(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5701855号
(P5701855)

(45)発行日　平成27年4月15日(2015.4.15)　(24)登録日　平成27年2月27日(2015.2.27)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640E

請求項の数 12　(全 23 頁)

(21)出願番号	特願2012-504116(P2012-504116)
(86)(22)出願日	平成22年4月2日(2010.4.2)
(65)公表番号	特表2012-523734(P2012-523734A)
(43)公表日	平成24年10月4日(2012.10.4)
(86)国際出願番号	PCT/IB2010/051448
(87)国際公開番号	WO2010/116310
(87)国際公開日	平成22年10月14日(2010.10.14)
審査請求日	平成25年3月28日(2013.3.28)
(31)優先権主張番号	09157811.2
(32)優先日	平成21年4月10日(2009.4.10)
(33)優先権主張国	欧州特許庁(EP)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
オランダ国　５６５６　アーエー　アインドーフェン　ハイテック　キャンパス　５
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】装置とユーザ認証

(57)【特許請求の範囲】
【請求項１】
装置とリモートサービスとを有するシステムにおける方法であって、
前記システムにおいて装置とユーザを登録する段階であって、
前記装置の装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記バイオメトリック測定結果から前記ユーザの鍵と、バイオメトリック測定から鍵を抽出するためのヘルパーデータを生成する段階と、
前記ヘルパーデータを格納する段階と、
前記装置ＩＤとユーザ識別情報とを前記リモートサービスに送信する段階と
により登録する段階と、
前記装置と前記ユーザを認証する段階であって、
前記装置において、
前記装置の前記装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記ユーザのヘルパーデータを読み出す段階と、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成する段階と、
前記ユーザのデータを測定する段階と、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コードまたは前記鍵から求めた前記測定したデータの署名のいずれかとを含むメッセージを生

成する段階と、
前記リモートサービスに前記メッセージを送信する段階と、
前記リモートサービスにおいて、
前記メッセージと、前記登録する段階で送信された前記装置ＩＤと、ユーザ識別情報とを用いて、前記装置と前記ユーザを認証する段階と
により認証する段階と、を有し、
前記バイオメトリック測定結果から前記ユーザの鍵とヘルパーデータを生成する段階は、前記バイオメトリック測定結果と前記装置ＩＤから前記ユーザの鍵とヘルパーデータを生成する段階を有し、
前記ヘルパーデータを格納する段階は、前記装置にユーザ識別情報と共に前記ヘルパーデータを格納する段階を有し、
前記装置ＩＤとユーザ識別情報とを前記リモートサービスに送信する段階は、さらに、前記鍵を前記リモートサービスに送信する段階を有し、
前記リモートサービスにおいて前記装置と前記ユーザを認証する段階は、前記メッセージと、前記登録する段階で送信された前記装置ＩＤ、ユーザ識別情報、及び鍵とを用いて、前記装置と前記ユーザを認証する段階を有する、
方法。
【請求項２】
前記バイオメトリック測定結果と前記装置ＩＤから前記ユーザの鍵とヘルパーデータを生成する段階は、
前記装置ＩＤとランダムストリングからコードワードを生成する段階と、
前記コードワードと前記バイオメトリック測定から前記鍵を生成する段階とを有する、請求項１に記載の方法。
【請求項３】
さらに、
前記メッセージに前記装置ＩＤ及び／またはユーザＩＤを含める段階を有する、請求項１または２に記載の方法。
【請求項４】
装置とリモートサービスとを有するシステムにおける方法であって、
前記システムにおいて装置とユーザを登録する段階であって、
前記装置の装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記バイオメトリック測定結果から前記ユーザの鍵と、バイオメトリック測定から鍵を抽出するためのヘルパーデータを生成する段階と、
前記ヘルパーデータを格納する段階と、
前記装置ＩＤとユーザ識別情報とを前記リモートサービスに送信する段階と
により登録する段階と、
前記装置と前記ユーザを認証する段階であって、
前記装置において、
前記装置の前記装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記ユーザのヘルパーデータを読み出す段階と、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成する段階と、
前記ユーザのデータを測定する段階と、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コードまたは前記鍵から求めた前記測定したデータの署名のいずれかとを含むメッセージを生成する段階と、
前記リモートサービスに前記メッセージを送信する段階と、
前記リモートサービスにおいて、
前記メッセージと、前記登録する段階で送信された前記装置ＩＤと、ユーザ識別情報と

を用いて、前記装置と前記ユーザを認証する段階と
により認証する段階と、を有し、
前記装置と前記ユーザを前記システムに登録する段階は、さらに、前記装置ＩＤとランダムストリングからコードワードを生成する段階を有し、
前記バイオメトリック測定から前記ユーザの鍵とヘルパーデータとを生成する段階は、前記バイオメトリック測定と前記コードワードから前記ユーザの鍵とヘルパーデータとを生成する段階を有し、
前記ヘルパーデータを格納する段階は、ユーザ識別情報とともに前記ヘルパーデータを前記装置に格納する段階を有し、
リモートサービスに前記装置ＩＤとユーザ識別情報を送信する段階は、前記リモートサービスに前記ランダムストリングを送信する段階をさらに有し、
前記リモートサービスにおいて前記装置と前記ユーザを認証する段階は、前記メッセージと、前記登録の段階で送信された前記装置ＩＤとユーザ識別情報とランダムストリングとを用いて、前記装置と前記ユーザを認証する段階を有する、方法。
【請求項５】
装置とリモートサービスとを有するシステムにおける方法であって、
前記システムにおいて装置とユーザを登録する段階であって、
前記装置の装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記バイオメトリック測定結果から前記ユーザの鍵と、バイオメトリック測定から鍵を抽出するためのヘルパーデータを生成する段階と、
前記ヘルパーデータを格納する段階と、
前記装置ＩＤとユーザ識別情報とを前記リモートサービスに送信する段階と
により登録する段階と、
前記装置と前記ユーザを認証する段階であって、
前記装置において、
前記装置の前記装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記ユーザのヘルパーデータを読み出す段階と、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成する段階と、
前記ユーザのデータを測定する段階と、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コードまたは前記鍵から求めた前記測定したデータの署名のいずれかとを含むメッセージを生成する段階と、
前記リモートサービスに前記メッセージを送信する段階と、
前記リモートサービスにおいて、
前記メッセージと、前記登録する段階で送信された前記装置ＩＤと、ユーザ識別情報とを用いて、前記装置と前記ユーザを認証する段階と
により認証する段階と、を有し、
前記リモートサービスに前記装置ＩＤとユーザ識別情報を送信する段階は、前記リモートサービスに前記鍵を送信する段階をさらに有し、
前記リモートサービスで前記装置と前記ユーザを認証する段階は、さらに、前記鍵を用いて前記装置ＩＤを暗号化する段階を有し、
前記生成する段階で生成されたメッセージは、さらに、前記暗号化された装置ＩＤを含み、
前記リモートサービスで前記装置と前記ユーザを認証する段階は、前記メッセージと、前記登録する段階に送信された前記装置ＩＤとユーザ識別情報と鍵とを用いて、前記装置と前記ユーザを認証する段階を有する、方法。
【請求項６】
装置とリモートサービスとを有するシステムにおける方法であって、

前記システムにおいて装置とユーザを登録する段階であって、
前記装置の装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記バイオメトリック測定結果から前記ユーザの鍵と、バイオメトリック測定から鍵を抽出するためのヘルパーデータを生成する段階と、
前記ヘルパーデータを格納する段階と、
前記装置ＩＤとユーザ識別情報とを前記リモートサービスに送信する段階と
により登録する段階と、
前記装置と前記ユーザを認証する段階であって、
前記装置において、
前記装置の前記装置ＩＤを取得する段階と、
前記ユーザのバイオメトリック測定を実行する段階と、
前記ユーザのヘルパーデータを読み出す段階と、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成する段階と、
前記ユーザのデータを測定する段階と、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コードまたは前記鍵から求めた前記測定したデータの署名のいずれかとを含むメッセージを生成する段階と、
前記リモートサービスに前記メッセージを送信する段階と、
前記リモートサービスにおいて、
前記メッセージと、前記登録する段階で送信された前記装置ＩＤと、ユーザ識別情報とを用いて、前記装置と前記ユーザを認証する段階と
により認証する段階と、を有し、
前記装置と前記ユーザを前記システムに登録する段階は、さらに、乱数値を発生し、前記乱数値と前記鍵から別のヘルパーデータを生成する段階を有し、
前記ヘルパーデータを格納する段階は、さらに、前記別のヘルパーデータを格納する段階を有し、
前記装置ＩＤと前記ユーザ識別情報を前記リモートサービスに送信する段階は、さらに、前記鍵、乱数値、及び前記装置ＩＤの関数を前記リモートサービスに送信する段階を有し、
前記ヘルパーデータを読み出す段階は、さらに、前記別のヘルパーデータを読み出す段階を有し、
前記リモートサービスで前記装置と前記ユーザを認証する段階は、前記別のヘルパーデータと前記鍵から前記乱数値を求める段階と、前記鍵、ランダム値、及び前記装置ＩＤの関数から別の鍵を生成する段階と、
前記生成する段階で生成したメッセージ認証コードを、前記測定データと前記別の鍵から求め、
前記リモートサービスで前記装置と前記ユーザを認証する段階は、前記メッセージと、前記装置ＩＤ、ユーザ識別情報、及び前記登録する段階に送信された前記鍵とランダム値と前記装置ＩＤとの関数とを用いて、前記装置と前記ユーザを認証する段階を有する、方法。

【請求項７】
装置とユーザを認証するシステムであって、
前記ユーザのバイオメトリック測定を実行するように構成された測定装置と、
プロセッサと、
前記ユーザのデータを測定する、格納された装置ＩＤを有する検知装置と、
リモートサービスとを有し、
リモートサービスで検知装置とユーザを登録する手順中に、前記プロセッサは、
前記検知装置からその装置ＩＤを取得し、
前記測定装置から前記ユーザのバイオメトリック測定結果を取得し、

