

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-142614

(P2017-142614A)

(43) 公開日 平成29年8月17日(2017.8.17)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/32 (2013.01)	G06F 21/32	5B043
G06T 7/00 (2017.01)	G06T 7/00 530	5E555
G06F 21/31 (2013.01)	G06F 21/31	
G06F 3/01 (2006.01)	G06F 3/01 510	

審査請求 有 請求項の数 5 O L (全 12 頁)

(21) 出願番号	特願2016-22918 (P2016-22918)	(71) 出願人	505205731 レノボ・シンガポール・プライベート・リミテッド
(22) 出願日	平成28年2月9日(2016.2.9)		シンガポール 556741、ニューテックパーク、#02-01、ローロンチュアン 151
(11) 特許番号	特許第6139719号 (P6139719)	(74) 代理人	100112737 弁理士 藤田 考晴
(45) 特許公報発行日	平成29年5月31日(2017.5.31)	(74) 代理人	100140914 弁理士 三舌 貴織
		(74) 代理人	100136168 弁理士 川上 美紀
		(74) 代理人	100169199 弁理士 石本 貴幸

最終頁に続く

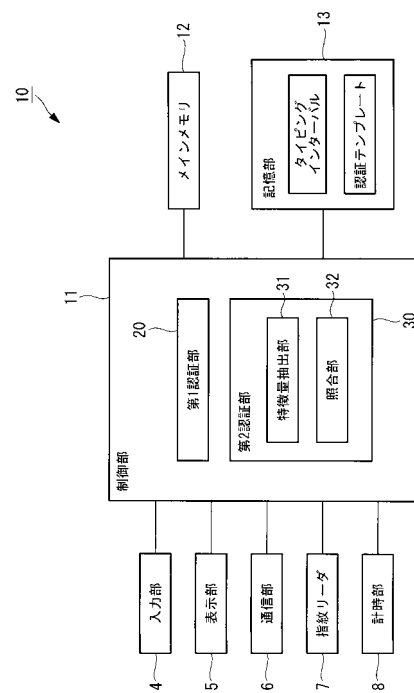
(54) 【発明の名称】 情報処理装置

(57) 【要約】 (修正有)

【課題】 利便性を損なわずに、セキュリティレベルを高めることのできる情報処理装置を提供する。

【解決手段】 ノートPC 10は、第1認証部20、記憶部13、計時部18、特徴量抽出部31及び照合部32を備える。記憶部13には、ユーザ本人の指紋の特徴量とタイピングインターバルの特徴量を含む認証テンプレートが予め登録されている。第1認証部20は、指紋リーダー17により読み取られた指紋の特徴量を認証テンプレートと照合し、本人認証を行う。本人であると判定された場合はログインが許可される。ログイン後、ユーザによりキーボードが操作されると、計時部18は、各キー入力の時間間隔を計時し、この時間間隔をタイピングインターバルとして記憶部13に格納する。特徴量抽出部31は、格納されたタイピングインターバルを分析して特徴量を抽出する。照合部32は、抽出された特徴量を認証テンプレートと照合し、本人か否かを判定する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

第 1 認証手段と、

タイピング時におけるユーザの挙動データを用いてユーザ認証を行う第 2 認証手段とを備える情報処理装置。

【請求項 2】

前記第 2 認証手段は、タイピング速度、タイピング強さ、タイピング時のパーム位置、及びタイピング時におけるユーザの姿勢の少なくともいずれか一つを用いてユーザ認証を行う請求項 1 に記載の情報処理装置。

【請求項 3】

前記第 2 認証手段は、

キー入力の時間間隔を前記挙動データとして取得する計時手段と、

前記計時手段によって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、

特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段と

を備える請求項 1 または請求項 2 に記載の情報処理装置。

【請求項 4】

前記第 2 認証手段は、タイピングの強さを前記挙動データとして取得する圧力センサと、

前記圧力センサによって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、

特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段と

を備える請求項 1 または請求項 2 に記載の情報処理装置。

【請求項 5】

前記第 2 認証手段は、

キーボードに設けられた加速度センサと、

前記加速度センサによって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、

特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段と

を備える請求項 1 または請求項 2 に記載の情報処理装置。

【請求項 6】

前記第 2 認証手段は、

タイピング時におけるユーザの姿勢に関する挙動データを取得する撮像手段と、

前記撮像手段によって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、

特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段と

を備える請求項 1 または請求項 2 に記載の情報処理装置。

【請求項 7】

前記特徴量抽出手段は、予め登録されている特定の単語またはフレーズが入力されたときの前記挙動データを用いて特徴量を抽出する請求項 3 から請求項 6 のいずれかに記載の情報処理装置。

