

(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2015-176268

(P2015-176268A)

(43) 公開日 平成27年10月5日(2015.10.5)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/31 (2013.01)	G06F 21/20 1 3 1 A	5 B 0 2 0
H04L 9/32 (2006.01)	H04L 9/00 6 7 3 A	5 E 5 5 5
G06F 3/023 (2006.01)	G06F 3/023 3 1 0 L	5 J 1 0 4
H03M 11/04 (2006.01)	G06F 3/023 3 1 0 G	
H03M 11/14 (2006.01)	G06F 3/023 3 2 0	
審査請求 未請求 請求項の数 12 O L (全 16 頁) 最終頁に続く		

(21) 出願番号 特願2014-51116 (P2014-51116)
 (22) 出願日 平成26年3月14日 (2014.3.14)

(71) 出願人 000003078
 株式会社東芝
 東京都港区芝浦一丁目1番1号
 (74) 代理人 110001737
 特許業務法人スズエ国際特許事務所
 (72) 発明者 森 知孝
 東京都港区芝浦一丁目1番1号 株式会社
 東芝内
 Fターム(参考) 5B020 DD22 DD30 FF14
 5E555 AA51 BA03 BA04 BB03 BB04
 BC03 BC16 CA18 CA22 CB12
 CB20 CB34 CB53 CB59 CC01
 EA14 FA16 FA17
 5J104 AA07 EA03 KA01 NA05 NA06
 PA07

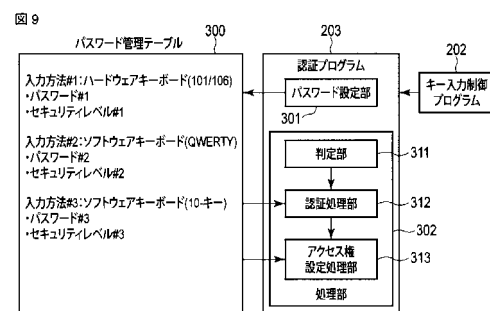
(54) 【発明の名称】 電子機器および認証方法

(57) 【要約】

【課題】パスワード入力操作を容易にすることができる電子機器を実現する。

【解決手段】実施形態によれば、設定手段は、第1入力方法に対応する第1パスワードと、第2入力方法に対応する第2パスワードとを設定する。処理手段は、前記第1入力方法または前記第2入力方法によって入力される入力パスワードが正しいか否かを前記入力パスワードと予め設定される登録パスワードとを比較することによって判定するための認証処理を実行する。前記処理手段は、前記入力パスワードを入力するためにユーザによって使用される入力方法が前記第1入力方法または前記第2入力方法のいずれであるかを判定し、前記ユーザによって使用される入力方法の判定の結果に基づいて、前記入力パスワードと比較される登録パスワードを、前記第1入力方法に対応する前記第1パスワードと前記第2入力方法に対応する前記第2パスワードとの間で変更する。

【選択図】 図9



【特許請求の範囲】

【請求項 1】

文字列を入力するための第 1 入力方法に対応する第 1 パスワードと、文字列を入力するための第 2 入力方法であって前記第 1 入力方法と異なる第 2 入力方法に対応する第 2 パスワードとを設定する設定手段と、

前記第 1 入力方法または前記第 2 入力方法によって入力される入力パスワードが正しいか否かを前記入力パスワードと予め設定される登録パスワードとを比較することによって判定するための認証処理を実行する処理手段とを具備し、

前記処理手段は、

前記入力パスワードを入力するためにユーザによって使用される入力方法が前記第 1 入力方法または前記第 2 入力方法のいずれであるかを判定し、

前記ユーザによって使用される入力方法の判定の結果に基づいて、前記入力パスワードと比較される登録パスワードを、前記第 1 入力方法に対応する前記第 1 パスワードと前記第 2 入力方法に対応する前記第 2 パスワードとの間で変更する、電子機器。

【請求項 2】

前記第 1 入力方法はハードウェアキーボードを使用して文字列を入力するための入力方法であり、前記第 2 入力方法はソフトウェアキーボードを使用して文字列を入力するための入力方法である請求項 1 記載の電子機器。

【請求項 3】

前記第 1 入力方法は第 1 タイプのソフトウェアキーボードを使用して文字列を入力するための入力方法であり、前記第 2 入力方法は前記第 1 タイプのソフトウェアキーボードと異なる第 2 タイプのソフトウェアキーボードを使用して文字列を入力するための入力方法である請求項 1 記載の電子機器。

【請求項 4】

前記処理手段は、

前記入力パスワードが前記第 1 パスワードに合致する正しいパスワードであることが判定された場合、ユーザに付与すべきアクセス権レベルを第 1 機能の実行が可能な第 1 アクセス権レベルに設定し、

前記入力パスワードが前記第 2 パスワードに合致する正しいパスワードであることが判定された場合、ユーザに付与すべきアクセス権レベルを前記第 1 機能の実行が制限された第 2 アクセス権レベルに設定する請求項 1 記載の電子機器。

【請求項 5】

文字列を入力するための第 1 入力方法に対応する第 1 パスワードと、文字列を入力するための第 2 入力方法であって前記第 1 入力方法と異なる第 2 入力方法に対応する第 2 パスワードとを設定することと、

パスワードを入力するためにユーザによって使用される入力方法が前記第 1 入力方法または前記第 2 入力方法のいずれであるかを判定することと、

パスワードを入力するためにユーザによって使用される入力方法が前記第 1 入力方法である場合、ユーザによって入力される入力パスワードが正しいか否かを前記入力パスワードと前記第 1 入力方法に対応する前記第 1 パスワードとを比較することによって判定するための第 1 認証処理を実行することと、

パスワードを入力するためにユーザによって使用される入力方法が前記第 2 入力方法である場合、ユーザによって入力される入力パスワードが正しいか否かを前記入力パスワードと前記第 2 入力方法に対応する前記第 2 パスワードとを比較することによって判定するための第 2 認証処理を実行することを含む、認証方法。

