ生成器１１０によって実行され得る。

【０１４５】

[00157]方法７００は、図４のアラインメント４０２と特徴抽出４０４とを含み得る。たとえば、図１の認証データ生成器１１０は、図３～図４を参照して説明されるように、バイオメトリックデータ１７０を受信することができ、バイオメトリックデータ１７０に基づいてアラインされたバイオメトリックデータ３７０を生成することができ、アラインされたバイオメトリックデータ３７０に基づいてバイオメトリック特徴１８２を抽出することができる。

【０１４６】

[00158]方法７００はまた、７０２において、特徴移行を含み得る。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリック特徴１８２に基づいてスペクトルエンベロープ１６０を生成することができる。ある特定の実施形態では、バイオメトリック特徴１８２は、指紋のスパイク（たとえば、特異点および特徴点）を示し得る。スペクトルエンベロープ１６０は、スパイクに対応し得る。別の特定の実施形態では、バイオメトリック特徴１８２は虹彩の特徴を示すことがあり、スペクトルエンベロープ１６０は虹彩の特徴に対応することがある。さらに別の特定の実施形態では、バイオメトリック特徴１８２は顔特徴を示すことがあり、スペクトルエンベロープ１６０は顔特徴に対応することがある。

【０１４７】

[00159]方法７００はさらに、７０４において、音符シーケンスの生成を含み得る。たとえば、図１の認証データ生成器１１０は、非バイオメトリックデータ１７６（たとえば、鍵）を受信することがある。ある特定の実施形態では、認証データ生成器１１０は、図１を参照して説明されるように、図１のユーザ入力１７２を受け取ることができ、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて音符シーケンス１６２を生成することができる。たとえば、認証データ生成器１１０は、アルペジエーター（たとえば、規則に基づく音符シーケンス生成器）を使用して、音符シーケンス１６２を生成することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６（たとえば、４桁の鍵）をアルペジエーターに提供することができ、アルペジエーターは、非バイオメトリックデータ１７６に基づいて音符シーケンス１６２を生成することができる。ある特定の実施形態では、アルペジエーターは、特定の長さ（たとえば、４桁）の非バイオメトリックデータ１７６に基づいて、特定の数（たとえば、１００００個）の異なる音符シーケンスを生成することができる。

【０１４８】

[00160]音符シーケンス１６２は、コード（たとえば、メジャーコード、マイナーコード、セブンスコード、１２ピッチクラスごとにディミニッシュするコードなど）、テンポ（たとえば、毎分６０ビート、毎分１２０ビートなど）、オクターブ範囲（たとえば、１オクターブ、２オクターブ、フルレンジなど）、または音符の進行（たとえば、アップ、ダウン、アップ／ダウンなど）のうちの少なくとも１つを示し得る。たとえば、アルペジエーターは、非バイオメトリックデータ１７６に基づいて、コード（たとえば、Ｆメジャー）、テンポ（たとえば、毎分６０ビート）、オクターブ範囲（たとえば、１オクターブ）、または音符の進行（たとえば、アップ／ダウン）のうちの少なくとも１つを決定することができる。

【０１４９】

[00161]認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいてバイ

オメトリックデータ１７０を可聴化することによって、図１のオーディオデータ１９８を生成することができる。たとえば、本明細書で説明されるように、認証データ生成器１１０は、バイオメトリック特徴１８２を抽出することによって、バイオメトリック特徴１８２に基づいてスペクトルエンベロープ１６０を生成することによって、および、非バイオメトリックデータ１７６に基づいて音符シーケンス１６２を生成することによって、バイオメトリックデータ１７０を可聴化することができる。オーディオデータ１９８は、スペクトルエンベロープ１６０と音符シーケンス１６２とを含むことがあり、またはそれらに対応することがある。ある特定の実施形態では、認証データ生成器１１０は、スペクトルエンベロープ１６０と音符シーケンス１６２とを組み合わせてオーディオ信号を生成することができる。オーディオデータ１９８はオーディオ信号を含み得る。ある代替的な実施形態では、認証データ生成器１１０は、スペクトルエンベロープ１６０と音符シーケンス１６２とを送信することができる。この実施形態では、図１の認証デバイス１０４におけるデコーダは、スペクトルエンベロープ１６０と音符シーケンス１６２とを組み合わせてオーディオ信号を生成することができる。オーディオデータ１９８は、スペクトルエンベロープ１６０と音符シーケンス１６２とを含み得る。

【０１５０】

[00162]ある特定の実施形態では、認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいてバイオメトリックデータ１７０を修正することによって、第２のバイオメトリックデータ１８０を生成することができる。認証データ生成器１１０は、第２のバイオメトリックデータ１８０に基づいてオーディオデータ１９８を生成することができる。たとえば、認証データ生成器１１０は、第２のバイオメトリックデータ１８０の特徴を抽出することができ、特徴に基づいてスペクトルエンベロープを生成することができる。オーディオデータ１９８は、第２のバイオメトリックデータ１８０の特徴に基づいて生成されたスペクトルエンベロープを含み得る。

【０１５１】

[00163]ある特定の実施形態では、認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて第２の画像１９６を生成することができる。認証データ生成器１１０は、第２の画像１９６を可聴化することによってオーディオデータ１９８を生成することができる。たとえば、オーディオデータのマッピングは、画像（たとえば、画像１９０、画像１９０の修正されたバージョン、および／または第２の画像１９６）をオーディオデータ（たとえば、スペクトルエンベロープ）にマッピングすることができる。認証データ生成器１１０は、オーディオデータのマッピング（たとえば、スペクトルエンベロープ）および第２の画像１９６に基づいてオーディオデータ１９８を選択することができる。

【０１５２】

[00164]ある特定の実施形態では、認証データ生成器１１０は、バイオメトリックデータ１７０を変換する（たとえば、可聴化する）ことによってオーディオデータ１９８を生成することができる。たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０に基づいて第１のオーディオデータ（たとえば、スペクトルエンベロープ１６０、第１の音波、搬送波信号など）を生成することができる。認証データ生成器１１０は、非バイオメトリックデータ１７６に基づいて第２のオーディオデータ（たとえば、第２のスペクトルエンベロープ、第２の音波、変調信号など）を生成することができる。たとえば、オーディオデータのマッピングは、非バイオメトリックデータ１７６の値をオーディオデータ（たとえば、スペクトルエンベロープ、音波、搬送波信号など）をマッピングすることができる。認証データ生成器１１０は、オーディオデータのマッピングおよび非バイオメトリックデータ１７６に基づいて第２のオーディオデータ（たとえば、第２のスペクトルエンベロープ、第２の音波、変調信号など）を選択することができる。認証データ生成器１１０は、第１のオーディオデータ（たとえば、スペクトルエンベロープ１６０、第１の音波、搬送波信号など）と第２のオーディオデータ（たとえば、第２のスペクトルエンベロープ、第２の音波、搬送波の変調など）を組み合わせることによって、オーディオデ

ータ１９８を生成することができる。
【０１５３】
[00165]ある特定の実施形態では、認証データ生成器１１０は、バイオメトリックデータ１７０を特定の聴覚範囲（たとえば、特定の可聴範囲、特定の非可聴範囲、または可聴の音と非可聴の音とを含むある範囲）内のオーディオ音声にマッピングすることによって、オーディオデータ１９８を生成することができる。たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０からバイオメトリック特徴１８２を抽出することができる。認証データ生成器１１０は、特定の聴覚範囲内に入るようにバイオメトリック特徴１８２の値を正規化することによって、バイオメトリックデータ１７０を音符シーケンスに変換することができる。たとえば、バイオメトリック特徴１８２に含まれる最高の値は特定の聴覚範囲の最大の値（たとえば、最高の周波数）に対応することがあり、バイオメトリック特徴１８２に含まれる最低の値は特定の聴覚範囲の最小の値（たとえば、最低の周波数）に対応することがある。認証データ生成器１１０は、バイオメトリックデータ１７０を音符シーケンスに変換するために非線形量子化または線形量子化を使用することができる。ある特定の実施形態では、認証データ生成器１１０は、特定の音調（たとえば、Ｄメジャー、Ｄマイナーなど）に対応する音符シーケンスにバイオメトリックデータ１７０を変換することができる。
【０１５４】
[00166]したがって、方法７００は、オーディオ認証データをユーザがバイオメトリックデータに基づいて生成することを可能にし得る。バイオメトリックデータは、非オーディオデータ（たとえば、画像データ）であり得る。ユーザは、認証のためにオーディオデータを使用するコンピュータセキュリティシステムへの登録および認証の間に、非オーディオバイオメトリックデータを使用することができる。ユーザは、コンピュータセキュリティシステムの再設計を伴わずに、認証のために非オーディオバイオメトリックデータを使用することができる。
【０１５５】
[00167]図８を参照すると、スペクトルエンベロープを生成するように構成されるシステムのある特定の実施形態の図が示されており、全体的に８００と指定されている。システム８００は、非バイオメトリックデータに基づいてバイオメトリックデータを可聴化することによって、スペクトルエンベロープを生成することができる。特定の実施形態では、システム８００は図１のシステム１００に対応し得る。たとえば、システム８００は、図１の認証データ生成器１１０を含み得る。
【０１５６】
[00168]動作の間に、認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０を受信することができる。バイオメトリックデータ１７０は、画像データ（たとえば、指紋スキャン、虹彩スキャン、または顔の画像）であり得る。認証データ生成器１１０は、バイオメトリックデータ１７０をある特定の数（たとえば、Ｋ個）のセグメント８０２に分割することができる。認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０からバイオメトリック特徴１８２（たとえば、指紋の特異点および特徴点、虹彩特徴、または顔特徴）を抽出することができる。虹彩特徴は、放射状のファロー、同心円のファロー、クリプト、捲縮輪、および／または瞳孔サイズを含み得る。セグメント８０２の特定のセグメント（ｒ）は、バイオメトリック特徴１８２のサブセットを含み得る。図１のメモリ１３２は、コサイン基底関数８０６を記憶し得る。コサイン基底関数８０６は、デフォルト値を含み得る。コサイン基底関数８０６の各々は、セグメント８０２の特定のセグメント（たとえば、ｒ）に対応し得る。
【０１５７】
[00169]認証データ生成器１１０は、バイオメトリック特徴１８２（たとえば、指紋の特異点および特徴点、虹彩特徴、または顔特徴）に基づいて、セグメント８０２に対応する振幅ベクトル８０４を生成することができる。たとえば、振幅ベクトル８０４は

【０１５８】
【数８】

$$a(r) = \sum_{l=1}^{N} \| p(r,l) - k(r) \| + c(r), \qquad \text{式６}$$

【０１５９】
によって与えられることが可能であり、ここで、ａ（ｒ）はセグメントｒに対応する振幅ベクトル８０４の振幅値であり、ｐ（ｒ，ｌ）はｒに含まれる特定のスパイク（または虹彩特徴または顔特徴）であり、ｋ（ｒ）はｒの局所基準点（たとえば、中心座標）であり、ｃ（ｒ）はコサイン基底関数８０６の対応するコサイン基底関数と関連付けられる特定の重みである。特定の重み（ｃ（ｒ））はデフォルト値であり得る。振幅値ａ（ｒ）は、対応するセグメント（たとえば、ｒ）がスパイク（または虹彩特徴または顔特徴）を含まない場合、特定のデフォルト値（たとえば、０）を有し得る。
【０１６０】
[00170]認証データ生成器１１０は、振幅ベクトル８０４およびコサイン基底関数８０６に基づいてメルバンド対数エンベロープを生成することができる。メルバンド対数エンベロープは、
【０１６１】
【数９】

$$\text{mel-band envelope (log)} = \sum_{r=1}^{K} a(r)\cos(2\pi f(r)t), \qquad \text{式７}$$

【０１６２】
によって与えられることが可能であり、ここでｆ＝周波数およびｔ＝時間である。認証データ生成器１１０は、メルバンドエンベロープ上でメル周波数から線形周波数への変換を実行することによって、スペクトルエンベロープ１６０を生成することができる。
【０１６３】
[00171]したがって、システム８００は画像データの可聴化を可能にし得る。たとえば、スペクトルエンベロープは、指紋スキャン、虹彩スキャン、または顔の画像に基づいて生成され得る。スペクトルエンベロープは、オーディオ認証データを生成するために使用され得る。
【０１６４】
[00172]図９を参照すると、指紋のスパイクのある特定の実施形態の図が示されており、全体的に９００と指定されている。スパイク９００は特異点９０２と特徴点９０４とを含む。特異点９０２は、渦９０６と、ループ９０８と、デルタ９１０とを含む。特徴点９０４は、稜線９１２と、分岐９１４と、終端９１６とを含む。
【０１６５】
[00173]図１０を参照すると、バイオメトリックデータのアラインメントの図が示されており、全体的に１０００と指定されている。図１０００は、バイオメトリックデータ１７０とバイオメトリックデータ１０７０とを含む。バイオメトリックデータ１０７０はメモリ１３２に記憶され得る。
【０１６６】
[00174]ある特定の実施形態では、バイオメトリックデータ１０７０はテンプレートバイオメトリックデータに対応し得る。ある代替的な実施形態では、図１の認証データ生成器１１０は、登録フェーズの間にバイオメトリックデータ１０７０を受信することができ、認証フェーズの間にバイオメトリックデータ１７０を受信することができる。ある特定の実施形態では、バイオメトリックデータ１０７０は、認証データ生成器１１０によって受信されるバイオメトリックデータのサブセットを含み得る。たとえば、認証データ生成器１１０は、指紋スキャン、虹彩スキャン、または顔の画像を受信することができる。認証データ生成器１１０は、指紋スキャン、虹彩スキャン、または顔の画像と関連付けられるデータの一部分（たとえば、曲率情報）を、バイオメトリックデータ１０７０としてメモリ１３２に記憶することができる。

【０１６７】
[00175]動作の間に、認証データ生成器１１０は、バイオメトリックデータ１７０（たとえば、指紋スキャン、虹彩スキャン、または顔の画像）をバイオメトリックデータ１０７０と揃えるようにバイオメトリックデータ１７０を修正することによって、図３のアラインされたバイオメトリックデータ３７０を生成することができる。たとえば、認証データ生成器１１０は、バイオメトリックデータ１０７０の第１のアラインメント特徴と、バイオメトリックデータ１７０の第２のアラインメント特徴とを決定することができる。ある特定の実施形態では、バイオメトリックデータ１７０は指紋スキャンに対応し、第１のアラインメント特徴は、バイオメトリックデータ１０７０によって示される、第１の湾曲点（たとえば、高曲率点）、第１の特異点、または両方に対応し、第２のアラインメント特徴は、バイオメトリックデータ１７０によって示される、第２の湾曲点（たとえば、高曲率点）、第２の特異点、または両方に対応する。ある代替的な実施形態では、バイオメトリックデータ１７０は虹彩スキャン（または顔の画像）に対応し、第１のアラインメント特徴はバイオメトリックデータ１０７０によって示される第１の虹彩特徴（または第１の顔特徴）に対応し、第２のアラインメント特徴はバイオメトリックデータ１７０によって示される第２の虹彩特徴（または第２の顔特徴）に対応する。

【０１６８】
[00176]認証データ生成器１１０は、第１のアラインメント特徴および第２のアラインメント特徴に基づいて、バイオメトリックデータ１７０をバイオメトリックデータ１０７０と揃えるようにバイオメトリックデータ１７０を修正することができる。たとえば、認証データ生成器１１０は、第１のアラインメント特徴と第２のアラインメント特徴の比較に基づいて、バイオメトリックデータ１７０に適用すべき変換関数を決定することができる。ある特定の実施形態では、認証データ生成器１１０は、第１の湾曲点、第１の特異点、または両方を、第２の湾曲点、第２の特異点、または両方と比較することができる。

【０１６９】
[00177]認証データ生成器１１０は、この比較に基づいて変換関数を決定することができる。たとえば、変換関数は、第２のアラインメント特徴（たとえば、第１の湾曲点、第１の特異点、または両方）を第１のアラインメント特徴（たとえば、第２の湾曲点、第２の特異点、または両方）と揃える、スケーリング関数、回転関数、および／または変換関数を含み得る。たとえば、認証データ生成器１１０は、アラインされたバイオメトリックデータ３７０の第２のアラインメント特徴が、バイオメトリックデータ１０７０の第１のアラインメント特徴の第１の座標と同じ座標を有する（または閾値の距離以内の座標を有する）ように、変換関数を決定することができる。認証データ生成器１１０は、図３のアラインされたバイオメトリックデータ３７０を生成するために、変換関数をバイオメトリックデータ１７０に適用することができる。

【０１７０】
[00178]バイオメトリックデータのアラインメントは、予想されるバイオメトリックデータとのバイオメトリックデータの一致度を上げることができ、誤った未検出の可能性を下げることができる。たとえば、バイオメトリックデータ１０７０は第１の指紋に基づいて登録フェーズの間に生成されてよく、バイオメトリックデータ１７０は第２の指紋に基づいて認証フェーズの間に生成されてよい。バイオメトリックデータ１７０をバイオメトリックデータ１０７０と揃えることで、バイオメトリックデータ１７０およびバイオメトリックデータ１０７０が同じ指の関連する指紋であるときの、アラインされたバイオメトリックデータ３７０をバイオメトリックデータ１０７０と比較することと関連付けられる信頼性スコアを上げることができる。

【０１７１】
[00179]図１１を参照すると、認証データを生成するように構成されるシステムのある特定の実施形態の図が示されており、全体的に１１００と指定されている。ある特定の実施形態では、システム１１００は図１のシステム１００に対応し得る。システム１１００はテレバンキングの使用事例と関連付けられ得る。

【０１７２】
[00180]システム１１００はモバイルデバイス１０２を含む。モバイルデバイス１０２は指紋センサ１１０８を含む。動作の間に、ユーザ１０６は、テレバンキングシステムへの電話呼の間にアカウント（たとえば、銀行口座）にアクセスするために、図１の認証データ１７８を提供するように促され得る。ユーザ１０６は、バイオメトリックデータ１７０をモバイルデバイス１０２の認証データ生成器１１０に提供するために、指紋センサ１１０８の上に、またはその近くに指を置くことができる。モバイルデバイス１０２は、認証データ生成器１１０に結合された話者および／または発話認識器（話者／発話認識器）１１０４を含み得る。ある特定の実施形態では、認証データ生成器１１０は、話者／発話認識器１１０４を含み得る。

【０１７３】
[00181]ユーザ１０６は、モバイルデバイス１０２に結合されたマイクロフォンに向かって話す（たとえば、「いち－に－さん－し」）ことによって、ユーザ入力１７２を話者／発話認識器１１０４に提供することができる。話者／発話認識器１１０４は、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。たとえば、話者／発話認識器１１０４は、ユーザ入力１７２に対して話者認識を実行することによって、信頼性スコア（たとえば、８３％または０．８３）を生成することができる。話者／発話認識器１１０４はまた、ユーザ入力１７２に対して発話認識を実行することによって、テキスト（たとえば、「１２３４」）または数（たとえば、１２３４）を生成することができる。話者／発話認識器１１０４は、信頼性スコア、テキスト（または数）、または両方に基づいて、非バイオメトリックデータ１７６を生成することができる。

【０１７４】
[00182]モバイルデバイス１０２はユーザ選好１１０６を含み得る。たとえば、ユーザ選好１１０６は図１のメモリ１３２に記憶され得る。ユーザ選好１１０６は、生成されるべき認証データのタイプ（たとえば、オーディオデータ、第２の（たとえば、非バイオメトリック）画像データ、または第２のバイオメトリックデータ）を示し得る。認証データ生成器１１０は、バイオメトリックデータ１７０、非バイオメトリックデータ１７６、およびユーザ選好１１０６に基づいて認証データ１７８を生成することができる。たとえば、オーディオデータ（たとえば、図１のオーディオデータ１９８）が生成されるべきであることをユーザ選好１１０６が示すとき、認証データ生成器１１０は、図１を参照して説明されるように、オーディオデータを生成するために非バイオメトリックデータ１７６に基づいてバイオメトリックデータ１７０を可聴化することができる。別の例として、第２の画像（たとえば、図１の第２の画像１９６）が生成されるべきであることをユーザ選好１１０６が示すとき、認証データ生成器１１０は、図１を参照して説明されるように、非バイオメトリックデータ１７６およびバイオメトリックデータ１７０に基づいて第２の画像を生成することができる。追加の例として、第２のバイオメトリックデータ（たとえば、図１の第２のバイオメトリックデータ１８０）が生成されるべきであることをユーザ選好１１０６が示すとき、認証データ生成器１１０は、図１を参照して説明されるように、非バイオメトリックデータ１７６およびバイオメトリックデータ１７０に基づいて第２のバイオメトリックデータを生成することができる。

【０１７５】
[00183]認証データ生成器１１０は、図１を参照して説明されるように、認証データ１７８（たとえば、オーディオデータ１９８、第２の画像１９６、または第２のバイオメトリックデータ１８０）を送信することができる。たとえば、モバイルデバイス１０２は、テレバンキングシステムへの電話呼の間に認証データ１７８を提供することができる。テレバンキングシステムは、認証データ１７８（たとえば、オーディオデータ１９８）に基づいて登録または認証を実行することができる。たとえば、登録の間に、テレバンキングシステムはオーディオデータ１９８を登録オーディオデータ（たとえば、パスワード）として記憶することができる。別の例として、認証の間に、テレバンキングシステムは、オーディオデータ１９８を登録オーディオデータと比較することによって信頼性スコアを決

定することができ、信頼性スコアが認証閾値を満たすことに基づいて銀行口座へのアクセス権を提供することができる。

【０１７６】

[00184]したがって、システム１１００は、認証データをユーザが指紋および発話信号に基づいて生成することを可能にし得る。ユーザは、発話信号を生成するために使用される語句を変更することによって、認証データを構成することができる。認証データは、バイオメトリックデータに基づくものであり、ユーザが認証データを生成するために簡単で覚えやすい語句を提供するとしても、比較的セキュアであると考えられ得る。

【０１７７】

[00185]図１２を参照すると、認証データを生成するように構成されるシステムのある特定の実施形態の図が示されており、全体的に１２００と指定されている。ある特定の実施形態では、システム１２００は図１のシステム１００に対応し得る。システム１２００はテレバンキングの使用事例と関連付けられ得る。

【０１７８】

[00186]システム１２００はモバイルデバイス１０２を含む。モバイルデバイス１０２はスマートアイウェアを含み得る。モバイルデバイス１０２は、マイクロフォン１２０２、虹彩スキャンセンサ１２０８、もしくは両方に結合されてよく、または含んでよい。動作の間に、ユーザ１０６は、目を虹彩スキャンセンサ１２０８の近くに置くことによって、バイオメトリックデータ１７０（たとえば、虹彩スキャン）を提供することができる。ユーザ１０６は、マイクロフォン１２０２を介してユーザ入力１７２を提供することができる。図１１を参照してさらに説明されるように、認証データ生成器１１０は、ユーザ選好１１０６、非バイオメトリックデータ１７６、およびバイオメトリックデータ１７０に基づいて、認証データ１７８を生成することができる。