【請求項 8】

前記第 2 認証手段は、ユーザ認証に失敗した場合に、前記第 1 認証手段によるユーザ認証をユーザに要求する請求項 1 から請求項 7 のいずれかに記載の情報処理装置。

【請求項 9】

第 2 認証手段は、タイピング時におけるユーザの挙動データを用いてユーザ認証を繰り返し

10

20

30

40

50

返し行う請求項 1 から請求項 8 のいずれかに記載の情報処理装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置に関するものである。

【背景技術】

【0002】

パーソナルコンピュータ、ノート PC、タブレット型パーソナルコンピュータ、スマートフォン、PDA (Personal Digital Assistance)、電子書籍閲覧端末等の情報処理装置には、第三者の不正なアクセスを防止するためにユーザ認証機能が設けられている。主な認証手法として、例えば、パスワードによる認証や、指紋等の生体特徴を利用した生体認証などがある。

また、情報処理装置では、ユーザ認証が一旦行われた後において、一定期間以上、ユーザによってキー操作等がされなかった場合には、スクリーンセーバを表示させたり、サスペンド状態に遷移させたりすることにより、画面に表示されているデータを第三者に見られないようにしている。そして、スクリーンセーバ等から復帰する際には、パスワード等によるユーザ認証が再び要求される。

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2012-150625 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

ところで、上述したスクリーンセーバを起動させるまでの待ち時間やサスペンド状態へ遷移させるまでの待ち時間は、ユーザが自由に設定できるようになっている。利便性を重視する場合、待ち時間を長めに設定すればよいが、待ち時間が長いほど、セキュリティレベルは低下する。例えば、ログイン状態が維持されたままユーザが席を離れた場合、待ち時間が長く設定されていればいるほど、第三者に使用されるリスクは高まる。その一方で、安全性を重視し、待ち時間を短めに設定した場合には、パスワード等の入力が頻繁に要求されることとなり、ユーザの負担が大きく、利便性が損なわれる。

【0005】

本発明は、このような事情に鑑みてなされたものであって、利便性を損なわずに、セキュリティレベルを高めることのできる情報処理装置を提供することを目的とする。

【課題を解決するための手段】

【0006】

本発明は、第 1 認証手段と、タイピング時におけるユーザの挙動データを用いてユーザ認証を行う第 2 認証手段とを備える情報処理装置を提供する。

【0007】

本発明によれば、第 1 認証手段によるユーザ認証に加えて、第 1 認証手段とは異なる第 2 認証手段によるユーザ認証も行われるので、セキュリティレベルを向上させることができる。また、第 2 認証手段は、タイピング時におけるユーザの挙動データを取得し、この取得した挙動データに基づいてユーザ認証を行うので、ユーザ認証のための特別なデータ入力をユーザに要求することなく、ユーザ認証を実施することができる。

【発明の効果】

【0008】

本発明によれば、利便性を損なうことなく、セキュリティレベルを高めることができるという効果を奏する。

【図面の簡単な説明】

【0009】

10

20

30

40

50

【図 1】本発明の第 1 実施形態に係る情報処理装置の概略構成を示した図である。

【図 2】本発明の第 1 実施形態に係る情報処理装置により実行されるユーザ認証の手順を示したフローチャートである。

【図 3】本発明の第 2 実施形態に係る情報処理装置の概略構成を示した図である。

【図 4】本発明の第 3 実施形態に係る情報処理装置の概略構成を示した図である。

【発明を実施するための形態】

【0010】

以下に、本発明の各実施形態に係る情報処理装置について、図面を参照して説明する。情報処理装置の一例として、パーソナルコンピュータ、ノート PC、タブレット型パーソナルコンピュータ、スマートフォン、PDA (Personal Digital Assistance)、電子書籍閲覧端末等が挙げられるが、本実施形態では情報処理装置としてノート PC を使用した場合について説明する。