【請求項 6】

前記第 1 入力方法はハードウェアキーボードを使用して文字列を入力するための入力方法であり、前記第 2 入力方法はソフトウェアキーボードを使用して文字列を入力するための入力方法である請求項 5 記載の認証方法。

【請求項 7】

前記第 1 入力方法は第 1 タイプのソフトウェアキーボードを使用して文字列を入力するための入力方法であり、前記第 2 入力方法は前記第 1 タイプのソフトウェアキーボードと異なる第 2 タイプのソフトウェアキーボードを使用して文字列を入力するための入力方法である請求項 5 記載の認証方法。

【請求項 8】

前記入力パスワードが前記第 1 パスワードに合致する正しいパスワードであることが判定された場合、ユーザに付与すべきアクセス権レベルを第 1 機能の実行が可能な第 1 アクセス権レベルに設定することと、

前記入力パスワードが前記第 2 パスワードに合致する正しいパスワードであることが判定された場合、ユーザに付与すべきアクセス権レベルを前記第 1 機能の実行が制限された第 2 アクセス権レベルに設定することとをさらに具備する請求項 5 記載の認証方法。

【請求項 9】

コンピュータによって実行されるプログラムであって、

文字列を入力するための第 1 入力方法に対応する第 1 パスワードと、文字列を入力するための第 2 入力方法であって前記第 1 入力方法と異なる第 2 入力方法に対応する第 2 パスワードとを設定する手順と、

前記第 1 入力方法または前記第 2 入力方法によって入力される入力パスワードが正しいか否かを前記入力パスワードと予め設定される登録パスワードとを比較することによって判定するための認証処理を実行する手順とを前記コンピュータに実行させ、

前記認証処理を実行する手順は、

前記入力パスワードを入力するためにユーザによって使用される入力方法が前記第 1 入力方法または前記第 2 入力方法のいずれであるかを判定する手順と、

前記ユーザによって使用される入力方法の判定の結果に基づいて、前記入力パスワードと比較される登録パスワードを、前記第 1 入力方法に対応する前記第 1 パスワードと前記第 2 入力方法に対応する前記第 2 パスワードとの間で変更する手順とを含む、プログラム。

【請求項 10】

前記第 1 入力方法はハードウェアキーボードを使用して文字列を入力するための入力方法であり、前記第 2 入力方法はソフトウェアキーボードを使用して文字列を入力するための入力方法である請求項 9 記載のプログラム。

【請求項 11】

前記第 1 入力方法は第 1 タイプのソフトウェアキーボードを使用して文字列を入力するための入力方法であり、前記第 2 入力方法は前記第 1 タイプのソフトウェアキーボードと異なる第 2 タイプのソフトウェアキーボードを使用して文字列を入力するための入力方法である請求項 9 記載のプログラム。

【請求項 12】

前記入力パスワードが前記第 1 パスワードに合致する正しいパスワードであることが判定された場合、ユーザに付与すべきアクセス権レベルを第 1 機能の実行が可能な第 1 アクセス権レベルに設定する手順と、

前記入力パスワードが前記第 2 パスワードに合致する正しいパスワードであることが判定された場合、ユーザに付与すべきアクセス権レベルを前記第 1 機能の実行が制限された第 2 アクセス権レベルに設定する手順とを前記コンピュータにさらに実行させる請求項 9 記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明の実施形態は、パスワードを使用して認証処理を行うための技術に関する。

【背景技術】

【0002】

近年、ノートブック（ラップトップ）型パーソナルコンピュータ、タブレット、スマー

10

20

30

40

50

トフォンといった様々な電子機器が開発されている。この種の電子機器は、電子文書、データベース、他の様々なデジタルコンテンツを閲覧または編集するための端末として広く利用されている。

【0003】

また、最近では、セキュリティ性を高めるために様々な認証システムが利用されている。認証システムの多くは、ユーザによって入力されるパスワードと予め設定されたパスワードとを比較することによってユーザの正当性を確認するための処理を実行する。

【先行技術文献】

【特許文献】

【0004】

10

【特許文献1】特開2007-310515号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

一般に、予め設定されるパスワードの長さが長いほど、高いセキュリティ性を得ることが可能となる。

【0006】

しかし、長いパスワードを常に使用することは、パスワードの入力に要する時間を長引かせる要因となり得、またパスワードの誤入力の可能性を高める要因にもなり得る。パスワードの誤入力が発生する度にパスワードの再タイプ入力が必要となるので、パスワードの誤入力回数の増加は、パスワード認証に要する時間の増加を引き起こす。

20

【0007】

本発明は、パスワード入力操作を容易にすることができる電子機器および認証方法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】

【0008】

実施形態によれば、電子機器は、設定手段と、処理手段とを具備する。前記設定手段は、文字列を入力するための第1入力方法に対応する第1パスワードと、文字列を入力するための第2入力方法であって前記第1入力方法と異なる第2入力方法に対応する第2パスワードとを設定する。前記処理手段は、前記第1入力方法または前記第2入力方法によって入力される入力パスワードが正しいか否かを前記入力パスワードと予め設定される登録パスワードとを比較することによって判定するための認証処理を実行する。前記処理手段は、前記入力パスワードを入力するためにユーザによって使用される入力方法が前記第1入力方法または前記第2入力方法のいずれであるかを判定し、前記ユーザによって使用される入力方法の判定の結果に基づいて、前記入力パスワードと比較される登録パスワードを、前記第1入力方法に対応する前記第1パスワードと前記第2入力方法に対応する前記第2パスワードとの間で変更する。

