(19)日本国特許庁(JP)　(12)登録実用新案公報(U)　(11)実用新案登録番号
実用新案登録第3230238号
(U3230238)
(45)発行日　令和3年1月14日(2021.1.14)　(24)登録日　令和2年12月18日(2020.12.18)

(51)Int.Cl.　　F I
G06F 21/60 (2013.01)　G06F 21/60
G06F 21/32 (2013.01)　G06F 21/32
G06F 21/64 (2013.01)　G06F 21/64

評価書の請求 未請求　請求項の数 30　ＯＬ　（全 40 頁）

(21)出願番号　実願2018-600052 (U2018-600052)
(86)(22)出願日　平成30年4月10日(2018.4.10)
(86)国際出願番号　PCT/US2018/026956
(87)国際公開番号　WO2019/199288
(87)国際公開日　令和1年10月17日(2019.10.17)

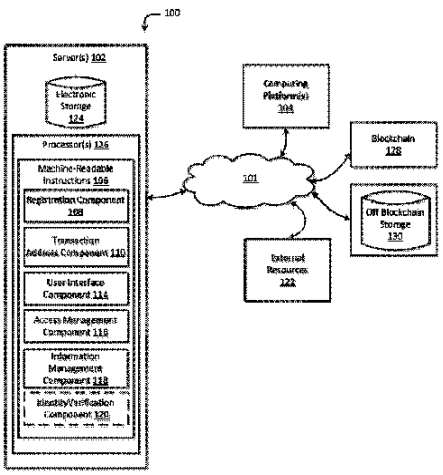
(73)実用新案権者　518130314
ブラック　ゴールド　コイン　インコーポレイテッド
ＢＬＡＣＫ　ＧＯＬＤ　ＣＯＩＮ，　ＩＮＣ．
アメリカ合衆国　８９１３０　ネバダ州　ラスベガス　アズールドライブ　７４９５　スイート　１００
７４９５　Ａｚｕｒｅ　Ｄｒｉｖｅ，　Ｓｕｉｔｅ　１００，　Ｌａｓ　Ｖｅｇａｓ，　Ｎｅｖａｄａ　８９１３０　Ｕ．Ｓ．Ａ．

最終頁に続く

(54)【考案の名称】電子データを安全に格納するシステム

(57)【要約】　（修正有）
【課題】電子データをより安全に格納する高度なシステムを提供する。
【解決手段】システムは、電子情報のファイルを受信し、安全に格納し、ファイルを受信すると、ファイルの少なくとも第１のフラグメントと第２のフラグメントとを含むフラグメントを形成するハードウェアプロセッサ１２６と、第１の非一時的記憶装置に情報のブロックを格納する複数のノードを有する分散型データストレージシステムと、分散型データストレージシステムの外部にある第２の非一時的記憶装置と、を有し、プロセッサは、第１のフラグメントを分散型データストレージシステムに格納し、第２のフラグメントを第２の非一時的記憶装置に格納する。格納されるファイルは、生体特徴又は部分生体特徴ファイルで、暗号化又はハッシュ化されてもよい。ファイルフラグメントは、暗号化され、完全に再構築されるまで、意味を成さないことが好ましい。
【選択図】図１

FIG. 1



【実用新案登録請求の範囲】
【請求項１】
電子データを安全に格納するシステムであって、
ユーザに関連付けられた意味を成す電子情報のファイルを受信し、安全に格納し、前記電子情報のファイルを受信すると、前記電子情報のファイルの少なくとも第１のフラグメント（＃１）と第２のフラグメント（＃２）とを含むフラグメント（２３２、３１４、４４２）を形成するように構成されたハードウェアプロセッサ（１２６）と、
第１の非一時的記憶装置に情報のブロックを格納する複数のノードを有する分散型データストレージシステム（２３４Ａ、３１６Ａ、４４４Ａ）と、
前記分散型データストレージシステムの外部にある第２の非一時的記憶装置（２３４Ｂ、３１６Ｂ、４４４Ｂ）と、を有し、
前記プロセッサは更に、前記ファイルの少なくとも前記第１のフラグメント（＃１）を前記分散型データストレージシステム（２３４Ａ、３１６Ａ、４４４Ａ）に格納し、前記ファイルの少なくとも前記第２のフラグメント（＃２）を前記分散型データストレージシステム（２３４Ｂ、３１６Ｂ、４４４Ｂ）の外部に格納するように構成される、システム。
【請求項２】
前記プロセッサは、前記ファイルの少なくとも前記第１のフラグメント及び少なくとも前記第２のフラグメントに対して、前記ファイルの少なくとも前記第１のフラグメント及び少なくとも前記第２のフラグメントの再構築用データを含む、位置データを格納するマッピングファイルを生成し、前記マッピングファイル又は前記マッピングファイルの少なくとも一部を、分散型台帳ストレージに格納するように構成される、請求項１に記載のシステム。
【請求項３】
前記ファイルの前記フラグメントはそれぞれ、前記ファイルに部分的又は完全に再構築されるまで、意味を成さない、請求項１に記載のシステム。
【請求項４】
前記プロセッサは、前記電子情報として、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含むデジタル生体特徴ファイルを受信するように構成される、請求項１に記載のシステム。
【請求項５】
前記プロセッサは、前記ファイルとして、前記ユーザに関連付けられたデジタルファイルを受信するように構成される、請求項１に記載のシステム。
【請求項６】
前記分散型データストレージシステムは、改竄不能データの格納のための信頼ユーティリティである、請求項１に記載のシステム。
【請求項７】
前記プロセッサは、前記電子情報として、前記ユーザに関連付けられたグラフィック又は画像ファイルを受信し、前記グラフィック又は画像を特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するように構成される、請求項１に記載のシステム。
【請求項８】
前記プロセッサは、前記特徴ブロックの内の少なくとも前記第１及び第２ブロックを格納する前に、前記特徴ブロックの内の少なくとも前記第１及び第２ブロックを変換し、変換結果を前記マッピングファイルに格納するように構成される、請求項７に記載のシステム。
【請求項９】

前記プロセッサは、前記マッピングファイルを、少なくとも第１のマッピングファイルフラグメンと第２のマッピングファイルフラグメントとに分割し、少なくとも前記第１のマッピングファイルフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記第２のマッピングファイルフラグメントを前記分散型データストレージシステムの外部に格納するように構成される、請求項８に記載のシステム。

【請求項１０】

前記プロセッサは、前記特徴ブロックの内の少なくとも前記第１ブロックと、前記特徴ブロックの内の少なくとも前記第２ブロックとを暗号化するように構成される、請求項８に記載のシステム。

【請求項１１】

前記プロセッサは、前記特徴ブロックの内の少なくとも前記第１ブロックと、前記特徴ブロックの内の少なくとも前記第２ブロックとを暗号化するように構成される、請求項９に記載のシステム。

【請求項１２】

前記プロセッサは、少なくとも前記マッピングファイルを暗号化するように構成される、請求項８に記載のシステム。

【請求項１３】

前記特徴ブロックの組は、前記グラフィック又は画像を形成する前記特徴ブロックのサブセットである、請求項８に記載のシステム。

【請求項１４】

前記グラフィック又は画像ファイルは、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含むファイルである、請求項８に記載のシステム。

【請求項１５】

前記プロセッサは、前記特徴ブロックの前記サブセットを暗号化し、前記暗号化された特徴ブロックのサブセットを少なくとも第１のフラグメント及び第２フラグメントに分解し、少なくとも前記第１のフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記第２のフラグメントを前記分散型データストレージシステムの外部に格納するように構成される、請求項１３に記載のシステム。

【請求項１６】

前記プロセッサは、前記生体特徴グラフィックの前記サブセットのハッシュを生成し、前記ハッシュの少なくとも一部を前記分散型データストレージシステムに格納し、前記ハッシュの少なくとも他部を前記分散型データストレージシステムの外部に格納するように構成される、請求項１３に記載のシステム。

【請求項１７】

前記プロセッサは、前記ユーザに関連付けられた、前記システムに格納された情報へアクセスするためのユーザリクエストに応じて、アクセスを許可する前に前記ユーザを認証するように構成され、当該認証は、前記ユーザから前記システムが新たに受信した生体特徴グラフィックファイルのハッシュの少なくとも一部を、前記分散型データストレージシステム内の少なくとも前記第１のフラグメントと、前記分散型データストレージシステム外の少なくとも前記第２のフラグメントとから得られたハッシュと比較することを含み、前記ユーザが認証される条件の少なくとも一部として、一致することが求められ、前記プロセッサは、前記ユーザに関連付けられた、前記システムに格納された情報へアクセスするためのユーザリクエストに応じて、アクセスを許可する前に前記ユーザを認証するように構成され、当該認証は、前記生体特徴グラフィックの前記特徴ブロックの前記サブセットを、前記ユーザから前記システムが新たに受信した生体特徴ファイルの、対応する特徴ブロックのサブセットと比較することを含み、前記ユーザが認証される条件の少なくとも一部として、一致することが求められる、請求項１５に記載のシステム。

【請求項１８】

前記特徴ブロックの前記サブセットは、前記生体特徴グラフィックの連続的なブロック又は非連続的なブロックをグループ化したものである、請求項１３に記載のシステム。

【請求項１９】
前記特徴ブロックの前記サブセット内の特徴ブロックは、格納される前に変換される、請求項１３に記載のシステム。
【請求項２０】
前記プロセッサは、前記ユーザに関連付けられた第２グラフィック又は画像ファイルを格納し、前記第２グラフィック又は画像ファイル内のグラフィック又は画像を、特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するように構成される、請求項７に記載のシステム。
【請求項２１】
前記プロセッサは、前記ユーザに関連付けられた第２グラフィック又は画像ファイルを格納し、前記第２グラフィック又は画像ファイル内のグラフィック又は画像を、特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するように構成される、請求項１７に記載のシステム。
【請求項２２】
前記プロセッサは、機械可読命令により、更に前記フラグメントが、どのように前記ファイルに再構築されるかを示すインデックスファイルを形成するように構成される、請求項１に記載のシステム。
【請求項２３】
前記プロセッサは更に、少なくとも第１のフラグメントと対応する第２のフラグメントとを含む、前記インデックスファイルのフラグメントを生成し、
前記インデックスファイルの少なくとも前記第１のフラグメントを分散型データストレージシステムに格納し、
前記インデックスファイルの少なくとも前記第２のフラグメントを前記分散型データストレージシステムの外部に格納するように構成される、請求項２２に記載のシステム。
【請求項２４】
前記プロセッサは更に、前記ファイルの少なくとも第３のフラグメントを生成し、前記第３のフラグメントを、前記分散型データストレージシステムに格納された前記第１のフラグメントとは別に、前記分散型データストレージシステムに格納するように構成される、請求項１に記載のシステム。
【請求項２５】
前記プロセッサは更に、少なくとも前記第１のフラグメントを、トランザクションとして前記分散型データストレージシステムに格納するように構成される、請求項１に記載のシステム。
【請求項２６】
前記プロセッサは更に、少なくとも前記第１のフラグメントと前記第３のフラグメントを、異なるトランザクションとして前記分散型データストレージシステムに格納するように構成される、請求項２４に記載のシステム。
【請求項２７】
前記プロセッサは、前記機械可読命令により更に、前記ユーザからのリクエストに応じて、前記ファイルフラグメントを、前記ファイルに再構築するように構成される、請求項１に記載のシステム。
【請求項２８】
前記プロセッサは、前記機械可読命令により更に、前記ファイルのヘッダの少なくとも一部を含む前記第１ファイルフラグメントを生成するように構成される、請求項１に記載

のシステム。
【請求項２９】
前記分散型データストレージの外部のストレージは、自身のＣＰＵを持たないデジタルストレージ装置である、請求項１に記載のシステム。
【請求項３０】
前記分散型データストレージは、分散型台帳ストレージである、請求項１に記載のシステム。
【請求項３１】
電子データを安全に格納する方法であって、
プロセッサにより、ユーザに関連付けられた意味を成す電子情報のファイルを格納するリクエストを受信することと、
前記電子情報のファイルを受信すると、前記電子情報のファイルの少なくとも第１のフラグメントと対応する第２フラグメントを含むフラグメントを形成することと、
第１の非一時的記憶装置に情報のブロックを格納する複数のノードを有する分散型データストレージシステムを設けることと、
前記分散型データストレージシステムの外部に第２の非一時的記憶装置を設けることと、
前記プロセッサにより、少なくとも前記ファイルの前記第１のフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記ファイルの前記第２のフラグメントを前記分散型データストレージシステムの外部に格納することと、を含む方法。
【請求項３２】
前記プロセッサは、前記ファイルの少なくとも前記第１のフラグメント及び少なくとも前記第２のフラグメントに対して、前記ファイルの少なくとも前記第１のフラグメント及び少なくとも前記第２のフラグメントの再構築用データを含む、位置データを格納するマッピングファイルを生成し、前記マッピングファイル又は前記マッピングファイルの少なくとも一部を、分散型台帳ストレージに格納するように構成される、請求項３１に記載の方法。
【請求項３３】
前記ファイルの前記フラグメントはそれぞれ、前記ファイルに部分的又は完全に再構築されるまで、意味を成さない、請求項３１に記載の方法。
【請求項３４】
前記受信するステップにおいて、前記プロセッサは、前記電子情報として、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含むデジタル生体特徴ファイルを受信する、請求項３１に記載の方法。
【請求項３５】
前記受信するステップにおいて、前記プロセッサは、前記ファイルとして、前記ユーザに関連付けられたデジタルファイルを受信する、請求項３１に記載の方法。
【請求項３６】
前記分散型データストレージシステムは、改竄不能データの格納のための信頼ユーティリティである、請求項３１に記載の方法。
【請求項３７】
前記受信するステップにおいて、前記プロセッサは、前記電子情報として、前記ユーザに関連付けられたグラフィック又は画像ファイルを受信し、前記グラフィック又は画像を特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納する、請求項３１に記載の方法。
【請求項３８】
前記プロセッサが、前記特徴ブロックの内の少なくとも前記第１及び第２ブロックを格

納する前に、前記特徴ブロックの内の少なくとも前記第１及び第２ブロックを変換し、変換結果を前記マッピングファイルに格納するステップを更に含む、請求項３７に記載の方法。

【請求項３９】

前記マッピングファイルを、少なくとも第１のマッピングファイルフラグメンと第２のマッピングファイルフラグメントとに分割し、少なくとも前記第１のマッピングファイルフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記第２のマッピングファイルフラグメントを前記分散型データストレージシステムの外部に格納するステップを更に含む、請求項３８に記載の方法。

【請求項４０】

前記特徴ブロックの内の少なくとも前記第１ブロックと、前記特徴ブロックの内の少なくとも前記第２ブロックとを暗号化するステップを更に含む、請求項３８に記載の方法。

【請求項４１】

前記特徴ブロックの内の少なくとも前記第１ブロックと、前記特徴ブロックの内の少なくとも前記第２ブロックとを暗号化するステップを更に含む、請求項３９に記載の方法。

【請求項４２】

少なくとも前記マッピングファイルを暗号化するステップを更に含む、請求項３８に記載の方法。

【請求項４３】

前記特徴ブロックの組は、前記グラフィック又は画像を形成する前記特徴ブロックのサブセットである、請求項３８に記載の方法。

【請求項４４】

前記グラフィック又は画像ファイルは、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含むファイルである、請求項３８に記載の方法。

【請求項４５】

前記特徴ブロックの前記サブセットを暗号化し、前記暗号化された特徴ブロックのサブセットを少なくとも第１のフラグメント及び第２フラグメントに分解し、少なくとも前記第１のフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記第２のフラグメントを前記分散型データストレージシステムの外部に格納するステップを更に含む、請求項４３に記載の方法。

【請求項４６】

前記生体特徴グラフィックの前記サブセットのハッシュを生成し、前記ハッシュの少なくとも一部を前記分散型データストレージシステムに格納し、前記ハッシュの少なくとも他部を前記分散型データストレージシステムの外部に格納するステップを更に含む、請求項４３に記載の方法。

【請求項４７】

前記ユーザに関連付けられた、前記システムに格納された情報へアクセスするためのユーザリクエストに応じて、アクセスを許可する前に前記ユーザを認証し、当該認証は、前記ユーザから前記システムが新たに受信した生体特徴グラフィックファイルのハッシュの少なくとも一部を、前記分散型データストレージシステム内の少なくとも前記第１のフラグメントと、前記分散型データストレージシステム外の少なくとも前記第２のフラグメントとから得られたハッシュと比較することを含み、前記ユーザが認証される条件の少なくとも一部として、一致することが求められ、前記ユーザに関連付けられた、前記システムに格納された情報へアクセスするためのユーザリクエストに応じて、アクセスを許可する前に前記ユーザを認証し、当該認証は、前記生体特徴グラフィックの前記特徴ブロックの前記サブセットを、前記ユーザから前記システムが新たに受信した生体特徴ファイルの、対応する特徴ブロックのサブセットと比較することを含み、前記ユーザが認証される条件の少なくとも一部として、一致することが求められるステップを更に含む、請求項４５に記載の方法。

【請求項４８】

前記特徴ブロックの前記サブセットは、前記生体特徴グラフィックの連続的なブロック又は非連続的なブロックをグループ化したものである、請求項４３に記載の方法。

【請求項４９】

前記特徴ブロックの前記サブセット内の特徴ブロックを、格納する前に変換するステップを更に含む、請求項４３に記載の方法。

【請求項５０】

前記プロセッサが、前記ユーザに関連付けられた第２グラフィック又は画像ファイルを格納し、前記第２グラフィック又は画像ファイル内のグラフィック又は画像を、特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するステップを更に含む、請求項３７に記載の方法。