【０１７９】

[00187]したがって、システム１２００は、認証データをユーザが虹彩スキャンおよび発話信号基づいて生成することを可能にし得る。ユーザは、発話信号を生成するために使用される語句を変更することによって、認証データを構成することができる。認証データは、バイオメトリックデータに基づくものであり、ユーザが認証データを生成するために簡単で覚えやすい語句を提供するとしても、比較的セキュアであると考えられ得る。

【０１８０】

[00188]図１３を参照すると、可聴化されたオーディオ信号を生成する方法のある特定の実施形態の図が示されており、全体的に１３００と指定されている。可聴化されたオーディオ信号はバイオメトリックデータに基づいて生成され得る。ある特定の実施形態では、方法１３００の１つまたは複数の動作は、認証データ生成器１１０、認証デバイス１０４、または両方によって実行され得る。

【０１８１】

[00189]方法１３００は、１３０２において、指紋スキャンを受信することを含む。たとえば、図１１を参照して説明されるように、ユーザ１０６は、指紋センサ１１０８にタッチすることによってバイオメトリックデータ１７０を提供することができ、認証データ生成器１１０は、バイオメトリックデータ１７０を受信することができる。

【０１８２】

[00190]方法１３００はまた、１３０４において、パスワードを受信することを含む。たとえば、図１を参照して説明されるように、ユーザ１０６は、パスワードを話すことによってユーザ入力１７２を提供することができ、認証データ生成器１１０は、ユーザ入力１７２を受信することができる。

【０１８３】

[00191]方法１３００はさらに、１３０６において、変形されたデータを生成することと、ユーザの選好の設定に基づいて変形されたデータを可聴化することとを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０から抽出されたバイオメトリック特徴１８２を修正することによって、

修正されたバイオメトリック特徴１８４を生成することができる。認証データ生成器１１０は、図１を参照して説明されるように、修正されたバイオメトリック特徴１８４を可聴化することによって、オーディオデータ１９８を生成することができる。認証データ生成器１１０は、図１１を参照して説明されるように、ユーザ選好１１０６に基づいて、オーディオデータ１９８を生成することができる。

【０１８４】

[00192]方法１３００はまた、１３０８において、ユーザの確認のために、可聴化されたデータをラウドスピーカーを介して音声として出力することを含む。たとえば、認証データ生成器１１０は、モバイルデバイス１０２に結合されたスピーカーを介して、認証データ１７８を出力することができる。ユーザ１０６は、図１を参照して説明されるように、スピーカーによって提供される認証データ１７８を受け入れ、または拒絶することができる。

【０１８５】

[00193]方法１３００はさらに、１３１０において、可聴化されたオーディオ信号を遠端のデバイス（たとえば、銀行における）に送信することを含む。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、認証データ１７８を認証デバイス１０４に送信することができる。認証デバイス１０４は、銀行と関連付けられ得る（たとえば、テレバンキングシステム）。

【０１８６】

[00194]方法１３００はまた、１３１２において、遠端のデバイスによって可聴化されたオーディオ信号を保存することを含む。たとえば、図１の認証デバイス１０４は、（たとえば、登録フェーズの間に受信された）認証データ１７８を登録認証データとしてメモリに記憶することができる。

【０１８７】

[00195]方法１３００はさらに、１３１４において、遠端のデバイスによる認証のために可聴化されたオーディオ信号を使用することを含み得る。たとえば、図１の認証デバイス１０４は、図１を参照して説明されるように、（たとえば、認証フェーズの間に受信された）認証データ１７８を認証のために使用することができる。たとえば、認証デバイス１０４は、認証データ１７８を登録認証と比較することができ、比較に基づいてユーザ１０６にアカウント（たとえば、銀行口座）へのアクセス権を選択的に提供することができる。

【０１８８】

[00196]したがって、方法１３００は、構成可能で比較的セキュアな認証データをユーザが指紋およびパスワードに基づいて生成することを可能にし得る。ユーザは、パスワードを変更することによって認証データを再構成することができる。認証データは、指紋から生成されるので、比較的セキュアであると考えられ得る。

【０１８９】

[00197]図１４を参照すると、認証データを生成する方法のある特定の実施形態の図が示されており、全体的に１４００と指定されている。認証データは、バイオメトリックデータおよび非バイオメトリックデータを共通のフォーマットに変換することによって生成され得る。ある特定の実施形態では、方法１４００の１つまたは複数の動作は、図１の認証データ生成器１１０、認証デバイス１０４、または両方によって実行され得る。

【０１９０】

[00198]方法１４００は、１４０２において、指紋の採取／虹彩のスキャンを含む。たとえば、認証データ生成器１１０は、第１のフォーマット（たとえば、画像データ）の第１のバイオメトリックデータ１４７０（たとえば、指紋スキャンおよび／または虹彩スキャン）を受信することができる。例示すると、認証データ生成器１１０は、指紋センサ、虹彩スキャンセンサ、または両方を介して、第１のバイオメトリックデータ１４７０を受信することができる。ある特定の実施形態では、認証データ生成器１１０は、モバイルデバイス１０２に結合されるカメラを介して第１のバイオメトリックデータ１４７０（たと

えば、顔の画像）を受信することができる。
【０１９１】
[00199]方法１４００はまた、１４０４において、オーディオ／声の記録を含む。たとえば、図１の認証データ生成器１１０は、第２のフォーマット（たとえば、オーディオデータ）の第２のバイオメトリックデータ１４７２（たとえば、発話信号、声紋など）を受信することができる。例示すると、認証データ生成器１１０は、モバイルデバイス１０２に結合されるマイクロフォンを介して第２のバイオメトリックデータ１４７２を受信することができる。
【０１９２】
[00200]方法１４００はさらに、１４０６において、可聴化を含む。たとえば、認証データ生成器１１０は、共通のフォーマットを有するように第１のバイオメトリックデータ１４７０と第２のバイオメトリックデータ１４７２とを変換することができる。図１４に示される実施形態では、認証データ生成器１１０は、第１のバイオメトリックデータ１４７０をあるオーディオフォーマットに変換することによって、画像オーディオ１４０８を生成することができる。たとえば、認証データ生成器１１０は、第１のバイオメトリックデータ１４７０のスペクトログラムを生成することができる。スペクトログラムは、特定の時間における、特定の周波数と関連付けられる特定の振幅値を示し得る。第１のバイオメトリックデータ１４７０は、正方形の格子を有するビットマップ画像に対応し得る。各正方形は、正方形の強度、色、または両方を示す特定の値を有し得る。格子の水平軸はスペクトログラムの時間軸に対応してよく、格子の垂直軸はスペクトログラムの周波数軸に対応してよい。正方形の値はスペクトログラムの振幅に対応し得る。
【０１９３】
[00201]認証データ生成器１１０は、スペクトログラムから特徴を抽出することができる。たとえば、特徴は、特定の時間における、特定の周波数と関連付けられる特定の振幅値を示し得る。認証データ生成器１１０は、スペクトログラムに基づいて、音符シーケンスに対応する画像オーディオ１４０８を生成することができる。たとえば、画像オーディオ１４０８は、特定の時間における特定の周波数の特定の振幅値に対応する特定の音符を含み得る。
【０１９４】
[00202]方法１４００はまた、１４０８において、組合せを含む。たとえば、図１の認証データ生成器１１０は、第２のバイオメトリックデータ１４７２と画像オーディオ１４０８とを組み合わせることができる。例示すると、認証データ生成器１１０は、第２のバイオメトリックデータ１４７２と画像オーディオ１４０８とをインターリーブし、または連結して、バイオメトリックデータ１７０を生成することができる。
【０１９５】
[00203]方法１４００はさらに、１４１０において、可聴化されたバイオメトリックオーディオの記憶と送信とを含む。たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０を図１のメモリ１３２に記憶することができる。認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて認証データ１７８を生成することができる。ある特定の実施形態では、認証データ生成器１１０は、第２のバイオメトリックデータ１４７２から非バイオメトリックデータ１７６を生成することができる。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、第２のバイオメトリックデータ１４７２に対して発話認識、話者認識、または両方を実行して、非バイオメトリックデータ１７６を生成することができる。ある代替的な実施形態では、認証データ生成器１１０は、第１のバイオメトリックデータ１４７０と第２のバイオメトリックデータ１４７２とを受信することとは独立に、非バイオメトリックデータ１７６を受信することができる。認証データ生成器１１０は、図１を参照して説明されるように、送受信機１４２を介して認証データ１７８を認証デバイス１０４に送信することができる。
【０１９６】

[00204]方法１４００はまた、１４１２において、認証を含む。たとえば、認証デバイス１０４は、図１を参照して説明されるように、認証データ１７８に基づいて認証を実行することができる。例示すると、認証デバイス１０４は、認証データ１７８（たとえば、認証フェーズの間に受信された）を登録データ（たとえば、登録フェーズの間に受信された）と比較して、信頼性スコアを決定することができる。認証デバイス１０４は、信頼性スコアが認証閾値を満たすと決定したことに応答して、特定の機能またはアプリケーションへのアクセス権を提供する（たとえば、アンロックする）ことができる。たとえば、認証デバイス１０４は、信頼性スコアが認証閾値を満たすと決定したことに応答して、アカウント（たとえば、銀行口座、メールアカウント、ソーシャルメディアアカウント、保険口座、健康管理アカウントなど）へのアクセスを可能にし得る。別の例として、認証デバイス１０４は、信頼性スコアが認証閾値を満たすと決定したことに応答して、ネットワークファイルリポジトリ（たとえば、ソフトウェアリポジトリ、ドキュメントリポジトリ、音楽リポジトリ、ビデオリポジトリなど）へのアクセス権を提供することができる。ある特定の実施形態では、認証デバイス１０４は、認証が成功したと決定したことに応答して、デバイス１０２の特定の機能へのアクセス権を提供する（またはアンロックする）ことができる。たとえば、認証デバイス１０４は、信頼性スコアが認証閾値を満たすと決定したことに応答して、デバイス１０２のカメラへのアクセス権を提供することができる。

【０１９７】

[00205]したがって、方法１４００は、第１のフォーマットを有する第１のバイオメトリックデータおよび第２のフォーマットを有する第２のバイオメトリックデータに基づいて、バイオメトリックデータをジェネレーティングすることができる。認証データは、バイオメトリックデータおよび非バイオメトリックデータに基づいて生成され得る。したがって、方法１４００は、異なるタイプのバイオメトリックデータの組合せに基づいて認証データを生成することを可能にし得る。こうして得られた認証データから第１のバイオメトリックデータおよび／または第２のバイオメトリックデータを導出する（たとえば、リバースエンジニアリング）ことは、単一のタイプのバイオメトリックデータから生成された認証データからそれらを導出するよりも、難しいことがある。

【０１９８】

[00206]図１５を参照すると、認証データを生成するように構成されるシステムのある特定の実施形態の図が示されており、全体的に１５００と指定されている。ある特定の実施形態では、システム１５００は図１のシステム１００に対応し得る。システム１５００はテレバンキングの使用事例と関連付けられ得る。

【０１９９】

[00207]システム１５００は、図１の認証データ生成器１１０がユーザ入力１７２を遠端のデバイス（たとえば、図１の認証デバイス１０４）に送信できるという点で、システム１０００と異なる。認証データ生成器１１０は、一致スコア１５０２を認証デバイス１０４に送信することができる。たとえば、認証データ生成器１１０は、ユーザ入力１７２に対して話者認識を実行することと関連付けられる信頼性スコア（たとえば、一致スコア１５０２）を決定することができる。例示すると、認証データ生成器１１０は、ユーザ入力１７２を、ユーザ１０６と関連付けられる第１の声紋または汎用的な声紋と比較することができる。認証データ生成器１１０は、ユーザ入力１７２に基づいて第２の声紋を生成することができ、第２の声紋を第１の声紋または汎用的な声紋と比較することができる。一致スコア１５０２は比較の結果であり得る。たとえば、一致スコア１５０２は、第２の声紋と第１の声紋または汎用的な声紋との間の類似性の程度を示し得る。汎用的な声紋は、話者のある集団と関連付けられる発話信号のデータベースに基づき得る。第１の声紋は、ユーザ１０６の発話信号（たとえば、訓練セッションの間に受信された）に基づき得る。

【０２００】

[00208]認証データ生成器１１０は、一致スコア１５０２を認証デバイス１０４に送る（たとえば、送信する）ことができる。

【０２０１】
[00209]認証デバイス１０４は、ユーザ入力１７２（たとえば、発話信号）、一致スコア１５０２、認証データ１７８、またはこれらの組合せを、モバイルデバイス１０２から受信することができる。認証デバイス１０４は、第２の一致スコアを生成するためにユーザ入力１７２に対して話者認識を実行することができ、一致スコア１５０２と第２の一致スコアとを比較することができる。認証デバイス１０４は、比較に基づいて認証データ１７８を処理することができる。たとえば、認証デバイス１０４は、一致スコア１５０２と第２の一致スコアとの差が特定の閾値を満たすと決定したことに応答して、認証データ１７８を処理することができる。例示すると、認証デバイス１０４は、その差が特定の閾値を満たすと決定したことに応答して、認証データ１７８に基づいて認証を実行することができる。認証デバイス１０４は、その差が特定の閾値を満たさないと決定したことに応答して、認証データ１７８を廃棄することができる。
【０２０２】
[00210]システム１５００は、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて認証データ１７８を生成するために、一方向性関数を使用することができる。一方向性関数を使用することは、ユーザ入力１７２、非バイオメトリックデータ１７６、または両方に基づいて、認証データ１７８からバイオメトリックデータ１７０を導出することを難しくし得る。したがって、システム１５００は、ユーザ入力１７２、非バイオメトリックデータ１７６（たとえば、一致スコア１５０２）、または両方が、認証デバイス１０４と共有されることを可能にし得る。
【０２０３】
[00211]図１６を参照すると、認証データを生成する方法のある特定の実施形態の流れ図が示されており、全体的に１６００と指定されている。認証データは、バイオメトリックデータおよび非バイオメトリックデータに基づいて生成され得る。特定の実施形態では、方法１６００は図１の認証データ生成器１１０によって実行され得る。
【０２０４】
[00212]方法１６００は、１６０２において、第１のバイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０を受信することができる。
【０２０５】
[00213]方法１６００はまた、１６０４において、非バイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、ユーザ入力１７２を受信することができる。ユーザ入力１７２は、非バイオメトリックデータ１７６に対応し得る。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。
【０２０６】
[00214]方法１６００はさらに、１６０６において、非バイオメトリックデータに基づいて第１のバイオメトリックデータを修正することによって、第２のバイオメトリックデータを生成することを含む。たとえば、図１を参照して説明されるように、図１の認証データ生成器１１０は、バイオメトリックデータ１７０からバイオメトリック特徴１８２を抽出することができ、非バイオメトリックデータ１７６に基づいてバイオメトリック特徴１８２を修正することによって、修正されたバイオメトリック特徴１８４を生成することができる。認証データ生成器１１０は、図１を参照して説明されるように、修正されたバイオメトリック特徴１８４に基づいて、第２のバイオメトリックデータ１８０を生成することができる。
【０２０７】
[00215]方法１６００はまた、１６０８において、第２のバイオメトリックデータをメモリに記憶することを含む。たとえば、図１の認証データ生成器１１０は、第２のバイオメトリックデータ１８０をメモリ１３２に記憶することができる。
【０２０８】

[00216]方法１６００はさらに、１６１０において、第２のバイオメトリックデータを送信することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、送受信機１４２を介して第２のバイオメトリックデータ１８０を認証デバイス１０４に送信することができる。

【０２０９】

[00217]したがって、方法１６００は、ユーザから受信されたバイオメトリックデータと非バイオメトリックデータに基づいて合成バイオメトリックデータが生成されることを可能にし得る。合成バイオメトリックデータは、認証データを生成するために使用され得る。合成バイオメトリックデータは、バイオメトリックデータと同じセキュリティのレベルを有することがあり、構成可能であることがある。たとえば、ユーザは、非バイオメトリックデータを修正することによって、異なる合成バイオメトリックデータを生成することができる。

【０２１０】

[00218]図１７を参照すると、認証データを生成する方法のある特定の実施形態の流れ図が示されており、全体的に１７００と指定されている。認証データは、バイオメトリックデータおよび非バイオメトリックデータに基づいて生成され得る。特定の実施形態では、方法１７００は図１の認証データ生成器１１０によって実行され得る。

【０２１１】

[00219]方法１７００は、１７０２において、バイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０を受信することができる。

【０２１２】

[00220]方法１７００はまた、１７０４において、非バイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、ユーザ入力１７２を受信することができる。ユーザ入力１７２は、非バイオメトリックデータ１７６に対応し得る。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。

【０２１３】

[00221]方法１７００はさらに、１７０６において、複数の画像のうちの第１の画像を選択することを含む。第１の画像はバイオメトリックデータに基づいて選択され得る。たとえば、図１の認証データ生成器１１０は、画像１９０のうちの第１の画像１９４を選択することができる。第１の画像１９４は、図１を参照して説明されるように、バイオメトリックデータ１７０に基づいて選択され得る。画像１９０は、デフォルトの画像であってよく、または、ユーザ（たとえば、ユーザ１０６）によって提供されてよい。

【０２１４】

[00222]方法１７００はまた、１７０８において、非バイオメトリックデータに基づいて第１の画像を修正することによって、第２の画像を生成することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、非バイオメトリックデータ１７６に基づいて第１の画像１９４を修正することによって、第２の画像１９６を生成することができる。

【０２１５】

[00223]方法１７００はさらに、１７１０において、第２の画像をメモリに記憶することを含む。たとえば、図１の認証データ生成器１１０は、第２の画像１９６をメモリ１３２に記憶することができる。

【０２１６】

[00224]方法１７００はまた、１７１２において、第２の画像を送信することを含む。たとえば、図１の認証データ生成器１１０は、送受信機１４２を介して第２の画像１９６を認証デバイス１０４に送信することができる。

【０２１７】

[00225]図１８を参照すると、認証データを生成する方法のある特定の実施形態の流れ

図が示されており、全体的に１８００と指定されている。認証データは、バイオメトリックデータおよび非バイオメトリックデータに基づいて生成され得る。ある特定の実施形態では、方法１８００は図１の認証データ生成器１１０によって実行され得る。

【０２１８】

[00226]方法１８００は、１８０２において、バイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０を受信することができる。

【０２１９】

[00227]方法１８００はまた、１８０４において、非バイオメトリックデータに対応するユーザ入力を受信することを含む。たとえば、図１の認証データ生成器１１０は、ユーザ入力１７２を受信することができる。ユーザ入力１７２は、非バイオメトリックデータ１７６に対応し得る。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。

【０２２０】

[00228]方法１８００はさらに、１８０６において、非バイオメトリックデータに基づいてバイオメトリックデータを可聴化することによって、オーディオデータを生成することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、非バイオメトリックデータ１７６に基づいてバイオメトリックデータ１７０を可聴化することによって、オーディオデータ１９８を生成することができる。

【０２２１】

[00229]方法１８００はまた、１８０８において、オーディオデータをメモリに記憶することを含む。たとえば、図１の認証データ生成器１１０は、オーディオデータ１９８を図１のメモリ１３２に記憶することができる。

【０２２２】

[00230]方法１８００はさらに、１８１０において、オーディオデータを送信することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、送受信機１４２を介してオーディオデータ１９８を認証デバイス１０４に送信することができる。

【０２２３】

[00231]したがって、方法１８００は、非バイオメトリックデータに基づいてバイオメトリックデータを可聴化することによって、認証データを生成することを可能にし得る。ユーザは、オーディオ認証データを生成するために、非オーディオ（たとえば、画像）バイオメトリックデータを使用することができる。方法１８００は、基本電話システム（ＰＯＴＳ）を使用した電話呼の間に、認証データを送信することを可能にし得る。

【０２２４】

[00232]図１９を参照すると、認証データを生成する方法のある特定の実施形態の流れ図が示されており、全体的に１９００と指定されている。認証データは、バイオメトリックデータおよび非バイオメトリックデータに基づいて生成され得る。ある特定の実施形態では、方法１９００は図１の認証データ生成器１１０によって実行され得る。

【０２２５】

[00233]方法１９００は、１９０２において、第１のフォーマットの第１のバイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、図１を参照して説明されるように、第１のバイオメトリックデータ１３７０を受信することができる。第１のバイオメトリックデータ１３７０は第１のフォーマット（たとえば、画像データ）であり得る。

【０２２６】

[00234]方法１９００はまた、１９０４において、第２のフォーマットの第２のバイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、図１４を参照して説明されるように、第２のバイオメトリックデータ１４７２を受信する

ことができる。第２のバイオメトリックデータ１４７２は第２のフォーマット（たとえば、オーディオデータ）であり得る。

【０２２７】

[00235]方法１９００はさらに、１９０６において、非バイオメトリックデータを受信することを含む。たとえば、図１の認証データ生成器１１０は、ユーザ入力１７２を受信することができる。ユーザ入力１７２は、非バイオメトリックデータ１７６に対応し得る。たとえば、認証データ生成器１１０は、図１を参照して説明されるように、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。

【０２２８】

[00236]方法１９００はまた、１９０８において、第１のバイオメトリックデータと第２のバイオメトリックデータとを共通のフォーマットに変換することによって認証データを生成するを含む。認証データは、非バイオメトリックデータに基づいて生成される。たとえば、図１の認証データ生成器１１０は、図１４を参照して説明されるように、第１のバイオメトリックデータ１４７０を画像オーディオ１４０８に変換することができる。画像オーディオ１４０８および第２のバイオメトリックデータ１４７２は共通のフォーマット（たとえば、画像データ）を有し得る。認証データ生成器１１０は、図１４を参照して説明されるように、画像オーディオ１４０８と第２のバイオメトリックデータ１４７２とを組み合わせることによってバイオメトリックデータ１７０を生成することができる。認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて認証データ１７８を生成することができる。

【０２２９】

[00237]方法１９００はさらに、１９１０において、認証データをメモリに記憶することを含む。たとえば、図１の認証データ生成器１１０は、認証データ１７８をメモリ１３２に記憶することができる。

【０２３０】

[00238]方法１９００はまた、１９１２において、認証データを送信することを含む。たとえば、図１の認証データ生成器１１０は、送受信機１４２を介して認証データ１７８を認証デバイス１０４に送信することができる。