30

【図面の簡単な説明】

【0009】

【図1】実施形態に係る電子機器の外観を示す斜視図。

40

【図2】同実施形態の電子機器とハードウェアキーボードとの関係の例を説明するための図。

【図3】同実施形態の電子機器とハードウェアキーボードとの関係の他の例を示す図。

【図4】同実施形態の電子機器のシステム構成を示すブロック図。

【図5】同実施形態の電子機器において使用されるハードウェアキーボードのキー配列の例を示す図。

【図6】同実施形態の電子機器において使用されるソフトウェアキーボードのキー配列の例を示す図。

【図7】同実施形態の電子機器において使用されるソフトウェアキーボードのキー配列の他の例を示す図。

50

【図 8】同実施形態の電子機器において使用される複数の入力方法にそれぞれ関連付けられる複数のパスワードと複数種のアクセス権を示す図。

【図 9】同実施形態の電子機器によって実行される認証プログラムの構成を示すブロック図。

【図 10】同実施形態の電子機器によって実行されるパスワード設定処理の手順を示すフローチャート。

【図 11】同実施形態の電子機器によって実行されるパスワード認証処理の手順を示すフローチャート。

【図 12】同実施形態の電子機器とサーバとを含むシステムの構成例を示すブロック図。

【発明を実施するための形態】

【0010】

図 1 は、一実施形態に係る電子機器の外観を示す斜視図である。この電子機器は、電子文書、データベース、他の様々なデジタルコンテンツの閲覧または編集のような処理を実行可能な機器である。この電子機器は、タブレットコンピュータ、ノートブック型パーソナルコンピュータ、スマートフォン、PDA 等として実現され得る。以下では、この電子機器がタブレットコンピュータ 10 として実現されている場合を想定する。

【0011】

タブレットコンピュータ 10 は、タブレットまたはスレートコンピュータとも称される携帯型電子機器である。このタブレットコンピュータ 10 は、図 1 に示すように、本体 11 とタッチスクリーンディスプレイ 17 とを備える。タッチスクリーンディスプレイ 17 は、本体 11 の上面に重ね合わせるように取り付けられている。

【0012】

本体 11 は、薄い箱形の筐体を有している。本体 11 の側面には、パワーボタン 12、USB ポート 13 などが配置されている。タッチスクリーンディスプレイ 17 には、フラットパネルディスプレイと、センサとが組み込まれている。センサは、フラットパネルディスプレイの画面上のペンまたは指の接触位置を検出するように構成されている。センサとしては、例えば、静電容量方式のタッチパネル、電磁誘導方式のデジタイザなどを使用することができる。フラットパネルディスプレイは、例えば、液晶表示装置 (LCD) であってもよい。

【0013】

タブレットコンピュータ 10 は、タッチスクリーンディスプレイ 17 上にソフトウェアキーボードを表示することが出来る。ソフトウェアキーボードは、複数のキーコードがそれぞれ割り当てられた複数のキー (ソフトウェアボタン) を含む。ユーザは、ペンまたは指でソフトウェアキーボード上の幾つかのキーをタップすることによって所望のキーコード、例えば、所望の文字列、を入力することが出来る。また、タブレットコンピュータ 10 は、ソフトウェアキーボードのみならず、必要に応じて、ハードウェアキーボードのような他の様々な入力デバイスを使用することも出来る。

【0014】

図 2 はタブレットコンピュータ 10 とハードウェアキーボード 21 との間の関係の例を示す。

タブレットコンピュータ 10 は、図 2 に示すように、タブレットコンピュータ 10 に接続可能なハードウェアキーボード 21 を入力デバイスとして使用することが出来る。ハードウェアキーボード 21 は有線または無線でタブレットコンピュータ 10 と接続されても良い。ハードウェアキーボード 21 とタブレットコンピュータ 10 との間を接続するための有線インタフェースは、例えば、USB であってもよい。この場合、ハードウェアキーボード 21 は、USB ケーブルを介してタブレットコンピュータ 10 の USB ポート 13 に接続される。ハードウェアキーボード 21 とタブレットコンピュータ 10 との間を接続するための無線インタフェースは、例えば、Bluetooth (登録商標) であってもよい。

【0015】

10

20

30

40

50

図3はタブレットコンピュータ10とハードウェアキーボード21との間の関係の別の例を示す。

ここでは、タブレットコンピュータ10が、キーボードドック22に取り外し自在に装着される場合を想定する。キーボードドック22のベースユニット上にはハードウェアキーボード23が配置されている。タブレットコンピュータ10がキーボードドック22にドッキングされた時、タブレットコンピュータ10の本体11に設けられたコネクタ（ドッキングポート）がキーボードドック22のヒンジ24内のコネクタに接続される。ハードウェアキーボード23はドッキングポートを介してタブレットコンピュータ10に電氣的に接続される。

【0016】

ユーザは、タッチスクリーンディスプレイ17上に表示されるソフトウェアキーボードを操作してキーコード列（文字列）を入力することもできるし、ハードウェアキーボード21または23を操作してキーコード列（文字列）を入力することもできる。

【0017】

図4は、タブレットコンピュータ10のシステム構成を示す。

タブレットコンピュータ10は、図4に示されるように、CPU101、システムコントローラ102、主メモリ103、グラフィクスコントローラ（GPU）104、BIOS-ROM105、ストレージデバイス106、BT（Bluetooth（登録商標））デバイス107、無線LANデバイス108、エンベデッドコントローラ（EC）109等を備える。

【0018】

CPU101は、タブレットコンピュータ10内の各種モジュールの動作を制御するプロセッサである。CPU101は、ソリッドステートドライブ（SSD）のようなストレージデバイス106から主メモリ103にロードされる各種プログラムを実行する。CPU101により実行されるプログラムには、オペレーティングシステム（OS）201と、様々なアプリケーション／ユーティリティプログラムが含まれている。アプリケーション／ユーティリティプログラムには、キー入力制御プログラム202、および認証プログラム203等が含まれている。

【0019】

キー入力制御プログラム202はソフトウェアキーボードまたはハードウェアキーボード（21または23）からキーコードを受信し、この受信したキーコードをアクティブなアプリケーションプログラムに渡す。

【0020】

認証プログラム203は、ユーザによって入力される入力パスワードが正しいか否かを入力パスワードと予め設定されたパスワード（登録パスワード）と比較することによって判定するための認証処理を実行する。この認証プログラム203は、例えば、データベースへのアクセスが要求された時、または画面ロックの解除が要求された時などに実行されてもよい。認証プログラム203が実行された時、認証プログラム203は、ユーザにパスワードの入力を促すためのパスワード入力画面をタッチスクリーンディスプレイ17上に表示する。