前記バイオメトリック測定結果から前記ユーザの鍵と、鍵を抽出するヘルパーデータを生成し、
前記ヘルパーデータを格納し、
前記装置ＩＤとユーザ識別情報を前記リモートサービスに送信するように構成され、
前記リモートサービスで前記検知装置と前記ユーザを認証する手順において、前記プロセッサは、
前記検知装置から前記装置の前記装置ＩＤを取得し、
前記ユーザのヘルパーデータを読み出し、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成し、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コード、または前記鍵から求め前記測定したデータのシグネチャのいずれかとを含むメッセージを生成し、
前記リモートサービスに前記メッセージを送信するように構成され、
前記リモートサービスは、前記メッセージと、前記登録手順において受信した前記装置ＩＤ及びユーザ識別情報とにより、前記検知装置と前記ユーザを認証するように構成され、
前記プロセッサは、
前記バイオメトリック測定と前記装置ＩＤから前記ユーザの鍵とヘルパーデータを生成し、
前記ヘルパーデータをユーザ識別情報とともに前記装置に格納し、
前記装置ＩＤとユーザ識別情報とともに前記鍵を前記リモートサービスに送信するように構成され、
前記リモートサービスは、前記メッセージと、前記登録手順において送信された前記装置ＩＤ、ユーザ識別情報、及び鍵とを用いて、前記検知装置と前記ユーザを認証するように構成された、
システム。
【請求項８】
前記プロセッサは、さらに、
前記装置ＩＤとランダムストリングからコードワードを生成し、前記コードワードとバイオメトリック測定から前記鍵を生成することにより、前記バイオメトリック測定と前記装置ＩＤから、前記ユーザの鍵とヘルパーデータを生成するように構成された、請求項７に記載のシステム。
【請求項９】
前記プロセッサは、さらに、前記メッセージに前記装置ＩＤ及び／またはユーザＩＤを含めるように構成された、
請求項７または８に記載のシステム。
【請求項１０】
装置とユーザを認証するシステムであって、
前記ユーザのバイオメトリック測定を実行するように構成された測定装置と、
プロセッサと、
前記ユーザのデータを測定する、格納された装置ＩＤを有する検知装置と、
リモートサービスとを有し、
リモートサービスで検知装置とユーザを登録する手順中に、前記プロセッサは、
前記検知装置からその装置ＩＤを取得し、
前記測定装置から前記ユーザのバイオメトリック測定結果を取得し、
前記バイオメトリック測定結果から前記ユーザの鍵と、鍵を抽出するヘルパーデータを生成し、
前記ヘルパーデータを格納し、
前記装置ＩＤとユーザ識別情報を前記リモートサービスに送信するように構成され、
前記リモートサービスで前記検知装置と前記ユーザを認証する手順において、前記プロ

セッサは、
前記検知装置から前記装置の前記装置ＩＤを取得し、
前記ユーザのヘルパーデータを読み出し、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成し、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コード、または前記鍵から求め前記測定したデータのシグネチャのいずれかとを含むメッセージを生成し、
前記リモートサービスに前記メッセージを送信するように構成され、
前記リモートサービスは、前記メッセージと、前記登録手順において受信した前記装置ＩＤ及びユーザ識別情報とにより、前記検知装置と前記ユーザを認証するように構成され、
前記装置と前記ユーザを前記システムに登録する手順において、前記プロセッサは、さらに、前記装置ＩＤとランダムストリングからコードワードを生成するように構成され、
前記プロセッサは、前記バイオメトリック測定と前記コードワードから前記ユーザの鍵とヘルパーデータとを生成するように構成され、
前記プロセッサは、ユーザ識別情報とともに前記ヘルパーデータを前記装置に格納するように構成され、
前記プロセッサは、前記装置ＩＤとユーザ識別情報とともに、前記リモートサービスに前記ランダムストリングを送信するように構成され、
前記リモートサービスは、前記メッセージと、前記登録の段階で送信された前記装置ＩＤとユーザ識別情報とランダムストリングとを用いて、前記装置と前記ユーザを認証するように構成された、システム。
【請求項１１】
装置とユーザを認証するシステムであって、
前記ユーザのバイオメトリック測定を実行するように構成された測定装置と、
プロセッサと、
前記ユーザのデータを測定する、格納された装置ＩＤを有する検知装置と、
リモートサービスとを有し、
リモートサービスで検知装置とユーザを登録する手順中に、前記プロセッサは、
前記検知装置からその装置ＩＤを取得し、
前記測定装置から前記ユーザのバイオメトリック測定結果を取得し、
前記バイオメトリック測定結果から前記ユーザの鍵と、鍵を抽出するヘルパーデータを生成し、
前記ヘルパーデータを格納し、
前記装置ＩＤとユーザ識別情報を前記リモートサービスに送信するように構成され、
前記リモートサービスで前記検知装置と前記ユーザを認証する手順において、前記プロセッサは、
前記検知装置から前記装置の前記装置ＩＤを取得し、
前記ユーザのヘルパーデータを読み出し、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成し、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コード、または前記鍵から求め前記測定したデータのシグネチャのいずれかとを含むメッセージを生成し、
前記リモートサービスに前記メッセージを送信するように構成され、
前記リモートサービスは、前記メッセージと、前記登録手順において受信した前記装置ＩＤ及びユーザ識別情報とにより、前記検知装置と前記ユーザを認証するように構成され、
前記プロセッサは、前記リモートサービスに、前記装置ＩＤとユーザ識別情報とともに前記鍵を送信する段階をさらに有し、
前記リモートサービスで前記装置と前記ユーザを認証する手順において、前記プロセッ

サは、さらに、前記鍵を用いて前記装置ＩＤを暗号化するように構成され、
前記プロセッサは、前記暗号化された装置ＩＤを含むメッセージを生成するように構成され、
前記リモートサービスは、前記メッセージと、前記登録する手順で送信された前記装置ＩＤとユーザ識別情報と鍵とを用いて、前記装置と前記ユーザを認証するように構成された、システム。
【請求項１２】
装置とユーザを認証するシステムであって、
前記ユーザのバイオメトリック測定を実行するように構成された測定装置と、
プロセッサと、
前記ユーザのデータを測定する、格納された装置ＩＤを有する検知装置と、
リモートサービスとを有し、
リモートサービスで検知装置とユーザを登録する手順中に、前記プロセッサは、
前記検知装置からその装置ＩＤを取得し、
前記測定装置から前記ユーザのバイオメトリック測定結果を取得し、
前記バイオメトリック測定結果から前記ユーザの鍵と、鍵を抽出するヘルパーデータを生成し、
前記ヘルパーデータを格納し、
前記装置ＩＤとユーザ識別情報を前記リモートサービスに送信するように構成され、
前記リモートサービスで前記検知装置と前記ユーザを認証する手順において、前記プロセッサは、
前記検知装置から前記装置の前記装置ＩＤを取得し、
前記ユーザのヘルパーデータを読み出し、
前記バイオメトリック測定と読み出したヘルパーデータから鍵を生成し、
前記測定したデータと、前記測定したデータ及び前記鍵から求めたメッセージ認証コード、または前記鍵から求め前記測定したデータのシグネチャのいずれかとを含むメッセージを生成し、
前記リモートサービスに前記メッセージを送信するように構成され、
前記リモートサービスは、前記メッセージと、前記登録手順において受信した前記装置ＩＤ及びユーザ識別情報とにより、前記検知装置と前記ユーザを認証するように構成され、
前記装置と前記ユーザを前記システムに登録する手順において、前記プロセッサは、さらに、乱数値を発生し、前記乱数値と前記鍵から別のヘルパーデータを生成するように構成され、
前記プロセッサは、前記別のヘルパーデータを格納するように構成され、
前記プロセッサは、前記装置ＩＤと前記ユーザ識別情報とともに、前記鍵、乱数値、及び前記装置ＩＤの関数を前記リモートサービスに送信するように構成され、
前記プロセッサは、前記別のヘルパーデータを読み出す段階を有し、
前記リモートサービスで前記装置と前記ユーザを認証する手順において、前記プロセッサは、前記別のヘルパーデータと前記鍵から前記乱数値を求め、前記鍵、ランダム値、及び前記装置ＩＤの関数から別の鍵を生成するように構成され、
前記プロセッサは、前記測定データと前記別の鍵から前記メッセージ認証コードを生成するように構成され、
前記リモートサービスは、前記メッセージと、前記装置ＩＤ、ユーザ識別情報、及び前記登録する段階に送信された前記鍵とランダム値と前記装置ＩＤとの関数とを用いて、前記装置と前記ユーザを認証するように構成された、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、装置とユーザの認証方法及びシステムに関する。本発明を用いて、装置IDを

用いた、ヘルスサービスのための患者認証を改善できる。

【背景技術】

【０００２】

ヘルスケア分野におけるトレンドとして、すべてのレベルにおいて消費者／患者による関与がますます重要になりつつある。消費者／患者が自分の健康管理にいままで以上に積極的な役割を果たしている。このような患者に対するエンパワーメント（enpowerment）というトレンドはすでに広く支持されている。患者が自分自身の健康関係情報を収集でき、ポータブルデバイス、ＰＣ、（ＣａｐＭｅｄ、ＷｅｂＭＤ、ＭｅｄＫｅｙなどの）オンラインサービスに格納できる多数のソリューションが市場に投入されてきた。これらのソリューションは個人健康記録サービス（Personal Health Record service、以下ＰＨＲ）と呼ばれることが多い。すでに市場に投入された多くの製品により、患者は測定結果その他の医療データを（ＬｉｆｅＳｅｎｓｏｒ、Ｍｉｃｒｏｓｏｆｔ ＨｅａｌｔｈＶａｕｌｔなどの）ＰＨＲに自動的に入力できる。このようなシステムでは、例えば体重計が情報をブルートゥースを介してＰＣに送信し、そのデータがＰＣからユーザのＰＨＲにアップロードされる。これにより、患者は自分自身の健康データを収集して管理し、さらに重要なことには、治療に係わる様々なヘルスケア専門家とそのデータを共有できる。