【０２３１】

[00239]したがって、方法１９００は、異なるタイプのバイオメトリックデータから認証データが生成されることを可能にし得る。複数のタイプのバイオメトリックデータから生成される認証データは、単一のタイプのバイオメトリックデータから生成される認証データよりセキュアであり得る。たとえば、複数のタイプのバイオメトリックデータから認証データを生成することは、認証データからバイオメトリックデータを導出する（たとえば、リバースエンジニアリング）ことをより難しくし得る。

【０２３２】

[00240]図２０を参照すると、認証データを生成する方法のある特定の実施形態の図が示されており、全体的に２０００と指定されている。認証データは、バイオメトリックデータに基づいて生成され得る。ある特定の実施形態では、方法２０００は、認証データ生成器１１０、モバイルデバイス１０２、図１の認証デバイス１０４、またはこれらの組合せによって実行され得る。たとえば、方法２０００の少なくとも１つの動作はモバイルデバイス１０２において実行されてよく、方法２０００の少なくとも１つの動作は認証デバイス１０４において実行されてよい。

【０２３３】

[00241]図２０では、ユーザと関連付けられるユーザデバイス（たとえば、図１のモバイルデバイス１０２）によって実行される動作は左側に示されており、「ユーザ」と指定されている。遠端のデバイス（たとえば、銀行の認証サーバと関連付けられる）によって実行される動作は右側に示されており、「遠端」と指定されている。遠端のデバイスは図１の認証デバイス１０４を含み得る。代替的な実施形態では、遠端は、クラウドストレー

ジ／コンピューティングサービスと関連付けられるサーバ、ホームオートメーションシステム、または、ユーザ認証および／もしくはセキュアな通信を実行する別のシステムなどの、別の遠隔認証エンティティを表し得る。ある説明のための実施形態では、図２０のユーザ動作はモバイルデバイス１０２の認証データ生成器１１０によって実行され、図２０の遠端動作は認証デバイス１０４の認証データ生成器によって実行される。

【０２３４】

[00242]方法２０００は、遠端の第１の「バイオメトリックデータ」２００２に基づいて、２００４において、遠端で特徴抽出を実行することを含む。第１のバイオメトリックデータ２００２は、遠端の秘密鍵として機能し得る。ある特定の実施形態では、第１のバイオメトリックデータ２００２は、遠端のユーザ（たとえば、銀行の従業員）の指紋、虹彩スキャン、顔の画像、または声紋を含む。ある代替的な実施形態では、第１のバイオメトリックデータ２００２は、特定の暗号システム（たとえば、Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ（ＲＳＡ）アルゴリズム、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式、楕円曲線暗号方式など）に基づいて選択される秘密鍵（たとえば、整数、自然数など）を含む。ある特定の実施形態では、遠端が個々のユーザと関連付けられない場合、第１のバイオメトリックデータ２００２は、遠端と一意に関連付けられる任意のバイオメトリックデータ（たとえば、銀行および／または銀行によって所有される特定のサーバを一意に識別するデータ）を含み得る。

【０２３５】

[00243]方法２０００はまた、ユーザの第１のバイオメトリックデータ２００１に基づいて、２００５において、ユーザデバイスで特徴抽出を実行することを含む。第１のバイオメトリックデータは、ユーザの秘密鍵として機能し得る。第１のバイオメトリックデータ２００１は、ユーザの指紋、ユーザの虹彩スキャン、ユーザの発話信号、ユーザの顔の画像などを含み得る。ユーザの第１のバイオメトリックデータは、遠端の第１のバイオメトリックデータとは別であり得る。

【０２３６】

[00244]方法２０００はさらに、遠端の第２の（合成）バイオメトリックデータ２００８を生成するために、共通鍵２００３に基づいて、２００６において、遠端で合成指紋／画像の生成を実行することを含む。共通鍵２００３は、特定の暗号化システム（たとえば、Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ（ＲＳＡ）アルゴリズム、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式、楕円曲線暗号化方式など）に基づいて選択され得る。たとえば、共通鍵２００３は特定の楕円曲線に対応し得る。

【０２３７】

[00245]ある特定の実施形態では、共通鍵２００３は、ユーザデバイスと遠端デバイスとの間で以前に共有されていた非バイオメトリック英数字鍵である。たとえば、ユーザは、銀行に口座を開設した際に、銀行と共通鍵２００３（たとえば、個人識別番号（ＰＩＮ））を共有していることがある。方法２０００はまた、ユーザの第２の（合成）バイオメトリックデータ２００９を生成するために、共通鍵２００３に基づいて、２００７において、ユーザデバイスで合成指紋／画像の生成を実行することを含む。ユーザデバイスおよび遠端のデバイスは合成バイオメトリックデータを生成するために数学的な関数／変換の共通のセットを実行し得るが、ユーザデバイスによって生成される合成バイオメトリックデータ２００９は遠端のデバイスによって生成される合成バイオメトリックデータ２００８とは異なることがあり、それは、合成バイオメトリックデータ２００９が異なるバイオメトリック入力２００１、２００２に基づいて各デバイスにおいて生成されるからである。ある特定の実施形態では、合成バイオメトリックデータはユーザデバイスにおいてビー生成され、合成バイオメトリックデータ２００８は共通の一方向性関数を実行することによって遠端のデバイスにおいて生成される。ある特定の実施形態では、合成バイオメトリックデータ２００８、合成バイオメトリックデータ２００９、または両方が、画像データを含み得る。たとえば、図１を参照して説明されるように、合成バイオメトリックデータ２００８、合成バイオメトリックデータ２００９、または両方が、第２の画像１９６また

は第２のバイオメトリックデータ１８０（たとえば、合成指紋スキャン、合成虹彩スキャン、顔の合成画像）に対応し得る。

【０２３８】

[00246]方法２０００はさらに、ユーザの合成バイオメトリックデータ２００９を遠端に移送するために、および、遠端の合成バイオメトリックデータ２００８をユーザデバイスに移送するために、２０３０において、セキュアな移送を行うことを含む。ある例では、セキュアな移送２０３０は、暗号化されたメッセージ交換方式（たとえば、ＲＳＡ）を使用して実行される。

【０２３９】

[00247]方法２０００はまた、ユーザの移送された第２の（合成）バイオメトリックデータ２０１０から特徴を抽出するために、２０１２において、遠端で特徴抽出を実行することを含む。方法２０００はさらに、遠端の移送された第２の（合成）バイオメトリックデータ２０１１から特徴を抽出するために、２０１３において、ユーザデバイスで特徴抽出を実行することを含む。

【０２４０】

[00248]方法２０００はまた、ユーザの第１のバイオメトリックデータ２００１および遠端の移送された第２の（合成）バイオメトリックデータ２０１１からの抽出された特徴に基づいて、２０１５において、ユーザデバイスで合成指紋／画像の生成を実行することを含む。方法２０００はさらに、遠端の第１の「バイオメトリックデータ」２００２およびユーザの移送された第２の（合成）バイオメトリックデータ２０１０からの抽出された特徴に基づいて、２０１６において、遠端で合成指紋／画像の生成を実行することを含む。図２０に示されるように、ユーザデバイスと遠端の両方が、同じ生成された共通のバイオメトリックデータ２０１７を出力し得る。共通のバイオメトリックデータ２０１７は、第２の（合成）バイオメトリックデータ２０１０、第２の（合成）バイオメトリックデータ２０１１、または両方と別であり得る。

【０２４１】

[00249]共通のバイオメトリックデータ２０１７は、ユーザデバイスと遠端のデバイスとの間でセキュアな通信セッションおよび／または認証された通信セッションを行うために使用され得る。たとえば、認証デバイス１０４（たとえば、遠端のデバイス）は、共通のバイオメトリックデータ２０１７に基づいて、モバイルデバイス１０２（たとえば、ユーザデバイス）、モバイルデバイス１０２のユーザ（たとえば、図１のユーザ１０６）、または両方を認証するように構成され得る。モバイルデバイス１０２は、通信チャネルを介して共通のバイオメトリックデータ２０１７を認証デバイス１０４に送信することができる。通信チャネルは、ワイヤレスフィデリティ（Ｗｉ－Ｆｉ（登録商標））ネットワーク、セルラーネットワーク、ローカルエリアネットワーク（ＬＡＮ）、またはワイドエリアネットワーク（ＷＡＮ）のうちの少なくとも１つに対応し得る。認証デバイス１０４は、モバイルデバイス１０２から受信された共通のバイオメトリックデータ２０１７および認証デバイス１０４において生成された共通のバイオメトリックデータ２０１７が同じ（または実質的に同様）であると決定したことに基づいて、モバイルデバイス１０２、モバイルデバイス１０２のユーザ、または両方が認証されると決定することができる。共通のバイオメトリックデータ２０１７は、認証デバイス１０４への送信の前にモバイルデバイス１０２において暗号化され得る。

【０２４２】

[00250]別の例として、共通のバイオメトリックデータ２０１７は、暗号化鍵として使用されてよく、または暗号化鍵を導出するために使用されてよい。モバイルデバイス１０２（または認証デバイス１０４）は、データを認証デバイス１０４（またはモバイルデバイス１０２）に送信する前に、共通のバイオメトリックデータ２０１７に基づいてデータを暗号化することができる。データは、共通のバイオメトリックデータ２０１７に基づいて暗号化された後で、セキュアに（または比較的セキュアに）送信され得る。バイオメトリック入力２００１、２００２は、暗号化されたデータおよび／または共通のバイオメト

リックデータ２０１７から復元不可能である（または実質的に復元不可能である）ことがある。

【０２４３】

[00251]認証デバイス１０４は、建物の扉、家の扉、車両のドア、車庫の扉、または別の扉のうちの少なくとも１つの施錠機構の動作を可能にするように構成され得る。たとえば、認証デバイス１０４は、モバイルデバイス１０２、モバイルデバイス１０２のユーザ、または両方を認証したことに応答して、施錠機構を有効（または無効）にすることができる。別の例として、認証デバイス１０４は、自動預け払い機（ＡＴＭ）または販売時点情報管理（ｐｏｉｎｔ　ｏｆ　ｓａｌｅ）機器のうちの少なくとも１つへのアクセスを可能にするように構成され得る。たとえば、認証デバイス１０４は、モバイルデバイス１０２、モバイルデバイス１０２のユーザ、または両方を認証したことに応答して、ＡＴＭおよび／または販売時点情報管理機器へのアクセスを可能にし得る。

【０２４４】

[00252]したがって、方法２０００は、合成バイオメトリックデータを使用して、鍵交換に基づいてユーザの遠隔認証を可能にし得る。有利には、ユーザを一意に識別するバイオメトリックデータ（たとえば、ユーザの第１のバイオメトリックデータ２００１）および遠隔認証サーバ（たとえば、遠端の第１のバイオメトリックデータ２００２）は、セキュアに保たれ得る（たとえば、デバイス間で送信されない）。

【０２４５】

[00253]図２１を参照すると、認証データを生成する方法の別の特定の実施形態の図が示されており、全体的に２１００と指定されている。ある特定の実施形態では、方法２１００は、認証データ生成器１１０、モバイルデバイス１０２、図１の認証デバイス１０４、またはこれらの組合せによって実行され得る。たとえば、方法２１００の少なくとも１つの動作はモバイルデバイス１０２において実行されてよく、方法２１００の少なくとも１つの動作は認証デバイス１０４において実行されてよい。

【０２４６】

[00254]図２１では、ユーザと関連付けられるユーザデバイスによって実行される動作は左側に示されており、「ユーザ」と指定されている。遠端のデバイス（たとえば、銀行の認証サーバと関連付けられる）によって実行される動作は右側に示されており、「遠端」と指定されている。代替的な実施形態では、遠端は、クラウドストレージ／コンピューティングサービスと関連付けられるサーバ、ホームオートメーションシステム、または、ユーザ認証および／もしくはセキュアな通信を実行する別のシステムなどの、別の遠隔認証エンティティを表し得る。ある説明のための実施形態では、図２１のユーザ動作はモバイルデバイス１０２の認証データ生成器１１０によって実行され、図２１の遠端動作は認証デバイス１０４の認証データ生成器によって実行される。

【０２４７】

[00255]方法２１００は、（たとえば、メッセージングのオーバーヘッドを減らすために）合成バイオメトリックデータ自体を交換する代わりに、合成バイオメトリックデータから抽出された特徴の交換を含むという点で、図２０の方法２０００とは異なる。

【０２４８】

[00256]方法２１００は、遠端の第２の（合成）バイオメトリックデータ２００８から特徴を抽出するために、２１１０において、遠端で特徴抽出を実行することを含む。方法２１００はまた、ユーザの第２の（合成）バイオメトリックデータ２００９から特徴を抽出するために、２１１１において、特徴抽出を実行することを含む。方法２１００はさらに、２１３０において、（図２０のように合成バイオメトリックデータ２００８と２００９とを交換する代わりに）抽出された特徴を交換するために、セキュアな移送を行うことを含む。

【０２４９】

[00257]方法２１００はまた、共通のバイオメトリックデータ２１１５を生成するために、ユーザの第１のバイオメトリックデータ２００１および遠端の第２の（合成）バイオ

メトリックデータ２００８から抽出された受信された特徴に基づいて、２１１３において、ユーザデバイスで合成指紋／画像の生成を実行することを含む。方法２１００はさらに、共通のバイオメトリックデータ２１１５を生成するために、遠端の第１の「バイオメトリックデータ」２００２およびユーザの第２の（合成）バイオメトリックデータ２００９から抽出された受信された特徴に基づいて、２１１４において、遠端で合成指紋／画像の生成を実行することを含む。共通のバイオメトリックデータ２１１５は、ユーザデバイスと遠端との間でセキュアな認証された通信セッションを行うために使用され得る。例として、共通のバイオメトリックデータ２１１５は、暗号化鍵として使用されてよく、または暗号化鍵を導出するために使用されてよい。

【０２５０】

[00258]図２２を参照すると、認証データを生成する方法のある特定の実施形態の図が示されており、全体的に２２００と指定されている。方法２２００は、バイオメトリックおよび共通鍵に基づく合成指紋／音声の生成を含むという点で方法２０００とは異なる。

【０２５１】

[00259]方法２２００は、遠端の第２の（合成）バイオメトリックデータ２２０８を生成するために、２２０６において、遠端で合成指紋／音声の生成を実行することを含む。方法２２００はまた、ユーザの第２の（合成）バイオメトリックデータ２２０９を生成するために、２２０７において、合成指紋／音声の生成を実行することを含む。合成バイオメトリックデータ２２０８、合成バイオメトリックデータ２２０９、または両方が、音声データに対応し得る。たとえば、合成バイオメトリックデータ２２０８、合成バイオメトリックデータ２２０９、または両方が、第２のバイオメトリックデータ１８０（たとえば、図２０のような、画像データを交換する代わりに合成声紋音声データ）に対応し得る。方法２２００はさらに、２２３０において、生成された合成バイオメトリックデータを交換するために（たとえば、図２０のように画像データを交換する代わりに音声データを交換する）、セキュアな移送を行うことを含む。

【０２５２】

[00260]方法２２００はさらに、ユーザの移送された第２の（合成）バイオメトリックデータ２２１０から特徴を抽出するために、２２１２において、遠端で特徴抽出２２１２を実行することを含む。方法２２００はまた、遠端の移送された第２の（合成）バイオメトリックデータ２２１１から特徴を抽出するために、２２１３において、ユーザデバイスで特徴抽出を実行することを含む。

【０２５３】

[00261]方法２２００はさらに、ユーザの第１のバイオメトリックデータ２００１および遠端の移送された第２の（合成）バイオメトリックデータ２２１１からの抽出された特徴に基づいて、２２１５において、ユーザデバイスで合成指紋／音声の生成を実行することを含む。方法２２００はまた、遠端の第１の「バイオメトリックデータ」２００２およびユーザの移送された第２の（合成）バイオメトリックデータ２２１０からの抽出された特徴に基づいて、２２１６において、遠端で合成指紋／音声の生成を実行することを含む。図２２に示されるように、ユーザデバイスと遠端の両方が、同じ生成された共通のバイオメトリックデータ２２１７を出力し得る。共通のバイオメトリックデータ２２１７。

【０２５４】

[00262]共通のバイオメトリックデータ２２１７は、ユーザデバイスと遠端との間でセキュアな認証された通信セッションを行うために使用され得る。例として、共通のバイオメトリックデータ２２１７は、暗号化鍵として使用されてよく、または暗号化鍵を導出するために使用されてよい。別の例として、ユーザデバイスは、共通のバイオメトリックデータ２２１７を「パスワード」として遠端に送信することができる。遠端は、ユーザデバイスから受信された共通のバイオメトリックデータ２２１７と遠端において生成された共通のバイオメトリックデータ２２１７との比較に基づいて、ユーザ、ユーザデバイス、または両方を選択的に認証することができる。例示すると、遠端は、ユーザデバイスから受信された共通のバイオメトリックデータ２２１７と遠端において生成された共通のバイオ

メトリックデータ２２１７が一致すると決定したことに応答して、ユーザ、ユーザデバイス、または両方が認証されると決定することができる。

【０２５５】

[00263]図２３を参照すると、認証データを生成する方法の別の特定の実施形態の図が示されており、全体的に２３００と指定されている。方法２３００は、バイオメトリックおよび共通鍵に基づく合成指紋／音声の生成を含むという点で方法２１００とは異なる。方法２３００は、（たとえば、メッセージングのオーバーヘッドを減らすために）合成バイオメトリックデータ自体を交換する代わりに、合成バイオメトリックデータから抽出された特徴の交換を含むという点で、方法２２００とは異なる。

【０２５６】

[00264]方法２３００は、遠端の第２の（合成）バイオメトリックデータ２２０８から特徴を抽出するために、２３１０において、遠端で特徴抽出を実行することを含む。方法２３００はまた、ユーザの第２の（合成）バイオメトリックデータ２２０９から特徴を抽出するために、２３１１において、特徴抽出を実行することを含む。方法２３００はさらに、２３３０において、（図２０のように合成バイオメトリックデータ２２０８と２２０９とを交換する代わりに）特徴を交換するために、セキュアな移送を行うことを含む。

【０２５７】

[00265]方法２３００はまた、共通のバイオメトリックデータ２３１５を生成するために、ユーザの第１のバイオメトリックデータ２００１および遠端の第２の（合成）バイオメトリックデータ２２０８から抽出された受信された特徴に基づいて、２３１３において、ユーザデバイスで合成指紋／音声の生成を実行することを含む。方法２３００はさらに、共通のバイオメトリックデータ２３１５を生成するために、遠端の第１の「バイオメトリックデータ」２００２およびユーザの第２の（合成）バイオメトリックデータ２２０９から抽出された受信された特徴に基づいて、２３１４において、遠端で合成指紋／音声の生成を実行することを含む。

【０２５８】

[00266]共通のバイオメトリックデータ２３１５は、ユーザデバイスと遠端との間でセキュアな認証された通信セッションを行うために使用され得る。例として、共通のバイオメトリックデータ２３１５は、暗号化鍵として使用されてよく、または暗号化鍵を導出するために使用されてよい。別の例として、ユーザデバイスは、共通のバイオメトリックデータ２３１５を「パスワード」として遠端に送信することができる。遠端は、ユーザデバイスから受信された共通のバイオメトリックデータ２３１５と遠端において生成された共通のバイオメトリックデータ２３１５との比較に基づいて、ユーザ、ユーザデバイス、または両方を選択的に認証することができる。例示すると、遠端は、ユーザデバイスから受信された共通のバイオメトリックデータ２３１５と遠端において生成された共通のバイオメトリックデータ２３１５が一致すると決定したことに応答して、ユーザ、ユーザデバイス、または両方が認証されると決定することができる。

【０２５９】

[00267]図２４を参照すると、バイオメトリックデータおよび非バイオメトリックデータに基づいて認証データを生成するように構成されるシステムのある特定の実施形態の図が開示されており、全体的に２４００と指定されている。システム２４００は、本明細書で説明されるように、合成バイオメトリックデータの「構成可能性」を示す。

【０２６０】

[00268]システム２４００は、ネットワーク２４２０を介して、認証デバイス２４５０（たとえば、銀行の認証サーバ）および認証デバイス２４５２（たとえば、ホームオートメーションシステムなどのための、家庭にある認証サーバ）に結合された、モバイルデバイス１０２を含む。ある特定の実施形態では、モバイルデバイス１０２は、２つよりも少ない、または２つよりも多くの認証デバイスに結合され得る。その上、認証デバイスは、銀行および家庭以外のエンティティと関連付けられ得る。

【０２６１】

[00269]ユーザ１０６は、複数のシステムにアクセスするためにモバイルデバイス１０２を使用することができる。たとえば、ユーザ１０６は、金融システム（たとえば、オンラインバンキングシステム、オンラインショッピングシステム、株取引システムなど）にアクセスするためにモバイルデバイス１０２を使用し得る。別の例として、ユーザ１０６は、建物のホームオートメーション機能（たとえば、ホームセキュリティシステム、車庫の扉、正面玄関、エンターテインメントシステム、暖房システム、冷房システム、スプリンクラーシステム、コーヒーメーカー、冷蔵庫、ガスレンジ、スロークッカー、照明システム、他の家電など）にアクセスするために、モバイルデバイス１０２を使用し得る。さらなる例として、ユーザ１０６は、車両（たとえば、車）のシステム（たとえば、温度制御システム、エンジン、セキュリティシステム、ドア、トランク、ライト、ウィンドウなど）にアクセスするために、モバイルデバイス１０２をユーザし得る。

【０２６２】

[00270]ユーザ１０６は、図１を参照して説明されるように、第１のインターフェース１３４（たとえば、センサ）を介して、バイオメトリックデータ１７０をモバイルデバイス１０２に提供することができる。認証データ生成器１１０は、バイオメトリックデータ１７０に基づいてバイオメトリック特徴１８２を生成することができる。認証データ生成器１１０は、バイオメトリックデータ１７０、バイオメトリック特徴１８２、または両方を、図１のメモリ１３２に記憶することができる。ユーザ１０６は、認証デバイス２４５０にアクセスするために第１の銀行鍵２４０２（たとえば、ユーザ入力）を提供することができる。たとえば、第１の銀行鍵２４０２は、ユーザ１０６の銀行口座と関連付けられる特定の非バイオメトリック鍵（たとえば、文字、数字、日付など）に対応し得る。

【０２６３】

[00271]認証データ生成器１１０は、図１を参照して説明されるように、バイオメトリックデータ１７０および第１の銀行鍵２４０２に基づいて第１の合成バイオメトリック銀行データ２４２２（たとえば、合成バイオメトリックデータ）を生成することができる。たとえば、第１の合成バイオメトリック銀行データ２４２２は図１の第２のバイオメトリックデータ１８０に対応してよく、第１の銀行鍵２４０２は図１のユーザ入力１７２に対応してよい。認証データ生成器１１０は、第１の合成バイオメトリック銀行データ２４２２を認証デバイス２４５０に提供することができる。