【0021】

認証プログラム203は、文字列を入力するための複数種の入力方法に対応するように設計されている。

【0022】

複数種の入力方法には、大別して、ハードウェアキーボードを使用してパスワード（文字列）を入力するための入力方法と、ソフトウェアキーボードを使用してパスワード（文字列）を入力するための入力方法とがある。また、通常、表示可能なソフトウェアキーボードの種類は複数種あるので、あるタイプのソフトウェアキーボードを使用してパスワード（文字列）を入力するための入力方法と、別のタイプのソフトウェアキーボードを使用してパスワード（文字列）を入力するための入力方法とがあってもよい。

10

20

30

40

50

【0023】

さらに、ハードウェアキーボードの種類には、101キー配列または106キー配列のような通常のキーボードの他に、キー数の少ないキーボード（10キーキーボード）もある。このため、ハードウェアキーボードのタイプ毎に入力方法が存在してもよい。

【0024】

一般に、文字列を入力するための上述の入力方法毎に、例えば、使用する入力デバイスの種類（ハードウェアキーボード、ソフトウェアキーボード、ハードウェアキーボードのタイプ、ソフトウェアキーボードのタイプ）毎に、文字列の入力のしやすさは異なる。このため、もし使用する入力方法とは無関係に、特定のパスワードを使用する構成を採用したならば、ユーザによって現在使用されている入力環境（入力方法）によっては、パスワードの入力に比較的多くの時間を要したり、パスワードの誤入力が発生する可能性がある。

10

【0025】

そこで、本実施形態では、認証プログラム203は、ユーザによって使用される入力方法毎に、例えば、ユーザによって使用される入力デバイスの種類毎に、パスワードを個別に設定する機能を有している。

【0026】

いま、文字列を入力するための第1入力方法と、文字列を入力するめの第2入力方法が存在する場合を想定する。第2入力方法は第1入力方法と異なる入力方法である。認証プログラム203は、ユーザの操作に応じて、第1入力方法に対応する第1パスワードと、第2入力方法に対応する第2パスワードとを設定することができる。

20

【0027】

認証処理においては、認証プログラム203は、パスワードを入力するためにユーザによって使用される入力方法が上述の第1入力方法または上述の第2入力方法のいずれであるかを判定する。パスワードを入力するためにユーザによって使用される入力方法は、例えば、現在使用されている入力デバイスの種類を検出することによって、または現在使用されているソフトウェアキーボードのタイプ等を検出することによって判定することができる。

【0028】

第1入力方法が使用されていることが判定されたならば、認証プログラム203は、入力されたパスワードと第1入力方法に対応する第1パスワードとを比較して、入力されたパスワードを検証する。一方、第2入力方法が使用されていることが判定されたならば、認証プログラム203は、入力されたパスワードと第2入力方法に対応する第2パスワードとを比較して、入力されたパスワードを検証する。

30

【0029】

このように、認証プログラム203は、入力されたパスワードと比較されるべき登録パスワードを、入力方法の判定結果に応じて、第1パスワードと第2パスワードとの間で自動的に変更することができる。したがって、ユーザは、現在の入力環境に対応するパスワードを用いて認証処理を受けることができる。

【0030】

また、CPU101は、BIOS-ROM105に格納された基本入出力システム（BIOS）も実行する。BIOSは、ハードウェア制御のためのプログラムである。

40

【0031】

システムコントローラ102は、CPU101のローカルバスと各種コンポーネントとの間を接続するデバイスである。システムコントローラ102には、メインメモリ103をアクセス制御するメモリコントローラも内蔵されている。

【0032】

グラフィクスコントローラ（GPU）104は、タブレットコンピュータ10のディスプレイモニタとして使用されるLCD17Aを制御する表示コントローラである。グラフィクスコントローラ（GPU）104はCPU101に内蔵されていても良い。

50

【0033】

グラフィクスコントローラ104によって生成される表示信号はLCD17Aに送られる。LCD17Aは、表示信号に基づいて画面イメージを表示する。LCD17Aの上層には、タッチパネルまたはデジタイザから構成されるセンサ17Bが配置されている。

【0034】

EC108は、電力管理のためのエンベデッドコントローラを含むワンチップマイクロコンピュータである。EC108は、ユーザによるパワーボタン12の操作に応じてタブレットコンピュータ10を電源オンまたは電源オフする機能を有している。

【0035】

次に、タブレットコンピュータ10によって使用可能な幾つかの入力デバイスの例について説明する。

図5は、ハードウェアキーボードの例を示す。図5のハードウェアキーボードは日本語配列のハードウェアキーボードを示している。ユーザによって使用されるハードウェアキーボードは、英語配列のキーボードであってもよい。

【0036】

図6はソフトウェアキーボードの例を示す。図6のソフトウェアキーボードは携帯入力（マルチタップ入力）用のソフトウェア10ーキーボードを示している。ユーザによって使用されるソフトウェアキーボードはフリック入力用のソフトウェア10ーキーボードであってもよい。

【0037】

図7はソフトウェアキーボードの別の例を示す。図7のソフトウェアキーボードはQWERTY配列のソフトウェアキーボードを示している。

【0038】

上述したように、文字列を入力するために使用する入力方法（ハードウェアキーボード、ソフトウェアキーボードのタイプ等）によって文字列の入力しやすさは異なる。

【0039】

通常、ハードウェアキーボードに関しては、タッチタイプ等の習熟性があり、慣れにより高速で打鍵することが可能である。

【0040】

これに対し、ソフトウェアキーボードに関しては、長い文字列の入力には不向きであり、誤入力も発生しやすい。また、入力文字種（アルファベット／数字／日本語など）を変更するときの処理が煩雑である。