【０００３】

ヘルスケアにおけるもう一つの重要なトレンドとして、ヘルスケアの提供が、医療機関における診療から、外来診療や在宅診療に徐々に広がってきている。情報技術や通信技術の発達により、遠隔治療や遠隔患者監視を含む遠隔ヘルスケアサービス（遠隔医療）が開発されている。市場では多くのサービスが遠隔医療（telehealth）インフラストラクチャを展開し、ホームハブを介して測定装置を遠隔バックエンドサーバに接続している。ヘルスケアプロバイダは、このアーキテクチャを用いて測定データに遠隔的にアクセスし、患者の役にたっている。例えば、（Philips Motive、PTSなどの）疾病管理サービスや（Philips Lifelineなどの）緊急応答サービスがある。

【０００４】

実現とこの市場のさらなる成長のために、測定装置、ホームハブ（home hubs）、およびバックエンドサービスの相互運用性が非常に重要になっている。Continua healthアライアンスはこの必要性を認識している。図１に示したように、この構想は、測定装置とホームハブ装置（アプリケーションホスティング）とオンラインヘルスケア／ウェルネスサービス（ＷＡＮ）とヘルスレコード装置（ＰＨＲ／ＥＨＲ）との間のプロトコルを標準化する。Ｃｏｎｔｉｎｕａは、データフォーマットとデータ交換の問題の次に、セキュリティ問題とセーフティ問題も解決しようとしている。

【０００５】

遠隔医療の領域における基本的なセキュリティ問題の１つとして、ユーザと装置の認証／識別の問題がある。すなわち、遠隔的に患者が測定したデータを遠隔医療サービスまたは医療専門家により用いられるとき、ヘルスケアプロバイダは患者が報告する情報を信用なければならない。具体的には、サービスプロバイダは、測定結果が患者本人からのものであり、その測定結果を取るのに適切な装置を用いたことを信頼しなければならない。例えば、血圧測定を考えると、登録したユーザの血圧を測定したこと、安物の装置ではなく認定を受けた装置により測定したことが分からなければならない。これは非常に重要なことである。間違ったデータに基づいてヘルスケア上の重大な結論を下してしまうおそれがあるからである。そのため、ユーザ認証と装置認証をサポートしなければならない。これには、患者の安全性（データの出所がはっきりして信頼できるデータに基づいて、診断と医療上の決定がなされること）、コストの低減（データが信頼でき、患者が提供したデータをコンシューマ医療及び専門家による医療の領域において再利用できること）、および患者の便宜（患者が自宅で医療上の測定をできること）という利益がある。

【０００６】

現在の実務では、装置識別子（装置ＩＤ）が、ユーザ識別子（ユーザＩＤ）として、または（同じ装置を複数のユーザが用いるとき）ユーザＩＤを求める手段として用いられる

。例えば、Ｃｏｎｔｉｎｕａでは、非特許文献１に記載されているように、ＰＡＮインタフェースにおいて（図１を参照）、各Ｃｏｎｔｉｎｕａ装置がそれ自身の固有の装置ＩＤを送る必要がある。ユーザＩＤは任意的である（１、２、Ａ、Ｂのように非常に簡単なものでもよい）。ハブ装置（アプリケーションホスティング装置）は、有効なユーザＩＤを取得し、装置ＩＤに関連する簡単なユーザＩＤを有効なユーザＩＤにマッピングできる。装置ＩＤの次に有効なユーザＩＤを送れる測定装置があってもよい。この場合、マッピングは必要ない。

【０００７】

現在のこのアプローチにはいくつかの問題がある。第１に、現在のアプローチはユーザ／装置の認証をサポートしておらず、測定結果にユーザＩＤを付加するだけである。データの出所がはっきりせず、あとでそれを処理する際、ヘルスケアプロバイダはその測定結果を得るのにどの装置を使ったか、確実には分からない。第２に、現在のマッピングアプローチはユーザと装置ＩＤとを素早く関連付けず、間違いが生じる余地がある。ユーザが図らずも間違うか（マニュアルマッピングが必要な場合、ユーザは測定ごとに、アプリケーションホスティング装置または測定装置で自分のＩＤを選択しなければならない）、またはシステムがユーザを取り違えることもある（アプリケーション設計者は特に注意して、測定結果を間違ったユーザに関連付ける可能性を低減するように、データ管理をすべきである）。第３に、悪意のあるユーザが、本当のユーザになりすまして、間違った測定結果を送る場合もある。

【先行技術文献】

【非特許文献】

【０００８】

【非特許文献１】Continua Health Alliance, "Recommendations for Proper User Identification in Continua Version 1 - PAN and xHR interfaces" (Draft v.0l) December ２００７

【発明の概要】

【課題を解決するための手段】

【０００９】

それゆえ、本発明の目的は従来技術の改良である。

【００１０】

本発明の第１の態様による方法は、装置とユーザを認証する方法であって、前記装置の装置ＩＤを取得する段階と、前記ユーザのバイオメトリック測定を行う段階と、前記ユーザのヘルパーデータを取得する段階と、前記バイオメトリック測定とヘルパーデータから鍵を生成する段階と、前記鍵を、または前記鍵から求めたコンポーネントを含むメッセージを生成する段階と、リモートサービスに前記メッセージを送信する段階と、前記メッセージを用いて、前記装置と前記ユーザを認証する段階と、を有する。

【００１１】

本発明の第２の態様によるシステムは、装置とユーザを認証するシステムであって、前記ユーザのバイオメトリック測定を実行するように構成された測定装置と、プロセッサとを有し前記プロセッサは、前記装置の装置ＩＤを取得し、前記ユーザのヘルパーデータを取得し、前記バイオメトリック測定とヘルパーデータから鍵を生成し、前記鍵を、または前記鍵から求めたコンポーネントを含むメッセージを生成し、リモートサービスに前記メッセージを送信する。

【００１２】

本発明により、ユーザの識別情報と装置の識別子を組み合わせて、その装置から来るそのデータが、その装置とそのユーザからのものでることを確認することができる。各ヘルスケア装置が、変更できない固有のＩＤを有するとの仮定の下に、患者の識別情報を装置ＩＤに密接に組み合わせる別の実施形態を提供する。これは、パーソナルヘルスケアアプリケーションにおけるデータ品質保証と信頼性を支持する。装置とユーザの認証／識別を確実なものとするため、各装置の固有のグローバルＩＤを、バイオメトリックスと組み合

わせて用いる。本発明は、ユーザＩＤと、測定に使われる装置の識別子との密接な結合を提供し、装置／ユーザが登録されていないと、それをすぐに検出して、バイオメトリックスを用いた強力なユーザ認証を行う。

【００１３】

好ましい実施形態において、鍵を生成する段階は、装置ＩＤから鍵を生成する段階を有する。プロセスの早い段階で、ユーザのバイオメトリック情報と装置ＩＤを強く結びつける一方法は、装置ＩＤを、セキュアプロセスで用いる鍵の生成に、用いることである。バイオメトリック情報とヘルパーデータと装置ＩＤを用いて、鍵を生成し、装置から取得した検出データとともに送ることができる。

【００１４】

有利にも、本方法は、さらに、ユーザの検出データを取得する段階を有し、鍵から求めたコンポーネントは鍵を用いて処理した検出データを含む。鍵を用いて検出データを署名し、サービスプロバイダに送るメッセージに含める。これにより、生成した鍵を用いて検出データを保護する簡単かつ効果的な方法を提供し、その検出データを提供した装置とユーザを認証プロセスにより確実に識別できる。

【００１５】

別の一実施形態において、本方法は、前記バイオメトリック測定とヘルパーデータからコードワードを生成する段階と、前記装置ＩＤが前記コードワードと一致するかチェックする段階とを有する。これは、第３者のサービスプロバイダにメッセージを送る前に装置ＩＤをチェックできるプロセスを支持する。この時、ユーザに警告を発することができるが、それでも、ユーザと、そのユーザが現在使っている装置を認証するセキュアな方法を提供する。

【００１６】

さらに別の実施形態では、メッセージを発する段階は、そのメッセージにユーザのヘルパーデータを含める段階をさらに有し、前記装置と前記ユーザを認証する段階は、前記ヘルパーデータと前記装置ＩＤとから前記鍵を生成する段階を有する。この方法により、装置とユーザに関する情報のセキュアな送信が可能になる。サービス側における認証により、ヘルパーデータと装置ＩＤにより必要となる鍵を生成するからである。ユーザまたは装置のどちらかが間違っているとき、正しい鍵は生成できない。

【００１７】

さらに別の一実施形態において、本プロセスは、さらに、前記鍵で前記装置ＩＤを暗号化する段階を有し、前記鍵から求めたコンポーネントは前記暗号化された装置ＩＤを含む。装置ＩＤで鍵を生成してその鍵をメッセージで送信するのではなく、本システムは、バイオメトリックデータとユーザのヘルパーデータから生成した鍵を用いて、装置ＩＤを暗号化できる。これにより、サービス側でユーザと装置をセキュアな方法で認証できる。