【０２６４】

[00272]認証デバイス２４５０は、第１の合成バイオメトリック銀行データ２４２２を、ユーザ１０６と関連付けられる以前に記憶されたバイオメトリックデータと比較することができる。認証デバイス２４５０は、第１の合成バイオメトリック銀行データ２４２２が以前に記憶されたバイオメトリックデータと一致すると決定したことに応答して、ユーザ１０６の認証が成功すると決定することができる。したがって、第１の合成バイオメトリック銀行データ２４２２は銀行の「パスワード」として機能し得る。モバイルデバイス１０２は、認証デバイス２４５０が第１の合成バイオメトリック銀行データ２４２２に基づいてユーザ１０６を認証するとき、ネットワーク２４２０を介して別の電子デバイスとの認証されたセッションを行うことができる。たとえば、認証デバイス２４５０は、認証サーバを含んでよく、ユーザ１０６の認証が成功したと決定したことに応答して別の電子デバイス（たとえば、金融システムのデバイス）へのアクセス権を与えることができる。認証デバイス２４５０は、第１の合成バイオメトリック銀行データ２４２２が以前に記憶されたバイオメトリックデータと一致しないと決定したことに応答して、ユーザ１０６の認証が成功しないと決定することができる。

【０２６５】

[00273]ユーザ１０６は、認証デバイス２４５０による認証の成功に続いて、（たとえば、銀行の「パスワード」を変更するために）第２の銀行鍵２４０４をモバイルデバイス１０２に提供することができる。たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０および第２の銀行鍵２４０４に基づいて第２の合成バイオメトリック銀行データ２４２４（たとえば、合成バイオメトリックデータ）を生成することができる。認

証データ生成器１１０は、第２の合成バイオメトリック銀行データ２４２４を生成するために以前に記憶されたバイオメトリックデータ１７０またはバイオメトリック特徴１８２を使用することができる。ある特定の実施形態では、認証データ生成器１１０は、以前に記憶されたバイオメトリックデータ１７０またはバイオメトリック特徴１８２が「期限切れ」になったと決定したことに応答して、バイオメトリックデータ１７０を提供するようにユーザ１０６に促すことができる。たとえば、認証データ生成器１１０は、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れになったことを、第１のタイムスタンプに基づいて決定することができる。例示すると、認証データ生成器１１０は、クロックの第１のタイムスタンプと第２の（たとえば、現在の）タイムスタンプの差が特定の期限切れ閾値（たとえば、２４時間）を満たすと決定したことに応答して、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れになったと決定することができる。第１のタイムスタンプは、バイオメトリックデータ１７０がユーザ１０６から受信される第１の時間、またはバイオメトリックデータ１７０もしくはバイオメトリック特徴１８２がメモリに記憶される第２の時間を示し得る。この実施形態では、認証データ生成器１１０は、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れではないと決定したことに応答して、第２の合成バイオメトリック銀行データ２４２４を生成するために、バイオメトリックデータ１７０またはバイオメトリック特徴１８２を使用することができる。

【０２６６】

[00274]認証データ生成器１１０は、第２の合成バイオメトリック銀行データ２４２４を認証デバイス２４５０に提供することができる。認証デバイス２４５０は、ユーザ１０６と関連付けられる認証データとして、第１の合成バイオメトリック銀行データ２４２２を第２の合成バイオメトリック銀行データ２４２４で置き換えることができる。たとえば、認証デバイス２４５０は、第１の合成バイオメトリック銀行データ２４２２を削除する（または削除のためにマークする）ことができる。例示すると、認証デバイス２４５０は、第１の合成バイオメトリック銀行データ２４２２とユーザ１０６との関連付けを削除する（または削除のためにマークする）ことができる。認証デバイス２４５０は、第２の合成バイオメトリック銀行データ２４２４、第２の合成バイオメトリック銀行データ２４２４とユーザ１０６との間の関連付け、またはこれらの両方を、メモリに記憶することができる。したがって、ユーザ１０６は、異なるユーザ入力（たとえば、非バイオメトリックデータ）を提供することによって、合成バイオメトリックパスワードを再構成することができる。

【０２６７】

[00275]ユーザ１０６は、認証デバイス２４５２にアクセスするために第１の家庭鍵２４０６を提供することができる。たとえば、第１の家庭鍵２４０６は、正面玄関２４５４と関連付けられるパスワード（たとえば、「ＤＯＯＲ」）に対応し得る。例示すると、ユーザ１０６の訪問客が、ユーザ１０６が離れている間にユーザ１０６の自宅に到着することがある。ユーザ１０６は、訪問客が自宅に入れるように、正面玄関２４５４をアンロックするための第１の家庭鍵２４０６を提供することができる。

【０２６８】

[00276]認証データ生成器１１０は、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れになったと決定したことに応答して、バイオメトリックデータ１７０を提供するようにユーザ１０６に促すことができる。認証データ生成器１１０は、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れではないと決定したことに応答して、第１の合成バイオメトリック家庭データ２４２６を生成することができる。たとえば、図１を参照してさらに説明されるように、認証データ生成器１１０は、第１の家庭鍵２４０６およびバイオメトリックデータ１７０（またはバイオメトリック特徴１８２）に基づいて第１の合成バイオメトリック家庭データ２４２６を生成することができる。認証データ生成器１１０は、第１の合成バイオメトリック家庭データ２４２６を認証デバイス２４５２に提供することができる。第１の合成バイオメトリック家

庭データ２４２６は、ユーザ１０６および正面玄関２４５４と関連付けられる認証データに対応し得る。認証デバイス２４５２は、第１の合成バイオメトリック家庭データ２４２６が正面玄関２４５４と関連付けられる以前に記憶された合成バイオメトリックデータ（たとえば、「パスワード」）と一致すると決定したことに応答して、アンロック信号を正面玄関２４５４に送ることができる。ある特定の実施形態では、モバイルデバイス１０２は、認証デバイス２４５２が第１の合成バイオメトリック家庭データ２４２６に基づいてユーザ１０６を認証するとき、ネットワーク２４２０を介して別の電子デバイス（たとえば、正面玄関２４５４）との認証されたセッションを行うことができる。

【０２６９】

[00277]ユーザ１０６はまた、認証デバイス２４５２に結合された別のシステム（たとえば、テレビジョン２４５６）にアクセスするために、第２の家庭鍵２４０８を提供することができる。たとえば、第２の家庭鍵２４０８は、テレビジョン２４５６と関連付けられるパスワード（たとえば、「リビングルームのＴＶのパスワード」）に対応し得る。例示すると、ユーザ１０６は、ユーザ１０６が自宅から離れている間、テレビジョン２４５６（またはテレビジョン２４５６の特定のチャンネル）を無効に保つことがある。ユーザ１０６は、訪問客がテレビジョン２４５６を使用できるようにするために、テレビジョン２４５６（またはテレビジョン２４５６の特定のチャンネル）をアンロックするための第２の家庭鍵２４０８を提供することができる。

【０２７０】

[00278]認証データ生成器１１０は、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れになったと決定したことに応答して、バイオメトリックデータ１７０を提供するようにユーザ１０６に促すことができる。認証データ生成器１１０は、バイオメトリックデータ１７０またはバイオメトリック特徴１８２が期限切れではないと決定したことに応答して、第２の合成バイオメトリック家庭データ２４２８を生成することができる。たとえば、図１を参照してさらに説明されるように、認証データ生成器１１０は、第２の家庭鍵２４０８およびバイオメトリックデータ１７０（またはバイオメトリック特徴１８２）に基づいて第２の合成バイオメトリック家庭データ２４２８を生成することができる。認証データ生成器１１０は、第２の合成バイオメトリック家庭データ２４２８を認証デバイス２４５２に提供することができる。第２の合成バイオメトリック家庭データ２４２８は、ユーザ１０６およびテレビジョン２４５６と関連付けられる認証データに対応し得る。認証デバイス２４５２は、第２の合成バイオメトリック家庭データ２４２８がテレビジョン２４５６（またはテレビジョン２４５６の特定のチャンネル）と関連付けられる以前に記憶された合成バイオメトリックデータと一致すると決定したことに応答して、アンロック信号をテレビジョン２４５６に送ることができる。

【０２７１】

[00279]本開示の実施形態は、上で説明された遠隔認証に加えてローカル認証を可能にし得ることに留意されたい。たとえば、ユーザ１０６は、モバイルデバイス１０２（またはモバイルデバイス１０２の特定の特徴）のセキュアなアクセスを確立するためにデバイス鍵２４１０を提供することができる。ユーザ１０６は、登録フェーズの間にデバイス鍵２４１０を提供することができる。認証データ生成器１１０は、バイオメトリックデータ１７０およびデバイス鍵２４１０に基づいて合成バイオメトリックデバイスデータ２４３０（たとえば、第１の合成バイオメトリックデータ）を生成することができる。認証データ生成器１１０は、合成バイオメトリックデバイスデータ２４３０をメモリに記憶することができる。モバイルデバイス１０２にアクセスするために（たとえば、モバイルデバイス１０２をスリープモードから起動するために）、ユーザ１０６は、認証フェーズの間にバイオメトリックデータとユーザ入力とをモバイルデバイス１０２に提供することができる。認証データ生成器１１０は、認証フェーズの間に受信されたバイオメトリックデータおよびユーザ入力に基づいて、第２のバイオメトリックデータ（たとえば、第２の合成バイオメトリックデータ）を生成することができる。認証データ生成器１１０は、第２のバイオメトリックデータを合成バイオメトリックデバイスデータ２４３０と比較して、ユー

ザ１０６を認証することができる。たとえば、認証データ生成器１１０は、第２のバイオメトリックデータが合成バイオメトリックデバイスデータ２４３０と実質的に一致すると決定したことに応答して、モバイルデバイス１０２（またはモバイルデバイス１０２の特徴）へのアクセス権を提供することができる。例示すると、認証データ生成器１１０は、第２のバイオメトリックデータと合成バイオメトリックデバイスデータ２４３０との類似性が特定の信頼性閾値を満たすと決定したことに応答して、第２のバイオメトリックデータおよび合成バイオメトリックデバイスデータ２４３０が実質的に一致すると決定することができる。

【０２７２】

[00280]したがって、システム２４００は、ユーザが非バイオメトリック鍵（たとえば、非バイオメトリックデータ）を変更することによって合成バイオメトリックパスワードを再構成することを可能にし得る。加えて、ユーザは、別個の機能または電子デバイスにアクセスするために、別個の合成バイオメトリックデータを認証デバイスに提供することができる。さらに、システム２００は多因子のローカルのデバイス認証を可能にし得る。

【０２７３】

[00281]図２５を参照すると、バイオメトリックデータおよび非バイオメトリックデータに基づいてアクセスを選択的に認証するように構成されるシステムのある特定の実施形態の図が示されており、全体的に２５００と指定されている。システム２５００は、本明細書で説明されるように、合成バイオメトリックデータを使用したＤｉｆｆｉｅ－Ｈｅｌｍａｎタイプの認証を示す。

【０２７４】

[00282]システム２５００は、ネットワーク２５７２を介して認証デバイス２５０２に結合されるモバイルデバイス１０２を含む。認証デバイス２５０２は、車両、認証サーバ、ホームオートメーションシステム、クラウドストレージ／コンピューティングシステム、販売時点情報管理機器、自動預け払い機（ＡＴＭ）、金融システム、銀行、店舗、ユーザアカウント、もしくはユーザ（またはデバイス）の認証を実行する別のシステムのうちの少なくとも１つを含んでよく、またはそれらに結合されてよい。ある特定の実施形態では、モバイルデバイス１０２は、２つよりも多くの認証デバイスに結合され得る。

【０２７５】

[00283]認証デバイス２５０２は、送受信機２５４２と、第２のメモリ２５６２と、認証データ生成器２５７０とを含み得る。認証データ生成器２５７０は、図１の認証データ生成器１１０と同様の方式で動作するように構成され得る。

【０２７６】

[00284]第１のユーザ２５２６は、複数のシステムにアクセスするためにモバイルデバイス１０２を使用することができる。たとえば、第１のユーザ２５２６は、金融システム（たとえば、オンラインバンキングシステム、オンラインショッピングシステム、株取引システムなど）にアクセスするためにモバイルデバイス１０２を使用し得る。別の例として、第１のユーザ２５２６は、車両（たとえば、車）のシステム（たとえば、温度制御システム、ブレーキシステム、エンジン、音響システム、エンターテインメントシステム、通信システム、全地球測位システム、ドアの施錠システム、セキュリティシステム、ドア、トランク、ライト、ウィンドウなど）にアクセスするために、モバイルデバイス１０２をユーザし得る。さらなる例として、第１のユーザ２５２６は、建物のホームオートメーション機能（たとえば、ホームセキュリティシステム、車庫の扉、正面玄関、エンターテインメントシステム、暖房システム、冷房システム、スプリンクラーシステム、コーヒーメーカー、冷蔵庫、ガスレンジ、スロークッカー、照明システム、他の家電など）にアクセスするために、モバイルデバイス１０２を使用し得る。

【０２７７】

[00285]鍵２５０４が、認証デバイス２５０２およびモバイルデバイス１０２（または第１のユーザ２５２６）に提供され得る。たとえば、第１のユーザ２５２６は、銀行に口座を開設した際に、銀行と鍵２５０４（たとえば、個人識別番号（ＰＩＮ））を共有して

いることがある。

【０２７８】

[00286]第１のユーザ２５２６は、図１を参照して説明されるように、第１のインターフェース１３４（たとえば、センサ）を介して、第１のバイオメトリックデータ２５２０をモバイルデバイス１０２に提供することができる。第１のバイオメトリックデータ２５２０は、図１のバイオメトリックデータ１７０、図２０～図２３の第１のバイオメトリックデータ２００１、またはこれらの組合せに対応し得る。たとえば、第１のバイオメトリックデータ２５２０は、第１のユーザ２５２６の指紋、虹彩スキャン、顔の画像、または声紋を含み得る。第１のバイオメトリックデータ２５２０は、第１のユーザ２５２６の秘密鍵として機能し得る。

【０２７９】

[00287]認証データ生成器１１０は、第１のバイオメトリックデータ２５２０に基づいて第１のバイオメトリック特徴（たとえば、バイオメトリック特徴１８２）を生成することができる。認証データ生成器１１０は、第１のバイオメトリックデータ２５２０、第１のバイオメトリック特徴、または両方を、メモリ１３２に記憶することができる。第１のユーザ２５２６は、鍵２５０４（たとえば、ユーザ入力）をモバイルデバイス１０２に提供することができる。認証データ生成器１１０は、鍵２５０４をメモリ１３２に記憶することができる。

【０２８０】

[00288]ある特定の実施形態では、第１のユーザ２５２６は、認証デバイス２５０２による各認証に対して、第１のバイオメトリックデータ２５２０、鍵２５０４、または両方を、モバイルデバイス１０２に提供することができる。たとえば、第１のユーザ２５２６は、第１のユーザ２５２６が銀行口座へのアクセスを要求するたびに、指紋スキャンとＰＩＮとを提供することができる。代替的な実施形態では、認証データ生成器１１０は、認証デバイス２５０２による認証に対するユーザの要求に応答して、メモリ１３２から第１のバイオメトリックデータ２５２０、第１のバイオメトリック特徴、鍵２５０４、またはこれらの組合せを取得することができる。たとえば、認証データ生成器１１０は、メモリ１３２から第１のバイオメトリックデータ２５２０（または第１のバイオメトリック特徴）を取得することができ、第１のユーザ２５２６から鍵２５０４を受信することができる。

【０２８１】

[00289]認証データ生成器１１０は、図１を参照して説明されるように、第１のバイオメトリックデータ２５２０および鍵２５０４に基づいて第１の合成バイオメトリックデータ２５２２（たとえば、合成バイオメトリックデータ）を生成することができる。たとえば、第１の合成バイオメトリックデータ２５２２は、図１の第２のバイオメトリックデータ１８０、図２０～図２１の合成バイオメトリックデータ２００９、図２２～図２３の合成バイオメトリックデータ２２０９、またはこれらの組合せに対応し得る。鍵２５０４は、図１のユーザ入力１７２、非バイオメトリックデータ１７６、図２０～図２３の共通鍵２００３、またはこれらの組合せに対応し得る。認証データ生成器１１０は、第１の情報２５２８を認証デバイス２５０２に提供することができる。たとえば、送受信機１４２は第１の情報２５２８を送信することができる。第１の情報２５２８は、第１の合成バイオメトリックデータ２５２２または第１の合成バイオメトリックデータ２５２２の特徴を含み得る。認証データ生成器１１０は、第１の情報２５２８をメモリ１３２に記憶することができる。

【０２８２】

[00290]ある特定の実施形態では、認証データ生成器１１０は、第１のバイオメトリックデータ２５２０、第１のバイオメトリック特徴、鍵２５０４、またはこれらの組合せを、メモリ１３２に記憶するのを控えることができる。認証データ生成器１１０は、認証デバイス２５０２による認証に対するユーザの要求に応答して、第１の情報２５２８を認証デバイス２５０２に提供することができる。第１の情報２５２８は、第１のユーザ２５２

６の公開鍵として機能し得る。

【０２８３】

[00291]認証データ生成器２５７０は、図１を参照して説明されるように、第２のバイオメトリックデータ２５５０および鍵２５０４に基づいて第２の合成バイオメトリックデータ２５５２（たとえば、合成バイオメトリックデータ）を生成することができる。たとえば、第２の合成バイオメトリックデータ２５５０は、図１の第２のバイオメトリックデータ１８０、図２０～図２１の合成バイオメトリックデータ２００８、図２２～図２３の合成バイオメトリックデータ２４０８、またはこれらの組合せに対応し得る。ある特定の実施形態では、認証データ生成器２５７０は、第１の情報２５２８を受信する前に第２の合成バイオメトリックデータ２５５２を生成することができる。たとえば、認証データ生成器２５７０は、（たとえば、パスワードの設定またはリセットのフェーズの間に）鍵２５０４を受信したことに応答して、第２の合成バイオメトリックデータ２５５２を生成することができる。例示すると、認証データ生成器２５７０は、第１のユーザ２５２６が銀行口座と関連付けられるＰＩＮを設定した（またはリセット）したことに応答して、第２の合成バイオメトリックデータ２５５２を生成することができる。認証データ生成器２５７０は、第１のユーザ２５２６の銀行口座と関連付けられる「パスワード」として、第２の合成バイオメトリックデータ２５２２を第２のメモリ２５６２に記憶することができる。ある代替的な実施形態では、認証データ生成器２５７０は、第１の情報２５２８を受信したことに応答して、第２の合成バイオメトリックデータ２５５２を生成することができる。

【０２８４】

[00292]第２のバイオメトリックデータ２５５０は、認証デバイス２５０２の秘密鍵として機能し得る。第２のバイオメトリックデータ２５５０は、図１のバイオメトリックデータ１７０、図２０～図２３の第１のバイオメトリックデータ２００１、またはこれらの組合せに対応し得る。ある特定の実施形態では、第２のバイオメトリックデータ２５５０は、認証デバイス２５０２の第２のユーザ２５５６（たとえば、銀行の従業員）の指紋、虹彩スキャン、顔の画像、または声紋を含む。ある代替的な実施形態では、第２のバイオメトリックデータ２５５０は、特定の暗号システム（たとえば、Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ（ＲＳＡ）アルゴリズム、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式、楕円曲線暗号方式など）に基づいて選択される秘密鍵（たとえば、整数、自然数など）を含む。ある特定の実施形態では、第２のバイオメトリックデータ２５５０は、認証デバイス２５０２と一意に関連付けられる任意のバイオメトリックデータ（たとえば、銀行および／または銀行によって所有される特定のサーバを一意に識別するデータ）を含み得る。

【０２８５】

[00293]認証データ生成器２５７０は、モバイルデバイス１０２から第１の情報２５２８を受信したことに応答して、第２の情報２５５８をモバイルデバイス１０２に送信することができる。第２の情報２５５８は、第２の合成バイオメトリックデータ２５５２または第２の合成バイオメトリックデータ２５５２の特徴を含み得る。第２の情報２５５８は、認証デバイス２５０２の公開鍵として機能し得る。認証データ生成器２５７０は、第２の情報２５５８を第２のメモリ２５６２に記憶することができる。認証データ生成器２５７０は、第２の情報２５５８をモバイルデバイス１０２に送信することができる。たとえば、送受信機２５４２は第２の情報２５５８を送信することができる。

【０２８６】

[00294]認証データ生成器１１０は、送受信機１４２を介して第２の情報２５５８を受信することができる。認証データ生成器１１０は、第２の情報２５５８および第１のバイオメトリックデータ２５２０に基づいて第１の共通合成データ２５３０を生成することができる。第１の共通合成データ２５３０は、図２０の共通バイオメトリックデータ２０１７、図２１の共通バイオメトリックデータ２１１５、図２４の共通バイオメトリックデータ２２１７、図２７の共通バイオメトリックデータ２２１７、またはこれらの組合せに対

応し得る。たとえば、認証データ生成器１１０は、図２０～２３を参照して説明されるように、第１のバイオメトリックデータ２５２０から第１の特徴を抽出することができ、第２の情報２５５８から第２の特徴を抽出することができる。認証データ生成器１１０は、図２０～図２３を参照して説明されるように、第１の特徴および第２の特徴に基づいて、合成指紋、画像、または音声の生成を実行することによって、第１の共通合成データ２５３０を生成することができる。たとえば、認証データ生成器１１０は、一方向性関数を第１の特徴および第２の特徴に適用することによって、第１の共通合成データ２５３０を生成することができる。

【０２８７】

[00295]認証データ生成器１１０は、送受信機１４２を介して、第１の共通合成データ２５３０を認証デバイス２５０２に送信することができる。認証データ生成器２５７０は、第１の共通合成データ２５３０を受信することができ、第１の共通合成データ２５３０を第２のメモリ２５６２に記憶することができる。

【０２８８】

[00296]認証データ生成器２５７０は、第１の情報２５２８を受信したことに応答して、第２の共通合成データ２５６０を生成することができる。たとえば、認証データ生成器２５７０は、第１の情報２５２８および第２のバイオメトリックデータ２５５０に基づいて第２の共通合成データ２５６０を生成することができる。例示すると、認証データ生成器２５７０は、図２０～図２３を参照して説明されるように、第１の情報２５２８から第１の特徴を抽出することができ、第２のバイオメトリックデータ２５５０から第２の特徴を抽出することができ、第１の特徴および第２の特徴に基づいて第２の共通合成データ２５６０を生成することができる。たとえば、認証データ生成器２５７０は、一方向性関数を第１の特徴および第２の特徴に適用することによって、第２の共通合成データ２５６０を生成することができる。第２の共通合成データ２５６０は、図２０の共通バイオメトリックデータ２０１７、図２１の共通バイオメトリックデータ２１１５、図２４の共通バイオメトリックデータ２２１７、図２７の共通バイオメトリックデータ２２１７、またはこれらの組合せに対応し得る。