【0041】

認証プログラム203は、パスワード入力のために使用される入力方法毎に異なるパスワードを登録パスワードとして設定することができる。これにより、ユーザは、例えば、高速に打鍵できる入力方法（ハードウェアキーボードを使用する入力方法）に対応するパスワードとして長い文字列のパスワードを設定し、長い文字列の入力に不向きの別の入力方法（ソフトウェアキーボードを使用する入力方法）に対応するパスワードとして短い文字列のパスワードを設定することができる。また、ソフトウェアキーボードのタイプ（ソフトウェア10ーキーボード（マルチタップ入力）、ソフトウェア10ーキーボード（フリック入力）、ソフトウェアキーボード（QWERTY））毎に、異なるパスワードを設定することも出来る。

【0042】

図8は、使用可能な複数の入力方法それぞれに関連付けられたパスワードの例を示す。

【0043】

ここでは、使用可能な入力方法として、

- (1) ハードウェアキーボード（101／106キー）
- (2) ハードウェア10ーキーボード
- (3) ソフトウェア10ーキーボード（マルチタップ入力）
- (4) ソフトウェア10ーキーボード（フリック入力）

10

20

30

40

50

(5) ソフトウェアキーボード (Q W E R T Y)
(6) ソフトウェアキーボード (手書き入力)、
の 6 種類の入力方法が例示されている。

【0044】

ユーザは、認証プログラム 203 を使用することにより、入力方法毎に異なるパスワードを設定することが出来る。認証処理において、入力パスワードと比較される登録パスワードは、パスワードの入力に使用される入力方法に応じて自動的に変更される。

【0045】

例えば、もしハードウェアキーボード (101 / 106 キー) を用いてパスワードが入力された場合には、この入力されたパスワードは、ハードウェアキーボード (101 / 106 キー) に対応する登録パスワードと比較される。また、もしソフトウェア 10 - キーボード (マルチタップ入力) を用いてパスワードが入力された場合には、この入力されたパスワードは、ソフトウェア 10 - キーボード (マルチタップ入力) に対応する登録パスワードと比較される。

【0046】

さらに、本実施形態では、認証処理において使用される登録パスワード毎に、ユーザに付与すべきセキュリティレベル (アクセス権レベル) を設定することも出来る。

【0047】

例えば、入力パスワードが、ハードウェアキーボード (101 / 106 キー) に対応する登録パスワードに合致する正しいパスワードであることが判定された場合には、ユーザに付与すべきアクセス権レベルは第 1 機能の実行が可能な第 1 アクセス権レベルに設定される。この場合、データベースにアクセスするためにユーザに付与されるべきセキュリティレベル (アクセス権レベル) は、データベース内のデータの閲覧 (read) と編集 (write) の双方をユーザに許可するセキュリティレベルに設定されても良い。

【0048】

一方、入力パスワードが、ソフトウェア 10 - キーボード (マルチタップ入力) に対応する登録パスワード (中くらいの長さのパスワード) に合致する正しいパスワードであることが判定された場合には、ユーザに付与すべきアクセス権レベルは第 1 機能の実行が制限された第 2 アクセス権レベルに設定される。この場合、データベースにアクセスするためにユーザに付与されるべきセキュリティレベル (アクセス権レベル) は、データベース内のデータの閲覧 (read) のみをユーザに許可するセキュリティレベルに設定されても良い。

【0049】

図 9 は、認証プログラム 203 の機能構成を示す。

認証プログラム 203 は、パスワード設定部 301 および処理部 302 を含む。パスワード設定部 301 は、ユーザの操作に応じてパスワードを設定するための処理を実行するように構成された設定制御部として機能する。このパスワード設定部 301 は、文字列を入力するための第 1 入力方法に対応する第 1 パスワードと、文字列を入力するための第 2 入力方法であって第 1 入力方法と異なる第 2 入力方法に対応する第 2 パスワードとをパスワード管理テーブル 300 に設定する。なお、使用可能な入力方法は 2 つの入力方法に限らず、3 以上の入力方法にそれぞれ対応する 3 種類以上のパスワードを設定しても良い。

【0050】

パスワード管理テーブル 300 は、各入力方法に対応するパスワード (登録パスワード) を格納するための記憶領域である。このパスワード管理テーブル 300 においては、各入力方法に対応するパスワードのみならず、各入力方法に対応するセキュリティレベル (アクセス権レベル) が設定されても良い。

【0051】

図 9 のパスワード管理テーブル 300 においては、入力方法 # 1 に対応する第 1 のパスワード (パスワード # 1) が登録パスワードとして設定され、第 1 のパスワード (パスワード # 1) に対応するセキュリティレベルとして第 1 のセキュリティレベル (セキュリティ

10

20

30

40

50

ィレベル#1)が設定されている。入力方法#1は、例えば、ハードウェアキーボード(101/106キー)を使用する入力方法であってもよい。

【0052】

さらに、パスワード管理テーブル300においては、入力方法#2に対応する第2のパスワード(パスワード#2)が登録パスワードとして設定され、第2のパスワード(パスワード#2)に対応するセキュリティレベルとして第2のセキュリティレベル(セキュリティレベル#2)が設定されている。入力方法#2は、例えば、ソフトウェアキーボード(QWERTY)を使用する入力方法であってもよい。

【0053】

さらに、パスワード管理テーブル300においては、入力方法#3に対応する第3のパスワード(パスワード#3)が登録パスワードとして設定され、第3のパスワード(パスワード#3)に対応するセキュリティレベルとして第3のセキュリティレベル(セキュリティレベル#3)が設定されている。入力方法#3は、例えば、ソフトウェア10ーキーボード(マルチタップ入力またはフリック入力)を使用する入力方法であってもよい。

【0054】

処理部302は、入力方法#1、入力方法#2または入力方法#3によって入力される入力パスワードが正しいか否かを入力パスワードと予め設定される登録パスワードとを比較することによって判定するための認証処理を実行する。この処理部302は、判定部311、認証処理部312、アクセス権設定処理部313を備える。

【0055】

判定部311は、入力パスワードを入力するためにユーザによって使用される入力方法が入力方法#1、入力方法#2、または入力方法#3のいずれであるかを判定する。入力方法の判定はオペレーティングシステム201と協同して実行しても良い。