【請求項５１】

前記プロセッサが、前記ユーザに関連付けられた第２グラフィック又は画像ファイルを格納し、前記第２グラフィック又は画像ファイル内のグラフィック又は画像を、特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するステップを更に含む、請求項４７に記載の方法。

【請求項５２】

前記プロセッサが、前記フラグメントを、どのように前記ファイルに再構築されるかを示すインデックスファイルを形成するステップを更に含む、請求項３１に記載の方法。

【請求項５３】

前記プロセッサが

少なくとも第１のフラグメントと対応する第２のフラグメントとを含む、前記インデックスファイルのフラグメントを生成し、

前記インデックスファイルの少なくとも前記第１のフラグメントを分散型データストレージシステムに格納し、

前記インデックスファイルの少なくとも前記第２のフラグメントを前記分散型データストレージシステムの外部に格納するステップを更に含む、請求項５２に記載の方法。

【請求項５４】

前記プロセッサが、前記ファイルの少なくとも第３のフラグメントを生成し、前記第３のフラグメントを、前記分散型データストレージシステムに格納された前記第１のフラグメントとは別に、前記分散型データストレージシステムに格納するステップを更に含む、請求項３１に記載の方法。

【請求項５５】

前記プロセッサが、少なくとも前記第１のフラグメントを、トランザクションとして前記分散型データストレージシステムに格納するステップを更に含む、請求項３１に記載の方法。

【請求項５６】

前記プロセッサが、少なくとも前記第１のフラグメントと前記第３のフラグメントを、異なるトランザクションとして前記分散型データストレージシステムに格納するステップを更に含む、請求項３１に記載の方法。

【請求項５７】

前記プロセッサが、前記ユーザからのリクエストに応じて、前記ファイルフラグメントを、前記ファイルに再構築するステップを更に含む、請求項３１に記載の方法。

【請求項５８】

前記プロセッサが、前記ファイルのヘッダの少なくとも一部を含む前記第１ファイルフ

ラグメントを生成するステップを更に含む、請求項３１に記載の方法。
【請求項５９】
前記ブロックチェーン外のストレージは、自身のＣＰＵを持たないデジタルストレージ装置である、請求項３１に記載の方法。
【請求項６０】
前記分散型データストレージは、分散型台帳ストレージである、請求項３１に記載の方法。
【考案の詳細な説明】
【関連出願の相互参照】
【０００１】
本願は、２０１６年１０月２６日に出願された米国特許出願第１５／３３５，３４４号、米国特許出願第１４／９４０，１４２号に関連し、両文献は参照により本願に組み込まれる。
【技術分野】
【０００２】
本開示は、電子データを安全に格納するシステム及び方法に関する。
【背景技術】
【０００３】
データファイル、グラフィックファイル、画像ファイル、動画ファイル、生体特徴ファイル、生体特徴データ等のあらゆる形態の電子データを安全に格納すること、更に／或いは当該情報をファイルフォーマットであるかを問わずに安全格納することが常に求められている。インターネットの発展により、如何に厳密に保護されていようと、世界中の誰もが個人又はエンティティのコンピュータシステムに対して不正アクセスができ得る状態となっている。例えば、狡猾なフィッシング詐欺、オンラインウィルス、トロイの木馬、ワーム等々により、ユーザ名やパスワードが盗まれる可能性がある。電子ＩＤの窃盗やその他サイバー犯罪が横行しており、誰もが無関係ではいられない。
【０００４】
従来から、不正アクセスに対抗する数多くの方法が存在する。例えば、１つの方法として、詐欺を認識できるように個人を訓練することが挙げられる。しかし人間は完璧ではない。ファイヤウォールや、アンチウィルスアプリケーションなどのセキュリティソフトウェアの使用をはじめとして、ある程度の保護が見込めるものは多種多様に存在する。しかし、セキュリティレベルを上げることで、コンピュータのパフォーマンスが低下する可能性がある。更に／或いは、ユーザが自身の電子データによりアクセスしにくくなる可能性がある。
【０００５】
より安全な方式として、二要素又は多要素認証が知られている。多要素認証は、２つ（この場合二要素となる）又はそれ以上の個別の（ユーザ）クレデンシャルを組み合わせるものである。例えば、ユーザはアクセスが承認されるために、パスワードの入力と、セキュリティトークン又は認証トークン（ユーザが持ち運ぶ小型ハードウェアデバイス）の提供が求められ得る。認証トークンは、多くの場合キーフォブ又はスマートカードである。多くの場合、ユーザは認証トークンを作動させるためのＰＩＮ（個人認証番号）を有する。これにより、認証トークンが盗まれても、セキュリティが侵害される可能性が最小限にとどめられる。
【０００６】
多要素認証の別の機構として、ウェブサイトにログインして一時パスワードをユーザの電話又はメールアドレスで取得すること、セキュリティ質問に答えること、ＶＰＮクライアントにより有効な電子証明書をダウンロードしてアクセスが承認される前にＶＰＮにログインすること、例えば指紋スキャン、網膜スキャン、顔認証、音声認証、その他生体特徴情報による生体特徴スキャニングが挙げられる。例えば、認証及び安全な通信のための生体認証プロトコル規格に関する米国特許第９，８３８，３８８号及び米国特許第出願公

開第２０１６／０３７３４４０号（両文献ともＭａｔｈｅｒによる）を参照のこと。
【０００７】
残念ながら、格納した生体特徴情報は盗まれる可能性がある。個人にとって、生体特徴情報が盗まれることは、社会保障番号が盗まれることに勝るとも劣らないほど深刻であろう。
【０００８】
従来、セキュアサーバへの電子データの格納という保護方策が採られている。しかし、この十分に保護されたサーバでも、サイバー攻撃の被害を受け得る。
【０００９】
現状、個人に関する情報を保護するためのシステム及び方法は、様々な欠陥がある。当技術分野では、文書などに関連する情報を保護するより高度な方法が必要とされている。例えば、当技術分野では、バイオメトリックセキュリティに関連するより高度な方法が求められている。
【００１０】
近年「ブロックチェーン」と呼ばれる技術が、主に暗号通貨のためのセキュリティ対策として開発された。ブロックチェーンによる格納は、分散型台帳の一種であり、ユーザが多数のノードに情報を格納する分散型データストア、或いはユーザが多数のピアネットワークノードに情報を格納するコンピュータネットワークを指す。ピアネットワークは、データストアネットワークの各ユーザ又は参加者が、自身のコンピュータを介して分散型データストアに接続されることを意味する。各ユーザとそのコンピュータを「ノード」と称する。各ノードは、同じ情報を格納し、分散型データストアの認証及び／又は照合に寄与する。ブロックチェーン／分散型台帳は、ユーザ数が膨大であり、そのシステムを破壊するには、サイバー攻撃者は全て又は大部分のノードに格納されたデータを短時間で変更しなければならないため、理論上、情報の改竄は不可能である。大部分のノードに変更を加えなければならない理由は、暗号通貨の場合、各ノードが同一のデータを保持しており、適切であるとノードが合意したデータが格納されるためである。暗号通貨の場合、ブロックチェーンデータは特定の暗号通貨に対する全てのデジタルトランザクションの台帳を提供する。
【００１１】
ブロックチェーン／分散型台帳は、その分散型という性質（全てのノードが同じデータを格納する）により、データの改竄及び／又は破壊に対して安全性を保証するのである。しかし、ブロックチェーン／分散型台帳は全てのトランザクションを格納し、それらトランザクションを全ノードにコピーするため（台帳）、ブロックチェーンに格納されるデータ量が限定されるように、ブロックチェーン／分散型台帳が効率的に動作することが非常に重要となる。ブロックチェーン／分散型台帳に対する格納制限は、セキュアサーバに対する格納制限と大幅に異なっている。
【００１２】
これは例えば、特定の種類の暗号通貨の全ノードが当該暗号通貨についての全トランザクションを格納していることを表す。
【００１３】
ブロックチェーン／分散型台帳は更に、ブロックチェーン／分散型台帳技術に加え、ファイルを暗号化するための暗号化技術により、ノード上及び送信時にファイルを保護する。また、格納されたデータは通常、読み取り専用である。
【００１４】
より具体的には、ブロックチェーン／分散型台帳におけるユーザは全てピアツーピアネットワークを介して接続されている。このネットワークは、従前のデータセンター型クラウドストレージソリューションと比較して、安全性が高く、速度は１０倍で、コストも半分で済む。したがって、ブロックチェーン／分散型台帳はユーザにデータを安全かつ分散的に格納可能とする。これは、トランザクション台帳、暗号化ハッシュ機能、公開／秘密鍵暗号化等のブロックチェーン／分散型台帳の特性により実現されるものである。

【００１５】
ブロックチェーン／分散型台帳は分散型であるため、侵害される中央サーバが存在しない。また、クライアント側の暗号化により、エンドユーザのみが自身の暗号化前のファイルと暗号化鍵に対する全アクセス権を有する。
【００１６】
いくつかの実施形態のブロックチェーン技術に基づく分散型データ格納では、そのデータブロックのハッシュのみが格納される。データブロックは、暗号化された分散型ハッシュにより十分正当性、信頼性が確認可能である。ブロックチェーンでは、データは暗号化され、分散して格納される上に、それぞれ自身の暗号化ハッシュを含む各ブロックが連続したチェーンを形成する。このようにブロックがリンクされることで、分散型トランザクション台帳が実現される。
【００１７】
多くのデータ専門家の考える、ブロックチェーン／分散型台帳がもたらす最大の影響は、ディスインターメディエーションであろう。誰にでもアクセスでき、且つアクセス制限も可能な、優れた設計のブロックチェーン／分散型台帳であれば、現在仲介金融機関が提供している信頼できる取引環境、詐欺や処理ミス防止、確実な契約遵守、金融取引に関する機能の多くを代替可能である。
【００１８】
ブロックチェーン／分散型台帳の強みは暗号化の強度のみではない。コンピュータのチェーン上の分散により、ブロックチェーン／分散型台帳は攻撃されにくい。ブロックチェーン／分散型台帳は、トランザクションや所有権又はＩＤを改竄不能に記録、契約の交渉、履行等々に利用可能な自己検証型格納方式を採る。
【００１９】
ただし、ブロックチェーン／分散型台帳の使用には問題点も存在する。ブロックチェーン／分散型台帳は台帳又はトランザクションのコピーを全てのノードに格納し、また格納したトランザクションを削除できないため、すぐに要求される格納量が莫大なものになり得る。また、ＲＢＡＣ（ロールベースアクセス制御）のような各種アクセス制御を実現するには、中央集権型システムを使用することが好ましい。しかし、その場合中央システムがハッキングされると、ブロックチェーンに対して不正アクセスを許してしまう。ブロックチェーン／分散型台帳に機密情報を格納する場合、ブロックチェーン／分散型台帳データは容易に削除が実行できないことから、セキュリティにより敏感にならざるを得ない。
【００２０】
上記セキュリティ処理以外の技術として、ファイルを分散して格納し、リクエストに応じて再構築するセキュアストレージシステムが存在する。例えば、米国特許出願公開第２０１６／０１９６２１８号（Ｋｕｍａｒによる）、米国特許出願公開第２０１７／０２７２１００（Ｙａｎｏｖｓｋｙによる）、米国特許第８，６９４，４６７（Ｓｕｎによる）が挙げられる。
【００２１】
ブロックチェーンを限定的に使用し、ファイル格納には使用しないことも提案されている。その例として、「分散型プライバシ：ブロックチェーンによる個人データ保護」（Ｚｙｓｋｉｎｄによる）及びＷＯ２０１７／１４５０１０（Ｗｒｉｇｈｔによる）が挙げられる。
【００２２】
しかし、ブロックチェーン／分散型台帳と、中央サーバストレージに対する制限により、これらシステムはいずれも、期待されるほどの安全性、機能性は実現できていない。
【００２３】
したがって、電子データを安全に格納する、より高度な方法が求められているのである。
【考案の概要】
【００２４】

本技術に係るいくつかの形態は、ソフトウェアを使用して、セキュリティ問題を解決することで、コンピュータ機能の向上を図ることを対象にする。個人（ユーザ）及び／又はエンティティに関連付けられた情報を安全に保存可能であることが、セキュリティ上望ましい。ユーザは、民間企業、政府機関、又はその他エンティティのような、エンティティの代理として行動し得る。

【００２５】

１又は複数の実施形態において、例えばデジタルファイルのような電子データを安全に格納するためのシステム及び方法が提供される。当該システム及び方法において、デジタルファイルはファイルフラグメントに分解され、１又は複数のフラグメントは１又は複数のブロックチェーン／分散型台帳に格納され、残りの（１又は複数）のフラグメントはブロックチェーン／分散型台帳外の、例えば１又は複数のセキュアサーバ、及び／又は１又は複数のユーザ装置に格納される。格納されたファイルは、生体特徴ファイルもしくは部分生体特徴ファイル及び／又は任意のデータファイルである。ファイルは暗号化又はハッシュ化されてもよい。ファイルフラグメントは、好ましくは暗号化され、完全に再構築されない限りは意味を成さない。いくつか又は任意の実施形態では、ファイルの１又は複数のフラグメントは、オフラインで、例えば、通常は自身のＣＰＵを有さないＵＳＢ又はサムドライブ、又はその他デジタル記憶装置に格納されてもよい。これら及び／又はその他任意の実施形態において、１又は複数のファイルフラグメントは、ファイルヘッダの全て又は一部のみを含んでもよい。

【００２６】

例えば、１のファイルフラグメントを窃盗、コピー、ハッキングしても、意味を成す、有用な情報の窃盗、コピーに対して有効な手段とはならない。

【００２７】

いくつかの実施形態では、（１又は複数の）ブロックチェーン／分散型台帳上に格納することの利点を１又は複数のセキュアサーバ（及び／又は１又は複数のユーザ装置）上に格納することの利点を組み合わせてもよい。

【００２８】

１又は複数の実施形態では、意味を成さない部分生体特徴ファイルは、格納箇所に関わらず、否認防止のために十分な情報を適用可能である。

【００２９】

任意の実施形態において、１又は複数のブロックチェーン／分散型台帳の特徴の一部又は全部を有する分散型データストレージが提供されてもよい。当該特徴としては、変更不能格納、暗号化、ピアツーピア、分散型、及び／又は合意が挙げられる。任意の実施形態において、部分的分散型台帳（例えば、コンソーシアムブロックチェーン）、別種のブロックチェーン又は分散型台帳が提供されてもよい。

【００３０】

本技術の上述及びその他の特性及び特徴、更に関連する構成要素及び各部品の組み合わせの動作方法及び機能、並びに製造の経済性については、添付図面を参照しつつ以下の詳細な説明と添付の実用新案登録請求の範囲を検討することによって更に明らかになる。これらはいずれも本明細書の一部を構成する。本明細書において、類似の参照符号は様々な図面において対応する部分を示している。但し、図面は例示及び説明のみを目的としており、本考案の限定事項の定義として用いることは意図されていないことは明確に理解されるべきである。本明細書及び請求項において、単数形の表記には別途指定のある場合を除いて複数のものへの言及が含まれる。