【０２８９】

[00297]認証データ生成器２５７０は、第１の共通合成データ２５３０を第２の共通合成データ２５６０と比較することができる。認証データ生成器２５７０は、第１の共通合成データ２５３０が第２の共通合成データ２５６０と一致すると決定したことに応答して、第１のユーザ２５２６、モバイルデバイス１０２、または両方の認証が成功すると決定することができる。たとえば、認証データ生成器２５７０は、第１の共通合成データ２５３０が第２の共通合成データ２５６０と一致すると決定したことに応答して、第１のユーザ２５２６、モバイルデバイス１０２、または両方によるアクセスを認証することができる。例示すると、認証データ生成器２５７０は、銀行口座、自動預け払い機（ＡＴＭ）、販売時点情報管理機器、金融システム、ユーザアカウント、車両のシステム、または建物のシステムのうちの少なくとも１つへのアクセスを認証することができる。車両のシステムは、ブレーキシステム、ドアの施錠システム、温度制御システム、音響システム、セキュリティシステム、エンターテインメントシステム、または全地球測位システムを含み得る。したがって、第１の共通合成データ２５３０は銀行の「パスワード」として機能し得る。

【０２９０】

[00298]認証データ生成器１１０は、鍵２５０４（たとえば、英数字パスワードなどの共有される秘密）および第１のバイオメトリックデータ２５２０（たとえば、モバイルデバイス１０２の秘密鍵）に基づいて、第１の情報２５２８を生成することができる。認証データ生成器１１０は、モバイルデバイス１０２の公開鍵として第１の情報２５２８を認証デバイス２５０２に提供することができる。

【０２９１】

[00299]認証データ生成器２５７０は、鍵２５０４（たとえば、共有される秘密）およ

び第２のバイオメトリックデータ２５５０（たとえば、認証デバイス２５０２の秘密鍵）に基づいて、第２の情報２５５８を生成することができる。認証データ生成器２５７０は、認証デバイス２５０２の公開鍵として第２の情報２５５８をモバイルデバイス１０２に提供することができる。

【０２９２】

[00300]認証データ生成器１１０は、第１のバイオメトリックデータ２５２０（たとえば、モバイルデバイス１０２の秘密鍵）および第２の情報２５５８（たとえば、認証デバイス２５０２の公開鍵）に基づいて、第１の共通合成データ２５３０を生成することができる。認証データ生成器１１０は、第１の共通合成データ２５３０を認証デバイス２５０２にパスワードとして提供することができる。

【０２９３】

[00301]認証データ生成器２５７０は、第２のバイオメトリックデータ２５５０（たとえば、認証デバイス２５０２の秘密鍵）および第１の情報２５２８（たとえば、モバイルデバイス１０２の公開鍵）に基づいて、第２の共通合成データ２５６０を生成することができる。認証データ生成器２５７０は、第１の共通合成データ２５３０が第２の共通合成データ２５６０と一致すると決定したことに応答して、アクセスを認証することができる。

【０２９４】

[00302]モバイルデバイス１０２は、認証デバイス２５０２が第１の合成バイオメトリックデータ２５２２に基づいて第１のユーザ２５２６、モバイルデバイス１０２、または両方を認証するとき、ネットワーク２５７２を介して別の電子デバイスとの認証されたセッションを行うことができる。たとえば、認証デバイス２５０２は、認証サーバを含んでよく、第１のユーザ２５２６、モバイルデバイス１０２、または両方の認証が成功したと決定したことに応答して別の電子デバイス（たとえば、金融システムのデバイス、車両のデバイス、建物のデバイスなど）へのアクセス権を与えることができる。認証デバイス２５０２は、第１の共通合成データ２５３０が第２の共通合成データ２５６０と一致しないと決定したことに応答して、第１のユーザ２５２６の認証が成功しないと決定することができる。

【０２９５】

[00303]したがって、システム２５００は、第１のバイオメトリックデータ２５２０および鍵２５０４に基づく選択的なアクセス認証を可能にし得る。モバイルデバイス１０２は、合成バイオメトリックデータ（たとえば、第１の情報２５２８および第１の共通合成データ２５３０）を認証デバイス２５０２に提供することができる。第１のバイオメトリックデータ２５２０は、第１の情報２５２８、第１の共通合成データ２５３０、または両方から復元不可能（または実質的に復元不可能）であり得る。

【０２９６】

[00304]図２６を参照すると、バイオメトリックデータおよび非バイオメトリックデータに基づいて車両のシステムへのアクセスを選択的に認証するように構成されるシステムのある特定の実施形態の図が示されており、全体的に２６００と指定されている。システム２６００は、認証デバイス２５０２が車２６０２に含まれるという点でシステム２５００と異なる。

【０２９７】

[00305]認証デバイス２５０２は、図２５を参照して説明されたように、第１の共通合成データ２５３０と第２の共通合成データ２５６０を比較することができる。認証デバイス２５０２は、比較に基づいて車２６０２のシステムへのアクセスを選択的に認証することができる。たとえば、認証デバイス２５０２は、第１の共通合成データ２５３０が第２の共通合成データ２５６０と一致すると決定したことに応答して、車２６０２のシステムへのアクセスを認証することができる。車のシステムは、ブレーキシステム、ドアの施錠システム、車庫の扉の起動システム、温度制御システム、音響システム、セキュリティシステム、エンターテインメントシステム、通信システム、または全地球測位システムのう

ちの少なくとも１つを含み得る。

【０２９８】

[00306]第１のユーザ２５２６は、車２６０２のシステムにアクセスするためにモバイルデバイス１０２を使用することができる。たとえば、第１のユーザ２５２６は、寒い朝に車２６０２の外に出ることなく車２６０２のエンジンを始動するために、鍵２５０４と第１のバイオメトリックデータ２５２０とを提供することができる。別の例として、第１のユーザ２５２６は、町の外にいることがあり、第１のユーザ２５２６の友人が第１のユーザ２５２６の自宅に入れるようにするためにモバイルデバイス１０２を使用することができる。例示すると、第１のユーザ２５２６は、車２６０２の車庫開扉機構を起動するために、鍵２５０４と第１のバイオメトリックデータ２５２０とをモバイルデバイス１０２に提供することができる。友人は、車庫の扉を通って自宅に入ることができる。さらなる例として、図２５の第２のバイオメトリックデータ２５５０は、図２５の第２のユーザ２５５６に対応し得る。第２のユーザ２５５６は、第１のユーザ２５２６の親であり得る。第２のユーザ２５５６は、車２６０２の認証デバイス２５０２へのユーザ入力を介して鍵２５０４を提供することができる。第２のユーザ２５５６は、車２６０２を第１のユーザ２５２６が使用できる状態であるとき、鍵２５０４を第１のユーザ２５２６に提供することができる。第２のユーザ２５５６は、車２６０２を第１のユーザ２５２６が使用できない状態であるとき、認証デバイス２５０２において鍵２５０４をリセットすることができる。第１のユーザ２５２６は、車２６０２に対する物理的な鍵を持っていないことがある。第１のユーザ２５２６は、車２６０２の鍵２５０４と一致する鍵２５０４がないと、車２６０２にアクセスすることが不可能であり得る。

【０２９９】

[00307]したがって、システム２６００は、第１のバイオメトリックデータ２５２０および鍵２５０４に基づく選択的なアクセス認証を可能にし得る。モバイルデバイス１０２は、合成バイオメトリックデータ（たとえば、第１の情報２５２８および第１の共通合成データ２５３０）を認証デバイス２５０２に提供することができる。認証デバイス２５０２は、図２５の第１の情報２５２８、第１の共通合成データ２５３０、鍵２５０４、および第２のバイオメトリックデータ２５５０に基づいて、車２６０２のシステムへのアクセスを認証することができる。第１のバイオメトリックデータ２５２０は、第１の情報２５２８、第１の共通合成データ２５３０、または両方から復元不可能（または実質的に復元不可能）であり得る。

【０３００】

[00308]図２７を参照すると、電子デバイスの特定の実施形態のブロック図が示されており、全体的に２７００と指定されている。デバイス２７００は、図１のシステムを使用して、バイオメトリックデータおよび非バイオメトリックに基づいて認証データを生成することができる。たとえば、デバイス２７００は、図１のモバイルデバイス１０２に対応し得る。デバイス２７００は、バイオメトリックデータおよび非バイオメトリックに基づいてアクセスを選択的に認証することができる。たとえば、デバイス２７００は、図２５～図２６の認証デバイス２５０２に対応し得る。

【０３０１】

[00309]デバイス２７００は、メモリ１３２に結合されたプロセッサ２７１０（たとえば、デジタルシグナルプロセッサ（ＤＳＰ））を含む。プロセッサ２７１０は、認証データ生成器１１０を含んでよく、またはそれに結合されてよい。説明のための例では、プロセッサ２７１０は、図１～図２６を参照して説明された１つまたは複数の動作もしくは方法を実行する。

【０３０２】

[00310]図２７はまた、プロセッサ２７１０とディスプレイ２７２８とに結合されたディスプレイコントローラ２７２６を示す。コーダ／デコーダ（コーデック）２７３４も、プロセッサ２７１０に結合され得る。スピーカー２７３６とマイクロフォン２７３８が、コーデック２７３４に結合され得る。ある特定の実施形態では、マイクロフォン２７３８

は図１２のマイクロフォン１２０２に対応し得る。デバイス２７００は、指紋センサ１１０８、虹彩スキャンセンサ１２０８、もしくは両方に結合されてよく、または含んでよい。ある特定の実施形態では、デバイス２７００は、指紋センサ１１０８、虹彩スキャンセンサ１２０８、または両方への１つまたは複数のインターフェース（たとえば、第１のインターフェース１３４、第２のインターフェース１３６、または両方）を介して結合され得る。

【０３０３】

[00311]図２７はまた、プロセッサ２７１０がワイヤレスアンテナ２７４２に送受信機１４２を介して結合され得ることを示す。ある特定の実施形態では、プロセッサ２７１０、ディスプレイコントローラ２７２６、メモリ１３２、コーデック２７３４、および送受信機１４２は、システムインパッケージまたはシステムオンチップデバイス２７２２に含まれる。ある特定の実施形態では、入力デバイス２７３０および電源２７４４が、システムオンチップデバイス２７２２に結合される。その上、特定の実施形態では、図２７に示されるように、ディスプレイ２７２８、入力デバイス２７３０、スピーカー２７３６、マイクロフォン２７３８、指紋センサ１１０８、虹彩スキャンセンサ１２０８、ワイヤレスアンテナ２７４２、ならびに電源２７４４は、システムオンチップデバイス２７２２の外部にある。しかしながら、ディスプレイ２７２８、入力デバイス２７３０、スピーカー２７３６、マイクロフォン２７３８、ワイヤレスアンテナ２７４２、指紋センサ１１０８、虹彩スキャンセンサ１２０８、および電源２７４４の各々は、インターフェース（たとえば、第１のインターフェース１３４または第２のインターフェース１３６）またはコントローラなどの、システムオンチップデバイス２７２２のコンポーネントに結合され得る。

【０３０４】

[00312]説明された実施形態とともに、第１の合成バイオメトリックデータに対応する第１の共通合成データと第１の情報とを受信するための手段を含む、通信のための装置が開示される。たとえば、受信するための手段は、図１の送受信機１４２、認証データ生成器１１０、図２５の認証データ生成器２５７０、送受信機２５４２、図２７のプロセッサ２７１０、図２５の第１の共通合成データ２５３０と第１の情報２５２８とを受信するように構成される１つまたは複数のデバイス（たとえば、非一時的コンピュータ可読記憶媒体において命令を実行するプロセッサ）、またはこれらの組合せを含み得る。

【０３０５】

[00313]装置はまた、第２のバイオメトリックデータを取得するための手段を含む。たとえば、取得するための手段は、図１の第１のインターフェース１３４、認証データ生成器１１０、図１１の指紋センサ１１０８、図１２のマイクロフォン１２０２、虹彩スキャンセンサ１２０８、図２５のマイクロフォン２６３８、認証データ生成器２５７０、図２７のプロセッサ２７１０、図２５の第２のバイオメトリックデータ２５５０を取得するように構成される１つまたは複数のデバイス（たとえば、非一時的コンピュータ可読記憶媒体において命令を実行するプロセッサ）、またはこれらの組合せを含み得る。

【０３０６】

[00314]装置はさらに、第１の情報および第２のバイオメトリックデータに基づいて第２の共通合成データを生成し、第１の共通合成データと第２の共通合成データの比較に基づいてアクセスを選択的に認証するように構成される、認証のための手段を含む。たとえば、認証のための手段は、図１の認証データ生成器１１０、図２６のプロセッサ２６１０、図２５の認証データ生成器２５７０、図２５の第２の共通合成データ２５６０を生成し、図２５の第１の共通合成データ２５３０と第２の共通合成データ２５６０の比較に基づいてアクセスを選択的に認証するように構成される１つまたは複数のデバイス（たとえば、非一時的コンピュータ可読記憶媒体において命令を実行するプロセッサ）、またはこれらの組合せを含み得る。

【０３０７】

[00315]本明細書で開示された実施形態に関して説明された様々な例示的な論理ブロック、構成、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コン

ピュータソフトウェア、または両方の組合せとして実装され得ることを、当業者はさらに諒解するだろう。様々な例示的なコンポーネント、ブロック、構成、モジュール、回路、およびステップが、上では概して、それらの機能に関して説明された。そのような機能がハードウェアとして実装されるか、ソフトウェアとして実装されるかは、具体的な適用例および全体的なシステムに課された設計制約に依存する。当業者は、説明された機能を各々の具体的な適用例ごとに様々な方法で実装することができるが、そのような実装の決定は、本開示の範囲からの逸脱を生じさせるものと解釈されるべきではない。

【０３０８】

[00316]本明細書で開示される実施形態に関して説明された方法またはアルゴリズムのステップは、直接ハードウェアで具現化され得るか、プロセッサによって実行されるソフトウェアモジュールで具現化され得るか、またはその２つの組合せで実行され得る。ソフトウェアモジュールは、ランダムアクセスメモリ（ＲＡＭ）、フラッシュメモリ、読取り専用メモリ（ＲＯＭ）、プログラマブル読取り専用メモリ（ＰＲＯＭ）、消去可能プログラマブル読取り専用メモリ（ＥＰＲＯＭ）、電気的消去可能プログラマブル読取り専用メモリ（ＥＥＰＲＯＭ（登録商標））、レジスタ、ハードディスク、リムーバブルディスク、またはコンパクトディスク読取り専用メモリ（ＣＤ－ＲＯＭ）の中に存在し得る。例示的な非一時的（たとえば、有形）記憶媒体（たとえば、記憶デバイス）は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合され得る。代替的に、記憶媒体はプロセッサと一体であり得る。プロセッサおよび記憶媒体は、特定用途向け集積回路（ＡＳＩＣ）中に存在し得る。ＡＳＩＣは、コンピューティングデバイスまたはユーザ端末中に存在し得る。代替的に、プロセッサおよび記憶媒体は、コンピューティングデバイスまたはユーザ端末中に個別のコンポーネントとして存在し得る。デバイス２７００は、通信デバイス、携帯情報端末（ＰＤＡ）、タブレット、コンピュータ、音楽プレーヤー、ビデオプレーヤー、エンターテインメントユニット、ナビゲーションデバイス、またはセットトップボックスを含み得る。

【０３０９】

[00317]記憶媒体（たとえば、記憶デバイス）は、プロセッサ（たとえば、プロセッサ２７１０）によって実行されると、図１～図２２を参照して説明された方法および動作の少なくとも一部分をプロセッサに実行させ得る命令（たとえば、命令２７４０）を含み得る。例として、メモリ１３２は、プロセッサ２７１０によって実行されると、図１～図２２を参照して説明された方法および動作の少なくとも一部分をプロセッサ２７１０に実行させる命令（たとえば、命令２７４０）を含む、非一時的コンピュータ可読記憶媒体（または記憶デバイス）であり得る。たとえば、プロセッサ２７１０は、バイオメトリックデータ１７０とユーザ入力１７２とを受信することができる。プロセッサ２７１０は、ユーザ入力１７２に基づいて非バイオメトリックデータ１７６を生成することができる。プロセッサ２７１０は、バイオメトリックデータ１７０および非バイオメトリックデータ１７６に基づいて認証データ１７８（たとえば、オーディオデータ１９８、第２の画像１９６、および／または第２のバイオメトリックデータ１８０）を生成することができる。プロセッサ２７１０は、送受信機１４２を介して認証データ１７８をワイヤレスアンテナ２７４２に提供することができる。たとえば、プロセッサ２７１０は、認証データ１７８に基づいてパケットを生成し、パケットを送受信機１４２に提供することができる。

【０３１０】

[00318]開示される実施形態の上の説明は、開示される実施形態を当業者が作成または使用することを可能にするために与えられる。これらの実施形態に対する様々な修正は、当業者には容易に明らかになり、本明細書において規定される原理は、本開示の範囲から逸脱することなく、他の実施形態に適用され得る。したがって、本開示は、本明細書において示される実施形態に限定されることは意図されず、特許請求の範囲によって規定される原理および新規の特徴と合致する、可能な限り最も広い範囲が与えられるべきである。