【0056】

認証処理部312は、ユーザによって使用される入力方法の判定の結果に基づいて、入力パスワードと比較される登録パスワードを、パスワード#1、パスワード#2、パスワード#3の間で自動的に変更する。

【0057】

すなわち、ユーザによって使用される入力方法が入力方法#1であるならば、認証処理部312は、ユーザによって入力される入力パスワードが正しいか否かを、入力パスワードと入力方法#1に対応するパスワード#1とを比較することによって判定するための第1認証処理を実行する。ユーザによって使用される入力方法が入力方法#2であるならば、認証処理部312は、ユーザによって入力される入力パスワードが正しいか否かを、入力パスワードと入力方法#2に対応するパスワード#2とを比較することによって判定するための第2認証処理を実行する。ユーザによって使用される入力方法が入力方法#3であるならば、認証処理部312は、ユーザによって入力される入力パスワードが正しいか否かを、入力パスワードと入力方法#3に対応するパスワード#3とを比較することによって判定するための第3認証処理を実行する。

【0058】

アクセス権設定処理部313は、ユーザに付与すべきアクセス権レベル(セキュリティレベル)を設定する。もし入力パスワードがパスワード#1に合致する正しいパスワードであることが判定されたならば、アクセス権設定処理部313は、ユーザに付与すべきアクセス権レベル(セキュリティレベル)をセキュリティレベル#1に設定する。またもし、入力パスワードがパスワード#2に合致する正しいパスワードであることが判定された場合、アクセス権設定処理部313は、ユーザに付与すべきアクセス権レベル(セキュリティレベル)をセキュリティレベル#2に設定する。またもし、入力パスワードがパスワード#1に合致する正しいパスワードであることが判定されたならば、アクセス権設定処理部313は、ユーザに付与すべきアクセス権レベル(セキュリティレベル)をセキュリティレベル#1に設定する。

【0059】

図10のフローチャートは、パスワード設定処理手順を示す。ここでは、入力方法#1～#3に対応する3種類のパスワードを設定する場合を想定する。

【0060】

パスワード設定部301は、入力方法#1に対応するパスワード#1を設定する（ステップS11）。このステップS11では、ユーザによって入力されるパスワードが入力方法#1に対応するパスワード#1としてパスワード管理テーブル300に設定される。ステップS11では、アクセス権設定処理部313は、ユーザの操作に応じて、パスワード#1に対応するアクセス権レベル（セキュリティレベル）をパスワード管理テーブル300に設定する。

【0061】

次に、パスワード設定部301は、入力方法#2に対応するパスワード#2を設定する（ステップS12）。このステップS12では、ユーザによって入力されるパスワードが入力方法#2に対応するパスワード#2としてパスワード管理テーブル300に設定される。ステップS12では、アクセス権設定処理部313は、ユーザの操作に応じて、パスワード#2に対応するアクセス権レベル（セキュリティレベル）をパスワード管理テーブル300に設定する。

【0062】

次に、パスワード設定部301は、入力方法#3に対応するパスワード#3を設定する（ステップS13）。このステップS13では、ユーザによって入力されるパスワードが入力方法#3に対応するパスワード#3としてパスワード管理テーブル300に設定される。ステップS13では、アクセス権設定処理部313は、ユーザの操作に応じて、パスワード#3に対応するアクセス権レベル（セキュリティレベル）をパスワード管理テーブル300に設定する。

【0063】

図11のフローチャートは、パスワード認証処理の手順を示す。

処理部302は、まず、パスワードの入力のためにユーザによって使用される入力方法の種類を判定する（ステップS21）。

パスワードの入力のためにユーザによって使用される入力方法が入力方法#1であるならば（ステップS22のYES）、処理部302は、ユーザによって入力される入力パスワードと入力方法#1に対応するパスワード#1とを比較することによって入力パスワードが正しいか否かを判定する（ステップS23）。入力パスワードがパスワード#1に合致する正しいパスワードであることが判定されたならば（ステップS24のYES）、処理部302は、ユーザにシステムの使用（例えば、データベースに対するアクセス、画面ロックの解除、等）を許可すると共に、ユーザに付与すべきセキュリティレベルをセキュリティレベル#1に設定する（ステップS25）。一方、入力パスワードがパスワード#1に合致しないならば（ステップS24のNO）、処理部302は、ユーザがシステムを使用することを禁止する（ステップS26）。

【0064】

パスワードの入力のためにユーザによって使用される入力方法が入力方法#2であるならば（ステップS27のYES）、処理部302は、ユーザによって入力される入力パスワードと入力方法#2に対応するパスワード#2とを比較することによって入力パスワードが正しいか否かを判定する（ステップS28）。入力パスワードがパスワード#1に合致する正しいパスワードであることが判定されたならば（ステップS29のYES）、処理部302は、ユーザにシステムの使用を許可すると共に、ユーザに付与すべきセキュリティレベルをセキュリティレベル#2に設定する（ステップS30）。一方、入力パスワードがパスワード#1に合致しないならば（ステップS29のNO）、処理部302は、ユーザがシステムを使用することを禁止する（ステップS26）。

【0065】

パスワードの入力のためにユーザによって使用される入力方法が入力方法#3であるならば（ステップS31のYES）、処理部302は、ユーザによって入力される入力パス

10

20

30

40

50

ワードと入力方法#3に対応するパスワード#3とを比較することによって入力パスワードが正しいか否かを判定する(ステップS32)。入力パスワードがパスワード#1に合致する正しいパスワードであることが判定されたならば(ステップS33のYES)、処理部302は、ユーザにシステムの使用を許可すると共に、ユーザに付与すべきセキュリティレベルをセキュリティレベル#3に設定する(ステップS34)。一方、入力パスワードがパスワード#3に合致しないならば(ステップS33のNO)、処理部302は、ユーザがシステムを使用することを禁止する(ステップS26)。