【図面の簡単な説明】

【００３１】

【図１】図１は、１以上の形態に係わる、ユーザの電子データのための、セキュアサーバストレージが組み合わされた汎用分散型ストレージを提供するシステムを示す。

【図２】図２は、電子データを安全に格納する処理の例を示す。

【図２Ａ】図２Ａは、生体特徴画像又は任意の画像ファイルの格納処理の例を示す概略的

フローチャートである。
【図３】図３は、生体特徴ファイル及び／又はその他任意の種類のファイル等の電子データを分割して格納する処理の例を示す。
【図３Ａ】図３Ａは、任意の種類のファイルを格納する処理の例を示す概略的フローチャートを示す。この処理は、図２Ａ及び４Ａの処理の一部であってもよい。
【図４】図４は、生体特徴ファイル等の電子データを分割して格納する処理の例を示す。
【図４Ａ】図４Ａは、生体特徴画像又は任意の画像ファイルを格納する別の処理の例を示す概略的フローチャートである。
【図５】図５は、安全に格納された生体特徴ファイル等のファイルを読み出して、再構築する１の方法を示す。
【図６】図６は、安全に格納された分割生体特徴ファイル（ＳＰＢＦ）等のファイルを読み出して、再構築する１の方法を示す。
【図７】図７は、任意のファイルを再構築する一般的処理の例を示す。
【図８】図８は、ファイル削除処理の例を示す。
【図９】図９は、暗号化ＳＰＢＦファイルを使用した生体認証処理の例を示す。
【図１０】図１０は、ハッシュ化ＳＰＢＦファイルを使用した生体認証処理の例を示す。
【図１１】図１１は、ＳＰＢＦファイル及び生体特徴ベクトルを使用した生体認証処理の例を示す。
【図１２】図１２は、ハッシュ化生体特徴ベクトルファイルを利用した生体認証処理の例を示す。
【図１３】図１３は、ユーザを登録する処理の例を示す。
【図１４】図１４は、電子データを安全に格納するための、ユーザのリクエストの処理の例を示す。
【図１５】図１５は、安全に格納された電子データを読み出すための、ユーザのリクエスト処理の例を示す。
【図１６】図１６は、適用されたブロックチェーン又は分散型台帳の例の概要を示す。
【考案を実施するための形態】
【００３２】
図１は、１以上の形態に係わる、ユーザの電子データを安全に格納するための、汎用分散型ソリューションを実現するシステム１００を示す。いくつかの形態では、システム１００は、１又は複数のサーバ１０２を含むことができる。（１以上の）サーバ１０２は、クライアントサーバ構造、ピアツーピア構造、及び／又は例えばクラウド１０１のようなその他の構造（例えばインターネット）に関わる１以上のコンピューティングプラットフォーム１０４と通信するように構成されてもよい。ユーザは、（１以上の）コンピューティングプラットフォーム１０４を介してシステム１００にアクセスしてもよい。当該アクセスはＡＰＩが伴う場合がある。（１以上の）サーバ１０２は、機械可読命令１０６を実行するように構成されてもよい。機械可読命令１０６は、登録要素１０８、トランザクションアドレス要素１１０、ユーザインタフェース要素１１４、アクセス管理要素１１６、情報管理要素１１８の内の１以上を含んでもよい。１以上の任意の実施形態では、身元認証要素１２０が含まれてもよい。当業者には明らかなように、その他機械可読命令要素が存在してもよい。各要素は、分割及び／又は統合されてもよい。ブロックチェーン又は分散型台帳ネットワークのトランザクションアドレスを構築するように、機械可読命令１０６が実行されてもよい。一般的に、ブロックチェーン又は分散型台帳とは、システム１００に参加するノードの一部又は全部が共有するトランザクションデータベースである。例えば、少なくとも１００、１，０００、１０，０００、１００，０００、１，０００，０００、或いはそれ以上の数のノードが存在し得る。当該参加は、ビットコインプロトコル、イーサリアムプロトコル、リップル合意ネットワーク（ＲＴＸＰ（リップルトランザクションプロトコル））、Ｌｉｎｕｘ（登録商標）によるハイパーレジャー、Ｒ３社のＣｏｒｄａ、シンビオント分散型台帳（アセンブリ）、及び／又はデジタル通貨、分散型台帳及び／又はブロックチェーンに関連するその他プロトコルに基づくものであってもよい。

ブロックチェーン又は分散型台帳の完全なコピーは、現在までの、関連するデジタル通貨に関する全てのトランザクション又はスマートコントラクト等のその他トランザクションの全てを含む。ブロックチェーンは、トランザクションに加えて、本明細書にて更に説明するもの等、その他の情報を含んでもよい。

【００３３】

本明細書で使用される「ブロックチェーン」という用語は、別の１又は複数の実施形態では「分散型台帳」とも称される。あらゆる種類のトランザクションが、分散型ストレージ、分散型台帳、ブロックチェーン、又はその他適切な分散型又はネットワーク型トランザクション機構を含む分散型ネットワーク又はネットワークデータストアに格納可能である。分散型ストレージ（又は「分散型データストア」）は、ネットワーク上のノードに格納されたファイル又はファイルセグメント、又はネットワークデータストアにおいて格納されたデータストリームを含んでもよい。分散型ストレージは特定のフォーマット又はプロトコルに限定されるものではなく、サーバ、デスクトップＰＣ、携帯装置、リムーバブルストレージ、又はその他適切な装置を含む、任意のアクセス可能ネットワークノードに格納された、任意の種類のファイルを含んでもよい。一実施形態において、１ファイルの全体が単一のノードに格納され、別のファイルが別のネットワークノードに格納されてもよい。或いは、単一のファイルを複数のセグメントに分けて、１以上のネットワークノードに格納してもよい。一実施形態において、１のファイルの全体が単一のネットワークデータストアに格納され、別のファイルが別のネットワークデータストアに格納されてもよい。或いは、単一のファイルを複数のセグメントに分けて、１以上のネットワークデータストアに格納してもよい。いくつかのトランザクションネットワークは、分散型支払システム、部分分散型支払システム、又は中央支払システムとして構成される。

【００３４】

一実施形態において、分散型台帳は、１又は複数の分散型ネットワーク全体で共有、同期されるデータベース又はデータベースの複製であってもよい。或いは、分散型台帳は、ネットワークデータストア内のデータストリームであってもよい。分散型台帳により、トランザクションが全体又は一部に公開されたり、複製されたりが可能であるので、サイバー攻撃を受けにくい。更に、分散型台帳は、信用が低い環境（即ち、共有データベースをホストする参加者がそれぞれ独立して役割を担い、互いに信用していない状況）でも、共有事実の存在や状態についての合意を維持可能である。合意は、データの格納に必要なものである。合意とは、分散型台帳に特有のものではない。別の分散型データベースでも、Ｐａｘｏｓ又はＲａｆｔ等の合意アルゴリズムが利用されている。改竄不能という点についても同様である。分散型台帳以外で使用されるデータベース（Ｇｏｏｇｌｅ　ＨＤＦＳ，Ｚｅｂｒａ，ＣｏｕｃｈＤＢ，Ｄａｔｏｍｉｃ等）にも改竄可能なものが存在するのである。

【００３５】

分散型台帳は、通常の分散型データベースと、以下の点で異なる。（ａ）リード／ライトアクセスの制御が完全に又は部分的に分散化している。他の分散型データベースの場合、論理的に集中している。そのため、（ｂ）信頼できる第３者が不在の、困難な環境でも、トランザクションを保護可能である。分散型台帳は、ブロックチェーンのように線形な構造を有することができる。或いは、ＩＯＴＡのＴａｎｇｌｅのようにＤＡＧ（有向非巡回グラフ）を含むことできる。ブロックチェーン、ＩＯＴＡのＴａｎｇｌｅ、Ｈｅｄｅｒａのハッシュｇｒａｐｈは、所定のフォーマット及びアクセスプロトコルを有する分散型台帳の具体例である。

【００３６】

ブロックチェーンは、トランザクションを時間順に格納する分散型台帳である。ブロックチェーン台帳の場合、全てのトランザクションは、定期的に「ブロック」で検証、格納される。ブロックは暗号ハッシュを介して前ブロックにリンクしている。ブロックチェーン台帳は、公開されているため、トランザクションは誰にでも視認、追跡可能である。各ネットワークノードは、ブロックチェーンのコピーを受信、保持可能である。

【００３７】
上記に加え、本明細書記載のストレージとは、ネットワークに格納されたデータと称される、ネットワークデータストアであってもよい。当該データは、ネットワークに格納されており、ネットワークのノードに格納されてはいない。
【００３８】
いくつかの実施形態において、ストレージは典型的なデジタルメモリであってもよいし、量子データストレージ又は量子ストレージネットワーク（例えばクラウドに基づく）であってもよい。量子ストレージの場合、情報はエネルギーとして１又は複数の粒子に格納され、例えば陽子等の粒子の衝突により移転される。粒子は、そのエネルギーが情報として移転されるため、新たに粒子と衝突すると、それまで情報を持っていた粒子から、当該情報は消滅する。
【００３９】
登録要素１０８は、個別ユーザ（個人又はエンティティ）を登録（及び特定を支援）するように構成されてもよい。
【００４０】
２０１６年１０月２６日に出願された米国特許出願第１５／３３５，３４４（参照により本明細書に組み込まれる）に詳細に説明されているが、システムは、登録要素の一部として、或いは自身の要素として、１以上の認証文書に関連する情報を、ブロックチェーン信頼ユーティリティにおいてエンティティから受信してもよい。１以上の認証文書は、上記ユーザ（例えば、個人）に関連付けられてもよく、身分証明書、即ちユーザの身元を証明する文書であってもよい。エンティティは、機関、企業、会社、政府機関、及び／又はその他エンティティの１以上を含んでもよい。
【００４１】
ブロックチェーンはいくつかのブロックに基づいていてもよい。ブロックは、１以上の待機中トランザクションを含み、確認するレコードを含んでもよい。定期的に（トランザクションの種類及びチェーンにおけるユーザの量に応じて）、トランザクション及び／又はその他の情報を含む新たなブロックをブロックチェーンに追加してもよい。いくつかの形態では、ブロックチェーン内の所与のブロックは、前ブロックのハッシュを含む。これにより、起源ブロック（即ち、ブロックチェーンにおける第１のブロック）から現在のブロックまで、ブロックのチェーンが形成されるという効果が得られる。所与のブロックは前ブロックのハッシュを含むため、時間的に前ブロックの後に来ることが保証され得る。ブロックチェーンに含まれた後、所与のブロックは、ハッシュ機能の特性により計算上改竄不能となり得る。更に、ブロックチェーンにおいては、全てのトランザクションのコピーが、全て、或いは少なくとも複数のノード（例えば、特定のブロックチェーン領域内に属する全てのコンピュータ）に格納される。したがって、ブロックチェーンネットワーク内の全ての（或いは少なくとも大部分の）ノードにおける対応するブロックも改竄しない限り、ネットワークにおいて不整合は一目瞭然となる。ブロックの内容は、ブロックチェーンを支えるノードのネットワークのその他参加者から見ることが出来る。
【００４２】
より詳細に後述するように、トランザクションアドレス要素１１０は、１又は複数のトランザクションアドレスを、システムの１又は複数の個別ユーザに割り当ててもよい。当該トランザクションアドレスは、関連付けられた公開及び秘密鍵又はその他認証及びアクセス制御に加えて、当該トランザクションアドレスに関連付けられた特定のブロック内の情報に、ブロックチェーンがアクセスするために必要なものであってもよい。
【００４３】
ユーザインタフェース要素１１４は、ユーザインタフェースを提供してもよい。
【００４４】
例えば、システム１００は、登録要素１０８を介してユーザを登録するように構成されてもよい。登録処理は、図１３に示すような、典型的な登録処理であってもよい。例えば、ステップ１３０２において、システムは、ユーザインタフェース要素１１４内のシステ

ムＡＰＩを介して、登録用のユーザリクエストを受信してもよい。ステップ１３０４において、システムは、ユーザのＩＤデータを受信してもよい。ＩＤデータの例としては、名前、住所、メールアドレスが挙げられる。本明細書他所で記載される好適な実施形態では、ＩＤデータは更に、ユーザの身元を十分証明できる文書による根拠を含んでもよい。ステップ１３０６において、システムは、１又は複数の固有クレデンシャル等の、（１以上の）ユーザ個別識別子を割り当ててもよい。例えば、クレデンシャルは、ユーザ名、パスワード又はユーザ名とパスワードの組、数字、英数字、及び／又は（１以上の）その他クレデンシャル、及び／又は個人に関連付けられるその他情報の１以上であってもよい。ステップ１３０８において、システムは任意で、ユーザから生体特徴情報を受信してもよい。これにより、比較的セキュリティレベルが高いユーザ認証が実現可能となる。

【００４５】

いくつかの形態によると、認証済み個人身元を有する個人は、様々な方法で認証済み個人身元有する状態となったものとされ得る。例えば、いくつかの形態では、個人は、その身分証明を提供することが求められる場合がある。当該証明（上記の情報）は、政府発行の身分証明書（例えばパスポート及び／又は運転免許証）のコピー提出、個人が受け取った郵便物（例えば、公共料金）のコピー提出、第三者による証明、及び／又は個人の身元についてのその他証明を含んでもよい。当該証明は、（１以上の）サーバ１０２に関連したエンティティに対するものであってもよい。

【００４６】

いくつかの形態において、ユーザに関連付けられた１以上の認証文書に関する情報は、第１の鍵及び第２の鍵により暗号化されてもよい。第１の鍵は、バックエンドサーバに格納されるサーバ鍵（例えば、公開鍵）であってもよい。第２の鍵は、第１のユーザに関連付けられた生命認証データのハッシュであるクライアント鍵であってもよい。いくつかの形態では、第１及び第２の鍵は、機密データフォーマット及び／又は関連文書のハイパー暗号化のためのブロックチェーンの不変ＩＤに適用されてもよい。身元認証は、任意であって、登録処理の一部として行われてもよい。

【００４７】

システム１００は、トランザクションアドレス要素１１０を使用して、ブロックチェーン上のトランザクションアドレスを、登録された個人に割り当てるように構成されてもよい。所与のトランザクションアドレスは、公開鍵と秘密鍵に関連付けられてもよい（これはブロックチェーンに基づく暗号通貨では一般的である）。一例として、第１のトランザクションアドレスを個人に関連付けてもよい。第１のトランザクションアドレスは、第１の公開鍵と、第１の秘密鍵とを含んでもよい。

【００４８】

概して、公開鍵／秘密鍵組を、１以上の公開鍵アルゴリズムに応じた暗号化、復号化に使用してもよい。非限定的な例として、鍵組をデジタル署名に使用してもよい。当該鍵組は、署名用の秘密鍵と、デジタル署名認証用の公開鍵を含んでもよい。秘密鍵は秘密で（例えば、所有者のみが知るものとする）、公開鍵は広く公開されてもよい。鍵同士は数学的に関連付けられてもよいが、公開鍵から秘密鍵を計算することは不可能である。

【００４９】

いくつかの形態では、システム１００は秘密鍵が（１以上の）コンピューティングプラットフォーム１０４内に格納されるように構成されてもよい。例えば、第１の秘密鍵は、コンピューティングプラットフォーム１０４及び／又は個人に関連付けられたその他の場所に格納されてもよい。いくつかの実施形態によると、秘密鍵は、「ｖｅｒｉｆｙ．ｄａｔ」ファイル、ＳＩＭカード、及び／又はその他の場所の内の１以上に格納されてもよい。

【００５０】

いくつかの形態では、システム１００は、複数のトランザクションアドレスが別々の個人に割り当てられるように構成されてもよい。例えば、第１のトランザクションアドレスに加えて、第２のトランザクションアドレスが第１の個人に割り当てられてもよい。１以

上の形態では、第１の個人に対して、１以上の更なるトランザクションアドレスが割り当てられてもよい。システムに登録された第２の個人は、第３のトランザクションアドレスを受信してもよく、それ以降も同様であってもよい。

【００５１】

システム１００は、個人に関連付けられた識別子及び生体特徴データを、対応するトランザクションアドレスに記録するように構成されてもよい。例えば、第１の個人に関連付けられた第１の識別子及び第１の生体特徴データが、第１のトランザクションアドレスに記録されてもよい。所与のトランザクションアドレスに情報を記録することは、ハッシュ又はその他の暗号化された情報の表現を記録することを含んでもよい。いくつかの形態では、所与の一個人に割り当てられた複数のトランザクションアドレスに、異なる生体特徴データが記録されてもよい。例えば、第１の個人（第１のユーザ）に関連付けられた第１の識別子と第１の生体特徴データとを第１のトランザクションアドレスに記録することに加え、第１の個人に関連付けられた第１の識別子と第２の生体特徴データとを第２のトランザクションアドレスに記録してもよい。

【００５２】

概して、生体特徴データは、人間特性に関する指標を含んでもよい。生体識別子は、個人を特定及び表現可能な、固有且つ測定可能な特徴である。生体識別子は、典型的には身体的特徴を含むものであるが、更に行動的特徴及び／又はその他の特徴を更に含んでもよい。身体的特徴は、個人の身体形状に関するものであってもよい。生体特徴データとして利用される身体的特徴の例としては、指紋、手のひら静脈、顔認証、ゲノム情報、（１以上の）ＤＮＡ配列及び（１以上の）ＤＮＡ修飾、プロテオミクス情報、（１以上の）タンパク質配列及び（１以上の）タンパク質修飾、掌紋、手の形状、虹彩認証、網膜、臭い又は香り、及び／又はその他の身体的特徴の１以上が挙げられる。行動的特徴は、個人の行動パターンに関するものであってもよい。生体特徴データとして利用される行動的特徴の例としては、タイピングのリズム、歩き方、声、心拍数、及び／又はその他の行動的特徴の１以上が挙げられる。

【００５３】

生体特徴データは、身体的特徴を示す画像又はその他の視覚的表現、行動的特徴の記録、身体的特徴及び／又は行動的特徴のテンプレート、及び／又はその他の生体特徴データの内の１以上を含んでもよい。テンプレートは、対象から抽出した関連する特性の組み合わせを含んでもよい。テンプレートは、身体的特徴及び／又は行動的特徴の特性を表すベクトル、身体的特徴及び／又は行動的特徴の数学的表現、特定の特性を有する画像、及び／又はその他の情報の内の１以上を含んでもよい。

【００５４】

生体特徴データは、個人に関連付けられたコンピューティングプラットフォーム１０４を介して受信されてもよい。例えば、第１の個人に関連付けられた生体特徴データは、第１の個人に関連付けられた第１のコンピューティングプラットフォーム１０４を介して受信されてもよい。第１のコンピューティングプラットフォーム１０４は、第１の個人の身体的特徴及び／又は行動的特徴を取得及び／又は記録するように構成された入力装置（不図示）を有してもよい。当該入力装置の例としては、カメラ、及び／又はその他の撮像装置、指紋スキャナ、マイク、加速度計、及び／又はその他の入力装置の内の１以上が挙げられる。

【００５５】

システム１００は、個人に対して提示されるインタフェースを、関連するコンピューティングプラットフォーム１０４を介して提供するように構成されてもよい。インタフェースは、個人のコンピューティングプラットフォーム１０４を介して提示される、ユーザインタフェース要素１１４を介するグラフィカルユーザインタフェースを含んでもよい。いくつかの形態では、インタフェースは、所与の個人に対して少なくとも１のストレージアドレスが割り当てられている限り、所与の個人が当該所与の個人に対して割り当てられるストレージアドレスを追加又は削除可能とするように構成されてもよい。