【図面の簡単な説明】

【００１８】

添付した図面を参照して、例により、本発明の実施形態を説明する。

【図１】ヘルスケアシステムを示す概略図である。

【図２】ヘルスケアシステムを示す別の概略図である。

【図３】装置とユーザ認証システムを示す概略図である。

【図４】登録および認証の手続を示すフローチャートである。

【図５】登録および認証の手続を示す別のフローチャートである。

【図６】登録および認証の手続を示すさらに別のフローチャートである。

【図７】登録および認証の手続を示すさらに別のフローチャートである。

【図８】登録および認証の手続を示すさらに別のフローチャートである。

【図９】登録および認証の手続を示すさらに別のフローチャートである。

【図１０ａ】認証システムの好ましい実施形態を示す概略図である。

【図１０ｂ】認証システムの好ましい実施形態を示す別の概略図である。

【発明を実施するための形態】

【００１９】
ヘルスケアシステムの一例を図１に示す。腕時計や血圧計などのいろいろなＰＡＮ（パーソナルエリアネットワーク）装置１０を示した。これらはユーザの生理的パラメータを直接測定する。また、トレッドミルなどのLAN(ローカルエリアネットワーク)装置１２が設けられている。これらは、ユーザに関する別のヘルスケア情報の収集に用いることができる。PAN装置１０とLAN装置１２は、コンピュータや携帯電話などの適切なアプリケーションホスティング装置１４に、好適な（有線及び／または無線の）インタフェースを介して接続されている。これらのアプリケーションホスティング装置は、例えば、ユーザの自宅にあるＰＡＮ装置１０やLAN装置１２に対してローカルなものである。ホスティング装置１４は好適なアプリケーションを実行し、いろいろなＰＡＮ装置１０やLAN装置１２からの出力を収集して、整理する。

【００２０】
アプリケーションホスティング装置１４はサーバなどのＷＡＮ（ワイドエリアネットワーク）装置１６に接続されている。ＷＡＮ接続はインターネット等のネットワークを介したものでもよい。また、サーバ１６は好適なインタフェースを介してヘルスレコード装置１８に接続されている。このヘルスレコード装置は、システムのユーザのヘルスレコードを保持する。各ユーザは装置１８にヘルスレコードを有している。上述の通り、最も重要なことは、第１に、装置１８に格納された個人のヘルスレコードにより記録されたデータが正しいユーザに割り当てられること、第２に、そのデータを最初に記録した装置１０または１２が確実に分かることである。また、それに関連するＰＡＮ装置１０やLAN装置１２が、システムにおける使用を認められていることも好ましい。

【００２１】
図２は、ユーザ２０がＰＡＮ装置１０で測定をしている、図１のシステムを示す。ホームハブ１４により、データを、患者のレコード２２を保持しているリモートレコード装置１８に送ることができる。リモートレコード装置１８もＧＰレコード２４と直接通信する。この例では、ユーザ２０は、装置１０に対して自分を偽っており、また、しようとする測定にとって正しくない装置１０を用いている。従来のシステムでは、これによりレコード２２に不正エントリーがなされ、患者の状態に関して不正な警報が発せられることがある。

【００２２】
図２に示したようなエラーを防ぐため、本発明によるシステムを図３に示す。この図は、ＰＡＮ装置１０、ＬＡＮ装置１２、ユーザ２０を示し、これらはリモートヘルスケア装置１８と通信している。基本原理は、ユーザ２０から、及び装置１０または装置１２からの情報から鍵を求める。一実施形態では、その鍵を用いて装置１０または１２からの検出データを符号化し、符号化データをリモートサーバ１８に送信する。ユーザ２０の（指紋などの）バイオメトリック測定を行い、このバイオメトリック測定により鍵を生成する。ユーザ２０からのデータと組み合わせて、装置１０または１２のどれが実際に測定しているかという情報を用いて、ユーザ２０と装置１０または１２を確実に識別できるように、データを保護する鍵を生成する。

【００２３】
バイオメトリック測定から取り出したユーザＩＤと、それぞれの装置１０または１２の装置ＩＤを、図１のコンポーネント１４であるアプリケーションホスティング装置で組み合わせることもできる。ほとんどの測定装置（ＰＡＮ装置１０とLAN装置１２）は、機能が限定されているため指紋センサを有していない。指紋センサはアプリケーションホスティング装置１４に取り付けることができる。ユーザが測定するとき、測定結果とともに装置ＩＤもホスティング装置１４に送られる。ここで、バイオメトリックＩＤと装置ＩＤが合成され、鍵が生成される。この鍵を用いて、装置１０または１２からのデータの署名（すなわち認証）をする。

【００２４】
バイオメトリックスは、人が何をもっているか（トークン）または何を知っているか（

パスワード）ではなく、その人が誰かに基づいて、人を識別または認証する。バイオメトリック特性は、トークンやパスワードと違って無くしたり忘れたりしないので、人を識別および認証する魅力的かつ便利な代替方法を提供する。しかし、個人のバイオメトリックスは、通常、一様にランダムな性質のものではなく、測定をするたびに正確に再生できるものでもない。この問題を軽減するため、「ファジーエクストラクタ（fuzzy extractors）」を用いて、個人のバイオメトリックスから、ほぼ一様かつ信頼性が高い鍵を抽出する（extract）。

【００２５】

人の指紋や虹彩スキャンなどのバイオメトリック情報は、明らかに、一様なランダムストリングではなく、測定するたびに正確に再生できるものでもない。このため、ファジーエクストラクタは、バイオメトリック入力からほぼ一様なランダム性Ｒを求めるのに用いられる。入力が変化しても、オリジナルに十分近い限り、Ｒは同じであるという意味で、この抽出もエラートレラント（error tolerant）である。このように、ファジーエクストラクタ、すなわちヘルパーデータアルゴリズム（helper data algorithm）は、ノイズが多いバイオメトリックデータから１つ（またはそれ以上）のセキュア鍵を抽出する必要がある。これらのトピックスに関するもっと詳しい情報は、次の文献を参考にされたい：J.-P. M. G. Linnartz and P. Tuyls, 「New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates」 in Audio-and Video-Based Biometrie Person Authentication, AVBPA ２００３, ser. LNCS, J. Kittler and M. S. Nixon, Eds., vol. ２６８８. Springer, June 9-11, ２００３, pp. ３９３-４０２；およびY. Dodis, M. Reyzin, and A. Smith, 「Fuzzy extractors: How to generate strong keys from biometrics and other noisy data」 in Advances in Cryptology, EUROCRYPT ２００４, ser. LNCS, C. Cachin and J. Camenisch, Eds., vol. ３０２７. Springer- Verlag, ２００４, pp. ５２３-５４０。

【００２６】

ファジーエクストラクタは２つの基本的な前提条件（primitives）を必要とする。第１に、情報の突き合わせまたはエラー訂正と、第２に、プライバシーの強化またはランダムネス抽出である。これにより、一様に分布したランダム変数に非常に近い出力を確保できる。これらの２つの前提条件を実現するために、加入または登録段階において、ヘルパーデータＷを生成する。その後、鍵再構成または認証段階において、ノイズが多い測定結果Ｒ１とヘルパーデータＷとに基づき、鍵を再構成する。

【００２７】

（トラステッド環境において行われる）加入段階において、Ｇｅｎと呼ぶ確率的手続を実行する。これは、入力として、ノイズが多いバイオメトリック測定結果Ｒを受け取り、出力として、鍵Ｋとヘルパーデータ Ｗ：（Ｋ，Ｗ）←Ｇｅｎ（Ｒ）を生成する。ヘルパーデータＷを生成するため、少なくとも「ｔ」個のエラーを訂正できるように、エラー訂正コードＣを選択する。訂正するエラー数は、具体的なアプリケーションとバイオメトリック測定の質による。適切なコードを選べば、ヘルパーデータＷは、まずＣからランダムコードワードＣｓを選び、Ｗ１＝Ｃｓ＋Ｒを計算することにより生成される。さらに、集合Ｈからランダムにユニバーサルハッシュ関数ｈｉを選択し、鍵ＫをＫ←ｈｉ（Ｒ）と定義する。そして、ヘルパーデータはＷ＝（Ｗ１，ｉ）と定義する。

【００２８】

鍵再構成段階において、Ｒｅｐと呼ぶ手続を実行する。これは、入力としてノイズが多い応答Ｒ′とヘルパーデータＷを受け取り、（Ｒ′がＲと同じ情報源からのものであれば）鍵Ｋを再構成する、すなわちＫ←Ｒｅｐ（Ｒ′，Ｗ）。鍵の再構成は、Ｃｓ′＝Ｗ１＋Ｒ′を計算し、Ｃの復号アルゴリズムによってＣｓ′をＣｓに復号して、Ｒ＝Ｃｓ＋Ｗ１を回復し、最終的にＫ＝ｈｉ（Ｒ）を計算することにより行う。本発明は、他の種類のヘルパーデータでも機能する。例えば、ＸＯＲではなく、置換を行うことも可能である。

【００２９】

前述の通り、本システムが解決する問題は、患者２０と、測定を行った装置１０または１２の認証である。これは、測定結果を装置ＩＤとユーザの両方にリンクすることにより実現する。Ｃｏｎｔｉｎｕａが認定した各ヘルスケア装置１０、１２は、固有のグローバルＩＤを有する。ユーザと装置を同時認証する方法は主に２つある。第１に、バイオメトリック測定結果をランダムエラー訂正コードＣに直接マッピングし、ヘルパーデータを生成する。しかし、バイオメトリック測定結果を直接マッピングするのではなく、バイオメトリック測定結果と装置１０または１２の固有のグローバルＩＤを共にランダムエラー訂正コードワードにマッピングする。

【００３０】

第２の方法では、装置の固有のグローバルＩＤを、ランダムストリングと組み合わせて、ランダムコードワードにマッピングする。そして、ユーザの登録において、バイオメトリックヘルパーデータの生成の際に、このコードワードを用いる。そのため、バイオメトリック測定結果のヘルパーデータは、装置の固有のグローバルＩＤに依存する。この場合、秘密のコードワードが固有の装置ＩＤに依存するので、装置とユーザを一度に認証することができる。以下に説明するすべての実施形態において、ユーザを識別するストリング（通常、「ｉ」を整数としてＵｉと記す）を用いる。このストリングはユーザの名前、電子メールアドレス、これらの「自然な」識別子の関数（例えば、かかる識別子の下位「ｂ」ビット）であってもよい。