【0066】

以上の説明では、入力されたパスワードが正しいか否かを判定するための認証処理を実行する認証システムがタブレットコンピュータ10内に存在する場合を想定したが、認証処理において使用されるべきパスワードを入力方法毎に変更する機能を含む本実施形態の認証方法は、認証システムが外部に存在するシステム構成にも適用可能である。

【0067】

図12は、サーバ60とタブレットコンピュータ10とを含むシステムの構成を示す。

【0068】

図12のシステムにおいては、サーバ60上に認証システム601が存在する。認証システム601は、図9で説明した認証処理部312およびアクセス権設定部313の機能を実行するように構成されている。

【0069】

タブレットコンピュータ10の処理部302は、入力パスワードを入力するためにユーザによって使用される入力方法を判定し、この判定結果に応じて、認証システム601に、入力パスワードと比較すべき登録パスワードを、複数の入力方法に対応する複数の登録パスワード間で変更させるための処理を実行する。この場合、タブレットコンピュータ10の処理部302は、入力方法の判定結果を認証システム601に送信してもよい。認証システム601は、処理部302から通知される入力方法の判定結果に応じて、入力パスワードと比較すべき登録パスワードを、複数の入力方法に対応する複数の登録パスワード間で変更する。

【0070】

入力パスワードを入力するためにユーザによって使用される入力方法が入力方法#1である場合、認証システム601は、入力パスワードと入力方法#1に対応するパスワード#1とを比較する。また、入力パスワードを入力するためにユーザによって使用される入力方法が入力方法#2である場合、認証システム601は、入力パスワードと入力方法#2に対応するパスワード#2とを比較する。また、入力パスワードを入力するためにユーザによって使用される入力方法が入力方法#3である場合、認証システム601は、入力パスワードと入力方法#3に対応するパスワード#3とを比較する。

【0071】

このように、図12のシステムにおいても、認証処理において使用されるべきパスワードを入力方法毎に変更することができる。

【0072】

以上説明したように、本実施形態においては、少なくとも、文字列を入力するための第1入力方法に対応する第1パスワードと、文字列を入力するための第2入力方法に対応する第2パスワードとを設定することができる。そして、パスワードを入力するためにユーザによって使用される入力方法が第1入力方法または第2入力方法のいずれであるかが判定され、この判定の結果に基づいて、入力パスワードと比較される登録パスワードが、第1入力方法に対応する第1パスワードと第2入力方法に対応する第2パスワードとの間で変更される。したがって、ユーザによって使用される入力方法に応じて、ユーザが入力すべきパスワードを動的に変更することが可能なる。よって、例えば、ユーザは、長い文字列を容易に入力可能な入力方法に対応するパスワードとして長いパスワードを設定し、長い文字列の入力に不向きな入力方法に対応するパスワードとして短いパスワードを設定しておくことにより、どの入力方法を使用する場合であっても、パスワード入力操作を

10

20

30

40

50

容易に行うことが可能となる。

【0073】

なお、本実施形態の各種処理はコンピュータプログラムによって実現することができるので、このコンピュータプログラムを格納したコンピュータ読み取り可能な記憶媒体を通じてこのコンピュータプログラムを通常のコンピュータにインストールして実行するだけで、本実施形態と同様の効果を容易に実現することができる。

【0074】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

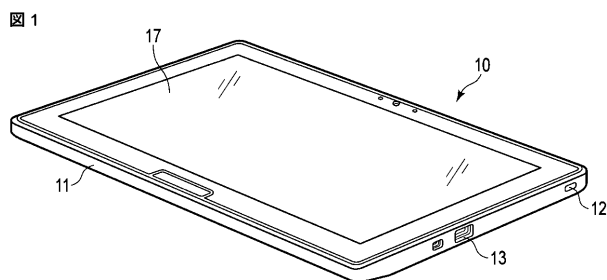
10

【符号の説明】

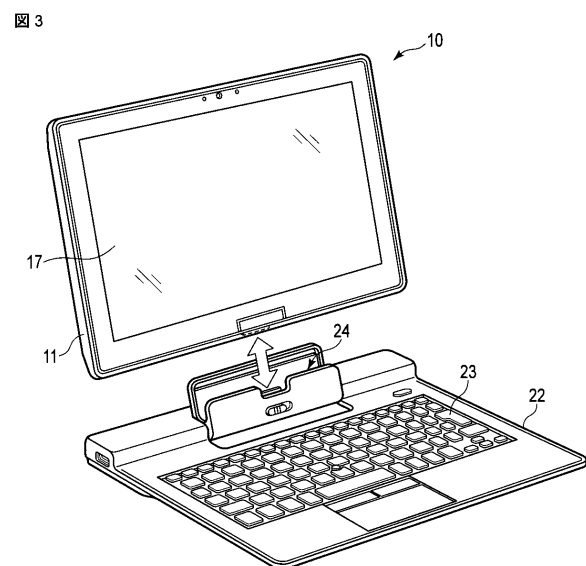
【0075】

10…タブレットコンピュータ、17…タッチスクリーンディスプレイ、21、23…ハードウェアキーボード、101…CPU、203…認証プログラム、301…パスワード設定部、302…処理部、311…判定部、312…認証処理部、313…アクセス権設定部。