【００５６】
いくつかの形態では、システム１００は、システム１００のユーザに関連付けられた１以上のユーザプロファイル及び／又はユーザ情報にアクセスする、更に／或いはそれを管理するように構成されてもよい。１以上のユーザプロファイル及び／又はユーザ情報は、（１以上の）サーバ１０２、（１以上の）コンピューティングプラットフォーム１０４、及び／又はその他の格納箇所に格納される情報を含んでもよい。ユーザプロファイルの例としては、ユーザを特定する情報（例えば、ユーザネーム、ハンドルネーム、番号、識別子、及び／又はその他の識別情報）、セキュリティログイン情報（例えば、ログインコード又はパスワード）、システムアカウント情報、閲覧情報、デジタル通貨アカウント情報（例えば、ユーザがクレジットで保有する通貨に関する）、関係性情報（例えば、システム１００のユーザ間の関係性に関する情報）、システム利用情報、ユーザに関する人口統計的情報、システム１００のユーザ間の交流履歴、ユーザが申請した情報、ユーザの購入情報、ユーザの閲覧履歴、ユーザに関連付けられたコンピューティングプラットフォーム識別、ユーザに関連付けられた電話番号、及び／又はユーザに関連付けられたその他の情報が挙げられる。

【００５７】
機械可読命令１０６は、１以上の個別識別子と（１以上の）トランザクションアドレスとにより、電子データがブロックチェーン又は１又は複数のセキュアサーバに基づいて格納されるように実行されてもよい。

【００５８】
図１４は、電子データを安全に格納するユーザのリクエストの処理を示す。当該電子データは、通常ファイル形式、又はその他固有な形式をとる。ステップ１４０２において、システムは、ユーザのサインインリクエストを、ＡＰＩを介して受信してもよい。ステップ１４０４において、システムは、格納されたユーザの生体特徴情報及び、登録処理で記録されたその他（１以上の）識別子により、ユーザ認証を行ってもよい。ステップ１４０６において、システムは、ユーザの格納リクエストを受信してもよい。ステップ１４０８において、システムは、格納されるユーザの電子データを受信してもよい。ステップ１４１０において、システムは、電子データをファイルフラグメントに分割してもよい。各フラグメントは、好ましくはファイルの一部であり、全てのフラグメントが完全に意味を成すファイルとして（機械又は人により）構築されない限り、単一又は集合では意味を成さないことが好ましい。１以上の実施形態では、例えば、１フラグメントがファイルヘッダで、別の１又は複数のフラグメントがファイルのデータ又は画像データであってもよい。ファイルヘッダも、１以上のフラグメントに分割してもよい。ステップ１４１２において、システムは、１又は複数の分散型台帳の１又は複数の場所、又は分散型データベースの１又は複数の場所において（好ましくはトランザクションとして）、１又は複数のファイルフラグメントを、１又は複数のブロックチェーンの１又は複数のブロックに（好ましくはトランザクションとして）格納してもよい。他の１又は複数のファイルフラグメントを、ブロックチェーン、分散型台帳、又は分散型データベース外の、例えば１又は複数のセキュアサーバ及び／又は１又は複数のユーザデバイスに格納してもよい。１又は複数のフラグメントは、オンライン又はオフラインで格納されてもよい。例えば、オンライン環境から外すことが可能で、通常は自身のＣＰＵを持たないＵＳＢ、ＳＩＭカード、サムドライブ又はその他適切な装置のような、１又は複数の別のデジタル記憶装置に格納されてもよい。

【００５９】
図２は、生体特徴及び／又はその他非常に個人的な情報、及び／又は機密情報のような電子データを安全に格納するため、以下のステップを実行するシステム１００の例を示す。システムは、この安全な格納要素を、ユーザ登録の際に、セキュアストレージシステムに実現し、例えば、ユーザの生体特徴電子データを認証要件の一部になるようにしてもよい。更に／或いは、当該格納は、ユーザがその後電子情報の安全な格納用の登録リクエストを行い、システムを使用して、ユーザの生体特徴電子データのような電子データを、安

全に格納したい場合に実現されてもよい。

【００６０】

ステップ２０２において、システムは、ユーザを登録、ユーザのＩＤ割り当て、認証（好ましくは二要素認証以上）の最中又はその後に、生体特徴電子情報を複数の特徴ブロックに分割し、各特徴ブロックにインデックス番号を付してもよい。インデックス番号は、インデックス付け処理の任意態様として、乱数発生器又はその他適切な乱数器により乱数化されてもよい。

【００６１】

任意のステップ２０４において、システムは、任意で１又は複数の特徴ブロックを、回転、フリッピング、マスキング、及び／又はその他方法で、変換してもよい。変換方法は、好ましくはランダムに行われるが、疑似ランダムでも、所定の形式で実行されてもよい。生体特徴情報が声で、特徴ブロックが声ブロックであれば、各ブロックは、任意で反転、マスキング、ピッチ変換、及び／又はその他方法により操作されてもよい。システムは、変換データ（例えば、フリッピング／回転情報）を記録する。なお、変換は必ずしも必要ではなく、この段階で実行されることが必要なものではなく、本明細書の任意の実施形態において、処理のより早い又は遅い段階で実行されてもよい。

【００６２】

ステップ２０６において、システムは、各データブロックのインデックス番号、変換データ、幾何学的位置をマッピングしてもよい。

【００６３】

ステップ２０８において、システムは、前ステップで収集したインデックス番号、変換データ、幾何学的位置のマッピングファイルを作成する。

【００６４】

任意のステップ２１０において、システムは、マッピングファイルを暗号化する。

【００６５】

ステップ２１１において、システムは、マッピングファイルも分割（任意で）し、格納する。システムがマッピングファイルを分割し、格納する一実施形態を図３の処理３００に示す。

【００６６】

ステップ２１２において、システムは、特徴ブロックの一部（例えば、特徴ブロックの３０％等の割合）を選択し、グループ化する。これはランダムに行うことが好ましいが、疑似ランダムでも、所定の手順で行われてもよい。このステップは、ステップ、２１４，２１６，３００において、複数回実行されてもよい。これにより、多数の分割された生体特徴ファイルが生成される。特徴ブロックの一部を選択してまとめる処理では、所与の特徴ブロックが複数回選択されてもよい。

【００６７】

ステップ２１４において、システムは、特徴ブロックのグループから、特徴ブロックを再構築して、新たなファイルを生成することで、スクランブル部分生体測定特徴（ＳＰＢＦ）を形成してもよい。以下に説明する１又は複数の手法によると、このステップを複数回実行して、複数のＳＰＢＦを生成してもよい。

【００６８】

任意のステップ２１６において、システムは、ＳＰＢＦファイルを暗号化してもよい。ＳＰＢＦファイルの暗号化は、ＡＥＳアルゴリズム、ＰＧＰアルゴリズム、Ｂｌｏｗｆｉｓｈアルゴリズム、又は他の適切な暗号化アルゴリズムによって実現してもよい。

【００６９】

ステップ２１８において、システムは、再度処理３００に進み、ＳＰＢＦファイルを分割、格納してもよい。

【００７０】

生体特徴ファイルの格納について、ファイルを分割、格納する方法は多数存在することが理解されよう。例えば、１の手法として、元の生体特徴ファイル又はＳＰＢＦファイル

（暗号化されているか否かは問わない）を複数のフラグメントに分割し、各フラグメントのファイルを生成して、１又は複数の記憶装置に格納することであってもよい。この方法は、元の電子データの再構築に必要な、インデックスファイル、マッピングファイル、幾何学的位置ファイル、及び／又はその他ファイルの格納に適用されてもよい。

【００７１】

全ての分割ファイル（即ち、ファイルを分割又は分解して得られた全ての「フラグメントファイル」）は、元のファイルを再構築するために、順序だてて格納されるべきである。ファイルがどのように分割されたかを示す情報を格納するための更なる１又は複数のファイル、即ち、再構築のため、ファイルフラグメントの順序（インデックス順番付け）を含むインデックスファイルが存在するべきである。インデックスファイルは、後に元のファイルを再構築するために必要である。この方法は、元の生体特徴ファイルのハッシュファイルにも適用できる。その場合、ＳＰＢＦファイルを生成する必要がない。むしろ生成されない方が好ましい。一実施形態において、インデックスファイルそのものが、元ファイル同様に、任意で分割されてもよく、一部がブロックチェーン、分散型台帳、又は分散型データベースに格納され、一部がブロックチェーン、分散型台帳、又は分散型データベース外に格納されることが好ましい。その結果、（第１）インデックスファイルに対するインデックスファイルが生成される。この「第２」インデックスファイルは、最も安全に格納されるべきであり、好ましくはオフラインで第１インデックスファイルとは異なる暗号化方法により暗号化されるべきである。

【００７２】

別の生体特徴ファイル分解、格納方法として、異なる複数の特徴ブロックを選択し、異なる複数のＳＰＢＦファイル（暗号化されているか否かは問わない）を生成し、当該異なる複数のＳＰＢＦファイルを１以上の記憶装置に格納することが挙げられる。ＳＰＢＦファイルの特徴ブロックは、元の生体特徴データファイルの全て又は一部（例えば、認証に利用される場合）を網羅してもよい。この方法の場合、単一の生体特徴に対して、１又は複数のＳＰＢＦファイルの任意の組み合わせが使用されて、１又は複数種類の生体認証が実現できる。

【００７３】

単一の生体特徴に対して、複数のＳＰＢＦファイル（複数生成された場合）と、対応するフラグメントファイルがそれぞれ別々に、１のブロックチェーンの異なる複数の場所に、１又は複数のトランザクションアドレス、及び／又は１又は複数のスマートコントラクトアドレス及び／又は１又は複数のブロックチェーンユーティリティアドレス下に格納できる。単一の生体特徴に対して、複数のＳＰＢＦファイル（複数生成された場合）と、フラグメントファイルがそれぞれ別々に、１又は各ブロックチェーンの１又は複数の独立したブロックチェーン及び／又は１又は複数のトランザクション記録、１又は複数の独立した分散型台帳、及び／又は１又は各分散型台帳の１又は複数のトランザクション記録、１又は複数の独立した分散型データベース及び／又各分散型データベースの１つの１又は複数の記録に格納されてもよい。単一の生体特徴に対して、１又は複数のＳＰＢＦファイル又はフラグメントファイルが格納の前に暗号化されてもよい。単一の生体特徴から得られた１又は複数の暗号化ＳＰＢＦファイル及び／又はフラグメントファイルに対して、特に当該ファイルがブロックチェーン、分散型台帳、又は分散型データベース（公開か秘密かは問わない）に格納されている場合、生体特徴の持ち主のみが当該ファイルを復号化するパスフレーズ／鍵を有する。これにより、生体特徴の持ち主以外が当該暗号化ファイルを生体認証に使用できないことが保証されやすくなる。ＳＰＢＦファイルは、格納される前にハッシュ化されてもよい。

【００７４】

上述の全ての生体特徴ファイル分解、格納方法は、単独又は組み合わせて実行可能である。

【００７５】

図２Ａは、生体特徴画像を格納する処理の例の、概略的フローチャートを示す。ステッ

プ２２０において、システムは、（図２の処理開始として）生体特徴の画像を受信してもよい。ステップ２２２（ステップ２０２同様）において、システムは、画像をブロック（特徴ブロック）に分割してもよい。ステップ２２４（ステップ２０４、２０８、２１２，２１４同様）において、システムは、結合又はグループ化されるいくつかの特徴ブロックを選択してもよい（例えば、ランダムに選択することで高い安全性となるが、疑似ランダム又は非ランダムに選択してもよい）。当該プロセスにおいて、システムは特徴ブロックを、例えば９０°又はランダムな角度で回転させることで変換する。ステップ２３０において、システムは、マッピングファイルを生成する（ステップ２０６、２０８、２１０同様）。その後、１又は複数のマッピングファイルは、ステップ２３２及び２３４において、（任意で）分割されてもよく、ファイルフラグメントは、部分的にブロックチェーン、分散型台帳、又は分散型データベースに格納され（２３４Ａにおいてストレージオプションと称する）、部分的にブロックチェーン、分散型台帳、又は分散型データ外のストレージに格納される。当該ストレージは、１又は複数のクラウドサーバ、１又は複数のセキュアサーバ（例えばエンティティ又は個人所有）、及び／又は１又は複数のクライアントデバイスを含む。例えば、クライアントデバイスは、ユーザの携帯電話、タブレット、ノートＰＣ、デスクトップＰＣ、又はその他ユーザデバイスである（図２のステップ２１１，２１８、図３の処理３００、２３４Ｂにてストレージオプションと称する）。ストレージオプション２３４Ｂは、ネットワークデータストアを含んでもよい。

【００７６】

１又は複数のフラグメントは、通常は自身のＣＰＵを持たないＳＩＭカード、ＵＳＢサムドライブ等の、１又は複数のその他デジタル記憶装置、又はその他適切な装置に格納されてもよい。ステップ２２６（ステップ２１６と同様）又はステップ２２８（処理２００にはないが、任意でそのステップ２１６の代わりに実行されてもよい）において、システムは、選択的に任意で暗号化又はハッシュ化をそれぞれ生体特徴ファイル、ＳＰＢＦファイル、又はステップ２２４で生成されたファイルの一部に適用してもよい。一実施形態において、生体測定／ＳＰＢＦファイルの一部に対するハッシュ化は、ＭＤ５アルゴリズム、ＳＨＡアルゴリズム（例えば、ＳＨＡ－０）、ＳＨＡ－２アルゴリズム（例えば、ＳＨＡ－２５６）、又はその他適切なハッシュ化アルゴリズムを適用することで実現できる。別の実施形態では、生体測定／ＳＰＢＦファイルの一部に対するハッシュ化は、ＡＥＳアルゴリズム、ＰＧＰアルゴリズム、Ｂｌｏｗｆｉｓｈアルゴリズム、又はその他適切な暗号化アルゴリズムを適用することで実現できる。なお、インデックスファイルの場合、元ファイルと同様、マッピングファイルそのものを任意で分割でき、部分的（又は全て）にブロックチェーンに格納して部分的にブロックチェーン外に格納したり、部分的（又は全て）に分散型台帳に格納して部分的に分散型台帳外に格納したり、部分的（又は全て）に分散型データベースに格納して部分的に分散型データベース外に格納したりしてもよい。その後、インデックスファイルが（第１）のマッピングファイルに対してマッピングされる。この「第２」マッピング又はインデックスファイルは、最も安全に格納されるべきであり、可能であれば、オフラインで、好ましくは第１マッピングファイルと異なる暗号化方法で暗号化される。好ましくは、本明細書記載の任意の実施形態において、マッピングファイル又はその少なくとも一部は、ブロックチェーン又は分散型台帳に格納される。

【００７７】

図３は、生体特徴ファイル等の電子データ及び／又はその他任意の種類のファイルを分割して格納するための、他の図同様、以下のステップを実行し得る、例示的ルーチン３００を示す。

【００７８】

ステップ３０２において、システムは、電子データを（２つ以上の）フラグメントに分割してもよい。各フラグメントは、格納される電子データの１又は複数のブロック、１又は複数のスライス、又はその他の１又は複数の断片であるファイル（「ファイルフラグメント」）である。システムはまた、フラグメントファイルの順序を示してもよい（インデックス順番付け）。生体特徴ファイルに対して、システムは、ファイルを特徴ブロック等

のフラグメントに分割して、インデックス順番付けをしてもよい。電子データから生成されたフラグメントファイルは、電子ファイル又はその他電子データの、データ及び／又は画像及び／又音声及び／又は動画の一部を含んでもよい。いくつかの実施形態では、フラグメントファイルは、ファイルヘッダ又はその一部を含んでもよい。このステップの一部として、システムは更に、上述のファイルフラグメントを１又は複数ブロックチェーンに格納して１又は複数ブロックチェーン外に格納したり、１又は複数分散型台帳に格納して１又は複数分散型台帳外に格納したり、１又は複数分散型データベースに格納して１又は複数分散型データベース外に格納したりしてもよい（以下のステップ３１０参照）。

【００７９】

ステップ３０４において、システムは、元ファイルの再構築のためにインデックスファイルを生成してもよい。

【００８０】

ステップ３０６において、システムは、任意でインデックスファイルを暗号化してもよい。

【００８１】

ステップ３０８において、システムは、インデックスファイルを格納してもよい（後にファイルを再構築するため）。システムは、インデックスファイルをブロックチェーン又はブロックチェーン外のストレージに格納してもよく、好ましくはブロックチェーン上の全てのノードに分散された位置データのハッシュテーブルを使用してもよい。この際、例えばインデックスファイルはブロックチェーン外に格納される。本項記載の別の実施形態では、インデックスファイルそのものは分割され、好ましくは部分的にブロックチェーンに格納され部分的にブロックチェーン外に格納されたり、部分的に分散型台帳に格納され部分的に分散型台帳外に格納されたり、部分的に分散型データベースに格納され部分的に分散型データベース外に格納されたりする。