10

【0011】

〔第 1 実施形態〕

図 1 は、本発明の第 1 実施形態に係るノート PC 10 の概略構成を示した図である。図 1 に示すように、ノート PC 10 は、制御部 11、メインメモリ 12、記憶部 13、入力部 14、表示部 15、通信部 16、指紋リーダ 17、計時部 18 等を備えており、各部はバスを介して電氣的に接続されている。

【0012】

メインメモリ 12 は、例えば、キャッシュメモリ、RAM (Random Access Memory) 等の書き込み可能なメモリで構成され、制御部 11 の実行プログラムの読み出しや実行プログラムによる処理データの書き込み等を行う作業領域として利用される。

20

【0013】

記憶部 13 は、例えば、ROM (Read Only Memory)、HDD (Hard Disk Drive)、フラッシュメモリ等であり、例えば、Windows (登録商標)、iOS (登録商標)、Android (登録商標) 等のノート PC 10 全体の制御を行うための OS、周辺機器類をハードウェア操作するための各種ドライバ、特定業務に向けられたアプリケーション、及び各種データやファイル等を格納する。

【0014】

入力部 14 は、ユーザが入力操作を行うためのユーザインターフェースであり、例えば、各種キーにより構成されるキーボード、及び画面上のカーソルを移動させたり、各種メニューを選択したりするためのポインティング・スティックやマウス等で構成される。また、キーボードはフィジカルキーボードであってもよいし、タッチパネル等に各種キーが表示されるソフトウェアキーボードであってもよい。

30

表示部 15 は、例えば、液晶表示装置であり、制御部 11 の制御に従って表示を行う。

【0015】

指紋リーダ 17 は、後述する第 1 のユーザ認証に用いられ、ユーザの指紋を読み取り、読み取った指紋情報を制御部 11 に出力する。

計時部 18 は、後述する第 2 のユーザ認証に用いられ、例えば、ユーザによってキーボードが操作された場合に、各キー入力の時間間隔を計時し、この時間時間をタイピングインターバルとして記憶部 13 に格納する。

40

【0016】

制御部 11 は、例えば、CPU (Central Processing Unit)、マイクロプロセッサ、DSP 等であり、ノート PC 10 の動作を統括的に制御して各種の処理を実現する。具体的には、制御部 11 は、バスを介して接続された記憶部 13 に格納された OS (Operating System) によりノート PC 10 全体の制御を行うとともに、記憶部 13 に格納された各種プログラムを実行することにより各種処理を実現する。

更に、制御部 11 は、記憶部 13 に格納されている第 1 認証プログラム、第 2 認証プロ

50

グラム等をメインメモリ 12 に展開して実行することにより、第 1 認証部 20、第 2 認証部 30 として機能する。

【0017】

第 1 認証部 20 は、指紋リーダ 17 によって読み取られた指紋の特徴量と、予め記憶部 13 に登録されているユーザ本人の指紋の特徴量とを照合し、本人認証を行う。なお、指紋認証に関する処理については、公知の技術であるため、詳細は省略する。

【0018】

第 2 認証部 30 は、タイピング入力時におけるユーザの挙動データに基づいてユーザ認証を繰り返し行う。本実施形態において、挙動データは、ユーザのタイピング速度に関するデータである。具体的には、第 2 認証部 30 は、記憶部 13 に格納されたタイピングインターバルのデータを分析して特徴量を抽出する特徴量抽出部 31 と、特徴量抽出部 31 によって抽出された特徴量と予め記憶部 13 に登録されているユーザ本人の特徴量である認証テンプレートとを照合し、本人か否かを判定する照合部 32 とを備えている。

10

【0019】

次に、本実施形態に係るノート PC 10 のユーザ認証に係る処理手順について図 2 を参照して説明する。図 2 は、本実施形態に係るノート PC 10 により実行されるユーザ認証の手順を示したフローチャートである。