【００３１】

使用する装置１０または１２に関して、以下のアルゴリズムが利用可能であると仮定する：－ＲｅａｓＩＤアルゴリズム。これはコールされると、装置の固有のグローバルＩＤを返す（これはD_{IDi}←ＲｅａｄＩＤ（ｉ）と記す。この記法は装置ｉに対してＲｅａｄＩＤコマンドを実行することを意味する）。－ＧｅｎＢｉｏアルゴリズム。これはユーザＵからバイオメトリック測定結果ＢＭｕを受け取ると（Ｋｕ，Ｗｕ）を出力する（これは（Ｋｕ，Ｗｕ）←ＧｅｎＢｉｏ（ＢＭｕ）と記す）。－ＲｅｐＢｉｏアルゴリズム。これはユーザＵからバイオメトリック測定結果ＢＭｕ′を受け取り、ヘルパーデータＷｕを受け取り、ＢＭｕとＢＭｕ′が十分近いと、鍵Ｋｕを出力する（これはＫｕ←ＲｅｐＢｉｏ（ＢＭｕ′，Ｗｕ）と記す）。

【００３２】

第１の実施形態では、本システムは次のように動作する。ユーザＵ１，Ｕ２，Ｕ３，．．．，Ｕｎのグループが装置ｉを有し、その装置ｉでユーザの信号を測定する。実施形態１の登録手続を図４の左側に示す。ステップＲ１．１は、実施形態１の登録プロセスの最初のステップである。図４の右側には、対応する認証プロセスを示す。ステップＡ１．１は、実施形態１の認証プロセスの最初のステップである。

【００３３】

ステップＲ１．１において、ユーザＵｊが装置ｉを初めて使うとき、ＧｅｎＢｉｏアルゴリズムを実行する前に、D_{IDi}←ＲｅａｄＩＤ（ｉ）するようにアルゴリズムＲｅａｄＩＤを実行する。ＤＩＤを受け取ると、ステップＲ１．２において、バイオメトリックデータＢｍｕｊを取得し、（Ｋｕｉｊ，Ｗｕｉｊ）←ＧｅｎＢｉｏ（ＢＭｕｊ||D_{IDi}）のように、ＢＭｕｊとD_{IDi}にＧｅｎＢｉｏアルゴリズムを実行する。ここで、「||」は、ＢＭｕｊとD_{IDi}の単純な連結またはＸＯＲを表すものとする。ＧｅｎＢｉｏアルゴリズムの出力は、ほぼ一様な鍵Ｋｕｉｊとヘルパーデータ Ｗｕｉｊである。ヘルパーデータＷｕｉｊは、バイオメトリック測定結果ＢＭｕと、装置の固有のグローバルＩＤすなわちD_{IDi}の両方に依存する。これはステップＲ１．３である。

【００３４】

装置ｉを使用したい全てのユーザに対して、ステップＲ１．２とＲ１．３を繰り返す。装置にはエントリー（Ｕｊ；Ｗｕｉｊ）を有するデータベースが格納されている。ここで、Ｕｊはユーザを特定するストリングである。このストリングは、電子メールアドレス、システムが生成した識別子、前記の関数（例えば、ユーザを特定する非常に長い識別子のうちの最下位１６ビット）などであり得る。あるいは、Ｋｕｉｊを用いてヘルパーデータ

にインデックス付けしてもよい。しかし、認証に用いる鍵が暗号化されずに格納されるので、セキュリティの点でこれは望ましくない。これはステップＲ１．４である。

【００３５】

計算した対称鍵「Ｋｕｉｊ」は、ユーザのバイオメトリックと装置のグローバルＩＤの両方に依存し、ステップＲ１．５において、装置ＩＤとユーザＵｊの識別子とともに、ヘルスサービスプロバイダにセキュアな方法で送信される。プライバシーの観点から、異なるステップのＵｊは同じ識別子である必要はない。しかし、その場合、装置またはサーバに格納された識別子間の１対１マッピングが必要である。

【００３６】

実施形態１の認証手続も図４に示した。ユーザＩｊは、装置ｉを用いて測定したいとき、その装置を操作する前に、ステップＡ１．１に示したように、D_{ID_i}←ＲｅａｄＩＤ（）を実行する。D_{ID_i}を得ると、Ｕｊはヘルパーデータを読み出し、それからバイオメトリックデータＢＭｕｊを取得する（ステップＡ１．２）。次に、Ｋｕｉｊ←ＲｅｐＢｉｏ（ＢＭｕｊ'||D_{ID_i}，Ｗｕｉｊ）を実行し、Ｋｕｉｊを回復する（ステップＡ１．３）。

【００３７】

ユーザのデータを測定し、Ｋｕｉｊを用いてそのデータのメッセージ認証コード（ＭＡＣ）を計算する（ステップＡ１．４）。ＭＡＣは専用のＭＡＣでもよいし、鍵利用ハッシュ関数（keyed hash function）であってもよい。ユーザＵｊの識別子（例えば、ユーザＩＤ、電子メールアドレス等）と共にデータとＭＡＣをサービスプロバイダに送る（ステップＡ１．５）。そして、ユーザと装置の認証を行う（ステップＡ１．６）。サービスプロバイダは、自分のデータベースを検索して、ユーザの識別子を探し、ＭＡＣを、このユーザに対して登録されているすべての鍵に対してチェックする。ＭＡＣが、これらの鍵の１つとうまく照合できたら、データを受け入れ、鍵を用いた装置に割り当てる。うまく照合できなければ、データを拒絶し、（任意的に）ユーザに通知を返す。

【００３８】

代替的に、ステップＡ１．５において、ＭＡＣと共に、ユーザＩＤと装置ＩＤを両方とも送信する。次に、サービスプロバイダはシングルＭＡＣをチェックしなければならない。これには、ステップＡ１．５において、追加のデータ帯域幅を用いるという代償が必要である。チャネルによるユーザ識別情報と装置ＩＤの送信に関してプライバシー問題があっても、既存の擬似ランダム化方法や暗号化方法を用いて、その問題を解決できる。ステップＡ１．５で、データとＭＡＣのみを送信し、ステップＡ１．６で、どの装置とユーザがデータを送信したかサーバに調べさせてもよい。

【００３９】

公開鍵暗号を用いる別の方法である実施形態２を図５に示す。このシステムでは、ユーザＵ１，Ｕ２，Ｕ３，．．．，Ｕｎのグループが装置ｉを有し、その装置でユーザの信号を測定するという点で実施形態１と同様である。実施形態２の登録手続を図５の左側に示し、認証手続を図５の右側に示した。

【００４０】

ユーザＵｊが装置ｉを初めて使うとき、ＧｅｎＢｉｏアルゴリズムを実行する前に、D_{ID_i}←ＲｅａｄＩＤ（ｉ）するようにアルゴリズムＲｅａｄＩＤを実行する（ステップＲ２．１）。このユーザの装置は、初期化後、または計算を実行する必要があることを示す信号を受信後、ユーザのための計算を実行する。D_{ID_i}を受け取ると、ＢＭｕｊを取得し（ステップＲ２．２）、（Ｋｕｉｊ，Ｗｕｉｊ）←ＧｅｎＢｉｏ（ＢＭｕｊ||D_{ID_i}）するように、ＢＭｕｊプラスD_{ID_i}にＧｅｎＢｉｏアルゴリズムを実行する。ここで、「||」は、ＢＭｕとD_{ID_i}の単純な連結またはＸＯＲを表すものとする。ＧｅｎＢｉｏアルゴリズムの出力は、ほぼ一様な鍵Ｋｕｉｊとヘルパーデータ Ｗｕｉｊである。ヘルパーデータＷｕｉｊは、バイオメトリック測定結果ＢＭｕと、装置の固有のグローバルＩＤであるD_{ID_i}の両方に依存する。これはステップＲ２．３である。装置を利用したいすべてのユーザに対して、これら２つのステップを繰り返す。装置に記憶されたデータ

ベースにエントリー（Ｕｊ；Ｗｕｉｊ）を格納する（ステップＲ２．４）。

【００４１】

計算された鍵Ｋｕｉｊは、ユーザのバイオメトリックと装置のグローバルＩＤの両方に依存し、ユーザｊと装置ｉのペアの秘密鍵として用いられる。利用する公開鍵暗号によっては、ユーザは、秘密鍵Ｋｕｉｊを入力し、公開鍵Ｋｕｉｊ＿ｐｕｂを出力する公開鍵生成プロセスを実行する。これはステップＲ２．５である。

【００４２】

そして、Ｋｕｉｊ＿ｐｕｂを、装置ＩＤとユーザの識別情報とともに、ヘルスサービスプロバイダにセキュアかつ認証して送信する（ステップＲ２．６）。あるいは、登録段階において、認証局（またはサービスプロバイダ）が、ユーザおよびその装置の公開鍵証明書を生成してもよい（この証明書は、ユーザ識別情報と、装置識別情報と、ユーザと装置のペアの公開鍵Ｋｕｉｊ＿ｐｕｂと、その他の年齢、住所等の個人データ情報とを含む）。これらの情報はすべて認証局の秘密鍵により署名される。自己証明を使う場合、ユーザはこのデータを自分の秘密鍵Ｋｕｉｊで署名する。

【００４３】

実施形態の認証手続では、ユーザＵｊは装置ｉを用いて測定することを望んでいる。ユーザＵｊは、装置を操作する前に、D_{IDi}←ＲｅａｄＩＤ（）を実行する（ステップＡ２．１）。ユーザＵｊは、D_{IDi}を取得すると、ヘルパーデータを読み出し、バイオメトリックデータＢＭｕｊを取得する（ステップＡ２．２）。そして、Ｋｕｉｊ←ＲｅｐＢｉｏ（ＢＭｕｊ'||D_{IDi}，Ｗｕｉｊ）を実行してＫｕｉｊを回復する（ステップＡ２．３）。検出データを測定してＫｕｉｊを用いて署名（sign）する（ステップＡ２．４）。