【００８２】

ステップ３１０において、システムは、電子データのフラグメント又はフラグメント群の内の任意の選択されたもの（ランダムに選択することが最も好ましいが、疑似ランダム又は所定の方法で選択されてもよい）を、格納してもよい。当該電子データは、ブロックチェーン、分散型台帳、分散型データ外のストレージに安全に格納されるものである。当該ストレージは、１又は複数のセキュアサーバ（例えばエンティティ又は個人所有）、及び／又は１又は複数のクライアントデバイスを含む。例えば、クライアントデバイスは、ユーザの携帯電話、タブレット、ノートＰＣ、デスクトップＰＣ、又はその他ユーザデバイスである。１又は複数のフラグメントは、通常は自身のＣＰＵを持たないＳＩＭカード、ＵＳＢサムドライブ等の、１又は複数のその他デジタル記憶装置、又はその他適切な装置に格納されてもよい。本明細書記載の全ての実施形態同様、あるステップが他のステップに関連して実行されるタイミングは、齟齬がない限り変更できる。

【００８３】

システムは、電子データの少なくとも１のフラグメントを、ブロックチェーン、分散型台帳、又は分散型データベースに格納できる。この１又は複数のフラグメントは、ファイル（電子データ）を機械又は人にとって意味を成すファイル（即ち、少なくとも一部理解可能な部分が存在する）に再構築するために必要である。例えば、本明細書記載の任意の実施形態のように、この少なくとも１のフラグメントは、安全に格納されたファイルのヘッダ部分又はヘッダの一部で、ファイルのその他部分を含んでも含まなくてもよい。この少なくとも１のフラグメントはまた、好ましくは、電子データが当該フラグメント無しでは成立しないことを前提にした上で、可能な限り小さいサイズ（バイト単位）ことが、データ格納上好ましい。これにより、ブロックチェーンシステムへの格納、抽出負荷が最小限にとどめられる。システムは任意で、ブロックチェーン、分散型台帳、又は分散型データベースの別々のストレージに、複数のフラグメントを格納してもよい。後述の図３Ａに、このような格納ステップを概略的に示す。

【００８４】

本明細書記載の全ての実施形態では、システムは、ブロックチェーンに１又は複数のフラグメントを格納する際に、当該フラグメントを、ブロックチェーン上の複数のブロック（例えば、トランザクション）に格納してもよい。システムは、分散型台帳に１又は複数のフラグメントを格納する際に、当該フラグメントを、分散型台帳上の複数の位置（例えば、トランザクション）に格納してもよい。或いは、システムは、分散型データベースに１又は複数のフラグメントを格納する際に、当該フラグメントを、分散型データベースの複数の箇所に格納してもよい。システム、ブロックチェーン、分散型台帳及び／又は分散型データベースは更に、格納された１又は複数のフラグメントを更に分解し、得られたフラグメントをネットワークデータストアにおけるデータストリームとして、複数のブロックチェーンノード、分散型台帳ノード、分散型データストレージノードに分散するように構成されてもよい。好ましくは、ファイルフラグメントを利用して再構築を行うためにブロックチェーンノード、分散型台帳ノード、分散型データストレージノード又はネットワークデータストアにアクセスするためには、認証が必要となり、秘密鍵とトランザクションアドレス又はスマートコントラクトアドレスが必要である。安全性向上のために、トランザクションアドレス又はスマートコントラクトアドレスは、時間に基づき定期的に更に／或いは使用毎に更新されてもよい。

【００８５】

図３Ａは、任意のファイルタイプの格納のための例示的処理を示す概略的フローチャートである。これは、図２Ａ及び４Ａのプロセスの一部であってもよく、図３のステップ３１０の詳細としてとらえられる。

【００８６】

ステップ３１２において、システムは、分割、格納されるファイルを受信できる。ステップ３１４において、システムは、ファイルをフラグメントに分割してもよい。ステップ３１６において、システムは、フラグメントの内の少なくとも１をブロックチェーン、分散型台帳、又は分散型データベースに格納し、残りのフラグメントをブロックチェーン、分散型台帳、分散型データ外のストレージ（ボックス３１６Ａにまとめる）に格納してもよい。当該ストレージは、１又は複数のクラウドサーバ、１又は複数のセキュアサーバ（例えばエンティティ又は個人所有）、及び／又は１又は複数のクライアントデバイスを含む。例えば、クライアントデバイスは、ユーザの携帯電話、タブレット、ノートＰＣ、デスクトップＰＣ、又はその他ユーザデバイスである（ボックス３１６Ｂにまとめる）。１又は複数のフラグメントは、通常は自身のＣＰＵを持たないＳＩＭカード、ＵＳＢサムドライブ等の、１又は複数のその他デジタル記憶装置、又はその他適切な装置に格納されてもよい。

【００８７】

図４は、他図ではルーチン３００の代わりに使用され得る、例えば生体特徴ファイル等の電子データを分割、格納するためのルーチン４００の例を示す。

【００８８】

ステップ４０２において、上述のステップ２０２と同様に、システムは生体特徴を特徴ブロックに分割し、生体特徴ファイルの各特徴ブロックにインデックス番号を付してもよい。このインデックス番号は、任意でインデックス付け処理の一環として、ランダム化されてもよい。但し、本明細書の任意の実施形態のように、疑似ランダムに選択されても、所定の方法で選択されてもよい。

【００８９】

任意のステップ４０４において、上述のステップ２０２と同様に、システムは特徴ブロックを変換してもよい。システムは、変換データ（例えば、フリップ／回転情報）を記録する。

【００９０】

ステップ４０６において、上記ステップ２０６と同様、システムは、各特徴ブロックのインデックス番号、変換データ、幾何学的位置をマッピングする。

【００９１】

ステップ４０８において、システムは、直前のステップ４０６で収集されたインデックス番号、変換データ、幾何学的位置のマッピングファイル（又はマッピングデータファイル）を生成する。

【００９２】

任意のステップ４１０において、システムは、マッピングデータを暗号化する。マッピングファイルの暗号化は、ＡＥＳアルゴリズム、ＰＧＰアルゴリズム、Ｂｌｏｗｆｉｓｈアルゴリズム、又はその他適切な暗号化アルゴリズムにより実現されてもよい。

【００９３】

ステップ４１１において、システムは上述のように、図３に詳細に示した処理３００により、マッピングファイルを分割（任意）し、格納する。本項記載のその他実施形態において、第１マッピング及び／又はインデックスファイルそのものが、元ファイルの分割、格納と同様の処理で、分割されてもよい。より安全性を追求するため、一部はオンライン（例えばブロックチェーン上、又はブロックチェーン外）に格納され、及び／又は部分的にオフラインで格納される。

【００９４】

ステップ４１２において、システムは、ランダムに特徴ブロックの一部（例えば特徴ブロックの３０％）を選択し、それをランダムな順序（或いは疑似ランダム又は所定の順序）で、二次元又は多次元に再構築する。

【００９５】

このステップは、ステップ４１４、４１６、４１８、３００、４２０、４２２、４２４、３００により、多数回実行されてもよい。これにより、多数のＳＰＢＦ、選択ブロック、幾何学的データファイルが得られる。

【００９６】

具体的には、ステップ４１４において、システムは、特徴ブロックの再構築順序データを、再構築順序データファイルとして記録してもよい。

【００９７】

ステップ４１６において、システムは、再構築順序データファイルを暗号化してもよい。再構築順序データファイルの暗号化は、ＡＥＳアルゴリズム、ＰＧＰアルゴリズム、Ｂｌｏｗｆｉｓｈアルゴリズム、又はその他適切な暗号化アルゴリズムにより実現されてもよい。

【００９８】

ステップ４１８において、システムは、選択ブロックデータと幾何学的データファイルを、処理３００等により、分割、格納してもよい。

【００９９】

ステップ４２０において、システムは、特徴ブロックを再構築し、新たなファイルを生成することでスクランブル部分生体特徴（ＳＰＢＦ）を生成してもよい。

【０１００】

任意のステップ４２２において、システムは、ＳＰＢＦ生体特徴ベクトルを抽出してもよい。

【０１０１】

任意のステップ４２４において、システムは、ＳＰＢＦファイル又はＳＰＢＦ生体特徴ベクトルファイルを暗号化／ハッシュしてもよい。

【０１０２】

ステップ４２６において、上述の処理３００同様、システムは、処理３００で説明した処理ステップにより、ＳＰＢＦ（ＳＰＢＦベクトル）ファイルを分割、格納してもよい。

【０１０３】

図４Ａは、生体特徴画像を格納する別の例示的処理の、概略的フローチャートを示す。ステップ４２８において、システムは、（図４の処理開始として）生体特徴の画像を受信する。ステップ４３０（図４のステップ４０２同様）において、システムは、画像をブロック（特徴ブロック）に分割してもよい。ステップ４３２（ステップ４０４、４０６、４

１２，４２０，４２２同様）において、システムは、集められるいくつかの特徴ブロックを選択してもよい（例えば、ランダムに選択することで高い安全性となるが、疑似ランダム又は非ランダムに選択してもよい）。当該プロセスにおいて、システムは、特徴ブロックを（例えば９０°又はランダムな角度で回転させることで）変換する。ステップ４３８において、システムは、選択生体特徴ブロック及び再構築順序データファイルを生成する（図４のステップ４１４，４１６同様）。その後、１又は複数の選択生体特徴ブロック及び再構築順序データファイルは、ステップ４４２及び４４４において、分割されてもよく、ファイルフラグメントは部分的にブロックチェーン、分散型台帳、又は分散型データベースに格納され、部分的にブロックチェーン、分散型台帳、又は分散型データ外のストレージに格納される。当該ストレージは、１又は複数のクラウドサーバ、１又は複数のセキュアサーバ、及び／又は１又は複数のクライアントデバイスを含む。例えば、クライアントデバイスは、ユーザの携帯電話、タブレット、ノートＰＣ、デスクトップＰＣ、又はその他ユーザデバイスである。ボックス４４４Ａは、ブロックチェーン、分散型台帳、又は分散型データベースのストレージオプションを示す。ボックス４４４Ｂは、ブロックチェーン、分散型台帳、及び／又は分散型データベース外のストレージオプションを示す。１又は複数のフラグメントは、通常は自身のＣＰＵを持たないＳＩＭカード、ＵＳＢサムドライブ等の、１又は複数のその他デジタル記憶装置、又はその他適切な装置に格納されてもよい。（任意の）ステップ４３３において、システムは、部分生体特徴ファイルから生体特徴ベクトルを抽出できる。次にステップ４３４において（図４のステップ４２４同様）、又はステップ４３６（図４のステップ４２４同様）において、システムは、選択的に任意で暗号化又はハッシュ化をそれぞれＳＰＢＦファイル、ＳＰＢＦ生体特徴ベクトルファイル、又はステップ４３２で生成されたファイルに適用してもよい。ステップ４４０において、システムは、生体特徴マッピングファイルを生成してもよい（任意で暗号化してもよい）（図４のステップ４０８、４１０同様）。ステップ４４２において、システムは、１又は複数のマッピングファイルをフラグメントに分割してもよい（図４のステップ４１１，４１８，４２６及び図３の処理３００同様）。ステップ４４４において、システムは、ファイルフラグメントを部分的にブロックチェーン、分散型台帳、又は分散型データベースに格納し、部分的にブロックチェーン、分散型台帳、又は分散型データ外のストレージに格納してもよい。当該ストレージは、１又は複数のクラウドサーバ、１又は複数のセキュアサーバ、及び／又は１又は複数のクライアントデバイスを含む（図４のステップ４１１，４１８，４２６、図３の処理３００と同様）。１又は複数のフラグメントは、通常は自身のＣＰＵを持たないＳＩＭカード、ＵＳＢサムドライブ等の、１又は複数のその他デジタル記憶装置、又はその他適切な装置に格納されてもよい。

【０１０４】

生体特徴ファイルが安全に格納されると、ユーザが生体特徴へのアクセスを望むか、システムが生体特徴又はＳＰＢＦファイルにアクセスして、ユーザの生体特徴又はＳＰＢＦと比較することでユーザ認証を行う必要があり得る。

【０１０５】

図１５は、安全に格納された電子データを、ユーザが取得するためのリクエストの処理を示す。ステップ１５０２において、システムは、ユーザのサインインリクエストを、ＡＰＩを介して受信してもよい。ステップ１５０４において、システムは、ユーザを、例えばユーザが格納した生体特徴情報、及び登録プロセス中に記録されたその他（１以上の）識別子を使用して認証してもよい。ステップ１５０６において、システムは、ユーザの取得リクエストを受信してもよい。ステップ１５０８において、システムは、ストレージからユーザの電子データのフラグメントを取得してもよい。ステップ１５１０において、システムは、ファイルフラグメントを１以上のファイルに再構築してもよい。ステップ１５１２において、例えば、表示又はリードオンリーで、ダウンロード可能として、及び／又はその他手段により、システムは当該（１以上の）ファイルをユーザに返信してもよい。

【０１０６】

図５は、生体特徴ファイル等の安全に格納されたファイルを取得し、再構築する方法の

１つを示す。ステップ５０２において、システムは、マッピングファイル及び位置インデックスファイルを取得してもよい。

【０１０７】

ステップ５０４において、システムは、マッピングファイル位置インデックスファイルを復号化してもよい。

【０１０８】

ステップ５０６において、システムは、マッピング分割ファイル、及びマッピングインデックスファイルを、マッピングファイル位置インデックファイルを使用して読み出してもよい。

【０１０９】

任意のステップ５０８において、システムは、マッピングインデックスファイルを復号化してもよい。

【０１１０】

ステップ５１０において、システムは、マッピングインデックスファイルとマッピング分割ファイルを使用して、マッピングファイルを再構築してもよい。

任意のステップ５１２において、システムは、マッピングファイルを復号化してもよい。

【０１１１】

ステップ５１４において、システムは、ＳＰＢＦインデックスファイルとＳＰＢＦ分割ファイルを読み出してもよい。

【０１１２】

任意のステップ５１６において、システムは、ＳＰＢＦインデックスファイルを復号化してもよい。

【０１１３】

ステップ５１８において、システムは、ＳＰＢＦインデックスファイルとＳＰＢＦ分割ファイルを使用して、ＳＰＢＦファイルを再構築してもよい。

【０１１４】

任意のステップ５２０において、システムは、ＳＰＢＦファイルを復号化してもよい。

【０１１５】

ステップ５２２において、システムは、マッピングファイルとＳＰＢＦファイルを使用して、部分生体特徴を再構築してもよい。

【０１１６】

ステップ５２４において、システムは、２以上の部分生体特徴を使用して、完全な生体特徴を再構築してもよい。

【０１１７】

或いは、図６の処理により、元のＳＰＢＦを再構築してもよい。

【０１１８】

ステップ６０２において、システムは、マッピングファイル位置インデックスファイルを取得してもよい。

【０１１９】

任意のステップ６０４において、システムは、マッピングファイル位置インデックスファイルを復号化してもよい。

【０１２０】

ステップ６０６において、システムは、マッピングファイル位置インデックスファイルを使用して、マッピング分割ファイルとマッピングインデックスファイルを取得してもよい。

【０１２１】

任意のステップ６０８において、システムは、マッピングインデックスファイルを復号化してもよい。

【０１２２】

ステップ６１０において、システムは、マッピングインデックスファイルとマッピング

分割ファイルを使用して、マッピングファイルを再構築してもよい。
【０１２３】
任意のステップ６１２において、システムは、マッピングファイルを復号化してもよい。
【０１２４】
ステップ６１４において、システムは、ＳＰＢＦ分割ファイル位置インデックスファイルを読み出してもよい。
【０１２５】
任意のステップ６１６において、システムは、ＳＰＢＦ分割ファイル位置インデックスファイルを復号化してもよい。
【０１２６】
ステップ６１８において、システムは、ＳＰＢＦ分割ファイル位置インデックスファイルを使用して、ＳＰＢＦインデックスファイルとＳＰＢＦ分割ファイルを取得してもよい。
【０１２７】
任意のステップ６２０において、システムは、ＳＰＢＦインデックスファイルを復号化してもよい。
【０１２８】
ステップ６２２において、システムは、ＳＰＢＦインデックスファイルとＳＰＢＦ分割ファイルを使用して、ＳＰＢＦファイルを再構築してもよい。
【０１２９】
任意のステップ６２４において、システムは、ＳＰＢＦファイルを復号化してもよい。
【０１３０】
ステップ６２６において、システムは、マッピングファイルとＳＰＢＦファイルを使用して、部分生体特徴を再構築してもよい。生体特徴マッピングファイルは、生体特徴を再構築するのに十分な情報を含んでいるべきである。
【０１３１】
ステップ６２８において、システムは、２以上の部分生体特徴を使用して、完全な生体特徴を再構築してもよい。
【０１３２】
図７は、任意のファイルの一般的な再構築処理の例を示す。
【０１３３】
ステップ７０２において、システムは、ファイル位置インデックスファイルを取得してもよい。任意のステップ７０４において、システムは、ファイル位置インデックスファイルを復号化してもよい。ステップ７０６において、システムは、ファイルインデックスファイルを取得してもよい。任意のステップ７０８において、システムは、ファイルインデックスファイルを復号化してもよい。ステップ７１０において、システムは、ファイル分割ファイルを取得してもよい。ステップ７１２において、システムは、ファイル分割ファイルとインデックスファイルを使用して、ファイルを再構築してもよい。任意のステップ７１４において、システムは、ファイルを復号化してもよい。
【０１３４】
図８は、ファイル削除プロセスの例を示す。ステップ８０２において、システムは、ファイルインデックスファイルを取得してもよい。任意のステップ８０４において、システムは、ファイルインデックスファイルを復号化してもよい。ステップ８０６において、システムは、ファイルインデックスファイルを使用して、適宜１又は複数のフラグメントファイルを削除してもよい（例えばブロックチェーン外のクラウドストレージ、企業サーバ、又はクライアント装置）。
【０１３５】
図９は、暗号化ＳＰＢＦファイルを使用した生体認証処理の例を示す。この生体認証は、ユーザを識別して、安全に格納された（１以上の）ファイルをアクセス可能にする、又