図 2 に示すように、ログイン時に指紋リーダ 17 及び第 1 認証部 20 による指紋認証が行われる（ステップ S A 1）。この結果、本人ではないと判定された場合は（ステップ S A 2 において「NO」）、ログインが拒否され（ステップ S A 3）、本人であると判定された場合は（ステップ S A 2 において「YES」）、ログインが許可される（ステップ S A 4）。

20

【0020】

ログインが許可され、ユーザによってキーボードからキー入力となされると、計時部 18 によってタイピングインターバルが計時され、記憶部 13 に格納される（ステップ S A 5）。続いて、ユーザのキー入力開始または前回の認証時から所定期間が経過したか否かが判定され（ステップ S A 6）、所定期間が経過した場合に（ステップ S A 6 において「YES」）、特徴量抽出部 31 による特徴量の抽出が行われる（ステップ S A 7）。例えば、特徴量抽出部 31 は、記憶部 13 に格納されているタイピングインターバルのデータを読み出し、横軸に絶対時間、縦軸にタイムインターバルをプロットしたグラフを作成し、これを周波数分析することにより、特徴量を抽出する。

30

【0021】

照合部 32 は、特徴量抽出部 31 によって抽出された特徴量と記憶部 13 に予め登録されているユーザの特徴量である認証テンプレートとを照合し、本人であるか否かを判定する（ステップ S A 8）。この結果、本人であると判定した場合には（ステップ S A 8 において「YES」）、ステップ S A 5 に戻る。これにより、今回の認証から所定期間経過後に、ユーザ認証が再び行われることとなる。ここで、照合部 32 は、認証が終了する度に、記憶部 13 に格納されているタイピングインターバルを消去することとしてもよい。これにより、タイピングインターバルによりメモリが圧迫されることを回避することができる。

40

一方、ステップ S A 8 において、本人でないと判定した場合には、ステップ S A 1 に戻り、指紋による認証がユーザに要求される。

【0022】

このように、本実施形態に係るノート PC 10 によれば、指紋認証を行う第 1 認証部 20 と、タイピング時のユーザの挙動データであるタイピングインターバルに基づいてユーザ認証を行う第 2 認証部 30 とを有し、第 1 認証部 20 によって認証が行われた後においても、第 2 認証部 30 によって認証が繰り返し行われる。これにより、ログイン状態のままユーザが席を立ち、その後、第三者によってノート PC が使用されてタイピングが行われた場合には、そのタイピングインターバルの特徴量から第三者であることを判別することが可能となる。これにより、第 1 認証部 20 のみによるユーザ認証を有している情報処

50

理装置に比べて、セキュリティレベルを向上させることが可能となる。

【0023】

更に、第2認証部30は、ユーザのタイピング時におけるタイピングインターバルからユーザ認証を行うので、ユーザは認証のために特別な入力や作業を行う必要がない。したがって、認証に対する煩わしさを解消することができる。このように、本実施形態に係るノートPC10によれば、ユーザのタイピング時における行動的特徴（癖）を用いてユーザ認証を行うことにより、利便性を損なうことなく、セキュリティレベルを上げることが可能となる。

【0024】

なお、本実施形態では、特徴量抽出部31は、一定の時間間隔で特徴量の抽出を行う場合について述べたが、特徴量を抽出するタイミングは上記例に限定されない。例えば、記憶部13に格納されたタイピングインターバルのデータ量が所定量以上となった場合に特徴量の抽出を行うこととしてもよい。

【0025】

また、本実施形態では、第1認証部20が指紋を用いてユーザ認証を行う場合を例示したが、第1認証部20はこの例に限定されず、他の生体認証、例えば、虹彩認証、静脈認証、網膜認証等の公知の認証手法を適宜用いることが可能である。また、このような生体認証に代えて、パスワードによる認証を適用することも可能である。

また、パスワードによる認証のように、第1認証部20による認証時において、ユーザによるキー入力及要求される場合には、第2認証部30は、第1認証時に入力されたキー入力のタイピングインターバルを用いてユーザ認証を行ってもよい。このように、第1認証部20による認証と同時に第2認証部30による認証も行うことにより、セキュリティレベルを更に向上させることが可能となる。