【図１】

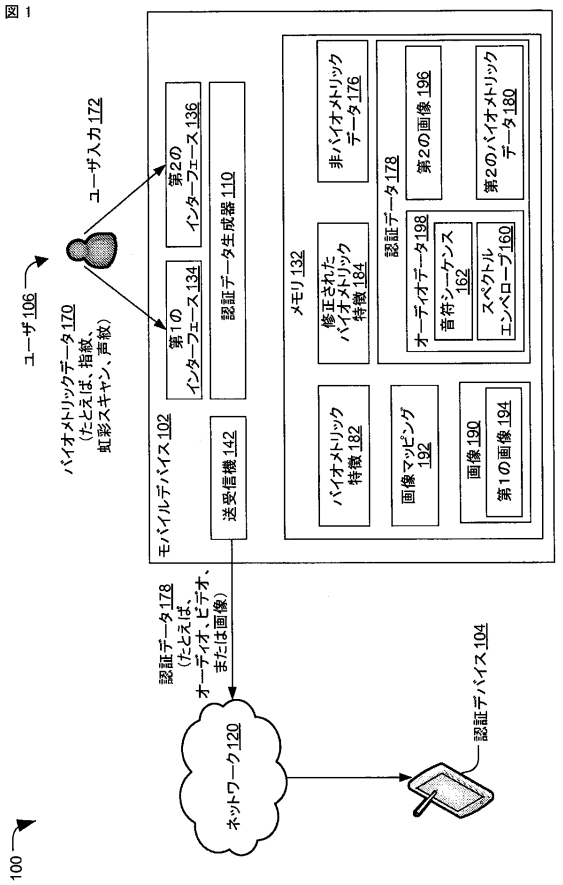

FIG. 1

【図２】

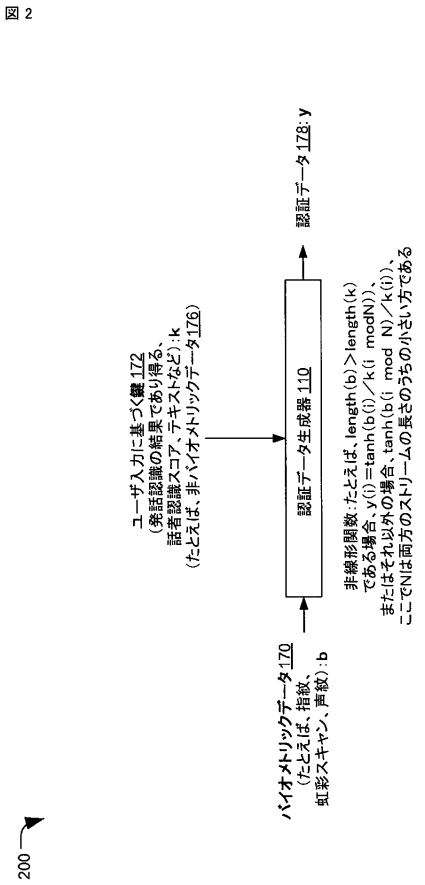

FIG. 2

【図３】

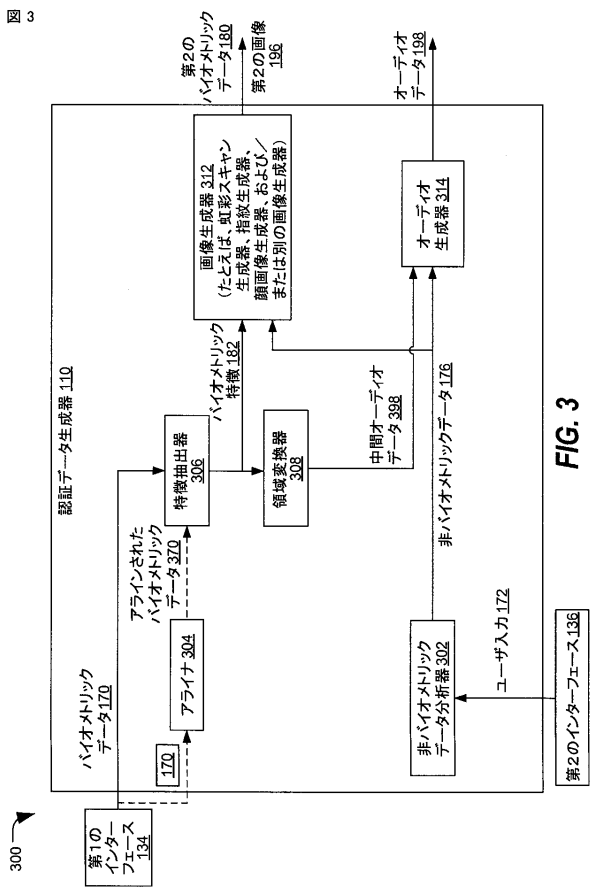

FIG. 3

【図４】

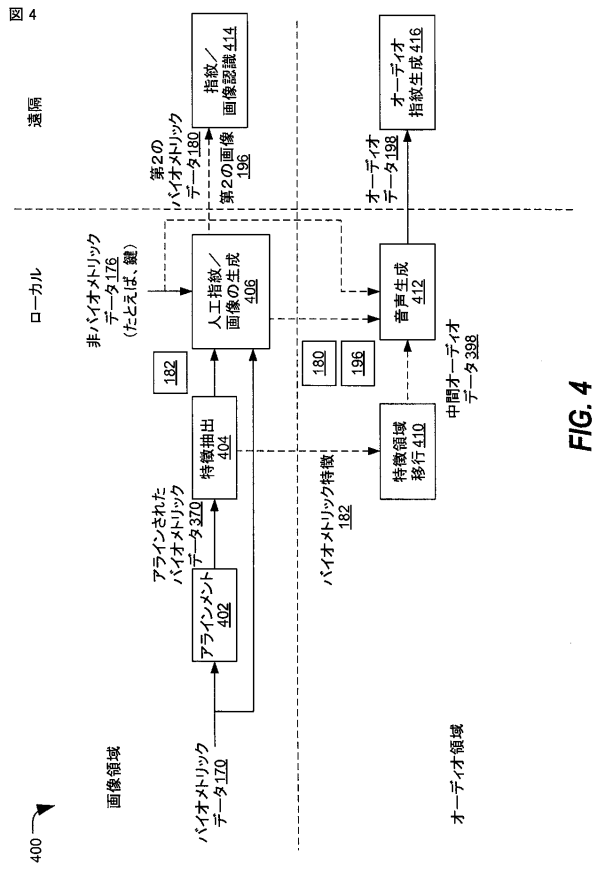

FIG. 4

【図５】

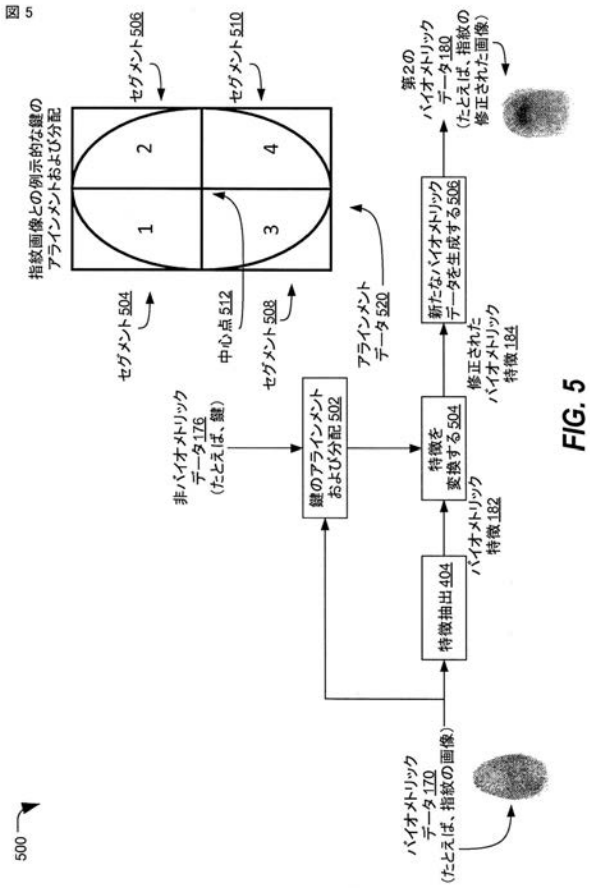

FIG. 5

【図６】

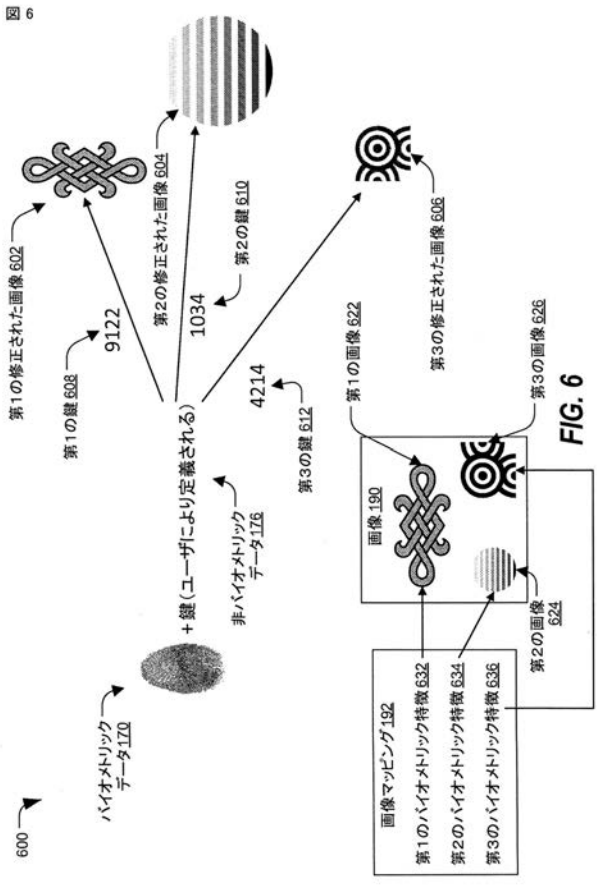

FIG. 6

【図７】

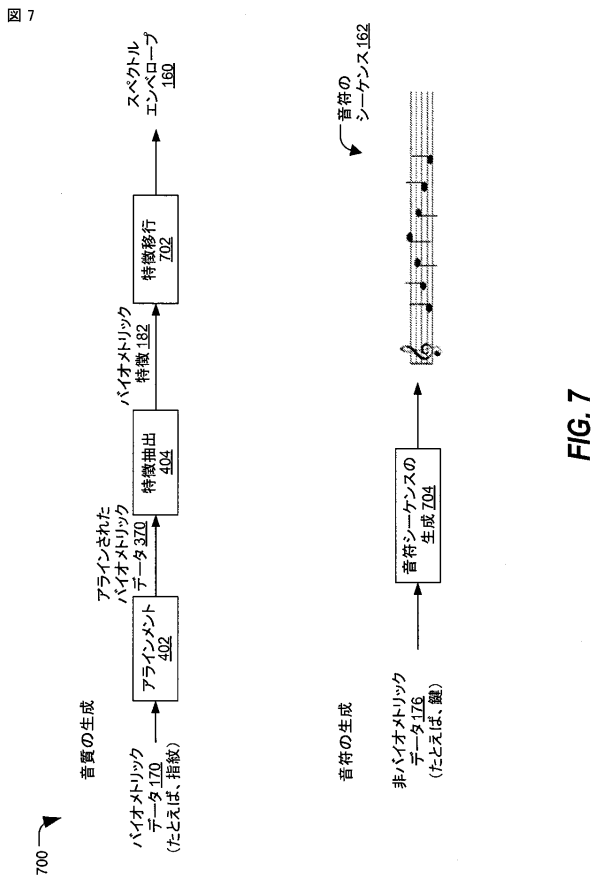

FIG. 7

【図８】

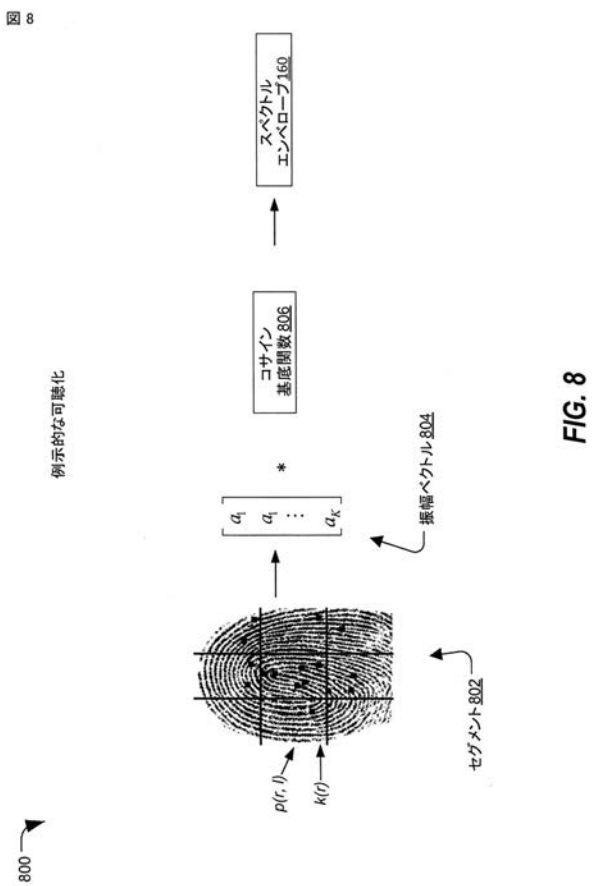

FIG. 8

【図９】

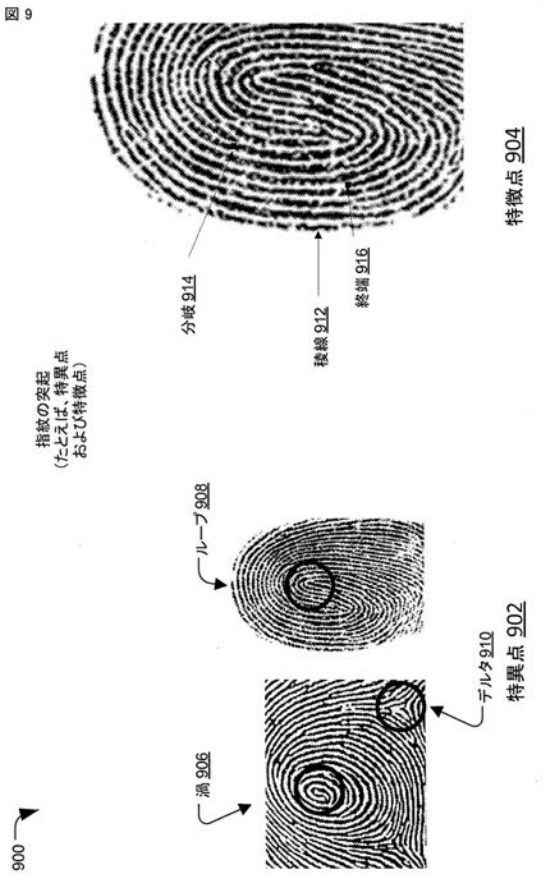

FIG. 9

【図１０】

FIG. 10

【図１１】

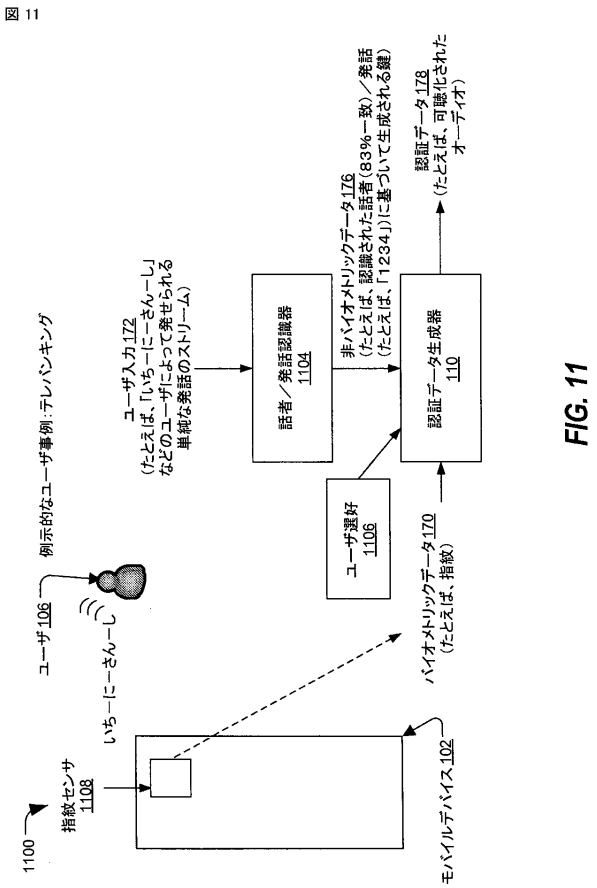

FIG. 11

【図１２】

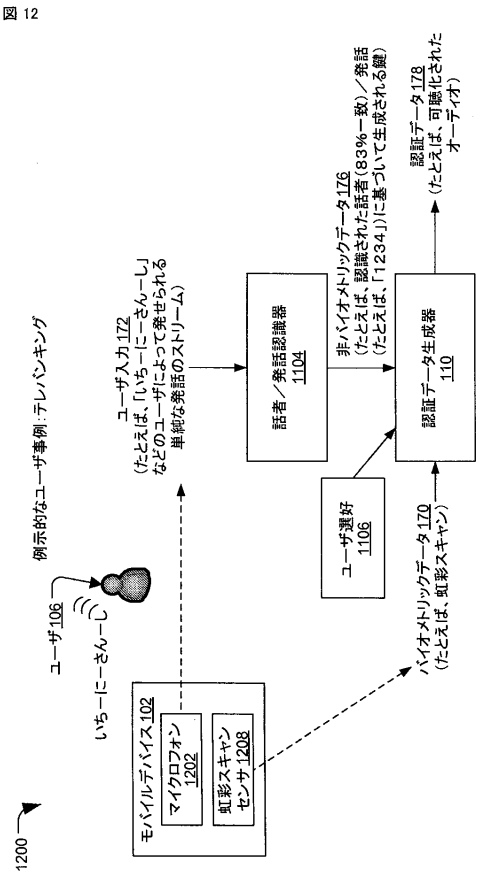

FIG. 12

【図１３】

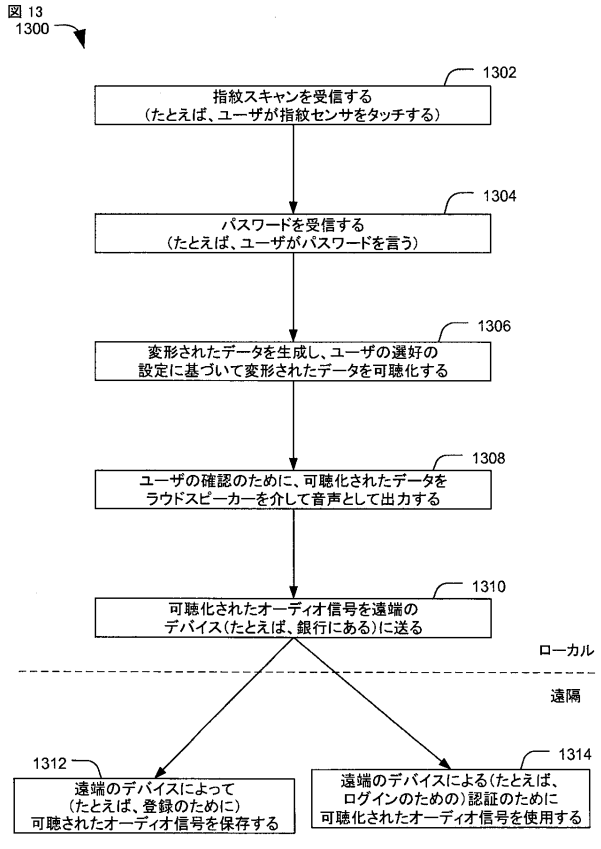

FIG. 13

【図１４】

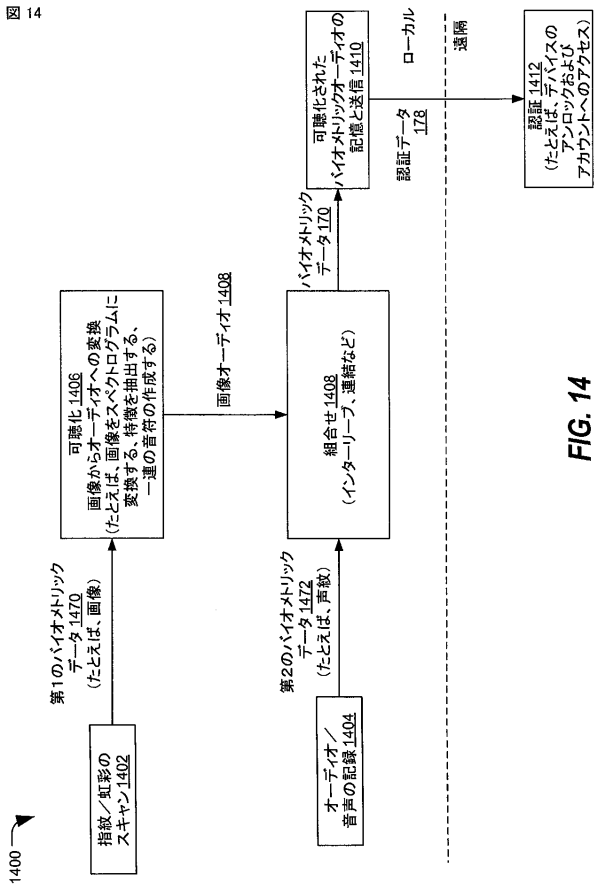

FIG. 14

【図１５】

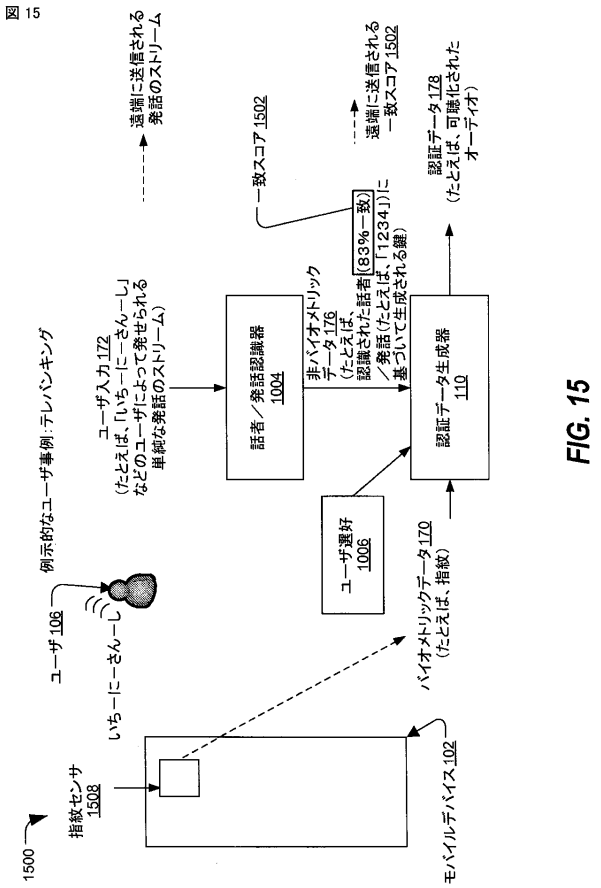

FIG. 15

【図１６】

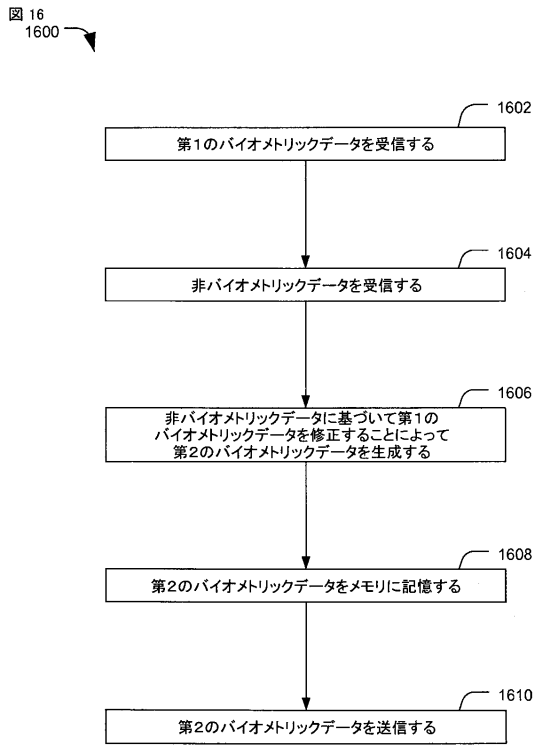

FIG. 16

【図１７】

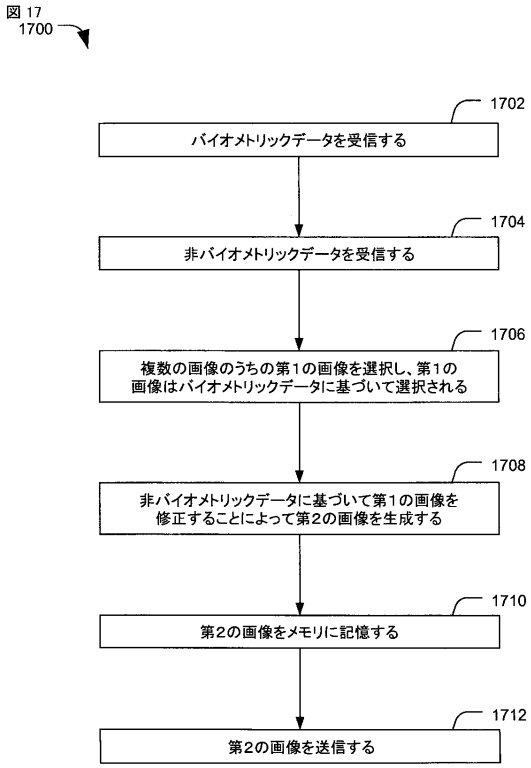

FIG. 17

【図１８】

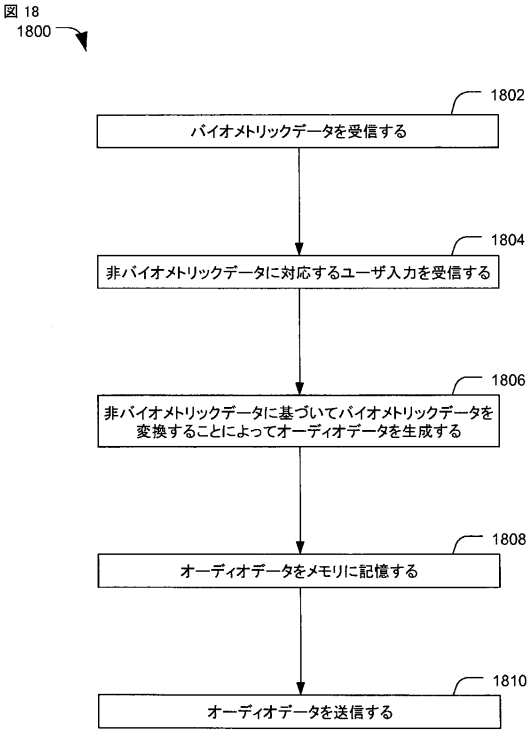

FIG. 18

【図１９】

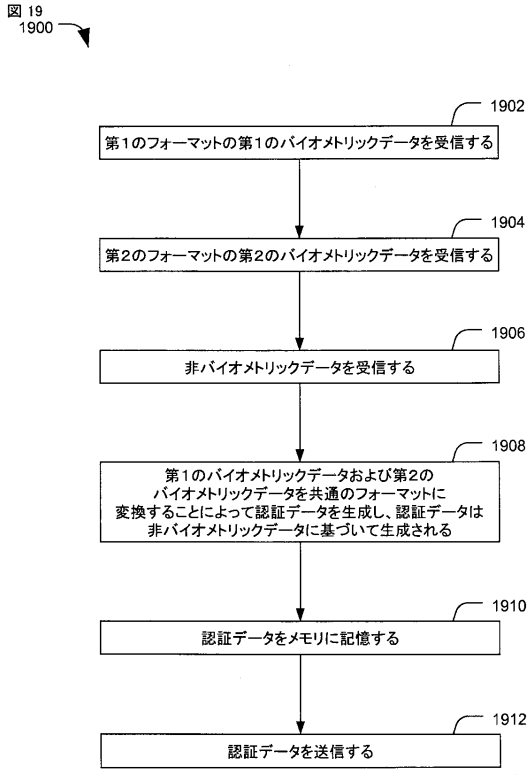

FIG. 19

【図２０】

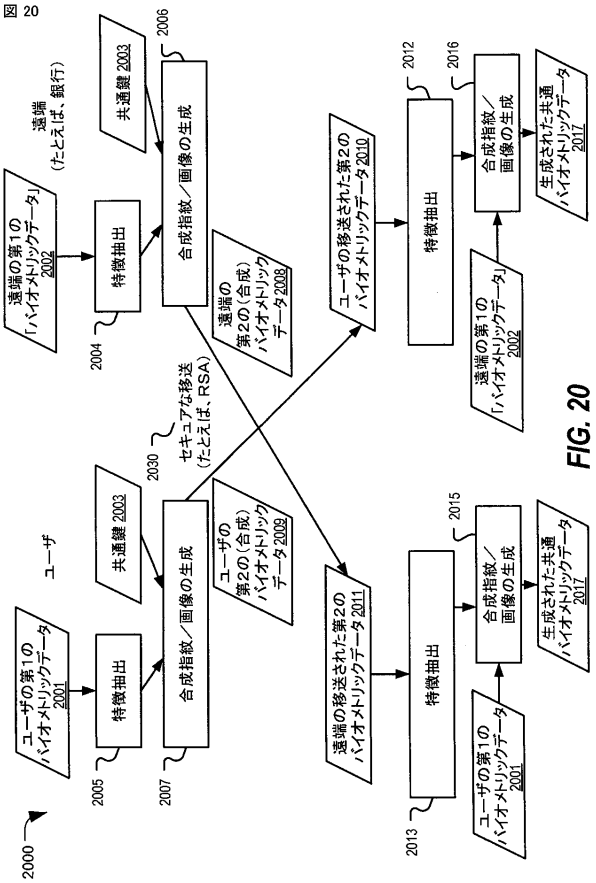

FIG. 20

【図２１】

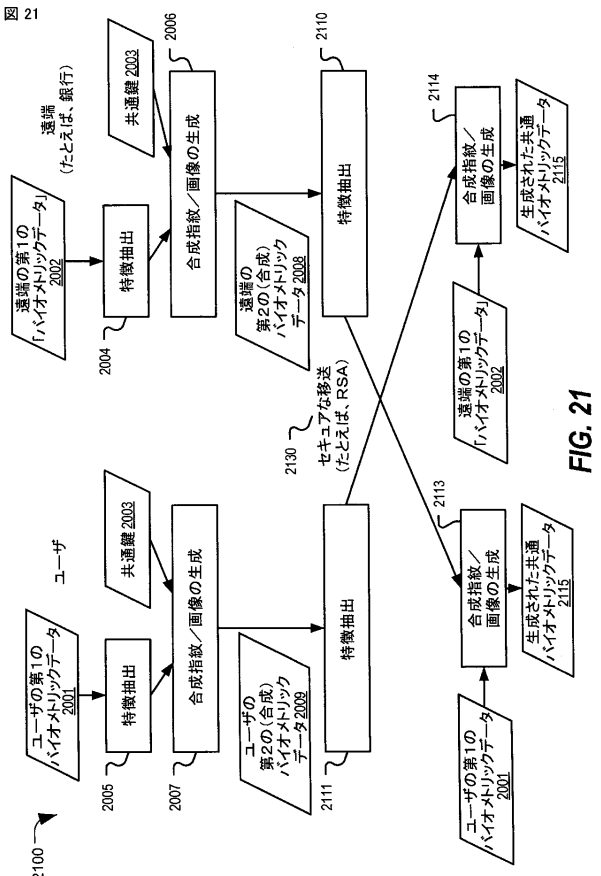

FIG. 21

【図２２】

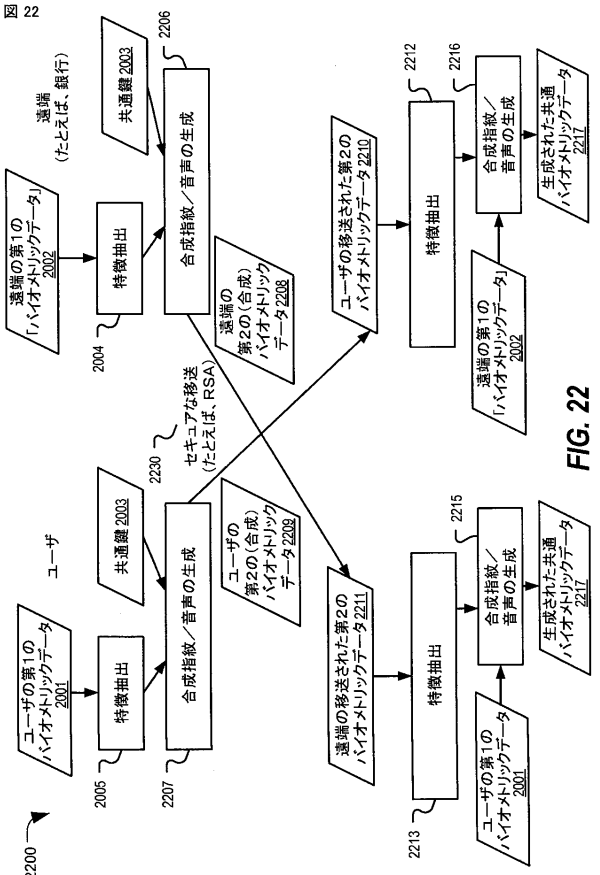

FIG. 22

【図２３】

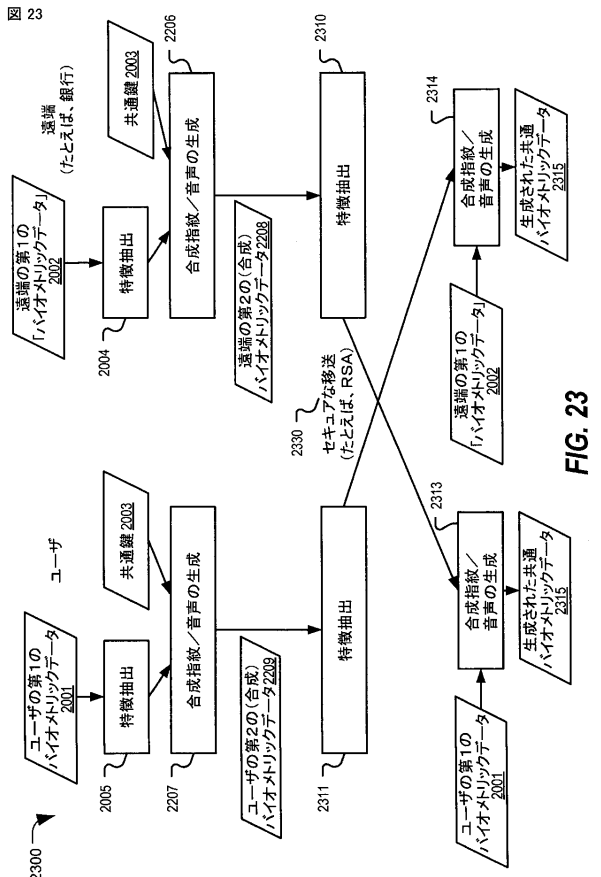

FIG. 23

【図２４】

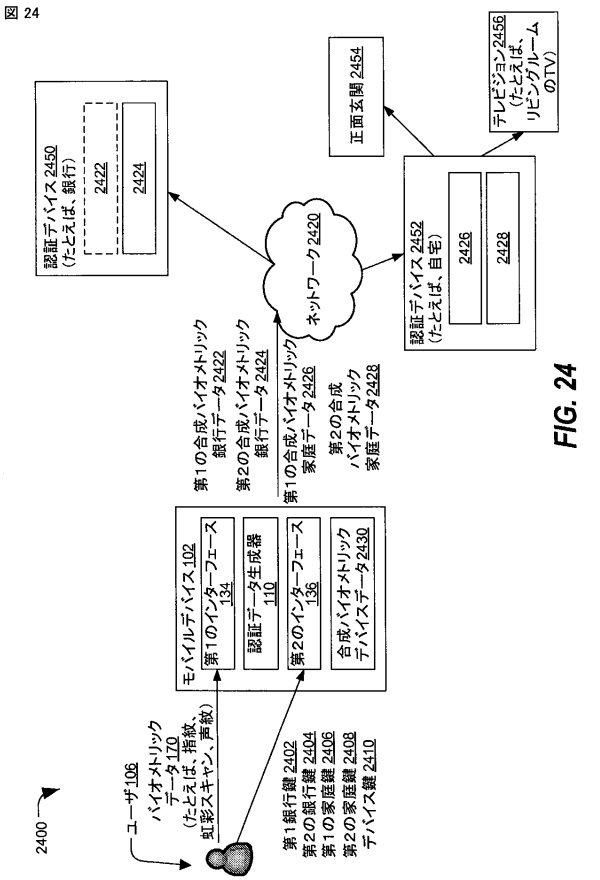

FIG. 24

【図２５】

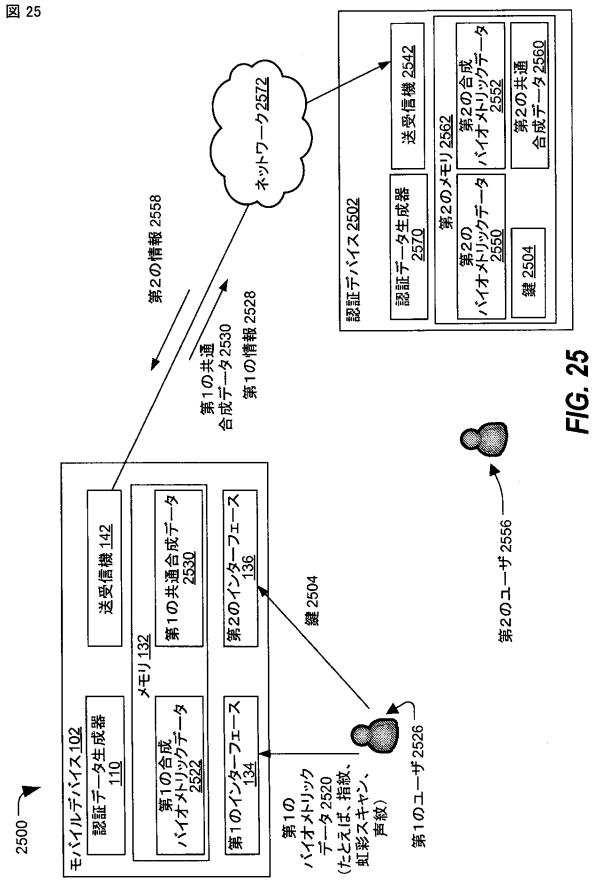

FIG. 25

【図２６】

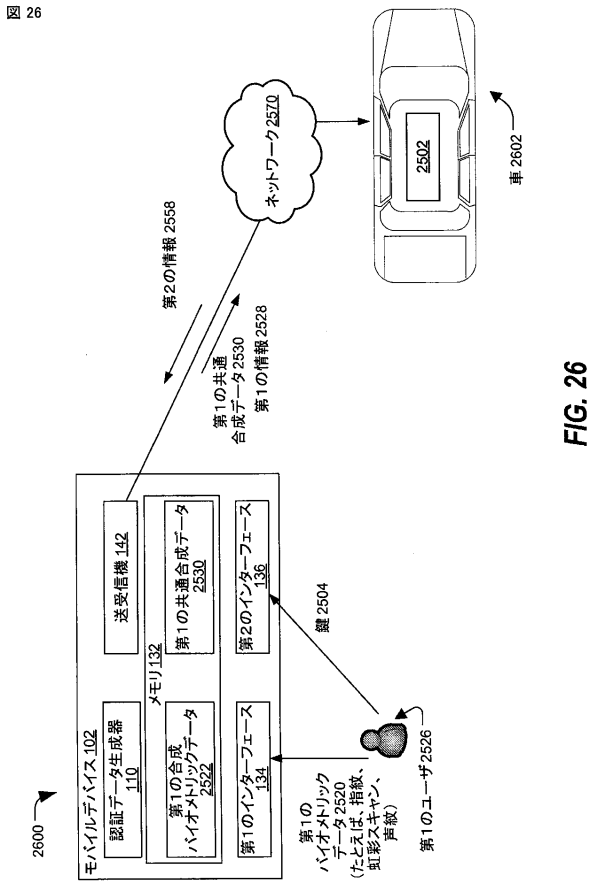

FIG. 26

【図２７】

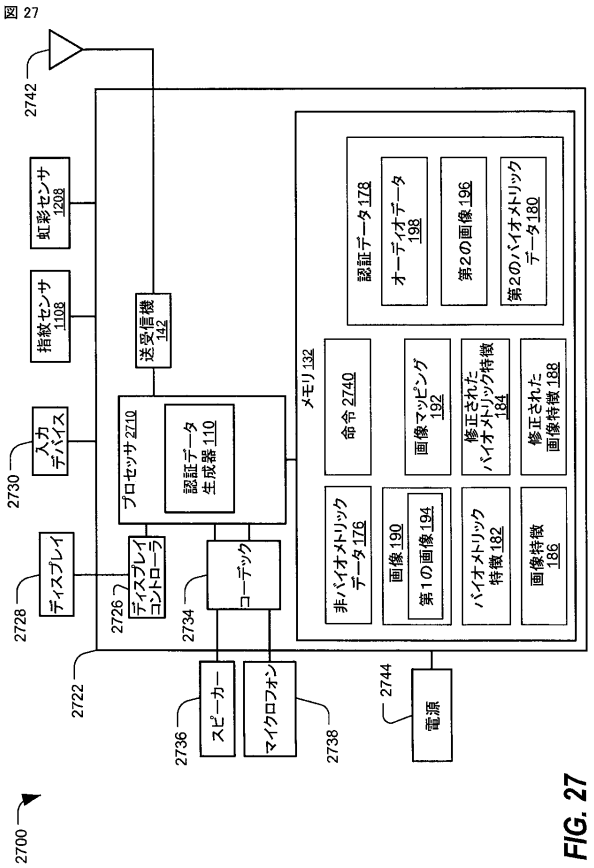

FIG. 27

【手続補正書】
【提出日】平成29年4月21日(2017.4.21)
【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】
ユーザからバイオメトリックデータを受信するように構成されたセンサと、
前記ユーザから非バイオメトリックデータを受信するように構成された入力インターフェースと、
前記非バイオメトリックデータに基づいて前記バイオメトリックデータを修正することと、
前記バイオメトリックデータと関連付けられるタイムスタンプに基づいて、合成バイオメトリックデータを生成することと
を行うように構成されたプロセッサと、
ネットワークを介して、前記ユーザを認証するために、認証サーバに前記合成バイオメトリックデータを送信するように構成されたネットワークインターフェースと
を備える、装置。
【請求項２】
前記バイオメトリックデータの修正の前に、前記センサから受信された前記バイオメトリックデータを記憶するように構成されたメモリをさらに備える、
請求項１に記載の装置。
【請求項３】
前記タイムスタンプは、前記バイオメトリックデータが前記センサで受信される、またはメモリに記憶される時間を示す、
請求項１に記載の装置。
【請求項４】
前記プロセッサは、第２のタイムスタンプと前記タイムスタンプとの差が閾値を超えるかどうかに基づいて、前記バイオメトリックデータが期限切れになったかどうかを決定するように構成され、前記第２のタイムスタンプは、前記タイムスタンプと関連付けられる第１の時間の後に続く第２の時間と関連付けられる、
請求項１に記載の装置。
【請求項５】
前記センサは、マイクロフォン、指紋スキャナ、虹彩スキャナ、またはカメラを備え、前記バイオメトリックデータは、前記ユーザの発話信号、前記ユーザの指紋、前記ユーザの虹彩スキャナ、または前記ユーザの顔画像を備える、
請求項１に記載の装置。
【請求項６】
閾値は、メモリに記憶され、バイオメトリック情報のタイプと関連付けられ、前記タイプは、前記バイオメトリック情報と関連付けられる生物学的特徴に対応する、
請求項１に記載の装置。
【請求項７】
前記非バイオメトリックデータは、英数字鍵を備え、前記合成バイオメトリックデータは、合成指紋、合成虹彩スキャン、合成発話信号、合成画像、またはこれらの任意の組み合わせを備える、
請求項１に記載の装置。
【請求項８】
前記ネットワークインターフェースは、前記合成バイオメトリックデータに基づいて前

記ユーザを認証する前記認証サーバに応答して、前記ネットワークを介して別の電子デバイスと認証されたセッションを行うようにさらに構成される、
請求項１に記載の装置。
【請求項９】
前記バイオメトリックデータは、前記合成バイオメトリックデータから非復元可能である、
請求項１に記載の装置。
【請求項１０】
前記バイオメトリックデータは、第１の領域内にあり、前記非バイオメトリックデータは、前記第１の領域と異なる第２の領域内にある、
請求項１に記載の装置。
【請求項１１】
前記第１の領域は、オーディオ領域または画像領域のうちの１つに対応し、前記第２の領域は、前記オーディオ領域または前記画像領域のうちのもう一方に対応する、
請求項１０に記載の装置。
【請求項１２】
前記第２のタイムスタンプは、前記合成バイオメトリックデータをメモリに記憶することと関連付けられる、
請求項４に記載の装置。
【請求項１３】
デバイスにおいて、ユーザからバイオメトリックデータを受信することと、
前記デバイスにおいて、前記ユーザから第１の非バイオメトリックデータを受信することと、
前記デバイスにおいて、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを修正することと、