はアクセス権を与えるように実行できる。なお、ＳＰＢＦファイルを使用して、元の生体特徴ファイルの全部又は一部を再構築する場合、当該ＳＰＢＦファイルは格納される前にハッシュ化されないことが好ましい。これは、ハッシュ化は元に戻せないため、再構築できなくなるのである。任意でＳＰＢＦ（暗号化もハッシュ化もされていない）から生体特徴ベクトルを抽出してもよい。生体特徴ベクトルを使用する場合、好ましくは、ハッシュ化は暗号化もハッシ化もされていない生体特徴ベクトルファイル（任意の）に対して行われるべきであり、ＳＰＢＦファイルには行われるべきではない。これは、通常有用な生体特徴ベクトルが１又は複数の暗号化もハッシュ化もされていないＳＰＢＦファイル又は１又は複数の暗号化もハッシュ化もされていない元の生体特徴ファイルからのみ得られるためである。

【０１３６】

図９のステップ９０２において、システムは、人（ユーザ）の生体特徴キャプチャを受信してもよい。これは、生体認証装置により確認されるものである。ステップ９０４において、システムは、上述の図５のプロセス５００又は図６のプロセス６００により、ＳＰＢＦを取得してもよい。ステップ９０６において、システムは、入力された生体特徴と、格納されたＳＰＢＦから再構築された画像又はパターンを比較してもよい。ステップ９０８において、システムは、比較結果として一致又は不一致を返す。

【０１３７】

図１０は、ハッシュ化ＳＰＢＦファイルを使用した生体認証処理の例を示す（例えば、ユーザの認証及び／又はアクセスリクエストに対して実行される）。ステップ１００２において、システムは、入力された生体特徴を、例えば生体特徴取得装置を利用してユーザから受信し、取得した生体特徴情報をシステムに送信する。

【０１３８】

ステップ１００４において、システムは、入力された生体特徴を、ユーザのＳＰＢＦファイルを格納する（例えば、図２，４，４Ａ）の場合と同様の変換方法により、ＳＰＢＦファイルに変換できる。即ち、システムは、元のＳＰＢＦファイル生成中に使用されたマッピングデータ、変換データ、構築順序、インデックスファイルを読み出して、同じ特徴ブロックを選択し、元の格納の際に実行された任意の変換及び構築を実行してもよい。

【０１３９】

ステップ１００６において、システムは、ＳＰＢＦファイルを、ユーザのＳＰＢＦファイルが格納（例えば、図２，４，４Ａ）の際にハッシュ化されたのと同じハッシュ化ルーチンにより、ＳＰＢＦをハッシュ化してもよい。

【０１４０】

ステップ１００８において、システムは、ＳＰＢＦハッシュファイルを格納されたＳＰＢＦハッシュファイルと比較してもよい。

【０１４１】

ステップ１０１０において、システムは、比較結果、即ち一致又は不一致を返し、認証ルーチンの生体特徴部分に、当該結果を使用してもよい。

【０１４２】

図１１は、ＳＰＢＦ生体特徴ベクトルを利用した生体認証処理の例を示す。ステップ１１０２において、システムは、入力された生体特徴を、例えば生体特徴取得装置を利用してユーザから受信し、取得した生体特徴情報をシステムに送信する。

【０１４３】

ステップ１１０４において、システムは、入力された生体特徴を、ユーザのＳＰＢＦファイルを格納する（例えば、図４，４Ａ）の場合と同様の変換方法により、ＳＰＢＦファイルに変換できる。即ち、システムは、元の生体特徴ＳＰＢＦファイル生成中に使用されたマッピングデータ、変換データ、構築順序、インデックスファイルを読み出して、同じ特徴ブロックを選択し、元の格納の際に実行された任意の変換及び構築を実行してもよい。

【０１４４】

ステップ１１０６において、システムは、生体特徴ベクトルが格納の際に抽出されたときと同じ生体特徴ベクトル抽出ルーチンにより、ＳＰＢＦ生体特徴ベクトルを抽出してもよい。

【０１４５】

ステップ１１０８において、システムは、ＳＰＢＦ生体特徴ベクトルファイルを格納されたＳＰＢＦ生体特徴ベクトルファイルと比較してもよい。

【０１４６】

ステップ１１１０において、システムは、比較結果、即ち一致又は不一致を返し、認証ルーチンの生体特徴部分に、当該結果を使用してもよい。

【０１４７】

図１２は、ハッシュ化生体特徴ベクトルファイルを利用した生体認証処理の例を示す。この処理において、ステップ１２０２，１２０４，１２０６は、図１１のステップ１１０２，１１０４，１１０６と同じである。

【０１４８】

ステップ１２０８において、システムは、新たに形成されたＳＰＢＦ（例えば、ユーザから新たに取得）から得られた生体特徴ベクトルファイルを、得られていた元のＳＰＢＦ生体特徴ベクトルを格納する際と同じハッシュ機能を使用して、ハッシュ化してもよい。

【０１４９】

ステップ１２１０において、システムは、ＳＰＢＦ生体特徴ハッシュファイルを格納された生体特徴ＳＰＢＦハッシュファイルと比較してもよい。

【０１５０】

ステップ１２１２において、システムは、比較結果、即ち一致又は不一致を返し、認証ルーチンの生体特徴部分に、当該結果を使用してもよい。

【０１５１】

本項に記載のように、セキュアストレージシステムの適用は多数存在する。当該適用の１つとして、システム１００は、１又は複数の個人の身元を認証するための１又は複数のリクエストに応じて、１又は複数の識別子を受信するように構成されてもよい。システムは、図１に示す身元認証要素１２０を利用して、当該リクエストに応えてもよい。例えば、上述の第１の識別子は、第１の個人の個人身元のリクエストに応じて受信されてもよい。金融取引、情報交換、及び／又はその他のインタラクションに応じて及び／又はこれらに関して、個人身元認証リクエストが出されてもよい。リクエストは、その他個人及び／又はその他第三者から受信されてもよい。

【０１５２】

システム１００は、１以上の個人に関連付けられた生体特徴データを、対応する認証アドレスから抽出するように構成されてもよい。例えば、第１の個人に関連付けられた第１の生体特徴データが、第１の認証アドレスから抽出されてもよい。認証アドレスからの情報（例えば、生体特徴データ）の抽出は、情報の暗号化を含んでもよい。

【０１５３】

いくつかの形態によると、システム１００は、第１の個人の身元認証リクエストの受信に応じて、第１の個人に第１の生体特徴データに一致する生体特徴データ及び第１の秘密鍵に一致する秘密鍵の提供を要求するように構成されてもよい。要求は、第１の個人に関連付けられたコンピューティングプラットフォーム１０４を介して伝えられてもよい。要求は、第１の個人に関連付けられたコンピューティングプラットフォーム１０４により提供されるグラフィカルユーザインタフェース及び／又はその他のユーザインタフェースを介して伝えられてもよい。要求は、視覚的標示、聴覚的標示、触覚的標示及び／又はその他の標示の内の１以上である標示を含んでもよい。

【０１５４】

いくつかの形態では、システム１００は、第１の個人の身元認証リクエストの受信に応じて、第１の個人に関連付けられたコンピューティングプラットフォーム１０４に要求が提供されるように構成されてもよい。要求は、コンピューティングプラットフォーム１０

４に、（１以上の）サーバ１０２に対して第１の生体特徴データに一致する生体特徴データ及び／又は第１の秘密鍵に一致する秘密鍵を自動的に提供させるものであってもよい。

【０１５５】

システム１００は、一致する生体特徴データ及び秘密鍵の受信に際して、又は応じて、１以上の個人の身元を認証するように構成されてもよい。例えば、第１の個人の個人身元は、（ｉ）第１の生体特徴データに一致する生体特徴データ及び（ｉｉ）第１の秘密鍵に一致する秘密鍵の受信に際して、認証されてもよい。第１の個人の個人身元の認証は、格納された情報を新たに受信した情報と比較することを含んでもよい。いくつかの形態によると、識別システム１００は、第１の個人の個人身元が、（ｉ）第１の生体特徴データ又は第２の生体特徴データに一致する生体特徴データ及び（ｉｉ）第１の秘密鍵に一致する秘密鍵の受信に際して、認証されるように構成されてもよい。このような形態では、個人認証用の、より大きな識別情報群のサブセットが求められる、いわゆる「Ｍ－ｏｆ－Ｎ」署名が実現されうる。

【０１５６】

いくつかの形態では、システム１００は、第１の生体特徴データに一致する生体特徴データと、第１の秘密鍵に一致する秘密鍵が、第１の個人の個人身元の認証のための、スマートコントラクトの署名に使用されるように構成されてもよい。

【０１５７】

いくつかの形態では、少なくとも１の専用ノードが、第１の個人又はユーザの個人身元の認証用にスマートコントラクトの署名を実行する。所与の専用ノードは、１以上のサーバ１０２を含んでもよい。所与の専用ノードは、新たなトランザクションを生成する、及び／又は認証のためにスマートコントラクト署名用に構成されたパブリックノード又はプライベートノードであってもよい。

【０１５８】

図１６は、１又は複数の形態に係わる、適用されたブロックチェーンの例の概要１６００を示す。図示のように、ブロックチェーンアクセス、分散型台帳アクセス、又は分散型データベースアクセスの承認管理層と機能し得るプライベート層１６０２を使用し得る。これは、例えば、管理用に、イーサリアムブロックチェーン（例えば、ブロックチェーン）、ハイパーレジャー分散型台帳（例えば分散型台帳１６０６）上に構築されてもよい。図示のように、ファイル（例えば、生体特徴データ及びその他ファイル）を格納するための機構が存在してもよい。これら要素は、ＲＥＳＴｆｕｌＡＰＩのようなＡＰＩ（アプリケーションプログラミングインタフェース）１６０４、及び例えばブロックチェーンデータベース１６０８に接続され、ビッグチェーンＤＢのようなストレージの提供及び／又は改善が実現されてもよい。これは、例えばバイオメトリックアップリケーション又はウェブサイト等に接続され得る。更に別の構成も採用可能である。

【０１５９】

例示的形態は、個人データにアクセスしやすくし得る。ブロックチェーンにおける個人データに対して、様々なアクセスレベルがあり得る。アクセス制御は、公開／秘密鍵組のレベルで、可能にできる。アクセスレベルの例としては、ネットワーク管理者（ブロックチェーンに対する無制限アクセス）、国家レベルの当局（無制限のリードオンリーアクセス）、州／地方レベルの当局（制限されたリードオンリーアクセス）、緊急対応に係わる警察及び救急隊を含むその他サービス（個人の指紋／網膜により、対応する所与の個人データへのアクセス）、参加店舗（限定的アクセス）、及び／又はその他のアクセスレベルが挙げられる。

【０１６０】

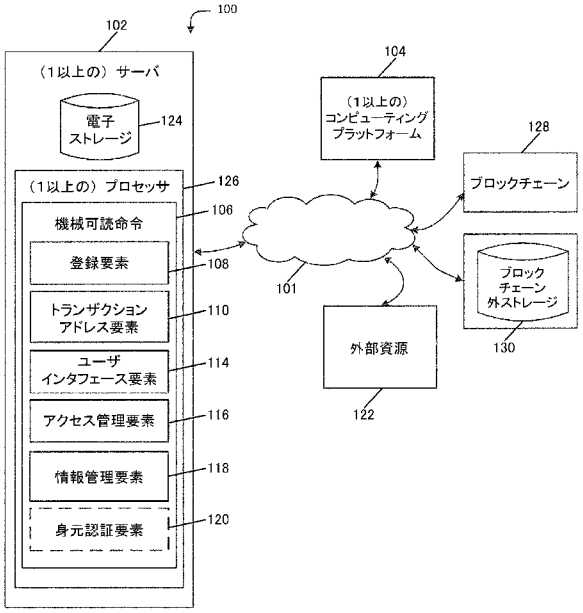
これらの態様は、（個人及び／又はクライアントのバイオメトリックアイデンティティに関するかどうかに関わらず）ブロックチェーン内で処理、照合、及び／又は保持されるモバイルデータに関連してもよい。

【０１６１】

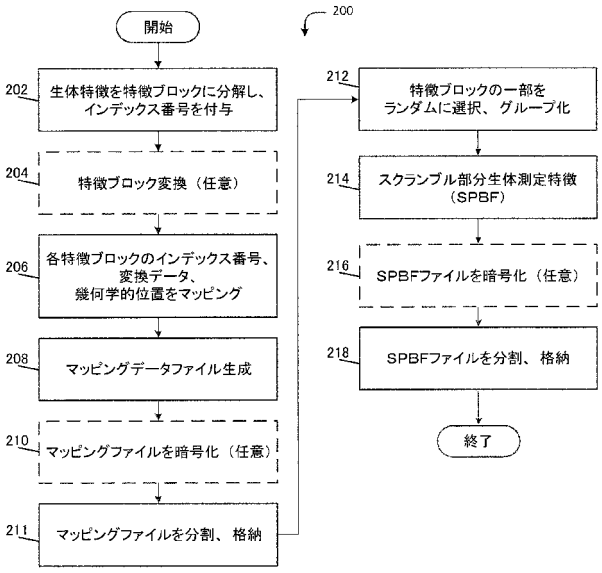
本技術は、現状最も実践的で好ましい形態と考えられるものに基づき例示的に詳細を説

明した。但し、この詳細は、あくまで例示的であって、本技術は開示された形態に限定されるものではなく、添付の請求項の精神及び範囲に含まれる変形例や、同一の構成も網羅するものである。例えば、本技術は、任意の形態の１以上の特徴は、その他任意形態の１以上の特徴と組み合わせ可能であることが想定されていることが理解されよう。

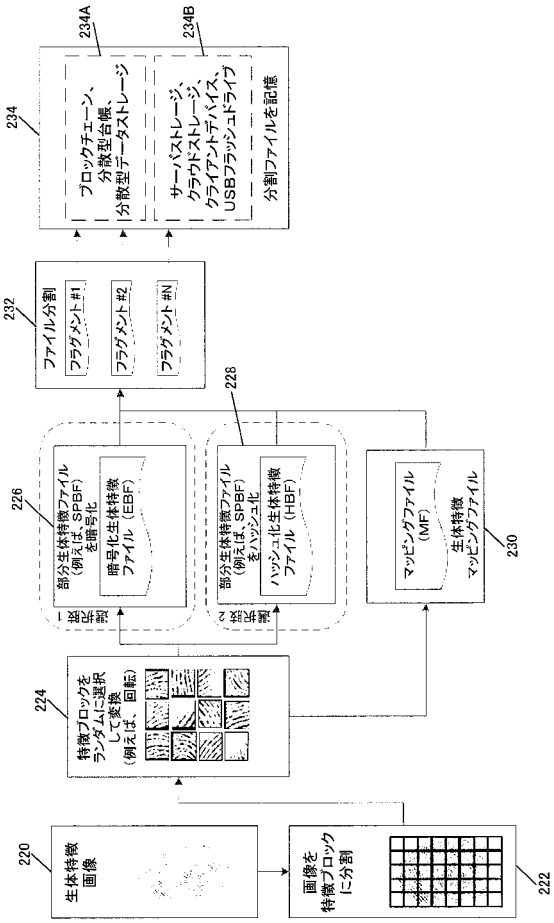
【図１】



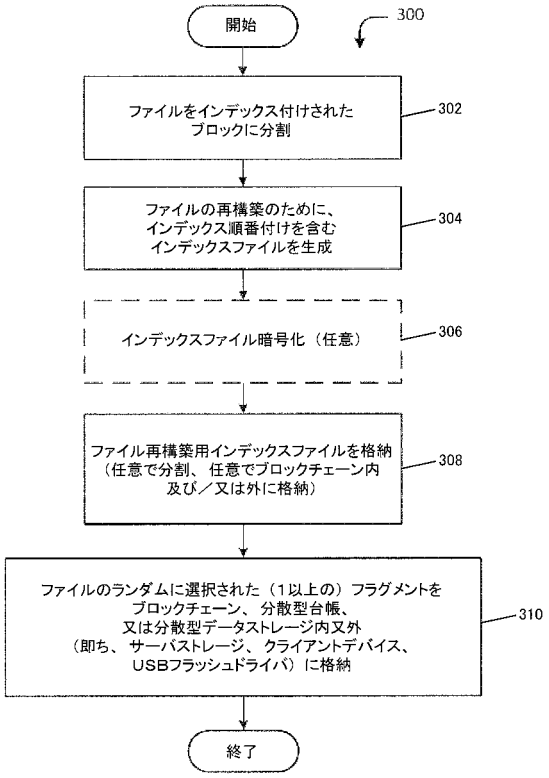
【図２】



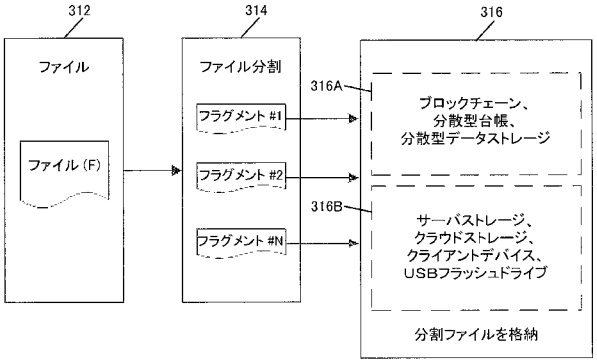
【図２Ａ】


234A
234B
234
ブロックチェーン、
分散型台帳、
分散型データストレージ
サーバストレージ、
クラウドストレージ、
クライアントデバイス、
USBフラッシュドライブ
分割ファイルを記憶
232
ファイル分割
フラグメント #1
フラグメント #2
フラグメント #N
228
226
部分生体特徴ファイル
（例えば、SPBF）
を暗号化
暗号化生体特徴
ファイル（EBF）
部分生体特徴ファイル
（例えば、SPBF）
をハッシュ化
ハッシュ化生体特徴
ファイル（HBF）
マッピングファイル
（MF）
生体特徴
マッピングファイル
230
224
特徴ブロックを
ランダムに選択
して変換
（例えば、回転）
220
生体特徴
画像
画像を
特徴ブロック
に分割
222