【0026】

また、本実施形態においては、タイピング時におけるユーザの挙動データとして、タイピングインターバルを採用し、タイピングインターバルを用いてユーザ認証を行ったが、タイピングインターバル以外の特徴をユーザの挙動データとして用いることとしてもよい。例えば、タイピングの強さ、タイピング時のパーム位置、タイピング時におけるユーザの姿勢等を用いることとしてもよい。

これらの特徴についても、タイピング時におけるユーザの癖を捉えることができ、これらの特徴を少なくとも一つ利用してユーザ認証を行うことで、ユーザ認証に関するユーザの負担を増大させることなく、セキュリティレベルを高めることが可能となる。

【0027】

〔第2実施形態〕

上述の第1実施形態では、タイピングインターバル（タイピング速度）を用いて第2認証部がユーザ認証を行う場合について説明したが、本実施形態では、タイピングの強さを用いて第2認証部がユーザ認証を行う。以下、本発明の第2実施形態に係る情報処理装置について、図3を参照して説明する。

【0028】

図3は、本発明の第2実施形態に係るノートPC10aの概略構成を示した図である。図3に示すように、ノートPC10aは、フィジカルキーボードの各キーの下方に設けられ、キーの押圧レベルを検出する圧力センサ40を有している。圧力センサ40によって取得された押圧データは、記憶部13に格納される。そして、上記実施形態と同様に、特徴量抽出部31aによって、押圧データから特徴量が抽出され、抽出された特徴量と予め記憶部13aに格納されている本人の特徴量である認証テンプレートとが照合部32aによって照合され、ユーザ認証が行われる。

【0029】

タイピングインターバルと同様に、タイピングの強さもユーザによって異なる。したがって、タイピングの押圧レベルに基づいて本人か否かを判断することが可能である。また、タイピングの強さを検出するセンサとして、圧力センサ40に代えて、加速度センサを

10

20

30

40

50

用いてもよい。この場合、キーボードに加速度センサを設け、加速度センサによってタイピング時の衝撃を検出し、加速度センサの検出値から特徴量を抽出し、この特徴量を用いてユーザ認証を行う。

【0030】

〔第3実施形態〕

上記実施形態では、タイピングインターバル等を用いて第2のユーザ認証を行う場合について説明したが、本実施形態では、タイピング時のパーム位置に関する特徴量を用いて第2のユーザ認証を繰り返し行う。以下、本発明の第3実施形態に係る情報処理装置について、図4を参照して説明する。

【0031】

図4は、本発明の第3実施形態に係るノートPC10bの概略構成を示した図である。本実施形態に係るノートPC10bは、パーム位置を検出するための撮像部41を備えている。撮像部41によって取得された映像データは、記憶部13bに格納される。そして、上記実施形態と同様に、特徴量抽出部31bによって、映像データから特徴量が抽出され、抽出された特徴量と予め記憶部13bに格納されている本人の特徴量である認証テンプレートとが照合部32bによって照合され、第2のユーザ認証が行われる。

この場合における特徴量としては、例えば、ホームポジションにおける左右のパームの重心位置、タイピング時におけるパームの重心位置の移動量、キーボード上における指の配置等が一例として挙げられる。

【0032】

〔第4実施形態〕

次に、本発明の第4実施形態に係る情報処理装置について説明する。本実施形態に係るノートPC10cは、タイピング時の姿勢に関する特徴量を用いて第2のユーザ認証を繰り返し行う。以下、本発明の第4実施形態に係る情報処理装置について説明する。

【0033】

本実施形態に係るノートPCは、上述した第3実施形態に係るノートPCと同様の構成を備えている。すなわち、本実施形態に係るノートPCは、ユーザの姿勢に関するデータを取得するための手段として撮像部41を備えている。そして、撮像部41によって取得された映像データから、ユーザの姿勢に関する特徴量を抽出する。この特徴量としては、例えば、画面と頭部との距離または両者の相対的な位置関係（例えば、角度）、タイピング中にユーザが画面を見ているときの時間とキーボードを見ているときの時間比率などが挙げられる。