前記デバイスにおいて、前記バイオメトリックデータと関連付けられるタイムスタンプに基づいて、第１の合成バイオメトリックデータを生成することと、
ネットワークを介して前記デバイスから第１の認証サーバに、前記ユーザを認証するために前記第１の合成バイオメトリックデータを送信することと
を備える、方法。
【請求項１４】
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータを生成することは、前記第２の非バイオメトリックデータに基づいて前記バイオメトリックデータを修正することを含む、と、
前記ユーザを認証するために、前記デバイスから第２の認証サーバに、前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１３に記載の方法。
【請求項１５】
前記第１の合成バイオメトリックデータを生成することは、前記デバイスにおいて、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含み、前記第１の認証サーバは、前記ユーザに対応する認証データとして前記第１の合成バイオメトリックデータを記憶するように構成され、前記認証データと受信した合成バイオメトリックデータを比較することによって前記ユーザを認証するように構成される、
請求項１３に記載の方法。
【請求項１６】
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、

前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータを生成することは、前記第２の非バイオメトリックデータに基づいて前記バイオメトリックデータを修正することを含む、と、
前記デバイスから前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信すること、ここにおいて、前記第２の合成バイオメトリックデータは、前記ユーザに対応する前記認証データとして前記第１の合成バイオメトリックデータを置き換える、と
をさらに備える、請求項１５に記載の方法。
【請求項１７】
プロセッサによって実行されると、前記プロセッサに、
ユーザからバイオメトリックデータを受信することと、
前記ユーザから第１の非バイオメトリックデータを受信することと、
前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを修正することと、
前記バイオメトリックデータと関連付けられるタイムスタンプに基づいて、第１の合成バイオメトリックデータを生成することと、
ネットワークを介して、前記ユーザを認証するために、第１の認証サーバに前記第１の合成バイオメトリックデータを送信することと
を備える、動作を実行させる命令を記憶した、コンピュータ可読記憶デバイス。
【請求項１８】
前記動作は、
前記バイオメトリックデータの特徴を抽出することと、
メモリに前記特徴を記憶することと
をさらに備え、前記第１の合成バイオメトリックデータは、前記第１の非バイオメトリックデータに基づいて前記特徴を修正することによって生成され、前記第１の合成バイオメトリックデータを生成することは、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項１９】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記第２の非バイオメトリックデータに基づいて前記特徴を修正することによって第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備え、前記第２の合成バイオメトリックデータは、前記ユーザに対応する認証データとして、前記第１の認証サーバにおいて、前記第１の合成バイオメトリックデータを置き換える、
請求項１８に記載のコンピュータ可読記憶デバイス。
【請求項２０】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れになったと決定することに応答して、第２のバイオメトリックデータを提供するように前記ユーザに促すことと、
前記ユーザから前記第２のバイオメトリックデータを受信することと、
前記第２のバイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２１】
前記動作は、前記バイオメトリックデータが第２のタイムスタンプと前記タイムスタンプとの差に基づいて期限切れになったかどうかを決定することをさらに備え、前記第２の

タイムスタンプは、クロックの時間に基づく、
請求項２０に記載のコンピュータ可読記憶デバイス。
【請求項２２】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れでないと決定することに応答して、前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２３】
前記第１の非バイオメトリックデータは、第１の電子デバイスと関連付けられ、前記第１の合成バイオメトリックデータは、前記ユーザおよび前記第１の電子デバイスと関連付けられる第１の認証データに対応する、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２４】
前記動作は、
前記ユーザから第２の電子デバイスに関連付けられた第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備え、前記第２の合成バイオメトリックデータは、前記ユーザおよび前記第２の電子デバイスと関連付けられた第２の認証データに対応する、
請求項２３に記載のコンピュータ可読記憶デバイス。
【請求項２５】
前記動作は、閾値と前記差を比較することをさらに備え、前記閾値は、前記バイオメトリックデータが期限切れになったかどうかを示す、
請求項２１に記載のコンピュータ可読記憶デバイス。
【請求項２６】
前記第１の合成バイオメトリックデータは、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータに一方向性関数を適用することによって生成される、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２７】
前記一方向性関数は、ハッシュ関数、指数関数、剰余関数、双曲線正接関数、または別の双曲線関数のうちの少なくとも１つを含む、
請求項２６に記載のコンピュータ可読記憶デバイス。
【請求項２８】
ユーザからバイオメトリックデータを受信するための手段と、
前記ユーザから非バイオメトリックデータを受信するための手段と、
前記非バイオメトリックデータに基づいて前記バイオメトリックデータを修正するための手段と、
前記バイオメトリックデータと関連付けられるタイムスタンプに基づいて、合成バイオメトリックデータを生成するための手段と、
ネットワークを介して、前記ユーザを認証するために、認証サーバに前記合成バイオメトリックデータを送信するための手段と
を備える、装置。
【請求項２９】
バイオメトリックデータを前記受信するための手段は、バイオメトリックセンサを含み、非バイオメトリックデータを前記受信するための手段は、ユーザ入力デバイスを含み、