【００４４】

データと署名は、公開鍵Ｋｕｉｊ＿ｐｕｂを含むユーザ／装置の証明書と共に、サービスプロバイダに送られる。ユーザ／装置の証明書は１度だけ送ればよく、バックエンドシステムに記憶される。これはステップＲ２．５である。サービスプロバイダはそのデータベースを検索してユーザの証明書を探し、署名をチェックする。署名を照合して正しいと、データを受け入れて、用いた鍵に対応するユーザと装置のペア、または（データが正しく生成されているかぎり、ユーザデータを格納できればよいのだから）単にユーザに割り当てる。うまく照合できなければ、データを拒絶し、（任意的に）ユーザに通知を返す。これはステップＲ２．６である。

【００４５】

本実施形態では、ユーザと装置を同時認証（combined user and device authentication）する別の方法も考えられる。主なアイデアは、装置ＤＩＤの固有のグローバルＩＤに基づくヘルパーデータの生成である。各装置は、（ＭＡＣアドレスのような）変更不能な固有のグローバルＩＤを有するものと仮定する。この固有のグローバルＩＤは、別の新しいランダムストリングと連結されて、コードワードＣにマッピングされる。バイオメトリックのヘルパーデータがコードワードＣに基づき生成される。この代替方法を図６に示した。

【００４６】

提案の登録手続では、ユーザＵ１，Ｕ２，Ｕ３，．．．，Ｕｎのグループが装置ｉを有し、その装置がユーザの信号を測定する。ステップＲ３．１において、装置ＩＤ D_{IDi}を取得する。ユーザＵｊは、装置を最初に使う前に、装置ｉＩＤに符号化手続を実行して、Ｃｉ←Ｅｎｃｏｄｅ（D_{IDi}||γｉ）を取得する。ここで、「γｉ」はランダムストリングであり、Ｃｉはコードワードである。これはステップＲ３．２である。各ユーザのランダムストリング「γｉ」は異ならねばならない。γｉの目的は、ヘルパーデータをバイオメトリックのための適切なサイズにすることである。

【００４７】

ユーザＵｊは自分のバイオメトリックデータを取得し（ステップＲ３．３）、ヘルパーデータを生成するために、手続ＧｅｎＨｅｌｐｅｒＤａｔａ（）を実行する。ＧｅｎＨｅ

ｌｐｅｒＤａｔａはステップＲ３．２で生成されたコードワード「Ｃｉ」と、デジタル化されたバイオメトリック測定結果ＢＭｕｊとに作用し、（Ｋｕｉｊ，Ｗｕｊ，ｉ）←ＧｅｎＢｉｏ′（Ｃｉ，ＢＭｕｊ）を生成する。次に、Ｃｉを、バイオメトリックシステムにおける擬似識別情報の生成に使われるランダムネス（randomness）として用いる。これはステップＲ３．４である。装置を利用したいすべてのユーザに対して、このステップを繰り返す。装置に記憶されたデータベースにエントリー（Ｕｊ；Ｗｕｊ，ｉ）を格納する（ステップＲ３．５）。Ｋｕｉｊの値を、装置ＩＤ D_{IDi} とユーザ名Ｕｊと共に、セキュアかつ認証された方法で、サーバに送る（ステップＲ３．６）。

【００４８】

この方法の認証手順も図６に示した。ユーザＵｊは、装置ｉを用いて測定することを望んでいる。ユーザＵｊは、D_{IDi} ←ＲｅａｄＩＤ（）のように装置ＩＤを読み出す。これがステップＡ３．１である。ユーザＵｊは、バイオメトリック測定を行い、ローカルデータベースから装置ＩＤ D_{IDi} に対応するヘルパーデータを回復する（ステップＡ３．２）。Ｋｕｉｊ←ＲｅｐＢｉｏ（ＢＭｕｊ′，Ｗｕｊ，ｉ）を実行し、Ｋｕｉｊを回復する（ステップＡ３．３）。手続ＲｅｐＢｉｏ中に、コードワードＣｉを再構成しなければならない。このように、コードワードＣｉの第１部分が D_{IDi} に対応するかチェックすることができる（ステップＡ３．４）。対応しなければ、認証手続を中止するか、ユーザに警告を送る。

【００４９】

装置ｉは、秘密鍵Ｋｕｉｊを用いて、測定したデータのメッセージ認証コード（ＭＡＣ）を計算し（ステップＡ３．５）、データとＭＡＣを、ユーザＩＤ及び（場合によって）装置ＩＤとともに、ヘルスサービスプロバイダに送る（ステップＡ３．６）。ヘルスサービスプロバイダは、ユーザと装置のＩＤに対応する鍵を読み出すことによりＭＡＣを確認（verify）し、確認できればデータを受け入れる（ステップＡ３．７）。実施形態１と同様に、ＭＡＣの替わりに、公開鍵方式（public-key primitives）（署名）を使うように、この登録と認証の手続を変更することは容易である。

【００５０】

もっとセキュアな変形例も可能である。上記の手続により、装置ＩＤ D_{IDi} を知ると、第三者はユーザのバイオメトリックスに関する情報の一部を取得できてしまう。これを避けるため、図７に示したように、次のバリエーションを実行することができる。

【００５１】

登録手順において、前述の通り、ユーザＵ１，Ｕ２，Ｕ３，．．．，Ｕｎのグループが装置ｉを有し、その装置がユーザの信号を測定する。ステップＲ４．１において、装置ＩＤ D_{IDi} を取得する。ユーザＵｊは、装置を最初に使う前に、装置ｉＩＤの関数とノンス（nonce）に符号化手順を実行して（この関数は、例えば、ハッシュ関数でもよいし、ＩＤを表すビットの一部でもよい）、Ｃｉ←Ｅｎｃｏｄｅ（ｆ（$D_{IDi}||\gamma i$））を取得する。ここで、「γｉ」はランダムストリングであり、Ｃｉはコードワードである。各ユーザのランダムストリング「γｉ」は異ならねばならない。γｉの目的は２つある。すなわち、（ｉ）ヘルパーデータをバイオメトリックに適したサイズにすること、及び（ｉｉ）装置ＩＤが分かっても、Ｃｉを予測できないようにすることである。ランダムなノンスγｉは秘密にしておかなければならない。関数ｆはその引数の任意の関数である。好ましくは、（ＳＨＡ－１、ＳＨＡ－２等の）ハッシュ関数などの暗号的にセキュアな片方向関数である。これはステップＲ４．２である。

【００５２】

ユーザＵｊは自分のバイオメトリックデータを取得し（ステップＲ４．３）、ヘルパーデータを生成するために、手続ＧｅｎＨｅｌｐｅｒＤａｔａ（）を実行する。ＧｅｎＨｅｌｐｅｒＤａｔａはステップＲ１で生成されたコードワード「Ｃｉ」と、デジタル化されたバイオメトリック測定結果ＢＭｕｊとに次のように作用する：（Ｋｕｉｊ，Ｗｕｊ，ｉ）←ＧｅｎＢｉｏ′（Ｃｉ，ＢＭｕｊ）。次に、Ｃｉを、バイオメトリックシステムにおける擬似識別情報の生成に使われるランダムネス（randomness）として用いる。これはス

テップＲ４．３である。装置を利用したいすべてのユーザに対して、このステップを繰り返す。装置に記憶されたデータベースにエントリー（Ｕｊ；Ｗｕｊ，ｉ）を格納する（ステップＲ４．５）。

【００５３】

ステップＲ４．６として、リモートサービスに、セキュアかつ認証を受けた方法で、次の値（D_{IDi}，γｉ，Ｕｊ）を送る。必ずしも必要ではないが、Ｋｕｉｊをサーバに送ることも可能である。場合によっては、Ｋｕｉｊを送ると、サーバに対して性能的に有利になることもある。サーバは、データを受け取るたびに新しい鍵を計算する必要がないからである。また、こうすることにより、ユーザのバイオメトリック測定結果が外部に漏れることを防止できる。一方、トリプレット（triplet）（D_{IDi}，γｉ，Ｕｊ）を送ると、２つの理由によりセキュリティ面で有利になる。第１に、攻撃者がサーバの情報を漏えいしても、鍵Ｋｕｉｊは漏れない。第２に、新しいデータセットごとに鍵を再計算するので、システムがエラートレラントになる。しかし、この変形例には、ユーザのバイオメトリックが漏れるという欠点がある。すなわち、この方法はプライバシーを保てない。

【００５４】

図７の、対応する認証手続は次のように働く。ユーザＵｊは、装置ｉを用いて測定することを望んでいる。ユーザＵｊは、D_{IDi}←ＲｅａｄＩＤ（）のように装置ＩＤを読み出す（ステップＡ４．１）。ユーザＵｊは、バイオメトリック測定を行い、ローカルデータベースから自分のユーザＩＤ　Ｕｊに対応するヘルパーデータを回復する（ステップＡ４．２）。Ｋｕｉｊ←ＲｅｐＢｉｏ（ＢＭｕｊ′，Ｗｕｊ，ｉ）を実行し、Ｋｕｉｊを回復する（ステップＡ４．３）。

【００５５】

装置ｉは、秘密鍵Ｋｕｉｊを用いて、測定したデータのメッセージ認証コード（ＭＡＣ）を計算し（ステップＡ４．４）、データとＭＡＣを、ユーザＩＤ及び関連するヘルパーデータＷｕｊ，ｉとともに、ヘルスサービスプロバイダに送る（ステップＡ４．５）。ヘルスサービスプロバイダは、（D_{IDi}，γｉ，Ｕｊ）と、ユーザ及び装置のＩＤに対応するヘルパーデータＷｕｊ，ｉとから鍵Ｋｕｉｊを再計算することにより、ＭＡＣを確認（verify）し、確認できれば、データを受け入れる。これはステップＲ４．６である。認証手続においてユーザにより送られたヘルパーデータＷｕｊ，ｉに対応するＩＤを検索することにより、サービスプロバイダには装置のＩＤが分かる。（登録手続４に示したように）鍵Ｋｕｉｊがサーバのデータベースにすでに格納されていれば、Ｋｕｉｊを再計算する必要はない。