このように、タイピング時における姿勢にも、個人の行動的特徴（癖）が現れるので、このような情報に基づいて本人か否かを判定することが可能である。

なお、ユーザの姿勢に関する特徴量として、画像と頭部との距離を用いる場合には、撮像部に代えて赤外線センサ等を用いることも可能である。

【0034】

以上、本発明の各実施形態を用いて説明してきたが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。発明の要旨を逸脱しない範囲で上記実施形態に多様な変更又は改良を加えることができ、該変更又は改良を加えた形態も本発明の技術的範囲に含まれる。更に、各実施形態を適宜組み合わせさせた態様も本発明の技術的範囲に含まれる。

【0035】

例えば、各実施形態では、第2認証部がタイピングインターバル（タイピング速度）、タイピングの強さ、タイピング時のパーム位置、及びタイピング時の姿勢のいずれかを用いてユーザ認証を行う場合について述べたが、第2認証部は、上述の各種特徴量のいずれか2つ以上を組み合わせ、多面的にユーザ認証を行うこととしてもよい。また、上記以外の特徴量、例えば、ミスタイピングの傾向等を用いてユーザ認証を行ってもよい。

【0036】

また、記憶部13には、事前に認証テンプレートが登録されている場合について述べたが、認証テンプレートは第1認証部による認証が行われる毎に更新されてもよい。例えば

10

20

30

40

50

、第１認証部２０による認証後において、特徴量抽出部３１、３１ａ、３１ｂによって最初に抽出された特徴量を認証テンプレートとして記憶部１３に格納することとしてもよい。

タイピング時におけるユーザの挙動は、その時々気分や環境によって異なる。したがって、第１認証部２０による認証後において、特徴量抽出部３１によって最初に抽出された特徴量を認証テンプレートとして登録しておくことにより、ユーザ認証の精度を向上させることが可能となる。

【００３７】

また、上記の各実施形態において、特徴量抽出部３１、３１ａ、３１ｂは、記憶部１３に格納されている全てのデータを用いて特徴量を抽出していたが、これに代えて、例えば、特定のキー入力されたときのデータを抽出し、そのときのデータを用いて特徴量を抽出することとしてもよい。例えば、予め入力頻度の高い単語（例えば、「to the」、「meeting」、「thank you」等）を登録しておき、これらの単語が入力されたときのデータのみを使用して特徴量を抽出し、抽出した特徴量に基づいて第２のユーザ認証を行うこととしてもよい。このように、第２のユーザ認証を行う単語を制限することで、第２のユーザ認証の精度向上を期待することができる。なお、この場合、記憶部１３には、ユーザの挙動データ（例えば、タイピングインターバル等）とそのデータが入力されたときのキーとが関連付けられて格納される。

【００３８】

また、上述の各実施形態では、タイピング時におけるユーザの行動的特徴を利用して第２のユーザ認証を行うこととしたが、スマートフォンなどのようにユーザが端末を把持して利用するような情報処理装置においては、例えば、端末の持ち方に基づいてユーザ認証を行ってもよい。この場合、例えば、情報処理装置の外周部に圧力センサを設け、他の箇所と比べて大きな圧力が検出される位置を特徴量として取得し、この特徴量を用いてユーザ認証を行ってもよい。

【符号の説明】

【００３９】

１０、１０ａ、１０ｂ ノートＰＣ（情報処理装置）
 １１、１１ａ、１１ｂ 制御部
 １２ メインメモリ
 １３、１３ａ、１３ｂ 記憶部
 １４ 入力部
 １５ 表示部
 １６ 通信部
 １７ 指紋リーダー
 １８ 計時部
 ２０ 第１認証部
 ３０、３０ａ、３０ｂ 第２認証部
 ３１、３１ａ、３１ｂ 特徴量抽出部
 ３２、３２ａ、３２ｂ 照合部
 ４０ 圧力センサ
 ４１ 撮像部