前記生成するための手段は、プロセッサを含み、前記送信するための手段は、ネットワークインターフェースを含む、
請求項２８に記載の装置。
【請求項３０】
バイオメトリックデータを前記受信するための手段、非バイオメトリックデータを前記受信するための手段、合成バイオメトリックデータを前記生成するための手段、および前記送信するための手段は、通信デバイス、携帯情報端末（ＰＤＡ）、タブレット、コンピュータ、音楽プレーヤー、ビデオプレーヤー、エンターテインメントユニット、ナビゲーションデバイス、またはセットトップボックスに統合される、
請求項２８に記載の装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０３１０
【補正方法】変更
【補正の内容】
【０３１０】
[00318]開示される実施形態の上の説明は、開示される実施形態を当業者が作成または使用することを可能にするために与えられる。これらの実施形態に対する様々な修正は、当業者には容易に明らかになり、本明細書において規定される原理は、本開示の範囲から逸脱することなく、他の実施形態に適用され得る。したがって、本開示は、本明細書において示される実施形態に限定されることは意図されず、特許請求の範囲によって規定される原理および新規の特徴と合致する、可能な限り最も広い範囲が与えられるべきである。
以下に本願の出願当初の特許請求の範囲に記載された発明を付記する。
［Ｃ１］
ユーザからバイオメトリックデータを受信するように構成されたセンサと、
前記ユーザから非バイオメトリックデータを受信するように構成された入力インターフェースと、
合成バイオメトリックデータを生成するように構成されたプロセッサ、ここにおいて、前記合成バイオメトリックデータは、前記非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
ネットワークを介して、前記ユーザを認証するために、認証サーバに前記合成バイオメトリックデータを送信するように構成されたネットワークインターフェースと
を備える、装置。
［Ｃ２］
前記センサは、指紋スキャナを備え、前記バイオメトリックデータは、前記ユーザの指紋を備える、
Ｃ１に記載の装置。
［Ｃ３］
前記センサは、虹彩スキャナを備え、前記バイオメトリックデータは、前記ユーザの虹彩スキャンを備える、
Ｃ１に記載の装置。
［Ｃ４］
前記センサは、マイクロフォンを備え、前記バイオメトリックデータは、前記ユーザの発話信号を備える、
Ｃ１に記載の装置。
［Ｃ５］
前記センサは、カメラを備え、前記バイオメトリックデータは、前記ユーザの顔画像を備える、
Ｃ１に記載の装置。
［Ｃ６］

前記非バイオメトリックデータは、英数字鍵を備える、
Ｃ１に記載の装置。
［Ｃ７］
前記合成バイオメトリックデータは、合成指紋、合成虹彩スキャン、合成発話信号、合成画像、またはこれらの任意の組み合わせを備える、
Ｃ１に記載の装置。
［Ｃ８］
前記ネットワークインターフェースは、前記認証サーバが前記合成バイオメトリックデータに基づいて前記ユーザを認証するとき、前記ネットワークを介して別の電子デバイスと認証されたセッションを行うようにさらに構成される、
Ｃ１に記載の装置。
［Ｃ９］
前記バイオメトリックデータは、前記合成バイオメトリックデータから非復元可能である、
Ｃ１に記載の装置。
［Ｃ１０］
前記バイオメトリックデータは、第１の領域内にあり、前記非バイオメトリックデータは、前記第１の領域と異なる第２の領域内にある、
Ｃ１に記載の装置。
［Ｃ１１］
前記第１の領域は、オーディオ領域または画像領域のうちの１つに対応し、前記第２の領域は、前記オーディオ領域または前記画像領域のうちのもう一方に対応する、
Ｃ１０に記載の装置。
［Ｃ１２］
前記ネットワークインターフェースは、基本電話サービス（ＰＯＴＳ）インターフェースに対応し、前記合成バイオメトリックデータは、ＰＯＴＳ互換オーディオ信号として送信される、
Ｃ１に記載の装置。
［Ｃ１３］
デバイスにおいて、ユーザからバイオメトリックデータを受信することと、
前記デバイスにおいて、前記ユーザから第１の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第１の合成バイオメトリックデータを生成すること、ここにおいて、前記第１の合成バイオメトリックデータは、前記デバイスにおいて、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
ネットワークを介して前記デバイスから第１の認証サーバに、前記ユーザを認証するために前記第１の合成バイオメトリックデータを送信することと
を備える、方法。
［Ｃ１４］
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータは、前記第２の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
前記ユーザを認証するために、前記デバイスから第２の認証サーバに、前記第２の合成バイオメトリックデータを送信することと
をさらに備える、Ｃ１３に記載の方法。
［Ｃ１５］
前記第１の認証サーバは、前記ユーザに対応する認証データとして前記第１の合成バイ

オメトリックデータを記憶するように構成され、前記認証データと受信した合成バイオメトリックデータを比較することによって前記ユーザを認証するように構成される、
Ｃ１３に記載の方法。
［Ｃ１６］
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータを生成することは、前記第２の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
前記デバイスから前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信すること、ここにおいて、前記第２の合成バイオメトリックデータは、前記ユーザに対応する前記認証データとして前記第１の合成バイオメトリックデータを置き換える、と
をさらに備える、Ｃ１５に記載の方法。
［Ｃ１７］
プロセッサによって実行されると、前記プロセッサに、
ユーザからバイオメトリックデータを受信することと、
前記ユーザから第１の非バイオメトリックデータを受信することと、
第１の合成バイオメトリックデータを生成すること、ここにおいて、前記第１の合成バイオメトリックデータを生成することは、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することを含む、と、
ネットワークを介して、前記ユーザを認証するために、第１の認証サーバに前記第１の合成バイオメトリックデータを送信することと
を備える、動作を実行させる命令を記憶した、コンピュータ可読記憶デバイス。
［Ｃ１８］
前記動作は、
前記バイオメトリックデータの特徴を抽出することと、
メモリに前記特徴を記憶することと
をさらに備え、前記第１の合成バイオメトリックデータは、前記第１の非バイオメトリックデータに基づいて前記特徴を修正することによって生成される、
Ｃ１７に記載のコンピュータ可読記憶デバイス。
［Ｃ１９］
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記第２の非バイオメトリックデータに基づいて前記特徴を修正することによって第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
を備え、前記第２の合成バイオメトリックデータは、前記ユーザに対応する認証データとして、前記第１の認証サーバにおいて、前記第１の合成バイオメトリックデータを置き換える、
Ｃ１８に記載のコンピュータ可読記憶デバイス。
［Ｃ２０］
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れになったと決定することに応答して、第２のバイオメトリックデータを提供するように前記ユーザに促すことと、
前記ユーザから前記第２のバイオメトリックデータを受信することと、前記第２のバイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備える、Ｃ１７に記載のコンピュータ可読記憶デバイス。

［Ｃ２１］
前記動作は、前記バイオメトリックデータが第１のタイムスタンプに基づいて期限切れになったことかどうかを決定することをさらに備え、前記第１のタイムスタンプは、前記バイオメトリックデータが前記ユーザから受信される第１の時間、または前記バイオメトリックデータがメモリに記憶される第２の時間を示す、
Ｃ２０に記載のコンピュータ可読記憶デバイス。
［Ｃ２２］
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れでないと決定することに応答して、前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
を備える、Ｃ１７に記載のコンピュータ可読記憶デバイス。
［Ｃ２３］
前記第１の非バイオメトリックデータは、第１の電子デバイスと関連付けられ、前記第１の合成バイオメトリックデータは、前記ユーザおよび前記第１の電子デバイスと関連付けられる第１の認証データに対応する、
Ｃ１７に記載のコンピュータ可読記憶デバイス。
［Ｃ２４］
前記動作は、
前記ユーザから第２の電子デバイスに関連付けられた第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記第１の認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備え、前記第２の合成バイオメトリックデータは、前記ユーザおよび前記第２の電子デバイスと関連付けられた第２の認証データに対応する、
Ｃ２３に記載のコンピュータ可読記憶デバイス。
［Ｃ２５］
前記第１の認証サーバは、建物のセキュリティシステム、または前記建物の温度制御器と関連付けられる、
Ｃ１７に記載のコンピュータ可読記憶デバイス。
［Ｃ２６］
前記第１の合成バイオメトリックデータは、前記第１の非バイオメトリックデータに基づいて前記バイオメトリックデータに一方向性関数を適用することによって生成される、
Ｃ１７に記載のコンピュータ可読記憶デバイス。
［Ｃ２７］
前記一方向性関数は、ハッシュ関数、指数関数、剰余関数、双曲線正接関数、または別の双曲線関数のうちの少なくとも１つを含む、
Ｃ２６に記載のコンピュータ可読記憶デバイス。
［Ｃ２８］
ユーザからバイオメトリックデータを受信するための手段と、
前記ユーザから非バイオメトリックデータを受信するための手段と、
前記非バイオメトリックデータに基づいて前記バイオメトリックデータを変換することによって合成バイオメトリックデータを生成するための手段と、
ネットワークを介して、前記ユーザを認証するために認証サーバに前記合成バイオメトリックデータを送信するための手段と
を備える、装置。
［Ｃ２９］

前記バイオメトリックデータを受信するための手段は、バイオメトリックセンサを含み、非バイオメトリックデータを前記受信するための手段は、ユーザ入力デバイスを含み、前記生成するための手段は、プロセッサを含み、前記送信するための手段は、ネットワークインターフェースを含む、
Ｃ２８に記載の装置。
［Ｃ３０］
バイオメトリックデータを前記受信するための手段、非バイオメトリックデータを前記受信するための手段、合成バイオメトリックデータを前記生成するための手段、および合成バイオメトリックデータを前記送信するための手段は、通信デバイス、携帯情報端末（ＰＤＡ）、タブレット、コンピュータ、音楽プレーヤー、ビデオプレーヤー、エンターテインメントユニット、ナビゲーションデバイス、またはセットトップボックスのうちの少なくとも１つに組み込まれる、
Ｃ２９に記載の装置。
【手続補正書】
【提出日】平成29年4月25日(2017.4.25)
【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】
ユーザからバイオメトリックデータを受信するように構成されたセンサと、
前記ユーザから非バイオメトリックデータを受信するように構成された入力インターフェースと、
合成バイオメトリックデータを生成するために、前記バイオメトリックデータに対しておよび前記非バイオメトリックデータに対して動作を実行することと、
オーディオ認証データを生成するために、前記合成バイオメトリックデータを可聴化することと
を行うように構成されたプロセッサと、
ネットワークを介して、認証サーバに前記オーディオ認証データを送信するように構成されたネットワークインターフェースと
を備える、装置。
【請求項２】
前記合成バイオメトリックデータの可聴化は、前記合成バイオメトリックデータの特徴に対応するデータの抽出と、前記特徴に対応する前記データに基づいたペクトルエンベロープの生成とを備え、前記合成バイオメトリックデータの生成の前に、前記センサから受信された前記バイオメトリックデータを記憶するように構成されたメモリをさらに備える、
請求項１に記載の装置。
【請求項３】
前記合成バイオメトリックデータは、修正された指紋に対応し、前記特徴は、前記修正された指紋のスパイクに対応する、
請求項２に記載の装置。
【請求項４】
前記動作は、前記バイオメトリックデータに適用された、および前記非バイオメトリックデータに適用された一方向性関数を備え、前記スパイクは、前記修正された指紋の特異点に対応し、前記プロセッサは、第２のタイムスタンプと第１のタイムスタンプとの差が閾値を超えるかどうかに基づいて、前記バイオメトリックデータが期限切れになったかどうかを決定するように構成され、前記第２のタイムスタンプは、前記タイムスタンプと関

連付けられる第１の時間の後に続く第２の時間と関連付けられる、
請求項３に記載の装置。
【請求項５】
前記閾値は、メモリに記憶され、前記バイオメトリックデータのタイプと関連付けられ、前記タイプは、前記バイオメトリックデータと関連付けられる生物学的特徴に対応する、
請求項４に記載の装置。
【請求項６】
前記センサは、マイクロフォン、指紋スキャナ、虹彩スキャナ、またはカメラを備え、前記バイオメトリックデータは、前記ユーザの発話信号、前記ユーザの指紋、前記ユーザの虹彩スキャナ、または前記ユーザの顔画像を備える、
請求項１に記載の装置。
【請求項７】
前記非バイオメトリックデータは、英数字鍵を備え、前記合成バイオメトリックデータは、合成指紋、合成虹彩スキャン、合成発話信号、合成画像、またはこれらの任意の組み合わせを備える、
請求項１に記載の装置。
【請求項８】
前記ネットワークインターフェースは、前記合成バイオメトリックデータに基づいて前記ユーザを認証する前記認証サーバに応答して、前記ネットワークを介して別の電子デバイスと認証されたセッションを行うようにさらに構成される、
請求項１に記載の装置。
【請求項９】
前記バイオメトリックデータは、前記合成バイオメトリックデータから非復元可能である、
請求項１に記載の装置。
【請求項１０】
前記バイオメトリックデータは、オーディオ領域または画像領域のうちの１つに対応する第１の領域内にあり、前記非バイオメトリックデータは、前記オーディオ領域または前記画像領域のうちのもう一方に対応する第２の領域内にある、
請求項１に記載の装置。
【請求項１１】
前記ネットワークインターフェースは、前記ユーザを認証するための前記認証サーバに前記合成バイオメトリックデータを送信するように構成される、
請求項１に記載の装置。
【請求項１２】
前記プロセッサは、
前記非バイオメトリックデータを音符シーケンスに変換することと、
前記バイオメトリックデータの特徴に対応するデータを抽出することと、
前記特徴に対応する前記データをスペクトルエンベロープに変換することと、
オーディオデータを生成するために、前記音符シーケンスと前記スペクトルエンベロープとを組み合わせることと、
前記オーディオデータを前記ネットワークインターフェースに提供することと
を行うようにさらに構成される、請求項１に記載の装置。
【請求項１３】
デバイスにおいて、ユーザからバイオメトリックデータを受信することと、
前記デバイスにおいて、前記ユーザから非バイオメトリックデータを受信することと、
合成バイオメトリックデータを生成するために、前記バイオメトリックデータに対しておよび前記非バイオメトリックデータに対して動作を実行することと、
オーディオ認証データを生成するために、前記合成バイオメトリックデータを可聴化す

ることと
ネットワークを介して前記デバイスから認証サーバに、前記オーディオ認証データを送信することと
を備える、方法。
【請求項１４】
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータを生成することは、第２の合成バイオメトリックデータを生成するために、前記バイオメトリックデータに対しておよび前記第２の非バイオメトリックデータに対して動作を実行することを含む、と、
前記ユーザを認証するために、前記デバイスから第２の認証サーバに、前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１３に記載の方法。
【請求項１５】
前記第２の合成バイオメトリックデータを可聴化することをさらに備える、
請求項１４に記載の方法。
【請求項１６】
前記デバイスにおいて、前記ユーザから第２の非バイオメトリックデータを受信することと、
前記デバイスにおいて、第２の合成バイオメトリックデータを生成すること、ここにおいて、前記第２の合成バイオメトリックデータを生成することは、第２の合成バイオメトリックデータを生成するために、前記バイオメトリックデータに対しておよび前記第２の非バイオメトリックデータに対して第２の動作を実行することを含む、と、
第２のオーディオ認証データを生成するために、前記第２の合成バイオメトリックデータを可聴化することと、
前記デバイスから前記認証サーバに前記第２のオーディオ認証データを送信すること、ここにおいて、前記第２のオーディオ認証データは、前記ユーザに対応する認証データとして前記オーディオ認証データを置き換える、と
をさらに備える、請求項１５に記載の方法。
【請求項１７】
プロセッサによって実行されると、前記プロセッサに、
ユーザからバイオメトリックデータを受信することと、
前記ユーザから非バイオメトリックデータを受信することと、
合成バイオメトリックデータを生成するために、前記バイオメトリックデータに対しておよび前記非バイオメトリックデータに対して動作を実行することと、
オーディオ認証データを生成するために、前記合成バイオメトリックデータを可聴化することと、
ネットワークを介して、認証サーバに前記オーディオ認証データを送信することと
を備える、動作を実行させる命令を記憶した、コンピュータ可読記憶デバイス。
【請求項１８】
前記動作は、
前記バイオメトリックデータの特徴に対応するデータを抽出することと、
メモリに前記特徴に対応する前記データを記憶することと
をさらに備える、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項１９】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
第２の合成バイオメトリックデータを生成するために、前記バイオメトリックデータに

対しておよび前記第２の非バイオメトリックデータに対して動作を実行することによって第２の合成バイオメトリックデータを生成することと、
第２のオーディオ認証データを生成するために、前記第２の合成バイオメトリックデータを可聴化することと、
前記認証サーバに前記第２のオーディオ認証データを送信することと
をさらに備え、前記第２のオーディオ認証データは、前記ユーザに対応する認証データとして、前記認証サーバにおいて、前記オーディオ認証データを置き換える、
請求項１８に記載のコンピュータ可読記憶デバイス。
【請求項２０】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れになったと決定することに応答して、第２のバイオメトリックデータを提供するように前記ユーザに促すことと、
前記ユーザから前記第２のバイオメトリックデータを受信することと、
前記第２のバイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２１】
前記動作は、前記バイオメトリックデータが、前記バイオメトリックデータの生成に関連付けられる第１のタイムスタンプと、第２のタイムスタンプとの差に基づいて期限切れになったかどうかを決定することをさらに備え、前記第２のタイムスタンプは、クロックの時間に基づく、
請求項２０に記載のコンピュータ可読記憶デバイス。
【請求項２２】
前記動作は、
前記ユーザから第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータが期限切れでないと決定することに応答して、前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備える、請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２３】
前記非バイオメトリックデータは、電子デバイスと関連付けられ、前記合成バイオメトリックデータは、前記ユーザおよび前記電子デバイスと関連付けられる認証データに対応する、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２４】
前記動作は、
前記ユーザから第２の電子デバイスに関連付けられた第２の非バイオメトリックデータを受信することと、
前記バイオメトリックデータおよび前記第２の非バイオメトリックデータに基づいて第２の合成バイオメトリックデータを生成することと、
前記認証サーバに前記第２の合成バイオメトリックデータを送信することと
をさらに備え、前記第２の合成バイオメトリックデータは、前記ユーザおよび前記第２の電子デバイスと関連付けられた第２の認証データに対応する、
請求項２３に記載のコンピュータ可読記憶デバイス。
【請求項２５】
前記動作は、閾値と前記差を比較することをさらに備え、前記閾値は、前記バイオメトリックデータが期限切れになったかどうかを示す、

請求項２１に記載のコンピュータ可読記憶デバイス。
【請求項２６】
前記動作は、複数の一方向性関数から選択された一方向性関数を備え、前記一方向性関数は、ユーザによって選択される、
請求項１７に記載のコンピュータ可読記憶デバイス。
【請求項２７】
前記一方向性関数は、双曲線正接関数を含む、
請求項２６に記載のコンピュータ可読記憶デバイス。
【請求項２８】
ユーザからバイオメトリックデータを受信するための手段と、
前記ユーザから非バイオメトリックデータを受信するための手段と、
合成バイオメトリックデータを生成するために、前記バイオメトリックデータに対しておよび前記非バイオメトリックデータに対して動作を実行するための手段、およびオーディオ認証データを生成するために、前記合成バイオメトリックデータを可聴化するための手段と、
ネットワークを介して、認証サーバに前記オーディオ認証データを送信するための手段と
を備える、装置。
【請求項２９】
バイオメトリックデータを前記受信するための手段は、バイオメトリックセンサを含み、非バイオメトリックデータを前記受信するための手段は、ユーザ入力デバイスを含み、前記動作を前記実行するための手段、および可聴化するための手段は、プロセッサを含み、前記送信するための手段は、ネットワークインターフェースを含む、
請求項２８に記載の装置。
【請求項３０】
バイオメトリックデータを前記受信するための手段、非バイオメトリックデータを前記受信するための手段、前記動作を前記実行するための手段、および可聴化するための手段、並びに前記送信するための手段は、通信デバイス、携帯情報端末（ＰＤＡ）、タブレット、コンピュータ、音楽プレーヤー、ビデオプレーヤー、エンターテインメントユニット、ナビゲーションデバイス、またはセットトップボックスに統合される、
請求項２８に記載の装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/043539

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06Q20/40 H04L9/32
ADD. G06K9/00

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)
G06F G06Q H04L G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TEOH ET AL: "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE COMPUTER SOCIETY, USA, vol. 27, no. 12, 1 December 2006 (2006-12-01), pages 1892-1901, XP011149692, ISSN: 0162-8828, DOI: 10.1109/TPAMI.2006.250 page 1893, left-hand column, line 4 - page 1894, left-hand column, line 46 page 1897, left-hand column, line 1 - page 1899, right-hand column, line 35 page 1900, left-hand column, line 29 - page 1901, left-hand column, line 10 ----- -/--	1-30

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* 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
8 January 2016	22/01/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Sauzon, Guillaume

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/043539

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/044917 A2 (CORPORATE THE REGENTS OF THE U [US]; BOULT TERRANCE EDWARD) 27 April 2006 (2006-04-27) paragraph [0029] - paragraph [0050] paragraph [0059] - paragraph [0059] paragraph [0069] - paragraph [0075] paragraph [0081] - paragraph [0086] figures 2,4, 8, 9	1-30
A	AJITA RATTANI ET AL: "Template Update Methods in Adaptive Biometric Systems: A Critical Review", 2 June 2009 (2009-06-02), ADVANCES IN BIOMETRICS, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 847 - 856, XP019118000, ISBN: 978-3-642-01792-6 page 847, line 17 - page 848, line 19 page 849, line 20 - page 853, line 6 page 855, line 16 - page 855, line 37	1-30

2

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/043539

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006044917 A2	27-04-2006	AU 2005295331 A1	27-04-2006
		CA 2584121 A1	27-04-2006
		EP 1805693 A2	11-07-2007
		US 2009022374 A1	22-01-2009
		WO 2006044917 A2	27-04-2006

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,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,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,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,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 キム、レーホン
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ナム、ジュハン
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ビッサー、エリック
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5J104 AA07 KA01 KA05 KA17 KA18 KA19 NA02 NA05 NA11 NA12
NA37 PA02