【００５６】

ユーザは、医療上の測定をするのに用いた装置のＩＤを秘密にして、知っているのはサービスプロバイダだけにしたいと欲する場合がある。この場合、次の実施形態を使える。この実施形態の基本的なアイデアは、バイオメトリックにより求めた鍵を用いて、装置ＩＤの関数を計算することである。その関数の正しい値は、用いたバイオメトリックに対応するユーザでないと計算できない。鍵としてバイオメトリックにより求めた秘密鍵を用いて、装置ＩＤの関数を計算する。

【００５７】

この手続における登録と認証を図８に示す。ユーザＵ１，Ｕ２，Ｕ３，．．．，Ｕｎのグループは装置ｉを有し、その装置でユーザの信号を測定する。ステップＲ５．１において、装置ＩＤ　D_{IDi}を読み取る。ユーザＵｊは、自分のバイオメトリックを測定し（ステップＲ５．２）、（Ｋｕｊ，Ｗｕｊ）←ＧｅｎＢｉｏ（ＢＭｕｊ）のようにヘルパーデータと鍵を生成する（ステップＲ５．３）。ヘルパーデータＷｕｊは、バイオメトリック再構成を行うところに格納される。例えば、装置からすべての測定結果を集めて、サーバに送るホームハブに格納される。これはステップＲ５．４である。

【００５８】

ユーザＵｊは、ステップＲ５．５において、サーバに、Ｋｕｊと、装置ｉのＩＤに対応するD_{IDi}を送る。ステップＲ５．３は、装置を利用したいすべてのユーザに対して繰

り返される。ユーザにより情報（Ｋｕｊ；D_{IDi}，Ｕｊ）がサーバに送られる。装置にはエントリー（Ｋｕｊ；D_{IDi}；Ｕｊ）を有するデータベースが格納されている。ここで、Ｕｊはユーザを特定するストリングである。

【００５９】

対応する認証手続を図８の右側に示した。ユーザＵｊは、装置ｉを用いて測定することを望んでいる。ステップＡ５．１において、装置ＩＤ D_{IDi}を読み取る。ユーザは、ステップＡ５．２において、バイオメトリック測定をして、記憶したヘルパーデータも取得する。ユーザＵｊは、装置を操作する前に、Ｋｕｊ←ＲｅｐＢｉｏ（ＢＭｕｊ，Ｗｕｊ）を実行し、Ｋｕｊを回復する。Ｋｕｊを用いて装置ＩＤ D_{IDi}を暗号化して、ｙｉ←ＥｎｃＫｕｊ（D_{IDi}）を生成する。一般的に、D_{IDi}とＫｕｊの関数はＫｕｊが分からないと可逆ではない。これはステップＡ５．３である。多くの場合D_{IDi}は公開された値なので、非可逆性は重要である。リプレイ攻撃の影響を受けにくくするため、ｙｉ←ｆ（Ｋｕｊ，D_{IDi}，γｉ）を計算できる。ここで、γｉはノンス（nonce）、または適当な関数ｆのカウンタである。関数ｆは、例えば、署名、ハッシュ関数、または暗号化関数である。

【００６０】

装置ｉは、秘密鍵Ｋｕｉｊを用いて、測定したデータと暗号化したｙｉのメッセージ認証コード（ＭＡＣ）を計算し（ステップＡ５．４）、データとｙｉとＭＡＣを、ユーザＵｊを識別するストリングと共に、ヘルスサービスプロバイダに送る。これはステップＡ５．５である。同等な公開鍵方式をつかってもよい。ヘルスサービスプロバイダは、ステップＡ５．６において、ＭＡＣを確認し、Ｋｕｊを用いてｙｉを復号し、その結果がデータベース中の装置D_{IDi}に対応することを確認し、確認できればデータを受け入れる。

【００６１】

効率がもう少し低いバリエーションも可能である。計算した装置ヘルパーデータを用いて装置とユーザの認証を行うことも可能である。これを、図９を参照して以下に説明する。図９の左側の登録プロセスをまず説明する。ユーザＵ１，Ｕ２，Ｕ３，．．．，Ｕｎのグループは装置ｉを有し、その装置でユーザの信号を測定する。最初に装置ＩＤを読み出す（ステップＲ６．１）。ユーザＵｊは、自分のバイオメトリックを測定し（ステップＲ６．２）、（Ｋｕｊ，Ｗｕｊ）←ＧｅｎＢｉｏ（ＢＭｕｊ）のようにヘルパーデータと鍵を生成する（ステップＲ６．３）。ステップＲ６．４において、ヘルパーデータＷｕｊは、バイオメトリック再構成を行うところに格納される。例えば、装置からすべての測定結果を集めて、サーバに送るホームハブに格納される。

【００６２】

登録の次のステップはＲ６．５であり、秘密のランダムな値Ｋｉを生成する。追加のヘルパーデータＷｉ，ｕｊをＷｉ，ｕｊ＝Ｋｉ＋Ｋｕｊで生成する。ここで、「＋」はＫｉとＫｕｊのＸＯＲを示す。データＷｉ，ｕｊを、測定する装置またはハブに格納する。装置を利用したいすべてのユーザに対して、これらステップを繰り返す。ステップＲ６．６において、ユーザにより情報（ｆ（Ｋｕｊ，Ｋｉ，D_{IDi}）；D_{IDi}，Ｕｊ）がサーバに送られる。ここで、ｆは、前述の実施形態と同様に、ＫｕｊとＫｉ（及び、場合によってはランダムなノンスまたは非反復的カウンタ）の何らかの関数である。装置に格納されたデータベースにエントリー（ｆ（Ｋｕｊ，Ｋｉ，D_{IDi}）D_{IDi}，Ｕｊ）が記憶される。ここで、Ｕｊはユーザの識別子である。

【００６３】

対応する認証手続は次のように働く。ユーザＵｊは、装置ｉを用いて測定を実行することを望んでいる。そして、ステップＡ６．１において、装置ＩＤを取得する。ユーザＵｊは、装置を操作する前に、自分のバイオメトリックデータを取得し（ステップＡ６．２）、Ｋｕｊ←ＲｅｐＢｉｏ（ＢＭｕｊ，Ｗｕｊ）を実行し、Ｋｕｊを回復する。Ｋｉ＝Ｗｉ，ｕｊ＋Ｋｕｊを計算することにより値Ｋｉを回復する。これはステップＡ６．３である。鍵Ｋｕｊ，ｉは、Ｋｕｊ，ｉ←ｆ（Ｋｕｊ，Ｋｉ，D_{IDi}）のように求める。ステップＡ６．４ないしＡ６．６で詳細に説明したように、前述の実施形態と同様の動作を実行

する（データに関するＭＡＣの計算、データとＭＡＣのサーバへの送信、サーバ側における適当な値の確認）。

【００６４】

ＭＡＣまたは署名の計算に関して、すべてのプロトコルを説明した。同様に、暗号を計算し、データの暗号によるＭＡＣをサービスプロバイダに送ることもできる。そうすると、２つの鍵を求める必要がある。これは、追加的なランダム値（randomness）を用いて、追加的なバイオメトリックの登録手続を実行する（すなわち、バイオメトリック測定結果から第２の鍵を求める）ことにより、容易に実現できる。秘密共有方式を用いて、ユーザごとに、一ファミリーの装置について１つの鍵を計算できる。

【００６５】

本発明の様々な実施形態にはいくつかの優位性がある。最も重要なのは、このアプローチにより、どの装置とユーザからデータが得られたのか認証できる。データの出所を明らかにするとき、システムは、強い認証メカニズムにより取得できる装置とユーザの識別子を、固有のグローバル装置ＩＤとバイオメトリックスを用いて、とても早く結合する。このアプローチでは、鍵の導出は１ステップで実行され、信頼性が高くなる。さらに、ユーザ・装置ペアごとに鍵をサービスプロバイダに登録する必要があるので、このアプローチは有利である。これは責任の分離を支持するものである。サービスプロバイダまたはＥＨＲインフラストラクチャは、測定装置の登録に関与しなくてよい。最後に、実施する実施形態に応じて、まだ登録していないユーザを識別することができ、測定データの信頼性にも貢献する。

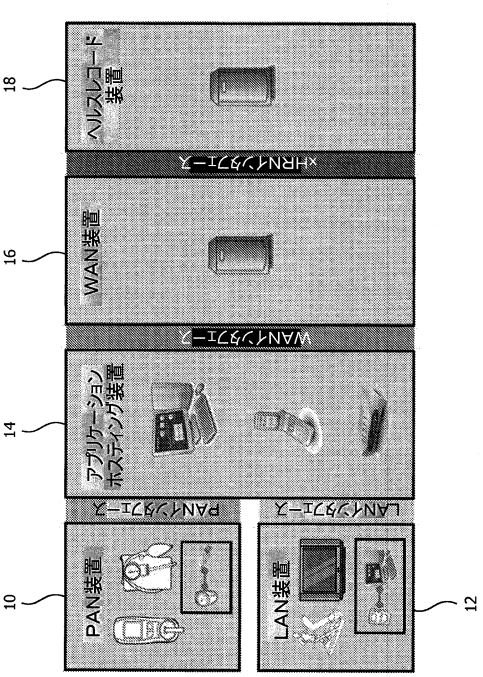
【００６６】

本発明の好ましい実施形態を図１０に示す。この図では、アプリケーションホスティング装置１４とホームハブが、検出装置１０と、バイオメトリック測定装置２６に接続されている。装置１０は、ユーザ２０の検出データ４０（本例では血圧）を測定する装置である。バイオメトリック測定装置２６は、ユーザ２０が装置２６に指を載せた時に、ユーザ２０の指紋を測定する装置である。この図のシステムは、登録プロセスがすでに行われ、ユーザ２０は装置１０で自分の血圧を測定したものと仮定する。ユーザ２０は、第３者のヘルスサービスプロバイダに、取得した検出データ４０を送信する前に、取得した検出データ４０を認証したいと思っている。