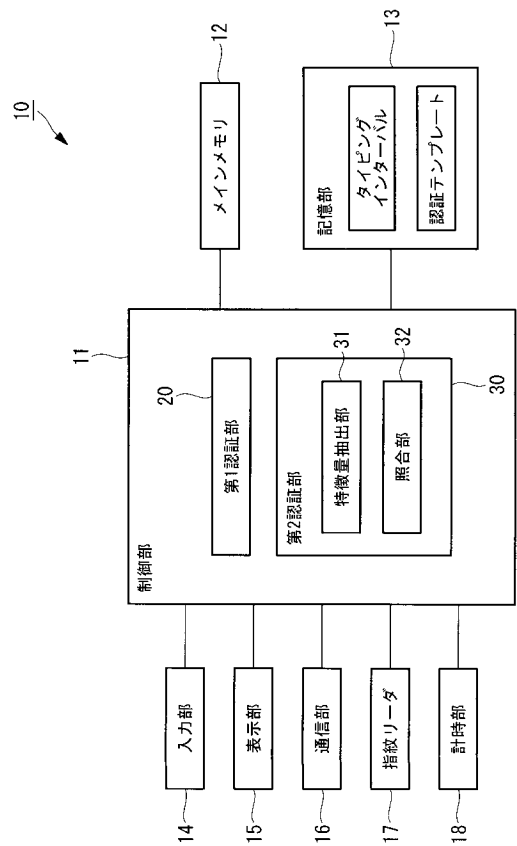
10

20

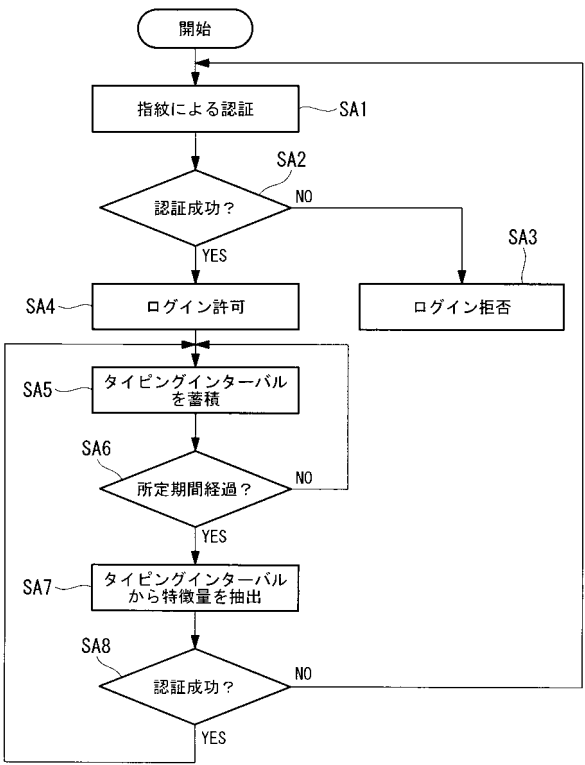
30

40

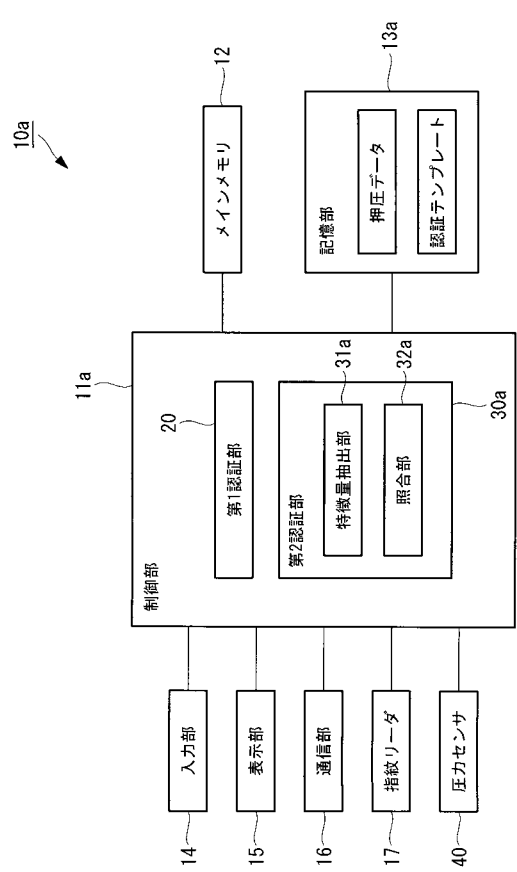
【図 1】



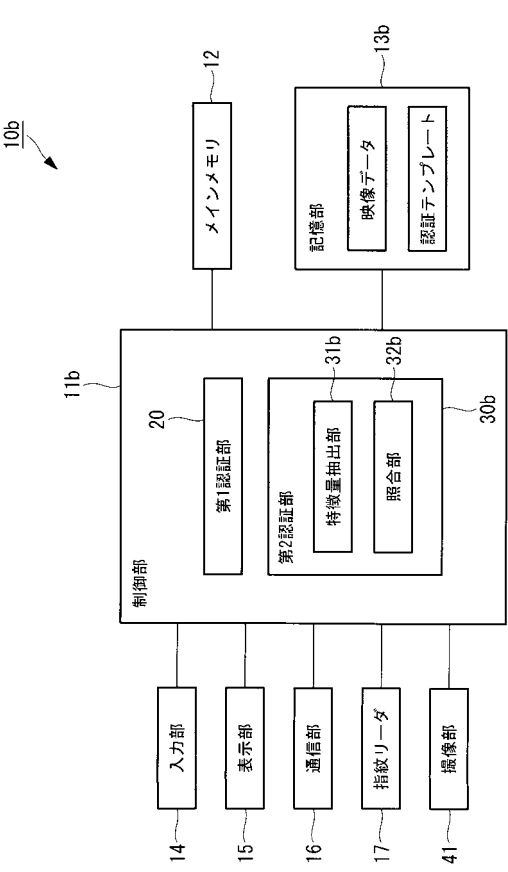
【図 2】



【図 3】



【図 4】



【手続補正書】

【提出日】平成29年4月7日(2017.4.7)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

第 1 認証手段と、

タイピング時におけるユーザの挙動データを用いてユーザ認証を行う第 2 認証手段とを備え、

前記第 2 認証手段は、

キーボードに設けられた加速度センサと、

前記加速度センサによって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、

特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段と

を備える情報処理装置。

【請求項 2】

第 1 認証手段と、

タイピング時におけるユーザの挙動データを用いてユーザ認証を行う第 2 認証手段とを備え、

前記第 2 認証手段は、

タイピング時におけるユーザの姿勢またはパーム位置に関する挙動データを取得する撮像手段と、

前記撮像手段によって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、

特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段と

を備える情報処理装置。

【請求項 3】

前記特徴量抽出手段は、予め登録されている特定の単語またはフレーズが入力されたときの前記挙動データを用いて特徴量を抽出する請求項 1 または請求項 2 に記載の情報処理装置。