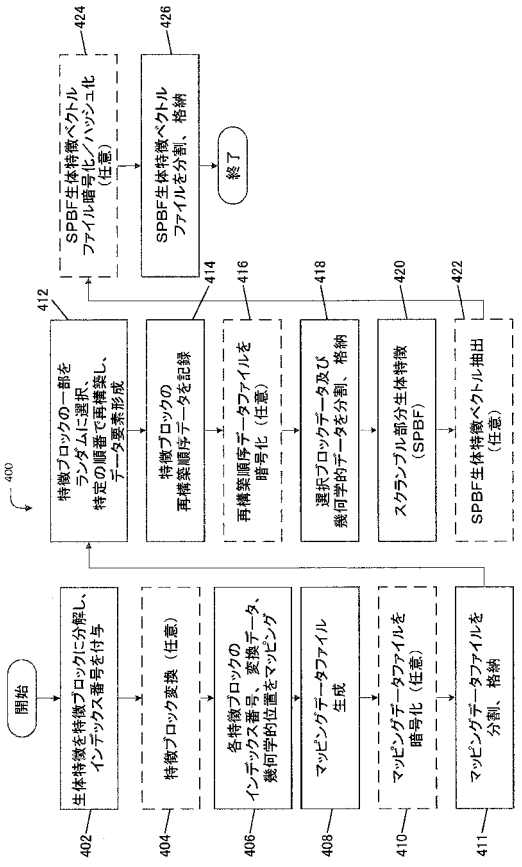
【図３】


開始
300
ファイルをインデックス付けされた
ブロックに分割
302
ファイルの再構築のために、
インデックス順番付けを含む
インデックスファイルを生成
304
インデックスファイル暗号化（任意）
306
ファイル再構築用インデックスファイルを格納
（任意で分割、任意でブロックチェーン内
及び／又は外に格納）
308
ファイルのランダムに選択された（1以上の）フラグメントを
ブロックチェーン、分散型台帳、
又は分散型データストレージ内又外
（即ち、サーバストレージ、クライアントデバイス、
USBフラッシュドライバ）に格納
310
終了

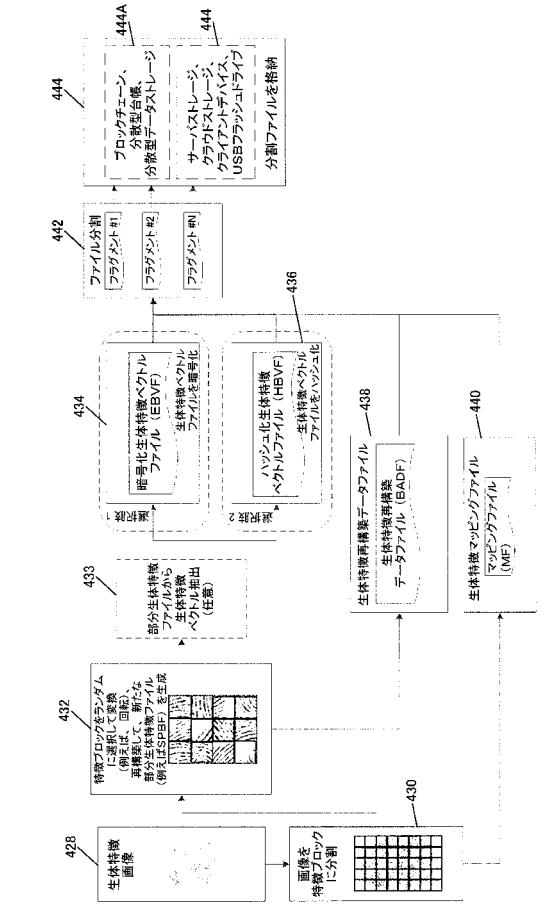
【図３Ａ】


312
ファイル
ファイル（F）
314
ファイル分割
フラグメント #1
フラグメント #2
フラグメント #N
316
316A
316B
ブロックチェーン、
分散型台帳、
分散型データストレージ
サーバストレージ、
クラウドストレージ、
クライアントデバイス、
USBフラッシュドライブ
分割ファイルを格納

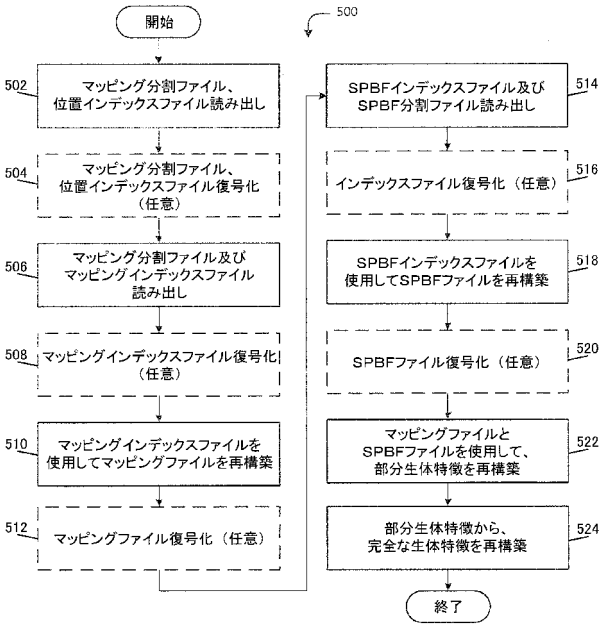
【図４】


424
SPBF生体特徴ベクトル
ファイル暗号化／ハッシュ化（任意）
426
SPBF生体特徴ベクトル
ファイルを分割、格納
終了
400
412
414
416
418
420
422
特徴ブロックの一部を
ランダムに選択、
特定の順番で再構築し、
データ要素形成
特徴ブロックの
再構築順序データを記録
再構築順序データファイルを
暗号化（任意）
選択ブロックデータ及び
幾何学的データを分割、格納
スクランブル部分生体特徴
（SPBF）
SPBF生体特徴ベクトル抽出
（任意）
開始
生体特徴を特徴ブロックに分解し、
インデックス番号を付与
特徴ブロック変換（任意）
各特徴ブロックの
インデックス番号、変換データ、
幾何学的位置をマッピング
マッピングデータファイル
生成
マッピングデータファイルを
暗号化（任意）
マッピングデータファイルを
分割、格納
402
404
406
408
410
411

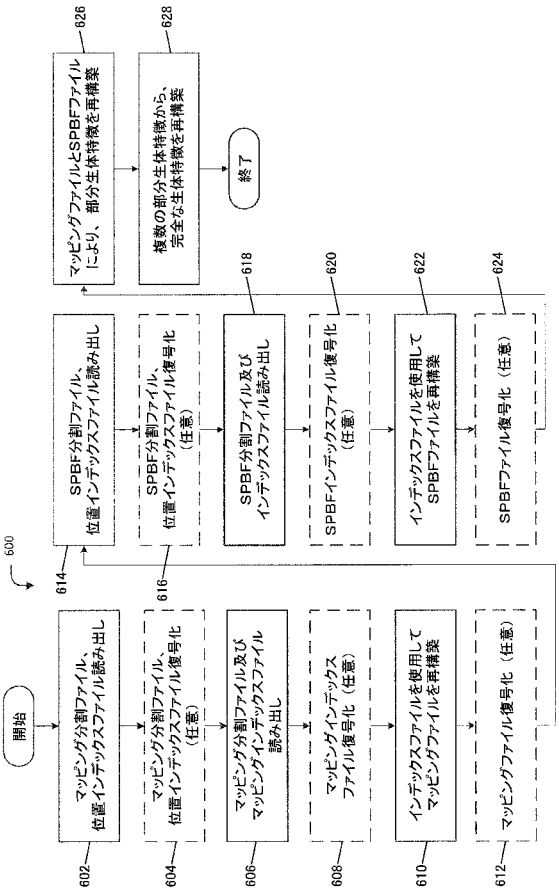
【図４Ａ】


444A
444
ブロックチェーン、分散型台帳、分散型データストレージ
サーバストレージ、クラウドストレージ、クライアントデバイス、USBフラッシュドライブ
分割ファイルを格納
442
ファイル分割
フラグメント #1
フラグメント #2
フラグメント #N
436
434
暗号化生体特徴ベクトルファイル（EBVF）
生体特徴ベクトルファイルを暗号化
ハッシュ化生体特徴ベクトルファイル（HBVF）
生体特徴ベクトルファイルをハッシュ化
438
生体特徴再構築データファイル
生体特徴再構築データファイル（BADF）
440
生体特徴マッピングファイル
マッピングファイル（MF）
433
部分生体特徴ファイルから生体特徴ベクトル抽出（任意）
432
特徴ブロックをランダムに選択して変換（例えば、回転）、新たな再構築して、新たな部分生体特徴ファイル（例えばSPBF）を生成
430
428
生体特徴画像
画像を特徴ブロックに分割

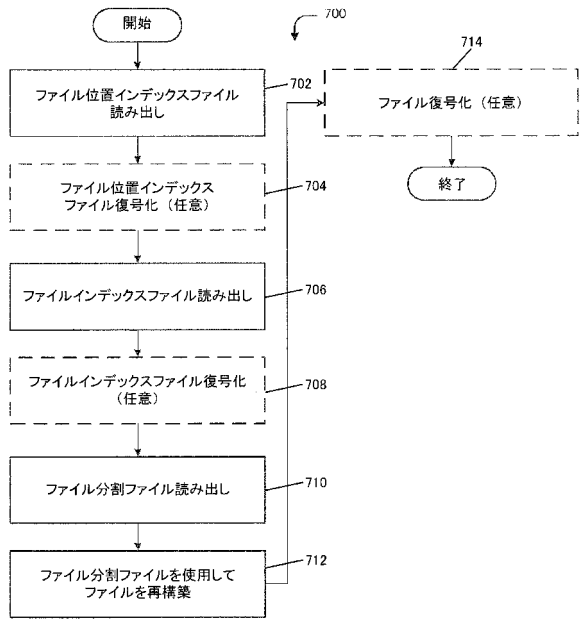
【図５】


500
開始
502
マッピング分割ファイル、位置インデックスファイル読み出し
504
マッピング分割ファイル、位置インデックスファイル復号化（任意）
506
マッピング分割ファイル及びマッピングインデックスファイル読み出し
508
マッピングインデックスファイル復号化（任意）
510
マッピングインデックスファイルを使用してマッピングファイルを再構築
512
マッピングファイル復号化（任意）
514
SPBFインデックスファイル及びSPBF分割ファイル読み出し
516
インデックスファイル復号化（任意）
518
SPBFインデックスファイルを使用してSPBFファイルを再構築
520
SPBFファイル復号化（任意）
522
マッピングファイルとSPBFファイルを使用して、部分生体特徴を再構築
524
部分生体特徴から、完全な生体特徴を再構築
終了

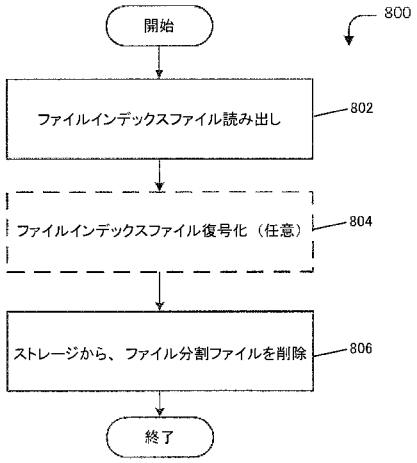
【図６】


600
開始
602
マッピング分割ファイル、位置インデックスファイル読み出し
604
マッピング分割ファイル、位置インデックスファイル復号化（任意）
606
マッピング分割ファイル及びマッピングインデックスファイル読み出し
608
マッピングインデックスファイル復号化（任意）
610
インデックスファイルを使用してマッピングファイルを再構築
612
マッピングファイル復号化（任意）
614
SPBF分割ファイル、位置インデックスファイル読み出し
616
SPBF分割ファイル、位置インデックスファイル復号化（任意）
618
SPBF分割ファイル及びインデックスファイル読み出し
620
SPBFインデックスファイル復号化（任意）
622
インデックスファイルを使用してSPBFファイルを再構築
624
SPBFファイル復号化（任意）
626
マッピングファイルとSPBFファイルにより、部分生体特徴を再構築
628
複数の部分生体特徴から、完全な生体特徴を再構築
終了

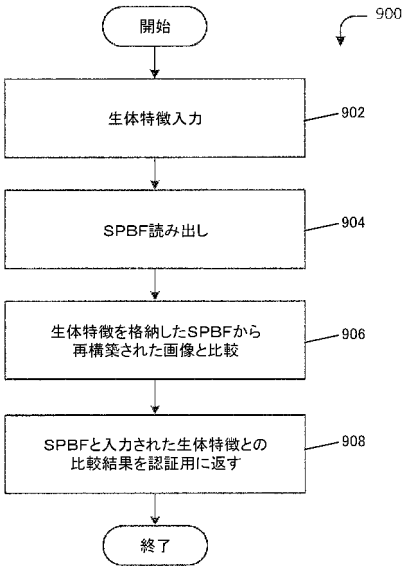
【図７】


700
開始
ファイル位置インデックスファイル読み出し
702
ファイル位置インデックスファイル復号化（任意）
704
ファイルインデックスファイル読み出し
706
ファイルインデックスファイル復号化（任意）
708
ファイル分割ファイル読み出し
710
ファイル分割ファイルを使用してファイルを再構築
712
714
ファイル復号化（任意）
終了

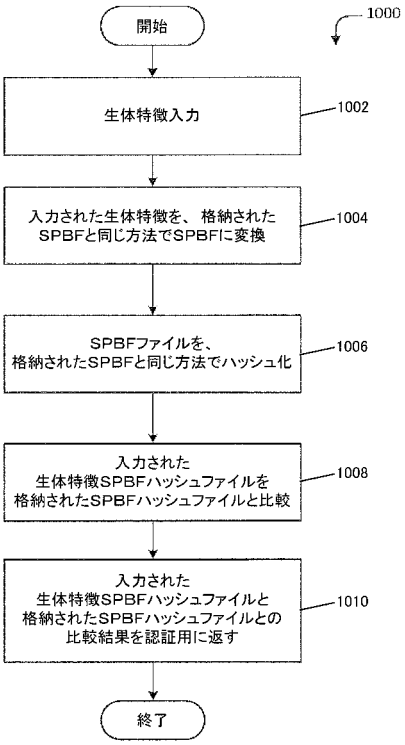
【図８】


開始
800
ファイルインデックスファイル読み出し
802
ファイルインデックスファイル復号化（任意）
804
ストレージから、ファイル分割ファイルを削除
806
終了

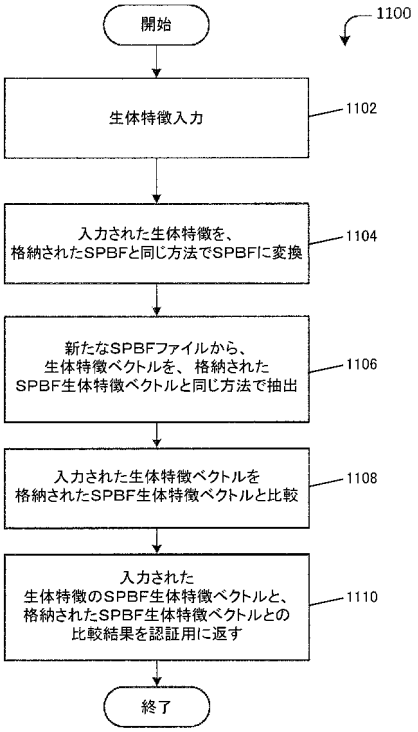
【図９】


開始
900
生体特徴入力
902
SPBF読み出し
904
生体特徴を格納したSPBFから
再構築された画像と比較
906
SPBFと入力された生体特徴との
比較結果を認証用に返す
908
終了