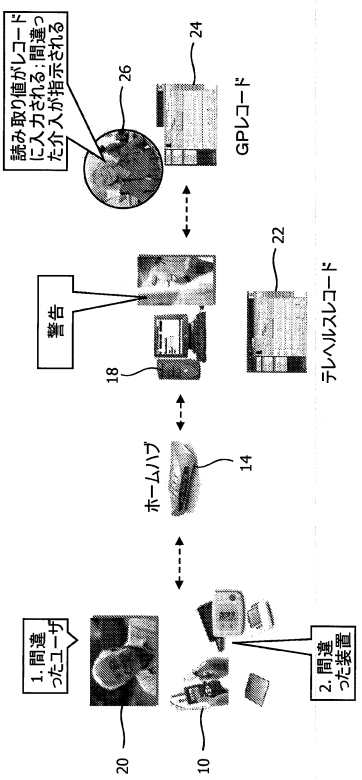
【００６７】

図１０ｂは、プロセッサ２８の動作を示す。このプロセッサ２８はホスティング装置１４の一部である。プロセッサ２８は、バイオメトリック測定装置２６から、ユーザの指紋のバイオメトリック測定結果３０を受け取る。装置ＩＤ３２も、装置１０へのクエリにより受け取られる。本システムには、装置１０にクエリをするクエリコンポーネントがある。このコンポーネント（図示せず）は装置１０内に設けてもよい。バイオメトリック測定結果３０は、ユーザヘルパーデータ３４と結合され、及びこの好ましい実施形態では、装置ＩＤ３２とも結合され、鍵３６を生成する。鍵３６を用いてメッセージ３８を生成する。メッセージ３８は検出データ４０を含み、リモートサービスに送信される。ユーザ２０と装置１０の認証が行われる。ユーザ２０と装置１０画セキュアに特定されているので、メッセージ３８に含まれるデータ４０は信頼できるものである。

【図１】



【図２】



【図３】

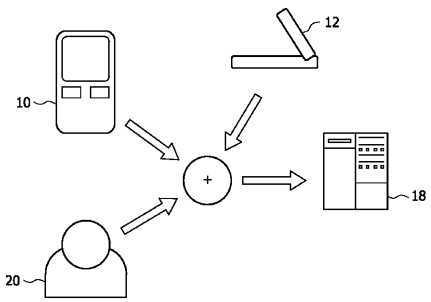
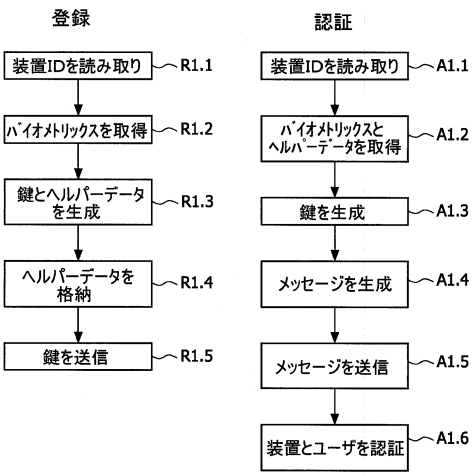
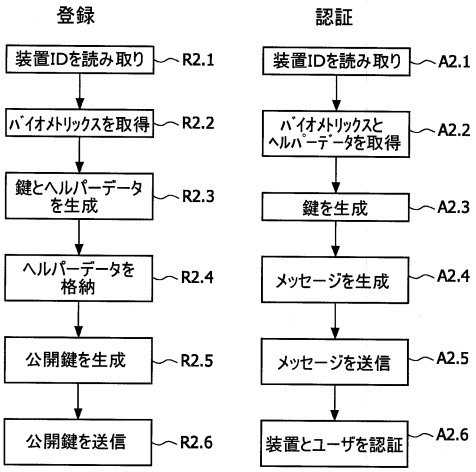


FIG. 3

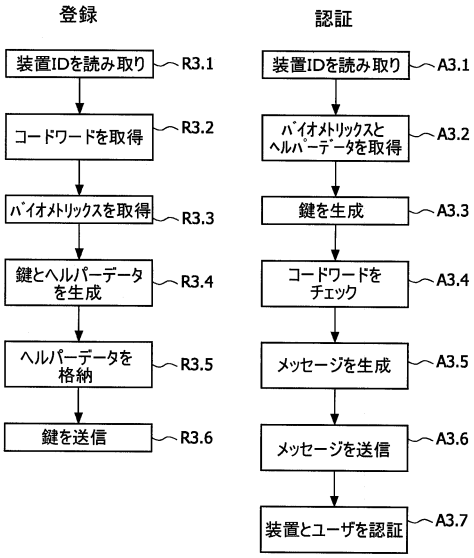
【図４】



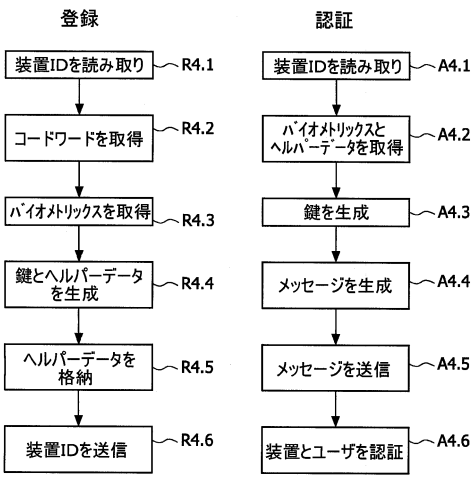
【図５】



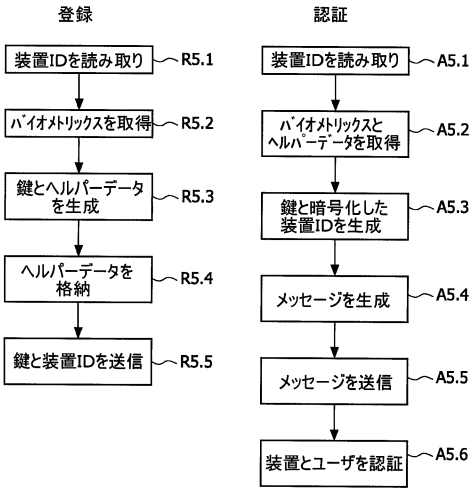
【図６】



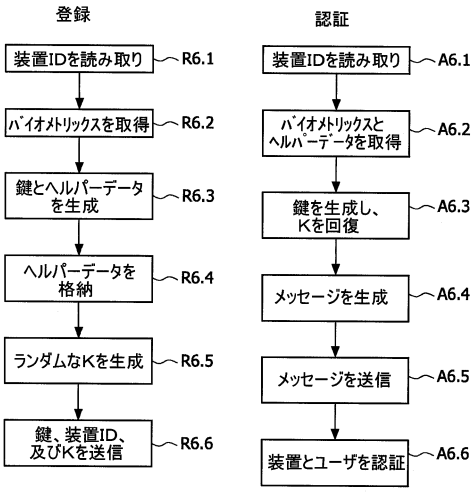
【図７】



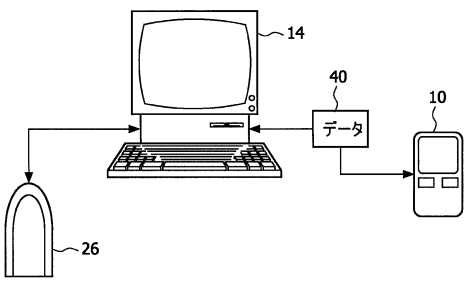
【図８】



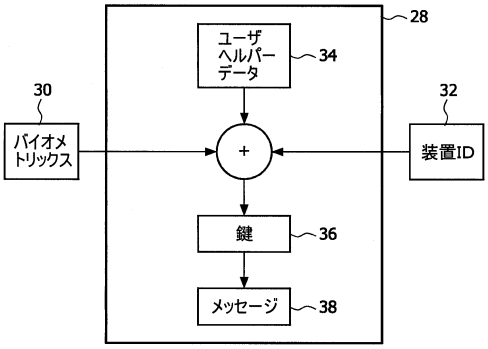
【図９】



【図１０ａ】



【図１０ｂ】



フロントページの続き

(72)発明者 アシム，ムハマド
オランダ国，５６５６ アーエー アインドーフェン，ハイ・テク・キャンパス ４４，フィリップス・アイピー・アンド・エス－エヌエル内
(72)発明者 グアハルド，メルチャン ホルヘ
オランダ国，５６５６ アーエー アインドーフェン，ハイ・テク・キャンパス ４４，フィリップス・アイピー・アンド・エス－エヌエル内
(72)発明者 ペトコヴィチ，ミラン
オランダ国，５６５６ アーエー アインドーフェン，ハイ・テク・キャンパス ４４，フィリップス・アイピー・アンド・エス－エヌエル内

審査官 打出 義尚

(56)参考文献 特表２００８－５２６０８０（ＪＰ，Ａ）
特表２００８－５１６４７２（ＪＰ，Ａ）
特表２００２－５４１５３３（ＪＰ，Ａ）
特表２００８－５０２０７１（ＪＰ，Ａ）
特表２００９－５１５２７０（ＪＰ，Ａ）
特表２００９－５３３７４２（ＪＰ，Ａ）
特表２０１２－５０３８１４（ＪＰ，Ａ）
国際公開第２００７／１１６３６８（WO，Ａ１）
国際公開第２０１０／０３５２０２（WO，Ａ１）
山崎 恭，４．脆弱性の解消に向けた最新対策技術の動向 １．安全性対策技術の動向，情報処理，日本，社団法人情報処理学会，２００６年 ６月１５日，第４７巻 第６号，ｐ．６００～６０４
泉 昭年 他，公開鍵暗号基盤における匿名バイオメトリクスを用いた秘密鍵管理の提案，情報処理学会研究報告 ２００７－ＣＳＥＣ－３８ コンピュータセキュリティ，日本，社団法人情報処理学会，２００７年 ７月１９日，Ｖｏｌ．２００７ Ｎｏ．７１，ｐ．１５３～１５８
Jean-paul Linnartz et al, New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates, [online], ２００３年, ［平成２６年３月１４日検索］，インターネット<URL: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.84.6261>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００