【請求項 4】

前記第 2 認証手段は、ユーザ認証に失敗した場合に、前記第 1 認証手段によるユーザ認証をユーザに要求する請求項 1 から請求項 3 のいずれかに記載の情報処理装置。

【請求項 5】

前記第 2 認証手段は、タイピング時におけるユーザの前記挙動データを用いてユーザ認証を繰り返し行う請求項 1 から請求項 4 のいずれかに記載の情報処理装置。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正の内容】

【0006】

本発明の第一態様は、第 1 認証手段と、タイピング時におけるユーザの挙動データを用いてユーザ認証を行う第 2 認証手段とを備え、前記第 2 認証手段は、キーボードに設けられた加速度センサと、前記加速度センサによって取得された前記挙動データから特徴量を

抽出する特徴量抽出手段と、特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段とを備える情報処理装置である。

本発明の第二態様は、第 1 認証手段と、タイピング時におけるユーザの挙動データを用いてユーザ認証を行う第 2 認証手段とを備え、前記第 2 認証手段は、タイピング時におけるユーザの姿勢またはパーム位置に関する挙動データを取得する撮像手段と、前記撮像手段によって取得された前記挙動データから特徴量を抽出する特徴量抽出手段と、特徴量抽出手段によって抽出された特徴量と、予め登録されている認証テンプレートとを照合する照合手段とを備える情報処理装置である。

フロントページの続き

(74)代理人 100172524

弁理士 長田 大輔

(72)発明者 河野 誠一

神奈川県横浜市西区みなとみらい3丁目6番1号 レノボ・ジャパン株式会社 横浜事業所内

Fターム(参考) 5B043 AA09 BA02 BA05 EA05 GA02 GA13

5E555 AA53 BA02 BA52 BB02 BC03 CA18 CA44 CB76 FA00