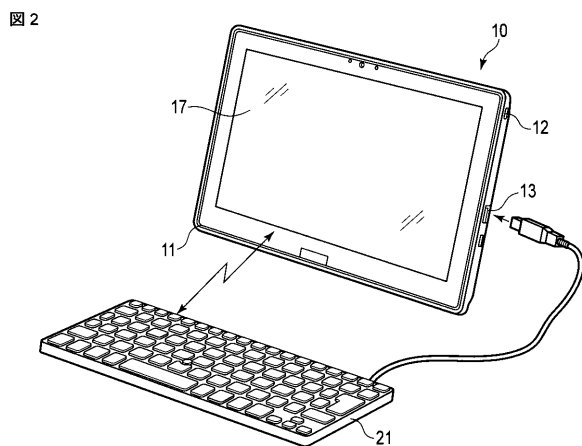
【図1】



【図3】

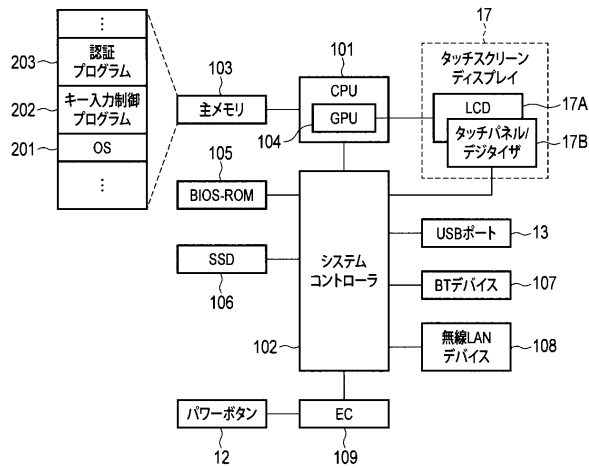


【図2】



【 図 4 】

图 4



【図 5】

图 5



【図 6】

图 6

↩	@	ABC	DEF	Delete
←	GHI	JKL	MNO	→
a ⇔ A	PQRS	TUV	WXYZ	space
A/1/あ	/&_	::; + -	.,! ?	Enter

【图 7】

图 7

Q	W	E	R	T	Y	U	I	O	P	BS
A	S	D	F	G	H	J	K	L	ENTER	
Shift	Z	X	C	V	B	N	M	/	Ctrl	Shift

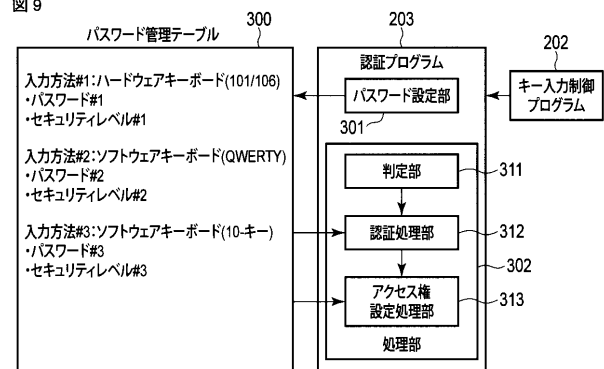
【 図 8 】

图 8

入力方法	入力操作	打鍵速度	タッチタイプ	想定される パスワード	セキュリティ (アタック検定)
ハードウェアキーボード (10/106)	五指・両手	高速	可能	長い文字列、 文字種変更あり	Read/Write
ハードウェア10-キー キーボード	指先・片手	中速	可能	中くさいの長さの 文字列	Read only
ソフトウェア10-キー キーボード(マルチタップ入力)	指先	中速	難	中くさいの長さの 文字列	Read only
ソフトウェア10-キー キーボード(フリック入力)	指先	中速	難	中くさいの長さの 文字列	Read only
ソフトウェアキーボード (QWERTY)	指先	低速	不可	短い文字列	Read only
ソフトウェアキーボード 手書き入力	指先	低速	不可	極短い文字列、 漢字等	Read only
...	...	...	...	...	...

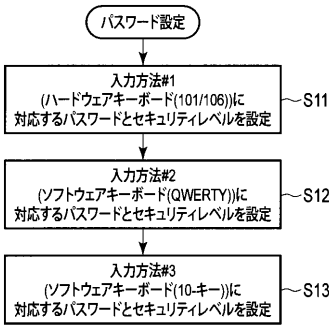
【図 9】

图 9



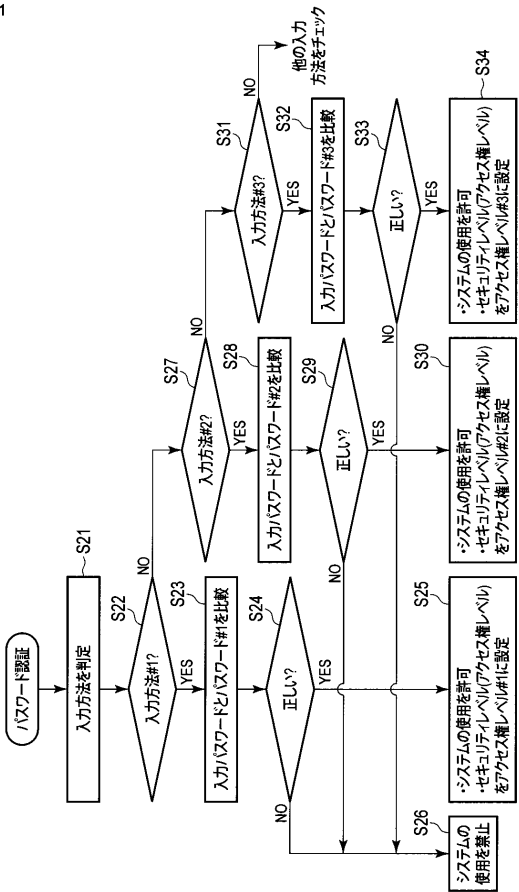
【図 10】

図 10



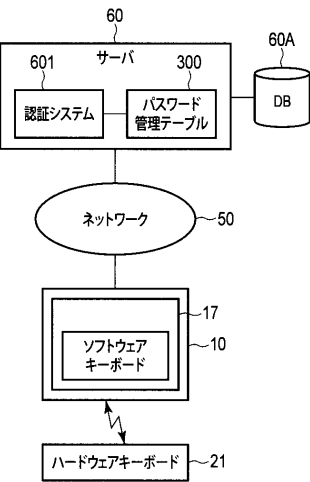
【図 11】

図 11



【図 12】

図 12



フロントページの続き

(51)Int.Cl.		F I			テーマコード (参考)
G 0 6 F	3/0489	(2013.01)	G 0 6 F	3/048	6 1 0
G 0 6 F	3/0488	(2013.01)	G 0 6 F	3/048	6 2 0
G 0 6 F	3/048	(2013.01)	G 0 6 F	3/048	6 5 1 A