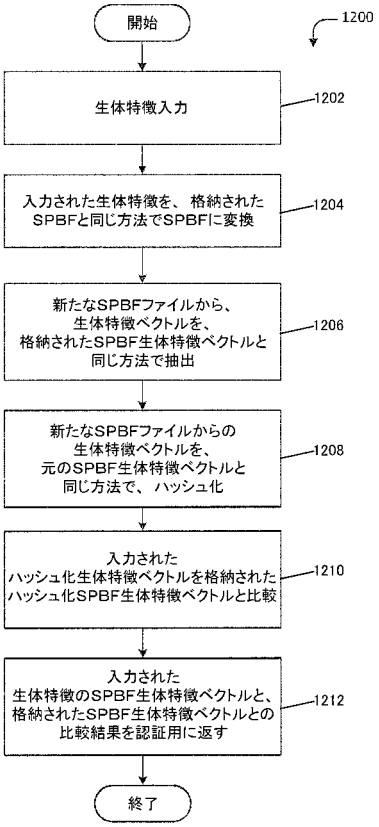
【図１０】


開始
1000
生体特徴入力
1002
入力された生体特徴を、格納された
SPBFと同じ方法でSPBFに変換
1004
SPBFファイルを、
格納されたSPBFと同じ方法でハッシュ化
1006
入力された
生体特徴SPBFハッシュファイルを
格納されたSPBFハッシュファイルと比較
1008
入力された
生体特徴SPBFハッシュファイルと
格納されたSPBFハッシュファイルとの
比較結果を認証用に返す
1010
終了

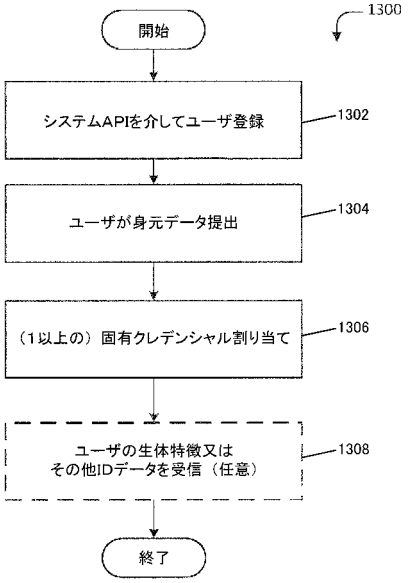
【図１１】


開始
1100
生体特徴入力
1102
入力された生体特徴を、
格納されたSPBFと同じ方法でSPBFに変換
1104
新たなSPBFファイルから、
生体特徴ベクトルを、格納された
SPBF生体特徴ベクトルと同じ方法で抽出
1106
入力された生体特徴ベクトルを
格納されたSPBF生体特徴ベクトルと比較
1108
入力された
生体特徴のSPBF生体特徴ベクトルと、
格納されたSPBF生体特徴ベクトルとの
比較結果を認証用に返す
1110
終了

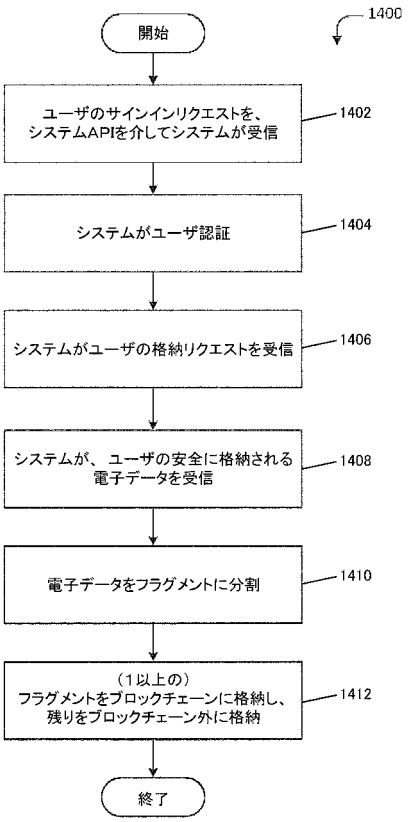
【図１２】



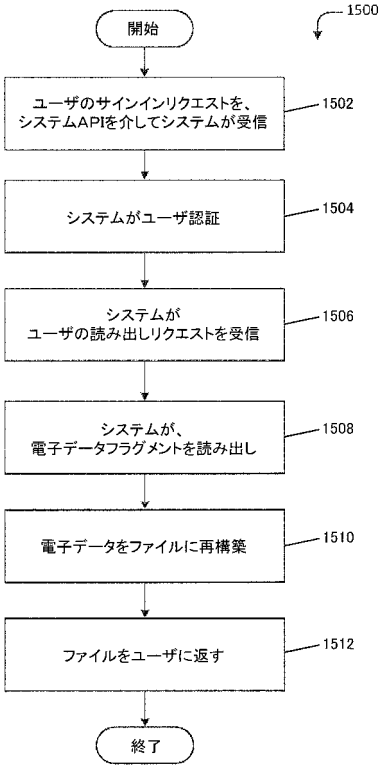
【図１３】



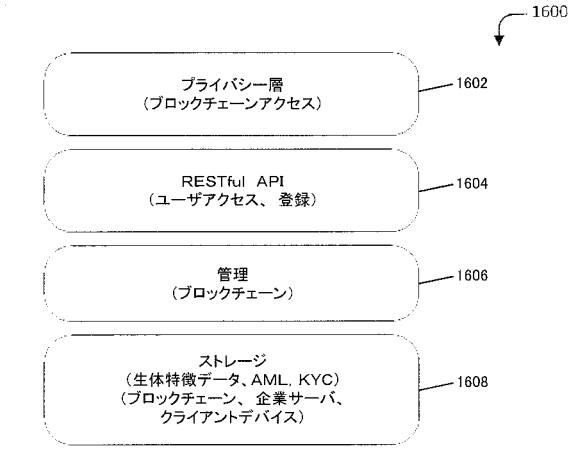
【図１４】



【図１５】



【図１６】



【手続補正書】
【提出日】平成30年8月14日(2018.8.14)
【手続補正１】
【補正対象書類名】実用新案登録請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【実用新案登録請求の範囲】
【請求項１】
電子データを安全に格納するシステムであって、
ユーザに関連付けられた意味を成す電子情報のファイルを受信し、安全に格納し、前記電子情報のファイルを受信すると、前記電子情報のファイルの少なくとも第１のフラグメント（＃１）と第２のフラグメント（＃２）とを含むフラグメント（２３２、３１４、４４２）を形成するように構成されたハードウェアプロセッサ（１２６）と、
第１の非一時的記憶装置に情報のブロックを格納する複数のノードを有する分散型データストレージシステム（２３４Ａ、３１６Ａ、４４４Ａ）と、
前記分散型データストレージシステムの外部にある第２の非一時的記憶装置（２３４Ｂ、３１６Ｂ、４４４Ｂ）と、を有し、
前記プロセッサは更に、前記ファイルの少なくとも前記第１のフラグメント（＃１）を前記分散型データストレージシステム（２３４Ａ、３１６Ａ、４４４Ａ）に格納し、前記ファイルの少なくとも前記第２のフラグメント（＃２）を前記分散型データストレージシステム（２３４Ａ、３１６Ａ、４４４Ａ）の外部のストレージに格納するように構成され、前記外部のストレージは前記第２の非一時的記憶装置（２３４Ｂ、３１６Ｂ、４４４Ｂ）を含む、システム。
【請求項２】

前記プロセッサは、前記ファイルの少なくとも前記第１のフラグメント及び少なくとも前記第２のフラグメントに対して、前記ファイルの少なくとも前記第１のフラグメント及び少なくとも前記第２のフラグメントの再構築用データを含む、位置データを格納するマッピングファイルを生成し、前記マッピングファイル又は前記マッピングファイルの少なくとも一部を、分散型台帳ストレージに格納するように構成される、請求項１に記載のシステム。

【請求項３】

前記ファイルの前記フラグメントはそれぞれ、前記ファイルに部分的又は完全に再構築されるまで、意味を成さない、請求項１に記載のシステム。

【請求項４】

前記プロセッサは、前記電子情報として、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含むデジタル生体特徴ファイルを受信するように構成される、請求項１に記載のシステム。

【請求項５】

前記プロセッサは、前記ファイルとして、前記ユーザに関連付けられたデジタルファイルを受信するように構成される、請求項１に記載のシステム。

【請求項６】

前記分散型データストレージシステムは、改竄不能データの格納のための信頼ユーティリティである、請求項１に記載のシステム。

【請求項７】

前記プロセッサは、前記電子情報として、前記ユーザに関連付けられたグラフィック又は画像ファイルを受信し、前記グラフィック又は画像を特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記外部のストレージに格納するように構成される、請求項１に記載のシステム。

【請求項８】

前記プロセッサは、前記特徴ブロックの内の少なくとも前記第１及び第２ブロックを格納する前に、前記特徴ブロックの内の少なくとも前記第１及び第２ブロックを変換し、変換結果を前記マッピングファイルに格納するように構成される、請求項７に記載のシステム。

【請求項９】

前記プロセッサは、前記マッピングファイルを、少なくとも第１のマッピングファイルフラグメンと第２のマッピングファイルフラグメントとに分割し、少なくとも前記第１のマッピングファイルフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記第２のマッピングファイルフラグメントを前記外部のストレージに格納するように構成される、請求項８に記載のシステム。

【請求項１０】

前記プロセッサは、前記特徴ブロックの内の少なくとも前記第１ブロックと、前記特徴ブロックの内の少なくとも前記第２ブロックとを暗号化するように構成される、請求項８に記載のシステム。

【請求項１１】

前記プロセッサは、前記特徴ブロックの内の少なくとも前記第１ブロックと、前記特徴ブロックの内の少なくとも前記第２ブロックとを暗号化するように構成される、請求項９に記載のシステム。

【請求項１２】

前記プロセッサは、少なくとも前記マッピングファイルを暗号化するように構成される、請求項８に記載のシステム。

【請求項１３】

前記特徴ブロックの組は、前記グラフィック又は画像を形成する前記特徴ブロックのサ

ブセットである、請求項８に記載のシステム。
【請求項１４】
前記グラフィック又は画像ファイルは、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含むファイルである、請求項８に記載のシステム。
【請求項１５】
前記プロセッサは、前記特徴ブロックの前記サブセットを暗号化し、前記暗号化された特徴ブロックのサブセットを少なくとも第１のフラグメント及び第２フラグメントに分解し、少なくとも前記第１のフラグメントを前記分散型データストレージシステムに格納し、少なくとも前記第２のフラグメントを前記外部のストレージに格納するように構成される、請求項１３に記載のシステム。
【請求項１６】
前記プロセッサは、前記生体特徴グラフィックの前記サブセットのハッシュを生成し、前記ハッシュの少なくとも一部を前記分散型データストレージシステムに格納し、前記ハッシュの少なくとも他部を前記外部のストレージに格納するように構成される、請求項１３に記載のシステム。
【請求項１７】
前記プロセッサは、前記ユーザに関連付けられた、前記システムに格納された情報へアクセスするためのユーザリクエストに応じて、アクセスを許可する前に前記ユーザを認証するように構成され、当該認証は、前記ユーザから前記システムが新たに受信した生体特徴グラフィックファイルのハッシュの少なくとも一部を、前記分散型データストレージシステム内の少なくとも前記第１のフラグメントと、前記分散型データストレージシステム外の少なくとも前記第２のフラグメントとから得られたハッシュと比較することを含み、前記ユーザが認証される条件の少なくとも一部として、一致することが求められ、前記プロセッサは、前記ユーザに関連付けられた、前記システムに格納された情報へアクセスするためのユーザリクエストに応じて、アクセスを許可する前に前記ユーザを認証するように構成され、当該認証は、前記生体特徴グラフィックの前記特徴ブロックの前記サブセットを、前記ユーザから前記システムが新たに受信した生体特徴ファイルの、対応する特徴ブロックのサブセットと比較することを含み、前記ユーザが認証される条件の少なくとも一部として、一致することが求められる、請求項１５に記載のシステム。
【請求項１８】
前記特徴ブロックの前記サブセットは、前記生体特徴グラフィックの連続的なブロック又は非連続的なブロックをグループ化したものである、請求項１３に記載のシステム。
【請求項１９】
前記特徴ブロックの前記サブセット内の特徴ブロックは、格納される前に変換される、請求項１３に記載のシステム。
【請求項２０】
前記プロセッサは、前記ユーザに関連付けられた第２グラフィック又は画像ファイルを格納し、前記第２グラフィック又は画像ファイル内のグラフィック又は画像を、特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するように構成される、請求項７に記載のシステム。
【請求項２１】
前記プロセッサは、前記ユーザに関連付けられた第２グラフィック又は画像ファイルを格納し、前記第２グラフィック又は画像ファイル内のグラフィック又は画像を、特徴ブロック群に分割し、前記グラフィック又は画像を構成する前記特徴ブロックの位置をマッピングするマッピングファイルを生成し、前記特徴ブロックの内の少なくとも第１ブロックを前記分散型データストレージシステムに格納し、前記特徴ブロックの内の少なくとも第２ブロックを前記分散型データストレージシステムの外部に格納するように構成される、

請求項１７に記載のシステム。
【請求項２２】
前記プロセッサは、機械可読命令により、更に前記フラグメントが、どのように前記ファイルに再構築されるかを示すインデックスファイルを形成するように構成される、請求項１に記載のシステム。
【請求項２３】
前記プロセッサは更に、少なくとも第１のフラグメントと対応する第２のフラグメントとを含む、前記インデックスファイルのフラグメントを生成し、
前記インデックスファイルの少なくとも前記第１のフラグメントを分散型データストレージシステムに格納し、
前記インデックスファイルの少なくとも前記第２のフラグメントを前記外部のストレージに格納するように構成される、請求項２２に記載のシステム。
【請求項２４】
前記プロセッサは更に、前記ファイルの少なくとも第３のフラグメントを生成し、前記第３のフラグメントを、前記分散型データストレージシステムに格納された前記第１のフラグメントとは別に、前記分散型データストレージシステムに格納するように構成される、請求項１に記載のシステム。
【請求項２５】
前記プロセッサは更に、少なくとも前記第１のフラグメントを、トランザクションとして前記分散型データストレージシステムに格納するように構成される、請求項１に記載のシステム。
【請求項２６】
前記プロセッサは更に、少なくとも前記第１のフラグメントと前記第３のフラグメントを、異なるトランザクションとして前記分散型データストレージシステムに格納するように構成される、請求項２４に記載のシステム。
【請求項２７】
前記プロセッサは、前記機械可読命令により更に、前記ユーザからのリクエストに応じて、前記ファイルフラグメントを、前記ファイルに再構築するように構成される、請求項１に記載のシステム。
【請求項２８】
前記プロセッサは、前記機械可読命令により更に、前記ファイルのヘッダの少なくとも一部を含む前記第１ファイルフラグメントを生成するように構成される、請求項１に記載のシステム。
【請求項２９】
前記分散型データストレージの前記外部のストレージは、自身のＣＰＵを持たないデジタルストレージ装置である、請求項１に記載のシステム。
【請求項３０】
前記分散型データストレージは、分散型台帳ストレージである、請求項１に記載のシステム。
【手続補正書】
【提出日】令和2年10月28日(2020.10.28)
【手続補正１】
【補正対象書類名】実用新案登録請求の範囲
【補正対象項目名】請求項１６
【補正方法】変更
【補正の内容】
【請求項１６】
前記グラフィックは、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含む生体特徴グラフィックであり、
前記プロセッサは、前記生体特徴グラフィックの前記サブセットのハッシュを生成し、

前記ハッシュの少なくとも一部を前記分散型データストレージシステムに格納し、前記ハッシュの少なくとも他部を前記外部のストレージに格納するように構成される、請求項１３に記載のシステム。
【手続補正２】
【補正対象書類名】実用新案登録請求の範囲
【補正対象項目名】請求項１８
【補正方法】変更
【補正の内容】
【請求項１８】
前記グラフィックは、前記ユーザに関連付けられた生体特徴情報の少なくとも一部を含む生体特徴グラフィックであり、
前記特徴ブロックの前記サブセットは、前記生体特徴グラフィックの連続的なブロック又は非連続的なブロックをグループ化したものである、請求項１３に記載のシステム。
【手続補正３】
【補正対象書類名】実用新案登録請求の範囲
【補正対象項目名】請求項２７
【補正方法】変更
【補正の内容】
【請求項２７】
前記プロセッサは、前記機械可読命令により更に、前記ユーザからのリクエストに応じて、前記フラグメントを、前記ファイルに再構築するように構成される、請求項２２に記載のシステム。
【手続補正４】
【補正対象書類名】実用新案登録請求の範囲
【補正対象項目名】請求項２８
【補正方法】変更
【補正の内容】
【請求項２８】
前記プロセッサは、前記機械可読命令により更に、前記ファイルのヘッダの少なくとも一部を含む前記第１ファイルフラグメントを生成するように構成される、請求項２２に記載のシステム。

フロントページの続き

(73)実用新案権者　518079046
マーカス　アンドレード
Ｍａｒｃｕｓ　ＡＮＤＲＡＤＥ
アメリカ合衆国　８９４０８　ネバダ州　ラスベガス　ウエストアズールドライブ　７４９５
７４９５ W.　Ａｚｕｒｅ　Ｄｒｉｖｅ，　Ｌａｓ　Ｖｅｇａｓ，　Ｎｅｖａｄａ　８９４０８
Ｕ．Ｓ．Ａ.
(74)上記1名の代理人　100090479
弁理士　井上　一
(74)代理人　100104710
弁理士　竹腰　昇
(74)代理人　100124682
弁理士　黒田　泰
(72)考案者　マーカス　アンドレード
アメリカ合衆国　８９１３０　ネバダ州　ラスベガス　アズールドライブ　７４９５　スイート
１００